Cisco Security Cloud Control: Secure Firewall Management

Cisco Security Cloud Control
Updated NaN,

© 2021-2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

Part I: Introduction.....29

1 Get started with Security Cloud Control Firewall Management.....31

Overview of Security Cloud Control.....32
Products and solutions supported by Security Cloud Control.....33
Overview of Security Cloud Control Firewall Management.....33
Security Cloud Control Firewall Management platform maintenance schedule.....34
Security Cloud Control Firewall Management licenses.....35
More supported devices and licenses.....36
Overview of Cloud-Delivered Firewall Management Center.....37
Determine the Cloud-Delivered Firewall Management Center Version in Security Cloud Control Firewall Management.....38
Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager.....39
Cloud-Delivered Firewall Management Center maintenance schedule.....40
Provision Security Cloud Control Firewall Management.....40
Open Security Cloud Control Firewall Management.....41
Create a new Cisco security cloud sign on account and configure duo multi-factor authentication.....42
Firewall management dashboard.....44

Part II: Configure basic settings.....47

2 Manage Firewall administration in Security Cloud Control Firewall Management.....49

General settings.....50
Enable AI assistant for firewall.....50
Enable the option to auto-accept device changes.....50
Enable Multicloud Defense SCC features.....51
Enable object sharing with Multicloud Defense.....51
Set the default conflict detection interval.....52
Enable scheduled automatic deployments.....52
Manage web analytics.....53
Set the FDM default recurring backup schedule.....53
Auto onboard On-Prem FMCs from Cisco security cloud.....54
Enable event data sharing with talos.....55
View firewall management instance details.....56
Use the Security Cloud Control Firewall Management platform navigator.....56
Manage users and groups within Security Cloud Control organization.....57
Manage API-Only users for Security Cloud Control Firewall Management.....58

View Security Cloud Control notifications....59
User notification preferences....60
View logging settings....62
User roles in Security Cloud Control Firewall Management....62
Read-only role....62
Edit-Only role....63
Deploy-Only role....64
VPN sessions manager role....65
Admin role....65
Super admin role....66

3 Firewall models and software supported....67
Security device management....68
Supported devices, software, and hardware for Security Cloud Control Firewall Management....69
ASA support specifics....70
Cloud device support specifics....71
Switching and routing support specifics....72

4 Onboard devices in Security Cloud Control Firewall Management....73
Secure connectors....75
Secure Device Connector....75

5 Manage objects....101
Introduction to objects....102
Supported object types....102
Shared objects....105
Object Overrides....105
Unassociated objects....106
Compare objects....106
Object filters....107
Delete objects....109
Create an ASA IP address pool....110
Network objects....111
Create or Edit ASA Network Objects and Network Groups....112
Create or Edit a Firepower Network Object or Network Groups....120
Objects Associated with Meraki Devices....129
Create a Local Meraki Network Object....130
Create or Edit a Meraki Network Object or Network Group....131
URL objects....134
Create or Edit an FDM-Managed URL Object....135
Create a Firepower URL Group....135
Geolocation objects....136
Create and Edit a Firepower Geolocation Filter Object....136

DNS group objects....137
Create a DNS Group Object....137
Edit a DNS Group Object....138
Delete a DNS Group Object....138
Certificate objects....139
About certificates....139
Certificate Types Used by Feature....140
Configuring Certificates....140
Uploading Internal and Internal CA Certificates....140
Uploading Trusted CA Certificates....142
Generating Self-Signed Internal and Internal CA Certificates....143
ASA trustpoint objects....144
Add an identity certificate object by using PKCS12....144
Create a self-signed ASA identity certificate object....146
Add an ASA identity certificate object for a Certificate Signing Request (CSR)....148
Add a trusted CA certificate object for ASA....150
Self-Signed and CSR certificate generation based on certificate contents....152
IPsec proposal and IKE policy objects....154
Create or edit an IKEv1 IPsec proposal object....155
Create or edit an IKEv2 IPsec proposal object....156
Global IKE policies....157
Create or edit an IKEv1 policy....157
Create or edit an IKEv2 policy....158
Remote access VPN objects....159
Identity sources for ASA....159
Create a new RA VPN group policy....164
Service objects....169
Create and Edit ASA Service Objects....170
Create and edit Firepower service objects....172
Create or Edit a Meraki Service Object....174
Security group tag group....175
Security Group Tags....175
Create an SGT Group....177
Edit an SGT Group....177
Add an SGT Group to an Access Control Rule....178
ASA time range objects....178
Create an ASA time range object....179
Edit an ASA time range object....179
Troubleshooting Objects....180
Resolve Duplicate Object Issues....180
Resolving Inconsistent or Unused Security Zone Objects....180
Resolve Unused Object Issues....181
Resolve Inconsistent Object Issues....182
Resolve Object Issues in Bulk....184
Unignore objects....184

Part III: Dynamic Attributes Connector.....185

6 About Dynamic Attributes Connector.....187

About the Dynamic Attributes Connector.....188

How It Works.....189

7 Configure the Dynamic Attributes Connector.....191

Enable the dynamic attributes connector.....192

Dashboard.....192

Dashboard of an unconfigured system.....193

Dashboard of a configured system.....194

Add, edit, or delete connectors.....195

Add, edit, or delete dynamic attributes filters.....197

Add, edit, or delete adapters.....198

Connectors.....199

Amazon Web Services connector user permissions and imported data.....200

Amazon Web Services security groups connector–About user permissions.....203

Create an AWS service tags connector.....204

Azure connector–About user permissions and imported data.....205

Create an Azure service tags connector.....208

Create a Multicloud Defense connector.....209

Create a Cisco cyber vision connector.....211

Create a generic text connector.....213

Create a GitHub connector.....217

Google cloud connector user permissions and imported data.....218

Create an office 365 connector.....220

Tenable connector.....221

Create a Webex connector.....224

Create a Zoom connector.....225

Create an adapter.....226

How to create an On-Premises Firewall Management Center adapter.....227

How to create a Cloud-Delivered Firewall Management Center adapter.....228

Create dynamic attributes filters.....228

Dynamic attribute filter examples.....230

Disable the dynamic attributes connector.....230

8 Dynamic Firewall.....233

Dynamic Firewall.....234

How to configure the dynamic firewall.....234

Get required information for Identity Intelligence.....236

Create an identity source and realm for the dynamic firewall.....237

Create a dynamic firewall instance.....238

Associate an identity source with Identity Intelligence....239
Configure Identity Intelligence....240
View system-defined filters....241
View system-defined access control rules....242
Edit the user exclusion list....243
View and edit the system-created access control policy....244
Create dynamic attributes filters....245

9 Use Dynamic Objects in Access Control Policies....247
Dynamic objects in access control rules....248
Create dynamic attributes filters....248
Dynamic attributes rule conditions....249
Create access control rules or DNS rules using dynamic attributes filters....250
Use dynamic objects in DNS policies....251

10 Troubleshoot the Dynamic Attributes Connector....253
Troubleshoot error messages....254
Get your tenant ID....254

Part IV: Manage Secure Firewall ASA....257

11 Onboard Secure Firewall ASA devices....259
Onboard a Secure Firewall ASA....260
Onboard a high availability pair of ASA devices to Security Cloud Control Firewall Management....262
Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management....262
Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management....263
Onboard multiple ASAs to Security Cloud Control Firewall Management....265
Pause and resume onboarding multiple ASA devices....266
Create and import an ASA model to Security Cloud Control Firewall Management....267
Import ASA configuration....267

12 Configure Secure Firewall ASA....269
Update ASA connection credentials in Security Cloud Control Firewall Management....270
Move an ASA from one SDC to Another....270
ASA interface configuration....271
Configure an ASA Physical Interface....271
Add an ASA VLAN Subinterface....275
About ASA EtherChannel Interfaces....280
ASA system settings policy in Security Cloud Control Firewall Management....282
Create an ASA Shared System Settings Policy....282
Configure or Modify Device Specific System Settings....290
Auto Assignment of ASA Devices to a Shared System Settings Policy....291

Filter ASA Shared System Settings Policy....292
Disassociate Devices from Shared System Settings Policy....292
Delete Shared Settings Policy....293
ASA routing in Security Cloud Control Firewall Management....293
About ASA Static Route....294
API tokens....296
ASA file management....297
Upload File to a Single ASA Device....298
Upload File to Multiple ASA Devices....299
Remove Files from ASA....300
Managing ASAs with pre-existing High Availability configuration....301
Configuration Changes Made to ASAs in Active-Active Failover Mode....301
Manage ASA configuration files....302
View a Device's Configuration File....302
Configure DNS on ASA....302
Procedure....303
ASA command line interface....303
Configure ASA Using Security Cloud Control CLI....303
ASA Bulk CLI Use Cases....304
ASA Command Line Interface Documentation....305
Manage the Device Configuration....306

13 Secure Firewall ASA Security Policy Management....311
Manage security policies in Security Cloud Control Firewall Management....312
Manage ASA network security policy....312
About ASA Access Control Lists and Access Groups....312
Create an ASA Access List....313
Add a Rule to an ASA Access List....313
Assign Interfaces to ASA Access Control List....316
Create an ASA Global Access List....316
Share an ASA Access Control List with Multiple ASA Devices....317
Copy an ASA Access Control List to Another ASA....317
Copy a Rule Within or Across ASA Access Lists and Devices....318
Unshare a Shared ASA Access Control List....319
View ASA Access Policies Listing Page....319
Global Search of ASA Access Lists....320
Rename an ASA Access Control List....320
Delete a Rule from an ASA Access Control List....321
Delete an ASA Access Control List....321
Compare ASA network policies....321
Hit rates....322
View Hit Rates of ASA Policies....322
Search and filter ASA network rules in the access list....322
Shadowed rules....324

Find Network Policies with Shadowed Rules....324
Resolve Issues with Shadowed Rules....324

14 Monitor Secure Firewall ASA Events....327
About Security Analytics and Logging (SAL SaaS) for ASA devices....328
How ASA events are displayed in Security Cloud Control....328
Implement secure logging analytics (SaaS) for ASA devices....329
Send ASA syslog events to the Cisco Cloud using a Security Cloud Control macro....331
Create an ASA security analytics and logging (SaaS) macro....331
Requirement: send ASA syslog events to the Cisco cloud using the command line interface....334
Security Cloud Control Command Line Interface for ASA....335
Forward ASA syslog events to the secure event connector....335
Send ASA syslog events to the Cisco cloud using CLI....335
Create a custom event list....338
Include the device ID in Non-EMBLEM format syslog messages....340
NetFlow secure event logging (NSEL) for ASA devices....341
Configuring NSEL for ASA devices by using a CDO macro....342
DELETE NetFlow secure event logging (NSEL) configuration from an ASA....348
Determine the name of an ASA global policy....350
Troubleshooting NSEL data flows....351
Parsed ASA syslog events....355

15 Monitor device health metrics 357
About device health metrics....358
Enable ASA health monitoring....358
Bulk opt in or opt out of device health metrics....359
View the device health metrics dashboard....359
Troubleshooting device health metrics....360

16 Use Cisco Secure Cloud Analytics Portal....361
Provision a Cisco secure cloud analytics portal....362
Review sensor health and Security Cloud Control integration status in Secure Cloud Analytics....363
Cisco secure cloud analytics sensor deployment for total network analytics and reporting....363
Cisco Secure Cloud Analytics alerts from Security Cloud Control....364
Invite users to join your secure cloud analytics portal....365
Cross-launch from Security Cloud Control to Secure Cloud Analytics....365
Cisco secure cloud analytics and dynamic entity modeling....366
Alerts based on firewall events....367
Best practice for triaging open alerts....368
Snooze alerts for later analysis....369
Update the alert for further investigation....369
Review the alert and start your investigation....370
Examine the entity and users....371

Best practice for remediating issues using secure cloud analytics....372
Update and close the alert....373
Modify alert priorities....373

17 Upgrade Secure Firewall ASA....375
Upgrade ASA and ASDM images using Security Cloud Control Firewall Management....376
Upgrade ASA Secure Client Packages....377
Upgrade ASA Secure Client Packages....377
Upgrade bulk ASA and ASDM in Security Cloud Control Firewall Management....380
Upgrade Multiple ASAs with Images from your own Repository....382
Upgrade ASA and ASDM images on a single ASA....384
Upgrade ASA and ASDM images in a high availability pair....385
Workflow for upgrading an ASA high availability pair....386
Workflow....386
Upgrade ASA and ASDM Images in a high availability pair....387
Upgrade an ASA or ASDM using your own image....388

18 Troubleshoot Secure Firewall ASA....391
Troubleshoot a Secure Firewall ASA device....392
ASA fails to reconnect to Security Cloud Control after reboot....392
Disable ASA client-side certificate authentication for onboarding....392
Troubleshoot ASA using CLI commands....395
Troubleshoot missing information on the RA VPN monitoring page....396
ASA real-time logging....396
ASA packet tracer....398
Cisco ASA Advisory cisco-sa-20180129-asa1....401
Confirming ASA running configuration size....402
Container Privilege Escalation Vulnerability Affecting Secure Device Connector: cisco-sa-20190215-runc....403
Limitation: large ASA running configuration files....405

Part V: Manage Secure Firewall Threat Defense with Cloud-Delivered Firewall Management Center....407

19 Onboard a Firewall Threat Defense Device....409
Onboarding methods....410
Maximum Firewall Threat Defense devices supported in Cloud-Delivered Firewall Management Center....411
Requirements: Prerequisites to onboard a device to Cloud-Delivered Firewall Management Center....411
Onboard a device with a CLI registration key....412
Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning....414

Onboard a Firewall Threat Defense Device to On-Prem Firewall Management Center using Zero-Touch Provisioning....416
Onboard Firewall Threat Defense Devices using Device Templates to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning....418
Cloud deployment....419
Configure FTDv enforcement point....420
Configure Multicloud Defense enforcement point....426
Onboard a Secure Firewall Threat Defense Cluster....435
Onboard a chassis....438
Delete Devices from Cloud-Delivered Firewall Management Center....440
Enable Cloud-Delivered Firewall Management Center....440
Troubleshooting....441
Troubleshoot Cloud-Delivered Firewall Management Center Connectivity with TCP....441
Troubleshoot Firewall Threat Defense Device Connectivity....442
Troubleshoot device connectivity loss after Cloud-Delivered Firewall Management Center update....443
Troubleshoot Onboarding a Device to the Cloud-Delivered Firewall Management Center Using the CLI Registration Key....444
Troubleshoot Onboarding a Device to Cloud-Delivered Firewall Management Center Using the Serial Number....444

20 Migrate Threat Defense to Cloud-Delivered Firewall Management Center...451

Firewall Threat Defense migration to Security Cloud Control....452
Evaluation period and manager changes....452
How Firewall Threat Defense licenses are handled during migration....453
End-to-end Firewall Threat Defense migration workflow....453
How Firewall Threat Defense migration to Security Cloud Control works....454
Event and Analytics Management options during Firewall Threat Defense migration....455
Supported features....457
Restriction: unsupported features in firewall threat defense migration....459
Recommendation: migration guidelines and limitations for VPN configuration....460
Supported On-Premises Firewall Management Center and Firewall Threat Defense software versions for migration....461
Prerequisites for migrating Firewall Threat Defense to Security Cloud Control....464
Migrate Firewall Threat Defense to Security Cloud Control....465
Review and manage Firewall Threat Defense migration job....469
Proceed migration process....471
Commit migration changes manually to Security Cloud Control....471
Revert manager ownership to On-Premises Firewall Management Center....472
View migrated devices and analytics-only entries....473
Generate a migration report....475
Remove a completed migration job....475
Configure migration notifications....476
Verify Firewall Threat Defense connectivity with Security Cloud Control....476

Use the troubleshoot feature for failed migrations....478
Troubleshoot Firewall Threat Defense migration failures....479

21 Configure Cloud-Delivered Firewall Management Center-Managed Secure Firewall Threat Defense....487

Security Cloud Control Firewall Management Integrations Page....488
Navigate to the Cloud-Delivered Firewall Management Center in your Security Cloud Control Tenant....491
Enable Cloud-Delivered Firewall Management Center....491

22 Introduction to AgenticOps insights....493

AgenticOps insights....494
AgenticOps licensing requirements....495
Requirements: Prerequisites to use AgenticOps....495
View summary dashboard....495
View AgenticOps insights....498
AgenticOps for On-Premises Firewall Management Center....500
Capacity and traffic insights....500
Analyze capacity trends and forecast resource usage....502
About policy change impact insights....503
Analyze policy change impact....507
Best practices and recommendations....509
Implement best practices and recommendations....510
Feature adoption insights....511
Assess and improve feature adoption....512
Software upgrade insights....513
Manage software upgrades....514
Application insights....516
Detect application outages....516
Compliance insights....517
Generate compliance reports....518
Insight preferences....520
Enable AgenticOps insights....520
Disable AgenticOps insights....521
Manage AgenticOps data sources....521
Capacity and traffic insights....522
Best practices and recommendations insights....523
Policy change impact analyzer insights....523
Policy change impact analyzer insights....524
Enable operational insights....525
Application insights....525
Frequently asked questions about AgenticOps....526
Additional resources....527

23 Introduction to Agent Workforce....529
About Agent Workforce....530
Available agents in Agent Workforce....530
Manage Conversations in Agent Workforce....530
Considerations for agent workforce limitations and deployment....531
VPN agent....531
Benefits of using the VPN agent....532
Use the VPN agent to investigate connectivity issues....532
Best practices for using the VPN agent....533
Example prompts and expected outcomes for the VPN agent....533
Elephant flow agent traffic congestion remediation....534
Benefits of using the elephant flow agent....535
Configure elephant flow remediation workflow....535
Best practices for using the elephant flow agent....536
Firewall insight agent....536
Benefits of using the firewall insight agent....537
How firewall insight agent works....537
Best practices for using the firewall insight agent....538
Example prompts and expected outcomes for the firewall insight agent....538

24 Monitor Cloud-Delivered Firewall Management Center-Managed Threat Defense Device Events....539
Security Analytics and Logging for Firewall Threat Defense....540
SAL (SaaS) for Cloud-Delivered Firewall Management Center-managed devices....540
Requirements and guidelines....540
How Firewall Threat Defense events are displayed in Security Cloud Control using a direct connection....542
Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection....544
Send Cloud-Delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog....545
Enable individual threat defense devices to send events to SAL (SaaS) using a direct connection....547
View AI Defense Events in Security Cloud Control....548

25 FTD Dashboard....549
FTD dashboard....550
View the FTD dashboard....551
FTD dashboard widgets....552
Top intrusion rules widget....552
Top intrusion attackers widget....552
Top intrusion targets widget....552
Top malware signatures widget....552
Top malware senders widget....552
Top malware receivers widget....553

Malware events by disposition widget....553
Network activity widget....553
Event activity widget....553
Access Control Actions Widget....553
Top access control policies widget....553
Top access control rules widget....553
Top devices widget....554
Top users widget....554
Top users by blocked connections widget....554
Top devices with health alerts widget....554
Top loaded devices widget....554
Top web applications widget....554
Top client applications widget....554
Top blocked web applications widget....555
Modify time settings for the FTD dashboard....555

26 Analyze and Remediate Security Policy Anomalies with Policy Analyzer and Optimizer....557

About Policy Analyzer and Optimizer....558
Common Policy Analyzer and Optimizer concepts....559
Requirements: Prerequisites to use Policy Analyzer and Optimizer....560
Enable Policy Analyzer and Optimizer for Security Cloud Control-managed On-Premises Firewall Management Center....562
Policy Analyzer and Optimizer licensing requirements....562
Open Policy Analyzer and Optimizer and select a data source....563
Sync and analysis behavior....563
Search and filter policies in Policy Analyzer and Optimizer....564
Access control policy analysis and optimization....564
Analyze access control policies....565
Access control policy analysis summaries....566
Duplicate rules in access control policy....568
Analyze expired rules in access control policy....569
Mergeable rules in access control policy....570
Overlapping objects in access control policy....571
Policy insights in access control policy....572
Access control policy remediation....573
Download access control analysis report....575
Network address translation policy analysis....575
NAT policy analysis....576
NAT rule sections and comparison behavior....577
Supported NAT address families for Policy Analyzer and Optimizer....577
NAT policy analysis summary....577
Download NAT analysis report....578
NAT policy remediation....579

View NAT remediation history....580
NAT Policy Analyzer and Optimizer and AgenticOps insights....581
Troubleshooting Policy Analyzer and Optimizer....582
Troubleshoot policy analyzer and optimizer analysis issues....582
Policy analyzer and optimizer does not fetch policies....583
Frequently asked questions about Policy Analyzer and Optimizer....583

Part VI: Manage Catalyst SD-WAN Manager Firewall Capabilities....585

27 Integrate Catalyst SD-WAN Manager with Security Cloud Control....587
Catalyst SD-WAN integration with Security Cloud Control Firewall Management....588
System topology diagram....588
Managing Catalyst SD-WAN Manager using Security Cloud Control....590
Minimum software requirements....591
Additional resources....591

28 Onboard Catalyst SD-WAN Manager....593
Onboard Catalyst SD-WAN Manager to Security Cloud Control....594
Deboard Catalyst SD-WAN Manager from Security Cloud Control....596
Alignment of RBAC models of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager....597
Security Cloud Control Firewall Management management of Catalyst SD-WAN NGFW capabilities....598
View intrusion events....600
View malware events....601

29 Configure Next-Generation Firewall Capabilities of Catalyst SD-WAN Manager....603
Catalyst SD-WAN devices....604
Supported operations on Catalyst SD-WAN devices....604
View configuration of Catalyst SD-WAN devices....605
Cross-launch policy groups from Security Cloud Control Firewall Management....606
Catalyst SD-WAN security objects and security profiles....606
Create new Catalyst SD-WAN security objects and security profiles....607
Application lists....608
Data prefix....609
FQDN....609
Geolocation....609
Identity....609
Port....610
Protocol....610
Security group tag....611
IPS signature....611

Allow URL objects....611
Block URL....612
Zones....612
Advanced inspection profile....613
Advanced malware protection....613
Intrusion prevention....614
TLS/SSL decryption....615
TLS/SSL profile....616
URL filtering....617
Modify Catalyst SD-WAN security objects and security profiles....617
Delete Catalyst SD-WAN security objects....618
Filter Catalyst SD-WAN security objects....619
Catalyst SD-WAN NGFW security policies....620
Manage existing Catalyst SD-WAN NGFW security policies....620
Create Catalyst SD-WAN security policies....621
Associate a policy group to Catalyst SD-WAN NGFW policy....626
Deploy policy group from Catalyst SD-WAN Manager....627

30 Monitor Catalyst SD-WAN Events....629
Security Analytics and Logging for Catalyst SD-WAN....630
How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management....630
Requirements and guidelines for SD-WAN integration....632
View Catalyst SD-WAN events in Security Cloud Control Firewall Management....632

Part VII: Manage On-Premises Firewall Management Center....633

31 Onboard an On-Premises Firewall Management Center....635
Onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management....636
Auto onboard an On-Premises Firewall Management Center integrated with Cisco Security Cloud....637
Onboard an On-Premises Firewall Management Center to Security Cloud Control with Credentials....641
Redirect Security Cloud Control to an On-Premises Firewall Management Center....643
Remove an On-Premises Firewall Management Center from Security Cloud Control....644

32 Configure On-Premises Firewall Management Center-Managed Threat Defense Devices....647
Manage On-Premises Firewall Management Center with Security Cloud Control....648
View onboarded On-Premises Firewall Management Center....651
Discover and manage On-Premises Firewall Management Center network objects....652

Part VIII: Manage Cisco Umbrella....655

33 Onboard an Umbrella Organization.....657
Onboarding an umbrella organization.....658
Umbrella license requirements.....658
Generate an API key and secret.....658
Locate umbrella organization ID.....659
Onboard an umbrella organization.....659
Reconnect an Umbrella organization to Security Cloud Control.....660
Cross-launch to the umbrella dashboard.....660

34 Configure an Umbrella Organization.....663
Read Umbrella tunnel configuration.....664
Cross-launch to the Umbrella tunnels page.....664
Configure a SASE tunnel for Umbrella.....665
Edit a SASE tunnel.....666
Delete a SASE tunnel from Umbrella.....666

Part IX: Manage Cisco Meraki.....669

35 Onboard Cisco Meraki MX devices.....671
Onboard Meraki MX to Security Cloud Control.....672
Generate and Retrieve Meraki API Key.....672
Onboard an MX Device to Security Cloud Control.....673
Onboard Meraki templates to Security Cloud Control.....673
Generate and Retrieve Meraki API Key.....674
Onboard an Meraki Template to Security Cloud Control.....674
Update Meraki MX connection credentials.....675

36 Configure Cisco Meraki.....677
Managing Meraki with Security Cloud Control.....678
How does Security Cloud Control communicate with Meraki.....679
Meraki Access Control Policy.....680
Meraki templates.....681

Part X: Manage AWS VPC.....683

37 Onboard AWS VPC.....685
Supported devices, software, and hardware for Security Cloud Control Firewall Management.....686
ASA support specifics.....687
Cloud device support specifics.....688
Switching and routing support specifics.....689

Onboard an AWS VPC....689

38 Configure AWS VPC....693
Manage AWS VPCs with Security Cloud Control Firewall Management....694
Update AWS VPC connection credentials....696
Monitor AWS VPC tunnels using AWS transit gateway....697
View AWS VPC tunnel history....697
AWS VPC Policy....698
AWS VPC Security Groups Rules....698
Create a Security Group Rule....699
Edit a Security Group Rule....700
Delete a Security Group Rule....701

Part XI: Manage Cisco IOS....703

39 Onboard Cisco IOS Devices....705
Onboard a Cisco IOS Device....706
Onboard a Cisco IOS Device....706
Configuration import for offline device management....709

40 Configure Cisco IOS....711
Manage IOS Devices with Security Cloud Control....712
Use the Security Cloud Control Command Line Interface Tool....712
View Device Configuration File....712

Part XII: Manage Network Devices with Generic SSH Access....715

41 Onboard an SSH Device....717
How to onboard an SSH device....718

42 Configure SSH Devices....721
Managing SSH Devices with Security Cloud Control....722
Use the Security Cloud Control Command Line Interface Tool....722
View a Device's Configuration File....722

Part XIII: Establish Secure Connections....725

43 Establish Site-to-Site VPN connection using Security Cloud Control Firewall Management....727
Introduction to Site-to-Site Virtual Private Network....728

Site-to-Site VPN concepts....728
Encryption and Hash Algorithms Used in VPN....729
Site-to-Site VPN configuration for FDM-Managed....732
Create a Site-To-Site VPN Tunnel Between FDM-managed Devices....734
Configure Networking for Protected Traffic Between the Site-To-Site Peers....735
Edit an Existing Security Cloud Control Site-To-Site VPN....737
Exempt Site-to-Site VPN Traffic from NAT....739
Site-to-Site VPN Configuration for Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense....746
Create a Site-to-Site VPN Tunnel Between Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense Devices....746
Create a Site-to-Site VPN Tunnel Between Cloud-Delivered Firewall Management Center-Managed Firewall Threat Defense and Multicloud Defense....748
Create a Site-to-Site VPN Between Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense and Secure Firewall ASA....750
Site-to-Site VPN for Secure Firewall ASA....752
Create a Site-to-Site VPN Tunnel Between Secure Firewall ASA....754
Create a Site-to-Site VPN Between ASA and Multicloud Defense Gateway....756
Exempt Site-to-Site VPN Traffic from NAT....757
Monitor ASA Site-to-Site Virtual Private Networks....764
Check Site-to-Site VPN Tunnel Connectivity....764
Site-To-Site VPN Dashboard....764
Identify VPN Issues....765
Search and filter site-to-site VPN tunnels....767
Onboard an Unmanaged Site-to-Site VPN Peer....768
Viewing AWS Site-to-Site VPN Tunnels....768
View IKE Object Details of Site-To-Site VPN Tunnels....769
View Last Successful Site-to-Site VPN Tunnel Establishment Date....769
View Site-to-Site VPN Tunnel Information....770

44 Establish Remote Access VPN connection using Security Cloud Control Firewall Management....773

Introduction to Remote Access Virtual Private Network....774
Configure Remote Access Virtual Private Network for ASA....774
End-to-End Remote Access VPN Configuration Process for ASA....774
Manage and Deploy Pre-existing ASA Remote Access VPN Configuration....787
Remote Access VPN Certificate-Based Authentication....792
Exempt Remote Access VPN Traffic from NAT....793
Install the AnyConnect Client Software on ASA....794
Modify ASA Remote Access VPN Configuration....795
Modify ASA Connection Profile....795
Upload RA VPN AnyConnect Client Profile....796
Verify ASA Remote Access VPN Configuration....797
View ASA Remote Access VPN Configuration Details....799

45 Configure Firewall for Universal Zero Trust Network Access.....801
Universal Zero Trust Network Access.....802
Onboard Applications in Security Cloud Control.....803
Enable Cloud-Delivered Firewall Management Center Center in Security Cloud Control.....803
Configure Security Devices.....803

Part XIV: Device Operations.....811

46 Manage device configuration.....813
Read, discard, and deploy configuration changes.....815
Read all device configurations.....815
Configuration reading from ASA to Security Cloud Control.....816
Reading changes from firewalls.....817
Preview and deploy configuration changes for all devices.....817
Deploy configuration changes from Security Cloud Control to ASA.....818
Deploy changes to a device.....823
Bulk deploy device configurations.....824
Preview and deploy On-Premises Firewall Management Center configurations.....825
Scheduled automatic deployments.....825
Check for configuration changes.....829
Discard configuration changes.....830
Discard On-Premises Firewall Management Center configuration changes.....831
Out-of-band changes on devices.....831
Synchronizing configurations between Security Cloud Control and device.....832
Conflict detection.....832
Auto-accept changes.....834
Resolve configuration conflicts.....836
Schedule polling for device changes.....838
Schedule a security database update.....839

47 Manage onboarded device settings.....841
Change a device's IP address in Security Cloud Control Firewall Management.....842
Change a device's name in Security Cloud Control Firewall Management.....842
Export a list of devices and services.....843
Export device configuration.....844
External links for devices.....844
Create an external link from your device.....845
Create an External Link to ASDM FDM.....845
Create an external link for multiple devices.....846
Edit or delete external links.....846
Edit or delete external links for multiple devices.....847
Bulk reconnect devices to Security Cloud Control Firewall Management.....847

Moving devices between organizations....848
Device certificate expiry detection....849
Write a device note....849
Delete a device from Security Cloud Control Firewall Management....850
Back up Firewall Threat Defense devices....850
Manage Firewall Threat Defense devices through Security Cloud Control Firewall Management....851
Filter security devices by hardware end-of-life status....852
Security Cloud Control Firewall Management labels and filtering....853
Apply labels to devices and objects....853
Labels and tags in AWS VPC....854
Filters on security devices, policies, and objects page....854
Use Security Cloud Control Firewall Management search functionality....855
Use page level search....855
Global search....856

48 Use the Security Cloud Control Command Line Interface Tool (CLI)....861
Use the command line interface on a single device....862
Use the bulk command line interface....864
Run a CLI macro....867
Export command line interface results....870

49 Manage CLI Templates....873
CLI templates....874
Create a CLI template....874
Edit a CLI template....875
Export a CLI template....875
Delete a CLI template....876

50 Migrate Firewalls with the Migration Tool in Security Cloud Control....877
Firewall migration tool guide audience....878
Firewall migration tool in Security Cloud Control....878
Supported configurations....879
Licenses....881
Initialize a new migration instance....881
Delete a migration instance....882
Demo mode in secure firewall migration tool....882
Migrate Secure Firewall ASA to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control....883
Migrate Microsoft Azure Native Firewall with the Firewall Migration Tool in Security Cloud Control....886
Migrate FDM-Managed Device to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control....888
Migrate Check Point Firewall to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control....891

Migrating Check Point Firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control....894
Migrate Fortinet Firewall with the Firewall Migration Tool in Security Cloud Control....896
Migrating Fortinet firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control....898
Migrate Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control....901
Migrate Secure Firewall ASA to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control....903
Migrate Palo Alto Networks Firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control....905
Related documentation....906

Part XV: Monitor and Analyze....909

51 Events in Security Cloud Control....911
Security Analytics and Logging (SaaS) in Security Cloud Control....912
Event types in Security Cloud Control....912
Troubleshoot network problems using security and analytics logging events....917
Caution: maintain active Cisco security analytics and logging subscription....918

52 Security Analytics and Logging Licenses....919
Security Analytics and Logging licenses....920
Subscribing to a Security Analytics and Logging license....921
View Security Analytics and Logging license information....923
View Security Analytics and Logging Storage usage and event ingest rate....923
Monitor Security Analytics and Logging service availability....925
Extend event storage duration and increase event storage capacity....926
View Security Analytics and Logging alerts....926
Frequently asked questions about Security Analytics and Logging license....927

53 Secure Event Connectors....929
Secure event connectors....930
Secure event connector installation....930
Install a secure event connector on an SDC virtual machine....930
Installing an SEC using a Security Cloud Control image....933
Deploy secure event connector on ubuntu virtual machine....939
SEC installation using VM images....939
Install a secure event connector on an AWS VPC using a terraform module....949
Secure event connector removal....951
Remove an SEC from Security Cloud Control....951
Remove a secure event connector from the secure device connector VM....952
Finding your device's TCP, UDP, and NSEL port used for secure logging analytics (SaaS)....953

54 Monitor Catalyst SD-WAN Events....955
Security Analytics and Logging for Catalyst SD-WAN....956
How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management....956
Requirements and guidelines for SD-WAN integration....958
View Catalyst SD-WAN events in Security Cloud Control Firewall Management....958

55 View Events in Security Cloud Control Firewall Management....959
View live events....960
Play/pause live events....960
View historical events....961
Customize the events view....961
Correlate Firewall Threat Defense event fields and column names....963
Show and hide columns on the event logging page....964
Change the time zone for the event timestamps....966
Create and save customizable event filters....967
Event logging page search and filter functionality....967
Filter live or historical events....968
Filter only NetFlow events....970
Filter for ASA or FDM-Managed Device Syslog Events but not ASA NetFlow Events....970
Combine filter elements....970
Search events using the events logging page....974
Event attributes in security analytics and logging....977
EventGroup and EventGroupDefinition attributes for some syslog messages....978
EventName Attributes for Syslog Events....980
Time attributes in a syslog event....998

56 Integrate Security Cloud Control with Splunk....1001
Splunk Federated Search Integration with Cisco Security Analytics and Logging....1002
How Splunk Federated Search Integrates with Cisco Security Analytics and Logging....1003
How Splunk Federated Search integration works with Cisco Security Analytics and Logging....1004
Requirements for Splunk Federated Search Integration with Cisco Security Analytics and Logging....1006
Enable Splunk Federated Search Integration with Cisco Security Analytics and Logging....1006
Verify Connection Status of Splunk Federated Search with Cisco Security Analytics and Logging...1008
Monitor and Troubleshoot Connection Status of Splunk Federated Search with Cisco Security Analytics and Logging....1009
Disconnect Splunk Federated Search....1010

57 Use Cisco Secure Cloud Analytics Portal....1013
Provision a Cisco secure cloud analytics portal....1014
Review sensor health and Security Cloud Control integration status in Secure Cloud Analytics....1015
Cisco secure cloud analytics sensor deployment for total network analytics and reporting....1015

Cisco Secure Cloud Analytics alerts from Security Cloud Control....1016
Invite users to join your secure cloud analytics portal....1017
Cross-launch from Security Cloud Control to Secure Cloud Analytics....1017
Cisco secure cloud analytics and dynamic entity modeling....1018
Alerts based on firewall events....1019
Best practice for triaging open alerts....1020
Snooze alerts for later analysis....1021
Update the alert for further investigation....1021
Review the alert and start your investigation....1022
Examine the entity and users....1023
Best practice for remediating issues using secure cloud analytics....1024
Update and close the alert....1025
Modify alert priorities....1025

58 Monitor Remote Access Virtual Private Network Sessions from Secure Firewall ASA and Firewall Threat Defense....1027

Remote access VPN session monitoring....1028
Monitor live AnyConnect remote access VPN sessions....1028
Monitor historical AnyConnect remote access VPN sessions....1030
Search and filter remote access VPN sessions....1031
Customize the remote access VPN monitoring view....1032
Export remote access VPN sessions to a CSV file....1033
View the remote access VPN dashboard....1033
Disconnect Remote Access VPN Sessions of an ASA User....1034
Disconnect Remote Access VPN Sessions on FDM-Managed Device....1034
Disconnect remote access VPN sessions on FTD....1035

59 Monitor and report change logs, workflows, and jobs....1037

Change logs in Security Cloud Control....1038
Change log entries after deploying to an ASA....1039
Change log entries after reading changes from an ASA....1040
View change log differences....1041
Change request management....1042
Enable change request management....1043
Create a change request....1043
Associate a change request with a change log event....1044
Search for change log events with change requests....1045
Search for a change request....1045
Filter change requests....1045
Clear the change request toolbar....1046
Clear a change request associated with a change log event....1046
Delete a change request....1047
Disable change request management....1047

Manage change requests and associate change log events....1047
Export the change log....1048
Differences between change log capacity in Security Cloud Control and size of an exported change log....1049
Monitoring Jobs in Security Cloud Control....1050
Reinitiate a bulk action....1051
Cancel a bulk action....1051
Monitor workflows in Security Cloud Control....1051

60 Smart Licensing Dashboard....1053
Smart licensing dashboard....1054
View smart licensing dashboard....1054

Part XVI: Troubleshoot....1057

61 Troubleshooting....1059
Troubleshoot a Secure Firewall ASA device....1060
ASA fails to reconnect to Security Cloud Control after reboot....1060
Disable ASA client-side certificate authentication for onboarding....1060
Troubleshoot ASA using CLI commands....1063
Troubleshoot missing information on the RA VPN monitoring page....1064
ASA real-time logging....1064
ASA packet tracer....1066
Confirming ASA running configuration size....1069
Limitation: large ASA running configuration files....1070
Troubleshoot a secure device connector....1071
Resolve unreachable SDC status....1071
Troubleshoot SDC status not active on Security Cloud Control after deployment....1071
Update the changed IP address of the SDC in Security Cloud Control....1072
Troubleshoot device connectivity with the SDC....1072
Resolve intermittent or no connectivity with SDC....1073
Container privilege escalation vulnerability affecting secure device connector: cisco-sa-20190215-runc....1074
Invalid system time....1077
Upgrade SDC version lower than 202311****....1078
Certificate or connection errors with AWS servers....1079
Secure event connector troubleshooting....1081
Troubleshoot SEC onboarding failures....1081
Troubleshoot secure event connector registration failure....1083
Collect troubleshooting logs for secure event connector....1084
Troubleshooting: SEC status is inactive in Security Cloud Control....1085
The SEC is online, but there are no events in Security Cloud Control Event Logging Page....1085
Remove an SEC from your host....1086

Use health check to learn the state of your secure event connector....1087
Troubleshoot Security Cloud Control....1089
Troubleshooting access and certificates....1089
Device connectivity states....1091
Troubleshoot device unregistered....1092
Troubleshoot insufficient licenses....1093
Troubleshoot invalid credentials....1094
Troubleshoot New Certificate Issues....1094
Troubleshoot onboarding error....1102
Resolve the conflict detected status....1102
Resolve the not synced status....1104

62 FAQ and support....1105
Security Cloud Control....1106
FAQ about onboarding devices to Security Cloud Control....1106
FAQs About Onboarding Secure Firewall ASA to Security Cloud Control....1106
FAQs About Onboarding Secure Firewall Threat Defense to Cloud-Delivered Firewall Management Center....1106
FAQs About On-Premises Firewall Management Center....1107
FAQs About Onboarding Meraki Devices to Security Cloud Control....1107
FAQs About Onboarding SSH Devices to Security Cloud Control....1107
FAQs About Onboarding IOS Devices to Security Cloud Control....1107
Device types....1108
Security....1109
End-of-Support for management of Secure Firewall Threat Defense devices, Version 7.0.*x*, managed by Cloud-Delivered Firewall Management Center....1109
Troubleshooting....1111
Terminologies and definitions used in Zero-Touch Provisioning....1111
Policy optimization....1112
Connectivity....1112
Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI....1113
About Data Interfaces....1116
How Security Cloud Control processes personal information....1117
Contact Security Cloud Control support....1117
Export The Workflow....1117
Open a Support Ticket with TAC....1118
Security Cloud Control Service Status Page....1120

Part XVII: Appendix....1121

63 Security and Internet Access....1123
Internet access requirements....1124

64 Terraform.....1125
About Terraform.....1126

65 Open Source and 3rd Party License Attribution.....1129
Open source and third-party license in SDC.....1130

Part I

Introduction

Topics:

- Get started with Security Cloud Control Firewall Management

Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator) is a cloud-based platform that unifies and simplifies security policy management across Cisco firewalls and devices. It streamlines policy consistency, offers intuitive and advanced interfaces, and reconciles configuration changes across multiple device managers.

1 Get started with Security Cloud Control Firewall Management

Topics:

- Overview of Security Cloud Control
- Overview of Security Cloud Control Firewall Management
- Overview of Cloud-Delivered Firewall Management Center
- Provision Security Cloud Control Firewall Management
- Open Security Cloud Control Firewall Management
- Create a new Cisco security cloud sign on account and configure duo multi-factor authentication
- Firewall management dashboard

Provision Firewall management for your organization, open the Firewall application, and review the dashboard sections that help you monitor and manage your environment.

Overview of Security Cloud Control

Describes Cisco Security Cloud Control as a unified platform for onboarding, managing, and navigating integrated Cisco security products.

Security Cloud Control is a security platform that

- allows you to manage your security products and achieve security outcomes from a single integrated interface
- provides streamlined integration of security products with a single claim code for all purchased subscriptions, and
- enables intuitive navigation between products with standardized platform menu and toolbar for all integrated products.

Core services and features

Security Cloud Control provides these core services to all integrated products on the platform:

- **Platform Management**: Common services such as managing role-based access control, claiming subscriptions and standardized regional deployment of product instances are provided by Security Cloud Control. By centralizing these functions, Security Cloud Control ensures a consistent user experience in provisioning and managing access across all Cisco security products managed from the platform. Administrators reach these common services from the Platform Management menu in the main navigation bar of Security Cloud Control.
- **AI Assistant**: The Cisco AI Assistant in Security Cloud Control is designed to streamline security operations by providing AI-driven insights, automation, and contextual guidance. It assists administrators in managing security policies, troubleshooting issues, and optimizing configurations across Cisco's security products, including Firewall, Duo, Hypershield, and Secure Access. By leveraging natural language processing and cross-platform intelligence, the assistant enhances efficiency, accelerates incident response, and simplifies security workflows.
- **Global Search**: Search for device names, policy names, object names, or values such IP addresses and CIDR blocks in supported objects managed by Security Cloud Control Firewall Management.
- **Shared Objects**: Creating and managing objects that can be shared across devices and policies.
- **Unified documentation portal**: A documentation "Help" experience where all documentation is accessible in one portal.

Within Security Cloud Control, user and group management occurs at the platform level. Roles are assigned to these users and groups to define their privileges for administering Security Cloud Control and the integrated products.

Integrating security products in the platform is a streamlined experience. After purchasing your subscriptions to Cisco security products, you receive a single email, with a single claim code for all the subscriptions you purchased. Entering the claim code in your new Security Cloud Control organization provisions all your products to Security Cloud Control simultaneously.

From Security Cloud Control, you can manage all of these security products:

- AI Defense
- Firewall Management
- Mesh Policy Engine
- Multicloud Defense
- Secure Access

From Security Cloud Control, you can open these security products. After they open, these products operate as standalone products and you cannot manage them through Security Cloud Control. You can only claim or deactivate the licenses of such products from Security Cloud Control.

In the Security Cloud Control toolbar, click the nine-dot menu  to launch these products:

- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Cisco XDR
- Cisco Duo

Products and solutions supported by Security Cloud Control

Lists products and solutions supported by Security Cloud Control and how they can be integrated or launched from the platform.

Currently, these are the products you can integrate with Security Cloud Control.

AI Defense: AI Defense addresses risks for users and providers of AI. Using network visibility and enforcement points in the Security Cloud Control, AI Defense adds detection and enforcement measures to discover sanctioned and unsanctioned AI workloads, applications, models, data, and user access across your distributed cloud environment. For organizations that develop and deliver AI-powered services, AI Defense detects vulnerabilities in your AI models before they're delivered. For your running AI applications, AI Defense guardrails intercept rapidly evolving threats, including prompt injections, denial of service, and data leakage. See AI Defense Documentation for more information.

Security Cloud Control Firewall Management: Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator) is a cloud-based security policy manager that simplifies and unifies policy across your Cisco firewalls and other devices. See Firewall in Security Cloud Control Documentation for more information.

Multicloud Defense: Multicloud Defense provides a simplified and highly automated approach to multicloud security. This solution allows organizations to manage and secure their multicloud environments using a single SaaS delivered control plane, and centralized or distributed PaaS-delivered data plane architectures. Multicloud Defense provides continuous visibility, unified protection and dynamic policy updates across all major cloud providers, thereby eliminating the need for separate point solutions for each cloud provider. See Multicloud Defense Documentation for more information.

Secure Access: Cisco Secure Access is a cloud-based platform that provides multiple levels of defense against internet-based threats. Connect securely to the internet, SaaS apps, and private digital resources from your organization's network or roaming off-network. Using policy rules, configure and enforce security controls on collections of resources, users, and devices. See Secure Access Documentation for more information. Secure Access subscriptions also include the Identity Intelligence integration via Security Cloud Control at no additional charge—this does not include access to the standalone Identity Intelligence dashboard. For more information, see Integrate Cisco Identity Intelligence with Secure Access.

Cisco XDR (Extended Detection and Response): Cisco XDR is a cloud-native, extensible security solution designed to simplify security operations and accelerate incident response. It collects and analyzes telemetry from multiple sources—including endpoint, network, firewall, email, identity, and DNS—to detect sophisticated threats with enriched context and threat intelligence from Cisco Talos.

Cisco XDR prioritizes threats based on potential risk and impact, reduces false positives, and provides AI-driven guidance and automation to streamline investigations and remediation. This unified approach enables Security Operations Center (SOC) teams to act faster, improve productivity, and build security resilience by integrating both Cisco and third-party security tools in a multi-vector, multi-vendor environment. See Cisco XDR Help Center for more information.

Overview of Security Cloud Control Firewall Management

Describes a cloud-based security policy manager that simplifies and unifies security policies across Cisco firewalls and devices, helping optimize configurations by identifying inconsistencies and providing tools to maintain policy consistency.

Security Cloud Control Firewall Management, formerly Cisco Defense Orchestrator, simplifies security policy management in distributed environments. It helps you maintain consistent policies across managed firewalls and devices. In Security Cloud Control, **Firewall** appears under **Products**.

Security Cloud Control Firewall Management helps optimize security policies by identifying inconsistencies and providing tools to resolve them. It also supports object sharing, policy sharing, and configuration templates so that you can apply consistent settings across devices.

Security Cloud Control Firewall Management can coexist with local device managers such as Adaptive Security Device Manager (ASDM). It tracks configuration changes that other managers make, then reconciles differences when needed.

The platform includes a guided Day 0 experience to help you onboard Threat Defense devices to your On-Premises Firewall Management Center or to Cloud-Delivered Firewall Management Center. It highlights key features and helps you activate and configure them.

Device onboarding requirements

Before you onboard a device, complete these prerequisites:

- Complete the installation wizard.
- License the device.

After you complete those prerequisites, use the Security Cloud Control Firewall Management onboarding wizard to onboard the device.

Keep these restrictions in mind:

- After you onboard devices to a Security Cloud Control Firewall Management associated with an organization, you cannot migrate those devices to another organization.
- To move devices to a new organization, you must re-onboard them to the new organization.

Manage your Devices with Security Cloud Control

See how Security Cloud Control Firewall Management can manage various device types:

- Manage On-Premises Firewall Management Center with Security Cloud Control on page 648
- Managing Secure Firewall Threat Defense with Cloud-Delivered Firewall Manager
- Multicloud Defense User Guide
- Manage IOS Devices with Security Cloud Control on page 712
- Managing SSH Devices with Security Cloud Control on page 722
- Managing Meraki with Security Cloud Control on page 678
- Manage AWS VPCs with Security Cloud Control Firewall Management on page 694

Cisco online privacy statement

Cisco Systems, Inc. and its subsidiaries (collectively referred to as "Cisco") are committed to protecting your privacy and providing you with a positive experience on Cisco websites and while using Cisco products and services ("Solutions"). Read the Cisco Online Privacy Statement carefully to get a clear understanding of how Cisco collects, uses, shares, and protects your personal information.

Security Cloud Control Firewall Management platform maintenance schedule

Provides the weekly maintenance schedule for Security Cloud Control Firewall Management platform updates and guidance for maintaining uninterrupted service during maintenance periods.

Security Cloud Control Firewall Management updates its platform every week with new features and quality improvements. Updates are made during a 3-hour period according to this schedule:

Day of the week	Time of day (24-hour time, UTC)
Thursday	09:00 UTC - 12:00 UTC

During the Security Cloud Control Firewall Management upgrade period, you can still access your organization and the Cloud-Delivered Firewall Management Center. Additionally, the devices that you have onboarded to Security Cloud Control Firewall Management continue to enforce their security policies.

Note

- During the maintenance period of the Security Cloud Control Firewall Management, refrain from creating or deploying configurations to the devices it manages.
- If there is any issue that stops Security Cloud Control Firewall Management from communicating, Cisco addresses that issue in all the affected tenants as quickly as possible, even if it is outside the maintenance window.

Security Cloud Control Firewall Management licenses

Describes the licensing requirements for device management, including base subscriptions for organization entitlement and device-specific licenses, with flexible term-based plans and Cisco TAC support.

Security Cloud Control Firewall Management requires a base subscription for organization entitlement and device licenses for managing devices. You can buy one or more Security Cloud Control Firewall Management base subscriptions based on the number of tenants you require and device licenses based on the device model number and the quantity. In other words, purchasing the base subscription provides you with a Security Cloud Control Firewall Management organization. For every device you choose to manage using Security Cloud Control Firewall Management, you need separate device licenses.

For the purposes of planning your deployment, note that each Security Cloud Control Firewall Management tenant can manage approximately 500 devices through the Secure Device Connector (SDC) and any number of devices using the cloud connector. See Secure Device Connector (SDC) for more information.

To onboard and manage devices from Security Cloud Control Firewall Management, you must purchase a base subscription and device-specific, term-based subscriptions based on the devices you want to manage.

Subscriptions

Security Cloud Control Firewall Management subscriptions are term-based:

- **Base**: Offers subscriptions for one, three, and five years, and provides entitlement to access the Security Cloud Control Firewall Management organization and onboard adequately licensed devices.
- **Device License**: Offers subscriptions for one, three, and five years for any supported device you choose to manage. For example, you can choose to manage a Cisco Firepower 1010 device using Security Cloud Control Firewall Management for three years if you purchase a three-year software subscription for the Cisco Firepower 1010 device.

See Software and Hardware Supported by Security Cloud Control Firewall Management for more information on Cisco security devices that Security Cloud Control Firewall Management supports.

When managing your firewalls with Security Cloud Control Firewall Management, you can combine Security Analytics and Logging with your Security Cloud Control Firewall Management subscription, or you can obtain Security Analytics and Logging entitlement as a separate subscription. For more information about Security Analytics and Logging subscriptions, see Security Analytics and Logging licenses on page 920.

Important

You do not require two separate device licenses to manage a high-availability device pair in Security Cloud Control Firewall Management. If you have a Secure Firewall ASA (ASA)orSecure Firewall Threat Defense (FTD) high-availability pair, purchasing one ASAorFTD device license is sufficient because Security Cloud Control Firewall Management considers the pair of high-availability devices as one single device.

Note

- Catalyst SD-WAN does not require an additional license for integration with Security Cloud Control Firewall Management. Customers with Cisco Digital Network Architecture (DNA) or WAN Essentials licenses can use these existing licenses for integration without needing any other license.
-

Note

You cannot manage Security Cloud Control Firewall Management licensing through the Cisco Smart Licensing portal.

Software subscription support

The Security Cloud Control Firewall Management base subscription includes software subscription support that is valid for the term of the subscription and provides access to software updates, major upgrades, and Cisco Technical Assistance Center (TAC) at no extra cost. While software support is selected by default, you can also leverage Security Cloud Control Firewall Management solution support based on your requirement.

More supported devices and licenses

Lists additional devices and licensing requirements that Security Cloud Control supports beyond Secure Firewall Threat Defense devices.

In addition to supporting Secure Firewall Threat Defense devices through the Cloud-Delivered Firewall Management Center, Security Cloud Control also manages these devices:

- Cisco Secure Firewall ASA
- On-premises Cisco Secure Firewall Management Center
- Cisco Meraki Security Appliance
- Cisco IOS devices
- Devices accessible using SSH
- Amazon Web Services (AWS) virtual private cloud (VPC)

- Umbrella Organization

You will need a Security Cloud Control base entitlement license and a license specific to the device you want to manage.

Overview of Cloud-Delivered Firewall Management Center

Explains Cloud-Delivered Firewall Management Center, including Threat Defense management, migration, onboarding, high availability, security analytics, and licensing.

Cloud-Delivered Firewall Management Center is a software-as-a-service product that

- manages Secure Firewall Threat Defense devices through Security Cloud Control Firewall Management
- provides many of the same functions as an On-Premises Firewall Management Center, and
- has the same appearance and behavior as an On-Premises Firewall Management Center and uses the same FMC API.

Migration and onboarding details

A migration wizard is available to help you migrate Threat Defense devices from an On-Premises Firewall Management Center to Cloud-Delivered Firewall Management Center.

Devices must run one of these Threat Defense software releases before you migrate them:

- Minimum On-Premises Firewall Management Center: 7.2
- Minimum Threat Defense: 7.2.x (not supported for Version 7.1)

Threat Defense 7.1 releases are not supported for migration.

You onboard Threat Defense devices in Security Cloud Control Firewall Management by using familiar methods, such as entering the serial number or using a CLI command that includes a registration key.

After onboarding:

- The device appears in both Security Cloud Control Firewall Management and Cloud-Delivered Firewall Management Center.
- You configure the device in Cloud-Delivered Firewall Management Center.
- In Security Cloud Control Firewall Management, you can review device information such as version, configuration status, connectivity, health status, and node status.
- When you click the health status in Security Cloud Control Firewall Management, the platform opens the device health monitoring page in the Cloud-Delivered Firewall Management Center user interface.

Because it is a SaaS product, the Security Cloud Control Firewall Management operations team deploys and maintains the Cloud-Delivered Firewall Management Center software. As new features are introduced, the operations team updates the Cloud-Delivered Firewall Management Center in your Security Cloud Control Firewall Management organization.

Availability and security analytics

Security Cloud Control Firewall Management supports high availability for the Threat Defense devices that it manages through the data interface. This feature is supported for devices that run software version 7.2 or later.

You can analyze security events from onboarded threat defense devices by using either Security Analytics and Logging (SaaS) or Security Analytics and Logging (On-Premises):

- Security Analytics and Logging (SaaS) stores events in the cloud, and you view those events in Security Cloud Control Firewall Management.

- Security Analytics and Logging (On-Premises) stores events on an on-premises Secure Network Analytics appliance, and analysis occurs in the On-Premises Firewall Management Center.

In both cases, you can still send logs directly from firewalls to a log collector of your choice.

Licenses

The license for Cloud-Delivered Firewall Management Center is a per-device-managed license and there is no license required for the Cloud-Delivered Firewall Management Center itself. Existing Secure Firewall Threat Defense devices re-use their existing smart licenses and new Secure Firewall Threat Defense devices provision new smart licenses for each feature implemented on the Secure Firewall Threat Defense For more information, see Cloud-Delivered Firewall Management Center license.

Existing customers can continue to use Security Cloud Control for managing other device types like, the Secure Firewall ASA, Meraki, Cisco IOS devices, Umbrella, and AWS virtual private clouds. If you use Security Cloud Control to manage a Secure Firewall Threat Defense device configured for local management with Firepower Device Manager, you can continue to manage them with Security Cloud Control as well.

To learn how to have a Cloud-Delivered Firewall Management Center provisioned on your tenant, see Enable Cloud-delivered Firewall Management Center on Your Security Cloud Control Tenant.

Determine the Cloud-Delivered Firewall Management Center Version in Security Cloud Control Firewall Management

Configure access to view the Cloud-Delivered Firewall Management Center version information in Security Cloud Control Firewall Management.

Information about the Cloud-Delivered Firewall Management Center version is required primarily for migration planning, feature support verification, troubleshooting, licensing, and operational management.

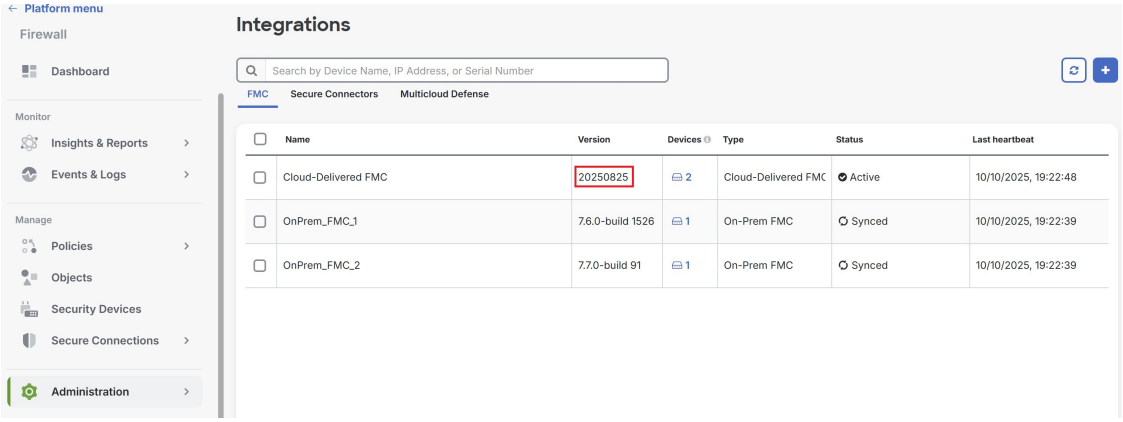
Use this procedure to determine the current version of your Cloud-Delivered Firewall Management Center in Security Cloud Control Firewall Management.

Before you begin

Enable Enable Cloud-Delivered Firewall Management Center in your organzation.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**.
3. Under the **FMC** tab, the version is displayed under the **Version** column.



For more information about Cloud-Delivered Firewall Management Center versions, see Release Notes for Cloud-Delivered Firewall Management Center.

The Cloud-Delivered Firewall Management Center version information is now visible in the Version column under the FMC tab.

Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager

Configure Cloud-Delivered Firewall Management Center registration with Cisco Smart Software Manager for Smart Licensing to enable export-controlled features and prevent deployment interruptions.

Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager to:

- Enable export-controlled features such as Remote access VPN and SSL VPN
- Prevent deployment interruptions after the 90-day evaluation period
- Ensure compliance and access to all licensed features

Cloud-Delivered Firewall Management Center is included with the base subscription and trial for Security Cloud Control Firewall Management and is provisioned with a 90-day evaluation license upon deployment. Features requiring export encryption remain disabled until registration with Cisco Smart Software Manager (CSSM) is completed. After the evaluation period ends, manually triggered or scheduled deployments are blocked until registration is completed.

Before you begin

- Ensure you have a Cisco Smart Software Manager account
- Access to Cloud-Delivered Firewall Management Center interface

Follow these steps to register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager:

Procedure

---

1. Create or access your Smart Account.

   Ensure you have a Cisco Smart Software Manager account. If you do not have one, create it at Smart Software Manager.

2. Generate a registration token or use an existing valid registration token.

   In the Smart Software Manager, use an existing valid registration token or generate a registration token for the virtual account to which you want to register the Cloud-Delivered Firewall Management Center.

   a) Navigate to **Inventory > New Token**.
   b) Check the **Enable Export Compliance** check box.
   c) Enter a description and set an expiration (Cisco recommends 30 days).
   d) Create and copy the token.

3. Register Cloud-Delivered Firewall Management Center with the token.
   a) Log in to the Cloud-Delivered Firewall Management Center interface.
   b) Navigate to **System > Licenses > Smart Licenses**.
   c) Click **Register** and paste the registration token into the **Product Instance Registration Token** field.
   d) Ensure there are no extra spaces or blank lines before or after the token.
   e) Click **Apply Changes**.

4. Verify registration status.

After registration, verify the license status under **System > Licenses > Smart Licenses** to confirm successful registration, license application, and that "Export-Controlled Features" are enabled.

Cloud-Delivered Firewall Management Center is successfully registered with Cisco Smart Software Manager, enabling all licensed features including export-controlled features such as Remote Access VPN and SSL VPN. The license is automatically applied upon registration and deployment restrictions are removed.

Cloud-Delivered Firewall Management Center maintenance schedule

Provides details about Cloud-Delivered Firewall Management Center maintenance schedule, including notification procedures and timing.

Customers who have a Cloud-Delivered Firewall Management Center deployed on their organization are notified approximately 1 week before Security Cloud Control updates the Cloud-Delivered Firewall Management Center environment.

Super Admin and Admin users of the tenant are notified by email. Security Cloud Control also displays a banner on its home page notifying all users of upcoming updates.

Note

- During the maintenance period of the Cloud-Delivered Firewall Management Center, refrain from creating or deploying configurations to the devices it manages.
- If there is any issue that stops Security Cloud Control or Cloud-Delivered Firewall Management Center from communicating, that failure is addressed on all affected tenants as quickly as possible, even if it is outside the maintenance window.

Provision Security Cloud Control Firewall Management

Configure a Security Cloud Control Firewall Management by setting up your organization, enabling Firewall management, claiming your subscription, and preparing your environment for secure policy configuration and deployment.

This task enables you to provision a **Firewall** within Security Cloud Control for secure network management.

Provisioning a firewall involves enabling the firewall feature for your organization, claiming your subscription, and preparing your environment for secure network management. The process ensures that your organization's firewall services are correctly set up and ready for configuration and policy deployment.

Procedure

---

1. Sign in to Security Cloud Control using Security Cloud Sign on account. Create an account if you do not have one.

   To create a Security Cloud Sign On account, you need to provide an email address where the account activation email will be sent. Every Security Cloud Sign On user account is required to use Duo multi-factor authentication (MFA). Duo MFA is included with Security Cloud Sign On account at no charge.

   For information on how to create a Security Cloud Sign On account, see Security Cloud Sign On..

> **Note**
>
> If you already have a Security Cloud Sign on account, see Signing in to Security Cloud Control.

2. Create an organization and set a preferred region. See Create an Organization.
3. (Optional) Enable Firewall management in Security Cloud Control.

   If you have a new Security Cloud Control organization and are entitled to Firewall in Security Cloud Control but do not yet have your subscription code, you will be able to enable the Firewall application using this procedure. For more information, see Enable Security Cloud Control Firewall Management.

4. After you receive the subscription code, enter the claim code that you receive in the Security Cloud Control welcome email in order to claim subscriptions for the product instances. For more information, see Claim your Product Subscription. Activate the new product instances.

   > **Note**
   >
   > In case you need to understand the claim subscription process, see the Overview of the Claim Subscription.

5. Add a domain to your product organization. For more information, see Add and Claim your Domain.
6. Integrate the identity provider with the Security Cloud Sign On account. For more information, see Integrate an Identity Provider.
7. Create users and groups; assign them roles for precise product management and control. For information on role-based access, see Role-based Access Control.

Your firewall is now provisioned and ready for configuration and policy deployment within Security Cloud Control.

Open Security Cloud Control Firewall Management

Configure access to the Firewall application from Security Cloud Control Firewall Management after your account and firewall management service are provisioned.

This task enables you to access the Firewall application within Security Cloud Control to manage your firewall configuration and policies.

This topic describes the steps to navigate to firewall application in Security Cloud Control

Ensure that you have a Cisco Security Cloud Sign-On account and that the firewall is provisioned within Security Cloud Control for your organization. For more information, see Provision Security Cloud Control Firewall Management

Procedure

1. Open Security Cloud Control at https://security.cisco.com/.
2. Sign in with your Security Cloud Sign On credentials and multi-factor authentication options that you established when creating your account.

3. From the Security Cloud Control Home page, click **Firewall**.

The Firewall application opens, providing access to firewall management capabilities within Security Cloud Control.

Create a new Cisco security cloud sign on account and configure duo multi-factor authentication

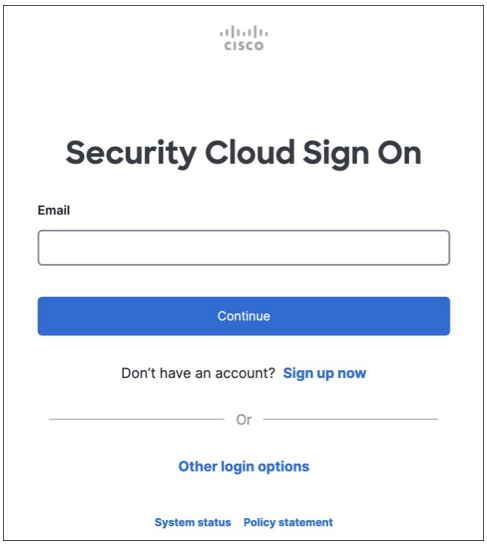
Configure a Cisco Security Cloud Sign On account with Duo multi-factor authentication, optional Google Authenticator, and account recovery options.

This task creates a new Cisco Security Cloud Sign On account with secure multi-factor authentication to protect access to Cisco security services.

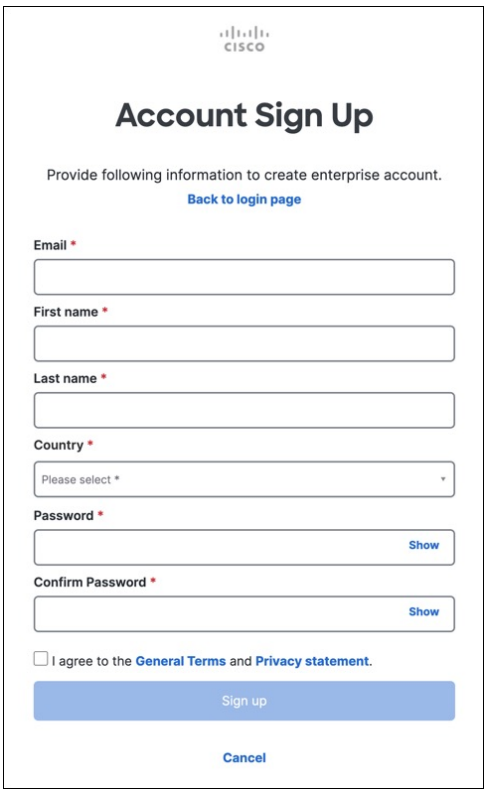
The initial sign-on workflow is a four-step process. You need to complete all four steps.

Procedure

1. **Sign Up for a New Cisco Security Cloud Sign On Account**.
   a. Open https://security.cisco.com.
   b. At the bottom of the sign in screen, click **Sign up now**.



   c. Provide the following information to create enterprise account.



Here are some tips:

- **Email**: Enter the email address that you will eventually use to log in to Security Cloud Control.
- **Password**: Enter a strong password.

d. Click **Sign up**.

Cisco sends you a verification email to the address you registered with. Open the email and click **Activate account**.

2. Set up Multi-factor Authentication Using Duo

We recommend using a mobile device when setting up multi-factor authentication.

a. In the **Set up multi-factor authentication** screen, click **Configure factor**.

b. Click **Start setup** and follow the prompts to choose a mobile device and verify the pairing of that mobile device with your account.

For more information, see Duo Guide to Two Factor Authentication: Enrollment Guide. If you already have the Duo app on your device, you'll receive an activation code for this account. Duo supports multiple accounts on one device.

c. At the end of the wizard click **Continue to Login**.

d. Log in to Cisco Security Cloud Sign On with the two-factor authentication.

3. (Optional) Setup Google Authenticator as an additional authenticator

a. Choose the mobile device you are pairing with Google Authenticator and click **Next**.

b. Follow the prompts in the setup wizard to setup Google Authenticator.

4. Configure Account Recovery Options for your Cisco Security Cloud Sign On

a. Choose a recovery phone number for resetting your account using SMS.

b. Choose a security image.

c. Click **Create My Account**.

You have successfully created a Cisco Security Cloud Sign On account with multi-factor authentication enabled and account recovery options configured.

Firewall management dashboard

Describes the central hub for monitoring and managing tenant-level details across various security and operational categories.

The Firewall Management dashboard is a central monitoring interface that

- provides tenant-level insights across security and operational categories
- offers customizable widgets for critical insights and actions
- enables optimization of security and operational efficiency.

Dashboard access and customization

Access the dashboard from the left pane by clicking **Dashboard**.

Customize the dashboard to fit your specific needs by modifying visible widgets:

1. On the **Home** page, click **Customize**.
2. Select or deselect the widgets you want to view on the dashboard.
3. You can drag and drop the widgets to arrange them as you prefer.

The dashboard is divided into three main sections: **Top Insights & Alerts**, **Top Actions**, and **Top Information**. Each section provides different categories of insights to help you maintain optimal security and operational control.

Top Insights & Alerts section is visible only if **AgenticOpsInsights** is enabled for your tenant. You can view insights related to high traffic caused by elephant flows, RA VPN forecast, access control policy anomalies, high CPU and memory usage, snort CPU and memory usage.

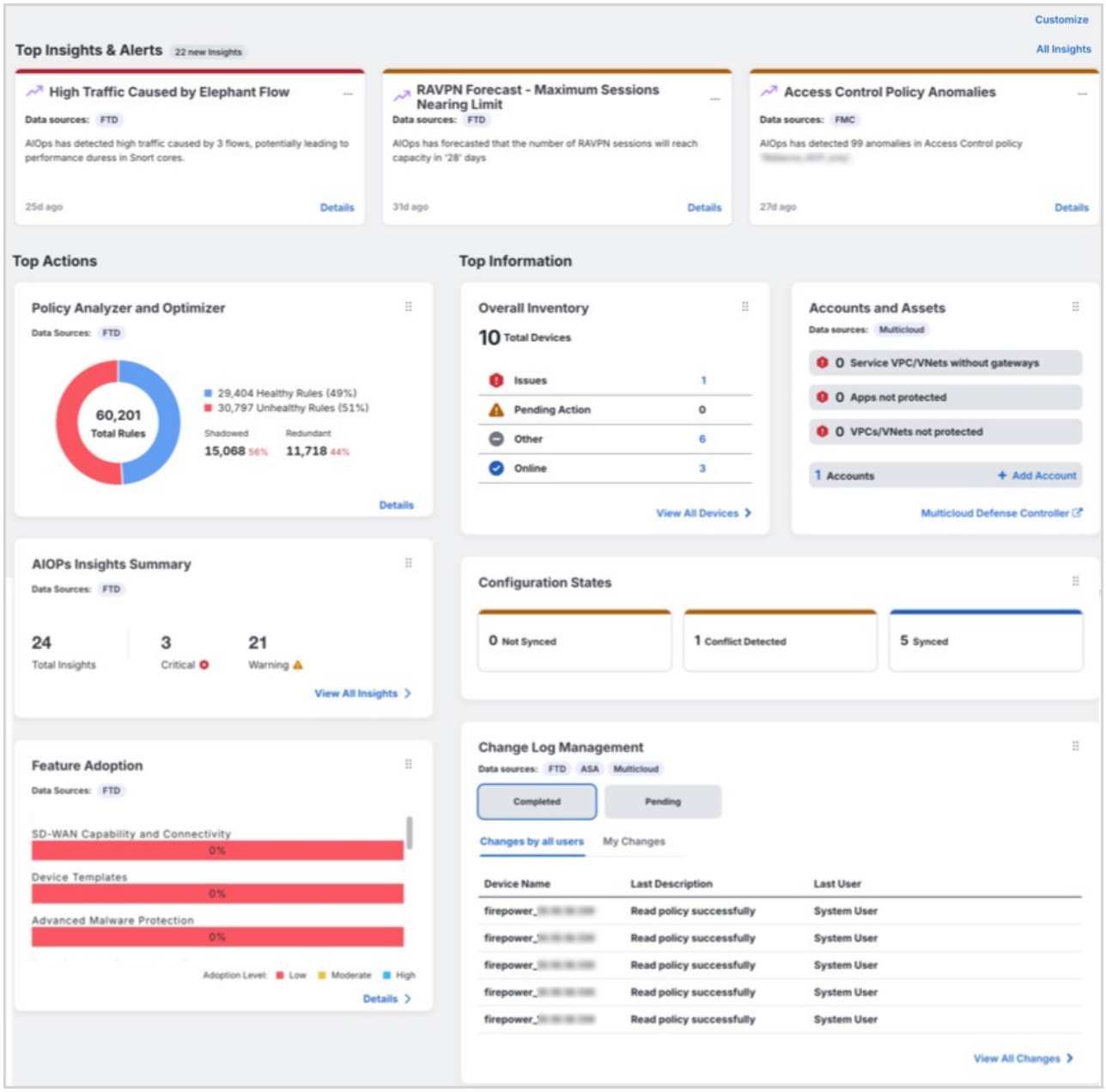
Top Actions section is visible only if **AgenticOps Insights** is enabled for your tenant. If enabled, you can view these widgets:

- **Policy Analyzer and Optimizer**: Analyzes security policies, detects anomalies, and and recommends changes that can improve firewall performance. For more information, refer to Policy Analyzer and Optimizer.
- **AgenticOps Insights**: Shows active insights and trends by category, including Configuration, Health & Operations, and Traffic & Capacity. For more information, refer to AgenticOpsInsights.
- **Feature Adoption**: Shows feature adoption rates so you can assess and improve usage. For more information, refer to Assess and Improve Feature Adoption.

Top Information section provides detailed insights into various tenant-level metrics. Depending on the features that are enabled for your tenant, you can view these widgets:

- **Configuration States**: Compares device configurations with the configurations maintained by Security Cloud Control so that you can identify inconsistencies or conflicts. For more information, refer to Device Management.

- **Change Log Management**: Shows completed and pending change logs so that you can track operational changes. The widget displays **Completed** and **Pending** change logs. For more information, refer to Change Logs.
- **RA VPN Sessions**: Shows Remote Access VPN session activity. For more information, refer to RA VPN Sessions.
- **Overall Inventory**: Shows the total number of devices and groups them by Issues, Pending Actions, Other, and Online. For more information, refer to All Devices.
- **Site-to-Site VPN**: Shows the total number of VPN tunnels and the percentage of tunnels that are Active and Idle. The widget displays the total number of VPN tunnels and the percentage that are **Active** and **Idle**. For more information, refer to Site-to-site VPN.
- **Accounts and Assets**: Helps you to track and manage your multicloud accounts and resources effectively. You can launch the Multicloud Defense Controller from here. Click **+Add Account** to add a new account. For more information, refer to Multicloud Defense Controller.
- **Top Risky Destinations**: Helps you identify and monitor the top risky destinations that are granted access. The widget lists Applications and URL Categories and allows you to filter data for the last 90, 60, or 30 days. You can filter between Allowed (default) and Blocked traffic.
- **Top Intrusion and Malware Events**: Helps you to monitor and respond to top intrusion and malware events. The widget displays Intrusion Events and Malware Events and allows you to filter data for the last 90, 60, and 30 days. You can filter between Allowed (default) and Blocked events.



Click the **Announcements** icon to look at the most recent Security Cloud Control features and updates. Links to related doucmentation is provided if you need more information on any of the items listed.

Part II

Configure basic settings

Topics:

- Manage Firewall administration in Security Cloud Control Firewall Management
- Firewall models and software supported
- Onboard devices in Security Cloud Control Firewall Management
- Manage objects

Security Cloud Control provides a unique view of policy management through a clear and concise interface. Below are topics that cover the basics of using Security Cloud Control for the first time.

2 Manage Firewall administration in Security Cloud Control Firewall Management

Topics:

- General settings
- Manage users and groups within Security Cloud Control organization
- Manage API-Only users for Security Cloud Control Firewall Management
- View Security Cloud Control notifications
- View logging settings
- User roles in Security Cloud Control Firewall Management

Learn how Firewall administration settings apply across the managed organization and can affect multiple devices and users.

Use this chapter if you administer Security Cloud Control Firewall Management for your organization. It explains how to manage organization-wide firewall settings, user access, notifications, logging visibility, and role permissions.

This section provides the following information:

- General Settings
- API User Management
- Logging Settings

What firewall administration settings control

Firewall administration settings apply across the managed organization and can affect multiple devices and users. Some toggle buttons appear only when the related feature is enabled for your managed organization.

General settings

Describes organization-wide settings that affect multiple managed devices and users in Security Cloud Control Firewall Management.

General settings are organization-wide configuration options that affect multiple managed devices and users in your managed organization.

Configuration process

Use **Administration** > **General Settings** to manage organization-wide settings that affect multiple managed devices and users in your managed organization.

> **Note**
>
> You do not see toggle buttons for features that are not enabled for your managed organization.

Enable AI assistant for firewall

Configure the AI Assistant setting to provide contextual guidance for managing security policies, troubleshooting, and optimizing configurations to enhance operational efficiency for your entire organization.

Enable or disable the AI Assistant to control access to AI-driven contextual guidance and insights for managing security policies, troubleshooting issues, and optimizing configurations across your organization.

AI Assistant is an AI-driven virtual companion that provides contextual guidance and insights to manage security policies, troubleshooting issues, and optimizing configurations. For more information, refer to Onboard with Cisco AI Assistant.

By default, the AI Assistant is enabled. When you enable or disable the AI Assistant, the change affects all users in your managed organization .

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn off the **Enable AI Assistant for Firewall** toggle button to disable the AI Assistant.

The AI Assistant setting is updated for all users in your organization based on the toggle button selection.

Enable the option to auto-accept device changes

Configure automatic acceptance of device changes to streamline configuration management by automatically syncing updates and eliminating the need for manual conflict reviews.

Enable auto-accept for device changes to streamline configuration management by automatically syncing updates, eliminating the need for manual conflict reviews.

When this setting is enabled, Security Cloud Control Firewall Management automatically accepts changes that users make directly on the device. If you leave this setting disabled, or disable it later, you must review each device conflict before you accept it.

This task should be performed when you want to automate change synchronization across your managed devices.

Follow these steps to enable automatic acceptance of device changes:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn on the **Enable the option to auto-accept device changes** toggle button.

The auto-accept device changes option is now enabled. Device changes made directly on managed devices will be automatically accepted without requiring manual review and approval.

Enable Multicloud Defense SCC features

Configure the Enable Multicloud Defense SCC features option to integrate specific platform capabilities directly into your Security Cloud Control Firewall Management environment.

This task enables you to leverage advanced Multicloud Defense functionalities within your existing security management workflow.

When you enable this feature, you can configure site-to-site IPsec VPN tunnels between Multicloud Defense and your ASA and Firewall Threat Defense devices that are managed by Security Cloud Control Firewall Management. Perform this task whenever you need to leverage advanced Multicloud Defense functionalities within your existing security management workflow.

Follow these steps to enable Multicloud Defense Security Cloud Control Firewall Management features:

Procedure

1. Choose **Settings** > **General Settings**.
2. Turn on the **Enable Multicloud Defense SCC features** toggle button.

After you enable the feature, you can establish and deploy VPN configurations between these managed devices to improve secure connectivity across your multicloud infrastructure.

Enable object sharing with Multicloud Defense

Configure the Enable object sharing with Multicloud Defense option to synchronize network objects seamlessly, ensuring policy consistency across platforms.

This task enables the sharing of Multicloud Defense network objects from Security Cloud Control Firewall Management to synchronize network objects seamlessly and ensure policy consistency across platforms.

This task should be performed when you need to integrate security objects between Security Cloud Control Firewall Management and Multicloud Defense for improved operational efficiency.

Follow these steps to enable object sharing with Multicloud Defense:

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn on the **Enable object sharing with Multicloud Defense** toggle button.

Object sharing with Multicloud Defense is enabled, allowing network objects to be synchronized between platforms for consistent security policies.

Set the default conflict detection interval

Configure the default conflict detection interval to determine how often the system polls onboarded devices for configuration changes.

This task allows you to configure the default conflict detection interval to determine how often the system polls onboarded devices for configuration changes.

This interval determines the frequency at which Security Cloud Control polls onboarded devices for changes. The selection applies to all devices managed in this tenant. You can change this option at any time.

> **Note**
>
> This selection can be overridden via the **Conflict Detection** option available from the **Security Devices** page after you have selected one or multiple devices.

This task should be performed whenever you need to adjust the frequency of automated monitoring across your managed organization to optimize system performance and visibility.

Follow these steps to set the default conflict detection interval:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. From the **Default conflict detection interval** drop-down list, select a time value.

The system will now poll onboarded devices for configuration changes at the selected interval frequency.

Enable scheduled automatic deployments

Configure the option to schedule automatic deployments to conveniently plan single or recurring updates for your devices.

Enable the option to schedule automatic deployments to automate deployment workflows and ensure updates occur at optimal times.

Enabling the option to schedule automatic deployments allows you to schedule future deployments at a date and time when it is convenient. Once you enable this option, you can schedule a single automatic deployment or set up recurring automatic deployments.

Changes you make on Security Cloud Control for a device are not automatically deployed to the device if it has pending changes . If a device is not in the **Synced** state, such as **Conflict Detected** or **Not Synced**, scheduled deployments are not executed. The jobs page lists any instance where a scheduled deployment fails.

If you turn off **Enable the Option to Schedule Automatic Deployments**, all scheduled deployments are deleted.

Important

If you use Security Cloud Control to create more than one scheduled deployment for a device, the new deployment overwrites the existing deployment. If you create more than one scheduled deployment for a device using the API, you **must** delete the existing deployment before scheduling the new deployment.

Follow these steps to enable scheduled automatic deployments:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn on the **Enable the option to schedule automatic deployments** toggle button to enable it.

The option to schedule automatic deployments is now enabled, allowing you to schedule single or recurring automatic deployments for your devices.

Manage web analytics

Configure web analytics settings to control whether anonymous product usage data is shared with Cisco to help improve the platform's features and performance.

Enable or disable web analytics to control the sharing of anonymous product usage data with Cisco, which helps improve the platform's features and performance based on your privacy preferences.

Web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, and device hostname. This data helps Cisco determine feature usage patterns and improve the product. All usage data is anonymous and no sensitive data is transmitted.

Web analytics is enabled by default. To disable web analytics or re-enable it in the future, complete these steps:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn on the **Web Analytics** toggle button to enable it.

Web analytics is now configured according to your privacy preferences. If enabled, anonymous usage data will be shared with Cisco to help improve the platform.

Set the FDM default recurring backup schedule

Configure the FDM default recurring backup schedule to automate data protection and standardize backup intervals across all managed FDM devices.

This task configures a default recurring backup schedule for FDM devices to automate data protection and standardize backup intervals across all managed devices.

Use this setting to configure a default recurring backup schedule for your devices. When you schedule a backup for a device, you can use the default values or customize them. If you change the default recurring backup schedule, existing scheduled backups keep their current recurring settings.

Follow these steps to set the FDM default recurring backup schedule:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Under the **FDM Default Recurring Backup Schedule** section, from the **Frequency** drop-down, select daily, weekly, or monthly backup.
4. Select the time of day for the backup. Enter the time using the 24-hour format in Coordinated Universal Time (UTC); for example, 22:00 (10:00 PM UTC).
5. For weekly backups, select the days of the week for the backup. For monthly backups, select the **Days of Month** field and add the days when the backup should run. If you enter day 31 for a month with fewer than 31 days, the backup will not run for that month. Enter a name and description for the backup schedule.
6. Click **Save**.

The FDM default recurring backup schedule is configured and will apply to new backup schedules created for FDM devices.

Auto onboard On-Prem FMCs from Cisco security cloud

Configure the auto-onboarding settings for On-Premises Firewall Management Centers from your Cisco Security Cloud to your Security Cloud Control tenant to ensure only authorized devices are added.

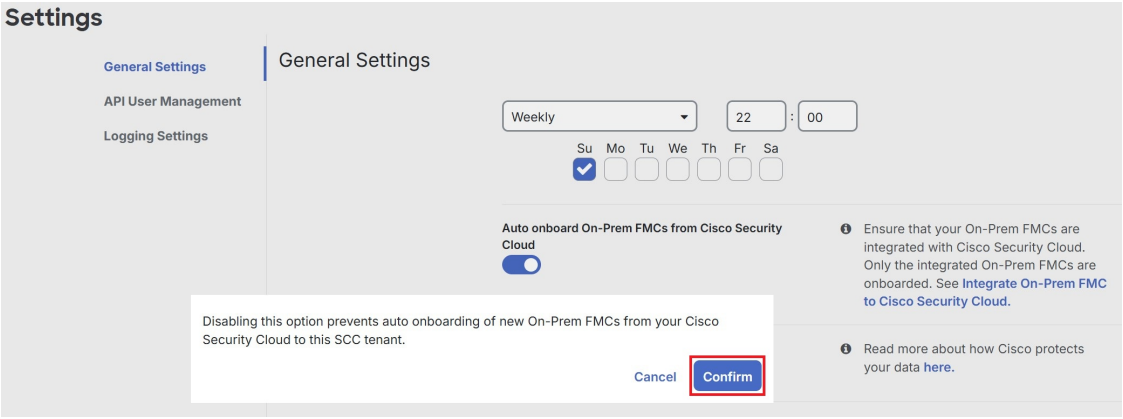
Disable the auto-onboarding of On-Premises Firewall Management Centers from your Cisco Security Cloud to your Security Cloud Control tenant to control device authorization.

Disabling the auto-onboarding functionality stops new On-Premises Firewall Management Centers from being automatically added from your Cisco Security Cloud tenant. This procedure is available to Super Admins and Admins.

> **Note**
>
> Only a Super Admin or Admin can enable or disable this functionality on Security Cloud Control.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn off the **Auto onboard On-Prem FMCs from Cisco Security Cloud** toggle button to disable the auto-onboarding of On-Premises Firewall Management Center.
4. Click **Confirm**.



Auto-onboarding is disabled and new On-Premises Firewall Management Centers will not be automatically added from your Cisco Security Cloud tenant.

Enable event data sharing with talos

Configure Talos event data sharing to contribute to Cisco's threat intelligence and enhance your organization's protection against new security threats.

Share malicious event data from your device with Talos, Cisco's threat intelligence organization. Sharing event data allows Talos to improve threat detection and response capabilities, provide more targeted security updates for your network, and deliver better protection against emerging threats.

You can opt in or out of anonymous event data sharing at any time depending on your organization's policy.

For more information about Talos, see the Cisco Talos product page.

Note

The **Enable event data sharing with Talos** setting in Security Cloud Control and the **Talos Threat Hunting Telemetry** option in Cloud-Delivered Firewall Management Center are separate settings. The setting in Security Cloud Control shares malicious event data from your devices with Talos.

To add threat-hunting rules to the global intrusion policy and send events from those rules to Talos, enable **Talos Threat Hunting Telemetry** in Cloud-Delivered Firewall Management Center at **Administration > Configuration > Intrusion Policy Preferences**.

Enabling the **Enable event data sharing with Talos** toggle button does not automatically activate the **Talos Threat Hunting Telemetry** feature in Cloud-Delivered Firewall Management Center. For the best results with this feature, also enable the **Talos Threat Hunting Telemetry** in Cloud-Delivered Firewall Management Center. For more information, see Set Intrusion Policy Preferences.

Sharing event data with Talos is enabled by default. To opt out, follow these steps:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn off the **Enable event data sharing with Talos** toggle button to disable this setting.

> **Note**
>
> Sharing event data enables Talos to provide relevant security insights for your network. Disabling this setting might limit your ability to fully leverage Talos's capabilities and could affect your network's defense against evolving threats.

Event data sharing with Talos is now disabled for your organization.

View firewall management instance details

Lists tenant details that are helpful when you need to contact the Cisco Technical Assistance Center (TAC).

Firewall Management Instance Details are helpful if you need to contact the Cisco Technical Assistance Center (TAC). You can copy these tenant details by clicking the copy icon.

The firewall management instance details include these identifiers:

- **Firewall Management Instance Name**: The display name of the firewall management instance.
- **Firewall Management Instance ID**: The system-generated unique identifier for the firewall management instance in Cisco Security Cloud Control.
- **Secure Services Exchange ID**: The unique identifier for the firewall management instance in the Secure Services Exchange environment. Cisco uses this value for service integration and backend correlation across cloud services.
- **Security Cloud Control Organization ID**: The unique identifier of the Security Cloud Control organization associated with the firewall management instance.

Use the Security Cloud Control Firewall Management platform navigator

Explains how the platform navigator provides users with quick, centralized access to various Cisco networking and security applications for seamless management of infrastructure and security operations.

A platform navigator is a nine-block applications cross-launcher that

- appears on the top-right corner of Security Cloud Control ( )
- provides users with quick, centralized access to various Cisco networking and security applications, and
- allows users to seamlessly transition between integrated Cisco platforms to manage their infrastructure and security operations.

Networking applications

You can readily cross-launch to these Cisco networking applications:

- **Catalyst**: Cisco Catalyst products include a wide variety of network switches, wireless controllers, wireless access points, and edge platforms and routers, supporting enterprise-class business needs to heavy-duty and rugged networking environments.
- **Intersight**: Cisco Intersight is a cloud operations platform that consists of optional, modular capabilities of advanced infrastructure, workload optimization, and Kubernetes services. Cisco Intersight infrastructure services include the deployment, monitoring, management, and support of your physical and virtual infrastructure. IT supports Cisco

Unified Computing System (Cisco UCS), Cisco HyperFlex hyperconverged infrastructure (HCI), and other third-party Intersight-connected targets.

- **IoT Operations Dashboard**: Cisco IoT Operations Dashboard is a cloud-based IoT services platform that empowers operations teams to securely connect, maintain, and gain insights from industrial networking devices and connected industrial assets at massive scale. With one comprehensive view of all their connected industrial assets, operations teams can uncover valuable insights that help them streamline operations and drive business continuity.
- **Meraki**: Cisco Meraki is an IT and IoT cloud-managed platform that provides a centralized management platform for Cisco Meraki devices.
- **Spaces**: Cisco Spaces is a cloud-based location services platform through which organizations can gain insights into how people and things move throughout their physical spaces. With these insights, they can deliver contextual engagements that are valuable and relevant. Besides looking at where people go, organizations can also drive operational efficiencies by monitoring the location, movement, and utilization of assets.
- **ThousandEyes**: Cisco ThousandEyes is a cloud service suite that helps monitor and measure the availability and performance of web applications, services, and networks. IT provides end-to-end visibility from any user to any application over any network, enabling enterprises to swiftly get to the source of issues, resolve them faster, and manage performance effectively.
- **Workflows**: Cisco Workflows is a cloud-hosted automation application that is part of the larger Cisco Networking Cloud vision. IT provides an entitlement to cross-domain automation capabilities for Cisco customers. IT streamlines repetitive and error-prone tasks across both Cisco and third-party applications using custom and premade automation templates, as well as various adapter options that can be provided by Cisco or built independently, reaching targets in the cloud or on-premises.

You can also cross-launch to these Cisco security applications:

- **Secure Access**: Cisco Secure Access simplifies IT operations through a single, cloud-managed console, unified client, centralized policy creation, and aggregated reporting. Extensive security capabilities converged in one solution (ZTNA, SWG, CASB, FWaaS, DNS security, RBI, and more) mitigate security risk by applying zero trust principles and enforcing granular security policies. Market leading Talos threat intelligence fuels unmatched threat blocking to mitigate risk and speed investigations.
- **Secure Endpoint**: Cisco Secure Endpoint, formerly known as Cisco AMP for Endpoints, is a cloud-managed endpoint security solution designed to prevent breaches and rapidly detect, contain, and remediate threats. IT instantly checks your files against a cloud-based scanner with advanced tracking features. These features enable security analysts to identify and isolate initial outbreak sources. The solution also provides retrospective quarantine for files found to be malicious.
- **Cisco Security Provisioning and Administration**: Cisco Security Provisioning and Administration is a web application that provides centralized management of Cisco Secure product instances, user identity, and user access management across Cisco Security Cloud. Security Cloud Control administrators can create new Security Cloud enterprises, manage users in an enterprise, claim domains, and integrate their organization's SSO identity provider, among other tasks.
- **XDR**: Cisco Extended Detection and Response (XDR) is a cloud-based solution designed to simplify security operations and empower security teams to detect, prioritize, and respond to sophisticated threats. By integrating both Cisco and third-party security solutions into a unified platform, Cisco XDR offers a comprehensive approach to threat management. Integrated with the threat intelligence provided by Talos, Cisco XDR enriches incident data with additional context and asset insights, reducing false positives and enhancing overall threat detection, response, and forensic capabilities.

Manage users and groups within Security Cloud Control organization

Configure centralized and automated management of user access across Cisco security products through role-based access control (RBAC) in Security Cloud Control.

The purpose of this task is to provide centralized and automated management of user access across Cisco security products through role-based access control (RBAC).

Security Cloud Control supports role-based access control (RBAC) to automate access management across the organization. A role defines the level of user access to functions within a product. With Security Cloud Control, you can centralize the management of user roles within an organization, allowing organization users to switch seamlessly between products without the need to log in repeatedly.

Additionally, you can create API-only users for Security Cloud Control Firewall Management. API-only users allow systems to interact with Security Cloud Control using APIs, eliminating the need for a user interface.

Procedure

1. From the Security Cloud Control Home page, click **Platform Management**.
2. Choose **Platform Management** > **Access Management** > **Administrator Access**

   For more information, see Managing users in the Security Cloud Control platform services documentation.

You can now manage users and groups within your organization using centralized role-based access control, allowing seamless access across Cisco security products.

Manage API-Only users for Security Cloud Control Firewall Management

Configure API-only users and generate API tokens for programmatic access to Security Cloud Control Firewall Management.

The purpose of creating an API-only user in Security Cloud Control Firewall Management is to enable secure, programmatic access to the system using API tokens.

Developers use Security Cloud Control Firewall Management API tokens when making Security Cloud Control Firewall Management REST API calls. The API token must be included in the REST API authorization header for a successful call. API-only users can generate API tokens. Regular users cannot create API tokens for themselves or others.

An API-only user role allows a user to interact with Security Cloud Control Firewall Management using APIs, eliminating the need for a user interface. API-only users cannot log in to the Security Cloud Control interface directly. The role benefits organizations that need automated processes and integrations.

Only API-only users can generate API tokens; regular users cannot create API tokens for themselves or others.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Administration** > **API User Management**.
3. Click the **Add a new user** () icon to add a new user to your tenant.
4. In the **Username** field, enter a name for the API-only user.
5. From the **Role** drop-down list, choose a role for the API-only user and click **Add**.
6. In the **Token** column for the new API Only user, click **Generate API Token** to obtain an API token. Save the token in a secure location in accordance with your enterprise's best practices for maintaining sensitive data.

> **Note**
>
> Click edit to change the role of the existing API-only user.

You have successfully created an API-only user and generated an API token for programmatic access to Security Cloud Control Firewall Management.

View Security Cloud Control notifications

Configure how to view, search, dismiss, and review Security Cloud Control notifications for device events, alerts, and reports.

This task helps you manage and monitor notifications to stay informed about device events, alerts, and reports in your Security Cloud Control Firewall Management tenant.

The notifications system provides visibility into the most recent alerts that have occurred or affected the devices that you onboarded to your tenant. The settings that you choose on the Notification Settings page determine the notification types that appear in Security Cloud Control Firewall Management.

The notifications drop-down page is grouped into three tabs: Overview, All, and Dismissed.

Procedure

1. Click the notifications icon  to view the most recent alerts.

   The **Overview** tab displays a combination of the most recent high-priority alerts and events to which you are subscribed. High priority events are the following:

   - Deployment Failed
   - Backup Failed
   - Upgrade Failed
   - Migrate FTD to Cloud-Delivered Firewall Management Center Failed
   - Device went offline
   - Device HA state changed
   - Device certificates expiring

2. To view all notifications regardless of priority, click the **All** tab.

   This tab displays all notifications, including email subscription notifications and all high-priority items.

3. To view dismissed notifications, click the **Dismissed** tab.

   This tab displays notifications that you dismissed. You can dismiss individual notifications by clicking the "x" of the notification.

Opting to **Dismiss** notifications from the drop-down menu dismisses notifications from both the "Overview" and "All" tabs. They will remain in the **Dismiss** tab for 30 days, after which they will be removed from Security Cloud Control.

4. To search for specific notifications, use the search bar at the top of the drop-down to query for key words or alerts.

   When viewing the notifications drop-down window, for any of the tabs mentioned above, you can use the search bar to filter notifications.

5. To configure notification preferences, click Notification Settings in the Notifications window or select **UserID** > **User Preferences** from the upper right corner of the dashboard.

   View your personal preferences in the **Notification Preferences** page. From this page you can configure the "Notify Me in Security Cloud Control When" alerts and enable email notifications to receive any of the alerts. See Notification Preferences.

You can now effectively manage and monitor all notifications in your Security Cloud Control Firewall Management tenant, including viewing high-priority alerts, searching for specific notifications, dismissing unwanted alerts, and configuring your notification preferences.

User notification preferences

Describes the customizable notification settings that allow users to control which alerts they receive from Security Cloud Control Firewall Management based on device events, workflow activities, and report generation tasks.

User notification preferences are customizable alert settings that

- control which notifications users receive from Security Cloud Control Firewall Management based on device events and workflow activities
- allow personal customization without affecting other tenant users, and
- provide real-time updates without requiring deployment.

Notification preference configuration

Security Cloud Control Firewall Management generates notifications whenever a device linked to your tenant encounters a specific event. This includes actions taken by the device, expiring or expired device certificates, or the start, completion, or failure of a report generation task. By default, these notifications are enabled and visible to all users associated with the tenant, regardless of their role. You have the option to customize your personal notification preferences to display only the alerts that interest you. These preferences are unique to you and do not impact other users connected to the tenant.

> **Note**
>
> Changes made to the notifications listed below are automatically updated in real time and do not require deployment.

Device workflow alerts include:

- **Deployments** - This action is applicable to Security Cloud Control and Cloud-Delivered Firewall Management Center, and does not include integration instances for SSH or IOS devices.
- **Backups** - This action is only applicable for FDM-managed devices.
- **Upgrades** - This action is only applicable for ASA and FDM-managed devices.

- **Migrate Firewall Threat Defense to cloud** - This action is applicable when changing the Firewall Threat Defense device manager from Firewall Management Center to Security Cloud Control.

Device event alerts include:

- **Went offline** - Applies to all devices associated with your tenant.
- **Back online** - Applies to all the devices associated with your tenant.
- **Conflict detected** - Applies to all the devices associated with your tenant.
- **HA state changed** - Indicates the device within an HA or failover pair, the current state, and the state it changed from. This action applies to all HA and failover configurations associated with your tenant.
- **Site-to-Site session disconnected** - Applies to all site-to-site VPN configurations configured in your tenant.

Event search report alerts include:

- **Report generation started**: Notifies you when a report generation task starts. This applies to both immediate and scheduled search reports.
- **Report generation completed**: Notifies you when a report generation task ends. This applies to both immediate and scheduled search reports.
- **Report generation failed**: Notifies you when a report generation task fails. This applies to both immediate and scheduled search reports. Check the parameters or query and try again.

Application insights alerts include:

- **Application available**: Notifies you when a monitored application becomes available.
- **Application unavailable**: Notifies you when a monitored application becomes unavailable.

Cisco Secure Dynamic Attributes Connector alerts enable notifications about the health of all dynamic attributes connectors in your organization. Check the **All Dynamic Attributes Connector health notifications** check box to enable notifications about the health of all dynamic attributes connectors in your organization.

These notifications alert you early in the workflow about unhealthy connector resources. A notification message includes the state of the resource (Error or Recovered) and diagnostic details if it is an error or unhealthy.

You can also configure notifications through e-mail, as well as webhook endpoints including Cisco Webex, Microsoft Teams, and Slack to receive notifications within those applications.

To configure direct notifications:

1. Click **Platform Management** > **Firewall Notification Settings**.
2. On the Firewall Notifications Settings page, click **Add Now** under the **Service Integrations** pane.
3. In the **Add Service Integrations** slide-in pane, enter the name of the service, select the messaging service from the drop-down list, enter the resulting URL, and choose the type of alerts you wish to receive.
4. Click **Save**.

By default, all notification types are enabled. To stop receiving a notification type, clear that notification and click **Save**.

Enable the Email notifications toggle button to receive email for the alerts that you select.

By default, **Use Security Cloud Control notification settings above** is selected. When this option is selected, email notifications match the same notifications and events that you selected in the **Notify Me in Security Cloud Control When** sections.

If you want email notifications for only some alerts, clear **Use Security Cloud Control notification settings above**, select the alert types that you want to receive by email, and then click **Save**.

View logging settings

Provides information about reviewing tenant logging usage, monthly limits, reset timing, historical usage, and storage options.

Use **Logging Settings** to check current logging usage for your tenant.

The page shows:

- Your monthly event logging limit.
- The number of days until the limit resets.
- Stored logging usage, which represents the compressed event data that the Cisco cloud received.

Click **View Historical Usage** to review the logs that your tenant received during the last 12 months.

The page also includes links that you can use to request additional storage.

User roles in Security Cloud Control Firewall Management

Explains how user roles define permissions for each Security Cloud Control Firewall Management organization.

A user role is a permission system that

- defines access permissions for each Security Cloud Control Firewall Management organization,
- assigns roles per user and per organization, and
- allows users to have different permission levels on different organizations.

Role assignment behavior

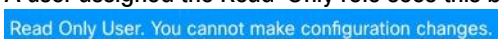
Security Cloud Control Firewall Management assigns roles per user and per organization. If a user has access to more than one tenant, that user can have the same user ID but different roles on different organizations. For example, a user can have the **Read-Only** role on one organization and the **Super Admin** role on another.

When the interface or documentation refers to a **Read-Only** user, **Admin** user, or **Super Admin** user, it describes that user's permission level on a specific organization.

Read-only role

Provides information about the read-only user role permissions and restrictions in the system.

A user assigned the Read-Only role sees this blue banner on every page:



Permitted actions

Users with the Read-Only role can:

- View any page or any setting in Security Cloud Control.
- View all device configuration details including sensitive values in device configurations, such as certificates, PSKs, and credentials.

> **Note**
>
> Note: For ASA devices, we recommend enabling password encryption as a best practice. Password encryption helps prevent PSKs and credentials from being visible in clear text in the configuration.

- Compare device configurations, view the change log, and see VPN mappings.
- Search and filter the contents of any page.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a read-only user revokes their own token, they cannot recreate it.
- Contact support through our interface and can export a change log.

Restricted actions

Users with the Read-Only role cannot:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

Edit-Only role

Lists the permissions and restrictions for users assigned the Edit-Only role.

Users with the Edit-Only role have specific permissions for editing device configurations while being restricted from deployment and certain administrative functions.

Permissions

Users with the Edit-Only role can:

- Edit and save device configurations, including but not limited to objects, policies, rulesets, interfaces, VPN, etc.
- Allow configuration changes that are made through the **Read Configuration** action.
- Utilize the Change Request Management action.

Restrictions

Users with the Edit-Only role cannot:

- Deploy changes to a device or to multiple devices.
- Discard staged changes or changes that are detected through OOB.
- Upload AnyConnect Packages, or configure these settings.

- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create Security Cloud Control user records.
- Change user role.

Deploy-Only role

Lists the capabilities and limitations of users with the Deploy-Only role in the system.

Users with the Deploy-Only role have specific permissions for deployment and management tasks, but are restricted from configuration and administrative functions.

Users with the Deploy-Only role can:

- Deploy staged changes to a device, or to multiple devices.
- Revert or restore configuration changes for ASA devices.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Utilize the Change Request Management action.

Users with the Deploy-Only role cannot:

- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create, update, configure, or delete anything on any page.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

VPN sessions manager role

Provides information about the VPN Sessions Manager role intended for administrators who monitor remote access VPN connections.

The VPN Sessions Manager role is intended for administrators who monitor remote access VPN connections, not site-to-site VPN connections.

Users with the VPN Sessions Manager role can:

- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see RA VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a VPN Sessions Manager user revokes their own token, they cannot recreate it.
- Contact support through our interface and export a change log.
- Terminate existing RA VPN sessions.

Users with the VPN Sessions Manager role cannot:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

Admin role

Provides information about the Admin role permissions and limitations in Security Cloud Control Firewall Management and Security Cloud Control.

Users with the Admin role have complete access to most areas of Security Cloud Control Firewall Management and can perform a wide range of administrative tasks with some limitations on user management functions.

Admin users have these capabilities:

- Create, read, update, and delete any object or policy in Security Cloud Control Firewall Management and configure any setting.
- Onboard devices.
- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can contact support through our interface and can export a change log.

Admin users **cannot** do the following:

- Create Security Cloud Control user records.
- Change user role.

Super admin role

Describes the Super Admin role and its comprehensive access privileges within Security Cloud Control Firewall Management.

A Super Admin role is a user permission level that

- provides complete access to all areas of Security Cloud Control Firewall Management,
- enables comprehensive administrative capabilities including user and device management, and
- allows full configuration control over objects, policies, and system settings.

Super admin capabilities

Users with the Super Admin role can perform these administrative functions:

- Change user roles.
- Create user records.
- Create, read, update, and delete any object or policy in Security Cloud Control Firewall Management and configure any setting.
- Onboard devices.
- View any page or any setting in Security Cloud Control Firewall Management.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens.
- Contact support through the interface and export a change log.

3 Firewall models and software supported

Topics:

- Security device management
- Supported devices, software, and hardware for Security Cloud Control Firewall Management

Security device management

Explains how to manage security devices in Security Cloud Control.

The **Security Devices** page displays all physical and virtual onboarded devices and templates created from onboarded devices. The page classifies devices and templates based on their type and displays them in corresponding tabs dedicated to each device type.

The **Filter** panel provides multiple options to narrow down results and find devices based on specific attributes, including **Devices/Services, Hardware Versions, Device End-of-Life, Software Versions, Snort Version, Configuration Status, Connectivity States, Conflict Detection, Health Status, Secure Device Connectors, and Labels**.

The page separates live devices from templates. **Devices** lists live devices added to Security Cloud Control. **Templates** lists model devices created from live devices or imported configuration files. Device types appear in their corresponding categories.

Security device management capabilities

From the **Security Devices** page you can:

- Onboard the following devices and services:
  - Secure Firewall ASA
  - Firewall Threat Defense
  - Onboard Umbrella Organization
  - Integrate SD-WAN Manager
  - Onboard Cisco Meraki
  - Integrate Generic SSH
  - Integrate IOS
- View the configuration state and connectivity state of managed devices and services.
- View onboarded devices and templates categorized in separate tabs. See Filter security devices by hardware end-of-life status on page 852.
- Evaluate and take action on individual devices and services.
- View device and service specific information and resolve issues.
- Search for a device or template by name, type, IP address, model name, serial number, or labels. Search is not case-sensitive. Providing multiple search terms brings up devices and services that match at least one of the terms. See Use page level search on page 855.
- Filter for a device or template filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. See Filters.
- Identify devices that are nearing or have reached their last day of hardware support. Refer to Filter security devices by hardware end-of-life status.
- Delete a device

For Firewall Threat Defense devices managed by the Cloud-Delivered Firewall Management Center, you can also see the node status for devices in a cluster.

Supported devices, software, and hardware for Security Cloud Control Firewall Management

Provides an overview of devices supported by Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management is a cloud-based management solution enabling the management of security policies and device configurations across multiple security platforms.

This section describes the supported device types, software, hardware, and constraints for managing firewall, cloud, SD-WAN, Cisco IOS, Cisco Umbrella, and management center integrations in Security Cloud Control Firewall Management.

Support scope

Security Cloud Control Firewall Management is a cloud-based management solution for security policies and device configurations across multiple security platforms. The source identifies support for these management areas:

- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Catalyst SD-WAN Manager
- Cisco Secure Firewall Management Center, on-premises
- Cisco Meraki MX
- Cisco IOS devices
- Cisco Umbrella
- AWS Security Groups

Security Cloud Control Firewall Management documentation identifies the devices, software, and hardware that Security Cloud Control Firewall Management supports. If the documentation does not explicitly claim support for a software version or device type, Security Cloud Control Firewall Management does not support it.

Cisco secure firewall ASA

Cisco Adaptive Security Appliance (ASA) is a security device that integrates firewall, VPN, and intrusion prevention capabilities. Security Cloud Control supports ASA device management to streamline configuration management and support regulatory compliance across the network infrastructure.

Cisco secure firewall threat defense

Cisco Secure Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It includes security functions such as intrusion prevention, application control, URL filtering, and advanced malware protection.

A Secure Firewall Threat Defense device can be deployed on ASA hardware appliances, Cisco firewall hardware appliances, and virtual environments. You can manage threat defense devices through management interfaces such as Cisco Firewall Management Center, Security Cloud Control, and Firewall Device Manager.

Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It offers comprehensive security functions, including intrusion prevention, application control, URL filtering, advanced malware protection, and so on. An FTD can be deployed on ASA hardware appliances, and Cisco firewall hardware appliances, and in virtual environments. Managing threat defense devices is possible through various management interfaces, such as Cisco Firewall Management Center, Security Cloud Control Firewall Management, and Firewall Device Manager.

For more information on software and hardware compatibility, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Firewall Device Manager is a web-based management interface explicitly designed for threat defense device management. It provides a simplified approach for configuring and monitoring threat defense devices, making it ideal for smaller-scale deployments or organizations preferring an intuitive interface.

FDM offers basic configuration capabilities for network settings, access control policies, NAT rules, VPN configuration, monitoring, and basic troubleshooting. Typically accessed through a web browser, FDM is directly available on the FTD device, eliminating the need for additional management servers or appliances.

Cisco Catalyst SD-WAN manager

Security Cloud Control offers centralized management for Catalyst SD-WAN and Branch WAN environments, allowing organizations to efficiently configure, monitor, and enforce security policies across their networks. This integration also facilitates advanced troubleshooting, rule optimization, and change management on the Catalyst SD-WAN Manager.

For more information on software and hardware compatibility, see Cisco Catalyst SD-WAN Device Compatibility.

Cisco secure firewall management center

Security Cloud Control Firewall Management simplifies the management of on-premises Firewall Management Center by establishing a secure integration, discovering security devices, and enabling centralized policy management. Security policies such as firewall rules, VPN settings, and intrusion prevention policies can be efficiently managed and deployed across all devices under FMC.

Cisco Meraki MX

The Cisco Meraki MX appliance is an enterprise-grade security and SD-WAN next-generation firewall appliance for decentralized deployments. Security Cloud Control Firewall Management supports management of layer 3 network rules on Meraki MX devices.

When you onboard a Meraki device to Security Cloud Control Firewall Management, Security Cloud Control Firewall Management communicates with the Meraki dashboard to manage that device. Security Cloud Control Firewall Management transfers configuration requests to the Meraki dashboard, and the Meraki dashboard applies the new configuration to the device.

Security Cloud Control Firewall Management support for Cisco Meraki MX includes centralized policy management, backup and restore, monitoring and reporting, compliance checking, and automation capabilities.

Cisco IOS devices

Cisco IOS software manages network functions such as routing, switching, and other networking protocols. Cisco IOS includes features and commands to configure and maintain Cisco network devices.

Cisco umbrella

Security Cloud Control Firewall Management manages Cisco Umbrella through integrations such as the Umbrella ASA Integration. This integration lets administrators include Cisco Adaptive Security Appliance (ASA) devices in their Umbrella configuration by using per-interface policies.

The integration enables ASA devices to redirect DNS queries to Umbrella and use Umbrella DNS security, web filtering, and threat intelligence capabilities.

AWS security groups

Security Cloud Control Firewall Management provides a simplified management interface for Amazon Web Services (AWS) Virtual Private Clouds (VPCs). Source-backed capabilities include monitoring AWS Site-to-Site VPN connections, tracking changes to AWS devices, and viewing AWS Site-to-Site VPN tunnels.

ASA support specifics

Lists the constraints and limitations for Security Cloud Control Firewall Management support of ASA platforms.

Security Cloud Control Firewall Management support for ASA has these constraints:

- Security Cloud Control Firewall Management can manage all ASA platforms that run currently supported code versions, including ASAv instances.
- Security Cloud Control Firewall Management does not support ASA Services Module (ASASM).
- Security Cloud Control Firewall Management does not test end-of-life ASA code versions and does not recommend them for production.
- Use currently supported ASA code versions for optimal results.
- ASA 8.3 is not supported with the new policy view.
- Security Cloud Control Firewall Management does not manage the ASA FirePOWER module because the module runs a different operating system from ASA. Manage the ASA FirePOWER module separately with Secure Firewall Management Center or ASDM.
- End-of-life code and hardware might continue to work with Security Cloud Control Firewall Management. Because end-of-life code and hardware are not part of Security Cloud Control Firewall Management testing, correct operation with end-of-life software and hardware is not guaranteed or assured.

  Refer to the version download page for Cisco "suggested release" or "gold star" versions.
- ASA versions 8.x, 9.1, and 9.2 do not support TLS 1.2 on the management plane and are considered insecure for ASA software management.

For a full discussion of ASA, ASDM, and hardware compatiblity, see the Cisco Secure Firewall ASA Compatibility guide.

Cloud device support specifics

Provides software and device type support information for cloud-based devices.

This table describes software and device type support for cloud-based devices. Read the affiliated links for more information about onboarding and feature functionality for the device types in the table.

Device Types	Notes
Meraki Security Appliance • MX Series • Meraki Templates	Meraki MX devices and the Meraki dashboard receive regular software updates through the Meraki cloud. Security Cloud Control Firewall Management works with the latest version of the Meraki dashboard to manage layer 3 network rules enforced by Meraki MX devices. Register the MX device to the Meraki dashboard, or create the template in the Meraki dashboard, before onboarding it to Security Cloud Control Firewall Management. For more information, refer to Managing Meraki with Security Cloud Control. You must register an MX device to, or create a template in, the Meraki dashboard before onboarding it to Security Cloud Control Firewall Management.
Amazon Web Services VPC	AWS VPC receives updates through the AWS console. Refer to AWS documentation for more information about the platform and available services. Launch an AWS VPC in the AWS console before onboarding it to Security Cloud Control Firewall Management.

Device Types	Notes
Google Cloud Platform	Google Cloud Platform (GCP) receives updates through the GCP console. Refer to Google Cloud documentation for more information about the platform and available services.
Microsoft Azure	Azure receives updates through the Azure console. Refer to Azure documentation for more information about the platform and available services.

Switching and routing support specifics

Provides Cisco IOS software and device type support information for devices specific to switching and routing.

This table describes Cisco IOS software and device type support for devices specific to switching and routing. Read the affiliated links for more information about onboarding and feature functionality for the device types in the table.

Devices Types	Notes
Cisco IOS	Security Cloud Control supports devices running Cisco IOS version 12.4 or later.

4 Onboard devices in Security Cloud Control Firewall Management

Topics:

- Secure connectors

Describes how to onboard devices in Cisco Defense Orchestrator, including prerequisites, connector selection, credentials, labels, and inventory results for both live devices and model devices.

You can onboard both live devices and model devices to Security Cloud Control Firewall Management. Model devices are uploaded configuration files that you can view and edit using Security Cloud Control Firewall Management.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect Security Cloud Control Firewall Management to the device or service.

What do you want to onboard?

ASA devices or templates

- Onboard a Secure Firewall ASA on page 260
- Onboard multiple ASAs to Security Cloud Control Firewall Management on page 265
- Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management on page 262
- Onboard a high availability pair of ASA devices to Security Cloud Control Firewall Management on page 262

Secure Firewall Threat Defense Devices to Cloud-Delivered Firewall Management Center

- Onboard a device with a CLI registration key on page 412
- Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning on page 414
- Onboard a Secure Firewall Threat Defense Cluster on page 435
- Onboard a chassis on page 438

AWS virtual private clouds

- Onboard an AWS VPC on page 689

Security Cloud Control Integrations

- Onboard a Cisco IOS Device on page 706
- Import ASR or ISR Configuration on page 708
- How to onboard an SSH device on page 718

Umbrella networks

- Onboard an umbrella organization on page 659

This chapter covers the following sections:

Secure connectors

Explains how secure connectors support communication between Security Cloud Control Firewall Management and managed resources in your network or cloud environment.

A secure connector is a connector instance that

- runs in your network or supported cloud environment
- provides a secure communication path between Security Cloud Control Firewall Management and managed resources, and
- helps Security Cloud Control Firewall Management manage devices that are not directly reachable from the internet and support event forwarding for logging and analytics workflows.

Secure connector types

Use the **Secure Connectors** page to view, deploy, and manage connector instances for your tenant.

The **Secure Connectors** page can include these connector types:

- Secure Device Connector (SDC): Provides a secure communication path between Security Cloud Control Firewall Management and supported managed devices.
- Secure Event Connectors (SEC): Receives events from supported devices and forwards the events to the Cisco cloud for logging and analytics.

Secure Device Connector

Describes an intelligent proxy that enables Cisco devices to communicate with Security Cloud Control Firewall Management when devices are not directly reachable from the internet.

A Secure Device Connector (SDC) is an intelligent proxy that

- monitors Security Cloud Control Firewall Management for commands and messages for managed devices
- executes commands on behalf of Security Cloud Control Firewall Management
- relays messages to managed devices and returns device responses, and
- lets Cisco devices communicate with Security Cloud Control Firewall Management when the devices are not directly reachable from the internet.

Device onboarding and deployment

When you onboard a device by using device credentials, you can deploy an SDC in your network to proxy communication between the device and Security Cloud Control Firewall Management. If the device is directly reachable from the internet, you can allow direct communication through the device's outside interface instead of using an SDC.

You can onboard these devices to Secure Device Connector through an SDC:

- Secure Firewall ASA
- FDM-Managed
- On-Premises Firewall Management Center using credentials method
- Meraki MX devices
- Generic SSH devices

- Cisco IOS devices

Communication between the SDC and Security Cloud Control Firewall Management uses HTTPS with TLS 1.3 and AES-128-GCM. Credentials for onboarded devices and services are encrypted from the browser to the SDC and are encrypted at rest by using AES-128-GCM. Only the SDC has access to those credentials.

A user with the Super Administrator role is required to create a Secure Device Connector or a Secure Event Connector (SEC).

Secure Firewall Threat Defense devices that are managed by Cloud-Delivered Firewall Management Center do not require an SDC and do not support onboarding through proxies. Ensure that these devices have proper DNS settings and outbound internet connectivity so they can connect to Cloud-Delivered Firewall Management Center.

See Allow inbound access for direct cloud connectivity on page 94 for information explaining how to allow communication between an SDC and Security Cloud Control.

For more information, refer to Deploy a VM for running the secure device connector and secure event connector on page 78.

Device connectivity planning

Describes how Security Cloud Control Firewall Management connects to managed devices through cloud connectors or on-premises data collectors.

Device connectivity planning is a network architecture consideration that

- determines whether Security Cloud Control Firewall Management connects to managed devices through the cloud connector or through an SDC
- requires specific network access permissions based on the connection method, and
- depends on device type and internet accessibility requirements.

Connection methods and requirements

The connection method depends on device internet accessibility and organizational requirements.

Table 1: Device connection methods

Connection method	Use when	Required network access
Direct cloud connector	The device is directly reachable from the internet.	Allow inbound access from the Security Cloud Control Firewall Management IP addresses for your cloud region on port 443, or on the port that you use for device management.
SDC	The device is not directly reachable from the internet, or the source explicitly requires an on-premises SDC.	Allow full inbound access from the SDC host on port 443, or on the port that you use for device management. Ensure that the SDC VM can reach the device management interface.

An FDM-managed device can be onboarded to Security Cloud Control Firewall Management by using device credentials, a registration key, or its serial number whether it is directly accessible from the internet. If the device does not have direct internet access, but it resides on a network that does, the Security Services Exchange connector that is delivered as part of the device can reach the Security Services Exchange cloud and allow the FDM-managed device to be onboarded.

The source explicitly states that you need an on-premises SDC to onboard these devices:

- An ASA device that is not accessible from the cloud

- An FDM-managed device that is not accessible from the cloud when you use the credentials onboarding method
- A Cisco IOS device
- A device with SSH access

All other devices and services do not require an on-premises SDC because Security Cloud Control Firewall Management connects by using its cloud connector.

Docker network considerations for the SDC

SDC runs as a Docker container. Docker commonly uses the **172.17.0.0/16** subnet for the default bridge network, docker0.

If **172.17.0.0/16**, or any part of the Docker-assigned network space, overlaps with your existing network IP space, change the Docker network defaults before deploying the SDC. To use alternate networks, edit /etc/docker/daemon.json configuration.

For example, Use the supernet **10.198.0.1/24** for Docker networking address pools and use IP address **10.198.128.0/17** as the default docker bridge interface, docker0, from the subnet **10.198.0.0/24**.

```
sudo vi /etc/docker/daemon.json

{
  "log-driver": "json-file",
  "log-opts": {
    "max-size": "100m",
    "max-file": "5"
  },
    "bip": "10.198.0.1/24",
    "default-address-pools": [
        {
            "base": "10.198.128.0/17",
            "size": 24
        }
    ]
}

(save and exit)

sudo reboot (required)
```

For more information, see Networking overview.

Plan SDC capacity and host requirements

Describes capacity planning and host requirements for SDC deployment in multi-device environments.

SDC capacity planning is a deployment strategy that

- supports approximately 500 devices per SDC, with actual capacity depending on enabled features and configuration file sizes
- allows unlimited SDCs per Security Cloud Control Firewall Management organization, and
- ensures each SDC belongs to one organization only and is not shared across organizations.

Multiple SDC deployment benefits

Deploying more than one SDC provides these benefits:

- Scale device management without performance degradation.

- Place SDCs in isolated network segments while keeping the devices in the same Security Cloud Control Firewall Management organization.
- Run multiple SDCs on one host by following the bootstrap procedure for each additional SDC.

The first SDC name includes the tenant name and the number 1. Each additional SDC is numbered in sequence.

Deploy a VM for running the secure device connector and secure event connector

Configure a virtual machine deployment to run the Secure Device Connector (SDC) and Secure Event Connector for managing communication between Security Cloud Control and your managed devices.

Deploy an SDC in your network to manage communication between Security Cloud Control and devices that are nonperimeter based and do not have a public IP address, or have an open port to the outside interface.

- The SDC monitors Security Cloud Control for commands that need to be executed on your managed devices
- The SDC executes commands on behalf of Security Cloud Control and returns replies from managed devices
- One SDC can support approximately 500 devices depending on device features and configuration file sizes

When using device credentials to connect Security Cloud Control to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between Security Cloud Control and the device.

This procedure describes how to install an SDC in your network, using Security Cloud Control's VM image. This is the recommended and most reliable way to create an SDC.

For more information, see Using Multiple SDCs on a Single Security Cloud Control Tenant.

Before you begin

- Security Cloud Control requires strict certificate checking and does not support Web or Content Proxy inspection between the Secure Device Connector (SDC) and the internet. If using a proxy server, disable inspection for traffic between the SDC and Security Cloud Control.
- The SDC must have full outbound access to the internet on TCP port 443, or the port you have configured for device management.
- The devices that are managed by Security Cloud Control must allow inbound traffic from the SDC VM's IP address.
- Review Connect Allow inbound access for direct cloud connectivity on page 94 to the Secure Device Connector to ensure proper network access.
- If you are using a proxy on your network, ensure that you have all the required details before running the host setup command. Most of the issues are related to incorrect proxy configurations. Important details are:
  - The IP/hostname of your proxy.
  - Whether or not your proxy intercepts traffic and reencrypts it using its own cert. This detail is the cause of most of the complications with the SDC VM setup.
    - If your proxy does intercept traffic, have the root certificate ready when configuring the VM. You can paste it in when prompted so that the host and the SDC know to trust the certificates generated by your proxy.
    - If your proxy does not intercept traffic, then nothing else is required here.
  - The items that are most likely the same for proxied HTTP and HTTPS connections. However, if you use a different proxy for each protocol, you would need all of these for each:
    - The IP address of your proxy
    - The port your proxy uses
    - Whether your proxy requires that the connection to the proxy itself be over HTTPS (typically not the case). For example, if the address of your proxy is listed as https://proxy.corp.com:80 then you would answer yes.

If the listed address is http://proxy.corp.com:80 then you would answer no. Note that both URLs use port 80, but the protocol is different.

- The authentication details of your proxy including:
  - Whether your proxy requires auth (most do not)
  - If yes, then you'll need the username and password available when you configure the host.

- Supported installations:
  - Security Cloud Control supports installing its SDC VM OVF image using the vSphere web client or the ESXi web client.
  - Security Cloud Control does not support installing the SDC VM OVF image using the vSphere desktop client.
  - Security Cloud Control supports installing the SDC on your own Ubuntu instance. Versions 20LTS – 24LTS are currently supported.
  - ESXi 5.1 hypervisor.
- System requirements for a VM with one SDC:
  - 2 vCPUs
  - 2 GB of memory
  - 64 GB of disk space
- Each SDC you add to your host requires an additional 1 vCPU and 1 GB of RAM.
- System requirements for a VM with one SEC (a component that is used in Cisco Security Analytics and Logging):
  - 4 vCPUs minimum
  - 8 GB of memory
- Each SEC you add to the host requires doubling its resources, therefore, these are the requirements for a VMware ESXi host with one SDC and one SEC:
  - 6 vCPUs
  - 10 GB memory
  - 64 GB of disk space
- To configure networking manually on the host, gather this information:
  - The static IP address that you want to use for your VM
  - The passwords to use for the `CDO`user (or whichever user has sudo access) and the SDC user (the user under which Docker runs)
  - The IP address of the DNS server your organization uses
  - The gateway IP address of the network the SDC address is on
  - The FQDN or IP address of your time/NTP server
- The SDC virtual machine is configured to install security patches regularly and to do this, opening port 80 outbound is required.

If your network is using allow/deny lists for outbound connections, you need to allow connections to ubuntu.com so those security updates can be applied.

> **Note**
>
> Ubuntu secures its updates with checksums and only uses HTTP, not HTTPS. To pull security updates, you must allow HTTP connections to ubuntu.com.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.
3. Select the **Secure Connectors** tab on the **Services** page, click the blue plus button, and select **Secure Device Connector**.
4. Click **Download the SDC VM** image. This opens in a new tab.
5. Extract all the files from the .zip file.

   They look similar to these:

   - CDO-SDC-VM-ddd50fa.OVF
   - CDO-SDC-VM-ddd50fa.mf
   - CDO-SDC-VM-ddd50fa-disk1.vmdk

6. Log in to your VMware server as an administrator using the vSphere Web Client.

   > **Note**
   >
   > Do not use the ESXi Web Client.

   Deploy the Secure Device Connector virtual machine from the OVF template by following the prompts.

7. When the setup is complete, power on the SDC VM.
8. Open the console for your new SDC VM.
9. Log in with the `CDO` username. The default password is `adm123`.
10. If you have deployed your own VM, SSH into it and run the command to install the CLI.

    Example

    ```
    curl -O
    https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
     && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh &&
    ./install.sh
    ```

    If you downloaded the Security Cloud Control-provided VM, the CLI is already installed, and you can proceed to the next step.

11. Start the host configuration by running the command:

Example

```
sudo sdc host configure
```

12. When prompted for the password, enter adm123 for the Security Cloud Control-provided VM or whatever admin password you chose for your own VM.
13. Follow the prompts to configure the `SDC` user.
14. When prompted for the networking configuration, choose one of these options:
    - Manually configure this host with a static IP: If you want to specify the IP, gateway, DNS server, and so on, for this host and write it to the system config on the VM.
    - DHCP: If you have a DHCP server assigning static IPs to your VMs.
    - Static IP is already configured and I don't want to change my networking now.
15. When prompted, answer the questions about your proxy configuration.

    Review the detailed list at the top of this topic for all the prerequisites and potential proxy configuration options.
16. If you have configured a proxy, you will be prompted to reboot the VM for all the proxy settings to take effect.

    If you did not configure a proxy, you will not be prompted to reboot.
17. Set a custom internet access test URL.

    You only need to do this if you deny all outbound connections by default. If you do, then specify a publicly accessible web URL such at https://google.com that is on your allow list.
18. Install the latest security patches, some requires os tools and Docker server.
19. When prompted, indicate whether you want to have the script harden your SSH configuration.

    If using our VM, proceed. If you are using your own VM and configuring SSH yourself, you may want to skip this step to avoid changing your current configuration.
20. When prompted to enable automatic updates for the SDC or SEC and the CLI itself, it is recommended that you do this to stay up to date with bug fixes, patches, and new features.

    If your policies prevent you from allowing automatic updates, see Update your Secure Device Connector.

You have successfully deployed and configured a VM to run the Secure Device Connector and Secure Event Connector. The VM is ready to manage communication between Security Cloud Control and your managed devices through the configured SDC.

Deploy a Secure Device Connector On Your VM

Configure and deploy the Secure Device Connector (SDC) on your network VM to securely manage device communications with Cisco Defense Orchestrator.

Enable secure command and message transmission between Cisco Defense Orchestrator and managed devices that lack perimeter exposure or public IP addresses.

When using device credentials to connect Security Cloud Control to a device, it is a best practice to download and deploy a Secure Device Connector (SDC) in your network to manage the communication between Security Cloud Control and the device. Typically, these devices are non-perimeter based, do not have a public IP address, or have an open port to the outside interface. Adaptive Security Appliances (ASAs), FDM-managed devices, and Firepower Management Centers (FMCs) devices can all be onboarded to Security Cloud Control using device credentials.

The SDC monitors Security Cloud Control for commands that need to be executed on your managed devices, and messages that need to be sent to your managed devices. The SDC executes the commands on behalf of Security Cloud Control ,

sends messages to Security Cloud Control on behalf of the managed devices, and returns replies from the managed devices to Security Cloud Control .

The number of devices a single SDC can manage depends on the features implemented on those devices and the size of their configuration files. For the purposes of planning your deployment, however, we expect one SDC to support approximately 500 devices. See Multiple Secure Device Connectors on one organization on page 97 for more information.

This procedure describes how to install an SDC in your network by using your own virtual machine image.

> **Note**
>
> The preferred, easiest, and most reliable way to install an SDC is to download Security Cloud Control 's SDC OVA image and install it.

Before you begin

- Security Cloud Control requires strict certificate checking and does not support a Web/Content Proxy between the SDC and the Internet.
- The SDC must have full outbound access to the Internecdot on TCP port 443 in order for it to communicate with Security Cloud Control .
- Devices that reach Security Cloud Control through the SDC must allow inbound access from the SDC on port 443.
- Review Connect to Security Cloud Control using Secure Device Connector for networking guidelines.
- VMware ESXi host installed with vCenter web client or ESXi web client.

  > **Note**
  >
  > We do not support installation using the vSphere desktop client.

- ESXi 5.1 hypervisor.
- Ubuntu 22.04 and Ubuntu 24.04 operating system.
- System requirements for a VM with only an SDC:
  - VMware ESXi host needs 2 CPUs.
  - VMware ESXi host needs a minimum of 2 GB of memory.
  - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice. This value assumes you are using Logical Volume Management (LVM) with the partition so you can expand required disk space as needed.
- System requirements for a VM with an SDC and **a single** Secure Event Connector (SEC) for your tenant. (The SEC is a component used in Cisco Security Analytics and Logging).

  Each SEC you add to the VMware ESXi host requires an additional 4 CPUs and an additional 8 GB of memory.

  Therefore, these are the requirements for a VMware ESXi host with one SDC and one SEC:
  - VMware ESXi host needs 6 CPU.
  - VMware ESXi host needs a minimum of 10 GB of memory.

- VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice.

- After you have updated the CPU and memory on the VM, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.
- Users performing this procedure should be comfortable working in a Linux environment and using the vi visual editor for editing files.
- If you are installing your on-premise SDC on a CentOS virtual machine, we recommend you install Yum security patches on a regular basis. Depending on your Yum configuration, to acquire Yum updates, you may need to open outbound access on port 80 as well as 443. You will also need to configure yum-cron or crontab to schedule the updates. Work with your security-operations team to determine if any security policies need to change to allow you to get the Yum updates.

Note

Before you get started : Do not copy and paste the commands in the procedure into your terminal window, type them instead. Some commands include an "n-dash" and in the cut and paste process, these commands can be applied as an "m-dash" and that may cause the command to fail.

Procedure

1. Log on to the Security Cloud Control tenant you are creating the SDC for.
2. From the Security Cloud Control Home page, click **Firewall**.
3. In the left pane, click **Administration** > **Integrations** > **Secure Connectors** .
4. On the **Services** page, select the **Secure Connectors** tab, click the blue plus button, and select **Secure Device Connector** .
5. Copy the bootstrap data in step 2 on the window to a notepad.
6. Install a **CentOS 7 virtual machine** with at least the following RAM and disk space allotted to the SDC:
   - 8GB of RAM
   - 10GB disk space
7. Once installed, configure basic networking such as specifying the IP address for the SDC, the subnet mask, and gateway.
8. Configure a DNS (Domain Name Server) server.
9. Configure a NTP (Network Time Protocol) server.
10. Install an SSH server on CentOS for easy interaction with SDC's CLI.
11. Run a Yum update and then install the packages: **open-vm-tools** , **nettools** , and **bind-utils**

```
[root@sdc-vm ~]#
yum update -y
[root@sdc-vm ~]#
yum install -y open-vm-tools net-tools bind-utils
```

12. Install the AWS CLI package; see https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html .

> **Note**
>
> Do not use the **--user** flag.

13. Install the Docker CE packages; see https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce

> **Note**
>
> Use the "Install using the repository" method.

14. Start the Docker service and enable it to start on boot:

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service
to
    /usr/lib/systemd/system/docker.service.
```

15. Create two users: `cdo` and `sdc` . Use the `cdo` user to perform administrative tasks without directly accessing the root user. The `sdc` user will be designated for running the SDC docker container.

```
[root@sdc-vm ~]#
                    useradd cdo
[root@sdc-vm ~]#
                    useradd sdc -d /usr/local/cdo
```

16. Set a password for the `sdc` user.

```
[root@sdc-vm ~]#
                    passwd cdo
Changing password for user cdo.
New password:
                    <type password>
Retype new password:
                    <type password>
passwd: all authentication tokens updated successfully.
```

17. Add the `sdc` user to the `wheel` group to give it administrative (sudo) privileges.

```
[root@sdc-vm ~]#
                    usermod -aG wheel cdo
[root@sdc-vm ~]#
```

18. When Docker is installed, there is a user group created. Depending on the version of CentOS/Docker, this may be called either "docker" or "dockerroot". Check the /etc/group file to see which group was created, and then add the sdc user to this group.

```
[root@sdc-vm ~]#
                    grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]#
                    usermod -aG docker sdc
[root@sdc-vm ~]#
```

19. If the /etc/docker/daemon.json file does not exist, create it, and populate with the contents below. Once created, restart the docker daemon.

> **Note**
>
> Make sure that the group name entered in the "group" key matches the group you found in the /etc/group file the previous step.

```
                    [root@sdc-vm ~]#
                    cat /etc/docker/daemon.json
{
   "live-restore": true,
   "group": "
                    docker
                    "
}
[root@sdc-vm ~]#
                    systemctl restart docker
[root@sdc-vm ~]#
```

20. If you are currently using a vSphere console session, switch over to SSH and log in with the `cdo` user. Once logged in, change to the `sdc` user. When prompted for a password, enter the password for the `cdo` user.

```
                    [CDO@sdc-vm ~]$
                    sudo su sdc
          [sudo] password for cdo: <
                    type password for cdo user
                    >
          [sdc@sdc-vm ~]$
```

21. Change directories to **/usr/local/CDO** .
22. Create a new file called `bootstrapdata` and paste the bootstrap data from Step 2 of the **Deploy an On-Premises Secure Device Connector** wizard into this file. **Save** the file. You can use `vi` or `nano` to create the file.

23. The bootstrap data comes encoded in base64. Decode it and export it to a file called `extractedbootstrapdata`

```
                        [sdc@sdc-vm ~]$
                        base64 -d /usr/local/
                        CDO/bootstrapdata >
/usr/local/CDO/extractedbootstrapdata
               [sdc@sdc-vm ~]$
```

Run the cat command to view the decoded data. The command and decoded data should look similar to this:

```
                        [sdc@sdc-vm ~]$
                        cat /usr/local/
                         CDO/extractedbootstrapdata
                CDO_TOKEN="<token string>"
                CDO_DOMAIN="www.defenseorchestrator.com"
                CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

24. Run the following command to export the sections of the decoded bootstrap data to environment variables.

```
                        [sdc@sdc-vm ~]$
                      sed -e 's/^/export /g' extractedbootstrapdata > sdcenv
 && source sdcenv
               [sdc@sdc-vm ~]$
```

25. Download the bootstrap bundle from Security Cloud Control .

```
                        [sdc@sdc-vm ~]$
                        curl -O -H "Authorization: Bearer
                         $
                        CDO_TOKEN" "$CDO_BOOTSTRAP_URL"

                                 100 10314 100 10314 0 0 10656 0 --:--:--
--:--:-- --:--:-- --:--:-- 10654
                [sdc@sdc-vm ~]$
                        ls -l /usr/local/
                        CDO/*SDC

                                  -rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48
/usr/local/CDO/
                        tenant-name-SDC
```

26. Extract the SDC tarball, and run the `bootstrap.sh` file to install the SDC package.

```
                        [sdc@sdc-vm ~]$
                        tar xzvf /usr/local/
                        CDO/tenant-name-SDC
                <snipped - extracted files>
                [sdc@sdc-vm ~]$
```

```
               [sdc@sdc-vm ~]$
                        /usr/local/
                        CDO/bootstrap/bootstrap.sh
               [2018-07-23 13:54:02] environment properly configured
               download: s3://onprem-sdc/toolkit/prod/toolkit.tar to
toolkit/toolkit.tar
               toolkit.sh
               common.sh
               [2018-07-23 13:54:04] startup new container
             Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest'
 locally

sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
Pulling from
               ciscodefenseorchestrator/sdc_prod
               08d48e6f1cff: Pull complete
               ebbd10b629b1: Pull complete
               d14d580ef2ed: Pull complete
               45421d451ab8: Pull complete
               <snipped - downloads>
               no crontab for sdc
```

The SDC should now show "Active" in Security Cloud Control .

The Secure Device Connector is successfully installed on your VM, enabling secure management and communication with your devices through Cisco Defense Orchestrator.

Bootstrap a secure device connector on the deployed host

Configure a Secure Device Connector by bootstrapping it on your deployed host using the bootstrap data from the user interface.

Bootstrap your Secure Device Connector to establish a secure connection between your on-premises devices and Cisco Defense Orchestrator.

After deploying the Secure Device Connector host, you need to bootstrap it with the configuration data from your CDO tenant to make it operational.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.
3. On the **Services** page, select the **Secure Connectors** tab, click the + icon, and select **Secure Device Connector**.
4. Copy the bootstrap data in step 2 on the window to a notepad.
5. SSH into your VM using the admin user, typically **cdo**, and your chosen password.
6. Switch to the **SDC** user using the command:

```
sudo su - sdc
```

7. Bootstrap your new SDC using the command:

```
sdc bootstrap <paste-your-bootstrap-data-here>
```

8. Select the version of the SDC you want to use.

   We have three options for the SDC version:

   - SDC 2024- This is the version that most will want to run.
   - SDC 2024 with FIPS enabled- Choose this version if you are subject to FedRamp compliance.
   - SDC Legacy- This version is no longer receiving feature updates and it is recommended to run SDC 2024 instead.

9. Validate that your SDC is active and operational on the user interface, and also on the host by running:

   The CLI pulls the container image and starts the SDC and you can validate that your SDC is active and operational on the user interface, and also on the host by running:

```
sdc show running
```

You should now see an SDC for your tenant.

Deploy a secure device connector to vSphere using terraform

Configure a Secure Device Connector deployment to vSphere using Terraform modules and the Security Cloud Control Terraform Provider.

This task enables you to automate the deployment of a Secure Device Connector to your vSphere environment using infrastructure as code with Terraform.

Use this procedure when you want to deploy an SDC to vSphere infrastructure using the Security Cloud Control SDC Terraform module for vSphere in conjunction with the Security Cloud Control Terraform Provider.

Before you begin

- You have vSphere datacenter version 7 and above
- You have an admin account on the datacenter with permissions to do the following:
  - Create VMs
  - Create folders
  - Create content libraries
  - Upload files to content libraries
- Terraform knowledge

Follow these steps to deploy a Secure Device Connector to vSphere using Terraform:

Procedure

---

1. Create an API-only user in Security Cloud Control and copy the API token.

   To know how to create an API-only user, see Create API Only Users.

2. Configure the Security Cloud Control Terraform provider in your Terraform repository.

   Follow the instructions in Security Cloud Control Terraform Provider.

Example

```
terraform {
  required_providers {
    cdo = {
      source = "CiscoDevNet/cdo"
      version = "0.7.0"
    }
  }
}

provider "cdo" {
  base_url = "<the CDO URL you use to access CDO>"
  api_token = "<the API Token generated in step 1>"
}
```

3. Write Terraform code to create a **cdo_sdc** resource using the Security Cloud Control Terraform provider.

   See the Terraform registry for Security Cloud Control-SDC resource for more information.

   The **bootstrap_data** attribute of this resource is populated with the value of the Security Cloud Control bootstrap data and is provided to the **cdo_sdc** Terraform module in the next step.

   Example

   ```
   Resource "cdo_sdc" "my-sdc" {
     name = "my-sdc-in-vsphere"
   }
   ```

4. Write Terraform code to create the SDC in vSphere using Security Cloud Control_sdc Terraform module.

   Example

   ```
   data "cdo_tenant" "current" {}

   module "vsphere-cdo-sdc" {
     source               = "CiscoDevNet/cdo-sdc/vsphere"
     version              = "1.0.0"
     vsphere_username     = "<replace-with-username-with-admin-privileges>"
     vsphere_password     = "<super-secure-password>"
     vsphere_server       = "<replace-with-address-of-vsphere-server>"
     datacenter           = "<replace-with-datacenter-name>"
     resource_pool        = "<replace-with-resource-pool-name>"
     cdo_tenant_name      = data.cdo_tenant.current.human_readable_name
     datastore           = "<replace-with-name-of-datastore-to-deploy-vm-in>"

     network              = "<replace-with-name-of-network-to-deploy-vm-in>"
     host                 = "<replace-with-esxi-host-address>"
     allow_unverified_ssl = <boolean; set to true if your vsphere server does
   not have a valid SSL certificate>
     ip_address           = "<sdc-vm-ip-address; must be in the subnet of the
   assigned network for the VM>"
     gateway              = "<replace-with-network-gateway-address>"
     cdo_user_password    = "<replace-with-password-for-cdo-user-in-sdc-vm>"
     root_user_password   = "<replace-with-password-for-root-user-in-sdc-vm>"
     cdo_bootstrap_data   = cdo_sdc.sdc-in-vsphere.bootstrap_data
   }
   ```

Note that the VM created has two users–a **root** user and a user called **cdo**–and the IP Address of the VM is configured statically. The **cdo_bootstrap_data** attribute is given the value of the **bootstrap_data** attribute generated when the **cdo_sdc** resource is created.

5. Plan and apply your Terraform using **terraform plan** and **terraform apply**.

   See the Security Cloud Control Automation Repository in the CiscoDevNet for a complete example.

The SDC is deployed to your vSphere environment and connects to Security Cloud Control. If your SDC stays in the onboarding state, connect to the vSphere VM using remote console, log in as the **cdo** user, and execute the following commands:

```
sdc host status
```

Depending on the readout, you may need to manually run:

```
sdc host configure
```

Note

The Security Cloud Control Terraform modules are published as Open Source Software under the Apache 2.0 license. You can file issues on GitHub if you require support.

Deploy a secure device connector on an AWS VPC using a terraform module

Configure deployment of a secure device connector on an AWS VPC using a Terraform module for network security management.

Deploy a Secure Device Connector (SDC) on your AWS VPC infrastructure to establish secure communication between your network devices and Security Cloud Control.

The Secure Device Connector serves as a secure bridge between your on-premises or cloud-based network devices and Security Cloud Control, enabling centralized management and orchestration of your security devices through a cloud-based platform.

Before you begin

Review these prerequisites before attempting to deploy an SDC on your AWS VPC:

- Security Cloud Control requires strict certificate checking and does not support Web/Content Proxy inspection between the SDC and the Internet. If using a proxy server, disable inspection for traffic between the Secure Device Connector (SDC) andSecurity Cloud Control.
- See Connect Security Cloud Control to the Secure Device Connector to ensure proper network access.
- You require an AWS account, an AWS VPC with at least one subnet, and an AWS Route53-hosted zone.
- Ensure you have the Security Cloud Control bootstrap data, your AWS VPC ID, and its subnet ID handy.
- Ensure that the private subnet to which you deploy the SDC has a NAT gateway attached.
- Open traffic on the port on which your firewall management HTTP interface is running, from your firewalls to the Elastic IP attached to the NAT gateway.

Follow these steps to deploy a Secure Device Connector on an AWS VPC using a Terraform module:

Procedure

1. Add the following lines of code in your Terraform file; make sure you manually enter inputs for variables:

   Example

   ```
   module "example-sdc" {
     source              =
   "git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"

     env                 = "example-env-ci"
     instance_name       = "example-instance-name"
     instance_size       = "r5a.xlarge"
     cdo_bootstrap_data  = "<replace-with-cdo-bootstrap-data>"
     vpc_id              = <replace-with-vpc-id>
     subnet_id           = <replace-with-private-subnet-id>
   }
   ```

   See the Secure Device Connector Terraform module for a list of input variables and descriptions.

2. Register **instance_id** as an output in your Terraform code:

   Example

   ```
   output "example_sdc_instance_id" {
     value = module. example-sdc.instance_id
   }
   ```

   You can use the **instance_id** to connect to the SDC instance for troubleshooting using the AWS Systems Manager Session Manager (SSM). See Outputs in the Secure Device Connector Terraform module for a list of available outputs.

   What to do next:

   For any troubleshooting of your SDC, you need to connect to the SDC instance using AWS SSM. See AWS Systems Manager Session Manager to know more about how to connect to your instance. Note that the ports to connect to the SDC instance using SSH are not exposed because of security reasons.

   > **Note**
   >
   > The Security Cloud Control Terraform modules are published as Open Source Software under the Apache 2.0 license. You can file issues on GitHub if you require support.

The Secure Device Connector is deployed on your AWS VPC and is ready to establish secure communication between your network devices and Security Cloud Control. You can use the instance ID output for troubleshooting through AWS Systems Manager Session Manager.

Migrate an On-Premises secure device connector and secure event connector from a CentOS 7 virtual machine to an ubuntu virtual machine

Configure migration of SDCs and SECs from deprecated CentOS 7 virtual machines to supported Ubuntu virtual machines.

Migrate Security Cloud Control's on-premises Secure Device Connector (SDC) from end-of-life CentOS 7 virtual machines to supported Ubuntu virtual machines.

Since CentOS 7 is now end-of-life and has been deprecated by Security Cloud Control, this migration process helps you migrate all SDCs from CentOS 7 to an Ubuntu virtual machine.

- The SDC must have full outbound access to the internet on TCP port 443.
- The Ubuntu virtual machine running the SDC must have network access to the management interfaces of the devices it communicates with, such as ASAs and Cisco IOS devices.
- Any networking rules created for the IP address or FQDN of the old SDC VM to reach your devices should be recreated with the IP address or FQDN of the new SDC VM.
- The migration will take 10 to 15 minutes. During this time, your device will continue to enforce security policy and route network traffic, but you will not be able to communicate with it through the SDC.

Before you begin

Deploy a new host by following the instructions on Deploy a VM for Running the Secure Device Connector and Secure Event Connector.

Follow these steps to migrate the SDC and/or SEC:

Procedure

1. Download the new VM image from here.
2. Unzip the CDO-SDC_VM.zip file.

   You should see three VM files named similarly to the following:

   - CDO-SDC-VM-708cd33-2024-05-30-2031-disk1.vmdk
   - CDO-SDC-VM-708cd33-2024-05-30-2031.mf
   - CDO-SDC-VM-708cd33-2024-05-30-2031.ovf
3. Deploy the VM you just downloaded.
4. Note the static IP address or FQDN you assigned to the new VM.
5. Using SSH, log in to the new VM as the **CDO** user.
6. At the prompt, enter the command:

   Example

   ```
   sudo sdc host configure
   ```

   Note

   - Follow the prompts in the migration script closely. The script is well-documented and will guide you through the migration process, explaining each step.
   - At the end of the migration script, you will receive a message indicating that your SDC has been migrated to the new VM. The SDC will retain its name after the migration.
7. Using SSH, log in to the old (CentOS) SDC as the **CDO** user.
8. Install the CLI using the command:

Example

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh &&
./install.sh
```

9. Run the following command and follow the prompts:

Example

```
sudo sdc migrate now
```

10. Log in to your Security Cloud Control tenant.
11. Select the SDC you migrated, and in the **Actions** pane, click **Request Heartbeat**.

> **Note**
>
> Ensure that the SDC is in the **Active** state.

12. Install the CLI on the old (CentOS) SDC using the command:

Example

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh &&
./install.sh
```

13. Run the following command and follow the prompts:

Example

```
sudo sdc eventing migrate
```

14. Configure your devices to point to the new IP address of the SEC or shut down the old host and assign the new host the same IP address that the old host had so that the devices do not need to be updated.

The SDC and SEC are successfully migrated from the CentOS 7 virtual machine to the Ubuntu virtual machine. For information on the state of the SEC, see Use Health Check to Learn the State of your Secure Event Connector.

What to do next

Do Not Restart Your Old SDC

After the migration is complete, do not restart your old SDC on the original virtual machine.

Revert Failed Migration

If the migration fails for any reason, or the result is not what you are expecting and you want to revert to the old SDC, follow the instructions below:

- Log in to the new VM and switch to the **SDC** user.

- Ensure the SDC is not currently running on the new VM using the command: **docker ps**
- If the SDC is running, run the command: **SDC stop**
- Confirm that the SDC has stopped running by executing **docker ps** again.
- Log in to the old VM and run the command: **SDC migrate revert**
- When the old SDC is active and visible in the UI, return to the new VM and execute the command: **SDC delete <your-tenant-name-here>**
- Refresh the browser completely, click on the SDC, and verify that the IP of the old host appears in the sidebar. If the new IP still appears despite these steps, request a new health check, refresh the browser, and check again.
- To revert the SEC migration, run the command: **SDC eventing revert**

Change the IP address of a secure device connector

Configure a new IP address for your Secure Device Connector (SDC) deployed on your own VM when migrating VMs to a different data center or for other network changes.

This task enables you to assign a new IP address to your SDC when you need to migrate your VMs to a different data center or make other network configuration changes while maintaining connectivity to Security Cloud Control.

When you are using a Secure Device Connector (SDC) deployed on your own VM, you might need to change the IP address of your SDC for several reasons, such as migrating your VMs to a different data center. You will not be required to re-onboard any devices to Security Cloud Control after changing the SDC's IP address.

Before you begin

- You must be an admin to perform this task.
- The SDC must have full outbound access to the Internet on TCP port 443, or the port you have configured for device management.

> **Note**
>
> You will not be required to re-onboard any devices to Security Cloud Control after changing the SDC's IP address.

Follow these steps to change the IP address of a Secure Device Connector:

Procedure

Your SDC now has the new IP address and maintains connectivity to Security Cloud Control. All existing device connections remain functional without requiring re-onboarding.

Allow inbound access for direct cloud connectivity

Provides the IP addresses and configuration requirements for allowing inbound access when connecting devices directly to Security Cloud Control through the cloud connector.

Security Cloud Control connects to the devices that it manages through the cloud connector or through an (SDC). When you connect Security Cloud Control Firewall Management directly to a device through the cloud connector, allow inbound access on port 443, or on the port that you have configured for device management, from the IP addresses for your region.

Region	URL	Allow inbound access from
Asia-Pacific-Japan (APJ)	https://security.cisco.com	54.199.195.111, 52.199.243.0
Australia (AUS)	https://security.cisco.com	13.55.73.159, 13.238.226.118
Europe, Middle East, and Africa (EMEA)	https://security.cisco.com	35.157.12.126, 35.157.12.15
India (IN)	https://security.cisco.com	35.154.115.175 13.201.213.99
United States (US)	https://security.cisco.com	52.34.234.2 52.36.70.147

Special Consideration for Connecting an ASA to an SDC

Specifically, for ASA the SDC uses the same secure communications channel used by ASDM.

If the ASA under management is also configured to accept AnyConnect VPN Client connections, the ASDM HTTP server port must be changed to a value of 1024 or higher. Note that this port number will be the same port number used when onboarding the ASA device into Security Cloud Control.

Example ASA Commands

These examples assume that the ASA outside interface is named 'outside' and an AnyConnect client is configured on the ASA so the ASDM HTTP server is listening on port 8443.

To enable the outside interface, enter these commands:

Asia-Pacific-Japan Region:

- HTTP 54.199.195.111 255.255.255.255 outside
- HTTP 52.199.243.0 255.255.255.255 outside

Australia Region

- HTTP 13.55.73.159 255.255.255.255 outside
- HTTP 13.238.226.118 255.255.255.255 outside

EMEA Region

- HTTP 35.157.12.126 255.255.255.255 outside
- HTTP 35.157.12.15 255.255.255.255 outside

India Region

- HTTP 35.154.115.175 255.255.255.255 outside
- HTTP 13.201.213.99 255.255.255.255 outside

United States Region

- HTTP 52.34.234.2 255.255.255.255 outside

- HTTP 52.36.70.147 255.255.255.255 outside

To enable the ASDM HTTP server port, IN the case where AnyConnect VPN Client is IN use, enter this command:

HTTP server enable 8443

Rename a secure device connector

Configure a new name for a Secure Device Connector to customize its identification in the CDO interface.

Rename a Secure Device Connector to provide a more descriptive or meaningful identifier for easier management and identification within the CDO interface.

You can customize the name of any Secure Device Connector to better reflect its purpose, location, or function in your network infrastructure. This helps with organization and identification when managing multiple connectors.

Procedure

1. In the left pane, choose **Administration** > **Integrations** > **Secure Connectors**.
2. Select the SDC you want to rename.
3. In the Details pane, click the edit icon next to the name of the SDC.
4. Rename the SDC.

This new name will appear wherever the SDC name appears in the Security Cloud Control interface including the Secure Device Connectors filter of the **Security Devices** pane.

Specify a default Secure Device Connector

Configure which SDC is automatically selected as the default for device onboarding.

This task allows you to designate a specific SDC as the default connector that will be automatically associated with devices during the onboarding process.

When you onboard devices that connect to Security Cloud Control Firewall Management through an SDC, they are associated with the default SDC for your tenant unless you specify another SDC during onboarding.

You can specify which SDC is selected by default on the Secure Connectors page:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Administration** > **Secure Connectors**.
3. Select the SDC that you want to be the default.
4. In the Actions pane, click **Make Default**. If you don't see the Make Default action, then the SDC already is the default SDC.

The selected SDC is now configured as the default connector and will be automatically assigned to new devices during onboarding unless another connector is explicitly specified.

Update a Secure Device Connector manually

Configure a manual update of your SDC when automatic updates encounter errors.

This task serves as a troubleshooting tool to manually update your SDC when automatic updates fail or encounter errors.

Use this task as a troubleshooting tool. The source says that the SDC is usually updated automatically and that you should not need to perform a manual update unless errors occur.

Procedure

1. Connect to your SDC. You can connect using SSH or use the console view in your Hypervisor.
2. Log in to the SDC as the admin user, typically **cdo**.
3. Switch to the SDC user to update the SDC docker container:

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

4. Upgrade the SDC:

```
sdc upgrade
```

> **Note**
>
> **Recommended updates and maintenance on the SDC Virtual Machine**
>
> Ensure that you monitor and apply updates to the SDC VM running on Ubuntu Linux following your organisation's internal IT security and patch management policies. We highly recommend regularly reviewing and applying relevant security patches to ensure that the SDC VM remains secure and functions optimally within your network environment.

The SDC is successfully updated with the latest version and can resume normal operations.

Multiple Secure Device Connectors on one organization

Describes the capability to deploy multiple SDCs within a single tenant for enhanced device management and network segmentation.

Multiple Secure Device Connectors on one organization is a deployment capability that

- allows installation of an unlimited number of SDCs on a single tenant
- enables management of more devices and placement of connectors in different network segments while keeping those devices in the same Security Cloud Control Firewall Management tenant, and
- uses the same deployment procedure for subsequent SDCs as the first SDC.

Deployment and naming information

The deployment and naming characteristics include:

- The procedure for deploying a second or subsequent SDC is the same for deploying your first SDC.
- The initial SDC for your tenant incorporates the name of your tenant and the number 1. Each additional SDC is numbered in order.

Find devices that use the same Secure Device Connector

Configure filtering to locate devices that connect through the same SDC.

This task helps you identify which devices share the same SDC connection for management and troubleshooting purposes.

Use this procedure when you need to view devices grouped by their SDC connection to understand your network topology or troubleshoot connectivity issues.

Before you begin

Follow these steps to find devices that connect through the same SDC:

Procedure

1. In the left pane, **Security Devices**.
2. Click the **Devices** tab to locate the device.
3. Click the appropriate device type tab.
4. If there is any filter criteria already specified, click the **clear** button at the top of the **Security Devices** page to show all the devices and services you manage with Security Cloud Control.
5. Click the filter button to expand the filter menu.
6. In the **Secure Device Connectors** section of the filter, check the name of the SDC(s) you're interested in.

   The **Security Devices** page displays only the devices that connect to Security Cloud Control through the SDC you checked in the filter.
7. (Optional) Check additional filters in the filter menu to refine your search further.
8. (Optional) When you're done, click the **clear** button at the top of the **Security Devices** page to show all devices and services you manage with Security Cloud Control.

You can now view all devices that connect through the selected SDC and use this information for management or troubleshooting purposes.

Remove a Secure Device Connector

Configure the removal of a secure device connector from your network by following this deletion process.

Remove an unused or problematic secure device connector from your infrastructure to maintain proper network management and connectivity.

Deleting an SDC is not reversible. After you remove it, you cannot manage the devices that were connected to that SDC until you install a new SDC and reconnect the devices. Reconnecting devices can require you to enter administrator credentials again.

Before you remove an SDC, move the connected devices to another SDC or remove them from Security Cloud Control Firewall Management.

Procedure

1. Remove any devices connected to the SDC you want to delete. You can do this one of two ways:
   - Remove from Security Cloud Control any devices connected to the SDC you want to delete.
     a. See Find all Devices that Connect to Security Cloud Control Using the Same SDC to identify all the devices used by the SDC.
     b. In the **Security Devices** page, select all the devices you identified.

c. In the Device Actions pane, click **Remove** and click **OK** to confirm your action.

2. From the Security Cloud Control Home page, click **Firewall**.
3. In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.
4. On the **Services** page with the **Secure Connectors** tab selected, click the blue plus button and select **Secure Device Connector**.
5. In the Secure Connectors table, select the SDC you want to remove. Its device count should now be zero.
6. In the Actions pane, click **Remove**. You receive this warning:

   Warning

   You are about to delete <sdc_name>. Deleting the SDC is not reversible. Deleting the SDC will require you to create and onboard a new SDC before you can onboard, or re-onboard, your devices.

   Because you currently have onboarded devices, removing the SDC will require you to reconnect those devices and provide credentials again after setting up a new SDC.

   - If you have any questions or concerns, click **Cancel** and contact Security Cloud Control support.
   - If you wish to proceed, enter <sdc_name> in the text box below and click **OK**.

7. In the confirmation dialog box, if you wish to proceed, enter your SDC's name as it is stated in the warning message.
8. Click **OK** to confirm the SDC removal.

The secure device connector is permanently removed from your network infrastructure and can no longer manage connected devices.

5 Manage objects

Topics:

- Introduction to objects
- Network objects
- URL objects
- Geolocation objects
- DNS group objects
- Certificate objects
- ASA trustpoint objects
- IPsec proposal and IKE policy objects
- Global IKE policies
- Remote access VPN objects
- Service objects
- Security group tag group
- ASA time range objects
- Troubleshooting Objects

This chapter describes how to create and manage reusable objects.

Introduction to objects

Learn how objects help you reuse network, URL, and service values across policies and manage object issues from the Objects page.

An object is a reusable container of information that you can use in one or more security policies. Objects help you maintain policy consistency because you can define a value once, use it in multiple policies, and update every policy that uses the object by changing the object.

When you onboard a device, Security Cloud Control Firewall Management recognizes all the objects used by that device, saves them, and lists them on the **Objects** page. From the **Objects** page, you can edit existing objects and create new ones to use in your security policies.

Security Cloud Control Firewall Management calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

You can use Security Cloud Control Firewall Management to manage objects in these ways:

- Search for and filter all your objects based on a variety of criteria.
- Find duplicate, unused, and inconsistent objects, and then consolidate, delete, resolve, ignore, or unignore object issues.
- Find and delete unassociated objects if they are not needed.
- Discover objects that are shared across devices.
- Evaluate which policies and devices are affected before you commit an object change.
- Compare a set of objects and their relationships with different policies and devices.
- Capture objects that are in use after a device is onboarded to Security Cloud Control Firewall Management.

Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices:

- **Duplicate objects**: Two or more objects on the same device have different names but the same values. These objects usually serve similar purposes and are used by different policies. Duplicate objects are identified by this issue icon:
- **Inconsistent objects**: Two or more devices have objects with the same name but different values. This issue can occur when objects start with the same name and content but later diverge. Inconsistent objects are identified by this issue icon:
- **Unused objects**: An object exists in a device configuration but is not referenced by another object, an access list, or a NAT rule. Unused objects are identified by this issue icon:

You can also create objects for immediate use in rules or policies. You can create an object that is unassociated with any rule or policy. When you use that unassociated object in a rule or policy, Security Cloud Control Firewall Management creates a copy of it and uses the copy.

You can view the objects managed by Security Cloud Control Firewall Management by navigating to the **Objects** menu or by viewing them in the details of a network policy.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Security Cloud Control for more information.

Supported object types

An overview of supported object types for devices, including identity certificates, trusted CA certificates, CSR handling, export, edit, and deletion tasks.

The object types that you can create and manage depend on the managed device type.

Common object types
Table 2: Common Objects

Object Type	Description
Network	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.
URL	Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies.

ASA object types
Table 3: Adaptive Security Appliance (ASA) Object Types

Object	Description
Network	Defines host or network addresses. This category includes network objects and network groups.
Service	Defines protocols or ports that are part of the TCP/IP protocol suite. This category includes service objects, service groups, and port groups.
Time Range	Defines a start time, an end time, and optional recurring entries for time-based access to features or assets.
Trustpoints	Manages and tracks digital certificates in ASA.

FDM-managed device object types
Table 4: FDM-Managed Device Object Types

Object	Description
AnyConnect Client Profile	Represents files used in configurations, typically for remote access VPN policies. These objects can contain AnyConnect Client Profile and AnyConnect Client Image files.
Certificate Filter	Provides digital identification for authentication. Certificates are used for SSL, TLS, and DTLS connections, such as HTTPS and LDAPS.
DNS Group	Defines DNS servers that resolve fully qualified domain names (FQDNs), such as www.example.com, to IP addresses. You can configure different DNS group objects for management and data interfaces.
Geolocation	Defines countries and continents that host the source or destination of traffic. You can use geolocation objects in policies instead of IP addresses.

Object	Description
IKEv1 Policy	Contains the parameters required for IKEv1 policies when defining VPN connections.
IKEv2 Policy	Contains the parameters required for IKEv2 policies when defining VPN connections.
IKEv1 IPSEC Proposal	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 1 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.
IKEv2 IPSEC Proposal	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.
Network	Defines host or network addresses. This category includes network objects and network groups.
Service	Defines protocols or ports that are part of the TCP/IP protocol suite. This category includes service objects, service groups, and port groups.
SGT Group	Identifies source or destination addresses based on a security group tag (SGT) assigned by Cisco ISE.
URL	Defines URLs or IP addresses for web requests. URL objects and URL groups can be used for manual URL filtering in access control policies or blocking in Security Intelligence policies.

On-Premises Firewall Management Center object types

Table 5: On-Premises Secure Firewall Management Center Object Types

Object	Description
Network	Defines host or network addresses. This category includes network objects and network groups.
Service	Defines protocols or ports that are part of the TCP/IP protocol suite. This category includes service objects, service groups, and port groups.

Meraki object types

Table 6: Meraki Object Types

Object	Description
Network	Defines host or network addresses. This category includes network objects and network groups.

Object	Description
Service	Defines protocols or ports that are part of the TCP/IP protocol suite. This category includes service objects, service groups, and port groups.

Shared objects

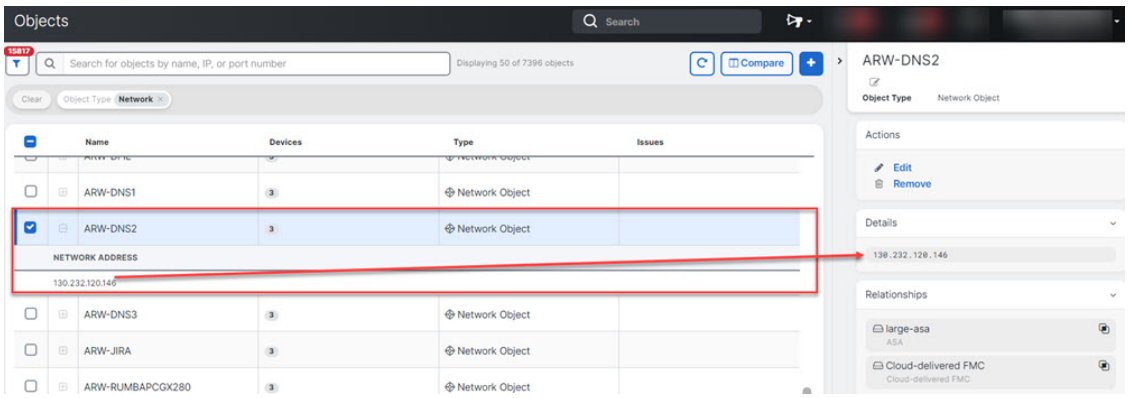
Learn how shared objects in Security Cloud Control help maintain policy consistency by letting one object definition apply across multiple devices and policies.

A shared object is an object on multiple devices that has the same name and the same contents. Shared objects help you maintain policies because one object change affects every policy that uses that shared object.

Shared objects are identified by this icon

on the **Objects** page. Shared objects make it easy to maintain policies because you can modify an object in one place and that change affects all the other policies that use that object. Without shared objects, you would need to modify all the policies individually that require the same change.

When looking at a shared object, Security Cloud Control shows you the contents of the object in the object table. Shared objects have exactly the same contents. Security Cloud Control shows you a combined or "flattened" view of the elements of the object in the details pane. Notice that in the details pane, the network elements are flattened into a simple list and not directly associated with a named object.



Object Overrides

An object override lets you customize a shared object for specific devices. When a device has an override, Security Cloud Control Firewall Management uses the override value for that device instead of the object's default value.

Overrides allow you to maintain a single shared policy across devices while tailoring individual object values where needed.

Use overrides when you want to maintain one shared policy across devices but need specific devices to use different object values. For example, a shared print-server object can use the default value 10.1.1.100 for most offices, while Office B uses an override value of 10.2.1.100.

Overrides on network object groups

For network object groups, overrides fully replace the default values for the devices that are assigned to the override. A device with an override receives only the override values, not the default values.

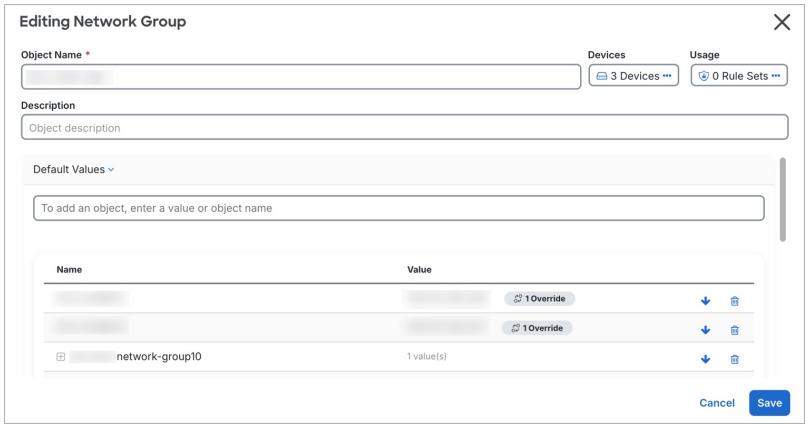
This replacement behavior has these effects:

- Changes to default values affect only devices without overrides.
- Changes to an override affect only the devices assigned to that override.

- If a device needs the default values plus a local value, add all required values to the override.

For example, a shared dns-servers network group contains default values primary-dns (10.0.1.53) and secondary-dns (10.0.2.53) for Branch A, Branch B, and Branch C. Branch C also needs local-dns-cache (10.30.1.53). Because a network group override replaces the defaults, the Branch C override must contain primary-dns, secondary-dns, and local-dns-cache.

If you later add a default value, such as tertiary-dns, Branch A and Branch B receive the new default value automatically. Branch C does not receive it until you add tertiary-dns to the Branch C override.



Unassociated objects

An unassociated object is not associated with any rule or policy. When you use an unassociated object in a rule or policy, Security Cloud Control Firewall Management creates and uses a copy of that object. The original unassociated object remains available until a nightly maintenance job deletes it or you delete it manually.

Security Cloud Control Firewall Management keeps unassociated objects as a copy so that configuration data is not lost if the related rule or policy is deleted accidentally.

To view unassociated objects, choose **Objects** > , and check **Unassociated**.

Compare objects

Use object comparison to review up to three objects side by side and inspect their details and relationships.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects** and choose an option.
3. Filter the objects on the page to find the objects you want to compare.
4. Click the **Compare** button Compare.
5. Select up to three objects.
6. Review the objects side-by-side at the bottom of the screen.
7. (Optional) In **Relationships**, select a device name, and then select **View Configuration** to view the device configuration with the object entry highlighted.

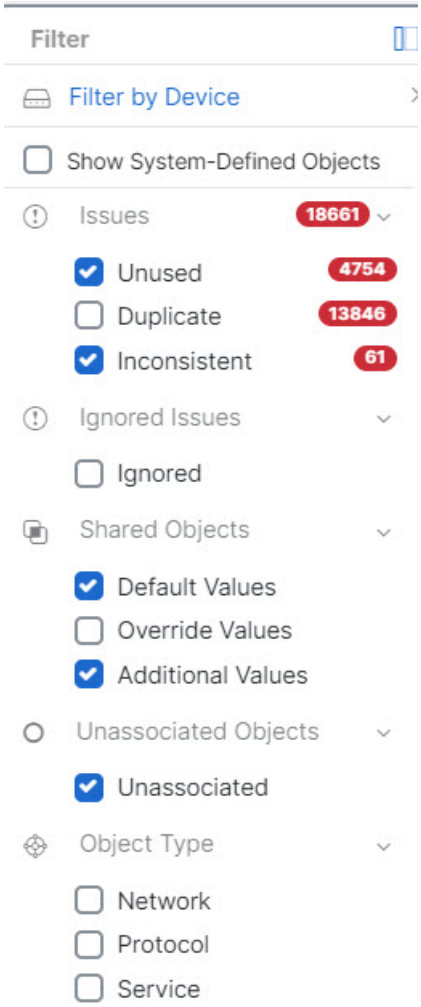
Object filters

Learn how to filter objects in Security Cloud Control by device, issue, shared state, association state, object type, system-defined status, and search value to find targeted object results.

Use filters on the **Objects** page to find objects by device, issue, shared state, association state, object type, or search value. You can also include or exclude system-defined objects.

The object type filter lets you filter by object types such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter lets you filter objects that have default values, override values, or additional values.

You can combine device and object filters to create focused search strategies. For example, you can search for objects that match this logic: **Issues** is **Unused** OR **Inconsistent**, AND **Shared Objects** has **Default Values** OR **Additional Values**, AND **Unassociated Objects** is selected.



To filter, click in the left-hand pane of the Objects tab:

- **Filter by Device**: Shows objects found on selected devices.
- **Show System-Defined Objects**: Includes predefined system objects in search and filter results. System objects cannot be edited or deleted. Some devices come with predefined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.

- **Issues**: Shows unused, duplicate, or inconsistent objects. If you select more than one issue, objects in any selected issue category are included.
- **Ignored Issues**: Shows objects whose issues were ignored by an administrator.
- **Shared Objects**: Shows shared objects. You can filter by default values, override values, additional values, or a combination.
- **Unassociated Objects**: Shows objects that are not associated with any rule or policy.
- **Object Type**: Shows selected object types, such as network objects, network groups, URL objects, URL groups, service objects, and service groups.

Within a main filter, subfilters can further narrow the results by object type, such as Network, Service, or Protocol. Filters across categories combine with an AND relationship. Multiple selections within a category can combine with an OR relationship.

For example, a filter set can search for objects that match this logic: objects on selected devices AND inconsistent objects AND network objects or service objects AND object names that contain **group**.

Configure object filters

You can filter on as few or as many criteria as you want. The more categories you filter by, the fewer results you should expect.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Open the filter panel by clicking the filter icon  at the top of the page. Uncheck any filters that have been checked to make sure no objects are inadvertently filtered out.
4. If you want to restrict your results to those found on particular devices:
   a. Click **Filter By Device**.
   b. Search all the devices or click a device tab to search for only devices of a certain kind.
   c. Check the device you want to include in your filter criteria.
   d. Click **OK**.
5. Check **Show System Objects** to include system objects in your search results. Uncheck **Show System Objects** to exclude system objects from your search results.
6. Check the object **Issues** you want to filter. If you check more than one issue, objects in any of the categories you check are included in your filter results.
7. Check **Ignored** issues if you want to see the object that had issues but was ignored by the administrator.
8. Check the required filter in **Shared Objects** if you are filtering for objects shared between two or more devices.
   - **Default Values**: Filters objects having only the default values.
   - **Override Values**: Filters objects having overridden values.
   - **Additional Values**: Filters objects having additional values.
9. Check **Unassociated** if you are filtering for objects that are not part of any rule or policy.
10. Check the **Object Types** you want to filter.

11. You can also add an object name, IP address, or port number to the Objects search field to find objects with your search criteria among the filtered results.

Exclude device filters when you need full relationships

When you filter by device, Security Cloud Control Firewall Management shows objects on that device but does not show the object's relationships to all other devices.

For example, if ObjectA is shared between ASA1 and ASA2, and you filter for shared objects on ASA1, Security Cloud Control Firewall Management shows `ObjectA`, but the **Relationships** pane shows only that ObjectA is on ASA1.

To view every device and policy relationship for an object, do not specify a device in the filter criteria. Filter by other criteria, select the object, and review the **Relationships** pane.

Delete objects

You can delete a single object or mulitple objects.

See important caveats at Deleting Network Objects and Groups in Security Cloud Control on page 119.

Delete a single object

> **Note**
>
> If Cloud-Delivered Firewall Management Center is deployed on your tenant:
>
> Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.
>
> Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object you want to delete by using object filters and the search field, and select it.
4. Review the **Relationships** pane. If the object is used in a policy or in an object group, you cannot delete the object until you remove it from that policy or group.
5. In the **Actions** pane, click the **Remove** icon .
6. Confirm that you want to delete the object by clicking **OK**.
7. Review and deploy the changes you made, or wait and deploy multiple changes at once.

Delete a group of unused objects

As you onboard devices and start resolving object issues, you find many unused objects. You can delete up to 50 unused objects at a time.

Procedure

1. Use the **Issues** filter to find **unused** objects. You can also use the Device filter to find objects that are not associated with a device by selecting **No Device**.
2. Check the **Select all** checkbox in the object table header to select all the objects found by the filter that appear in the object table; or, check individual checkboxes for individual objects you want to delete.
3. In the **Actions** pane, click the **Remove** icon .
4. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create an ASA IP address pool

ASA address pool objects define IPv4 or IPv6 address pools that ASA devices assign to remote VPN clients. If you configure more than one address pool for a connection profile or group policy, the ASA uses the pools in the order in which you added them.

To define an IPv4 address pool, provide the IP address range. For example, 10.10.147.100 - 10.10.147.177.

To define an IPv6 address pool, provide the starting IP address, prefix, and number of addresses in the pool. For example, 2001:DB8:1::1.

If you assign addresses from a nonlocal subnet, add pools that fall on subnet boundaries so that routes for these networks are easier to add.

Perform the following to create an IP address pool:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click the blue plus button and select **ASA** > **Address Pool**.
4. In the **Create IP Address Pool** dialog box, enter this information:
   - **Object Name**: Enter the name of the address pool. It can be up to 64 characters
   - **IPv4 address pool**: Select this radio button to configure IPv4 address pools.
     - **IPv4 Address Range**: Enter the first IP address and the last IP address available in each configured pool. For example, 10.10.147.100 - 10.10.147.177.
     - **Mask**: Identifies the subnet on which this IP address pool resides.
   - **IPv6 address pool**: Select this radio button to configure IPv6 address pools.
     - **IPv6 Address**: Enter the first IP address available in the configured pool and prefix length in bits in <address>/<prefix> format. For example, 2001:DB8:1::1/3.
     - **Number of Addresses**: Identifies the number of IPv6 addresses, starting at the IP Address, that are in the pool.
5. Click **Save**.

Network objects

Learn how to manage network objects and network groups for hosts, networks, IP ranges, FQDNs, access rules, policies, and NAT rules.

A network object can contain a host name, a network IP address, a range of IP addresses, a fully qualified domain name (FQDN), or a subnetwork expressed in CIDR notation. **Network groups** are collections of network objects and other individual addresses or subnetworks that you add to the group. Network objects and network groups are used in access rules, network policies, and NAT rules.

Not all platforms support network objects, such as Cisco Meraki and Multicloud Defense; when you share dynamic objects, Security Cloud Control Firewall Management automatically translates the appropriate information from the originating platform or device into a set of usable information that Security Cloud Control Firewall Management can use.

Table 7: Permitted Contents of a Network Group

Device type	IP Value	Network Object	Network Groups
ASA	Yes	Yes	Yes
FTD	No	Yes	Yes
Meraki	Yes	Yes	Yes
Multicloud Defense	Yes	Yes	Yes

Reuse network objects across products

If you have a Security Cloud Control tenant with a Cloud-Delivered Firewall Management Center and one or more On-Premises Firewall Management Centers onboarded to your tenant:

- When you create a Secure Firewall Threat Defense, FDM-managed Firewall Threat Defense, ASA, or Meraki network object or group, a copy of the object is also added to the objects list on the **Objects** page used when configuring Cloud-Delivered Firewall Management Center, and vice versa.
- When you create a Secure Firewall Threat Defense, FDM-managed Firewall Threat Defense, or ASA network object or group, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center for which **Discover & Manage Network Objects** is enabled. From this list, you can choose and deploy the object to the On-Premises Firewall Management Center on which you want to use the object and discard the ones that you do not want. Navigate , **Administration** > **Firewall Management Center** select the On-Premises Firewall Management Center, and click **Objects** to see your objects in the On-Premises Firewall Management Center user interface and assign them to policies.

Changes you make to network objects or groups on either page apply to the object or group instance on both pages. Deleting an object from one page also deletes the corresponding copy of the object from the other page.

The following exceptions apply:

- If a network object of the same name already exists for Cloud-Delivered Firewall Management Center, the new Secure Firewall Threat Defense, FDM-managed Firewall Threat Defense, ASA, or Meraki network object will not be replicated on the **Objects** page of Security Cloud Control.
- Network objects and groups in onboarded Firewall Threat Defense devices that are managed by on-premises Secure Firewall Management Center are not replicated and cannot be used in Cloud-Delivered Firewall Management Center.

  Note that for on-premises Secure Firewall Management Center instances that have been *migrated* to Cloud-Delivered Firewall Management Center, network objects and groups *are* replicated to the Security Cloud Control objects page if they are used in policies that were deployed to FTD devices.

- Sharing Network Objects between Security Cloud Control and Cloud-Delivered Firewall Management Center is automatically enabled on new tenants but must be requested for existing tenants. If your network objects are not being shared with Cloud-Delivered Firewall Management Center, contact TAC to have the features enabled on your tenant.
- Sharing network objects between Security Cloud Control and On-Premises Firewall Management Center is not automatically enabled on Security Cloud Control for new On-Premises Firewall Management Centers onboarded to Security Cloud Control. If your network objects are not being shared with On-Premises Firewall Management Center, ensure the **Discover & Manage Network Objects** toggle button is enabled for the On-Premises Firewall Management Center in **Settings** or contact TAC to have the features enabled on your tenant.

Viewing network objects

Network objects that you create in Security Cloud Control Firewall Management, and network objects that Security Cloud Control Firewall Management recognizes in onboarded device configurations, appear on the **Objects** page. They are labeled with their object type. This allows you to filter by object type to quickly find the object you are looking for.

When you select a network object, the **Details** pane shows the object values. The **Relationships** pane shows whether the object is used in a policy and which device stores the object.

When you select a network group, Security Cloud Control Firewall Management shows the contents of the group as the combined values from the network objects in that group.

Create or Edit ASA Network Objects and Network Groups

An ASA network object can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects, network groups, and IP addresses that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using Security Cloud Control.

Table 8: Permitted Values of ASA Network Objects and Groups

Device type	IPv4 / IPv6	Single Address	Range of addresses	Partially Qualified Domain Name (PQDN)	Subnet using CIDR Notation
ASA	IPv4 / IPv6	Yes	Yes	Yes	Yes

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Create an ASA Network Object

A network object can contain a host name, a network IP address, a range of IP addresses, a fully qualified domain name (FQDN), or a subnetwork expressed in CIDR notation. Network objects are used in access rules, network policies, and NAT rules. You can create, update, and delete network objects and network groups using Security Cloud Control.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click the blue plus button  to create an object.
4. Click **ASA** > **Network**.

5. Enter an object name.
6. Select **Create a network object**.
7. (optional) Enter an object description.
8. In the **Value** section, add the IP address information in one of these ways:
   - Select **eq** and then enter a single IP address, a subnet address using CIDR notation, or a Partially Qualified Domain Name (PQDN).
   - Select **range** and then enter a range of IP addresses. Enter the range with the beginning and ending address in the range separated by a space. For example, 10.1.1.1 10.1.1.255 or 2001:DB8:1::1 2001:DB8:1::3
9. Click **Add**.

Important

The newly created network objects aren't associated with any ASA device as they aren't part of any rule or policy. To see these objects, select the **Unassociated** objects category in object filters.

For more information, see Object Filters. Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create an ASA Network Group

A **network group** can contain IP address values, network objects, and network groups. When you are creating a new network group, you can search for existing objects by their name, IP addresses, IP address range, or FQDN and add them to the network group. If the object isn't present, you can instantly create that object in the same interface and add it to the network group. Network groups can contain both IPv4 and IPv6 addresses.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click the blue plus button  to create an object.
4. Click **ASA** > **Network**.
5. Enter an **Object Name**.
6. Select **Create a network group**.

7. (optional) Enter an object description.
8. In the **Values** field, enter a value or object name. When you start typing, Security Cloud Control provides object names or values that match your entry.
9. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
10. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
11. If you have entered a value or object that is not present, you can perform one of the following:
    - Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the check mark to save it.
    - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the check mark to save it.
    - Click **Add Value** to create an inline value without using an object. Enter a value and click the check mark to save it.

    It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

    Note

    You can click the edit icon to modify the details. Clicking the delete button doesn't delete the object itself; instead, it removes it from the network group.

12. After adding the required objects, click **Add** to create a new network group.
13. Preview and deploy configuration changes for all devices on page 817.

Edit an ASA Network Object

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object you want to edit by using object filters and search field.

4. Select the network object and click the edit icon in the **Actions** pane.
5. Edit the values in the dialog box in the same fashion that you created in the procedures above.

> **Note**
>
> Click the delete icon next to remove the object from the network group.

6. Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
7. Click **Confirm** to finalize the change to the object and any devices affected by it.

Edit an ASA Network Group

> **Note**
>
> If Cloud-Delivered Firewall Management Center is deployed on your tenant:
>
> Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.
>
> Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the network group you want to edit by using object filters and search field.
4. Select the network group and click the edit icon in the **Actions** pane.
5. If you want to change the objects or network groups that are already added to the network group, perform the following steps:
   a. Click the edit icon appearing beside the object name or network group to modify them.
   b. Click the checkmark to save your changes.

> **Note**
>
> You can click the remove icon to delete the value from a network group.

6. If you want to add new network objects or network groups to this network group, you have to perform the following steps:
   a. In the **Values** field, enter a new value or the name of an existing network object. When you start typing, Security Cloud Control provides object names or values that match your entry. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
   b. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object, or network group to the new network group.
   c. If you have entered a value or object that is not present, you can perform one of the following:
      - Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
      - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.
      - Click **Add Value** to create an inline value without using an object. Enter a value and click the checkmark to save it.

   It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.
7. Click **Save**. Security Cloud Control displays the policies that will be affected by the change.
8. Click **Confirm** to finalize the change to the object and any devices affected by it.
9. Preview and deploy configuration changes for all devices on page 817.

Add Additional Values to a Shared Network Group in Security Cloud Control

The values in a shared network group that are present on all devices associated with it are called "default values." Security Cloud Control allows you to add "additional values" to the shared network group and assign those values to some devices associated with that shared network group. When Security Cloud Control deploys the changes to the devices, it determines the contents and pushes the "default values" to all devices associated with the shared network group and the "additional values" only to the specified devices.

For example, consider a scenario where you have four AD main servers in your head office that should be accessible from all your sites. Therefore, you have created an object group named "Active-Directory" to use it in all your sites. Now you want to add two more AD servers to one of your branch offices. You can do this by adding their details as additional values specific to that branch office on the object group "Active-Directory." These two servers do not participate in determining whether the object "Active-Directory" is consistent or shared. Therefore, the four AD main servers are accessible from all your sites, but the branch office (with two additional servers) can access two AD servers and four AD main servers.

Note

If there are inconsistent shared network groups, you can combine them into a single shared network group with additional values. See Resolve Inconsistent Object Issues for more information.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the shared network group that you want to edit by using object filters and search field.
4. Click the edit icon  in the **Actions** pane.
   - The **Devices** field shows the devices that the shared network group is present.
   - The **Usage** field shows the rulesets associated with the shared network group.
   - The **Default Values** field specifies the default network objects and their values associated with the shared network group that was provided during their creation. Next to this field, you can see the number of devices that contain this default value, and you can click to see their names and device types. You can also see the rulesets associated with this value.
5. In the **Additional Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.
6. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
7. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
8. If you have entered a value or object that is not present, you can perform one of the following:
   - Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
   - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.
   - Click **Add Value** to create an inline value without using an object. Enter a value and click the checkmark to save it.

It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

9. In the **Devices** column, click the cell associated with the newly added object and click **Add Devices**.
10. Select the devices that you want and click **OK**.
11. Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
12. Click **Confirm** to finalize the change to the object and any devices affected by it.
13. Preview and deploy configuration changes for all devices on page 817.

Edit Additional Values in a Shared Network Group in Security Cloud Control

> **Note**
>
> If Cloud-Delivered Firewall Management Center is deployed on your tenant:
>
> Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.
>
> Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object having the override you want to edit by using object filters and search field.
4. Click the edit icon in the **Actions** pane.
5. Modify the override value:
   - Click the edit icon to modify the value.
   - Click the cell in the **Devices** column to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
   - Click arrow in **Default Values** to push and make it an additional value of the shared network group. All devices associated with the shared network group are automatically assigned to it.
   - Click arrow in **Override Values** to push and make it as default objects of the shared network group.
   - Click the delete icon next to remove the object from the network group.
6. Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
7. Click **Confirm** to finalize the change to the object and any devices affected by it.
8. Preview and deploy configuration changes for all devices on page 817.

Deleting Network Objects and Groups in Security Cloud Control

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the **Objects** page deletes the replicated network object or group from the **Objects** page on the Cloud-Delivered Firewall Management Center and vice-versa.

Create or Edit a Firepower Network Object or Network Groups

A Firepower network object can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects and network groups that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using Security Cloud Control.

Firepower network objects and groups can be used by ASA, Firewall Threat Defense, FDM-managed, and Meraki devices. See Reuse network objects across products on page 111.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Table 9: IP addresses that can be added to network objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Partially Qualified Domain Name (PQDN)	Subnet using CIDR Notation
Firepower	IPv4 / IPv6	Yes	Yes	Yes	Yes

Create a Firepower Network Object

> **Note**
>
> If Cloud-Delivered Firewall Management Center is deployed on your tenant:
>
> When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click the blue plus button  to create an object.
4. Click **FTD** > **Network**.
5. Enter an **Object Name**.
6. Select **Create a network object**.
7. In the **Value** section:
   - Select **eq** and enter a single IP address, a subnet address expressed in CIDR notation, or a Partially Qualified Domain Name (PQDN).
   - Select **range** and enter an IP address range.

   > **Note**
   >
   > Do not set a host bit value. If you enter a host bit value other than 0, Security Cloud Control unsets it while creating the object, because the Cloud-Delivered Firewall Management Center only accepts IPv6 objects with host bits not set.

8. Click **Add**.

   Attention: The newly created network objects aren't associated with any FDM-managed device as they aren't part of any rule or policy. To see these objects, select the **Unassociated** objects category in object filters. For more information, see Object Filters. Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create a Firepower Network Group

A **network group** can contain network objects and network groups. When you create a new network group, you can search for existing objects by their name, IP addresses, IP address range, or FQDN and add them to the network group. If the object isn't present, you can instantly create that object in the same interface and add it to the network group.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click the blue plus button to create an object.
4. Click **FTD** > **Network**.
5. Enter an **Object Name**.
6. Select **Create a network group**.
7. In the **Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.
8. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
9. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
10. If you have entered a value or object that is not present, you can perform one of the following:
    - Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
    - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

    It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

    Note: You can click the edit icon to modify the details. Clicking the delete button doesn't delete the object itself; instead, it removes it from the network group.
11. After adding the required objects, click **Save** to create a new network group.
12. Preview and Deploy Configuration Changes for All Devices.

Edit a Firepower Network Object

> **Note**
>
> If Cloud-Delivered Firewall Management Center is deployed on your tenant:
>
> Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.
>
> Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object you want to edit by using object filters and search field.
4. Select the network object and click the edit icon in the **Actions** pane.
5. Edit the values in the dialog box in the same fashion that you created them in "Create a Firepower Network Group".

   > **Note**
   >
   > Click the delete icon next to remove the object from the network group.

6. Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
7. Click **Confirm** to finalize the change to the object and any devices affected by it.

Edit a Firepower Network Group

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the network group you want to edit by using object filters and search field.
4. Select the network group and click the edit icon in the **Actions** pane.
5. Change the object name and description if needed.
6. If you want to change the objects or network groups that are already added to the network group, perform the following steps:
   a. Click the edit icon appearing beside the object name or network group to modify them.
   b. Click the checkmark to save your changes. **Note**: You can click the remove icon to delete the value from a network group.
7. If you want to add new network objects or network groups to this network group, you have to perform the following steps:
   a. In the **Values** field, enter a new value or the name of an existing network object. When you start typing, Security Cloud Control provides object names or values that match your entry. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
   b. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
   c. If you have entered a value or object that is not present, you can perform one of the following:
      - Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
      - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

   It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.
8. Click **Save**. Security Cloud Control displays the policies that will be affected by the change.
9. Click **Confirm** to finalize the change to the object and any devices affected by it.

10. Preview and Deploy Configuration Changes for All Devices.

Add an Object Override

> **Note**
>
> If Cloud-Delivered Firewall Management Center is deployed on your tenant:
>
> Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.
>
> Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object to which you want to add an override, using object filters and search field.
4. Select the network object and click the edit icon in the **Actions** pane.
5. Enter the value in the **Override Values** dialog box and click **+ Add Value**.

   Important

   The override you are adding must have the same type of value that the object contains. For example, to a network object, you can configure an override only with a network value and not a host value.

6. Once you see that the value is added, click the cell in the **Devices** column in **Override Values**.
7. Click **Add Devices**, and choose the device to which you want the override to be added. The device you select must contain the object to which you are adding the override.
8. Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
9. Click **Confirm** to finalize the addition of the override to the object and any devices affected by it.

   > **Note**
   >
   > You can add more than one override to an object. However, you must select a different device, which contains the object, each time you are adding an override.

10. See Object Overrides on page 105 to know more about object overrides and Edit Object Overrides on page 125 to edit an existing override.

Edit Object Overrides

You can modify the value of an existing override as long as the object is present on the device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Navigate to **Objects**.
3. Locate the object having override you want to edit by using object filters and search field.
4. Select the object having override and click the edit icon in the Actions pane.
5. Modify the override value:
   - Click the edit icon to modify the value.
   - Click on the cell in the **Devices** column in **Override Values** to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
   - Click arrow in **Override Values** to push and make it as the default value of the shared object.
   - Click the delete icon next to the override you want to remove.
6. Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
7. Click **Confirm** to finalize the change to the object and any devices affected by it.
8. Preview and Deploy Configuration Changes for All Devices.

Add Additional Values to a Shared Network Group

The values in a shared network group that are present on all devices associated with it are called "default values." Security Cloud Control allows you to add "additional values" to the shared network group and assign those values to some devices associated with that shared network group. When Security Cloud Control deploys the changes to the devices, it determines the contents and pushes the "default values" to all devices associated with the shared network group and the "additional values" only to the specified devices.

For example, consider a scenario where you have four AD main servers in your head office that should be accessible from all your sites. Therefore, you have created an object group named "Active-Directory" to use in all your sites. Now you want to add two more AD servers to one of your branch offices. You can do this by adding their details as additional values specific to that branch office on the object group "Active-Directory." These two servers do not participate in determining whether the object "Active-Directory" is consistent or shared. Therefore, the four AD main servers are accessible from all your sites, but the branch office (with two additional servers) can access two AD servers and four AD main servers.

Note

If there are inconsistent shared network groups, you can combine them into a single shared network group with additional values. See Resolve Inconsistent Object Issues on page 182 for more information.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the shared network group you want to edit by using object filters and search field.
4. Click the edit icon in the **Actions** pane.
   - The **Devices** field shows the devices the shared network group is present.
   - The **Usage** field shows the rulesets associated with the shared network group.
   - The **Default Values** field specifies the default network objects and their values associated with the shared network group that was provided during their creation. Next to this field, you can see the number of devices that contain this default value, and you can click to see their names and device types. You can also see the rulesets associated with this value.
5. In the **Additional Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.
6. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
7. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
8. If you have entered a value or object that is not present, you can perform one of the following:
   - Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
   - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

   It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

9. In the **Devices** column, click the cell associated with the newly added object and click **Add Devices**.
10. Select the devices that you want and click **OK**.
11. Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
12. Click **Confirm** to finalize the change to the object and any devices affected by it.
13. Preview and Deploy Configuration Changes for All Devices.

Edit Additional Values in a Shared Network Group

> **Note**
>
> If Cloud-Delivered Firewall Management Center is deployed on your tenant:
>
> Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.
>
> Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object having the override you want to edit by using object filters and search field.
4. Click the edit icon in the **Actions** pane.
5. Modify the override value:
   - Click the edit icon to modify the value.
   - Click the cell in the **Devices** column to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
   - Click arrow in **Default Values** to push and make it an additional value of the shared network group. All devices associated with the shared network group are automatically assigned to it.
   - Click arrow in **Override Values** to push and make it as default objects of the shared network group.
   - Click the delete icon next to remove the object from the network group.
6. Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
7. Click **Confirm** to finalize the change to the object and any devices affected by it.
8. Preview and Deploy Configuration Changes for All Devices.

Deleting Network Objects and Groups in Security Cloud Control

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the **Objects** page deletes the replicated network object or group from the **Objects** page on the Cloud-Delivered Firewall Management Center and vice-versa.

Objects Associated with Meraki Devices

Learn how Security Cloud Control represents Meraki dashboard rule values as network, service, or protocol objects for MX device policy management.

About Objects Used with Meraki Devices

The Meraki dashboard utilizes groups of IP addresses, protocols, or port ranges in source and destination fields in outbound access control rules. Once onboarded, Security Cloud Control translates IP address into network objects, and application layer protocol values into either service objects or protocol objects.

A single rule in Security Cloud Control can translate into multiple rules in the dashboard. For example, if you add an ASA protocol group that includes both TCP and UDP protocols to a single access control rule in Security Cloud Control, Security Cloud Control translates the one Security Cloud Control rule into multiple rules in the dashboard: one rule containing a TCP protocol and one rule containing a UDP protocol.

Note that the Meraki dashboard and Security Cloud Control both support CIDR subnet notation. For more information on layer 3 switch interfaces and MX device layout, see the Meraki Knowledge Base.

Which Objects Can You Use With a Meraki Device in Security Cloud Control?

There are no objects in Security Cloud Control that are exclusive to MX devices. Instead, you can create or share FTD, FDM, and ASA objects and associate these objects in rules that are deployed to the device. Because Meraki is not fully compatible with FTD and ASA objects, there may be a few limitations that affect how the MX device uses objects.

Note that if you associate an FTD, FDM, and ASA objects with an MX device, that object becomes shared. Any changes to that object will affect all the devices it is shared with and the devices' configuration status will appear as *Not Synced*. For additional object states that could affect your objects, see the **Related Articles** section listed at the bottom of this page.

Meraki does not support objects containing IPv6 addresses or FQDNs.

Object in Security Cloud Control	Compatible with Meraki
Protocol Objects	TCP, UDP, ICMP
Network Objects	yes
Network Groups	yes
Service Objects	yes
ASA Service Groups	no
FTD Service Groups	no

Local Network Objects and Object Groups From the Meraki Cloud

Network objects and object groups provide easier management of firewall rules for Meraki devices. They serve as labels to IP Subnets and FQDN that can be used on access policies such as firewall rules. If there are needs to modify multiple access policies that use the same IP Subnets or FQDN, you only need to modify the network object to have it reflect on all policies. At this time, you must use the Meraki dashboard to create and modify these objects. For more information about what these objects can do for your environment, see Meraki's Network Objects Highlights.

> **Note**
>
> Once a device configuration referencing a Meraki network object or network object group is onboarded or synchronized to the Security Cloud Control UI, these objects are displayed as **FTD Network** objects.
>
> These objects and object groups are **read-only** in Security Cloud Control.

What Do Meraki Rules Look Like in Security Cloud Control

You can view the objects from the device's policy page, or you can filter the objects page based on device. From the policy page you can view, edit, and reorder the access control rules. Because Security Cloud Control translates the outbound rules from the Meraki dashboard into access control rules with objects, rules and protocols from the Meraki dashboard may look different. The following table addresses the new names for protocols once the device is onboarded to Security Cloud Control:

Rule or Protocol Header in the Meraki dashboard	Rule or Object Header in Security Cloud Control
Policy	Action
Source IP	Network Object or Network Group
Destination IP	Network Object or Network Group
Source Port	Network Object or Network Group
Destination Port	Network Object or Network Group
Layer 3 Application Protocol	Ports (Protocol Groups, Port Groups, or Service Objects)

The following is an example of what the outbound rules from the Meraki dashboard look in Security Cloud Control:



Create a Local Meraki Network Object

Learn how to create local Meraki network objects in the Meraki dashboard and synchronize them into Security Cloud Control as read-only FTD network objects or object groups.

A local Meraki network object must be made in the Merkai dashboard. If you have a Meraki device that has not been onboarded to Security Cloud Control yet, any pre-existing local objects are onboarded with the device; if you have a Meraki device that **has** been onboarded, sychronize the device in Security Cloud Control to read the new configuration and local objects.

Note

Once a device configuration referencing a Meraki network object or network object group is onboarded or synchronized with the Security Cloud Control UI, these objects are displayed as **FTD Network** objects or object groups.

These objects and object groups are **read-only** in Security Cloud Control.

Before you begin

If you have not enabled Merkai's **Open Beta Network Objects**, log into the Meraki dashboard and navigate to **Organization** > **Policy Object** to enroll and get access to local objects and object groups

Procedure

1. Log into the Meraki dashboard and create a local object or a local object group. See the Meraki Network Objects Configuration Guide for more information.
2. Log into Security Cloud Control.

   Note: If you have not yet onboarded your Meraki device to Security Cloud Control, see Onboard an MX Device to Security Cloud Control on page 673 for more information. Onboarding a device also onboards all the pre-existing objects.
3. In the left pane, click **Security Devices**.
4. Locate the Merkai device and select it so the device row is highlighted. The device status is **Conflict detected**. In the pane located to the right, select either **Review Conflict** to review the changes made to the device's configuration or **Accept without Review** to accept all configuration changes.

Create or Edit a Meraki Network Object or Network Group

MX devices use the same format as Firepower and ASA **network objects** and can contain a host name, an IP address or a subnet address expressed in CIDR notation. **Network groups** are a collection of network objects and other individual addresses or subnets you add to the group. Network objects and network groups are used in access rules. You can create, read, update, and delete network objects and network groups using Security Cloud Control.

IP addresses that can be added to network objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Fully Qualified Domain Name	Subnet using CIDR Notation
MX	IPv4	Yes	Yes	No	Yes

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Create a Meraki Network Object

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click , then click **FTD** > **Network** or **ASA** > **Network**.
4. Enter an object name.
5. Select **Create a network object**.
6. In the Value section, enter a single IP address or a subnet address expressed in CIDR notation.
7. Click **Add**.

8. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create a Meraki Network Group

A network group is made up of multiple network objects or IP addresses.

If you want your network group to be made up of network objects, use the "Create a Network Object" procedure above to create individual network objects for your IP addresses.

> **Note**
>
> If Cloud-Delivered Firewall Management Center is deployed on your tenant:
>
> When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the On-Premises Firewall Management Center on which you want these objects.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the Security Cloud Control navigation bar on the left, click **Objects**.
3. Click , then click either **FTD** > **Network** or **ASA** > **Network**.
4. Enter an object name.
5. Select **Create a network group**.
6. Click **Add Object**, select the network object from the list and click **Select**. Continue to do this until you have added all the network objects you want.
7. Click **Add**.
8. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Edit a Firepower Network Object or Network Group

Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the On-Premises Firewall Management Center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object you want to edit by using object filters and search field.
4. Select the object you want to edit.
5. Click the edit button in the details pane.
6. Edit the values in the dialog box in the same fashion that you created them in the procedures above.
7. Click **Save**.
8. Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.
9. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Deleting Network Objects and Groups in Security Cloud Control

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the **Objects** page deletes the replicated network object or group from the **Objects** page on the Cloud-Delivered Firewall Management Center and vice-versa.

URL objects

An overview of url objects including DNS, HTTP, SSH, NTP, logging, sysopt, and device association settings.

URL objects and URL groups are used by Firepower devices. Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies. A URL object defines a single URL or IP address, whereas a URL group defines more than one URL or IP address.

When creating URL objects, keep the following points in mind:

- If you do not include a path, meaning the URL has no / character, Security Cloud Control matches by the server host name only. The host name matches if it appears after the :// separator or after any dot in the host name. For example, ign.com matches ign.com and www.ign.com, but not verisign.com.

- If you include one or more `/` characters, Security Cloud Control uses the entire URL string for substring matching, including the server name, path, and query parameters.
- Do not use manual URL filtering to block or allow individual web pages or parts of sites unless you accept the risk of unexpected matches. Server paths can change, and substring matching can match unintended servers, paths, or query parameter strings.
- Security Cloud Control disregards the encryption protocol. If you block a website, HTTP and HTTPS traffic to that website is blocked unless you use an application condition to target a specific protocol.
- Do not include the protocol when you create a URL object. For example, use example.com, not http://example.com.
- If you use a URL object to match HTTPS traffic in an access control rule, create the object with the subject common name in the public key certificate used to encrypt the traffic. Do not include subdomain information. For example, use example.com, not www.example.com.
- The subject common name in a certificate might not match the website domain name. For more consistent HTTPS URL filtering, use SSL Decryption policy so that URL filtering rules evaluate decrypted traffic.

> **Note**
>
> URL objects do not match HTTPS traffic if the browser resumes a TLS session, because certificate information is no longer available. HTTPS connection matching can therefore be inconsistent.

Create or Edit an FDM-Managed URL Object

URL objects are reusable components that specify a URL or IP address.

To create a URL object, follow these steps:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click  > **FTD** > **URL**.
4. Enter an object name and description.
5. Select **Create a URL object.**
6. Enter the specific URL or IP address for your object.
7. Click **Add**.

Create a Firepower URL Group

A URL group can be made up of one or more URL objects representing one or more URLs or IP addresses. The Firepower Device Manager and Firepower Management Center also refer to these objects as "URL Objects."

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.

3. Click + > **FTD** > **URL**.
4. Enter an object name and description.
5. Select **Create a URL group.**
6. Add an existing object by clicking **Add Object,** selecting an object, and clicking **Select**. Repeat this step to add more objects.
7. Click **Add** when you are done adding URL objects to the URL group.

Edit a Firepower URL Object or URL Group

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Filter the objects to find the object you want to edit and then select the object in the object table.
4. In the details pane, click ✎ to edit.
5. Edit the values in the dialog box in the same fashion that you created them in the procedures above.
6. Click **Save**.
7. Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Geolocation objects

An overview of geolocation objects, including translated addresses, rule behavior, interface scope, and policy impact.

A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses. For example, using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

You can usually select geographical locations directly in a policy without using geolocation objects. Use an object when several policies need the same countries or continents.

Update the geolocation database

To use current geographical location data to filter traffic, Cisco recommends that you regularly update the geolocation database (GeoDB). You cannot update the GeoDB in Security Cloud Control. Refer to the following sections of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running to learn more about the GeoDB and how to update it.

- Updating System Databases and Feeds
- Updating System Databases

Create and Edit a Firepower Geolocation Filter Object

You can create a geolocation object by itself on the object page or when creating a security policy. This procedure creates a geolocation object from the object page.

To create a geolocation object, follow these steps:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click + > **FTD** > **Geolocation**.
4. Enter an **object name** for the object and optionally, a **description**.
5. In the filter bar, start typing the name of a country or a region and you are presented with a list of possible matches.
6. Check the country, countries, or regions that you want to add to the object.
7. Click **Add**.

Edit a Geolocation Object

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Objects**.
3. Use the filter panes and search field to locate your object.
4. In the **Actions** pane, click **Edit**.
5. You can change the name of the object and add or remove countries and regions to your object.
6. Click **Save**.
7. You will be notified if any devices are impacted. Click **Confirm**.
8. If a device or policy was impacted, open the **Security Devices** page and **Preview and Deploy** the changes to the device.

DNS group objects

An overview of DNS group objects, including DNS, HTTP, SSH, NTP, logging, sysopt, and device association settings.

A DNS group defines a list of DNS servers and associated attributes. DNS servers resolve FQDNs, such as www.example.com, to IP addresses. You can configure different DNS group objects for management and data interfaces.

Create a DNS Group Object

Use the following procedure to create a new DNS group object in Security Cloud Control:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click + > **FTD** > **DNS Group**.
4. Enter an **Object Name**.
5. (Optional) Add a description.
6. Enter the IP address of a **DNS server**. You can add up to six DNS servers; click the **Add DNS Server**. If you want to remove a server address, click the delete icon.

> **Note**
>
> The list is in priority order: the first server in the list is always used, and subsequent servers are used only if a response is not received from the servers above it. Although you can add up to six servers, only the first 3 servers listed will be used for the management interface.

7. Enter the **Domain Search Name**. This domain is added to hostnames that are not fully qualified; for example, serverA instead of serverA.example.com.
8. Enter the number of **Retries**. The number of times, from 0 to 10, to retry the list of DNS servers when the system does not receive a response. The default is 2. This setting applies to DNS groups used on the data interfaces only.
9. Enter the **Timeout** value. The number of seconds, from 1 to 30, to wait before trying the next DNS server. The default is 2 seconds. Each time the system retries the list of servers, this timeout doubles. This setting applies to DNS groups used on the data interfaces only.
10. Click **Add**.

Edit a DNS Group Object

You can edit a DNS group object that was created in Security Cloud Control or in Firewall Device Manager. Use the following procedure to edit an existing DNS group object:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the Security Cloud Control navigation bar on the left, click **Objects**.
3. Locate the **DNS Group Object** you want to edit by using object filters and search field.
4. Select the object and click the edit icon in the **Actions** pane.
5. Edit any of the following entries:
   - Object Name.
   - Description.
   - DNS Server. You can edit, add, or remove DNS servers from this list.
   - Domain Search Name.
   - Retries.
   - Timeout.
6. Click **Save**.
7. Preview and Deploy Configuration Changes for All Devices.

Delete a DNS Group Object

Use the following procedure to delete a DNS Group Object from Security Cloud Control:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the **DNS Group Object** you want to edit by using object filters and search field.
4. Select the object and click the **Remove** icon .
5. Confirm you want to delete the DNS group object and click **Ok**.
6. Preview and Deploy Configuration Changes for All Devices.

Certificate objects

An overview of certificate objects, including identity certificates, trusted CA certificates, CSR handling, export, edit, and deletion tasks.

Digital certificates provide digital identification for authentication. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

See the **About Certificates** and **Configuring Certificates** following sections of the Resuable Objects chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

About certificates

Digital certificates provide digital identification for authentication. Certificates include information that identifies a device or user, such as a name, serial number, company, department, or IP address. Certificates also include a copy of the public key for the user or device. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

You can create the following types of certificate:

- **Internal certificates**–Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a certificate authority (CA). You can also generate a self-signed certificate.

  The system comes with the following pre-defined internal certificates, which you can use as is or replace: **DefaultInternalCertificate** and **DefaultWebServerCertificate**

- **Internal Certificate Authority (CA)** certificates–Internal CA certificates are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a certificate authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

  The system comes with the following pre-defined internal CA certificate, which you can use as is or replace: **NGFW-Default-InternalCA**

- **Trusted Certificate Authority (CA)** certificates–A trusted CA certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

  Certificate Authorities (CAs) are trusted authorities that "sign" certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security. A CA can be a trusted third party, such as VeriSign, or a private (in-house) CA that you establish within your organization. CAs are responsible for managing certificate requests and issuing digital certificates.

The system includes many trusted CA certificates from third-party certificate authorities. These are used by SSL decryption policies for Decrypt Re-Sign actions.

For more information, see the **Certificate Types Used by Feature** section of the Reusable Objects chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Certificate Types Used by Feature

You need to create the right type of certificate for each feature. The following features require certificates.

Identity Policies (Captive Portal)—Internal Certificate

(Optional.) Captive portal is used in identity policies. Users must accept this certificate when authenticating to the device for purposes of identifying themselves and receiving the IP address associated with their usernames. If you do not supply a certificate, the device uses an automatically generated certificate.

SSL Decryption Policy—Internal, Internal CA, and Trusted CA Certificates.

(Required.) The SSL decryption policy uses certificates for the these purposes:

- Internal certificates are used for known key decryption rules.
- Internal CA certificates are used for decrypt re-sign rules when creating the session between the client and FDM-managed device.
- Trusted CA certificates
  - They are used indirectly for decrypt re-sign rules when creating the session between the FDM-managed device and server. Unlike the other certificates, you do not directly configure these certificates in the SSL decryption policy; they simply need to be uploaded to the system. The system includes a large number of trusted CA certificates, so you might not need to upload any additional certificates.
  - When creating an Active Directory Realm object and configuring the directory server to use encryption.

Configuring Certificates

Certificates used in identity policies or SSL decryption policies must be an X509 certificate in PEM or DER format. You can use OpenSSL to generate certificates if needed, obtain them from a trusted Certificate Authority, or create self-signed certificates.

Use these procedures to configure certificate objects:

- Uploading Internal and Internal CA Certificates
- Uploading Trusted CA Certificates
- Generating Self-Signed Internal and Internal CA Certificate
- To view or edit a certificate, click either the edit icon or the view icon for the certificate.
- To delete an unreferenced certificate, click the trash can icon (delete icon) for the certificate. See Deleting Objects.

Uploading Internal and Internal CA Certificates

Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

Internal Certificate Authority (CA) certificates (Internal CA certificates) are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

For information on the features that use these certificates, see Certificate Type Used by Feature.

Procedure

This procedure creates an internal or internal CA certificate by uploading a certificate file or pasting existing certificate text into a text box. If you want to generate a self-signed certificate, see Generating Self-Signed Internal and Internal CA Certificates.

To create an internal or internal CA certificate object, or when adding a new certificate object to a policy, follow this procedure:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Do one of the following:
   - Create the certificate object in the Objects page:
     a. In the left pane, click **Objects**.
     b. Click the plus button and select **FTD** > **Certificate**
   - Click **Create New Object** when adding a new certificate object to a policy.
3. Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.
4. In step 1, select **Internal Certificate** or **Internal CA.**
5. In step 2, select **Upload** to upload the certificate file.
6. In step 3, in the **Server Certificate** area, paste the certificate contents in the text box or upload the certificate file as explained in the wizard. If you paste the certificate into the text box, the certificate must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

7. In step 3, in the **Certificate Key** area, paste the key contents into the Certificate Key text box or upload the key file as explained in the wizard. If you paste the key into the text box, the key must include the BEGIN PRIVATE KEY or BEGIN RSA PRIVATE KEY and END PRIVATE KEY or END PRIVATE KEY lines.

   Note

   The key cannot be encrypted.

8. Click **Add**.

Uploading Trusted CA Certificates

A trusted Certificate Authority (CA) certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

For information on the features that use these certificates, see Certificate Type Used by Feature.

Obtain a trusted CA certificate from an external certificate authority, or create one using your own internal CA, for example, with OpenSSL tools. Then, use the following procedure to upload the certificate.

Procedure

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Do one of the following:
   - Create the certificate object in the Objects page:
     a. In the left pane, click **Objects**.
     b. Click + > **FTD** > **Certificate**.
   - Click **Create New Object** when adding a new certificate object to a policy.
3. Enter a **Name** for the certificate. The name is used in the configuration as an object name only; it does not become part of the certificate itself.
4. In step 1, select **External CA Certificate** and click **Continue**. The wizard advances to step 3.
5. In step 3, in the **Certificate Contents** area, paste the certificate contents in the text box or upload the certificate file as explained in the wizard.

   The certificate must adhere to these guidelines:
   - The name of the server in the certificate must match the server Hostname / IP Address. For example, if you use 10.10.10.250 as the IP address but ad.example.com in the certificate, the connection fails.
   - The certificate must be an X509 certificate in PEM or DER format.
   - The certificate you paste must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

6. Click **Add**.

Generating Self-Signed Internal and Internal CA Certificates

Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

Internal Certificate Authority (CA) certificates (Internal CA certificates) are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

You can also create these certificates using OpenSSL, or obtain them from a trusted CA, and upload them. For more information, see Uploading Internal and Internal CA Certificates.

For information on the features that use these certificates, see Certificate Type Used by Feature.

Note

New self-signed certificates are generated with a 5-year validity term. Be sure to replace certificates before they expire.

Warning

Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Procedure

This procedure generates a self-signed certificate by entering the appropriate certificate field values in a wizard. If you want to create an internal or internal CA certificate by uploading a certificate file, see Uploading Internal and Internal CA Certificates.

To generate a self-signed certificate, follow this procedure:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Do one of the following:
   - Create the certificate object in the Objects page:
     a. In the left pane, click **Objects**.
     b. Click + > **FTD** > **Certificate**.
   - Click **Create New Object** when adding a new certificate object to a policy.
3. Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.
4. In step 1, select **Internal Certificate** or **Internal CA.**
5. In step 2, select **Self-Signed** to create the self-signed certificate in this step.

6. Configure at least one of the following for the certificate subject and issuer information.
   - Country (C)– Select the country code from the drop-down list.
   - State or Province (ST)– The state or province to include in the certificate.
   - Locality or City (L)– The locality to include in the certificate, such as the name of the city.
   - Organization (O)– The organization or company name to include in the certificate.
   - Organizational Unit (Department) (OU)– The name of the organization unit (for example, a department name) to include in the certificate.
   - Common Name (CN)– The X.500 common name to include in the certificate. This could be the name of the device, web site, or another text string. This element is usually required for successful connections. For example, you must include a CN in the internal certificate used for remote access VPN.
7. Click **Add**.

ASA trustpoint objects

An overview of ASA trustpoint objects, including identity certificates, trusted CA certificates, CSR handling, export, edit, and deletion tasks.

A trustpoint object lets you add digital certificates and install them on one or more managed ASA devices. A trustpoint object can contain an identity pair, an identity certificate only, or a CA certificate only. An identity pair includes an identity certificate and the issuer CA certificate.

You can configure many trustpoints in an ASA device. Supported certificate formats are PKCS12, PEM, and DER.

Add an identity certificate object by using PKCS12

This procedure creates an internal certificate identity or internal identity certificate by uploading a certificate file or pasting existing certificate text into a text box. You can generate as many identity certificates as you want.

You can upload a file encoded in **PKCS12** format. A PKCS12 is a single file that holds the CA server certificate, any intermediate certificates, and the private key in one encrypted file. A PKCS#12, or PFX, file holds a server certificate, intermediate certificates, and a private key in one encrypted file. Enter the **Passphrase** value for decryption.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click  and select **ASA** > **Trustpoints**.
4. Enter an **Object Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.
5. In the **Certificate Type** step, select **Identity Certificate**.
6. In the **Import Type** step, select **Upload** to upload the certificate file.

   The **Enrollment** step is set to Terminal.
7. In the **Certificate Contents** step, enter the PKCS12 format details.

   A PKCS#12, or PFX, file holds a server certificate, intermediate certificates, and a private key in one encrypted file. Enter the **Passphrase** value for decryption.

8. Click **Continue**.
9. In the **Advanced Options** step, you can configure the following:

   In the **Revocation** tab, you can configure the following:

   - **Enable Certificate Revocation Lists (CRL)** – Check to enable CRL checking.

     By default the **Use CRL distribution point from the certificate** check box is selected to obtain the revocation lists distribution URL from the certificate.

     Cache Refresh Time (in minutes) – Enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1-1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the ASA removes the least recently used CRL until more space becomes available.

   - **Enable Online Certificate Status Protocol (OCSP)** – Check to enable OCSP checking.

     OCSP Server URL–The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with `http://`.

     Disable Nonce Extension – Enable the check box which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable Nonce Extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.

     Evaluation Priority – Specify whether to evaluate the revocation status of a certificate first in CRL or OSCP.

   - **Consider the certificate valid if revocation information cannot be reached**– Select this check box to consider the certificate to be a valid certificate if revocation information is unreachable.

     For more information on revocation check, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

   Click the **Others** tab:

   - **Use CA Certificate for the Validation of** – Specify the type of connections that can be validated by this CA.
     - **IPSec Client** – Validates certificate presented by remote SSL servers.
     - **SSL Client** – Validates certificates presented by incoming SSL connections.
     - **SSL Server** – Validates certificates presented by incoming IPSec connections.
   - **Use Identity Certificate for** – Specify how the enrolled ID certificate can be used.
     - **SSL & IPSec** – Use for authenticating SSL & IPSec connections
     - **Code Signer** – Code signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.
   - **Other Options**:
     - **Enable CA flag in basic constraints extension** – Select this option if this certificate should be able to sign other certificates. The basic constraints extension identifies whether the subject of the certificate is a Certificate Authority (CA), in which case the certificate can be used to sign other certificates. The CA flag is part of this extension.
     - **Accept certificates issued by this CA** – Select this option to indicate that the ASA should accept certificates from the specified CA.

- **Ignore IPSec Key Usage** – Select this option if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

10. Click **Add**.

Create a self-signed ASA identity certificate object

This procedure describes steps for generating a self-signed certificate for your ASA by entering the appropriate certificate field values in a wizard. You can generate as many self-signed certificates as you want.

To create a Self-Signed identity certificate object, perform these steps:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click  and select **ASA** > **Trustpoints**.
4. Enter an **Object Name** for the certificate.

   The name is used in the configuration as an object name only; it does not become part of the certificate itself.

5. In the **Identity Certificate** step, select **Identity Certificate**.
6. In the **Import Type** step, select **New** to upload the certificate file and click **Continue**.
7. In the **Enrollment** step, select **Self-Signed** and click **Continue**.

   The **Certificates Content** step appears. Read Self-Signed and CSR Certificate Generation Based on Certificate Contents to understand the CN and SANS content in the Self-Signed certificate that is being generated.

8. In the **Certificate Contents** step, configure the following:
   - **Country (C)**– Select the country code from the drop-down list.
   - **State or Province (ST)**–The state or province to include in the certificate.
   - **Locality or City (L)**–The locality to include in the certificate, such as the name of the city.
   - **Organization (O)**–The organization or company name to include in the certificate.
   - **Organizational Unit (Department) (OU)**–The name of the organization unit (for example, a department name) to include in the certificate.
   - **Common Name (CN)**–The X.500 common name to include in the certificate. This could be the name of the device, web site, or another text string. This element is usually required for successful connections. For example, you must include a CN in the internal certificate used for remote access VPN.
   - **Email Address (EA)**– The e-mail address associated with the identity certificate.
   - **IP Address**– The ASA IP address on the network in four-part dotted-decimal notation.
   - **Device's FQDN**– An unambiguous domain name, to indicate the position of the node in the DNS tree hierarchy.
   - **Include Device's Serial Number**– Select the check box if you want to add the ASA serial number to the certificate parameters.

   a) Click the **Key** tab.
      - Choose the **RSA** or **ECDSA** key type.

- **Key Size**: If the key pair does not exist, defines the desired key size (modulus), in bits. The recommended key size for RSA is 1024 and for ECDSA is 348. The larger the modulus size, the more secure the key. However, keys with larger modulus sizes take longer to generate (a minute or more when larger than 512 bits) and longer to process when exchanged.
- Click **Continue**.

9. In the **Advanced Options** step, you can configure the following:

   In the **Revocation** tab, you can configure the following:

   - **Enable Certificate Revocation Lists (CRL)** – Check to enable CRL checking.

     By default the **Use CRL distribution point from the certificate** check box is selected to obtain the revocation lists distribution URL from the certificate.

     Cache Refresh Time (in minutes) – Enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1 to 1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the ASA removes the least recently used CRL until more space becomes available.

   - **Enable Online Certificate Status Protocol (OCSP)** – Check to enable OCSP checking.

     OCSP Server URL – The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with `http://`.

     Disable Nonce Extension – Enable the check box which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable Nonce Extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.

     Evaluation Priority – Specify whether to evaluate the revocation status of a certificate first in CRL or OSCP.

   - **Consider the certificate valid if revocation information cannot be reached** – Select this check box to consider the certificate to be a valid certificate if revocation information is unreachable.

     For more information on revocation check, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

   Click the **Others** tab:

   - **Use CA Certificate for the Validation of** – Specify the type of connections that can be validated by this CA.
     - **IPSec Client** – Validates certificate presented by remote SSL servers.
     - **SSL Client** – Validates certificates presented by incoming SSL connections.
     - **SSL Server** – Validates certificates presented by incoming IPSec connections.
   - **Use Identity Certificate for** – Specify how the enrolled ID certificate can be used.
     - **SSL & IPSec** – Use for authenticating SSL & IPSec connections
     - **Code Signer** – Code signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.
   - **Other Options**:
     - **Enable CA flag in basic constraints extension** – Select this option if this certificate should be able to sign other certificates. The basic constraints extension identifies whether the subject of the certificate is

a Certificate Authority (CA), in which case the certificate can be used to sign other certificates. The CA flag is part of this extension. The presence of these items in a certificate i

- **Accept certificates issued by this CA** – Select this option to indicate that the ASA should accept certificates from the specified CA.
- **Ignore IPSec Key Usage** – Select this option if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

10. Click **Add**.

Add an ASA identity certificate object for a Certificate Signing Request (CSR)

The Certification Authority (CA) server information and enrollment parameters are required to generate Certificate Signing Requests (CSRs) and obtain Identity Certificates from the specified CA. You need to select either Rivest-Shamir-Adleman (RSA) or Elliptic Curve Digital Signature Algorithm (ECDSA) key type to generate the request.

Create a trustpoint object by providing identification information and optionally uploading a CA certificate obtained from a CA.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click  and select **ASA** > **Trustpoints**.
4. Enter an **Object Name** for the certificate.

   The name is used in the configuration as an object name only; it does not become part of the certificate itself.
5. In the **Identity Certificate** step, select **Identity Certificate**.
6. In the **Import Type** step, select **New** to upload the certificate file and click **Continue**.
7. In the **Enrollment** step, select **Manual**.
8. (optional) You can paste or upload the CA certificate obtained from your CA. You can leave the field empty.
9. Click **Continue**.

   The Certificates Content step appears. Read Self-Signed and CSR Certificate Generation Based on Certificate Contents to understand the CN and SANS content in the Signed certificate that is being generated.
10. In the **Certificate Contents** step, configure the following:
    - **Country (C)**– Select the country code from the drop-down list.
    - **State or Province (ST)**–The state or province to include in the certificate.
    - **Locality or City (L)**–The locality to include in the certificate, such as the name of the city.
    - **Organization (O)**–The organization or company name to include in the certificate.
    - **Organizational Unit (Department) (OU)**–The name of the organization unit (for example, a department name) to include in the certificate.
    - **Common Name (CN)**–The X.500 common name to include in the certificate. This could be the name of the device, web site, or another text string. This element is usually required for successful connections. For example, you must include a CN in the internal certificate used for remote access VPN.

- **Email Address (EA)**– The e-mail address associated with the identity certificate.
- **IP Address**– The ASA IP address on the network in four-part dotted-decimal notation.
- **Subject Alternative Name (SAN)**– This field will be part of Certificate Subject DN as 'unstructuredName' as well. We recommend you use this field if the certificate is used for multiple domains or IP addresses.
  - **Use Device Host Name:** Host name of the device is used.
  - **Custom: Device's FQDN**– An unambiguous domain name, to indicate the position of the node in the DNS tree hierarchy.

    Note

    We recommend the values specified in CN and **Custom FQDN** are the same.

- **Include Device's Serial Number**– Select the check box if you want to include the serial number of ASA in the certificate. The CA uses the serial number to either authenticate certificates or to later associate a certificate with a particular device. If you are in doubt, include the serial number, as it is useful for debugging purposes.

a) Click the **Key** tab.

- Choose the **RSA** or **ECDSA** key type.
- **Key Size**: If the key pair does not exist, defines the desired key size (modulus), in bits. The recommended key size for RSA is 1024 and for ECDSA is 348. The larger the modulus size, the more secure the key. However, keys with larger modulus sizes take longer to generate (a minute or more when larger than 512 bits) and longer to process when exchanged.
- Click **Continue**.

11. In the **Advanced Options** step, you can configure the following:

In the **Revocation** tab, you can configure the following:

- **Enable Certificate Revocation Lists (CRL)** – Check to enable CRL checking.

  By default, the **Use CRL distribution point from the certificate** check box is selected to obtain the revocation lists distribution URL from the certificate.

  Cache Refresh Time (in minutes) – Enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1 to 1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the ASA removes the least recently used CRL until more space becomes available.

- **Enable Online Certificate Status Protocol (OCSP)** – Check to enable OCSP checking.

  OCSP Server URL–The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with `http://`.

  Disable Nonce Extension – Enable the check box which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable Nonce Extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.

  Evaluation Priority – Specify whether to evaluate the revocation status of a certificate first in CRL or OSCP.

- **Consider the certificate valid if revocation information cannot be reached**– Select this check box to consider the certificate to be a valid certificate if revocation information is unreachable.

  For more information on revocation check, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Click the **Others** tab:

- **Use CA Certificate for the Validation of** – Specify the type of connections that can be validated by this CA.
  - **IPSec Client** – Validates certificate presented by remote SSL servers.
  - **SSL Client** – Validates certificates presented by incoming SSL connections.
  - **SSL Server** – Validates certificates presented by incoming IPSec connections.
- **Use Identity Certificate for** – Specify how the enrolled ID certificate can be used.
  - **SSL & IPSec** – Use for authenticating SSL & IPSec connections
  - **Code Signer** – Code signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.
- **Other Options**:
  - **Enable CA flag in basic constraints extension** – Select this option if this certificate should be able to sign other certificates. The basic constraints extension identifies whether the subject of the certificate is a Certificate Authority (CA), in which case the certificate can be used to sign other certificates. The CA flag is part of this extension. The presence of these items in a certificate i
  - **Accept certificates issued by this CA** – Select this option to indicate that the ASA should accept certificates from the specified CA.
  - **Ignore IPSec Key Usage** – Select this option if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

12. Click **Add**.

    This creates a trustpoint certificate object.

Add a trusted CA certificate object for ASA

Obtain a trusted CA certificate from an external certificate authority, or create one using your own internal CA, for example, with OpenSSL tools. You can upload a file encoded in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click  and select **ASA** > **Trustpoints**.

4. Enter an **Object Name** for the certificate.

   The name is used in the configuration as an object name only; it does not become part of the certificate itself.

5. In the **Certificate Type** step, select **Trusted CA Certificate**.
6. In the **Certificate Contents** step, paste the certificate contents in the text box or upload the CA certificate file as explained in the wizard.
7. Click **Continue**. The wizard advances to step 4.

   The certificate must follow these guidelines:

   - The name of the server in the certificate must match the server Hostname / IP Address. For example, if you use 10.10.10.250 as the IP address but ad.example.com in the certificate, the connection fails.
   - The certificate must be an X509 certificate in PEM or DER format.
   - The certificate you paste must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

8. In the **Advanced Options** step, you can configure the following:

   In the **Revocation** tab, you can configure the following:

   - **Enable Certificate Revocation Lists (CRL)** – Check to enable CRL checking.

     By default, the **Use CRL distribution point from the certificate** check box is selected to obtain the revocation lists distribution URL from the certificate.

     Cache Refresh Time (in minutes) – Enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1 to 1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the ASA removes the least recently used CRL until more space becomes available.

   - **Enable Online Certificate Status Protocol (OCSP)** – Check to enable OCSP checking.

     OCSP Server URL–The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with **`http://`**.

     Disable Nonce Extension – Enable the check box which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable Nonce Extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.

     Evaluation Priority – Specify whether to evaluate the revocation status of a certificate first in CRL or OSCP.

   - **Consider the certificate valid if revocation information cannot be reached**– Select this check box to consider the certificate to be a valid certificate if revocation information is unreachable.

     For more information on revocation check, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Click the **Others** tab:

- **Use CA Certificate for the Validation of** – Specify the type of connections that can be validated by this CA.
  - **IPSec Client** – Validates certificate presented by remote SSL servers.
  - **SSL Client** – Validates certificates presented by incoming SSL connections.
  - **SSL Server** – Validates certificates presented by incoming IPSec connections.
- **Other Options**:
  - **Enable CA flag in basic constraints extension** – Select this option if you want to validate if the subject of the certificate is a CA using the basic constraints extension.
  - **Accept certificates issued by this CA** – Select this option to indicate that the ASA should accept certificates from the specified CA.
  - **Accept certificates issued by the subordinates CAs of this CA** – Select this option to indicate that the ASA should accept certificates from the subordinate CA.
  - **Ignore IPSec Key Usage** – Select this option if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

9. Click **Add**.

   This creates a trustpoint certificate object.

Self-Signed and CSR certificate generation based on certificate contents

You need to have an idea of the CN and SANS content in the Self-Signed and CSR certificates. The content is based on the parameters you specify during their creation. You need to configure the parameters precisely for the AnyConnect clients to connect to the intended VPN headends of your organization.

This section provides different use cases with examples to give you an idea of the content of Self-Signed and CSR certificates based on the parameters specified.

Usecase 1: Different CN and FQDN values

Example:

- Common Name (CN): mywebsite.com
- FQDN: mysan.com

Table 10: Example: Different CN and FQDN values

	Common Name	unstructuredName	SANS
Self-Signed	mywebsite.com	mysan.com	mysan.com
CSR	mywebsite.com	mysan.com	-

Usecase 2: FQDN field set to None

Example:

- Common Name (CN): mywebsite.com
- FQDN: None

Table 11: Example: FQDN field set to None

	Common Name	SANS
Self-Signed	Host Name	-
CSR	mywebsite.com	-

Usecase 3: No FQDN (Default FQDN)

Example:

- Common Name (CN): mywebsite.com

Table 12: Example: No FQDN (Default FQDN)

	Common Name	unstructuredName	SANS
Self-Signed	mywebsite.com	Host Name	-
CSR	mywebsite.com	Host Name	Host Name

Usecase 4: IP Address is specified in FQDN

Example:

- Common Name (CN): mywebsite.com
- FQDN: 4.5.6.7

Table 13: Example: IP Address is specified in FQDN

	Common Name	unstructuredName	SANS
Self-Signed	mywebsite.com	4.5.6.7	-
CSR	mywebsite.com	4.5.6.7	4.5.6.7

Usecase 5: IP Address is Specified

Example:

- IP Address: 4.5.6.7
- Common Name (CN): mywebsite.com
- FQDN: fqdn.com

Table 14: Example: IP Address is specified

	Common Name	unstructuredAddress	unstructuredName	SANS
Self-Signed	mywebsite.com	4.5.6.7	fqdn.com	-
CSR	mywebsite.com	4.5.6.7	fqdn.com	fqdn.com

Usecase 6: Serial Number Check box is Selected

Example:

- Serial Number: 9AQXMWOKDT9

Table 15: Example: IP Serial Number Check box is Selected

	serialNumber	SANS
Self-Signed	9AQXMWOKDT9	-
CSR	9AQXMWOKDT9	fqdn.com

Usecase 7: Email Address is Specified

Example:

- EA: abc@xyz.com

Table 16: Example: Email Address is Specified

	unstructredName	emailAddress	SANS
Self-Signed	Host Name	abc@xyz.com	Host Name
CSR	Host Name	abc@xyz.com	-

IPsec proposal and IKE policy objects

An overview of IPsec proposal and ike policy objects, including VPN peers, protected networks, connection settings, monitoring, and verification.

IPsec is one of the most secure methods for setting up a VPN. IPsec provides data encryption at the IP packet level, offering a robust security solution that is standards-based. With IPsec, data is transmitted over a public network through tunnels. A tunnel is a secure, logical communication path between two peers. Traffic that enters an IPsec tunnel is secured by a combination of security protocols and algorithms called a transform set. During the IPsec security association (SA) negotiation, peers search for a transform set that is the same at both peers.

There are separate IPsec proposal objects based on the IKE version, IKEv1, or IKEv2:

- When you create an IKEv1 IPsec proposal, you select the mode in which IPsec operates, and define the required encryption and authentication types. You can select single options for the algorithms. If you want to support multiple combinations in a VPN, create and select multiple IKEv1 IPsec Proposal objects.

- When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and antireplay services. ESP is IP protocol type 50.

Note

We recommend using both encryption and authentication on IPsec tunnels.

Create or edit an IKEv1 IPsec proposal object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently, Security Cloud Control supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note

We recommend using both encryption and authentication on IPsec tunnels.

There are several pre-defined IKEv1 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

This procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv1 IPsec Proposals objects while editing the IKEv1 IPsec settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Proposal** link shown in the object list.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. From the left pane, click **Objects**.
3. Do one of these things:
   - Click , and select **FTD > IKEv1 IPsec Proposal** to create the new object.
   - On the object page, select the IPsec proposal you want to edit and click **Edit** in the **Actions** pane at the right.
4. Enter an **object name** for the new object.
5. Select the Mode in which the IKEv1 IPsec Proposal object operates.
   - **Tunnel mode** encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.

- **Transport mode** encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.

6. Select the **ESP Encryption** (Encapsulating Security Protocol encryption) algorithm for this proposal. For an explanation of the options, see Deciding which encryption algorithm to use.
7. Select the **ESP Hash** or integrity algorithm to use for authentication. For an explanation of the options, see Deciding which encryption algorithm to use.
8. Click **Add**.

Create or edit an IKEv2 IPsec proposal object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.

When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

There are several pre-defined IKEv2 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv2 IPsec Proposals objects while editing the IKEv2 IPsec settings in a VPN connection by clicking the Create New IPsec Proposal link shown in the object list.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Do one of these things:
   - Click  and select **FTD > IKEv2 IPsec Proposal** to create the new object.
   - In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.
4. Enter an **object name** for the new object.
5. Configure the IKE2 IPsec proposal objects:
   - **Encryption**–The Encapsulating Security Protocol (ESP) encryption algorithm for this proposal. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN on page 729.
   - **Integrity Hash**–The hash or integrity algorithm to use for authentication. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon.
6. Click **Add**.

Global IKE policies

An overview of global ike policies, including rule order, interface assignment, logging, search, and deployment considerations.

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

IKE policy objects define the IKE proposals for these negotiations. The objects that you enable are the ones used when the peers negotiate a VPN connection: you cannot specify different IKE policies per connection. The relative priority of each object determines which of these policies are tried first, with the lower number being a higher priority. The connection is not established if the negotiation fails to find a policy that both peers can support.

To define the global IKE policy, you select which objects to enable for each IKE version. If the pre-defined objects do not satisfy your requirements, create new policies to enforce your security policy.

Create or edit an IKEv1 policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv1 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Policy** link shown in the object list.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Do one of these things:
   - Click  and select **FTD > IKEv1 Policy** to create a new IKEv1 policy.
   - In the object page, select the IKEv1 policy you want to edit and click **Edit** in the Actions pane at the right.
4. Enter an **object name**, up to 128 characters.
5. Configure the IKEv1 properties.
   - **Priority**: The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
   - **Encryption**: The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.

- **Diffie-Hellman Group**: The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Lifetime**: The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).
- **Authentication**: The method of authentication to use between the two peers. For more information, see Deciding Which Encryption Algorithm to Use.
  - **Preshared Key**: Use the preshared key that is defined on each device. These keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If the peer is not configured with the same preshared key, the IKE SA cannot be established.
  - **Certificate**: Use the device identity certificates for the peers to identify each other. You must obtain these certificates by enrolling each peer in a Certificate Authority. You must also upload the trusted CA root and intermediate CA certificates used to sign the identity certificates in each peer. The peers can be enrolled in the same or a different CA. You cannot use self-signed certificates for either peer.
- **Hash**: The hash algorithm for creating a message digest, which is used to ensure message integrity. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.

6. Click **Add**.

Create or edit an IKEv2 policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv2 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv2 Policy** link shown in the object list.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the Security Cloud Control navigation bar on the left, click **Objects**.
3. Do one of these things:
   - Click  and select **FTD > IKEv2 Policy** to create a new IKEv2 policy.
   - In the object page, select the IKEv2 policy you want to edit and click **Edit** in the Actions pane at the right.
4. Enter an **object name**, up to 128 characters.
5. Configure the IKEv2 properties.

- **Priority**: The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **State**: Whether the IKE policy is enabled or disabled. Click the toggle to change the state. Only enabled policies are used during IKE negotiations.
- **Encryption**: The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. Select all algorithms that you want to allow, although you cannot include both mixed-mode (AES-GCM) and normal mode options in the same policy. (Normal mode requires that you select an integrity hash, whereas mixed-mode prohibits a separate integrity hash selection.) The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding which encryption algorithm to use.
- **Diffie-Hellman Group**: The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest group until a match is agreed upon.
- **Integrity Hash**: The integrity portion of the hash algorithm for creating a message digest, which is used to ensure message integrity. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. The integrity hash is not used with the AES-GCM encryption options. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN.
- **Pseudo-Random Function (PRF) Hash**: The pseudo-random function (PRF) portion of the hash algorithm, which is used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN on page 729.
- **Lifetime**: The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).

6. Click **Add**.

Remote access VPN objects

Find details about remote access VPN objects for ASA and FDM-managed device, including identity sources, group policies, connection profiles, address pools, NAT exemption, and verification.

Remote access VPN (RA VPN) objects include identity sources, RADIUS servers and groups, and group policy objects for ASA and FDM-managed devices.

Identity sources for ASA

Identity sources, such as Microsoft Active Directory (AD) realms and RADIUS Servers, are AAA servers and databases that define user accounts for the people in your organization. You can use this information in a variety of ways, such as providing the user identity associated with an IP address or authenticating remote access VPN connections or access to Security Cloud Control.

Click **Objects**, then click ( )**>Identity Source** to create your sources. You would then use these objects when you configure the services that require an identity source. You can apply appropriate filters to search existing sources and manage them.

Determining the directory base DN

When you configure directory properties, you need to specify the common base distinguished name (DN) for users and groups. The base is defined in your directory server and differs from network to network. You must enter the correct bases for identity policies to work. If the base is wrong, the system cannot determine user or group names, and thus identity-based policies will be inoperable.

Note

To get the correct bases, consult the administrator who is responsible for the directory servers.

For an active directory, you can determine the correct bases by logging into the Active Directory server as a domain administrator, and using the **dsquery** command at a command prompt as follows to determine the bases:

User search base

Enter the **dsquery user** command with known username (partial or complete) to determine the base distinguished name. For example, the following command uses the partial name "John*" to return information for all users that start with "John."

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

The base DN would be "DC=csc-lab,DC=example,DC=com."

Group search base

Enter the **dsquery group** command with a known group name to determine the base distinguished name. For example, the following command uses the group name Employees to return the distinguished name:

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

The group base DN would be "DC=csc-lab,DC=example,DC=com."

You can also use the ADSI Edit program to browse the Active Directory structure (**Start** > **Run** > **adsiedit.msc**). In ADSI Edit, right-click any object, such as an organizational unit (OU), group, or user, and choose **Properties** to view the distinguished name. You can then copy the string of DC values as the base.

To verify that you have the correct base:

Procedure

1. Click the Test Connection button in the directory properties to verify connectivity. Resolve any problems, and save the directory properties.
2. Commit changes to the device.
3. Create an access rule, select the **Users** tab, and try to add known user and group names from the directory. You should see auto-complete suggestions as you type for matching users and groups in the realm that contains the directory. If these suggestions appear in a drop-down list, then the system was able to query the directory successfully.

If you see no suggestions, and you are certain the string you typed should appear in a user or group name, you need to correct the corresponding search base. See Create or Edit an ASA Active Directory Realm Object for more information.

RADIUS servers and groups

You can use RADIUS servers to authenticate and authorize administration users. When you configure a feature to use RADIUS servers, you select a RADIUS group instead of individual servers. A RADIUS group is a collection of RADIUS servers that are copies of each other. If a group has more than one server, they form a chain of backup servers to provide redundancy in case one server becomes unavailable. But even if you have only one server, you must create a one-member group to configure RADIUS support for a feature.

You can use this source for the following purposes:

- Remote Access VPN, as an identity source for authentication, and for authorization and accounting. You can use AD in conjunction with a RADIUS server.
- Identity policy, as a passive identity source to collect user identity from remote access VPN logins.

See Create and Edit an Adaptive Security Appliance RADIUS Server Object or Group for more information.

Create an ASA Active Directory realm object

When you create or edit an identity source object such as an AD realm object, Security Cloud Control Firewall Management sends the configuration request to the ASA devices through the SDC. The ASA then communicates with the configured AD realm.

Use the following procedure to create an object:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click **Create Object** ()**RA VPN Objects (ASA & FDM)** > **Identity Source**.
4. Enter an **Object Name** for the object.
5. Select the **Device Type** as **ASA**.
6. In the first part of the wizard, select **Active Directory Realm** as the **Identity Source Type**. Click **Continue**.
7. Configure the basic realm properties.
   - **Directory Username, Directory Password** - The distinguished username and password for a user with appropriate rights to the user information you want to retrieve. For Active Directory, the user does not need elevated privileges. You can specify any user in the domain. The username must be fully qualified; for example, Administrator@example.com (not simply Administrator).

> **Note**
>
> The system generates ldap-login-dn and ldap-login-password from this information. For example, Administrator@example.com is translated as cn=administrator,cn=users,dc=example,dc=com. Note that cn=users is always part of this translation, so you must configure the user you specify here under the common name “users” folder.

- **Base Distinguished Name** - The directory tree for searching or querying user and group information, that is, the common parent for users and groups. For example, cn=users,dc=example,dc=com.

8. Configure the directory server properties.
   - **Hostname/IP Address**–The hostname or IP address of the directory server. If you use an encrypted connection to the server, you must enter the fully-qualified domain name, not the IP address.
   - **Port**–The port number used for communications with the server. The default is 389. Use port 636 if you select LDAPS as the encryption method.
   - **Encryption**–To use an encrypted connection for downloading user and group information, select **LDAPS** to use SSL to secure communications between the ASA and the LDAP server. It requires LDAP over SSL. Use port 636.

     The default is **None**, which means that user and group information is downloaded in clear text.
9. (Optional) Use the **Test** button to validate the configuration.
10. (Optional) Click **Add another configuration** to add multiple Active Directory (AD) servers to the AD realm. The AD servers need to be duplicates of each other and support the same AD domain. Therefore, the basic realm properties such as **Directory name**, **Directory Password**, and **Base Distinguished Name** must be the same across all AD servers associated with that AD realm.
11. Click **Add**.

Edit an ASA Active Directory realm object

Note that you cannot change the Identity Source Type when editing an Identity source object. You must create a new object with the correct type.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object you want to edit by using object filters and search field.
4. Select the object you want to edit.
5. Click the edit icon in the **Actions** pane of the details panel.
6. Edit the values in the dialog box in the same fashion that you created in the procedures above. Expand the configuration bar listed below to edit or test the hostname/IP address or encryption information.
7. Click **Save**.
8. Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

9. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create an ASA RADIUS server object or group

When you create or edit an identity source object such as a RADIUS server object or a group of RADIUS server objects, Security Cloud Control sends the configuration request to ASA devices through the SDC.

Create an ASA RADIUS server object

RADIUS servers provide AAA (authentication, authorization, and accounting) services.

Use the following procedure to create an object:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click **Create Object** (+)**> RA VPN Objects (ASA & FDM)** > **Identity Source**.
4. Enter an **Object name** for the object.
5. Select the **Device Type** as **ASA**.
6. Select **RADIUS Server** as the **Identity Source Type**. Click **Continue**.
7. Edit the Identity Source configuration with the following properties:
   - **Server Name or IP Address** - The fully-qualified host name (FQDN) or IP address of the server.
   - **Authentication Port** (Optional) - The port on which RADIUS authentication and authorization are performed. The default is 1812.
   - **Timeout** - The length of time, 1-300 seconds, that the system waits for a response from the server before sending the request to the next server. The default is 10 seconds.
   - Enter the **Server Secret Key**(Optional) - The shared secret that is used to encrypt data between the ASA device and the RADIUS server. The key is a case-sensitive, alphanumeric string of up to 64 characters, with no spaces. The key must start with an alphanumeric character or an underscore, and it can contain the special characters: $ & - _ . + @. The string must match the one configured on the RADIUS server. If you do not configure a secret key, the connection is not encrypted.
8. Click **Add**.
9. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create an ASA RADIUS server group

A RADIUS server group contains one or more RADIUS server objects. Servers in the group must be copies of each other and form a backup chain.

Use the following procedure to create an object group:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click **Create Object** (+) **RA VPN Objects (ASA & FDM) Identity Source**.
4. Enter an **Object name** for the object.

5. Select the **Device Type** as **ASA**.
6. Select **RADIUS Server Group** as the Identity Source Type. Click **Continue**.
7. Edit the Identity Source configuration with the following properties:
   - **Dead Time** : Time to wait after the last server fails before reactivating all servers. Failed servers are reactivated only after all servers have failed.
   - **Maximum Failed Attempts** : Number of failed requests sent to a RADIUS server before the system tries the next server. When this number is exceeded, the system marks the server as failed.
   - **Dynamic Authorization/Port** Optional change of authorization (CoA) services. Enable only when this server group is used in RA VPN with Cisco ISE.
8. Select an AD realm that supported the RADIUS server from the drop-down menu. If you have not already created an AD realm, click **Create** from inside the drop-down menu.
9. Click the **RADIUS SERVER Add** button  to add existing RADIUS server objects. Optionally, you can create a new RADIUS server object from this window is necessary.

   Note

   Add RADIUS server objects in priority order. The first server is used until it becomes unresponsive, and ASA then uses the next server in the list.

10. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Edit an ASA Radius server object or group

Use the following procedure to edit a Radius server object or Radius server group:

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the object you want to edit by using object filters and search field.
4. Select the object you want to edit.
5. Click the edit icon  in the **Actions** pane of the details panel.
6. Edit the values in the dialog box in the same fashion that you created them in the procedures above. To edit or test the hostname/IP address or encryption information, expand the configuration bar.
7. Click **Save**.
8. Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.
9. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create a new RA VPN group policy

A group policy is a set of user-oriented attribute/value pairs for remote access VPN connections. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

The system includes a default group policy named "DfltGrpPolicy". You can create additional group policies to provide the services you require.

> **Note**
>
> You cannot add inconsistent group policy objects to RA VPN configuration. Resolve all inconsistencies before adding the group policy to the RA VPN Configuration.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click + > **RA VPN Objects (ASA & FTD)** > **RA VPN Group Policy**.
4. Enter a name for the group policy. The name can be up to 64 characters and spaces are allowed.
5. In the **Device Type** drop-down, select **FTD** or **ASA**.
6. Click the required tabs and configure the attributes on the page. For more information, refer to Group policy attributes.
7. Click **Save** to create the group policy.

RA VPN group policy attributes

The general attributes of a group policy define the name of the group and some other basic settings. The Name attribute is the only required attribute.

- **DNS Server**: Select the DNS server group that defines the DNS servers clients should use for domain name resolution when connected to the VPN. If the group you need is not yet defined, click **Create DNS Group** and create it now.
- **Banner**: The banner text, or welcome message, to present to users at login. The default is no banner. The length can be up to 496 characters. The AnyConnect client supports partial HTML. To ensure that the banner displays properly to remote users, use the <BR> tag to indicate line breaks.
- **Default Domain**: The default domain name for users in the RA VPN. For example, example.com. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.
- **AnyConnect Client Profiles**: Click + and select the AnyConnect Client Profiles to use for this group. See Configure and Upload AnyConnect Client Profiles. If you configure a fully-qualified domain name for the outside interface (in the connection profile), a default profile will be created for you. Alternatively, you can upload your client profile. Create these profiles using the Standalone AnyConnect Profile Editor, which you can download and install from software.cisco.com. If you do not select a client profile, the AnyConnect client uses default values for all options. The items in this list are AnyConnect Client Profile objects rather than the profiles themselves. You can create (and upload) new profiles by clicking **Create New AnyConnect Client Profile** in the drop-down list.

AnyConnect Client profiles

This feature is supported on Firewall Device Manager running software version 6.7 or later versions.

Cisco AnyConnect VPN client offers enhanced security through various built-in modules. These modules provide services such as web security, network visibility into endpoint flows, and off-network roaming protection. Each client module includes a client profile that includes a group of custom configurations as per your requirement.

You can select the AnyConnect VPN profile object and AnyConnect modules to be downloaded to clients when the VPN user downloads the VPN AnyConnect client software.

1. Choose or create an AnyConnect VPN profile object. See Upload RA VPN AnyConnect Client Profile on page 796. Except for DART and Start Before Login modules, the AnyConnect VPN profile object must be selected.
2. Click **Add Any Connect Client Module**.

   The following AnyConnect modules are optional and you can configure these modules to be downloaded with VPN AnyConnect client software:

   - **AMP Enabler** – Deploys advanced malware protection (AMP) for endpoints.
   - **DART** – Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
   - **Feedback** – Provides information about the features and modules customers have enabled and used.
   - **ISE Posture** – Uses the OPSWAT library to perform posture checks to assess an endpoint's compliance.
   - **Network Access Manager** – Provides 802.1X (Layer 2) and device authentication to access both wired and wireless networks.
   - **Network Visibility** – Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics.
   - **Start Before Login** – Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.
   - **Umbrella Roaming Security** – Provides DNS-layer security when no VPN is active.
   - **Web Security** – Analyzes the elements of a web page, allows acceptable content, and blocks malicious or unacceptable content based on a defined security policy.
3. In the **Client Module** list, select an **AnyConnect module**.
4. In the **Profile** list, choose or create a profile object containing an AnyConnect Client Profile.
5. Select **Enable Module Download** to enable endpoints to download the client module along with the profile. If not selected, the endpoints can download only the client profile.

Session setting attributes

The session settings of a group policy control how long users can connect through the VPN and how many separate connections they can establish.

- **Maximum Connection Time**: The maximum length of time, in minutes, that users can stay connected to the VPN without logging out and reconnecting, from 1- 4473924 or blank. The default is unlimited (blank), but the idle timeout still applies.
- **Connection Time Alert Interval**: If you specify a maximum connection time, the alert interval defines the amount of time before the maximum time is reached to display a warning to the user about the upcoming automatic disconnect. The user can choose to end the connection and reconnect to restart the timer. The default is 1 minute. You can specify 1 to 30 minutes.
- **Idle Time**: The length of time, in minutes, that the VPN connection can be idle before it is automatically closed, from 1-35791394. If there is no communication activity on the connection for this consecutive number of minutes, the system stops the connection. The default is 30 minutes.
- **Idle Time Alert Interval**: The amount of time before the idle time is reached to display a warning to the user about the upcoming automatic disconnect due to an idle session. Any activity resets the timer. The default is 1 minute. You can specify 1 to 30 minutes.
- **Simultaneous Login Per User**: The maximum number of simultaneous connections allowed for a user. The default is 3. You can specify 1 to 2147483647 connections. Allowing many simultaneous connections might compromise security and affect performance.

Address assignment attributes

The address assignment attributes of a group policy define the IP address pool for the group. The pool defined here overrides the pool defined in any connection profile that uses this group. Leave these settings blank if you want to use the pool defined in the connection profile.

- **IPv4 Address Pool, IPv6 Address Pool**: These options define the address pools for the remote endpoints. Clients are assigned an address from these pools based on the IP version they use to make the VPN connection. Select a network object that defines a subnet for each IP type you want to support. Leave the list empty if you do not want to support that IP version. For example, you could define an IPv4 pool as `10.100.10.0/24`. The address pool cannot be on the same subnet as the IP address for the outside interface. You can specify a list of up to six address pools to use for local address allocation. The order in which you specify the pools is significant. The system allocates addresses from these pools in the order in which the pools appear.
- **DHCP Scope**: If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same pool identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group. If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address. To specify a scope, select the network object that contains the network number host address. Click **Create New Network** if the object does not yet exist. For example, to tell the DHCP server to use addresses from the `192.168.5.0/24` subnet pool, select a network object that specifies `192.168.5.0` as a host address. You can use DHCP for IPv4 addressing only.

Split tunneling attributes

The split tunneling attributes of a group policy define how the system should handle traffic meant for the internal network vs. externally-directed traffic. Split tunneling directs some network traffic through the VPN tunnel (encrypted) and the remaining network traffic outside the VPN tunnel (unencrypted or in clear text).

- **IPv4 Split Tunneling**, **IPv6 Split Tunneling**: You can specify different options based on whether the traffic uses IPv4 or IPv6 addresses, but the options for each are the same. If you want to enable split tunneling, specify one of the options that require you to select network objects.
  - **Allow all traffic over tunnel**: Do no split tunneling. Once the user makes an RA VPN connection, all the user's traffic goes through the protected tunnel. This is the default. It is also considered the most secure option.
  - **Allow specified traffic over the tunnel**: Select the network objects that define destination network and host addresses. Any traffic to these destinations goes through the protected tunnel. The client routes traffic to any other destination to connections outside the tunnel (such as a local Wi-Fi or network connection).
  - **Exclude networks specified below**: Select the network objects that define destination network or host addresses. The client routes any traffic to these destinations to connections outside the tunnel. Traffic to any other destination goes through the tunnel.
- **Split DNS** - You can configure the system to send some DNS requests through the secure connection while allowing the client to send other DNS requests to the DNS servers configured on the client. You can configure the following DNS behavior:
  - **Send DNS Request as per split tunnel policy**: With this option, DNS requests are handled the same way as the split tunnel options are defined. If you enable split tunneling, DNS requests are sent based on the destination addresses. If you do not enable split tunneling, all DNS requests go over the protected connection.
  - **Always send DNS requests over tunnel**: Select this option if you enable split tunneling, but you want all DNS requests sent through the protected connection to the DNS servers defined for the group.
  - **Send only specified domains over tunnel**: Select this option if you want your protected DNS servers to resolve addresses for certain domains only. Then, specify those domains, separating domain names with commas. For example, example.com, example1.com. Use this option if you want your internal DNS servers to resolve names for internal domains, while external DNS servers handle all other Internet traffic.

AnyConnect attributes

The AnyConnect attributes of a group policy define some SSL and connection settings used by the AnyConnect client for a remote access VPN connection.

- **SSL Settings**
  - **Enable Datagram Transport Layer Security (DTLS)**: Whether to allow the AnyConnect client to use two simultaneous tunnels: an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect with an SSL tunnel only.
  - **DTLS Compression**: Whether to compress Datagram Transport Layer Security (DTLS) connections for this group using LZS. DTLS Compression is disabled by default.
  - **SSL Compression**: Whether to enable data compression, and if so, the method of data compression to use, **Deflate**, or **LZS**. SSL Compression is **Disabled** by default. Data compression speeds up transmission rates but also increases the memory requirement and CPU usage for each user session. Therefore, SSL compression decreases the overall throughput of the device.
  - **SSL Rekey Method**, **SSL Rekey Interval**: The client can rekey the VPN connection, renegotiating the crypto keys and initialization vectors, to increase the security of the connection. Disable rekeying by selecting **None**. To enable rekey, select **New Tunnel** to create a new tunnel each time. (The **Existing Tunnel** option results in the same action as **New Tunnel**.) If you enable rekeying, also set the rekey interval, which is 4 minutes by default. You can set the interval to 4-10080 minutes (1 week).
- **Connection Settings**
  - **Ignore the DF (Don't Fragment) bit**: Whether to ignore the Don't Fragment (DF) bit in packets that need fragmentation. Select this option to allow the forced fragmentation of packets that have the DF bit set, so that these packets can pass through the tunnel.
  - **Client Bypass Protocol** - Allows you to configure how the secure gateway manages IPv4 traffic (when it is expecting only IPv6 traffic), or how it manages IPv6 traffic (when it is expecting only IPv4 traffic).

    When the AnyConnect client makes a VPN connection to the headend, the headend assigns it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the headend assigns the AnyConnect connection only an IPv4 address or only an IPv6 address, you can configure the Client Bypass Protocol to drop network traffic for which the headend did not assign an IP address (default, disabled, not checked), or allow that traffic to bypass the headend and be sent from the client unencrypted or "in the clear" (enabled, checked).

    For example, assume that the secure gateway assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual-stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.
  - **MTU**: The maximum transmission unit (MTU) size for SSL VPN connections established by the Cisco AnyConnect VPN Client. The default is 1406 bytes. The range is 576 to 1462 bytes.
    - **Keepalive Messages Between AnyConnect and VPN Gateway**: Whether to exchange keepalive messages between peers to demonstrate that they are available to send and receive data in the tunnel. Keepalive messages transmit at set intervals. The default interval is 20 seconds, and the valid range is 15 to 600 seconds.
    - **DPD on Gateway Side Interval**, **DPD on Client Side Interval**: Enable Dead Peer Detection (DPD) to ensure that the VPN gateway or VPN client quickly detects when the peer is no longer responding. You can separately enable gateway or client DPD. The default interval is 30 seconds for sending DPD messages. The interval can be 5-3600 seconds.

Traffic filters attributes

The traffic filter attributes of a group policy define restrictions you want to place on users assigned to the group. You can use these attributes instead of creating access control policy rules to restrict RA VPN users to specific resources, based on host or subnet address and protocol, or VLAN. By default, RA VPN users are not restricted by the group policy from accessing any destination on your protected network.

- **Access List Filter**: Restrict access using an extended access control list (ACL). Select the Smart CLI Extended ACL object. The extended ACL lets you filter based on source address, a destination address, and protocol (such as IP or TCP). ACLs are evaluated on a top-down, first-match basis, so ensure that you place specific rules before more general rules. There is an implicit "deny any" at the end of the ACL, so if you intend to deny access to a few subnets while allowing all other access, ensure that you include a "permit any" rule at the end of the ACL. Because you cannot create network objects while editing an extended ACL Smart CLI object, you should create the ACL before editing the group policy. Otherwise, you might need to simply create the object, then go back later to create the network objects and then all the access control entries that you need. To create the ACL, log in to Firewall Device Manager, go to **Device** > **Advanced Configuration** > **Smart CLI** > **Objects**, create an object, and select **Extended Access List** as the object type.
- **Restrict VPN to VLAN**: Also called "VLAN mapping," this attribute specifies the egress VLAN interface for sessions to which this group policy applies. The system forwards all traffic from this group to the selected VLAN. Use this attribute to assign a VLAN to the group policy to simplify access control. Assigning a value to this attribute is an alternative to using an ACL to filter traffic on a session. Ensure that you specify a VLAN number that is defined on a subinterface on the device. Values range from 1 to 4094.

Windows browser proxy attributes

The Windows browser proxy attributes of a group policy determine how, and whether, a proxy defined on the user's browser operates.

You can select one of the following values for **Browser Proxy During VPN Session**:

- **No change in endpoint settings**: Allow the user to configure (or not configure) a browser proxy for HTTP and use the proxy if it is configured.
- **Disable browser proxy**: Do not use the proxy defined for the browser, if any. No browser connections will go through the proxy.
- **Auto detect settings**: Enable the use of automatic proxy server detection in the browser for the client device.
- **Use custom settings**: Define a proxy that should be used by all client devices for HTTP traffic. Configure the following settings:
  - **Proxy Server IP or Hostname**, **Port**: The IP address, or hostname, of the proxy server, and the port used for proxy connections by the proxy server. The host and port combined cannot exceed 100 characters.
  - **Browser Proxy Exemption List**: Connections to the hosts/ports in the exemption list do not go through the proxy. Add all the host/port values for destinations that should not use the proxy. For example, www.example.com port 80. Click **Add proxy exemption** to add items to the list. Click the trash can icon to delete items. The entire proxy exception list, combining all addresses and ports, cannot be longer than 255 characters.

Service objects

Learn how service objects represent protocols and ICMP values that Security Cloud Control Firewall Management recognizes and manages in supported device configurations.

ASA service objects

ASA service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the IP protocol suite. In a service object you can specify a single protocol and assign it to a source port, destination port, or both source and destination ports. A service group contains many service objects and can include a mix of protocols.

A port group is a kind of ASA service object. Port groups contain port objects that pair a service type, such as TCP or UDP, and a port number or a range of port numbers. You can then use the objects in security policies for the purposes of defining traffic matching criteria. For example, you can use them in access control rules to allow traffic to a specific range of TCP ports.

See Create and Edit ASA Service Objects for more information.

Firepower service objects

FTD service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the IP protocol suite.

FTD service groups are collections of service objects. A service group may contain objects for one or more protocols. You can use the objects and groups in security policies for purposes of defining network traffic matching criteria, for example, to use access rules to allow traffic to specific TCP ports. The system includes several pre-defined objects for common services. You can use these objects in your policies; however, you cannot edit or delete system-defined objects.

Firepower Device Manager and Firepower Management Center refer to service objects as port objects and service groups and port groups.

See Create and Edit Firepower Threat Defense Service Objects for more information.

Protocol objects

Protocol objects are a type of service object that contain less-commonly used or legacy protocols. Protocol objects are identified by a name and protocol number. Security Cloud Control recognizes these objects in ASA and Firepower (FDM-managed device) configurations and gives them their own filter of "Protocols" so you can find them easily.

See Create and Edit Firepower Threat Defense Service Objects for more information.

ICMP objects

An Internet Control Message Protocol (ICMP) object is a service object specifically for ICMP and IPv6-ICMP messages. Security Cloud Control recognizes these objects in ASA and Firepower configurations when those devices are onboarded and Security Cloud Control gives them their own filter of "ICMP" so you can find the objects easily.

Using Security Cloud Control, you can rename or remove ICMP objects from an ASA configuration. You can use Security Cloud Control to create, update, and delete ICMP and ICMPv6 objects in a Firepower configuration.

Note

For the ICMPv6 protocol, AWS does not support choosing specific arguments. Only rules that allow all ICMPv6 messages are supported.

See Create and Edit Firepower Threat Defense Service Objects for more information.

Create and Edit ASA Service Objects

In a service object, you can specify a single protocol and assign it to a source port, destination port, or both source and destination ports.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click **Create Object** > **ASA** > **Service**.
4. Enter an object name.
5. Select **Create a service object**
6. Click the **Service Type** button and select the protocol for which you want to make an object.
   - **For TCP, UDP, and TCP-UDP service types,** enter a source port, destination port, or both:
     - The source port identifier allows you to match traffic originating from a particular numbered port. In the source port identifier, select an operator: equal to, range, less than, greater than, or not equal to and provide the appropriate port number or range.
     - The destination port identifier allows you to match traffic arriving at a particular numbered port. In the destination port identifier, select an operator: equal to, range, less than, greater than, or not equal to and provide the appropriate port number or range.
   - **For Protocol service types**, enter a protocol number between 0-255, or a well-known name, such as ip, tcp, udp, gre, and so forth.
7. Click **Add**.

Examples

- A service object that identifies incoming FTP traffic would be one with a TCP Service type and a destination port range of 21.
- A service object that identifies outgoing DNS and DNS over TCP traffic would be one with a tcp-udb service type and a source port equal to 53.

Create an ASA Service Group

A service group can be made up of one or more service objects representing one or more protocols.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Objects**.
3. Choose **Create Object** > **ASA** > **Service**.
4. Enter an object name.
5. Select **Create a service group.**
6. Add an existing object by clicking **Add Object,** selecting an object, and clicking **Select**. Repeat this step to add more objects.
7. If needed, add an extra individual service type value to the service group
   - **For TCP, UDP, and TCP-UDP service types,** enter a source port, destination port, or both:
     - The source port identifier allows you to match traffic originating from a particular numbered port. In the source port identifier, select an operator: equal to, range, less than, greater than, or not equal to and provide the appropriate port number or range.

- The destination port identifier allows you to match traffic arriving at a particular numbered port. In the destination port identifier, select an operator: equal to, range, less than, greater than, or not equal to and provide the appropriate port number or range.

- **For Protocol service types**, enter a protocol number between 0-255, or a well-known name, such as ip, tcp, udp, gre, and so forth.

8. To add more individual port values, click **Add Another Value** and repeat step 6.
9. Click **Add** when you are done adding service objects and service values to the service group.

Edit an ASA Service Object or Service Group

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Filter the objects to find the object you want to edit and then select the object in the object table.
4. In the details pane, click edit .
5. Edit the values in the dialog box in the same fashion that you created them in the procedures above.
6. Click **Save**.
7. Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Create and edit Firepower service objects

To create a firepower service object, follow these steps:

Firewall Device Manager (FDM-managed) service objects are reusable components that specify a TCP/IP protocol and a port. The Firewall Device Manager, On-Premises Firewall Management Center and Cloud-Delivered Firewall Management Center refer to these objects as "Port Objects."

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click > **FTD** > **Service**.
4. Enter an object name and description.
5. Select **Create a service object.**
6. Click the **Service Type** button and select the protocol for which you want to create an object.
7. Configure the protocol as follows:

   - **TCP**, **UDP**

     - Select **eq** and then enter either a port number or a protocol name. For example, you could enter 80 as a port number or HTTP as the protocol name.

     - You can also select **range** and then enter a range of port numbers, for example, **1 65535** (to cover all ports).

- **ICMP**, **IPv6-ICMP**-Select the ICMP **Type.** Select **Any** for the type to apply to all ICMP messages. For information on the types and codes, see the following pages:
  - ICMP-http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6-http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **Other**-Select the desired protocol.

8. Click **Add**.
9. Review and deploy the changes you made now, or wait and deploy multiple changes at once.

Create a Firepower Service Group

A service group can be made up of one or more service objects representing one or more protocols. The service objects need to be created before they can be added to the group. The Firepower Device Manager and Firepower Management Center refer to these objects as "Port Objects."

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click  > **FTD** > **Service**.
4. Enter an object name and description.
5. Select **Create a service group.**
6. Add an object to the group by clicking **Add Object.**
   - Click **Create** to create a new object as you did above in Create a Firepower Service Object above.
   - Click **Choose** to add an existing service object to the group. Repeat this step to add more objects.
7. Click **Add** when you are done adding service objects to the service group.
8. Review and deploy the changes you made now, or wait and deploy multiple changes at once.

Edit a Firepower service object or service group

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Filter the objects to find the object you want to edit and then select the object in the object table.
4. In the Actions pane, click **Edit** .
5. Edit the values in the dialog box in the same fashion that you created them in the procedures above.
6. Click **Save**.
7. Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.
8. Review and deploy the changes you made now, or wait and deploy multiple changes at once.

Create or Edit a Meraki Service Object

About Service Objects

Service objects are reusable components that specify a TCP/IP protocol and a port. Security Cloud Control categorizes these objects as service objects. When you deploy to the MX device, Security Cloud Control translates the objects into protocols or port ranges. See Objects associated with Meraki devices for more information about how Security Cloud Control handles Meraki protocols as objects.

Create a Service Object

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click , then click **FTD** > **Service** or **ASA** > **Service**.
4. Enter an object name and description.
5. Select **Create a service object**.
6. Click the **Service Type** button and select the protocol for which you want to create an object.
7. Enter the information to identify the protocol by taking one of these actions:
   - Enter the specific port number for the TCP or UDP port.
   - Select the ICMP or ICMPv6 message type.
   - If you selected the "other" service type, select one of the TCP/IP protocols from the list.
8. Click **Add**.
9. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create a Service Group

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click , then click **FTD** > **Service**.

   Note

   Meraki does not support ASA service groups.
4. Enter an object name and description.
5. Select **Create a service group.**
6. Add an existing object by clicking **Add Object,** selecting an object, and clicking **Select**. Repeat this step to add more objects.
7. Click **Add** when you are done adding service objects and service values to the service group.

8. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Edit a Service Object or a Service Group

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Filter the objects to find the object you want to edit and then select the object in the object table.
4. In the details pane, click edit .
5. Edit the values in the dialog box in the same fashion that you created them in the procedures above.
6. Click **Save**.
7. Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it. The object is now ready to be used in the Meraki policy.
8. Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Security group tag group

An overview of security group tag group, including Security Group Tag Group Security, and expected results.

Security Group Tags

About Security Group Tags

If you use Cisco Identity Services Engine (ISE) to define and use **security group tag** (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as matching criteria. Thus, you can block or allow access based on security group membership rather than IP addresses.

In ISE, you can create a SGT and assign host or network IP addresses to each tag. If you assign an SGT to a user's account, the SGT is assigned to the user's traffic. After you configure FDM-managed device to connect to an ISE server and create the SGT, you can create SGT groups in Security Cloud Control and build access control rules around them. Note that you must configure ISE's SGT Exchange Protocol (SXP) mapping before you can associate an SGT to an FDM-managed device. See **Security Group Tag Exchange Protocol** in the Cisco Identity Services Engine Administrator Guide of the version you are currently running for more information.

When an FDM-managed device evaluates SGT as a traffic matching criteria for an access control rule, it uses the following priority:

1. The source SGT defined in the packet, if any. No destination matching is done using this technique. For the SGT 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.
2. The SGT assigned to the user session, as downloaded from the ISE session directory. You need to enable the option to listen to session directory information for this kind of SGT matching, but this option is on by default when you first create the ISE identity source. The SGT can be matched to source or destination. Although not required, you would also normally set up a passive authentication identity rule, using the ISE identity source along with an AD realm, to collect user identity information.
3. The SGT-to-IP address mapping downloaded using SXP. If the IP address is within the range for an SGT, then the traffic matches the access control rule that uses the SGT. The SGT can be matched to source or destination.

> **Note**
>
> You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information. Your SGT groups can refer to more than one SGT, so you can apply policy based on a relevant collections of tags if that is appropriate.

Version Support

Security Cloud Control currently supports SGT and SGT groups on FDM-managed devices running Version 6.5 and later. an FDM-managed device allows you to configure and connect to an ISE server in Version 6.5 and later but not does not support SGT configuration in the UI until Version 6.7.

From the FDM-managed UI, this means that an FDM-managed device running Version 6.5 or later can download SXP mappings of SGTs but cannot be manually added to objects or access control rules. To make changes to the SGTs for devices running Version 6.5 or Version 6.6, you must use the ISE UI. If the device running Version 6.5 is onboarded to Security Cloud Control, however, you can see the current SGTs associated with the device and create SGT groups.

SGT in Security Cloud Control

Security Group Tags

SGTs are read-only in Security Cloud Control. You cannot create or edit an SGT in Security Cloud Control. To create an SGT, see the Cisco Identity Services Engine Administrator Guide of the version your are currently running.

SGT Groups

> **Note**
>
> An FDM-managed device refers to groups of SGTs as SGT dynamic objects. In Security Cloud Control, these lists of tags are currently called SGT groups. You can create an SGT group in Security Cloud Control without referring to the FDM-managed device or ISE UI.

Use SGT groups to identify source or destination addresses based on an SGT assigned by ISE. You can then use the objects in access control rules for purposes of defining traffic matching criteria. You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information.

Your SGT groups can refer to more than one SGT, so you can apply policy based on relevant collections of tags if that is appropriate.

In order to create an SGT group in Security Cloud Control, you must have at least one SGT already configured and SGT mappings from an ISE server configured for the FDM-managed console of the device you want to use. Note that if more than one FDM-managed device is associated with the same ISE server, an SGT or SGT group can be applied to more than one device. If a device is not associated with an ISE server, you cannot include SGT objects in your access control rule, or apply an SGT group to that device configuration.

SGT Groups in Rules

SGT groups can be added to access control rules; they appear as source or destination network objects. For more information about how networks work in rules, see Source and Destination Criteria in an FDM Access Control Rule.

You can create an SGT group from the Objects page. See Create an SGT Group on page 177 for more information.

Create an SGT Group

To create an SGT group that can be used for an access control rule, use the following procedure:

Before you begin

You must have the following configurations or environments configured prior to creating a security group tag (SGT) group:

- FDM-managed device must be running at least Version 6.5.
- You must configure the ISE identity source to subscribe to SXP mappings and enable deploy changes. To manage SXP mappings, see **Configure Security Groups and SXP Publishing in ISE** of the Firepower Device Manager Configuration Guide for the version you're using, Version 6.7 and later.
- All SGTs must be created in ISE. To create an SGT, see the Cisco Identity Services Engine Configuration Guide of the version your are currently running.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. On the left pane, click **Objects**.
3. Click  > **FTD** > **Network**.
4. Enter an **Object Name**.
5. (Optional) Add a description.
6. Click **SGT** and use the drop-down menu to check all the applicable SGTs you want included in the group. You can sort the list by SGT name.
7. Click **Save**.

> **Note**
>
> You cannot create or edit SGTs in Security Cloud Control, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Edit an SGT Group

To edit an SGT group, use the following procedure:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Locate the SGT group you want to edit by using object filters and search field.
4. Select the SGT group and click the edit icon  in the **Actions** pane.
5. Modify the SGT group. Edit the name, description, or the SGTs associated with the group.

6. Click **Save**.

> **Note**
>
> You cannot create or edit SGTs in Security Cloud Control, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Add an SGT Group to an Access Control Rule

To add an SGT group to an access control rule, use the following procedure:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the **FTD** tab and select the device you want to add the SGT group to.
4. In the**Management** pane, select **Policy**.
5. Click the blue plus button  for either the **Source** or **Destination** objects and select **SGT Groups**.
6. Locate the SGT group(s) you want to edit by using object filters and search field.
7. Click **Save**.
8. Preview and Deploy Configuration Changes for All Devices.

> **Note**
>
> If you need to create an additional SGT group, click **Create New Object**. Fill in the required information mentioned in Create an FTD SGT Group and **Add** the SGT group to the rule.

ASA time range objects

An overview of ASA time range objects, including rule order, interface assignment, logging, search, and deployment considerations.

A time range object defines a specific time that consists of a start time, an end time, and optional recurring entries. You use time range objects in network policies to provide time-based access to features or assets. Creating a time range object does not restrict access to the device. The configured times are local to the device.

You can add absolute or recurring time ranges to a time range object. Recurring ranges are periodic time ranges.

> **Note**
>
> If a time range has both absolute and periodic values, Security Cloud Control evaluates the periodic values only after the absolute start time is reached and stops evaluating them after the absolute end time is reached.

Create an ASA time range object

Use the following procedure to create a time range object for an ASA device:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Click  > **ASA** > **Time Range**.
4. Enter an object name.
5. Define a time range.
   - Absolute Time Range: Enter a start time and an end time. A time range object can have only one absolute time range.
   - Recurring Time Ranges: Click the  icon to add a periodic time range that repeats during the week. Select the frequency, days of the week, start time, and end time. A time range object can have multiple periodic ranges.

   > **Note**
   >
   > Start and end times are optional. If no start time is configured, the time range starts immediately. If no end time is configured, the time range lasts indefinitely.

6. Click **Add** to create the object.

Edit an ASA time range object

Use the following procedure to edit a time range object for an ASA device:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Filter the objects to find the object you want to edit and then select the object in the object table.
4. In the details pane, click edit .
5. Edit the values as needed and click **Save**.

6. If the object is currently used by any policies, Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.
7. If the object is used in a policy on a device, review and deploy now the changes you made, or wait and deploy multiple changes at once.

Troubleshooting Objects

Learn how to troubleshoot object issues in Security Cloud Control, including duplicate, unused, and inconsistent objects, bulk issue resolution, and ignored object review.

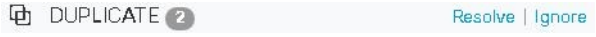
Resolve Duplicate Object Issues

Duplicate objects are two or more objects on the same device with different names but the same values. These objects are usually created accidentally, serve similar purposes, and are used by different policies. After resolving duplicate object issues, Security Cloud Control updates all affected object references with the retained object name.

To resolve duplicate object issues:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects** and choose an option.
3. Then filter the objects to find duplicate object issues.
4. Select one of the results. In the objects details panel, you will see the DUPLICATE field with the number of duplicates affected:



5. Click **Resolve**. Security Cloud Control displays the duplicate objects for you to compare.
6. Select two of the objects to compare.
7. You now have these options:
   - If you want to replace one of the objects with the other, click **Pick** for the object you to keep, click **Resolve** to see what devices and network policies will be affected, and then click **Confirm** if you are satisfied with the changes. Security Cloud Control keeps the object you selected as the replacement and deletes the duplicate.
   - If you have an object in the list that you want to ignore, click **Ignore**. If you ignore an object, it will be removed from the list of duplicate objects that Security Cloud Control shows you.
   - Click **Ignore All** if you want to keep the object but do not want Security Cloud Control to find it in a search for duplicate objects.
8. Once the duplicate object issue has been resolved review and deploy the changes you made now, or wait and deploy multiple changes at once.

Resolving Inconsistent or Unused Security Zone Objects

Security zone objects can be marked inconsistent or unused like other objects. See Resolve Unused Object Issues and Resolve Inconsistent Object Issues for instructions on how to resolve these issues.

Resolve Unused Object Issues

Unused objects are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule.

Resolve an Unused Object Issue

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects** and choose an option.
3. Then filter the objects to find unused object issues.
4. Select one or more unused objects.
5. You now have these options:
   - In the Actions pane, click **Remove** to remove the unused object from Security Cloud Control.
   - In the Issues pane, click **Ignore.** If you ignore an object, Security Cloud Control will stop displaying it among the results of unused objects objects.
6. If you removed the unused object, Preview and deploy configuration changes for all devices on page 817 the changes you made now, or wait and deploy multiple changes at once.

> **Note**
>
> To resolve unused object issues in bulk, see Resolve Object Issues in Bulk on page 184.

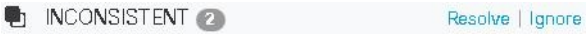
Remove Unused Objects in Bulk

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects** and choose an option.
3. Then filter the objects to find unused object issues.
4. Select the unused objects you want to delete:
   - Click the checkbox in the object table header row to select all the objects on the page.
   - Select individual unused objects in the object table.
5. In the Actions pane on the right, click **Remove** to remove all the unused objects you selected in Security Cloud Control. You can remove 99 objects at a time.
6. Click **OK** to confirm you want to delete the unused objects.
7. You have two choices to deploy these changes:
   - Review and deploy the changes you made now, or wait and deploy multiple changes at once.

- Open the **Security Devices** page and find the devices that were affected by the change. Select all the devices affected by the change and, in the **Management** pane, click **Deploy All**. Read the warning and take the appropriate action.

Resolve Inconsistent Object Issues

Inconsistent objects 

are objects with the same name, but different values, on two or more devices. Sometimes users create objects in different configurations with the same name and content, but over time the values of these objects diverge, which creates the inconsistency.

Note: To resolve inconsistent object issues in bulk, see Resolve Object Issues in Bulk.

You can perform the following on inconsistent objects:

- **Ignore:** Security Cloud Control ignores the inconsistency between objects and retains their values. The objects will no longer be listed under the inconsistency category.
- **Merge:** Security Cloud Control combines all selected objects and their values into a single object group.
- **Rename:** Security Cloud Control allows you to rename one of the inconsistent objects and give it a new name.
- **Convert Shared Network Objects to Overrides:** Security Cloud Control allows you to combine inconsistent shared objects (with or without overrides) into a single shared object with overrides. The most common default value from the inconsistent objects is set as a default in the newly formed object.

  > **Note**
  >
  > If there are multiple common default values, one of them is selected as the default. The remaining default values and override values are set as overrides of that object.

- **Convert Shared Network Group to Additional Values:** - Security Cloud Control allows you to combine inconsistent shared network groups into a single shared network group with additional values. The criteria for this functionality is that the inconsistent network groups to be converted must have a minimum of one common object with the same value. All default values that match this criterion becomes the default values, and the remaining objects are assigned as additional values of the newly formed network group.

  For example, consider two inconsistent shared network groups. The first network group 'shared_network_group' is formed with 'object_1' (192.0.2.x) and 'object_2' (192.0.2.y). It also contains additional value 'object_3' (192.0.2.a). The second network group 'shared_network_group' is formed with 'object_1' (192.0.2.x) and additional value 'object_4' (192.0.2.b). On converting the shared network group to additional values, the newly formed group 'shared_network_group' contain 'object_1' (192.0.2.x) and 'object_2' (192.0.2.y)' as default values and 'object_3' (192.0.2.a) and 'object_4' (192.0.2.b) as additional values.

  > **Note**
  >
  > When you create a new network object, Security Cloud Control auto assigns its value as an override to an existing shared network object with the same name. This is also applicable when a new device is onboarded to Security Cloud Control.

The auto-assignment happens only when the following criteria are met:

1. The new network object must be assigned to a device.
2. Only one shared object with the same name and type must be existing in the tenant.
3. The shared object must already contain overrides.

To resolve inconsistent object issues:

Procedure

1. In the Security Cloud Control navigation bar on the left, click **Objects** and choose an option.
2. Then filter the objects to find inconsistent object issues.
3. Select an inconsistent object. In the objects details panel, you will see the INCONSISTENT field with the number of objects affected:
   
4. Click **Resolve**. Security Cloud Control displays inconsistent objects for you to compare.
5. You now have these options:
   - **Ignore All:**
     a. Compare the objects presented to you and on one of the objects, click **Ignore**. Or, to ignore all objects, click **Ignore All**.
     b. Click **OK** to confirm.
   - **Resolve by merging objects:**
     a. Click **Resolve by Merging X Objects**.
     b. Click **Confirm**.
   - **Rename:**
     a. Click **Rename**.
     b. Save your changes to affected network policies and devices and click **Confirm**.
   - **Convert to Overrides (for inconsistent shared objects):** When comparing shared objects with overrides, the comparison panel shows only the default values in the **Inconsistent Values** field.
     a. Click **Convert to Overrides**. All inconsistent objects will be converted to a single shared object with overrides.
     b. Click **Confirm**. You can click **Edit Shared Object** to view the details of the newly formed object. You can use up and down arrows to move the values between default and override.
   - **Convert to Additional Values (for inconsistent network groups):**
     a. Click **Convert to Additional Values**. All inconsistent objects will be converted to a single shared object with additional values.
     b. Save your changes to affected network policies and devices and click **Confirm**.
6. After resolving the inconsistencies, review and deploy now the changes you made, or wait and deploy multiple changes at once.

Resolve Object Issues in Bulk

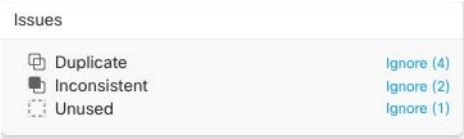
Important

If the object becomes associated with another issue type at a later time, the ignore action you committed only affects the issues you selected at that time. For example, if you ignored an object because it was a duplicate and the object is later marked inconsistent, ignoring it as a duplicate object does not mean it will be ignored as an inconsistent object.

To ignore issues in bulk, follow this procedure:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects** and choose an option.
3. To narrow your search, you can filter object issues.
4. In the Object table, select all the applicable objects you want to ignore. The Issues pane groups objects by issue type.



5. Click **Ignore** to ignore issues by type. You must **Ignore** each issue type separately.
6. Click **OK** to confirm you want to ignore those objects.

Unignore objects

Unignore Objects refers to the process of reversing the action of ignoring certain objects that have been marked as unused, duplicate, or inconsistent. Ignoring objects is a way to temporarily leave unresolved issues with these objects when there are valid reasons. However, if you later decide to address these ignored objects, you can unignore them to bring them back into view and take action.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects** and choose an option.
3. Filter and search for ignored objects.
4. In the **Object** table, select the object you want to unignore. You can unignore one object at a time.
5. Click **Unignore** in the details pane.
6. Confirm your request. Now, when you filter your objects by issue, you should find the object that was previously ignored.

Part III

Dynamic Attributes Connector

Topics:

- About Dynamic Attributes Connector
- Configure the Dynamic Attributes Connector
- Dynamic Firewall
- Use Dynamic Objects in Access Control Policies
- Troubleshoot the Dynamic Attributes Connector

The following topics discuss how to configure and use the Dynamic Attributes Connector.

6 About Dynamic Attributes Connector

Topics:

- About the Dynamic Attributes Connector

About the Dynamic Attributes Connector

General information about the dynamic attributes connector.

The dynamic attributes connector enables your access control and DNS policy to adapt in real time to the changes in public and private cloud workloads and business-critical software-as-a-service (SaaS) applications. It simplifies policy management by keeping rules up to date without tedious manual updates and policy deployment. Customers require policy rules to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

Supported connectors

We currently support:

Table 17: List of supported connectors by dynamic attributes connector version and platform

CSDAC version	AWS	AWS security groups	AWS service tags	Azure	Azure Service Tags	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Tenable	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

More information about connectors:

- Cisco Cyber Vision

  See Create a Cisco cyber vision connector on page 211.

- Cisco Multicl. Defense

  See Create a Multicloud Defense connector on page 209.

- Generic text list of IP addresses you specify

  For more information, see Create a generic text connector on page 213.

- GitHub

  For more information, see Create a GitHub connector on page 217.

- Google Cloud

  For more information, see Setting Up Your Environment in the Google Cloud documentation.

  See Google cloud connector user permissions and imported data on page 218.

- Tenable vulnerabilities

  For more information, see Tenable connector on page 221

- Webex IP addresses

For more information, see Create a Webex connector on page 224.

- Zoom IP addresses

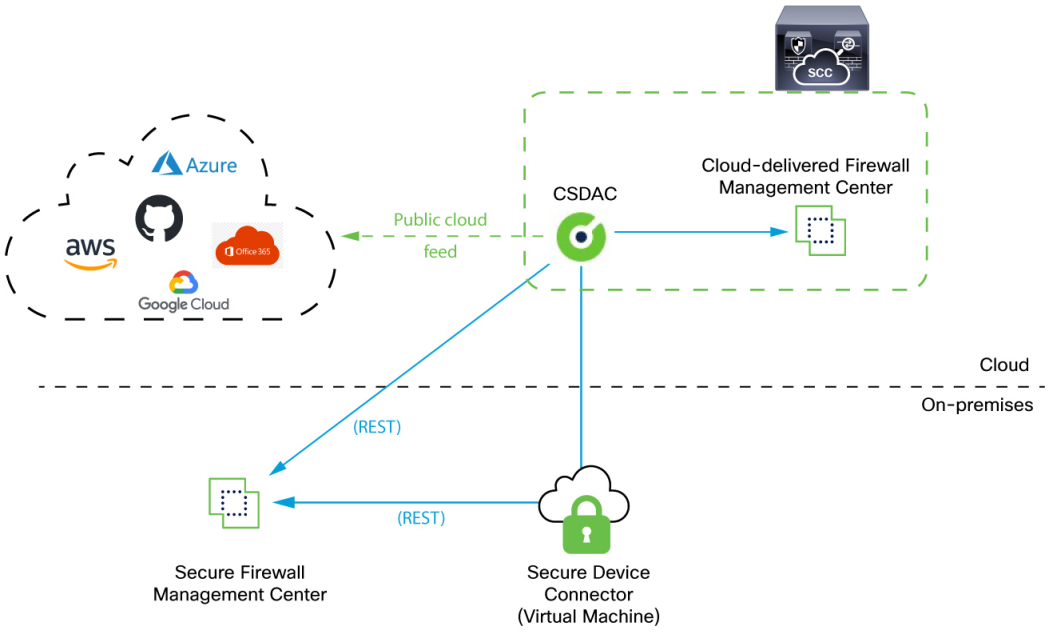
  For more information, see Create a Zoom connector on page 225.

How It Works

High-level overview of using the dynamic attributes connector in Security Cloud Control.

This topic discusses the architecture of the dynamic attributes connector.

The following figure shows how the system functions at a high level.



- The system supports certain public cloud providers.

  This topic discusses supported *connectors* (which are the connections to those providers).

- The dynamic attributes connector is provided with Security Cloud Control; it includes a Cloud-Delivered Firewall Management Center adapter and you can connect to an On-Prem Firewall Management Center using the Secure Device Connector.

  For more information about the Secure Device Connector, see Secure Device Connector (SDC).

- The *adapter* defined by the dynamic attributes connector receives those dynamic attributes filters as *dynamic objects* and enables you to use them in access control rules.

  You can create the following types of adapters:

  - *On-Prem Firewall Management Center* for an on-premises device.

    This type of device might be managed by Security Cloud Control or it might be a standalone.

  - *Cloud-Delivered Firewall Management Center* for devices managed by Security Cloud Control.

7 Configure the Dynamic Attributes Connector

Topics:

- Enable the dynamic attributes connector
- Dashboard
- Connectors
- Create an adapter
- Create dynamic attributes filters
- Disable the dynamic attributes connector

Enable the dynamic attributes connector

Enable the dynamic attributes connector for use in the Cloud-Delivered Firewall Management Center.

Enable the dynamic attributes connector to allow objects from cloud networking products to be used in Cloud-Delivered Firewall Management Center access control and DNS rules.

This task discusses how to enable the dynamic attributes connector in the Cloud-Delivered Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in Cloud-Delivered Firewall Management Center access control and DNS rules.

Procedure

1. Log in to the Cloud-Delivered Firewall Management Center if you have not done so already.
2. Click **Administration** > **Dynamic Attributes Connector**.
3. Slide to **Enabled**.
4. The system displays messages when the dynamic attributes connector is enabled.

   In the event of errors, try again. If errors persist, contact Cisco TAC.

   See Connectors on page 199.

Dashboard

Explains how you can use the dynamic atttributes connector dashboard to find information at a glance, configure components; or add or delete them.

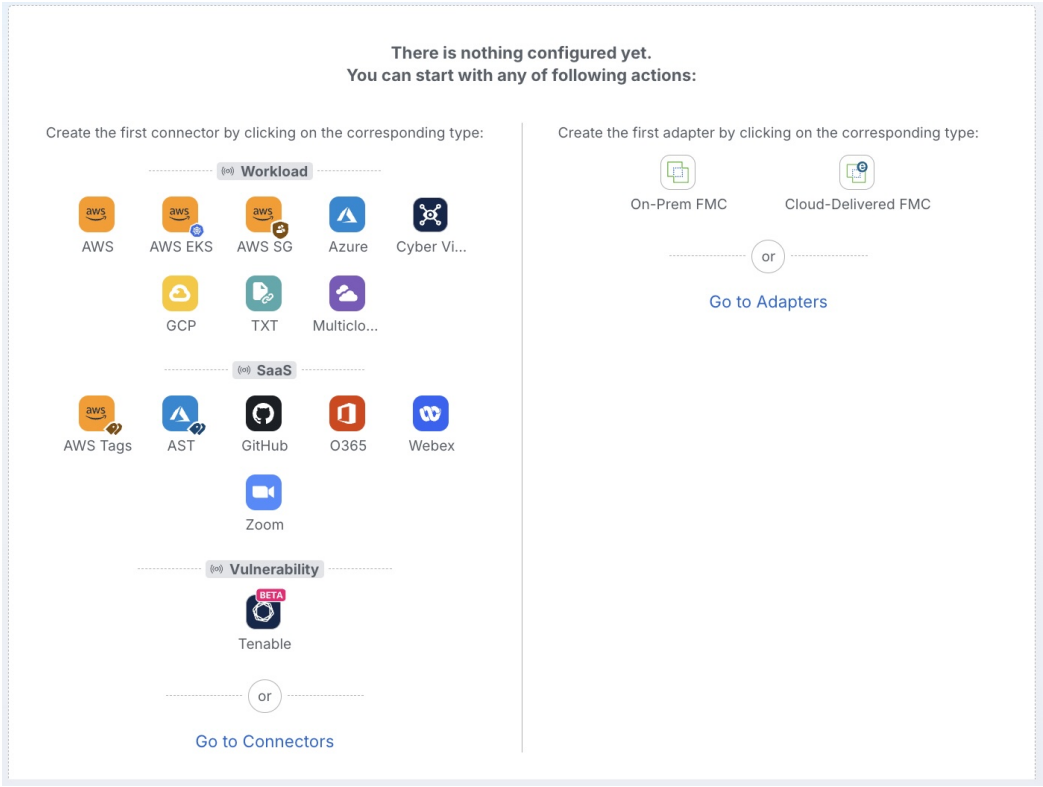
Dashboard capabilities include:

- Add, edit, and delete connectors,dynamic attributes filters, and adapters.
- See how connectors,dynamic attributes filters, and adapters are related to each other.
- View warnings and errors.

Dashboard access and functionality

To access the dynamic attributes connector dashboard, log in to Security Cloud Control and click **Administration** > **Dynamic Attributes Connector** at the top of the page.

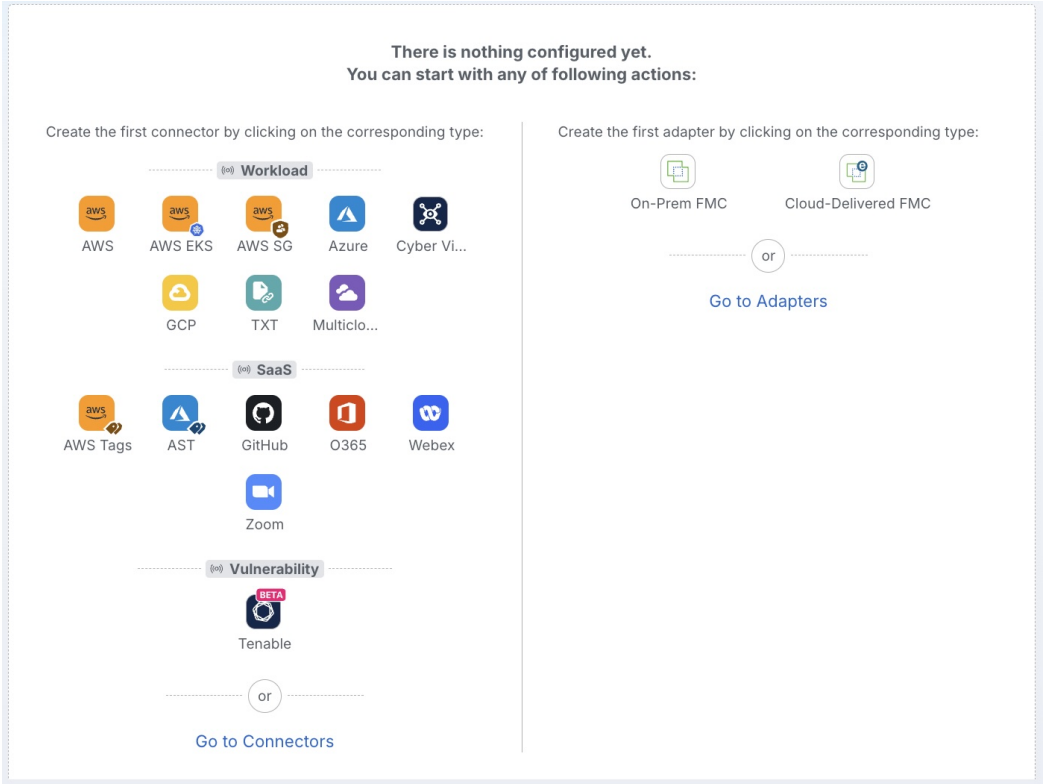
The dynamic attributes connector Dashboard page displays an example of an unconfigured system:



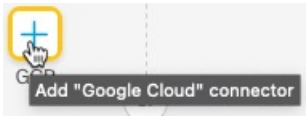
Dashboard of an unconfigured system

Provides a sample dynamic attributes connector dashboard for an unconfigured system.

This sample dynamic attributes connector Dashboard page shows how an unconfigured system appears initially.



The Dashboard initially displays all the types of connectors and adapters you can configure for your system. You can do any interaction:

- Hover the mouse pointer over a connector or adapter and click 

to create a new one.
- Click **Go to Connectors** to add, edit, or delete connectors (good for creating, editing, or deleting multiple connectors at the same time).

  For more information, see Connectors on page 199.
- Click **Go to Adapters** to add, edit, or delete adapters (good for creating, editing, or deleting multiple adapters at the same time).

  For more information, see Create an adapter on page 226.

Related Topics:

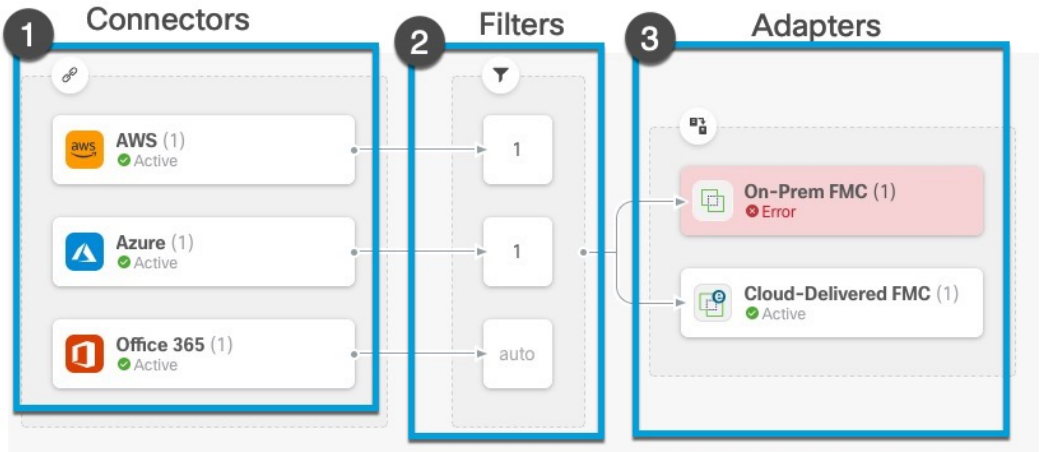
- Dashboard of a configured system on page 194
- Add, edit, or delete connectors on page 195
- Add, edit, or delete dynamic attributes filters on page 197
- Add, edit, or delete adapters on page 198

Dashboard of a configured system

Provides a sample dynamic attributes connector dashboard of a configured system.

Sample dynamic attributes connector Dashboard page of a configured system displays at-a-glance information about configured connectors, filters, and adapters.

Click an area in the figure to learn more about it or click one of the links that follow the figure.



rect 14, 42, 238, 272 Connectors on page 199
rect 259, 41, 377, 288 Create dynamic attributes filters on page 228
rect 398, 40, 632, 285 Create an adapter on page 226

The Dashboard shows the following (from left to right):

Connectors column	Filters column	Adapters column
List of connectors with a number indicating how many of each type are configured. Connectors collect dynamic attributes that could be sent to the configured adapter. Dynamic attributes filters specify what data is sent. Click to view more information about all configured connectors. You can also click the name of a connector to add, edit, or delete connectors; or to view detailed information about them. For more information, see Add, edit, or delete connectors on page 195.	List of dynamic attributes filters associated with each connector with a number indicating how many of each filter are associated with a connector. Click to view more information about all configured filters. You can also click the name of a filter to add, edit, or delete filters; or to view detailed information about them. For more information, see Add, edit, or delete dynamic attributes filters on page 197.	List of adapters. Adapters receive dynamic objects from configured connectors using configured dynamic attributes filters; these dynamic objects can be used in access control policies without the need to deploy them. Click to view more information about all configured adapters. You can also click the name of an adapter to add, edit, or delete adapters; or to view detailed information about them. For more information, see Create an adapter on page 226.

Note

Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

The Dashboard indicates whether or not an object is available. The Dashboard page is refreshed every 15 seconds but you can click **Refresh** ( ) at the top of the page at any time to refresh immediately. If issues persist, check your network connection.

Add, edit, or delete connectors

Configure the dynamic attributes connector dashboard to add, edit, or delete connectors.

The Dashboard enables you to manage connectors by viewing, adding, editing, or deleting them. You can also view error information for connectors and troubleshoot issues.

Use the dynamic attributes connector dashboard when you need to manage connectors for your network security infrastructure. The dashboard provides comprehensive options for connector management and troubleshooting.

Procedure

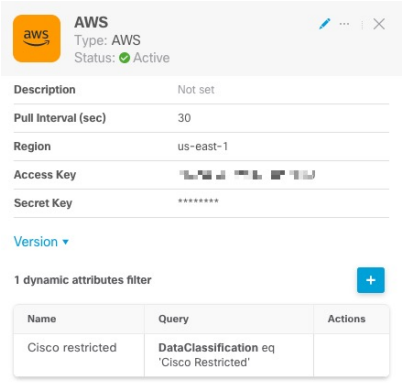
1. Access the connector dashboard and select your desired action.

   The Dashboard enables you to view or edit connectors. You can click the name of a connector to view all instances of that connector or you can click for the following additional options:

   - **Go to Connectors** to view all connectors at the same time; you can add, edit, and delete connectors from there.
   - **Add Connector** > ***type*** to add a connector of the indicated type.

2. Click any connector in the connectors column ( ) to display more information about it.

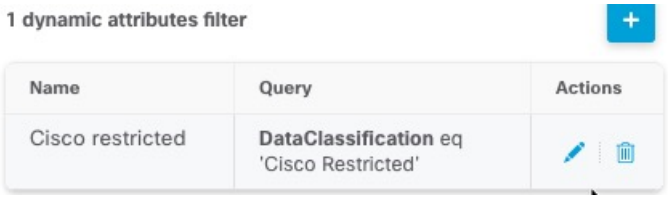
An example follows:



3. Choose from the following management options.
   - Click the Edit icon ( ) to edit this connector.
   - Click the More icon ( ) for additional options.
   - Click to close the panel.
   - Click **Version** to display the version of the . You can optionally copy the version to the clipboard if necessary for Cisco TAC.

4. Use the table at the bottom of the panel to add dynamic attributes filters or to edit or delete connectors.

   A sample follows:

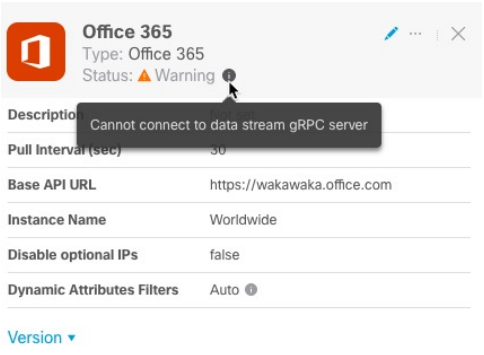


   Click the Add icon ( ) to add a dynamic attributes filter for this connector. For more information, see Create dynamic attributes filters on page 228.

   Hover the mouse pointer over the Actions column to either edit or delete the indicated connector.

5. To view error information for a connector, click the name of the connector that is displaying the error.
6. In the right pane, click **Information** ( ).

   An example follows.



7. To resolve this issue, edit the connector settings as discussed in Create an office 365 connector on page 220.
8. If you cannot resolve the issue, click **Version** and copy the version to a text file.
9. Get your Security Cloud Control tenant ID as discussed in Get your tenant ID on page 254.

   Provide all of this information to Cisco TAC.

Add, edit, or delete dynamic attributes filters

Provides general information about using the dynamic attributes connector dashboard to manage dynamic attributes filters.

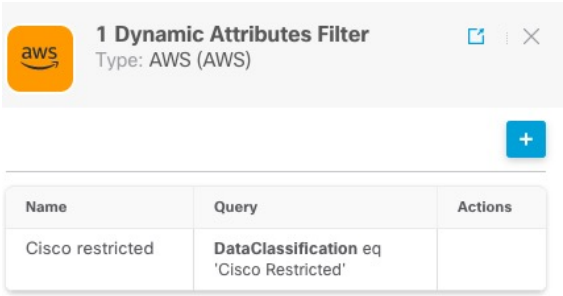
The dashboard enables you to add, edit, or delete dynamic attributes filters. You can click the name of a filter to view all instances of that filter or you can click  for additional options.

You can click the name of a filter to view all instances of that filter or you can click  for the following additional options:

- **Go to Dynamic Attributes Filters** to view all configured dynamic attributes filters. You can add, edit, or delete dynamic attributes filters from there.
- **Add Dynamic Attributes Filters** to add a filter.

For more information about adding dynamic attributes filters, see Create dynamic attributes filters on page 228.

Click any adapter in the filters column ( ) to display more information about it; an example follows:



Note

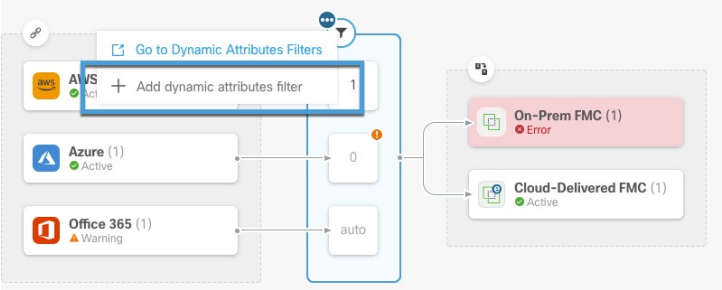
Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

You have these options:

- Click a filter instance to view summary information about dynamic attributes filters associated with a connector.
- Click the Add icon ( ) to add a new dynamic attributes filter.

  For more information, see Create dynamic attributes filters on page 228.
- Click in the filters column ( ) indicates the indicated connector has no associated dynamic attributes filters. Without associated filters, the connector can send nothing to Cloud-Delivered Firewall Management Center.

One way to resolve the issue is to click in the filters column and click **Add Dynamic Attributes Filter**. A sample follows.



- Click to add, edit, or delete filters.
- Click to close the panel.

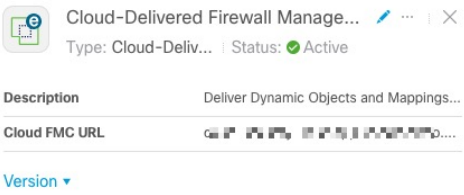
Add, edit, or delete adapters

How to use the dynamic attributes connector dashboard to add, edit, or delete adapters.

The Dashboard enables you to view or edit adapters. You can click the name of an adapter to view all instances of that adapter or you can click for the following additional options:

- **Go to Adapters** to view all adapters at the same time; you can add, edit, and delete adapters from there.
- **Add Adapter** > ***type*** to add an adapter of the indicated type.

Click any adapter in the adapters column ( ) to display more information about it; an example follows:



You have the following options:

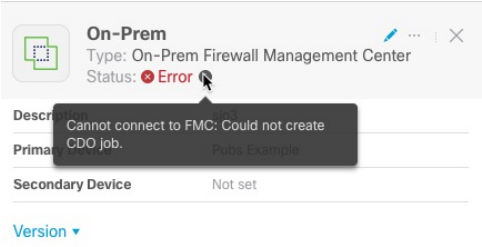
- Click the Edit icon ( ) to edit this connector.
- Click the More icon ( ) for additional options.
- Click **Version** to display the version of the dynamic attributes connector. You can optionally copy the version to the clipboard if necessary for Cisco TAC.
- Click to add, edit, or delete adapters. You can also view error details on the resulting page.
- Click to close the panel.

View error information

To view error information for an adapter:

1. On the Dashboard, click the name of the adapter that is displaying the error.
2. In the right pane, click **Information** ( ) .

   An example follows.



3. To resolve this error, make sure the On-Prem Firewall Management Center is onboarded correctly. For more information, see Onboard an FMC in *Managing FMC with Security Cloud Control* (link to topic).
4. If you cannot resolve the issue, click **Version** and copy the version to a text file.
5. Get your Security Cloud Control tenant ID as discussed in Get your tenant ID on page 254
6. Provide all of this information to Cisco TAC.

Related Topics

- Create an adapter on page 226

Connectors

Explains dynamic attributes connectors, their interface functionality, and the types of network information they retrieve from cloud services.

A connector is an interface with a cloud service. It retrieves network information from the cloud service to enable the network information to be used in policies on the Security Cloud Control. It supports both air gap mode and network download mode configurations.

Supported connectors

We support these connectors:

Table 18: List of supported connectors by dynamic attributes connector version and platform

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Cloud-delivered (Security Cloud Control)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Cloud-Delivered Firewall Management Center 7.4	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-Delivered Firewall Management Center 7.6	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-Delivered Firewall Management Center 7.7	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-Delivered Firewall Management Center 10.0.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

For more information about connectors, see the configuration guide.

Amazon Web Services connector user permissions and imported data

Explains the minimum user permissions required for the Amazon Web Services connector and which dynamic attributes are reported.

The dynamic attributes connector imports dynamic attributes from Amazon Web Services (AWS) to Security Cloud Control for use in policies.

Dynamic attributes imported

The connector imports these dynamic attributes from AWS:

- *Tags*, user-defined key-value pairs you can use to organize your AWS EC2 resources.

  For more information, see Tag your EC2 Resources in the AWS documentation

- *IP addresses* of virtual machines in AWS.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with a policy that permits `ec2:DescribeTags`, `ec2:DescribeVpcs`, and `ec2:DescribeInstances` to be able to import dynamic attributes.

Create an AWS user with minimal permissions for the dynamic attributes connector

Configure an AWS user with minimal permissions to work with the dynamic attributes connector.

This task creates a service account with minimum permissions to send dynamic attributes to Security Cloud Control.

For a list of the dynamic attributes that can be sent, refer to Amazon Web Services connector user permissions and imported data on page 200.

Before you begin

You must already have set up your Amazon Web Services (AWS) account. For more information about doing that, see this article in the AWS documentation.

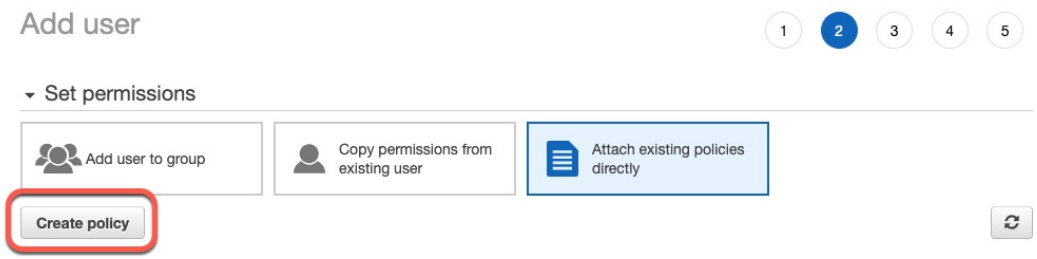
Follow these steps to create an AWS user with minimal permissions for the dynamic attributes connector:

Procedure

1. Log in to the AWS console as a user with the admin role.
2. From the Dashboard, click **Security, Identity & Compliance** > **IAM**.
3. Click **Access Management** > **Users**.
4. Click **Add Users**.
   a) In the **User Name** field, enter a name to identify the user.
   b) Click **Access Key - Programmatic Access**.
   c) At the Set permissions page, click **Next** without granting the user access to anything. You can grant user access later.
   d) Add tags to the user if desired.
   e) Click **Create User**.
   f) Click **Download .csv** to download the user's key to your computer.

   > **Note**
   >
   > This is the only opportunity you have to retrieve the user's key.

   g) Click **Close**.
5. At the Identity and Access Management (IAM) page in the left column, click **Access Management** > **Policies**.
6. Click **Create Policy**.
   a) On the Create Policy page, click **JSON**.



   b) Enter the following policy in the field:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

   c) Click **Next**.

7. Click **Review**.

   On the Review Policy page, enter the requested information and click **Create Policy**.

8. Attach your policy
   a) On the Policies page, enter all or part of the policy name in the search field and press Enter.
   b) Click the policy you just created.
   c) Click **Actions** > **Attach**.
   d) If necessary, enter all or part of the user name in the search field and press Enter.
   e) Click **Attach Policy**.

What to do next:

Create an AWS connector on page 202.

Create an AWS connector

Create a connector to send dynamic objects from AWS to the firewall.

Create a connector to send dynamic objects from AWS to the firewall for use in security policies.

This task discusses how to configure a connector that sends data from AWS to the Security Cloud Control for use in policies.

Before you begin

Create a user with at least the privileges discussed in Create an AWS user with minimal permissions for the dynamic attributes connector on page 200.

Follow these steps to create an AWS connector:

Procedure

---

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of these actions:
   - Add a new connector: click Add icon (), then click the name of the connector.
   - Edit a connector: click Edit icon ().
   - Delete a connector: click Delete icon ().
5. Enter the required information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS.
Region	(Required.) Enter your AWS region code.

Value	Description
Access Key	(Required.) Enter your access key.
Secret Key	(Required.) Enter your secret key.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.

The Status column displays **Ok**.

Amazon Web Services security groups connector—About user permissions

Lists the minimum permissions required to use the Amazon Web Services Security Groups connector.

The dynamic attributes connector imports dynamic attributes from AWS to Security Cloud Control for use in policies.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with a policy that permits `ec2:DescribeTags`, `ec2:DescribeVpcs`, and `ec2:DescribeInstances` to be able to import dynamic attributes.

Create an AWS security groups connector

Configure a connector to send dynamic objects from AWS security groups to the firewall.

This task creates a connector that sends AWS security groups data to the Security Cloud Control for use in policies.

This task discusses how to configure a connector that sends AWS security groups data to the Security Cloud Control for use in policies.

Before you begin

Complete these steps:

- Create AWS security groups as discussed in Work with security groups on the AWS documentation site.
- Create a user with at least the privileges discussed in Create an AWS user with minimal permissions for the dynamic attributes connector on page 200.

Follow these steps to create an AWS Security Groups connector:

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon (), then click the name of the connector.
   - Edit a connector: click Edit icon ().
   - Delete a connector: click Delete icon ().
5. Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Region	(Required.) Enter your AWS region code.
AWS Access Key	(Required.) Enter your access key.
AWS Secret Key	(Required.) Enter your secret key.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.

The Status column displays **Ok**.

What to do next

Create an AWS service tags connector

Configure a connector to send dynamic objects from AWS to the firewall.

Create a connector for Amazon Web Services (AWS) service tags to the Security Cloud Control for use in policies.

For more information, see resources like the following on the AWS documentation site:

- What are tags?
- AWS IP address ranges
- Tagging your AWS resources
- Guidance for Tagging on AWS
- AWS service points

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon (), then click the name of the connector.

- Edit a connector: click Edit icon (Edit).
- Delete a connector: click Delete icon (Delete).

5. Enter the necessary information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
URL	(Required.) Do not change the URL unless advised to do so.

a) Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.
b) Click **Save**.

The Status column displays **Ok**.

What to do next

Azure connector—About user permissions and imported data

Lists the minimum user permissions required for the Azure connector and also which dynamic attributes we import.

The dynamic attributes connector imports dynamic attributes from Azure to Security Cloud Control for use in policies.

Dynamic attributes imported

We import these dynamic attributes from Azure:

- *Tags*, key-value pairs associated with resources, resource groups, and subscriptions.

  For more information, see this page in the Microsoft documentation.
- *IP addresses* of virtual machines in Azure.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with the **Reader** permission to be able to import dynamic attributes.

Create an Azure user with minimal permissions for the dynamic attributes connector

Create an Azure user with minimal permissions to use with the dynamic attributes connector.

Create an Azure service account with minimal permissions to send dynamic attributes to Security Cloud Control.

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to Security Cloud Control. For a list of these attributes, see Azure connector–About user permissions and imported data on page 205.

Before you begin

You must already have a Microsoft Azure account. To set one up, see this page on the Azure documentation site.

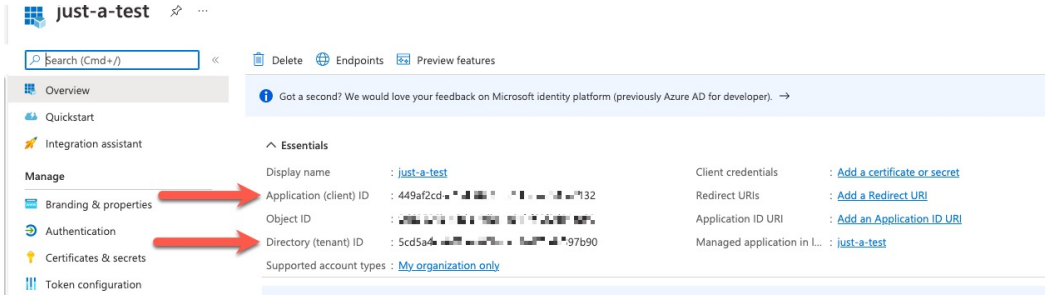
Follow these steps to create an Azure user with minimal permissions for the dynamic attributes connector:

Procedure

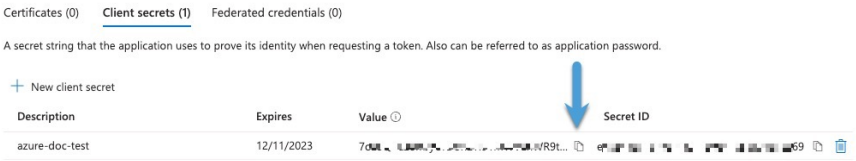
1. Log in to the Azure Portal as the owner of the subscription.
2. Click **Azure Active Directory**.

   Find the instance of Azure Active Directory for the application you want to set up.
3. Click **Add** > **App registration**.
   a) In the **Name** field, enter a name to identify this application.
   b) Enter other information on this page as required by your organization.
   c) Click **Register**.
4. On the next page, write down or copy the Client ID (also referred to as *application ID*) and the tenant ID (also referred to as the *directory ID*).

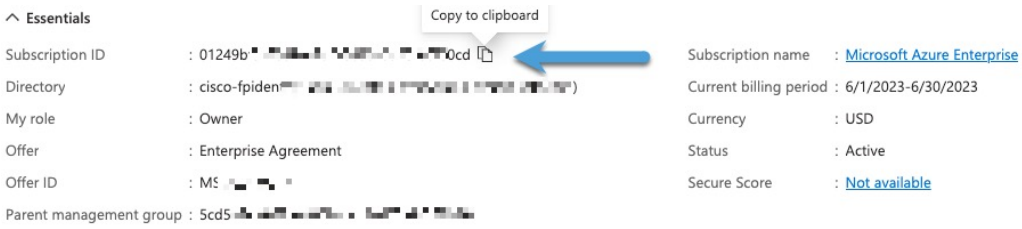
   Here is a sample:



5. Next to Client Credentials, click **Add a certificate or secret**.
6. Click **New Client Secret**.
   a) Enter the requested information and click **Add**.
   b) Copy the value of the **Value** field to the clipboard. This value, *and not the* ***Secret ID***, is the client secret.



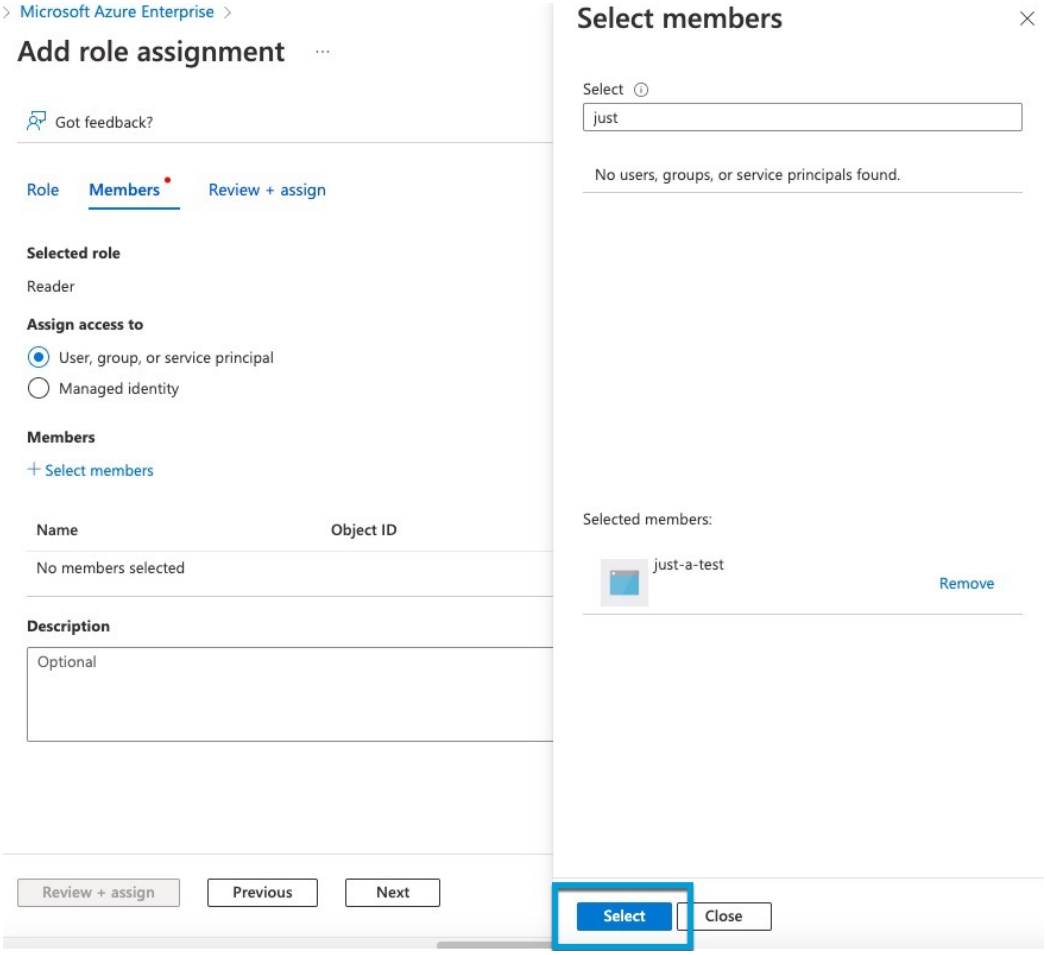
7. Go back to the main Azure Portal page and click **Subscriptions**.
   a) Click the name of your subscription.
   b) Copy the subscription ID to the clipboard.



8. Click **Access Control (IAM)**.
   a) Click **Add** > **Add role assignment**.
   b) Click **Reader** and click **Next**.

c) Click **Select Members**.

d) On the right side of the page, click the name of the app you registered and click **Select**.



e) Click **Review + Assign** and follow the prompts to complete the action.

Also see Create an Azure connector on page 207.

Create an Azure connector

Configure a connector to get dynamic objects from Azure.

Create a connector to send data from Azure to Security Cloud Control for use in policies.

This connector enables integration between Azure and your security management platform to retrieve dynamic object information for policy implementation.

Before you begin

Create an Azure user with at least the privileges discussed in Create an Azure user with minimal permissions for the dynamic attributes connector on page 205.

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.

3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon ( ), then click the name of the connector.
   - Edit a connector: click Edit icon (Edit).
   - Delete a connector: click Delete icon (Delete).
5. Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Subscription ID	(Required.) Enter your Azure subscription ID.
Tenant ID	(Required.) Enter your tenant ID.
Client ID	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

   a) Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.
   b) Click **Save**.
   The Status column displays **Ok**.

What to do next

Create an Azure service tags connector

Configure an Azure Service Tags connector to enable dynamic IP address mapping updates for security policies.

Create a connector for Azure service tags to enable use in policies with automatically updated IP addresses from Microsoft.

This topic discusses how to create a connector for Azure service tags to the Security Cloud Control for use in policies. The IP addresses associated with these tags are updated every week by Microsoft.

For more information, see Virtual network service tags on Microsoft TechNet.

Procedure

---

1. Log in to Security Cloud Control.

2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon ( ), then click the name of the connector.
   - Edit a connector: click Edit icon (Edit).
   - Delete a connector: click Delete icon (Delete).
5. Enter the required information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Subscription ID	(Required.) Enter your Azure subscription ID.
Tenant ID	(Required.) Enter your tenant ID.
Client ID	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

   a) Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.
   b) Click **Save**.

      The Status column displays **Ok**.

What to do next

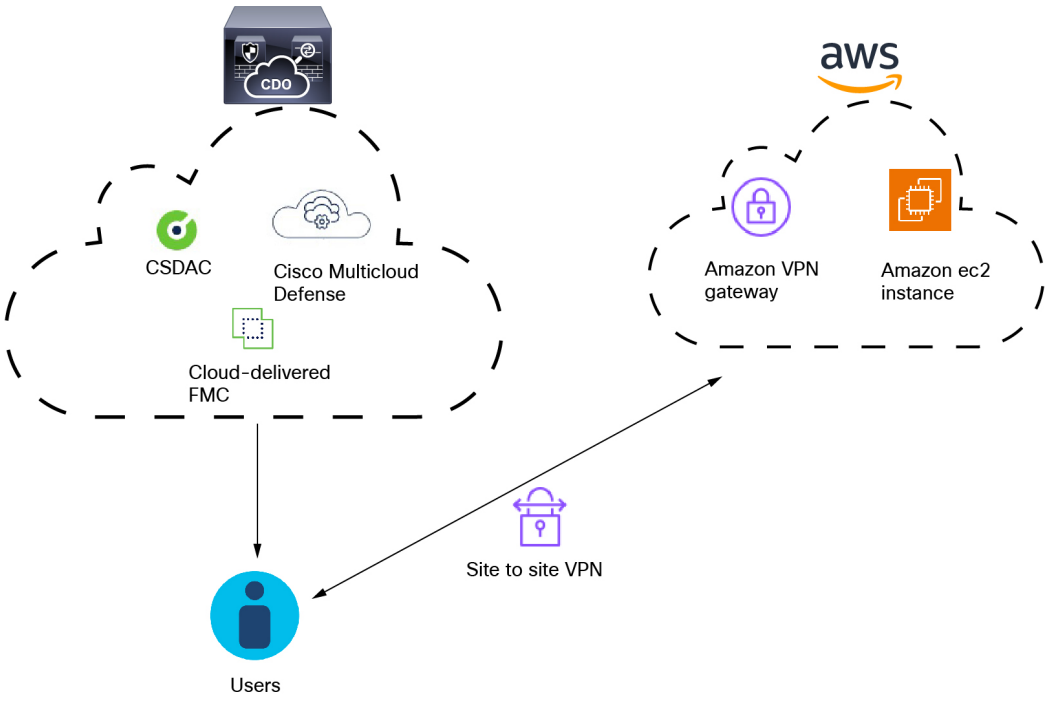
Create a Multicloud Defense connector

Create a connector to send data from Multicloud Defense to the firewall.

This topic discusses how to create a connector for Cisco Multicloud Defense. The connector sends dynamic application address objects to the configured Cloud-Delivered Firewall Management Center.

For more information, see the Address Objects chapter in the *Cisco Multicloud Defense User Guide* and address object API documentation.

The following figure shows how the Cisco Multicloud Defense connector works.



As the figure shows:

- Users logging in and out of AWS create activity monitored by Multicloud Defense.
- The dynamic attributes connector and Multicloud Defense, both included in Security Cloud Control, send IP addresses from that activity to the Cloud-Delivered Firewall Management Center.
- These IP addresses can then be used in access control rules by the Cloud-Delivered Firewall Management Center.

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon ( ), then click the name of the connector.
   - Edit a connector: click Edit icon (Edit).
   - Delete a connector: click Delete icon (Delete).
5. Enter a **Name** and optional **Description** to identify the connector.
6. Enter a **Pull Interval**. (Default 30 seconds.) Interval at which objects are retrieved from the Multicloud Defense Connector.
7. Click **Test** and make sure the test succeeds before you save the connector.
8. Click **Save**.
9. Make sure **Ok** is displayed in the Status column.

You must create a Cloud-Delivered Firewall Management Center adapter as discussed in Create an adapter on page 226.

Create a Cisco cyber vision connector

Configure a connector to send data from Cisco Cyber Vision to the firewall.

This task creates a connector to send data from Cisco Cyber Vision to the firewall, enabling dynamic attribute integration between these systems.

This task discusses how to send data from Cisco Cyber Vision to the Security Cloud Control.

Before you begin

Cisco Cyber Vision must be reachable from the machine on which the dynamic attributes connector is running. You must know its IP address, port, and API key.

To find the API key in the Cyber Vision management console, click **Admin** > **API** > **Token**, then click **Show** to display the token and  to copy the token to the clipboard.

Follow these steps to create a Cisco Cyber Vision connector:

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon (), then click the name of the connector.
   - Edit a connector: click Edit icon ().
   - Delete a connector: click Delete icon ().
5. Enter the required information.

Value	Description
Name	(Required) Enter a name to uniquely identify this connector.
Description	Optional description.
Cyber Vision Prefix	Enter an alphanumeric string to identify dynamic objects from this Cyber Vision's IP address when objects are sent to Security Cloud Control. If you have one Cyber Vision IP address, you can enter any value such as **1**.

Value	Description
Pull Interval	(Default 60 seconds) Interval at which data mappings are retrieved from Cyber Vision. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Host	(Required) Enter the Cyber Vision fully qualified host name or IP address.
Port	(Required) Enter the Cyber Vision listen port.
Version 4	(Required) Toggle this button to enable or disable Version 4. When you enable Version 4, the connector fetches hosts and vulnerabilities from the Cyber Vision platform. The Network Map API on the uses this data. When you disable Version 4, the connector fetches groups from the Cyber Vision platform and adds them as dynamic objects.
Token	(Required) Enter the API token.
Score Type	Choices are CVSS and CSRS. **CVSS**: Common vulnerability scoring system (CVSS) is an industry-standard system that retrieves values from the national vulnerability database to describe risk associated with vulnerabilities. CVSS scores power a vulnerability's severity and risk value. **CSRS**: The Cisco Security Risk Score (CSRS) CSRS evaluates vulnerabilities beyond technical severity, focusing on how attackers might exploit them. Scores range from 0 to 100 and are based on factors such as existing vulnerabilities, threat intelligence, and the effectiveness of security controls. This score helps prioritize critical vulnerabilities and allocate resources effectively.
Severity	Click the minimum vulnerability severity level for the dynamic attributes connector to send IP addresses to the Secure Firewall Management Center. (For example, if you click high, IP addresses of hosts with either high or severe vulnerabilities are sent.) Choices: • Critical • High • Medium • Low

Value	Description
Dynamic Object Name	Enter a name to identify the dynamic object created by this connector.
Certificate	You have these options: • Paste the certificate authority (CA) chain as discussed in Manually get a certificate authority (CA) chain on page 214. • Click **Get Certificate** > **Fetch** to automatically fetch the certificate. Ensure that you have specified a valid host and IP address that exactly matches the server certificate. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously. The configured hostname or IP address must be valid for the server certificate. Upload the CA certificate chain used to validate that certificate

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.

Status column displays **Ok**.

Create an adapter on page 226

Create a generic text connector

Create a connector to send IP addresses from a text file to the firewall.

Use this task to create a connector that retrieves IP addresses from text files and sends them to the firewall for use in access control rules.

This task discusses how to create an ad hoc list of IP addresses you maintain manually and retrieve at an interval you select (30 seconds by default). You can update the list of addresses anytime you want.

For example, you might have a list of IP addresses for an "allow list" in access control rules and another list of IP addresses for a "block list" in access control rules.

Before you begin

Create text files with IP addresses and put it on a web server that is accessible from the Security Cloud Control. IP addresses can include CIDR notation. The text file must have only one IP address per line.

You can specify up to 10,000 IP addresses per text file.

Follow these steps to create a generic text connector:

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:

- Add a new connector: click Add icon ( ), then click the name of the connector.
- Edit a connector: click Edit icon (Edit).
- Delete a connector: click Delete icon (Delete).

5. Enter the following information:

Item	Description
Name	Enter a name to identify the connector.
Description	(Optional.) Enter a description
Pull Interval	Change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from the text file. The default is 30 seconds. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
URLs	Enter a URL from which to retrieve IP addresses.
Add another URL	(Optional.) Click the link to add more URLs to an existing list.
Certificate	(Optional.) If a certificate chain is required for a secure connection to the web server, you have these options: • Click **Get Certificate** > **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually get a certificate authority (CA) chain on page 214. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.
c) Status column displays **Ok**

What to do next

Manually get a certificate authority (CA) chain

Retrieves a certificate authority chain manually when automatic fetching fails to support secure connections to dynamic attribute connector components.

If the certificate authority chain is not fetched automatically, use one of these browser-specific procedures to get a certificate chain to securely connect to vCenter or , or Cloud-Delivered Firewall Management Center .

The *certificate chain* is the root certificate and all subordinate certificates.

Procedure

1. Get a Certificate Chain–Mac (Chrome and Firefox)
   a. Open a Terminal window.
   b. Enter this command:

      ```
      security verify-cert -P
      url[:port]
      ```

      where *url* is the URL (including scheme) to vCenter or , or Cloud-Delivered Firewall Management Center . For example:

      ```
      security verify-cert -P https://myvcenter.example.com
      ```

      If you access vCenter or , or Cloud-Delivered Firewall Management Center using NAT or PAT, you can add a port as follows:

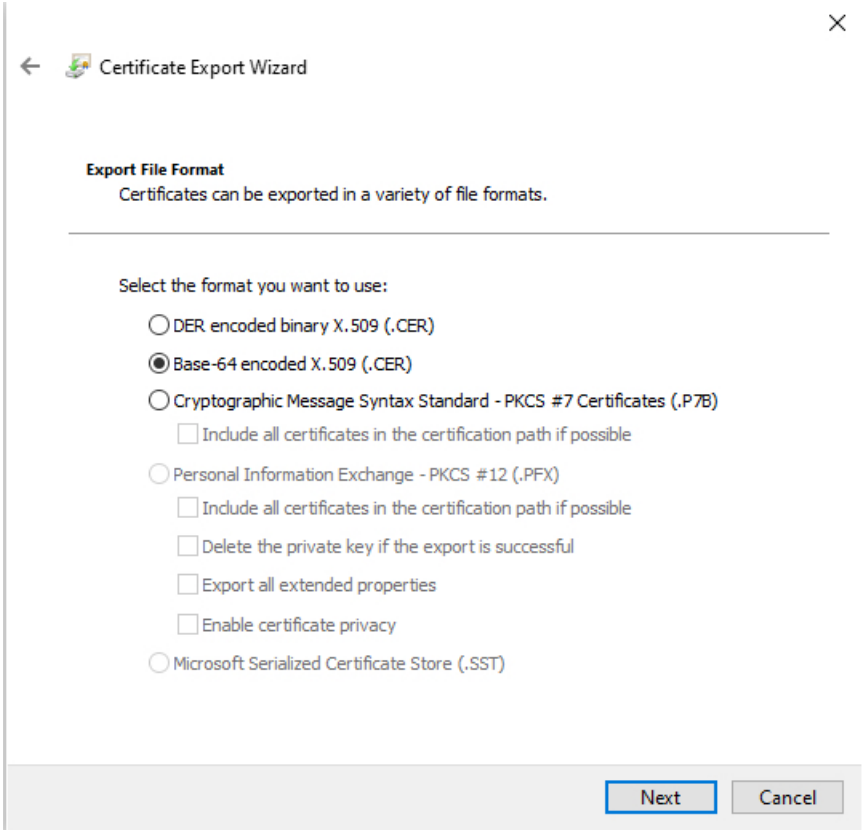
      ```
      security verify-cert -P https://myvcenter.example.com:12345
      ```

   c. Save the entire certificate chain to a plaintext file.
      - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
      - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets themselves.

   d. Repeat these tasks for vCenter , or Cloud-Delivered Firewall Management Center .

2. Get a Certificate Chain–Windows Chrome
   a. Log in to vCenter or , or Cloud-Delivered Firewall Management Center using Chrome.
   b. In the browser address bar, click the lock to the left of the host name.
   c. Click **Certificate**.
   d. Click the **Certification Path** tab.
   e. Click the top (that is, first) certificate in the chain.
   f. Click **View Certificate**.
   g. Click the **Details** tab.
   h. Click **Copy to File**.
   i. Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain.

      When you're prompted to choose an export file format, click **Base 64-Encoded X.509 (.CER)**.



Follow the prompts to complete the export.

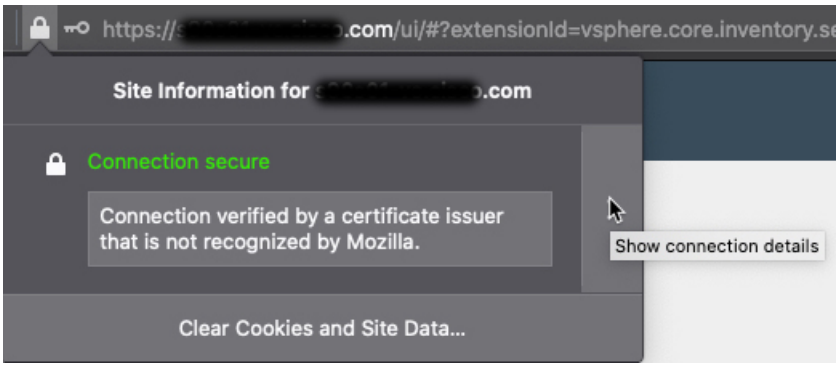
Open the certificate in a text editor.

Repeat the process for all certificates in the chain.

You must paste each certificate in the text editor in order, first to last.

Repeat these tasks for vCenter or , or Cloud-Delivered Firewall Management Center .

3. Get a Certificate Chain–Windows Firefox
   a. Log in to vCenter or , or Cloud-Delivered Firewall Management Center using Firefox.
   b. Click the lock to the left of the host name.
   c. Click the right arrow (**Show connection details**).

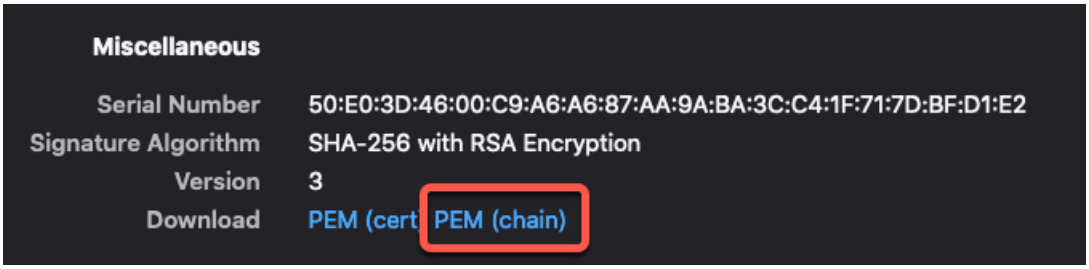


   d. Click **More Information**.
   e. Click **View Certificate**.

f. If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA.

g. Scroll to the Miscellaneous section.

h. Click **PEM (chain)** in the Download row.



i. Save the file.

Repeat these tasks for vCenter or , or Cloud-Delivered Firewall Management Center .

Create a GitHub connector

Create a connector to send dynamic objects from GitHub to the firewall.

Create a GitHub connector that sends data to the Security Cloud Control for use in policies. The IP addresses associated with these tags are maintained by GitHub.

For more information, see About GitHub's IP addresses.

Note

Do not change the URL because doing so will fail to retrieve any IP addresses.

Before you begin

You do not have to create a dynamic attributes filters.

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon ( ), then click the name of the connector.
   - Edit a connector: click Edit icon (Edit).
   - Delete a connector: click Delete icon (Delete).
5. Enter a **Name** and an optional description.
   a) (Optional) In the **Pull Interval** field, change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from GitHub. The default is 21,600 seconds (6 hours).

b) Click **Test** and make sure the test succeeds before you save the connector.
c) Click **Save**.

The Status column displays **Ok**.

What to do next

Google cloud connector user permissions and imported data

Explains the minimum required user permissions required to use the Google Cloud connector as well as what Google Cloud attributes are used as dynamic objects.

A Google Cloud connector imports dynamic attributes from Google Cloud to Security Cloud Control for use in policies.

Dynamic attributes imported

The connector imports these dynamic attributes from Google Cloud:

- *Labels*: Key-value pairs assigned to virtual machine instances. Use the labels to organize your Google Cloud resources. For more information, see Creating and Managing Labels in the Google Cloud documentation.
- *Network tags*: Text values assigned to virtual machine instances that help identify groups of instances. For more information, see Creating and Managing Tags in the Google Cloud documentation.
- *IP addresses*: IP addresses associated with virtual machine instances in your Google Cloud project and region.

The dynamic attributes connector requires a user at minimum with the **Basic** > **Viewer** permission to be able to import dynamic attributes.

Create a Google Cloud user with minimal permissions for the dynamic attributes connector

Create a user with minimal permissions to use with the dynamic attributes connector.

Create a service account with minimum permissions to send dynamic attributes to Security Cloud Control.

This task sets up a service account that provides the minimum permissions necessary for the dynamic attributes connector. For a list of these attributes, see Google cloud connector user permissions and imported data on page 218.

Before you begin

You must already have set up your Google Cloud account. For more information about doing that, see Setting Up Your Environment in the Google Cloud documentation.

Procedure

---

1. Log in to your Google Cloud account as a user with the owner role.
2. Click **IAM & Admin** > **Service Accounts** > **Create Service Account**.
3. Enter the following information:
   - **Service account name**: A name to identify this account; for example, `CSDAC`.
   - **Service account ID**: Should be populated with a unique value after you enter the service account name.
   - **Service account description**: Enter an optional description.

   For more information about service accounts, see Understanding Service Accounts in the Google Cloud documentation.

   Click **Create and Continue**.

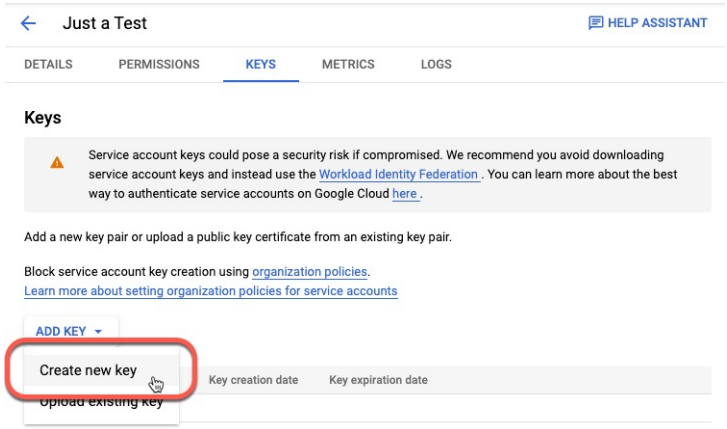
4. Follow the prompts on your screen until the Grant users access to this service account section is displayed.

   Grant the user the **Basic** > **Viewer** role.

   Click **Done**.

   A list of service accounts is displayed.

5. Click **More** (⋮) at the end of the row of the service account you created.
6. Click **Manage Keys**.
7. Click **Add Key** > **Create New Key**.



8. Click **JSON**.
9. Click **Create**.

   The JSON key is downloaded to your computer.

   Keep the key handy when you configure the GCP connector.

   See Create a google cloud connector on page 219.

Create a google cloud connector

Configure a connector to send data from Google Cloud to the firewall.

Create a Google Cloud connector to enable data transmission from your Google Cloud environment to the firewall for dynamic security attribute monitoring and management.

The Google Cloud connector allows the firewall to receive real-time data from your Google Cloud infrastructure, enabling dynamic security policies based on cloud resource attributes.

Before you begin

Have your Google Cloud JSON-formatted service account data ready; it's required to set up the connector.

Follow these steps to create a Google Cloud connector:

Procedure

---

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:

- Add a new connector: click Add icon ( ), then click the name of the connector.
- Edit a connector: click Edit icon (Edit).
- Delete a connector: click Delete icon (Delete).

5. Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
GCP region	(Required.) Enter the GCP region in which your Google Cloud is located. For more information, see Regions and Zones in the Google Cloud documentation.
Service account	Paste the JSON code for your Google Cloud service account.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.

The Status column displays **Ok**.

What to do next

Create an office 365 connector

Configure a connector to send dynamic objects from Office 365 to the dynamic attributes connector.

Create a connector for Office 365 tags to send data to the Security Cloud Control for use in policies.

The IP addresses associated with these tags are updated every week by Microsoft. You do not have to create a dynamic attributes filter to use the data.

For more information, refer to Office 365 URLs and IP address ranges on docs.microsoft.com.

Procedure

1. Log in to Security Cloud Control.

   Click **Firewall**.

2. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.

3. Do any of the following:
   - Add a new connector: click Add icon ( ), then click the name of the connector.
   - Edit a connector: click Edit icon (Edit).
   - Delete a connector: click Delete icon (Delete).
4. Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Base API URL	(Required.) Enter the URL from which to retrieve Office 365 information, if it's different from the default. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Instance name	(Required.) From the list, click an instance name. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Disable optional IPs	(Required.) Enter **true** or **false**.

   Click **Test** and make sure the test succeeds before you save the connector.
5. Click **Save**.

   The Status column displays **Ok**.

   Create an adapter on page 226

Tenable connector

These topics provide information about creating and using the Tenable connector for vulnerability management.

About the Tenable connector

Describes how to use the Tenable connector to manage vulnerabilities.

Tenable Vulnerability Management is a platform that helps organizations understand, report, and manage known vulnerabilities. When used with the Cloud-Delivered Firewall Management Center, the Tenable connector:

- Creates a dynamic object with a list of IP addresses known to have Common Vulnerability Exposures (CVEs).

- Populates those IP addresses and associated vulnerabilities to the Cloud-Delivered Firewall Management Center network map as host entries.

  Network map entries provide the basis for intrusion policy recommendations.

The dynamic object created by this connector can be used in access control rules, or anywhere dynamic objects are supported. For example, you can use the dynamic object to block vulnerable devices from accessing highly sensitive resources.

Supported products

We support Tenable Vulnerability Management only. We *do not* support Tenable Security Center.

Get the Tenable API key and secret

Get the API key and secret required to configure a Tenable connector.

To configure the Tenable connector, you must create an API key and secret as described in this topic.

> **Note**
>
> API keys inherit the permissions of the user account that generates them. Create the API key and secret using an account with full visibility to all hosts and vulnerabilities. For more information, see Permissions.

Procedure

1. Log in to Tenable as an administrator.
2. Click your profile image in the top right of the page.
3. Click **My Profile** > **API Keys**.
4. Click **Generate**.
   You are required to confirm the action.
5. Under Custom API keys, click (Copy to clipboard) to copy both the access key and secret key to the clipboard.
6. Save these values for later use.

What to do next

Create a Tenable connector

Create a connector to send vulnerability data to the firewall.

This task explains how to configure the Tenable connector in Cisco Security Cloud. After you configure the connector, you must also configure an adapter to receive the dynamic object.

Before you begin

- Configure Tenable Vulnerability Management : Consult Tenable documentation.
- Get required information: Get the Tenable API key and secret on page 222.

We support Tenable Vulnerability Management only. We *do not* support Tenable Security Center.

Required User Role:

- Super Admin

Procedure

1. Log in to Cisco Security Cloud.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon ( ), then click the name of the connector.
   - Edit a connector: click Edit icon (Edit).
   - Delete a connector: click Delete icon (Delete).
5. Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 21600 seconds or six hours.) Interval at which IP mappings are retrieved from Tenable. We recommend a minimum value of 3600 seconds (one hour) to avoid issues with Tenable rate limiting.
Integration Key	Enter the API key you got in Get the Tenable API key and secret on page 222.
Secret Key	Enter the secret key obtained in Get the Tenable API key and secret on page 222.
Dynamic Object Name	Enter a name to identify the dynamic object created by this connector.
Severity Score	Click the minimum vulnerability severity level for the dynamic attributes connector to send IP addresses to the Cloud-Delivered Firewall Management Center. (For example, if you click **high**, IP addresses of hosts with either high or severe vulnerabilities are sent.) Choices: • **Critical** • **High** • **Medium** • **Low**

Value	Description

Severity System	Choices:
	• **VPR**: (Vulnerability priority rating.) Proprietary Tenable vulnerability rating that dynamically scores threats.
	VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit:
	  • VPR **critical** is 9.0 and greater
	  • VPR **high** is 7.0 and greater
	  • VPR **medium** is 4.0 and greater
	  • VPR **low** is 0.1 and greater
	• **CVSSv3**: (Common vulnerability scoring system version 3.) Industry-standard system that retrieves values from the national vulnerability database to describe risk associated with vulnerabilities. CVSS scores power a vulnerability's severity and risk value.
	For more information, see CVSS vs. VPR.

6. Click **Test**. Save the connector only after the test succeeds.
7. Click **Save**.
8. Make sure **Ok** is displayed in the Status column.

See Create an adapter on page 226.

About Tenable dynamic objects in IDS, IPS, and access control policies

Overview of Tenable dynamic objects.

You can use IPS, IDS, and access control policies and rules to monitor or block traffic to and from servers with vulnerabilities identified by the Tenable connector:

1. To monitor traffic and inform you about vulnerabilities *without* blocking the traffic, create an intrusion detection system (IDS) policy with recommendations.
2. To monitor traffic, inform you about vulnerabilities, and block matching traffic, create an intrusion prevention system (IPS) policy with recommendations.
3. Create a new access control policy or add rules to an existing policy. Associate your IDS or IPS policy with an access control rule.

For information about intrusion policies for access control, refer to the Snort 3 configuration guide.

Create a Webex connector

Configure a Webex connector to send its IP addresses to the firewall.

This task creates a Webex connector that sends IP addresses to the management system for use in policies. The IP addresses associated with these tags are maintained by Webex.

This section discusses how to create a Webex connector that sends data to the Security Cloud Control for use in policies. The IP addresses associated with these tags are maintained by Webex. You do not have to create a dynamic attributes filters.

For more information, see Port Reference for Webex Calling.

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon ( ), then click the name of the connector.
   - Edit a connector: click Edit icon (Edit).
   - Delete a connector: click Delete icon (Delete).
5. Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Webex. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Provider Reserved IPs	(Required.) (Required.) Slide to enabled to retrieve any reserved IP addresses.

   a) Click **Test** and make sure the test succeeds before you save the connector.
   b) Click **Save**.
   c) The Status column displays **Ok**.

What to do next

Create a Zoom connector

Configure a Zoom connector to send its IP addresses to the firewall.

Create a Zoom connector that sends data to the Security Cloud Control for use in policies.

The IP addresses associated with these tags are maintained by Zoom. You do not have to create a dynamic attributes filters.

For more information, see Zoom network firewall or proxy server settings.

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new connector: click Add icon ( ), then click the name of the connector.
   - Edit a connector: click Edit icon (Edit).
   - Delete a connector: click Delete icon (Delete).
5. Enter this information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Zoom. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Provider Reserved IPs	(Required.) Slide to enabled to retrieve any reserved IP addresses.

   a) Click **Test** and make sure the test succeeds before you save the connector.
   b) Click **Save**.

   The Status column displays **Ok**.

What to do next

Create an adapter

General information about creating an adapter to send dynamic objects to either the Cloud-Delivered Firewall Management Center or the On-Prem Firewall Management Center.

An *adapter* is a secure connection to Cloud-Delivered Firewall Management Center or an On-Prem Firewall Management Center to which you push network information from cloud objects for use in access control policies.

You can create the following adapters:

- *On-Prem Firewall Management Center* for an on-premises Cloud-Delivered Firewall Management Center.
- *Cloud-Delivered Firewall Management Center* for devices managed by Cisco Security Cloud.

Note

You must have a **Super Admin** user role to create the first adapter. To view or modify existing adapters, you must have an Admin or Super Admin user role.

How to create an On-Premises Firewall Management Center adapter

This topic discusses how to create an adapter to push dynamic objects to On-Premises Firewall Management Center.

This topic discusses how to create an adapter to push dynamic objects from the dynamic attributes connector to Cisco Security Cloud.

Before you begin

Onboard the firewall manager to Cisco Security Cloud as discussed in *Onboard a Management Center* in the *Managing Security and Network Devices with Security Cloud Control* online help.

Note

Currently, you can use the Tenable connector with the On-Premises Firewall Management Center only to create the dynamic object. The On-Premises Firewall Management Center does *not* receive network map entries from the Tenable connector, so you cannot use it with intrusion policy recommendations.

Required User Role: Super Admin

Procedure

1. Log in to Cisco Security Cloud as a user with the Super Admin role.
2. On-Premises Firewall Management Center
3. Click **Administration** > **Dynamic Attributes Connector** > **Adapters**.
4. To add an adapter, click Add icon ( ) **>** On-Premises Firewall Management Center.
5. To edit or delete an adapter, click Edit icon (Edit), or Delete icon (Delete).
6. Add or edit this information.

Value	Description
Name	(Required.) Enter a unique name to identify this adapter.
Description	(Optional) Enter a description of the adapter.
Primary Device	Click the IP address of a management center associated with your tenant.
Secondary Device	(Optional) If you have a secondary On-Premises Firewall Management Center, click its name.

7. Click **OK**.

How to create a Cloud-Delivered Firewall Management Center adapter

Create an adapter to send dynamic objects to the Cloud-Delivered Firewall Management Center.

This topic discusses how to create an adapter to push dynamic objects from the dynamic attributes connector to Cisco Security Cloud.

Before you begin

Required User Role:

- Super Admin

Procedure

1. Log in to Cisco Security Cloud as a user with the Super Admin role.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Adapters**.
4. To add an adapter, click Add icon (+) **>** Cloud-Delivered Firewall Management Center.
5. To edit or delete an adapter, click Edit icon (Edit), or Delete icon (Delete).
6. Edit the following information.

Value	Description
Name	(Required.) Enter a unique name to identify this adapter.
Description	Optional description of the adapter.
Cloud FMC URL	From the list, click the URL for your Cloud-Delivered Firewall Management Center.

7. Click **Test** and make sure the test succeeds before you save the adapter.
8. Click **Save**.

Create dynamic attributes filters

Configure dynamic attributes filters using the Dynamic Attributes Connector.

Create dynamic attributes filters to expose them as dynamic objects in Security Cloud Control for use in access control policies.

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Security Cloud Control as dynamic objects that can be used in access control policies. For example, restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

Note

You cannot create dynamic attributes filters for Azure Service Tags, Cisco Multicloud Defense, Generic Text, GitHub, Outlook 365, Tenable, Webex, and Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control rules, see Create access control rules or DNS rules using dynamic atttributes filters.

Procedure

1. Log in to Security Cloud Control.
   a) Click **Firewall**.
   b) Click **Administration** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.
2. Do any of the following:
   - Add a new filter: click **Add** ( ).
   - Edit or delete a filter: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.
3. Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a policy and in the Security Cloud Control Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	Click Add .

4. To add or edit a query, enter the following information.

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: • **Equals** to exactly match the key to the value. • **Contains** to match the key to the value if any part of the value matches.
Values	Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

5. Click **Show Preview** to display a list of networks or IP addresses returned by your query.
6. When you're finished, click **Save**.

7. (Optional.) Verify the dynamic object in the Security Cloud Control.
   a) Log in to the Security Cloud Control.
   b) Click **Policies** > **Firewall Threat Defense**.
   c) Click **Objects** > **External Attributes** > **Dynamic Object**.

      The dynamic attribute query you created should be displayed as a dynamic object.

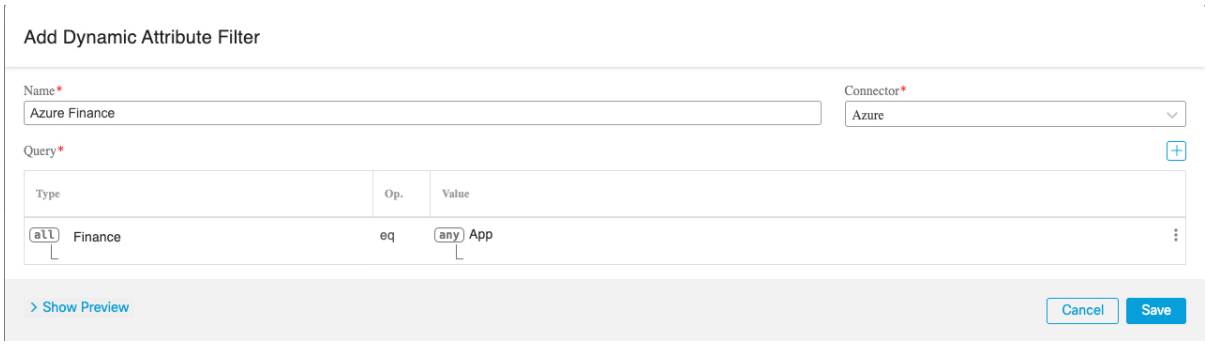
Dynamic attribute filter examples

Provides dynamic attribute filter examples.

This topic provides some examples of setting up dynamic attribute filters.

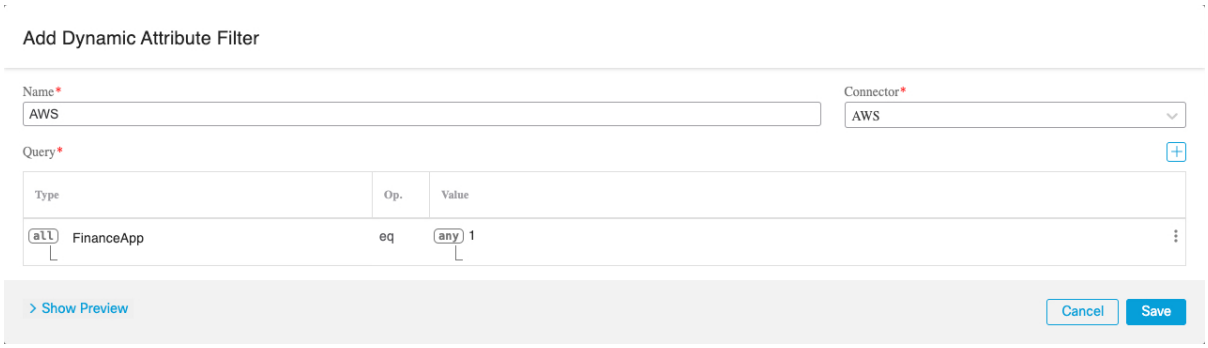
Example: azure

This example shows one criterion: a server tagged as a Finance app.



Example: AWS

This example shows one criterion: a FinanceApp with a value of 1.



Disable the dynamic attributes connector

Configure the dynamic attributes connector to disable dynamic object collection from cloud sources in the Cloud-Delivered Firewall Management Center.

Disable the Dynamic Attributes Connector when you no longer wish to collect dynamic objects from cloud sources.

If you no longer wish to collect dynamic objects from cloud sources, you can disable the Dynamic Attributes Connector in the Cloud-Delivered Firewall Management Center.

Procedure

1. Log in to the Cloud-Delivered Firewall Management Center if you have not done so already.
2. Click **Administration** > **Dynamic Attributes Connector**.
3. Slide to **Disabled**.

8 Dynamic Firewall

Topics:

- Dynamic Firewall
- How to configure the dynamic firewall
- Create dynamic attributes filters

Describes the integration of user identity data with user trust data to enhance detection of identity-based exploits in your network.

A dynamic firewall integrates user identity data with user trust data provided by Identity Intelligence to enhance your ability to detect identity-based exploits in your network.

Identity data integration

The dynamic firewall integrates user identity data from Microsoft AD and ISE with user trust data.

Dynamic Firewall

Describes the dynamic firewall, which integrates identity sources with Identity Intelligence to provide user and device trust information in addition to identity.

A dynamic firewall integrates identity sources with Identity Intelligence to provide user and device trust information.

Enhanced identity information

Previously, the Security Cloud Control collected information about users exclusively from the configured identity sources, such as Microsoft Active Directory, the passive identity agent, Cisco Identity Services Engine (Cisco ISE), and so on. This information generally included user name, group, and IP address.

The dynamic firewall enables you to pair user identity with intelligence and use that information in reporting and access control policies.

To use the dynamic firewall, you must:

- Have an Identity Intelligence tenant

  See Duo Identity Security with Cisco Identity Intelligence.

- Set up an identity source:
  - Cisco Identity Services Engine (Cisco ISE)
  - pxGrid Cloud

    pxGrid Cloud combines identity and posture in the same feed

    More information: What is pxGrid?

  In addition to providing authentication information, Cisco ISE and pxGrid Cloud can provide the following:

  - SGT Exchange Protocol (SXP) over TCP binding and directory session information if desired. For more information, see the *Cisco Identity Services Engine Administrator Guide*
  - Posture and mobile device management compliance. For more information, see Compliance.

- Set up an identity realm:
  - Create an LDAP Realm or an Active Directory Realm and Realm Directory
  - Create an Azure AD (SAML) Realm for Passive Authentication

The *identity source* provides authentication information (login, logout) as well as posture. The identity source can also provide SXP binding and session directory information if desired.

The *identity realm* provides user, group, and IP address information.

How to configure the dynamic firewall

Workflow of high-level tasks to configure the dynamic firewall.

This topic helps you understand the concepts and options to configure the dynamic firewall discussed in Dynamic Firewall on page 234.

Summary

The dynamic firewall integrates an identity source (such as Cisco ISE) with Cisco Identity Intelligence, which provides user trust information to the Cloud-Delivered Firewall Management Center.

1. Configure Cisco Identity Intelligence to collect user trust information.
2. Configure a supported Cloud-Delivered Firewall Management Center identity source.
3. Configure a supported identity realm.
4. Enable the dynamic attributes connector.
5. Configure the dynamic firewall.

Workflow

The following procedure provides a high-level overview of how to configure the dynamic firewall.

1. As a Duo user with the Owner role, provision a Cisco Identity Intelligence tenant.

   You can provision a tenant from Duo Advantage as discussed in *Provision Your Cisco Identity Intelligence Tenant*.

2. In Cisco Identity Intelligence, create an API integration and use the information to set up the dynamic firewall.

   We use Cisco Identity Intelligence to find user and device risk information in your network.

   For more information about Cisco Identity Intelligence, see How-to Guides.

   For more information about this task, see Get required information for Identity Intelligence on page 236.

3. (Microsoft Azure AD realm only.) In Identity Intelligence, create a Microsoft Entra ID integration.

   For more information, see Microsoft Entra ID (Azure AD) Data Integration.

4. Create an identity source. (If you already have an identity source, continue with the next step.)

   You can do this in any of the following ways:

   - The Configure Dynamic Firewall dialog box displays **Configure** links to start setting up your identity source.
   - Click **Integrations** > **Identity** > **Identity SourcesSystem** (⚙) > **Integration** > **Identity Sources**.

   For more information about creating identity sources, see:

   - Ways to Configure the Cisco Identity Services Engine (Cisco ISE) Identity Source
   - How to Configure a pxGrid Cloud Identity Source (ISE 3.3 or Earlier)
   - How to Configure a pxGrid Cloud Identity Source (ISE 3.4 or Later)

5. Create an identity realm.

   We support the following realms:

   - Create an LDAP Realm or an Active Directory Realm and Realm Directory

     Only Microsoft AD is supported; LDAP realms are not supported.

   - Create an Azure AD (SAML) Realm for Passive Authentication

6. Create the dynamic firewall instance. (If you already have a dynamic firewall instance, continue with the next step.)

   Click **Administration** > **Dynamic Attributes Connector** and click **Configure Dynamic Firewall**.

   See Create a dynamic firewall instance on page 238.

7. Associate your identity source with Cisco Identity Intelligence.

   See Associate an identity source with Identity Intelligence on page 239.

8. View system-defined filters.

   We create dynamic attributes filters for the following:

- Untrusted device
- Trusted device
- Untrusted user
- Questionable user

You can edit or replace these dynamic attributes filters as discussed in Create dynamic attributes filters on page 245.

9. View system-defined access control rules.

   We create an access control policy named Dynamic Firewall Policy (or similar) with the following rules:

   - Block an untrusted user from any source network to any destination network.
   - Monitor a questionable user from any source network to any destination network.
   - Block an untrusted device from any source network to any destination network.

   You can edit or delete the access control policy and rules as discussed in View and edit the system-created access control policy on page 244.

Get required information for Identity Intelligence

Configure required information from your Identity Intelligence tenant before you create a dynamic firewall instance.

Get the necessary credentials and configuration values from Identity Intelligence to enable integration with the dynamic firewall.

This task discusses how to create an API client, which provides all the get required information to set up Identity Intelligence in the dynamic firewall.

If you already have an API client and you know the values of all these parameters, you can skip this procedure and continue with :

- **Client ID**
- **API URL**
- **Token URL**
- **Client Secret**

Before you begin

Integrating with the dynamic firewall requires you to create an *API client integration* in Identity Intelligence.

Among the values you must know about your API client integration is the client secret, which is displayed when you create the API client only. For that reason you might need to create the API integration first.

For more information about creating an API cilent integration, see Public API.

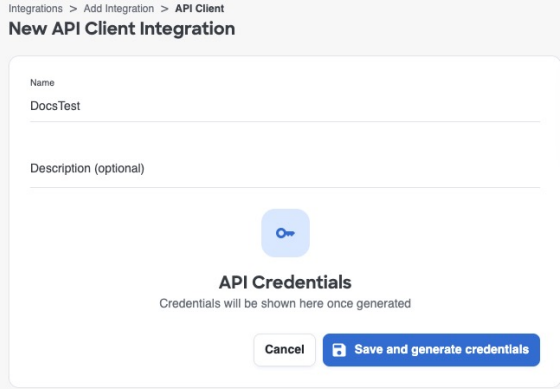
Follow these steps to get required information for Identity Intelligence:

Procedure

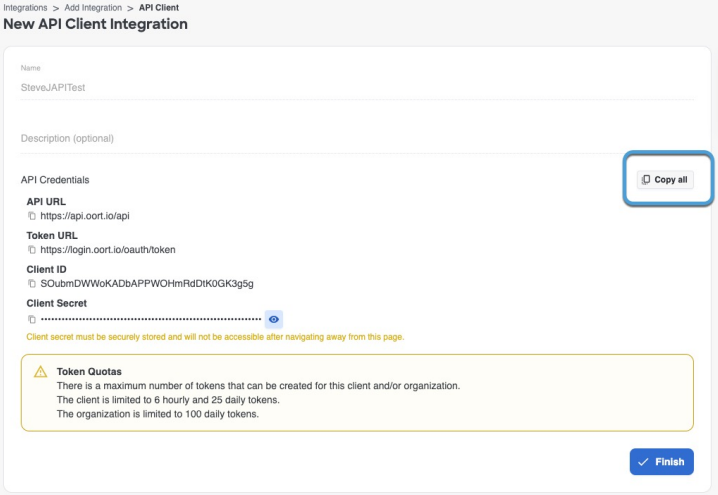
1. Log in to your Identity Intelligence tenant.
2. Click  (**Integrations**).
3. Click **Add Integration**.
4. On the next page, under API Clients, click **Add API Client**.
5. Enter a **Name** and an optional **Description**.

6. Click **Save and Generate Credentials**.

   This figure shows an example.



7. On the next page, click **Copy all** as this figure shows.



8. Save the credentials for later use.
9. Click **Finish**.

What to do next

Create an identity source and realm for the dynamic firewall

Outlines prerequisites for configuring the dynamic firewall.

Before you configure the dynamic firewall, you must configure a supported identity realm and identity source.

Configure an identity realm

These identity realms are supported:

- Create an LDAP realm or an Active Directory realm and realm directory

  Only Microsoft AD is supported; LDAP realms are not supported.

- Create an Azure AD (SAML) realm for passive authentication

Configure an identity source

These identity sources are supported:

- On-premises Cisco ISE: Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
- Single or multiple Cisco ISE clusters:
  - How to configure a pxGrid cloud identity source (ISE 3.3 or earlier)
  - How to configure a pxGrid cloud identity source (ISE 3.4 or later)

Create a dynamic firewall instance

Configure a dynamic firewall instance.

Create a new instance of the dynamic firewall to establish an association between an identity source and Identity Intelligence.

This task discusses how to create a new instance of the dynamic firewall, which is an association between an identity source and Identity Intelligence.

Before you begin

Complete all these steps:

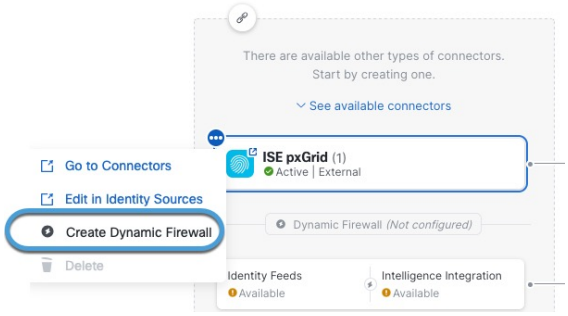
- Create an identity source:
  - On-premises Cisco ISE: Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
  - Single or multiple Cisco ISE clusters:
    - How to configure a pxGrid cloud identity source (ISE 3.3 or earlier)
    - How to configure a pxGrid cloud identity source (ISE 3.4 or later)

Follow these steps to create a dynamic firewall instance:

Procedure

1. If you haven't already done so, log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector**.
4. Click next to the name of the identity source with which to add the dynamic firewall.

   The following figure shows an example.



> **Note**
>
> If you do not see an identity source, create one before continuing:
>
> - Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source.
> - How to configure a pxGrid cloud identity source (ISE 3.3 or earlier)
> - How to configure a pxGrid cloud identity source (ISE 3.4 or later)

5. Click **Create Dynamic Firewall**.
6. Continue with Associate an identity source with Identity Intelligence.

Associate an identity source with Identity Intelligence

Configure an identity source association with Identity Intelligence as part of dynamic firewall configuration.

Associate a supported identity source with Identity Intelligence to enable user and device trust ratings for dynamic firewall configuration.

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device trust ratings to the Security Cloud Control.

For more information, see User Trust Level.

Before you begin

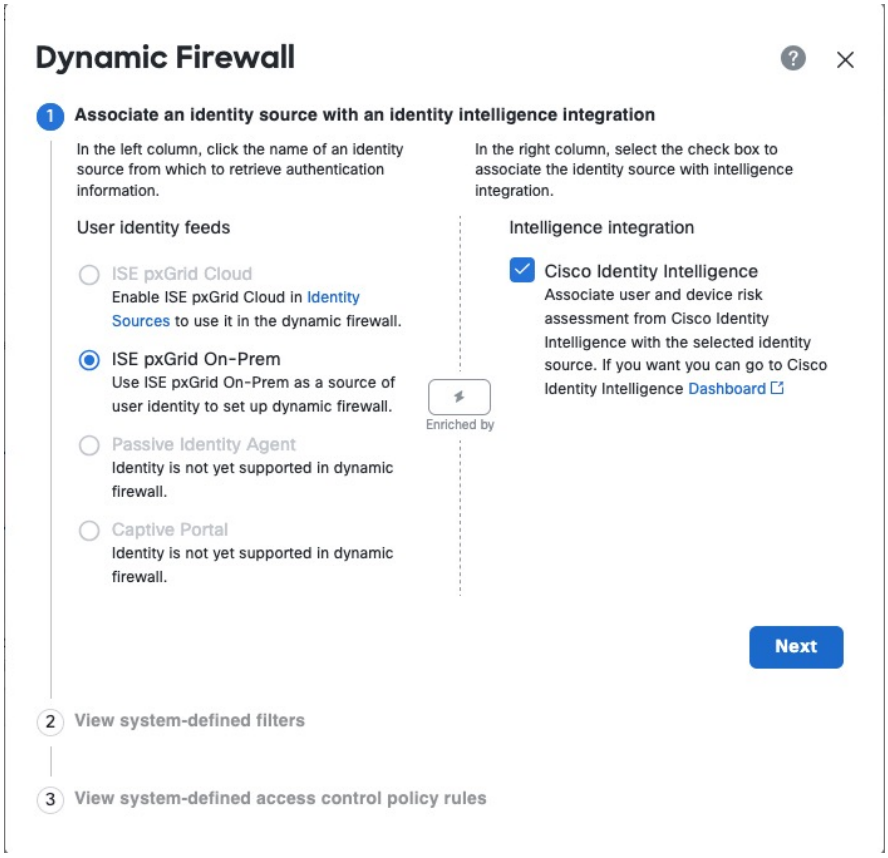
Before you begin, make sure you:

- Understand how the identity realm, identity source, and Identity Intelligence work together as discussed in Dynamic Firewall on page 234.
- Completed the tasks discussed in Create a dynamic firewall instance on page 238.

Procedure

1. Start with Create a dynamic firewall instance.
2. On the next page, from the left column, click your identity source. Then, in the right column, select the **Cisco Identity Intelligence** check box to add user intelligence, including user and device risk.

   The following figure shows an example.



3. Click **Next**.
4. Continue with Configure Identity Intelligence on page 240.

Configure Identity Intelligence

Configure the dynamic firewall to integrate with Identity Intelligence.

This task enables integration between the dynamic firewall and Identity Intelligence.

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device risk ratings to the Security Cloud Control.

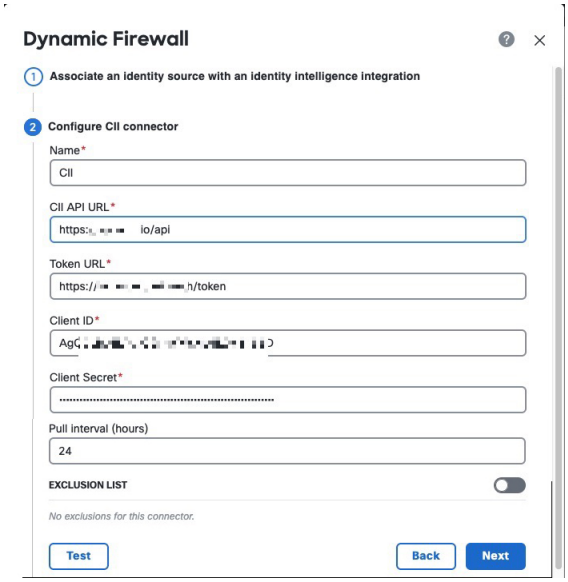
Before you begin

Complete the tasks discussed in Associate an identity source with Identity Intelligence on page 239.

Procedure

1. Complete the tasks discussed in Associate an identity source with Identity Intelligence on page 239.
2. If you selected the **Cisco Identity Intelligence** check box, enter the information you found for Identity Intelligence as described in Get required information for Identity Intelligence on page 236.

   The following figure shows an example.



3. (Optional.) For Identity Intelligence to consider a specific set of users as trusted, slide **Exclusion List** to **Slider enabled** ( ).

   Enter one user name per line in **username@domain.com** format. Users in this list are considered trusted by Identity Intelligence.

4. Click **Test**.

   Only if the test succeeds, continue with the next step.

   If any errors are displayed, check all of your Identity Intelligence values and try again.

5. Click **Next**.
6. Continue with View system-defined filters on page 241.

View system-defined filters

View the system-defined dynamic attributes filters created by the dynamic firewall wizard.

This task allows you to examine and understand the system-defined dynamic attributes filters that are automatically created during the configuration process.

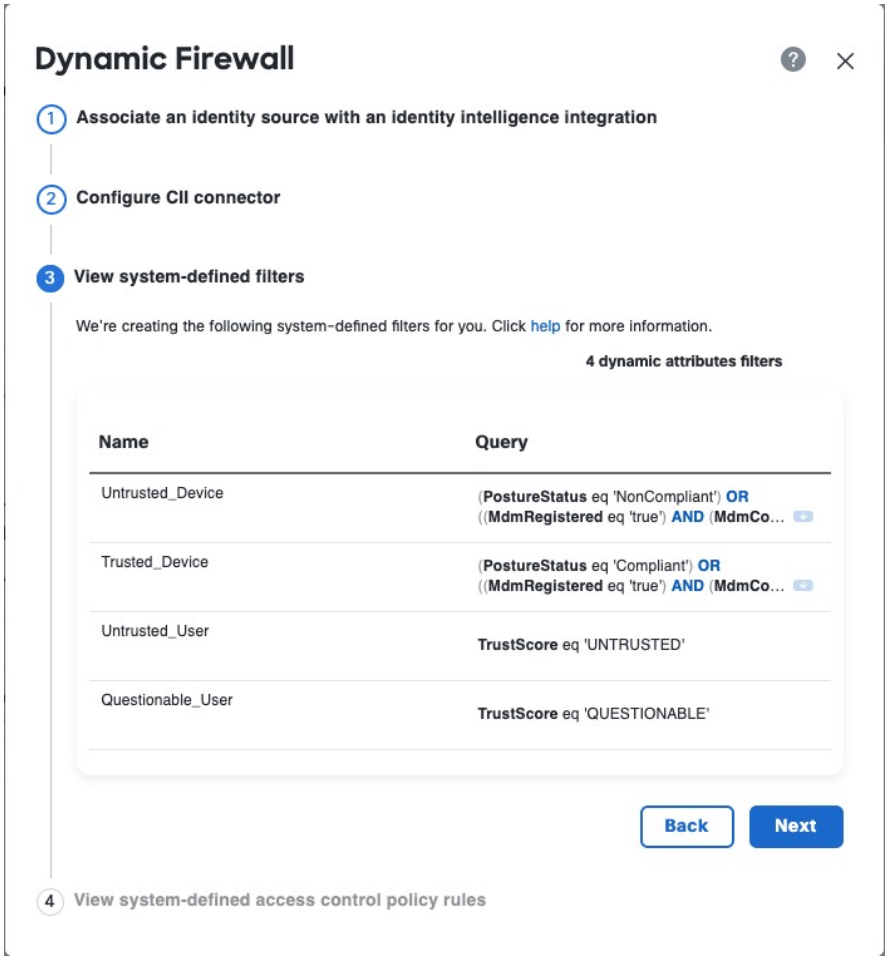
This task discusses how you associate an identity source with Cisco Identity Intelligence, which provides user and device risk ratings to the Security Cloud Control.

Before you begin

See Configure Identity Intelligence.

Procedure

1. The system displays a set of system-defined dynamic attributes filters, as shown in the following figure.



2. View the system-created filters. Click on any row to expand the filter so you can view the filter and see its details.
3. Click **Next**.
4. Continue with View system-defined access control rules on page 242.

View system-defined access control rules

View the access control rules created by the dynamic firewall instance.

This task allows you to review and decide whether to create system-defined access control rules for your dynamic firewall instance.

This task discusses access control rules created by the dynamic firewall.

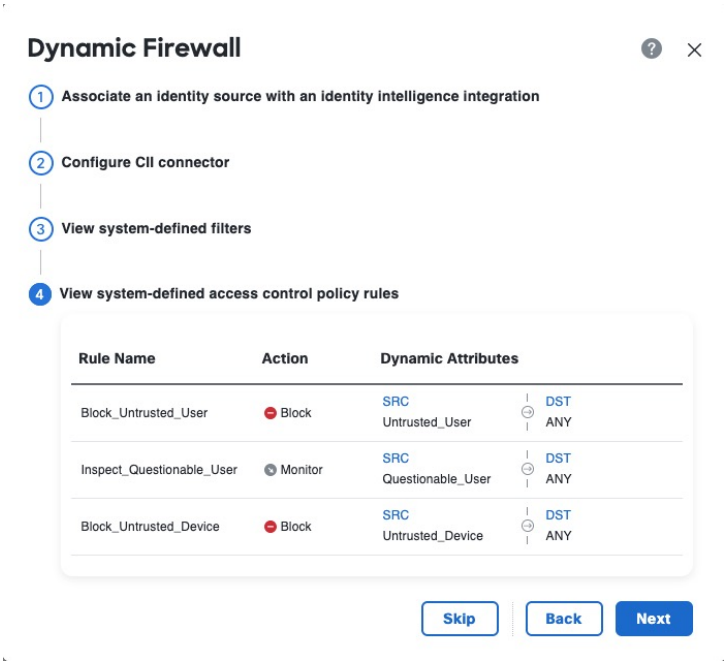
Before you begin

See View system-defined filters on page 241.

Procedure

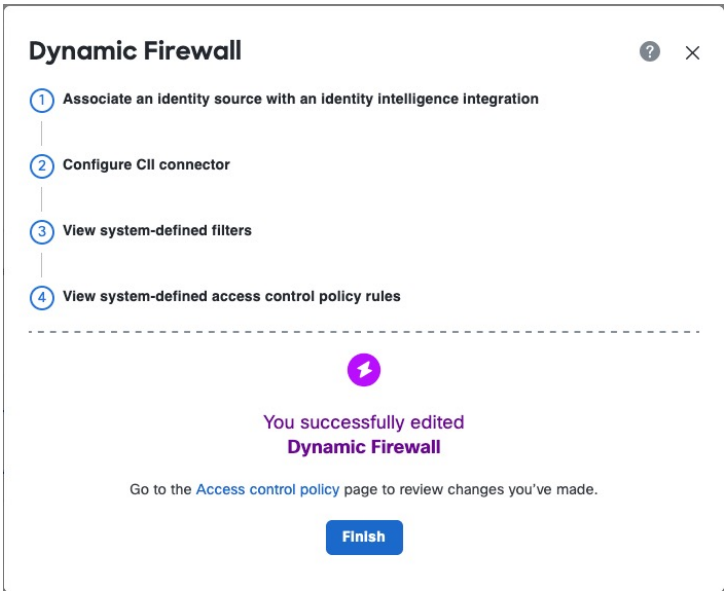
1. View the system-created access control rules.

   The following figure shows an example.



2. Choose one of these options:
   - Click **Skip** to skip creating these access control rules. You can create your own anytime.
   - Click **Next** to create an access control policy named Dynamic Firewall Policy with the rules shown in the preceding figure.
   - Click **Back** to return to system-created filters.

3. After you click **Next**, if you created access control rules successfully, the following page is displayed:



Edit the user exclusion list

Configure specific users provided by Identity Intelligence as always being trusted.

Specify users provided by Identity Intelligence as always being trusted.

You can instruct Identity Intelligence to treat specific users as trusted.

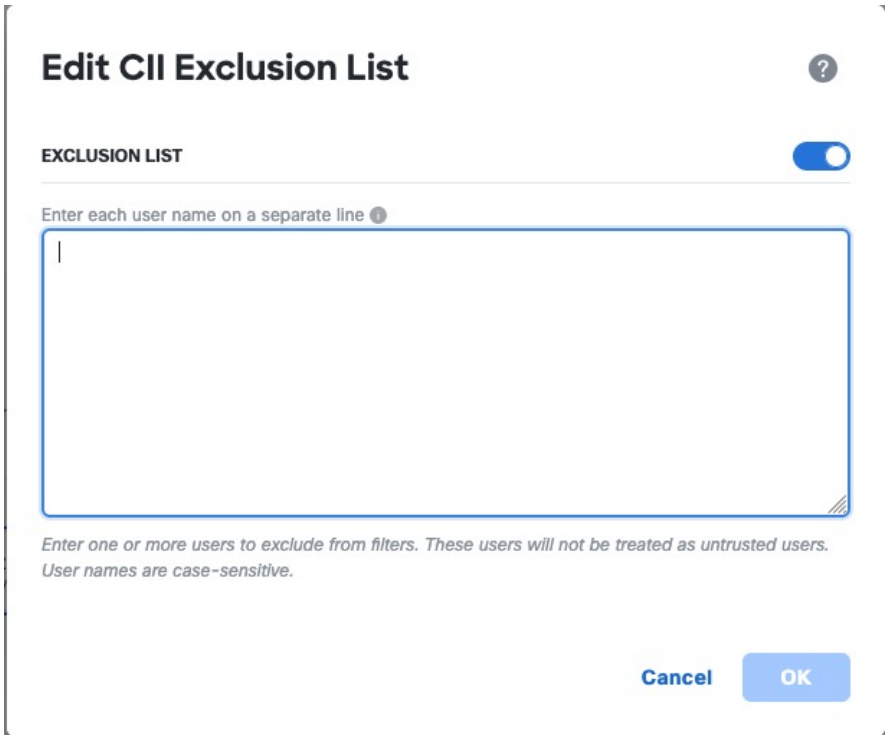
Before you begin

Configure the dynamic firewall as discussed in Create a dynamic firewall instance on page 238.

Procedure

1. Click **Administration** > **Dynamic Attributes Connector**.
2. Click next to the name of the identity source.
3. Click **Edit CII Exclusion List**.

   The following dialog box is displayed.



4. In the provided field, enter one user name in `username@domain.com` format on a line, press Enter, and enter another user name.

   Each user name is considered as trusted by Identity Intelligence.

View and edit the system-created access control policy

Configure the access control policy that the dynamic firewall creates for use as-is or edit to suit your needs.

Customize the system-created access control policy by adding devices, changing rules, reordering rules, or deleting rules to meet your specific network security requirements.

This topic discusses how you can edit the system-created access control rules and policy. Initially, the policy isn't associated with any devices but if you want to use it you can add devices, change rules, reorder rules, or delete rules.

Before you begin

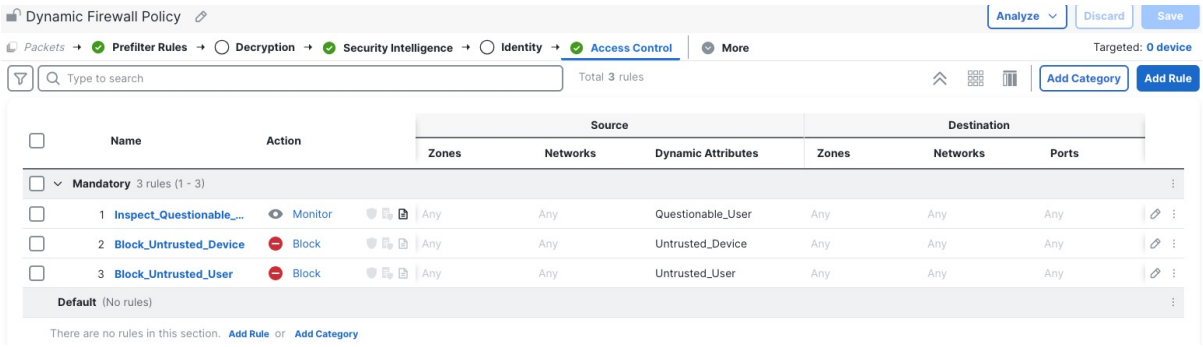
Complete the tasks described in View system-defined access control rules on page 242.

Follow these steps to view and edit the system-created access control policy:

Procedure

1. If you haven't already done so, log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Policies** > **Firewall Threat Defense** > **Access Control heading** > **Access Control**.
4. Click **Edit** ( ) next to the policy named Dynamic Firewall Policy (or similar).

   The following figure shows a sample access control policy.



   Note that in this access control policy, only the rule set to monitor questionable users logs anything. To adjust the logging settings, see Logging Settings for Access Control Policies.

5. Do any of the following:
   - Target the access control policy at devices: Assigning devices to an access control policy.
   - Edit the policy, including adding logging: Managing access control policies.
   - Edit access control rules: Managing access control rules.
   - Set advanced policy options: Access control policy advanced settings.
   - Associate other policies with this access control policy: Associating other policies with access control .

Create dynamic attributes filters

Configure dynamic attributes filters to use as dynamic objects in access control policies.

Create dynamic attributes filters that can be used as dynamic objects in access control policies to restrict access based on specific criteria such as group membership.

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Security Cloud Control as dynamic objects that can be used in access control policies. For example, you could restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

Note

You cannot create dynamic attributes filters for Azure Service Tags, Cisco Multicloud Defense, Generic Text, GitHub, Outlook 365, Tenable, Webex, and Zoom. These types of cloud objects provide their own IP addresses.

Procedure

1. Log in to Security Cloud Control.
2. Click **Firewall**.
3. Click **Administration** > **Dynamic Attributes Connector** > **Connectors**.
4. Do any of the following:
   - Add a new filter: click **Add** ( ).
   - Edit or delete a filter: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.
5. Enter the following information.
   - **Name**: Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in the Security Cloud Control Object Manager (**External Attributes** > **Dynamic Object**).
   - **Connector**: From the list, click the name of a connector to use.
6. To add a query, enter the following information.
   - **Key**: Click a key from the list. Keys are fetched from the connector.
   - **Operation**: Click one of the following:
     - **Equals** to exactly match the key to the value.
     - **Contains** to match the key to the value if any part of the value matches.
   - **Values**: Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.
7. Click **Show Preview** to display a list of networks or IP addresses returned by your query.

   When you're finished, click **Save**.

What to do next

Verify the dynamic object in the Security Cloud Control.

1. Log in to the Security Cloud Control.
2. Click **Policies** > **Firewall Threat Defense**.
3. Click **Objects** > **External Attributes** > **Dynamic Object**.

The dynamic attribute query you created should be displayed as a dynamic object.

9 Use Dynamic Objects in Access Control Policies

Topics:

- Dynamic objects in access control rules
- Create dynamic attributes filters
- Dynamic attributes rule conditions
- Create access control rules or DNS rules using dynamic attributes filters
- Use dynamic objects in DNS policies

The dynamic attributes connector enables you to configure dynamic attributes filters, seen in the Security Cloud Controlas dynamic objects, in access control rules.

Dynamic objects in access control rules

Explains how dynamic objects are used in access control rules.

You can use dynamic objects on the access control rule's **Dynamic Attributes** tab page. You can add dynamic objects as source or destination attributes.

Dynamic object usage examples

In an access control block rule, you can add a Finance dynamic object as a destination attribute to block access to Finance servers by whatever objects match the other criteria in the rule.

Dynamic attributes filter limitations

> **Note**
>
> You cannot create dynamic attributes filters for Azure Service Tags, Cisco Multicloud Defense, Generic Text, GitHub, Outlook 365, Tenable, Webex, and Zoom. These types of cloud objects provide their own IP addresses.

Create dynamic attributes filters

Configure dynamic attributes filters using the Dynamic Attributes Connector.

Create dynamic attributes filters to expose them as dynamic objects in Security Cloud Control for use in access control policies.

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Security Cloud Control as dynamic objects that can be used in access control policies. For example, restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

> **Note**
>
> You cannot create dynamic attributes filters for Azure Service Tags, Cisco Multicloud Defense, Generic Text, GitHub, Outlook 365, Tenable, Webex, and Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control rules, see Create access control rules or DNS rules using dynamic atttributes filters.

Procedure

1. Log in to Security Cloud Control.
   a) Click **Firewall**.
   b) Click **Administration** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.
2. Do any of the following:
   - Add a new filter: click **Add** ( ).
   - Edit or delete a filter: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.

3. Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a policy and in the Security Cloud Control Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	Click Add .

4. To add or edit a query, enter the following information.

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: • **Equals** to exactly match the key to the value. • **Contains** to match the key to the value if any part of the value matches.
Values	Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

5. Click **Show Preview** to display a list of networks or IP addresses returned by your query.
6. When you're finished, click **Save**.
7. (Optional.) Verify the dynamic object in the Security Cloud Control.
   a) Log in to the Security Cloud Control.
   b) Click **Policies** > **Firewall Threat Defense**.
   c) Click **Objects** > **External Attributes** > **Dynamic Object**.

   The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attributes rule conditions

Lists information about dynamic attributes rule conditions.

Dynamic attributes rule conditions allow you to specify access control rules based on real-time properties such as network objects, device types, locations, and security tags. These conditions determine how access control rules match traffic based on various attributes, optimizing policy flexibility and accuracy.

Types of dynamic attributes

Dynamic attributes include:

- (source or destination) Dynamic objects (such as from the dynamic attributes connector)

The dynamic attributes connector enables you to collect data (such as networks and IP addresses) from cloud providers and send it to the so they can be used in access control rules.

For more information about the dynamic attributes connector, see About the Dynamic Attributes Connector on page 188About the dynamic attributes connector.

- (source only) SGT objects contain tags either manually defined or defined in ISE. For more information, see Source and Destination Security Group Tag (SGT) Matching and Security Group Tag.
- (source only) Location IP objects, defined by Cisco ISE
- (source only) Device type objects, defined by Cisco ISE (also referred to as endpoint profile objects)

Combining objects in rules

Dynamic attributes can be used as source criteria and destination criteria in access control rules. Use these guidelines:

- Objects of different types are ANDd together
- Objects of a similar type are ORd together

For example, if you choose source destination criteria SGT 1, SGT 2, and device type 1, the rule matches if device type 1 is detected on either SGT 1 or SGT 2.

If you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originating from, or destined to, one of those IP addresses.

Create access control rules or DNS rules using dynamic attributes filters

Configure access control rules or DNS rules using dynamic attributes filters.

Create access control rules using dynamic objects that are based on dynamic attributes filters you have previously configured.

This topic discusses how to create access control rules using dynamic objects.

To add dynamic attributes filters to DNS policies, see Creating Basic DNS Policies.

Before you begin

Create dynamic attributes filters as discussed in Create dynamic attributes filters.

> **Note**
>
> You cannot create dynamic attributes filters for Azure Service Tags, Cisco Multicloud Defense, Generic Text, GitHub, Outlook 365, Tenable, Webex, and Zoom. These types of cloud objects provide their own IP addresses.

Follow these steps to create access control rules or DNS rules using dynamic attributes filters:

Procedure

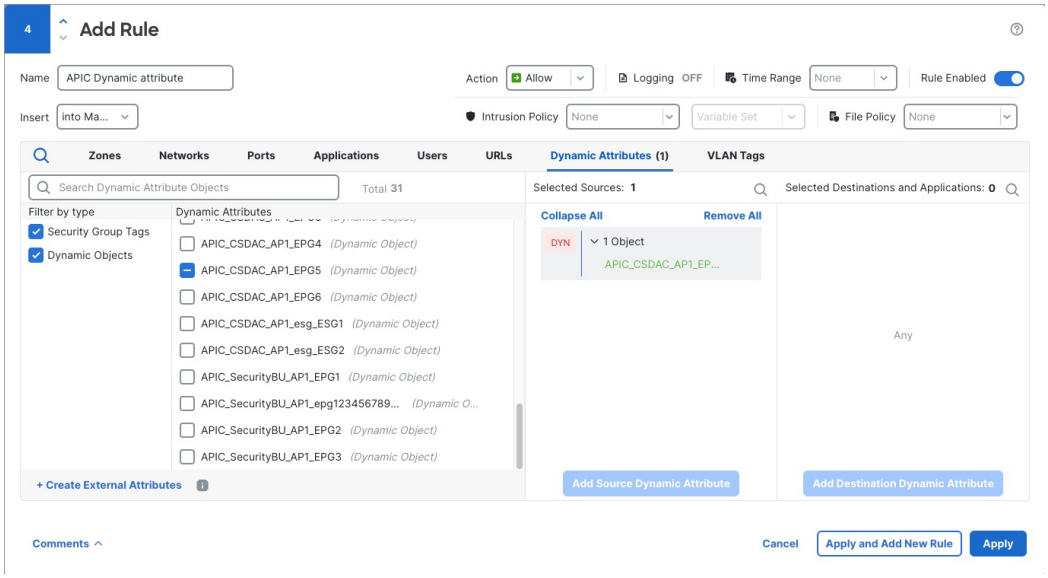
1. Log in to Security Cloud Control as a user with the Super Admin role.

   Click **Policies** > **Firewall Threat Defense** > **Access Control heading** > **Access Control**.

2. Click **Firewall**.

3. Click **Edit** (✎) next to an access control policy.
4. Click **Add Rule**.
5. Click the **Dynamic Attributes** tab.
6. In the Available Attributes section, from the list, click **Dynamic Objects**.

   The following figure shows an example.



   This example shows a dynamic object named `APIC Dynamic Attribute` that corresponds to the dynamic attribute filter created in the dynamic attributes connector.
7. Add the desired object to source or destination attributes.
8. Add other conditions to the rule if desired.

   See Dynamic attributes rule conditions.

Use dynamic objects in DNS policies

Configure dynamic objects from the dynamic attributes connector in DNS policies.

Use dynamic objects in DNS rules to enable dynamic filtering capabilities based on attributes from the dynamic attributes connector.

The dynamic attributes connector enables you to configure dynamic filters seen in the Cloud-Delivered Firewall Management Center as dynamic objects, in DNS rules. For information about DNS policies, see .

A dynamic object is automatically pushed from the dynamic attributes connector to the Cloud-Delivered Firewall Management Center after you create connectors and save a dynamic attributes filter on the connector.

You can use these dynamic objects on the DNS rule's Dynamic Attributes tab page, similarly to the way you use Security Group Tags (SGTs). You can add dynamic objects as source or destination attributes, except for endpoint device type objects, which are source only.

Procedure

1. Click **Policies** > **Security policies** > **DNS** and create or edit a DNS policy.
2. Add or edit a rule.

3. Click the **Dynamic Attributes** tab.
4. In the **Dynamic Attributes** list, select the objects you want to use, then add them to the source or destination lists as appropriate.

   Initially, all security group and dynamic objects are listed, by you can uncheck the Security Group option to see dynamic objects only.

5. On the **DNS** tab, select the appropriate list or feed to match the DNS requests you are targeting.
6. Add other conditions to the rule if desired and set the action.
7. Click **Save**.

10 Troubleshoot the Dynamic Attributes Connector

Topics:

- Troubleshoot error messages
- Get your tenant ID

How to troubleshoot issues with the dynamic attributes connector.

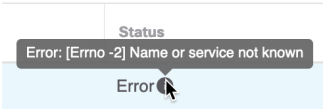
Troubleshoot error messages

Lists error message reference for the dynamic attributes connector.

This reference provides error messages and troubleshooting solutions for dynamic attributes connectors and adapters in the dynamic attributes connector.

Problem: name or service not known error

This error is displayed as a tooltip when you hover the mouse over an error condition on an adapter or connector. An example follows; yours might look different.

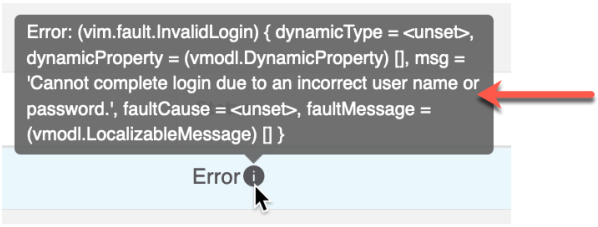


Solution: Edit the connector or adapter and check for:

- A trailing slash on a host name
- Verify the password is correct

Problem: incorrect username or password

This error is displayed as a tooltip when you hover the mouse over an error condition on a connector.



Solution: Edit the connector and change the user name or password.

Get your tenant ID

Configure the tenant ID required to ask Cisco TAC to troubleshoot issues with Security Cloud Control.

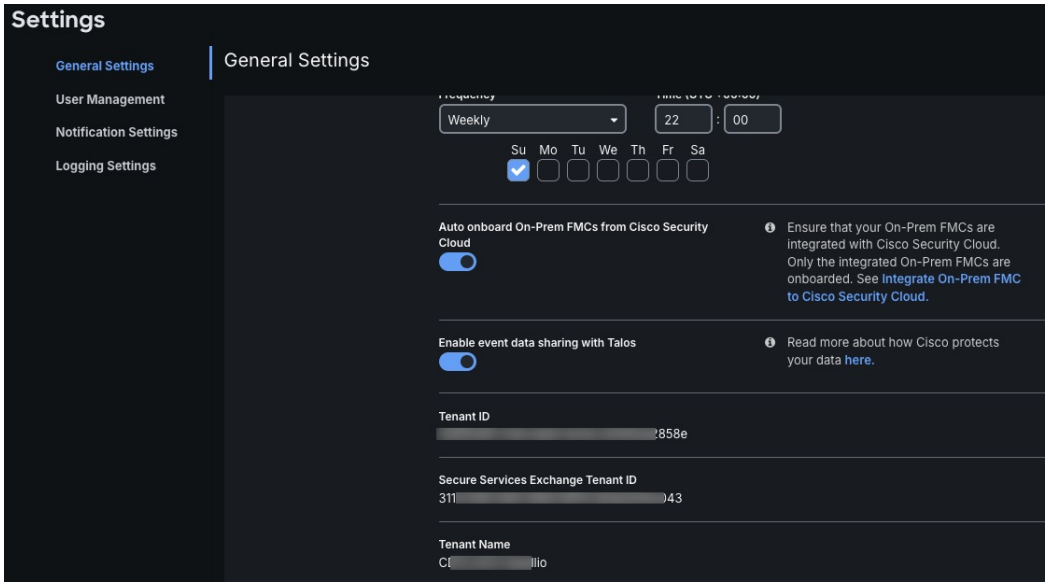
This task provides your tenant ID to Cisco TAC for troubleshooting assistance with the dynamic attributes connector.

If you require assistance with the dynamic attributes connector, you must provide your tenant ID to Cisco TAC so we can look at your logs.

Procedure

1. Click **Administration** > **General Settings**.
2. Copy your tenant ID to the clipboard to provide to Cisco TAC.

   A sample follows.


Settings
General Settings
User Management
Notification Settings
Logging Settings
General Settings
Weekly
22
00
Su Mo Tu We Th Fr Sa
Auto onboard On-Prem FMCs from Cisco Security Cloud
Ensure that your On-Prem FMCs are integrated with Cisco Security Cloud. Only the integrated On-Prem FMCs are onboarded. See Integrate On-Prem FMC to Cisco Security Cloud.
Enable event data sharing with Talos
Read more about how Cisco protects your data here.
Tenant ID
Secure Services Exchange Tenant ID
Tenant Name

Part IV

Manage Secure Firewall ASA

Topics:

- Onboard Secure Firewall ASA devices
- Configure Secure Firewall ASA
- Secure Firewall ASA Security Policy Management
- Monitor Secure Firewall ASA Events
- Monitor device health metrics
- Use Cisco Secure Cloud Analytics Portal
- Upgrade Secure Firewall ASA
- Troubleshoot Secure Firewall ASA

11 Onboard Secure Firewall ASA devices

Topics:

- Onboard a Secure Firewall ASA
- Onboard a high availability pair of ASA devices to Security Cloud Control Firewall Management
- Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management
- Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management
- Onboard multiple ASAs to Security Cloud Control Firewall Management
- Create and import an ASA model to Security Cloud Control Firewall Management

Explains the various methods for onboarding Cisco Secure Firewall ASA devices, including prerequisites, connector selection, credential configuration, labeling, and reviewing inventory results.

This chapter explains the various different methods using which a Secure Firewall ASA can be onboarded.

Onboard a Secure Firewall ASA

Learn how to onboard a single Cisco ASA device to Security Cloud Control Firewall Management with essential prerequisites including software versions, configuration file size, certificate requirements, and supported cipher suites.

This task connects a single live ASA device to Security Cloud Control Firewall Management for centralized management and monitoring.

Use this procedure to onboard a single ASA device, not an ASA model, to Security Cloud Control Firewall Management. If you want to onboard multiple ASAs at once, refer to Onboard ASAs in Bulk.

Before you begin

Device Prerequisites

- Review Allow inbound access for direct cloud connectivity on page 94.
- The device must be running version 8.4 or later.

> **Note**
>
> TLS 1.2 became available for the ASA management plane in version 9.3(2). To onboard to Security Cloud Control Firewall Management using version 9.3(2), a local SDC is required.

- The running configuration file of your ASA must be less than 4.5 MB.

  To confirm the size of your running configuration file, refer to Confirming ASA Running Configuration Size.

- IP addressing: Each ASA, ASAv, or ASA security context must have a unique IP address, and the SDC must connect to it on the interface configured to receive management traffic.

Certificate Prerequisites

If your ASA device does not have a compatible certificate, onboarding the device may fail. Make sure that these requirements are met:

- The device must use TLS version 1.0 or later.
- The certificate presented by the device must not be expired, and its issuance date must be in the past. This means the certificate is already valid and not scheduled to become valid later.
- The certificate must be a SHA-256 certificate. SHA-1 certificates are not accepted.
- One of the following conditions must be met:
  - The device uses a self-signed certificate, and it is the same as the most recent one trusted by an authorized user.
  - The device uses a certificate signed by a trusted Certificate Authority (CA) and provides a certificate chain that links the presented leaf certificate to the relevant CA.

For more information about certificate errors during the onboarding process, refer to Disable ASA client-side certificate authentication for onboarding on page 392.

Open SSL Cipher Prerequisites

If the device does not have a compatible SSL cipher suite, it cannot successfully communicate to the Secure Device Connector (SDC). Use any of these cipher suites:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

If the cipher suite you use on your ASA is not in this list, it is not supported by the SDC. You must update the cipher suite on your ASA.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose Security Devices.
3. Click the **Onboard device or service** () icon.
4. Click the **ASA** tile.
5. In the **Locate Device** step, perform these actions:
   a. Click the **Secure Device Connector** button and select a Secure Device Connector installed in your network. If you do not want to use an SDC, Security Cloud Control Firewall Management can connect to your ASA using the Cloud Connector. The method you select depends on how you connect Security Cloud Control Firewall Management to your managed devices.
   b. Enter a name for the device.
   c. Enter the location of the device or service (IP address, FQDN, or URL). The default port is 443.
   d. Click **Next**.
6. In the **Credentials** step, enter the username and password of the ASA administrator, or similar highest-privilege ASA user, that Security Cloud Control Firewall Management will use to connect to the device and click **Next**.
7. (Optional) You can enter a label for the device in the **Done** step. This label lets you filter your list of devices. For more information about labels and label groups, refer to Labels and Label Groups.
8. After labeling your device or service, you can view it in the **Security Devices** list.

> **Note**
>
> Analyzing the configuration may take some time, depending on its size and the number of devices or services.

The ASA device is successfully onboarded and appears in the **Security Devices** list, where you can manage and monitor its configuration.

Onboard a high availability pair of ASA devices to Security Cloud Control Firewall Management

Explains how to onboard a high availability (HA) pair of Cisco ASA devices to Security Cloud Control Firewall Management.

A high availability ASA device onboarding process is a network management approach that

- requires onboarding only the primary ASA to Security Cloud Control Firewall Management
- uses the failover link to manage the secondary ASA automatically, and
- eliminates the need to onboard the secondary device separately.

Additional onboarding information

For more information about onboarding ASA devices to Security Cloud Control Firewall Management, refer to Onboard a Secure Firewall ASA on page 260.

Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management

Explains how to onboard an ASA in multi-context mode to Security Cloud Control Firewall Management, including prerequisites, connector selection, credentials, labels, and inventory results.

ASA multi-context mode onboarding is a process that

- partitions a single ASA into multiple logical devices known as contexts
- onboards each security context and admin context as a separate ASA in Security Cloud Control Firewall Management, and
- manages each context as if it were a separate ASA device.

Multi-context mode configuration types

The three types of configurations used in an ASA configured in multi-context mode are:

- Security context
- Admin context
- System configuration

Security contexts:

Each security context acts as an independent device, with its own security policy, interfaces, and administrators. Multiple security contexts are similar to having multiple standalone devices. A security context is not a virtual ASA in the sense of a virtual machine image installed in a private cloud infrastructure. A security context is configured on an ASA that is installed on a hardware appliance. Each context is configured on a physical interface of that appliance.

For more information about multi-context mode, refer to ASA CLI and ASDM configuration guides.

Security Cloud Control Firewall Management onboards each security context as a separate ASA and manages it as if it were a separate ASA.

Admin contexts:

The admin context is similar to a security context, except that when a user logs in to the admin context, the user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way and can be used as a regular context. However, because logging into the admin context grants administrator privileges over all contexts, access to the admin context should be restricted to authorized users.

Security Cloud Control Firewall Management onboards each admin context as a separate ASA and manages it as if it were a separate ASA. Security Cloud Control Firewall Management also uses the admin context when upgrading ASA and ASDM software on the appliance.

System configuration:

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and setting other context operating parameters within the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself. When the system needs to access network resources, such as downloading the contexts from the server, it uses one of the contexts designated as the admin context.

Security Cloud Control Firewall Management does not onboard the system configuration.

Onboard prerequisites for security and admin contexts:

Before you onboard security or admin contexts, check the prerequisites in Onboard a Secure Firewall ASA on page 260.

To learn which Cisco appliances support ASAs in multi-context mode, refer to the "Multiple Context Mode" chapter in the *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide* for your ASA software version.

An ASA running as a single context firewall, or as the admin context of a multiple-context firewall, can use different port numbers for ASDM and Security Cloud Control Firewall Management access. ASA security contexts use a fixed port (port 443) for ASDM and Security Cloud Control Firewall Management access.

Onboard ASA security and admin contexts:

To onboard a security context or admin context, follow the instructions in Onboard a Secure Firewall ASA on page 260 or Onboard multiple ASAs to Security Cloud Control Firewall Management on page 265.

Upgrade security contexts:

Security Cloud Control Firewall Management treats each security and admin context of a multiple-context ASA as a separate ASA and each is onboarded separately. However, all security and admin contexts of a multiple-context ASA run the same version of ASA software installed on the appliance.

Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management

Explains how to onboard an ASA in multi-context mode to Security Cloud Control Firewall Management, including prerequisites, connector selection, credentials, labels, and inventory results.

ASA multi-context mode onboarding is a process that

- partitions a single ASA into multiple logical devices known as contexts

- onboards each security context and admin context as a separate ASA in Security Cloud Control Firewall Management, and
- manages each context as if it were a separate ASA device.

Multi-context mode configuration types

The three types of configurations used in an ASA configured in multi-context mode are:

- Security context
- Admin context
- System configuration

Security contexts:

Each security context acts as an independent device, with its own security policy, interfaces, and administrators. Multiple security contexts are similar to having multiple standalone devices. A security context is not a virtual ASA in the sense of a virtual machine image installed in a private cloud infrastructure. A security context is configured on an ASA that is installed on a hardware appliance. Each context is configured on a physical interface of that appliance.

For more information about multi-context mode, refer to ASA CLI and ASDM configuration guides.

Security Cloud Control Firewall Management onboards each security context as a separate ASA and manages it as if it were a separate ASA.

Admin contexts:

The admin context is similar to a security context, except that when a user logs in to the admin context, the user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way and can be used as a regular context. However, because logging into the admin context grants administrator privileges over all contexts, access to the admin context should be restricted to authorized users.

Security Cloud Control Firewall Management onboards each admin context as a separate ASA and manages it as if it were a separate ASA. Security Cloud Control Firewall Management also uses the admin context when upgrading ASA and ASDM software on the appliance.

System configuration:

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and setting other context operating parameters within the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself. When the system needs to access network resources, such as downloading the contexts from the server, it uses one of the contexts designated as the admin context.

Security Cloud Control Firewall Management does not onboard the system configuration.

Onboard prerequisites for security and admin contexts:

Before you onboard security or admin contexts, check the prerequisites in Onboard a Secure Firewall ASA on page 260.

To learn which Cisco appliances support ASAs in multi-context mode, refer to the "Multiple Context Mode" chapter in the *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide* for your ASA software version.

An ASA running as a single context firewall, or as the admin context of a multiple-context firewall, can use different port numbers for ASDM and Security Cloud Control Firewall Management access. ASA security contexts use a fixed port (port 443) for ASDM and Security Cloud Control Firewall Management access.

Onboard ASA security and admin contexts:

To onboard a security context or admin context, follow the instructions in Onboard a Secure Firewall ASA on page 260 or Onboard multiple ASAs to Security Cloud Control Firewall Management on page 265.

Upgrade security contexts:

Security Cloud Control Firewall Management treats each security and admin context of a multiple-context ASA as a separate ASA and each is onboarded separately. However, all security and admin contexts of a multiple-context ASA run the same version of ASA software installed on the appliance.

Onboard multiple ASAs to Security Cloud Control Firewall Management

Configure bulk onboarding of multiple ASA devices to Security Cloud Control Firewall Management using a .CSV file with prerequisites, connector selection, credentials, labels, and inventory results.

Security Cloud Control Firewall Management allows you to bulk onboard ASA devices by providing the necessary information for all the ASA devices in a .CSV file.

As the ASA devices are being onboarded, you can use the filter pane to show which onboarding attempts are queued, loading, complete, or have failed.

Before you begin

- Review Allow inbound access for direct cloud connectivity on page 94.
- Prepare a .CSV file with the connection information for the ASA devices you want to onboard. Add the information about each ASA on a separate line. To include a comment, add a # at the beginning of the line.
  - ASA location (either IP address or FQDN)
  - ASA administrator username
  - ASA administrator password
  - (Optional) Device name for Security Cloud Control Firewall Management
  - In the SDCName field, specify the name of a Secure Device Connector (SDC) in your network you want to use to connect Security Cloud Control Firewall Management to your ASA. You can also enter "none" if you are not going to connect your ASA to Security Cloud Control Firewall Management using an SDC. When onboarding the device, specifying "none" in SDCName field, onboards the ASA using the Cloud Connector. The Cloud Connector allows you to connect your device to Security Cloud Control Firewall Management without installing an SDC. Choose an option based on how you connect Security Cloud Control Firewall Management to your managed device.
  - (Optional) device labels for Security Cloud Control Firewall Management
  - To add one label, add the label name to the last CSV field.
  - To add more than one label to a device, surround the values with quotation marks. For example, `alpha,beta,gamma`.
  - To add a category and choice label, separate the two values with a colon (:). For example, `Rack:50`.

Here is a sample configuration file.

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

> **Caution**
>
> Security Cloud Control Firewall Management does not validate any of the data in the .CSV file. You need to ensure the accuracy of the entries.

Follow these steps to onboard multiple ASAs to Security Cloud Control Firewall Management:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose Security Devices.
3. Click the plus button  to onboard an ASA.
4. On the Onboarding page, click the **Multiple ASAs** tile.
5. Click **Browse** to locate the .CSV file containing your ASA entries. The devices you specify appear in the ASA Bulk Onboarding table as queued and are ready for onboarding.

   > **Caution**
   >
   > Stay on the ASA Bulk Onboarding page until the onboarding process is complete. If you leave the page, the onboarding process stops.

6. Click **Start**.

   The status column in the ASA Bulk Onboarding table shows the progress of onboarding. When onboarding finishes, the status displays "Complete."

   To pause bulk onboarding and resume later, refer to Pause and resume onboarding multiple ASA devices on page 266.

The ASA devices are successfully onboarded to Security Cloud Control Firewall Management and appear with "Complete" status in the ASA Bulk Onboarding table.

Pause and resume onboarding multiple ASA devices

Configure the bulk onboarding process to pause and resume as needed while onboarding multiple ASA devices.

This task allows you to control the bulk onboarding process by pausing it when needed and resuming it later without losing progress on devices that have already been processed.

During bulk onboarding of multiple ASA devices, you may need to temporarily stop the process and resume it later. The system maintains the state of already onboarded devices and continues with the remaining queued devices when resumed.

Procedure

1. To pause the onboarding process, click **Pause**.

   Security Cloud Control Firewall Management completes onboarding any device it has started.

2. To resume bulk onboarding, click **Start**.

   Security Cloud Control Firewall Management will begin onboarding the next queued device.

   The bulk onboarding process can be paused and resumed as needed. If you leave the page after pausing, you must return and restart the process. Security Cloud Control Firewall Management identifies already onboarded devices, flags duplicates from this new attempt, and quickly starts onboarding the remaining queued devices.

Create and import an ASA model to Security Cloud Control Firewall Management

Configure an ASA model to Security Cloud Control Firewall Management, including configuration file import, device identity, labels, and offline policy setup.

This task allows you to create and import an ASA model to Security Cloud Control Firewall Management, enabling configuration management and offline policy setup for ASA devices.

Use this process when you need to download an ASA device configuration file from the management interface to your local computer for further configuration management tasks.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose Security Devices.
3. Click the **Devices** tab.
4. Click the **ASA** tab.
5. Select an ASA device. In the **Management** section, click **Configuration**.
6. To download the device configuration to your local computer, click **Download**.

The ASA device configuration file is downloaded to your local computer and can be used for creating and importing an ASA model with device identity, labels, and offline policy configuration.

Import ASA configuration

Configure offline management for your Cisco ASA security devices by importing configuration files. This topic covers the step-by-step process of onboarding ASA security devices, including file size requirements, browsing for configuration files, and applying device labels.

Import your Cisco ASA configuration file to enable offline management of ASA security devices through the platform interface.

Use this procedure when you need to onboard ASA security devices for offline management by uploading existing configuration files to the platform.

Before you begin

The ASA running configuration file you are onboarding must be less than 4.5 MB. Confirm the size of the configuration file before you onboard it.

Follow these steps to import ASA configuration:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.

2. Choose Security Devices.
3. Click the add button () to import the configuration file.
4. Click **Import configuration for offline management**.
5. Select the **Device Type** as **ASA**.
6. Click **Browse**, and select the configuration file in text format to upload.
7. Once the configuration is verified, you are prompted to label the device or service. For more information about labels and label groups, refer to Labels and Label Groups.
8. After labeling your model device, you can view it in the **Security Devices** list.

> **Note**
>
> The configuration may take some time to be analyzed, depending on its size and the number of other devices or services.

12 Configure Secure Firewall ASA

Topics:

- Update ASA connection credentials in Security Cloud Control Firewall Management
- ASA interface configuration
- ASA system settings policy in Security Cloud Control Firewall Management
- ASA routing in Security Cloud Control Firewall Management
- API tokens
- ASA file management
- Managing ASAs with pre-existing High Availability configuration
- Manage ASA configuration files
- Configure DNS on ASA
- ASA command line interface

Learn how to configure Cisco Secure Firewall ASA.

This chapter explains the steps involved to configure a Secure Firewall ASA device.

Update ASA connection credentials in Security Cloud Control Firewall Management

Configure updated ASA connection credentials in Security Cloud Control Firewall Management, including device location, username, password, connector access, and connectivity validation.

This task allows you to update ASA connection credentials in Security Cloud Control Firewall Management without having to re-onboard the device when credentials are changed on the ASA.

In the process of onboarding an ASA, you entered the username and password Security Cloud Control Firewall Management must use to connect to the device. If those credentials are changed on the device, use the **Update Credentials** device action to update those credentials on Security Cloud Control Firewall Management as well. This feature allows you to update the credentials on Security Cloud Control Firewall Management without having to re-onboard the device. The username and password combination you switch to must already exist on the ASA or Authentication, Authorization, and Accounting (AAA) server for that user. This process only affects the Security Cloud Control Firewall Management database; no changes to the ASA configuration are made when using the Update Credentials feature.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab and then click **ASA**.
3. Select the ASAs whose connection credentials it is you want to update. You can update the credentials on one or multiple ASAs at once.
4. In the **Device Actions** pane, click **Update Credentials**.
5. Select the Cloud Connector or the Secure Device Connector (SDC) you use to connect the ASA(s) to Security Cloud Control.
6. Enter the new username and password you want to use to connect to the ASAs.
7. After the credentials are changed, Security Cloud Control syncs the device.

   Note

   If Security Cloud Control Firewall Management fails to sync the device, the connectivity status in Security Cloud Control Firewall Management may show "Invalid Credentials." If that's the case, you may have tried to use an invalid username and password combination. Make sure the credentials you want to use are stored on your ASA or AAA server, and try again.

The ASA connection credentials are updated in Security Cloud Control Firewall Management and the device syncs successfully with the new credentials.

Move an ASA from one SDC to Another

Security Cloud Control supports the use of more than one SDC per tenant. You can move a managed ASA from one SDC to another using this procedure:

Procedure

1. In the left pane, click **Security Devices**
2. Select the ASAs you want to move to the other SDC.

3. In the Device Actions pane, click **Update Credentials**.
4. Click the Secure Device Connector button and select the SDC you want to move the device to.
5. Enter the administrator username and password you used to onboard the ASA, and click Update. You do not have to deploy these changes to the device.

ASA interface configuration

An overview of ASA interface configuration, including interface names, security levels, IP addressing, VLANs, and enablement options.

Security Cloud Control Firewall Management simplifies ASA interface configuration by providing a user-friendly interface that eliminates the need to use the command line interface. You have complete control over configuring the ASA's physical interfaces, subinterfaces, and EtherChannels. Moreover, you can also view Virtual Tunnel Interfaces that are created during route-based site-to-site VPN, but they are read-only. You can use Security Cloud Control Firewall Management to configure and edit data interfaces or the management/diagnostic interface on an ASA device.

When you attach a cable to an interface connection (physically or virtually), you need to configure the interface. At minimum, you need to name the interface and enable it for traffic to pass through it. If the interface is a member of a bridge group, naming the interface is sufficient. If the interface is a bridge virtual interface (BVI), you need to assign the BVI an IP address. If you intend to create VLAN subinterfaces rather than a single physical interface on a given port, you would typically configure the IP addresses on the subinterface, not on the physical interface. VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs.

The interface list shows the available interfaces, their names, addresses, and states. You can change the state of an interface, on or off, or edit an interface, by selecting the interface row and clicking **Edit** in the Actions pane. The list shows the interface characteristics based on your configuration. Expand an interface row to see subinterfaces or bridge group member.

Management interface

You can manage the ASA by connecting to:

- Any through-traffic interface
- A dedicated Management Slot/Port interface (if available for your model)

Use MTU settings

The MTU specifies the maximum frame payload size that the device can transmit on a given Ethernet interface. The MTU value is the frame size without Ethernet headers, VLAN tagging, or other overhead. For example, when you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when using VLAN. Do not set the MTU value higher to accommodate these headers.

Read-only support for Virtual Tunnel Interface (VTI)

Configuring a route based site-to-site VPN tunnel between two ASA devices creates a Virtual Tunnel Interface (VTI) between the devices. Devices with configured VTI tunnels can be onboarded to Security Cloud Control Firewall Management, which discovers and lists them on the **ASA Interfaces** page but doesn't support their management.

Configure an ASA Physical Interface

Procedure

1. In the left pane, click **Security Devices**.

2. Click the **ASA** tab.
3. Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
4. Click a physical interface that you want to configure, and click **Edit**.

   The **Editing Physical Interface** dialog box appears.

5. In the **Logical Name** field, enter a name for the interface.
6. Continue with one of the following procedures:
   - Configure IPv4 Addressing for the Physical Interface if you intend to assign an IPv4 address to this interface.
   - Configure IPv6 Addressing for ASA Physical Interface on page 273 if you intend to assign an IPv6 address to this interface.
   - Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
   - If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Configure IPv4 Addressing for ASA Physical Interface

Procedure

---

1. In the **Edit Physical Interface** dialog box, configure the following in the **IPv4 Address** tab:
   - **Type**: You can use either static IP addressing or DHCP for the interface.

     Static - Choose this option if you want to assign an address that should not change.

     - **IP Address and Subnet Mask**: Enter the interface's IP address and the subnet mask for the network attached to the interface.
     - **Standby IP Address**: If you configured high availability and are monitoring this interface for HA, also configure a standby IP address on the same subnet. This interface on the standby device uses the standby address.

       For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

     DHCP: Choose this option if the address should be obtained from the DHCP server on the network.

     You can check the **Obtain Default Route** check box to get the default route from the DHCP server. You would normally check this option.

2. Click **Save** if you are done or continue with one of these procedures.
   - Configure IPv6 Addressing for ASA Physical Interface on page 273 if you intend to assign an IPv6 address to this interface.
   - Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
   - If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Configure IPv6 Addressing for ASA Physical Interface

Procedure

1. In the **Editing Physical Interface** dialog box, click the **IPv6 Address** tab.
2. Configure the following:

   - **State**: To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the **State** slider to enable it. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

     > **Note**
     >
     > Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

   - **Address Auto Configuration**:

     Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

     Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

   - **Suppress RA**: Check this box if you want to suppress router advertisements. The device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

     Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

     You might want to suppress these messages on any interface for which you do not want the device to supply the IPv6 prefix (for example, the outside interface).

   - **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

   - **Link-Local Address**: If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

> **Note**
>
> A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby Link-Local Address**: Configure this address if the interface connects a high availability pair of devices. Enter the link-local address of the interface on the other device, to which this interface is connected.
- **Static Address/Prefix**: If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. You can add another static address.
- **Standby IP Address**: If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

3. Click **Save** if you are done or continue with one of these procedures.
   - Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
   - If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Configure Advanced ASA Physical Interface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

This procedure and all of the steps in it are optional.

Procedure

---

1. In the **Editing Physical Interface** dialog box, click the **Advanced** tab.
2. Configure the following advanced settings:
   - **HA Monitoring**: Enable to include the health of the interface as a factor when the HA pair decides whether to fail over to the peer unit in a high availability configuration. This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.
   - **Management Only**: Enable to make a data interface management only.

     A management only interface does not allow through traffic, so there is very little value in setting a data interface as a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.
   - **MTU**: The default MTU is 1500 bytes. You can specify a value from 64 - 9198. Set a high value if you typically see jumbo frames on your network.

- **Duplex and Speed (Mbps)**: The default is that the interface negotiates the best duplex and speed with the interface at the other end of the wire, but you can force a specific duplex or speed if necessary. The options listed are only those supported by the interface. Before setting these options for interfaces on a network module, please read Limitations for Interface Configuration.
  - **Duplex**: Choose Auto, Half, or Full. Auto is the default when the interface supports it.
  - **Speed**: Choose Auto to have the interface negotiate the speed (this is the default), or pick a specific speed: 10, 100, 1000, 10000 Mbps. You can also select these special options:
- **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.
- **MAC Address**: The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)
- **Standby MAC Address**: For use with high availability. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

3. If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Interface.
4. Click **Save**.

Enable the ASA Physical Interface

Procedure

---

1. Select the physical interface you want to enable.
2. Move the **State** slider at the top right of the window associated with the interface's logical name.
3. Review and deploy the changes you made.

Add an ASA VLAN Subinterface

VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or devices.

Create subinterfaces if you attach the physical interface to a trunk port on a switch. Create a subinterface for each VLAN that can appear on the switch trunk port. If you attach the physical interface to an access port on the switch, there is no point in creating a subinterface.

- Configure ASA VLAN Subinterfaces

  Configure IPv4 Addressing for ASA Subinterface on page 276
- Configure IPv6 Addressing for ASA Subinterface on page 277
- Configure Advanced ASA Subinterface Options on page 278
- Enable the Subinterface on page 279

Configure ASA VLAN Subinterfaces

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
4. You can add a subinterface using one of the following methods:
   - Choose  > **Subinterface**
   - Click a physical interface that you want to configure and in the **Actions** pane on the right, click **New Subinterface**.
5. In the **VLAN ID** field, enter the VLAN ID between 1 and 4094.

   Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration.
6. In the **Subinterface ID** field, enter the subinterface ID as an integer between 1 and 4294967293.

   The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.
7. Continue with one of the following procedures:
   - Configure IPv4 Address for the subinterface if you intend to assign an IPv4 address to this interface.
   - Configure IPv6 Address for the subinterface if you intend to assign an IPv6 address to this interface.
   - Configure Advanced ASA subinterface. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
   - If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the Subinterface.

Configure IPv4 Addressing for ASA Subinterface

Procedure

1. In the **Creating Subinterface** dialog box, configure the following in the **IPv4 Address** tab:
   - **Type**: You can use either static IP addressing or DHCP for the interface.

     Static - Choose this option if you want to assign an address that should not change.
     - **IP Address and Subnet Mask**: Enter the interface's IP address and the subnet mask for the network attached to the interface.
     - **Standby IP Address**: If you configured high availability and are monitoring this interface for HA, also configure a standby IP address on the same subnet. This interface on the standby device uses the standby address.

       For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

     DHCP: Choose this option if the address should be obtained from the DHCP server on the network.

You can check the **Obtain Default Route** check box to get the default route from the DHCP server. You would normally check this option.

2. Click **Save** if you are done or continue with one of these procedures.
   - Configure IPv6 Address for the subinterface if you intend to assign an IPv6 address to this interface.
   - Configure Advanced ASA subinterface. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
   - If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the subinterface.

Configure IPv6 Addressing for ASA Subinterface

Procedure

---

1. In the **Creating Subinterface** dialog box, click the **IPv6 Address** tab.
2. Configure the following:
   - **State**: To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the **State** slider to enable it. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

     Note

     Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

   - **Address Auto Configuration**:

     Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

     Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

   - **Suppress RA**: Check this box if you want to suppress router advertisements. The device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

     Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

     You might want to suppress these messages on any interface for which you do not want the device to supply the IPv6 prefix (for example, the outside interface).

   - **DAD Attempts** How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses

before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- **Link-Local Address**: If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

> **Note**
>
> A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby Link-Local Address**: Configure this address if the interface connects a high availability pair of devices. Enter the link-local address of the interface on the other device, to which this interface is connected.
- **Static Address/Prefix**: If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. You can add another static address.
- **Standby IP Address**: If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

3. Click **Save** if you are done or continue with one of these procedures.
   - Configure Advanced ASA subinterface. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
   - If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the Subinterface.

Configure Advanced ASA Subinterface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

This procedure and all of the steps in it are optional.

Procedure

---

1. In the **Creating Subinterface** dialog box, click the **Advanced** tab.
2. Configure the following advanced settings:
   - **HA Monitoring**: Enable to include the health of the interface as a factor when the HA pair decides whether to fail over to the peer unit in a high availability configuration. This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.

- **Management Only**: Enable to make a data interface management only.

  A management only interface does not allow through traffic, so there is very little value in setting a data interface as a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.

- **MTU**: The default MTU is 1500 bytes. You can specify a value from 64 - 9198. Set a high value if you typically see jumbo frames on your network.
- **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.
- **MAC Address**: The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)
- **Standby MAC Address**: For use with high availability. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

3. If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Subinterface.
4. Click **Save**.

Enable the Subinterface

Procedure

---

1. Select the subinterface you want to enable.
2. Move the **State** slider at the top right of the window associated with the interface's logical name.
3. Review and deploy the changes you made.

Remove ASA Subinterface

Use the following procedure to remove an subinterface from ASA.

Procedure

---

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
4. On the **Interfaces** page, expand the physical interface linked with the subinterface you want to delete and then select that specific subinterface.
5. In the **Actions** pane located to the right, click **Remove**.
6. Confirm you want to delete the EtherChannel interface and click **Delete**.
7. Review and deploy the changes you made.

About ASA EtherChannel Interfaces

An 802.3ad EtherChannel is a logical interface (called a port-channel interface) consisting of a bundle of individual Ethernet links (a channel group) so that you increase the bandwidth for a single network. A port channel interface is used in the same way as a physical interface when you configure interface-related features.

You can configure up to 48 EtherChannels, depending on how many interfaces your model supports.

Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

See the **EtherChannel and Redundant Interfaces** chapter of ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, X, Y for more information on ASA EtherChannel interfaces.

Configure ASA EtherChannel

Use this procedure to add a new EtherChannel interface to an ASA.

Before you begin

To configure EtherChannel on ASA interface, the following prerequisites must be met:

- All interfaces in the channel group must be the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface, except for the Secure Firewall 3100, which supports different interface capacities as long as the speed is set to Detect SFP; in this case, the lowest common speed is used.
- You cannot add a physical interface to the channel group if you configured a name for it. You must first remove the name.
- You cannot add an interface part of another EtherChannel interface group, Switchport interfaces, and interfaces with subinterfaces.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
4. Choose  > **EtherChannel Interface**.
5. In the **Logical Name** field, provide a name for the EtherChannel interface.
6. In the **EtherChannel ID**, enter an integer between 1 and 8.
7. Click the drop-down button for **Link Aggregation Control Protocol** and select one of the two options:
   - **Active** –Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
   - **On**– The EtherChannel is always on, and LACP is not used. An **on** EtherChannel can only establish a connection with another EtherChannel that is also configured to be **on**.

8. Search for and select the interfaces you want to include in the EtherChannel as members. You **must** include at least one interface.

   > **Warning**
   >
   > If you add an EtherChannel interface as a member and it already has an IP address configured, Security Cloud Control removes the IP address of the member.

9. Select the **IPv4**, **IPv6**, or **Advanced** tab to configure the IP address of the subinterface.
   - Configure IPv4 Addressing for ASA EtherChannel Interface if you intend to assign an IPv4 address to this interface.
   - Configure IPv6 Addressing for ASA EtherChannel Interface if you intend to assign an IPv6 address to this interface.
   - Configure Advanced ASA EtherChannel Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

10. Move the **State** slider at the top right of the window to enable the EtherChannel interface.
11. Click **Save**.
12. Review and deploy the changes you made.

Edit ASA EtherChannel

Use this procedure to edit an existing EtherChannel on ASA.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
4. On the **Interfaces** page, select the EtherChannel interface you want to edit.
5. In the **Actions** pane located to the right, click **Edit**.
6. Modify the values you want and click **Save**.
7. Review and deploy the changes you made.

Remove ASA EtherChannel Interface

Use the following procedure to remove an EtherChannel interface from ASA.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
4. On the **Interfaces** page, select the EtherChannel interface you want to delete.
5. In the **Actions** pane located to the right, click **Remove**.
6. Confirm you want to delete the EtherChannel interface and click **Delete**.

7. Review and deploy the changes you made.

ASA system settings policy in Security Cloud Control Firewall Management

An overview of ASA system settings policy, including DNS, HTTP, SSH, NTP, logging, sysopt, and device association settings.

Introduction to ASA system settings policy

Manage your ASA device's operations and functionalities using a System Settings policy. This policy includes essential configurations like domain name services, enabling the secure copy server, message logging, and permitting VPN traffic without checking ACLs. By setting up a policy, you can ensure that your device is properly configured to maintain a secure network environment.

When configuring an ASA device, it's important to note that you have the option to manage multiple devices' settings with a shared system settings policy, or you can individually edit the settings for any single device.

Shared system settings policy

A shared system settings policy applies to multiple ASA devices in your network. It makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes made to a parameter of a shared policy affect the other ASA devices that use the policy.

Choose **Policies** > **ASA** > **System Settings**. See Create an ASA Shared System Settings Policy on page 282.

You can also modify the device-specific system settings specific to a single ASA device to override the shared system settings policy values. Choose **Security Devices** > **ASA device** > **Management** > **Settings**. See Configure or Modify Device Specific System Settings on page 290.

Create an ASA Shared System Settings Policy

Use this section to create a new shared system settings policy for ASA devices.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **System Settings**.
3. Click .
4. In the **Name** field, enter a name for the policy and click **Save**.
5. In the edit ASA shared system settings page, configure the parameters you want:
   - Configure Basic DNS Settings on page 283
   - Configure HTTP Settings on page 284
   - Set the Date and Time Using an NTP Server on page 285
   - Configure SSH Access on page 286
   - Configure System Logging on page 287
   - Enable Sysopt Settings on page 288

> **Note**
>
> - An orange dot ( ) on the corresponding parameter highlights unsaved changes.
> - The denied symbol ( ) highlights parameters that use existing local values from the device.

Configure Basic DNS Settings

You need to configure a DNS server so that the ASA can resolve host names to IP addresses. You also must configure a DNS server to use fully qualified domain names (FQDN) network objects in access rules.

Procedure

1. In the edit ASA system settings page, click **DNS** in the left pane.
2. Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

   Important

   If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

3. In the **DNS** section, click to configure servers.
   - **IP Version**: Select the IP address version you want to use.
   - **IP Address**: Specify DNS server's IP address.
   - **Interface Name**: Specify the interface where the DNS lookup should be enabled.

   > **Note**
   >
   > Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.

4. Click **Save**.
5. In the **Domain name** field, specify the domain name for the ASA.

   The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com” and specify a syslog server by the unqualified name of “jupiter,” then the ASA qualifies the name to “jupiter.example.com.”

6. In the **DNS Lookup** section, click and specify the interface name.

If you do not enable DNS lookup on an interface, then the ASA will not communicate with the DNS server on that interface. Make sure to enable DNS lookup on all interfaces that will be used to access DNS servers.

> **Note**
>
> To remove a configured interface, you can click the delete icon under **Actions**.

7. Click **Save**.

Configure HTTP Settings

To access the ASA interface for management access, you must specify the addresses of all hosts/networks which are allowed to access the ASA using HTTP. If you configure HTTP redirect to redirect HTTP connections to HTTPS automatically, you must enable an access rule to allow HTTP; otherwise, the interface cannot listen to the HTTP port.

Procedure

---

1. In the edit ASA system settings page, click **HTTP** in the left pane.
2. Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

   Important

   If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

3. Check the **Enable HTTP Server** check box to enable the HTTP server.
4. In the **Port Number** field, set the port number. The port identifies the port from which the interface redirects HTTP connections.

   > **Warning**
   >
   > If you change the HTTP port on your device, it may cause some problems with its connection to Security Cloud Control. It's important to remember this if you plan to alter any settings related to your device's network connection.

5. Click  to add HTTP information.
   - **Interface**: Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
   - **IP Version**: Select the IP address version you want to use.
   - **IP Address**: Specify the addresses of all hosts/networks that can access the ASA using HTTP.
   - **Netmask**: Specify the subnet mask for the network.

> **Note**
>
> To remove a host, you can click the delete icon under **Actions**.

6. Click **Save**.

Set the Date and Time Using an NTP Server

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The ASA chooses the server with the lowest stratum–a measure of how reliable the data is.

Time derived from an NTP server overrides any time set manually.

The ASA supports NTPv4.

Procedure

---

1. In the edit ASA system settings page, click **NTP** in the left pane.
2. Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

   Important

   If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

3. Click  to add NTP server details.
   - **IP Version**: Select the IP address version you want to use.
   - **IP Address**: Specify the NTP server's IP address.

     You cannot enter a hostname for the server; the ASA does not support DNS lookup for the NTP server.
   - **Key Id**: Enter a number between 1 and 4294967295.

     This setting specifies the key ID for this authentication key, which enables you to use authentication to communicate with the NTP server. The NTP server packets must also use this key ID.
   - **Interface Name**: Specify the interface name. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.

     NTP uses an algorithm to determine which server is the most accurate and synchronizes to it. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the ASA uses the more accurate one.
   - **Prefer**: (optional) Check the **Preferred** check box to set this server as a preferred server.

> **Note**
>
> To remove an NTP server, you can click the delete icon under **Actions**.

4. Click **Save**.

Configure SSH Access

You can enable the secure copy (SCP) server on the ASA. Only clients that are allowed to access the ASA using SSH can establish a secure copy connection.

Procedure

---

1. In the edit ASA settings policy page, click **SSH** in the left pane.
2. Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

   Important

   If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

3. Enable **Enable Scopy SSH** (secure copy SSH).
4. In the **Timeout in Minutes** field, set the timeout from 1 to 60 minutes. The default is 5 minutes. The default duration is too short in most cases, and should be increased until all pre-production testing and troubleshooting have been completed.
5. Click  and configure the following:
   - **Interface**: Specify the interface name. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
   - **IP Version**: Select the IP address version you want to use.
   - **IP Address**: Specify the addresses of all hosts/networks that can access the ASA using SSH.
   - **Netmask**: Specify the subnet mask for the network.

   > **Note**
   >
   > To remove SSH details, you can click the delete icon under **Actions**.

6. Click **Save**.

Configure System Logging

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

Security Levels

The following table lists the syslog message severity levels.

Table 19: Syslog Message Severity Levels

Level Number	Security Level	Description
0	**emergencies**	System is unusable
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only. Log at this level only temporarily, when debugging issues. This log level can potentially generate so many messages that system performance can be affected.

Note

ASA does not generate syslog messages with a severity level of zero (emergencies).

Procedure

1. In the edit ASA system settings page, click **Syslog** in the left pane.
2. Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

   Important

   If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

3. Configure the following:

- **Logging Enabled**: Enable secure logging.
- **Timestamp Enabled**: Enable to include the date and time in syslog messages.
- **Permit host down**: (Optional) Disable the feature to block new connections when a TCP-connected syslog server is down.
- **Buffer Size**: Specify the size of the internal log buffer. The allowed range is 4096 to 1048576 bytes.
- **Buffered Logging Level**: Specify which syslog messages should be sent to the internal log buffer, which serves as a temporary storage location.
- **Console Logging Level**: Specify which syslog messages should be sent to the console port.
- **Trap Logging Level**: Specify which syslog messages should be sent to the syslog server.

4. Click  to add Syslog server details.
   - **Interface Name**: Specify the interface name on which the syslog server resides. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
   - **IP Version**: Select the IP address version you want to use.
   - **IP Address**: Specify the IP address of the syslog server.
   - **Protocol**: Choose the protocol (**TCP** or **UDP**) the ASA should use to send syslog messages to the syslog server.
     - **Port**: Specify the port that the syslog server listens to for syslog messages. The allowed TCP port range is 1 to 65535, and the UDP port range is 1025 to 65535.
     - **Log messages in Cisco EMBLEM format (UDP only)**: Enables EMBLEM format logging for the syslog server with UDP only.
     - **Enable secure syslog using SSL?**: Specifies that the connection to the remote logging host should use SSL/TLS for TCP only.
   - **Reference Identity**: Specify the reference identity type to enable RFC 6125 reference identity checks on the certificate based on the previously configured reference identity object. See Configure Reference Identities for details on the reference identity object.

> **Note**
>
> To remove a Syslog server, you can click the delete icon under **Actions**.

5. Click **Save**.

Enable Sysopt Settings

The crypto map ACL bound to the outgoing interface either permits or denies IPsec packets through the VPN tunnel. IPsec authenticates and deciphers packets that arrive from an IPsec tunnel, and subjects them to evaluation against the ACL associated with the tunnel.

ACLs define which IP traffic to protect. For example, you can create ACLs to protect all IP traffic between two subnets or two hosts.

Procedure

1. In the edit ASA system settings page, click **Sysopt** in the left pane.
2. Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

   Important

   If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

3. Enable **Allow VPN traffic to bypass interface access lists** bypasses the ACL inspection.
4. Click **Save**.

Assign a Policy from the Shared System Settings Page

After configuring a shared system settings policy, assign onboarded ASA devices and deploy the settings to the devices for the changes to take effect. Any change made to the policy affects the devices that are associated with the policy.

You can also assign a policy from the device-specific settings page.

> **Note**
>
> You can associate an ASA device to only one shared system settings policy.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **System Settings**.
3. Select a shared policy and click **Edit**.
4. Click the filter appearing beside the policy name to assign devices.
5. Select the ASA devices you want to associate with the selected policy and click **OK**.

   > **Note**
   >
   > The checkboxes are ticked for devices that are already associated with the selected policy.

   If you see a red icon , it means that an error has occurred while applying the shared system settings policy to your devices. To troubleshoot the issue, click the policy on the **ASA System Settings** page and in the **Error Detected** pane, click the **Device Workflows** to get more information.

6. Review and deploy the changes you have made.

Configure or Modify Device Specific System Settings

A device-specific system settings are existing values specific to an ASA device that can be modified using Security Cloud Control. You can override the shared system settings policy values with existing device-specific values for parameters you want.

This topic describes configuring an onboarded ASA device's system settings.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select the ASA device you want and in the **Management** pane on the right, click **Settings**.

   You will see the device-specific system settings of the selected ASA device.

   > **Note**
   >
   > If the selected device is assigned with a shared system settings policy, the **Parent Policy** provides a link to open the policy. You can also assign a policy from the device-specific settings page. Select the ASA devices you want to associate with the selected policy and click **OK**

4. Configure or modify the values of the system settings you want and click **Save**.

   > **Note**
   >
   > The field descriptions for a shared and device-specific system settings remain the same. You can click the corresponding link below for more information.
   >
   > - Configure Basic DNS Settings on page 283
   > - Configure HTTP Settings on page 284
   > - Set the Date and Time Using an NTP Server on page 285
   > - Configure SSH Access on page 286
   > - Configure System Logging on page 287
   > - Enable Sysopt Settings on page 288

   You can click **Return to Security Devices** to navigate to the **Security Devices** page.

5. Click **Save** after making the changes.

> **Note**
>
> An orange dot ( ) on the corresponding parameter highlights unsaved changes.

Assign a Policy from Device-Specific Settings Page

You can also assign a policy from the device-specific settings page of an onboarded ASA device.

Procedure

---

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select the ASA device you want and in the **Management** pane on the right, click **Settings**.

   You will see the device-specific settings of the selected ASA device.

   > **Note**
   >
   > If the selected device is assigned with a shared system settings policy, the **Parent Policy** provides a link to open the policy. Select the ASA devices you want to associate with the selected policy and click **OK**

4. Click the **Parent Policy** button to assign a shared system settings policy.
5. Select a policy and click **Apply**.
6. Review and deploy the changes you have made.

Auto Assignment of ASA Devices to a Shared System Settings Policy

When onboarding a new ASA device, or checking for changes or handing out-of-band changes for existing devices, Security Cloud Control verifies whether:

- The device-specific settings match a pre-existing shared system settings policy. If there is a match, the device gets assigned to the shared system settings policy.
- The device-specific settings of the onboarded devices match each other. If they do, a new shared system settings policy gets created automatically, and devices with the same local settings are assigned to this shared policy.

> **Note**
>
> You can rename the Shared Settings policy whether it was created by the user or the system.

Filter ASA Shared System Settings Policy

If you're searching for specific shared system settings policies on the ASA System Setting page, you can use filters based on issues and usage to narrow down your search and find what you're looking for more easily.

Click **Policies** > **ASA** > **System Settings** > .

- **Issues**:
  - **Issue Detected**: Displays only the policies that have issues when applying devices to them.
  - **No issue**: Displays only the policies that are successfully applied to devices.
- **Usage**:
  - **In Use**: Displays policies that have are assigned to devices.
  - **Unused**: Displays policies that have not been assigned to any devices yet.

Disassociate Devices from Shared System Settings Policy

If an ASA device is no longer needed in the shared system settings policy, you can easily dissociate it. The device detaches from the policy when:

- Changes are made to the device-specific settings, where the corresponding setting on the shared policy is not configured to retain existing values from the device.
- Devices are detached manually from the shared system settings policy.
- Shared system settings policy is deleted from Security Cloud Control. However, this doesn't delete the device. See Delete Shared Settings Policy on page 293.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **System Settings**.
3. Select a shared policy and click **Edit**.
4. Click the filter appearing beside the policy name to detach devices.
5. Uncheck the devices you want to detach from the selected shared system settings policy and click **OK**.

> **Note**
>
> The changes are saved automatically and don't require any manual deployment.

Delete Shared Settings Policy

If you want to remove some shared settings policies, you have the option to select one or more of them and delete them. However, it's important to note that you can only delete them if they haven't been applied or committed to any devices yet.

Before you begin

Ensure the devices are dissociated from the shared settings policy you wish to delete. See Disassociate Devices from Shared System Settings Policy for more information.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **System Settings**.
3. Select a shared policy and click **Delete**.
4. Click **OK** to confirm your action.

> **Note**
>
> If you delete an ASA from Security Cloud Control, the device-specific settings and configurations will also be deleted, and the device references will be removed from the shared settings policy.

ASA routing in Security Cloud Control Firewall Management

An overview of ASA routing, including interfaces, destination networks, gateways, metrics, and traffic path validation.

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which include route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with various information. Destination or next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the next hop on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

Routing tables can also include other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used.

Routers communicate with one another and maintain their routing tables through the transmission of various messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message that is sent between routers, informs other routers of the state of the sender links. Link information can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

About ASA Static Route

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing. Generally, you must configure at least one static route: a default route for all traffic that is not routed by other means to a default network gateway, typically the next hop router.

For general information on how ASA routing concepts and CLI commands, see the following documents:

- *Static and Default Routes* chapter from ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, X,Y.
- *Static and Default Routes* chapter from CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, X,Y.

Default Route

The simplest option is to configure a default static route to send all traffic to an upstream router, relying on the router to route the traffic for you. A default route identifies the gateway IP address to which the ASA sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.

You should always define a default route.

Static Route

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. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the ASA.
- You are using a feature that does not support dynamic routing protocols.

Static Route Tracking

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the ASA goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The ASA implements static route tracking by associating a static route with a monitoring target host on the destination network that the ASA monitors using ICMP echo requests. If an echo reply is not received within a specified time period, the host is considered down, and the associated route is removed from the routing table. An untracked backup route with a higher metric is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that you choose, but you should consider using the following:

- The ISP gateway (for dual ISP support) address.
- The next hop gateway address (if you are concerned about the availability of the gateway).
- A server on the target network, such as a syslog server, that the ASA needs to communicate with.

- A persistent network object on the destination network.

Configure ASA Static Route

A static route defines where to send traffic for specific destination networks.

This section describes the steps to add a static route to an ASA device.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select a device you want to configure a static route.
4. In the **Management** pane on the right, click **Routing**.
5. Click  to add a static route.
6. You can enter a **Description** for the route.
7. Select whether the route is for an **IPv4** or **IPv6** address.
8. Configure the route properties:
   - **Interface**: Select the interface through which you want to send traffic. The gateway address needs to be accessible through this interface.

     You can use a **Null0** route to forward unwanted or undesirable traffic so the traffic is dropped. Static Null0 routes have a favorable performance profile. You can also use static null0 routes to prevent routing loops.

     The ASA CLI accepts both Null0 or null0 strings.
   - **Gateway IP**: (Not applicable to a **Null0** route) Select the network object that identifies the IP address for the gateway to the destination network. Traffic is sent to this address.
   - **Metric**: The administrative distance for the route, between 1 and 254. The default for static routes is 1. If there are additional routers between the interface and the gateway, enter the number of hops as the administrative distance.

     Administrative distance is a parameter used to compare routes. The lower the number, the higher precedence the route is given. Connected routes (networks directly connected to an interface on the device) always take precedence over static routes.
   - **Destination IP**: Select the network object(s), that identifies the destination network, that contains the host(s), that uses the gateway in this route.
   - **Destination Mask** (only for IPv4 addressing): Enter the subnet mask for the destination IP.
   - **Tracking** (only for IPv4 addressing): Enter a unique identifier for the route tracking process.
9. Click **Save**.
10. Review and deploy the changes you made, or wait and deploy multiple changes at once.

Edit ASA Static Route

You can edit the static route parameters associated with an ASA device.

> **Note**
>
> However, you cannot select a different IP version while modifying the static route. Alternatively, you can create a new static route based on your requirement.

Procedure

1. Select an ASA device you want to edit the static route.
2. In the **Management** pane on the right, click **Routing**.
3. In the routing listing page, select a route you want to modify and in the **Actions** pane on the right, click **Edit**.
4. Modify the values you want and click **Save**. See Configure ASA Static Route on page 295 for information on the routing parameters.
5. Review and Deploy the changes you made, or wait and deploy multiple changes at once.

Delete a Static Route

Before you begin

Deleting a static route may impact the connectivity to your device's local SDC or Security Cloud Control. Ensure a proper disaster recovery procedure is in place for any connectivity loss.

Procedure

1. Select an ASA device you want to delete.
2. In the **Management** pane on the right, click **Routing**.
3. In the routing listing page, select a route you want to modify and in the **Actions** pane on the right, click **Delete**.
4. Click OK to confirm the changes.
5. Review and Deploy the changes you made, or wait and deploy multiple changes at once.

API tokens

Learn how Security Cloud Control API tokens support REST API access, including how users generate, renew, revoke, and use tenant-specific JWT tokens in authorization headers.

Developers use Security Cloud Control API tokens when making Security Cloud Control REST API calls. The API token must be inserted in the REST API authorization header for a call to succeed. API tokens are "long-lived" access tokens which do not expire; however, you can renew and revoke them.

You can generate API tokens from within Security Cloud Control. These tokens are only visible immediately after they're generated and for as long as the General Settings page is open. If you open a different page in Security Cloud Control and return to the General Settings page, the token is no longer visible, although it is clear that a token has been issued.

Individual users can create their own tokens for a particular tenant. One user cannot generate a token on behalf of another. Tokens are specific to an account-tenant pair and cannot be used for other user-tenant combinations.

API Token Format and Claims

The API token is a JSON Web Token (JWT). To learn more about the JWT token format, read the Introduction to JSON Web Tokens.

The Security Cloud Control API token provides the following set of claims:

- **id** - user/device uid
- **parentId** - tenant uid
- **ver** - the version of the public key (initial version is 0, for example, **cdo_jwt_sig_pub_key.0**)
- **subscriptions** - Security Services Exchange subscriptions (optional)
- **client_id** - "**api-client**"
- **jti** - token id

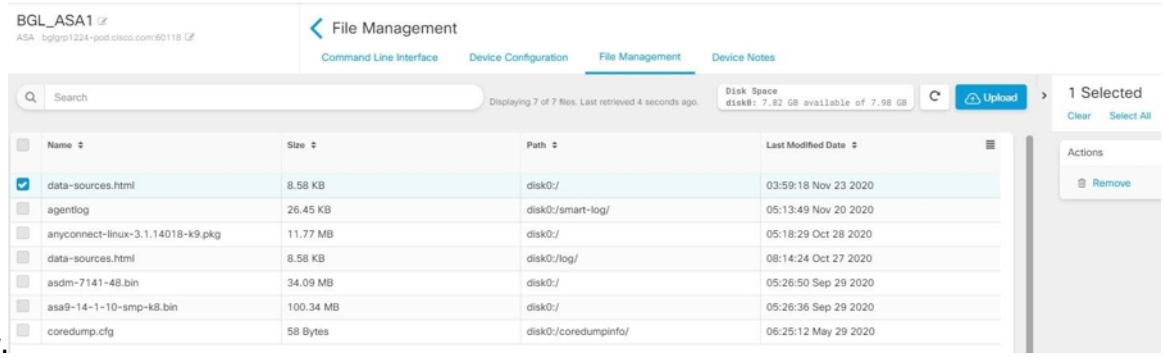
ASA file management

An overview of ASA file management, including file selection, target devices, package replacement, and cleanup tasks.

Security Cloud Control provides the file management tool to help you perform basic file management tasks such as viewing, uploading, or deleting files present on the ASA device's flash (disk0) space.

> **Note**
>
> You cannot manage files present on disk1.

The File Management screen lists all the files present on the device's flash (disk0). On a successful file upload, you can click the refresh icon to see the file. By default, this screen refreshes automatically every 10 minutes. The **Disk Space** field shows the amount of disk space on the disk0 directory.



You can upload the AnyConnect image to single or multiple ASA devices. After a successful upload, the AnyConnect image is associated with the RA VPN configuration on the selected ASA devices. This helps you to upload the newly released AnyConnect package to multiple ASA devices simultaneously.

Upload File to the Flash System

Security Cloud Control supports only URL based file upload from the remote server. The supported protocols for uploading the file are HTTP, HTTPS, TFTP, FTP, SMB, or SCP. You can upload any files such as the AnyConnect software images, DAP.xml, data.xml, and host scan image files to a single or multiple ASA device.

> **Note**
>
> Security Cloud Control doesn't upload the file to selected ASA devices if the remote server's URL path is invalid or for any issues that may occur. You can navigate to the device **Workflows** for more details.

Suppose the device is configured for High Availability, Security Cloud Control uploads the file to the standby device first, and only after a successful upload, the file is uploaded to the active device. The same behavior applies during the file removal process.

The syntax of supported protocols for uploading the file:

Protocol	Syntax	Example
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	ftp://user:NKT9g78RgRmWGHe@ftp.test.com/asa9-0-0.img
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/ filename]	scp://root:cisco123@10.10.16.6//root/events_send.py

Before You Begin

- Make sure that the remote server is accessible from the ASA device.
- Make sure that the file is already uploaded to the remote server.
- Make sure that there is a network route from the ASA device to that server.
- If FQDN is used in the URL, make sure that DNS is configured.
- The remote server's URL must be a direct link without prompting for authentication.
- If the remote server IP address is NATed, you have to provide the NATed public IP address of the remote server location.

> **Note**
>
> If you upload a file to an ASA that is configured as a peer in a failover, Security Cloud Control does not acknowledge the new file for the other peer in the failover pair and the device status changes to **Not Synced**. You must manually deploy changes to **both** devices for Security Cloud Control to recognize the file in both devices.

Upload File to a Single ASA Device

Use this procedure to upload a file to a single ASA device.

Procedure

1. In the navigation bar, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the **ASA** tab and select an ASA device.
4. In the **Management** pane on the right, click **File Management**. You can view available disk space and the files present on the ASA device.
5. Click the **Upload** button on the right.
6. In the **URL link**, specify the server's path where the file is pre-uploaded. The **Destination Path** field shows the name of the file that is being uploaded to the **disk0** directory. If you want to upload the file to a specific directory within disk0, specify its name in this field. For example, if you're going to upload a dap.xml file to the "DAPFiles" directory, specify "**disk0:/**DAPFiles/dap.xml" in the field.

   Note

   You can view the directories present in the disk0 folder by executing the **dir** command in the Security Cloud Control ASA CLI interface.

7. If the specified server path points to an AnyConnect file, the **Associate file with RA VPN Configuration** check box is enabled. **Note**: This check box is enabled only for an AnyConnect file name that follows the right naming convention, which is 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg', or 'anyconnect-mac-xxx.pkg' format. On selecting this check box, Security Cloud Control associates the AnyConnect file to the RA VPN configuration on the selected ASA device after a successful upload.
8. Click **Upload**. Security Cloud Control uploads the file to the device.
9. If you have chosen to associate the AnyConnect package with the RA VPN configuration in step 5, deploy the new RA VPN configuration to the ASA device.

Upload File to Multiple ASA Devices

Use this procedure to upload a file to multiple ASA devices at the same time.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the **ASA** tab and select multiple ASA devices to perform a bulk upload.
4. In the **Device Actions** pane on the right, click **Upload File**. Note: The **Upload File** link appears if ASA devices are online.
5. In the **URL link**, specify the server's paths where the file is pre-uploaded. The **Destination Path** field shows the name of the file that is being uploaded to the **disk0** directory. If you want to upload the file to a specific directory within disk0, specify its name in this field. For example, if you're going to upload a dap.xml file to the "DAPFiles" directory, specify "**disk0:/**DAPFiles/dap.xml" in the field.

> **Note**
>
> You can view the directories present in the disk0 folder by executing the **dir** command in the Security Cloud Control ASA CLI interface.

6. If the specified server path points to an AnyConnect file, the **Associate file with RA VPN Configuration** check box is enabled.

   > **Note**
   >
   > This check box is enabled only for an AnyConnect file name that follows the right naming convention, which is 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg', or 'anyconnect-mac-xxx.pkg' format. On selecting this check box, Security Cloud Control associates the AnyConnect file to the RA VPN configuration on the selected ASA devices after a successful upload.

7. Click **Upload**.
8. If you have chosen to associate the AnyConnect package with the RA VPN configuration in step 4, deploy the new RA VPN configuration to ASA devices.

   You can view the progress of uploading the file on individual devices. Select the ASA device, and in the **Management** pane on the right, click **File Management**. If the file upload is in progress, wait for the operation to complete.

   You don't have to deploy the configuration changes on the device.

Remove Files from ASA

You are not allowed to remove AnyConnect files associated with the RA VPN configuration. You have to disassociate the AnyConnect file from the corresponding RA VPN configuration and then remove the file from the File Management tool.

> **Note**
>
> If you upload a file to an ASA that is configured as a peer in a failover, Security Cloud Controldoes not acknowledge the new file for the other peer in the failover pair and the device status changes to **Not Synced**. You must manually deploy changes to **both** devices for Security Cloud Control to recognize the file in both devices.

The remove operation deletes the selected files permanently from the flash memory. A message appears when deleting files asking for confirmation. Use the following procedure to remove files from a selected ASA device:

Procedure

1. In the navigation bar, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the **ASA** tab and select an ASA device.

4. In the **Management** pane on the right, click **File Management**.
5. Select the files you want to remove, and under **Actions** on the right, click **Remove**. A maximum of 25 files can be selected. If Security Cloud Control fails to remove some files, you can see the device **Workflows** to determine the removed and retained files.
6. If you have chosen to remove the AnyConnect package, deploy the new RA VPN configuration to the ASA device.

Managing ASAs with pre-existing High Availability configuration

Find details about managing ASAs with pre-existing high availability configuration, including failover state, peer selection, synchronization, and upgrade workflow considerations.

Configuration Changes Made to ASAs in Active-Active Failover Mode

When Security Cloud Control) changes an ASA's running configuration with the one staged on Security Cloud Control, or when it changes the configuration on Security Cloud Control with the one stored on the ASA, it attempts to change only the relevant lines of the configuration file if that aspect of the configuration can be managed by the Security Cloud Control GUI. If the desired configuration change cannot be made using the Security Cloud Control GUI, Security Cloud Control attempts to overwrite the entire configuration file to make the change.

Here are two examples:

- You *can* create or change a network object using the Security Cloud Control GUI. If Security Cloud Control needs to deploy that change to an ASA's configuration, it overwrites the relevant lines of the running configuration file on the ASA when the change occurs.
- You *cannot* create a new ASA user using the Security Cloud Control GUI. If a new user is added to the ASA using the ASA's ASDM or CLI, when that out-of-band change is accepted and Security Cloud Control updates the stored configuration file, Security Cloud Control attempts to overwrite that ASA's entire configuration file staged on Security Cloud Control.

These rules are not followed when the ASA is configured in active-active failover mode. When Security Cloud Control manages an ASA configured in active-active failover mode, Security Cloud Control cannot always deploy all configuration changes from itself to the ASA or read all configuration changes from the ASA into itself. Here are two instances in which this is the case:

- **Changes to an ASA's configuration file made in Security Cloud Control, that Security Cloud Control does not otherwise support in the Security Cloud Control GUI, cannot be deployed to the ASA**. Also, a combination of changes made to the configuration file that Security Cloud Control does not support, along with changes made to the configuration file that Security Cloud Control does support, cannot be deployed to the ASA. In both cases, you receive the error message, "Security Cloud Control does not support replacing full configurations for devices in failover mode at this time. Please click Cancel and apply changes to the device manually." Along with the message in the Security Cloud Control interface, you see a Replace Configuration button that is disabled.
- **Out-of-band changes made to an ASA configured in active-active failover mode will not be rejected by Security Cloud Control**. If you make an out-of-band change to an ASA's running configuration, the ASA gets marked with "Conflict Detected" on the **Security Devices** page. If you review the conflict and try to reject it, Security Cloud Control blocks that action. You receive the message, "Security Cloud Control does not support rejecting out-of-band changes for this device. Either this device is running an unsupported software version or is a member of a active/active failover pair. Please proceed to accept the out-of-band changes by clicking Continue."

> ⚠ **Caution**
>
> If you find yourself having to accept out-of-band changes from the ASA, any configuration changes staged on Security Cloud Control, but not yet deployed to the ASA, will be overwritten and lost.

Security Cloud Control does support configuration changes made to an ASA in failover mode when those changes are supported by the Security Cloud Control GUI.

Manage ASA configuration files

Learn how to manage ASA configuration files, including configuration versions, comparison results, restore choices, and troubleshooting checks.

ASA stores their configurations in a single configuration file. You can view the device configuration file on Security Cloud Control Firewall Management and perform a variety of operations on it depending on the device.

View a Device's Configuration File

The ASA stores the entire configuration in a single configuration file. You can view the configuration file using Security Cloud Control.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the ASA device type tab.
4. Select the device or model whose configuration it is you want to view.
5. In the **Management** pane on the right, click **Configuration**.
   The full configuration file is displayed.

Configure DNS on ASA

Learn how to configure DNS on ASA, including DNS, HTTP, SSH, NTP, logging, sysopt, and device association settings.

Use this procedure to configure a domain name server (DNS) on each of your ASAs.

Prerequisites

- The ASA must be able to reach the internet.
- Before you begin, gather this information:
  - The name of the ASA interface that can reach the DNS server; for example, inside, outside, or dmz.
  - The IP address of the DNS server your organization uses. If you don't maintain your own DNS server, you can use Cisco Umbrella. The IP address for Cisco Umbrella is 208.67.220.220.

Procedure

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the **ASA** tab and select all the ASAs on which you want to configure DNS.
4. In the Actions pane to the right, select **Command Line Interface**.
5. Click the CLI macro favorites star.
6. Select the **Configure DNS** macro in the Macros panel.
7. Se;ect **>_View Parameters** and in the parameters column, fill in the values for these parameters:
   - IF_Name - The name of the ASA interface that can reach the DNS server.
   - IP_ADDR - The IP address of the DNS server your organization uses.
8. Click **Send to devices**.

ASA command line interface

An overview of ASA command line interface, including interface names, security levels, IP addressing, VLANs, and enablement options.

You can use the Security Cloud Control Firewall Management command line interface (CLI) for managing or troubleshooting the ASA and other device types.

For more information, see Use the Security Cloud Control Command Line Interface Tool (CLI) on page 861.

Configure ASA Using Security Cloud Control CLI

You can configure an ASA device by running the CLI commands in the CLI interface provided in Security Cloud Control. See ASA command line interface on page 303.

Add a New Logging Server

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts.

For more information, see the 'Monitoring' section of the 'Logging' chapter in the CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide of the ASA version you are running.

Configure the DNS Server

You need to configure DNS servers so that the ASA can resolve host names to IP addresses. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

For more information, see the 'Basic Settings' chapter of the 'Configure the DNS Server' section in CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide of the ASA version you are running.

Add Static and Default Routes

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing.

For more information, see the 'Static and Default Routes' chapter of CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide.

Configure Interfaces

You can configure the management and data interfaces using CLI commands. For more information, see the 'Basic Interface Configuration' chapter of CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide.

ASA Bulk CLI Use Cases

The following cases are possible workflows you may experience when using Security Cloud Control's bulk CLI function for ASA devices.

Show all users in the running configuration of an ASA and then delete one of the users

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device.
3. Click the **ASA** tab.
4. Search and filter the device list for the devices from which you want to delete the user and **select** them.

   > **Note**
   >
   > Make sure that the devices you choose are synced. Only the following commands are allowed when the device is not synced: `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `copy`, and `write`.

5. Click **>_Command Line Interface** in the details pane. Security Cloud Control lists the devices you chose in the My List pane. If you decide to send the command to fewer devices, uncheck devices in that list.
6. In the command pane, enter `show run | grep user` and click **Send.** All the lines in the running configuration file that contain the string user will be displayed in the response pane. The Execution tab opens to display the devices on which the command was executed.
7. Click the By Response tab and review the responses to determine which devices have the user that you want to delete.
8. Click the My List tab and select the list of devices from which you want to delete the user.
9. In the command pane, enter the no form of the user command to delete user2 and then click **Send**. For the sake of this example, you are going to delete user2:

   ```
   no user user2 password reallyhardpassword privilege 10
   ```

10. Look in the history panel for the instance of the `show run | grep user` command, you used to search for the user name. Select that command, look at the list of devices in the Execution list and select **Send**. You should see that the username has been deleted from the devices you specified.
11. If you are satisfied that you have deleted the correct users from the running configuration and that the correct users remain in the running configuration:
    a. Select the `no user user2 password reallyhardpassword privilege 10` command from the history pane.
    b. Click the **By Device** tab and click **Execute a command on these devices**.
    c. In the command pane, click **Clear** to clear the command pane.

d. Enter the command `deploy memory` and click **Send**.

Find all SNMP configurations on selected ASAs

This procedure shows you all the SNMP configuration entries in the running configuration of the ASA.

Procedure

---

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device.
3. Click the **ASA** tab.
4. Filter and search for the devices on which you want to analyze the SNMP configuration in the running configuration and **select** them.

> **Note**
>
> Make sure that the devices you choose are synced. Only the following commands are allowed when the device is not synced: `show, ping, traceroute, vpn-sessiondb, changeto,` and `dir`.

5. Click **Command Line Interface** in the details pane. The devices you chose are in the My List pane. If you decide to send the command to fewer devices, uncheck devices in the list.
6. In the command pane, enter `show run | grep snmp` and click **Send.** All the lines in the running configuration file that contain the string snmp will be displayed in the response pane. The Execution tab opens to display the devices on which the command was executed.
7. Review the command output in the response pane.

ASA Command Line Interface Documentation

Security Cloud Control fully supports the ASA command line interface. We provide a terminal-like interface within Security Cloud Control for users to send ASA commands to single devices and multiple devices simultaneously. The ASA command line interface documentation is extensive. Rather than recreating parts of it in the Security Cloud Control documentation, here are pointers to the ASA CLI documentation on Cisco.com.

ASA Command Line Interface Configuration Guides

Starting with ASA version 9.1, the ASA CLI Configuration Guide is broken into three separate books:

- CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide
- CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide
- CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide

You can reach the ASA CLI Configuration Guides on Cisco.com by navigating, Support > Products by Category > Security > Firewalls > ASA 5500 > Configure > Configuration Guides.

A Few Specific ASA Command Line Interface Configuration Guide Sections

Filtering show and more Command Output. You can learn about filtering show command output by using regular expressions in CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide under Filter show and more Command Output.

ASA Command Reference

The ASA Command Reference Guide is an alphabetical listing of all the ASA commands and their options. The ASA command reference is not version specific. It is published in four books:

- Cisco ASA Series Command Reference, A - H Commands
- Cisco ASA Series Command Reference, I - R Commands
- Cisco ASA Series Command Reference, S Commands
- Cisco ASA Series Command Reference, T - Z Commands and IOS Commands for the ASASM

You can reach the ASA Command Reference Guides on Cisco.com by navigating, Support > Products by Category > Security > Firewalls > ASA 5500 > Reference Guides > Command References > ASA Command References.

Manage the Device Configuration

The ASA stores its configuration in a single configuration file. You can view the configuration file on Security Cloud Control and perform a variety of operations on it.

Compare ASA Configurations Using Security Cloud Control

Use this procedure to compare the configurations of two ASAs.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the ASA device or the **Templates** tab to locate the ASA model device.
3. Click the **ASA** tab.
4. Filter your device list for the devices you want to compare.
5. Select two of your ASAs. Their status does not matter. You are comparing the configurations of the ASAs stored on Security Cloud Control.
6. In the Device Actions pane on the right, click **Compare.**
7. In the Comparing Configurations dialog, click **Next** and **Previous** to skip through the differences, highlighted in blue, in the configuration files.

Restore an ASA Configuration

If you make a change to an ASA's configuration, and you want to revert that change, you can restore an ASA's past configuration. This is a convenient way to remove a configuration change that had unexpected or undesired results.

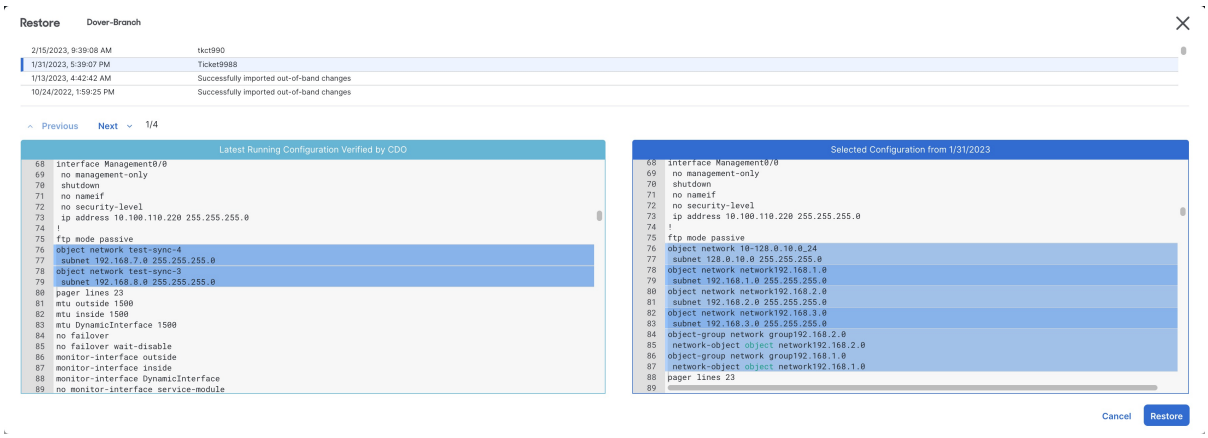
About Restoring an ASA Configuration

Review these notes before restoring a configuration:

- Security Cloud Control compares the configuration you choose to restore with the last known configuration deployed to the ASA, it does not compare the configuration you choose to restore with a configuration that is staged but not deployed to the ASA. If you have any undeployed changes on your ASA and you restore a past configuration, the restore process will overwrite your undeployed changes and you will lose them.

- Before you can restore a past configuration, the ASA can be in a Synced or Not Synced state but if the device is in a Conflict Detected state, the conflict must be resolved before you restore a past configuration.
- Restoring a past configuration overwrites all intermediate deployed configurations changes. For example, restoring the configuration from 1/31/2023 in the list below overwrites the configuration changes made on 2/15/2023.
- Clicking the Next and Previous buttons will move you through the configuration file and highlight the configuration file changes
- If you originally applied a change request label to your configuration changes, that label appears in the Restore Configuration list.

Figure 1: ASA Restore Configuration Screen



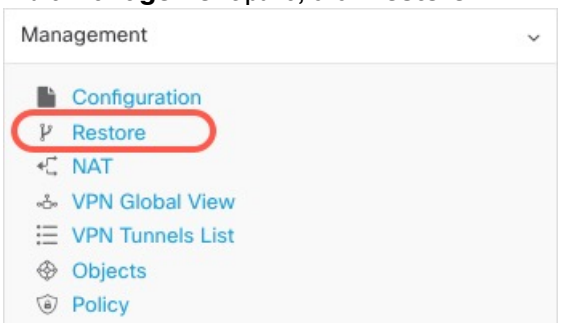
How Long are Configuration Changes Kept?

You can restore an ASA configuration that is 1 year old or less. Security Cloud Control restores configuration changes logged in its changelog. The change log records changes every time a configuration change is written to or read from an ASA. Security Cloud Control stores 1 year's worth of changelogs and there is no limitation on the number of the backups made within the previous year.

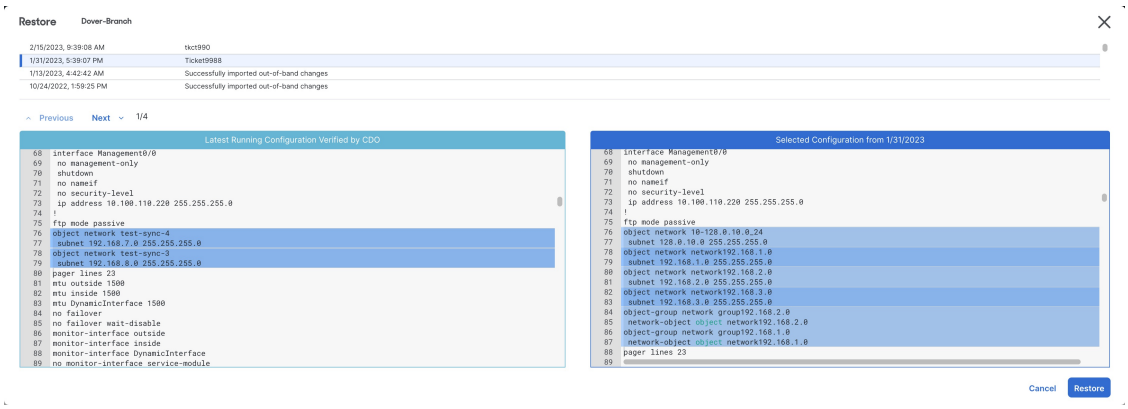
How to Restore an ASA Configuration

Procedure

1. In the left pane, click **Security Devices**.
2. Click the ASA tab.
3. Select the ASA whose configuration it is you want to restore.
4. In the **Management** pane, click **Restore.**



5. In the **Restore** page, select the configuration you want to revert to.



For example, in the picture above, the configuration from 1/31/2023 is selected.

6. Compare the "Latest Running Configuration Verified by Security Cloud Control" and the "Selected Configuration from <*date*>" to ensure you want to restore the configuration displayed in the Selected Configuration from <*date*> window. Use the Previous and Next to compare all the changes.
7. Click **Restore,** this stages the configuration in Security Cloud Control. In the **Security Devices** page, you see that the configuration status of the device is now "Not Synced."
8. Click **Deploy Changes...** in the right-hand pane to deploy the changes and sync the ASA.

Troubleshooting

How do I recover changes I lost but wanted to keep?

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the ASA tab.
4. Select the required device.
5. Click **Change Log** in the right pane.
6. Review the changes in the change log. You may be able to reconstruct your lost configurations from those records.

View a Device's Configuration File

The ASA stores the entire configuration in a single configuration file. You can view the configuration file using Security Cloud Control.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the ASA device type tab.
4. Select the device or model whose configuration it is you want to view.
5. In the **Management** pane on the right, click **Configuration**.
   The full configuration file is displayed.

Edit a Complete Device Configuration File

For these devices, you can view the device configuration file on Security Cloud Control and perform a variety of operations on it depending on the device.

Currently, only ASA configuration files can be edited directly using Security Cloud Control.

> ⚠ **Caution**
>
> This procedure is for advanced users who are familiar with the syntax of the device's configuration file. This method makes changes directly to copy of the configuration file stored on Security Cloud Control.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the **ASA** tab.
4. Select the device whose configuration it is you want to edit.
5. In the **Management** pane on the right, click **Configuration**.
6. In the **Device Configuration** page, click **Edit**.
7. Click the editor button on the right and select the **Default** text editor, **Vim**, or **Emacs** text editors.
8. Edit the file and save the changes.
9. Return to the **Security Devices** page and preview and deploy the change.

13 Secure Firewall ASA Security Policy Management

Topics:

- Manage security policies in Security Cloud Control Firewall Management
- Manage ASA network security policy
- Compare ASA network policies
- Hit rates
- Search and filter ASA network rules in the access list
- Shadowed rules

Manage security policies in Security Cloud Control Firewall Management

Learn how to manage security policies in Security Cloud Control Firewall Management for firewalls, including rule order, interface assignment, logging, search, and deployment considerations.

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use Security Cloud Control to configure security policies on many different types of devices.

Manage ASA network security policy

Learn how to manage ASA network security policy, including rule order, interface assignment, logging, search, and deployment considerations.

The ASA network security policy includes access control lists (ACLs) that determine whether to permit or deny traffic from accessing another network through the ASA firewall. This section outlines the steps to create an ASA access list and configure access rules within it. It also details the steps to assign an interface to an access control list and share it among other ASA devices managed by Security Cloud Control Firewall Management.

About ASA Access Control Lists and Access Groups

ASA Access Control Lists

Access control lists (ACLs) are used to identify traffic flows based on various characteristics such as source and destination IP address, IP protocol, ports, source, and other parameters.

The following is an access list sample:

```
access-list ACL extended permit ip any any
```

`ACL` is the name of the access list.

You can avoid the creation of the same access list on multiple devices individually, and instead create a single access list and share it across multiple ASA devices. Changes made to the shared access list automatically apply to all the devices to which the ACL is assigned. You also have the option to copy the access list to other ASA devices as needed.

Access Rules

An access list includes access rules that permit or deny traffic flow to a network based on specific characteristics such as source and destination IP addresses, IP protocol, port number, and security group tags.

ASA Access Groups

An access group is a specific association that is established when an access list is assigned to a device interface configured for traffic flow in any direction. The access list contains specific rules that either permit or deny traffic passing through the device interface.

The following is an access group sample that is created when a device interface is assigned to an access list.

```
access-group ACL out interface giginterface0
```

`ACL` is the name of the access list and `giginterface0` is the logical name of the device interface that is assigned to the access list.

> **Note**
>
> To use API endpoints to manage your ASA access groups, see Get Access Groups on the Cisco DevNet website.

Create an ASA Access List

When configuring an access list on an ASA firewall, a rule is automatically created to allow traffic from a source to a destination outside your network. You can create additional rules and assign the access list to an interface to regulate the traffic network.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. Click **Create Access List**.
5. In the **Name** field, enter a name for the access list and click **Save**.

   > **Note**
   >
   > You cannot have two access lists with the same name on a device.

6. Click **Save**.

   Security Cloud Control creates an access group and a default rule that permits all traffic.

   You can now add new rules to the access list. See Add a Rule to an ASA Access List on page 313.

   To assign interfaces and traffic directions to the access list, see Assign Interfaces to ASA Access Control List on page 316.

Add a Rule to an ASA Access List

You can add rules in ascending order by rule number. Packets will be verified against the rules in the sequence in which the rules were created, with the first rule taking precedence, followed by subsequent rules. You can adjust the position of any rule, if required.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, select an access list that you want.
5. Click the **Add Rule** () icon that is displayed on the right.

> **Note**
>
> In the ordered list, hover over the desired position and click **Add Rule Here**.

6. In the **New Access Rule** window, provide the following information:
   - **Order**: Select where you want to insert the rule in the ordered list of rules. Rules are applied on a first-match basis and prioritized by position in the list of rules from 1 to last.
   - **Action**: Specify whether you are allowing (permitting) the described traffic or are blocking (dropping) it.
   - **Protocol**: Specify the protocol of the traffic, such as IP, TCP, UDP, ICMP, or ICMPv6. The default is IP, but you can select a more specific protocol to target traffic with more granularity.
   - **Source/Destination**: Define the source (originating address) and destination (target address of the traffic flow). You typically configure the IPv4 address of hosts or subnets, which you can represent with network object groups. You can assign only one object to the source or destination.

     To create a new network object or group, see Create or Edit ASA Network Objects and Network Groups.
   - **Port**: Select the port object that pairs a service type, such as TCP or UDP, and a port number or a range of port numbers.
   - **SGT Group**: Assign the security group you want from the list. By default, the value is **Any**. See Security Group Tags in ASA Policies.
   - **Time Range**: Define a time range for ASA network policies to allow access to networks and resources based on time of day.

     See ASA Time Range Objects.
   - **Logging**: Activity resulting from a network policy rule is not logged by default. You can activate logging for individual rules. See Log Rule Activity.
7. Click **Save**.

   The rule is added to the access list and set to **Active** state.
8. Review and deploy the changes you made now, or wait and deploy multiple changes.

About System Log Activity

Learn how to configure system log activity for rules, including syslog severity levels, logging frequency, and interval settings used to monitor and analyze rule activity.

When you set up a new rule, you can specify how often and at what severity level you want to collect its activity. To do this, you can select the corresponding severity levels and then choose the frequency of data collection. This will ensure that you have the necessary information to monitor and analyze the activity generated by your rules.

> **Note**
>
> ASA does not generate syslog messages with a severity level of zero (emergencies).

You have the option to adjust the logging interval, which indicates how frequently the log records are updated. This interval is measured in seconds and can be set from 1 to 600. By default, the interval is set to 300 seconds. This interval value is also utilized as a timeout period for removing an inactive flow from the cache that collects drop statistics.

Table 20: Log Rule Activity

Security Level	Description
emergencies	System is unusable.
alert	Immediate action is needed.
critical	Critical conditions.
error	Error conditions.
warning	Warning conditions.
notification	Normal but significant conditions.
informational	Informational messages only.
debugging	Debugging messages only.

Deactivate Rules in an Access Control List

When you create a new rule in an access control list, it is activated by default. However, you can temporarily deactivate individual rules to optimize traffic flow, resolve conflicts, or isolate issues.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, choose the access control list you want.
5. In the rule list, check the corresponding rule check box that you want.
6. In the selected row, slide the **Active** setting off.
7. Review and deploy the changes you made now, or wait and deploy multiple changes.

About Security Group Tags in ASA Policies

If you onboard an ASA that uses security group tags (SGT) in its access control rules, Security Cloud Control allows you to edit the rules that use SGT groups and manage the policies that have these rules. However, you cannot create SGT groups or edit them using the Security Cloud Control GUI. To create or edit SGT groups, you must use ASA's Adaptive Security Device Manager (ASDM) or the CLI available in Security Cloud Control.

In Security Cloud Control's object page, when looking at the details of SGT groups, you'll see that those objects are identified as noneditable, system-provided objects.

Security Cloud Control administrators can perform these tasks on ACLs and ASA policies that contain SGT groups:

- Edit all aspects of ACLs except the source and destination security groups.
- Copy a policy containing SGT groups from one ASA to another.

For detailed instruction, on configuring Cisco TrustSec using the command line interface, see the "ASA and Cisco TrustSec" chapter of the ASA CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide pertaining to your ASA release.

Assign Interfaces to ASA Access Control List

When you assign ASA interfaces to access control list, the device establishes a specific association between the list and interfaces. The rules that are associated with access control list are applied only to the interfaces through which the traffic flows in the specified directions.

You can only assign one access list per interface for a single traffic flow direction.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, choose an access list.
5. In the **Actions** pane displayed on the right, click **Assign Interfaces**.
6. From the **Interface** drop-down list, choose an interface.
7. From the **Direction** drop-down list, specify the direction for applying the selected access list.

   The designated access list is applied to the interface through which traffic flows in the specified direction. This access list can be applied to multiple interfaces and directions.

   To apply the access list to all the interfaces on the ASA device, see Create an ASA Global Access List on page 316.
8. Click **Save**.
9. Review and deploy the changes you made now, or wait and deploy multiple changes.

Create an ASA Global Access List

Global access policies are network policies that are applied to all the interfaces on an ASA. These policies are only applied to inbound network traffic. You can create a global access policy to ensure that a set of rules is applied uniformly to all the interfaces on an ASA.

Only one global access policy can be configured on an ASA. However, a global access policy can have more than one rule assigned to it, just like any other policy.

This is the order of rule-processing on the ASA:

1. Interface access rules
2. Bridge Virtual Interface (BVI) access rules
3. Global access rules
4. Implicit deny rules

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, choose an access list.
5. In the **Actions** pane displayed on the right, click **Assign Interfaces**.
6. Check the **Create as a global access list** check box.
7. Click **Save**.
8. Review and deploy the changes you made now, or wait and deploy multiple changes.

Share an ASA Access Control List with Multiple ASA Devices

Sharing access policies in network security effectively improves efficiency, consistency, and centralized management, leading to an overall improved security posture. To share an access control list across ASA devices, create an access control list and define access rules on a single ASA device and then share it with the desired ASA devices rather than configuring them separately. This ensures consistency in the network and reduces the risk of misconfigurations. Additionally, shared access control lists provide scalability because networks grow and evolve by allowing you to manage access control lists for increasing users and ASA devices.

Keep the following points in mind:

- Access control list rules are shared, but the interfaces are not included.
- Sharing an access control list with other ASA devices will overwrite any existing access control lists with the same name.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, choose an access control list.
5. In the **Actions** pane that is displayed on the right, click **Share**.
6. Select the ASA devices by checking the corresponding check box and click **Save**.

   In the **Device Relationships** pane displayed on the right, the ASA devices that share the selected access control list are displayed.
7. Review and deploy the changes you made now, or wait and deploy multiple changes.

Copy an ASA Access Control List to Another ASA

An ASA access control list can be easily copied to another Security Cloud Control-managed device in the same tenant. After copying an access list file to a target ASA device, any further changes made to the access list won't be automatically applied to the target device. This is different from access control list sharing feature, where changes are automatically applied.

Keep the following points in mind:

- You cannot copy an access list to a target device if that device already has another access list with the same name.

- You cannot copy an access list if another access list on the target device is associated with the same interface and direction.
- You cannot only copy an access list to a disabled interface on the target device.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, choose an access list.
5. In the **Actions** pane on the right, click **Copy**.
6. Select the target device to which you want to copy the access list.
7. Choose an interface and specify the direction for applying the selected access list.

   The designated access list is applied to the interface through which traffic flows in the specified direction. This access list can be applied to multiple interfaces and directions.

   To apply the access list to all the interfaces on the selected target, see Create an ASA Global Access List on page 316.
8. Click **Copy**.

   A message appears at the bottom right corner on the Security Cloud Control screen on a successful copy.
9. Review and deploy the changes you made now, or wait and deploy multiple changes.

Copy a Rule Within or Across ASA Access Lists and Devices

You can copy an access control rule in the following ways:

- Within the same access list.
- From one access list to another, either within the same ASA device or across different ASA devices.

> **Note**
>
> The paste operation fails if you attempt to add a rule that already exists in the access list.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, select an access list that you want.
5. Select a rule by clicking the corresponding check box and in the **Actions** pane on the right, click **Copy**.
6. Perform the following:

- To paste the rule within the same access list, hover the mouse pointer in the desired position until you see the **Paste Rule Here** option and click it. The Add/Edit rule dialog box is displayed, allowing you to modify the copied rule, as identical rules are not permitted in the same access list.
- To paste the rule within the same ASA device, from the **Selected Access List** drop-down list, select an access list you want.
- To paste the rule to a different ASA device, in the left pane, go to **Security Devices** > select an ASA device > **Policy** > **Selected Access List**.

7. To paste the copied rule in the desired position, select a rule that comes after where you want the new rule to be. In the **Actions** pane on the right, click **Paste**. The copied rule will be inserted before the selected rule.

   You can use the **Move Up** and **Move Down** buttons to position the rule as needed.

   Note

   Alternatively, you can hover over a desired position in the rule listing table until you see **Paste Rule Here**, and then click it.

Unshare a Shared ASA Access Control List

If the rules governing the interface handling your network become outdated, you can unshare the access control list from the devices currently linked. Unsharing an ASA device from the shared access control list will not have any impact on other ASA devices currently sharing this list.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, choose an access list.
5. In the **Actions** pane on the right, click **Share**.
6. Uncheck the ASA devices that share the selected access list and click **Save**.
7. Review and Deploy the changes you made now, or wait and deploy multiple changes.

View ASA Access Policies Listing Page

The ASA access policy listing page shows a comprehensive overview of all access lists associated with the ASA devices that have been onboarded to the Security Cloud Control tenant.

Note

Click the filter ( ) button, then click **Filter by Device** to search for policies that are either shared across multiple ASA devices or specific to a single ASA device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **Access Policies**.

   The page provides the following information:

   - **Name**: The name of the access list.
   - **Device**: The corresponding ASA devices associated with each access list. Additionally, for access lists that are shared across multiple devices, it displays a list of all ASA devices that use the shared access list.

     Click the button to view the ASA devices associated with the selected access list.

     To navigate to the policy page of the selected device, click **View Policies**. You can create or edit an access list.

     To return to this page, click **ASA Access Policies**.
   - **Interfaces**: The network interfaces to which each access list is assigned.
3. To view the ASA devices associated with an access list, click the corresponding button in the **Device** column.
4. To navigate to the policy page of the selected device, click **View Policies**. You can create or edit an access list.
5. To return to the policy listing page, in the top-left corner, click **← ASA Access Policies**.

Global Search of ASA Access Lists

Use the global search functionality to search the following in your Security Cloud Control tenant:

- ASA devices and all their associated access lists.
- Access lists or shared access lists and their occurrences across all onboarded ASA devices.

See more: global search.

Rename an ASA Access Control List

It is possible to modify the name of an access list to suit your specific needs. Whether you want to rename a global access list or a shared access control list, it is a straightforward process. If the access list is shared, changing its name updates the name on all the other devices where the shared access control list is used. Remember that the updated name will only reflect after the configuration is deployed to those devices.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.

4. From the **Selected Access List** drop-down list, choose an access list that you want to rename.
5. Click the **Rename** ( ) icon in the right pane.
6. Click the **Save** ( ) button.
7. Review and deploy the changes you made now, or wait and deploy multiple changes.

Delete a Rule from an ASA Access Control List

You can remove access rules from the access list, but at least one rule must remain for the list to exist.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane on the right, click **Policy**.
4. Click an access list and select the rules to be deleted.
5. In the **Actions pane** on the right, click **Remove**.
6. Review and deploy the changes you made now, or wait and deploy multiple changes at once.

Delete an ASA Access Control List

This procedure can be used to delete the access control list, shared access list, or a global access list. Deleting a shared access list from one device does not impact other devices where the access list is in use. On those devices, the access list persists as a local access list.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab and select an ASA device by checking the corresponding check box.
3. In the **Management** pane displayed on the right, click **Policy**.
4. From the **Selected Access List** drop-down list, choose an access list you want to delete.
5. In the **Actions** pane on the right, click **Delete**.
6. Review and deploy the changes you made now, or wait and deploy multiple changes at once.

Compare ASA network policies

Learn how to compare ASA network policies, including rule order, interface assignment, logging, search, and deployment considerations.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **Access Policies**.
3. Click **Compare** in the top right corner of the viewer.
4. Select up to two policies to compare.

5. Click **View Comparison** at the bottom of the viewer. This will bring up the comparison viewer. When you are finished, click **Done** and then **Done Comparing**.

Hit rates

An overview of hit rates for ASA devices, including rule usage counts, policy review, and cleanup decisions.

Security Cloud Control enables you to evaluate the outcome of policy rules, on top of secure and scalable orchestration of policies, providing a simple visualization for more accurate policy analysis and an immediate, actionable pivot to root cause, all in a single pane from the cloud. The Hit Rates feature enables you to:

- Eliminate obsolete and never-matched policy rules, increasing security posture.
- Optimize firewall performance by instantly identifying bottlenecks as well as ensuring correct and efficient prioritization is enforced (for example, most triggered policy rule is prioritized higher).
- Maintain a history of Hit Rates information, even upon device or policy rule reset, for a configured data retention period (1 year).
- Strengthen validation of suspected shadow and unused rules based on actionable information. Removing doubt about update or delete.
- Visualize policy rule usage in the context of the entire policy, leveraging predefined time intervals (day, week, month, year) and scale of actual hits (zero, >100, >100k, etc.) to evaluate impact on packets traversing the network.

View Hit Rates of ASA Policies

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **System Settings**.
3. Click the filter icon and pin it open.
4. In the Hits area, click the various hit count filters to display which policies are being hit more or less often than others.

Search and filter ASA network rules in the access list

An overview of search and filter ASA network rules in the access list, including rule order, interface assignment, logging, search, and deployment considerations.

Search

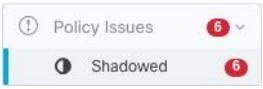
Use the search bar to search for names, keywords, or phrases in the names of the rules within the access list. Search is not case-sensitive.

Filter

Use the filter sidebar to find network policy issues. Filtering is not additive, each filter setting acts independently of the other.

Policy Issues

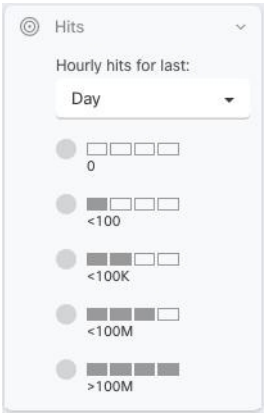
Security Cloud Control identifies network policies that contain shadow rules. The number of policies that contain shadow rules is indicated in the **Policy Issues** filter:



Security Cloud Control marks shadowed rules and network policies that contain them with the shadow badge shadow_badge.png on the network policies page. Click Shadowed to view all the policies containing shadow rules. See Shadow Rules for more information.

Hits

Use this filter to find rules across the access lists that have been triggered a number of times over a specified period.



Filter Use Cases

Find all rules that have zero hits

If you have rules without any hits, you can edit them to make them more effective or simply delete them.

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select 0 hits.

Find out how often rules in a network policy are being hit

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select the different hits filters to see what category the different rules fall into.

Filter network policies by hit rate

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.

3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select the different hit rate categories. Security Cloud Control displays the rules that are getting hit at the rate you specify.

Shadowed rules

An overview of shadowed rules for ASA devices, including rule analysis, affected policies, conflict details, and remediation steps.

A network policy with shadowed rules is one in which at least one rule in the policy will never trigger because a rule that precedes it prevents the packet from being evaluated by the shadowed rule.

For example, consider these network objects and network rules in the "example" network policy:

```
object network 02-50
range 10.10.10.2 10.10.10.50
object network 02-100
range 10.10.10.2 10.10.10.100
```

```
access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

No traffic is evaluated by this rule,

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

because the previous rule,

```
access-list example extended deny ip any4 object 02-50
```

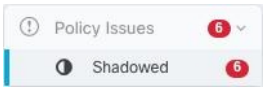
denies any ipv4 address from reaching any address in the range 10.10.10.2 - 10.10.10.50.

Find Network Policies with Shadowed Rules

To find network policies with shadowed rules, use the network policies filter:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **Access Policies**.
3. Click the filter icon at the top of the ASA Access Policies table.
4. In the Policy Issues filter, check **Shadowed** to view all the policies with shadowed rules.



Resolve Issues with Shadowed Rules

This is how Security Cloud Control displays the rules described in the "example" network policy above:



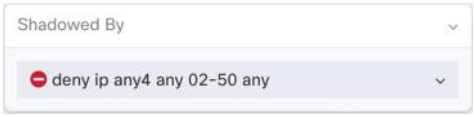
The rule on line 1 is marked with a shadow warning badge ⚠ because it's shadowing another rule in the policy. The rule on line 2 is marked as being shadowed ◑ by another rule in the policy. The action for the rule on line 2 is grayed-out because it's entirely shadowed by another rule in the policy. Security Cloud Control is able to tell you which rule in the policy shadows the rule in line 2.

The rule on line 3 can only be triggered some of the time. This is a partially shadowed rule. Network traffic from any IPv4 address trying to reach an IP address in the range 10.10.10.2-10.10.10.50 would never be evaluated because it would have already been denied by the first rule. However, any IPv4 address attempting to reach an address in the range 10.10.10.51-10.10.10.100 would be evaluated by the last rule and would be permitted.

> **Caution**
>
> Security Cloud Control does not apply a shadow warning badge ⚠ to partially shadowed rules.

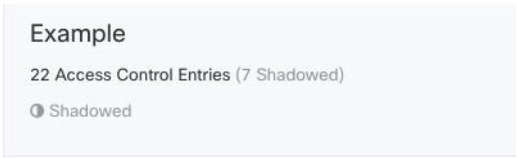
Procedure

1. Select the shadowed rule in the policy. In the example above, that means clicking on line 2.
2. In the rule details pane, look for the **Shadowed By** area. In this example, the **Shadowed By** area for the rule in line 2 shows that it is being shadowed by the rule in line 1:



3. Review the shadow*ing* rule. Is it too broad? Review the shadow*ed* rule. Do you really need it? Edit the shadow*ing* rule or delete the shadow*ed* rule.

> **Note**
>
> By deleting shadowed rules, you reduce the number of access control entries (ACEs) on your ASA. This frees up space for the creation of other rules with other ACEs. Security Cloud Control calculates the number of ACEs derived from all the rules in a network policy and displays that total at the top of the network policy details pane. If any of the rules in the network policy are shadowed, it also lists that number.



Security Cloud Control also displays the number of ACEs derived from a single rule in a network policy and displays that information in the network policy details pane. Here is an example of that listing:



4. Determine which devices use the policy by looking in the Devices area of the network policy details pane.
5. Open the **Security Devices** page and **Deploy Changes** back to the devices affected by the policy change.

14 Monitor Secure Firewall ASA Events

Topics:

- About Security Analytics and Logging (SAL SaaS) for ASA devices
- Implement secure logging analytics (SaaS) for ASA devices
- Send ASA syslog events to the Cisco Cloud using a Security Cloud Control macro
- Requirement: send ASA syslog events to the Cisco cloud using the command line interface
- NetFlow secure event logging (NSEL) for ASA devices
- Parsed ASA syslog events

This chapter covers information on how to share events from your Secure Firewall ASA and view them in Security Cloud Control.

About Security Analytics and Logging (SAL SaaS) for ASA devices

An overview of security analytics and logging (sal SaaS) for ASA, including event details, device status, reporting views, and follow-up actions.

Security Analytics and Logging (SaaS) allows you to capture all syslog events and Netflow Secure Event Logging (NSEL) from your ASA and view them in one place in Security Cloud Control .

The events are stored in the Cisco cloud and viewable from the Event Logging page in Security Cloud Control where you can filter and review them to gain a clear understanding of what security rules are triggering in your network. The **Logging and Troubleshooting** package gives you these capabilities.

Licensing

To configure this solution you need the following accounts and licenses:

- Security Cloud Control : You must have a Security Cloud Control tenant.
- **Secure Device Connector** : There is no separate license for a Secure Device Connector.
- **Secure Event Connector** : There is no separate license for a Secure Event Connector.
- **Secure Logging Analytics (SaaS)** : See Security Analytics and Logging licenses on page 920 .
- **Adaptive Security Appliance (ASA)** : Base license or higher.

Next step

Go to Implementing Secure Logging Analytics (SaaS) for ASA Devices

A Security Analytics and Logging is a service that captures syslog events and Netflow Secure Event Logging, stores events in the Cisco cloud, and provides filtering and review capabilities.

- captures syslog events and Netflow Secure Event Logging
- stores events in the Cisco cloud, and, and
- provides filtering and review capabilities.

How ASA events are displayed in Security Cloud Control

Describes how ASA devices share syslog and NSEL events with Security Cloud Control for display to SOC analysts.

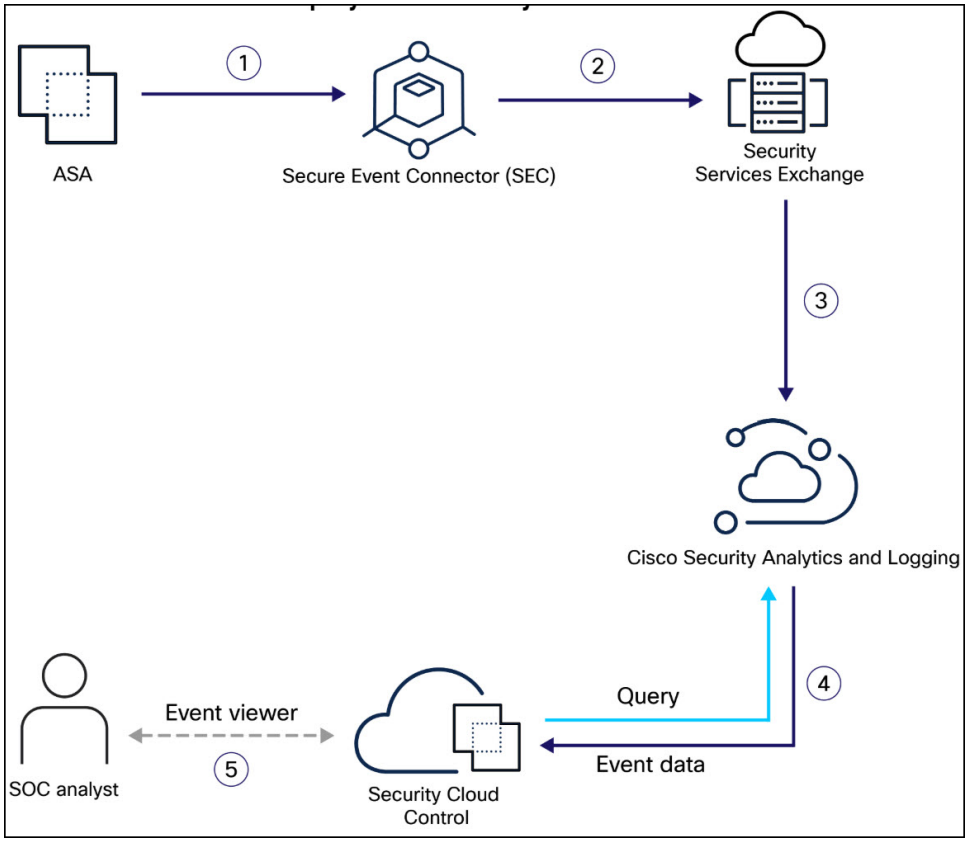
Summary

The key components involved in displaying ASA events in Security Cloud Control are:

- ASA devices: Generate and forward syslog and NSEL events when logging is enabled and network traffic matches access control rule criteria
- Secure Event Connectors: Receive events from ASA devices and forward them to Security Services Exchange
- Security Services Exchange: Aggregates event data from all devices, converts it to JSON format, and sends it for storage
- Security Analytics and Logging: Processes and enriches event data for use by Security Cloud Control
- Security Cloud Control: Stores event data and provides SOC analysts with relevant information

Workflow

Figure 2: How ASA events are displayed in security cloud control



These stages describe how ASA events are processed and displayed in Security Cloud Control:

1. You configure the ASA to forward syslog and NSEL events to any one of your Secure Event Connectors as if they were syslog servers and enable logging on the device.

   Syslog events and NSEL events are generated when logging is enabled on the ASA, and network traffic matches access control rule criteria. The ASA device forwards the syslog and NSEL events to the configured Secure Event Connector.

2. The Secure Event Connector forwards the events to Security Services Exchange.
3. Security Services Exchange aggregates the event data from all the ASA devices, converts it to JSON format, and sends it to Security Analytics and Logging for storage.
4. Security Analytics and Logging process the event data using various services to classify and enrich it for use by the Security Cloud Control.
5. Security Cloud Control stores the event data in the cloud data store. Security Cloud Control queries the stored data to provide SOC analysts with the relevant information.

Implement secure logging analytics (SaaS) for ASA devices

Configure Secure Logging Analytics (SaaS) for ASA devices including SEC destinations, ports, severity levels, custom event lists, and cloud event delivery.

Implement Secure Logging Analytics (SaaS) to send ASA device events to the Cisco cloud for security analysis and monitoring.

Use this workflow to set up secure logging analytics for ASA devices, enabling cloud-based security monitoring and analysis capabilities.

Before you begin

- Review Secure Logging Analytics (SaaS) for ASA devices to learn about:
  - How events are sent to the Cisco cloud
  - Applications in the solution
  - Licenses you need
  - Data plan you need
- You have contacted your managed service provider or Security Cloud Control Sales representative to create a Security Cloud Control tenant.
- Review Secure Device Connector on page 75. Connecting Security Cloud Control to your ASA using an SDC is considered a "best practice" but it is not required.
- If you choose to deploy an SDC in your network, you can use this method to install it:
  - Use Deploy a VM for running the secure device connector and secure event connector on page 78.
- You have installed one or more SECs for your tenant and you can send events from any ASA to any SEC onboarded to your tenant.

Follow these steps to implement Cisco Security Analytics and Logging (SaaS) and send events through the Secure Event Connector to the Cisco Cloud:

Procedure

1. Be sure to review "Before you Begin" above to make sure your environment is properly configured.
2. Onboard a Secure Firewall ASA on page 260 using username and password.
3. Send ASA Syslog Events to the Cisco Cloud.
4. Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.
5. Confirm events are visible in Security Cloud Control.

   From the navigation bar, select **Events & Logs** > **Events** > **Event Logging**. Click the **Live** tab to view live events.

You have successfully implemented Secure Logging Analytics (SaaS) for your ASA devices. Events are now being sent to the Cisco cloud for analysis and monitoring. If you have the appropriate licenses, you can also access Secure Cloud Analytics for advanced security monitoring and alerting capabilities.

What to do next

For troubleshooting and monitoring:

- Troubleshooting Secure Event Connector Onboarding Failures
- Event Logging Troubleshooting Log Files
- Use Health Check to Learn the State of your Secure Event Connector
- Troubleshooting Using Security and Analytics Logging Events

For reviewing Cisco Secure Cloud Analytics alerts by cross-launching from Security Cloud Control:

- Cisco Secure Cloud Analytics alerts from Security Cloud Control on page 364
- Secure Cloud Analytics and Dynamic Entity Modeling

- Working with Alerts Based on Firepower Threat Defense Events

Send ASA syslog events to the Cisco Cloud using a Security Cloud Control macro

Explains how to send ASA syslog events to the Cisco cloud using a Security Cloud Control macro, including command entry, selected devices, preview, review, and deployment results.

A Security Cloud Control macro is a configuration tool that

- allows you to assemble a list of CLI commands and turn elements of the command syntax into parameters
- can be saved and used more than once, and
- can be run on multiple devices at the same time to configure all your ASAs to send events to the Cisco cloud.

Macro benefits

Using proven macros promotes configuration consistencies between devices and prevents syntax errors that can occur when using the command line interface.

You can configure all your ASAs to send events to the Cisco cloud by creating a Security Cloud Control macro that uses all the commands described in Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface and running that macro on all your ASA in the same batch.

Before you read further, review macros in Security Cloud Control configuration guide Run a CLI macro on page 867 so that you understand the mechanics of using macros. This article will only describe assembling the final macro.

Create an ASA security analytics and logging (SaaS) macro

Configure an ASA Security Analytics and Logging (SaaS) macro to automate the process of sending ASA syslog events to the Cisco cloud using predefined CLI commands with customizable parameters.

This task helps you create a reusable macro that automates the configuration of ASA logging to send syslog events to a Secure Event Connector (SEC) in the Cisco cloud. The macro allows you to define parameters that can be customized each time you run it, making it easy to deploy consistent logging configurations across multiple ASA devices.

There are two types of formatting you'll see in the following procedure, ASA CLI commands and macro formatting. The ASA CLI commands are written to follow ASA syntax conventions. See Use command line interface for more information about using the CLI in Security Cloud Control.

Before you begin, open Send ASA Syslog Events to the Cisco Cloud in a separate window and read it in parallel with this procedure so you can read the command descriptions as you create your macros.

Before you begin

Note

If a logging config is already in place on the ASA, running the macro from Security Cloud Control will *not* first clear out all of the existing logging config. Rather, the settings defined in the Security Cloud Control macro will merge into whatever might already be in place.

Procedure

1. Open a plain text editor and create a list of commands you are going to turn into a macro, based on the instructions and options below. Security Cloud Control will execute the commands in the order they are written in the macro. Some command will have values that you turn into {{parameters}} that you will fill in when it comes time to run the macro.
2. **Configure the** ASA **to send messages to an SEC as if it were a syslog server.**

   Use the **logging host** command to specify the SEC as the syslog server you send messages to. You can send events to any one of the SECs you have onboarded to your tenant.

   The **logging host** command specifies a TCP or UDP port to send events to. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging to determine what ports you should use.

   logging host*interface_nameSEC_IP_address* **TCP/port UDP/port**

   Turn this command into one of two different macros depending on what protocol you use to send syslog events to the SEC:

   logging host {{interface_name}} {{SEC_ip_address}} TCP/{{port_number}}

   logging host {{interface_name}} {{SEC_ip_address}} UDP/{{port)_number}}

   (Optional) If you use TCP, you can add this command to your list of commands in your macro. It does not need any parameters.

   logging permit-hostdown

3. **Specify which syslog messages should be sent to the syslog server.**

   Use the **logging trap** command to specify which syslog messages should be sent to the syslog server:

   logging trap *severity_level message_list*

   If you want to define the events sent to the SEC by severity level, turn the command into this macro:

   logging trap {{severity_level}}

   If you only want to send events to the SEC that are part of a message list, turn the command into this macro:

   logging trap {{message_list_name}}

   If you chose the **logging trap message_list** command in the previous step, you need to define the syslogs in your message list. Open Create a Custom Event List so you can read the command descriptions as you create the macro. Start with this command:

   logging list*name* **level***level* **class***message_class* **message***start_id -end_id*

   And break it down into these variations:

   logging list {{message_list_name}} level {{security_level}}

   logging list {{message_list_name}} level {{security_level}} class {{message_class}}

   logging list {{message_list_name}} message {{syslog_range_or_number}}

In the last variation, the message parameter {{syslog_range_or_number}} could be entered as a single syslog ID, 106023, or a range, 302013-302018. Use one or more of the command variations in as many lines as you like to create your message list. Keep in mind that, in a single macro, all parameters with the same name will use the same value you enter. Security Cloud Control will not run a macro with empty parameters.

Important

The **logging list** command has to come before the **logging trap** command in your macro. You define the list first and then the **logging trap** command can use it. See the sample macro below.

4. **(Optional) Add the syslog timestamp.** Add this command if you want to add the date and time to the message that the syslog message originated on the ASA. The timestamp value is displayed in the **SyslogTimestamp** field. Add this command to your list of commands, it will not need any parameters:

   logging timestamp

   Note

   Beginning with version 9.10(1), ASA provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time as per RFC 5424 format. This is a sample output with RFC 5424 format:

   ```
   <166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress
   interface for protocol from src interface :src IP/src port to dest IP/dest
   port
   ```

5. **(Optional) Include a device ID in non-EMBLEM format syslog messages.** Open Include the Device ID in Non-EMBLEM Format Syslog Messages so you can read the command descriptions as you create the macro. This is the CLI command you will base your macro on:

   logging device-ID cluster-ID context-name hostname ipaddress *interface_name* **system string***text*

   And break it down into these variations:

   logging device-ID cluster-ID

   logging device-ID context-name

   logging device-ID hostname

   logging device-ID ipaddress {{interface_name}} **system**

   logging device-ID string {{text_16_char_or_less}}

6. **Enable logging**. Add this command to your macro as it is. It does not have any parameters:

   logging enable

7. **Do not add write memory** to the last line of the macro. Add the **show running-config logging** command instead to review the results of the logging commands you entered before committing them to the ASA's startup config.

   show running-config logging

8. After you are confident your configuration changes were made, you can create a separate macro for the **write memory** command or use Security Cloud Control's Bulk Command Line Interface tool to issue the command to all the devices you configured using your macro.

   write memory

9. **(Optional) Enable logging on access control rule " permit" events.** This step in the described in the Send ASA Syslog Events to the Cisco Cloud procedure but it is not included in this macro. It is performed in the Security Cloud Control GUI instead.
10. Save the macro.

You have successfully created an ASA Security Analytics and Logging macro that can be run to configure multiple ASA devices with consistent logging settings. The macro includes commands for specifying the SEC as a syslog server, defining which messages to send, and enabling logging functionality.

Here is a sample of a list of commands combined into a single macro:

```
logging host {{interface_name}} {{SEC_ip_address}}
{{tcp_or_udp}}/{{port_number}}
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

Note

There are several logging list commands to add different specific syslog IDs or ranges. The {{syslog_range_or_number_X}} parameter requires a number or some other differentiator, otherwise their values will all be the same when the macro is filled in. Also keep in mind that Security Cloud Control will not run a macro if not all the parameters are given a value, so only include the commands in the macro you want to execute. We do want all the syslog IDs contained in the same list so event_list_name stays the same for in each line.

Run the Macro

After you have created and saved the ASA Security Analytics and Logging Macro, run the macro to send ASA syslog events to the Cisco cloud.

Requirement: send ASA syslog events to the Cisco cloud using the command line interface

Outlines the procedure to forward ASA syslog events to a Secure Event Connector (SEC) and enable logging, including limitations on supported commands and message formats.

Limitations on supported ASA commands

This procedure explains how to forward ASA syslog events to a Secure Event Connector (SEC) and then enable logging. These procedures explain only what is needed to complete that workflow. For a broader discussion of all the ways you

can configure logging on the ASA, see the Monitoring chapter of either ASDM1: Cisco ASA Series General Operations ASDM Configuration Guide or CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide.

- Security Cloud Control does not yet support EMBLEM format for syslogs.
- Security Cloud Control does not yet support Secure Syslogs.

Security Cloud Control Command Line Interface for ASA

Configure access to the Security Cloud Control command line interface for ASA devices to perform configuration tasks.

Access the command line interface to configure ASA devices directly through Security Cloud Control.

For all the tasks in this procedure, you will be working on the Security Cloud Control's command line interface for ASA.

Procedure

1. From the left navigation bar, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab and select the ASA for which you want to enable logging.
4. In the Device Actions pane on the right, click **>_ Command Line Interface**.
5. Click the **Command Line Interface** tab.

   After entering every command, you will click **Send**. Because Security Cloud Control's CLI Interface is a direct connection to the ASA, the command is written to the device's running configuration immediately. For changes to be written to the ASA's startup configuration, you need to issue the `write memory` command in addition.

You are now ready to enter commands at the command line interface prompt.

Forward ASA syslog events to the secure event connector

Configure the ASA to forward syslog events to onboarded Secure Event Connectors and enable logging for event collection.

This task enables ASA syslog event forwarding to Secure Event Connectors for centralized logging and monitoring.

To forward ASA syslog events to one of the Secure Event Connectors (SECs) you have onboarded and then enable logging, you need complete these tasks in the procedure that follows.

Procedure

1. Configure the ASA to send messages to the SEC as if it were a syslog server.
2. Decide what severity level of all logs, or what list of syslog events, you want to send to the SEC.
3. Enable logging.
4. Save the changes to the ASA's startup config.

ASA syslog events are now forwarded to the configured Secure Event Connector with logging enabled and changes saved to startup configuration.

Send ASA syslog events to the Cisco cloud using CLI

Configure ASA to send syslog events to the Cisco cloud through the Secure Event Connector using command line interface commands.

This task configures the ASA to forward syslog events to the Cisco cloud for security analytics and logging purposes through the Secure Event Connector.

When sending syslog events from the ASA to the Cisco cloud, you forward them to the SEC as if it were an external syslog server, and it forwards the messages to the Cisco cloud.

Procedure

1. Configure the ASA to send messages to the SEC as if it were a syslog server

   To send syslog messages to the SEC, perform the following steps:

   a. Configure the ASA to send messages, using TCP or UDP, to the SEC as if it were a syslog server. The SEC can use an IPv4 or IPv6 addresss. You will be sending events to either a TCP or UDP port. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging to determine what ports you should use.

   Here is an example of the **logging host** command syntax:

   logging host *interface_name SEC_IP_address* **TCP/port UDP/port**

   Examples:

```
 > logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

   - The **interface_name** argument specifies the ASA interface from which messages are sent to the syslog server. It is a "best practice" to send the syslog messages to the SDC over the same ASA interface already in use for communication with the SDC.
   - The **SEC_IP_address** argument should contain the IP address of the VM on which the SEC is installed.
   - The **TCP/port** or **UDP/port** keyword-argument pair specifies that syslog messages should be sent using either TCP protocol and relevant port, or the UDP protocol and relevant port. You can configure the ASA to send data to a syslog server using either UDP or TCP, but not both. The default protocol is UDP if you do not specify a protocol.

     If you specify TCP, the ASA will discover syslog server failures and as a security protection, new connections through the ASA are blocked. To allow new connections regardless of connectivity to a TCP syslog server, see step b. If you specify UDP, the ASA continues to allow new connections whether or not the syslog server is operational. Valid port values

     > **Note**
     >
     > If you want to send ASA messages to two separate syslog servers, you can run a second logging host command with the appropriate interface, IP address, protocol and port of the other syslog server.

   b. (Optional) If you send events to the SEC over TCP, and if either the SEC is down or the log queue on the ASA is full, then new connections are blocked. New connections are allowed again after the syslog server is back up and the log queue is no longer full. To allow new connections regardless of connectivity to a TCP syslog server, disable the feature to block new connections when a TCP-connected syslog server is down using this command:

   logging permit-hostdown

Example:

```
> logging permit-hostdown
```

2. Specify which syslog messages should be sent to the syslog server with the following command:

   logging trap severity_level message_list

   Examples:

   ```
   > logging trap 3
   > logging trap asa_syslogs_to_cloud
   ```

   You can specify the severity level number (1 through 7) or name. For example, if you set the severity level to 3, then the ASA sends syslog messages for severity levels 3, 2, and 1.

   The message_list argument is replaced with the name of a custom event list, if you have created one. When specifying a custom event list, you only send the syslog messages that are in that list to the Secure Event Connector. In the example above, asa_syslogs_to_cloud is the name of the event list.

   Using a message_list could save you money by tightly defining which syslog messages are sent to the Cisco cloud.

   See Create a Custom Event List to create a message_list. See Security Analytics and Logging licenses on page 920 for more information about data ingest and storage costs.

3. (Optional) Add the syslog timestamp

   Add the date and time that the syslog message originated on the ASA to the message using the logging timestamp command. The timestamp value is displayed in the **SyslogTimestamp** field.

   Example:

   ```
   > logging timestamp
   ```

   > **Note**
   >
   > Beginning with version 9.10(1), ASA provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time as per RFC 5424 format. Following is a sample output with RFC 5424 format:

   ```
   <166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress
   interface for protocol from src interface :src IP/src port to dest IP/dest
   port.
   ```

4. (Optional) Include a device ID in non-EMBLEM format syslog messages

   A device ID is an identifier you can insert in a syslog message that will help you easily distinguish all syslog messages sent from a particular ASA. See Include the Device ID in Non-EMBLEM Format Syslog Messages for instructions.

5. (Optional) Enable logging on access control rule "permit" events

   When an access control rule denies access to a resource, the event is automatically logged. If you also want to log events generated when an access control rule allows access to a resource, you need to turn on logging for the access control rule and configure a severity type.

   See Log Rule Activity for instructions on how to turn on logging for an individual network access control rule.

> **Note**
>
> Enabling logging on access control rule "permit" events will use-up more of your purchased data plan as it is based on your daily ingest rate of events.

6. Enable logging

   At the command prompt, type logging enable. On the ASA, logging is enabled for the entire device, not for individual rules.

   Example:

```
> logging enable
```

> **Note**
>
> At this time, Security Cloud Control does not support enabling secure logging.

7. Save your Changes to the Startup Config

   At the command prompt, type write memory. On the ASA, logging is enabled for the entire device, not for individual rules.

   Example:

```
> write memory
```

The ASA is now configured to send syslog events to the Cisco cloud through the Secure Event Connector. Logging is enabled and messages will be forwarded according to your specified configuration.

Create a custom event list

Configure a custom event list to send specific ASA syslog events to the Cisco Cloud based on event class, severity, or message ID criteria.

Create a custom event list to filter and send specific ASA syslog events to logging destinations such as syslog servers or Secure Event Connectors in the Cisco Cloud.

Create a custom event list when you are sending ASA syslog events to the Cisco Cloud using one of these methods:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Send ASA Syslog Events to the Cisco Cloud using a Security Cloud Control Macro

You can create an event list, also referred to as a message_list, based on these three criteria:

- Event Class
- Severity

- Message ID

Before you begin

Follow these steps to create a custom event list to send to a specific logging destination:

Procedure

1. From the left navigation bar, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate tab and select the ASA whose syslog messages you want to include in a custom event list.
4. In the **Device Actions** pane, click **>_ Command Line Interface.**
5. Use this command syntax to issue the **logging list** command to the ASA:

   logging list *name* **level** *level* **class** *message_class* **message** *start_id -end_id*

   The *name* argument specifies the name of the list. The **level** *level* keyword and argument pair specify the severity level. The **class** *message_class* keyword-argument pair specify a particular message class. The **message** *start_id* [*-end_id*] keyword-argument pair specify an individual syslog message number or a range of numbers.

   > **Note**
   >
   > Do not use the names of severity levels as the name of a syslog message list. Prohibited names include emergencies, alert, critical, error, warning, notification, informational, and debugging. Similarly, do not use the first three characters of these words at the beginning of an event list name. For example, do not use an event list name that starts with the characters "err."

   - **Add syslog messages to the event list based on severity**. For example, if you set the severity level to 3, then the ASA sends syslog messages for severity levels 3, 2, and 1.

     Example:

     ```
     > logging list asa_syslogs_to_cloud level 3
     ```

   - **Add syslog messages based on other criteria to the event list**:

     Enter the same command as in the previous step, specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion that you want to add to the list. For example, you can specify criteria for syslog messages to be included in the list as follows:

     - Syslog message IDs that fall into the range of 302013-302018.
     - All syslog messages with the critical severity level or higher (emergency, alert, or critical).
     - All HA class syslog messages with the warning severity level or higher (emergency, alert, critical, error, or warning).

       Example:

       ```
       > logging list asa_syslogs_to_cloud message 302013-302018
       > logging list asa_syslogs_to_cloud level critical
       > logging list asa_syslogs_to_cloud level warning class ha
       ```

> **Note**
>
> A syslog message is logged if it satisfies any of these conditions. If a syslog message satisfies more than one of the conditions, the message is logged only once.

6. **Save your Changes to the Startup Config**

   At the command prompt, type **write memory**.

   Example:

```
> write memory
```

The custom event list is created and saved to the ASA startup configuration. The ASA will now filter and send syslog messages to the Cisco Cloud based on your specified criteria.

Include the device ID in Non-EMBLEM format syslog messages

Configure the ASA to include a device ID in non-EMBLEM-format syslog messages for proper identification in the SensorID field.

Configure the ASA to include a device identifier in non-EMBLEM-format syslog messages to ensure proper identification and tracking in the Event Logging page's SensorID field.

You can configure the ASA to include a device ID in non-EMBLEM-format syslog messages. You can specify only one type of device ID for syslog messages. This procedure is referred to by these procedures:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Send ASA Syslog Events to the Cisco Cloud using a Security Cloud Control Macro

This device identifier will be reflected in the SensorID field of a syslog event displayed on the Event Logging page.

Procedure

1. Select the ASA whose syslog messages you want to assign a device-ID to.
2. In the Device Actions pane, click **>_ Command Line Interface.**
3. Use this command syntax to issue the **logging device-ID** commands to the device.

   logging device-ID cluster-ID context-name hostname ipaddress*interface_name* **system string***text*

   Example:

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

   The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID.

> **Note**
>
> In an ASA cluster, always use the primary unit IP address for the selected interface.

The **cluster-ID** keyword specifies the unique name in the boot configuration of an individual ASA unit in the cluster as the device ID.

The **hostname** keyword specifies that the hostname of the ASA should be used as the device ID.

The **ipaddress** *interface_name* keyword-argument pair specifies that the interface IP address specified as *interface_name* should be used as the device ID. If you use the **ipaddress** keyword, the device ID becomes the specified ASA interface IP address, regardless of the interface from which the syslog message is sent. In the cluster environment, the **system** keyword dictates that the device ID becomes the system IP address on the interface. This keyword provides a single, consistent device ID for all syslog messages that are sent from the device.

The **string** *text* keyword-argument pair specifies that the text string should be used as the device ID. The string can include as many as 16 characters.

You cannot use blank spaces or any of the following characters:

- & (ampersand)
- ' (single quote)
- " (double quote)
- < (less than)
- > (greater than)
- ? (question mark)

4. **Save your Changes to the Startup Config**

   At the command prompt, type **write memory**.

   Example:

```
> write memory
```

The ASA is now configured to include the specified device ID in non-EMBLEM-format syslog messages, which will appear in the SensorID field on the Event Logging page.

NetFlow secure event logging (NSEL) for ASA devices

Explains NetFlow Secure Event Logging (NSEL) for ASA devices, including NSEL destinations, class maps, policy maps, macros, packet capture, and event verification.

NetFlow Secure Event Logging (NSEL) is a stateful IP flow tracking method that

- provides Security Analytics and Logging with granular data that basic syslog messages from the ASA lack
- exports only those records that indicate significant events in a flow, and
- supports NetFlow Version 9 services on Cisco ASA devices.

Flow characteristics and implementation details

A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device. These collected flows are exported to an external device, the NetFlow collector. Network flows are highly granular; for example, flow records include details such as IP addresses, packet and byte counts, timestamps, Type of Service (ToS), application ports, input and output interfaces, etc.[1]

The Cisco ASA supports NetFlow Version 9 services. The ASA implementation of NSEL provides a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes.

This documentation describes a straight forward approach to configuring NetFlow for your ASAs using a Security Cloud Control macro. The Cisco ASA NetFlow Implementation Guide provides an extremely detailed discussion of configuring NetFlow on the ASA and you may find it a valuable resource to accompany this content.

What to do Next

Go to Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.

Related Articles

- Configuring NSEL for ASA Devices Using a Security Cloud Control Macro
- Delete NetFlow Secure Event Logging (NSEL) Configuration from an ASA
- Determine the Name of an ASA Global Policy

1. ("Cisco Systems NetFlow Services Export Version 9." Internet Engineering Task Force, Network Working Group, Request for Comments: 3954, October 2004, B. Claise, Ed. https://www.ietf.org/rfc/rfc3954.txt)

Configuring NSEL for ASA devices by using a CDO macro

Describes how to configure Netflow Secure Event Logging (NSEL) on an ASA device and send NSEL events to a flow collector using a CDO macro.

ASAs report detailed connection event data using Netflow Secure Event Logging (NSEL). You can apply Secure Cloud Analytics to this connection event data, which includes bidirectional flow statistics. This procedure describes how to configure NSEL on an ASA device and send those NSEL events to a flow collector. In this case, the flow collector is a Secure Event Connector (SEC).

Summary

The key components involved in configuring NSEL for ASA devices are:

- **ASA device**: Reports detailed connection event data using NSEL
- **Secure Event Connector (SEC)**: Acts as the flow collector that receives NSEL events
- **CDO macro**: Automates the configuration process for NSEL settings
- **Flow-export destination**: Defines where NSEL events are sent
- **Class-map**: Defines which NSEL events will be sent to the SEC
- **Policy-map**: Applies the flow-export configuration to specific traffic classes

Workflow

These are the stages of configuring NSEL for ASA devices by using a Security Cloud Control macro:

1. Before beginning the configuration process, gather the required information including the IPv4 address of the SEC, the ASA interface, the UDP port number, and the global policy name.
   - IPv4 address of the SEC that will receive data from the ASA
   - Interface on the ASA that will send data to the SEC

- UDP port number used to forward NetFlow events. See Finding your device's TCP, UDP, and NSEL port used for secure logging analytics (SaaS) on page 953.
- Determine the name of an ASA global policy on page 350

2. Execute the configuration workflow by following each step in sequence to properly configure NSEL using the CDO macro.
   - Open the configuring NSEL macro on page 343.
   - Define the destination of NSEL messages and the interval at which they are sent to the SEC on page 344.
   - Create a Class-Map that defines which NSEL events will be sent to the SEC on page 345.
   - Define a Policy-Map for NSEL events on page 346.
   - Recommendation: disable redundant syslog messages when using NetFlow on page 346.
   - Review and send the macro on page 348.

   This procedure refers to this macro, **Configure NSEL**:

```
 flow-export destination {{interface}} {{SEC_IPv4_address}}
{{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination
{{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

   Here is an example of the Configure NSEL macro with all the default values filled in, a generic name for the class-map, and the class map added to the global_policy, When you are done with these procedures, your macro will resemble this:

```
 flow-export destination {{interface}} {{SEC_IPv4_address}}
{{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

Open the configuring NSEL macro

Configure access to the NSEL macro for ASA devices through the Command Line Interface.

This task allows you to access the Configuring NSEL macro to configure NetFlow Secure Event Logging on ASA devices.

This is the first part in a longer workflow for configuring NSEL on ASA devices using CDO macros.

Before you begin

This is first part in a longer workflow, see Configuring NSEL for ASA devices by using a CDO macro on page 342 before getting started.

Follow these steps to open the Configuring NSEL macro:

Procedure

1. On the **Security Devices** page, click the **Devices** tab.
2. Click the appropriate device type tab and select the ASA(s) on which you want to configure NetFlow Secure Event Logging (NSEL).
3. In the **Device Actions** pane, click **Command Line Interface**.
4. Click the Macro star  to show the list of available macros.
5. From the list of macros, select **Configuring NSEL**.
6. Under the Macro box, click **View Parameters**.

   Continue to Define the destination of NSEL messages and the interval at which they are sent to the SEC on page 344.

The Configuring NSEL macro parameters are displayed, allowing you to proceed with configuring NSEL settings for the selected ASA devices.

Define the destination of NSEL messages and the interval at which they are sent to the SEC

Configure the destination and timing settings for NSEL messages sent to the SEC collector.

This task configures the destination SEC collector and timing intervals for NSEL message transmission from ASA devices.

NSEL messages can be sent to any one of the SECs you have onboarded to your tenant. These instructions refer to this section of the macro:

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA devices by using a CDO macro on page 342 before getting started.

Procedure

1. The **flow-export destination** command defines the collector to which the NetFlow packets are sent. In this case, you are sending them to an SEC. Fill in the fields for these parameters:
   - **{{interface}}**–Enter the name of the interface on the ASA from which the NetFlow events are sent.
   - **{{SEC_IPv4_address}}**–Enter the IPv4 address of the SEC. The SEC functions as the flow collector.
   - **{{SEC_NetFlow_port}}**–Enter the UDP port number on the SEC to which NetFlow packets are sent.

2. The **flow-export template timeout-rate** command specifies the interval at which template records are sent to all configured output destinations.
   - **{{timeout_rate_in_mins}}-**Enter the number of minutes before templates are resent. **We recommend using a value of 60 minutes**. The SEC does not process the templates. A large number reduces traffic to the SEC.

3. The **flow-export delay flow-create** command delays the sending of flow-create events by the specified number of seconds. This value matches the recommended Active Timeout value and reduces the number of flow events exported from the ASA. At that rate, expect NSEL events to first appear in Security Cloud Control at the close of a connection or within 55 seconds of the creation of the connection, whichever happens earlier. If this command is not configured, there is no delay, and the flow-create event is exported as soon as the flow is created.
   - **{{delay_flow_create_rate_in_secs}}-**Enter the number of seconds delay between sending flow-create events. **We recommend using a value of 55 seconds**.

4. The **flow-export active refresh-interval** command defines the frequency that status updates for long-lived flows will be sent from ASA. Valid values are from 1-60 minutes. In the Flow Update Interval field, configuring the **flow-export active refresh-interval** to be at least 5 seconds more than the **flow-export delay flow-create** interval prevents flow-update events from appearing before flow-creation events.
   - **{{refresh_interval_in_mins}}**-**We recommend using a value of 1 minute**. Valid values are from 1-60 minutes.

Continue to Create a Class-Map that defines which NSEL events will be sent to the SEC on page 345

The NSEL message destination and timing parameters are configured for transmission to the specified SEC collector.

Create a Class-Map that defines which NSEL events will be sent to the SEC

Configure a class-map to define which NSEL events will be sent to the Secure Event Connector (SEC).

Create a class-map that identifies NSEL traffic for export to the SEC and define the matching criteria for traffic classification.

The following commands in the macro group all NSEL events in a class and then export that class to the Secure Event Connector (SEC). These instructions refer to this section of the macro:

class-map {{flow_export_class_name}}

match {{add_this_traffic_to_class_map}}

Procedure

---

1. The **class-map** command names the class map that identifies NSEL traffic that will be exported to the SEC.
   - **{{flow-export-class-name}}-**Enter a name for your class map. The name may be up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot re-use a name already used by another type of class map.

2. Identify the traffic that is going to be associated with (matched with) your class-map. Choose one of these options for the value of **{{add_this_traffic_to_class_map}}:**
   - Enter **any** in the **{{add_this_traffic_to_class_map}}** field. This monitors all traffic types for NSEL traffic. **We recommend using the value "any".**

- Enter **access-list *name-of-access-list*** in the **{{add_this_traffic_to_class_map}}** field. This associates all the traffic associated with an access-list that you have created. See Configure Flow-Export Actions Through Modular Policy Framework in the Cisco ASA NetFlow Implementation Guide for more information.

Continue to Define a Policy-Map for NSEL events on page 346.

You have created a class-map that defines which NSEL events will be sent to the SEC and specified the traffic matching criteria.

Define a Policy-Map for NSEL events

Configure a policy-map that assigns NetFlow export actions to the class for NSEL events.

Create a policy-map that assigns NetFlow export actions to the class and associates the class with a new policy map for managing NSEL events.

This task assigns NetFlow export actions to the class you created in the previous task, and the class to a new policy map. These instructions refer to this section of the macro:

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

Procedure

---

1. The **policy-map** command creates a policy-map. In the next task, you associate this policy map with the global policy.
   - **{{global_policy_map_name}}**-Enter a name for the policy map. **We recommend using the name of the firewall's existing global policy if there is one**. The default name for the global policy is **global_policy**. See Determine the Name of an ASA Global Policy. If you create a new policy map and apply it globally according to Configure Flow-Export Actions Through Modular Policy Framework in Cisco ASA NetFlow Implementation Guide, the remaining inspection policies are deactivated.
2. The **class** command inherits the name of the class-map you created in Create a Class-Map that defines which NSEL events will be sent to the SEC on page 345.
3. The **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} command defines which event types should be sent to flow collector, (in this case the SEC).
   - **{{event-type}}**-The event_type keyword is the name of the supported event being filtered. **We recommend using the value "all"**.
   - **{{SEC_IPv4_address}}**-This is the IPv4 address of the SEC. Its value is inherited from the value you entered in Define the destination of NSEL messages and the interval at which they are sent to the SEC on page 344.

Continue to Recommendation: disable redundant syslog messages when using NetFlow on page 346.

The policy-map is created with NetFlow export actions assigned to the specified class for managing NSEL events.

Recommendation: disable redundant syslog messages when using NetFlow

Outlines the process for disabling redundant syslog messages when NetFlow is enabled to export flow information for improved performance.

When NetFlow is enabled to export flow information, disable redundant syslog messages for improved performance. The same information is exported through NetFlow, making these syslog messages unnecessary.

Enabling NetFlow to export flow information makes certain syslog messages redundant because the same information is exported through NetFlow. Disabling these messages improves performance.

The macro includes the command **logging flow-export-syslogs disable** to disable redundant syslog messages. You do not need to modify this command.

If you do not want to disable redundant syslog messages, you can edit this macro and delete only this line from it:

logging flow-export-syslogs disable

You can later enable or disable individual syslog messages by following the procedure in the Disabling and Reenabling NetFlow-related Syslog Messages.

Note

When NSEL and syslog messages are both enabled, there is no guarantee of chronological ordering between the two logging types.

Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
106100	Generated whenever an access control rule (ACL) is encountered.	1-Flow was created (if the ACL allowed the flow). 3-Flow was denied (if the ACL denied the flow).	0-If the ACL allowed the flow. 1001-Flow was denied by the ingress ACL. 1002-Flow was denied by the egress ACL.
106015	A TCP flow was denied because the first packet was not a SYN packet.	3-Flow was denied.	1004-Flow was denied because the first packet was not a TCP SYN packet.
106023	When a flow was denied by an ACL attached to an interface through the **access-group** command.	3-Flow was denied.	1001-Flow was denied by the ingress ACL. 1002-Flow was denied by the egress ACL.
302013, 302015, 302017, 302020	TCP, UDP, GRE, and ICMP connection creation.	1-Flow was created.	0-Ignore.
302014, 302016, 302018, 302021	TCP, UDP, GRE, and ICMP connection teardown.	2-Flow was deleted.	0-Ignore. > 2000-Flow was torn down.
313001	An ICMP packet to the device was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.
313008	An ICMP v6 packet to the device was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.

Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
710003	An attempt to connect to the device interface was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.

Review and send the macro

Configure macro commands by reviewing and sending them to the ASA device after completing the field configuration.

Review and send macro commands to the ASA device to complete the NSEL configuration workflow.

This task is performed after filling in the macro fields as part of configuring NSEL for ASA devices using a CDO macro.

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA devices by using a CDO macro on page 342, before getting started.

Follow these steps to review and send the macro:

Procedure

1. After filling in the fields of the macro, click **Review** to review the commands before they are sent to the ASA.
2. If you are satisfied with your responses to the commands, click **Send**.
3. After you send the command, you may see the message, "Some commands may have made changes to the running config" along with two links.



   - Clicking **Write to Disk** saves the changes made by this command, and any other changes in the running-configuration, to the device's startup configuration.
   - Clicking **Dismiss** dismisses the message.

You have finished the workflow described in Configuring NSEL for ASA devices by using a CDO macro on page 342.

DELETE NetFlow secure event logging (NSEL) configuration from an ASA

Configure the removal of NetFlow Secure Event Logging (NSEL) configuration on an ASA device that specifies the Secure Event Connector (SEC) as the NSEL flow collector.

This task removes the NetFlow Secure Event Logging (NSEL) configuration from an ASA device, which reverses the configuration that specifies the Secure Event Connector (SEC) as the NSEL flow collector.

This procedure reverses the macro described in Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.

Procedure

Use the **DELETE NSEL** macro to remove the NetFlow configuration.

Example

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

The NetFlow Secure Event Logging (NSEL) configuration is removed from the ASA device.

Open the DELETE-NSEL macro

Configure access to the DELETE-NSEL macro for removing NetFlow Secure Event Logging configuration from ASA devices.

This task enables you to access and prepare the DELETE-NSEL macro for removing NetFlow Secure Event Logging (NSEL) configuration from ASA devices.

Use this task when you need to DELETE the NetFlow Secure Event Logging configuration from one or more ASA devices using the command line interface and macro functionality.

Procedure

---

1. On the **Security Devices** page, click the **Devices** tab.
2. Click the appropriate device type tab and select the ASA(s) on which you want to DELETE the configuration of NetFlow Secure Event Logging (NSEL).
3. In the **Device Actions** pane, click **Command Line Interface**.
4. Click the Macros star  to show the list of available macros.
5. In the list of macros, select **DELETE-NSEL**.
6. Under the Macro box, click **View Parameters**.

The DELETE-NSEL macro is now open and ready for parameter configuration before execution.

Enter the values in the macro to complete the no commands

Configure the macro values to complete the "no" form of NetFlow commands for removing policy-map configurations on ASA.

Remove NetFlow policy-map configurations by completing the "no" form of commands with appropriate macro values.

The ASA CLI uses the "no" form of a command to delete it. Fill in the fields in the macro to complete the "no" form of the command:

Procedure

---

1. policy-map {{flow_export_policy_name}}
   - **{{flow_export_policy_name}}**-Enter the value of the policy-map name.

2. no class {{flow_export_class_name}}
   - **{{flow_export_class_name}}**-Enter the value of the class-map name.
3. no class-map {{flow_export_class_name}}
   - **{{flow_export_class_name}}**-The value of the class-map name is inherited from the step above.
4. no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
   - **{{interface}}**-Enter the name of the interface on the ASA from which the NetFlow events were sent.
   - **{{IPv4_address}}**-Enter the IPv4 address of the SEC. The SEC functions as the flow collector.
   - **{{NetFlow_port}}**-Enter the UDP port number on the SEC to which NetFlow packets were sent.
5. no flow-export template timeout-rate {{timeout_rate_in_mins}}
   - **{{timeout_rate_in_mins}}**-Enter the flow-export template timeout-rate.
6. no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
   - **{{delay_flow_create_rate_in_secs}}**-Enter the flow-export delay flow-create rate.
7. no flow-export active refresh-interval {{refresh_interval_in_mins}}
   - **{{refresh_interval_in_mins}}**-Enter the flow-export active refresh-interval interval.

The NetFlow policy-map configuration is removed from the ASA device after completing all the "no" commands with the appropriate macro values.

Determine the name of an ASA global policy

Configure the identification of an ASA's global policy name using the command line interface.

This task enables you to identify the specific name assigned to an ASA's global policy configuration.

You may need to determine the name of an ASA's global policy when troubleshooting or configuring security policies on your device.

Before you begin

Follow these steps to determine the name of an ASA global policy:

Procedure

---

1. From the **Security Devices** page, select the device for which you want to find the name of the global policy.
2. In the Device Actions pane, select **>_Command Reference**.
3. In the Command Line Interface window, at the prompt, type:

   show running-config service-policy

   In the output of the example below, global_policy is the name of the global policy.

   Example:

   >show running-config service-policy

service-policy global_policy global

The command output displays the global policy name in the service-policy configuration line.

Troubleshooting NSEL data flows

Describes procedures to verify that NSEL events are being sent from your ASA to the Cisco Cloud and that the Cisco Cloud is receiving them.

Troubleshooting NSEL data flows is a verification process that

- verifies that NSEL events are being sent from your ASA to the Cisco Cloud
- confirms that the Cisco Cloud is receiving NSEL events, and
- uses flow-export counters and capture commands to diagnose data flow issues.

NSEL data flow verification requirements

Once you have configured Netflow Secure Event Logging (NSEL), data does not flow immediately. It could take a few minutes for the first NSEL packets to arrive assuming there is NSEL-related traffic being generated on the ASA.

This verification process involves these tasks:

- Verify that NetFlow Packets are Being Sent to the SEC
- Verify that NetFlow Packets are Being Received by the Cisco Cloud

> **Note**
>
> This workflow shows you a straight-forward use of the "flow-export counters" command and "capture" commands to Troubleshoot NSEL Data Flows. See "Packet Captures" CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide and "Monitoring NSEL" in the Cisco ASA NetFlow Implementation Guide for a more detailed discussion of the usage of these commands.

Verify that NSEL events are being sent to the SEC

Verify that NSEL packets are being sent to the SEC using flow-export counters or capture commands.

This task verifies that NSEL events are successfully being transmitted from ASA devices to the SEC for security event monitoring.

Use one of two commands to verify that NSEL packets are being sent to the SEC:

- flow-export counters
- capture

Use the "flow-export counters" Command to Check for flow-export Packets Being Sent and for NSEL errors

- Make sure you have configured your ASA to send NSEL events to the SEC. See Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.
- The SEC IP address is the flow collector address for NSEL events. If you have onboarded more than one SEC to your tenant, be sure you are using the correct IP address.

- Find the UDP port number used to forward NetFlow events. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging.
- Our recommended interface on the ASA from which to send NSEL events is the management interface; your interface may be different.

Use the command line interface in Security Cloud Control to send these commands to the ASAs that you have configured for NSEL.

Procedure

1. In the navigation pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device tab and select the ASA you configured to send NSEL events to the SEC.
4. In the **Device Actions** pane on the right, click **Command Line Interface**.
5. Reset the flow export counters by running the **clear flow-export counters** command. This resets the clear export flow counters to zero so that you can easily tell if new events are coming in.

   example:

   >clear flow-export counters

   Done!
6. Run the show flow-export counters command to see the destination of the NSEL packets, how many packets were sent and any errors:

   example:

   >show flow-export counters

   destination: management 209.165.200.225 10425

   Statistics:

   packets sent 25000

   Errors:

   block allocation errors 0

   invalid interface 0

   template send failure 0

   no route to collector 0

   source port allocation 0

   In the output above, the destination line shows the interface on the ASA from which NSEL events are sent, the IP address of the SEC, port 10425 of the SEC. It also shows packets sent of 25000.

Error descriptions:

- **block allocation errors**-If you receive a block allocation error, the ASA did not allocate memory to the flow-exporter.
  - Recovery action: Call Cisco Technical Assistance Center (TAC).
- **invalid interface**-Indicates that you are trying to send NSEL events to the SEC but the interface you've defined for flow export isn't configured to do so.

  - Recovery action: Review the interface you chose when configuring NSEL. We recommend using the management interface, your interface may be different.

- **template send failure**-The template you had to define NSEL was not parsed correctly.
  - Recovery action: Contact Security Cloud Control support.

- **no route to collector**-Indicates there is no network route from the ASA to the SEC.
  - Recovery actions:
    - Make sure that the IP address you used for the SEC when you configured NSEL is correct.
    - Make sure the SEC's status is Active and it has sent a recent heartbeat. See Resolve unreachable SDC status on page 1071.
    - Make sure the Secure Device Connector's status is Active and it has sent a recent heartbeat.

- **source port allocation**-May indicate that there is a bad port on your ASA.

Use the "capture" command to capture NSEL packets sent from the ASA to the SEC

Configure packet capture on the ASA to verify NSEL events are being sent to the SEC using the capture command.

This task captures NSEL packets to verify that your ASA is successfully sending NSEL events to the SEC.

Use the command line interface in Security Cloud Control to send these commands to the ASAs that you have configured for NSEL.

Before you begin

- Make sure you have configured your ASA to send NSEL events to the SEC. See Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.
- The SEC IP address is the flow collector address for NSEL events. If you have onboarded more than one SEC to your tenant be sure you are using the correct IP address.
- Find the UDP port number used to forward NetFlow events. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging.
- Our recommended interface on the ASA from which to send NSEL events is the management interface; your interface may be different.

Follow these steps to capture NSEL packets sent from the ASA to the SEC:

Procedure

1. In the navigation pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab and select the ASA you configured to send NSEL events to the SEC.
4. In the **Device Actions** pane on the right, click **Command Line Interface**.
5. In the command window, run this **capture** command:

   capture*capture_name* **interface***interface_name* **match UDP any host** *IP_of_SEC* **eq***NetFlow_port*

   Where

   - *capture_name* is the name of the packet capture.
   - *interface_name* is the name of the interface from which NSEL packets leave the ASA.

- *IP_of_SEC* is the IP address of the SEC VM.
- *NetFlow_port* is the port to which NSEL events are sent.

This starts the packet capture.

6. Run the **show capture** command to view the captured packets:

   > **show capture***capture_name*

   Where *capture_name* is the name of the packet capture you defined in the previous step.

   Here is an example of the output showing the time of the capture, the IP address from which the packet was sent, the IP address, and the port the packet was sent to. In this example, 192.168.25.4 is the IP address of the SEC and port 10425 is the port on the SEC that receives NSEL events.

   6 packets captured

   ```
   1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: UDP 476
   2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: UDP 248
   3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: UDP 1436
   4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: UDP 1276
   5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: UDP 112
   6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: UDP 196
   ```

7. Run the **capture stop** command to manually stop the packet capture:

   > **capture** *capture_name***stop**

   Where *capture_name* is the name of the packet capture you defined in the previous step.

The packet capture shows NSEL packets being sent from the ASA to the SEC, confirming that NSEL events are successfully transmitted to the configured destination.

Check for live NSEL events

Verify live NSEL events that the Cisco Cloud has received within the last hour by filtering events in the analytics interface.

This task allows you to verify that NSEL events are being properly received and processed by the Cisco Cloud system.

Check for both live and historical events. This procedure will filter for NSEL events that the Cisco Cloud has received within the last hour.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click the **Live** tab.
4. Pin-open the event filter.
5. In the ASA Events section, make sure **NetFlow** is checked.
6. In the Sensor ID field, enter the IP address of the ASA you configured to send NSEL events.
7. At the bottom of the filter, make sure that **Include NetFlow Events** is checked.

The system displays live NSEL events from the specified ASA device, confirming that events are being successfully received and processed.

Check for historical NSEL events

Configure historical event filtering to check for NSEL events that Cisco Cloud has received within your specified time-frame.

Filter for NSEL events that the Cisco Cloud has received within a specific time-frame to verify event receipt and troubleshoot connectivity issues.

This procedure will filter for NSEL events that the Cisco Cloud has received within the time-frame you specify.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click the **Historical** tab.
4. Pin-open the event filter.
5. In the ASA Events section, make sure **NetFlow** is checked.
6. Set the Start time far enough back in time to check if Security Cloud Control ever did receive NSEL events.
7. In the Sensor ID field, enter the IP address of the ASA you configured to send NSEL events.
8. At the bottom of the filter, make sure that **Include NetFlow events** is checked.

The historical event filter displays NSEL events received from the specified ASA within your configured time-frame, confirming successful event transmission to Cisco Cloud.

Parsed ASA syslog events

Explains parsed ASA syslog events, including SEC destinations, ports, severity levels, custom event lists, and cloud event delivery.

Parsed ASA syslog events are specialized syslog messages that

- contain more event attributes than other syslog events
- let you search on any specific parsed field, and
- are forwarded by the SEC to the Cisco cloud with italicized EventTypes for identification.

Parsed syslog event processing

The SEC forwards all ASA events you specify to the Cisco cloud but only specific syslog messages are parsed. All parsed Syslogs events are shown with their EvenTypes italicised to help you identify.

For detailed explanations of syslogs see, Cisco ASA Series Syslog Messages.

Syslog ID	Syslog Category	Purpose of syslog messge
106015	Firewall	Represents out of state TCP Deny
106023	Firewall	A real IP packet was denied by the ACL. This message appears even if you do not have the **log** option enabled for an ACL.

Syslog ID	Syslog Category	Purpose of syslog messge
106100	Access Lists/User Session	Packet was permitted or denied by an ACL.
113019	User Authentication	Critical AnyConnect
302013, 302015, 302017, 302020	User Session	Connection start and end syslogs for TCP, UDP, GRE, and ICMP connection creation.
302014, 302016, 302018, 302021	User Session	Connection start and end syslogs for TCP, UDP, GRE, and ICMP connection creation.
302020 - 302021	User Session	ICMP session establishment and teardown.
305006	User Session/NAT and PAT	NAT connection failure
305011-305014	User Session/NAT and PAT	NAT Build/Teardown related
313001, 313008	IP Stack	Represents denied connections to the box.
414004	System	Critical AnyConnect
609001 - 609002	Firewall	A network state container was reserved/removed for host **ip-address** connected to a zone.
710002,710004 710005	User Session	To the box connections failures
710003	User Session	Represents denied connections to the box.
746012, 746013	User Session	Critical AnyConnect

Related information:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Filtering Events in the Event Logging Page

15 Monitor device health metrics

Topics:

- About device health metrics
- Enable ASA health monitoring
- Bulk opt in or opt out of device health metrics
- View the device health metrics dashboard
- Troubleshooting device health metrics

Learn how to monitor device health metrics for ASA devices, including event details, device status, reporting views, and follow-up actions.

This chapter explains how to use the Device Health Metrics dashboard to gain detailed insights of your device.

About device health metrics

An overview of device health metrics for ASA devices, including interface names, security levels, IP addressing, VLANs, and enablement options.

Use the Device Health Metrics dashboard to gain detailed insights into the performance of your ASA devices. By enabling this feature, you can monitor key performance metrics to ensure optimal device operation and identify potential issues.

For Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center, Health Monitoring is enabled by default. For more information, see Health Monitoring.

Benefits of Device Health Metrics

- Enhanced monitoring: Gain insights into device performance with real-time data snapshots.
- Enhanced decision-making: Use detailed metrics to make data-driven decisions about device management and troubleshooting.
- Efficient resource management: Track CPU, memory, and interface usage to allocate resources effectively.

Enable ASA health monitoring

Enable ASA Health Monitoring to collect and analyze device health data within the dashboard. You must perform this task at the tenant level to ensure comprehensive monitoring of ASA devices managed by the system.

You must enable Device Health Metrics at the managed organization level. For ASA devices managed by Secure Device Connector, you must also enable the feature at the individual device level. These steps ensure health data is collected and made available for analysis within the dashboard.

You must have the **Super Admin** user role to enable this feature.

Follow these steps to enable ASA health monitoring for the managed organization:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn on the **Enable ASA Health Monitoring** toggle button to enable the Device Health Metrics feature for your managed organization.

   #### Device Type Considerations

   - For ASA devices managed by Cloud Device Gateway (CDG), health metrics are enabled when the **Enable Device Health Metrics** toggle in **General Settings** is enabled.
   - For ASA devices managed by Secure Device Connector (SDC), manually enable health metrics for each device:
     a. Choose **Security Devices**.
     b. Select the SDC-managed ASA device.
     c. In the **Device Actions** pane, choose **Opt-in to Health Metrics**.

        If the device is already opted in, you will see the option to **Opt-out of Health Metrics** instead.

> **Note**
>
> Each SDC can support health metrics collection for up to 50 ASA devices.

Bulk opt in or opt out of device health metrics

Learn how to bulk opt in or opt out of device health metrics for ASA devices, including source and destination Secure Device Connector selection, reachability, and connection status.

On the **Security Devices** page, you can bulk opt in or opt out of **Device Health Metrics** for ASA devices managed by Secure Device Connector (SDC).

Procedure

1. In the left pane, click **Security Devices**.
2. You can select multiple ASA devices to modify the health metrics settings.
3. In the right pane, under **Device Actions**, click **Opt in/Opt out Health Metrics**.

   The **Opt in/Opt out Health Metrics** pop-up appears displaying the following information:

   - The total number of devices selected.
   - Devices that are not managed by SDCs.
   - Lists of devices categorized by their current health metrics.

4. Click **Opt out** or **Opt in** as required.

View the device health metrics dashboard

Learn how to view the device health metrics dashboard for ASA devices, including interface names, security levels, IP addressing, VLANs, and enablement options.

The Device Health Metrics dashboard provides a centralized view of critical performance data for your ASA devices. Use this dashboard to monitor device health, resource usage, and interface statistics to ensure optimal network operations.

Procedure

1. In the left pane, click **Insights & Reports** > **Reports & Analytics** > **Device Health Metrics**.
2. In the **Interfaces** section, select a device from the drop-down menu. All interfaces for the selected device are listed. The data auto-refreshes every 5 minutes.
3. Choose a **Duration** from the drop-down menu, or a select a custom date and time range to view data for interfaces during the specified period.
4. You can select up to four interfaces to compare the data.

5. Click **View Security Devices** to view more details about the selected device. The device you selected in the **Device Health Metrics** dashboard will be selected on the **Security Devices** page, and its details are displayed in the right pane.
   - Additionally, from the **Security Devices** page, select an ASA device.
   - Under **Device Actions**, click **Health Metrics** to view the **Device Health Metrics** dashboard.

Troubleshooting device health metrics

Troubleshoot device health metrics by reviewing symptoms, configuration details, likely causes, and corrective actions for managed ASA devices.

Consider the following reasons for data not being displayed in the **Device Health Metrics** dashboard:

- **Health metrics not enabled for tenant**

  Workaround: Navigate to **Administration > General Settings** and ensure that the **Enable ASA Health Monitoring** toggle is enabled. This will enable health metrics for all devices within the tenant.

- **No ASA devices have been onboarded**

  Workaround: Navigate to the **Security Devices** page to onboard your ASA devices. Ensure that devices are properly onboarded to start monitoring them.

- **Health metrics are not enabled for the individual ASA devices using on-prem SDC**

  Workaround: Verify that health metrics are enabled for each device using an on-prem Secure Device Connector. Note that each SDC supports monitoring up to 50 devices.

- **The device is unreachable**

  Workaround: Check the connectivity of the device. Ensure that the device online. Navigate to the **Security Devices** page to verify and troubleshoot connectivity issues.

16 Use Cisco Secure Cloud Analytics Portal

Topics:

- Provision a Cisco secure cloud analytics portal
- Review sensor health and Security Cloud Control integration status in Secure Cloud Analytics
- Cisco secure cloud analytics sensor deployment for total network analytics and reporting
- Cisco Secure Cloud Analytics alerts from Security Cloud Control
- Cisco secure cloud analytics and dynamic entity modeling
- Alerts based on firewall events
- Modify alert priorities

This chapter provides information about Cisco Secure Cloud Analytics portal.

Provision a Cisco secure cloud analytics portal

Configure a Cisco Secure Cloud Analytics portal to view alerts and monitor network flow data after purchasing the required license.

Provision a Cisco Secure Cloud Analytics portal to view Secure Cloud Analytics alerts and monitor network analytics after deploying and configuring the Secure Event Connector (SEC).

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

If you purchase a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, after you deploy and configure the Secure Event Connector (SEC), you must associate a Secure Cloud Analytics portal with your Security Cloud Control portal to view Secure Cloud Analytics alerts. When you purchase the license, if you have an existing Secure Cloud Analytics portal, you can provide the Secure Cloud Analytics portal name and immediately link it to your Security Cloud Control portal.

Otherwise, you can request a new Secure Cloud Analytics portal from the Security Cloud Control UI. The first time you access Secure Cloud Analytics alerts, the system takes you to a page to request the Secure Cloud Analytics portal. The user that requests this portal is granted administrator permission in the portal.

Procedure

1. In the left pane, click **Analytics** > **Secure Cloud Analytics** to open the Secure Cloud Analytics UI in a new window.
2. Click **Start Free Trial** to provision a Secure Cloud Analytics portal and associate it with your Security Cloud Control portal.

   Note

   After you request the portal, the provisioning may take up to several hours.

   What to do next:

   - If you purchased a **Logging Analytics and Detection** license, your configuration is complete. If you want to view the status of your Security Cloud Control integration or sensor health from the Secure Cloud Analytics portal UI, see Review sensor health and Security Cloud Control integration status in Secure Cloud Analytics on page 363 for more information. If you want to work with alerts in the Secure Cloud Analytics portal, see Cisco Secure Cloud Analytics alerts from Security Cloud Control on page 364 and Working with Alerts Based on Firepower Events for more information.
   - If you purchased a **Total Network Analytics and Monitoring** license, deploy one or more Secure Cloud Analytics sensors to your internal network to pass network flow data to the cloud. If you want to monitor cloud-based network flow data, configure your cloud-based deployment to pass flow data to Secure Cloud Analytics. See Cisco secure cloud analytics sensor deployment for total network analytics and reporting on page 363 for more information.

Ensure that your portal is provisioned before moving on to the next step.

1. In the left pane, click **Analytics** > **Secure Cloud Analytics** to open the Secure Cloud Analytis UI in a new window.
2. You have these options:

- If you requested a Secure Cloud Analytics portal, and the system states it is still provisioning the portal, wait and try to access the alerts later.
- If the Secure Cloud Analytics portal is provisioned, enter your **Username** and **Password**, then click **Sign in**.

> **Note**
>
> The administrator user can invite other users to create accounts within the Secure Cloud Analytis portal. See Cisco Secure Cloud Analytics alerts from Security Cloud Control on page 364 for more information.

Review sensor health and Security Cloud Control integration status in Secure Cloud Analytics

Configure visibility into sensor health and Security Cloud Control integration status in Secure Cloud Analytics for ASA devices, including ASA integration with Cisco Umbrella and secure internet gateway use cases.

This task allows you to monitor the operational status of your sensors and Security Cloud Control integration to ensure proper connectivity and configuration.

Sensor Status

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

In the Secure Cloud Analytics web UI, you can view your Security Cloud Control integration status and your configured sensors from the Sensor List page. The Security Cloud Control integration is the read-only *connection-events* sensor. Stealthwatch Cloud provides an overall health of your sensors in the main menu:

- green cloud icon ( ) - connectivity established with all sensors, and Security Cloud Control if configured
- yellow cloud icon ( ) - connectivity established with some sensors, or Security Cloud Control if configured, and one or more sensors is not configured properly
- red cloud icon ( ) - connectivity lost with all configured sensors, and Security Cloud Control if configured

Per sensor or Security Cloud Control integration, a green icon signifies connectivity established, and a red icon signifies connectivity lost.

Procedure

1. In the Secure Cloud Analytics portal UI, select **Settings** ( ) > **Sensors**.
2. Select **Sensor List**.

The Sensor List page displays the status of all configured sensors and Security Cloud Control integration, allowing you to identify any connectivity or configuration issues.

Cisco secure cloud analytics sensor deployment for total network analytics and reporting

Explains Cisco Secure Cloud Analytics sensor deployment for total network analytics and reporting, including configuration options for on-premises and cloud-based environments.

Cisco Secure Cloud Analytics sensor deployment for total network analytics and reporting is a network monitoring solution that

- deploys sensors within on-premises networks to pass network flow data to the cloud for analysis
- configures cloud-based deployments to pass network flow log data to Secure Cloud Analytics for analysis, and
- requires a Total Network Analytics and Monitoring license for provisioning a Secure Cloud Analytics portal.

Secure cloud analytics sensor overview and deployment

Required License: Total Network Analytics and Monitoring

If you obtain a **Total Network Analytics and Monitoring** license, after you provision a Secure Cloud Analytics portal, you can:

- Deploy and configure a Secure Cloud Analytics sensor within your on-premises network to pass network flow data to the cloud for analysis.
- Configure your cloud-based deployment to pass network flow log data to Secure Cloud Analytics for analysis.

Firewalls at your network perimeter gather information about traffic between your internal network and external networks, while Secure Cloud Analytics sensors gather information about traffic within your internal network.

Note

FDM-managedSecure Firewall Threat Defense devices may be configured to pass NetFlow data. When you deploy a sensor, do not configure it to pass NetFlow data from any of your FDM-managedSecure Firewall Threat Defense devices which you also configured to pass event information to Security Cloud Control.

See the Secure Cloud Analytics Sensor Installation Guide for sensor deployment instructions and recommendations.

See the Secure Cloud Analytics Public Cloud Monitoring Guides for cloud-based deployment configuration instructions and recommendations.

Note

You can also review instructions in the Secure Cloud Analytics portal UI to configure sensors and your cloud-based deployment.

See the Secure Cloud Analytics Free Trial Guide for more information about Secure Cloud Analytics.

Next steps:

- Continue with Cisco Secure Cloud Analytics alerts from Security Cloud Control on page 364.

Cisco Secure Cloud Analytics alerts from Security Cloud Control

Describes how to view Cisco Secure Cloud Analytics alerts from Security Cloud Control, including symptoms, checks, likely causes, and corrective actions for managed devices.

Cisco Secure Cloud Analytics alerts from Security Cloud Control are security notifications that

- are generated from firewall event data and network flow data
- require cross-launching from Security Cloud Control to the Secure Cloud Analytics portal for review, and
- display in the Security Analytics menu with a badge showing the number of open alerts.

License requirements and access methods

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

While you can review your firewall events on the Events logging page, you cannot review Cisco Secure Cloud Analytics alerts from the Security Cloud Control portal UI. You can cross-launch from Security Cloud Control to the Secure Cloud Analytics portal using the Security Analytics menu option, and view alerts generated from firewall event data (and from network flow data if you enabled **Total Network Analytics and Monitoring**). The Security Analytics menu option displays a badge with the number of Secure Cloud Analytics alerts in an open workflow status, if 1 or more are open.

If you use a Security Analytics and Logging license to generate Secure Cloud Analytics alerts, and you provisioned a new Secure Cloud Analytics portal, log into Security Cloud Control, then cross-launch to Secure Cloud Analytics using Cisco Security Cloud Sign On. You can also directly access your Secure Cloud Analytics portal through its URL.

See Cisco Security Cloud Sign On for more information.

Invite users to join your secure cloud analytics portal

Configure user access to your Secure Cloud Analytics portal by inviting users via email to join and create their Cisco Security Cloud Sign On credentials.

Invite other users by email to join your Secure Cloud Analytics portal and enable them to create Cisco Security Cloud Sign On credentials for cross-launch access from Security Cloud Control to Secure Cloud Analytics.

The initial user to request the Secure Cloud Analytics portal provision has administrator privileges in the Secure Cloud Analytics portal. That user can invite other users by email to join the portal. If these users do not have Cisco Security Cloud Sign On credentials, they can create them using the link in the invite email. Users can then use Cisco Security Cloud Sign On credentials to log in during the cross-launch from Security Cloud Control to Secure Cloud Analytics.

Before you begin

Follow these steps to invite other users to your Secure Cloud Analytics portal by email:

Procedure

1. Log into your Secure Cloud Analytics portal as an administrator.
2. Select **Settings** > **Account Management** > **User Management**.
3. Enter an **Email** address.
4. Click **Invite**.

The invited user receives an email invitation to join the Secure Cloud Analytics portal and can create Cisco Security Cloud Sign On credentials if needed.

Cross-launch from Security Cloud Control to Secure Cloud Analytics

Configure cross-launching to view security alerts from Security Cloud Control in Secure Cloud Analytics.

This task enables you to access and view security alerts through the integrated interface between Security Cloud Control and Secure Cloud Analytics.

To view security alerts from Security Cloud Control:

Procedure

1. Log into the Security Cloud Control portal.
2. In the left pane, choose **Analytics** > **Secure Cloud Analytics**.
3. In the Secure Cloud Analytics interface, select **Monitor** > **Alerts**.

You can now view and monitor security alerts from the Secure Cloud Analytics interface.

Cisco secure cloud analytics and dynamic entity modeling

Describes Cisco Secure Cloud Analytics and dynamic entity modeling, including translated addresses, rule behavior, interface scope, and policy impact.

Cisco Secure Cloud Analytics is a software as a service (SaaS) solution that

- monitors your on-premises and cloud-based network deployments by gathering information about your network traffic from sources including firewall events and network flow data,
- creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns, and
- generates alerts using this information combined with other sources of threat intelligence, such as Talos, which constitute a warning that there is behavior that may be malicious in nature.

License requirements

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

Dynamic entity modeling overview:

Dynamic entity modeling tracks the state of your network by performing a behavioral analysis on firewall events and network flow data. In the context of Secure Cloud Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they take on your network.

Secure Cloud Analytics, integrated with a **Logging Analytics and Detection** license, can draw from firewall events and other traffic information in order to determine the types of traffic the entity usually transmits. If you purchase a **Total Network Analytics and Monitoring** license, Secure Cloud Analytics can also include NetFlow and other traffic information in modeling entity traffic. Secure Cloud Analytics updates these models over time, as the entities continue to send traffic, and potentially send different traffic, to keep an up-to-date model of each entity.

From this information, Secure Cloud Analytics identifies:

- Roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Cloud Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- Observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, or a remote access session established with another entity. If you integrate with Security Cloud Control, these facts can be obtained from firewall events. If you also purchase a **Total Network Analytics and Monitoring** license, the system can also obtain facts from NetFlow, and generate observations from both firewall events and NetFlow. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

Alerts and analysis process

Based on the combination of roles, observations, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system. Note that one alert may represent multiple observations. If a firewall logs multiple connection events related to the same connection and entities, this may result in only one alert.

For example, a New Internal Device observation on its own does not constitute possible malicious behavior. However, over time, if the entity transmits traffic consistent with a Domain Controller, then the system assigns a Domain Controller role to the entity. If the entity subsequently establishes a connection to an external server that it has not established a connection with previously, using unusual ports, and transfers large amounts of data, the system would log a New Large Connection (External) observation and an Exceptional Domain Controller observation. If that external server is identified as on a Talos watchlist, then the combination of all this information would lead Secure Cloud Analytics to generate an alert for this entity's behavior, prompting you to take further action to research, and remediate malicious behavior.

When you open an alert in the Secure Cloud Analytics web portal UI, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about the entities involved, including the traffic that they transmitted, and external threat intelligence if it is available. You can also see other observations and alerts that entities were involved with, and determine if this behavior is tied to other potentially malicious behavior.

> **Note**
>
> When you view and close alerts in Secure Cloud Analytics, you cannot allow or block traffic from the Secure Cloud Analytics UI. You must update your firewall access control rules to allow or block traffic, if you deployed your devices in active mode, or your firewall access control rules if your firewalls are deployed in passive mode.

Alerts based on firewall events

Describes the workflow for working with alerts based on firewall events, including event details, device status, reporting views, and follow-up actions.

An alert based on firewall events is a security notification that

- generates from observations produced by firewall event data
- follows a workflow based on status changes from open to closed
- allows assignment, tagging, and investigation to help identify and resolve potential security issues, and
- requires a Logging Analytics and Detection or Total Network Analytics and Monitoring license.

Alert workflow process

When the system generates an alert, the default status is Open, and no user is assigned. When you view the Alerts summary, all open alerts are displayed by default, as these are of immediate concern.

> **Note**
>
> If you have a **Total Network Analytics and Monitoring** license, your alerts can be based on observations generated from NetFlow, observations generated from firewall events, or observations from both data sources.

As you review the Alerts summary, you can assign, tag, and update status on alerts as an initial triage. You can use the filters and search functionality to locate specific alerts, or display alerts of different statuses, or associated with different tags or assignees. You can set an alert's status to Snoozed, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove Snoozed status from an alert, to display it as an open alert again. As you review alerts, you can assign them to yourself or another user in the system. Users can search for all alerts assigned to their username.

From the Alerts summary, you can view an alert detail page. This page allows you to review additional context about the supporting observations that resulted in this alert, and additional context about the entities involved in this alert. This information can help you pinpoint the actual issue, in order to further research the issue on your network, and potentially resolve malicious behavior.

As you research within the Secure Cloud Analytics web portal UI, in Security Cloud Control, and on your network, you can leave comments with the alert that describe your findings. This helps create a record for your research that you can reference in the future.

If you complete your analysis, you can update the status to Closed, and have it no longer appear by default as an open alert. You can also re-open a closed alert in the future if circumstances change.

These general guidelines and suggestions for investigating alerts use the additional context that Secure Cloud Analytics provides when it logs an alert to help guide your investigation.

These steps are meant to be neither comprehensive, nor all-inclusive. They merely offer a general framework with which to start investigating an alert.

You can take these steps when you review an alert:

1. Best practice for triaging open alerts on page 368
2. Snooze alerts for later analysis on page 369
3. Update the alert for further investigation on page 369
4. Review the alert and start your investigation on page 370
5. Examine the entity and users on page 371
6. Best practice for remediating issues using secure cloud analytics on page 372
7. Update and close the alert on page 373

Best practice for triaging open alerts

Outlines the systematic approach for investigating and prioritizing open alerts, particularly when multiple alerts require attention.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

Triage the open alerts, especially if more than one have yet to be investigated:

- See Monitoring Secure Cloud Analytics Alerts Generated from FTD Events for more information on cross-launching from Security Cloud Control to Secure Cloud Analytics, and viewing alerts.
- Have you configured this alert type as high priority?

- Did you set a high sensitivity for the affected subnet?
- Is this unusual behavior from a new entity on your network?
- What is the entity's normal role, and how does the behavior in this alert fit that role?
- Is this an exceptional deviation from normal behavior for this entity?
- If a user is involved, is this expected behavior from the user, or exceptional?
- Is protected or sensitive data at risk of being compromised?
- How severe is the impact to your network if this behavior is allowed to continue?
- If there is communication with external entities, have these entities established connections with other entities on your network in the past?

If this is a *high* priority alert, consider quarantining the entity from the internet, or otherwise closing its connections, before continuing your investigation.

Snooze alerts for later analysis

Configure alert snoozing to temporarily hide lower-priority alerts from the active alert list for later review.

Snooze alerts when they are of lesser priority, as compared to other alerts, allowing you to focus on more critical alerts while preserving lower-priority alerts for future analysis.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

For example, if your organization is repurposing an email server as an FTP server, and the system generates an Emergent Profile alert (indicating that an entity's current traffic matches a behavior profile that it did not previously match), you can snooze this alert as it is intended behavior, and revisit it at a later date. A snoozed alert does not show up with the open alerts; you must specifically filter to review these snoozed alerts.

Follow these steps to snooze an alert:

Procedure

1. Click **Close Alert**.
2. In the Snooze this alert pane, select a snooze period from the drop-down.
3. Click **Save**.

   When you are ready to review these alerts, you can unsnooze them. This sets the status to Open, and displays the alert alongside the other Open alerts.

   Unsnooze a snoozed alert:

   - From a snoozed alert, click **Unsnooze Alert**.

The alert is snoozed for the selected period and removed from the active alerts view until the snooze period expires or you manually unsnooze it.

Update the alert for further investigation

Configure alert assignment and tagging to enable further investigation and tracking of security events.

Update alerts with assignment and categorization information to enable effective investigation and establish tracking patterns for security events.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

Open the alert detail and prepare to assign and categorize the alert for investigation.

Procedure

1. Select **Monitor** > **Alerts**.
2. Click an alert type name.

What to do next:

Based on your initial triage and prioritization, assign the alert and tag it:

a. Select a user from the **Assignee** drop-down to assign the alert, so a user can start investigating.

b. Select one or more **Tags** from the drop-down to add tags to the alert, to better categorize your alert's for future identification, as well as to try and establish long-term patterns in your alerts.

c. Enter a **Comment on this alert**, then click **Comment** to leave comments as necessary to track your initial findings, and assist the person assigned to the alert. The alert tracks both system comments and user comments.

The alert is assigned to a specific user with appropriate tags and comments, enabling organized investigation and tracking of security events.

Review the alert and start your investigation

Configure your investigation process by reviewing alert details and analyzing supporting observations to determine if source entity behavior indicates malicious activity.

Review the alert detail to understand why Secure Cloud Analytics generated an alert and examine supporting observations to understand what these observations mean for the source entity.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

If you are reviewing an assigned alert, review the alert detail to understand why Secure Cloud Analytics generated an alert. Review the supporting observations to understand what these observations mean for the source entity.

Note that if the alert was generated based on firewall events, the system does not note that your firewall deployment was the source of this alert.

View all of the supporting observations for this source entity to understand its general behavior and patterns, and see if this activity may be part of a longer trend:

Procedure

1. From the alert detail, click the arrow icon () next to an observation type to view all logged observations of that type.
2. Click the arrow icon () next to **All Observations for Network** to view all logged observations for this alert's source entity.

Download the supporting observations in a comma-separated value file, if you want to perform additional analysis on these observations:

- From the alert detail, in the Supporting Observations pane, click **CSV**.

From the observations, determine if the source entity behavior is indicative of malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet.

View additional context surrounding the source entity from a source entity IP address or hostname, including other alerts and observations it may be involved in, information about the device itself, and what type of session traffic it is transmitting:

- Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
- Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
- Select **Device** from the IP address or hostname drop-down to view information about the device.
- Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that the source entity in Secure Cloud Analytics is always internal to your network. Contrast this with the Initiator IP in a firewall event, which indicates the entity that initiated a connection, and may be internal or external to your network.

From the observations, examine information about other external entities. Examine the geolocation information, and determine if any of the geolocation data or Umbrella data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior.

Review the context for an external entity IP address or hostname with which the source entity established a connection:

- Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
- Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
- Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
- Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
- Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
- Select **Talos Intelligence** from the IP address or hostname drop-down to view information about this information on Talos's website.
- Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
- Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that connected entities in Secure Cloud Analytics are always external to your network. Contrast this with the Responder IP in a firewall event, which indicates the entity that responded to a connection request, and may be internal or external to your network.

Leave comments as to your findings.

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Examine the entity and users

Configure examination procedures for source entities and users involved in firewall-based security alerts to identify potential malicious activity or unauthorized access.

Perform detailed examination of source entities and users following alert review to identify potential security threats, malware, vulnerabilities, or unauthorized activities that triggered the alert.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

After you review the alert in the Secure Cloud Analytics portal UI, you can perform an additional examination on a source entity directly, any users that may have been involved with this alert, and other related entities.

Procedure

1. Examine the source entity location and access logs

   Determine where the source entity is on your network, physically or in the cloud, and access it directly. Locate the log files for this entity. If it is a physical entity on your network, access the device to review the log information, and see if there is any information as to what caused this behavior. If it is a virtual entity, or stored in the cloud, access the logs and search for entries related to this entity. Examine the logs for further information on unauthorized logins, unapproved configuration changes, and the like.

2. Examine the entity for malware and vulnerabilities

   Examine the entity. Determine if you can identify malware or a vulnerability on the entity itself. See if there has been some malicious change, including if there are physical changes to a device, such as a USB stick that is not approved by your organization.

3. Investigate user involvement

   Determine if a user on your network, or from outside your network, was involved. Ask the user what they were doing if possible. If the user is unavailable, determine if they were supposed to have access, and if a situation occurred that prompted this behavior, such as a terminated employee uploading files to an external server before leaving the company.

4. Enter a **Comment on this alert**, then click **Comment**

   Leave comments as to your findings from the alert detail.

You have examined the source entity, users, and related components to identify potential security threats and documented your findings in the alert comments for future reference and investigation tracking.

Best practice for remediating issues using secure cloud analytics

Outlines remediation actions for malicious behavior detected through Secure Cloud Analytics alerts.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

If malicious behavior caused the alert, remediate the malicious behavior.

- If a malicious entity or user attempted to log in from outside your network, update your firewall rules and firewall configuration to prevent the entity or user from accessing your network.
- If an entity attempted to access an unauthorized or malicious domain, examine the affected entity to determine if malware is the cause. If there are malicious DNS redirects, determine if other entities on your network are affected, or part of a botnet. If this is intended by a user, determine if there is a legitimate reason for this, such as testing firewall settings. Update your firewall rules and firewall configuration to prevent further access to the domain.
- If an entity is exhibiting behavior that is different from the historical entity model behavior, determine if the behavior change is intended. If it is unintended, examine whether an otherwise authorized user on your network is responsible for the change. Update your firewall rules and firewall configuration to address unintended behavior if it involves connections with entities that are external to your network.
- If you identify a vulnerability or exploit, update or patch the affected entity to remove the vulnerability, or update your firewall configuration to prevent unauthorized access. Determine if other entities on your network may similarly be affected, and apply the same update or patch to those entities. If the vulnerability or exploit currently does not have a fix, contact the appropriate vendor to let them know.

- If you identify malware, quarantine the entity and remove the malware. Review the firewall file and malware events to determine if other entities on your network are at risk, and quarantine and update the entities to prevent this malware from spreading. Update your security intelligence with information about this malware, or the entities that caused this malware. Update your firewall access control and file and malware rules to prevent this malware from infecting your network in the future. Alert vendors as necessary.
- If malicious behavior resulted in data exfiltration, determine the nature of the data sent to an unauthorized source. Follow your organization's protocols for unauthorized data exfiltration. Update your firewall configuration to prevent future data exfiltration attempts by this source.

Update and close the alert

Configure alert tags and close alerts after completing your security investigation in Secure Cloud Analytics.

Update alerts with relevant tags and close them after completing your security investigation to maintain accurate alert tracking and provide feedback on alert usefulness.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

Add additional tags based on your findings:

Procedure

1. In the Secure Cloud Analytics portal UI, select **Monitor** > **Alerts**.
2. Select one or more **Tags** from the drop-down.

Add final comments describing the results of your investigation, and any remediation steps taken:

- From an alert's detail, enter a **Comment on this alert**, then click **Comment**.

Close the alert, and mark it as helpful or not helpful:

1. From an alert's detail, click **Close Alert**.
2. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. Note that this does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
3. Click **Save**.

Reopen a closed alert

If you discover additional information related to a closed alert, or want to add more comments related to that alert, you can reopen it, changing the status to Open. You can then make changes as necessary to the alert, then close it again when your additional investigation is complete.

Reopen a closed alert:

- From a closed alert's detail, click **Reopen Alert**.

Modify alert priorities

Configure alert priorities to adjust system sensitivity for generating alerts based on your network environment requirements.

Modifying alert priorities allows you to customize how sensitive the system is to generating alerts of specific types, emphasizing certain alerts that are of concern in your network environment.

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Alert types come with default priorities, which affect how sensitive the system is to generating alerts of this type. Alerts default to *low* or *normal* priority, based on Cisco intelligence and other factors. Based on your network environment, you may want to reprioritize alert types, to emphasize certain alerts that you are concerned with. You can configure any alert type to be *low*, *normal*, or *high* priority.

Procedure

1. Select **Monitor** > **Alerts**.
2. Click the settings drop-down icon (), then select **Alert Types and Priorities**.
3. Click the edit icon () next to an alert type and select *low*, *medium*, or *high* to change the priority.

The alert priority is modified according to your selection, affecting the system's sensitivity to generating alerts of that type.

17 Upgrade Secure Firewall ASA

Topics:

- Upgrade ASA and ASDM images using Security Cloud Control Firewall Management
- Upgrade ASA Secure Client Packages
- Upgrade bulk ASA and ASDM in Security Cloud Control Firewall Management
- Upgrade ASA and ASDM images on a single ASA
- Upgrade ASA and ASDM images in a high availability pair
- Upgrade an ASA or ASDM using your own image

This chapter describes the various ways in which you can upgrade a Secure Firewall ASA device.

Upgrade ASA and ASDM images using Security Cloud Control Firewall Management

Find prerequisites for ASA and ASDM upgrades in Security Cloud Control Firewall Management, including image repository options, connectivity, synchronization, custom URL requirements, supported device models, failover limits, and minimum software versions.

Security Cloud Control provides a wizard that helps you upgrade the ASA and ASDM images installed on an individual ASA, multiple ASAs, ASAs in an active-standby configuration, and ASAs running in single-context or multi-context mode.

Security Cloud Control Firewall Management maintains a repository of ASA and ASDM images that you can upgrade to. When you choose your upgrade images from Security Cloud Control Firewall Management's image repository, Security Cloud Control Firewall Management performs all the necessary upgrade steps behind the scenes. The wizard guides you through the process of choosing compatible ASA software and ASDM images, installs them, and reboots the device to complete the upgrade. We secure the upgrade process by validating that the images you chose on Security Cloud Control are the ones copied to, and installed on, your ASA. Security Cloud Control Firewall Management periodically reviews its inventory of ASA binaries and adds the newest ASA and ASDM images to its repository when they are available. This is the best option for customers whose ASAs have outbound access to the internet.

Security Cloud Control's image repository only contains generally available (GA) images. If you do not see a specific GA image in the list, please contact Cisco TAC or email support from the **Contact Support** page. We will process the request using the established support ticket SLAs and upload the missing GA image.

If your ASAs do not have outbound access to the internet, you can download the ASA and ASDM images you want from Cisco.com, store them in your own repository, provide the upgrade wizard with a custom URL to those images, and Security Cloud Control performs upgrades using those images. In this case, however, you determine what images you want to upgrade to. Security Cloud Control does not perform the image integrity check or disk-space check. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB.

Configuration Prerequisites for All ASAs

- DNS needs to be enabled on the ASA.
- ASA should be able to reach the internet if you use upgrade images from Security Cloud Control Firewall Management's image repository.
- Ensure HTTPS connectivity between the ASA and the repository FQDN.
- The ASA has been successfully onboarded to Security Cloud Control Firewall Management.
- The ASA is synced to Security Cloud Control Firewall Management.
- The ASA is online.
- For custom URL upgrades:
  - Use the Cisco ASA Upgrade Guide to determine what version of ASA and ASDM are compatible with your ASAs.
  - Download the ASA and ASDM images to your image repository.
  - Ensure that the ASA has access to your image repository.
  - Ensure you have enough disk space on your ASA for your ASA and ASDM images.
  - Read Custom URL Upgrade for URL syntax information.

Configuration Prerequisites for Firepower 1000 and Firepower 2100 Series Devices

- The FXOS mode of a Firepower 2100 series device must be configured for **appliance** mode. See Set the Firepower 2100 to Appliance or Platform Mode for more information.
- The device must be running ASA Version 9.13(1) or later.

- You must upgrade the FXOS bundle prior to upgrading the ASA software. See Firepower 2100 ASA and FXOS Compatibility for more information.

Firepower 4100 and Firepower 9300 Series Devices Running ASA

Security Cloud Control does not support the upgrade for the Firepower 4100 or Firepower 9300 series devices. You must upgrade these devices outside of Security Cloud Control.

Upgrade Guidelines

- Security Cloud Control can upgrade ASAs configured as an Active/Standby "failover" pair. Security Cloud Control cannot upgrade ASAs configured in an Active/Active "clustered" pair.

Software and Hardware Prerequisites

Minimum ASA and ASDM versions from which you can upgrade:

- ASA: ASA 9.1.2
- ASDM: There is no minimum version.

Supported Hardware Versions

- See ASA Software and Hardware Support.

Upgrade ASA Secure Client Packages

Explains how ASA Secure Client package upgrades are managed and distributed to users by Cloud Control.

A Secure Client package upgrade is a software distribution feature that

- enables administrators to manage and deploy Cisco Secure Client (formerly AnyConnect) webdeploy packages,
- automates upgrades for users connecting to ASA Remote Access (RA) VPN headends, and
- ensures that managed organizations receive the latest client versions seamlessly upon VPN connection.

Benefits for ASA Secure Client Packages Upgrade

- Simplify the upgrade process by utilizing a centralized, guided workflow.
- Upgrade Secure Client packages for multiple ASA RA VPN headends.
- Provides full visibility into currently installed packages to verify compatibility before deployment.
- Updates all platforms simultaneously or target specific operating systems.

Upgrade ASA Secure Client Packages

Follow the steps below to select compatible versions, manage platform-specific packages, and monitor your deployment status.

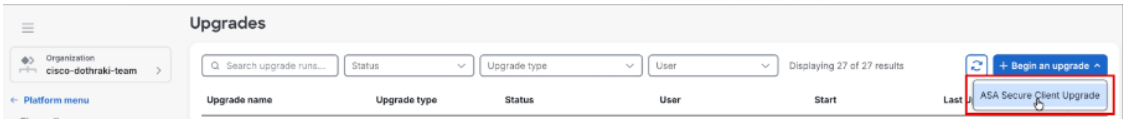
Before you begin

Before initiating an upgrade, ensure your devices meet the following criteria:

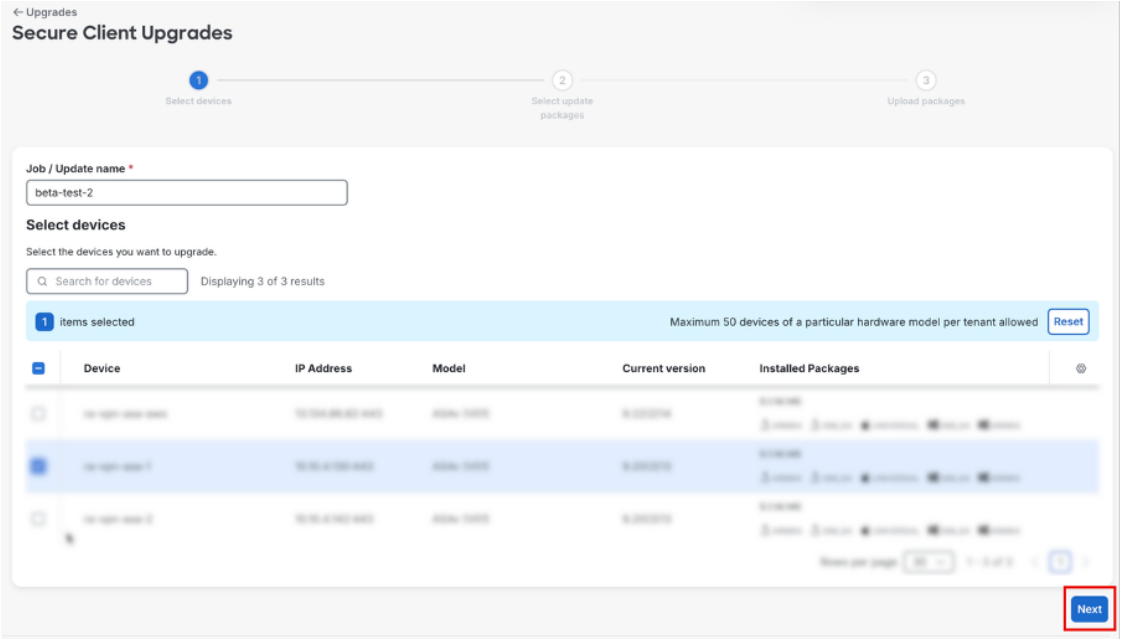
- Devices must be online and synced with Security Cloud Control Firewall Management for connectivity.
- Devices must be configured as ASA RA VPN headends.

Procedure

1. From the Security Cloud Control Firewall Management Home page, click **Firewall**.
2. Choose **Operations > Upgrades**.
3. Click **Begin an Upgrade** and select **ASA Secure Client Upgrade** from the drop-down list.



4. Enter a name for your upgrade in the **Job / Update name** name field.
5. Select the ASA devices you want to upgrade and click **Next**.



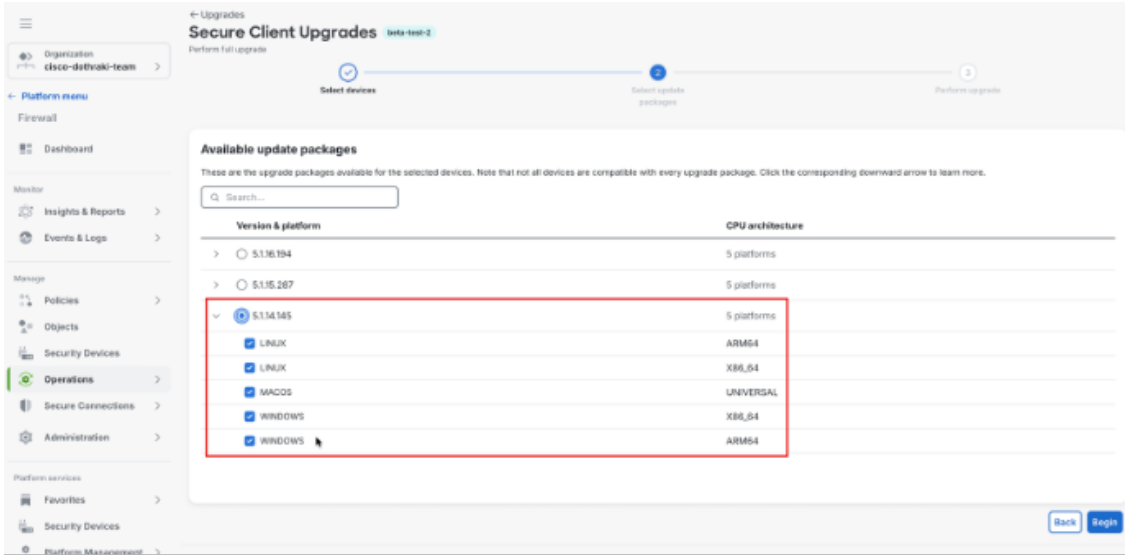
Note

- Only eligible ASA RA VPN headends are displayed.
- The device list includes information such as device name, IP address, model, current version, and installed Secure Client packages.

6. Select the Secure Client version you want to install.

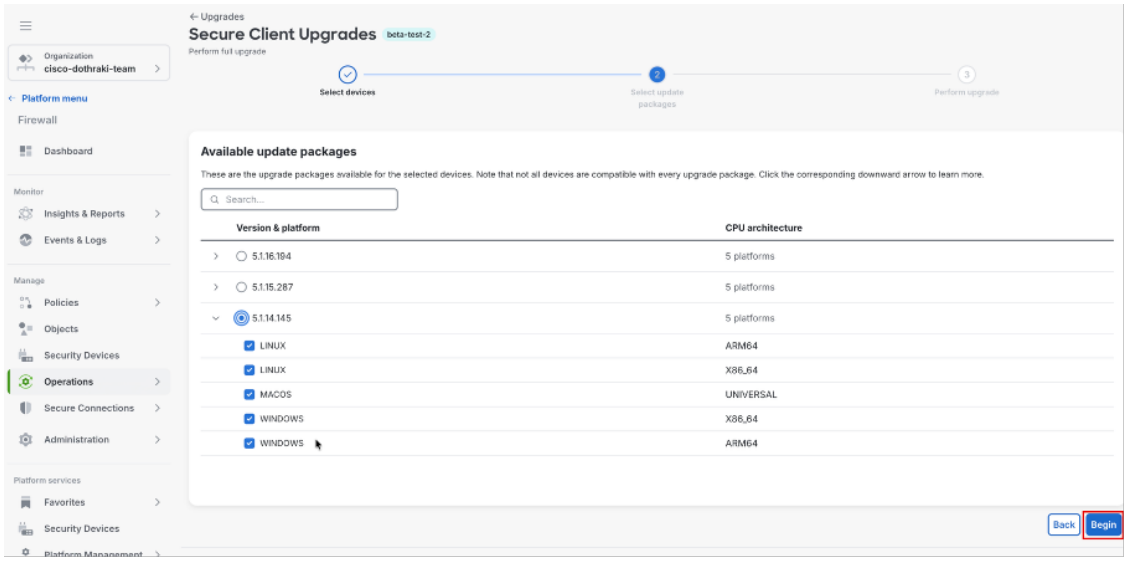
   Note: The available versions are based on compatibility with the selected ASA devices. Not all devices are compatible with every Secure Client version.

7. Review the available platform packages for the selected version.

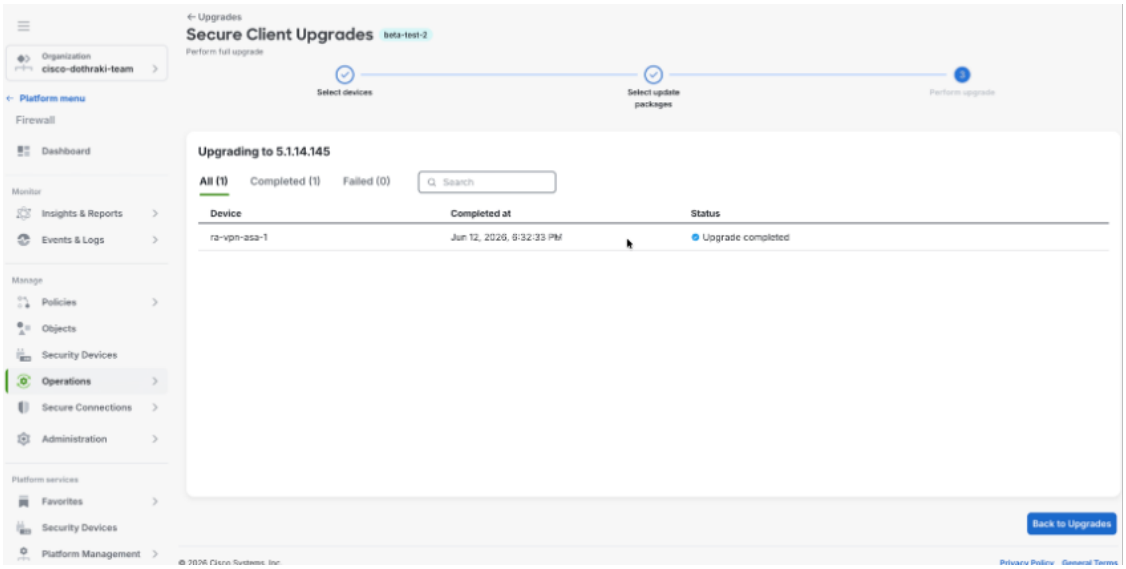


Note: By default, all available platforms are selected. To upgrade only specific packages, select the required platforms, such as Windows, macOS, or Linux.

8. Click **Begin** to start the upgrade.



9. Click **Back to Upgrades** to navigate to the **Upgrades** page and monitor your progress.



Note

The Status column provides real-time updates on your upgrade; if the process fails or completes with warnings, you must check this column to review the specific error details.

Your selected ASA devices now run the upgraded Secure Client packages. Real-time progress and errors appear in the Status column.

Upgrade bulk ASA and ASDM in Security Cloud Control Firewall Management

Learn how to upgrade ASA and ASDM images on multiple ASA devices in Security Cloud Control Firewall Management using compatible images from the Cisco repository or your own repository.

Procedure

1. Review ASA and ASDM Upgrade Prerequisites for upgrade requirements and important information about upgrading ASA and ASDM images.

   Note

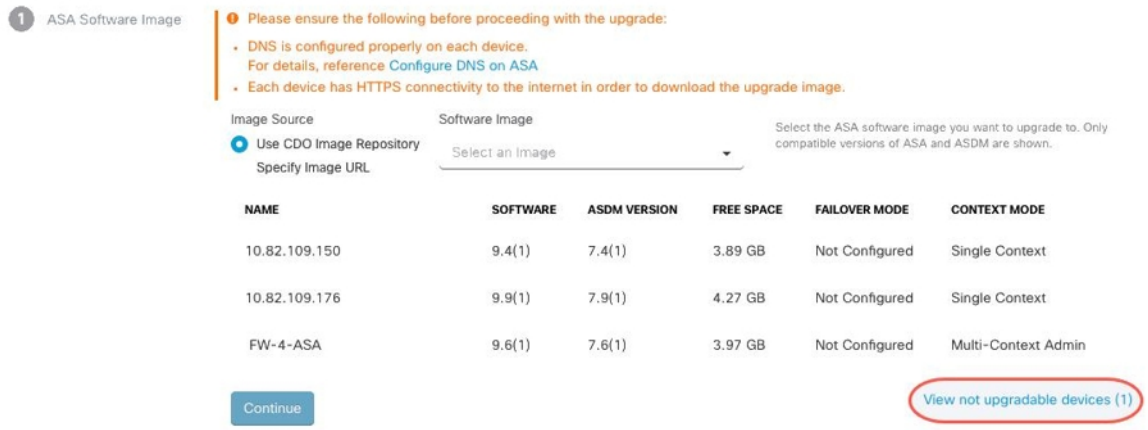
   If you are upgrading an ASA 1000 or 2000 series device, be sure to read Configuration Prerequisites for 1000 and 2000 Series.

2. (Optional) In the left pane, click **Security Devices**.
3. Create a change request label to identify the devices upgraded by this action in the change log.
4. Click the **Devices** tab.
5. Use the filter to narrow down the list of devices you may want to include in your bulk upgrade.

6. From the filtered list of devices, select the devices you want to upgrade.

> **Note**
>
> You can include up to 50 ASA devices in a single immediate or scheduled bulk upgrade job. For large fleets, we recommend upgrading devices in smaller batches so that you can monitor upgrade progress and recover more easily if an issue occurs.

7. In the **Device Actions** pane, click **Upgrade**.
8. On the Bulk Device Upgrade page, the devices that can be upgraded are presented to you. If any of the devices you chose are not upgradable, Security Cloud Control gives you a link to view the not upgradable devices.



9. In step 1, click **Use** Security Cloud Control **Image Repository** to select the ASA software image you want to upgrade to, and click **Continue**.

   The list indicates how many of the ASAs you chose can be upgraded to the software version you chose. In the example below, all of the devices can be upgraded to version 9.9(1.2), two devices can be upgraded to 9.8(2), and one of the devices can be upgraded to 9.6(1).



   Security Cloud Control alerts you if any of the software versions you chose are incompatible with any of the devices you chose. In the example below, Security Cloud Control cannot upgrade the 10.82.109.176 device to a version earlier than it already runs.

NAME	SOFTWARE	ASDM VERSION	FREE SPACE	FAILOVER MODE	CONTEXT MODE
✔ 10.82.109.150	9.4(1)	7.4(1)	3.89 GB	Not Configured	Single Context
✔ FW-4-ASA	9.6(1)	7.6(1)	3.97 GB	Not Configured	Multi-Context Admin
✖ 10.82.109.176	9.9(1)	7.9(1)	4.27 GB	Not Configured	Single Context

10. In step 2, select the ASDM image you want to upgrade to. You are only presented with ASDM choices that are compatible with the ASA you can upgrade.

11. In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.
12. Click **Perform Upgrade** when you are ready.

> **Note**
>
> If the upgrade fails, Security Cloud Control displays a message. Often the reason for a failed upgrade is a network issue preventing the ASA and ASDM images from being transferred to the ASA.

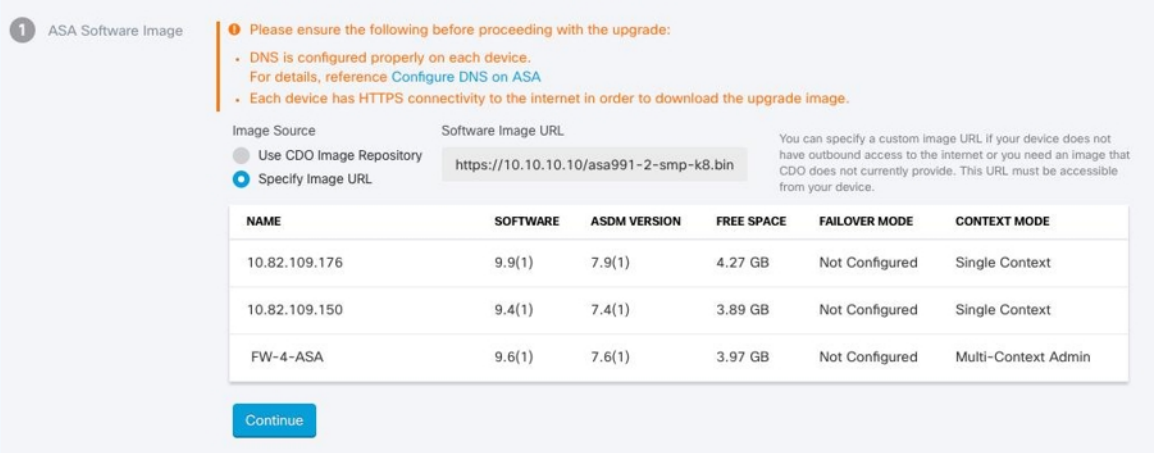
13. Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.
14. (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade.
15. Look at the notifications tab (notifications tab) for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Jobs page (Jobs page).
16. If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

Upgrade Multiple ASAs with Images from your own Repository

Procedure

1. Review ASA and ASDM Upgrade Prerequisites for upgrade requirements and important information about upgrading ASA and ASDM images.
2. (Optional) In the left pane, click **Security Devices**.
3. Create a change request label to identify the devices upgraded by this action in the change log.
4. Click the **Devices** tab.
5. Use the Filters on security devices, policies, and objects page on page 854 to narrow down the list of devices you may want to include in your bulk upgrade.
6. From the filtered list of devices, select the devices you want to upgrade.
7. In the **Device Actions** pane, click **Upgrade**.
8. In step 1, click **Specify Image URL,** enter the URL to the ASA image you want to upgrade to in the In the **Software Image URL** field, and click **Continue**. See Custom URL Upgrade for URL syntax information.

> **Note**
>
> The picture below shows an HTTPS URL in the Software Image URL field. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB. See Custom URL Upgrade for URL syntax information.



9. In step 2, click **Specify Image URL,** enter the URL to the ASDM image you want to upgrade to in the In the **Software Image URL** field, and click **Continue**.
10. In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.
11. Click **Perform Upgrade** when you are ready.

> **Note**
>
> If the upgrade fails, Security Cloud Control displays a message. Often the reason for a failed upgrade is a network issue preventing the ASA and ASDM images from being transferred to the ASA.

12. Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.
13. (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade.
14. Look at the notifications tab (notifications tab) for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Jobs page (Jobs page).
15. If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

Upgrade Notes:

- You can also monitor the progress of the batch of upgrades by opening the **Security Devices** page and viewing the Configuration Status column in the table.

- You can view the progress of a single device that was included in the bulk upgrade by selecting that device on the **Security Devices** page and clicking the upgrade button. Security Cloud Control takes you to the Device Upgrade page for that device.

Upgrade ASA and ASDM images on a single ASA

Learn how to upgrade ASA and ASDM images on a single ASA in Security Cloud Control Firewall Management using Cisco repository images or custom image URLs.

Follow this procedure to upgrade the ASA and ASDM images on a single ASA.

Procedure

1. Review ASA and ASDM Upgrade Prerequisites for upgrade requirements and important information about upgrading ASA and ASDM images.

   Note

   If you are upgrading an ASA 1000 or 2000 series device, be sure to read Configuration Prerequisites for 1000 and 2000 Series.

2. In the left pane, click **Security Devices**.
3. Click the **Devices** tab.
4. (Optional) Create a change request label to identify the device upgraded by this action in the change log.
5. Select the device you want to upgrade.
6. In the **Device Actions** pane, click **Upgrade**.
7. On the Device Upgrade page, follow the instructions presented to you by the wizard.
   a. In step 1, click **Use** Security Cloud Control **Image Repository** to select the ASA software image you want to upgrade to, and click **Continue**.

      Note

      When upgrading your ASAs and ASDMs to images stored in your own repository, select **Specify Image URL** and enter the URL of the ASA or ASDM image in the Software Image URL field. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB. See Custom URL Upgrade for URL syntax information.

      (Optional) If you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click **Schedule Upgrade**.

   b. In step 2, select the ASDM image you want to upgrade to. You are only presented with ASDM choices that are compatible with the ASA you can upgrade.

c. In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.

8. Click **Perform Upgrade** when you are ready.
9. (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade. Want to see a demo? Watch a screencast of this procedure!

Upgrade Notes

- If you select an image to upgrade to, and you change your mind, check the **Skip Upgrade** check box associated with the software image. The image will not be copied to the device, nor will the device be upgraded with the image.
- In the **Perform Upgrade** step, if you choose only to copy the images to the ASA, you can return to the Device Upgrade page later and click "Upgrade Now" to perform the upgrade. After the copying task is complete, you will see the message "Ready to Upgrade" for that device on the **Security Devices** page.
- You cannot take action on a device during the process of copying the image, installing it, and rebooting the device. Devices that are installing the image and then rebooting are shown as "Upgrading" in the **Security Devices** page.
- You cannot take action on a device during the upgrade process; that is, installing the image and rebooting the device.
- You can take action on a device if you choose only to copy the images to the device. Devices that are copying images are shown as "Copying Images" in the **Security Devices** page.
- Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Upgrade ASA and ASDM images in a high availability pair

Learn how to upgrade ASA and ASDM images in an active/standby high availability pair in Security Cloud Control, including workflow, prerequisites, upgrade sequence, and failover behavior.

Security Cloud Control Firewall Management supports upgrading Cisco Secure Firewall ASA devices that are configured in an Active/Standby High Availability (HA) pair.

During the upgrade, Security Cloud Control Firewall Management upgrades the devices sequentially to minimize traffic disruption:

1. The standby ASA is upgraded first.
2. The standby device reboots and returns to the Standby-Ready state.
3. Security Cloud Control Firewall Management initiates a failover, making the upgraded device the active ASA.
4. The primary ASA device is then upgraded and rebooted.

Because one device remains active during most of the process, the upgrade provides **near-zero downtime**. During the failover event, a brief traffic interruption or a small number of dropped packets may occur depending on the network environment.

If you need more information about how ASAs are configured and work in failover mode, see Failover for High Availability in the ASA documentation.

Workflow for upgrading an ASA high availability pair

The following workflow describes how Secure Firewall Management Center upgrades ASA devices in an Active/Standby high availability pair.

1. Download images to both devices

   Secure Firewall Management Center downloads the ASA and ASDM images to both devices in the high availability pair.

   > **Note**
   >
   > Users have the choice of downloading ASA and ASDM images but not upgrading immediately. If the ASA and ASDM images were downloaded previously, Security Cloud Control will not download them again; Security Cloud Control continues the upgrade workflow with the next step.

2. Secure Firewall Management Center upgrades the standby device

   The secondary ASA (standby device) is upgraded and rebooted while the primary ASA continues to process traffic.

3. Verify standby readiness

   After reboot, the upgraded device enters the Standby-Ready state.

4. Initiate failover

   Secure Firewall Management Center initiates a failover so that the upgraded device becomes the active ASA.

5. Upgrade the remaining device

   The original primary ASA, which is now the standby device, is upgraded and rebooted.

6. Restore the original active device

   After the device returns to the Standby-Ready state, Secure Firewall Management Center initiates another failover so that the original primary ASA becomes active again.

This process ensures that one device remains active throughout the upgrade, minimizing service interruption.

> **Warning**
>
> Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Workflow

This is the process by which Security Cloud Control upgrades the active/standby pair of ASAs:

Procedure

1. Security Cloud Control downloads the ASA and ASDM images to both ASAs.

> **Note**
>
> Users have the choice of downloading ASA and ASDM images but not upgrading immediately. If the ASA and ASDM images were downloaded previously, Security Cloud Control will not download them again; Security Cloud Control continues the upgrade workflow with the next step.

2. Security Cloud Control upgrades the secondary ASA first.
3. Once the upgrade is complete and the secondary ASA returns to the "Standby-Ready" state, Security Cloud Control initiates a failover so that the secondary ASA becomes the active ASA.
4. Security Cloud Control upgrades the primary ASA, which is now the current standby ASA.
5. Once the primary ASA returns to the "Standby-Ready" state, Security Cloud Control initiates a failover so that the primary ASA becomes the active ASA.

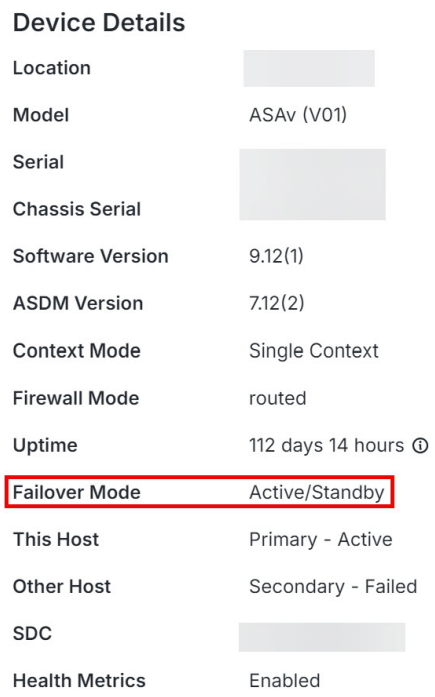
> **Warning**
>
> Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Upgrade ASA and ASDM Images in a high availability pair

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Select the device you want to upgrade.
4. In the **Device Actions** pane, click **Upgrade**.

   Notice that the failover mode of the device is Active/Standby:



5. (Optional) If you want Secure Firewall Management Center to perform the upgrade later, select the **Schedule Upgrade** check box. Click the field to select a date and time in the future. When you are done, click **Done**.
6. In step 1, click **Use SCC Image Repository** to select the ASA software image you want to upgrade to, and click **Continue**.

   If you are upgrading from images stored in your own repository, select **Specify Image URL** and enter the image location. Supported protocols include FTP, TFTP, HTTP, HTTPS, SCP, and SMB.

   See Custom URL Upgrade for URL syntax information.
7. In step 2, select the ASDM image you want to upgrade to. You are only presented with ASDM choices that are compatible with the ASA you can upgrade.
8. In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.
9. Click **Perform Upgrade**.

Secure Firewall Management Center automatically performs the HA upgrade workflow described earlier.

> **Note**
>
> The upgrade process is designed to provide near-zero downtime. If the upgrade of the standby device fails, the process stops and a failure notification is sent by email or webhook, if configured, or displayed in the user interface.

Upgrade an ASA or ASDM using your own image

Learn how to upgrade ASA or ASDM images in Security Cloud Control Firewall Management using images from your own repository and supported custom image URLs.

When you upgrade your ASA with new ASA software and ASDM images, you can either use images that Learn how to upgrade ASA or ASDM images in Security Cloud Control using images from your own repository and supported custom image URLs. stores in its image repository or you can use images that you store in your own image repository. If your ASA does not have outbound access to the internet, maintaining your own image repository is the best option for upgrading your ASAs using Learn how to upgrade ASA or ASDM images in Security Cloud Control using images from your own repository and supported custom image URLs..

Learn how to upgrade ASA or ASDM images in Security Cloud Control using images from your own repository and supported custom image URLs. uses ASA's copy command to retrieve the image and copy it to the flash drive (disk0:/) of your ASA. In the Specify Image URL field you are providing the URL portion of the copy command. For example, if the whole copy command would have been:

```
ciscoasa# copy ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin disk:/0
```

You are providing:

```
ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin
```

in the Specify Image URL field.

Security Cloud Control supports http, https, ftp, tftp, smb, and scp methods of retrieving the upgrade image.

URL Syntax examples

Here are examples of URL syntax for the ASA copy command. For the sake of these URL examples, assume the following:

- **Image repository address**: 10.10.10.10
- **Username to access the image repository**: admin
- **Password**: adminpass
- **Path**: images/asa
- **Image filename**: asa991-smp-k8.bin

http[**s**]**://** [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename*]

```
https://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin
HTTP[s] example without a username and password:
https://10.10.10.10:8080/images/asa/asa991-smp-k8.bin
```

ftp:// [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename* [**;type=** *xx*]]â€”The **type** can be one of these keywords: **ap** (ASCII passive mode)**,an** (ASCII normal mode)**, ip**(Defaultâ€”Binary passive mode)**, in** (Binary normal mode).

```
ftp://admin:adminpass@10.10.10.10:20/images/asa/asa991-smp-k8.bin
FTP example without a username and password:
ftp://10.10.10.10:20/images/asa/asa991-smp-k8.bin
```

tftp:// [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename* [**;int=** *interface_name*]]

```
tftp://admin:adminpass@10.10.10.10/images/asa/asa991-smp-k8.bin outside
TFTP example without a username and password:
tftp://10.10.10.10/images/asa/asa991-smp-k8.bin outside
```

Note

The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command. The **;int=** *interface* option bypasses the route lookup and always uses the specified interface to reach the TFTP server.

smb:/[[*path* **/**] *filename*] - Indicates a UNIX server local file system.

```
smb:/images/asa/asa991-smp-k8.bin
```

scp:// [[*user* [**:** *password*] **@**] *server* [**/** *path*] **/** *filename* [**;int=** *interface_name*]]â€”The**;int=** *interface* option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server.

```
 scp://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
SCP example without a username and password:
scp://10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
```

The complete copy command with URL syntax in the Cisco ASA Series Command Reference, A - H Commands guide.

See ASA and ASDM Upgrade Prerequisites for more information about upgrading ASA and ASDM images using a custom URL.

18 Troubleshoot Secure Firewall ASA

Topics:

- Troubleshoot a Secure Firewall ASA device

This chapter covers the various troubleshooting steps for Secure Firewall ASA.

Troubleshoot a Secure Firewall ASA device

Explains how to troubleshoot common device issues including connectivity problems, configuration errors, synchronization failures, and deployment challenges to ensure proper device functionality.

ASA fails to reconnect to Security Cloud Control after reboot

Describes a connection issue where ASA devices fail to reconnect to Security Cloud Control after a reboot due to cipher suite incompatibility.

An ASA reconnection failure is a connectivity issue that

- occurs when an ASA device fails to reconnect to Security Cloud Control after a reboot
- happens because the ASA has fallen back to using an OpenSSL cipher suite that is not supported by Security Cloud Control's Secure Device Connector (SDC), and
- requires troubleshooting to test for the cipher suite issue and apply remediation steps.

Symptoms

- ASA reboots and Security Cloud Control and the ASA fail to reconnect. Security Cloud Control displays the message, "Failed to reconnect."
- When attempting to onboard an ASA, Security Cloud Control displays the message: *Certificate could not be retrieved for <ASA_IP_Address>*.

Disable ASA client-side certificate authentication for onboarding

Configure ASA to disable client-side certificate authentication to resolve onboarding issues with Security Cloud Control.

Disable client-side certificate authentication on ASA to enable successful onboarding to Security Cloud Control.

Environment: ASA is configured with client-side certificate authentication.

Solution: Disable client-side certificate authentication.

Details: ASAs support credential-based authentication as well as client-side certificate authentication. Security Cloud Control cannot connect to ASAs that use client-side certificate authentication. Before onboarding your ASA to Security Cloud Control, make sure it does not have client-certificate authentication enabled by using this procedure:

Procedure

1. Open a terminal window and connect to the ASA using SSH.
2. Enter global configuration mode.
3. At the hostname (config)# prompt, enter this command:

   no ssl certificate-authentication interface*interface-name***port 443**

   The interface name is the name of the interface Security Cloud Control connects to.

Client-side certificate authentication is disabled on the ASA, allowing successful onboarding to Security Cloud Control.

Determine the OpenSSL cipher suite used by your ASA

Verify the OpenSSL cipher suite being used by your ASA to ensure compatibility with the SDC.

This task helps you identify whether the OpenSSL cipher suite on your ASA is compatible with the Secure Device Connector (SDC).

Use this procedure to identify the OpenSSL cipher suite being used by your ASA. If the cipher suite named in the command output is not in the list of supported cipher suites, the SDC doesn't support that cipher suite and you will need to update the cipher suites on your ASA.

Procedure

1. Open a console window on a computer that can reach the SDC.
2. Connect to your SDC using SSH. You can log in as a regular user such as Security Cloud Control or SDC or some other user you created. You don't need to be logged in as root.

   Tip

   To find your SDC IP address:

   a. Open Security Cloud Control.

   b. From the user menu, select Secure Device Connectors.

   c. Click the SDC displayed in the table. The IP address of the SDC is displayed in the details pane for the device.

3. At the command prompt enter: **openssl s_client -showcerts -connect** *ASA_IP_Address*:**443**
4. Look for these lines in the command output.

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

   In this example, the cipher suite being used by the ASA is `DES-CB3-SHA`.

The command output displays the OpenSSL cipher suite being used by your ASA, allowing you to verify its compatibility with the SDC.

Cipher suites supported by Security Cloud Control's Secure Device Connector

Lists the cipher suites supported by Security Cloud Control's Secure Device Connector for secure communications.

Security Cloud Control's Secure Device Connector uses node.js which only accepts the latest and most secure ciphers. As a result, Security Cloud Control's SDC only supports this list of ciphers:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

If the cipher suite you use on your ASA is not in this list, SDC does not support it and you will need to Update your ASA's cipher suite on page 394.

Update your ASA's cipher suite

Configure TLS cipher suites on an ASA device to enhance security by specifying supported encryption protocols.

Update the TLS cipher suites on your ASA to ensure secure communication by configuring specific encryption protocols that meet your security requirements.

You need to modify the TLS cipher suite configuration when strengthening the security posture of your ASA device or when compliance requirements mandate specific encryption standards.

Procedure

1. Connect to the ASA using SSH.
2. Once connected to the ASA, elevate your privileges to global configuration mode.

   Your prompt should look like this: asaname(config)#
3. At the prompt, enter a command similar to this:

   Example

   ```
   ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256
   ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384
   ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256
    DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384
   ECDHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA256"
   ```

   Note

   The cipher suites this command configures your ASA to support are contained between quotes and after the word custom. In this command, the cipher suites specified begin with `ECDHE-RSA-AES128-GCM-SHA256` and end with `DHE-RSA-AES256-SHA256`. When you enter the command on your ASA, remove any cipher suites you know your ASA will not support.
4. After you submit the command, enter write memory at the prompt to save the local configuration.

   Example

   ```
   asaname(config)#write memory
   ```

The ASA is now configured with the specified TLS cipher suites, and the configuration has been saved to memory.

Troubleshoot ASA using CLI commands

Provides important commands to troubleshoot the ASA and test basic connectivity using the CLI interface.

This section discusses some of the important commands you may want to use to troubleshoot the ASA and test basic connectivity. See CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide to learn about other troubleshooting scenarios and CLI commands. In the 'System Administration' section, navigate to the 'Testing and Troubleshooting' chapter.

You can use the Security Cloud Control CLI interface available for each ASA device to execute these commands.

See ASA command line interface on page 303 to learn about how to use the CLI interface in Security Cloud Control.

NAT policy settings

Some of the important commands to determine the NAT settings are as follows:

- To determine NAT policy statistics, use **show NAT**.
- To determine the NAT pools, including the addresses and ports allocated, and how many times they were allocated, use **show NAT pool**.

For more commands related to NAT, see CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, and navigate to the 'Network Address Translation (NAT)' chapter.

Test basic connectivity: pinging addresses

You can ping the ASA device using the **ping <IP address>** command using the ASA CLI interface.

Display the routing table

Use the **show route** command to view the entries in the routing table.

ciscoasa# show route

Example output for a routing table of an ASA:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF

Gateway of last resort is 192.168.0.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, management
C 10.0.0.0 255.0.0.0 is directly connected, Outside
L 10.10.10.1 255.255.255.255 is directly connected, Outside
C 192.168.0.0 255.255.255.0 is directly connected, management
L 192.168.0.118 255.255.255.255 is directly connected, management
```

Monitor switch ports

- **show interface**

  Displays interface statistics.

- **show interface IP brief**

  Displays interface IP addresses and status.

- **show ARP**

Shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds.

Example output of ARP entries:

```
management 10.10.32.129 0050.568a.977b 0
management 10.10.32.136 0050.568a.5387 21
LANFAIL 20.20.21.1 0050.568a.4d70 96
outsi 10.10.16.6 0050.568a.e6d3 3881
outsi 10.10.16.1 0050.568a.977b 5551
```

Troubleshoot missing information on the RA VPN monitoring page

Configure the outside interface for Webvpn to resolve missing information on the remote access VPN monitoring page.

This task resolves issues where information is missing on the RA VPN monitoring page by enabling the outside interface for Webvpn on an ASA device.

This issue may occur if the outside interface is not enabled for Webvpn when configuring remote access VPN on an ASA device.

Procedure

1. In the left pane, click **Security Devices** and then click the **ASA** tab.
2. Select the RA VPN headend ASA device that is having issues.
3. In the **Management** pane on the right, click **Configuration**.
4. Click **Edit** and search for 'webvpn'.
5. Press **Enter** and add **enable** *interface_name*.

   Here, the interface_name is the name of the outside interface to which users connect when making the remote access VPN connection. Although this is normally the outside (internet-facing) interface, choose whichever interface is between the device and the end-users you are supporting with this connection profile.

   #### Example

   For example:

   ```
   webvpn
   enable outside
   ```

6. Click **Save**.
7. Preview and deploy the configuration to the device.

The outside interface is now enabled for Webvpn, and information should appear correctly on the RA VPN monitoring page.

ASA real-time logging

Describes a logging feature that displays recent logged data from ASA devices with specific data limits and configuration changes.

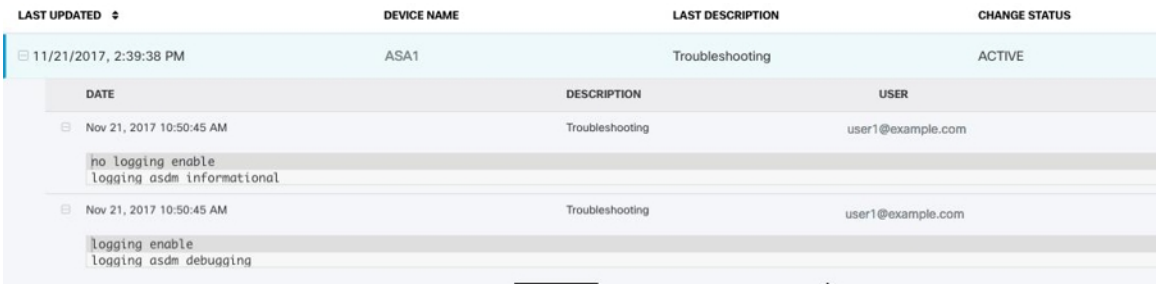
ASA real-time logging is a logging feature that

- displays the last 20 seconds of logged data or the last 10 KB of logged data, whichever limit is reached first
- temporarily changes the existing logging configuration to request debugging-level data during data retrieval, and
- returns the logging configuration to its previous state after data collection completes.

Real-time logging operation

When Security Cloud Control retrieves the real-time data, it reviews the existing logging configuration on your ASDM, changes it to request debugging-level data, and then returns the logging configuration to your configuration. The logging Security Cloud Control displays reflects any logging filters you may have set in ASDM.

You can see the commands that Security Cloud Control sends to perform logging by reviewing the change log. The first entry (on the bottom) indicates that Security Cloud Control "turned on" logging with the logging enable command and changed the ASDM logging level to debugging. The second entry (on the top) shows that the logging configuration was returned to its previous state. Logging was "turned off" with the no logging enable command and the ASDM logging level was returned to informational.



View ASA real-time logs

Configure real-time log viewing for ASA devices to monitor and troubleshoot network activity.

View real-time logging data from ASA devices to monitor network activity and troubleshoot issues as they occur.

Real-time logs provide immediate visibility into ASA device activity, allowing you to monitor traffic, security events, and system status in real time. You can apply filters to refine the log data and focus on specific events or criteria.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the appropriate device type tab and select the device for which you want to view real-time data.
3. Click **Troubleshoot** Troubleshoot .
4. (Optional) Before clicking View Real-time Log, you can define a filter in the left pane to refine the results of your logging search.
5. Click **View Real-time Log**.

   Security Cloud Control retrieves the real-time logging data based on your filtering criteria and displays it.
6. To see an additional 20 seconds of logged data or the last 10 KB of logged data, click **View Real-Time Log** again.

Real-time logging data is displayed based on your filtering criteria, allowing you to monitor ASA device activity and troubleshoot issues as they occur.

ASA packet tracer

Explains a network troubleshooting tool that sends synthetic packets to evaluate routing configuration, NAT rules, and policy configurations on ASA devices.

ASA Packet Tracer is a network troubleshooting tool that

- sends synthetic packets into the network to evaluate how existing routing configuration, NAT rules, and policy configurations affect that packet
- works on live, online ASA devices either physical or virtual, and
- evaluates packets based on the saved configuration on the ASA, not staged changes.

Troubleshooting use cases

Use this tool to troubleshoot these kinds of issues:

- Users report that they cannot reach resources that they should be able to.
- Users report that they can reach resources they should not be able to.
- Test a policy to determine if it works as you expect.

Packet tracer can be used on a live, online, ASA device either physical or virtual. Packet Tracer does not work on ASA model devices. Packet tracer evaluates packets based on the saved configuration on the ASA. Staged changes on Security Cloud Control are not evaluated by packet tracer.

We consider it a best-practice to run packet tracer on an ASA that is in the synced state. Though packet tracer will run if the device is not synced, you could encounter some unexpected results. For example, if you deleted a rule in the staged configuration on Security Cloud Control, and this same rule was triggered on the ASA during packet tracing, Security Cloud Control won't be able to show you the result of the packet's interaction with that rule.

As packet tracer sends the packet through the routing configuration, NAT rules, and security policies of your ASA, it displays the packet's status at each step. If the packet is allowed by the policy it receives a green checkmark ✅. If a packet is denied and dropped, Security Cloud Control displays a red X ❌.

Packet tracer also displays a real time log of the result of the packet trace. In the example below, you can see where a rule denied a tcp packet.



Troubleshoot an ASA device security policy

Configure packet tracer to troubleshoot security policies on ASA devices by virtually sending packets through the device.

Use packet tracer to troubleshoot security policies by simulating packet flow through your ASA device to identify potential connectivity issues and policy violations.

Packet tracer allows you to test how packets traverse through your ASA device's security policies without actually sending real traffic. This helps diagnose connection problems and verify policy configurations.

Procedure

1. In the left pane, click **Security Devices**.
2. Select your ASA and view troubleshooting details in the **Troubleshooting** pane.

3. In the pane, select the interface and packet type you want to send virtually through your ASA.
4. (Optional) If you want to trace a packet where the security group tag value is embedded in the Layer 2 CMD header (Trustsec), check SGT number and enter the security group tag number, 0-65535.
5. Specify the source and destination. You can specify IPv4 or IPv6 addresses, fully-qualified domain names (FQDN), or security group names or tags if you use Cisco Trustsec. For the source address, you can also specify a username in the format Domain\username.
6. Specify other protocol characteristics:
   - ICMP-Enter the ICMP type, ICMP code (0-255), and optionally, the ICMP identifier.
   - TCP/UDP/SCTP-Enter the source and destination ports by selecting them from the list or entering a value in the port combo box.
   - IP-Enter the protocol number, 0-255.
7. Click **Run Packet Tracer**.
8. Continue with Analyze packet tracer results on page 401.

The packet tracer results display the path the simulated packet takes through your ASA device, showing which security policies are applied and whether the packet is allowed or denied.

Troubleshoot an access rule

Configure packet tracer troubleshooting for a specific access rule in your network policy to analyze traffic flow and rule behavior.

Use packet tracer troubleshooting to analyze how traffic flows through your network policy and identify issues with specific access rules.

When you need to verify that an access rule is working correctly or diagnose traffic flow issues, the packet tracer tool allows you to simulate network traffic and see how it interacts with your configured rules.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **Access Policies**.
3. Select a policy that is associated with your ASA.
4. Select a rule in the network policy to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane.

   In the values panel of the troubleshoot page, many of the fields are pre-populated with the attributes of the rule you chose.
5. Enter information in the remaining required fields.

   Once you have completed all the required fields the Run Packet Tracer button becomes active.
6. Click **Run Packet Tracer.**
7. Continue with Analyze packet tracer results on page 401.

The packet tracer runs and provides analysis results for the selected access rule, showing how traffic flows through your network policy.

Troubleshoot a NAT rule

Configure troubleshooting for a NAT rule by selecting the rule and running packet tracer analysis to identify configuration issues.

This task enables you to diagnose and resolve issues with NAT rules by using packet tracer functionality to analyze traffic flow and rule behavior.

Use this procedure when you need to troubleshoot NAT rule configuration issues on ASA devices. The troubleshooting process helps identify why traffic is not being translated as expected.

Procedure

1. In the left pane, click **Security Devices** and then click the **ASA** tab.
2. Select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.
3. Select the rule from the NAT Rules table that you want to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. Notice that in the values panel of the Troubleshoot page, many of the fields are pre-populated with the attributes of the rule you chose.
4. Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer becomes active.
5. Click **Run Packet Tracer.**
6. Continue with Analyze packet tracer results on page 401.

The packet tracer runs and provides analysis results that help identify NAT rule issues and traffic flow problems.

Troubleshoot a twice NAT rule

Configure packet tracer troubleshooting for a Twice NAT rule to analyze source and destination packet translations.

Troubleshoot a Twice NAT rule to identify and resolve issues with packet translation by running packet tracer analysis on source or destination packet flows.

Use this procedure when you need to analyze NAT rule behavior and identify potential issues with packet translation in your ASA configuration. For bi-directional Twice NAT rules, you can troubleshoot either source packet translation or destination packet translation.

Procedure

1. In left pane, click **Security Devices**.
2. Click the **ASA** tab, select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.
3. Select the rule from the NAT Rules table that you want to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. For a bi-directional Twice NAT rule, this opens a dropdown where you choose to troubleshoot the source packet translation or the destination packet translation.
4. Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer becomes active.
5. Click **Run Packet Tracer**.

The packet tracer analysis runs and displays the results, showing how the NAT rule processes the specified packet flow and identifying any issues with the translation.

Analyze packet tracer results

Verify packet tracer results to understand why packets are dropped or allowed and take appropriate action based on the findings.

This task helps you understand the reasons behind packet tracer results, whether packets are dropped or allowed, and enables you to make necessary configuration changes to achieve desired access results.

Packet tracer provides detailed information about packet processing decisions. When you run packet tracer, you receive results that show whether packets are allowed or denied, along with the specific rules and policies that influenced these decisions.

Procedure

1. Expand a row in the packet trace table to view detailed rule or logging information.

   Whether the packet is dropped or allowed, you can learn why by expanding a row in the packet trace table and reading the rule or logging information related to that action.

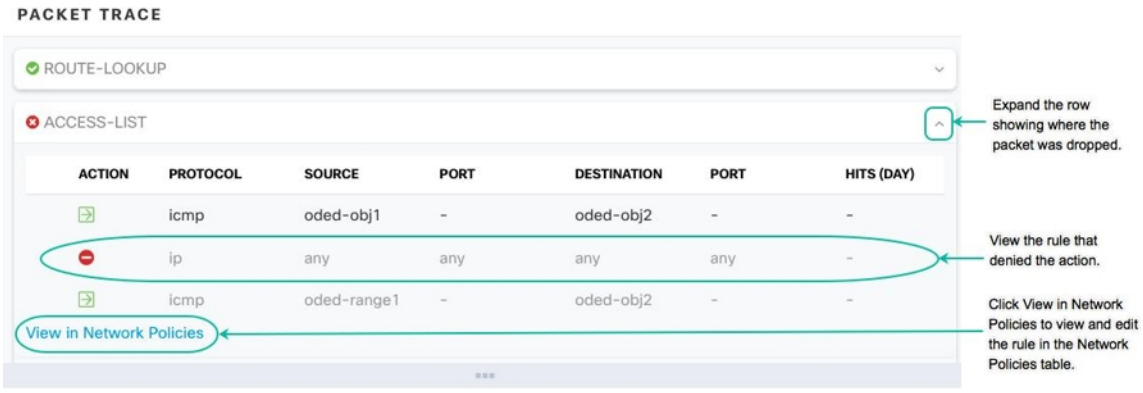
   The expanded view shows the specific access list policy and rules that affected the packet, such as a rule to deny an IP packet coming from any source and going to any destination.

2. If the action is not what you want, click the **View in Network Policies** link to edit the rule.

   This link allows you to immediately access and modify the relevant network policy rule.

3. Deploy the configuration change to the ASA after editing the rule.
4. Re-run packet tracer to verify that you get the expected access results.
5. Review the ASA real-time logging on page 396 from the ASA.

   Along with the packet tracer results, Security Cloud Control displays the real-time logging from the ASA.



You have successfully analyzed the packet tracer results and understand the reasons for packet processing decisions. Any necessary rule modifications have been deployed and verified through re-running packet tracer.

Cisco ASA Advisory cisco-sa-20180129-asa1

The Cisco Product Security Incident Response Team (PSIRT) **published the security advisory** cisco-sa-20180129-asa1 which describes a critical-severity ASA and Firepower security vulnerability. Read the entire PSIRT team advisory for a full explanation of what ASA and Firepower hardware, software, and configurations are affected.

If you determine that your ASAs are impacted by the advisory, you can upgrade your ASAs to the patched version using Security Cloud Control. Use this process:

Procedure

1. Configure a DNS server on each ASA that is affected.
2. Return to the advisory to determine which software patch you need.
3. See Upgrade ASA and ASDM images on a single ASA on page 384 for topics that describe how to use Security Cloud Control to upgrade your ASAs to the fixed releases listed in the ASA advisory. Start with the upgrade prerequisites and then read about upgrading individual ASAs, upgrading ASAs in an active-standby configuration, or upgrading ASAs in bulk.

   For your convenience, here is the summary of the security advisory that Cisco reported:

   UPDATED 2/5/2018: After further investigation, Cisco has identified additional attack vectors and features that are affected by this vulnerability. In addition, it was also found that the original fix was incomplete so new fixed code versions are now available. Please see the Fixed Software section for more information. A vulnerability in the XML parser of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. It was also possible that the ASA could stop processing incoming Virtual Private Network (VPN) authentication requests due to a low memory condition. The vulnerability is due to an issue with allocating and freeing memory when processing a malicious XML payload. An attacker could exploit this vulnerability by sending a crafted XML packet to a vulnerable interface on an affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, cause a reload of the affected device or stop processing of incoming VPN authentication requests. To be vulnerable the ASA must have Secure Socket Layer (SSL) services or IKEv2 Remote Access VPN services enabled on an interface. The risk of the vulnerability being exploited also depends on the accessibility of the interface to the attacker. For a comprehensive list of vulnerable ASA features please refer to the table in the Vulnerable Products section. Cisco has released software updates that address this vulnerability. There are no workarounds that address all the features that are affected by this vulnerability. This advisory is available at the following link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

Confirming ASA running configuration size

Verify the size of your ASA running configuration file by copying it to flash memory and checking its file size.

Confirm the size of your running configuration file to ensure it meets system requirements or limitations.

Use this procedure to determine if your ASA running configuration exceeds the 4.5 MB size limit by copying it to flash storage and examining the file properties.

Before you begin

Follow these steps to confirm the size of your running configuration file:

Procedure

1. Access the ASA's command line interface in one of these ways:
   - Open a terminal window and log into your ASA using SSH. Elevate your privilege to "privileged EXEC" mode so you see the prompt with `hostname#`.
   - If you managed to get your ASA onboarded, open the **Security Devices** page, select the device you want to connect to, and click **>_ Command Line Interface** button in the Device Actions pane.
2. At the prompt type `copy running-config flash`
3. When prompted for the Source filename, don't type anything and press <Enter>
4. When prompted for the destination filename, enter a name for the output file. After ASA copies the running configuration the file you specified, it returns you to the privileged EXEC prompt.

5. At the prompt, type `show flash`
6. Look in the length column. If your file is over 4718592 bytes, it is larger than 4.5 MB.

   Here is a sample set of commands and output:

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

You have successfully determined the size of your ASA running configuration file. Files over 4718592 bytes exceed the 4.5 MB limit.

Container Privilege Escalation Vulnerability Affecting Secure Device Connector: cisco-sa-20190215-runc

The Cisco Product Security Incident Response Team (PSIRT) published the security advisory cisco-sa-20190215-runc which describes a high-severity vulnerability in Docker. Read the entire PSIRT team advisory for a full explanation of the vulnerability.

This vulnerability impacts all Security Cloud Control customers:

- Customers using Security Cloud Control's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the Security Cloud Control Operations Team.
- Customers using an SDC deployed on-premise need to upgrade their SDC host to use the latest Docker version. They can do so by using the following instructions:

Update a Security Cloud Control-Standard SDC Host

Configure Docker service updates on your Secure Device Connector host to maintain compatibility with Firewall in Security Cloud Control.

This task updates Docker on your SDC host to ensure continued compatibility and security patching for your Secure Device Connector deployment.

- The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

  For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

  This procedure applies if you are still using CentOS.
- Use these instructions if you deployed an SDC using the Security Cloud Control image.

Procedure

---

1. Connect to your SDC host using SSH or the hypervisor console.

2. Check the version of your Docker service by running this command:

```
docker version
```

3. If you are running one of the latest virtual machines (VMs) you should see output like this:

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

   It's possible you may see an older version here.

4. Run these commands to update Docker and restart the service:

```
> sudo yum update docker-ce
> sudo service docker restart
```

> **Note**
>
> There will be a brief connectivity outage between Security Cloud Control and your devices while the docker service restarts.

5. Run the docker version command again.

   You should see this output:

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

You have successfully upgraded to the latest, patched version of Docker on your SDC host.

Recommendation: migrate SDC from CentOS to ubuntu

Outlines migration guidelines for Secure Device Connector hosts from unsupported CentOS 7 to Ubuntu virtual machines.

Migrate all SDCs from CentOS 7 to an Ubuntu virtual machine. The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

- If you have created your own SDC host you will need to follow the instructions to update based on how you installed Docker. If you used CentOS, yum and Docker-ce (the community edition) the preceding procedure will work.

- If you have installed Docker-ee (the enterprise edtion) or used an alternate method to install Docker, the fixed versions of Docker may be different. You can check the Docker page to determine the correct versions to install: Docker Security Update and Container Security Best Practices.

This procedure applies if you are still using CentOS.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

Bug tracking

Provides information about tracking bugs related to security vulnerabilities and advisory updates.

This reference provides details on how Cisco tracks and updates vulnerability information through bug tracking systems, enabling users to access the latest information on security advisories and associated fixes.

Cisco is continuing to evaluate this vulnerability and will update the advisory as additional information becomes available. After the advisory is marked Final, you can refer to the associated Cisco bug for further details:

CSCvo33929-CVE-2019-5736: runc container breakout

Limitation: large ASA running configuration files

Outlines limitations and solutions when ASA running configuration files exceed size thresholds in Security Cloud Control.

Configuration file size limitations

Be aware that Security Cloud Control cannot predictably manage ASA devices with running configuration files that are 4.5 MB or larger, contain approximately 22,000 lines or more, or have too many access-list entries for a single access group.

This limitation affects ASA onboarding and ongoing management in Security Cloud Control. You may see behavior such as the ASA failing to onboard, Security Cloud Control not displaying all of the configuration defined in the ASA's running configuration file, or Security Cloud Control failing to write to the change log.

When you onboard an ASA to Security Cloud Control, Security Cloud Control stores a copy of the ASA's running configuration file in its database. Large configuration files exceed database storage and processing capabilities.

To confirm the size of your running configuration file, see Confirming ASA running configuration size on page 402. Contact your Cisco account team for help safely reducing the size of your configuration file without disrupting your security policies.

Part V

Manage Secure Firewall Threat Defense with Cloud-Delivered Firewall Management Center

Topics:

- Onboard a Firewall Threat Defense Device
- Migrate Threat Defense to Cloud-Delivered Firewall Management Center
- Configure Cloud-Delivered Firewall Management Center-Managed Secure Firewall Threat Defense
- Introduction to AgenticOps insights
- Introduction to Agent Workforce
- Monitor Cloud-Delivered Firewall Management Center-Managed Threat Defense Device Events
- FTD Dashboard
- Analyze and Remediate Security Policy Anomalies with Policy Analyzer and Optimizer

19 Onboard a Firewall Threat Defense Device

Topics:

- Onboarding methods
- Maximum Firewall Threat Defense devices supported in Cloud-Delivered Firewall Management Center
- Requirements: Prerequisites to onboard a device to Cloud-Delivered Firewall Management Center
- Onboard a device with a CLI registration key
- Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning
- Onboard a Firewall Threat Defense Device to On-Prem Firewall Management Center using Zero-Touch Provisioning
- Onboard Firewall Threat Defense Devices using Device Templates to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning
- Cloud deployment
- Onboard a Secure Firewall Threat Defense Cluster
- Onboard a chassis
- Delete Devices from Cloud-Delivered Firewall Management Center
- Enable Cloud-Delivered Firewall Management Center
- Troubleshooting

Learn how to onboard a Firewall Threat Defense.

There are various ways to onboard a Firewall Threat Defense device for management.

Onboarding methods

Explains how to choose an onboarding method for Firewall Threat Defense devices in Cloud-Delivered Firewall Management Center, including registration key, Zero-Touch Provisioning, migration scenarios, version support, connectivity requirements, and post-onboarding visibility.

Onboarding is a device management process that

- connects Firewall Threat Defense devices to Cloud-Delivered Firewall Management Center for centralized management
- supports multiple methods including registration key and Zero-Touch Provisioning, and
- enables policy configuration and device monitoring through the management platform.

Onboarding requirements and compatibility

Review these use cases and supported software versions that are compatible with Cloud-Delivered Firewall Management Center management.

> **Note**
>
> You must ensure that the Firewall Threat Defense device ports have external and outbound access for the Cloud-Delivered Firewall Management Center to onboard them. There is no requirement for an on-premises or cloud-based Security Device Controller (SDC) for this operation. For more information, see Network Requirements.
>
> To send Firewall Threat Defense Syslog events to the Cisco cloud, you can set up the Secure Event Connector (SEC). For more information, see Installing Secure Event Connectors.

Firewall Threat Defense devices currently managed by Cloud-Delivered Firewall Management Center

These scenarios occur when you either move or migrate a device to the Cloud-Delivered Firewall Management Center:

- If you delete a device from an On-Premises Firewall Management Center or Secure Firewall Threat Defense Firewall Device Manager to onboard to the Cloud-Delivered Firewall Management Center, the change of managers wipes any policies configured through the On-Premises Firewall Management Center.
- If you **migrate** a device from an On-Premises Firewall Management Center to the Cloud-Delivered Firewall Management Center, the device retains the majority of your previously configured policies.

> **Note**
>
> If you do not know if your device is already managed by an alternative manager, use the **show managers** command in the device's CLI.

Onboarding methods

Cloud-Delivered Firewall Management Center supports these onboarding methods:

- Registration Key - Onboard a device with a registration key. The initial device setup wizard is complete on the device.

- Zero-Touch Provisioning - Onboard a new factory-shipped device with its serial number. Note that this method only supports Firepower 1000, Firepower 2100, or Secure Firewall 3100 devices.
- Zero-Touch Provisioning using a device template - Onboard new factory-shipped devices using serial numbers and a device template. Note that this method only supports Firepower 1000, Firepower 2100, Secure Firewall 1200 or Secure Firewall 3100 devices.

Maximum Firewall Threat Defense devices supported in Cloud-Delivered Firewall Management Center

Lists the supported Firewall Threat Defense device capacity for Cloud-Delivered Firewall Management Center, including standalone devices, high-availability pairs, cluster nodes, supported versions, and capacity planning considerations.

Cloud-Delivered Firewall Management Center supports up to 2,000 Firewall Threat Defense devices per deployment. This total can include a combination of standalone devices, devices in high-availability pairs, and devices that are cluster nodes.

The Cloud-Delivered Firewall Management Center can manage Firewall Threat Defense Version 7.2.0 and later.

> **Note**
>
> The maximum number of supported Secure Firewall Threat Defense devices in Cloud-Delivered Firewall Management Center includes devices that are deployed for analytics on Firewall Management Center and onboarded to Cloud-Delivered Firewall Management Center for management. These devices count toward the platform device capacity limit and must be included in your capacity planning to ensure proper sizing and performance.

Requirements: Prerequisites to onboard a device to Cloud-Delivered Firewall Management Center

Outlines onboarding limitations, requirements, network ports, and interface prerequisites for Firewall Threat Defense devices in Cloud-Delivered Firewall Management Center.

Onboard limitations and requirements

Be aware of the following limitations when onboarding a device to the Cloud-Delivered Firewall Management Center:

- Devices **must** be running version 7.2 and later.
- You can migrate an HA pair that is managed by an On-Premises Firewall Management Center by following the Migrate FTD to Cloud-Delivered Firewall Management Center process. Confirm both peers are in a healthy state prior to migrating.
- Devices managed locally by Firewall Device Manager can be onboarded using the serial number.
- Firewall Threat Defense devices can be onboarded to Cloud-Delivered Firewall Management Center using zero-touch provisioning if they are new (just unboxed) or have undergone a factory reset.
- If the device is managed by an On-Premises Firewall Management Center, you can either onboard the device to Cloud-Delivered Firewall Management Center or migrate the device. Migrating retains any existing policies and objects, whereas onboarding the device removes most policies and all objects. See Migrate FTD to Cloud-Delivered Firewall Management Center for more information.

- If your device is currently managed by a Firewall Device Manager, unregister all your smart licenses before you onboard the device. Even if you switch device management, the Cisco Smart Software Manager will retain the smart licenses.
- If you have previously onboarded a device that was managed by a Firewall Device Manager and deleted the device from Security Cloud Control with the intention of re-onboarding for cloud management, you **must** register the Firewall Device Manager to the Security Services Exchange cloud after deleting the device. See the "Access Security Services Exchange" chapter in the *Firepower and Cisco SecureX Threat Response Integration Guide.*

Tip

Onboarding a device to the Cloud-Delivered Firewall Management Center removes any policies and most objects configured through the previous manager. If your device is currently managed by an On-Premises Firewall Management Center, it is possible to migrate the device and retain your policies and objects. See Migrate FTD to Cloud-Delivered Firewall Management Center for more information.

Network requirements

Before you onboard a device, ensure the following ports have external and outbound access. Confirm the following ports on the device are allowed. If communication ports are blocked behind a firewall, onboarding the device may fail.

Note

You cannot configure these ports in the Security Cloud Control UI. You must enable these ports through the device's SSH.

Table 21: Device port requirements

Port	Protocol / Feature	Details
443/tcp	HTTPS	Send and receive data from the internet.
443	HTTPS	Communicate with the AMP cloud (public or private)
8305/tcp	Appliance communications	Securely communicate between appliances in a deployment.

Management and data interfaces

Make sure your device is correctly configured with either a management or data interface.

To configure a management or data interface on your device, see Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI on page 1113.

Onboard a device with a CLI registration key

Configure device onboarding to Cloud-Delivered Firewall Management Center using a CLI registration key for Firewall Threat Defense devices.

This task enables you to onboard a Firewall Threat Defense device to Cloud-Delivered Firewall Management Center using a CLI registration key method, allowing for remote management and policy deployment to the device.

Use this procedure to onboard a device for Cloud-Delivered Firewall Management Center with a CLI registration key.

Note

If your device is currently managed by an On-Premises Firewall Management Center, onboarding the device will fail. You can either delete the device from the On-Premises Firewall Management Center and onboard as a fresh, new device with no policies or objects, or you can migrate the device and retain the existing policies and objects. See Migrate FTD to Cloud-Delivered Firewall Managmenet Center for more information.

Important

You can create a Security Cloud Control-managed, standalone logical Firewall Threat Defense device using the Secure Firewall chassis manager or the FXOS CLI.

Before you begin

Before you onboard a device, be sure to complete these tasks:

- Cloud-Delivered Firewall Management Center is enabled for your tenant.
- Confirm the device's CLI configuration is successfully completed. See Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI on page 1113 for more information.
- Review the prerequesites and limitations before you onboard the device. See "Prerequisites to Onboard a Device to Cloud-Delivered Firewall Management Center" in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.
- The device can be configured for either local management with Secure Firewall Device Manager or remote management with Cloud-Delivered Firewall Management Center.
- Device must be running version 7.2.0 and later.
- You have reset the device's SSH password as part of the bootstrap process. If you have you not reset the SSH password, Security Cloud Control recommends using the Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning on page 414 method.

Follow these steps to onboard a device with a CLI registration key:

Procedure

1. In the left pane, click **Security Devices**.
2. Click **Onboard device or service** () icon.
3. Click the **FTD** tile.
4. Under **Management Mode**, select **FTD**.

   By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.
5. Select **Use CLI Registration Key** as the onboarding method.

6. Enter the device name in the **Device Name** field and click **Next**.
7. In the **Policy Assignment** step, use the drop-down menu to select an access control policy to deploy once the device is onboarded.

   If you have no policies configured, select the **Default Access Control Policy**.

8. Specify whether the device you are onboarding is a physical or virtual device.

   If you are onboarding a virtual device, you must select the device's performance tier from the drop-down menu.

9. Select the subscription licenses you want to apply to the device and click **Next**.
10. Security Cloud Control generates a command with the registration key. Connect to the device you are onboarding using SSH, log in as "admin" or a user with equivalent admin privileges and paste the entire registration key as is into the device's CLI.

    Note: For Firepower 1000, Firepower 2100, ISA 3000, and Firewall Threat Defense Virtual devices, open an SSH connection to the device and log in as **admin**. Copy the entire registration command and paste it into the device's CLI interface at the prompt. In the CLI, enter **Y** to complete the registration. If your device was previously managed by Firewall Device Manager, enter **Yes** to confirm the submission.

11. Click **Next** in the Security Cloud Control onboarding wizard.
12. (Optional) Add labels to your device to help sort and filter the **Security Devices** page.

    Enter a label and select the blue plus button. Labels are applied to the device after it's onboarded to Security Cloud Control.

    Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:

    - If you did not already, create a custom access control policy to customize the security for your environment. See Access Control Overview in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.
    - Enable Cisco Security Analytics and Logging (SAL) to view events in the Security Cloud Control dashboard **or** register the device to an Secure Firewall Management Center for security analytics. See Cisco Security Analytics and Logging in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.

The device is successfully onboarded to Cloud-Delivered Firewall Management Center and appears in the Security Devices page. The selected access control policy is deployed to the device, and any configured labels are applied for device management and filtering.

Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning

Configure onboarding of a Firewall Threat Defense device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, including tenant requirements, supported devices, serial number registration, policy assignment, and licensing.

This task enables you to onboard a Firewall Threat Defense device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning for automated device registration and configuration.

Only the Firepower 1000, Firepower 2100, Secure Firewall 1200, and Secure Firewall 3100 devices can be onboarded with the zero-touch provisioning method.

Before you begin

Confirm that the following is completed before onboarding:

- You have a Security Cloud Control tenant. If you do not, see Request a Security Cloud Control Tenant for more information.
- Cloud-Delivered Firewall Management Center is enabled for your tenant.
- The device is freshly installed but has never been logged into by either the device CLI, a Firewall Management Center, or the Firewall Device Manager.
- The device is running version 7.2 or later.
- The device's outside or management interface should be able to access the Security Services Exchange domain registration.us.sse.itd.cisco.com.

Procedure

1. In the left pane, click **Security Devices**.
2. Click **Onboard device or service** () icon.
3. Click the **FTD** tile.
4. Under **Management Mode**, select **FTD**.

   By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.
5. Click the **Use Serial Number** tile.
6. Select Cloud-Delivered Firewall Management Center from the drop-down list. Click **Next**.

   For information on onboarding a threat defense device to On-Prem Firewall Management Center, see Onboard a Threat Defense Device to On-Prem Firewall Management Center using Zero-Touch Provisioning.
7. Enter the **Device Serial Number** and the **Device Name**. Select **Next**.
8. Choose an option depending on whether the device is logged into and configured for a manager:
   - If your device is brand new and has never been configured for a manager, click **Yes, this new device has never been logged into or configured for a manager**.
   - If your device has been previously registered for a manager or is **still** registered to a manager, click **No, this device has been logged into and configured for a manager**.
9. Click **Next**.
10. In the **Policy Assignment** step, use the drop-down menu to select an access control policy to deploy once the device is onboarded.

    If you have no policies configured, select the **Default Access Control Policy**.
11. Select the subscription licenses you want to apply to the device and click **Next**.
12. Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:
    - If you did not already, create a custom access control policy to customize the security for your environment.

      For more information, see Access Control Overview.
    - You can enable Cisco Security Analytics and Logging to view events in the Security Cloud Control dashboard, or register the device to a Secure Firewall Management Center for security analytics.

For more information, see Cisco Security Analytics and Logging.

The Firewall Threat Defense device is successfully onboarded to Cloud-Delivered Firewall Management Center and appears in the Security Devices list with synchronized status.

Onboard a Firewall Threat Defense Device to On-Prem Firewall Management Center using Zero-Touch Provisioning

Configure a Firewall Threat Defense device to onboard to an on-premises Firewall Management Center using Zero-Touch Provisioning.

This task allows you to onboard a Firewall Threat Defense device to an on-premises Firewall Management Center using Zero-Touch Provisioning, enabling centralized security management.

Only the Firepower 1000, Firepower 2100, Secure Firewall 1200, and Secure Firewall 3100 devices can be onboarded to On-Premises Firewall Management Center using the zero-touch provisioning method.

Before you begin

Confirm the following is completed prior to onboarding:

- Before onboarding any new devices, ensure an on-prem FMC is fully set up, configured, and recognized as a management center within your Security Cloud Control tenant.
- The device is freshly installed and has never been logged into through the device CLI, a Firewall Management Center, or the Firewall Device Manager.
- The device is running version 7.2 or later. .

Procedure

1. In the left pane, click **Security Devices**.
2. Click **Onboard device or service** () icon.
3. Click the **FTD** tile.
4. Under **Management Mode**, select **FTD**.

   By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.
5. Click **Use Serial Number**.
6. Select an available on-prem FMC from the drop-down list. Click **Next**.

> **Note**
>
> - On-prem FMCs running version 7.4 or later and onboarded with Cisco Security Cloud are displayed in the drop-down.
> - Provide the **Public IP address** or **FQDN** value of the selected on-prem FMC unless
>   - The FTD is publicly reachable
>   - The FTD is running a version earlier than 7.4
>   - The connection is being made through the data interface

For information on onboarding a threat defense device to a Cloud-Delivered Firewall Management Center, see Onboard a Threat Defense Device to Cloud-delivered Firewall Management Center using Zero-Touch Provisioning.

7. Enter the **Device Serial Number** and the **Device Name**. Click **Next**.
8. Choose an option depending on whether the device is logged into and configured for a manager:
   - If your device is brand new and has never been configured for a manager, click **Yes, this new device has never been logged into or configured for a manager**.
   - If your device has been previously registered for a manager or is **still** registered to a manager, click **No, this device has been logged into and configured for a manager**.
9. Click **Next**.
10. In the **Policy Assignment** step, use the drop-down menu to select an access control policy to deploy once the device is onboarded.

    If you have no policies configured, select the **Default Access Control Policy**.
11. Select the subscription licenses you want to apply to the device and click **Next**.
12. Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:
    - If you did not already, create a custom access control policy to customize the security for your environment.

      For more information, see Access Control Overview.
    - You can enable Cisco Security Analytics and Logging to view events in the Security Cloud Control dashboard, or register the device to a Secure Firewall Management Center for security analytics.

      For more information, see Cisco Security Analytics and Logging.

The Firewall Threat Defense device is successfully onboarded to the on-premises Firewall Management Center and appears in your Security Devices page for centralized management and monitoring.

Onboard Firewall Threat Defense Devices using Device Templates to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning

Configure bulk onboarding of Firewall Threat Defense devices to Security Cloud Control using Zero-Touch Provisioning and device templates.

This task enables you to efficiently onboard multiple Firewall Threat Defense devices to Security Cloud Control using Zero-Touch Provisioning, device templates, and CSV files with serial numbers, template variables, object overrides, and licensing information.

Only the Firepower 1000, Firepower 2100, Secure Firewall 1200, Secure Firewall 200, and Secure Firewall 3100 devices can be onboarded with the zero-touch provisioning method.

Before you begin

Confirm that the following is completed before onboarding:

- You have a Security Cloud Control tenant. If you do not, see Request a Security Cloud Control Tenant for more information.
- Cloud-Delivered Firewall Management Center is enabled for your tenant.
- The device is freshly installed but has never been logged into by either the device CLI, a Firewall Management Center, or the Firewall Device Manager.
- The device is running version 7.4 or later.

Procedure

1. In the left pane, click **Security Devices**.
2. Click **Onboard device or service** () icon.
3. Click the **FTD** tile.
4. Under **Management Mode**, select **FTD**.

   By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.
5. Click the **Bulk Onboard using CSV File** tile.
6. In the **Template Assignment** field, select a template from the drop-down list. The access control policy associated with the template and the supported device models for the selected template are then displayed. Click **Next**.
7. In the **Upload CSV File** field, **Drag & drop** your CSV template file or **Click** to select the CSV template file that you want to upload.

   You can download a **CSV Sample Template File** to have a look at the required header details that have to be used in the template. The CSV template file must be less than 2 MB in size. The filename must satisfy the following criteria:

   - Can have a maximum of 64 characters.
   - Only alphanumeric characters and special characters such as dash (-), period (.), and underscore (_) are allowed.
   - Must not contain any spaces.

   A properly formatted .CSV file has the following fields:

   - Mandatory fields

  - Display Name - Name of the device. Type: string. Example: test1
  - Serial Number - Serial number of the device. Type: string, Example: JADX345670EG
- Optional fields
  - Device Group - Name of the device group, Type: string, Example: testgroup
  - Admin Password - Password for admin access, Type: string, Example: E28@2OiUrhx
- Variables - Use the following format: $<*varName*>. Sample variable: $LAN-Devices-IPv4Address - IPv4 address of the LAN device. Type: string. Example: 1.2.3.4.
- Network object overrides - Use the following format:<*objType*>:<*objName*>. Sample network object override: Network:LAN-Devices-Network - IP address of the network of LAN devices. Type: string. Example: 1.2.3.4.

A sample CSV template file containing configuration for two devices is as given below.

DisplayName	SerialNumber	AdminPassword	$WANLinkIP	Host:gateway
Branch A FTD	JADX345410AB	C15c05n0rt#	10.20.30.1	10.2.3.1
Branch B FTD	JADX345670CE	Admin123!	10.20.30.5	10.2.3.1

8. Click **Next**.
9. A statement mentioning that the devices are being onboarded is displayed. You can check the onboarding status of the devices in the **Security Devices** window.

   Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:

   - If you did not already, create a custom access control policy to customize the security for your environment. See Access Control Overview in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.
   - Enable Cisco Security Analytics and Logging (SAL) to view events in the Security Cloud Control dashboard **or** register the device to an Secure Firewall Management Center for security analytics. See Cisco Security Analytics and Logging in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.

The devices are successfully onboarded to Security Cloud Control using Zero-Touch Provisioning. You can view the onboarding status and manage the devices from the Security Devices window.

Cloud deployment

Describes a deployment approach that streamlines the configuration of Cisco Secure Firewall Threat Defense Virtual and Multicloud Defense across AWS, Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI).

A cloud deployment is a deployment approach that

- streamlines the configuration of Cisco Secure Firewall Threat Defense Virtual and Multicloud Defense across multiple cloud platforms,
- enables selection and launch of optimal enforcement points for scalable network security, and
- ensures high performance within complex multicloud environments.

Cloud deployment capabilities and enforcement points

Cloud deployment helps you deploy cloud-based enforcement points based on your intended outcomes and use cases. This provides the most cost-effective, scalable, and fully featured security for your multicloud needs.

With cloud deployment, you can:

- deploy faster with a guided, intuitive interface,
- select and launch the right enforcement point for your use case, and
- scale automatically to match demand and sustain performance.

Available enforcement points:

- Cisco Secure Firewall Threat Defense Virtual (FTDv): recommended for TLS Decrypt, IDS/IPS, Antivirus, Geo IP, or Malicious IP.
- Multicloud Defense: recommended for Proxy, WAF – L7 DOS, DLP, or Two-Core Enforcement.

Supported cloud service providers are:

- AWS
- Azure
- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI): Supported in this release by Multicloud Defense gateway only

Configure FTDv enforcement point

Use Cloud Deployment to configure and launch Cisco Secure Firewall Threat Defense Virtual (FTDv) gateways across AWS, Azure, and GCP. This process enables critical security features such as IDS/IPS, TLS decryption, and malware protection to secure cloud workloads during initial infrastructure setup.

Enable critical security features such as IDS/IPS, TLS decryption, and malware protection for cloud workloads across AWS, Azure, and GCP.

Cloud Deployment helps you deploy cloud-based enforcement points based on your intended outcomes and use cases. If you select TLS Decrypt, IDS/IPS, Antivirus, Geo IP, or Malicious IP, Cloud Deployment uses the Cisco Secure Firewall Threat Defense Virtual (FTDv) gateway for deployment.

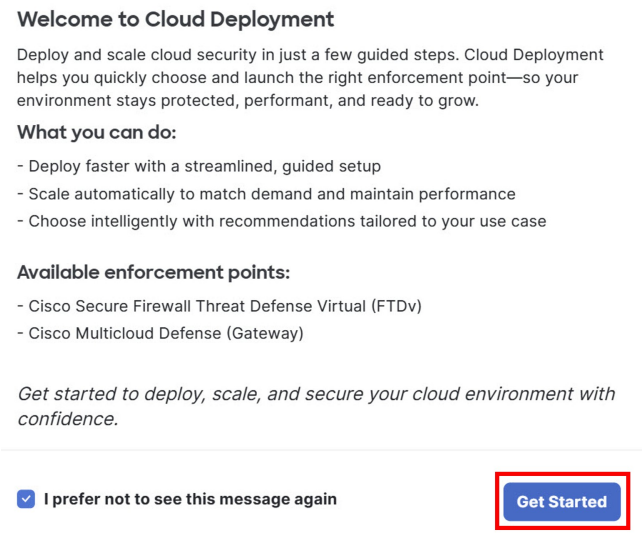
Follow these steps to configure your FTDv enforcement point:

Before you begin

- Ensure you have access credentials and administrative permissions on your AWS, Azure, or GCP account.
- Prepare any required network settings, such as VPC/VNet information, security groups, and key pairs.
- Identify which security features you will enable (e.g., IDS/IPS, TLS decryption, Antivirus).

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices** > **Cloud Deployment** .
3. Click **Get Started** .



4. On the **Account & Enforcement Type** tab, enter these details.

Field	Description
Account	Select an account from the drop-down list: AWS, Azure, or Google Cloud Platform (GCP).
Region	Select the region this gateway will be deployed into.
Select the type of Traffic Flow	Select the type of traffic flow (at least one must be selected): Ingress: Traffic entering from external destination Egress: Traffic leaving a network to external destination East-West: Traffic communicated across workloads with the network
Select your architectural requirements	Select TLS Decrypt, IDS/IPS, Antivirus, Geo IP, or Malicious IP to deploy through the FTDv gateway. Select Proxy, WAF - L7 DOS, DLP, or Two-Core Enforcement to deploy through Multicloud Defense gateway. Note that if you select Two-Core Enforcement, Antivirus is unavailable as it is not supported.

5. Click **Next** .
6. On the **Configure Enforcement Point** tab, enter these details.

Firepower Threat Defense Virtual Enforcement Information

Name	Enter a unique name for this enforcement point; the name can be up to 53 characters long and must be alphanumeric and include an underscore or a hyphen.
Description	(Optional) Enter a description for this enforcement point.

If you selected AWS account earlier, enter these details:

VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. After creation and activation, the wizard auto-populates the related network fields. This step can take up to three to four minutes.
Mgmt. Security Group	Select the security group to associate with the management interface.
Datapath Security Group 1	Select the security group to associate with datapath 1 interface.
Datapath Security Group 2	Select the security group to associate with datapath 2 interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular FTDv gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet 1	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Datapath Subnet 2	(Optional) Select the subnet for the secondary datapath interface.
Cisco Secure Firewall Threat Defense Virtual	
License Model	Select the licensing model for the deployment: **Smart Licensing** , **Gateway Hours** , or **Pay As You Go**
Smart Licensing/Gateway Hours/Pay As You Go	
Software Version	Select the FTDv release to deploy.
Admin Password	Enter the Admin password. It must be between 12 and 72 characters in length and include uppercase and lowercase letters, numeric digits, and special characters, excluding the backslash (\) and hyphen (-) characters. The password cannot contain more than two identical or sequential characters in a row (such as 'aaa' or '123').
Policy Ruleset	Select the FMC policy to attach to the FTDv deployment.
Performance Tier	(Smart Licensing only) Expand the drop-down menu and select the appropriate performance tier for your device. FTDv50 is selected by default.
License Types	(Smart Licensing only) Expand the drop-down menu and select the appropriate license type that you have purchased or will purchase in the future. The **Base** license is auto-selected. For more information about different licensing types, refer to Licensing . If you want to enable malware defense features, you must also have the THREAT license active. The THREAT license is required to support the MALWARE license functionalities.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances that you plan to deploy. This must be at least 1.

Maximum Instances	(Optional) Enter the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	(Optional) Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Cloud Configuration	
Key Pair	Select the key pair that is associated with the cloud account you selected earlier. You must select an existing key pair from the chosen region.
EBS Encryption	Select the appropriate EBS encryption for your AWS account.
Advanced Settings	
Disable Public IP	Check the **Disable Public IP** check box. Disabling this setting reduces the exposure of your network to external threats. Private IP addresses help protect against unauthorized access, potential attacks, and provide better control over internal traffic. This setting applies only when using NAT-based service and only for data interfaces.

If you selected Azure account earlier, enter these details:

VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. After creation and activation, the wizard auto-populates the related network fields. This step can take up to three to four minutes.
Resource Group	Select the resource group that owns the deployment resources.
Mgmt. Security Group	Select the security group to associate with the management interface.
Datapath Security Group 1	Select the security group to associate with datapath 1 interface.
Datapath Security Group 2	Select the security group to associate with datapath 2 interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular FTDv gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet 1	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Datapath Subnet 2	(Optional) Select the subnet for the secondary datapath interface.
Cisco Secure Firewall Threat Defense Virtual	
License Model	Select the licensing model for the deployment: **Smart Licensing** or **Gateway Hours**
Smart Licensing/Gateway Hours	

Software Version	Select the FTDv release to deploy.
Admin Password	Enter the Admin password. It must be between 12 and 72 characters in length and include uppercase and lowercase letters, numeric digits, and special characters, excluding the backslash (\) and hyphen (-) characters. The password cannot contain more than two identical or sequential characters in a row (such as 'aaa' or '123').
Policy Ruleset	Select the FMC policy to attach to the FTDv deployment.
Performance Tier	(Smart Licensing only) Expand the drop-down menu and select the appropriate performance tier for your device. FTDv50 is selected by default.
License Types	(Smart Licensing only) Expand the drop-down menu and select the appropriate license type that you have purchased or will purchase in the future. The **Base** license is auto-selected. For more information about different licensing types, refer to Licensing . If you want to enable malware defense features, you must also have the THREAT license active. The THREAT license is required to support the MALWARE license functionalities.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances that you plan to deploy. This must be at least 1.
Maximum Instances	(Optional) Enter the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	(Optional) Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Azure Configuration	
Key Selection	You can either provide an **SSH Public Key** directly or select an existing **SSH Key Pair** from the drop-down list.
Disk Encryption	Select either a provider-managed encryption key or a customer-managed key (CMK). If using a CMK, provide the **Disk Encryption Set ID** .
Advanced Settings	
Disable Public IP	Check the **Disable Public IP** check box. Disabling this setting reduces the exposure of your network to external threats. Private IP addresses help protect against unauthorized access, potential attacks, and provide better control over internal traffic. This setting applies only when using NAT-based service and only for data interfaces.

If you selected GCP account earlier, enter these details:

GCP Configuration

Datapath VPC	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. After creation and activation, the wizard auto-populates the related network fields. This step can take up to three to four minutes.
Datapath Network Tag 1	Select the network tag used for datapath firewall rules.
Datapath Network Tag 2	This is the second datapath tag used for dual-interface FTDv layouts. This identifies a separate management VPC.
Management VPC	Select the management VPC from the drop-down list.
Management Network Tag	Select the network tag used for management firewall rules from the drop-down list.
SSH Public Key	(Optional) Paste the SSH public key.
Disk Encryption	Select either a provider-managed encryption key or a customer-managed key (CMK). If using a CMK, provide the **Cloud KMS key resource name** .
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular FTDv gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet 1	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Datapath Subnet 2	(Optional) Select the subnet for the secondary datapath interface.

Cisco Secure Firewall Threat Defense Virtual

License Model	Select the licensing model for the deployment: **Smart Licensing** or **Gateway Hours**
Smart Licensing/Gateway Hours	
Software Version	Select the FTDv release to deploy.
Admin Password	Enter the Admin password. It must be between 12 and 72 characters in length and include uppercase and lowercase letters, numeric digits, and special characters, excluding the backslash (\) and hyphen (-) characters. The password cannot contain more than two identical or sequential characters in a row (such as 'aaa' or '123').
Policy Ruleset	Select the FMC policy to attach to the FTDv deployment.
Performance Tier	(Smart Licensing only) Expand the drop-down menu and select the appropriate performance tier for your device. FTDv50 is selected by default.

License Types	(Smart Licensing only) Expand the drop-down menu and select the appropriate license type that you have purchased or will purchase in the future. The **Base** license is auto-selected. For more information about different licensing types, refer to Licensing . If you want to enable malware defense features, you must also have the THREAT license active. The THREAT license is required to support the MALWARE license functionalities.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances that you plan to deploy. This must be at least 1.
Maximum Instances	(Optional) Enter the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	(Optional) Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Advanced Settings	
Disable Public IP	Check the **Disable Public IP** check box. Disabling this setting reduces the exposure of your network to external threats. Private IP addresses help protect against unauthorized access, potential attacks, and provide better control over internal traffic. This setting applies only when using NAT-based service and only for data interfaces.

7. Click **Next** . If you want to modify the settings, click **Back**
8. On the **Review & Deploy** tab, review your configuration and deploy the enforcement point. If you encounter an error, return to the **Configure Enforcement Points** tab to correct it.
9. Click **Deploy** .

   Multicloud Defense deploys the gateway.

   You must attach at least one ruleset to the gateway before you secure a spoke VPC/VNet. For more information about rule sets, refer to Rule Sets and Rule Set Groups .

The Cisco Secure Firewall Threat Defense Virtual (FTDv) enforcement point is deployed in your cloud environment, protecting workloads with the specified security features

Configure Multicloud Defense enforcement point

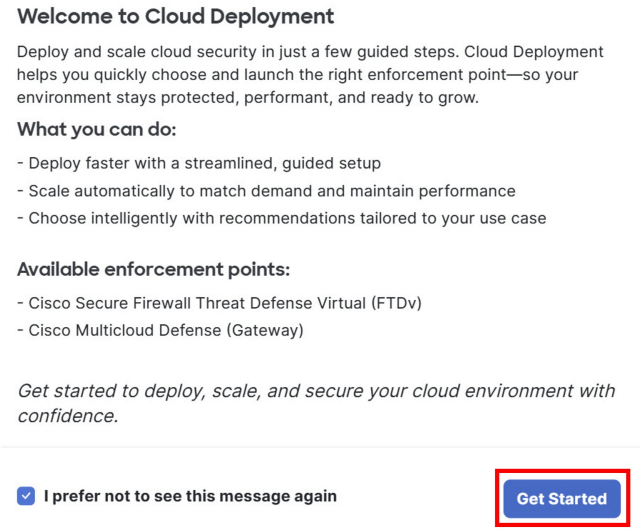
Use Cloud Deployment to configure and launch Multicloud Defense enforcement points across AWS, Azure, GCP, and OCI environments. This process enables critical security features such as WAF, proxy, and DLP to protect cloud workloads and manage traffic flow effectively during initial infrastructure setup.

Cloud Deployment helps you deploy cloud-based enforcement points based on your intended outcomes and use cases. If you select Proxy, WAF – L7 DOS, DLP, or Two-Core Enforcement, Cloud Deployment uses the Multicloud Defense gateway for deployment.

Follow these steps to configure Multicloud Defense enforcement point:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices** > **Cloud Deployment** .
3. Click **Get Started** .



4. On the **Account & Enforcement Type** tab, enter these details.

Field	Description
Account	Select an account from the drop-down list: AWS, Azure, Google Cloud Platform (GCP), or Oracle Cloud Infrastructure (OCI).
Region	Select the region this gateway will be deployed into.
Select the type of Traffic Flow	Select the type of traffic flow (at least one must be selected): Ingress: Traffic entering from an external destination Egress: Traffic leaving a network to external destination East-West: Traffic communicated across workloads with the network
Select your architectural requirements	Select TLS Decrypt, IDS/IPS, Antivirus, Geo IP, or Malicious IP if you want to deploy these features through the FTDv gateway. Select Proxy, WAF - L7 DOS, DLP, or Two-Core Enforcement if you want to deploy through the Multicloud Defense gateway. Note that if you select Two-Core Enforcement, Antivirus is unavailable as it is not supported.

5. Click **Next** .
6. On the **Configure Enforcement Point** tab, enter these details.

Multicloud Defense Gateway Enforcement Information

Name	Enter a unique name for this enforcement point; the name can be up to 53 characters long and must be alphanumeric and include an underscore or a hyphen.
Description	(Optional) Enter a description for this enforcement point.

If you selected AWS account earlier, enter these details:

Multicloud Defense Gateway Enforcement Information

Deployment	Click **Centralized** or **Distributed** to select the deployment type. **Centralized** allows you to select only a Service VPC. **Distributed** allows you to select only a regular VPC/VNet. If you select a Service VPC, the deployment operates in Hub mode. If you select a regular VPC or VNet, the deployment operates in Edge mode.
VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. You cannot create a new Service VPC/VNet if you selected **Distributed** earlier. After you create and activate the service, the wizard automatically fills in the related network fields. This step can take up to 3 to 4 minutes.
Mgmt. Security Group	Select the security group to associate with the management interface.
Datapath Security Group	Select the security group to associate with the datapath interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular Multicloud Defense gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.

Gateway Configuration

Instance Type	Select the VM size used for the gateway instances from the drop-down list.
Minimum Instances	(Optional) Enter the minimum number of instances you plan to deploy. This must be at least one.
Maximum Instances	(Optional) Enter the maximum number of instances you plan to deploy. This is the maximum number that is used for autoscaling in each availability zone. This number must be greater than or equal to minimum instances.

Health Check Port	Enter the port number used by Multicloud Defense load balancer to check the health of the instances. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Gateway Image Group	Select the logical grouping of available gateway images from the drop-down list.
Gateway Image	Select the exact gateway image/version to deploy from the drop-down list.
Policy Ruleset	Select the Multicloud Defense policy ruleset to attach to the gateway.
Cloud Configuration	
Key Pair	Select the key pair associated with the cloud account you selected in the previous screen.
Gateway IAM Role	Select the IAM role that allows the gateway to perform READ and WRITE operations on your AWS account. Multicloud Defense creates this role for you when you save and deploy the gateway.
EBS Encryption	Select the appropriate EBS encryption for your specific AWS account.
Multicloud Defense Profiles	
Packet Capture Profile	(Optional) Select the packet capture profile for threat and flow PCAPs.
Log Forwarding Profile	(Optional) Select the log forwarding profile used to forward Events/Logs to a security information and event management (SIEM) system.
Metrics Profile	(Optional) Select the metrics profile.
NTP Profile	(Optional) Select the Network Time Protocol (NTP) for time synchronization.
Advanced Settings	
Use Global Accelerator	(Ingress only) Associate the gateway with an AWS Global Accelerator listener so that traffic uses your accelerator.
Disable Public IP	By default, the Multicloud Defense gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** check box. This reduces the exposure of your network to external threats.
Use Internal Load Balancer	To reduce the exposure of your network to external threats, you can use an internal load balancer instead of a public one for the gateway front end (Ingress only). While the Multicloud Defense gateway enables a public router IP by default, you can opt for a private configuration by checking the **Disable Public IP** check box.

If you selected Azure account earlier, enter these details:

Multicloud Defense Gateway Enforcement Information

Deployment	Click **Centralized** or **Distributed** to select the deployment type. **Centralized** allows the selection of only a Service VPC. **Distributed** allows the selection of only a regular VPC/VNet. If you select a Service VPC, the deployment operates in Hub mode. If you select a regular VPC or VNet, the deployment operates in Edge mode.
VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. You cannot create a new Service VPC/VNet if you selected **Distributed** earlier. After you create and activate the service, the wizard automatically fills in the related network fields. This step can take up to 3 to 4 minutes.
Resource Group	Select the resource group that owns the deployment resources.
Mgmt. Security Group	Select the security group to associate with the management interface.
Datapath Security Group 1	Select the security group to associate with the datapath interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular Multicloud Defense gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances you plan to deploy. This must be at least one.
Maximum Instances	(Optional) Enter the maximum number of instances you plan to deploy. This is the maximum number that is used for autoscaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Gateway Image Group	Select the logical grouping of available gateway images from the drop-down list.
Gateway Image	Select the exact gateway image/version to deploy from the drop-down list.

Policy Ruleset	Select the Multicloud Defense policy ruleset to attach to the gateway.
Azure Configuration	
Key Selection	You can either provide an **SSH Public Key** directly or select an existing **SSH Key Pair** from the drop-down list.
Username	The default SSH username is centos.
User Assigned Identity ID	(Optional) Used for accessing Key Vault or writing PCAP files to Blob Storage.
Disk Encryption	(Optional) Select the disk encryption type from the drop-down list
Multicloud Defense Profiles	
Packet Capture Profile	(Optional) Select the packet capture profile for threat and flow PCAPs.
Log Forwarding Profile	(Optional) Select the log forwarding profile used to forward Events/Logs to a security information and event management (SIEM) system.
Metrics Profile	(Optional) Select the metrics profile.
NTP Profile	(Optional) Select the Network Time Protocol (NTP) for time synchronization.
Advanced Settings	
Management DNS Server	(Optional) Enter the IP address of a DNS server reachable by the gateway for management traffic.
Attach Additional Load Balancer	(Optional) Click **+ Add** to associate Azure Load Balancers with this gateway for advanced traffic distribution. Select the **Azure LB Name** from the drop-down list and enter the **Backend Pool Name** and **Resource Group** .
Disable Public IP	By default, the Multicloud Defense gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** check box. This reduces the exposure of your network to external threats.
Use Internal Load Balancer	To reduce the exposure of your network to external threats, you can use an internal load balancer instead of a public one for the gateway front end (Ingress only). While the Multicloud Defense gateway enables a public router IP by default, you can opt for a private configuration by checking the **Disable Public IP** check box.

If you selected GCP account earlier, enter these details:

Deployment	Click **Centralized** or **Distributed** to select the deployment type. **Centralized** allows the selection of only a Service VPC. **Distributed** allows the selection of only a regular VPC/VNet. If you select a Service VPC, the deployment operates in Hub mode. If you select a regular VPC or VNet, the deployment operates in Edge mode.

GCP Configuration	
Service Account Email	Enter the service account email attached to gateway instances.
Datapath VPC	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. After you create and activate the service, the wizard automatically fills in the related network fields. This step can take up to 3 to 4 minutes.
Datapath Network Tag	Select the network tag used for datapath firewall rules.
Management VPC	Select the management VPC from the drop-down list.
Management Network Tag	Select the network tag used for management firewall rules from the drop-down list.
Username	The default SSH username is centos.
SSH Public Key	(Optional) Paste the SSH public key.
Disk Encryption	(Optional) Select the disk encryption type from the drop-down list
Network Details	
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular Multicloud Defense gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet	(Optional) Select the subnet for datapath interface in the selected availability zone.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances you plan to deploy. This must be at least one.
Maximum Instances	(Optional) Enter the maximum number of instances you plan to deploy. This is the maximum number that is used for autoscaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Gateway Image Group	Select the logical grouping of available gateway images from the drop-down list.
Gateway Image	Select the exact gateway image/version to deploy from the drop-down list.
Policy Ruleset	Select the Multicloud Defense policy ruleset to attach to the gateway.

Multicloud Defense Profiles

Packet Capture Profile	(Optional) Select the packet capture profile for threat and flow PCAPs.
Log Forwarding Profile	(Optional) Select the log forwarding profile used to forward Events/Logs to a security information and event management (SIEM) system.
Metrics Profile	(Optional) Select the metrics profile.
NTP Profile	(Optional) Select the Network Time Protocol (NTP) for time synchronization.

Advanced Settings

Disable Public IP	By default, the Multicloud Defense gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** check box. This reduces the exposure of your network to external threats.
GCP LB Protocol UDP	Check this check box to enable UDP on the gateway's GCP load balancer configuration.

If you selected Oracle Cloud Infrastructure (OCI) account earlier, enter these details:

Multicloud Defense Gateway Enforcement Information

Deployment	Click **Centralized** or **Distributed** to select the deployment type. **Centralized** allows the selection of only a Service VPC. **Distributed** allows the selection of only a regular VPC/VNet. If you select a Service VPC, the deployment operates in Hub mode. If you select a regular VPC or VNet, the deployment operates in Edge mode.
VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. You cannot create a new Service VPC/VNet if you selected **Distributed** earlier. After you create and activate the service, the wizard automatically fills in the related network fields. This step can take up to 3 to 4 minutes.
Mgmt. Security Group	(Optional) Select the security group to associate with the management interface.
Datapath Security Group	(Optional) Select the security group to associate with the datapath interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular Multicloud Defense gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.

Datapath Subnet	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances from the drop-down list.
Minimum Instances	(Optional) Enter the minimum number of instances you plan to deploy. This must be at least one.
Maximum Instances	(Optional) Enter the maximum number of instances you plan to deploy. This is the maximum number that is used for autoscaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	Enter the port number used by Multicloud Defense load balancer to check the health of the instances. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Gateway Image Group	Select the logical grouping of available gateway images from the drop-down list.
Gateway Image	Select the exact gateway image/version to deploy from the drop-down list.
Policy Ruleset	Select the Multicloud Defense policy ruleset to attach to the gateway.
OCI Configuration	
Compartment	OCI Compartment where Multicloud Defense gateway will be deployed.
SSH Public Key	Paste the SSH public key.
Multicloud Defense Profiles	
Packet Capture Profile	Select the packet capture profile for threat and flow PCAPs.
Log Forwarding Profile	Select the log forwarding profile used to forward Events/Logs to a security information and event management (SIEM) system.
Metrics Profile	Select the metrics profile.
NTP Profile	Select the Network Time Protocol (NTP) for time synchronization.
Advanced Settings	
Internal Load Balancer	To reduce the exposure of your network to external threats, you can use an internal load balancer instead of a public one for the gateway front end (Ingress only). While the Multicloud Defense gateway enables a public router IP by default, you can opt for a private configuration by selecting the **Disable Public IP** check box.
User ID	Enable User ID on the gateway if your account supports it.
Management DNS Server	Enter the IP address of a DNS server reachable by the gateway for management traffic.

Public IP	By default, the Multicloud Defense gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** check box. This reduces the exposure of your network to external threats.

7. Click **Next** . If you want to modify the settings, click **Back** .
8. On the **Review & Deploy** tab, review your configuration and deploy the enforcement point. If you encounter an error, return to the **Configure Enforcement Points** tab to correct it.
9. Click **Deploy** .

   Multicloud Defense deploys the gateway.

   You must attach at least one ruleset to the gateway before you secure a spoke VPC/VNet. For more information about rule sets, refer to Rule Sets and Rule Set Groups .

Onboard a Secure Firewall Threat Defense Cluster

Configure onboarding of a Threat Defense cluster to Cloud-Delivered Firewall Management Center using a CLI registration key.

This task enables you to register a Secure Firewall Threat Defense cluster with Cloud-Delivered Firewall Management Center for centralized management and policy enforcement.

The following table provides information about device models that support cluster onboarding and creation on the Cloud-Delivered Firewall Management Center:

Secure Firewall Threat Defense Platforms	Minimum Secure Firewall Threat Defense Version for Cluster Management	Support cluster creation from Cloud-Delivered Firewall Management Center?
VMware, KVM	7.2.1	Yes
AWS, GCP	7.2.1	No
Azure	7.3	No
Secure Firewall 3100	7.2.1	Yes
Firepower 4100	7.2.x	No
Secure Firewall 4200	7.4	Yes
Firepower 9300	7.2.x	No

> **Note**
>
> When you onboard a Secure Firewall Threat Defense cluster to Cloud-Delivered Firewall Management Center, you register only the cluster CONTROL NODE. After the CONTROL NODE registers, Cloud-Delivered Firewall Management Center discovers the DATA nodes in the cluster.

Before you begin

Review these limitations:

- Firepower 4100 and Firepower 9300 devices must be clustered through the device's Firewall Chassis Manager.
- Secure Firewall 3100 devices, Secure Firewall 4200 devices, KVM, and VMware environments must be clustered through the Cloud-Delivered Firewall Management Center UI.
- Azure, AWS, and GCP environment clusters must be created through their own environment and onboarded to Cloud-Delivered Firewall Management Center.
- Verify that the Secure Firewall Threat Defense virtual devices are successfully configured as a cluster before you register the cluster with Cloud-Delivered Firewall Management Center.

  For example, in the Secure Firewall Threat Defense CLI, enter the `show cluster info` command. Confirm that the output shows the cluster as `On`, one unit in `CONTROL_NODE` state, and the remaining units in `DATA_NODE` state.

```
> show cluster info
Cluster mAZ-ngfw-cl: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "74-a" in state DATA_NODE
        ID        : 2
        Version   : 9.22(1)1
        Serial No.: 9AUVQ3DSF66
        CCL IP    : 1.1.1.74
        CCL MAC   : 02e2.778f.d3ed
        Module    : NGFWv
        Resource  : 4 cores / 7680 MB RAM
        Last join : 07:28:26 UTC Sep 25 2024
        Last leave: 07:28:11 UTC Sep 25 2024
Other members in the cluster:
    Unit "135-b" in state CONTROL_NODE
        ID        : 0
        Version   : 9.22(1)1
        Serial No.: 9A6W0A51KGK
        CCL IP    : 1.1.2.135
        CCL MAC   : 1294.34ae.4ce9
        Module    : NGFWv
        Resource  : 4 cores / 7680 MB RAM
        Last join : 09:45:52 UTC Sep 24 2024
        Last leave: N/A
    Unit "183-c" in state DATA_NODE
        ID        : 1
        Version   : 9.22(1)1
        Serial No.: 9A1S400HL8F
        CCL IP    : 1.1.3.183
        CCL MAC   : 0aff.e889.f193
        Module    : NGFWv
        Resource  : 4 cores / 7680 MB RAM
        Last join : 07:29:29 UTC Sep 25 2024
        Last leave: 07:28:11 UTC Sep 25 2024
>
```

Follow these steps to onboard a Secure Firewall Threat Defense cluster:

Procedure

1. In the left pane, click **Security Devices**.
2. Click **Onboard device or service** ( ) icon.
3. Click the **FTD** tile.
4. Under **Management Mode**, select **FTD**.

   By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.
5. Select **Use CLI Registration Key**.
6. Enter the device name in the **Device Name** field and click **Next**.

7. In the **Policy Assignment** step, use the drop-down menu to select an access control policy to deploy once the device is onboarded.

   If you have no policies configured, select the **Default Access Control Policy**.

8. Specify whether the device you are onboarding is a physical or virtual device.

   If you are onboarding a virtual device, you must select the device's performance tier from the drop-down menu.

9. Select the subscription licenses you want to apply to the device and click **Next**.
10. Security Cloud Control generates a command with the registration key. Paste the entire registration key into the device's CLI without making changes.
11. (Optional) Add labels to your device to help sort and filter the **Security Devices** page.

    Enter a label and select the blue plus button. Labels are applied to the device after it's onboarded to Security Cloud Control.

    Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:

    - If you did not already, create a custom access control policy to customize the security for your environment. See Access Control Overview in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.
    - Enable Cisco Security Analytics and Logging (SAL) to view events in the Security Cloud Control dashboard **or** register the device to an Secure Firewall Management Center for security analytics. See Cisco Security Analytics and Logging in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.

Onboard a chassis

Configure how to onboard a Firepower 4100/9300 or Secure Firewall 3100/4200 chassis to Cloud-Delivered Firewall Management Center using FXOS CLI registration, chassis naming, and device group assignment.

This task allows you to add a Firepower 4100/9300 or Secure Firewall 3100/4200 chassis to the Cloud-Delivered Firewall Management Center for centralized management and health monitoring.

You can add a Firepower 4100/9300 chassis to the Cloud-Delivered Firewall Management Center. The management center and the chassis share a separate management connection using the chassis MGMT interface. The Cloud-Delivered Firewall Management Center offers chassis-level health alerts. For configuration, you still need to use the Firewall Chassis Manager or FXOS CLI.

Security Cloud Control does not record the processes on the **Workflow** page when you onboard a chassis or provision a multi-instance Firewall Management CenterFirewall Threat Defense device from the Cloud-Delivered Firewall Management Center chassis manager page.

Note

For the Secure Firewall 3100, you need to first convert to multi-instance mode. See Onboard the multi-instance chassis using the CLI.

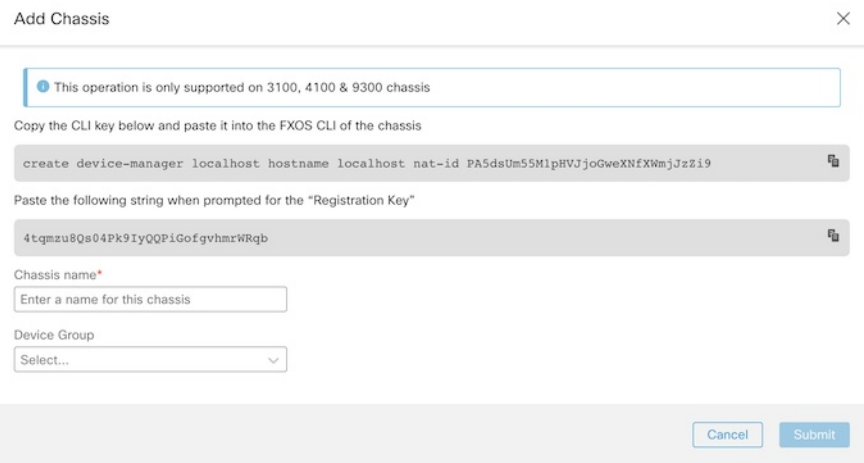
Procedure

1. Connect to the chassis FXOS CLI, either using the console port or SSH.
2. In the left pane, click **Security Devices**.
3. Click **Onboard device or service** ( ) icon.
4. Click the **FTD Chassis** tile to open the **Add Chassis** dialog box.

Figure 3: FTD chassis tile



Figure 4: Add chassis



5. Click **Copy** ( ) to copy the top generated command, then paste it at the FXOS CLI of your chassis.
6. When prompted for the Registration Key at the FXOS CLI, click **Copy** ( ) on the **Add Chassis** dialog box for the generated registration key and paste it at the FXOS CLI.

   You can disconnect from the FXOS CLI at this point.
7. In the Cloud-Delivered Firewall Management Center **Chassis Name** field, enter a name for the chassis as you want it to display in the Cloud-Delivered Firewall Management Center.
8. Optional: Add the chassis to a **Device Group**.
9. Click **Submit**.

The chassis is added to the **Device** > **Device Management** page.

The chassis is successfully onboarded and appears on the Device Management page where you can monitor its health and manage its configuration through the Cloud-Delivered Firewall Management Center.

Delete Devices from Cloud-Delivered Firewall Management Center

Configure device removal from Cloud-Delivered Firewall Management Center by deleting them from Security Cloud Control, including HA device selection and AWS VPC deletion limits.

This task removes devices from Cloud-Delivered Firewall Management Center management by deleting them from the Security Cloud Control dashboard.

Though devices may be registered to Cloud-Delivered Firewall Management Center, Security Cloud Control still manages device enrollment. You must delete the device from the Security Cloud Control dashboard to remove a device from Cloud-Delivered Firewall Management Center.

> **Note**
>
> Security Cloud Control does not synchronize the deletion of devices that are associated with an AWS VPC environment. You must delete a device direclty from the AWS VPC UI. See AWS documentation for more information.

Procedure

1. Log into Security Cloud Control and click **Security Devices**.
2. Locate the device you want to delete by using the filters or search bar. Select it so the device row is highlighted. If your device is part of a high availability pair, locate and select the active device.
3. In the Device Actions pane located to the right, click **Remove**.
4. When prompted, select **OK** to confirm the removal of the selected device. Click **Cancel** to keep the device onboarded.

The device is removed from Cloud-Delivered Firewall Management Center and no longer appears in the Security Devices list.

Enable Cloud-Delivered Firewall Management Center

Configure Cloud-Delivered Firewall Management Center for a Security Cloud Control tenant to manage your Secure Firewall Threat Defense devices.

Enable Cloud-Delivered Firewall Management Center to manage your Secure Firewall Threat Defense devices through Security Cloud Control.

If you want to manage your Secure Firewall Threat Defense devices, you can enable the Cloud-Delivered Firewall Management Center on your tenant. You need to have an admin or a super admin user role to perform this task.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.

2. From the Security Cloud Control menu, click **Administration** > **Integrations** > **Firewall Management Center** and click **Enable Cloud-Delivered FMC**.

   Security Cloud Control starts provisioning a Cloud-Delivered Firewall Management Center instance in the background; it typically takes 15 to 30 minutes for this to be complete. You can track the provisioning progress on the **Status** column of **Cloud-Delivered FMC**.

   After the provisioning is complete, the status changes to **Active**. In addition, you get a **Cloud-Delivered Firewall Management Center is Ready** notification on the Security Cloud Control notifications panel and on the applications on which you have configured incoming webhooks. See Notification Settings for more information.

   > **Note**
   >
   > After you receive the **Cloud-Delivered Firewall Management Center is Ready** notification, ensure that you log out of and log in back to your tenant once, to see the **Cloud-Delivered FMC** right pane options, such as **Actions**, **Management**, and **System**.

   What to do next:

   a. Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager (CSSM) to activate smart license. For detailed steps, refer to Register the Cloud-Delivered Firewall Management Center with the Smart Software Manager.

   b. Onboard your Firewall Threat Defense devices to the Cloud-Delivered Firewall Management Center and manage them.

After the provisioning is complete, the status changes to **Active** and you receive readiness notifications. You can then proceed to register with the Smart Software Manager and onboard your devices.

Troubleshooting

Explains how to troubleshoot Firewall Threat Defense onboarding issues in Cloud-Delivered Firewall Management Center, including connectivity problems, update-related connection loss, CLI registration key onboarding, and serial number onboarding.

Troubleshooting is a diagnostic process that identifies and resolves onboarding issues between Firewall Threat Defense devices and management systems.

Troubleshooting scenarios

Use these scenarios to troubleshoot any onboarding issues.

Troubleshoot Cloud-Delivered Firewall Management Center Connectivity with TCP

Configure TCP port 8305 connectivity troubleshooting between the Cloud-Delivered Firewall Management Center and a Firewall Threat Defense device.

This task helps diagnose and resolve connectivity issues between the Cloud-Delivered Firewall Management Center and a Firewall Threat Defense device using TCP port 8305.

Use this procedure to troubleshoot connectivity between the Cloud-Delivered Firewall Management Center and a Firewall Threat Defense device with TCP port 8305.

Procedure

1. Log into Security Cloud Control.
2. Navigate to **Tools & Services** in the left panel and select **Firewall Management Center** to open the **Services** page. Choose **Cloud-Delivered FMC** and locate the Cloud-Delivered Firewall Management Center's FQDN in the top righthand corner.
3. Make sure the Firewall Threat Defense device's state in Security Cloud Control is currently **Onboarding**. Cloud-Delivered Firewall Management Center will not respond if the device is not in an onboarding state. If onboarding has failed, click **Retry Onboarding**.
4. Log into the Firewall Threat Defense device with SSH.
5. Enter into Expert mode with the following command:

```
> expert
admin@devicename:~$
```

6. Execute a TCP handshake:

```
admin@devicename:~$ nc -v xxxxxx.cdo.cisco.com 8305
Connection to xxxxxx.cdo.cisco.com 8305 port [tcp/*] succeeded!
^C (CTRL-C to exit netcat)
admin@devicename:~$.
```

If there is still no response from the Cloud-Delivered Firewall Management Center, then there is a chance that outbound port TCP 8305 may be blocked upstream from your Firewall Threat Defense device and that network path will need to be assured before your Firewall Threat Defense will be able to connect to Cloud-Delivered Firewall Management Center.

You have successfully tested the TCP connectivity between the Cloud-Delivered Firewall Management Center and the Firewall Threat Defense device. If the connection succeeded, the devices can communicate properly on TCP port 8305. If the connection failed, network path issues need to be resolved before the devices can connect.

Troubleshoot Firewall Threat Defense Device Connectivity

Verify Internet connectivity from the management-plane of the Firewall Threat Defense device by testing ping connectivity.

Test connectivity to identify potential L1-L3 networking issues or DNS resolution problems that may affect device management operations.

Test connectivity to the Internet from the management-plane of the Firewall Threat Defense device:

Procedure

1. Log into the Firewall Threat Defense device with SSH.
2. Ping one or both of the following:

```
ping system 208.67.222.222
```

```
ping system cisco.com
```

If either of these tests fail, there is likely an L1-L3 issue and you will need to check your management networking configuration (**show network**) and/or a DNS issue.

Successful ping results confirm Internet connectivity from the management-plane. Failed ping tests indicate networking or DNS configuration issues that require further investigation.

Troubleshoot device connectivity loss after Cloud-Delivered Firewall Management Center update

Configure firewall rules to allow threat defense traffic to flow to the FQDN and port of the management center rather than its IP address when connectivity is lost after a management center update.

This task helps restore management connectivity between your threat defense device and the Cloud-Delivered Firewall Management Center after the management center receives a new dynamic IP address during an update.

A Cloud-Delivered Firewall Management Center is assigned a dynamic IP address when it is added to a Security Cloud Control tenant. When the management center is updated, the management center receives a new dynamic IP address.

If you have a firewall inspecting the outbound traffic from your threat defense device to the Cloud-Delivered Firewall Management Center, your firewall rules must allow the threat defense traffic to flow to the FQDN and port of the management center rather than its IP address, or the management center will not be able to manage your threat defense device.

Procedure

1. Change your existing IP-based firewall rule to use FQDN-based rules for both required ports.

   For example, if your network traffic rule allowing management traffic from your threat defense device to the Cloud-Delivered Firewall Management Center looks like this:

   ```
   allow all traffic <my-threat-defense-IP-src> to 200.165.200.225
   ```

   where 200.165.200.225 is the management address of the Cloud-Delivered Firewall Management Center, change the one allow rule to these two allow rules as both ports 443 and 8305 need to be open:

   ```
   allow all traffic <my-threat-defense-IP-src > to <my-cdfFMC-FQDN>:443
   ```

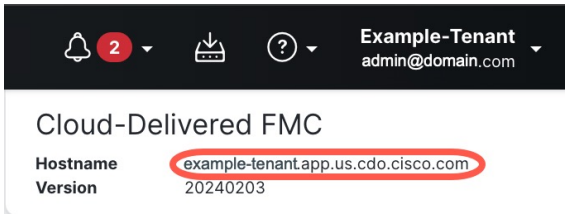
   ```
   allow all traffic <my-threat-defense-IP-src > to <my-cdfFMC-FQDN>:8305
   ```

   See "Network Requirements" in Prerequisites to Onboard a Device to Cloud-delivered Firewall Management Center for more port information.

2. Find the domain name of your Cloud-Delivered Firewall Management Center.
   a) Log in to Security Cloud Control.
   b) In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**
   c) Select **Cloud-Delivered FMC** in the FMC table.

   In the top-right corner of the screen, you will see the Hostname of the management center. This is the FQDN.

   Figure 5: Cloud-delivered FMC FQDN

Your threat defense device can now maintain management connectivity with the Cloud-Delivered Firewall Management Center using FQDN-based firewall rules, even when the management center's IP address changes during updates.

Troubleshoot Onboarding a Device to the Cloud-Delivered Firewall Management Center Using the CLI Registration Key

Describes how to troubleshoot common issues when onboarding a device using CLI registration key commands, including key validation errors and connection problems.

Error: device remains in pending setup state after onboarding

Configure device registration when a device fails to register and displays a Pending Setup connectivity status.

This task resolves device registration failures that occur when the configuration manager command is not executed within 3 minutes after onboarding.

When a device fails to register, the device's connectivity status is displayed as **Pending Setup**. In the panel located to the right, Security Cloud Control displays a **Registration Failed** message as well as a **Retry Onboarding** button to immediately allow you to reattempt onboarding the device.

If you fail to execute the `configuration manager` command in the device CLI within 3 mins after onboarding it to Security Cloud Control, the device's registration attempt expires and results in a registrationg failure.

Procedure

1. Log into Security Cloud Control and navigate to the **Security Devices** page. Locate the device that failed to register.
2. In the panel located to the right, locate the **Registration Failed** window. Beside the device's CLI registration key, click **Copy**. This actions copies the CLI key to a local clipboard.
3. Open an SSH connection to the device and log in as `admin`.
4. Paste the CLI registration key into the device's CLI interface. In the CLI, enter **Y** to complete the registration. If your device was previously managed by Firewall Device Manager, enter **Yes** to confirm the submission.

The device registration completes successfully and the device status changes from Pending Setup to an active connectivity status.

Troubleshoot Onboarding a Device to Cloud-Delivered Firewall Management Center Using the Serial Number

Describes how to identify and resolve common issues when onboarding a device using its serial number, including verification steps and error resolution techniques.

Device is offline or unreachable

Lists potential causes when a device shows an unreachable connectivity status during or after onboarding.

If the device is unreachable during the onboarding process, or at any point post-onboarding, Security Cloud Control displays an **Unreachable** connectivity status. The device will not be able to fully onboard to Security Cloud Control until the device is able to connect.

These scenarios might be the cause:

- The device is cabled incorrectly.
- Your network may require a static IP address for the device.
- Your network uses custom DNS, or there is external DNS blocking the network.
- If your device is associated with the European region (https://defenseorchestrator.eu/), you may need to enable PPPoE authentication.For other domains, review the domain requirements.

- The device may be blocked by a firewall, or is incorrectly blocking a port for connectivity. Review the device #unique_489/unique_489_Connect_42_cdfmc_network and confirm the correct outgoing ports are enabled.

Error: Serial Number Already Claimed

The Device was Purchased From an External Vendor

If the device was purchased from an external vendor and fails to onboard with a **Serial Number Already Claimed** error, it's possible the device is still associated to the vendor's tenant. Use the following steps to claim the device and its serial number:

1. Delete the device from your Security Cloud Control tenant.
2. Install the FXOS image on the device. For more information, see the "Reimage Procedures" chapter of the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100 Firepower Threat Defense guide.
3. Connect a laptop to the device's console port.
4. Connect to the FXOS CLI and log in as **admin**.
5. In the FXOS CLI, connect to **local-mgmt** with the `firepower # connect local-mgmt` command.
6. Execute the `firepower(local-mgmt) # cloud deregister` command to deregister the device from the cloud tenancy.
7. Once the device is successfully unregistered, the CLI interface returns a success message. An example of the message:

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected
RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id:
2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

> **Note**
>
> If the device was never registered to another Security Cloud Control tenant, the message above states `RESULT=success MESSAGE=DEVICE_NOT_FOUND`.

8. Onboard the device to your Security Cloud Control tenant with its serial number. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning on page 414 for more information.

The Device is Claimed By a Security Cloud Control Tenant in Another Region

The device may have been previously managed by another Security Cloud Control instance in a different region and is still registered to that tenant.

If you **do** have access to the tenant the device is currently registered to, use the following procedure:

1. Delete the device from the incorrect Security Cloud Control tenant.
2. Log into the device's Firewall Device Manager UI.
3. Navigate to **System Settings** > **Cloud Services**.
4. Click **Cloud Services** and select **Unregister Cloud Services** from the drop-down list.
5. Confirm the action and click **Unregister**. This action generates a warning to indicate that the device has been removed from Security Cloud Control. This is expected behavior.

6. Log into Security Cloud Control tenant in the correct region and onboard the device. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning on page 414 for more information.
7. Navigate to **System Settings** > **Cloud Services**.
8. Click **Cloud Services** and select **Unregister Cloud Services** from the drop-down list.
9. Select the **Auto-enroll with Tenancy from Security Cloud Control** and click **Register**. The device maps to the new tenant that belongs to the new region and Security Cloud Control onboards the device.

If you **do not** have access to the tenant, use the procedure below:

1. Connect to the FXOS CLI from the console port and log in as **admin**. For information on how to log into the FXOS CLI, see Accessing the FXOS CLI.
2. In the FXOS CLI, connect to **local-mgmt** with the `firepower # connect local-mgmt` command.
3. Execute the `firepower(local-mgmt) # cloud deregister` command to deregister the device from the cloud tenancy.
4. Once the device is successfully unregistered, the CLI interface returns a success message. An example of the message:

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected
RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id:
2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

> **Note**
>
> If the device was never registered to another Security Cloud Control tenant, the message above states `RESULT=success MESSAGE=DEVICE_NOT_FOUND`.

5. In your Security Cloud Control tenant in the correct domain, onboard the device. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning on page 414 for more information.
6. In the device's Firewall Device Manager UI, navigate to **System Settings** > **Cloud Services**.
7. Select the **Auto-enroll with Tenancy from Security Cloud Control** and click **Register**. The device maps to the new tenant that belongs to the new region and Security Cloud Control onboards the device.

Resolve claim error

Configure the correct device serial number to resolve a claim error that occurs when an incorrect serial number is entered during device onboarding.

Resolve claim errors that result from entering incorrect serial numbers during device onboarding.

If you enter the wrong serial number when onboarding a device, Security Cloud Control generates a **Claim Error** status.

> **Note**
>
> Confirm that the device is claimed in the correct region within Security Cloud Control.

Follow these steps to resolve claim error issues:

Procedure

1. Log into Security Cloud Control and navigate to the **Security Devices** page. Locate the device with the error.
2. Select the device so it is highlighted and **Remove** the device from Security Cloud Control.
3. Confirm the following:
   - The device is online and can reach the internet.
   - The device has not already been onboarded to your Security Cloud Control instance or claimed by a Security Cloud Control tenant in another region.
4. Locate the device's serial number. You can use one of the following methods:
   - For the 1000, 2100 and 3100 series model, locate the serial number on the physical device.
   - Open an SSH connection to the device and issue the **show serial-number** command.
5. In Security Cloud Control, onboard the device with the correct serial number. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning on page 414 for more information.

The device is successfully onboarded with the correct serial number and the claim error is resolved.

Error: failed to claim

Verify device connectivity and resolve claim failures by removing and re-onboarding the device to your Security Cloud Control tenant.

This task helps resolve device onboarding failures when you see an **Error: Failed to Claim** connectivity status or error message after attempting to onboard a device.

If you see an **Error: Failed to Claim** connectivity status or error message after attempting to onboard a device, the following might be the cause:

- The Security Services Exchange platform may have temporary issues that result in no connectivity.
- The Security Cloud Control server may be down.

Follow these steps to resolve this issue:

Procedure

1. Log into Security Cloud Control and navigate to the **Security Devices** page. Locate the device that failed to register.
2. Select the device so it is highlighted and **Remove** the device from your Security Cloud Control tenant.
3. Wait at least 10 minutes before attempting to onboard the device back to your Security Cloud Control tenant. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning on page 414 for more information.

If you are still unable to claim the device, review the device's workflow to see is there is an error message. If there is,Export the Workflow and open a support case to further troubleshoot the issue.

The device should successfully onboard to your Security Cloud Control tenant without the claim failure error.

Resolve provisional error for device onboarding

Configure device password settings or retry onboarding to resolve UnProvisioned connectivity status that occurs during device onboarding to Security Cloud Control.

Resolve UnProvisioned connectivity status that occurs when onboarding devices to Security Cloud Control due to password configuration mismatches or other provisional errors.

Devices can generate an UnProvisioned connectivity status during onboarding for various reasons, including password configuration mismatches between the device state and the onboarding wizard selections. This task provides multiple resolution approaches based on different scenarios.

Procedure

---

1. Determine which scenario applies to your device.

   Table 22: Device password configuration scenarios

If...	Then...
You did not change the default password and selected **No, this device has been logged into and configured for a manager** during onboarding	Proceed to step 2 to change the device password
You did change the default password and selected **Is this a new device that has never been logged into or configured before?** during onboarding	Proceed to step 3 to confirm and proceed with onboarding
Neither scenario applies or the issue persists	Proceed to step 4 to try alternative resolution methods

2. If the device password has not been changed, change the device password.
   a. Log into Security Cloud Control and navigate to the **Security Devices** page.
   b. Locate and select the device with the **UnProvisioned** connectivity status so it is highlighted.
   c. In the pane located to the right, locate the **Change Password** window.
   d. Click **Change Password** and enter a new password for your device. This overwrites the default password.

   It may take a few minutes for the device to onboard and fully synchronize to Security Cloud Control.

3. If the device password has already been changed, confirm and proceed with onboarding.
   a. Log into Security Cloud Control and navigate to the **Security Devices** page.
   b. Locate and select the device with the **UnProvisioned** connectivity status so it is highlighted.
   c. In the pane located to the right, locate the **Confirm and Proceed** window.
   d. Click **Confirm and Proceed**. This action ignores the password that was provided in the onboarding wizard and reinstates the default password for the device. Security Cloud Control then continues to onboard the device.

4. If other provisional error scenarios occur, try alternative resolution methods.

   If you confirm the password selection in the onboarding wizard is accurate for the state of the device, consider these options:

   - Select the device so it is highlighted. In the window located on the right pane of the screen, click **Retry** to force Security Cloud Control to re-onboard the device with existing provisional parameters.
   - Delete the device from the **Security Devices** page and attempt to re-onboard the device.
   - In the device's Firewall Device Manager UI, navigate to **System Settings** > **Cloud Services**. Select the **Auto-enroll with Tenancy from** Security Cloud Control and click **Register**.

   If you are still unable to claim the device, review the device's workflow to see is there is an error message. If there is, Export the Workflow and open a support case to further troubleshoot the issue.

The device successfully onboards to Security Cloud Control and displays a normal connectivity status instead of UnProvisioned.

20 Migrate Threat Defense to Cloud-Delivered Firewall Management Center

Topics:

- Firewall Threat Defense migration to Security Cloud Control
- End-to-end Firewall Threat Defense migration workflow
- Event and Analytics Management options during Firewall Threat Defense migration
- Supported features
- Restriction: unsupported features in firewall threat defense migration
- Recommendation: migration guidelines and limitations for VPN configuration
- Supported On-Premises Firewall Management Center and Firewall Threat Defense software versions for migration
- Prerequisites for migrating Firewall Threat Defense to Security Cloud Control
- Migrate Firewall Threat Defense to Security Cloud Control
- Review and manage Firewall Threat Defense migration job
- Configure migration notifications
- Verify Firewall Threat Defense connectivity with Security Cloud Control
- Use the troubleshoot feature for failed migrations

This chapter provides the steps to migrate On-Prem Firewall Management Center-managed Threat Defense to Cloud-Delivered Firewall Management Center.

Firewall Threat Defense migration to Security Cloud Control

Explains how to migrate Firewall Threat Defense devices from On-Premises Firewall Management Center to Security Cloud Control while preserving policies, configurations, and settings through Security Cloud Control Firewall Management.

Firewall Threat Defense migration to Security Cloud Control is a feature that

- enables organizations to move device management from on-premises infrastructure to Cisco's cloud-based management through Security Cloud Control,
- migrates Firewall Threat Defense devices from On-Premises Firewall Management Center to Security Cloud Control, and
- preserves existing policies, objects, and configurations during the migration process.

Customer benefits

This migration provides these benefits:

- Preserves existing policies and configuration
- Imports device-specific configuration, including interfaces, routing, and related settings
- Handles duplicate policy and object names according to defined conflict-resolution rules
- Transfers feature licenses automatically
- Supports high availability pairs and clusters
- Provides 14-day evaluation window before permanent commit
- Allows analytics to remain on-prem or move to cloud
- Provides an intuitive troubleshooting page with status summaries and step-by-step progress to pinpoint issues.
- Provides migration reports for validation and audit

The user roles of the On-Premises Firewall Management Center are no longer applicable in Security Cloud Control after migration. Your authorization to perform tasks on the migrated device is based on your user role in Security Cloud Control. See the Users topic to understand the On-Premises Firewall Management Center Center and Security Cloud Control user role mapping.

Evaluation period and manager changes

Describes the 14-day evaluation period for migration changes in Cloud-Delivered Firewall Management Center before automatic commit, during which you can test, revert, or manually commit changes with certain restrictions.

An evaluation period is a migration assessment phase that

- provides 14 days to test and assess migration changes using Security Cloud Control
- allows you to undo changes and continue managing the device with On-Premises Firewall Management Center or commit migration changes manually, and
- automatically commits changes after the evaluation period expires if no manual action is taken.

Evaluation period phases

The evaluation period consists of three distinct phases with specific capabilities and restrictions.

After successful migration, you have these options:

- Evaluate configuration for 14 days.
- Undo the changes and continue managing the device with On-Premises Firewall Management Center.
- Commit migration changes to Cloud-Delivered Firewall Management Center.

During the evaluation window, these restrictions apply:

- High availability break may not be supported (depending on onboarding method).
- Advanced high availability or cluster operations can cause commit failure. Commit before changing HA or cluster configuration.
- Deleting devices is not allowed.
- Changes made in Cloud-Delivered Firewall Management Center are lost, if reverted.
- Do not create or modify domains or subdomains on the On-Premises Firewall Management Center if the domain change includes a Firewall Threat Defense device that was migrated to Security Cloud Control. Commit the migration changes in Security Cloud Control, or revert device management to the on-premises On-Premises Firewall Management Center, before you make domain changes that include the migrated device.

If you create or modify a domain before the migration job is committed, deployment of the device and domain configuration can fail. You can continue to create or modify domains on the On-Premises Firewall Management Center for devices that remain managed by that On-Premises Firewall Management Center and are not part of an uncommitted migration job.

After the evaluation period expires, these conditions apply:

- Changes are automatically committed.
- Selected commit actions cannot be revoked.ß

How Firewall Threat Defense licenses are handled during migration

Explains how Firewall Threat Defense licenses are handled during migration to cloud management, including license transfer to Security Cloud Control, release to the Smart License pool, device license reclamation, and analytics-only license considerations.

Firewall Threat Defense license handling during migration is a process that

- transfers all feature licenses associated with the device to Security Cloud Control and releases them from the Firewall Management Center to the Smart License pool
- enables the device to reclaim device-specific licenses during its registration with Security Cloud Control, and
- does not require device-specific licenses if devices remain in the Firewall Management Center for analytics only.

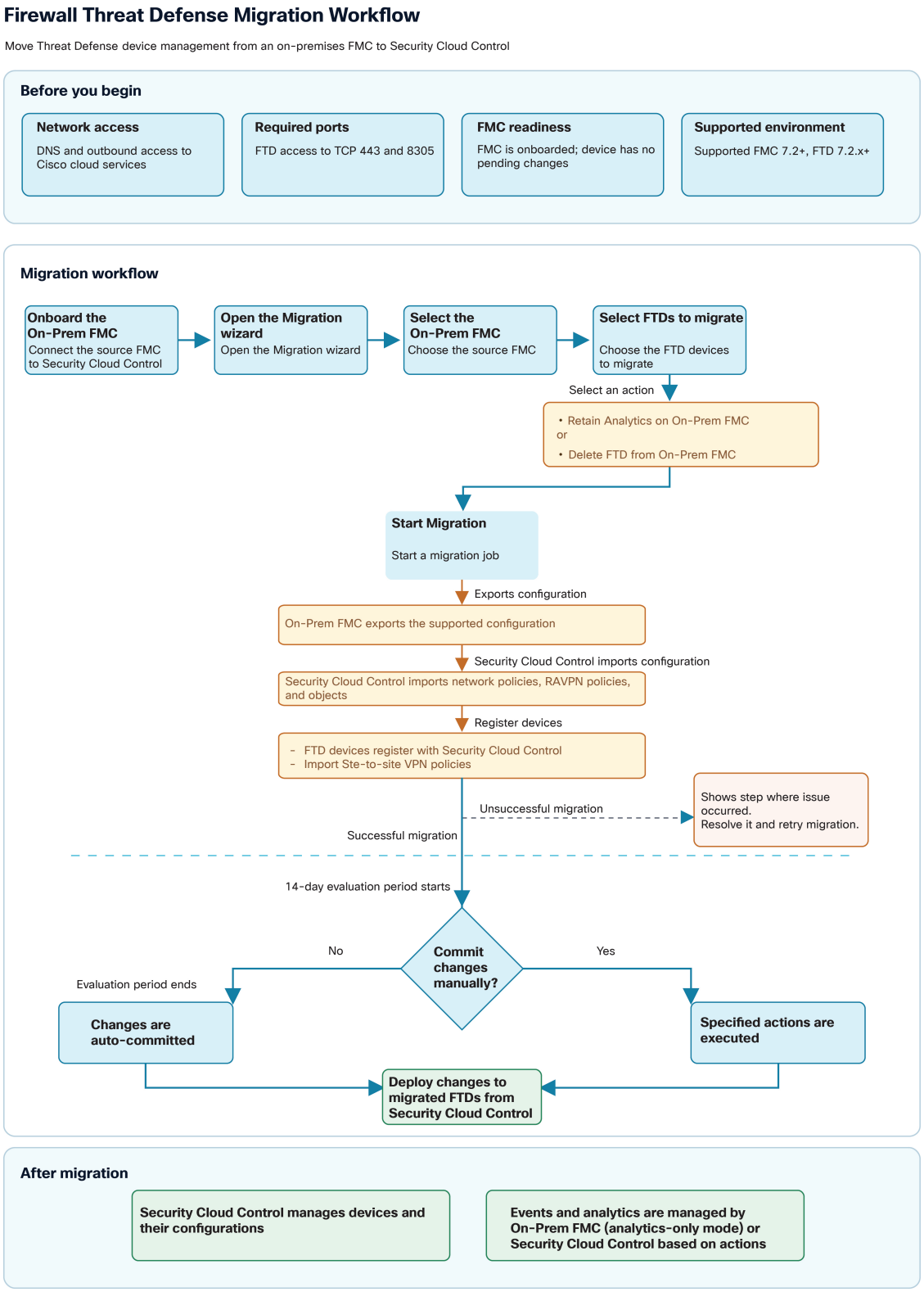
License handling details

You need not apply license on the device again after migration, as the license reclamation process occurs automatically during registration.

End-to-end Firewall Threat Defense migration workflow

Describes the end-to-end migration workflow for Firewall Threat Defense, providing a high-level flowchart that illustrates the key steps and processes involved in the migration procedure.

The following flowchart illustrates the high-level workflow for migrating Firewall Threat Defense to Security Cloud Control.



How Firewall Threat Defense migration to Security Cloud Control works

Describes how Firewall Threat Defense migration to cloud management works, including onboarding On-Premises Firewall Management Center, importing configurations, registering devices, evaluating changes, and committing or reverting management.

Summary

The key components involved in the Firewall Threat Defense migration to Security Cloud Control are:

- Security Cloud Control Firewall Management: Performs the migration sequence and manages the process workflow
- On-Premises Firewall Management Center: Source management center that exports configurations and manages analytics
- Firewall Threat Defense devices: Target devices to be migrated and managed
- Security Cloud Control: Cloud management platform that imports configurations and manages migrated devices

Workflow

The Firewall Threat Defense migration to Security Cloud Control involves these stages:

1. **Check readiness** Confirm that the On-Premises Firewall Management Center and Firewall Threat Defense versions are supported, the On-Premises Firewall Management Center is onboarded with no pending changes, and the required DNS and outbound access are available, including TCP ports 443 and 8305.
2. **Connect the source FMC** Onboard the On-Premises Firewall Management Center to Security Cloud Control, then open the migration wizard.
3. **Choose devices and actions** Select the source On-Premises Firewall Management Center and Firewall Threat Defense devices to migrate. Choose whether to retain analytics on the On-Premises Firewall Management Center or delete the Firewall Threat Defenses from that On-Premises Firewall Management Center.
4. **Start migration.** The On-Premises Firewall Management Center exports the supported configuration. Security Cloud Control imports the network and remote-access VPN policies and objects, registers the Firewall Threat Defenses, and imports site-to-site VPN policies.
5. **Resolve migration failures.** If migration fails, address the issue reported at the failed step and retry the migration.
6. **Evaluate the migration.** After a successful migration, review the configuration during the 14-day evaluation period.
7. **Commit the changes.** Commit manually to execute the selected actions, or allow the changes to be committed automatically when the evaluation period ends.
8. **Deploy and manage devices.** Deploy the intended changes to the migrated Firewall Threat Defenses from Security Cloud Control. After migration, Security Cloud Control manages device configuration; analytics are handled by the On-Premises Firewall Management Center in analytics-only mode or by Security Cloud Control, depending on the selected actions.

Result

After migration:

- Security Cloud Control manages devices and their configuration.
- Events and analytics can be handled by either the On-Premises Firewall Management Center (analytics-only mode) or Security Cloud Control.
- Migrated devices appear on the Security Cloud Control **Security Devices** page.

Event and Analytics Management options during Firewall Threat Defense migration

Describes the options for managing where Firewall Threat Defense events and analytics are sent during migration, with choices between on-premises Firewall Management Center or Security Cloud Control as the analytics manager.

Event and Analytics Management options during Firewall Threat Defense migration are configuration choices that

- determine where device events and analytics are sent during the migration process
- allow selection between retaining analytics on the On-Premises Firewall Management Center or transferring to Security Cloud Control, and
- vary by device model and analytics destination requirements.

Analytics destination options

The events and analytics management can be retained in the On-Premises Firewall Management Center or transferred to Security Cloud Control, where the devices must be configured to send events to Security Cloud Control.

While initiating the migration process, you are allowed to choose the manager where the device events must be sent for analytics:

- Retain analytics on the On-Premises Firewall Management Center

  Security Cloud Control manages configuration. Source On-Premises Firewall Management Center remains connected in analytics-only mode and receives events.

- Transfer analytics to Security Cloud Control

  Security Cloud Control manages configuration and analytics. The device sends events to Cisco cloud analytics through SSE or SEC.

Choose an analytics destination for each selected device. Configuration management moves to Security Cloud Control in either case

Special requirement for FMC 1000/2500/4500

If you are migrating from an On-Premises Firewall Management Center 1000/2500/4500, you **cannot** retain analytics on the On-Premises Firewall Management Center due to limited availability.

In this case, devices must send events to:

- Security Analytics and Logging (On-Prem), or
- Security Analytics and Logging (SaaS).

See Cisco Security Analytics and Logging.

If you retain On-Premises Firewall Management Center for analytics

- Security Cloud Control becomes the configuration manager.
- The devices remain on the On-Premises Firewall Management Center in **analytics-only mode**.
- Devices continue sending events to the On-Premises Firewall Management Center.
- Security Cloud Control manages configuration changes only.

> **Note**
>
> The maximum number of supported Secure Firewall Threat Defense devices in Security Cloud Control includes devices that are deployed for analytics on Firewall Management Center and onboarded to Security Cloud Control for management. These devices count toward the platform device capacity limit and must be included in your capacity planning to ensure proper sizing and performance.

If you select Security Cloud Control for analytics

- Secure Firewall Management Center becomes both:
  - Configuration manager, and
  - Analytics manager.
- The devices are removed from the On-Premises Firewall Management Center.
- You must configure the devices to send events to the Cisco cloud.
- Events can be sent using:
  - Security Services Exchange (SSE), or
  - Secure Event Connector (SEC)
- Events are processed by Cisco Secure Analytics and Logging (SAL) in the cloud.

Note

If you initially select On-Premises Firewall Management Center **for analytics**, you have a 14-day evaluation period during which you can change the analytics destination to Secure Firewall Management Center.

After either:

- Manually committing the migration, or
- The 14-day evaluation period expires, the analytics selection becomes permanent. Events will continue to be sent to the selected destination, and the setting cannot be changed.

To modify analytics settings after the evaluation period or after commit, refer to the migration troubleshooting procedures. see Troubleshoot Firewall Threat Defense migration failures on page 479

eStreamer Server Streaming

When you manage a Firewall Threat Defense device with Security Cloud Control, the device supports sending only fully-qualified events (FQE) to eStreamer clients. If you have configured eStreamer clients in the On-Premises Firewall Management Center, ensure that the clients support the detailed data formats used by FQE when you migrate the device management to Security Cloud Control. Any legacy clients, security information and event management (SIEM) systems, or log management solutions that do not support the data format of FQE or lack the necessary storage to handle the larger volume of FQE data will not work when you migrate.

Supported features

Lists how Security Cloud Control imports shared policies and device configurations from On-Premises Firewall Management Center, including supported policy types and duplicate policy or object name handling.

Security Cloud Control imports shared policies and device configurations from On-Premises Firewall Management Center, including supported policy types and duplicate policy or object name handling.

Shared policies imported

These policies are imported first and then followed by the device configuration:

- Access control

- IPS
- SSL
- Prefilter
- NAT
- QoS
- Identity
- Platform settings
- Flex config
- Network analysis
- DNS
- Malware & file
- Health
- Remote Access VPN
- Site-to-Site VPN

Handling duplicate names

If a policy or object name in Security Cloud Control Firewall Management matches one imported from the On-Premises Firewall Management Center, Security Cloud Control Firewall Management will take these actions after a successful management change.

Policies, Objects	Condition	Action
Access control, SSL, IPS, Prefilter, NAT, QoS, Identity, Platform settings, Network analysis, DNS, Malware & File policies.	Name of the Cloud-Delivered Firewall Management Center policy matches the On-Premises Firewall Management Center policy.	Cloud-Delivered Firewall Management Center policy is used.
RA VPN Default group policy **DfltGrpPolicy**	The default group policy**DfltGrpPolicy** from the On-Premises Firewall Management Center is ignored.	Existing Cloud-Delivered Firewall Management Center default group policy **DfltGrpPolicy** is used.
Network, Port objects	Name and content of network and port objects in the Cloud-Delivered Firewall Management Center match the ones in the On-Premises Firewall Management Center.	Existing Cloud-Delivered Firewall Management Center network and port objects with the same name and content are used. If the object has the same name but different content, an object override is created. See Object Overrides.
All other objects		Existing Cloud-Delivered Firewall Management Center object is used.

> **Note**
>
> Syslog alert objects used by access control policies are imported. If Security Cloud Control has an SNMP or email alert object with the same name as a source-On-Premises Firewall Management Center syslog alert object, the existing object is reused. Check for name collisions and rename the source syslog object before migration when necessary.

Restriction: unsupported features in firewall threat defense migration

Outlines which Firewall Threat Defense migration features are unsupported in Security Cloud Control, including excluded configurations, analytics-only devices, EVE exception rules, rule recommendations, and custom network analysis policy requirements.

Migration of a Firewall Threat Defense device registered only for analytics-only with the Firewall Management Center feature is not currently supported.

- Custom Widgets, Application Detectors, Correlation, SNMP and Email Alerts, Scanners, Groups, Dynamic Access Policy, Custom AMP Configuration, Users, Domains, Scheduled Deployment Tasks, ISE configuration, Scheduled GeoDB Updates, Threat Intelligence Director configuration, Dynamic Analysis Connections.
- ISE internal certificate object is not imported as part of the migration. You must export a new system certificate or a certificate and its associated private key from ISE and import it into Security Cloud Control.
- Custom Network Analysis Policies (NAPs). Remove them from source access control policies before migration; create a supported NAP in Security Cloud Control afterward if needed.
- New or updated intrusion rule recommendations. Migrated recommendations remain linked to the intrusion policy, but Security Cloud Control does not generate new ones or automatically update imported ones.

Encrypted Visibility Engine exception rules not migrated from On-Premises Firewall Management Center running Version 7.6 or 7.7

When migrating a Firewall Threat Defense device, which is managed by an On-Premises Firewall Management Center running Version 7.6 or 7.7, to Cloud-Delivered Firewall Management Center, Encrypted Visibility Engine (EVE) exception rules configured on the On-Premises Firewall Management Center are not migrated. This results in the loss of exception rules.

The Cisco support team will reach out to assist you in re-creating the EVE exception rules.

Alternatively, you can do this after the migration:

1. Identify exception rules in On-Premises Firewall Management Center: Access your On-Premises Firewall Management Center to identify all the EVE exception rules that were configured in the **Exception list**. For details, refer to the "Encrypted Visibility Engine" chapter in the Cisco Secure Firewall Management Center Device Configuration Guide, 7.7/7.6.
2. Reconfigure rules in Cloud-Delivered Firewall Management Center: In Cloud-Delivered Firewall Management Center, navigate to **Manage > Objects > EVE Exception List**. Manually reconfigure the identified EVE exception rules into the global EVE exception list object. For details, refer to "Encrypted Visibility Engine Exception List" topic in the "Object Management" chapter of the Cloud-Delivered Firewall Management Center guide.

Secure firewall recommended rules

Migrating Firewall Threat Defense to the cloud migrates existing rule recommendations linked to intrusion policies. However, the Cloud-Delivered Firewall Management Center does not generate new rule recommendations or auto-update migrated ones post-migration, as it does not support rule recommendations. See Auto Cisco Recommended Rules.

Remove custom network analysis policies

Before migration, Custom Network Analysis policies must be removed from the On-Premises Firewall Management Center.

1. Log on to the On-Premises Firewall Management Center.
2. Choose **Policies** > **Access Control**.
3. Click the edit icon on the access control policy you want to disassociate the custom NAP and then click the **Advanced** tab.
4. In the **Network Analysis and Intrusion Policies** area, click the edit icon.
5. In the **Default Network Analysis Policy** list, select a system-provided policy.
6. Click **OK**.
7. Click **Save** to save the changes and then click **Deploy** to download the changes to the device.

After migration, you can manually create the Network Analysis Policy in Security Cloud Control Firewall Management.

Recommendation: migration guidelines and limitations for VPN configuration

Outlines VPN migration guidelines for Firewall Threat Defense devices, including Remote Access VPN and Site-to-Site VPN settings, unsupported items, object overrides, certificates, local users, topology peers, and SASE tunnel limits.

Migration guidelines for remote access VPN

Keep the following in mind when you migrate a device with VPN configuration. Security Cloud Control Firewall Management imports all remote access VPN policy settings, with the following exceptions:

- Object overrides are not migrated. If overrides are used in the address pool object, manually add them to the imported object in Security Cloud Control Firewall Management after migration. See Object Overrides.
- Local users. If the authentication server uses a local database, the associated local realm object is imported into Security Cloud Control Firewall Management. However, you must manually add the local users to the imported local realm object after migration. See Create a Realm and Realm Directory.
- Load-balancing configuration is not migrated.
- Certificate enrollment with domain configuration. Perform the following after migration to enroll the certificate with domain configuration:

Perform the following after migration to enroll the certificate with domain configuration:

1. Choose **Security Devices**.
2. Select the migrated FTD and in the **Device Management** on the right, click **Device Overview**.
3. Choose **Devices** > **Certificates**. Perform one of the following tasks:
   - If the certificates are imported in an **Error** state, click the **Refresh certificate status** icon to synchronize the certificate status with the device. The certificate status turns green.
   - If the certificates are not imported, you must manually add the certificates defined in the Remote Access VPN policy that is configured in the Firewall Management Center.

Migration guidelines for Site-to-Site VPN

Selecting one device automatically selects its peers from associated topologies, as all devices within a topology must migrate together. Migration wizard doesn't list the extranet devices that are associated with them, but they will still be automatically included during the migration process. All settings will be migrated, with the following exceptions:

- Network object overrides are not migrated. They must be manually added to the imported object in Security Cloud Control Firewall Management after migration. See Object Overrides.
- If the authentication type configured as **Preshared Automatic Key** in the On-Premises Firewall Management Center:
  - Cloud-Delivered Firewall Management Center generates new pre-shared key post-deployment.
  - Existing tunnels remain active.
  - New tunnels use newly generated key.
- If devices are moved to Security Cloud Control Firewall Management but the changes are not yet committed, the associated site-to-site VPN policy can still be modified in the On-Premises Firewall Management Center, however, it those changes do not update the device configuration in Security Cloud Control Firewall Management.
- Devices configured for SASE tunnels on Cisco Umbrella are not migrated.

Supported On-Premises Firewall Management Center and Firewall Threat Defense software versions for migration

Lists supported On-Premises Firewall Management Center and Firewall Threat Defense versions for migration, including high availability, cluster, multi-instance, interim upgrade, evaluation period, and post-migration requirements.

This reference provides the minimum supported versions for On-Premises Firewall Management Center and Firewall Threat Defense migration. It covers migration requirements for physical On-Premises Firewall Management Center models, high availability configurations, cluster deployments, and multi-instance devices.

Minimum supported versions

- Minimum On-Premises Firewall Management Center: 7.2
- Minimum Firewall Threat Defense: 7.2.x (not supported for Version 7.1)

Physical On-Premises Firewall Management Center 1000/2500/4500 Model-Managed Firewall Threat Defense

- Migration is supported from **physical FMC 1000/2500/4500** models.
- *Temporary upgrade from 7.0 to 7.4* is supported for migration purposes only. The On-Premises Firewall Management Center Version 7.4 is "unsupported for general operations," but allowed as an interim step until migration completes. You can download the upgrade package here.
- After migration, do these tasks:
  1. Return to On-Premises Firewall Management Center to a supported version after migration.
  2. Remove re-migrated devices.
  3. Reimage back to 7.2.x.
  4. Re-register the devices.

> **Note**
>
> Unzip (but do not untar) the upgrade package before uploading it to the On-Premises Firewall Management Center. To upgrade to Version 7.4, see Cisco Secure Firewall Management Center Upgrade Guide, Version 6.0-7.0.

We recommend upgrading the devices to Version 7.2.x before upgrading the On-Premises Firewall Management Center to Version 7.4.

Important

An upgrade is necessary because Version 7.0 On-Premises Firewall Management Centers do not support cloud device migration. Only Version 7.4 is supported during the migration and evaluation process. These On-Premises Firewall Management Centers cannot run intermediate versions. Only standalone and high availability Firewall Threat Defense devices running Version 7.0.3+ (7.0.5 recommended) are eligible for migration.

Firewall Threat Defense in a High Availability Pair

- High availability pairs migrate as a single node.
- Both active and standby Firewall Threat Defense devices migrate together.

Important

We highly recommend committing manager changes before performing advanced operations, like creating or breaking high availability configurations from the On-Premises Firewall Management Center on the devices being migrated. Carrying out these tasks during the evaluation period is unsupported and may lead to migration commit failure.

Firewall Management Center in a High Availability Pair

- Onboard the active On-Premises Firewall Management Center and not the standby.
- Use either the auto-onboarding method or the credentials method for onboarding the On-Premises Firewall Management Center.

> **Note**
>
> If you have already onboarded a standalone On-Premises Firewall Management Center and later configured it as a standby, delete the standby On-Premises Firewall Management Center and onboard the active one.

Points to Remember:

- **Auto-onboarding On-Premises Firewall Management Center Method**
  - High availability break is not supported during the 14 days evaluation period.

You can break high availability after changes are committed, manually or automatically, after the evaluation period.

- High availability switchover is supported during the 14 days evaluation period.

- **Onboarding On-Premises Firewall Management Center Method Using Credentials**
  - High availability break and high availability switchover are not supported during the 14 days evaluation period. You can perform these operations after committing the changes manually or automatically after the evaluation period.
  - After a switchover, onboard the new active unit, which was previously in standby mode, and then start a migration job on the devices.

Note

During the 14-day evaluation period after migrating a Firewall Threat Defense device, if you have performed advanced operations on the device, such as converting it to a multi-instance chassis, note that the evaluation period becomes nullified, and you will not be able to revert the device management back to the On-Premises Firewall Management Center.

If you want to manage a multi-instance chassis using Cloud-Delivered Firewall Management Center, onboard the chassis manually to Security Cloud Control.

Firewall Threat Defense cluster

Firewall Threat Defense cluster migration is supported on these platforms with minimum versions:

Platforms	Minimum Firewall Threat Defense	Minimum On-Premises Firewall Management Center Version
VMware, KVM	7.2.1	7.4.1
AWS, GCP	7.2.1	7.4.1
Azure	7.3	7.4.1
Secure Firewall 3100	7.2.1	7.4.1
Firepower 4100	7.2.x	7.4.1
Secure Firewall 4200	7.4	7.4.1
Firepower 9300	7.2.x	7.4.1

Important

Before migrating the Firewall Threat Defense cluster, remember these points:

- Do not migrate the Firewall Threat Defense cluster during clustering-related operations from the On-Premises Firewall Management Center.
- After migration, manually commit manager changes before performing advanced operations, such as adding a node, breaking a node, breaking a cluster, or converting a device from native mode to multi-instance (container)

mode from the On-Premises Firewall Management Center. Performing such tasks during the evaluation period may result in migration commit failure.

Migration Support for Multi-instance Firewall Threat Defense Devices

You can migrate a multi-instance Firewall Threat Defense device that is part of a chassis (Secure Firewall 3100). The multi-instance device gets listed as one of the devices in the **Select Devices** page, and you can choose it to proceed with the migration. This migration is supported in Firewall Threat Defense device versions 7.6 or later.

If you decide to do such a multi-instance Firewall Threat Defense device migration, it is strongly recommended that you unregister the corresponding chassis device manually from the On-Premises Firewall Management Center and onboard it to Security Cloud Control, by navigating to the **Security Devices** page.

Prerequisites for migrating Firewall Threat Defense to Security Cloud Control

Outlines prerequisites for migrating Firewall Threat Defense devices to Security Cloud Control, including DNS, port access, on-premises Firewall Management Center onboarding, user permissions, backups, synchronization, VPN peers, object conflicts, FlexConfig objects, and HA failover health.

DNS and network configuration requirements

Ensure that the following network prerequisites are met before you begin the migration process.

- **DNS Server Configuration**: The Firewall Threat Defenses must have the correct DNS server configuration to resolve Security Cloud Control hostnames. For details about checking connectivity with Security Cloud Control, see Check device connectivity with Security Cloud Control.
- **Network Access**: The required network access must be enabled for Firewall Threat Defenses to reach Security Cloud Control through the TCP port 8305. Note that outbound connectivity from the Firewall Threat Defenses to Security Cloud Control is sufficient.
- **Firewall Threat Defense Outbound Port 443**: The Firewall Threat Defenses must be able to access port 443 and 8305 of Security Cloud Control.
- **On-Premises Firewall Management Center Outbound Port 443**: The On-Premises Firewall Management Center must have access to outbound port 443 open to reach "*.cdo.cisco.com" domain.
- On-Premises Firewall Management Center should allow outbound HTTP/HTTPS to upload configurations to Amazon S3.

On-Premises FMC onboarding and version requirements

Verify that the On-Premises Firewall Management Center is onboarded to Security Cloud Control. Onboarding the On-Premises Firewall Management Center also onboards all the Firewall Threat Defense devices registered to that On-Premises Firewall Management Center. See Onboard an On-Prem FMC.

- For the On-Premises Firewall Management Center 1000/2500/4500 migration: Run Version 7.4 (available for these models on a temporary basis). We recommend devices be running Version 7.0.5.
- We recommend that you create a backup of On-Premises Firewall Management Center. For versions On-Premises Firewall Management Center Version 6.5 to 7.1, see the *Back up the FMC* topic in the Firepower Management Center Configuration Guide. For On-Premises Firewall Management Center Version 7.2 and later, see the *Back up the Management Center* topic in the Cisco Secure Firewall Management Center Administration Guide.

User account and permission requirements

Create a new user in the On-Premises Firewall Management Center with Administrator role or a custom user role with "Devices" and "System" permissions for onboarding purposes.

If you onboard an On-Premises Firewall Management Center to Security Cloud Control and simultaneously sign in to that On-Premises Firewall Management Center with the same user name, the onboarding fails.

Device synchronization and VPN requirements

Ensure proper device and VPN configuration before initiating migration.

- The Firewall Threat Defense devices must be synchronized and not have pending changes on them. The migration fails on a device if Security Cloud Control identifies pending changes on that device.
- All peer devices in a site-to-site VPN topology must be online and have no pending deployment.

Object conflict and FlexConfig considerations

Verify and resolve potential object conflicts and FlexConfig issues before migration.

- Security Cloud Control imports Syslog alert object used in the access control policy from the On-Premises Firewall Management Center. If Security Cloud Control already contains an alert object with the same name but a different type (SNMP, Email), it is reused during configuration import. The user must check whether the Syslog object name matches the existing SNMP or Email alert object in Security Cloud Control. If the name matches, you must rename the Syslog object in the On-Premises Firewall Management Center before starting the migration process.
- If you attempt to migrate firewalls with modified system defined FlexConfig text objects from an On-Premises Firewall Management Center to the Security Cloud Control, the values of the modified system defined FlexConfig text objects are not migrated to the Security Cloud Control, and the deployment will fail. To avoid this, copy the modified system defined FlexConfig text object values from the On-Premises Firewall Management Center to Security Cloud Control before migration and initiate migration from On-Premises Firewall Management Center to Security Cloud Control after verifying the predefined FlexConfig text objects.

Policy and object name conflicts

If a policy in Security Cloud Control shares the same name as one in On-Premises Firewall Management Center (excluding network, port, URL, and VLAN objects), the Security Cloud Controlversion will be retained. See Handling Shared Policies and Objects.

After migration, policies and objects aren't auto-synced between On-Premises Firewall Management Center and Security Cloud Control. For phased migrations, you must update them manually.

You can revert to On-Premises Firewall Management Center within 14 days of migration. After that, changes are finalized automatically. See Revert the Threat Defense Management to On-Prem Firewall Management Center.

Requirement: high availability failover link must be up

The high availability failover link should be up for a successful migration. Before initiating the migration process on Security Cloud Control, determine the health status of the failover link on the On-Premises Firewall Management Center.

To identify the failover interfaces of all HA pairs you want to migrate to Cloud-Delivered Firewall Management Center, choose **Devices** > **Device Management**, click **Edit** , click the **High Availability** tab, and view the **Interface** field in the **High Availability Link** area. To check the health status of the failover interfaces, choose **Devices** > **Device Management**, click **Health Monitor**, expand the high availability pair, click the device with the exclamation mark, click the **Critical** button, and check the **Interface Status** for errors. If the failover interface is down, the **Interface 'failover_interfacename' has no link** message is displayed. Rectify the issue and click **Sync from onprem FMC now** to obtain the latest changes on the device.

Migrate Firewall Threat Defense to Security Cloud Control

Configure migration of Firewall Threat Defense devices from On-Premises Firewall Management Center to Security Cloud Control, including device selection, VPN peer handling, commit actions, policy review, and deployment options.

This task migrates Firewall Threat Defense devices from an on-premises Firewall Management Center to cloud management, enabling centralized cloud-based device management and policy deployment.

Migration transfers device management from on-premises infrastructure to cloud services while preserving existing configurations and policies. The process includes automatic VPN peer device selection and provides options for policy review and deployment timing.

Before you begin

Confirm FMC and FTD versions, disk space, DNS, outbound access, device synchronization, topology peers, and backup. See prerequisites for migrating and supported software versions.

Follow these steps to migrate Firewall Threat Defense devices to cloud management:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation bar on the left, click **Administration** > **Migration** > **Migrate FTD to cdFMC**.
3. Click  and choose **On-Prem FMC-managed FTD to** Cloud-Delivered Firewall Management Center.

   Note

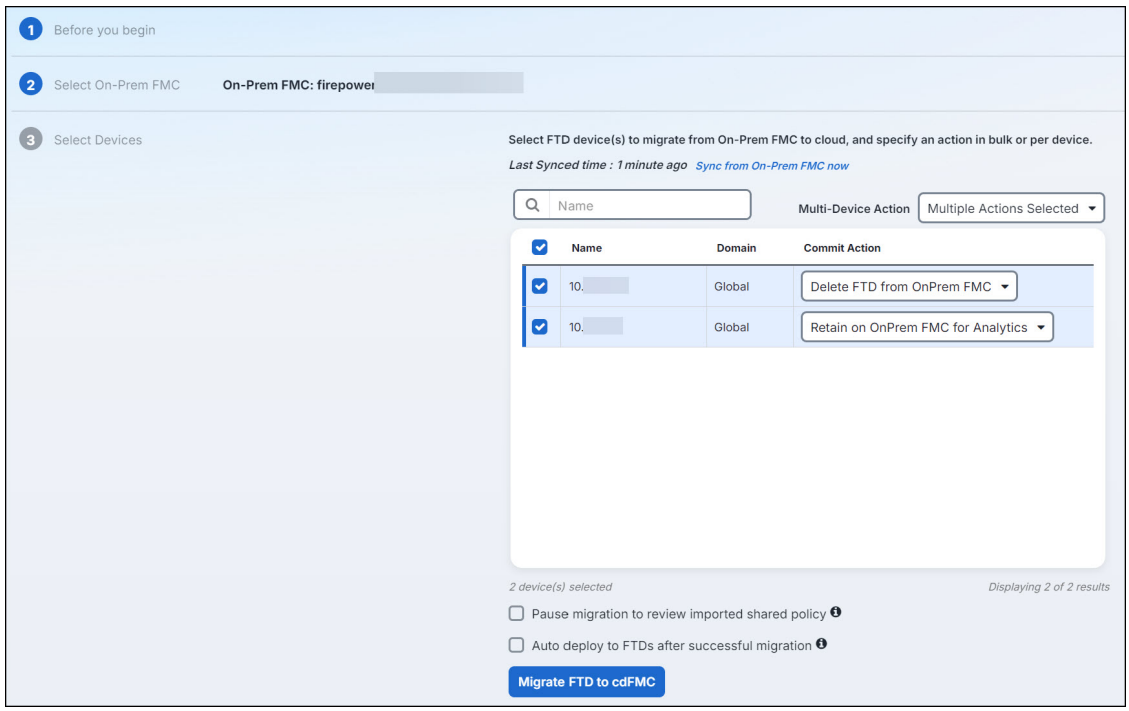
   You can initiate only one migration job at one time.

4. In the **Select On-Prem FMC** area, perform these actions:
   a. You can click the **Onboard an FMC** link to onboard the On-Premises Firewall Management Center if you have not done already. See Onboard an FMC.
   b. Select the On-Premises Firewall Management Center from the available list and click **Next**.

   In the **Select Devices** step, you will see the Firewall Threat Defense devices that the selected On-Premises Firewall Management Center manages. If a high-availability pair is set up on the on-premise On-Premises Firewall Management Center, the high availability node will be shown instead of the active and standby devices.

   The **Last Synced time** field indicates the time that is elapsed since the device configuration is synchronized into the On-Premises Firewall Management Center. You can click **Sync from OnPrem FMC now** to fetch the latest device changes.
5. In the **Select Devices** step, configure device selection and commit actions:
   a) Select the devices that you want to migrate.

   These devices can include standalone, high-availability pairs, or clusters. If you have a high-availability pair or a cluster, select the node that represents it. Also, you can hover your mouse pointer over the cluster to view more details about the control node.



Note

- The devices running on unsupported versions are not available for selection.
- The devices that are registered for analytics only with the On-Premises Firewall Management Center or have pending changes to be deployed are not eligible for migration.
- When you select a device that is associated with a site-to-site VPN topology, Security Cloud Control automatically selects its peer devices belonging to either the same topology or a different topology, because all devices in the site-to-site VPN topology must be migrated together for a successful migration to take place. The wizard does not list the extranet devices, if any. However, Security Cloud Control migrates extranet devices.

  The **S2S VPN Topology** column indicates the number of site-to-site VPN topologies in which a selected device participates. You click the topology link to view the topologies and devices that are migrated along with the selected device. This field is not applicable to devices that are not part of the site-to-site VPN topology.
- A high availability pair is presented as a single node. You must select this node to include active and standby devices in the migration.

b) In the **Multi-Device Action** list, you can choose a common action to apply on all devices.
c) In the **Commit Action** column, you can choose one of these actions for the selected device:

- **Retain on OnPrem FMC for Analytics**: After the migration process is completed, the analytics management for selected Firewall Threat Defense devices is retained on the On-Premises Firewall Management Center.
- **Delete FTD from OnPrem FMC**: After the migration process is completed, the selected devices are removed from the On-Premises Firewall Management Center and are available for Security Cloud Control to handle the analytics. You must configure the devices to send events to Security Cloud Control for managing

analytics. When the devices are deleted from the On-Premises Firewall Management Center, they cannot be revoked.

> **Note**
>
> For the On-Premises Firewall Management Center 1000/2500/4500, when you select devices to migrate, make sure you choose **Delete FTD from OnPrem FMC**. Note that the device is not fully deleted unless you commit the changes or 14 days pass.

> **Note**
>
> The actions that are specified here are committed automatically after the 14 days evaluation period or after the changes are committed manually.

6. (Optional) Check the **Pause migration to review imported shared policies** check box.

   When you enable this option, the migration process will pause after the shared access policies like Access Control and NAT policies are staged in the Cloud-Delivered Firewall Management Center. This pause ensures that the evaluation doesn't start and that the device's current state and manager remain unaffected. It gives you ample time to review the imported configuration for accuracy. After you've assessed everything, you can resume the migration during the planned migration interval, which will then kick off the 15-day evaluation period.

7. Check the **Auto deploy to FTDs after successful migration** check box to deploy the migrated configuration automatically to the device after successfully migrating and registering the device with the Cloud-Delivered Firewall Management Center.

   However, if you prefer to review and manually deploy the configuration from the Cloud-Delivered Firewall Management Center after successful migration, you can uncheck this option and proceed to the next step.

   > **Note**
   >
   > Perform the migration during a maintenance window. If you check **Auto deploy to FTDs after successful migration**, the migrated policies are deployed to the devices as soon as migration succeeds, which can disrupt traffic.
   >
   > If you leave this option unchecked, deploy the policies manually during the maintenance window. Do not perform any modification until you finish successful first deployment after migration. Deploying the migrated policies promptly also helps reduce the risk that configuration operations during the evaluation period will cause later commits to fail.

8. Click **Migrate FTD to cdFMC**.
9. Click **View Migration to Cloud Progress** to see the progress.

What to do next:

If you selected **Pause migration to review imported shared policies**, Security Cloud Control pauses after staging shared policies such as access control and NAT. The job does not start evaluation or change the device

manager at that point. You must manually click **Proceed Migration** to import the remaining configuration. See Proceed migration process on page 471.

You can view the overall and individual status of migration jobs and generate a report when a job is completed successfully. See Review and manage Firewall Threat Defense migration job on page 469.

The migration job begins and transfers device management from the on-premises FMC to cloud management. You can monitor progress through the migration status interface and receive notifications when the process completes successfully.

Review and manage Firewall Threat Defense migration job

Configure review and management of Firewall Threat Defense migration job status in Security Cloud Control, including device progress monitoring, evaluation-period actions, report downloads, and deployment issue resolution.

Use this task to effectively monitor and manage Firewall Threat Defense migration jobs, track device migration progress, handle evaluation period activities, and resolve deployment or identity policy issues that may arise during the migration process.

The migration dashboard provides the status of all migration jobs initiated from the Security Cloud Control. You can expand a specific job to see the status of individual devices associated with that tenant. This helps you keep track of the progress of your migration and identify issues, if any, that need to be addressed.

When a migration job is successful, you have 14 days to test and assess migration changes. If you are convinced about the migration changes, we recommend that you commit the devices manually, and not wait for Security Cloud Control to automatically commit the migration changes.

Procedure

---

1. Check migration job status in the migration dashboard.

   If you have set up alerts for device workflows, click the notifications icon  to see the alerts that have been triggered during the migration process. Additionally, if you have opted to receive email notifications from Security Cloud Control, you will also receive an email notification regarding alerts, if any.

   Review the following information for each migration job:

   - **Name**: Represents the job name that shows the On-Premises Firewall Management Center name and the date and time when the job was initiated.
   - **Number of FTDs**: Shows the total number of devices that are being migrated to the cloud.
   - **Status**: Shows the status of the job. Expand the job to see the status of individual devices.
   - **Last Update**: Shows the date and time that are updated only when a change is made to the device.

2. Manage migration job actions using the Actions menu.

   Click to execute the following actions:

   - **Workflows**: Takes you to the **Workflows** to monitor the job. See Monitor workflows in Security Cloud Control on page 1051.
   - **Download Report**: Allows you to generate and download a report of every job that is completed successfully. See Generate a migration report on page 475.

- **Commit Manager Changes**: Allows you to apply the changes manually to devices before the evaluation period ends. See Commit migration changes manually to Security Cloud Control on page 471.
- **Remove Migration Job**: Allows you to remove a completed job. Link is available only for completed jobs. See Remove a completed migration job on page 475.

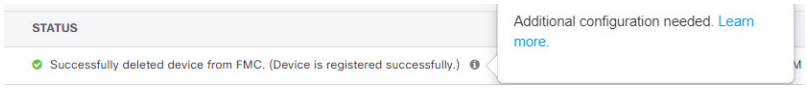
3. Monitor deployment status and address validation issues.

   After a successful migration, Security Cloud Control deploys the configuration to the device. If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Messages** window. To view complete details, click the arrow icon before the warnings or errors. If the deployment fails, see the *Best Practices for Deploying Configuration Changes* section of Firepower Management Center Device Configuration Guide X.Y.

4. Configure realm sequence for identity policy if required.

   If the device contains an identity policy with a Realm or ISE configuration, configure your device as a proxy for Security Cloud Control to communicate with the identity source. The identity policies don't function if Security Cloud Control fails to connect to the Identity Realms.

   A tooltip appears in the **Status** column for a device that requires additional configuration.

   a) Click the tooltip icon and then click **Learn more**.
   b) In the **Configure Proxy** window, click **Configure my realms**.

      To add a proxy sequence, see the *Create a Proxy Sequence* section in the Firepower Management Center Device Configuration Guide, 7.2.

5. Commit migration changes if satisfied with the evaluation.

   When a job is completed successfully, the **FTD Migration job is successful message** appears in the **Status** column. You can click the tooltip to see the number of days remaining for evaluating the manager.

   You can click Commit Migration Changes to commit the changes manually before the 14 days evaluation period ends.

   Note

   - You cannot revoke the actions that are specified in the migration commit window after committing the changes.
   - You can cancel the migration during the evaluation period and return the device to the On-Premises Firewall Management Center.
   - You cannot delete a device from either the On-Premises Firewall Management Center or Cloud-Delivered Firewall Management Center during the evaluation period.

   Important

   Changes can be made and deployed to the device using Security Cloud Control during the evaluation period. If you switch device management back to the On-Premises Firewall Management Center, Security Cloud Control-specific changes made during the evaluation period is not saved on the device once it is reverted to the source Security

Cloud Control tenant. You must deploy the changes from the On-Premises Firewall Management Center to the device after reverting the device's manager.

You have successfully reviewed and managed the Firewall Threat Defense migration job. The migration status is monitored, any deployment issues are addressed, identity policy configurations are updated as needed, and migration changes are committed or cancelled based on your evaluation.

Note that for the On-Premises Firewall Management Center 1000/2500/4500, you would have migrated devices from Version 7.4, which is unsupported for general operations. To return the On-Premises Firewall Management Center to a supported version you must remove the re-migrated devices, reimage back to Version 7.2.x, restore from backup, and re-register the devices.

Proceed migration process

Configure the continuation of a paused Firewall Threat Defense migration to complete device-specific configurations and registration.

This task resumes a paused migration process to complete the import of device-specific configurations and register devices with Security Cloud Control.

If the **Pause migration to review imported shared policies** option was checked during the migration setup, the migration process will pause after the shared access policies were staged in the Security Cloud Control. After you've reviewed the staged configurations, you must manually instruct Security Cloud Control to resume the migration, which will then import device-specific configurations such as routing and interfaces, as well as register the Firewall Threat Defense with the Security Cloud Control. Completion of the migration triggers a 14-day evaluation period.

Procedure

Go to the migration job page and click **Proceed with migration** for the relevant job.

The migration process resumes and completes the import of device-specific configurations and registration with Security Cloud Control. A 14-day evaluation period begins upon completion.

What to do next

Remember that deployment from the Security Cloud Control must be done after a successful migration.

Commit migration changes manually to Security Cloud Control

Configure manual commit of Firewall Threat Defense migration changes in Security Cloud Control, choose analytics ownership actions, and track commit progress.

This task enables you to manually commit Firewall Threat Defense migration changes to Security Cloud Control when you are confident in your changes and do not want to wait for automatic commit.

We recommend that you commit migration changes manually if you are convinced with your changes and not waiting for Security Cloud Control to auto commit changes. The **Commit Migration Changes** window shows the remaining days to commit the migration to Security Cloud Control or revert the device to On-Premises Firewall Management Center. During the evaluation period, you can modify the actions for selected threat defense devices before committing the changes. Once the changes are committed, you can't revoke the actions.

> **Note**
>
> The commit manager changes actions are disabled in the following conditions:

- The 14-day evaluation period has passed.
- The Firewall Threat Defense devices have either been reverted to the On-Premises Firewall Management Center or deleted from On-Premises Firewall Management Center, in which case, no further actions can be taken.

Procedure

1. In the migration jobs page, click the under the **Actions** column of a completed job.
2. Click **Commit Migration Changes**.

   This link is available only after a job is completed successfully.
3. Select a device and in the **Commit Actions** list, choose one of the following actions:
   - **Retain on OnPrem FMC for Analytics**: After committing the changes, analytics management for selected Firewall Threat Defense devices is retained on the management center.
   - **Delete Firewall Threat Defense from OnPrem FMC**: After committing the changes, the selected devices are removed from the On-Premises Firewall Management Center and are available for Security Cloud Control to handle the analytics. You must configure the Firewall Threat Defense to send events to Security Cloud Control for managing analytics. After the Firewall Threat Defense devices are deleted from the On-Premises Firewall Management Center, they cannot be revoked.

   > **Note**
   >
   > If you want to revert the device management to On-Premises Firewall Management Center, refer to Revert manager ownership to On-Premises Firewall Management Center on page 472.
4. Click **Commit** executes your specified actions immediately without further confirmation.

   On the migration jobs screen, you can expand the job to check the progress of the actions specified.

   The migrated devices appear on Security Cloud Control's **Security Devices** page. These devices can be managed using the Cloud-Delivered Firewall Management Center portal that is linked to Security Cloud Control. Ensure you deploy the changes to the devices from Cloud-Delivered Firewall Management Center.

Migration changes are committed to Security Cloud Control with the selected analytics ownership actions applied. The migrated devices become available for management through Security Cloud Control.

Revert manager ownership to On-Premises Firewall Management Center

Configure device management reversion to On-Premises Firewall Management Center during the migration evaluation period and redeploy changes from the original manager.

This task reverts Firewall Threat Defense device management to the original On-Premises Firewall Management Center during the evaluation period, allowing you to discontinue management through the Security Cloud Control platform.

You can revert the device management to the On-Premises Firewall Management Center during the evaluation period. This means that the devices will no longer be managed through the Security Cloud Control platform. However, it is important to note that any changes made during the migration process in the Security Cloud Control will not be reflected in the On-Premises Firewall Management Center after reverting Firewall Threat Defense management.

Note

When the Firewall Threat Defense management has been returned to the On-Premises Firewall Management Center, you can begin the migration job again to switch the Firewall Threat Defense management to Security Cloud Control.

Procedure

1. In the migration jobs page, click the ... under the **Actions** column of a completed job.
2. Click **Commit Migration Changes**.

   This link is available only after a job is completed successfully.
3. Select a device and in the **Commit Actions** list, choose **Revert Manager to OnPrem FMC**.
4. Click **Commit** executes your specified actions immediately without further confirmation.
5. Deploy the changes to the device from the On-Premises Firewall Management Center.

The device management is reverted to the On-Premises Firewall Management Center and the device is no longer managed through the Security Cloud Control platform.

View migrated devices and analytics-only entries

Configure the viewing of migrated Firewall Threat Defense devices and analytics-only entries in Security Cloud Control to distinguish configuration-managed and analytics-managed instances.

This task allows you to view and distinguish between configuration-managed and analytics-managed device instances after migration.

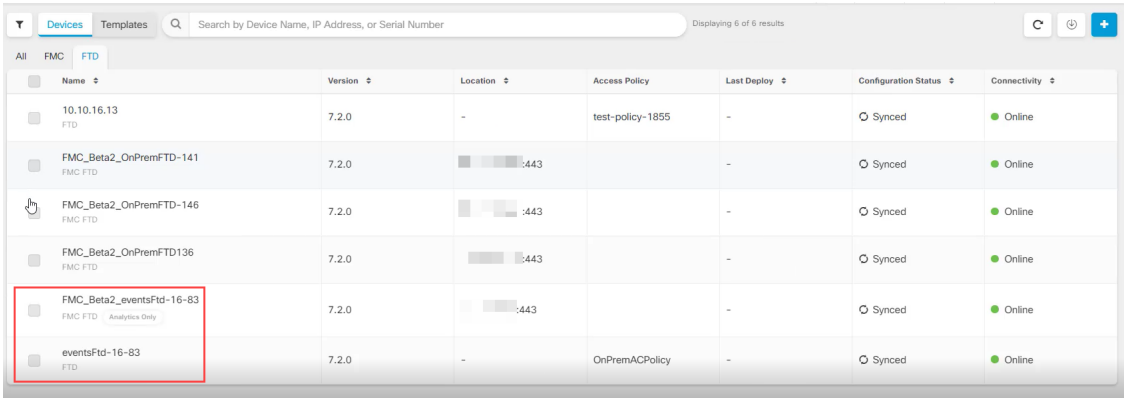
The migrated devices appear on the **Security Devices** page in Security Cloud Control. You can cross-launch and configure the required feature on the Cloud-Delivered Firewall Management Center.

> **Note**
>
> The devices on the Cloud-Delivered Firewall Management Center device listing page may show **No-IP** instead of the device's management IP address. Because the device registration uses the NAT ID, the device initiates the process, and therefore, the management IPs aren't discovered or used for the connection. Note that this applies to newly onboarded devices and devices migrated from the On-Premises Firewall Management Center.

Procedure

1. Navigate to the **Security Devices** page to view migrated devices.

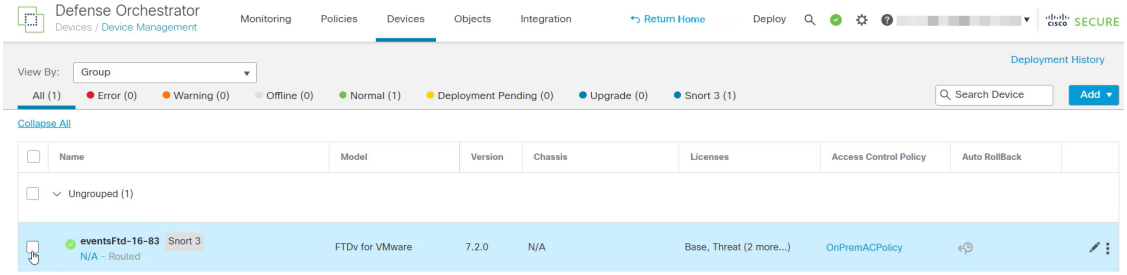
   Security Cloud Control creates two instances of the same device that is configured to retain on the Firewall Management Center for analytics.



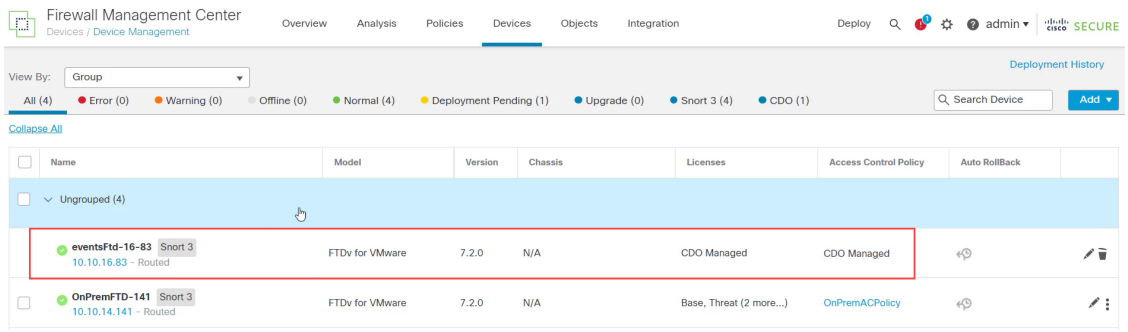
   The device instance with **FMC FTD** and **Analytics Only** labels shows that the Firewall Management Center handles the analytics. The device instance with the **FTD** label indicates that Security Cloud Control manages its configuration.

2. Select the device having **FTD** label and in the **Management** pane on the right, click **Device Summary**.

   You can manage the configuration of the device using Security Cloud Control. This will show the device in the Cloud-Delivered Firewall Management Center.



3. To view events from the device, select the device having **FMC FTD** and **Analytics Only** labels and on the right, click the **Manage Devices** link.
4. Log on to the on premise Firewall Management Center.
5. Choose **Device** > **Device Management**.



You can't select this device as Security Cloud Control manages the configuration. The Firewall Management Center shows the **Security Cloud Control Managed** label for this device.

6. To see the live events in the Firewall Management Center, click **Analysis** > **Events**.

You can now view and distinguish between migrated devices and analytics-only entries, access device summaries for configuration-managed instances, and view live events from analytics-only instances.

Generate a migration report

Configure a migration report download to review configuration imported from On-Premises Firewall Management Center to Security Cloud Control, including device, policy, object, routing, interface, and network details.

Generate and download a PDF migration report to review imported settings after a successful migration job. The report provides comprehensive details about device configurations, shared-policy values, objects, routing, interfaces, network settings, and other imported parameters.

After completing a migration job from On-Premises Firewall Management Center to Security Cloud Control, you can access a detailed report that documents all imported configurations. This report is available for download within one year of job completion and serves as a reference for reviewing the migration results.

Procedure

---

1. On the migration jobs page, click the ... under the **Actions** column of a completed job.
2. Click **Download Report**.

   You must download the report within a year after the job starts.

A PDF report downloads containing device details, shared-policy values, objects, routing, interfaces, network settings, and other imported parameters from the migration job.

Remove a completed migration job

Configure the removal of a completed migration job from the migration page when you no longer need it displayed, keeping the job list easier to navigate.

Remove a completed migration job to clean up the migration page and make it easier to navigate when the job is no longer needed.

Remove a job only after it is no longer needed. This cleans up the migration page and make it easier to navigate.

> **Attention**
>
> If you want to delete a migration job during the evaluation period, you must first commit the migration changes or revert the manager to the on-prem management center. Failing to do so may result in an inconsistent state of the on-prem management center, which could be unrecoverable. See Commit Migration Changes Manually.
>
> If you don't have access to your On-Premises Firewall Management Center or if it is no longer available and you are blocked from performing a commit or revert, you can delete the job.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click **Administration** > **Migration** > **Migrate FTD to cdFMC**.
3. Click the ... under the **Actions** column and then click **Remove Migration Job**.
4. Click **Delete** to confirm your action.

The migration job is removed from the migration page, making the job list cleaner and easier to navigate.

Configure migration notifications

Provides information on enabling email notifications for Firewall Threat Defense migration events in Security Cloud Control.

You can subscribe to get email notifications from Security Cloud Control whenever a device associated with your tenant experiences a specific action when migrating a Firewall Threat Defense device to Security Cloud Control.

Security Cloud Control sends an email if you enable to receive a notification for these states during migration:

- **Failed**: When a migration job fails.
- **Started**: When a migration job is initiated.
- **Succeeded**: When a migration job is completed successfully.
- **Commit Pending**: When the manager changes have to be committed.

To enable notification settings, see Notification Settings.

Verify Firewall Threat Defense connectivity with Security Cloud Control

Provides commands to verify Firewall Threat Defense connectivity to Security Cloud Control by checking internet reachability, validating hostname resolution, and correcting DNS configuration from the device CLI.

This section provides the commands to determine the Firewall Threat Defense connectivity with the Security Cloud Control.

Test internet reachability from the device

Execute the **ping system** *<any OpenDNS server address>* command to check whether the device can reach the internet.

1. Connect to the CLI of the device, either from the console port or using SSH.
2. Log in with the Admin username and password.

3. Enter **ping system** *<OpenDNS IPAddress>*.

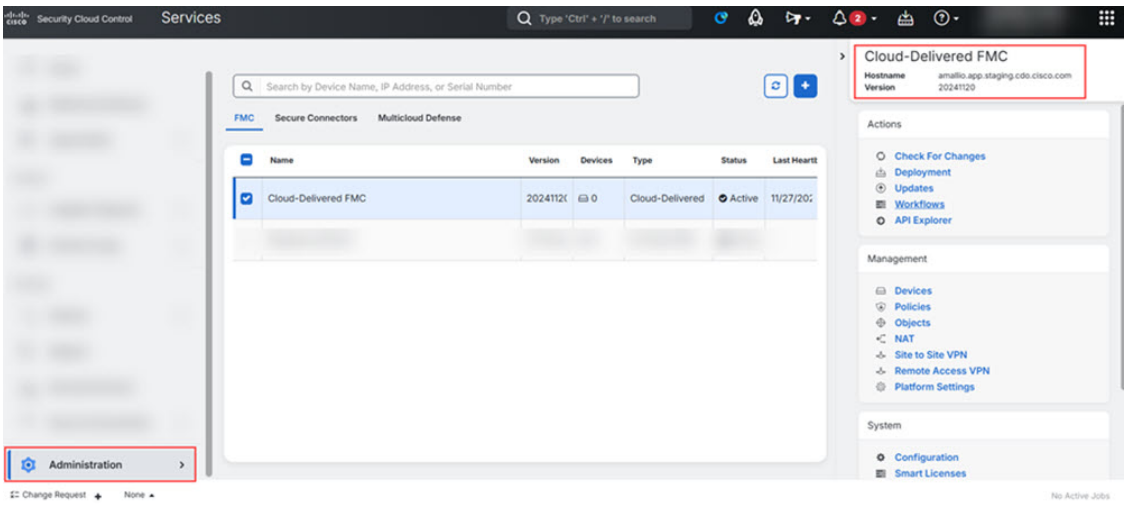
```
ping system 208.67.222.222
PING 208.67.222.222 (208.67.222.222) 56(84) bytes of data.
64 bytes from 208.67.222.222: icmp_seq=1 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=2 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=3 ttl=48 time=22.8 ms
64 bytes from 208.67.222.222: icmp_seq=4 ttl=48 time=22.6 ms
^C
--- 208.67.222.222 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 22.588/22.841/22.995/0.223 ms
```

The above example shows that the device can connect to the internet using the OpenDNS Server IP address. Also, the number of packets transmitted is the same as received, indicating that internet connectivity is available on the device. This shows that the device can reach the internet.

> **Note**
>
> If your results don't match, check the internet connection manually.

Check hostname resolution

1. Obtain the host name of the Cloud-Delivered Firewall Management Center.
   a. In the Security Cloud Control left pane, click **Administration** > **Integrations** > **Firewall Management Center**.
   b. Choose **Cloud-Delivered FMC** to see the Cloud-Delivered Firewall Management Center details on the right pane.
   c. In the **Hostname** field, copy only the hostname shown in this example image.



In the above figure, the highlighted text is the hostname (*Security Cloud Control-acc10.app.us.Security Cloud Control.cisco.com*) of the FMC to be copied.

2. Connect to the CLI of the device, either from the console port or using SSH.

3. Enter **ping system** *<hostname of the FMC>*.

```
ping system cdo-acc10.app.us.cdo.cisco.com
PING cdo-acc10.app.us.cdo.cisco.com (54.187.125.161) 56(84) bytes of data.
^C
--- cdo-acc10.app.us.cdo.cisco.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 64ms
```

In the above example, the hostname is resolved with the IP address, indicating your connection is successful. Ignore the " 100% packet loss" message shown in the response.

> **Note**
>
> If you can't connect to the host, you can rectify the DNS configuration in the CLI using **configure network DNS** *<address>*.

Use the troubleshoot feature for failed migrations

Configure troubleshooting for failed or partially successful migration jobs using the inbuilt troubleshoot feature on the migration jobs page.

Use the Troubleshoot feature to identify and resolve issues with failed or partially successful migrations by providing a summary and detailed progress of migration steps.

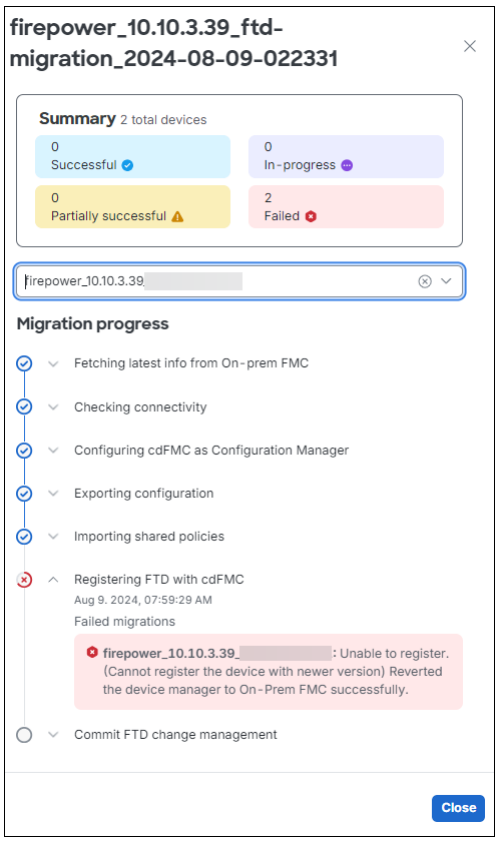
There might be a few instances where, owing to some issues, the migration fails or is not thoroughly successful. To help resolve issues around such failed or partially successful migrations, you can use the inbuilt **Troubleshoot** feature.

Procedure

1. On the migration jobs page, click the ... under the **Actions** column of a failed or a partially migrated job.
2. Click **Troubleshoot**.

   This opens up a sliding window that contains the following information:

   - A **Summary** containing additional details about the status of the migration.
   - A detailed **Migration progess** listing all the steps in the migration and also indicating the step at which the migration has failed.



3. Based on the stage at which the migration seems to have failed, refer Troubleshoot Firewall Threat Defense Migration to Cloud-Delivered Firewall Management Center for information on how to troubleshoot.

The troubleshoot feature provides detailed information about the migration status and identifies the specific step where the migration failed, enabling you to resolve the issue.

Troubleshoot Firewall Threat Defense migration failures

Learn how to troubleshoot Firewall Threat Defense migration failures to Security Cloud Control, including export, import, registration, connectivity, deployment, commit, rollback, VPN topology, analytics, and Secure Device Connector issues.

This section details how to troubleshoot specific errors that may occur when migrating Firewall Threat Defense devices to Cloud-Delivered Firewall Management Center.

Migration of Firewall Threat Defense cluster fails

The migration of a Firewall Threat Defense cluster to the Cloud-Delivered Firewall Management Center fails during the migration process. When the failure occurs, Cloud-Delivered Firewall Management Center automatically performs a rollback, returning device management to the original On-Premises Firewall Management Center to maintain configuration integrity and service continuity.

Cause :

The migration failure may occur due to temporary service latency, transient connectivity issues, or other temporary conditions that interrupt the migration process.

Workaround :

- **Retry migration** : Wait for some time and then initiate the migration again from the Secure Firewall Management Center .

- **Contact support** : If the migration continues to fail after multiple attempts, contact Cisco Technical Support and provide the relevant error messages and migration details to assist with troubleshooting.

Configuration export from On-Premises Firewall Management Center failed

Cause :

- Disk space is full or nearly full, preventing the export process from being completed.
- Concurrent operations such as device upgrade, upgrade revert, moving a device between domains, device import and export, device template import and export, or policy analysis are running in On-Premises Firewall Management Center .
- Connectivity issues exist between the On-Premises Firewall Management Center and Security Cloud Control .

Workaround:

1. Perform these actions according to your requirements:
   - Ensure that at least 10% of disk space is available to accommodate the creation of necessary export files.
   - Ensure that no parallel operations are running during the migration.
   - Ensure that the network connection between On-Premises Firewall Management Center and Security Cloud Control is stable and reliable.
2. Retry the migration.
3. If the issue persists, contact Cisco TAC.

Failed to initiate import in Security Cloud Control

Cause:

Import can fail if:

- Disk space is full or nearly full, preventing the import process from being completed.
- Concurrent operations such as device upgrade, upgrade revert, moving a device between domains, device import and export, device template import and export, or policy analysis are running in Cloud-Delivered Firewall Management Center .

Workaround:

1. Ensure that no other operations are running during import and retry migration.
2. If the issue persists, contact Cisco TAC.

Failed to retrieve the most recent device information from On-Premises Firewall Management Center

Cause:

- Network connectivity issues.
- DNS settings.
- Device synchronization issues.

Workaround:

1. Perform these actions according to your requirements:

- Ensure that the network connection between Security Cloud Control and On-Premises Firewall Management Center is stable.
- Ensure that DNS settings for resolving Firewall Management Center hostnames are correct.
- Ensure network access for Firewall Threat Defense devices through TCP ports 8305 and 443.
- Ensure outbound connectivity to port 443 to Security Cloud Control and Cloud-Delivered Firewall Management Center hosts.
- Ensure that the devices are synchronized without any pending changes.

2. Retry migration.
3. If the issue persists, contact Cisco TAC.

Failed to select Security Cloud Control as the manager for events and analytics

Cause:

Selected On-Premises Firewall Management Center for analytics during Firewall Threat Defense migration and committed it or the Security Cloud Control automatically committed it after the 14-day evaluation period.

Workaround:

1. Log in to the On-Premises Firewall Management Center and remove the Firewall Threat Defense device from the On-Premises Firewall Management Center .
2. Enable the Firewall Threat Defense device to send events to Security Analytics and Logging (SaaS) directly. For more information, see Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection on page 544 .
3. Verify if the SSE Connector is running in the Firewall Threat Defense device. To verify, access Firewall Threat Defense CLI and do the following:

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

4. Verify the connectivity between Firewall Threat Defense and the SSE portal. The following URLs need to be allowed as IPs can change:
   - api.apj.sse.itd.cisco.com (primary SSE cloud API endpoint)
   - est.sco.cisco.com (common endpoint across geographies)
   - mx.apj.sse.itd.cisco.com
   - dex.apj.sse.itd.cisco.com (for customer success services)
   - eventing-ingest.apj.sse.itd.cisco.com (for Cisco XDR and Security Cloud Control services)
   - registration.apj.sse.itd.cisco.com (enables Firewall Threat Defense device registration to the regional Cisco cloud)
5. access Firewall Threat Defense CLI and perform a CURL request to validate tenant details using the following command:

   ```
   root@firepower:/home/admin# curl localhost:8989/v1/contexts/default/tenant
   ```
6. Verify that the event logs are appearing in Security Cloud Control .

Failed to import configuration from On-Premises Firewall Management Center

Cause:

The On-Premises Firewall Management Center configuration may include policies or object configurations that are unsupported or are conflicting, leading to migration failure.

Workaround:

1. Check the On-Premises Firewall Management Center configuration for unsupported policies or object configurations to ensure compatibility.
2. Retry migration.
3. If the issue persists, contact Cisco TAC.

Failed to complete device discovery

Cause:

Conflicts or unhandled scenarios exist in the device configuration or within Security Cloud Control 's internal operations, such as incompatible settings or unsupported conditions that Security Cloud Control does not support.

Workaround:

1. Perform these actions according to your requirements:
   - Inspect the device configuration in On-Premises Firewall Management Center for incompatible settings or unsupported scenarios that Security Cloud Control does not support and make necessary updates.
   - Check system logs for errors and confirm that both the On-Premises Firewall Management Center and the device are functioning properly.
2. Retry migration.
3. If the issue persists, contact Cisco TAC.

Failed to connect the device to Security Cloud Control

Cause:

Possible causes include the device being powered off, network connectivity issues, or a firewall blocking the necessary ports.

Workaround:

1. Perform these actions according to your requirements:
   - Confirm that the device is powered on, and network connection is stable. Look for Firewall issues, blocked ports, and incorrect cabling.
   - Ensure that your device has the correct DNS server configuration for resolving Security Cloud Control hostnames.
2. Retry migration.
3. If the issue persists, contact Cisco TAC.

Failed to register the device, causing the manager to revert to On-Premises Firewall Management Center

Cause:

The device failed to register with Cloud-Delivered Firewall Management Center during migration, causing the system to revert the device manager to On-Premises Firewall Management Center . This may be because of connectivity issues.

Workaround:

1. Perform these actions according to your requirements:
   - Verify DNS settings for resolving Security Cloud Control hostnames.
   - Ensure that network access is enabled for TCP port 8305, allowing the Firewall Threat Defense devices to connect to the Cloud-Delivered Firewall Management Center .
   - Allow outbound HTTPS connections on Firewall Threat Defense devices to reach the Cloud-Delivered Firewall Management Center and upload configurations to Security Cloud Control .
2. Retry migration.
3. If the issue persists, contact Cisco TAC.

Failed to unregister the device due to an ongoing deployment

Cause:

Migration failed because a deployment is in progress on the device.

Workaround:

1. Perform these actions according to your requirements:
   - Wait for the ongoing deployment to finish.
   - Confirm that the device is stable, with no pending tasks.
2. Retry migration.
3. If the issue persists, contact Cisco TAC for support.

Report generation failed after successful FTD migration to Cloud-Delivered Firewall Management Center

Cause:

The report generation failure may be because of temporary system glitches.

Workaround:

- Generate the report after some time to overcome the temporary system issues that might have caused the initial failure.
- If the issue persists, contact Cisco TAC.

Failed to initiate FTD migration to Cloud-Delivered Firewall Management Center

Cause:

- Ongoing migration in the source manager.
- Unsupported device version.
- Incorrect DNS and network configuration.

Workaround:

1. Perform these actions according to your requirements:
   - Confirm that no other migration jobs are active in the same source manager.
   - Verify that the devices are on supported versions, have no pending changes to be deployed, and are active.

- Ensure that the DNS settings are correct, and network access is available to communicate with Cloud-Delivered Firewall Management Center .

2. If the issue persists, contact Cisco TAC.

Failed to deploy changes from Security Cloud Control

Cause:

Device migration to Cloud-Delivered Firewall Management Center failed during deployment.

Workaround:

1. Perform these actions according to your requirements:
   - Attempt the deployment again from the **Deployment** page on Cloud-Delivered Firewall Management Center .
   - Check for out-of-band changes, which are changes made directly in the device, and not through Security Cloud Control . If out-of-band changes exist, they may interfere with the deployment. Use Security Cloud Control 's **Check for changes** functionality to identify and address out-of-band changes.
   - Ensure that all the configurations are supported and do not conflict with the current device settings.
   - Verify that the device is onboarded and reachable by both the Security Cloud Control and management center, with the necessary internet access and communication capabilities.
2. If the issue persists, contact Cisco TAC.

Failed to commit FTD migration to Cloud-Delivered Firewall Management Center

Cause:

- The 14-day evaluation period has expired.
- Firewall Threat Defense devices have been reverted to or deleted from the On-Premises Firewall Management Center , preventing further actions.

Workaround:

1. Try committing again to address any transient network or device issues.
2. If the issue persists, contact Cisco TAC.

Failed to retain device on On-Premises Firewall Management Center for Analytics

Cause:

If your source manager is an On-Premises Firewall Management Center 1000/2500/4500, it cannot support retaining for Analytics because of the limited resources.

Workaround:

1. Ensure that the **Retain on On-Prem FMC for Analytics** option is selected during the migration process.
2. If the issue persists, contact Cisco TAC.

Failed to revert the device manager to On-Premises Firewall Management Center

Cause:

- The device cannot be reverted if the 14-day evaluation period has expired.

- Firewall Threat Defense devices have been reverted to or deleted from the On-Premises Firewall Management Center , preventing further actions.

Workaround:

1. Perform these actions according to your requirements:
   - Try committing the changes again to address the temporary server or network issues.
   - If changes have occurred in the high availability configuration after migration, reset the devices to their original migration state before attempting to commit.
2. If the issue persists, contact Cisco TAC.

Failed to configure Security Cloud Control as the configuration manager

Cause:

The device already has a configuration manager.

Workaround:

1. If another configuration manager is present, remove it manually and retry the migration.
2. If the issue persists, contact Cisco TAC.

Failed to commit migration; the device is ineligible

Cause:

- The device has pending changes that have to be deployed.
- The device to be migrated is part of FTD high availability (HA), but the current state is invalid, for example, it is in Active/Active state.
- The device to be migrated is connected in Analytics-only mode.
- Cluster migration is supported only for FTDs version 7.4 and above.
- Migration for chassis and MI FTDs on models 3100/4200 is currently not supported.

Workaround:

1. Perform these actions according to your requirements:
   - Verify that the device is up to date with On-Premises Firewall Management Center , then retry migration.
   - Ensure all pending changes on the devices are deployed.
   - Confirm that the Firewall Threat Defense device is in a valid state, such as Active/Standby. If the status isn't correctly reflected in On-Premises Firewall Management Center , use the **Force refresh node status** option on the device listing page to update the correct status on management center.
2. If the issue persists, contact Cisco TAC.

Failed to import site-to-site VPN policies from On-Premises Firewall Management Center

Cause:

The failure may be due to various factors, such as VPN policy configuration or network connectivity issues.

Workaround:

1. Perform these actions according to your requirements:

- Verify your site-to-site VPN policies in On-Premises Firewall Management Center to ensure there are no configuration errors. If object overrides are used within network objects, manually add these overrides to Security Cloud Control after migration.
- Ensure that both the On-Premises Firewall Management Center and the targeted device have stable and reliable network connections to Security Cloud Control .
- If the authentication type is set as **Pre-shared Automatic Key** in On-Premises Firewall Management Center , Security Cloud Control generates a new pre-shared key for the VPN post-migration deployment without disrupting existing tunnels.

2. Retry migration.
3. If the issue persists, contact Cisco TAC.

Failed to migrate as all devices within the topology need to be migrated simultaneously

Cause:

Migrating multiple devices, particularly those within the same network topology, requires synchronizing their migrations to avoid inconsistencies and potential errors. All devices should be migrated within the same timeframe.

Workaround:

1. Perform these actions according to your requirements:
   - Devices registered for Analytics -only with the On-Premises Firewall Management Center or those with pending changes are not eligible for migration.
   - When selecting a device associated with a site-to-site VPN topology, Security Cloud Control automatically selects peer devices from the same or different topology, as all devices in the topology must be migrated together for success. Extranet devices, if any, are not listed by the wizard.
   - The **S2S VPN Topology** column shows the number of site-to-site VPN topologies a device is part of. Click the topology link to view the topologies and devices migrating with the selected device. This field does not apply to devices outside the site-to-site VPN topology.
   - A high-availability pair is shown as a single node. Select this node to include both active and standby devices in the migration.
2. If the issue persists, contact Cisco TAC.

HTTP status code 201 (created) found in On-Premises Firewall Management Center response

Cause:

The Secure Device Connector (SDC) version is not compatible.

Workaround:

1. Ensure that the SDC is upgraded to version **202205191350** or later.
   - In the left pane, click **Administration** > **Integrations** > **Secure Connectors Administration** > **Secure Connectors** .
   - Click the SDC to view the existing version in the **Details** pane on the right.
   - Update your Secure Device Connector .

21 Configure Cloud-Delivered Firewall Management Center-Managed Secure Firewall Threat Defense

Topics:

- Security Cloud Control Firewall Management Integrations Page
- Navigate to the Cloud-Delivered Firewall Management Center in your Security Cloud Control Tenant
- Enable Cloud-Delivered Firewall Management Center

Learn how to manage and configure Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense devices.

This chapter provides information on how to manage the Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense onboarded to Security Cloud Control.

Security Cloud Control Firewall Management Integrations Page

Outlines how to use the Integrations page to view and manage infrastructure, onboard and configure Firewall Management Centers and devices, perform actions such as deployment and event monitoring, and access management, system, and connector settings across multiple tabs.

The **Integrations** page provides a comprehensive view of your managed infrastructure within Security Cloud Control Firewall Management:

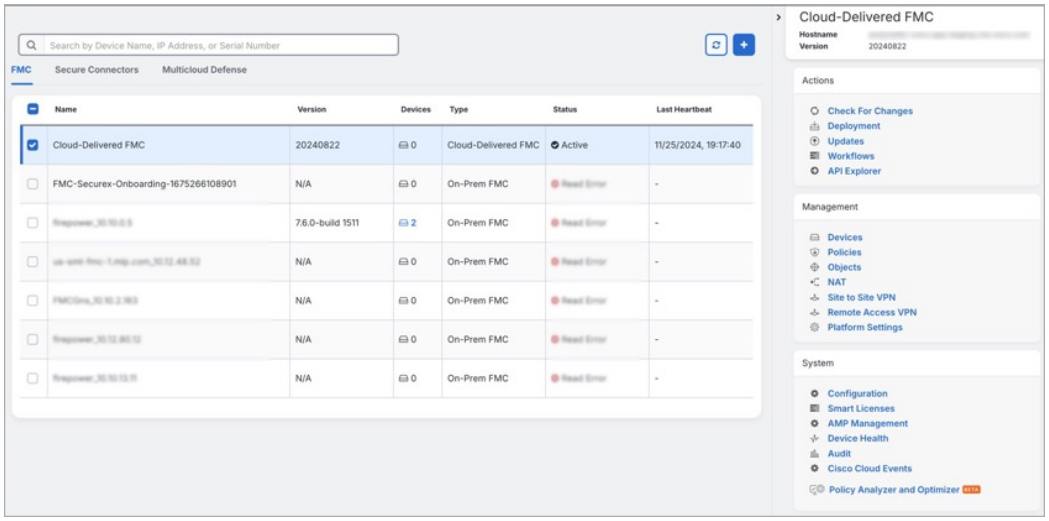
- **FMC** tab:
  - View the Cloud-Delivered Firewall Management Center that is linked to the Security Cloud Control Firewall Management account. Refer to Request a Cloud-delivered Firewall Management Center for your Security Cloud Control tenant .
  - View which On-Premises Firewall Management Centers are onboarded to Security Cloud Control Firewall Management. Devices managed by these On-Premises Firewall Management Centers appear in **Security Devices**. Refer to Managing On-Prem Firewall Management Center with Security Cloud Control.
  - Lists the **Secure Device Connector** and **Secure Event Connector** available under the **Secure Connectors**. Refer to Secure Device Connector and Secure Event Connectors.

Security Cloud Control. page. The **Integrations** page also lists tab.

Click the **FMC** tab, then click **Onboard FMC** ( ) icon to onboard an On-Premises Firewall Management Center. In the right pane, perform device actions as needed. Refer to Onboard an On-Prem Firewall Management Center.

View device information, including version, device count, device type, and synchronization status. Click the managed devices icon to go to the **Security Devices** page. Devices managed by the selected On-Premises Firewall Management Center are filtered and displayed. On the **Integrations** page, select multiple On-Premises Firewall Management Center to perform actions on several management centers at once. Deselect the Cloud-Delivered Firewall Management Center before selecting other On-Premises Firewall Management Center. To add a new secure connector or perform actions on existing secure connectors, choose the **Secure Connectors** tab and click .

In the left pane, click **Administration** > **Firewall Management Center**.



For your Cloud-Delivered Firewall Management Center, the Integrations page displays this information:

- If you do not have a Cloud-Delivered Firewall Management Center deployed on your tenant, click **Enable Cloud-Delivered FMC**. Refer to Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control Tenant for more information.

- The number of Secure Firewall Threat Defense devices deployed on the Cloud-Delivered Firewall Management Center.
- Status of the connection between Security Cloud Control and the Cloud-Delivered Firewall Management Center page.
- The last heartbeat of the Cloud-Delivered Firewall Management Center. This time shows when the Cloud-Delivered Firewall Management Center's status and device count last synchronized with the table on this page..
- The hostname of the selected Cloud-Delivered Firewall Management Center.

Choose **Cloud-Delivered FMC** and using the links in the **Actions** , **Management**, or **Settings** pane, you open the Cloud-Delivered Firewall Management Center user interface to perform the configuration tasks that are associated with the link you clicked.

Actions:

- **Check For Changes**: The Device Count and Status information in the table is updated with the information available the last time this page and the Cloud-Delivered Firewall Management Center were synchronized. Synchronization happens every 10 minutes.
- **Deployment**: Takes you to the device configuration deployment page on Cloud-Delivered Firewall Management Center. Refer to Deploy Configuration Changes.
- **Workflows**: Takes you to the **Workflows** page to monitor every process that Security Cloud Control runs when communicating with devices. Refer to Workflows page.
- **API Explorer**: Takes you to the page that lists the Cloud-Delivered Firewall Management Center REST APIs. Refer to Secure Firewall Management Center REST API Guide .
- **Unified Events**: Takes you to the **Unified Events** page on the Cloud-Delivered Firewall Management Center portal, which provides a single-screen view of various firewall events, including connection, intrusion, file, malware, and security-related connection events. For more information, refer to Unified Events .

> **Note**
>
> The Unified Events feature requires activation. If you have not yet activated this feature, contact your Cisco sales representative to enable it.

Management:

- **Devices**: Takes you to the Firewall Threat Defense device listing page on the Cloud-Delivered Firewall Management Center portal. Refer to Configure Devices.
- **Policies**: Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to edit system-provided access control policies and create custom access control policies. Refer to Manage Access Control Policies.
- **Objects**: Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to manage reusable objects. Refer to Object Management.
- **NAT**: Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to configure Network Address Translation policies on the Firewall Threat Defense devices. Refer to Manage NAT policies.
- **Site to Site VPN**: Takes you to the site-to-site VPN dashboard page on the Cloud-Delivered Firewall Management Center portal to configure site-to-site VPN policy between two sites. Refer to Site-to-Site VPNs.
- **Remote Access VPN**: Takes you to the remote access VPN dashboard page on the Cloud-Delivered Firewall Management Center portal to configure a remote access VPN configuration. Refer to Remote Access VPN.

- **Platform Settings**: Takes you to the platform settings page on the Cloud-Delivered Firewall Management Center portal to configure a range of unrelated features whose values you might want to share among several devices. Refer to Platform Settings.

System:

- **Configuration**: Takes you to the system configuration settings page on the Cloud-Delivered Firewall Management Center portal to configure system configuration settings. Refer to System Configuration .
- **Smart Licenses**: Takes you to the smart licenses page on the Cloud-Delivered Firewall Management Center portal to assign licenses to devices. Refer to Assign Licenses to Devices.
- **AMP Management**: Takes you to the AMP management page on the Cloud-Delivered Firewall Management Center portal that supplies data the system uses to detect and block malware on your network. Refer to Cloud Connections for Malware Protection.
- **Device Health**: Takes you to the health monitoring page on the Cloud-Delivered Firewall Management Center portal, which tracks various health indicators to ensure the hardware and software in the system are working correctly. Refer to About Health Monitoring.
- **Audit**: Takes you to the audit log page on the Cloud-Delivered Firewall Management Center portal to show the generated audit record for each user interaction with the web interface.
- **Cisco Cloud Events**: Takes you to the configure Cisco Cloud events page on the Security Cloud Control portal to configure Cloud-Delivered Firewall Management Center to send events directly to SAL (SaaS). Refer to Send Events to SAL (SaaS).

After you open the Cloud-Delivered Firewall Management Center page, click the blue question mark button and select **Page-level Help** for more information.

Support to open Security Cloud Control and Cloud-Delivered Firewall Management Center applications in separate tabs

As you configure Firewall Threat Defense devices or objects in Cloud-Delivered Firewall Management Center , you can open the appropriate configuration pages in additional browser tabs to work simultaneously in the Security Cloud Control and the Cloud-Delivered Firewall Management Center portals without logging off.

For example, you can create an object on Cloud-Delivered Firewall Management Center and simultaneously monitor event logs on Security Cloud Control that are generated from the security policies.

This feature is available for all Security Cloud Control links that navigate to the Cloud-Delivered Firewall Management Center portal. To open the Cloud-Delivered Firewall Management Center portal in a new tab:

On the Security Cloud Control portal, press and hold the Ctrl (Windows) or Command (Mac) button, then click the corresponding link.

> **Note**
>
> A single click opens the Cloud-Delivered Firewall Management Center page in the same tab.

Here are some examples of opening the Cloud-Delivered Firewall Management Center portal page in a new tab:

- Choose **Administration** > **Firewall Management Center** and select **Cloud-Delivered FMC**. In the right pane, press and hold the Ctrl (Windows) or Command (Mac) button, and then click the page that you want to access.
- Choose **Objects** > **Other FTD Objects**.
- Click the search icon on the Security Cloud Control page and enter your search terms in the search field.

From the search result, press and hold the Ctrl (Windows) or Command (Mac) button, and then click the arrow icon.

- Choose **Dashboard** > **Quick Actions**. Press and hold the Ctrl (Windows) or Command (Mac) button, and then click **Manage FTD Policies** or **Manage FTD Objects**.

> **Note**
>
> If you switch to a new Security Cloud Control tenant, the Cloud-Delivered Firewall Management Center portal open in another tab logs out automatically.

Navigate to the Cloud-Delivered Firewall Management Center in your Security Cloud Control Tenant

Configure access to Cloud-Delivered Firewall Management Center from a Security Cloud Control tenant and use available service actions.

This task enables you to access the Cloud-Delivered Firewall Management Center from your Security Cloud Control tenant to perform firewall management actions.

The Cloud-Delivered Firewall Management Center is accessible through the Services page in your Security Cloud Control tenant, where you can access management functions, settings, and other actions.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Administration** > **Integrations** > **Firewall Management Center** to view the **Services** page.

   The **Services** page displays the information about the Cloud-Delivered Firewall Management Center provisioned for the Security Cloud Control tenant.
3. Choose **Cloud-Delivered FMC** and click the links in the **Actions**, **Management**, or **Settings** pane to navigate to Cloud-Delivered Firewall Management Center to perform various actions.

   See Security Cloud Control Firewall Management Integrations Page on page 488.

   Once in the Cloud-Delivered Firewall Management Center, click the blue question mark button and select **Page-level Help** to learn more about the page you are on and further action you can take.

You have successfully navigated to the Cloud-Delivered Firewall Management Center and can now access management functions, settings, and perform firewall management actions.

Enable Cloud-Delivered Firewall Management Center

Configure Cloud-Delivered Firewall Management Center for a Security Cloud Control tenant to manage your Secure Firewall Threat Defense devices.

Enable Cloud-Delivered Firewall Management Center to manage your Secure Firewall Threat Defense devices through Security Cloud Control.

If you want to manage your Secure Firewall Threat Defense devices, you can enable the Cloud-Delivered Firewall Management Center on your tenant. You need to have an admin or a super admin user role to perform this task.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. From the Security Cloud Control menu, click **Administration** > **Integrations** > **Firewall Management Center** and click **Enable Cloud-Delivered FMC**.

   Security Cloud Control starts provisioning a Cloud-Delivered Firewall Management Center instance in the background; it typically takes 15 to 30 minutes for this to be complete. You can track the provisioning progress on the **Status** column of **Cloud-Delivered FMC**.

   After the provisioning is complete, the status changes to **Active**. In addition, you get a **Cloud-Delivered Firewall Management Center is Ready** notification on the Security Cloud Control notifications panel and on the applications on which you have configured incoming webhooks. See Notification Settings for more information.

   > **Note**
   >
   > After you receive the **Cloud-Delivered Firewall Management Center is Ready** notification, ensure that you log out of and log in back to your tenant once, to see the **Cloud-Delivered FMC** right pane options, such as **Actions**, **Management**, and **System**.

   What to do next:

   a. Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager (CSSM) to activate smart license. For detailed steps, refer to Register the Cloud-Delivered Firewall Management Center with the Smart Software Manager.

   b. Onboard your Firewall Threat Defense devices to the Cloud-Delivered Firewall Management Center and manage them.

After the provisioning is complete, the status changes to **Active** and you receive readiness notifications. You can then proceed to register with the Smart Software Manager and onboard your devices.

22 Introduction to AgenticOps insights

Topics:

- AgenticOps insights
- Capacity and traffic insights
- About policy change impact insights
- Best practices and recommendations
- Feature adoption insights
- Software upgrade insights
- Application insights
- Compliance insights
- Insight preferences
- Frequently asked questions about AgenticOps
- Additional resources

AgenticOps brings AI-driven intelligence to firewall management, helping you proactively identify issues, optimize configurations, plan software upgrades, analyze policy health, track feature adoption, and assess capacity requirements. Use AgenticOps capabilities to gain operational visibility, prioritize remediation efforts, and improve the performance, security, and reliability of your firewall deployment.

AgenticOps insights

Explains how AgenticOps leverages artificial intelligence and machine learning to provide actionable operational guidance for improving security posture, optimizing performance, planning upgrades, and making informed operational decisions.

AgenticOps insights is a firewall management solution that

- leverages artificial intelligence (AI) and machine learning (ML) to streamline and enhance firewall management and network security
- addresses the complexity of managing firewalls as organizations expand and the threat landscape evolves, and
- provides actionable operational guidance based on data collected from your environment to improve security posture, optimize performance, plan upgrades, and make informed operational decisions.

Supported devices and management platforms

Note

Currently, AgenticOps supports:

- Firewall Threat Defense devices that are managed by Cloud-Delivered Firewall Management Center.
- Firewall Threat Defense devices managed by On-Premises Firewall Management Center integrated with Cisco Security Cloud.

  For information on supported versions, see AgenticOps Support for On-Premises Firewall Management Centers.

Key functionalities include:

- **Traffic and capacity monitoring**: Monitors network traffic and system capacity in real-time, and detects anomalies such as elephant flows. This ensures resources are optimized for peak performance.
- **Policy anomaly detection**: Analyzes firewall policies and detects misconfigurations or anomalies before they impact performance or security.
- **Feature adoption insights and best practice recommendations**: Provides insights into the level of feature adoption and suggests best practices to optimize security configurations.
- **Predictive forecasting for network issues**: Predicts potential future network issues, allowing you to address them proactively and minimize downtime.
- **Operational insights**: Evaluates device readiness for software upgrades, suggests compatible versions, and helps plan upgrades to maintain consistency, stability, and compliance across deployments.
- **Critical alerts**: Filters and prioritizes the most urgent security events, helping you focus on critical issues.

Key features include:

- **Policy Analyzer and Optimizer**: Analyzes security policies, detects anomalies, and provides recommendations on remediations that can be performed to optimize the policies, thereby improving the firewall performance.
- **Policy Change Impact Analyzer**: Provides visibility into pending access control policy rule changes across devices, analyzes affected rules and traffic segments, and assesses potential traffic impacts to help you make informed deployment decisions.

- **Best Practices and Recommendations**: Generates detailed assessment reports that highlight failed checks against Cisco Secure Firewall best practices and provides actionable recommendations to resolve issues, ensuring optimal firewall performance.
- **Feature Adoption**: Provides insights into the features that are adopted and the percentage of adoption to modify the usage pattern and achieve optimal security. Analyze the adoption rate of different features to improve usage patterns and enhance security measures.
- **Software Upgrade Planner**: Provides upgrade suggestions for your devices through a centralized dashboard. The dashboard displays the current and suggested versions and details about security vulnerabilities and bug fixes.
- **Application Outage Insights**: Detects application outages that may impact users, sites, and business-critical services. The feature correlates outage telemetry, operational insights, and affected resources to help you reduce troubleshooting time.
- **Capacity and Trend Analyzer**: Analyzes firewall capacity utilization and traffic trends to identify abnormal spikes, sustained resource consumption, and emerging performance risks. The feature provides operational visibility into throughput, connection behavior, and traffic patterns to optimize firewall performance.
- **Compliance Posture**: Assess firewall compliance posture against supported security standards. The feature evaluates firewall configurations, identifies compliance gaps, and provides actionable remediation insights to improve security posture
- **Configuration Settings**: Provides the ability to configure thresholds for AgenticOps features and enable or disable insight preferences. You can customize these settings to suit your specific needs.

AgenticOps licensing requirements

Lists the licensing requirements for AgenticOps and how to access AI-driven insights, recommendations, and operational guidance available with eligible firewall licenses.

If you have licenses for the Secure Firewall Management Center, you can access AgenticOps by enabling AgenticOps Insights in your organization. The initial version of AgenticOps is included as part of your firewall license and is granted on a per-device basis.

Requirements: Prerequisites to use AgenticOps

Outlines the prerequisites for using AgenticOps, including licensing, user permissions, and device onboarding requirements.

Ensure that these prerequisites are met before using AgenticOps:

- Ensure that AgenticOps Insights is enabled for your Security Cloud Control organization and that Cloud-Delivered Firewall Management Center is provisioned.
- You must have **Super Admin** or **Admin** user roles to opt in and opt out of AgenticOps Insights for your organization.
- If you are using an On-Premises Firewall Management Center, ensure it is integrated with Cisco Security Cloud before onboarding AgenticOps. For information on supported on-prem Firewall Management Center software versions, see AgenticOps Support for On-Premises Firewall Management Center.
- Configure the required thresholds and preferences for supported AgenticOps features.

Meeting these prerequisites ensures that AgenticOps can collect the data needed to generate insights and recommendations.

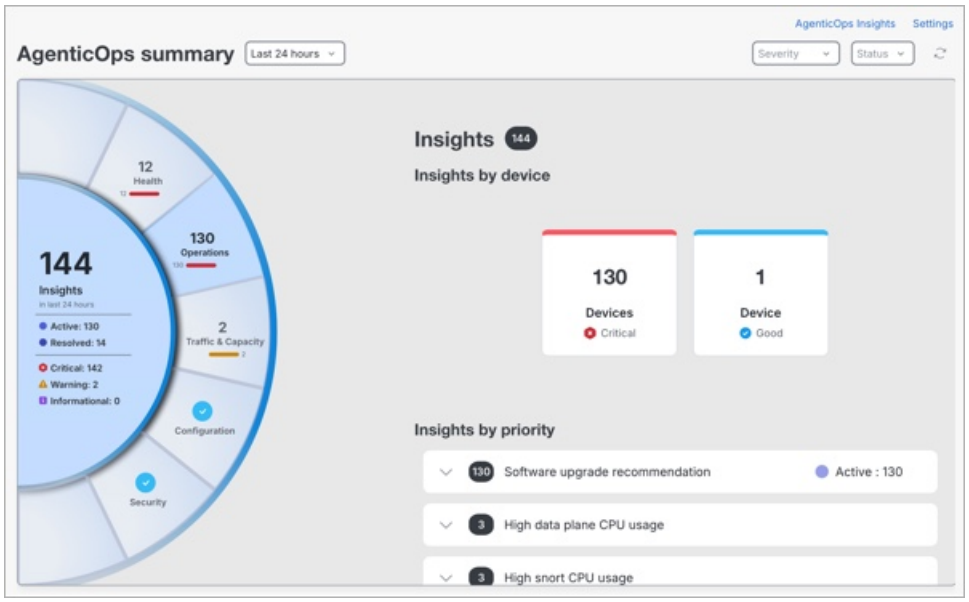
View summary dashboard

Provides access to the AgenticOps summary dashboard for insights, recommendations, and operational metrics in a single location. Use dashboard widgets to monitor trends, identify risks, and prioritize actions across your environment.

The **Summary** dashboard provides a consolidated view of all insights across your environment. It enables identification of areas that require attention and gives you the ability to drill down for operational, configuration, and security analysis. You can filter insights by time range, severity, and status.

AgenticOps summary dashboard

Figure 6: AgenticOps summary



- **Insights visualization panel**: Visual representation of your insights, helping you quickly understand overall system posture and where to prioritize action.
  - The inner ring summarizes insights by status and severity.
  - The outer ring represents insight categories. Selecting a category displays related details.

    The insight categories include:

    - **Operations**: Focuses on insights that help maintain the operational health and software lifecycle readiness of your devices. This includes upgrade recommendations for your Firewall Threat Defense devices and End-of-Life notifications.
    - **Configuration**: Focuses on insights that evaluate your network policies, configurations, and adherence to Cisco Firewall best practices. This includes identifying misconfigurations, policy anomalies, and deviations that may impact performance, security, or compliance.
    - **Security**: Focuses on insights that detect suspicious, risky, or anomalous activities within your environment. These insights highlight behaviors that may indicate compromised accounts and malicious intent.

  Select any insight category to view the insights associated with it.
- **Insights by device**: Click on a device to view insights.
- **Insights by priority**: Expand the section to view all devices with related insights.
- Use the icons at the top right of the page for additional actions:
  - **AgenticOps Insights**: Navigate to the view of all AgenticOps insights.
  - **Settings**: Navigate to configure preferences and thresholds for insights.

Confidence levels in AgenticOps

A confidence level represents the reliability of a forecast-based insight generated by AgenticOps. It indicates how accurately AgenticOps can predict future behavior for a given condition, helping you decide when immediate action is required versus when monitoring is sufficient.

Applicable forecast-based insight types

Confidence levels are displayed for these forecast-based AgenticOps insights:

- Remote Access VPN – Maximum Sessions Nearing Limit
- CPU (LINA) Utilization Forecast Breach
- CPU (Snort) Utilization Forecast Breach
- Memory (LINA) Utilization Forecast Breach
- Memory (Snort) Utilization Forecast Breach

How AgenticOps determines confidence levels ?

For forecast-based insights, such as **High Snort Memory Usage**, **High Snort CPU Usage**, and **RA VPN Forecast**, AgenticOpsevaluates how accurately its machine learning models can predict future behavior using historical patterns and current trends.

Based on this forecast accuracy, each insight is automatically assigned a confidence level. Insights that do not meet a minimum reliability threshold are not generated.

- **High**
  - The forecast is highly reliable and strongly supported by historical data.
  - Recommended action: Prioritize the investigation and take proactive corrective measures.
- **Medium**
  - The forecast is reliable but may show moderate variability.
  - Indicates a strong trend that is likely to continue.
  - Recommended action: Review the insight and plan mitigation.
- **Low**
  - The forecast indicates a possible emerging condition.
  - Limited data or higher variability reduces certainty.
  - Recommended action: Monitor closely and validate with additional operational context.
- **Very low**
  - The forecast signal is weak or in an early stage.
  - Higher uncertainty due to insufficient or inconsistent data.
  - Recommended action: Observe trends. No immediate action is required.

Insight statuses and transitions

This table outlines the possible insight statuses, their descriptions, transitions, and examples.

Status	Description	Transition	Triggered by	Example
Active	• An issue is detected and ongoing. • This is the initial state when an issue is identified.	–	System	Upgrade options suggested for Firewall Threat Defense devices.
Resolved	• AgenticOps automatically marks an active insight as resolved when the issue no longer exists. • Historical details are available for reference.	**Active** to **Resolved**: After you fix the issue and the system confirms it in the next check.	• Automatically by the system for performance issues. • By the user (with system confirmation) for configuration issues.	Overlapping firewall rules corrected by the user.
Not Applicable (N/A)	• The issue existed earlier but it is no longer present. • No historical data is available for reference.	**Active** to **Not Applicable**	System	• When an Access Control policy is deleted, the corresponding insight is marked as NA. • When a device is deleted from FMC inventory, all insights for that device are marked as NA. • When earlier Policy Analyzer and Optimizer results showed issues but a recheck finds zero issues and no details to display, the insight is marked as NA.

View AgenticOps insights

Configure summary insights to monitor key findings across AgenticOps capabilities from a single dashboard. Review insights by category, priority, and impacted resources to identify issues, assess their impact, and prioritize remediation efforts.

View AI-driven alerts that help you detect, prioritize, and resolve issues across your environment by accessing comprehensive insights from a centralized dashboard.

The **AgenticOps Insights** page provides AI-driven alerts that help you detect, prioritize, and resolve issues across your environment.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Summary**.
3. On the **Summary** page, click **AgenticOps Insights** at the top right.

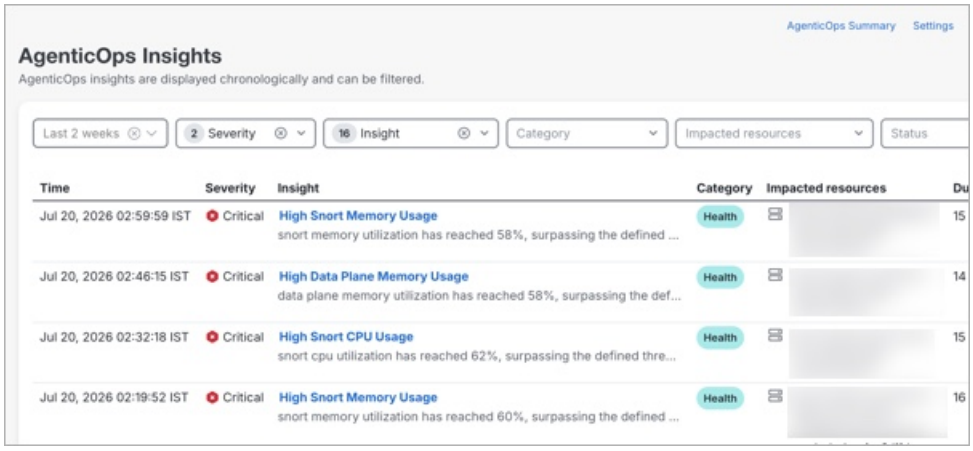
   Insights are displayed in chronological order and can be filtered by the following:

   - **Time**: Select a time range to view insights generated within that window
   - **Severity**: Select a severity level, such as **Critical**, **Warning**, or **Informational**.
   - **Insight**: Select a type of insight to view.
   - **Category**: Select a category such as **Configuration**, **Health**, **Operations**, and so on.
   - **Impacted Resources**: Select a device or service affected by the insight.
   - **Status**: Select a status, such as **Active**, **Not applicable**, or **Resolved** stauses.

   Clicking **Reset all** clears all applied filters and returns to the default view.
4. In the insights table, click an **Insight** or **Impacted Resource** to view additional details.

   The details include a summary of the issue, the probable cause, related metrics, and recommended remediation or upgrade actions to ensure optimal performance.
5. Use the icons at the top right of the page for additional actions:

   Figure 7: AgenticOps insights



   - **AgenticOps Summary**: Navigate to the view the high-level summary of all insights.
   - **Settings**: Navigate to configure preferences for AgenticOps features.

You can now view and filter AI-driven insights to identify issues, assess their impact, and prioritize remediation efforts across your environment.

AgenticOps for On-Premises Firewall Management Center

Learn about the AgenticOps features supported for On-Premises Firewall Management Center, the supported software versions, and deployment requirements.

AgenticOps supports Firewall Threat Defense devices managed by an On-Premises Firewall Management Center that is integrated with Cisco Security Cloud and onboarded to AgenticOps. Support for individual AgenticOps features depends on the On-Premises Firewall Management Center software version.

> **Note**
>
> Currently, On-Premises Firewall Management Center registered through Secure Device Connector (SDC) are not supported.

AgenticOps feature	Supported On-Premises Firewall Management Center versions
Capacity and Trend Analyzer	10.0.0+
Policy Analyzer and Optimizer	7.4.0+
Software Upgrade Planner	7.4.0+
Best Practices and Recommendations	10.0.0+
Feature Adoption	10.0.0+
Application Insights (ThousandEyes)	7.6.0+
User Risks Insights	10.0.0+
Policy Analyzer and Optimizer - Network Address Translation	7.6 +
Policy Analyzer and Optimizer - Access Control Policy	7.2.0 +

After onboarding, supported On-Premises Firewall Management Center- managed devices are available throughout AgenticOps, including the Summary page, AgenticOps Insights, and supported feature dashboards.

Capacity and traffic insights

Describes visibility into resource utilization and capacity trends across your environment to identify potential constraints, track growth patterns, and support proactive planning and operational decision-making.

Capacity and traffic insights are analytical capabilities that

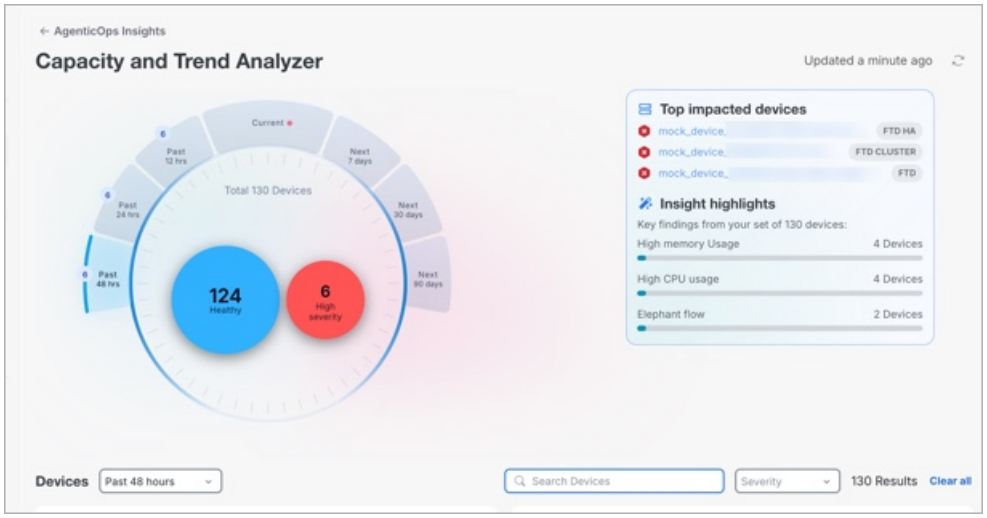
- provide visibility into resource utilization across devices and highlight emerging risks
- predict when risks may lead to performance issues by combining historical trends with predictive insights
- enable proactive capacity planning by identifying future risks before they impact system performance, and
- anticipate problems and support action before they affect users.

How AgenticOps generates capacity insights

Forecasted insights predict future resource utilization based on historical trends and patterns. AgenticOps continuously analyzes historical data and runs periodic forecasts to identify when resources are likely to reach configured thresholds.

AgenticOps uses multiple analytical approaches to identify and predict issues. AgenticOps runs forecasts on a recurring weekly basis to identify potential capacity risks in advance, including:

- Detect threshold breaches: Identifies when CPU or memory usage exceeds configured limits in real time.
- Detect anomalies: Identifies unusual deviations from expected behavior based on historical patterns.
- Detect elephant flows: Detects large traffic flows that can impact system performance and resource utilization.
- Detect Remote Access VPN session limits: Detects or predicts when VPN session capacity limits are reached.
- Forecast capacity risks: Predicts future threshold breaches using historical trends, enabling proactive planning.



Note

- The accuracy of insights depends on the availability and quality of historical data. Limited or inconsistent data may delay or reduce insight accuracy.
- In environments with limited activity or newly onboarded devices, insights and forecasts may take time to appear.

This table shows key features of Capacity and Trend Analyzer:

Table 23: Key features of capacity and trend analyzer

Feature	Description
Capacity insights dashboard	Provides a fleet-level view of device capacity status, displaying past, current, and predicted capacity insights across all monitored devices.
Capacity insights	Generates insights based on CPU, memory, connection, throughput, and VPN session activity to highlight potential resource constraints.

Feature	Description
Device capacity analysis	Displays detailed capacity insights for an individual device, including resource metrics, AI-generated summaries, and forecast information.
Predictive capacity forecasting	Uses historical resource utilization data to predict future usage trends and identify potential capacity risks before thresholds are reached.
Timeline-based analysis	Allows you to analyze capacity insights across different time windows, including past events, current conditions, and predicted future risks.
Device health indicators	Displays device health status based on active and predicted capacity insights, helping you quickly identify devices that require attention.

The Capacity and Trend Analyzer supports:

- Secure Firewall Threat Defense devices
- Secure Firewall Threat Defense High Availability (HA) deployments
- Secure Firewall Threat Defense cluster deployments

Note

For High Availability (HA) and cluster deployments:

- Capacity analysis runs at the system level.
- Individual member devices are not displayed separately.

Analyze capacity trends and forecast resource usage

Configure Capacity and Trend Analyzer to evaluate resource utilization trends across your environment and analyze historical data to identify growth patterns.

This task enables you to analyze historical data, identify growth patterns, and understand how resource consumption changes over time to support capacity planning and operational decision-making.

Use Capacity and Trend Analyzer to evaluate resource utilization trends across your environment. The analyzer helps you move from reactive troubleshooting to proactive capacity management by enabling you to identify risks early and take informed action.

Before you begin

Ensure that **Capacity and Trend Analyzer** is enabled under **Settings**. For more information, see enable Capacity and Trend Analyzer.

Follow these steps to analyze capacity trends and forecast resource usage:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Capacity and Trend Analyzer**.

   This opens the dashboard where you can view capacity insights across your environment.
3. Use the circular timeline to select a timeframe, such as **Current**, **Past (12 hours**, **24 hours**, or **48 hours)**, **Next (7 days**, **30 days**, or **90 days)**.
   - **Current** shows active capacity insights.
   - **Past 12, 24, or 48 hours** show insights from the selected past period.
   - **Next 7, 30, or 90 days** show predicted capacity risks.

   The timeline also displays the total number of devices and their health status, such as **Healthy**, **Needs attention**, and **High severity**.
4. Review the summary panel.
   - Use the **Top impacted devices** section to identify devices with the most critical capacity issues.
   - Use the **Insight highlights** section to understand the most common capacity risks across your organization.
5. Review device insights in the **Devices** section.
   - Search for a device or use filters such as timeframe and severity to locate devices that require attention.
   - Each device displays a summary of detected or predicted issues, along with associated insight tags.
6. Select a device to view detailed insights.

   This view provides summaries and detailed insights for the selected device.
7. On the device details page, review the **AI summary**, **Resolved insights**, **Active insights**, and **Future insights**.
8. In the **Device metrics** section, select a metric to view historical trends and forecast data.
9. Use the insights and forecasts to determine appropriate actions, such as redistributing traffic, scaling resources, or planning capacity upgrades. After taking action, use the **Current** view to monitor whether the issue has been resolved.

   The **Capacity and Trend Analyzer** helps you move from reactive troubleshooting to proactive capacity management by enabling you to identify risks early and take informed action.

You can now analyze capacity trends and forecast resource usage across your environment. The Capacity and Trend Analyzer provides insights into historical data, growth patterns, and resource consumption changes to support proactive capacity planning and operational decision-making.

About policy change impact insights

Review the potential impact of pending access control policy rule changes across devices before deployment.

Changes to an access control policy can affect network traffic in unexpected ways. A modification that appears minor, such as updating a network object, expanding a rule, or changing rule conditions, can alter how traffic is evaluated by other rules in the policy. These effects are often difficult to identify before deployment.

Policy Change Impact Analyzer helps you review the potential impact of pending access control policy rule changes across devices before deployment. The analysis helps you identify affected rules, impacted connections, and traffic

segments so that you can better understand the consequences of a change before deploying it. The **Policy Change Impact Analyzer** evaluates proposed policy changes and provides visibility into:

- The overall analysis result for each device
- Affected devices and rules
- Impacted traffic segments
- Historical connections affected by a changed rule, when traffic data is available
- Rule-level inferred impact
- AI-generated summaries that explain the potential effect of a rule change

Limitations and considerations

- Currently, **Policy Change Impact Analyzer** supports Cloud-Delivered Firewall Management Center -managed Firewall Threat Defense devices only.
- **Policy Change Impact Analyzer** is available only for deployments in the US, AUS and EU regions.
- High Availability and cluster deployments are represented by their parent target during analysis.
- Impacted connection counts are available only when **Security Analytics and Logging** is enabled and connection events are sent for FTD Management Services.
- Running an analysis does not deploy, edit, approve, or reject policy changes.
- AI-generated explanations support decision-making. Validate important findings against your security requirements and operational policies before deployment.
- Review analysis results before approving production changes, especially high-risk policy modifications.

Understand analysis results

Review the assessment result to understand the likely effect of pending policy changes and the recommended next steps.

> **Note**
>
> An analysis result does not indicate whether a change is approved. Review the transition direction, affected rule, and traffic conditions before deployment.

Analysis result	What it means	Recommended action
Critical	One or more changes may expose the network to threats or disrupt services.	• Review affected rules and traffic segments before deployment. • Revise and rerun when the change is not intended.
Potential impact	One or more changes expand access or may affect traffic.	Validate the affected traffic and the expected business outcome before deploying.

Analysis result	What it means	Recommended action
Improved security posture	One or more changes reduce exposure or block risky traffic.	Confirm that the affected traffic is intentionally restricted, then continue through normal change review.
No traffic impact	No behavior-changing traffic transition was identified from the policy comparison.	• Confirm that the proposed rule is needed and is positioned as intended. • This result is different from a change that has zero observed connections.
Indeterminate	The available evidence was insufficient to determine a reliable impact.	• Review the changed rule and traffic criteria manually. • Consider gathering additional operational context and rerunning the analysis.

Understand job statuses

Job Status shows the current state of the policy impact analysis and whether the latest result is available and up to date.

Job status	Description
Verifying analysis is up to date	The system is checking whether the latest analysis still matches the pending policy changes.
Queued	The analysis request was accepted and is waiting to run. Wait for the status to change to **In progress** .
Completed	The latest analysis completed successfully. A warning icon may appear if a policy analysis returned an error.
Partial success	Useful assessment results are available, but one or more stages did not complete. Review the available details and **Workflows** before deciding whether to rerun.
In progress	The system is preparing policy data, calculating impact, or collecting connection evidence. Wait for the result or open **Workflows** to monitor progress.
Out of date	The policy changed after the analysis started, or the analysis is more than 24 hours old and its traffic evidence may no longer be current. Rerun the analysis to get the latest results.
Failed	The latest overall analysis failed. Review the error and **Workflows** details, then rerun the analysis if appropriate.

Job status	Description
Cancelled	The analysis was cancelled by an authorized user before completion.
Not analyzed	No analysis is available for the device, or the device has pending changes that have not yet been analyzed. Select a device and run the analysis.
Not applicable	No pending policy changes are available for analysis. Create or save the intended policy changes, then run the analysis.
Unknown	The system could not determine a reliable current status. Refresh the device list and try again later. If the issue persists, review the workflow details.

Understand inferred impact

Inferred Impact describes the likely effect of an individual changed rule or affected rule.

Inferred impact	Description
Potential threat exposure risk	The change may allow risky applications, risky URL categories, broad application or URL scope, sensitive destination ports, or broad Internet exposure.
Potential service disruption	The change may block sensitive services or high-volume business traffic.
Access expansion	The change may allow traffic that was previously blocked without a clear risky-application or sensitive-port signal.
Indeterminate	The available evidence was insufficient, or the impact assessment did not complete.
Improved security	The change blocks risky or untrusted traffic, or reduces broad external exposure.
No traffic impact	No behavior-changing traffic transition was detected.

Impacted traffic segments and connections

An **Impacted Traffic Segment** is a distinct combination of traffic conditions whose policy outcome, such as allow or block, changes when the proposed policy changes are deployed.

- Traffic conditions may include source and destination zones, networks, applications, URLs, users, services, ports, security-group tags, and geolocation identities.
- The number of impacted traffic segments is not the number of rules, packets, IP addresses, or historical connections.

Impacted Connections shows the number of historical connections associated with traffic affected by a changed rule.

- The count is based on available Security Analytics and Logging connection-event data. It represents observed historical activity, not a forecast of future traffic.

- If connection events are unavailable, the analyzer can still identify impacted traffic segments, but historical connection counts are not available.
- Review the policy comparison and traffic segments instead of treating unavailable data as zero traffic.

Understand policy analysis limitations

Some policy constructs are not fully evaluated during analysis. Review affected rules manually before deployment when these constructs are involved.

- Object overrides are not considered during analysis. For example, if a port object has the value `8080` but is overridden to `80` for a particular device, the device-specific value `80` is not considered.
- Country, continent, and custom geolocation objects are expanded to country-level identities. They are not expanded to IP-level identities, and individual IP addresses are not compared.
- URL category reputation is not considered. For example, if a new rule uses the same URL category with a different reputation, the analyzer may report **No Traffic Impact** even though the reputation changed.
- URL list and URL feed objects are not expanded into individual URLs. The analyzer reports an impact only when the object is used in an affected traffic fragment or segment. Individual entries in the list or feed are not evaluated separately.
- Time-range support is limited. Only active time ranges are considered. Rules with future or expired time ranges are treated as disabled. Changes to the time-range configuration itself are not considered during analysis.
- Dynamic-attribute support is limited to Security Group Tags (SGTs), including supported FMC and ISE SGT references. CSDAC-backed dynamic attributes and other unsupported dynamic-object criteria are not analyzed.
- Application filters entered directly in the application field, such as **Very High** or **High** risk or business relevance criteria, are not supported when they are inline filters rather than user-defined application filter objects. User-defined application filters, including filters that combine multiple criteria, are supported.

A policy change impact analyzer is a service that reviews potential impact of policy changes, identifies affected rules and connections, and provides AI-generated summaries.

- reviews potential impact of policy changes
- identifies affected rules and connections, and
- provides AI-generated summaries.

Analyze policy change impact

Configure analysis of pending access control policy rule changes across devices and review their potential traffic impact before deployment.

Analyze pending access control policy rule changes to understand their potential impact on network traffic before deploying the changes to production devices.

The Policy Change Impact Analyzer helps administrators assess the consequences of policy modifications by analyzing rule changes, identifying affected traffic segments, and providing historical connection data. This proactive analysis enables informed decision-making during the policy deployment process.

Before you begin

- Enable the **Policy Change Impact Analyzer** toggle under **Insights & Reports** > **Settings**.
- To view historical impacted connection counts, enable **Security Analytics and Logging**.
- **Policy Change Impact Analyzer** currently supports Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense devices.

Procedure

1. In the left pane, click **Insights & Reports > Policy Change Impact Analyzer**.

   The **Policy Change Impact Analyzer** page displays an **Impact Analysis** summary, including the number of identified impacts.

   The device list displays:

   - **Device Name**
   - **Job Status**
   - **Analysis Result**

2. Select one or more devices, and then click **Run Impact Analyzer**.

   You can select up to 10 devices for analysis. The analyzer evaluates the pending policy changes for the selected devices.

3. Monitor the analysis in the device list.

   Use the search field to search by device name, analysis result, or job status.

4. Click a device row to open the details pane.

   The pane displays the device status and may include these actions:

   - **View change impact details** to open the detailed analysis.
   - **Re-analyze** to generate an updated result.
   - **Deploy** to open the standard deployment workflow.
   - **Workflows** to review analysis execution details and errors.

5. Click the device name to open the analysis report.

   The analysis details page displays the overall impact assessment for the selected device.

6. Review the **Analysis Result**, **Rule Change Summary**, **Impacted Traffic Segments**, **Impacted Connections**, and **Inferred Impact**.
7. If the analysis is incomplete, failed, out of date, or indeterminate, review the policy manually before deployment and rerun the analysis as needed.

   > **Note**
   >
   > **Policy Change Impact Analyzer** does not deploy, edit, approve, or reject policy changes. Use the standard deployment and change-control process after reviewing the analysis results.

   You can also run a **Pre-deployment Assessment**. It performs the basic assessment and uses Policy Change Impact Analyzer to evaluate saved, pending access control policy changes. The report summarizes affected rules and traffic decision changes, with historical connection evidence when available, to help you review potential impacts before deployment. See Pre-deployment assessments for more information.

The **Policy Change Impact Analyzer** displays the potential impact of pending access control policy changes, including changed rules, impacted traffic segments, historical connections, inferred impact, and rule change summaries.

Best practices and recommendations

Describes how AIOps best practices and recommendations assess Cisco Secure Firewall configurations, identify failed checks, and provide actionable guidance to improve firewall performance and security.

Best practices and recommendations are a security assessment mechanism that

- enhances your organization's security posture with AgenticOps by identifying deviations from Cisco Secure Firewall best practices
- runs assessments on your devices, generates reports, and receives insights that guide you toward optimal performance, and
- addresses trending issues, incorporates industry best practices, and enhances the reliability of recommendations through input from Cisco's Technical Assistance Center (TAC) and Customer Experience (CX) teams.

Assessment and recommendation features

Best practices and recommendations include these key components:

- **Assessment**: Evaluates your firewall configuration across multiple categories. Each check determines alignment with Cisco Secure Firewall best practices. The report summarizes the total number of checks performed. It categorizes the results as **Passed** or **Requires review**.

  Checks that require review indicate deviations that could impact firewall efficiency and security. Each failed check presents an opportunity for improvement. Addressing these checks contributes directly to optimizing firewall performance.

- **Recommendation**: Provides specific recommendations to address identified issues, ensuring optimal firewall performance. These include detailed information such as the nature of the problem, symptoms, impact, and required actions.

Implement these recommendations to resolve issues, align with best practices, and optimize firewall performance.

Table 24: Key features

Feature	Description
Automated assessments	Runs periodic evaluations of firewall devices against Cisco best practices.
Checks summary	Displays how many checks passed and highlights those requiring review.
Trend visualization	Shows the number of checks over time, helping you compare passed and failed checks across assessment cycles.
Device reports	Provides device-specific results and percentage of improvement potential.
Review category and check control	Enable or disable review categories or individual checks for future assessments.

Implement best practices and recommendations

Configure best practices assessments to review device configurations and implement recommended improvements for optimal network performance.

This task enables you to implement best practices and recommendations by reviewing assessment results, managing device reports, and configuring automated assessments to maintain optimal network performance.

The Best Practices and Recommendations feature provides automated assessments of device configurations to identify potential improvements and ensure adherence to Cisco recommended practices. Use this workflow to review assessment results and implement necessary changes.

Before you begin

Ensure that **Best Practices** is enabled under **Settings**. For more information, see Enable Best Practices.

Follow these steps to implement best practices and recommendations:

Procedure

1. In the left pane, click **Insights & Reports > Best Practices and Recommendations**.

   The **Assessment Summary** provides a high-level overview of assessment results. It includes two tiles:

   - **Checks summary**: Displays the total number of checks and highlights those requiring review.
   - **Best practices assessment trend**: Helps you track assessment outcomes over time. The Y-axis represents the number of checks, and the X-axis shows assessment dates. You can hover over data points to view summary statistics.
   - **Feedback**: A mechanism for you to provide feedback on the assessments. You can enter optional comments and grant consent for follow-up contact regarding your feedback.

2. In the **Device reports** section, you can view the list of all available device reports. Filter devices by **Device status, Review categories,** or **Assessment status** to narrow down results.

   Assessment Statuses: Each device report has an **Assessment Status**, which indicates the current state of the assessment.

   - In progress: An assessment is actively running. After completion, a report will be generated.
   - In queue: The previous assessment is outdated, and a new one has been scheduled.
   - Updated: The assessment is complete, and the latest report is available for review.
   - Error: The assessment could not be completed due to an error. The report will be automatically generated after 24 hours. If the issue persists, contact **Cisco TAC** for assistance.

3. From the three-dot menu icon next to each device:

   a. Click **Run assessment** to initiate a new assessment.

   b. Click **Download report** to export the Best Practices assessment summary report in PDF format.

   #### Schedule Device Assessment

   Periodic assessments run automatically, but you can also run assessments manually at any time. In environments with more than **50 devices**, only **50 devices can be analyzed per day**. Use the **Select devices** option on the **Best Practices and Recommendations** page to choose which devices are included in automated assessments.

   - **Select devices for automated assessments**:

a. Click **Select devices** in the notification banner to open the **Schedule devices for assessment** dialog. This dialog allows you to choose which devices run automated assessments.

b. Devices in the **Scheduled devices** panel are included in automated assessments. Click **Save**.

- **Mange scheduled devices**: You can update the list of scheduled devices at any time. Devices removed from the **Scheduled devices** panel are no longer included in automated assessments. Devices added to this panel are included in future automated assessments.
- **Device scheduling limits**: You can schedule a maximum of **50 devices** for automated assessments. The **Scheduled devices** panel displays the number of currently scheduled devices, for example **48 / 50 devices**. When 50 devices are selected, further selection is disabled and a tooltip indicates that the maximum number of scheduled devices has been reached.

4. Click on a **Device name** to view a detailed report for that specific device.
   - Check the **Show passed checks** checkbox to view successful checks in the detailed view. This provides full visibility into all checks.
   - In the **Best practices assessment** section, view the **Total checks**, how many **Passed** and **Require review**.
   - Expand each check to view the remediations and corrective actions.
5. Enable or disable an entire category from future assessments. You can also disable individual checks within a category.
   - Disable the toggle to exclude a review category or check from future assessments.
   - Enable the toggle to include it in future assessments.

> **Note**
>
> Disabling a category or check does not affect the actual feature or its operation. The feature continues to function normally, but it is excluded from **Best Practices** assessments.

You have successfully implemented best practices and recommendations by reviewing assessment results, configuring device assessments, and managing category settings. The system will continue to run automated assessments based on your configuration and provide ongoing recommendations for maintaining optimal network performance.

Feature adoption insights

Explains how Feature Adoption Insights in AIOps tracks feature usage across eligible devices, groups adoption by license category, and helps identify underused capabilities to improve security outcomes.

A feature adoption insight is a dashboard capability that

- provides a comprehensive view of how effectively different features are being utilized across your environment
- calculates adoption rates based on the total number of eligible devices and the number of those devices configured with the feature, and
- helps you identify underutilized capabilities and take steps to improve overall adoption.

Feature adoption insight capabilities

The dashboard groups features into license categories to help you understand adoption patterns:

- **Essentials**
- **IPS**
- **Remote Access VPN**
- **Features not requiring license**
- **Subscription-Based Features**

> **Note**
>
> If a license is not available for a given category, the adoption rate for that category will always be **0%**.

By tracking the adoption rate at both the feature and license category levels, you can prioritize improvements and maximize the usage of available features. **Feature Adoption** helps you use available capabilities to achieve your intended outcomes

Assess and improve feature adoption

Configure feature adoption assessment to review and enhance the utilization of available security features across your organization.

This task helps you evaluate the current adoption status of security features in your organization and provides actionable insights to improve overall security posture through better feature utilization.

Feature adoption assessment provides visibility into which security features are being used, partially used, or not used at all. This analysis helps security administrators identify opportunities to enhance their organization's security by enabling and configuring underutilized features. The assessment includes adoption rates, recommendations, and specific steps to improve feature usage.

Before you begin

Ensure that you have selected the list of features under **Insights & Reports** > **Settings** > **Feature Adoption**.

Follow these steps to assess and improve feature adoption:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Feature Adoption**.
   - The **Summary** tile provides a quick overview of overall adoption status:
     - **Adoption rate**: Percentage of features currently adopted across their applicable scope.
     - **Total features**: Total number of features available for adoption.
     - **Not adopted**: Number of features that have not been enabled or configured.
     - **Partially adopted**: Number of features that are enabled or in use but not fully across all applicable scope.
     - **Adopted**: Number of features that are fully enabled and in use.

- In the **Feature Recommendation** tile, you can watch short videos about recommended features that will help enhance your organization's security.

> **Note**
>
> - The data updates every 24 hours, but you can click **Refresh** to update it manually.
> - We recommend that you increase the usage of these features to improve overall performance.

3. Click on a feature name to view detailed information.
   - A short description of the feature.
   - The feature adoption rate can range from 0% to 100%, based on how much the feature is used. Enable the toggle to include the feature in adoption calculations or disable it to exclude it.

     > **Note**
     >
     > Enabling or disabling a feature affects only the adoption score and does not impact the functionality of the feature.

   - Steps to improve your feature adoption rate.

You can view comprehensive feature adoption metrics, understand which features need attention, and access specific recommendations to improve your organization's security posture through better feature utilization.

Software upgrade insights

Explains how Software Upgrade Insights helps plan Firewall Threat Defense upgrades by showing current and recommended versions, upgrade readiness, threat campaign exposure, security vulnerability fixes, bug fixes, and guided remediation insights.

A Software Upgrade Planner is a firewall management tool that

- analyzes deployed Firewall Threat Defense devices and provides upgrade recommendations based on compatibility, stability, security vulnerabilities, and bug fixes
- provides a centralized view of the current software version running on each device along with the suggested version, and
- identifies potential risks and compatibility concerns before the upgrade process begins to reduce operational issues and minimize downtime.

Software upgrade planner capabilities

The feature provides these key capabilities to help you make informed upgrade decisions and maintain a consistent software version across the environment:

- Highlights important details such as bug fixes, vulnerability fixes, and upgrade readiness insights
- Simplifies firewall software upgrade planning and management
- Provides guided remediation insights for vulnerabilities and bugs affecting your devices
- Identifies devices that are exposed to active threat campaigns

Need a visual guide? Explore the Software Upgrade Planner feature walkthrough to see it in action.

When you view the details of a security vulnerability or bug, guided remediation provides AI-generated insights to help you understand the issue and determine an appropriate upgrade version. These insights can include:

- **Root cause analysis**: Summarizes the issue and its potential impact
- **Workaround**: When available, helps mitigate the issue before upgrading
- **Remediation guidance**: Identifies how many devices in your deployment are affected and recommends whether upgrading to a specific software version resolves the issue

When applicable, you can view the active threat campaigns affecting a device and access Cisco Talos intelligence resources to learn more about each campaign, including its scope, impact, and recommended mitigations.

Manage software upgrades

Configure software upgrade management using the Software Upgrade Planner to review suggested versions and evaluate security benefits for your devices.

Use the Software Upgrade Planner to review suggested software versions for your Firewall Threat Defense devices and evaluate the security and operational benefits of upgrading. In addition to suggested upgrade versions, the planner provides insights into active threat campaigns and guided remediation for vulnerabilities and bugs affecting your devices.

The Software Upgrade Planner helps evaluate suggested software versions, review threat campaign exposure, analyze security vulnerabilities and bug fixes, and use AI-generated remediation insights to make informed upgrade decisions.

Before you begin

Ensure that the **Software Upgrade Planner** toggle is enabled under **Insights & Reports** > **Settings** > **Operations**.

Follow these steps to manage software upgrades:

Procedure

1. In the left pane, click **Insights & Reports > Software Upgrade Planner**.

   The **Software Upgrade Planner** page displays a summary of upgrade opportunities across your deployment. The **Summary** section provides an overview of:

   - Devices with upgrades available
   - Total available fixes
   - Details on threat campaigns
   - Security vulnerability fixes
   - Bug fixes

   You can click **View all** in the **CVE Fixes** or **Bug Fixes** tiles to review the corresponding issues across your deployment.

2. Review the suggested upgrade versions for your devices.

- Multiple upgrade options are available based on vulnerabilities, bugs, and new features. The Cisco-suggested version is indicated by a gold star. Choose the version that suits your requirements.
- For each device, the planner displays the current software version and suggested upgrade versions. If a device is affected by one or more active threat campaigns, the current software version displays the number of threat campaigns affecting the device.
- Hover over the **Current version** to view additional details, including the current software version, vulnerabilities found, bugs found, and the active threat campaigns affecting the device.
- Select a threat campaign to open the corresponding Cisco Talos Intelligence blog and learn more about the campaign.

3. To perform an upgrade, click **More actions** (⋮) for the device, and click **Go to product upgrade**

   The **Product Upgrades** page opens in Cloud-Delivered Firewall Management Center, where you can perform the upgrade.

   - View available upgrade packages.
   - Perform an upgrade by clicking **Upgrade** in the **Actions** column. For more information, see Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-delivered Firewall Management Center.

4. In the **Software Upgrade Planner** page, select a device to view more details.

   The device details page displays **Suggested** and **Golden** versions. For each suggested version, you can review:

   - Active threat campaigns resolved
   - Security vulnerability fixes and bug fixes
   - Estimated downtime
   - New features included in the release
   - Link to detailed release notes

   Use this information to compare the available upgrade versions and determine the most appropriate upgrade version for your deployment.

5. Review the **Security vulnerability fixes** or **Bug fixes** tabs.

   - These tabs list the vulnerabilities and bugs affecting the selected device. You can search and filter the results or export the list as a CSV file.
   - Select a CVE ID or bug ID to open the details pane. The details pane provides AI-generated insights to help you understand the issue, including:
     - **Root cause analysis** that summarizes the issue and its potential impact.
     - **Workaround** information, when available, to help mitigate the issue before upgrading.
     - **Remediation** guidance that identifies how many devices in your deployment are affected and explains whether upgrading resolves the issue.
   - In the **Bug fixes** tab, bugs are categorized as **Impacting bugs** and **Other bugs**. Impacting bugs are affecting the selected device and its environment. You can search the list, filter bugs by status (**Fixed bugs**, **Open bugs**, or **All**), and export the results as a CSV file.

You can use the **Software Upgrade Planner** to evaluate suggested software versions, review threat campaign exposure, analyze security vulnerabilities and bug fixes, and use AI-generated remediation insights to make informed upgrade decisions.

You can now manage software upgrades using the Software Upgrade Planner, including reviewing suggested versions, evaluating security benefits, and performing upgrades with informed decision-making based on threat campaigns and vulnerability analysis.

Application insights

Explains how application insights provide visibility into application availability and outage events to help identify service disruptions and assess their impact.

Application insights is a monitoring capability that

- provides visibility into application availability and outage events
- identifies service disruptions and assesses their impact
- enables more effective responses to application-related issues.

How application insights work

Application Insights identifies outages for monitored cloud applications by consuming outage intelligence provided by **ThousandEyes Internet Insights.**

ThousandEyes Internet Insights collects telemetry from globally distributed vantage points that continuously measure application and network availability. When an outage affecting a SaaS or cloud service is detected, an outage event is generated. Application Insights uses this intelligence to display outage details such as affected applications, outage duration, impacted regions, and affected domains for the applications you monitor.

For more information about **ThousandEyes Internet Insights**, see Internet Insights.

The application insights monitoring process works as follows:

1. Once **Application Insights** is enabled, AgenticOps periodically evaluates Cloud-Delivered Firewall Management Center policies to determine which applications are eligible for monitoring.
2. The Cloud-Delivered Firewall Management Center policy is scanned every 24 hours. Applications that are enabled in the policy are automatically monitored, and any detected outages are reported on the **Application Insights** page using outage intelligence from **ThousandEyes Internet Insights**.
3. On the **Settings** page, applications that are allowed in the Cloud-Delivered Firewall Management Center policy are preselected by default. You can optionally select additional applications from the list to include them in outage monitoring.

Need a visual guide? Explore the Application Insights feature walkthough to see it in action.

Detect application outages

Configure monitoring to investigate application outages detected for the applications you track using Application insights to view outage summaries, identify affected services, and access detailed information about active and resolved outage events.

This task enables you to monitor and investigate application outages for applications you are tracking.

Application Insights provides a comprehensive view of application outage events, allowing you to track both active and resolved outages across your monitored applications.

Before you begin

Ensure that the **Application outage insights** toggle is enabled under **Insights & Reports** > **Settings** > **Application Insights**.

Procedure

1. In the left pane, click **Insights & Reports > Application Insights**.

   The Application Insights page displays a summary of detected outages, including the total number of outages, active outages, resolved outages, and the number of applications being monitored for the selected time range.

2. Review the list of affected applications. For each application outage, the following information is displayed:
   - Application name
   - Affected domains
   - Outage duration
   - Start and end timestamps
   - Affected regions

3. Click an application to view detailed outage information in the right pane.

You can now monitor application outages and access detailed information about affected services for both active and resolved outage events.

Compliance insights

Explains automated compliance evaluation features that help organizations assess firewall configurations against industry security standards and identify areas requiring attention.

Compliance insights are automated evaluation features that

- evaluate firewall configurations against supported compliance requirements and identify areas that may require attention
- highlight compliance gaps and potential risks, and
- provide actionable guidance to help maintain a compliant and secure deployment.

Compliance evaluation details

Organizations spend significant time and effort validating firewall configurations against industry security standards. This process is often manual, inconsistent, and dependent on specialized expertise. As compliance requirements evolve, teams must repeatedly revisit configurations, which slows down deployments and increases operational overhead.

Even small misconfigurations such as, overly permissive access rules or missing segmentation controls, can lead to compliance violations that are difficult to detect through manual review.

Compliance Posture in AgenticOps evaluates firewall configurations against industry-standard requirements. It translates compliance guidelines into programmatic checks that can be applied consistently across environments. The current implementation evaluates firewall configurations against the **Payment Card Industry Data Security Standard (PCI DSS) v4.0.1 framework**. Currently, **Compliance Posture** is available only for deployments in the US, EU, and AUS regions.

Disclaimer: The report is provided for informational purposes only and is created using AI. It does not constitute legal or professional compliance advice and is not a substitute for a formal audit or assessment performed by a qualified security assessor. You are responsible for independently verifying the contents of the report for accuracy and completeness. Cisco disclaims all liability related to the report.

Benefits of compliance insights:

- **Automate compliance validation** by evaluating firewall policies against predefined rules, eliminating manual review and reducing the risk of human error.
- **Generate compliance reports** that provide detailed findings and recommendations to help you assess and improve your security posture.
- **Review actionable recommendations** that guide remediation, such as restricting overly broad access, validating business intent, or removing redundant rules.
- **Review security zone mappings** to evaluate segmentation controls based on relationships between network zones.

Environment preparation requirements for compliance evaluation:

- Cloud-Delivered Firewall Management Center is provisioned in your organization.
- AgenticOps is activated in your organization.
- Firewall Threat Defense devices are onboarded and managed through Security Cloud Control Firewall Management.
- The device that you want to evaluate is online and reachable.

Generate compliance reports

Generate compliance reports to evaluate your environment against the PCI DSS 4.0.1 compliance standard.

Generate compliance reports to evaluate your firewall configuration against PCI DSS 4.0.1 compliance standards, review findings to identify security gaps, and export reports to support remediation efforts and compliance reviews.

Compliance reports help organizations assess their network security posture against industry standards. The PCI DSS 4.0.1 template evaluates firewall configurations for network security, access control, secure configuration, and logging requirements.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Compliance Posture**.

   The **Compliance Posture** page displays previously generated reports and allows you to create new compliance evaluations.
3. Click **Generate Report** to begin defining the report.
4. Enter a name and choose the device to evaluate.
   - Currently, **PCI DSS 4.0.1 Compliance Template** is the only supported template. This template evaluates firewall configurations against requirements for network security, access control, secure configuration, and logging.
   - Only devices that are currently online are available for selection.
5. Review the security zones.

   PCI DSS requires the Cardholder Data Environment (CDE) to be accurately defined. The CDE includes systems that store, process, or transmit cardholder data or sensitive authentication data, as well as environments with unrestricted

connectivity to systems handling such data. An automated assessment identifies security zones that are likely to be part of the CDE based on the existing configuration. Review the selected security zones and update the selections based on your knowledge of the network before generating the report.

6. In the **Security Zones** table, select the checkbox in the **CDE** column for each security zone that is part of the CDE. Clear the checkbox for any zone that is not part of the CDE.

   Note

   Incorrect security zone selections can result in inaccurate compliance findings, particularly for checks related to segmentation and traffic between network zones.

7. Click **Generate Report** to begin the compliance evaluation process.

   Note

   - Compliance reports are generated manually and are not evaluated automatically.
   - The system analyzes firewall policies and validates them against the selected compliance template. Report generation can fail due to device connectivity issues. Verify that the device is online and reachable.
   - The page confirms that report generation has started. A comprehensive review and analysis of the policies on the selected device will be performed. This process may take some time.
   - Click **Return to compliance reports** to return to the **Compliance Posture** page.

8. Find the generated report.

   Use the search field to search reports by name, user, or template. You can also click **Filters** to narrow the results. The **Compliance Status** column shows the number of checks that passed, need review, or failed.

9. Click the report name to view the detailed compliance results.

   - The report page displays the report name, evaluated device, last update time, compliance score, and compliance summary.
   - The **Compliance Score** shows the number of compliant checks out of the total number of checks.
   - The **Compliance Summary** displays total findings, checks that passed, need review, or failed.
   - The report displays a list of **Compliance Checks**, each representing a specific requirement being evaluated (for example, restricting inbound traffic to the CDE or validating VPN security). Select a compliance check to view its details, which may include:
     - A description
     - References to relevant compliance standards
     - Identified findings associated with the check
     - Recommendations for remediation

   The number next to each compliance check indicates how many findings were identified for that check.

10. Click **Download Report** to export the report in JSON format for audit and offline review.
11. Rerun a report.

    After making changes to address compliance findings, rerun the report to evaluate the updated configuration.

You can view compliance findings from the **Summary** page. Navigate to **Insights & Reports > Summary** and click **Operations** to view compliance-related insights for the selected time range.

Insight preferences

Describes how to manage AIOps insight preferences for a Security Cloud Control tenant, including enabling or disabling AIOps insights and configuring feature-specific insight settings.

Insight preferences are tenant-level configuration settings that

- enable or disable AgenticOps insights for your tenant
- allow configuration of feature-specific insight settings, and
- control insight preferences for multiple AgenticOps features.

Available features

You can enable or disable insight preferences for your tenant for these AgenticOps features:

Enable AgenticOps insights

Configure AgenticOps Insights to start onboarding your organization and unlock AI-driven insights, recommendations, and planning tools for your firewall environment.

Enable AgenticOps Insights to unlock AI-driven insights, recommendations, and planning tools for your firewall environment and improve performance, security, and operational efficiency.

To take advantage of AgenticOps' benefits, you must enable AgenticOps insights. You must have **Super Admin** or **Admin** user roles to enable **AgenticOps Insights** in your tenant.

Procedure

---

1. In the left pane, click **Insights & Reports** > **Settings**.
2. Select **Confirm AgenticOps activation**, and click **Get Started**.
3. Review the available AgenticOps features for each detected Firewall Management Center. The page displays the supported AgenticOps features, software version, and the number of managed devices for each Firewall Management Center. Click **Setup AgenticOps**.
4. Click **Confirm Onboard**.

   The onboarding process begins, and it takes a few minutes to fetch the data that is required to provide the insights. When completed, the **AgenticOps** > **summary** page is displayed.

After onboarding, AgenticOps begins analyzing data and the summary page displays, providing AI-driven insights and recommendations for your firewall environment.

Disable AgenticOps insights

Configure the disable option for AgenticOps insights to stop data collection and insight generation for your organization.

This task disables AgenticOps insights to stop data collection and insight generation. When opting out, you can choose to retain or permanently delete existing AgenticOps data.

You can choose to opt out of AgenticOps if you no longer want to use the capabilities. When you opt out, AgenticOps stops collecting data from your devices and deactivates all data processing and alerts. You must have **Super Admin** or **Admin** user roles to disable AgenticOps insights in your tenant.

Data cleanup options

When opting out, you can decide how existing data is handled:

- **Keep existing data**: Stops the AgenticOps service but retains your historical data. If you choose to opt in again later, this data can be reused for improved insights.
- **Remove all data**: Stops the AgenticOps service and permanently deletes all existing AgenticOps data. Deleted data cannot be recovered.

Procedure

1. In the left pane, click **Insights & Reports** > **Settings**.
2. Click **Miscellaneous**.
3. Under **Opt out of AgenticOps**, choose your preferred data cleanup option.
4. Click **Opt out of AgenticOps**.

AgenticOps insights are disabled for your organization, and data collection stops according to your selected cleanup option.

Manage AgenticOps data sources

Configure the On-Premises Firewall Management Centers that provide data to AgenticOps.

Manage data sources to control which Firewall Management Centers provide information to AgenticOps for generating insights and enabling AI-powered capabilities.

You can review newly detected data sources, onboard supported Firewall Management Centers, monitor onboarding status, and remove data sources that you no longer want AgenticOps to use.

Data sources include Cloud-Delivered Firewall Management Center and On-Premises Firewall Management Centers registered with Cisco Security Cloud. You can onboard data sources to enable AgenticOps capabilities or offboard data sources that you no longer want AgenticOps to use.

> **Note**
>
> Cloud-Delivered Firewall Management Center is required for AgenticOps and can't be offboarded.

Before you begin

- Ensure that AgenticOps is enabled for your organization.
- If you're using an On-Premises Firewall Management Center, ensure that it is integrated with Cisco Security Cloud.

Procedure

1. Navigate to **Insights & Reports > Settings**.
2. Under **AgenticOps Settings**, click **Data Sources**.
3. Choose one of these options:
   - To onboard a data source: When AgenticOps detects a supported data source that isn't onboarded, a banner appears on the **Data Sources** page. Click **Review & Onboard**, review the supported AgenticOps features for the selected data source, then click **Confirm Onboard**.
   - To offboard a data source: Locate the onboarded data source and turn off the toggle for the data source.

- When onboarding: The selected data source becomes available for supported AgenticOps features.
- When offboarding: AgenticOps no longer collects data or generates insights from the selected data source.

Capacity and traffic insights

Configure Capacity and Traffic insights to gain visibility into traffic patterns and capacity utilization across your organization.

Enable Capacity and Traffic insights to review insights that help identify resource constraints, track growth trends, and support capacity planning.

You can modify the preferences for Capacity and Traffic-related insights. These insights help monitor firewall performance, detect anomalies, and identify potential capacity risks.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports > Settings**.
3. Click **Capacity & Traffic Analysis**.
4. Enable the toggle buttons for the insights you want to monitor:
   a. Traffic-related insights
      - High traffic caused by elephant flow
      - RAVPN capacity assessment
   b. System health-related insights
      - High data plane CPU usage
      - High snort CPU usage
      - High data plane memory usage
      - High snort memory usage
   c. Anomaly detection-related insights
      - Connections rate (CPS) anomaly
      - Network throughput anomaly

5. For each insight, expand the section and configure the available settings. Depending on the insight, you can select severity levels, configure thresholds, or specify forecast parameters.
6. Click **Submit**.

After you enable the feature for the organization, you can view the detected anomalies in the **Summary** page, and the respective widgets are also displayed in the dashboard.

Best practices and recommendations insights

Enable Best Practices and Recommendations to evaluate your firewall deployment against Cisco Secure Firewall best practices. Review assessment results and recommended actions to identify risks, address configuration gaps, and optimize firewall operations.

Enable Best Practices and Recommendations insights to evaluate your firewall deployment against Cisco Secure Firewall best practices and optimize firewall operations.

You can modify the preferences for **Best Practices & Recommendations**-related insights.

> **Note**
>
> The setting for **Best Practices & Recommendations** is enabled by default.

Procedure

1. In the left pane, click **Insights & Reports** > **Settings**.
2. Click **Best Practices**.
3. Enable the **Best Practices & Recommendations Analysis** toggle button to view the assessment categories, checks performed under each category, and the number of failed checks for each device.
4. Enable the **Automatic assessment** toggle to activate automated report generation.
5. Click **Submit**.

After you enable the feature for your tenant, you can view the detected anomalies in the **Summary** page, and the respective widget is displayed on the dashboard.

Policy change impact analyzer insights

Enable Policy Change Impact Analyzer to assess the potential impact of pending access control policy changes before deployment.

Enable Policy Change Impact Analyzer to assess the potential impact of pending access control policy changes before deployment. AgenticOps provides visibility into affected rules, traffic segments, and historical connections to help you make informed deployment decisions.

You can modify the preferences for Policy Change Impact Analyzer-related insights.

> **Note**
>
> The **Policy Change Impact Analyzer** toggle is enabled by default.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Settings**.
3. Click **Policy Change Impact Analyzer**.
4. Enable the **Policy Change Impact Analyzer** toggle.

   This feature helps you review the potential impact of pending rule changes in Access Control policies before deployment. It currently supports Cloud-delivered Firewall Management Center-managed Firewall Threat Defense devices.
5. Click **Submit**.

After the feature is enabled, you can access it by clicking **Insights & Reports** > **Policy Change Impact Analyzer**.

Policy change impact analyzer insights

Enable Policy Change Impact Analyzer to assess the potential impact of pending access control policy changes before deployment.

Enable Policy Change Impact Analyzer to assess the potential impact of pending access control policy changes before deployment. AgenticOps provides visibility into affected rules, traffic segments, and historical connections to help you make informed deployment decisions.

You can modify the preferences for Policy Change Impact Analyzer-related insights.

> **Note**
>
> The **Policy Change Impact Analyzer** toggle is enabled by default.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Settings**.
3. Click **Policy Change Impact Analyzer**.
4. Enable the **Policy Change Impact Analyzer** toggle.

   This feature helps you review the potential impact of pending rule changes in Access Control policies before deployment. It currently supports Cloud-delivered Firewall Management Center-managed Firewall Threat Defense devices.
5. Click **Submit**.

After the feature is enabled, you can access it by clicking **Insights & Reports** > **Policy Change Impact Analyzer**.

Enable operational insights

Configure Software Upgrade Planner to evaluate the readiness of your Firewall Threat Defense devices for software upgrades.

Enable Software Upgrade Planner to evaluate the readiness of your Firewall Threat Defense devices for software upgrades. Use upgrade insights and recommendations to identify potential issues and support a smoother upgrade process.

You can modify the preferences for operations-related insights.

> **Note**
>
> The setting for **Software Update Planner** is enabled by default.

Procedure

1. In the left pane, click **Insights & Reports** > **Settings**.
2. Click **Operations**.
3. Enable the **Software Update Planner** toggle. You can view the software versions running on your devices and our upgrade recommendations.
4. Click **Submit**.

   After you enable this feature for your tenant, detected insights are listed in the **Summary** page.

Software Upgrade Planner is enabled and will begin evaluating device readiness for software upgrades. Insights and recommendations will appear in the Summary page.

Application insights

Configure Application Insights to detect and monitor application outages across selected applications. When outages occur, AgenticOps generates insights and notifications to help you identify and respond to service disruptions.

Enable Application Insights to automatically detect application outages and receive proactive notifications when service disruptions occur across your monitored applications.

You can modify the preferences for application outages-related insights.

> **Note**
>
> The setting for **Application Insights** is enabled by default.

Procedure

1. In the left pane, click **Insights & Reports** > **Settings**.
2. Click **Application insights**.
3. Enable the **Application outage insights** toggle button to receive insights and notifications when application outages occur.

4. In the **Selected applications** list, search for an application and check the checkbox to include it for monitoring. Clear the checkbox to remove an application from monitoring.
5. Click **Submit**.

After you enable the feature for your organization, you can view detected application outages on the **Application Insights** page, and corresponding insights are displayed on the **AgenticOps Summary** dashboard under the **Operations** category.

Frequently asked questions about AgenticOps

Provides answers to common questions about AgenticOps capabilities, onboarding, licensing, data collection, assessments, insight management, and feature configuration.

This section helps you understand how AgenticOps Insights, Best Practices and Recommendations, Feature Adoption, Software Upgrade Planner, Capacity and Trend Analyzer, and other AgenticOps services operate within your environment.

What is AgenticOps?

AgenticOps for firewalls leverages artificial intelligence (AI) and machine learning (ML) to streamline and enhance firewall management. By continuously analyzing the data, AgenticOps provides insights that help you:

- Optimize firewall policies and configurations.
- Detect misconfigurations before they impact performance.
- Improve feature adoption and adherence to best practices.
- Receive upgrade suggestions for Secure Firewall Threat Defense devices, including bugs fixes and security vulnerabilities fixes.

Are AgenticOps features available for all types of FMC-managed Firewall Threat Defense devices?

AgenticOps supports Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center and On-Premises Firewall Management Centers registered with Cisco Security Cloud. Feature availability varies by management type. For details, see AgenticOps Support for On-Premises Firewall Management Centers.

Can onboarding AgenticOps fail?

If an onboarding failure occurs, open a support ticket with Cisco Technical Assistance Center (TAC).

Can AgenticOps Insights be disabled?

Opting out of AgenticOps stops data collection and disables insights. You can choose whether to retain or permanently delete historical data. For more information, see Disable AgenticOps insights on page 521.

Can I disable specific AgenticOps modules?

Yes. From AgenticOps Settings, you can enable or disable modules such as Feature Adoption, Best Practices & Recommendations, and Operations. Disabled modules stop generating insights but do not affect device functionality.

Can i manually run best practices and recommendations assessments?

Periodic assessments run automatically, but you can also run assessments manually at any time. For large-scale deployments with more than 50 devices, you must run assessments manually due to processing limits.

Does AgenticOps automatically make changes to my firewall configuration?

No. AgenticOps provides recommendations and guidance based on analysis of your environment. Configuration changes are not automatically applied unless you explicitly review and implement them.

Additional resources

Lists additional AIOps resources for Security Cloud Control, including related documentation and guidance for using AI-driven firewall management features.

This reference provides links to additional resources for AIOps in Security Cloud Control, including blog posts about AI-driven firewall operations and autonomous security management evolution.

- From AIOps to AgenticOps: The Autonomous Evolution of Firewall Operations
- Managing Firewall complexity and Augmenting Effectiveness with AIOps for Cisco Firewall
- Security Cloud Control: Pioneering the Future of Security Management

23 Introduction to Agent Workforce

Topics:

- About Agent Workforce
- VPN agent
- Elephant flow agent traffic congestion remediation
- Firewall insight agent

This chapter introduces Agent Workforce, an AI-driven operational framework in Security Cloud Control that helps you troubleshoot network issues, analyze operational behavior, and manage firewall policies using natural language interactions.

Agent Workforce uses specialized agents to assist with operational workflows such as VPN troubleshooting, traffic remediation, and policy analysis. You can interact with agents conversationally to investigate issues, review recommendations, and perform guided operational tasks.

About Agent Workforce

Explains how ai-driven agents help streamline operational and security workflows using conversational interactions to assist with troubleshooting, remediation, analysis, and policy management tasks.

Agent Workforce is an AI-driven operational framework that

- enables you to interact with specialized agents using natural language to troubleshoot issues, analyze network behavior, and manage firewall policies
- allows you to describe operational problems or intended actions conversationally instead of relying solely on manual investigation, command-line analysis, or complex configuration workflows, and
- provides insights, recommendations, diagnostics, or policy actions through agents that are optimized for specific operational areas and perform focused analysis based on their specialization.

How Agent Workforce works

Based on the user query, the appropriate agent analyzes telemetry, configurations, policies, and operational data to provide insights, recommendations, diagnostics, or policy actions. Each agent is optimized for a specific operational area and performs focused analysis based on its specialization.

Available agents in Agent Workforce

Lists the specialized agents available in Agent Workforce and their operational capabilities for workflows such as VPN troubleshooting, traffic remediation, and policy management.

Agent Workforce includes specialized agents designed to assist with different operational and security workflows. Each agent focuses on a specific operational domain and uses relevant telemetry, protocol awareness, policy analysis, and contextual operational data to provide diagnostics, recommendations, and actionable outcomes.

When you enter a query, Agent Workforce interprets the intent and automatically routes the conversation to the most appropriate agent. You can describe operational issues or tasks in natural language without determining which agent should handle the request.

> **Note**
>
> Currently, Agent Workforce capabilities are available only for deployments in the US, EU, and AUS regions.

Depending on the workflow, Agent Workforce may also present contextual quick actions to help you initiate common investigative or remediation tasks more efficiently. Currently, Agent Workforce includes these agents:

- **VPN agent** helps troubleshoot site-to-site VPN connectivity, routing, tunnel negotiation, and secure traffic flow issues.
- **Elephant flow agent** helps analyze and remediate high-bandwidth traffic flows that may impact firewall performance and operational stability.
- **Firewall insight agent** helps analyze firewall inventory, configurations, policies, routing, and device status.

Manage Conversations in Agent Workforce

Configure and manage conversation threads with specialized agents for troubleshooting, investigation, and remediation workflows.

This task enables you to create new conversations, monitor active investigations, and interact with specialized agents for troubleshooting, investigation, and remediation workflows.

Use the **Conversations** page to create new conversations, monitor active investigations, and interact with specialized agents for troubleshooting, investigation, and remediation workflows.

Procedure

1. In the left pane, click **Insights & Reports** > **Agent Workforce** > **Conversations.**
2. Review the list of available conversation threads.

   Each conversation displays information such as the thread title, assigned agent, workflow status, creator, and creation date.
3. To locate a specific conversation, use the **Search** field to search by keywords.
4. To narrow the conversation list, click **Filters** and filter conversations using one or more criteria.
5. To create a new conversation, click **New Conversation**.
6. Enter your query in natural language.

   Agent Workforce automatically selects the most appropriate agent based on the operational intent of the request.
7. Continue interacting with the assigned agent if additional investigation, troubleshooting, or remediation actions are required.

You have successfully created and managed conversation threads with specialized agents for your troubleshooting, investigation, and remediation needs.

Considerations for agent workforce limitations and deployment

Outlines the current limitations, operational considerations, and deployment requirements for Agent Workforce.

Consider these limitations and requirements when deploying and using Agent Workforce:

- Currently, Agent Workforce capabilities are available only for deployments in the US, EU, and AUS regions.
- AI-generated insights, recommendations, and remediation actions must always be reviewed and validated before deployment.
- The accuracy of generated responses depends on the availability, completeness, and correctness of telemetry, policies, device configurations, logs, objects, and operational context within the environment.
- Missing, incomplete, or unresolved configuration entities may prevent certain workflows, recommendations, remediation actions, or deployment operations from completing successfully.
- Agent responses and operational analysis may vary depending on the enabled platform capabilities, configured integrations, available data sources, and device reachability.
- Some workflows may require manual validation, administrative approval, or additional configuration updates before operational changes can be applied to managed devices or policies.
- AI-generated operational guidance is intended to assist administrators and must not replace standard security review, compliance validation, or change-management procedures.

VPN agent

Explains how the VPN agent helps diagnose and troubleshoot site-to-site VPN connectivity and traffic flow issues by analyzing routing behavior, tunnel negotiation, telemetry, and policy enforcement.

A VPN agent is an intelligent troubleshooting agent that

- diagnoses and resolves site-to-site VPN connectivity and access issues
- analyzes operational telemetry, VPN configurations, routing behavior, packet flow, and access control policies to identify issues affecting secure connectivity between sites, and
- provides protocol-aware diagnostics across technologies such as BGP, EIGRP, OSPF, IPsec, and IKE to accelerate root-cause analysis and reduce manual troubleshooting effort.

Benefits of using the VPN agent

Lists the operational and troubleshooting benefits provided by the VPN agent.

The VPN agent provides operational and troubleshooting benefits for network analysis and packet-level investigation of VPN communication issues.

- Investigate VPN tunnel failures and connectivity disruptions.
- Analyze traffic flow between remote networks.
- Detect routing inconsistencies affecting VPN communication.
- Identify access control or policy-related packet drops.
- Perform packet-level troubleshooting and operational analysis.

Use the VPN agent to investigate connectivity issues

Configure the VPN agent to analyze operational data and correlate VPN-related telemetry to investigate connectivity issues across site-to-site VPN tunnels.

The VPN agent helps you investigate VPN connectivity issues by analyzing operational data and correlating VPN-related telemetry. The agent evaluates routing behavior, tunnel states, traffic flow activity, and policy enforcement to generate actionable insights for troubleshooting site-to-site VPN configurations.

When a query is submitted, the VPN agent correlates operational data across routing protocols, tunnel negotiation states, traffic flow behavior, and policy enforcement to identify the most likely root cause and provide actionable insights. Depending on the issue being investigated, the VPN agent can:

- Identify affected site-to-site VPN tunnels.
- Analyze IKE Phase 1 and Phase 2 negotiation states.
- Review tunnel establishment and peer connectivity status.
- Investigate routing behavior across the VPN tunnel.
- Evaluate traffic flow behavior between local and remote networks.
- Correlate logs, telemetry, and operational events to identify likely root causes.
- Generate operational findings, root-cause analysis, and remediation recommendations.

> **Note**
>
> The VPN agent works only for Firewall Threat Defense site-to-site VPN configurations managed by Cloud-delivered Firewall Management Center or On-Premises Firewall Management Center.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Agent Workforce** > **Conversations**.
3. Click **New Conversation**.
4. Enter a query describing the VPN connectivity issue or traffic-flow problem.

   Agent Workforce automatically assigns the request to the VPN agent based on the operational intent.
5. Review the generated diagnostics, tunnel analysis, routing behavior, traffic flow analysis, and remediation recommendations.
6. Continue refining the investigation by providing additional operational details such as affected sites, peer devices, tunnel names, or observed behavior.
7. Review the recommended remediation actions and validate the operational impact before applying configuration changes.

After the analysis is completed, the VPN agent summarizes operational findings, identified root cause, impact assessment, additional observations, recommended remediation steps and next actions.

Best practices for using the VPN agent

Outlines recommended practices to improve troubleshooting accuracy and operational visibility when using the VPN agent.

To improve troubleshooting accuracy and reduce analysis time:

- Include source and destination networks whenever possible.
- Specify the affected VPN tunnel, site, or peer device if known.
- Clearly describe observed behavior such as packet drops, intermittent connectivity, or failed tunnel establishment.
- Refine prompts with additional operational context if further analysis is needed.
- Validate recommended remediation steps before deployment.

Example prompts and expected outcomes for the VPN agent

Provides example prompts and describes the expected operational outcomes generated by the VPN agent. Use these examples to understand supported workflows and improve conversational interactions during investigations.

This reference provides example prompts and describes the expected operational outcomes generated by the VPN agent. Use these examples to understand supported workflows and improve conversational interactions during investigations.

User intent	Example prompt	Expected outcome
Troubleshoot connectivity between remote sites	Troubleshoot why the connectivity is down between [remote site 1] and [remote site 2].	VPN agent identifies the relevant Site-to-Site VPN tunnel associated with the affected networks and performs guided troubleshooting analysis.
Troubleshoot a VPN tunnel outage	My VPN tunnel is down. Help me troubleshoot the issue.	VPN agent identifies available VPN tunnels, allows tunnel selection if needed, and analyzes tunnel state, negotiation behavior, routing, and connectivity conditions.
Investigate VPN traffic flow issues	Investigate why VPN traffic is not flowing across the [tunnel name].	VPN agent analyzes traffic forwarding behavior, routing conditions, and policy enforcement affecting traffic flow across the VPN tunnel.
Review configured VPN tunnels	How many VPN tunnels are configured and what state are they in?	VPN agent displays configured site-to-site VPN tunnels along with operational state, tunnel health, and connectivity status details.
Visualize VPN routing paths	Visualize the routing between various devices connected by my VPN tunnels.	VPN agent analyzes VPN topology, connected networks, and routing relationships, and provides communication paths across VPN tunnels.

Elephant flow agent traffic congestion remediation

Explains how the Elephant flow agent remediates high-bandwidth traffic flows identified by an AgenticOps-generated elephant flow insight.

The Elephant flow agent is an intelligent remediation agent that

- helps you remediate high-bandwidth traffic flows that impact network performance and critical applications
- relies on a valid AgenticOps-generated insight and uses the device and application information provided in the insight to construct a trust rule and guide the remediation workflow, and
- provides a guided remediation experience directly within the conversation workflow.

Elephant flow impact and remediation approach

Large traffic flows, commonly referred to as elephant flows, can consume excessive bandwidth, increase firewall processing overhead, and degrade application performance across the network. Unlike traditional troubleshooting workflows that require manual investigation across multiple dashboards and telemetry sources, the Elephant flow agent provides a guided remediation experience directly within the conversation workflow.

> **Note**
>
> The Elephant flow agent remediates only high-bandwidth traffic flows identified in a valid AgenticOps-generated insight; it does not detect elephant flows.

Benefits of using the elephant flow agent

Lists the operational and remediation benefits provided by the Elephant flow agent.

The Elephant flow agent helps identify traffic patterns, investigate congestion issues, and recommend remediation actions for affected devices and applications.

- Analyze previously detected elephant flows affecting network performance.
- Investigate abnormal traffic spikes and sustained utilization.
- Identify applications or traffic flows contributing to congestion.
- Recommend remediation actions to reduce processing overhead and congestion.
- Stage policy updates associated with remediation workflows.

Configure elephant flow remediation workflow

Configure the Elephant flow agent to analyze detected traffic insights and guide remediation workflows that help you review affected traffic patterns, evaluate remediation recommendations, and deploy updates when required.

This task enables you to configure and execute the Elephant flow remediation workflow to address high traffic issues caused by elephant flows through guided analysis and automated policy recommendations.

The Elephant flow agent provides an automated workflow to analyze traffic insights and recommend remediation actions. This process helps network administrators efficiently manage high-impact traffic flows that can affect network performance.

Before you begin

- Ensure that **Cloud-Delivered Firewall Management Center** is provisioned in your organization.
- Ensure that AgenticOps is onboarded in your organization.
- Ensure that **High traffic caused by elephant flow** is enabled under **Insights & Reports** > **AgenticOps Insights** > **Settings** > **Capacity & Traffic Analysis**. For more information, see Capacity and traffic insights.
- Ensure that valid AgenticOps-generated elephant flow insights exist. Remediation cannot begin without a valid insight.

Follow these steps to configure the Elephant flow remediation workflow:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** >**Summary**.
3. On the AgenticOps **Summary** page, select the **Traffic & Capacity** insights category.
4. In the **High traffic caused by elephant flow** section, select the affected device.
5. Review the detected elephant flow insight details, affected resources, applications, and traffic impact information.
6. Click **Review proposed remediation** to open the remediation workflow in **Agent Workforce** > **Conversations**.

a. Alternatively, navigate to **Insights & Reports > Agent Workforce > Conversations**.

b. Click **New Conversation** and select **View elephant flow insights** to start the remediation workflow.

> **Note**
>
> Manual prompt entry is not required to start the workflow.

7. Review the proposed remediation actions, operational warnings, shared policy impact, and success criteria.
8. Approve or cancel the remediation workflow as required.
9. Deploy the generated policy updates to the affected devices.

> **Note**
>
> Elephant flow events displayed in the Unified Event Viewer might not be available to the remediation agent if AgenticOps did not generate a corresponding insight.

The Elephant flow remediation workflow is configured and executed. Policy updates are deployed to the affected devices to address high traffic issues caused by elephant flows.

Best practices for using the elephant flow agent

Outlines recommended practices for reviewing, validating, and deploying elephant flow remediation actions to minimize operational impact and improve remediation accuracy.

To improve remediation accuracy and operational visibility:

- Review affected applications before approving remediation actions.
- Verify the operational impact of policy updates before deployment.
- Review shared policy impact warnings before approving remediation actions.
- Monitor application and network behavior after remediation is completed.

Firewall insight agent

Explains how the Firewall insight agent helps you investigate firewall inventory, configurations, policies, routing, and device status by analyzing device data and operational state to provide detailed insights and support operational troubleshooting.

A Firewall insight agent is an analysis tool that

- investigates the configuration and operational state of managed firewalls
- provides information about device inventory, interfaces, routing, policies, licensing, compliance, software, and security configuration, and
- identifies conflicts, inconsistencies, and other issues that may require attention.

Benefits of using the firewall insight agent

Lists the operational and troubleshooting benefits provided by the Firewall insight agent.

The Firewall insight agent provides comprehensive operational and troubleshooting capabilities for firewall management and monitoring.

- View firewall inventory by device type, connectivity state, licensing status, compliance status, and onboarding state.
- Identify unlicensed or out-of-compliance devices.
- Identify access control or policy-related packet drops.
- Review routing configuration, BGP configurations, and route exchange between devices.
- Review interface status and device connectivity information.
- Review syslog and email alert configuration.
- Ask follow-up questions to investigate findings in greater detail.

How firewall insight agent works

Configure firewall analysis queries using the Firewall insight agent to investigate operational data, device inventory, policies, routing, and security configurations.

The Firewall insight agent analyzes operational data and correlates firewall-related telemetry to investigate issues. It provides information about device inventory, interfaces, routing, policies, licensing, compliance, software, and security configuration, and identifies conflicts, inconsistencies, and other issues that may require attention.

When you submit a query, Firewall insight agent identifies the relevant devices, configurations, policies, or operational data and returns the associated information. The agent can:

- Identify the devices, policies, routes, interfaces, or configurations related to the query.
- Correlate information across devices, policies, routing, security configuration, and operational state.
- Compare related configurations and identify conflicts, overlaps, redundancies, or inconsistencies.
- Explain when a device or configuration cannot be found and identify the information required to continue the investigation.
- Generate operational findings, root-cause analysis, and recommended next steps.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Agent Workforce** > **Conversations**.
3. Click **New Conversation**.
4. Enter a query about firewall inventory, device state, routing, policies, security configuration, or operational data.

   Agent Workforce automatically assigns the request to an agent based on the operational intent.
5. Review the returned firewall information, analysis, and key observations.

   The Firewall insight agent analyzes firewall data and reports findings, comparisons, and recommended next steps. It does not modify configurations, create or deploy policies, or approve changes.
6. Continue the investigation by providing additional context, such as device names, policy names, object names, interfaces, or other relevant identifiers.

7. Review the recommended next steps and validate the operational impact before applying configuration changes.

After the analysis is completed, Firewall insight agent summarizes the operational findings, identified root cause, impact, additional observations, and recommended next steps.

Best practices for using the firewall insight agent

Outlines recommended practices to improve troubleshooting accuracy and operational visibility when using the Firewall insight agent.

To improve troubleshooting accuracy and reduce analysis time:

- Include device names, policy names, object names, or other identifiers when available.
- Clearly describe observed behavior such as packet drops, intermittent connectivity, unexpected policy behavior, or configuration inconsistencies.
- Provide additional operational context if further analysis is needed.
- Review recommended next steps and validate their operational impact before deployment.

Example prompts and expected outcomes for the firewall insight agent

Provides example prompts and describes the expected operational outcomes generated by the VPN agent.

Use these examples to understand supported workflows and improve conversational interactions during investigations.

User intent	Example prompt	Expected outcome
Review firewall inventory	What devices do I have in my firewall inventory?	The agent summarizes devices by type and connectivity state. It can also provide software versions, addresses, manager associations, licensing status, and compliance status.
Review interfaces	List all interfaces and their status for `[device name]`.	The agent lists the device interfaces and their status. If the device cannot be found, it explains the lookup failure.
Review BGP configuration	Show the current BGP configuration on `[device name]`.	The agent returns BGP neighbors, local and remote AS numbers, peering type, tunnel interfaces, redistribution, and related configuration details.
Review licensing and compliance	Which Firewall Threat Defense devices are unlicensed or out of compliance?	The agent lists affected devices and provides their license and compliance status, software version, and other relevant device details.
Review software updates	Which Firewall Threat Defense devices have a recommended software update?	The agent identifies devices with available updates and provides current versions, target versions, fixes, and affected defects or threats.

24 Monitor Cloud-Delivered Firewall Management Center-Managed Threat Defense Device Events

Topics:

- Security Analytics and Logging for Firewall Threat Defense
- SAL (SaaS) for Cloud-Delivered Firewall Management Center-managed devices
- Requirements and guidelines
- How Firewall Threat Defense events are displayed in Security Cloud Control using a direct connection
- Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection
- Send Cloud-Delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog
- Enable individual threat defense devices to send events to SAL (SaaS) using a direct connection
- View AI Defense Events in Security Cloud Control

Learn how to send and monitor Cloud-Delivered Firewall Management Center-managed Threat Defense events in Security Cloud Control using Security Analytics and Logging, direct cloud connections, syslog, device-level controls, and AI Defense event views.

View events from Threat Defense devices that are managed by Cloud-Delivered Firewall Management Center in Security Cloud Control.

Security Analytics and Logging for Firewall Threat Defense

Explains how Security Analytics and Logging captures Firewall Threat Defense events from Cloud-Delivered Firewall Management Center-managed devices and makes them available for filtering and review in Security Cloud Control.

SAL (SaaS) is a cloud-based security service that

- captures connection, intrusion, file, malware, and Security Intelligence events from all Firewall Threat Defense devices
- stores events in the Cisco cloud for centralized viewing in Security Cloud Control, and
- provides filtering and review capabilities through the **Event Logging** page to help understand what security rules are triggering in your network.

Additional capabilities

SAL (SaaS) for Cloud-Delivered Firewall Management Center-managed devices

Explains how to set up Security Analytics and Logging for Cloud-Delivered Firewall Management Center-managed Threat Defense devices using direct cloud event delivery or syslog.

SAL (SaaS) for Cloud-Delivered Firewall Management Center-managed devices is an integration that

- enables event data storage in SAL (SaaS)
- supports deployment using either syslog or a direct connection, and
- provides security analytics and logging capabilities for Cloud-Delivered Firewall Management Center-managed Threat Defense devices.

Implementation methods

You can implement SAL (SaaS) using these methods:

- Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection on page 544
- Send Cloud-Delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog on page 545

Requirements and guidelines

Outlines requirements for sending Threat Defense events to Security Analytics and Logging, including supported versions, cloud regions, subscriptions, ingest planning, and connectivity.

Requirements: Cisco Secure Firewall Threat Defense

Ensure that your environment meets these device and system requirements for Firewall Threat Defense integration.

- Security Cloud Control-managed standalone Firewall Threat Defense devices, Version, 7.2 and later.
- To send events using syslog, you must have Firewall Threat Defense device, Version 6.4 or later.
- To send events directly, you must have Firewall Threat Defense device, Version 7.2 or later.
- To optionally exclude individual Firewall Threat Defense devices from sending events directly, you must have Firewall Threat Defense device, Version 7.4.1 or later.

- Your firewall system must be deployed and successfully generating events.

Requirements: regional cloud configuration

Select the appropriate regional cloud for your event management and ensure consistency across your security integrations.

- Determine the regional cloud that you want to send events to.
- Events cannot be viewed from or moved between different regional clouds.
- If you use a direct connection to send events to the Cisco Security Cloud for integration with Cisco SecureX, or Cisco SecureX threat response, or Cisco XDR, you must use the same cloud region for this integration.
- If you send events directly, the regional cloud you specify in Security Cloud Control must match the region of your Security Cloud Control tenant.

Requirements: Security Analytics and Logging subscription plan

Obtain and configure the appropriate Security Analytics and Logging subscription plan for your event volume requirements.

- You must have a valid Security Analytics and Logging subscription plan. For more information about the subscription plans, see Security Analytics and Logging Licenses.
- If your do not have a Security Analytics and Logging plan subscribed, you can request a 90-day trial by logging in to Security Cloud Control and navigating to **Events & Logs** > **Events** > **Event Logging** tab. You can purchase the desired subscription plan by following the instructions in the Security Cloud Control Firewall Management Ordering Guide.
- You must buy a data plan that reflects the number of events the Cisco cloud receives from your threat defense devices daily. This is called your daily ingest rate.
- Use the Logging Volume Estimator Tool to estimate your data storage requirements.

Requirements: account configuration

When you purchase a license for this integration, you are provided with a Security Cloud Control tenant account to support the integration.

Requirements: connectivity

The Firewall Threat Defense devices must be able to connect outbound on port 443 to the Cisco Security Cloud at the addresses specified for your regional cloud.

- US region:
  - api-sse.cisco.com
  - mx*.sse.itd.cisco.com
  - dex.sse.itd.cisco.com
  - eventing-ingest.sse.itd.cisco.com
  - registration.US.sse.itd.cisco.com
  - https://security.cisco.com
  - edge.US.cdo.cisco.com
- EU region:
  - api.EU.sse.itd.cisco.com
  - mx*.EU.sse.itd.cisco.com
  - dex.EU.sse.itd.cisco.com

    - eventing-ingest.EU.sse.itd.cisco.com
    - registration.EU.sse.itd.cisco.com
    - https://security.cisco.com
    - edge.EU.cdo.cisco.com
- Asia (APJ) region:
    - api.APJ.sse.itd.cisco.com
    - mx*.APJ.sse.itd.cisco.com
    - dex.APJ.sse.itd.cisco.com
    - eventing-ingest.APJ.sse.itd.cisco.com
    - registration.APJ.sse.itd.cisco.com
    - APJ.cdo.cisco.com
    - edge.APJ.cdo.cisco.com
- Australia region:
    - api.aus.sse.itd.cisco.com
    - mx*.aus.sse.itd.cisco.com
    - dex.au.sse.itd.cisco.com
    - eventing-ingest.aus.sse.itd.cisco.com
    - registration.au.sse.itd.cisco.com
    - aus.cdo.cisco.com
- India region:
    - api.in.sse.itd.cisco.com
    - mx*.in.sse.itd.cisco.com
    - dex.in.sse.itd.cisco.com
    - eventing-ingest.in.sse.itd.cisco.com
    - registration.in.sse.itd.cisco.com
    - in.cdo.cisco.com

How Firewall Threat Defense events are displayed in Security Cloud Control using a direct connection

Describes how Threat Defense events sent through a direct cloud connection become available for monitoring and analysis in Security Cloud Control.

This process describes how Firewall Threat Defense devices that are managed by Security Cloud Control shares security events (connection, security-related connection, intrusion, file, and malware events) with Security Cloud Control.

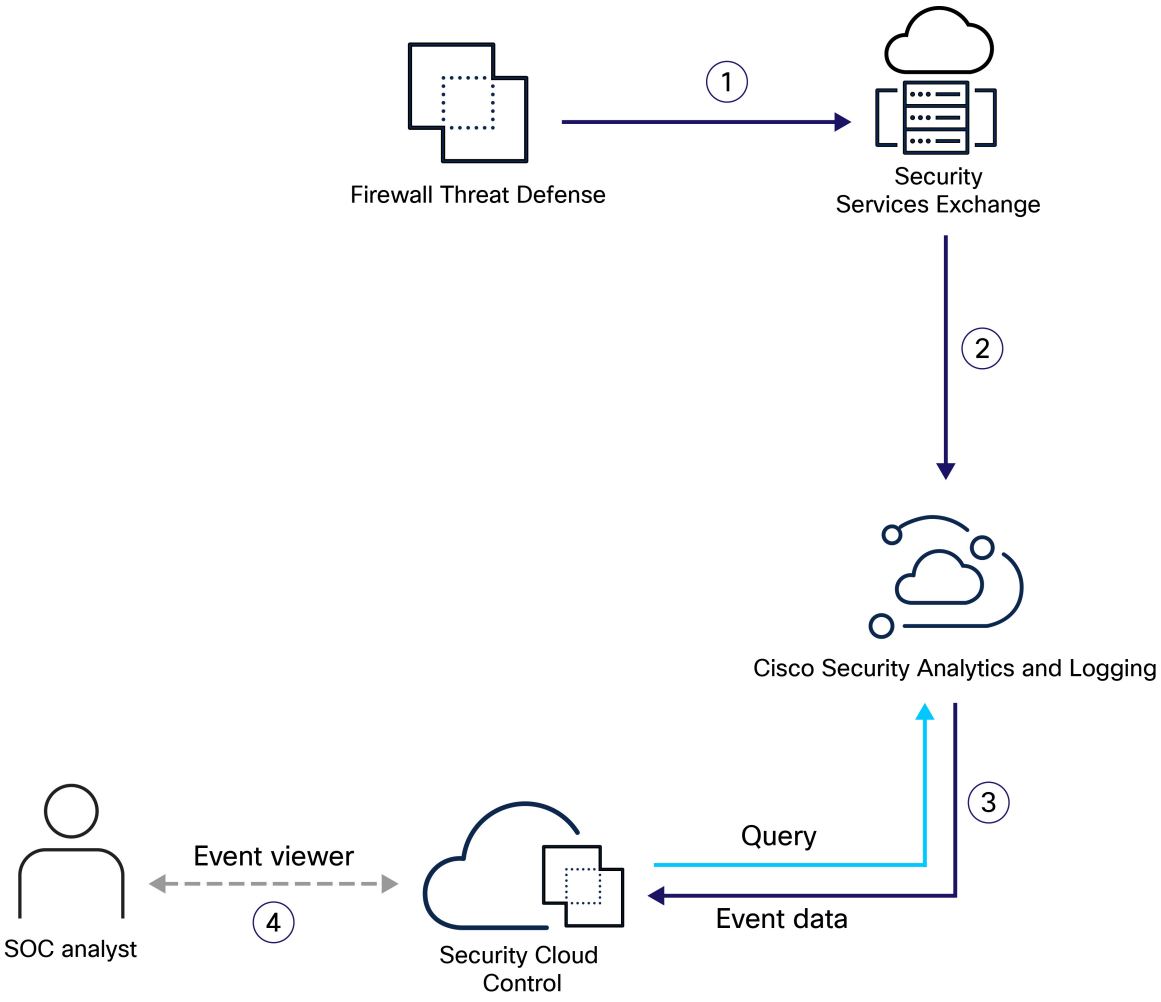
Summary

The key components involved in displaying Firewall Threat Defense events in Security Cloud Control are:

- Firewall Threat Defense device: Generates and sends security events directly to Cisco cloud when logging is enabled
- Security Services Exchange: Aggregates event data, converts it to JSON format, and forwards it for storage
- Security Analytics and Logging: Processes and enriches event data using various classification services
- Security Cloud Control: Queries stored data to provide SOC analysts with relevant information

Workflow

Figure 8: How Firewall Threat Defense events are displayed in Security Cloud Control



The process involves these stages:

1. You configure the Firewall Threat Defense device to send security events directly to Cisco cloud.

   Security events are generated when logging is enabled on the Firewall Threat Defense device, and network traffic matches access control rule criteria. The Firewall Threat Defense device sends the events directly to Security Services Exchange.

2. Security Services Exchange aggregates the event data from all the Firewall Threat Defense devices, converts it to JSON format, and sends it to Security Analytics and Logging for storage.

3. Security Analytics and Logging process the event data using various services to classify and enrich it for use by the Security Cloud Control.

4. Security Analytics and Logging stores the event data in the cloud data store. Security Cloud Control queries the stored data to provide SOC analysts with the relevant information.

Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection

Configure Cloud-Delivered Firewall Management Center-Managed -managed event logs to send directly to Security Analytics and Logging (SaaS), including enabling Cisco Cloud Events and choosing which event types to send.

This task enables the Cloud-Delivered Firewall Management Center to send events directly to SAL (SaaS) by configuring the Cisco cloud event global setting.

This procedure enables the Cisco cloud event global setting in the Cloud-Delivered Firewall Management Center. When needed, you can exclude individual Firewall Threat Defense devices from sending event logs to SAL (SaaS). For more information, see Enable or Disable Threat Defense Devices to Send Event logs to SAL (SaaS) Using a Direct Connection.

Before you begin

- Onboard devices to the Cloud-Delivered Firewall Management Center, assign licenses to these devices, and configure these devices to send events directly to SAL (SaaS).
- Enable connection logging on a per-rule basis by editing a rule and choosing the **Log at Beginning of Connection** and **Log at End of Connection** options.

Procedure

1. Log in to Security Cloud Control.
2. From the Security Cloud Control Home page, click **Firewall**.
3. In the left pane, click **Administration** > **Firewall Management Center**.
4. Click **Cloud-Delivered FMC**, and in the **System** pane that is located at the right-side, click **Cisco Cloud Events**.
5. In the **Configure Cisco Cloud Events** widget, do the following:
   a. Click the **Send Events to the Cisco Cloud** toggle button to enable the overall configuration.
   b. Check the **Send Intrusion Events to the cloud** check box to send the intrusion events to the cloud.

      Note

      When you enable sending intrusion events, the Firewall Threat Defense device sends the captured packet data to the cloud along with the intrusion events. Cisco Talos uses this packet data to analyze and eliminate false threats. This ensures focus on actual threats, enhancing the accuracy and efficiency of Talos' threat recommendations.

   c. Check the **Send File and Malware Events to the cloud** check box to send the file and malware events to the cloud.
   d. Choose an option to send the connection events to the cloud:
      - Click the **None** radio button to not send connection events to the cloud.
      - Click the **Security Events** radio button to send only security intelligence events to the cloud.

- Click the **All** radio button to send all the connection events to the cloud.

e. Click **Save**.

The Cloud-Delivered Firewall Management Center is now configured to send the selected event types directly to SAL (SaaS).

Send Cloud-Delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog

Configure Cloud-Delivered Firewall Management Center-managed devices to send intrusion, file, malware, and connection events directly to Security Analytics and Logging.

This task enables your Cloud-Delivered Firewall Management Center-managed devices to send security events (connection, security intelligence, intrusion, file, and malware events) directly to SAL (SaaS) using syslog messages.

This procedure provides information about the configuration for sending syslog messages for security events (connection, security intelligence, intrusion, file, and malware events) from devices managed by Security Cloud Control.

Before you begin

- Configure policies to generate security events, and verify that the events you expect to see are displayed in the applicable tables under the **Events & Logs** menu.
- Gather information relating to the syslog server IP address, port, and protocol (UDP or TCP).
- Ensure that your devices can reach the syslog server.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Administration** > **Firewall Management Center** to open the **Services** page.
3. Click and select **Cloud-Delivered FMC** and then click **Configuration**.
4. Configure the syslog settings for your threat defense device:
   a) Click **Devices** > **Platform Settings** and edit the platform settings policy that is associated with your threat defense device.
   b) In the left-side navigation pane, click **Syslog** and configure the syslog settings as follows:

Click this UI Element...	To Do the Following:
Logging Setup	Enable logging, specify FTP server settings, and the Flash usage.
Logging Destination	Enable logging to specific destinations and to specify filtering by message severity level, event class, or by a custom event list.
E-mail Setup	Specify the email address that is used as the source address for syslog messages that are sent as emails.
Events Lists	Define a custom event list that includes an event class, a severity level, and an event ID.

Click this UI Element...	To Do the Following:
Rate Limit	Specify the volume of messages being sent to all the configured destinations and define the message severity level to which you want to assign the rate limits.
Syslog Settings	Specify the logging facility, enable the inclusion of a time stamp, and enable other settings to set up a server as a syslog destination.
Syslog Servers	Specify the IP address, protocol that is used, format, and security zone for the syslog server that is designated as a logging destination.

c) Click **Save**.

5. Configure the general logging settings for the access control policy (including file and malware logging):
   a) Click **Policies** > **Access Control** and then edit the access control policy that is associated with your threat defense device.
   b) Click **More** and then choose **Logging**. Configure the general logging settings for the access control policy (including file and malware logging) as follows:

Click this UI Element...	To Do the Following:
Send using specific syslog ALERT	Select a syslog ALERT from the list of existing predefined alerts or add one by specifying the name, logging host, port, facility, and severity.
Use the syslog settings configured in the FTD Platform Settings policy deployed on the device	Unify the syslog configuration by configuring it in **Platform Settings** and reuse the settings in the access control policy. The selected severity is applied to all the connection and intrusion events. The default severity is **ALERT**.
Send Syslog messages for IPS events	Send events as syslog messages. The default syslog settings are used unless you override them.
Send Syslog messages for File and Malware events	Send file and malware events as syslog messages. The default syslog settings are used unless you override them.

   c) Click **Save**.

6. Enable logging for security intelligence events for the access control policy:
   a) In the same access control policy, click the **Security Intelligence** tab.
   b) Click the logging icon and enable security intelligence logging using these criteria:
      - By Domain Name: Click the logging icon next to the **DNS Policy** drop-down list.
      - By IP address: Click the logging icon next to **Networks**.
      - By URL: Click the logging icon next to **URLs**.
   c) Click **Save**.

7. Enable syslog logging for each rule in the access control policy:
   a) In the same access control policy, click the **Access Control** tab, and click a rule to edit.
   b) Click the **Logging** tab in the rule.

c) Check the **Log at beginning of connection** and **Log at end of connection** check boxes.
d) If you want to log file events, check the **Log Files** check box.
e) Check the **Syslog Server** check box.
f) Verify that the rule is **Using default syslog configuration in Access Control Logging**.
g) Click **Confirm**.
h) Click **Apply** to save the rule.
i) Repeat steps 7.a through 7.h for each rule in the policy and click **Save** to save the policy.

8. If you have made all the required changes, deploy your changes to the managed devices.

Your Cloud-Delivered Firewall Management Center-managed devices now send intrusion, file, malware, and connection events to SAL (SaaS) using syslog messages. Security events should appear in the configured syslog server.

Enable individual threat defense devices to send events to SAL (SaaS) using a direct connection

Configure individual Threat Defense devices managed by Cloud-Delivered Firewall Management Center to enable or disable direct event delivery to SAL (SaaS).

Enable or disable FTD devices managed by the Cloud-Delivered Firewall Management Center to send events directly to SAL (SaaS). This device-level control allows you to optionally exclude specific FTD devices from sending event logs to the Cisco cloud to reduce traffic or to maintain a combination of SAL and on-premises event log storage.

Note

- To enable or disable sending events to the Cisco cloud from the FTD devices, enable the Cisco cloud event global setting in the Cloud-Delivered Firewall Management Center. For more information on enabling the Cisco cloud event global setting, see Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection on page 544.

  Sending events to the Cisco cloud is enabled by default for all FTD devices when the Cisco cloud event global setting is enabled in the Cloud-Delivered Firewall Management Center.

- The option to enable or disable FTD devices to send event logs to the cloud is supported on FTD Version 7.4.1 or later.

Before you begin

- Onboard devices to the Cloud-Delivered Firewall Management Center, assign licenses to these devices, and configure these devices to send events directly to SAL (SaaS).
- Enable connection logging on a per-rule basis by editing a rule and choosing the **Log at Beginning of Connection** and **Log at End of Connection** options.

Procedure

1. Log in to Security Cloud Control.
2. From the left pane, click **Security Devices**.
3. Click the **Devices** tab to view the device.

4. Click the **FTD** tab to view FTD devices.
5. Choose the FTD devices whose configurations you want to edit, from the **Security Devices** list.
6. In the **Device Management** pane, click **Cloud Events**.
7. Click the **Send Events to the Cisco Cloud** toggle button to enable or disable the configuration.
8. Click **Save**.

The FTD device configuration is updated to enable or disable sending events directly to SAL (SaaS).

View AI Defense Events in Security Cloud Control

Configure AI Defense event viewing in Security Cloud Control after enabling AI Defense and cloud event logging for supported Threat Defense devices.

View AI Defense events in Security Cloud Control to monitor activities within your AI environment, including prompts submitted, responses generated, and any triggered AI Defense policy violations.

AI Defense events record activities within your AI environment. They capture interactions such as prompts submitted, responses generated, and any triggered AI Defense policy violations. Each event includes key information, such as the application and AI model involved, the specific rule triggered, and the action taken.

Before you begin

- Enable the AI Defense service in your Security Cloud Control tenant. For information on enabling the AI Defense service, see the AI Defense User Guide.
- You must be managing Firewall Threat Defense devices with Version 10.0 or higher.
- Enable your Firewall Threat Defense device to send events to the cloud. For more information, see Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection on page 544.

Follow these steps to view AI Defense events in Security Cloud Control:

Procedure

1. In the navigation pane, choose **Events & Logs** > **Events** > **Event Logging**.
2. Click the filter icon ( ).
3. Check the **AI Defense** check box.

AI Defense events are displayed in the event logging interface, showing activities within your AI environment including prompts, responses, and policy violations.

25 FTD Dashboard

Topics:

- FTD dashboard
- View the FTD dashboard
- FTD dashboard widgets
- Modify time settings for the FTD dashboard

This chapter provides information about the FTD dashboard and describes the predefined widgets that offer an overview of your system.

FTD dashboard

Describes the FTD Dashboard in Security Cloud Control, including device health, event activity, threat, network, application, and status widgets for managed Firewall Threat Defense devices.

The FTD dashboard is a monitoring interface that

- provides an at-a-glance view of the status and events data collected by all Security Cloud Control-managed Firewall Threat Defense devices
- displays collective information related to device status and overall health of devices in your deployment, and
- uses tabs with predefined widgets that provide insights into different aspects of the system.

FTD dashboard capabilities

The information that the FTD dashboard provides depends on how you license, configure, and deploy the devices in your system. The FTD dashboard displays data for all Security Cloud Control-managed Firewall Threat Defense devices, but you can choose to filter device-based data. You can also choose the time range to display for specific time range.

This dashboard uses tabs to display predefined widgets: small, self-contained components that provide insights into different aspects of the system. For example, the Network Activity widget shows you event graphs that display information about all connection, malware, and intrusion events. The widgets in the dashboard are predefined and cannot be customized. This dashboard is visible to all Security Cloud Control users who have access to a Security Cloud Control tenant.

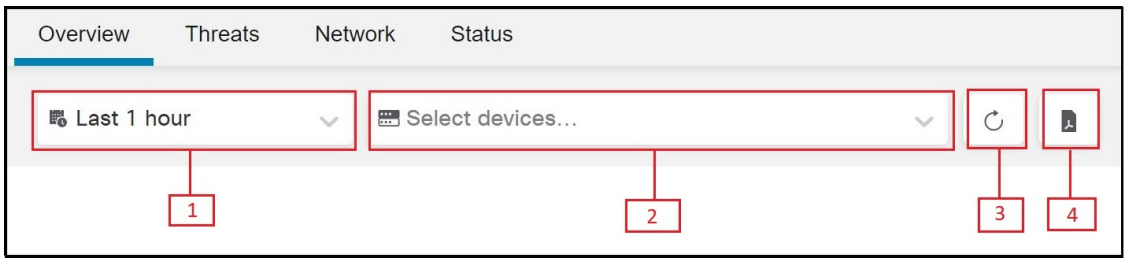
- The dashboard does not displays any event statistics for historic events.
- Since the aggregation service batch processes the events to aggregate every five minutes, you can expect a five-minute latency between the time the events are aggregated to the time the statistics are displayed.

The dashboard provides these control options:

Table 25: FTD dashboard controls

Number	Description
1	Allows you to change the time range to reflect a period as short as the last hour or as long as the last year. When you change the time range, the widgets automatically update the events data to reflect the new time range.
2	Allows you to filter the events data based on selected devices. If no devices are selected, the widgets display all available events data.
3	Reinitiates the events data query
4	Displays the events data in a PDF output format. You can choose to download or save a copy of this PDF on your local machine.

Figure 9: FTD dashboard



View the FTD dashboard

Lists the FTD Dashboard tabs and widgets available in Security Cloud Control, including Overview, Threat, Network, Applications, and Status tabs with predefined widgets.

From the Security Cloud Control menu, choose **Insights & Reports** > **Firewall Threat Defense** > **Dashboard** to view the **FTD Dashboard**.

By default, the home page for your tenant displays the **Overview** tab.

The dashboard includes widgets that are listed under each tab: Threat, Network, Applications, and Status tab.

Table 26: FTD dashboard tabs and widgets

Name of the Tab	Available Widgets
Overview	All available widgets
Threat	• Top Intrusion Rules • Top Intrusion Attackers • Top Intrusion Targets • Top Malware Signatures • Top Malware Senders • Top Malware Receivers • Malware Events by Disposition
Network	• Network Activity • Event Activity • Access Control Actions • Top Access Control Policies • Top Access Control Rules • Top Devices • Top Users • Top Users by Blocked Connections
Status	• Top Devices with Health Alerts • Top Loaded Devices

Name of the Tab	Available Widgets
Applications	• Top Web Applications • Top Client Applications • Blocked Web Applications

FTD dashboard widgets

Explains FTD dashboard widgets in Security Cloud Control, including predefined threat, network, application, and device health views for monitoring Firewall Threat Defense event and status data.

FTD dashboard widgets are predefined display components that

- provide at-a-glance views of current system status
- display data about events collected and generated by Firewall Threat Defense devices managed FMC, and
- show information about the status and overall health of the devices in your deployment.

Top intrusion rules widget

Describes a dashboard widget that displays counts of intrusion events organized by priority over a specified time range.

A Top Intrusion Rules Widget is a dashboard widget that displays counts of the intrusion events that have occurred over the specified time range and are organized by priority, includes statistics on intrusion events with dropped packets and different impacts, and provides a scrollable generated list.

Top intrusion attackers widget

Describes the Top Intrusion Attackers widget that displays event counts for the top attacking host IP addresses causing intrusion events on your monitored network.

The **Top Intrusion Attackers** widget displays counts of intrusion events for the top attacking host IP addresses (causing those events) on your monitored network.

Top intrusion targets widget

Describes a monitoring dashboard component that tracks network security events by destination IP address.

A Top Intrusion Targets widget is a dashboard component that displays counts of intrusion events for the top target host IP addresses (targeted in the connections causing those events) on your monitored network.

Top malware signatures widget

Describes a widget that shows counts of the most frequently detected malware signatures in network traffic, organized by the top file-sending host IP addresses.

The **Top Malware Signatures** widget displays counts of the top malware signatures detected in the network traffic for top file-sending host IP addresses.

Top malware senders widget

Describes the Top Malware Senders widget that displays counts of the top malware threats detected in network traffic for the highest file-sending host IP addresses.

The **Top Malware Senders** widget displays counts of the top malware threats that are detected in the network traffic for top file-sending host IP addresses.

Top malware receivers widget

Describes the Top Malware Receivers widget that displays counts of the most detected malware threats in network traffic for the highest file-receiving host IP addresses.

The **Top Malware Receivers** widget displays counts of the top malware threats that are detected in the network traffic for all top file-receiving host IP addresses.

Malware events by disposition widget

Explains the widget that displays counts of malware event dispositions when managed devices detect files containing malware.

The **Malware Events by Disposition** widget is a display component that shows counts of all disposition of malware events that are generated when the managed device detects a file containing malware.

Network activity widget

Describes the Network Activity widget that displays ingress and egress data rates based on connection event information.

The **Network Activity** widget displays all ingress and egress data rate that is based on information from the connection events.

Event activity widget

Describes the Event Activity widget, which shows counts of events that occurred in the last hour and displays the total number of each event type available in the database.

The **Event Activity** widget displays counts of events that have occurred in the last hour and the total number of each event type that is available in the database.

Access Control Actions Widget

The **Access Control Actions** widget displays counts of events that are logged based on the allowed or blocked access control actions for each event. If you hover on the pie chart, you can view the percentage of the allowed and blocked actions.

Top access control policies widget

Describes the Top Access Control Policies widget, which displays counts of the access control policies that are generating the most events in your network environment.

The **Top Access Control Policies** widget displays counts of top access control policies generating events.

Top access control rules widget

Describes a dashboard widget that displays access control rule usage statistics for network security monitoring.

The **Top Access Control Rules** widget is a dashboard component that

- displays the top five counts of the access control rules that are used for each event
- provides sorting capabilities by bytes or events, and
- helps monitor network security policy effectiveness.

Top devices widget

Describes the Top Devices widget that displays event counts per device, with sorting options available by bytes or events to help analyze network device activity.

The **Top Devices** widget displays counts of events per devices. These count can be sorted by bytes or events.

Top users widget

Explains a network monitoring widget that displays users with the highest intrusion event counts.

The **Top Users** widget is a network monitoring display that

- displays a list of users on your monitored network that are associated with the highest intrusion event counts
- draws data primarily from the intrusion detection (IDS) User Statistics and Intrusion Events tables, and
- displays authoritative user data.

Top users by blocked connections widget

Describes a widget that displays users who have the highest number of blocked connection events associated with them in your monitored network.

A **Top Users by Blocked Connections** widget is a network monitoring tool that displays users who have the highest number of blocked connection events associated with them in your monitored network.

Top devices with health alerts widget

Describes the Top Devices with Health Alerts widget that displays the current compiled health status for managed devices, providing visibility into device health conditions and alerts.

The **Top Devices with Health Alerts** widget displays the current compiled health status for Security Cloud Control-managed Firewall Threat Defense devices.

Top loaded devices widget

Describes the Top Loaded Devices widget that displays a list of devices with their corresponding CPU usage information to help monitor system performance.

The **Top Loaded Devices** widget displays a list of Secure Firewall Threat Defense devices along with the CPU usage information.

Top web applications widget

Explains the Top Web Applications widget and its functionality in network monitoring.

A Top Web Applications widget is a network monitoring interface element that displays the web applications that are associated with the highest number of connection events in your monitored network and allows you to sort this list based on bytes or event count.

Top client applications widget

Describes the Top Client Applications widget that displays the most frequently used client applications in your monitored network, with sorting options by bytes or event count.

The **Top Client Applications** widget displays the most used client applications in your monitored network. You can sort this list based on bytes or event count.

Top blocked web applications widget

Describes a widget that displays the top web applications associated with blocked connection events in your monitored network.

A **Top Blocked Web Applications** widget is a network monitoring display that shows the top web applications that are associated with blocked connection events and the count of blocked connection events in your monitored network.

Modify time settings for the FTD dashboard

Lists time range options and data point configurations for the FTD Dashboard in Security Cloud Control.

You can change the time range to reflect a period as short as the last hour (the default) or as long as the last year. When you change the time range, the widgets that can be constrained by time automatically update to reflect the new time range.

The maximum number of data points in any graph is 300, and the time setting determines how much time is summarized within each data point. These are the number of data points, and the time span covered, in the FTD dashboard for each time range:

- 1 hour = 12 data points, 5 minutes each
- 6 hours = 72 data points, 5 minutes each
- 1 day = 288 data points, 5 minutes each
- 1 week = 300 data points, 33.6 minutes each
- 2 weeks = 300 data points, 67.2 minutes each
- 30 days = 300 data points, 144 minutes each
- 90 days = 300 data points, 432 minutes each
- 180 days = 300 data points, 864 minutes each
- 1 year = 300 data points, 1752 minutes each

26 Analyze and Remediate Security Policy Anomalies with Policy Analyzer and Optimizer

Topics:

- About Policy Analyzer and Optimizer
- Common Policy Analyzer and Optimizer concepts
- Requirements: Prerequisites to use Policy Analyzer and Optimizer
- Enable Policy Analyzer and Optimizer for Security Cloud Control-managed On-Premises Firewall Management Center
- Policy Analyzer and Optimizer licensing requirements
- Open Policy Analyzer and Optimizer and select a data source
- Search and filter policies in Policy Analyzer and Optimizer
- Access control policy analysis and optimization
- Network address translation policy analysis
- Troubleshooting Policy Analyzer and Optimizer
- Frequently asked questions about Policy Analyzer and Optimizer

This chapter provides information on how to analyze security policies, detect anomalies, and provide recommendations on remediations using the Policy Analyzer and Optimizer feature in Security Cloud Control.

About Policy Analyzer and Optimizer

Explains how Policy Analyzer and Optimizer in Security Cloud Control Firewall Management analyzes access control and NAT policies, identifies rule anomalies, reports optimization opportunities, and supports remediation where available.

Policy Analyzer and Optimizer is an AgenticOps capability in Security Cloud Control Firewall Management. It evaluates firewall policy rules and identifies duplicate, shadowed, redundant, expired, mergeable, and overlapping conditions that can make a policy harder to maintain or slower to deploy.

For more information, refer to AgenticOpsInsights to know more about the various other functionalities that AgenticOps provides.

Policy Analyzer and Optimizer is an intelligent Security Cloud Control Firewall Management service that:

- supports access control policies and Network Address Translation (NAT) policies for Cloud-Delivered Firewall Management Center and supported Security Cloud Control-managed On-Premises Firewall Management Center data sources.
- analyzes firewall policies and detects rule anomalies
- helps you understand where a policy can be optimized, and

Capabilities and benefits

Secure Firewall Threat Defense devices with extensive policies may have numerous duplicate or shadowed rules. Such large policies with unoptimized rulesets can lead to excessive consumption of device memory, delayed loading of rules, and long search duration, resulting in inefficient security policy enforcement, reduced network speeds, and extended deployment durations.

Policy Analyzer and Optimizer can perform these functions:

- View policy health and optimization opportunities for the selected management center data source.
- Analyze policies on demand or rely on scheduled analysis that runs every 24 hours.
- Download analysis reports as PDFs after analysis completes.
- Use Access Control Policy Analyzer and Optimizer remediation workflows where supported.
- Use Network Address Translation Policy Analyzer and Optimizer findings and AgenticOps insights to investigate NAT policies that contain optimizable rules.
- Stage and apply remediation for an entire anomaly category, selected observations, or individual rules within supported observations.

Table 27: Supported policy types for Policy Analyzer and Optimizer

Policy type	Use this section when	Current scope
Access control policy	You want to analyze access control policies, review access control findings, and apply supported remediations.	Analysis, remediation, reporting, remediation history, and policy insights.
Network address translation policy	You want to analyze NAT policies for shadowed and redundant NAT rules.	Analysis and reporting for fully shadowed and fully redundant NAT rules. NAT remediation is not available in this release.

Common Policy Analyzer and Optimizer concepts

Lists details about common Policy Analyzer and Optimizer concepts. Policy Analyzer and Optimizer uses these shared concepts across access control policy analysis and NAT policy analysis.

Policy Analyzer and Optimizer uses these shared concepts across access control policy analysis and NAT policy analysis.

Table 28: Common Policy Analyzer and Optimizer concepts

Concept	Common behavior	Policy-type difference
Data source	A Cloud-Delivered Firewall Management Center or an On-Premises Firewall Management Center selected in Policy Analyzer and Optimizer.	The Access Control tab can be used for supported On-Premises Firewall Management Center data sources. The Network Address Translation tab is available only when Network Address Translation Policy Analyzer and Optimizer is enabled through AgenticOps for the selected data source.
Sync	Fetches current policy inventory and metadata, including newly created, deleted, or modified policies.	Sync does not, by itself, create a new analysis summary. If the policy changed after the last analysis, run analysis again or wait for scheduled analysis.
Analysis	Evaluates selected policies and produces policy health information, observations, and report data.	Access control Policy Analyzer and Optimizer evaluates access control rule and object findings. Network Address Translation Policy Analyzer and Optimizer evaluates NAT rule shadowing and redundancy.
Reporting	Provides a downloadable analysis report after analysis completes.	Access control Policy Analyzer and Optimizer also provides remediation reports after supported remediation is applied.

Concept	Common behavior	Policy-type difference
Remediation	A workflow that stages selected changes and applies them only when you select Apply Remediation.	Available for access control policies. Network Address Translation Policy Analyzer and Optimizer does not provide an Apply Remediation workflow. You can stage remediation for an entire anomaly category, selected observations within a category, or individual rules within an expanded observation. You can also select individual rules within an expanded observation. Using the suggested remediations, you can disable or delete selected Duplicate Rules and Expired Rules, remove selected fully overlapped objects from rules, and merge selected Mergeable Rules.

Requirements: Prerequisites to use Policy Analyzer and Optimizer

Outlines the prerequisites that apply to your policy type and data source before using Policy Analyzer and Optimizer.

General prerequisites

Before you use Policy Analyzer and Optimizer, verify the prerequisites that apply to your policy type and data source.

- Integrate each On-Premises Firewall Management Center with Security Cloud Control.

> **Note**
>
> In the On-Premises Firewall Management Center, navigate to **Integration > Cisco Security Cloud** and check the **Enable Policy Analysis & Optimization** checkbox after integrating with the Cisco Security Cloud.

AgenticOps onboarding requirements

Policy Analyzer and Optimizer access depends on the customer state and whether onboarding is complete.

Customer and onboarding state	Policy Analyzer and Optimizer access	Required action
New customer and AgenticOps is not onboarded	Policy analysis and optimization are unavailable. Selecting the analysis action opens an AgenticOps onboarding prompt.	Onboard AgenticOps for the organization and the selected management center data source.

Customer and onboarding state	Policy Analyzer and Optimizer access	Required action
Existing customer during the grace period	Manual and scheduled analysis, existing results, and remediation history remain available. Security Cloud Control displays the deadline or remaining time.	Complete AgenticOps onboarding before the displayed deadline to prevent an interruption.
Existing customer after the grace period	New manual and scheduled analyses are blocked. Existing analysis and remediation data is retained.	Complete AgenticOps onboarding to restore policy analysis. You can onboard after the grace period ends.
AgenticOps is onboarded	Policy Analyzer and Optimizer analyzes supported policies and displays available results normally.	No onboarding action is required.

Management Center interface behavior

The management center interface determines where onboarding, grace-period, and blocked-state information appears.

Data source interface	During the grace period	After the grace period
Cloud-Delivered Firewall Management Center	Policy Analyzer and Optimizer remains available. A banner or onboarding action directs you to Security Cloud Control.	The interface displays an onboarding prompt and directs you to Security Cloud Control. New analysis is unavailable.
On-Premises Firewall Management Center Version 10.5 or later	The newer interface displays the AgenticOps banner and onboarding action while analysis remains available.	The interface displays the AgenticOps onboarding action. New analysis is unavailable.
On-Premises Firewall Management Center Versions 7.6 through 10.4.x	Analysis continues. Grace-period information appears after you cross-launch to Security Cloud Control.	The local interface can show Analysis changes pending in **Last Analyzed** and return a generic analysis error. Select the optimizable percentage to cross-launch and onboard AgenticOps.
On-Premises Firewall Management Center Versions 7.2 through 7.5.x	The management center has no local Policy Analyzer and Optimizer interface. Use Security Cloud Control to view policies and the grace-period information.	Use Security Cloud Control to review the onboarding requirement and onboard AgenticOps.

Access control policy prerequisites

Verify these access control policy requirements.

- Access control policy analysis is supported on the On-Premises Firewall Management Center operating on Version 7.2 or later. The Cisco-recommended Version is 7.6 or later, because these versions support cross-launch to Policy Analyzer and Optimizer directly from On-Premises Firewall Management Center.
- Access control policy to be analyzed must be associated with a Firewall Threat Defense device that is managed by an On-Premises Firewall Management Center integrated with Security Cloud Control.
- The policy is synchronized to Security Cloud Control and appears on the Access Control page.

Network address translation prerequisites

Verify these NAT policy requirements: NAT policy analysis requires specific version requirements and AgenticOps enablement.

- The On-Premises Firewall Management Center runs Version 7.6 or later.
- NAT policy analysis is supported on the On-Premises Firewall Management Center operating on Version 7.6 or later. For more information, refer to Enable AgenticOps Insights.
- AgenticOps is onboarded for the organization and the selected management center data source, or an existing-customer grace period is active.
- Enable AgenticOps for the Cloud-Delivered Firewall Management Center or On-Premises Firewall Management Center data source that you want to analyze. Choose **Insights & Reports** > **Settings** > **Policy Analyzer and Optimizer** > **Data Sources** and enable AgenticOps for the management center you want.
- The NAT rules to be analyzed are enabled. Policy Analyzer and Optimizer excludes disabled NAT rules.

If an On-Premises Firewall Management Center is running a version earlier than 7.6, access control Policy Analyzer and Optimizer may still be available for analyzing access control policy, but Network Address Translation Policy Analyzer and Optimizer is not available for that data source.

Enable Policy Analyzer and Optimizer for Security Cloud Control-managed On-Premises Firewall Management Center

Explains how to integrate an On-Premises Firewall Management Center with Security Cloud Control and complete the AgenticOps requirement for policy analysis.

This task enables Policy Analyzer and Optimizer functionality for your On-Premises Firewall Management Center to provide policy analysis and optimization capabilities through Security Cloud Control.

Onboard your On-Premises Firewall Management Center to Security Cloud Control, navigate to **Administration** > **Integrations** > **Firewall Management Center**, select the On-Premises Firewall Management Center, and choose **Policy Analyzer and Optimizer** under **System** in the right pane. See Onboard an On-Premises Firewall Management Center for more information.

If you have an On-Premises Firewall Management Center Version 7.6 and want to use Policy Analyzer and Optimizer, follow these steps:

Procedure

1. In your On-Premises Firewall Management Center, navigate **Integration** > **Security Cloud Control**.
2. If you have not integrated your On-Premises Firewall Management Center with Cisco Security Cloud, click **Enable Security Cloud Control** and follow the steps. To authorize the cloud integration, you must choose an existing Security Cloud Control tenant or provision a new one, to which your On-Premises Firewall Management Center will get onboarded, after the cloud integration is successful.
3. After integrating your On-Premises Firewall Management Center with Security Cloud Control, check the **Enable Policy Analyzer and Optimizer** checkbox and click **Save**.

Policy Analyzer and Optimizer licensing requirements

Describes the licensing requirements for Policy Analyzer and Optimizer, which requires no additional licensing and is included as part of the base subscription.

Policy Analyzer and Optimizer requires no additional licensing. It comes as part of the Security Cloud Control Firewall Management base subscription.

An On-Premises Firewall Management Center customer can use Policy Analyzer and Optimizer through an existing Security Cloud Control organization or a tenant provisioned during Cisco Security Cloud integration without purchasing the Security Cloud Control Firewall Management base license. Other Security Cloud Control Firewall Management capabilities can require the base subscription and applicable device licenses.

Open Policy Analyzer and Optimizer and select a data source

Configure access to Policy Analyzer and Optimizer from Security Cloud Control Firewall Management or cross-launch from supported On-Premises Firewall Management Center policy pages.

Use this task to access policy analysis and optimization capabilities for your firewall management systems.

You can open Policy Analyzer and Optimizer from Security Cloud Control Firewall Management or cross-launch from supported On-Premises Firewall Management Center policy pages.

Follow these steps to open Policy Analyzer and Optimizer and select a data source:

Procedure

1. In the Security Cloud Control Firewall Management left pane, choose **Administration** > **Integrations** > **Firewall Management Center**.
2. Select **Cloud-Delivered FMC** or an On-Premises Firewall Management Center.
3. Click Policy Analyzer and Optimizer under **System**.

   Note

   Alternatively, choose **Insights & Reports** > **Policy Analyzer and Optimizer**.

4. Use the data source selector at the top of the Policy Analyzer and Optimizer page to choose the Cloud-Delivered Firewall Management Center or On-Premises Firewall Management Center whose policies you want to review.
5. Choose the **Access Control** tab depending on the policy type that you want to analyze.

   Note

   If the selected data source is not enabled for AgenticOps, the **Network address translation** tab shows a message indicating that the NAT Policy Analyzer and Optimizer require AgenticOps for the selected data source. However, you can still utilize the access control Policy Analyzer and Optimizer if the access control prerequisites are met.

Sync and analysis behavior

Explains how Policy Analyzer and Optimizer displays policy metadata and manages synchronization with management centers.

Sync and analysis behavior is a Policy Analyzer and Optimizer functionality that

- displays policy metadata, including analysis status, last modified time, and last analyzed time

- tracks when policies were last modified in the management center and when analysis was last performed, and
- provides synchronization capabilities to fetch the latest policy inventories from management centers.

Policy metadata and synchronization details

Policy Analyzer and Optimizer displays policy metadata, including analysis status, last modified time, and last analyzed time. Last modified reflects changes made to the policy in the management center that manages it. Last analyzed reflects the analysis run that produced the current Policy Analyzer and Optimizer summary.

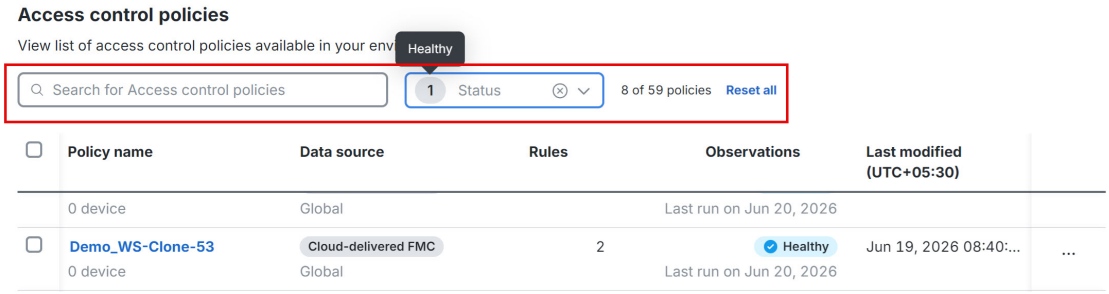
Use **Sync with FMC** to fetch the latest access control and NAT policy inventories and modified timestamps from the management center. Each Policy Analyzer and Optimizer tab shows the sync success or failure status for the policy type on that tab. If a policy was modified after the last analysis, the displayed analysis can be out of date until you run analysis again or a scheduled analysis runs.

Search and filter policies in Policy Analyzer and Optimizer

Provides the Search for access control policies field and the Status field to narrow the access control policy list.

Use the **Search for access control policies** field and the **Status** field to narrow the access control policy list.

Search helps you find a policy by name. Status filtering helps you find policies by analysis state, such a **Healthy**, **Error**, **In progress**, **Analysis pending**, **Optimizable**, or **Analysis out of date**.



- **Search for access control policies**: Finds access control policies that match the policy name you enter.
- **Status**: Filters access control policies by their current analysis state.

Access control policy analysis and optimization

Explains how to analyze access control policies in Policy Analyzer and Optimizer, review findings, and apply supported remediations for access control rules and objects.

Access control policy analysis and optimization is a security management process that

- analyzes access control policies using the **Access Control** tab
- reviews access control policy findings, and
- applies remediations that Policy Analyzer and Optimizer supports for access control rules and objects.

Prerequisites

After provisioning a Cloud-Delivered Firewall Management Center or onboarding an On-Premises Firewall Management Center to your Security Cloud Control Firewall Management organization and creating policies, you can start analyzing them using the Policy Analyzer and Optimizer.

For more information, refer to Onboard an On-Premises Firewall Management Center and Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control.

Analyze access control policies

Configure the Policy Analyzer and Optimizer to assess an access control policy before making changes or review policy health.

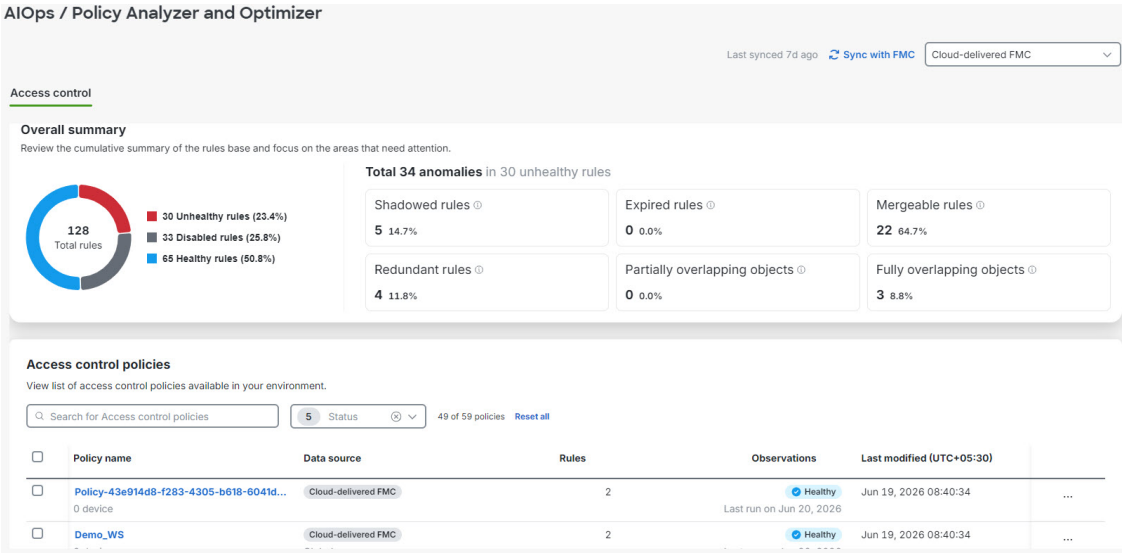
This task allows you to assess an access control policy before making changes, review policy health, or re-run analysis after policy updates.

If a policy has not been analyzed, you can start a new analysis. If the analysis is out of date, you can re-analyze the policy to refresh the results.

> **Note**
>
> When you create a new policy, it might take a while for the Policy Analyzer and Optimizer to fetch the policy details and show up on the **Policy Analyzer and Optimizer**. Click the refresh ( ) button on the top-right corner to manually refresh the page to see new policies.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Insights & Reports** > **Policy Analyzer and Optimizer**.



3. In the right pane, select **Cloud-delivered FMC** or an On-Premises Firewall Management Center from the drop-down list as the data source whose policies you wish to analyze.
4. In the **Access Control** area, select the policy you want to analyze or review.

> **Note**
>
> - For an unanalyzed policy, click on **Analyze Policies**.
> - If the policy status indicates **Analysis out of date**, click on **Re-analyze Policy** under **Analysis Actions** on the right.

The **Overall summary** section displays the total number of rules categorized by their health status: healthy, disabled, or unhealthy, for the selected management center (Cloud-Delivered Firewall Management Center or On-Premises Firewall Management Center).

The dashboard also highlights specific anomalies within your unhealthy rules. You can review the count and percentage for the categories: Shadowed rules, Expired rules, Mergeable rules, Redundant rules, Partially overlapping rules, Fully overlapping objects.

The Policy Analyzer and Optimizer displays the analysis results, showing rule health status and identifying any policy anomalies that require attention.

Access control policy analysis summaries

Describes the summary information displayed after access control policy analysis completes.

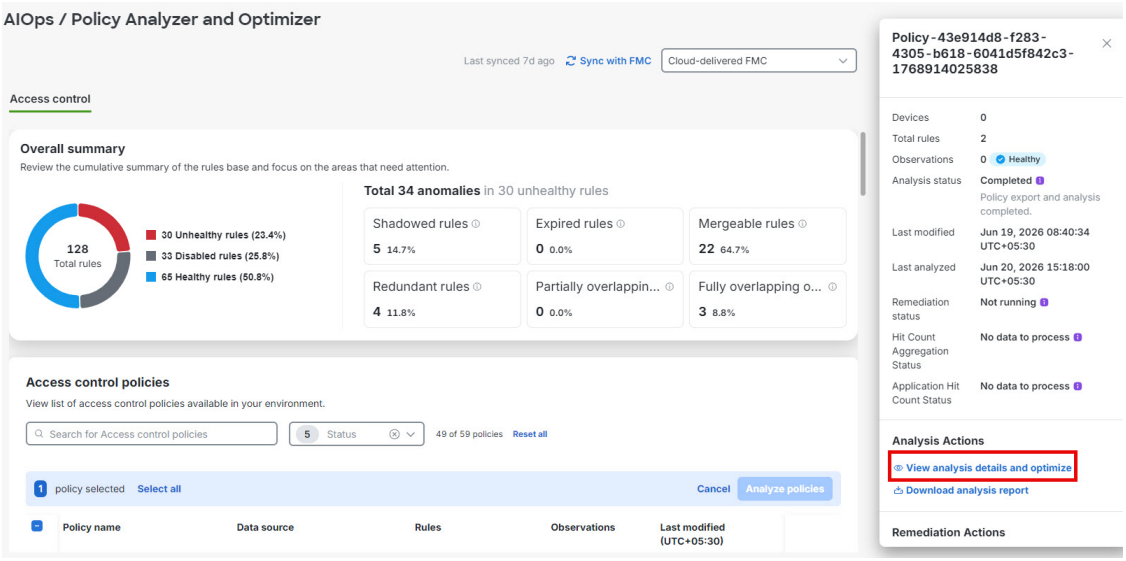
An access control policy analysis summary is a dashboard that

- provides insights on rule health, usage, and anomalies through visual representations
- displays right-pane summary information when you select a policy, and
- enables access to detailed analysis and optimization options.

Policy analysis summary components

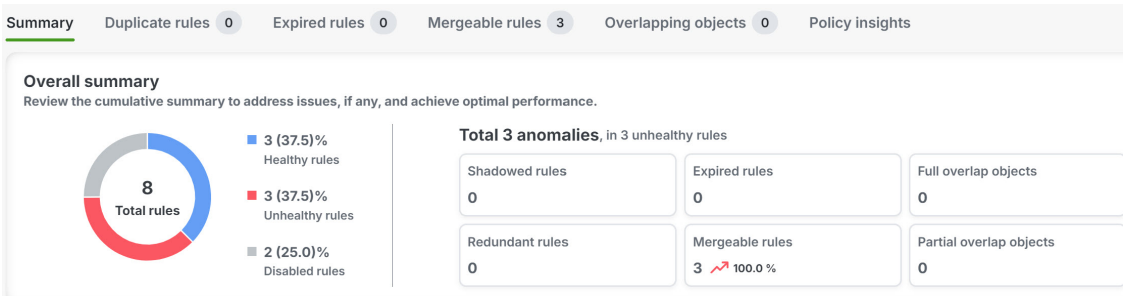
When analysis completes, select an access control policy to review the right-pane summary and click **View analysis details and optimize**.

Alternatively, you can click the ellipse button associated with a policy and select **View details** to see the right-pane summary.



The analysis summary includes these components:

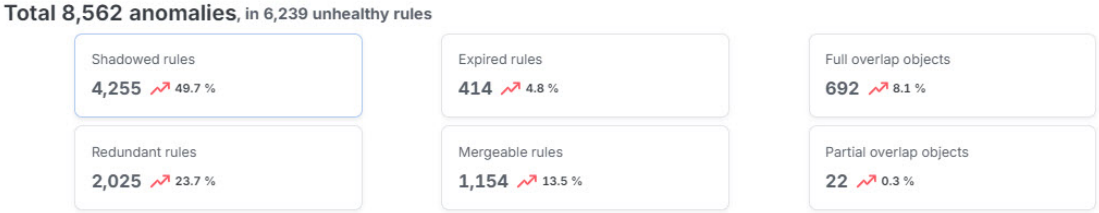
- **Overall summary**: Provides insights on how many rules are healthy, disabled, expired, and contain anomalies, using a pie chart for the selected access control policy. You can also hover over the part of the pie to view the percentage of rules.



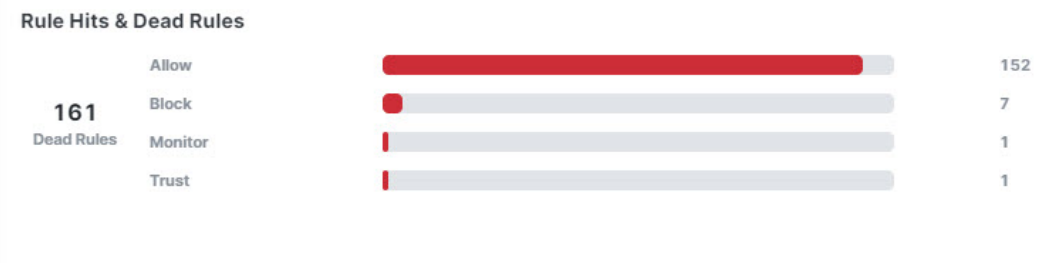
- **Rule usage history**: Shows how recently rules were used, with time periods.



- **Rules with Anomalies**: Provides insights on how many rules have anomalies.



- **Hits rules & dead rules**: Provides insights on hitcount of expired rules, for rule types including allow, block, monitor, and trust.



In remediation tabs such as **Duplicate rules**, **Expired rules**, **Mergeable rules**, **Overlapping objects**, and **Policy insights** you can select the check box next to a category to stage all observations in that category, or expand the category and select specific observations or rules. Available actions depend on the anomaly type.

Duplicate rules in access control policy

Explains duplicate rules that are detected in access control policies and how to remediate them.

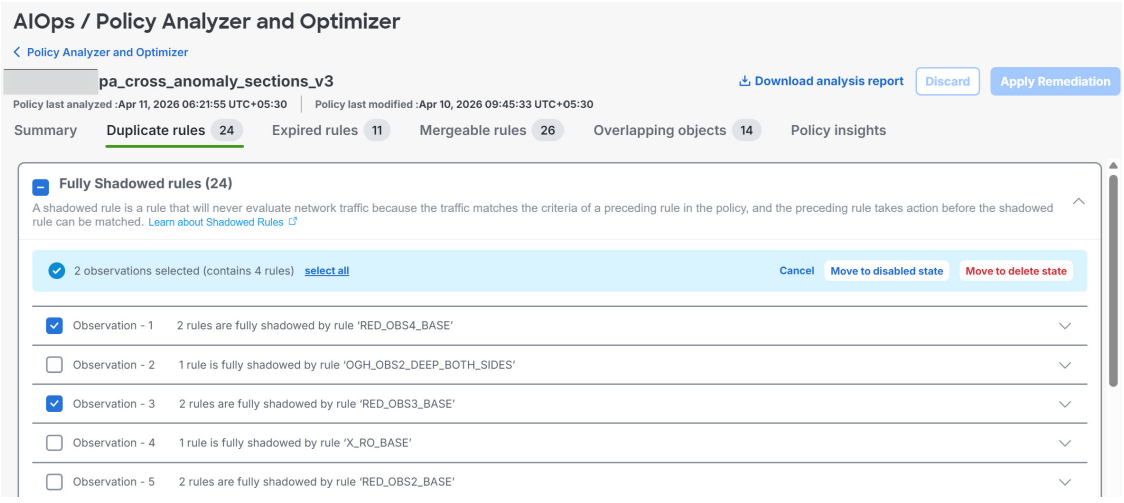
Duplicate rules are access control policy rules that

- are shadowed or redundant rules with anomalies detected by analysis
- include fully shadowed rules that will never evaluate network traffic because another rule that precedes it overshadows this rule, and
- include fully redundant rules that are part of another larger rule, such that removing this redundant rule does not impact network traffic.

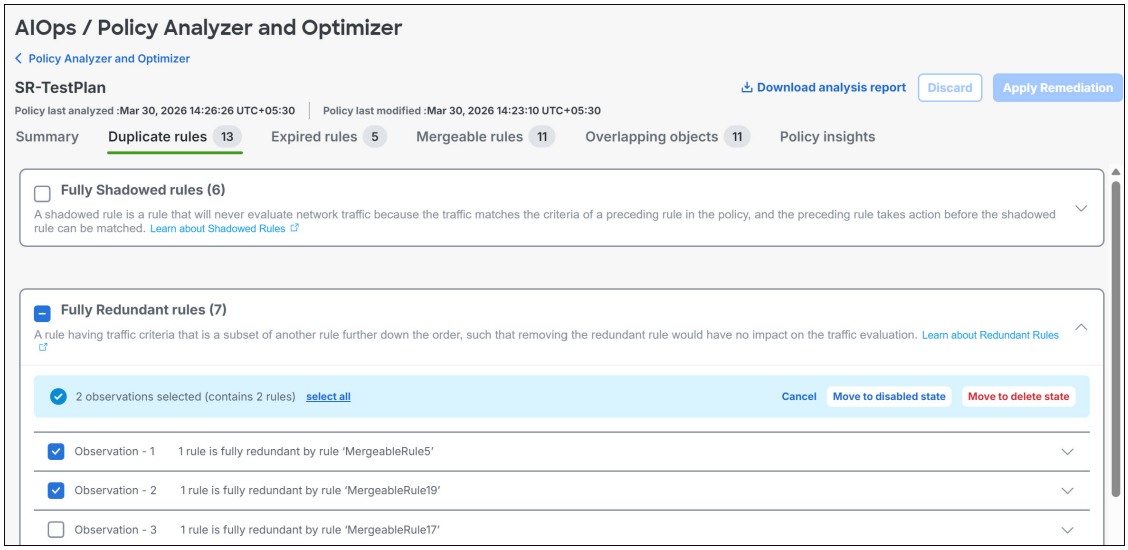
Duplicate rule analysis

The **Duplicate Rules** tab lists shadowed and redundant rules with anomalies:

- A **Fully Shadowed rules** is one that will never evaluate network traffic because another rule that precedes it over shadows this rule.



- A **Fully Redundant rules** is one that is just a part of another larger rule, such that removing this redundant rule does not have an impact on the network traffic, because the traffic evaluation that this rule must perform is already performed by another rule.



You can remediate all duplicate-rule observations in a category, selected fully shadowed or fully redundant observations, or individual rules within an expanded observation. For selected duplicate rules, choose **Move to disabled state** or **Move to delete state**. Disable rules first when you want to measure the impact before deleting them.

> **Note**
>
> Expand each observation to review the affected rules before you stage a remediation. Each rule in the list is displayed with a set of attributes; click the settings button on the top right to select which rule attributes you want to display along with the rule.

When duplicate-rule remediation removes shadowed or redundant rules and retains a base rule, Policy Analyzer and Optimizer adds a standardized comment to the retained rule. The comment identifies the retained rule and the removed rules, which helps you audit the cleanup.

After you stage the selected duplicate-rule remediations, you can still **Undo** them before clicking **Apply Remediation**. It is recommended that you disable rules first to measure the impact and delete them later, because deleting them permanently removes them.

You can enable the disabled rules any time by navigating to the Cloud-Delivered Firewall Management Center or the On-Premises Firewall Management Center on which the rules are present.

Analyze expired rules in access control policy

Explains how to analyze and remediate expired rules in access control policies using the Expired Rules tab.

Analyzing expired rules in access control policy is a policy management feature that

- lists rules that were configured with a time range and the time range has expired
- provides rule information such as the date on which the rule expired, hit count, last hit time, and the time range, and
- enables remediation of expired rule observations through selective actions.

Expired rules remediation options

You can remediate expired rules using these methods:

- All expired-rule observations in the category

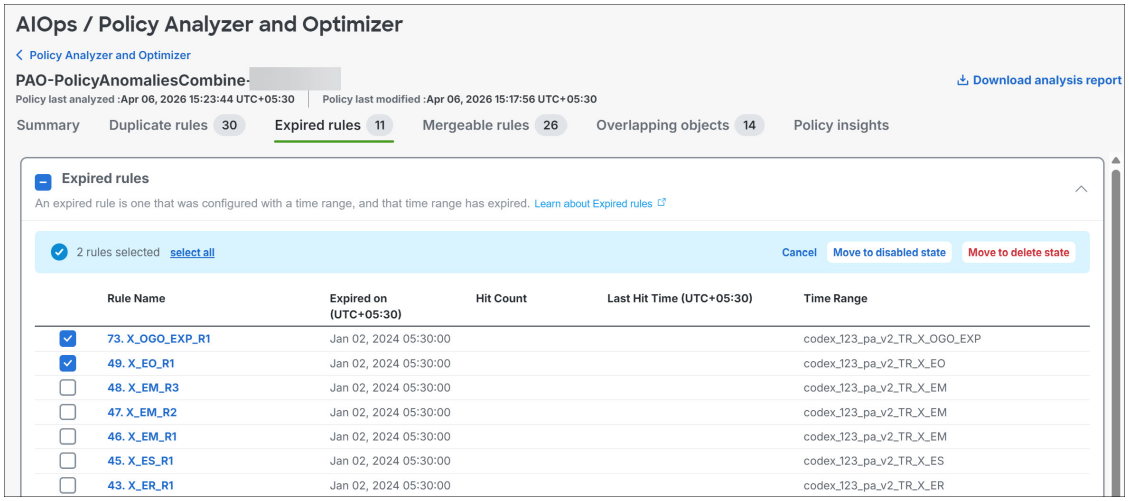
- Selected expired-rule observations
- Selected expired rules

For selected expired rules, you can choose these actions:

- **Move to disabled state**
- **Move to delete state**

> **Note**
>
> Only selected rules are changed when you apply remediation.

The **Expired Rules** tab displays this information in the interface.



Mergeable rules in access control policy

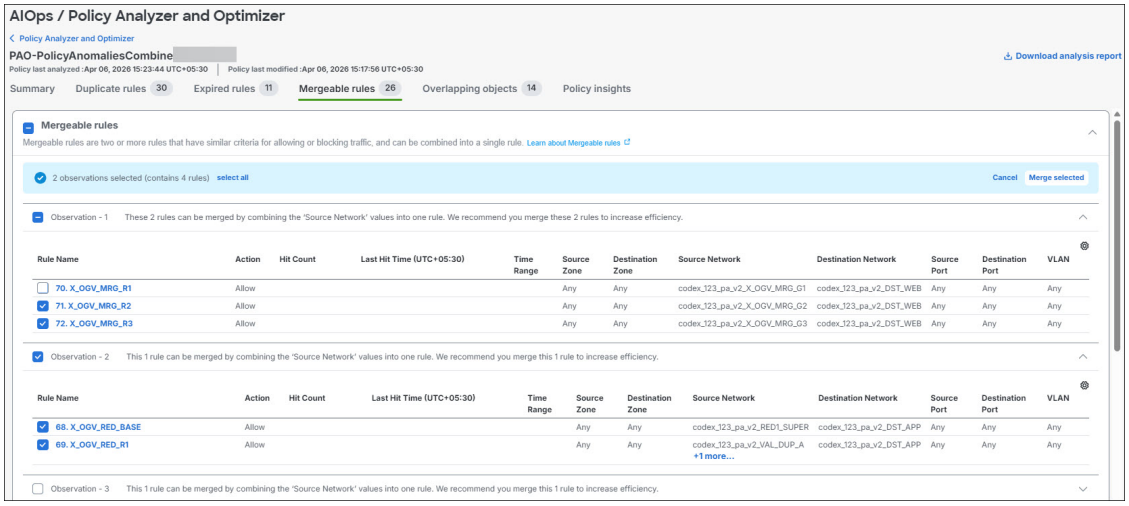
Explains the mergeable rules feature that identifies and consolidates similar access control policy rules to optimize policy management.

Mergeable rules are access control policy rules that

- have similar allow and block settings
- can be consolidated into a single rule to optimize policy management, and
- are identified and listed in the **Mergeable Rules** tab for review and remediation.

Mergeable rules management process

You can review the mergeable-rule observations and stage remediation for the entire category, selected observations, or individual rules within an expanded observation. Click **Merge Selected** to merge only the staged items. Unselected mergeable-rule observations remain unchanged until you stage and apply remediation for them.



Note

When you select individual rules to merge, select only consecutive rules. The first selected rule in the sequence is updated with the merged rule criteria, and the remaining selected rules are removed. You can start the merge from any rule in a consecutive set. The first rule in the observation does not need to be selected.

Overlapping objects in access control policy

Explains overlapping objects in access control policy that can be analyzed and remediated to optimize rule configuration.

Overlapping objects in access control policy are network objects that

- contain IP addresses or port numbers that are either the same or a complete subset (fully overlapping)
- contain some subset of repeated IP addresses but not all (partially overlapping), and
- are listed in the **Overlapping Objects** tab for analysis and remediation.

Overlapping object types and remediation

The system identifies two types of overlapping objects:

- **Fully overlapping objects**: Objects where the IP addresses or port numbers are either the same or a complete subset. For example, if a rule contains an object for 192.168.1.1 and another for 192.168.1.0/24, the 192.168.1.1 object is fully overlapped by the other object and is not needed in the rule.
- **Partially overlapping objects**: Objects where some subset of IP addresses are repeated, but not all addresses overlap.

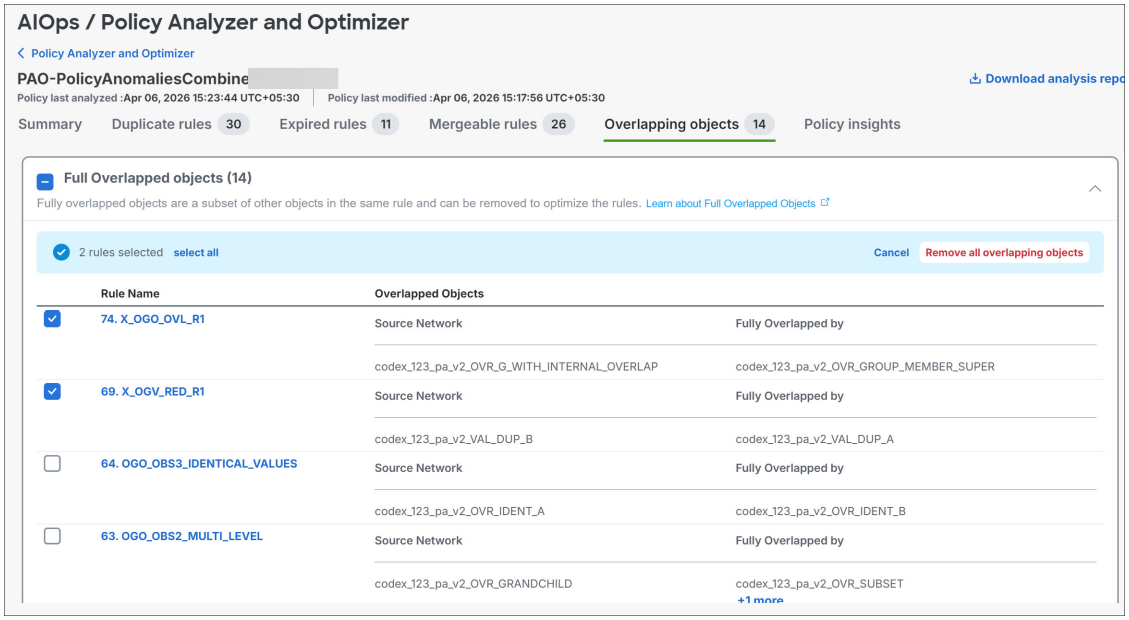
For fully overlapped objects, you can remediate all fully overlapped observations in the category, selected observations, or selected rules. Click **Remove All Fully Overlapped Objects from Rules** to remove fully overlapped objects only from the staged items.

For partial overlaps, you need to evaluate each occurrence, determine if any changes can be made, and implement those changes directly by editing the objects.

Fully overlapping objects analysis

This example shows the analysis interface for fully overlapping objects:

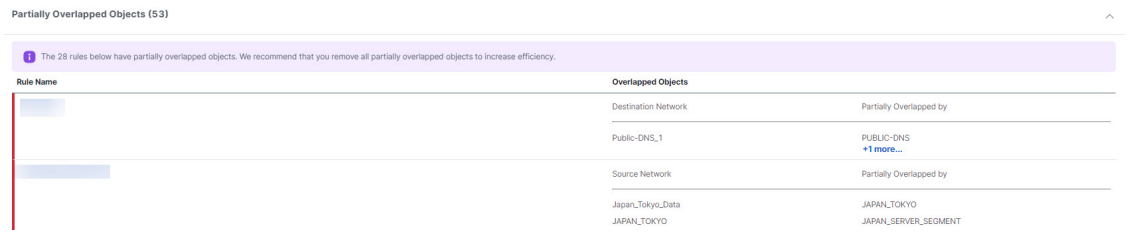
Figure 10: Fully overlapping objects interface



Partially overlapping objects analysis

This example shows the analysis interface for partially overlapping objects:

Figure 11: Partially overlapping objects interface



Policy insights in access control policy

Describes the analysis capabilities for access control policy rules using hit count data and filtering options to optimize policy performance.

Policy insights in access control policy is a monitoring feature that

- tracks rule usage through hit count information from all devices assigned to the policy
- provides filtering capabilities based on actions, hit information, and time periods, and
- enables rule management through disable or delete operations for unused or underutilized rules.

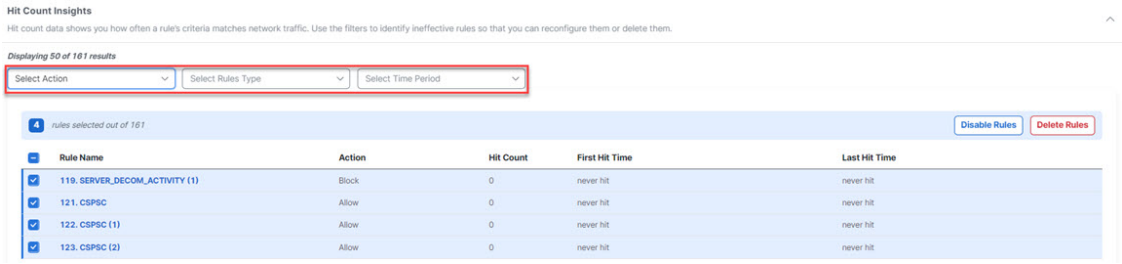
Policy insights filtering options

The **Policy Insights** tab has a **Hit Count** section that initially lists any rules that have never been triggered (**Never Hit Rules**). The hit count information is from all devices that are assigned to the policy. You can change criteria and see other hit count information, for example, **Not Hit Rules** for the past six months, or **Hit Rules** over a selected time period. You can filter the rules using the actions set in the rules, hit information, and time period:

- **Never Hit Rules**–Rules that have never been hit from the time they were created.
- **Hit Rules**–Rules that have been hit in the selected time period.
- **Not Hit Rules**–Rules that have not been hit in the selected time period.

Select the rules that you want to disable or delete, and select **Disable Rules** or **Delete Rules**. These changes are staged until you select **Apply Remediation**. First, disable the rules when you want to measure their impact before deleting them.

Figure 12: Policy insights interface



Access control policy remediation

Configure remediation for access control policy anomalies by staging and applying changes to fix identified issues.

Apply remediation to fix access control policy anomalies that were identified during policy analysis. This process helps optimize policy performance by addressing issues such as unused rules, shadowed rules, and overlapping objects.

Policy Analyzer and Optimizer stages remediation changes before it updates the policy. You can stage remediation for an entire anomaly category, selected observations, or individual rules within an expanded observation. Before you apply remediation, unselected observations and rules remain unchanged and available for later selection in the same analysis report.

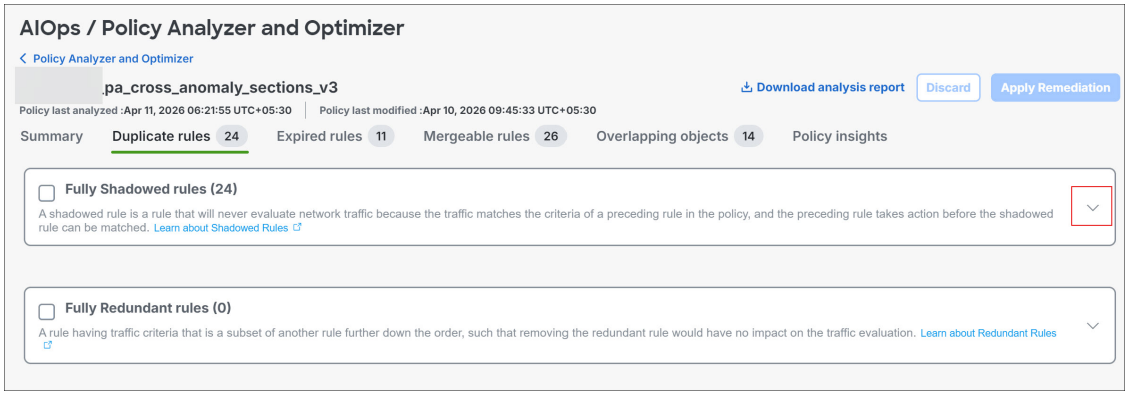
Review staged changes before you select **Apply Remediation**. After you apply remediation, you cannot apply more changes from the same analysis report. To remediate remaining anomalies, run policy analysis again on the updated policy and use the new report.

Before you begin

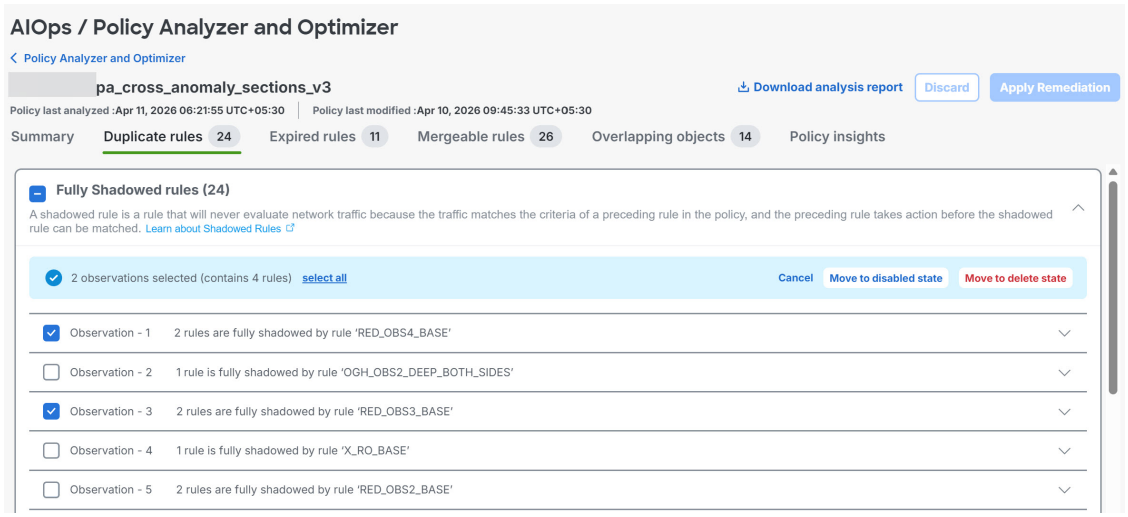
- Back up all policies before you apply remediation.
- Ensure that at least one remediation is staged. If no remediation is staged, **Apply Remediation** is disabled.
- Verify the **Policy Last Modified** and **Policy Last Analyzed** timestamps, and review the number of rules that are staged for remediation.

Procedure

1. In the **Policy Analyzer and Optimizer** page, select the policy to see details about the analysis on the right pane and click **View analysis details & optimize**.
2. Click the remediation tab that contains the anomalies that you want to fix.
3. Expand a remediation category. Select the check box for the category to stage all observations, or select the check boxes for specific observations or rules to stage only those items. Repeat this step in other remediation tabs, as needed.



4. Select the remediation action that applies to the staged items, such as **Move to disabled state**, **Move to delete state**, **Merge Selected**, **Remove All Fully Overlapped Objects from Rules**, **Disable Rules**, or **Delete Rules**.



5. Review the staged remediation. If you need to change the staged remediation before applying it, use the available undo or discard action.
6. Click **Apply Remediation**.
7. Read the confirmation message, which summarizes the remediations that will be applied. Confirm that the selected policy and staged remediation are correct.
8. Click **Apply**.

> **Note**
>
> For an On-Premises Firewall Management Center in which the Change Management Workflow is enabled, when policy remediations are applied, an internal workflow ticket is created and the changes are staged. The changes take effect only when the ticket is submitted or approved. See Change Management in *Cisco Secure Firewall Management Center Administration Guide* for more information.

After remediation is complete, the selected rules are updated. Policy Analyzer and Optimizer automatically analyzes the updated policy and generates a refreshed summary that shows any remaining issues. Verify the intended changes in the corresponding access control policy.

Download access control analysis report

Download a PDF summary report that contains completed remediations for a selected access control policy.

The access control analysis report provides a PDF summary of completed remediations for a selected policy. It includes only the remediation categories that apply to the changes you selected and applied.

Each section lists the rule name, remediation action, and related comments. For example, if no duplicate rules were remediated, the report excludes the duplicate-rule remediation section.

The report includes only the remediation sections and rule details for remediations that you selected and applied. Unselected anomalies are not included in the report.

Procedure

1. In the Policy Analyzer and Optimizer page, click **Access control**.
2. Select an access control policy, and in the right pane, click **Download analysis report**.

The report can include these sections:

- Remediation Summary
- Hit Count Remediation
- Expired Rules Remediation
- Duplicate Rules Remediation
- Mergeable Rules Remediation

Note

To determine whether a policy is remediated by the Policy Analyzer and Optimizer, navigate to **Policies** > **Access Policies** and edit a policy to view the rules in the **Policy Editor**. When a policy is remediated, a comment is added to the rules that are optimized.

You can also filter all the optimized rules using "updated by Policy Analyzer and Optimizer" to view all the remediated rules.

During duplicate rule remediation, the retained rule is updated with a comment specifying which rule was preserved and which were removed.

Network address translation policy analysis

Explains how to analyze NAT policies in Policy Analyzer and Optimizer, identify shadowed or redundant rules, review conflict ownership, and download NAT analysis reports.

Network Address Translation policy analysis is a security management capability that

- analyzes NAT policies to find rules that are shadowed or redundant
- helps identify rules that are not contributing to effective NAT behavior
- provides understanding of which rule owns the conflict, and

- enables downloading of NAT analysis reports for review.

NAT Policy Analyzer and Optimizer requirements

NAT Policy Analyzer and Optimizer has these requirements:

- NAT Policy Analyzer and Optimizer is available only when AIOps is enabled for the tenant and for the selected data source.
- For On-Premises Firewall Management Center, NAT Policy Analyzer and Optimizer requires Version 7.6 or later.
- If NAT Policy Analyzer and Optimizer is disabled in AIOps settings, NAT Policy Analyzer and Optimizer operations are blocked for all data sources.
- When AIOps is enabled for a data source, Policy Analyzer and Optimizer initiates the initial NAT synchronization and analysis for onboarded data sources.
- NAT Policy Analyzer and Optimizer performs analysis at the management center level, not on a per-device basis.

> **Note**
>
> Disabled NAT rules are excluded from being analyzed by the Policy Analyzer and Optimizer.

NAT policy analysis

Explains how Network Address Translation policy optimization and analysis categorizes NAT findings into shadowed rules and redundant rules.

NAT policy analysis is a security optimization feature that

- analyzes Cloud-Delivered Firewall Management Center and On-Premises Firewall Management Center NAT policies
- categorizes NAT findings into shadowed rules and redundant rules, and
- uses Policy Analyzer and Optimizer to optimize network address translation configurations.

NAT finding types

NAT Policy Analyzer and Optimizer reports these NAT finding types.

Table 29: NAT finding types and meanings

NAT finding	Meaning	How to interpret it
Shadowed NAT rule	A rule that will never evaluate network traffic because another rule that precedes it over shadows this rule.	Review the shadowing rule and the shadowed rules together. A rule is marked shadowed only when the overlap is complete for the compared dimensions.
Redundant NAT rule	A rule can be removed without changing the final NAT behavior because another rule can handle the traffic with the same effective NAT action.	Policy Analyzer and Optimizer checks the translated action for redundancy. Matching traffic criteria alone is not enough when translated source, destination, service, or PAT behavior differs.

NAT rule sections and comparison behavior

Lists the NAT rule sections and their comparison behavior in NAT Policy Analyzer and Optimizer.

NAT Policy Analyzer and Optimizer follows the high-level NAT evaluation model used by Cisco Secure Firewall NAT policies. NAT rules are evaluated in section order: Manual NAT before Auto NAT, Auto NAT, and Manual NAT after Auto NAT.

The NAT section determines the rule comparisons that can be reported by NAT Policy Analyzer and Optimizer.

NAT section	What it contains	NAT Policy Analyzer and Optimizer comparison behavior
Manual NAT before Auto NAT	Manual or twice NAT rules evaluated before Auto NAT.	Rules in this section can be compared with rules in the same section, Auto NAT, and Manual NAT after Auto NAT.
Auto NAT	Object NAT rules whose device order is determined internally.	Auto NAT rules can participate in comparisons with Manual NAT before or after sections. NAT Policy Analyzer and Optimizer does not report shadowed or redundant rules within the same Auto NAT section.
Manual NAT after Auto NAT	Manual or twice NAT rules evaluated after Auto NAT.	Rules in this section can be compared with rules in the same section and with rules from earlier comparable sections.

Supported NAT address families for Policy Analyzer and Optimizer

Lists the NAT address family flows supported by Policy Analyzer and Optimizer.

NAT Policy Analyzer and Optimizer supports these address-family flows.

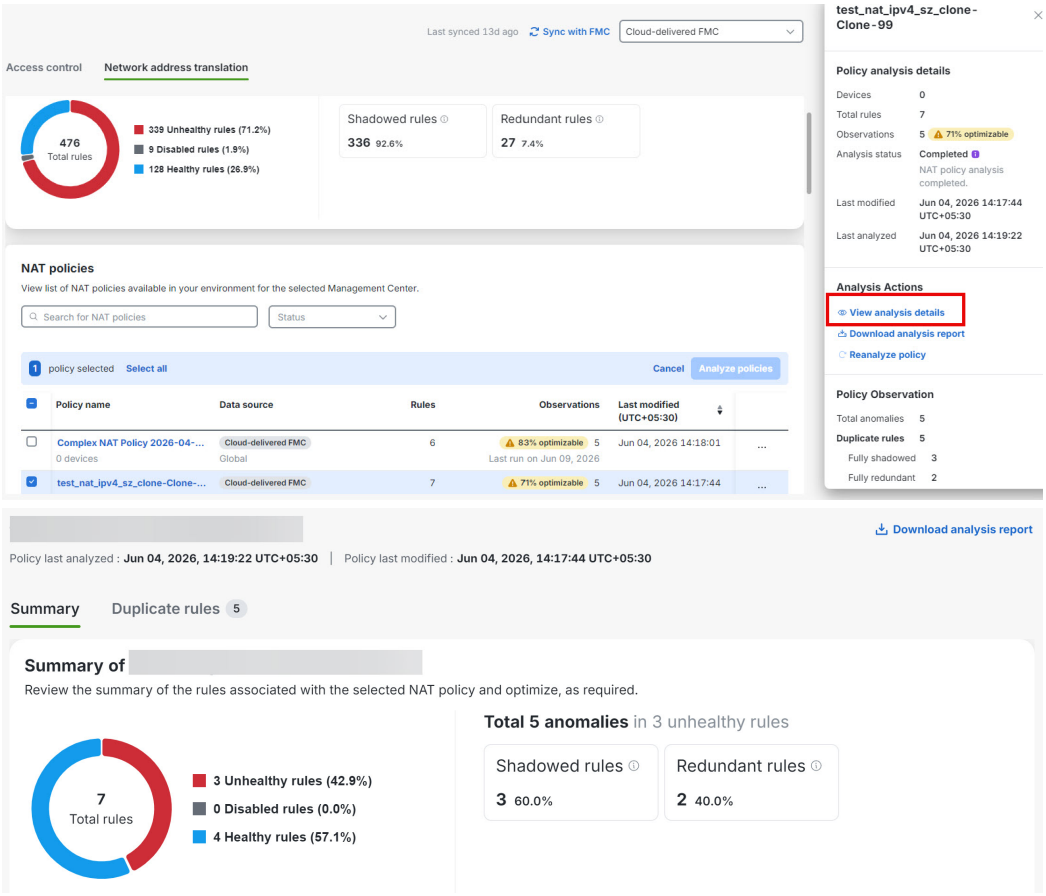
Flow	Traffic family	Notes
NAT44	IPv4 to IPv4	Supported for standard IPv4 NAT and PAT behavior.
NAT66	IPv6 to IPv6	Supported for IPv6 NAT behavior.
NAT64	IPv6 to IPv4	Supported when cross-family behavior is explicitly configured.
NAT46	IPv4 to IPv6	Supported when cross-family behavior is explicitly configured.

NAT policy analysis summary

Provides a summary of NAT policy analysis results and anomaly details for rule health assessment.

When analysis completes, select a NAT policy to review the right-pane summary and click **View analysis details**.

The policy-specific page displaying the anomaly details is shown.



- **Overall summary**–provides insights on how many rules are unhealthy, disabled, healthy, using a pie chart for the selected NAT policy. You can also hover over the part of the pie to view the percentage of rules.
- **Total anomalies**–shows the number of rule anomalies detected in the selected NAT policy. Also indicates how many unhealthy rules contain those anomalies.

Download NAT analysis report

Configure the download of a NAT analysis report as a PDF that includes policy metadata, analysis timestamps, summary charts, and rule details.

Download a comprehensive NAT analysis report that contains policy metadata, analysis timestamps, summary charts, counts for healthy, disabled, shadowed, and redundant rules, and tabular observation details to evaluate your NAT policy configuration.

The NAT analysis report becomes available after NAT policy analysis is complete and provides detailed information about rule configurations including NAT section, rule type, direction, interface objects, and service details. Use this report to evaluate whether changes are needed in the management center.

Follow these steps to download the NAT analysis report:

Procedure

1. In the Policy Analyzer and Optimizer page, click **Network address translation**.
2. Select a NAT policy, and in the right pane, click **Download analysis report**.

The NAT analysis report downloads as a PDF. The detailed rule information includes NAT section, rule type, direction, source and destination interface objects, original source, original destination, original service, translated source, translated destination, and translated service. NAT Policy Analyzer and Optimizer does not apply NAT remediations in this release.

NAT policy remediation

Configure and apply remediation actions for a NAT policy to resolve duplicate-rule anomalies.

This task helps you resolve duplicate-rule anomalies in NAT policies by applying targeted remediation actions to affected rules.

Policy Analyzer and Optimizer stages NAT remediation changes before it updates the policy. You can stage remediation for individual rules or for all rules in a duplicate-rule observation.

The available actions depend on the NAT rule type:

- Manual NAT rules: You can delete or disable selected manual rules
- Auto NAT rules: You can only delete Auto NAT rules, but you cannot disable them.

> **Note**
>
> Back up your policy before applying any remediation. The changes made modify the NAT policy and cannot be automatically reverted.

Before you begin

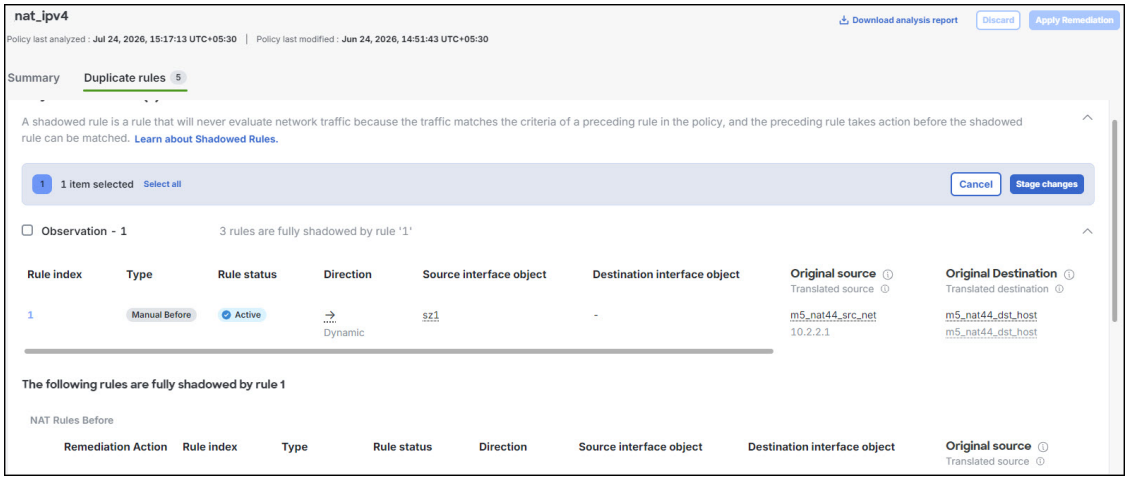
- Ensure that NAT policy analysis is complete and that duplicate-rule observations are available.
- Verify the **Policy last analyzed** and **Policy last modified** values for the policy that you want to remediate.

Procedure

1. In Policy Analyzer and Optimizer, select the NAT policy and under **Analysis Actions**, click **View analysis details** to open its analysis details.
2. Click **Duplicate rules** and expand fully shadowed or redundant rules section that contains anomalies.
3. Expand the observation that contains the rules that you want to remediate.

   You can select the rules or select the observation to stage all rules in that observation.

   Figure 13: NAT rule remediation



4. Click **Stage changes**.
5. In **Select rules to remediate**, select the action for each rule type:
   - **Manual rules**: **Delete all selected** or **Disable all selected**
   - **Auto NAT Rules**: **Delete all selected**. You cannot disable **Auto NAT** rules.
6. Select **Confirm staging**.

   Note

   Staged changes are visible to any user who opens the policy in Policy Analyzer and Optimizer. They remain until a user selects **Discard** or **Apply Remediation**, or until a new analysis runs after the policy is edited.

   Click **View details** to inspect and review the staged changes. You can click **Undo** or **Discard** to revise the staged remediation.
7. Select **Apply Remediation**.
8. On the **Apply NAT duplicate-rule remediation** page, verify the policy and the number of rules to modify, and then select **Apply remediation**.

After you apply the remediation, Policy Analyzer and Optimizer updates the selected NAT rules and automatically starts a new analysis because the previous analysis is stale. While the new analysis runs, the **Observations** column for the NAT policy shows In progress. After analysis completes, review the refreshed duplicate-rule observations and policy status. If no analyzed anomalies remain, the policy can show a healthy status.

View NAT remediation history

View NAT policy remediation versions, status, and reports.

Use remediation history to review when the remediation ran, the job that ran it, the user who started it, the remediation status, and the report for that version.

After you apply remediation to a NAT policy, Policy Analyzer and Optimizer records the remediation as a version in remediation history. The history lists the latest version first.

> **Note**
>
> Remediation history records changes applied to the NAT policy. It does not indicate whether the updated policy has been deployed to managed devices. Deploy the policy separately as required.

Before you begin

Apply remediation to the NAT policy. Remediation history is available after the policy has at least one remediation version.

Procedure

1. Open Policy Analyzer and Optimizer and click the Network address translation tab.
2. Select the NAT policy that you want to review. The policy analysis details open.
3. Under **Remediation Actions**, select **View remediation history**. The link shows the number of remediation versions that are available.
4. Review the remediation history. The list displays the latest remediation version first and then the older versions.
5. Review the date and time, Job ID, user, download option, and Remediation Status for each version.

   For a completed remediation, select **Download** to download the remediation report.

   The remediation report is a PDF that summarizes the selected NAT remediation, its status, and the resulting changes to the policy.

   > **Note**
   >
   > Policy Analyzer and Optimizer displays up to 10 remediation versions, from the latest version to the oldest available version.

You can view the remediation history for the NAT policy, including version details, status information, and download remediation reports for completed versions.

NAT Policy Analyzer and Optimizer and AgenticOps insights

Describes the integration between NAT Policy Analyzer and Optimizer analysis and AgenticOps for detecting and managing NAT policy anomalies.

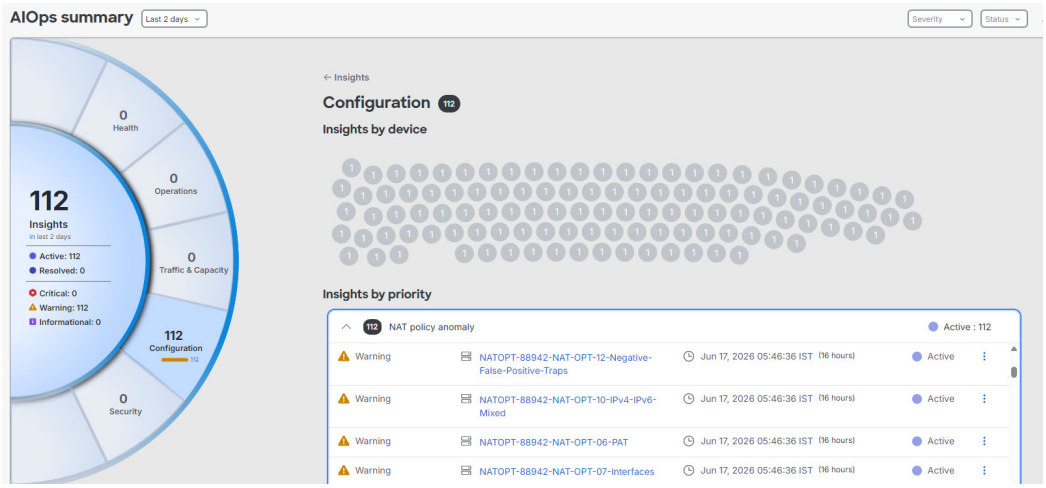
NAT Policy Analyzer and Optimizer and AgenticOps insights are an integrated monitoring system that

- detects NAT policy anomalies through automated analysis
- raises NAT policy anomaly insights when issues are detected, and
- provides navigation capabilities to review anomaly counts and access affected data sources or policies.

NAT anomaly insight management

When NAT Policy Analyzer and Optimizer analysis detects NAT policy anomalies, AgenticOpscan raise a NAT policy anomaly insight. From AIOps Insights, you can review NAT anomaly counts by data source, open the affected data source or policy, and navigate back to the NAT Policy Analyzer and Optimizer analysis details.

Navigation: **Insights & Reports** > **Summary**.



If you dismiss a NAT anomaly insight, it is dismissed for the current insight occurrence. A later scheduled analysis can raise the insight again if NAT anomalies are detected again.

Troubleshooting Policy Analyzer and Optimizer

Describes how to troubleshoot Policy Analyzer and Optimizer when policies fail to analyze or appear correctly, providing guidance for resolving common issues.

Read the following sections to troubleshoot any issues with the Policy Analyzer and Optimizer:

Troubleshoot policy analyzer and optimizer analysis issues

Configure troubleshooting steps to resolve issues when Policy Analyzer and Optimizer does not analyze policies despite clicking Analyze Policy.

This task helps you identify and resolve workflow errors that prevent Policy Analyzer and Optimizer from analyzing policies.

If you notice that Policy Analyzer and Optimizer is not analyzing policies despite clicking **Analyze Policy**, you can check for workflow errors and resolve them.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Navigate **Administration** > **Integrations** > **Firewall Management Center**.
3. Select the On-Premises Firewall Management Center or **Cloud-Delivered FMC** for which the policy analysis is not happening and choose **Workflows** under **Actions** on the right pane.
4. If you see that the latest workflow's **Current STATE** shows up as **ERROR**, expand the workflow and scroll to the last action whose **END STATE** is **ERROR**.
5. Click **ERROR Message** under the **RESULT** column to see a detailed ERROR message or click **Stack Trace** to see the series of exceptions that occurred, which caused the ERROR.

6. Resolve the ERROR or contact Cisco TAC for assistance.

You have identified the workflow ERROR preventing policy analysis and can now resolve the issue or escalate to Cisco TAC for further assistance.

Policy analyzer and optimizer does not fetch policies

Configure Policy Analyzer and Optimizer to properly fetch and display policies when they are not appearing on the CDO page.

This task resolves issues when policies are not displayed on the Policy Analyzer and Optimizer page in CDO, ensuring proper integration between your FMC and CDO services.

If policies on your On-Premises Firewall Management Center are not displayed on the Policy Analyzer and Optimizer page on Security Cloud Control, perform these steps to restore policy visibility.

Procedure

1. On the On-Premises Firewall Management Center, navigate **Integration** > **Cisco Security Cloud**.
2. Ensure that the **Enable Policy Analyzer and Optimizer** checkbox is checked.
3. Optional: In the left navigation pane of your Security Cloud Control tenant, navigate **Administration** > **Integrations** > **Firewall Management Center**, and ensure that the On-Premises Firewall Management Center is active and reachable.

The Policy Analyzer and Optimizer service is now properly configured and should display policies from your FMC on the CDO page.

Frequently asked questions about Policy Analyzer and Optimizer

Provides answers to common questions about Policy Analyzer and Optimizer, including AI Assistant support, analysis scheduling, reporting, licensing, remediation limits, rule handling, and failed remediation recovery.

This reference provides answers to frequently asked questions about Policy Analyzer and Optimizer functionality, capabilities, and limitations.

Can Cisco AI Assistant analyze and remediate policies instead of manually doing it using Policy Analyzer and Optimizer?

The Cisco AI Assistant collaborates with Policy Analyzer and Optimizer to scrutinize policies with anomalies and notify users. However, the AI Assistant cannot automatically analyze and remediate policies.

Can Policy Analyzer and Optimizer detect new changes to an already-analyzed policy and run analysis again on the same policy?

No, the Policy Analyzer and Optimizer can analyze policies only when manually triggered or at a 24-hour scheduled policy analysis run.

For a shared policy, does the Policy Analyzer and Optimizer provide individual device-based reports?

No. The Policy Analyzer and Optimizer provides reports only based on the access policy analysis data.

I am an On-Premises Firewall Management Center user. Should I purchase the Security Cloud Control base license to use the Policy Analyzer and Optimizer?

No. The Policy Analyzer and Optimizer comes as part of an existing or a newly created Security Cloud Control tenant during the Cisco Security Cloud integration.

I provisioned a Security Cloud Control tenant when I integrated my On-Premises Firewall Management Center with the Cisco Security Cloud. What other features, except Policy Analyzer and Optimizer, can I leverage in Security Cloud Control?

You can only leverage Policy Analyzer and Optimizer capabilities of this Security Cloud Control tenant. To use other features of Security Cloud Control, you need to purchase the Security Cloud Control base license and other device-specific licenses.

For an On-Premises Firewall Management Center on which the change management workflow is enabled and there are policies with pending changes to be approved, can the Policy Analyzer and Optimizer still apply remediations those policies?

No. The remediation will be hindered with an error saying the policies are locked for use.

Is there a maximum number of rules that Policy Analyzer and Optimizer can analyze in a policy?

There are no such limits. The Policy Analyzer and Optimizer can analyze any number of policies and rules. However, when the policies have more number of rules, the analysis takes a long time too.

What is the difference between disable rules and delete rules? which is the better option?

Deleting a rule removes the rule completely from the device memory. However, disabling a rule keeps it in the device memory as a backup and does not get deployed to the device.

If a policy remediation fails when it is partially done, are the changes automatically revoked by Policy Analyzer and Optimizer?

No. In such a case, you get a failure notification and a remediation report. You can read the report to know which rules were impacted by the half-done remediation, manually revoke the changes, and start the remediation all over again.

Part VI

Manage Catalyst SD-WAN Manager Firewall Capabilities

Topics:

- Integrate Catalyst SD-WAN Manager with Security Cloud Control
- Onboard Catalyst SD-WAN Manager
- Configure Next-Generation Firewall Capabilities of Catalyst SD-WAN Manager
- Monitor Catalyst SD-WAN Events

Manage Catalyst SD-WAN Manager Firewall capabilities with Security Cloud Control.

27 Integrate Catalyst SD-WAN Manager with Security Cloud Control

Topics:

- Catalyst SD-WAN integration with Security Cloud Control Firewall Management
- System topology diagram
- Managing Catalyst SD-WAN Manager using Security Cloud Control
- Minimum software requirements
- Additional resources

This chapter explains the integration of Catalyst SD-WAN Manager with Security Cloud Control.

Catalyst SD-WAN integration with Security Cloud Control Firewall Management

Describes the integration of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager that enables efficient configuration, monitoring, and enforcement of security policies, advanced threat detection, log analysis, and AI-driven troubleshooting.

The Catalyst SD-WAN integration with Security Cloud Control Firewall Management is a centralized management solution that

- provides unified control for Cisco Catalyst SD-WAN and Branch WAN environments
- enables configuration, monitoring, and enforcement of security policies across networks, and
- facilitates advanced troubleshooting, rule optimization, and change management on Catalyst SD-WAN Manager.

Integration capabilities

You can use Cisco SD-WAN solutions, including the Catalyst and Secure Router series, with Cisco security portfolio to control and manage network security features.

This integration allows you to:

- Efficiently manage security policies and objects, configure and edit them, and push changes using the Security Cloud Control Firewall Management dashboard.
- Effective monitoring and detection of security threats from a centralized Security Cloud Control Firewall Management dashboard.
- Analyze security threats from logs and events in the Security Cloud Control Firewall Management dashboard with data sent from Security Analytics and Logging.

Security Cloud Control Firewall Management provides these capabilities:

- Identifies existing security configurations and policies through the onboarded Catalyst SD-WAN Manager.
- Enables the creation of new security objects and policies using its platform.
- Supports a cohesive strategy for implementing security objects, policies, and profiles across multiple Cisco solutions.
- Offers capabilities for viewing logs and analytics data.
- Displays intrusion and malware events detected within the network from Secure Router.
- Leverages troubleshooting and AI-driven tools for efficient problem resolution.

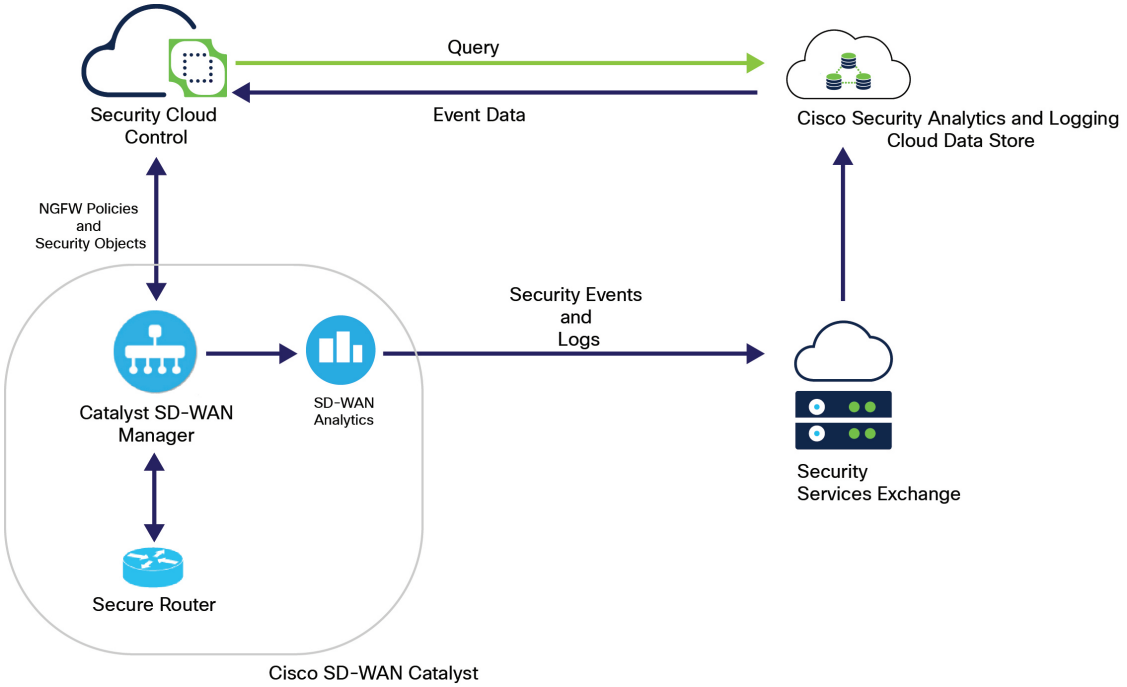
System topology diagram

Provides topology diagram that illustrates the integration of Catalyst SD-WAN with Security Cloud Control Firewall Management and shows the flow of information and interactions between various components.

The primary use case for managing the Next-Generation Firewall (NGFW) capabilities of Catalyst SD-WAN through Security Cloud Control Firewall Management is to streamline and centralize security management across Cisco's security products.

The topology diagram illustrates the integration of Catalyst SD-WAN with Security Cloud Control Firewall Management and other cloud services. The diagram shows the flow of information and interactions between various components.

> **Note**
>
> The Cisco Catalyst 8000 and Secure 8000 devices are collectively referred to as the 'Secure Router' hereafter.



- **Security Cloud Control**: A central point for security policy enforcement and event correlation. It reads Next-Generation Firewall (NGFW) policies and security objects from the onboarded Catalyst SD-WAN Manager and allows customers to modify these NGFW configurations. It also sends queries to Cisco Security Analytics and Logging cloud data store for events.
- **Cisco Catalyst SD-WAN** consists of:
  - **Catalyst SD-WAN Manager:** Manages the SD-WAN fabric and displays NGFW policies and security objects in Security Cloud Control when onboarded to it. Catalyst SD-WAN Manager sends the event data received from Secure Router to **SD-WAN Analytics**.
  - **SD-WAN Analytics**: Provides analytics data to the Security Services Exchange.
  - **Secure Router:** The SD-WAN edge device.
- **Cisco Security Analytics and Logging Cloud Data Store**: A cloud-based repository for security analytics and logging data. It receives security events and logs from **Security Services Exchange**, which obtains the analytics data from SD-WAN Analytics engine.
- **Security Services Exchange**: A cloud-based platform designed to facilitate the integration, communication, and management of various Cisco security services. It sends security events and logs received from the SD-WAN environment and forwards them to the Cisco Security Analytics and Logging Cloud data store.

Managing Catalyst SD-WAN Manager using Security Cloud Control

Describes the high-level end-to-end workflow for managing the firewall capabilities of Catalyst SD-WAN Manager using Security Cloud Control.

The integration of Catalyst SD-WAN Manager with Security Cloud Control Firewall Management enables you to manage Next-Generation Firewall (NGFW) capabilities through Security Cloud Control platform.

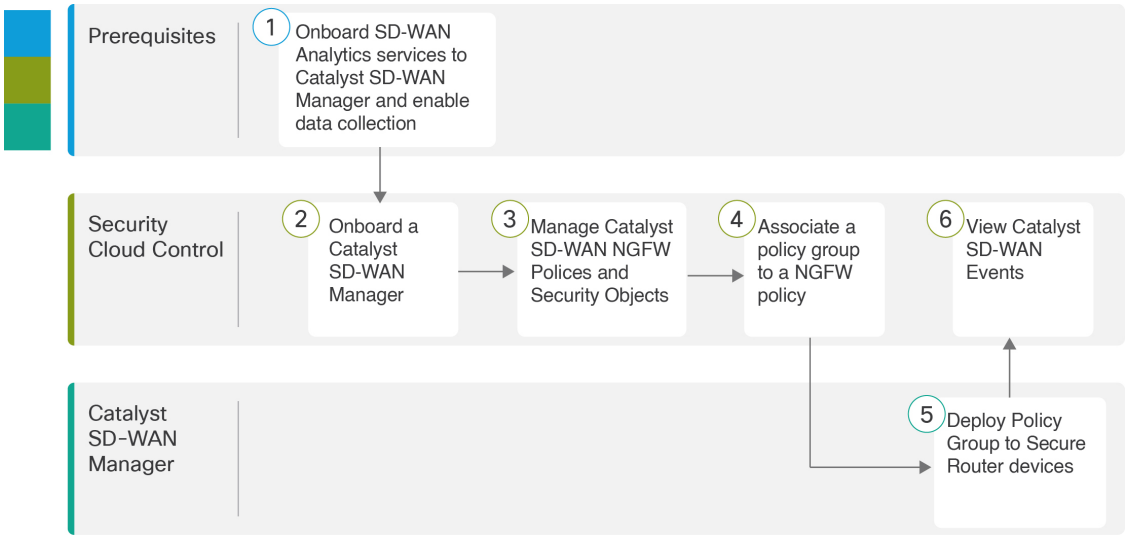
Summary

The key components involved in managing Catalyst SD-WAN Manager using Security Cloud Control are:

- Catalyst SD-WAN Manager: Provides SD-WAN Analytics services and deploys policy groups to routers
- Security Cloud Control: Manages security objects, profiles, and NGFW policies centrally
- Secure Router routers: Execute deployed firewall policies and generate security events

Workflow

Figure 14: Workflow for managing the firewall capabilities of Catalyst SD-WAN using security cloud control



These are the stages of managing Catalyst SD-WAN Manager using Security Cloud Control:

1. Prerequisites: Onboard SD-WAN Analytics services to Catalyst SD-WAN Manager and enable data collection. For more information, see Onboard Cisco SD-WAN analytics.
2. In Security Cloud Control, onboard your Catalyst SD-WAN Manager. The onboarding process also imports your associated Secure Router routers. For more information, see Integrate Catalyst SD-WAN Manager with Security Cloud Control on page 587.
3. In Security Cloud Control, create, modify, or delete Catalyst SD-WAN security objects, security profiles, and Next-Generation Firewall (NGFW) policies. For more information, see Manage objects and profiles and Manage NGFW policies.
4. In Security Cloud Control, associate a policy group to your Catalyst SD-WAN NGFW policy. For more information, see Associate a group policy.
5. In Catalyst SD-WAN Manager, deploy the policy group to Secure Router routers. For more information, see Policy groups configuration.

6. In Security Cloud Control, view the security events received from Catalyst SD-WAN with Security Analytics and Logging for monitoring and threat detection. For more information, see Security Analytics and Logging (Saas) for Catalyst SD-WAN Devices.

Minimum software requirements

Lists minimum software requirements for Catalyst SD-WAN integration with Security Cloud Control Firewall Management.

Minimum software requirements for Catalyst SD-WAN integration with Security Cloud Control Firewall Management require Catalyst SD-WAN Manager version 20.18 or later. Secure router compatibility follows Catalyst SD-WAN Manager backward support for the previous two device releases (for example, 20.15 and 20.12 with 20.18).

Minimum software requirements for Catalyst SD-WAN integration with Security Cloud Control Firewall Management:

- Catalyst SD-WAN Manager supported versions: 20.18 or later
- Secure Router supported versions: Devices supported by the last two versions of Catalyst SD-WAN Manager are compatible from version 20.18 onward. For example, if you use Catalyst SD-WAN Manager version 20.18, devices from versions 20.15 and 20.12 are compatible.

  Contact Cisco TAC to check which indexes are not compatible, and remove any incompatible indexes. For more information, see Cisco SD-WAN Control Components Compatibility Matrix.

Network requirements

If a firewall protects your network, add *.sdwan.cisco.com to the allowed list for inbound port 443 traffic to Catalyst SD Manager. This configuration allows the Cisco API Gateway to communicate with your environment.

Additional resources

Provides additional resources such as Catalyst SD-WAN configuration guide and policy groups configuration guide.

This reference provides links to additional configuration guides and resources for security and policy management.

- Cisco Catalyst SD-WAN Security Configuration Guide
- Policy Groups Configuration Guide, Cisco IOS XE Catalyst SD-WAN
- Security Cloud Control Integration with Cisco Catalyst SD-WAN Manager

28 Onboard Catalyst SD-WAN Manager

Topics:

- Onboard Catalyst SD-WAN Manager to Security Cloud Control
- Deboard Catalyst SD-WAN Manager from Security Cloud Control
- Alignment of RBAC models of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager
- Security Cloud Control Firewall Management management of Catalyst SD-WAN NGFW capabilities
- View intrusion events
- View malware events

This chapter explains how Catalyst SD-WAN Manager is onboarded to Security Cloud Control

Onboard Catalyst SD-WAN Manager to Security Cloud Control

Configure the onboarding of Catalyst SD-WAN Manager to Security Cloud Control by verifying Smart or Virtual Account admin privileges, noting the SD-WAN Organization Name, and enabling Cloud Services, Analytics, and Service Access Authorization.

This task enables you to manage Catalyst SD-WAN Manager security operations from Security Cloud Control platform, including policies, objects, and profiles management.

Use this procedure to onboard Catalyst SD-WAN Manager to Security Cloud Control platform.

Note

After you onboard Catalyst SD-WAN Manager to Security Cloud Control, security operations (management of policies, objects, and profiles) can be carried out only from Security Cloud Control.

The version control feature is not supported in Security Cloud Control.

Before you begin

Note

Use a publicly resolvable URL or public IP address to access Cisco Catalyst SD-WAN Manager. The Cisco API Gateway must be able to reach the address from the Cisco cloud environment. Internal-only URLs and private IP addresses prevent the API Gateway from connecting and cause onboarding and other cloud services to fail.

- You must have Smart Account Administrator or Virtual Account Administrator privileges on a virtual account linked to a controller profile containing the information of the organization you want to onboard.

  For more information about Smart Account and Virtual Account, see Access the Cisco Catalyst SD-WAN Portal.

- You must have the **Organization Name** of your Catalyst SD-WAN Manager because it will be required during onboarding.

  1. Log in to your Catalyst SD-WAN Manager.
  2. Choose **Administration > Settings > System > Organization Name**.

     The **Organization Name** field contains a unique identifier that establishes secure control connections within the SD-WAN environment.

- Enable **Service Access Authorization** to ensure the onboarding process completes successfully.

  1. Log in to your Catalyst SD-WAN Manager.
  2. Choose **Administration > Settings > Cloud Services**.
  3. Enable **Cloud Services**, **Analytics**, and **Service Access Authorization**.

Note

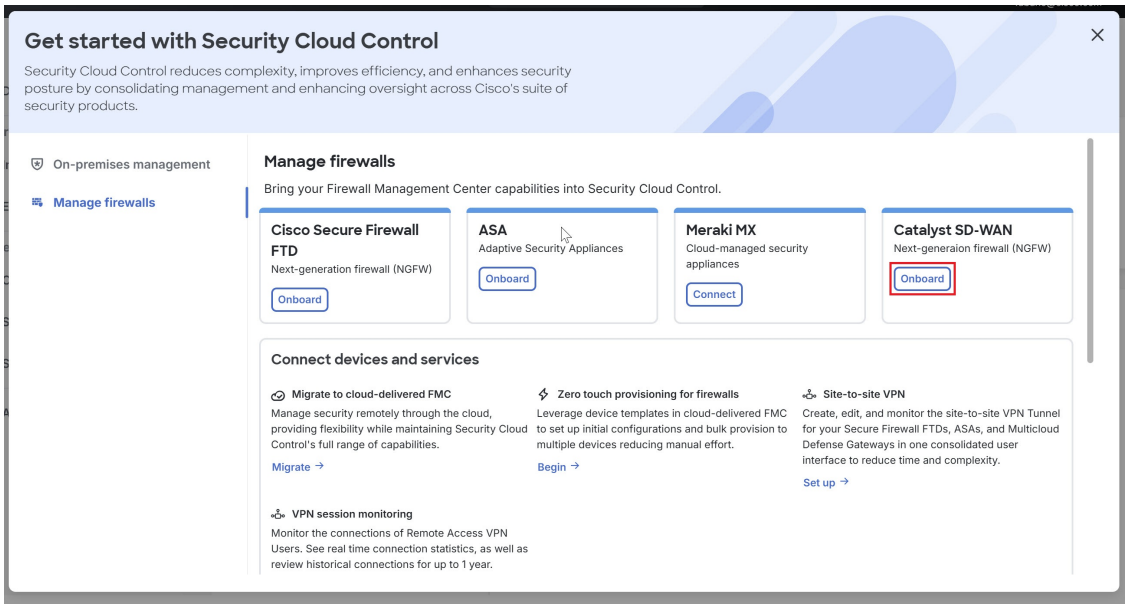
All Secure Router devices managed by Catalyst SD-WAN Manager are onboarded to Security Cloud Control regardless of their **Device Status**.

- You must have either an Admin or Super Admin role on Security Cloud Control.

Follow these steps to onboard Catalyst SD-WAN Manager to Security Cloud Control:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click the + icon at the top-right corner of the **Catalyst SD-WAN** tab.
3. Alternatively, you can use the **Get started with Security Cloud Control** interface to onboard Catalyst SD-WAN Manager.
   a. In the top menu, click .
   b. Click the **Manage firewalls** tab.
   c. Click **Onboard** on the **Catalyst SD-WAN** tile.



4. From the **Select Organization** drop-down list, choose an organization.

   The list of organizations displayed in the drop-down depends on the region where Security Cloud Control is deployed.

5. In the **Create label** field, enter the desired label and click **Connect**.

   After you onboard the device to Security Cloud Control, the system applies labels. You can use these labels to group devices and filter them on the **Security Devices** page.

6. Verify the details on the Catalyst SD-WAN Manager you are onboarding, and then click **Close**.

In the **Services** page, the **Catalyst SD-WAN** displays the onboarded manager.

After a successful onboarding, these details are displayed in Security Cloud Control:

- All security objects, security profiles, and NGFW policies. The system displays these imported policies in **Policies** > **WAN Branch Edge**.
- Secure Router devices and their running configuration.

What to do next: In the **Management** pane, click **Devices** to see the onboarded Secure Router devices.

Deboard Catalyst SD-WAN Manager from Security Cloud Control

Configure the deboarding of Catalyst SD-WAN Manager from Security Cloud Control to automatically remove associated devices, NGFW policies, and security objects.

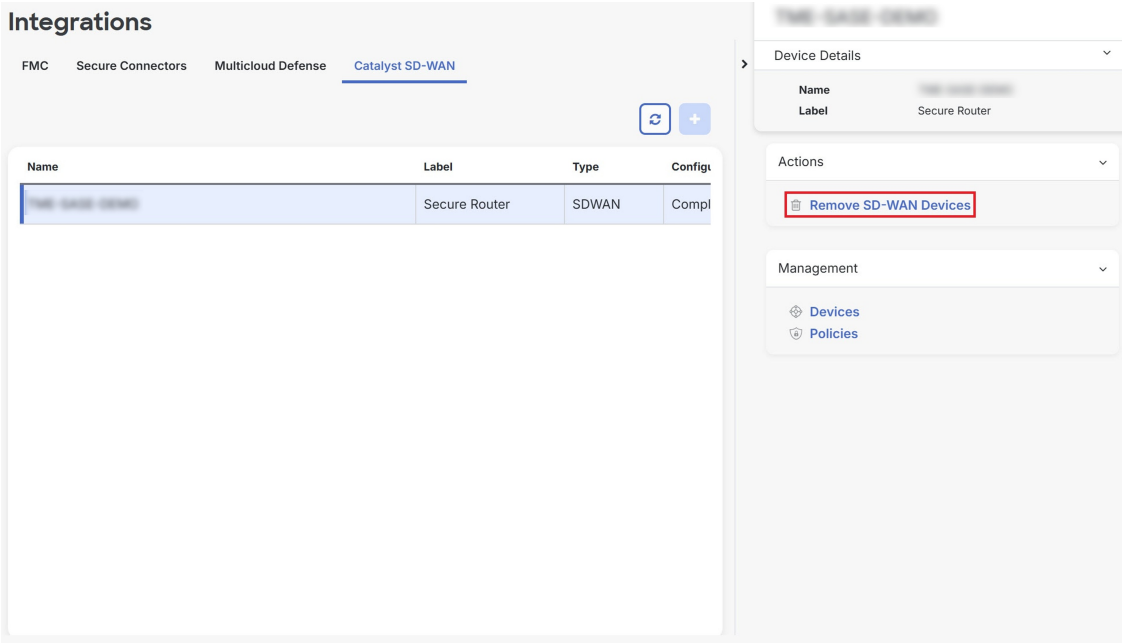
This task removes Catalyst SD-WAN Manager and its associated components from Security Cloud Control while preserving the original configurations in the manager for future independent management.

Deboarding Catalyst SD-WAN Manager from Security Cloud Control automatically removes its associated devices, policies, and objects from Security Cloud Control.

> **Note**
>
> When you deboard Catalyst SD-WAN Manager from Security Cloud Control, all the policies and objects created through Security Cloud Control are deleted from Security Cloud Control but remain in Catalyst SD-WAN Manager. You can then edit security objects and policies from Catalyst SD-WAN Manager.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Catalyst SD-WAN**.
3. Select the manager that you want to delete and click **Remove SD-WAN Devices**.



4. Click **OK** to confirm the action.

The Catalyst SD-WAN Manager is deboarded from Security Cloud Control, and all associated devices, policies, and objects are removed from Security Cloud Control while remaining accessible in the original manager.

Alignment of RBAC models of Security Cloud Control Firewall Management and Catalyst SD-WAN Manager

Lists user roles in Catalyst SD-WAN Manager and Security Cloud Control Firewall Management that operate independently, with each role defined by its specific responsibilities. The Role-Based Access Control (RBAC) models for both platforms are aligned to provide consistency and seamless user actions.

User roles in Catalyst SD-WAN Manager and Security Cloud Control Firewall Management operate independently, with each role defined by its specific responsibilities. However, the Role-Based Access Control (RBAC) models across these platforms are aligned to ensure consistent and seamless user actions.

A user with elevated permissions in Security Cloud Control Firewall Management may still encounter restrictions if their role in Catalyst SD-WAN Manager has lower permissions, and vice versa.

Attempting to save changes in Security Cloud Control Firewall Management without appropriate permissions in Catalyst SD-WAN Manager results in an error. For example, users assigned the 'Super Admin' role in Security Cloud Control Firewall Management cannot save NGFW security policies changes to Catalyst SD-WAN Manager if they have the 'Operator' role in that platform.

This table outlines the access permissions for various combinations of user roles in Catalyst SD-WAN Manager and Security Cloud Control Firewall Management.

Table 30: RBAC mapping of user roles in Catalyst SD-WAN Manager and Security Cloud Control Firewall Management

Security Cloud Control Firewall Management Role Name	Catalyst SD-WAN Manager Role Name	Allowed Actions
Read Only	Operator	Allowed read-only access in Security Cloud Control Firewall Management Allowed read-only access in Catalyst SD-WAN Manager
VPN Sessions Manager	Operator	Allowed read-only access in Catalyst SD-WAN Manager
Administrator	security_operations	Allowed to create/edit security policies in Security Cloud Control Firewall Management Allocated SecOps user role in Catalyst SD-WAN Manager
Super Administrator	security_operations	Unrestricted access to all functions in Security Cloud Control Firewall Management Allocated SecOps user role in Catalyst SD-WAN Manager
Deploy Only	Operator	Not allowed to create/edit security policies in Security Cloud Control Firewall Management Allowed read-only access in Catalyst SD-WAN Manager
Edit Only	security_operations	Not allowed to onboard or deboard Catalyst SD-WAN Manager Unrestricted access to all functions in Security Cloud Control Firewall Management Allocated SecOps user role in Catalyst SD-WAN Manager

Security Cloud Control Firewall Management management of Catalyst SD-WAN NGFW capabilities

Describes how Security Cloud Control Firewall Management enables centralized creation, modification, and deletion of Next-Generation Firewall policies, security objects, and profiles for Catalyst SD-WAN NGFW policies with automatic synchronization to Catalyst SD-WAN Manager.

Security Cloud Control Firewall Management management of Catalyst SD-WAN NGFW capabilities is an integration model that

- enables centralized management of Next-Generation Firewall policies, security objects, and profiles through Security Cloud Control Firewall Management

- automatically synchronizes configuration changes between Security Cloud Control Firewall Management and Catalyst SD-WAN Manager, and
- requires manual deployment to Secure Router devices via Catalyst SD-WAN Manager.

Integration behavior and restrictions

When Catalyst SD-WAN Manager is integrated with Security Cloud Control Firewall Management, the existing Next-Generation Firewall policies, security objects, and security profiles from Catalyst SD-WAN Manager are automatically imported into Security Cloud Control Firewall Management. You can modify these NGFW parameters or create new ones in Security Cloud Control Firewall Management. Any changes you make in Security Cloud Control Firewall Management are synchronized and saved in Catalyst SD-WAN Manager.

After Catalyst SD-WAN Manager is onboarded to Security Cloud Control Firewall Management, you can no longer manage policies, objects, or profiles through Catalyst SD-WAN Manager. You must manage them exclusively from Security Cloud Control Firewall Management.

A "*Managed by Security Cloud Control (SCC)*" banner is displayed on Catalyst SD-WAN Manager that is onboarded to Security Cloud Control Firewall Management, indicating the integration. You can view this message in Catalyst SD-WAN Manager by navigating to the relevant configuration sections.

- For Security Objects and Profiles: Choose **Configuration** > **Policy Groups** > **Objects and Profiles** > **Security Objects**.
- For NGFW Policies: Choose **Configuration** > **Policy Groups** > **NGFW**

Restrictions for Catalyst SD-WAN Manager integration with Security Cloud Control Firewall Management:

- Cloud connectivity is essential

  Catalyst SD-WAN Manager can be deployed either on-premises or hosted in the Cisco cloud. To function properly, it must have cloud connectivity. If Catalyst SD-WAN Manager is placed behind a NAT device, it is supported but with restrictions. Specifically, only port 443 (HTTPS) needs to be open to enable cloud connectivity.

- Deboard Catalyst SD-WAN Manager to edit NGFW policies, security objects, and security profiles

  To make changes in NGFW policies, security objects, and security profiles from Catalyst SD-WAN Manager, you have to deboard it from Security Cloud Control Firewall Management.

- Customized IPS profiles not supported

  You cannot edit or customize IPS policies (Signature set objects) within security profiles.

- Live logs unavailable with Cisco Security Analytics and Logging (SAL)

  Live logs cannot be viewed on Security Cloud Control Firewall Management using SAL. You can only view historical events.

- Modify user role privileges for Security Cloud Control Firewall Management users with caution

  Exercise caution when changing user role privileges on Catalyst SD-WAN Manager for users who are part of Security Cloud Control Firewall Management. Modifying privileges for Security Cloud Control Firewall Management-associated users can result in configuration failures.

- On-premises multitenant Catalyst SD-WAN Manager not supported

  On-premises multitenant deployments of Catalyst SD-WAN Manager are not supported in Security Cloud Control Firewall Management for version 20.18.1. In this release, only single-tenant Catalyst SD-WAN Manager deployments are compatible with Security Cloud Control Firewall Management.

- Dark mode not supported

  Keep dark mode disabled in Security Cloud Control Firewall Management when Catalyst SD-WAN Manager is integrated.

> **Note**
>
> Changes to NGFW policies, objects, and profiles can only be made in Catalyst SD-WAN Manager after it has been deboarded from Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management allows you to perform these operations:

- Create, modify, or delete NGFW policies, security objects, and security profiles.
- Search for security objects across devices using global search functionality.
- Associate a policy group with a Catalyst SD-WAN NGFW policy.

Policy deployment to Secure Router devices

Changes that are made to NGFW policies, security objects, and security profiles in Security Cloud Control Firewall Management are automatically saved to Catalyst SD-WAN Manager. However, the updated configuration must be manually deployed to Secure Router devices using Catalyst SD-WAN Manager. These changes cannot be pushed directly to devices from Security Cloud Control Firewall Management.

View intrusion events

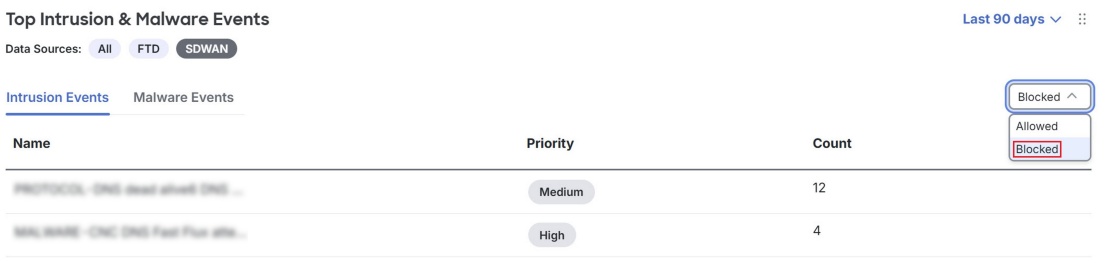
Intrusion Prevention System (IPS) dashlet highlights blocked and allowed network attacks using Cisco Talos threat intelligence. This dashboard view maps to Catalyst SD-WAN Manager Security Monitor IPS/AMP dashlets.

The Intrusion Prevention System (IPS) helps you detect and block network intrusions and malicious activities based on Cisco Talos threat intelligence.

The **Top Intrusion & Malware Events** dashlet in the Security Cloud Control Firewall Management dashboard is mapped to **Intrusion Prevention** and **Advanced Malware Protection** dashlets in the **Monitor** page of Catalyst SD-WAN Manager on the **Security** tab.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click **Dashboard**.
3. Navigate to the **Top Intrusion & Malware Events** dashlet.
4. Click **SDWAN** under **Data Sources**.
5. Click the **Intrusion Events** tab.
6. Select **Blocked** in the drop-down near the dashlet.
   By default, **Allowed** is selected.



7. Click the event you want to view in Catalyst SD-WAN Manager.

   A cross-launch window of the Catalyst SD-WAN Manager **Monitor** page appears.

8. Navigate to the **Intrusion Prevention** dashlet to view the event.

View malware events

View the Advanced Malware Protection (AMP) events dashlet, which shows malicious, unknown, and clean file counts over time. This dashboard view maps to Catalyst SD-WAN Manager Security Monitor IPS/AMP dashlets.

The Advanced Malware Protection (AMP) events dashlet displays the counts of malicious, unknown, and clean files identified by AMP over a selected period. AMP blocks malware based on file reputation and uploads unknown files to Cisco AMP Threat Grid for further analysis.

The **Top Intrusion & Malware Events** dashlet on the Security Cloud Control Firewall Management dashboard is mapped to the **Intrusion Prevention** and **Advanced Malware Protection** dashlets on the **Monitor** page of Catalyst SD-WAN Manager on the **Security** tab.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click **Dashboard**.
3. Navigate to the **Top Intrusion & Malware Events** dashlet.
4. Click **SDWAN** under **Data Sources**.
5. Click the **Malware Events** tab.
6. Select **Blocked** in the drop-down near the dashlet. By default, **Allowed** is selected.



7. Click the event you want to view in Catalyst SD-WAN Manager.

   A cross-launch window of the Catalyst SD-WAN Manager **Monitor** page appears.

8. Navigate to the **Advanced Malware Protection** dashlet to view the event.

29 Configure Next-Generation Firewall Capabilities of Catalyst SD-WAN Manager

Topics:

- Catalyst SD-WAN devices
- Supported operations on Catalyst SD-WAN devices
- View configuration of Catalyst SD-WAN devices
- Cross-launch policy groups from Security Cloud Control Firewall Management
- Catalyst SD-WAN security objects and security profiles
- Create new Catalyst SD-WAN security objects and security profiles
- Modify Catalyst SD-WAN security objects and security profiles
- Delete Catalyst SD-WAN security objects
- Filter Catalyst SD-WAN security objects
- Catalyst SD-WAN NGFW security policies
- Manage existing Catalyst SD-WAN NGFW security policies
- Create Catalyst SD-WAN security policies
- Associate a policy group to Catalyst SD-WAN NGFW policy
- Deploy policy group from Catalyst SD-WAN Manager

This chapter explains how to configure Catalyst SD-WAN Manager Firewall capabilities in Security Cloud Control

Catalyst SD-WAN devices

Describes how to manage Catalyst SD-WAN devices in Security Cloud Control Firewall Management, including viewing onboarded devices and templates, reviewing device configurations, launching policy groups, and removing devices.

Catalyst SD-WAN devices are advanced networking solutions that

- provide secure, high-performance connectivity
- integrate SD-WAN capabilities and robust security features, and
- enable organizations to connect users to applications seamlessly across multicloud environments, branch offices, and data centers.

Management in Security Cloud Control Firewall Management

Security Cloud Control Firewall Management provides centralized visibility and security policy management for Catalyst SD-WAN devices.

Supported operations on Catalyst SD-WAN devices

Describes the operations available for managing Catalyst SD-WAN devices in Security Cloud Control Firewall Management.

Supported operations on Catalyst SD-WAN devices are management capabilities that

- enable viewing and managing onboarded WAN Branch Edge or Secure Router devices through Security Cloud Control Firewall Management
- provide access to device configurations and policy groups on the **Security Devices** page, and
- allow management of devices after the related Catalyst SD-WAN Manager is onboarded.

Available operations

Security Cloud Control Firewall Management provides the ability to view, manage, and remove your onboarded devices on the **Security Devices** page. From the **Security Devices** page, you can:

- View onboarded devices and templates in separate tabs.

  For more information, see About Security Devices Page.
- View the configuration file of the onboarded devices.
- Launch policy groups on the Catalyst SD-WAN platform.

> **Note**
>
> You can onboard only one Security Cloud Control Firewall Management organization to a single Catalyst SD-WAN Manager.

View configuration of Catalyst SD-WAN devices

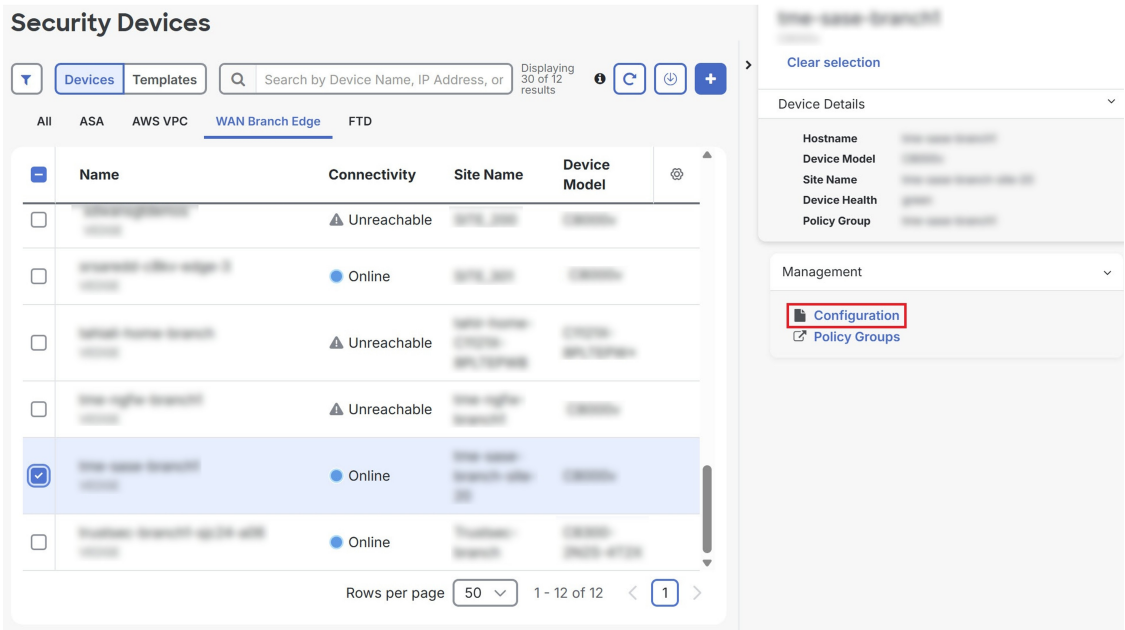
Configure access to device configurations for onboarded Catalyst SD-WAN devices in Security Cloud Control Firewall Management.

View and export device configurations for your onboarded Catalyst SD-WAN devices to manage and monitor device settings.

Security Cloud Control Firewall Management provides the ability to view the device configuration of your onboarded devices on the **Security Devices** page.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Manage** > **Security Devices**.
3. Click the **WAN Branch Edge** tab.
4. Select a device and click **Configuration** under **Management**.



5. To export the list of devices as a CSV file, click the export icon ( ).

The device configuration is displayed, and you can optionally export the device list as a CSV file for external use.

Cross-launch policy groups from Security Cloud Control Firewall Management

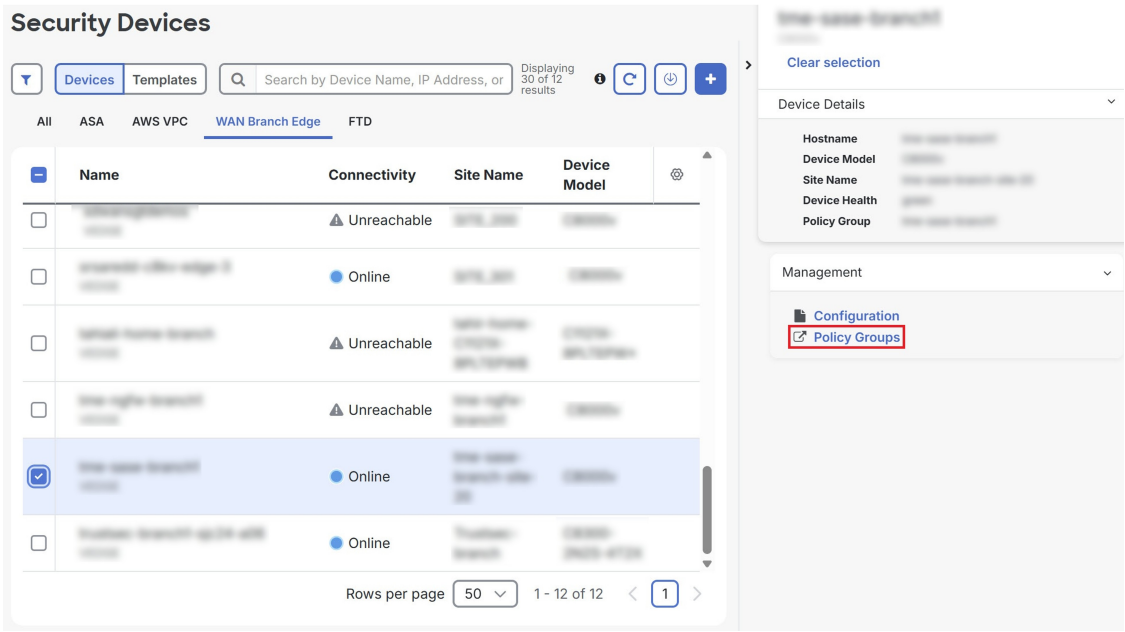
Configure cross-launch access to policy groups in Catalyst SD-WAN Manager from Security Cloud Control Firewall Management for onboarded devices.

This task enables you to navigate directly to the Policy Groups page in Catalyst SD-WAN Manager from Security Cloud Control Firewall Management for managing Catalyst SD-WAN devices.

Security Cloud Control Firewall Management lets you cross-launch to the **Policy Groups** page in Catalyst SD-WAN Manager for the onboarded Catalyst SD-WAN Manager.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Manage** > **Security Devices**.
3. Click the **WAN Branch Edge** tab.
4. Select a device and click **Policy Groups** under **Management**.



The Policy Groups page opens in Catalyst SD-WAN Manager, allowing you to manage policy configurations for the selected device.

Catalyst SD-WAN security objects and security profiles

Explains Catalyst SD-WAN security objects and security profiles that are essential for creating and enforcing next-generation firewall security policies.

Catalyst SD-WAN security objects and security profiles are reusable policy components that

- are essential for creating and enforcing next-generation firewall (NGFW) security policies
- safeguard networks from cyber threats while ensuring seamless connectivity and optimized application performance

- Security Cloud Control Firewall Management imports, manages, and synchronizes for Catalyst SD-WAN security policy control, and
- are vital for robust network security management and effective NGFW policy implementation.

Create new Catalyst SD-WAN security objects and security profiles

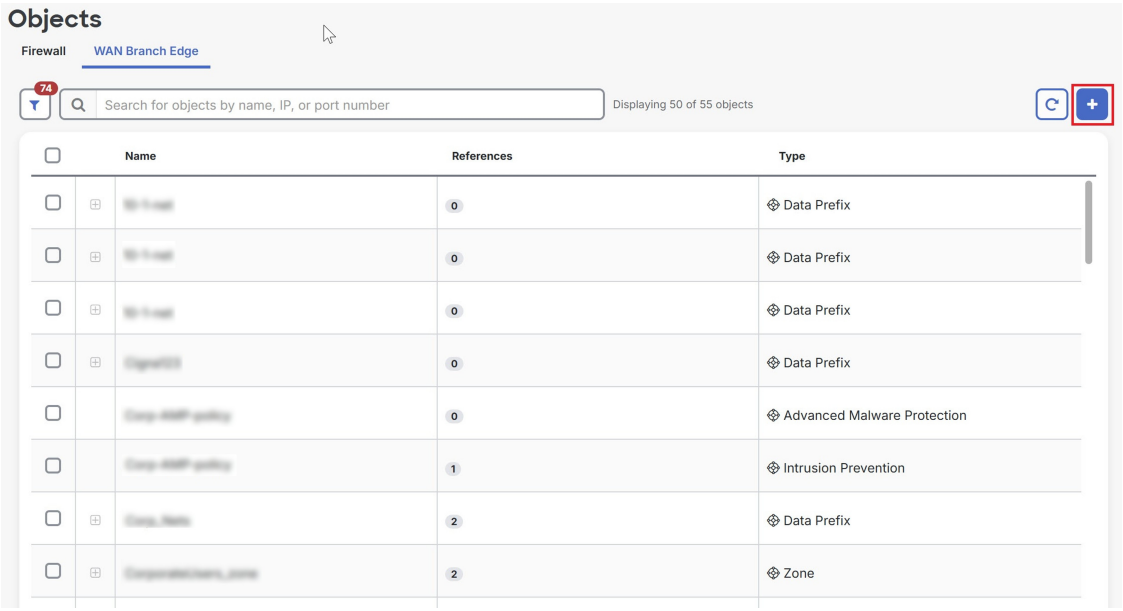
Configure new Catalyst SD-WAN security objects and security profiles using Security Cloud Control Firewall Management.

This task enables you to create security objects and profiles for network protection and policy enforcement in your Catalyst SD-WAN environment.

Use Security Cloud Control Firewall Management to create new Catalyst SD-WAN security objects and security profiles.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Objects**.
3. Click the **WAN Branch Edge** tab.
4. Click the **Create Object** ( ) icon.



5. Click the object or profile you want to create:

   Objects:

   - Application List
   - Data Prefix
   - FQDN
   - Geolocation
   - Identity
   - Port

- Protocol
- Security Group Tag
- Signature
- URL Allow
- URL Block
- Zone

Profiles:

- Advanced Inspection Profile
- Advanced Malware Protection
- Intrusion Prevention
- TLS/SSL Decryption
- TLS/SSL Profile
- URL Filtering

6. Click **Save**.

The objects are created in Security Cloud Control Firewall Management. To see the logs in Catalyst SD-WAN Manager, navigate to **Monitor** > **Logs** > **Audit Logs**.

Application lists

Describes the application list object that groups applications into a list for use in NGFW policies.

An application list is an object that groups applications into a list for use in NGFW policies.

Application list information

This table describes the fields and descriptions for application lists.

Table 31: Application list

Field	Description
Object Name	The name of the application list.
Application or Application Family	The **Application** is a collection of specific applications grouped together for policy configuration. It allows administrators to define and manage traffic rules for multiple applications as a single entity. For example, "Webex," "Microsoft Teams," "Zoom." The **Application Family** groups applications based on their functional category. For example, "Web," "Instant Messaging," "Network Services."

The **Selected items** field displays the items that have been chosen.

Data prefix

Lists specific IP address ranges or prefixes that are used to define and manage traffic routing policies within the SD-WAN fabric.

The **Data Prefix** objects are specific IP address ranges or prefixes that are used to define and manage traffic routing policies within the SD-WAN fabric.

Table 32: Data prefix

Field	Description
Object Name	The name of the data prefix object.
Data Prefix	The data prefix value.

FQDN

Provides information about the Fully Qualified Domain Name (FQDN) object used to match standalone servers in data centers or private clouds.

The Fully Qualified Domain Name (FQDN) object is used to match standalone servers in data centers or private clouds. When matching public URLs, the recommended match action is **drop**. If you use **inspect** for public URLs, you must define all the related sub URLs and redirect URLs.

Table 33: FQDN

Field	Description
Object Name	The name of the FQDN object.
FQDN	The URL names separated by commas. For example, cisco.com.

Geolocation

Lists the geolocation object that allows you to configure firewall rules based on geographical locations rather than IP addresses.

The **Geolocation** object allows you to configure firewall rules based on geographical locations rather than IP addresses.

Table 34: Geolocation

Field	Description
Object Name	The name of the geolocation object.
Geolocation	Select one or more geolocations from the drop-down list. For example, Africa, Antarctica, Asia, or Europe.

Identity

Describes the identity object, a security object used to represent user identities and user groups within the SD-WAN fabric.

An identity object is a security object that

- represents user identities and user groups within the SD-WAN fabric,
- integrates identity information into the SD-WAN fabric, and
- enables identity-based firewall policies and micro-segmentation.

Identity object fields
Table 35: Identity

Field	Description
Object Name	The name of the identity object.
Users **User Groups**	The source of **Users** and **User Groups** is Cisco Identity Services Engine (ISE) Active Directory (AD), which is configured in Catalyst SD-WAN Manager.

Port

Provides a configuration element used to define and manage port-related settings for devices within the SD-WAN fabric.

The **Port** object is a configuration element used to define and manage port-related settings for devices within the SD-WAN fabric.

Table 36: Port

Field	Description
Object Name	The name of the port object.
Port	The port values separated by commas. The range is 0 to 65535.

Protocol

Lists protocols that can be selected from a predefined list (for example, TCP, UDP, ICMP) to define specific rules for traffic management and security enforcement within security policies.

Within security policies, **Protocol** objects can be selected from a predefined list (for example, TCP, UDP, ICMP) to define specific rules for traffic management and security enforcement.

Table 37: Protocol

Field	Description
Object Name	The name of the protocol object.
Protocol	Select one or more protocol names from the drop-down list. For example, SNMP, TCP, UDP, ICMP, Echo, Telnet.

The **Selected items** field displays the items that have been chosen.

Security group tag

Provides information about security group tag (SGT) for classifying traffic in a Cisco TrustSec network using Cisco Identity Services Engine (ISE).

If you use Cisco Identity Services Engine (ISE) to define and use security group tag (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGTs as matching criteria.

SGTs cannot be created or edited in Security Cloud Control Firewall Management. You must create all SGTs in ISE.

Table 38: Security group tag

Field	Description
Object Name	The name of the security group tag.
Security Group Tags	Choose the security group tags by checking the appropriate checkboxes.

The **Selected items** field displays the items that have been chosen.

IPS signature

Provides information about the IPS signature object in Catalyst SD-WAN Manager which refers to a set of rules used by the Intrusion Prevention System (IPS) to detect and prevent network attacks.

The **IPS Signature** object refers to a set of rules used by the Intrusion Prevention System (IPS) to detect and prevent network attacks. It blocks vulnerabilities that have a Common Vulnerability Scoring System (CVSS) score of 9 or higher. It also blocks Common Vulnerabilities and Exposures (CVEs) published within the last two years if they belong to the rule categories of Malware CNC, Exploit Kits, SQL Injection, or blocked list.

Table 39: IPS signature

Field	Description
Object Name	The name of the object.
IPS Signature	The IPS signatures in the format `Generator ID:Signature ID`, separated by commas. For example, `1234:5678`. Range is 0 to `4294967295`.

Allow URL objects

Describes the allow URL object in Catalyst SD-WAN Manager used to define URLs that should be explicitly permitted through SD-WAN URL filtering feature.

An allow URL object is a configuration element that

- defines URLs that should be explicitly permitted through SD-WAN URL filtering feature
- ensures allowed URLs are not subjected to any category-based filtering, and
- takes precedence over blocked lists when the same item is configured in both allowed and blocked lists.

Allow URL object behavior

Important points to note about allow URL objects:

- URLs that are allowed are not subjected to any category-based filtering.
- If the same item is configured under both the allowed and blocked lists, the traffic is allowed.
- If the traffic does not match either the allowed or blocked lists, it is subjected to category-based and reputation-based filtering.

The configuration fields for allow URL objects:

Table 40: Allow URL

Field	Description
Object Name	The name of the allow URL object.
Allow URL	The URLs to allow.

Block URL

Lists the block URL object in Catalyst SD-WAN Manager used to define URLs that should be denied through SD-WAN URL filtering feature.

The **Block URL** object is used to define URLs that should be denied through SD-WAN URL filtering feature.

Table 41: Block URL

Field	Description
Object Name	The name of the block URL object.
Block URL	The URLs to block.

Zones

Explains the zone object in Catalyst SD-WAN Manager used to define security boundaries for traffic control.

A zone is a security boundary object that

- defines security boundaries for traffic control
- can be configured based on VPNs or interfaces, and
- allows granular application of security policies to traffic within or between network segments.

Zone configuration options

Zones can be configured based on **VPNs** or **Interfaces**:

- Zones can be created for specific VPNs, such as the Payment Processing Network, Corporate Users, or Local Internet for Guests. These zones allow you to apply security policies to traffic within or between VPNs.
- Interfaces can also be assigned to zones. For example, Ethernet, GigabitEthernet, or other interface types can be grouped into zones. This allows for granular control of traffic between interfaces.

Table 42: Zone

Field	Description
Object Name	The name of the zone.
VPN	Choose to configure zones with zone type as **VPN**. Add the VPNs to the zones from the drop-down list. Available options include: • Payment Processing Network • Corporate Users • Local Internet for Guests • Physical Security Devices
Interface	Choose to configure zones with zone type as **Interface**. Add the interfaces to the zones from the **Add Interface** drop-down list.

The **Selected items** field displays the items that have been chosen.

Advanced inspection profile

Provides a global Advanced Inspection Profile (AIP) at the device level that ensures all traffic matching the device's predefined rules is thoroughly inspected using the advanced inspection profile.

Apply a global **Advanced Inspection Profile** (AIP) at the device level. This ensures that all traffic matching the device's predefined rules is thoroughly inspected using the AIP.

Table 43: Advanced inspection profile

Field	Description
Object Name	The name of the advanced inspection profile.
Intrusion Prevention	Choose an intrusion prevention option from the drop-down list.
URL Filtering	Choose a URL filter from the drop-down list.
Advanced Malware Protection	Choose an advanced malware protection option.
TLS Action	Choose the TLS action. Available options include: • Decrypt • Pass Through • Do not Decrypt

Advanced malware protection

Provides advanced malware protection capabilities integrated into the unified security policy framework.

The **Advanced Malware Protection** (AMP) policy is a security policy specifically designed to integrate advanced malware protection capabilities into the unified security policy framework.

Note

For some advanced configurations, a Threat Grid Server configuration is required in Catalyst SD-WAN.

Table 44: Advanced malware protection

Field	Description
Object Name	The name of the advanced malware protection policy.
AMP Cloud Region	**AMT Cloud Region** refers to the **Analytics, Management, and Telemetry (AMT) Cloud Region** associated with the Cisco SD-WAN cloud architecture.
Alert Log Level	All syslog messages are associated with priority levels that indicate the severity of syslog messages to save.
File Analysis	Enables file analysis on the uploaded files.
TG Cloud Region	Choose a region. This refers to the geographical region where the Threat Grid (TG) cloud services are hosted.
File Types	Choose the file types to be analyzed.

Intrusion prevention

Provides information about the intrusion prevention policy profile, a security feature designed to detect and block known network attacks by leveraging predefined rules and signatures.

The **Intrusion Prevention** policy profile is a security feature designed to detect and block known network attacks by leveraging predefined rules and signature.

Table 45: Intrusion prevention

Field	Description
Object Name	The name of the intrusion prevention policy.
Signature Set	Choose a signature set that defines rules for evaluating traffic from the **Signature Set** drop-down list.
Inspection Mode	Select the inspection mode.
Custom Signature Set:	Select one or more web categories from the drop-down list. Custom signature must be enabled from Catalyst SD-WAN Manager under **Administration** > **Settings** > **External Services** > **UTD Snort Subscribe Signature** > .
Signature Allow List	Select a signature allow list.

Field	Description
Alerts Log Level	Choose the alert log level. This refers to the severity levels of logs generated by the system, which can be configured to control the granularity of information logged.

TLS/SSL decryption

Provides a TLS/SSL decryption profile feature that enables administrators to inspect and manage encrypted traffic passing through the network in Catalyst SD-WAN Manager.

The **TLS/SSL Decryption** profile allows administrators to inspect and manage encrypted traffic within the network.

> **Note**
>
> Before creating a **TLS/SSL Decryption** profile in Security Cloud Control Firewall Management, you must configure certificate authority (CA) from Catalyst SD-WAN Manager under **Configuration** > **Certificates** > **Certificate Authority**.

Table 46: TLS/SSL decryption

Field	Description
Object Name	The name of the TLS/SSL decryption policy. The name can contain a maximum of 32 characters.
Server Certificate Checks	
Expired Certificate	Defines what the policy should do if the server certificate has expired. Available options include: • Drop: Drop traffic • Decrypt: Decrypt traffic
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted. Available options include: • Drop: Drop traffic • Decrypt: Decrypt traffic
Certificate Revocation Status	Defines whether the Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate. Available options include: **Enabled** or **Disabled**.
Unknown Revocation Status	Defines the policy action if the OCSP revocation status is **unknown**. • Drop: Drop traffic • Decrypt: Decrypt traffic
Unsupported Mode Checks	

Field	Description
Unsupported Protocol Versions	Defines the unsupported protocol versions. • Drop: Drop the unsupported protocol versions. • No Decrypt: Decrypt the unsupported protocol versions.
Unsupported Cipher Suites	Defines the unsupported cipher suites. • Drop: Drop the unsupported cipher suites. • No Decrypt: Decrypt the unsupported cipher suites.
Failure Mode	Defines the failure mode. The options are **Close** and **Open**.
Certificate Bundle	Select the **Use Default CA Certificate** checkbox to use the default CA.
Minimal TLS Version	Sets the minimum version of TLS that the proxy should support. Available options include: TLS 1.0, TLS 1.1, or TLS 1.2
Proxy Certificate Attributes	
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modules. Available options include: 1024-bit RSA, 2048-bit RSA, or 4096-bit RSA
EC Key Type	Defines the key type. Available options include: P256, P384, or P521
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate (in days).

TLS/SSL profile

Provides information about the TLS/SSL profile policy in Catalyst SD-WAN Manager that manages encrypted traffic within a unified security policy.

The **TLS/SSL Profile** policy is used to manage encrypted traffic within a unified security policy. To create a TLS/SSL profile policy in Security Cloud Control Firewall Management, you must first configure the certificate authority (CA) certificate in Catalyst SD-WAN. This is a prerequisite for enabling the TLS proxy functionality.

Table 47: TLS/SSL profile

Field	Description
Object Name	The name of the TLS/SSL profile.
Categories to assign action	Set the categories and assign actions: Decrypt, No Decrypt, and Pass Through URL Categories. Alternatively, choose multiple categories and set the action.
Reputation	Enable reputation to choose the **Decrypt Threshold**. Supports actions based on URL reputation levels.
Decrypt Domain List	Choose the decrypt domain list.
No Decrypt Domain List	Choose the no decrypt domain list.
Fail Decrypt	Enable the fail decrypt option if decryption fails.

URL filtering

Provides information about the URL filtering profile policy in Catalyst SD-WAN Manager that allows administrators to control access to websites based on categories, reputation, and custom lists.

The **URL Filtering** profile policy is a security feature that allows administrators to control access to websites based on categories, reputation, and custom lists.

Table 48: URL filtering

Field	Description
Object Name	The name of the URL filtering policy.
Web Category	Choose the web category. Available options include: Block and Allow. The websites are classified into categories.
Web Reputation	Choose the web reputation from the drop-down list. The URLs are assigned a reputation score based on their risk level.
Allowlist	Select an allow URL list.
Blocklist	Select a block URL list.
Block Page Server	Choose one of the options: • Block Page Content: Enter the default content header and content body. • Redirect URL: Enter the redirect URL. The blocked users can be redirected to a custom page or shown a message.
Alerts and Logs	Choose the alert and log type: • Blocklist • Allowlist • Reputation/Category

Modify Catalyst SD-WAN security objects and security profiles

Configure the values associated with the Catalyst SD-WAN security objects and security profiles from Security Cloud Control Firewall Management.

This task allows you to modify the values associated with Catalyst SD-WAN security objects and security profiles to update configurations as needed.

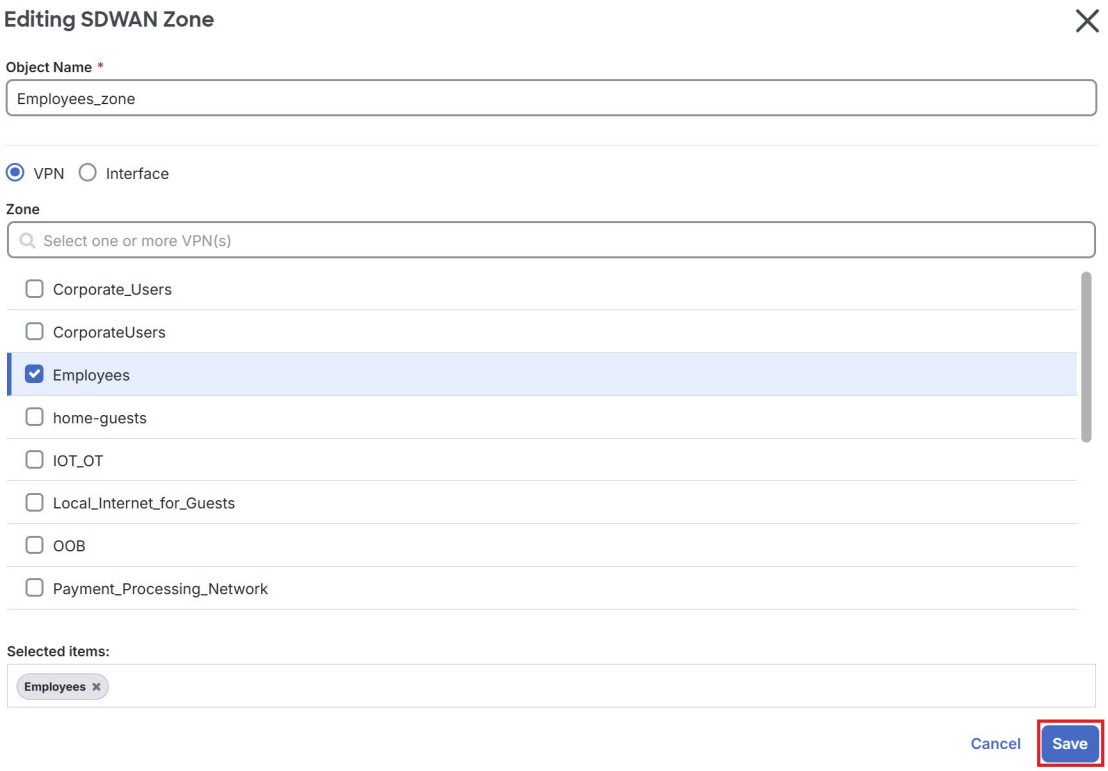
Use this procedure to modify the values associated with Catalyst SD-WAN security objects and security profiles from Security Cloud Control Firewall Management.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Objects**.
3. Click the **WAN Branch Edge** tab.

4. Select the security object or profile to modify. To find an object, use the filter.
5. In the **Actions** pane, click **Edit**.

   Modify the configurations you want to change.
6. Click **Save** to confirm.



The security object or profile is updated with your modifications and the changes are saved.

Delete Catalyst SD-WAN security objects

Configure the removal of Catalyst SD-WAN security objects in Security Cloud Control Firewall Management if they are not referenced by any policies, objects, or configurations.

This task removes unused Catalyst SD-WAN security objects to maintain system cleanliness and prevent clutter in the configuration.

You can delete one or multiple Catalyst SD-WAN security objects.

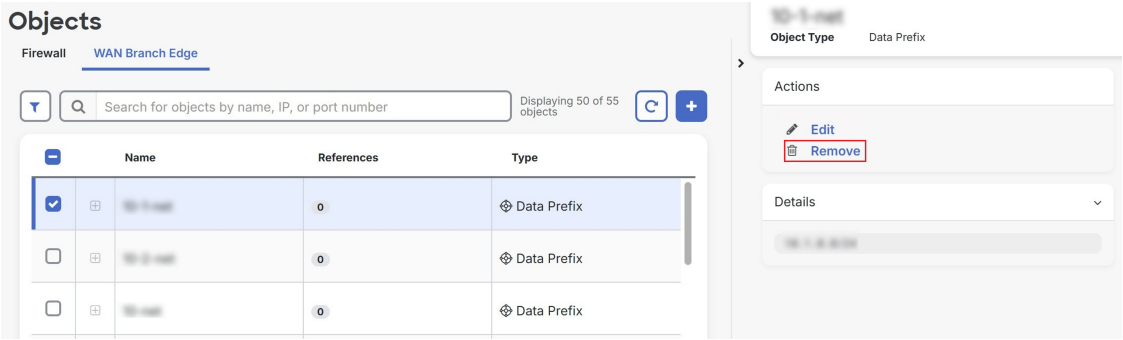
- If the security object was synchronized with Catalyst SD-WAN Manager, deleting it updates both Security Cloud Control Firewall Management and Catalyst SD-WAN Manager for consistency.
- Security policies or configurations that reference the deleted object do not get deleted automatically. You must remove the references manually from the security policies before deleting the object.
- Delete actions are logged for auditing and traceability.

Before you begin

Verify that the Catalyst SD-WAN security objects you want to delete are not used or referenced in other objects, policies, or configurations.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Objects**.
3. Click the **WAN Branch Edge** tab.
4. Check one or multiple security objects you want to delete.
5. In the **Actions** pane, click **Remove**.



6. Click **OK** to confirm.

Selected Catalyst SD-WAN security objects are deleted. Delete actions are logged for audit purposes, ensuring traceability of changes.

To view the logs:

- In the Security Cloud Control application, choose **Events & Logs** > **Logs** > **Change Log**.
- In the Catalyst SD-WAN Manager application, choose **Monitor** > **Logs** > **Audit Logs**.

Filter Catalyst SD-WAN security objects

Configure filtering and searching of security objects by Object Type and Profile Type to streamline network security management.

Filter and search for Catalyst SD-WAN security objects to efficiently locate, review, modify, or delete security objects, optimizing system performance and ensuring effective SD-WAN security object administration for WAN Branch Edge environments.

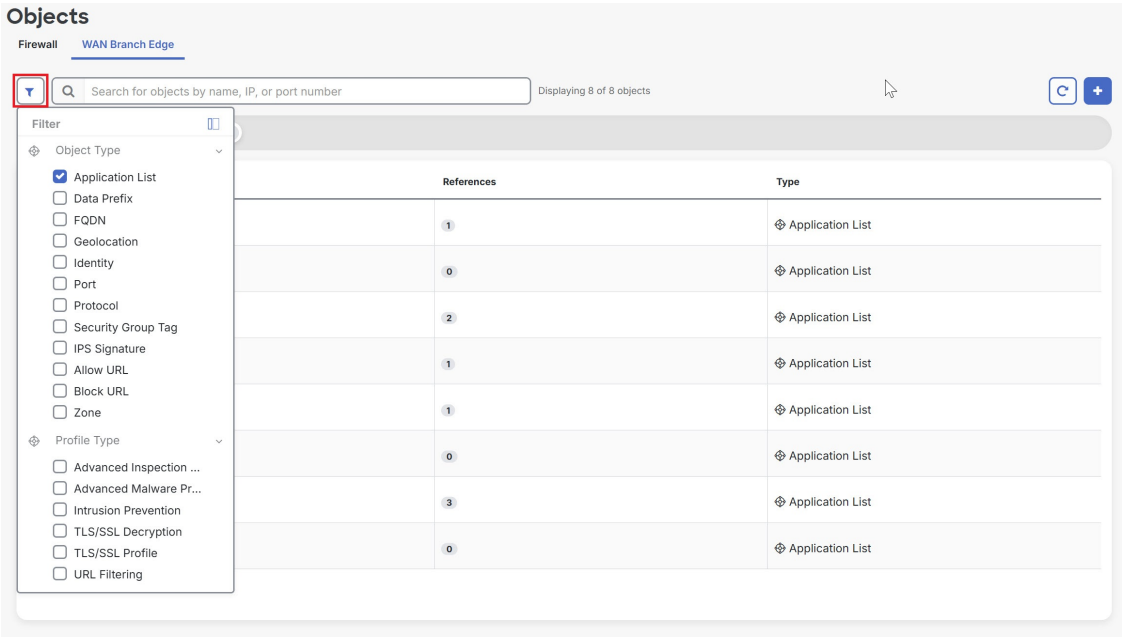
Catalyst SD-WAN Manager enables users to efficiently filter and search security objects by Object Type and Profile Type, streamlining network security management. This feature enhances the ability to locate, review, modify, or delete security objects, optimizing system performance and ensuring effective SD-WAN security object administration for WAN Branch Edge environments.

You can filter objects using two parameters: **Object Type** and **Profile Type**.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2.
3. Choose **Objects**.
4. Click the **WAN Branch Edge** tab.

5. Click the filter icon ( ) and select objects by **Object Type** or **Profile Type**.



You can use filters to search for objects. Refine the results by typing the object name, IP address, or port number to narrow the search.

The ability to filter and search for Catalyst SD-WAN security objects by **Object Type** and **Profile Type** allows users to efficiently locate, review, modify, and, when needed, delete these objects. This approach helps maintain optimal system performance.

Catalyst SD-WAN NGFW security policies

Explains how Catalyst SD-WAN Manager NGFW security policies offer robust protection for networks, systems, and data against unauthorized access and threats through comprehensive management framework for advanced cybersecurity.

NGFW security policies in Catalyst SD-WAN Manager are a set of rules and configurations that

- protect systems, networks, and data from unauthorized access, misuse, or threats
- provide comprehensive framework for implementing and managing NGFW security policies, and
- ensure advanced cybersecurity, streamlined policy control, and enhanced threat prevention for enterprise environments.

Manage existing Catalyst SD-WAN NGFW security policies

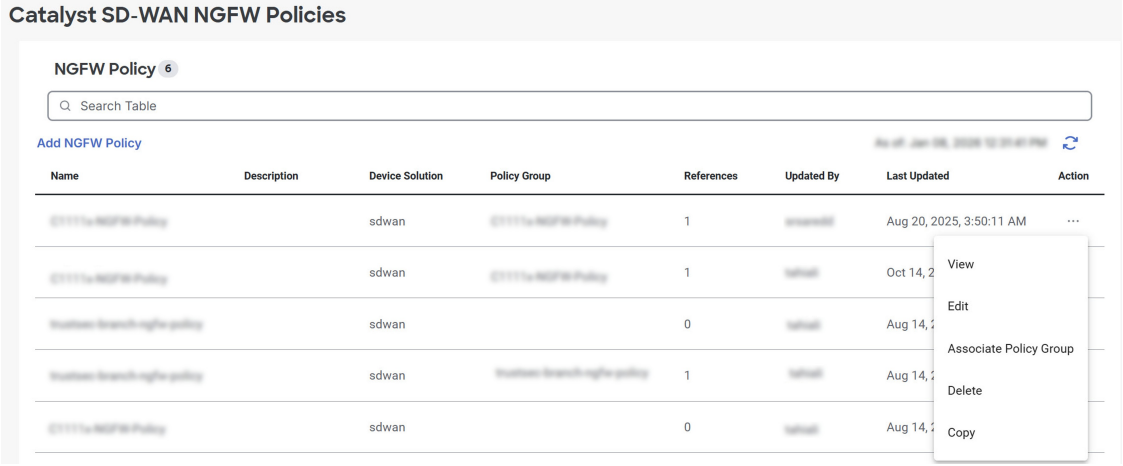
Configure management options for Catalyst SD-WAN NGFW security policies from Security Cloud Control Firewall Management.

Manage existing NGFW security policies by viewing, editing, associating policy groups, deleting, or copying them in Security Cloud Control Firewall Management.

You cannot delete a Next-Generation Firewall (NGFW) policy from Security Cloud Control Firewall Management if it is already associated with a policy group in Catalyst SD-WAN.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Policies** > **WAN Branch Edge**.
3. Navigate to the policy and click the ellipsis (...) under the **Action** column.
4. Click **View**, **Edit**, **Associate Policy Group**, **Delete**, or **Copy**.



The selected action is performed on the NGFW policy. You can view policy details, edit configurations, associate the policy with a policy group, delete the policy (if not associated), or create a copy of the policy.

Create Catalyst SD-WAN security policies

Configure Catalyst SD-WAN NGFW security policies in Security Cloud Control Firewall Management using the Create NGFW policy workflow.

Create Catalyst SD-WAN NGFW security policies to control and secure network traffic through defined sub-policies and rules.

Security policies provide granular control over network traffic flow and enable inspection of data packets based on source and destination zones, protocols, and applications.

Before you begin

Make sure you have deployed and managed these devices using a configuration group. For more information about creating configuration groups, see Configuration Groups and Feature Profiles.

Follow these steps to create Catalyst SD-WAN NGFW security policies in Security Cloud Control Firewall Management using the Create NGFW policy workflow:

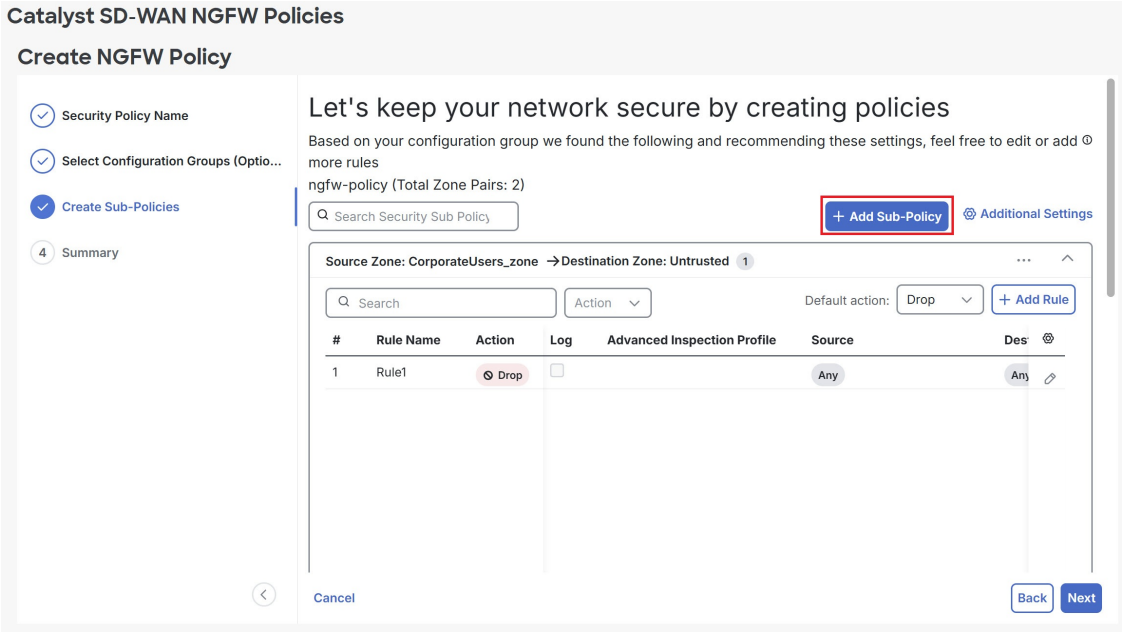
Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Policies** > **WAN Branch Edge**.
3. Click **Add NGFW Policy** on the **Catalyst SD-WAN NGFW Policies** page.

   This launches the **Create NGFW policy** workflow.

4. On the **Security Policy Name** tab, enter **Policy Name** and **Description**, and under **Device Solution**, click the **SDWAN** radio button.

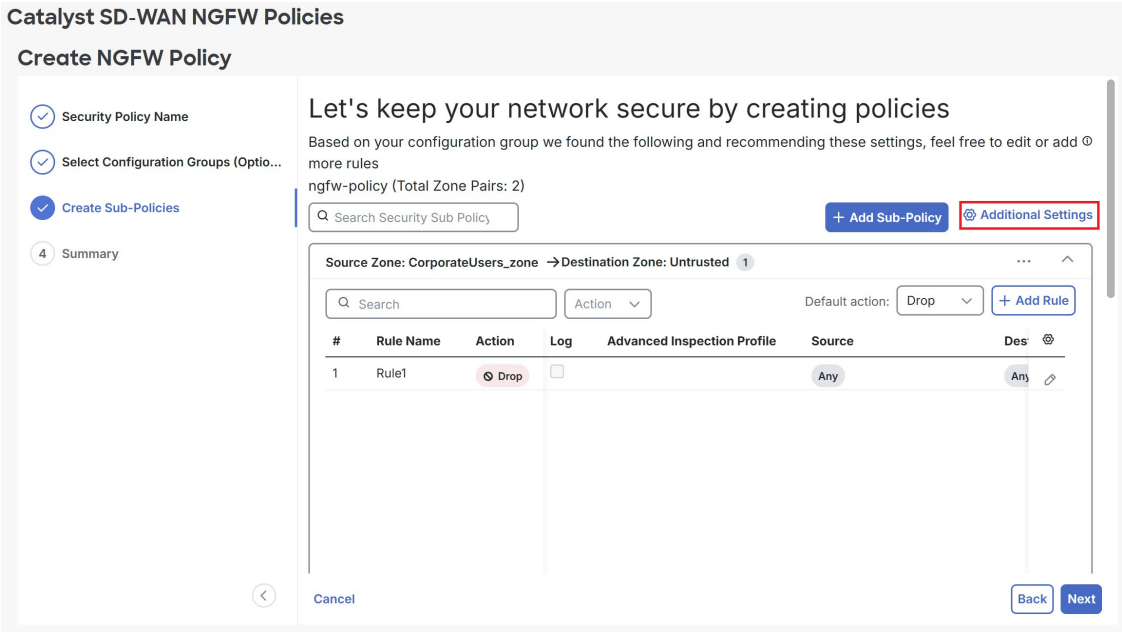
5. Click **Next**.
6. On the **Select the optional Configuration Group to associate with the NGFW policy** page, choose the configuration group to associate with the NGFW policy and click **Next**.
7. On the **Create Sub-Policies** tab, click **+Add Sub-Policy** to add sub-policies for a security policy.



Field	Description
VPN / Interface	Specify the VPN or the interface.

Field	Description
Source Zone	Choose the zone that is the source of the data packets. You can choose from these options: • Corporate_Users_zone • Local_Internet_for_Guests_zone • No_zone • Payment_Processing_Network_zone • Physical_Security_Devices_zone • Self • Untrusted Click **+ Create New** to create a new Source Zone. Enter the **Name** and select the **VPN** from the drop-down. **Note** You can select multiple VPNs within a Source Zone.
Destination Zone	Select the zones to which data traffic is sent. You can choose from these options: • Corporate_Users_zone • Local_Internet_for_Guests_zone • No_zone • Payment_Processing_Network_zone • Physical_Security_Devices_zone • Self • Untrusted To create a new Destination Zone, click **+ Create New**. Enter the **Name** and select the **VPN** from the drop-down. **Note** You can select multiple VPNs within a Destination Zone.

8. Click **Additional Settings** to configure additional settings for a security policy. For more information about the steps used in the procedure, Configure NGFW Additional Settings.
9. Click **Save**.



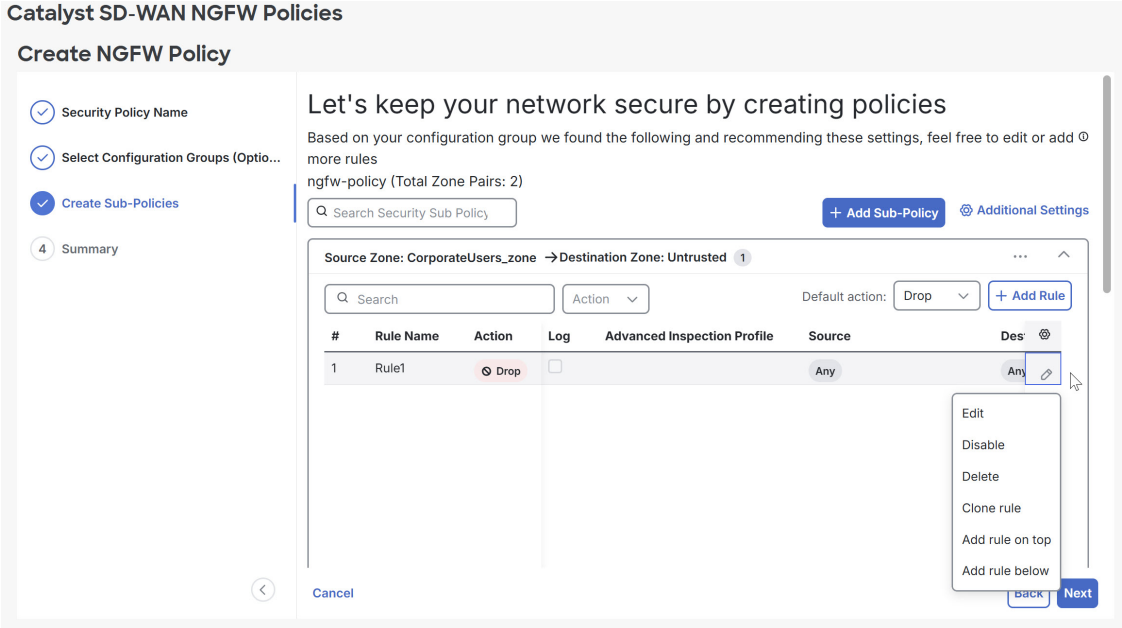
10. Click the ellipsis (...) at the top-left corner of the existing sub-policy to **Edit**, **Delete**, or **Copy** it.
11. To add an NGFW policy rule to a sub-policy, navigate to the sub-policy and click **+ Add Rule**.

Field	Description
Rule Name	The name of the rule.
Sequence	Specify the sequence.

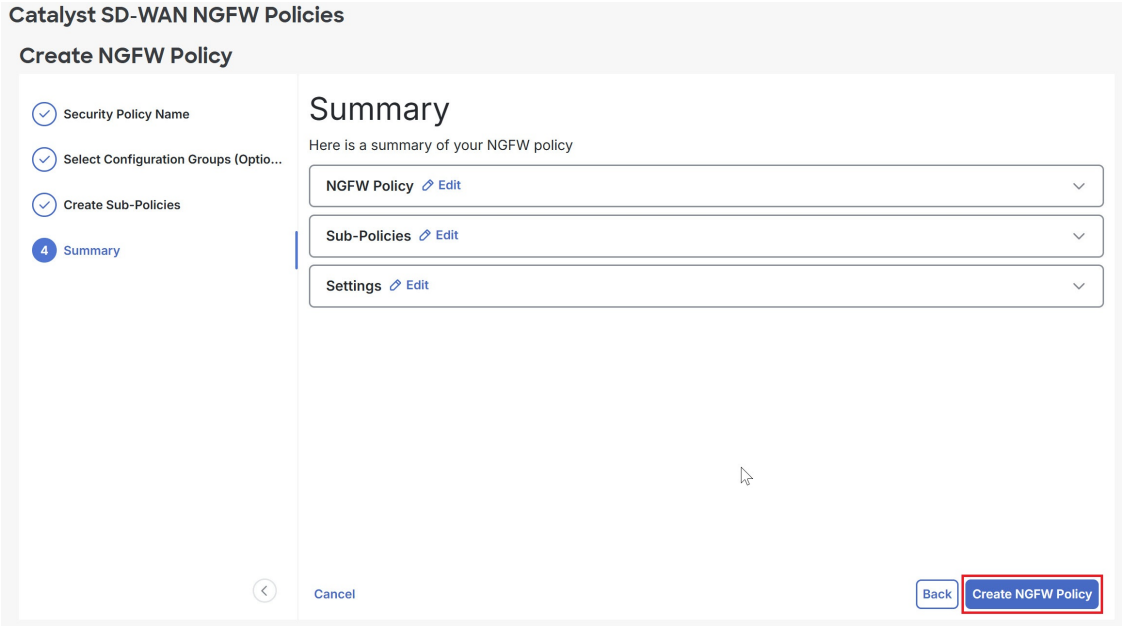
Match	Choose the desired match conditions from the **Add Conditions** drop-down list. You can choose from these options:
	• Source
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	• Destination
	  • FQDN
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	• Protocol
	• Applications
	When Identity Services Engine (ISE) is enabled, the SGT option is available in the **Source** and **Destination** fields. Identity User or User group is only supported for **Source**.

Field	Description
Action	Choose the desired action conditions. You can choose from these options: • Pass • Drop • Inspect • Log Events: Unified Logging for Inspect Action.

12. To modify an existing rule, click the pencil icon to **Edit**, **Disable**, **Delete**, **Clone rule**, **Add rule on top**, or **Add rule below**.



13. Click **Next**.
14. Review the **NGFW Policy**, **Sub-Policies**, and **Settings** on the **Summary** page, and click **Create NGFW Policy**.



The NGFW security policy is created and available in the Catalyst SD-WAN NGFW Policies list for deployment and management.

Associate a policy group to Catalyst SD-WAN NGFW policy

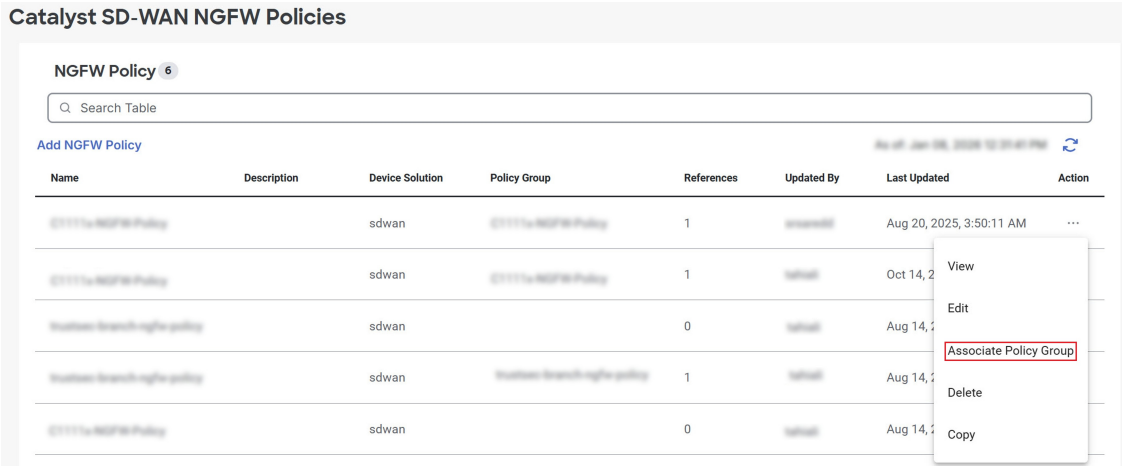
Configure policy group association with a Catalyst SD-WAN NGFW policy to ensure consistent security enforcement across managed devices.

Associate a policy group with a Catalyst SD-WAN NGFW policy to ensure consistent security enforcement across managed devices. Using Security Cloud Control Firewall Management, administrators can easily link policy groups to NGFW policies and deploy them, streamlining network security management and enhancing centralized policy deployment for WAN Branch Edge environments.

This section outlines the steps to associate a policy group with a Catalyst SD-WAN NGFW policy, enabling the policy to be deployed to devices managed by that group. This ensures consistent security enforcement across those devices. Once associated, you can deploy the policy group to activate the policy on the devices.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Policies** > **WAN Branch Edge**.
3. Navigate to the policy you want to associate with a policy group. Click the ellipsis (…) under the **Action** column, then select **Associate Policy Group**.



4. Select the policy and click **Save**.

The policy group is now associated with the NGFW policy and can be deployed to activate the policy on the managed devices within that group.

Deploy policy group from Catalyst SD-WAN Manager

Describes how a policy group in Catalyst SD-WAN streamlines NGFW security policy deployment across multiple devices or sites using Catalyst SD-WAN Manager.

A policy group in Catalyst SD-WAN is a logical grouping that

- contains related items or configurations used in Next-Generation Firewall (NGFW) security policies
- simplifies the process of applying policies across multiple devices or sites, and
- enables deployment of NGFW policy modifications, including security objects and security profiles, from Security Cloud Control Firewall Management to Secure Router devices.

Policy group deployment workflow

You can access the workflow from the **Workflows** > **Deploy Policy Group** menu in Catalyst SD-WAN Manager. This workflow enables you to associate Secure Router devices and deploy the policy group to the selected devices.

For more information, refer to the *Deploy Policy Group Workflow* section in the Policy Groups Configuration Guide, Cisco IOS XE Catalyst SD-WAN.

30 Monitor Catalyst SD-WAN Events

Topics:

- Security Analytics and Logging for Catalyst SD-WAN
- How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management
- Requirements and guidelines for SD-WAN integration
- View Catalyst SD-WAN events in Security Cloud Control Firewall Management

This chapter covers information on how to share events from your Cisco Catalyst SD-WAN Manager and view them in Security Cloud Control.

Security Analytics and Logging for Catalyst SD-WAN

Describes how Catalyst SD-WAN integrates advanced firewall and security features for centralized policy enforcement and secure cloud access. Explains how onboarding devices to Security Cloud Control enables centralized monitoring and analysis of connection events.

Security Analytics and Logging for Catalyst SD-WAN is a security management solution that

- integrates advanced firewall and security features directly into the SD-WAN fabric
- enables centralized policy enforcement and secure cloud access through Direct Internet Access (DIA) and Direct Cloud Access (DCA)
- provides centralized monitoring and analysis of connection events when devices are onboarded to Security Cloud Control, and
- supports threat hunting and comprehensive security management across distributed networks.

Security capabilities

The Secure Router integrates firewall capabilities into its architecture, ensuring robust security across distributed networks.

- Catalyst SD-WAN integrates security features directly into the SD-WAN fabric, enabling secure Direct Internet Access (DIA) and Direct Cloud Access (DCA).
- It includes next-generation firewall, integrated intrusion prevention capabilities, and URL filtering.
- The Catalyst SD-WAN platform enables you to enforce centralized policies for all users, extending enterprise VPN architectures into your private cloud.

Onboard Catalyst SD-WAN Manager to Security Cloud Control to manage the security capabilities of managed devices.

- Onboarded Catalyst SD-WAN devices send connection events to Security Analytics and Logging for storage in the cloud data store.
- Security Analytics and Logging enables you to view connection events from all Catalyst SD-WAN devices in one centralized location–the **Event Logging** page in Security Cloud Control.
- On the **Event Logging** page, you can view, filter, and search for events to perform threat hunting and analyze security rules triggered in your network.

How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management

Describes how Catalyst SD-WAN event flow enables automated sharing of security events with Security Cloud Control, allowing seamless data export, cloud storage, and enrichment for enhanced threat detection.

This process describes how Catalyst SD-WAN shares security events with Security Cloud Control Firewall Management in Security Cloud Control. This integration streamlines event visibility and analysis, empowering SOC analysts to monitor network activity and enhance threat detection using Catalyst SD-WAN security data in real time.

Summary

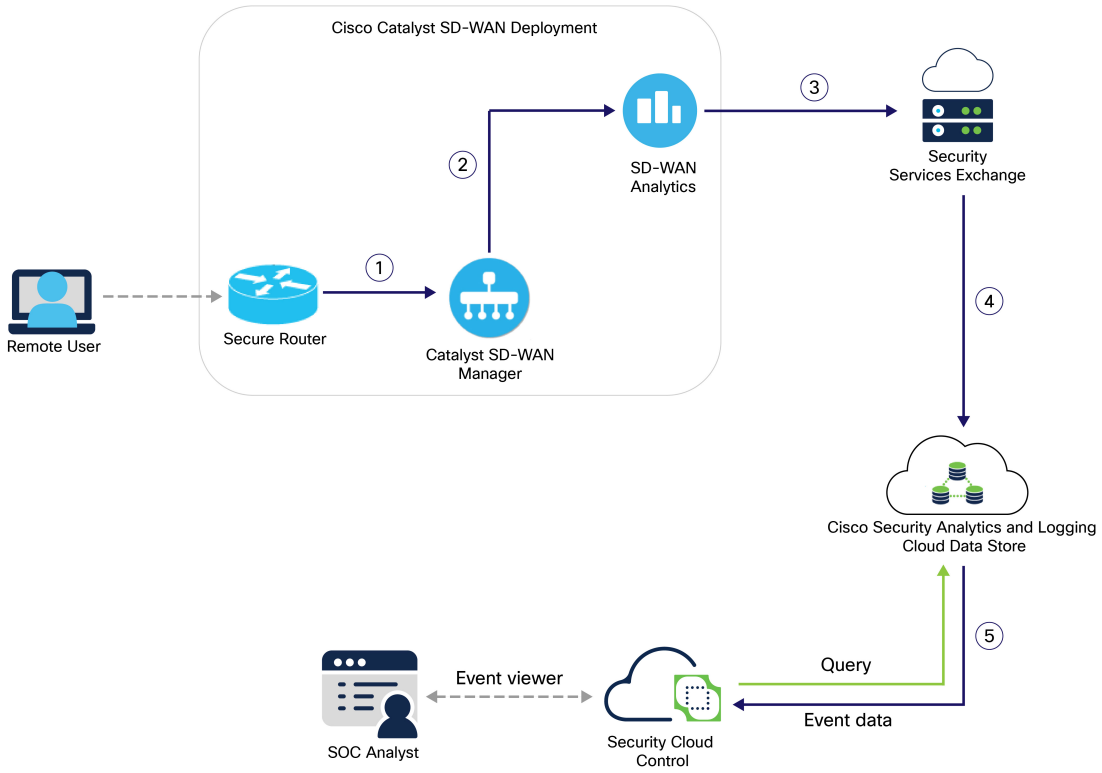
The key components involved in the event sharing process are:

- Catalyst SD-WAN device: Generates event logs for network traffic and exports data to PSV files
- Catalyst SD-WAN Manager: Receives event data from SD-WAN devices and forwards to analytics cloud

- SD-WAN Analytics cloud: Stores event data and notifies Security Services Exchange
- Security Services Exchange: Downloads event data and converts from PSV to JSON format
- Security Analytics and Logging (SaaS): Processes, classifies, and enriches event data for SOC analysts

Workflow

Figure 15: Event flow from Catalyst SD-WAN to Security Cloud Control



These stages describe how security events flow from Catalyst SD-WAN to Security Cloud Control:

1. A remote user accesses the network, and the Catalyst SD-WAN device generates an event log for the corresponding traffic. The device then exports the event data to a PSV file and sends it to Catalyst SD-WAN Manager.
2. Catalyst SD-WAN Manager sends the event data to the SD-WAN Analytics cloud.
3. SD-WAN Analytics stores the event data in cloud to make it accessible for Security Services Exchange and notifies Security Services Exchange.

   After receiving the notification from SD-WAN Analytics cloud, Security Services Exchange downloads the event data from SD-WAN AWS cloud.
4. Security Services Exchange converts the event data from PSV to JSON format and sends it to Cisco Security Analytics and Logging (SaaS).
5. Security Analytics and Logging (SaaS) processes the event data using various services to classify and enrich it for use by Security Cloud Control.

   Security Analytics and Logging (SaaS) stores the event data in the cloud data store. The event viewer queries this data store to provide security operations center (SOC) analysts with relevant event data.

Requirements and guidelines for SD-WAN integration

Outlines the requirements and guidelines for onboarding Catalyst SD-WAN Manager to Security Cloud Control for centralized visibility of connection events.

Onboard the Catalyst SD-WAN Manager to the Security Cloud Control organization where you want to view the security events.

Onboard the SD-WAN Analytics services to your Catalyst SD-WAN Manager and enable data collection.

Ensure you have a Security Cloud Control Firewall Management organization with a valid Security Analytics and Logging subscription plan.

Note that this integration supports only viewing the connection events from your Catalyst SD-WAN devices in Security Cloud Control.

Ensure that you have a Security Analytics and Logging subscription plan that reflects the number of events the Cisco cloud receives from your on-boarded Catalyst SD-WAN devices on a daily basis. This is called your *daily ingest rate*. You can use the Logging Volume Estimator tool to estimate your daily ingest rate and as that rate changes you can update your data plan.

If you do not have a Security Analytics and Logging plan subscribed, you can request a 90-day trial by logging in to Security Cloud Control and navigating to **Events & Logs** > **Events** > **Event Logging** tab. You can accurately estimate your daily ingest rate and purchase the desired subscription plan by following the instructions in the Security Cloud Control Firewall Management Ordering Guide.

View Catalyst SD-WAN events in Security Cloud Control Firewall Management

Configure filtering for Catalyst SD-WAN connection events in the event logging page to quickly identify network activity and security events.

This task enables you to streamline event analysis, enhance threat detection, and maintain compliance by filtering specific network events.

Network administrators should perform this task regularly for effective security monitoring. Use this feature to focus on relevant connection events and improve your network security posture.

Before you begin

Ensure that you have met all the requirements described in Requirements and guidelines for SD-WAN integration on page 632.

Follow these steps to view Catalyst SD-WAN events in Security Cloud Control Firewall Management:

Procedure

1. In the navigation pane, choose **Events & Logs** > **Events** > **Event Logging**.
2. Click the filter (▼) icon.
3. Scroll to the **Catalyst SD-WAN Events** section and check the **Connection** check box.

The event logging page displays filtered Catalyst SD-WAN connection events, allowing you to focus on relevant network activity and security events for analysis.

Part VII

Manage On-Premises Firewall Management Center

Topics:

- Onboard an On-Premises Firewall Management Center
- Configure On-Premises Firewall Management Center-Managed Threat Defense Devices

31 Onboard an On-Premises Firewall Management Center

Topics:

- Onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management
- Remove an On-Premises Firewall Management Center from Security Cloud Control

This chapter provides steps to onboard an On-Premises Firewall Management Center and manage associated Threat Defense devices.

Onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management

Explains how to onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management, enabling centralized device visibility, shared policy management, and streamlined provisioning using recommended integration methods and best practices.

Onboarding an On-Premises Firewall Management Center to Security Cloud Control Firewall Management is an integration process that

- enables centralized device visibility and management across security infrastructure
- provides consistent policy enforcement through shared object management, and
- supports zero-touch provisioning of devices and cloud assist capabilities.

Onboarding methods and capabilities

Security Cloud Control Firewall Management provides two methods to onboard On-Premises Firewall Management Centers.

- Preferred method (direct onboarding without Secure Device Connector): Auto discover and onboard On-Premises Firewall Management Center integrated with Cisco Security Cloud. This direct method is recommended because most cloud assist features are supported only when On-Premises Firewall Management Center is onboarded directly without using Secure Device Connector (SDC). Direct onboarding provides full access to cloud assist capabilities, such as zero-touch provisioning, centralized device visibility, and policy optimization. This is the preferred method for most use cases. For more information about integrating On-Premises Firewall Management Center with Cisco Security Cloud, refer to Integrate an On-Premises Firewall Management Center with Cisco Security Cloud on page 638.

  > **Attention**
  >
  > This method is not available to Government customers. Government customers must use the credentials method to onboard an On-Premises Firewall Management Center to Security Cloud Control.

- Alternative method (using SDC): Use On-Premises Firewall Management Center credentials with SDC is supported but intended only for very rare use cases. Onboarding with SDC limits access to many cloud assist features available with direct onboarding. Choose SDC if direct onboarding is not possible.

  For more information, see Allow inbound access for direct cloud connectivity on page 94.

Security Cloud Control complements FMC by enabling:

- Consistent policy enforcement through shared object management with FMCs.

  For more information, see the **Objects** section in Managing On-Prem Firewall Management Center with Security Cloud Control.

- Zero-touch provisioning of Firewall Threat Defense devices. For more information, refer to Onboard a Device to On-Premises Firewall Management Center with Zero-Touch Provisioning.
- Centralized visibility and management of security devices. For more information, refer to Device and Service Management.
- Integration with cloud Cisco Secure Dynamic Attributes Connector (CSDC) and Cloud-Delivered Firewall Management Center. For more information, refer to Cisco Secure Dynamic Attributes Connector.

Configuration limitations and guidelines:

- Onboarding an On-Premises Firewall Management Center also onboards all devices registered to it. Disabled or unreachable devices may appear in the **Security Devices** page in Security Cloud Control but cannot be managed or queried.
- Onboarding does not cascade policies from On-Premises Firewall Management Center to Security Cloud Control or Cloud-Delivered Firewall Management Center. To migrate Firewall Threat Defense devices to Cloud-Delivered Firewall Management Center, use the built-in **Migrate FTD to** Cloud-Delivered Firewall Management Center feature. For more information, refer to Migrate Threat Defense to Cloud-delivered Firewall Management Center.
- We recommend creating a dedicated user on the On-Premises Firewall Management Center with administrator-level permissions specifically for Security Cloud Control communication. If you log in to On-Premises Firewall Management Center with the same credentials during onboarding, the process will fail. This recommendation applies only to credentials-based onboarding, not to direct integration.
- For this dedicated user, set the **Maximum Number of Failed Logins** to zero.
- For On-Premises Firewall Management Centers version 7.4 or later, if a switchover causes a loss of cloud connectivity, disable and then re-enable **SecureX**, **Security Cloud Control**, or **Cisco Security Cloud** (depending on your version) to restore the connection.

Auto onboard an On-Premises Firewall Management Center integrated with Cisco Security Cloud

Configure automatic onboarding of an On-Premises Firewall Management Center integrated with Cisco Security Cloud, ensuring seamless discovery and enrollment of both the management center and its associated devices for centralized security management.

This task enables automatic discovery and onboarding of an On-Premises Firewall Management Center integrated with Cisco Security Cloud for centralized security management.

> **Attention**
>
> This method is not available to Government customers. Government customers must use the credentials method to onboard an On-Premises Firewall Management Center to Security Cloud Control.

The auto-discovery and onboarding feature is enabled by default in Security Cloud Control. All On-Premises Firewall Management Centers running version 7.2 or later and integrated with Cisco Security Cloud are automatically discovered and onboarded to Security Cloud Control. The associated Firewall Threat Defense devices are onboarded to Security Cloud Control.

Security Cloud Control also onboards the On-Premises Firewall Management Center high-availability (HA) pair.

Before you begin

Ensure that outbound traffic is allowed from port 443 on the On-Premises Firewall Management Center.

Follow these steps to auto onboard an On-Premises Firewall Management Center integrated with Cisco Security Cloud:

Procedure

1. Integrate the On-Premises Firewall Management Center you want to onboard with Cisco Security Cloud and register it with a Security Cloud Control tenant.

   For more information, see Integrate an On-Premises Firewall Management Center with Cisco Security Cloud on page 638.

2. Log in to the Security Cloud Control tenant that was registered with the On-Premises Firewall Management Center.
3. From the Security Cloud Control Home page, click **Firewall**.
4. Choose **Administration** > **Integrations** > **Firewall Management Center**.

   All On-Premises Firewall Management Centers associated with your tenant are displayed in the **FMC** tab. For more information, see View Onboarded On-Premises Firewall Management Center.

The On-Premises Firewall Management Center and its associated devices are automatically onboarded to Security Cloud Control for centralized security management.

Integrate an On-Premises Firewall Management Center with Cisco Security Cloud

Configure an On-Premises Firewall Management Center integration with Cisco Security Cloud to enable seamless registration, tenant selection or creation, and centralized management of your firewall devices using a guided integration process.

This integration enables your management center to be registered to the Cisco cloud tenancy and provides centralized management capabilities for your firewall devices.

This procedure describes how to integrate the On-Premises Firewall Management Center with Cisco Security Cloud. By enabling Cisco Security Cloud integration, your management center gets registered to the Cisco cloud tenancy.

Before you begin

When onboarding an On-Premises Firewall Management Center:

- If you already have a Security Cloud Control tenant, you will be prompted to confirm whether you want to attach the On-Premises Firewall Management Center to that existing tenant.
- If you do not have a tenant or account, the On-Premises Firewall Management Center integration wizard will automatically create a new tenant for you during the registration task the onboarding process. This tenant is a free tier provided exclusively for On-Premises Firewall Management Center AI Assist enablement. Allow the wizard to manage tenant creation so that you do not receive a trial tenant that would later require conversion. The wizard manages this process to provide a seamless experience.
- If you intend to use the Cloud-Delivered Firewall Management Center or manage firewalls using the Security Cloud Control, you must purchase a base license and device entitlements. For detailed licensing information and product options, refer to the Security Cloud Control Licensing Overview.

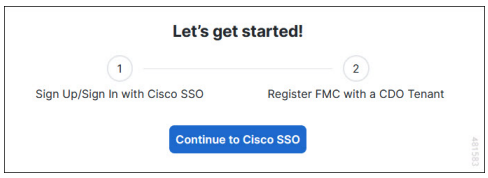
Procedure

---

1. Based on your On-Premises Firewall Management Center version, do:
   - For On-Premises Firewall Management Center version between 7.2 and 7.4.x, click **Enable Secure X**.
   - For On-Premises Firewall Management Center version 7.6 or later, click **Cisco Security Cloud**.
   - For On-Premises Firewall Management Center version 10.0 or later, click **Security Cloud Control**.

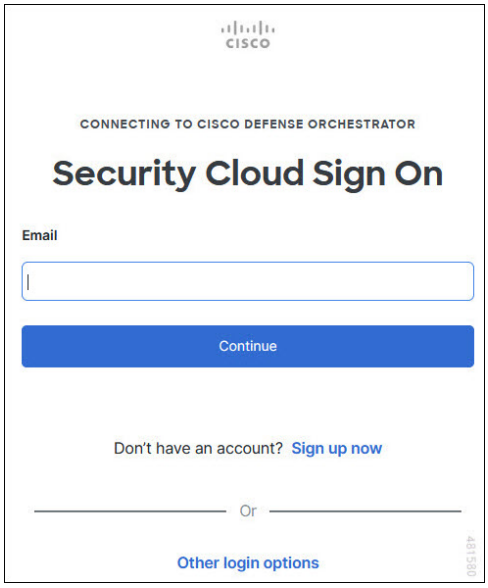
   A separate browser tab opens to log you in to your Security Cloud Control account. Make sure this page is not blocked by a pop-up blocker.
2. Click **Continue to Cisco SSO**.

   Figure 16: Cisco security cloud welcome page



3. Log in to your Security Cloud Control account.

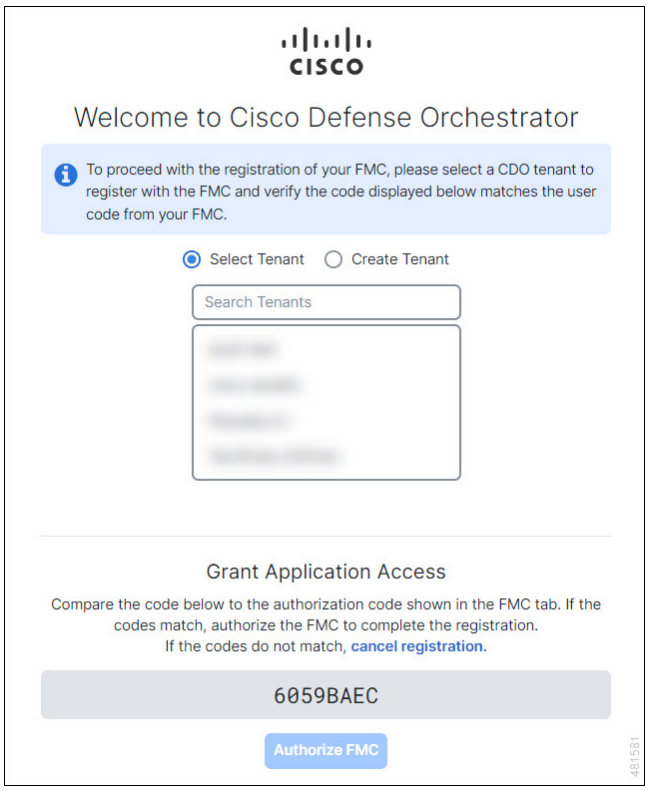
Figure 17: Cisco security cloud sign on



If you do not have a security cloud sign on account to log in to Security Cloud Control and you want to create one, click **Sign up now** in the **Security Cloud Sign On** page.

4. Choose a Security Cloud Control tenant that you want to use for this integration. The On-Premises Firewall Management Center and the managed devices get onboarded to the Security Cloud Control tenant that you choose here.

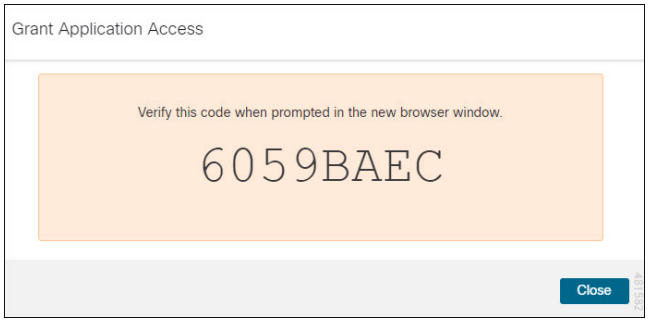
Figure 18: Choose the Security Cloud Control Tenant



If you do not have a security cloud sign on account to log in to Security Cloud Control and you want to create one, click **Sign up now** in the **Security Cloud Sign On** page. See Create a New Cisco Security Cloud Sign On Account.

5. Verify that the code displayed in the Security Cloud Control login page matches the code provided by the On-Premises Firewall Management Center.

Figure 19: Verification Code in the On-Premises Firewall Management Center



6. Click **Authorize FMC**.
7. In the On-Premises Firewall Management Center UI, click **Save** to save the configuration.

   You can view the task progress under **Notifications** > **Tasks**.

   The registration task can take up to 90 seconds to complete. If you must use On-Premises Firewall Management Center while the registration task is in progress, open the On-Premises Firewall Management Center in a new window.

The On-Premises Firewall Management Center is now integrated with Cisco Security Cloud and registered to your selected tenant for centralized management capabilities.

Auto onboard On-Prem FMCs from Cisco security cloud

Configure the auto-onboarding settings for On-Premises Firewall Management Centers from your Cisco Security Cloud to your Security Cloud Control tenant to ensure only authorized devices are added.

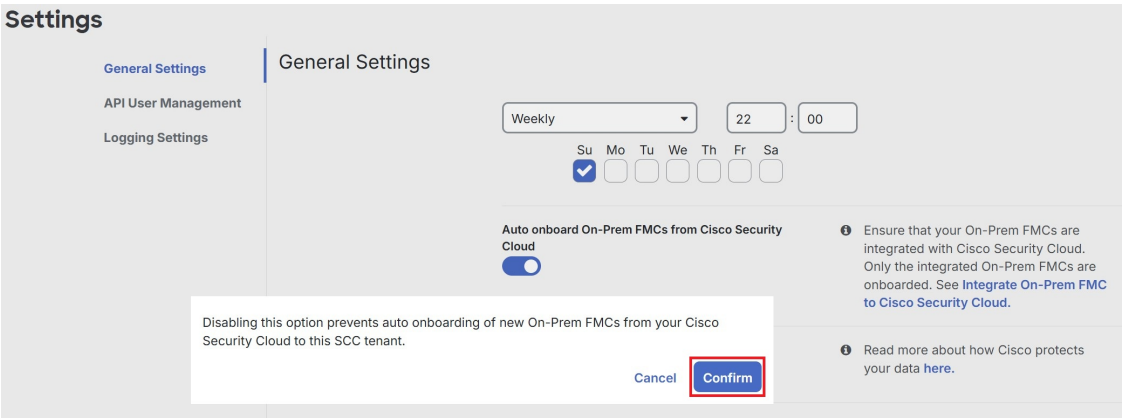
Disable the auto-onboarding of On-Premises Firewall Management Centers from your Cisco Security Cloud to your Security Cloud Control tenant to control device authorization.

Disabling the auto-onboarding functionality stops new On-Premises Firewall Management Centers from being automatically added from your Cisco Security Cloud tenant. This procedure is available to Super Admins and Admins.

> **Note**
>
> Only a Super Admin or Admin can enable or disable this functionality on Security Cloud Control.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn off the **Auto onboard On-Prem FMCs from Cisco Security Cloud** toggle button to disable the auto-onboarding of On-Premises Firewall Management Center.
4. Click **Confirm**.



Auto-onboarding is disabled and new On-Premises Firewall Management Centers will not be automatically added from your Cisco Security Cloud tenant.

Onboard an On-Premises Firewall Management Center to Security Cloud Control with Credentials

Configure an On-Premises Firewall Management Center to connect to Security Cloud Control using credentials, ensuring proper connectivity and secure access through either a Secure Device Connector or Cloud Connector.

This task enables centralized management of your On-Premises Firewall Management Center through Security Cloud Control by establishing secure connectivity and authentication.

To onboard an On-Premises Firewall Management Center to Security Cloud Control with credentials, follow this procedure:

Before you begin

These prerequisites must be met:

- **For Cloud Secure Device Connector (SDC)**: Allow inbound traffic on port 443 of the On-Premises Firewall Management Center.

  The SDC reaches the On-Premises Firewall Management Center by allowing inbound traffic on port 443.



  Both the Security Cloud Control and the SDC are hosted in the cloud.

- **For On-Premises Secure Device Connector (SDC)**: Allow outbound connectivity on port 443 of the SDC.

  The SDC requires connectivity to the Security Cloud Control, making it imperative to permit outbound traffic from the SDC to the Security Cloud Control. No additional port configuration is required on on-premises Firewall Management Center.

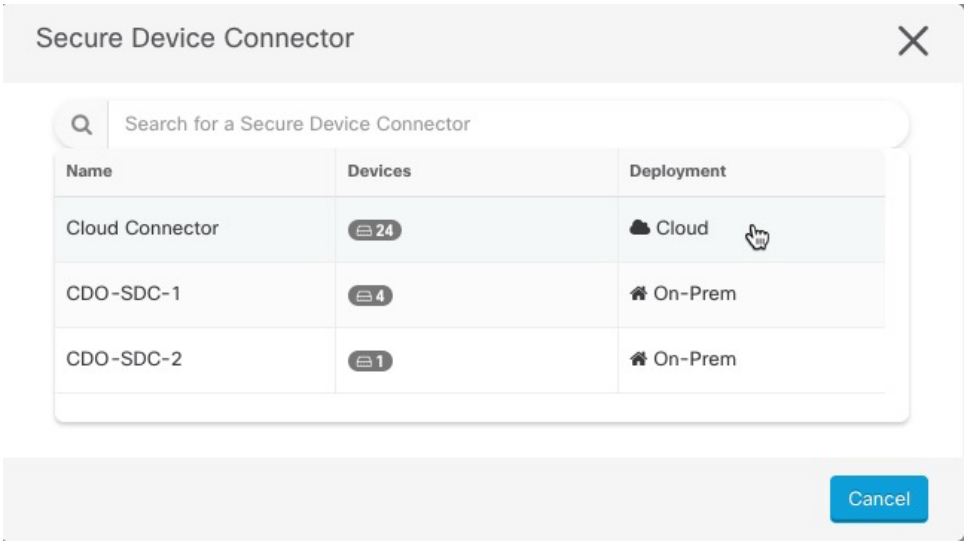


Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Click  to onboard an On-Premises Firewall Management Center.
4. Click **Firewall Management Center**.
5. Select the **Use Credentials** card.
6. Click the **Secure Device Connector** button and select an SDC installed in your network.

   If you would rather not use an SDC, Security Cloud Control can connect to your On-Premises Firewall Management Center using the Cloud Connector. Your choice depends on how you connect Security Cloud Control to your managed devices.

Figure 20: Choose a secure device connector



7. Enter the device name and location and click **Next**.
8. Enter the **Username** and **Password** of the account credentials you want to use to access the On-Premises Firewall Management Center. Click **Next**.
9. After you onboard the device, you can add labels to your On-Premises Firewall Management Center, or you can click **Go to Services** to view the page of onboarded devices. If the device is healthy, the FMC displays a **Synced** status.

> **Note**
>
> Devices managed by On-Premises Firewall Management Center are automatically named as "*<fmcname>_<manageddevicename>*."

The On-Premises Firewall Management Center is successfully onboarded to Security Cloud Control and can be managed centrally with a **Synced** status indicating successful connectivity.

Redirect Security Cloud Control to an On-Premises Firewall Management Center

Configure the management interface hostname to include the FQDN in your On-Premises Firewall Management Center, enabling seamless cross-launch from Security Cloud Control to the device UI.

Update the management interface hostname to enable cross-launch functionality from Security Cloud Control to the On-Premises Firewall Management Center UI.

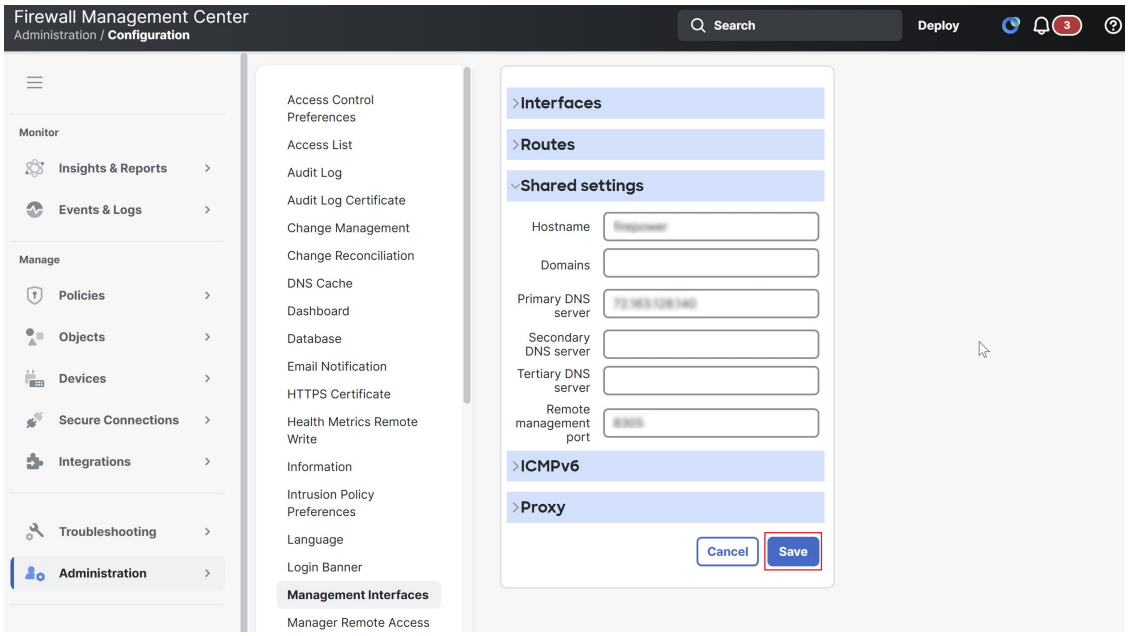
After you onboard an On-Premises Firewall Management Center to Security Cloud Control, update the management interface's hostname in the On-Premises Firewall Management Center UI so that it contains the FQDN. If you do not update the management interface's hostname, you cannot cross-launch from Security Cloud Control.

Follow these steps to update the management interface hostname and redirect from Security Cloud Control to On-Premises Firewall Management Center:

Procedure

1. Log in to the On-Premises Firewall Management Center UI.
2. Choose **Administration** > **Configuration**.

3. Click the **Management Interfaces** tab.
4. Under **Shared Settings**, locate the **Hostname** field and enter the Firewall Management Center's FQDN.
5. Click **Save**.



> **Note**
>
> You may have to log out of Security Cloud Control before you can click **Manage Devices in Firepower Management Center** and cross-launch to the On-Premises Firewall Management Center UI.

The management interface hostname is updated with the FQDN, enabling cross-launch functionality from Security Cloud Control to the On-Premises Firewall Management Center UI.

Remove an On-Premises Firewall Management Center from Security Cloud Control

Configure removal of an On-Premises Firewall Management Center and its managed devices from Security Cloud Control by disabling auto-onboarding and following the device removal steps in the **Administration** settings.

This task removes an On-Premises Firewall Management Center and all its managed devices from your Security Cloud Control tenant to clean up your device inventory.

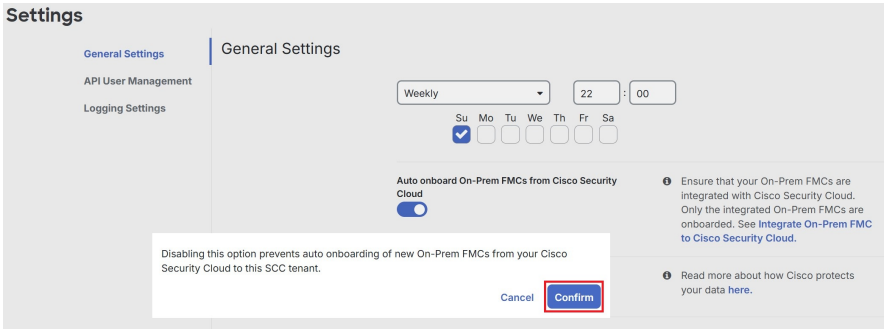
If you remove an On-Premises Firewall Management Center from Security Cloud Control, all devices managed by that On-Premises Firewall Management Center will also be removed.

Before you begin

To remove one or more On-Premises Firewall Management Centers that were onboarded using auto-onboarding, first disable the auto-onboarding option.

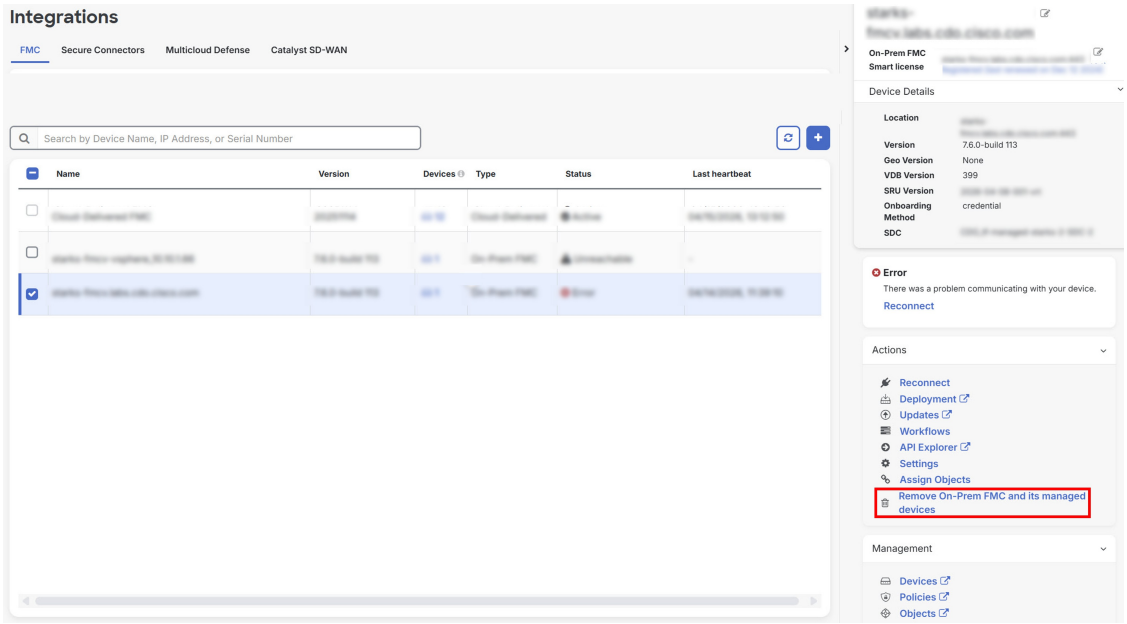
1. Choose **Administration** > **General Settings**.

2. In the **Tenant Settings** section, disable **Auto onboard On-Prem FMCs integrated to Cisco Security Cloud**.



Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Firewall Management Center**.
3. Click the **FMC** tab.
4. Choose the On-Premises Firewall Management Center you want to remove.
5. In the **Device Actions** pane, click **Remove On-Prem FMC and its managed devices**.



6. Click **OK** to confirm that you want to remove On-Premises Firewall Management Center and its managed devices from your tenant.
7. Refresh your browser to see an updated list of devices.

The On-Premises Firewall Management Center and all its managed devices are removed from your Security Cloud Control inventory.

32 Configure On-Premises Firewall Management Center-Managed Threat Defense Devices

Topics:

- Manage On-Premises Firewall Management Center with Security Cloud Control
- View onboarded On-Premises Firewall Management Center
- Discover and manage On-Premises Firewall Management Center network objects

This chapter guides users through configuring, managing, and deploying changes to On-Premises Firewall Management Center devices using Security Cloud Control, including viewing, updating, and removing managed resources.

This chapter provides steps to configure On-Premises Firewall Management Center-managed Threat Defense devices.

Manage On-Premises Firewall Management Center with Security Cloud Control

Learn how to onboard, view, manage, and cross-launch to On-Premises Firewall Management Center in Security Cloud Control. You can manage devices, monitor status, and handle network objects.

About On-Premises Firewall Management Center

On-Premises Firewall Management Center is a centralized management console with graphical user interface. You can use it to perform administrative, management, analysis, and reporting tasks. This console is similar to ASDM and FDM, but provides different features.

On-Premises Firewall Management Center support is limited to onboarding, viewing its managed devices, viewing, managing network objects, and cross-launching to the On-Premises Firewall Management Center UI for managing associated devices and objects. Additional features will be available soon.

If a feature is not supported by Security Cloud Control at this time, use the On-Premises Firewall Management Center console. To learn more about the features provided by On-Premises Firewall Management Center, see Cisco Secure Firewall Management Center Configuration Guide for your system's version.

For a list of On-Premises Firewall Management Center devices and software versions that Security Cloud Control supports, see Software and Hardware support by Security Cloud Control.

Version Support

Security Cloud Control supports version 6.4 and later. On-Premises Firewall Management Center can manage older devices, typically a few major versions back. For example, devices running version 6.6.0 can manage devices running version 6.4.0. If an On-Premises Firewall Management Center manages a device that is running a version earlier than 6.4, the device may be displayed in the **Security Devices** page, but cannot be deployed to or its policies modified from Security Cloud Control. You must make changes and deploy from the On-Premises Firewall Management Center UI.

> **Note**
>
> If a managed device is disabled, or unreachable, Security Cloud Control may display the device in the **Security Devices** page, but cannot successfully send requests or view device information.

How does Security Cloud Control Communicate with an FMC

Security Cloud Control acts as a REST API client to send requests to On-Premises Firewall Management Center, and then On-Premises Firewall Management Center uses its designated client to channel the requests to its managed devices.

As the device does not allow multiple logins with the same credentials, you must create a new user on the On-Premises Firewall Management Center specifically for Security Cloud Control communication. This user must have administrator-level permissions. This new user will have to be replicated on Security Cloud Control, as either a Security Cloud Control-provided Administrator or a custom user role with **system** and **devices** permissions. Without an admin login, Security Cloud Control cannot use REST API commands to modify or create policies, rules, or objects.

Onboard or Remove an On-Premises Firewall Management Center

You can onboard or remove an On-Premises Firewall Management Center at any time. On-Premises Firewall Management Center and its registered devices must be running at least version 6.4 to be read by Security Cloud Control. To onboard an On-Premises Firewall Management Center and its registered devices, see Onboard an FMC.

Once an On-Premises Firewall Management Center is onboarded, select the On-Premises Firewall Management Center from **Administration** > **Integrations** > **Firewall Management Center** and click **Devices** under **Management** or any actions on the right pane to open up the **Verify FMC Cross Launch URL** wizard, which allows you to enter

the public IP address or the FQDN and the port number of your management center. Click **Continue** to cross-launch to the selected On-Premises Firewall Management Center web UI in a new tab using the IP address you entered. You can also add external links manually using the **Add External Links** option under **External Links** on the right pane.

Removing an On-Premises Firewall Management Center from your Security Cloud Control tenant also removes the devices registered to that On-Premises Firewall Management Center. See Remove an FMC from Security Cloud Control for more information.

If an On-Premises Firewall Management Center experiences an "Invalid Credentials" status after onboarding, you can **reconnect** the appliance. See Troubleshoot Invalid Credentials for more information.

> **Note**
>
> Devices running Firewall 6.6 do not support the **reconnect** feature. If you have to reconnect the appliance, we recommend removing the On-Premises Firewall Management Center and re-onboarding the appliance.

Devices Managed by an On-Premises Firewall Management Center

Once you onboard an On-Premises Firewall Management Center to Security Cloud Control, all the devices registered to that On-Premises Firewall Management Center are also imported into Security Cloud Control. On the **Security Devices** page, you can view device information such as name, IP address, device type, software version, and state.

> **Note**
>
> Your On-Premises Firewall Management Center is displayed on the **Services** page, and the devices it manages are listed on the **Security Devices** page.

In the **Services** page, you can see information such as version, devices managed, device type, and status. Clicking the devices icon on the **Services** page, which shows the number of devices your FMC manages, directs you to the **Security Devices** page with a filter applied to display all devices managed by the selected On-Premises Firewall Management Center.

You can perform actions using options in the **Device Actions**, **Monitoring**, **Device Management**, and **Policies** panels available from the **Security Devices** page. If you select a device that is currently managed by an FMC and click these options, Security Cloud Control automatically launches the On-Premises Firewall Management Center console that manages the devices using the cross-launch URL you had entered.

Use the filter icon to further organize the **Security Devices** page. From this page, you can view all the devices managed by the onboarded On-Premises Firewall Management Center and other supported device types. In addition, you can expand or collapse devices in a cluster and select them individually or as a group to perform actions.

Device Health Status

Security Cloud Control displays the health status of threat defense devices on the **Security Devices** page, such as **Normal**, **Error**, **Warning**, and **Disabled**. You can click the status of a device to navigate to the **Health Monitoring** page that corresponds to the device in the On-Premises Firewall Management Center UI.

> **Note**
>
> Security Cloud Control automatically updates the device health status every 10 minutes. You can also do this manually by selecting the device and clicking **Check for Changes**.

Objects

After you onboard an On-Premises Firewall Management Center to Security Cloud Control, you can choose to discover objects from On-Premises Firewall Management Center and manage them in Security Cloud Control. You can do this by choosing **Administration** > **Integrations** > **Firewall Management Center**, selecting the desired On-Premises Firewall Management Center, and clicking **Settings**. You can enable the **Discover & Manage Network Objects** toggle button. When this option is enabled, Security Cloud Control automatically imports all the objects from the On-Premises Firewall Management Center-managed devices into Security Cloud Control. Once imported, the objects can be managed from Security Cloud Control.

> **Note**
>
> You must have the super-admin or admin user role to use the **Settings** button.

When you change an object configuration in Security Cloud Control, Security Cloud Control stages the change. After you review it in **Pending Changes**, you can manually push the change to On-Premises Firewall Management Center. When you make a configuration change to an object from the On-Premises Firewall Management Center UI, Security Cloud Control detects that change as an out-of-band change that can be synchronized later. If you want your changes to be automatically synchronized with On-Premises Firewall Management Center and not staged for review, enable the **Enable automatic sync of network objects** toggle button.

If you have existing objects in Security Cloud Control that you want to assign to your On-Premises Firewall Management Center, select the On-Premises Firewall Management Center from the **Services** page and choose **Assign Objects** on the right pane. Security Cloud Control displays all the existing objects and allows you to select the ones that you want to associate with the On-Premises Firewall Management Center that you selected. Use this to ensure that network object definitions are consistent across all platforms you manage with Security Cloud Control. You can use the **Assign Objects** button only if **Discover & Manage Network Objects** is enabled for the selected On-Premises Firewall Management Center.

> **Note**
>
> - You cannot enable the **Discover & Manage Network Objects** toggle button if the On-Premises Firewall Management Center that you have selected has one or more child domains or has the Change Management workflow enabled on it.
> - You cannot enable the **Enable automatic sync of network objects** toggle button if the **Discover & Manage Network Objects** toggle button is disabled.

On-Premises Firewall Management Center supports the following object types:

- Network Objects

- Network Group Objects

Object Issues

Security Cloud Control identifies duplicate, inconsistent, or unused objects, and you can filter the issues based on their issue states. However, Security Cloud Control cannot resolve object issues.

Eventing

Searching and filtering the historical and live event tables for specific events works the same way as it does for other information in Security Cloud Control. For more information, see Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide.

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging allows you to capture connection, intrusion, file, malware, and security intelligence events from all your devices and view them in a single location in Security Cloud Control.

You can view events stored in the Cisco cloud on the Event Logging page in Security Cloud Control. Use filters to review which security rules are triggered in your network. The **Logging and Troubleshooting** package gives you these capabilities.

With the **Firewall Analytics and Monitoring** package, the system can apply Secure Cloud Analytics dynamic entity modeling to your events and use behavioral modeling analytics to generate Secure Cloud Analytics observations and alerts. If you obtain a **Total Network Analytics and Monitoring** package, the system applies dynamic entity modeling to both your device events and your network traffic and generates observations and alerts. You can cross-launch from Security Cloud Control to a Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On.

View onboarded On-Premises Firewall Management Center

Configure viewing and management of onboarded On-Premises Firewall Management Centers, including high-availability pairs, and cross-launch directly to the active or specific management center node using customizable URLs in Security Cloud Control Firewall Management.

This task enables you to view onboarded On-Premises Firewall Management Centers, manage high-availability pairs, and cross-launch directly to management center nodes.

Use this procedure when you need to access and manage onboarded On-Premises Firewall Management Centers in your Security Cloud Control Firewall Management environment. This includes viewing high-availability configurations and cross-launching to specific management center nodes.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Firewall Management Center**.
3. Click the **FMC** tab.
4. View the On-Premises Firewall Management Center high-availability pair in the **Services** page.

   When you expand the pair, you can see the primary and secondary On-Premises Firewall Management Center nodes and their current statuses.
5. To cross-launch the active On-Premises Firewall Management Center, check the corresponding high-availability pair in the **Services** page.
6. Click the option you want to open in On-Premises Firewall Management Center.

The **Verify FMC Cross Launch URL** window is displayed. By default, the public IP address or FQDN of the currently active On-Premises Firewall Management Center is shown and will be used to open On-Premises Firewall Management Center. If necessary, specify the URL of the standby On-Premises Firewall Management Center to launch it.

7. To cross-launch to a specific On-Premises Firewall Management Center node, expand the high-availability pair and click primary or secondary On-Premises Firewall Management Center node you want to launch.
8. In the **External Links** pane, click **FMC Cross Launch URL** to cross-launch the selected On-Premises Firewall Management Center.

   To update the public IP address or the FQDN and the port number of your On-Premises Firewall Management Center hover over the **FMC Cross Launch URL** and click the edit icon.

   Add cross-launch URLs to each On-Premises Firewall Management Center node. When you launch from the pair, only the active node is launches. Verifying which node is currently active is not necessary.

> **Note**
>
> If high availability is broken or roles are switched on On-Premises Firewall Management Center (version 7.4.x or earlier), disable the SecureX integration, then enable it again on the secondary On-Premises Firewall Management Center. To complete this task, navigate to the secondary On-Premises Firewall Management Center and choose the appropriate option.
>
> If you break a high-availability On-Premises Firewall Management Center pair, the participating management centers become two standalone On-Premises Firewall Management Centers.

You can view and manage onboarded On-Premises Firewall Management Centers and cross-launch to either the active node in a high-availability pair or a specific management center node.

Discover and manage On-Premises Firewall Management Center network objects

Configure the discover and manage objects feature for On-Premises Firewall Management Centers managed by Security Cloud Control.

Enable object discovery and management for On-Premises Firewall Management Centers so you can share and manage network objects across platforms managed by Security Cloud Control.

If you have an On-Premises Firewall Management Center that you manage using Security Cloud Control and you want to share and manage its objects, perform this procedure.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Firewall Management Center** to view the **Services** page.
3. If you have already onboarded an On-Premises Firewall Management Center to Security Cloud Control, select it.

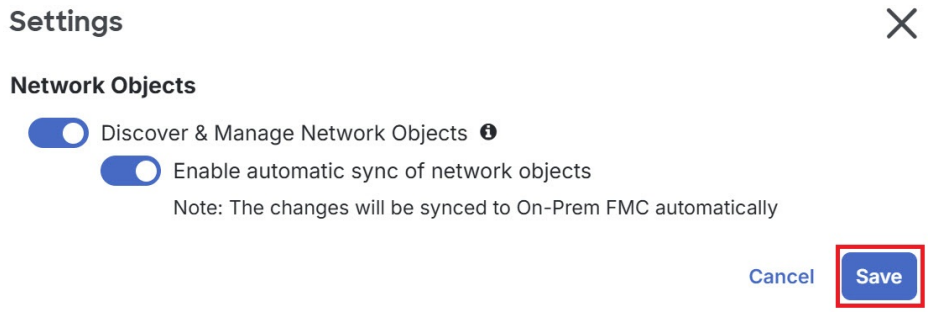
   If you want to onboard a new On-Premises Firewall Management Center, see Onboard an On-Prem Firewall Management Center.

4. Choose **Settings** from the **Actions** pane.

   The **Actions** pane does not appear when you select more than one On-Premises Firewall Management Center.

> **Note**
>
> You must be an admin or super admin to use **Settings**.

5. Enable the **Discover & Manage Network Objects** toggle button. To automatically synchronize your changes with On-Premises Firewall Management Center instead of staging them for review, turn on the **Enable automatic sync of network objects** toggle button. Then, click **Save**.



> **Note**
>
> - You cannot enable the **Discover & Manage Network Objects** toggle button if the selected On-Premises Firewall Management Center has one or more child domains or if it has the Change Management workflow enabled.
> - You cannot enable the **Enable automatic sync of network objects** toggle button if the **Discover & Manage Network Objects** toggle button is disabled.

For every new On-Premises Firewall Management Center onboarded to Security Cloud Control, this toggle button needs to be enabled manually. After you enable this option, Security Cloud Control discovers objects from your On-Premises Firewall Management Center. You can then share and manage these objects, and use them to set consistent object definitions across other platforms managed by Security Cloud Control.

In Security Cloud Control, when you add overrides to objects that are discovered from an On-Premises Firewall Management Center and push the changes back, these objects can now be overridden, even if overrides were not allowed previously. The **Allow Overrides** check box in the **View Network Object** window is selected automatically when an override is added from Security Cloud Control.

> **Note**
>
> If you want to assign already-existing objects in Security Cloud Control to your On-Premises Firewall Management Center, choose the On-Premises Firewall Management Center and click **Assign Objects** from the **Actions** pane.

The discover and manage network objects feature is enabled for the selected On-Premises Firewall Management Center, allowing Security Cloud Control to discover and manage its network objects.

Part VIII

Manage Cisco Umbrella

Topics:

- Onboard an Umbrella Organization
- Configure an Umbrella Organization

33 Onboard an Umbrella Organization

Topics:

- Onboarding an umbrella organization

This chapter provides steps to onboard Cisco Umbrella Organization.

Onboarding an umbrella organization

Explains how to onboard an Umbrella organization to the system, including the required prerequisites, connector selection process, credential configuration, label assignment, and inventory results review.

Umbrella license requirements

Lists the required license packages for onboarding an Umbrella organization to Security Cloud Control.

To onboard an Umbrella organization to Security Cloud Control, you must have one of these license packages selected from the Umbrella dashboard.

- Umbrella SIG Essentials
- SIG Advantage

To verify the licenses that are currently enabled, log in to the Umbrella dashboard and navigate to **Admin** > **Licensing**.

Generate an API key and secret

Configure a new API key and retrieve both the API Key and the corresponding Secret before you onboard an Umbrella organization to Security Cloud Control.

This task enables you to create API credentials required for integrating Umbrella with Security Cloud Control.

Generate a new API key and retrieve both the **API Key** and the corresponding **Secret** before you onboard an Umbrella organization to Security Cloud Control.

If you do not currently have an API key, use this procedure to create one.

Before you begin

The management API key from Umbrella is used for these Umbrella services.

- Networks and Domains
- Network Tunnels
- Users and Roles
- Destination Lists
- Service Providers

You cannot onboard an Umbrella organization without allowing Security Cloud Control access to these services.

Procedure

1. Access the Cisco Umbrella dashboard and log in to your organization.
2. In the Umbrella dashboard, click **Admin** in the navigation pane and select **API Keys**.
3. Click **Create API Key**.

   If you already have an API key but do not have the secret saved, navigate to the **Admin** > **API Keys** screen and click **Refresh** to update the key and secret.
4. To create a new API key and secret, click the add button.
5. Enter a **Name** and add the scopes listed here to the API key:
   - Deployments
   - Policies

6. Click **Generate Key**.
7. Copy the API Key and the corresponding secret. Paste the information into a note or .txt file to store it temporarily until you are ready to use it.

You have successfully generated an API key and secret that can be used to onboard your Umbrella organization to Security Cloud Control.

Locate umbrella organization ID

Configure access to your Umbrella organization by locating the organization ID from the Cisco Umbrella dashboard URL.

Locate the organization ID for Umbrella to successfully onboard the organization to Security Cloud Control.

You must locate the organization ID for Umbrella and use that and your login credentials to successfully onboard the organization to Security Cloud Control.

Procedure

---

1. Access the Cisco Umbrella dashboard and log in to your organization.
2. The page URL will contain a numeric identifier. For example, the Organization ID for https://dashboard.umbrella.com/o/**123456**/#/overview is **123456**.
3. Copy the Organization ID from the URL. Paste the Organization ID into a note until you are ready to use it.

You have successfully located and copied the Umbrella organization ID from the dashboard URL. This organization ID can now be used for onboarding the organization.

Onboard an umbrella organization

Configure an Umbrella organization to integrate with Security Cloud Control for centralized management and security oversight.

This task enables integration between an Umbrella organization and Security Cloud Control for centralized security management and monitoring.

Use this procedure to onboard an Umbrella organization to Security Cloud Control.

Before you begin

Read the Umbrella license requirements on page 658 before you begin onboarding this environment.

Follow these steps to onboard an Umbrella organization:

Procedure

---

1. In the Umbrella dashboard, locate the Locate umbrella organization ID on page 659 and Generate an API key and secret on page 658. Keep these items available during this procedure.
2. Log in to Security Cloud Control.
3. Choose **Security Devices**.
4. Click the plus button () to begin onboarding the device.
5. Click **Umbrella Organization**.
6. Enter the Umbrella Network Device **API Key**, the corresponding **Secret** generated from the Umbrella dashboard, and the **Organization ID** from the Umbrella dashboard URL.

7. Click **Next**.
8. (Optional) Add unique **Labels** for the device. You can filter your list of devices by these labels.
9. Click **Security Devices**.

The Umbrella organization is successfully onboarded to Security Cloud Control and appears in the Security Devices inventory for centralized management.

Reconnect an Umbrella organization to Security Cloud Control

Configure the connection between an Umbrella organization and Security Cloud Control when API credentials have been refreshed or have timed out.

This task allows you to restore the connection between an Umbrella organization and Security Cloud Control when the stored API credentials become invalid due to refresh or timeout.

> **Warning**
>
> Security Cloud Control cannot successfully deploy or read configuration changes to or from an Umbrella organization if the stored credentials are invalid. However, Security Cloud Control may still deploy or read changes from any ASA devices associated with the organization. If you update and validate the credentials afterward, this may cause issues. Update the organization credentials before deploying any configuration changes.

If the API key and secret to an Umbrella organization have been refreshed or have timed out, you must manually reconnect the Umbrella organization to Security Cloud Control. Use this procedure to reconnect.

Procedure

1. On the Umbrella dashboard, click **Admin** in the navigation pane and select the existing Umbrella management **API Keys**.
2. Click **Refresh**. When prompted, confirm to refresh the API key and secret.
3. Copy the API key and the corresponding secret.
4. Log in to Security Cloud Control.
5. Choose **Security Devices**.
6. Use the filter or search bar to locate the Umbrella organization.
7. In the **Device Actions** pane, click **Reconnect**. Security Cloud Control confirms the stored API key and secret are no longer valid.
8. Paste the API key and secret into the pop-up window.
9. Click **Continue**.
10. Once Security Cloud Control confirms the new key and secret are valid, click **Close**.

The Umbrella organization is successfully reconnected to Security Cloud Control with updated credentials, allowing configuration deployment and reading to resume normally.

Cross-launch to the umbrella dashboard

Configure cross-launch access to the Umbrella dashboard from Security Cloud Control after onboarding your ASA device and Umbrella organization.

This task allows you to directly access your organization's Umbrella dashboard from the Security Cloud Control interface without having to log in separately to Umbrella.

After you onboard the ASA device and the Umbrella organization to Security Cloud Control, you can open the organization's dashboard from the Security Cloud Control UI.

Before you begin

Follow these steps to open your device's Umbrella dashboard:

Procedure

1. Log in to Security Cloud Control.
2. Choose **Security Devices**.
3. Locate or filter for the Umbrella organization.
4. Click **Manage Umbrella Organization** in the **Management** pane.

   A new tab opens in your browser and displays the Umbrella dashboard for the selected organization.

The Umbrella dashboard opens in a new browser tab, providing direct access to manage your Umbrella organization settings and policies.

34 Configure an Umbrella Organization

Topics:

- Read Umbrella tunnel configuration
- Cross-launch to the Umbrella tunnels page
- Configure a SASE tunnel for Umbrella
- Edit a SASE tunnel
- Delete a SASE tunnel from Umbrella

This chapter provides steps to configure an Umbrella Organization.

Read Umbrella tunnel configuration

Learn how to read Umbrella tunnel configuration for ASA devices, including ASA integration with Cisco Umbrella and secure internet gateway use cases.

After onboarding an Umbrella organization to Security Cloud Control, you can manually prompt Security Cloud Control to request and update the tunnel configuration from Umbrella. This update process applies to any tunnels that were added, deleted, or modified.

> **Warning**
>
> If you delete a tunnel from Security Cloud Control while the Umbrella organization credentials are invalid or have changed since you onboarded the organization, Security Cloud Control can deploy the tunnel configuration only to the ASA devices associated with the organization. When you update the credentials, Security Cloud Control reads the Umbrella configuration and restores any deleted tunnels. If the tunnel exists in the Umbrella organization but not in any ASA device, a synchronization issue occurs. In this case, you may not see the ASA devices as peers to the organization.

Procedure

1. Log in to Security Cloud Control.
2. Choose **Security Devices**.
3. Click the **ASA** tab.
4. Select the Umbrella organization so it is highlighted.
5. Under **Actions**, select **Read Tunnels**.

Cross-launch to the Umbrella tunnels page

Learn how to cross-launch to the Umbrella tunnels page for ASA devices, including ASA integration with Cisco Umbrella and secure internet gateway use cases.

After you successfully onboard the ASA device and the Umbrella organization to Security Cloud Control, you can cross-launch to the Umbrella dashboard for tunnels from the Security Cloud Control UI.

Use this procedure to cross-launch to your device's Umbrella tunnels page:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Select the tunnel you want to highlight.
4. In the **Actions** pane, click **Manage Tunnel in Umbrella**. A new tab opens in your browser to display the Tunnels overview page.

Configure a SASE tunnel for Umbrella

Learn how to configure a SASE tunnel for Umbrella for ASA devices, including ASA integration with Cisco Umbrella and secure internet gateway use cases.

Use this procedure to create a SASE tunnel for an Umbrella organization:

Before you begin

The Umbrella organization and the ASA device you want to create the tunnel for must already be onboarded to Security Cloud Control.

If the ASA or Umbrella organization associated with the tunnel you just deployed is in an unhealthy state, Security Cloud Control may not be able to successfully deploy the tunnel. If you experience any issues, contact Cisco TAC.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Click the add button and select **Create SASE Tunnel**.
4. Enter the Umbrella peer information:
   - **Select Umbrella**: Select the **Umbrella** organization of your choice.
   - **Datacenter**: Select a head-end datacenter that is geographically close to the ASA associated with the Umbrella organization.
5. Enter the ASA peer information:
   - **Select ASA Device**: Select an ASA device that is associated with the Umbrella organization from the drop-down list and click **Select**.
   - **Public Facing Interface**: Select an IPv4 address that is static and publicly routable. The address used should not be used for NAT.
   - **LAN Address**: Select the LAN interfaces that control the LAN subnet. At least one interface must be selected for the LAN.
   - **Virtual Tunnel Interface**: This field is automatically filled once you select the Umbrella organization and the ASA peer device. If necessary, you can manually enter an IP address that will be used as the new VTI.
6. The **Passphrase** is automatically filled once you select the Umbrella organization and the ASA peer device. The **Confirm Passphrase** is also automatically filled. You can manually enter these fields if necessary.
7. (Optional) The **Deploy changes to ASA immediately** toggle at the bottom of the pop-up window is enabled by default. When enabled, the SASE tunnel configuration is immediately deployed to the ASA peer selected in the tunnel configuration. To stage changes and deploy later, manually disable the option.
8. Click **Deploy**. Optionally, click **Deploy and Create Another** to simultaneously deploy this SASE tunnel and create another tunnel. Once deployed, the tunnel will appear in the VPN Tunnels page. If you choose to **Deploy and Create Another SASE tunnel**, Security Cloud Control saves both the Umbrella organization selection and the **Deploy changes to ASA immediately** toggle setting and automatically applies these selections to the next tunnel configuration. You can manually alter these selections prior to deploying.

Edit a SASE tunnel

Learn how to edit a SASE tunnel for ASA devices, including interface names, security levels, IP addressing, VLANs, and enablement options.

Use this procedure to modify an existing SASE tunnel:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Select the tunnel you want to modify.
4. In the **Actions** pane, select **Edit**.
5. Edit these fields of the SASE tunnel:
   - **Name**: Change the name of the SASE tunnel as it appears in Security Cloud Control and the Umbrella dashboard.
   - **Umbrella Peer's Datacenter**: Select a new headend data center from the drop-down list.
   - **ASA Peer's Public Facing Interface**: Select a new IPv4 address from the drop-down list.
   - **ASA Peer's LAN Interfaces**: Select one or more new LAN interfaces from the drop-down list.
   - **ASA Virtual Tunnel Interface (VTI) Address**: Manually edit the VTI.
   - **Passphrase**: Modify the passphrase for the tunnel.
   - **Confirm Passphrase**: Manually modify this entry to match the passphrase and confirm the new value.
6. (Optional) The **Deploy changes to ASA immediately** toggle at the bottom of the pop-up window is enabled by default. When enabled, the SASE tunnel configuration is deployed immediately to the ASA peer selected in the tunnel configuration. To stage changes and deploy later, manually set the option to disable. If you choose to stage changes and deploy later, the status of the ASA peer in the **Security Devices** page appears as `Deploy Pending`.
7. Select **Save Updates**.

Delete a SASE tunnel from Umbrella

Learn how to delete a SASE tunnel from Umbrella for ASA devices, including ASA integration with Cisco Umbrella and secure internet gateway use cases.

Use this procedure to delete a SASE tunnel on Security Cloud Control:

Before you begin

To delete a SASE tunnel, the ASA associated with it must have a synced status in Security Cloud Control. If the device is unhealthy, you cannot delete the tunnel.

When you delete a SASE tunnel from Security Cloud Control, the tunnel is removed from both the ASA device and its Umbrella organization.

> **Warning**
>
> Before deleting a tunnel, confirm that the Umbrella organization credentials are valid. If the credentials are invalid or have changed, Security Cloud Control deploys the tunnel configuration only to the associated ASA devices. After you update the credentials, Security Cloud Control reads the Umbrella configuration and restores any tunnels you deleted. Because the tunnel exists in the Umbrella organization but not on any ASA device, synchronization issues can occur. The ASA devices may not appear as peers to the organization.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Select the tunnel you want to delete from Security Cloud Control.
4. Under **Actions**, click **Delete**.
5. Confirm you want to delete the tunnel and click **OK**.

Part IX

Manage Cisco Meraki

Topics:

- Onboard Cisco Meraki MX devices
- Configure Cisco Meraki

35 Onboard Cisco Meraki MX devices

Topics:

- Onboard Meraki MX to Security Cloud Control
- Onboard Meraki templates to Security Cloud Control
- Update Meraki MX connection credentials

Learn how to onboard Cisco Meraki MX Devices for Cisco Meraki environments so the device or service is available for management.

This chapter provides steps to onboard Cisco Meraki MX device.

Onboard Meraki MX to Security Cloud Control

Learn how to onboard Meraki MX to Security Cloud Control so the device or service is available for management.

MX devices can be managed by both Security Cloud Control and the Meraki dashboard. Security Cloud Control deploys configuration changes to the Meraki dashboard. The dashboard then securely deploys the configuration to the device.

Before you begin

- For information about connecting Security Cloud Control to your managed devices, refer to Allow inbound access for direct cloud connectivity on page 94.
- You must first register the Meraki MX in the Meraki dashboard. Without access to the Meraki dashboard, your organization will not be recognized by the Meraki cloud. As a result, you will not be able to generate an API token to onboard your device.
- Security Cloud Control converts invalid CIDR prefix notation IP addresses and IP address ranges to valid form by setting all bits associated with the host to zero.
- Onboarding Meraki MX devices or templates no longer requires a connection through a Secure Device Connector (SDC). If you have Meraki MX devices that were previously onboarded and connect to Security Cloud Control using an SDC, their connection will continue to work. If you remove and re-onboard the device or update its connection credentials, the connection will stop working.
- MX devices do not need to be connected to the Meraki cloud to be managed by Security Cloud Control. If an MX device has *never* connected to the cloud, the device connectivity is listed as **unreachable**. This status is normal and does not affect your ability to manage the device or deploy policies to the device.

Procedure

1. When you onboard a Meraki MX device, you must generate a Meraki API key. This key lets the dashboard authenticate your request so you can securely onboard the device. For more information on generating and retrieving a Meraki API key, refer to Generate and Retrieve Meraki API Key on page 672.
2. Onboard a Meraki device to Security Cloud Control using the API key.

Generate and Retrieve Meraki API Key

Use this procedure to enable Security Cloud Control access to the Meraki dashboard with API access:

Before you begin

Review the notes and prerequisites in Onboard Meraki MX to Security Cloud Control on page 672

Procedure

1. Log in to the Meraki dashboard.
2. Choose **Organization** > **Settings**.
3. In the **Dashboard API Access** section, check **Enable access to the Cisco Meraki Dashboard API**. If you do not enable this option, you cannot generate API keys to onboard MX devices to Security Cloud Control.
4. Click **Save changes**.
5. On the Meraki dashboard, click your **username** and then click **My Profile**.

6. Locate the API access header and click **Generate new API key**. Copy the API key, and paste it into a note until you are ready to use it. If you close the window or tab containing the API key before pasting it, you will lose access to the copied API key.

   Note

   You only need one API key per device. You can re-onboard a Meraki device without generating a new key.

   Continue to Onboard a Meraki Device to Security Cloud Control.

Onboard an MX Device to Security Cloud Control

Use this procedure to onboard a Cisco Meraki device.

Before you begin

Generate and Retrieve Meraki API Key on page 672.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the blue add button .
4. Click the **Meraki** tile.
5. Select the Secure Device Connector on page 75 that this device will communicate with. The default SDC is displayed but you can change it by clicking the blue **Change** link.
6. On the **Connect to Cisco Meraki** page, follow these steps:
   a) Paste the API access key you copied, and click **Connect**.
      If the key is incomplete or incorrect, you will not be able to onboard the device.
   b) Use the drop-down list to select the correct organization. The generated list of organizations is retrieved from the Meraki dashboard and includes devices and templates. Click **Select**.
   c) Use the drop-down list to select the correct network. The generated list of networks is retrieved from the Meraki network. Click **Select**.
   d) (Optional) Add unique labels for the device. You can filter your list of devices by these labels. Click **Continue**.

   The device begins the onboarding process. After the process completes, you are redirected to the **Security Devices** page.

Onboard Meraki templates to Security Cloud Control

Learn how to onboard Meraki templates to Security Cloud Control so the device or service is available for management.

Meraki templates help manage multiple locations or networks using a single policy. You can manage these templates using both Security Cloud Control and the Meraki dashboard. Security Cloud Control deploys configuration changes to the Meraki dashboard, and the dashboard then securely deploys the configuration to the template. For more information about how Security Cloud Control communicates with Meraki.

> **Note**
>
> To onboard a template to Security Cloud Control, you must first create a template in the Meraki dashboard. Without access to the Meraki dashboard, the Meraki cloud will not recognize your organization, and you will not be able to generate an API token for your device. In the Meraki dashboard, click **Organization** > **Configuration templates**. For more information, refer to Managing Multiple Networks with Configuration Templates.

You must complete these three steps to onboard a Meraki template.

Procedure

1. Create a template network in the Meraki dashboard. For more information about Meraki template best practices, refer to Meraki Templates Best Practices.
2. Generate and Retrieve Meraki API Key on page 672. When you onboard a Meraki template, you must generate a Meraki API key. Use the key to authenticate the dashboard and securely onboard a device.
3. Onboard a Meraki Template to Security Cloud Control using the key.

Generate and Retrieve Meraki API Key

Use this procedure to enable Security Cloud Control access to the Meraki dashboard with API access:

Procedure

1. Log in to the Meraki dashboard.
2. Choose **Organization** > **Settings**.
3. In the **Dashboard API Access** section, check **Enable access to the Cisco Meraki Dashboard API**. If you do not enable this option, you cannot generate API keys to onboard MX devices to Security Cloud Control.
4. Click **Save changes**.
5. On the Meraki dashboard, click your **username** and then click **My Profile**.
6. Locate the API access header and click **Generate new API key**. Copy the API key, and paste it into a note until you are ready to use it. If you close the window or tab containing the API key before pasting it, you will lose access to the copied API key.

   > **Note**
   >
   > You only need one API key per template. You can re-onboard a template without generating a new key.

Onboard an Meraki Template to Security Cloud Control

Learn how to troubleshoot Firewall Threat Defense migration failures to Cloud-Delivered Firewall Management Center, including export, import, registration, connectivity, deployment, commit, rollback, VPN topology, analytics, and Secure Device Connector issues.

Use this procedure to onboard a Meraki template.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the blue add button .
4. Click **Connect to Cisco Meraki**.
5. Paste the API access key you copied. If the key is incomplete or incorrect, you will not be able to onboard the device. Click **Connect**.
6. Use the drop-down list to select the template name as an **Organization**. The generated list of organizations is retrieved from the Meraki dashboard and includes devices and templates. Select the desired template and click **Select**.
7. (Optional) You can add unique labels for the device. You can filter your list of devices by these labels.
8. Click **Continue**.

   The device begins the onboarding process. Once completed, Security Cloud Control redirects you to **Security Devices**. Once the template is synched to Security Cloud Control, the **Security Devices** page displays the names of the devices associated with the template and the **Device Details** window of displays the number of networks bound to the template.

Update Meraki MX connection credentials

Configure updated Meraki MX connection credentials when you generate a new API key from the Meraki dashboard.

Update the connection credentials in Security Cloud Control Firewall Management when you generate a new API key from the Meraki dashboard to restore communication between the device and the management platform.

If you generate a new API key from the Meraki dashboard, you must update the connection credentials in Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management does not allow you to update the connection credentials for the device itself. If necessary, manually refresh the API key in the Meraki dashboard. You must manually update the API key in the Security Cloud Control Firewall Management UI to update the credentials and restore communication.

> **Note**
>
> If Security Cloud Control fails to sync the device, the connectivity status in Security Cloud Control may show "Invalid Credentials." In this situation, you may have tried to use an API key. Confirm the API key for the selected Meraki MX is correct.

Use this procedure to update the credentials for a Meraki MX device:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.

3. Click the **Devices** tab and then click the **Meraki** tab.
4. Select the Meraki MX whose connection credentials you want to update.
5. In the **Device Actions** pane, click **Update Credentials**.
6. Enter the **API key** Security Cloud Control Firewall Management uses to log into the device, and click **Update**. This API key matches the credential that you used to onboard the Meraki MX unless you changed it. These changes do not require deployment to the device.

The connection credentials for the Meraki MX device are updated, restoring communication between the device and Security Cloud Control Firewall Management.

36 Configure Cisco Meraki

Topics:

- Managing Meraki with Security Cloud Control
- How does Security Cloud Control communicate with Meraki
- Meraki Access Control Policy
- Meraki templates

This chapter describes the steps to configure Cisco Meraki device.

Managing Meraki with Security Cloud Control

An overview of Cisco Meraki management in Security Cloud Control, including supported Meraki MX use cases and the main setup and configuration tasks.

After you onboard a Meraki device to Security Cloud Control, Security Cloud Control communicates with the Meraki dashboard to manage that device. Security Cloud Control does not communicate directly with the MX device.

Security Cloud Control securely transfers configuration requests to the Meraki dashboard which then applies the new configuration to the device. For more information, refer to How does Security Cloud Control communicate with Meraki on page 679.

Security Cloud Control provides tools to optimize your Meraki environment by detecting problems with objects and policies and suggesting possible fixes or alternative options. This applies to policies that are associated with both devices and templates. Use Security Cloud Control to:

- Simultaneously manage policies on one or more Meraki devices.
- Monitor and manage Meraki policies or templates along with your FTD and ASA devices in a comprehensive environment.
- Use a Meraki template to manage multiple networks.
- Customize access rules by using objects that are compatible with other supported platforms, such as FTD and ASA devices.

Onboard Meraki MX devices

Before onboarding a device to Security Cloud Control, you must create an account with the Meraki dashboard and onboard your device or template to the dashboard. To generate an API token and communicate with Security Cloud Control, your organization must have an account in the Meraki dashboard.

You can onboard a Meraki MX device or a Meraki template to Security Cloud Control.

Handle Meraki MX log in credentials and permissions through the Security Cloud Control console. Without the correct credentials or permissions, Security Cloud Control cannot communicate with the Meraki device.

For more information, refer to Updating Meraki MX Credentials and Generate and Retrieve Meraki API Key.

Meraki layer 3 rules and Security Cloud Control

At this time, Security Cloud Control supports Layer 3 firewall rules only. Layer 3 rules let you manage policy at the network layer of the OSI model. For more information, refer to Using Layer 3 Firewall Rules.

You can create Layer 3 outbound rules in the Meraki dashboard. When you onboard a device into Security Cloud Control, Security Cloud Control reads the Layer 3 rules that you have defined in the Meraki dashboard. You can then manage these rules in Security Cloud Control in the same way as you manage FTD or ASA rules. For more information, refer to Manage Meraki Access Control Policy.

Objects

You can optimize your new access control policy with objects. The Meraki dashboard uses protocols and groups of IP addresses or IP address ranges. In contrast, Security Cloud Control uses a variety of objects to manage rules. To understand how Security Cloud Control transfers Meraki protocols into objects, refer to Objects Associated with Meraki Devices. You can create these objects in Security Cloud Control, and they are translated into IP groups in the Meraki dashboard:

- Network objects or object groups
- Network service (port) objects

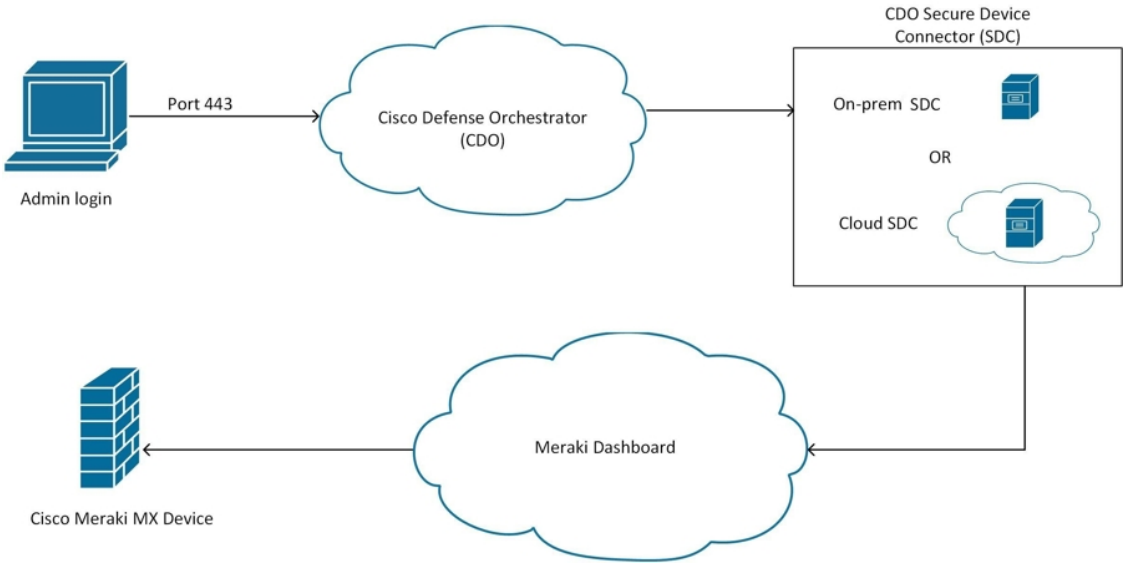
You can create Layer 3 outbound rules in the Meraki dashboard. Security Cloud Control reads in the Layer 3 rules you have defined in the Meraki dashboard when you onboard a device into Security Cloud Control. You can then manage these rules just as you would manage FTD or ASA rules in Security Cloud Control. For more information about Meraki access control policy, refer to Manage Meraki Access Control Policy.

How does Security Cloud Control communicate with Meraki

An overview of how does Security Cloud Control communicate with Meraki, including Deploy From Security Cloud Control to your Meraki device Security Cloud Control does not deploy configuration changes directly to a Meraki MX device; deployment.

Deploy from Security Cloud Control to your Meraki device

Security Cloud Control does not deploy configuration changes directly to a Meraki MX device; deployment is a multistep process. The diagram below shows the deployment process.



Configuration changes that you make in Security Cloud Control for a Meraki MX device are staged in Security Cloud Control until you deploy them. When you deploy the configuration changes, Security Cloud Control forwards them to the Meraki dashboard, which implements them on the Meraki MX device. Security Cloud Control manages firewall policies while Meraki dashboard manages the network the policies are applied to. Both operations affect the way the Meraki MX device manages and processes network traffic.

Some customers with older tenants may connect the Meraki MX device to Security Cloud Control through an SDC. If you are one of those customers, you can continue to use this method or you can remove the SDC by onboarding your Meraki MX again or updating the connection credentials. You do not need an SDC to connect Security Cloud Control to Meraki MX.

One difference between Security Cloud Control and the Meraki dashboard is the use of objects. For rules that are created on the Meraki dashboard, Security Cloud Control takes Meraki IP address groups or IP address ranges and turns them into objects that can be attached or associated to rules and the device policy. When you deploy objects that are created in Security Cloud Control to Meraki appliances, the Meraki dashboard translates those objects back into IP address groups or ranges. Objects in Security Cloud Control are unique and versatile because they are compatible with other device platforms. If you have other devices onboarded in Security Cloud Control, you may be able to create a single object for all your devices. For more information about objects associated with Meraki devices, refer to Objects Associated with Meraki Devices on page 129.

Meraki Access Control Policy

Learn how to manage a Meraki access control policy in Security Cloud Control, including creating, editing, deleting, reordering, and deploying access control rules for Meraki MX device templates.

Before you onboard to Security Cloud Control, the Meraki MX devices may have been managed by the Meraki dashboard, and the device may already have some outbound rules. These rules will appear as access control rules in Security Cloud Control.

You can modify these rules and create additional rules within the access control policy. To customize your access control policy, create and attach objects. For more information, refer to the related articles section.

> **Note**
>
> The action of the Meraki access control policy is **Allow** by default. You cannot change the action.

Use this procedure to edit a Meraki access control policy using Security Cloud Control:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Templates** tab.
4. Click the **Meraki** tab, and select the Meraki MX device template whose access control policy you want to edit.
5. In the **Management** pane, select **Policy**.
6. Do any of the following:
   - To create a new rule, click the add button .
   - To edit an existing rule, select the rule and click the edit button in the **Actions** pane. You can make simple edits inline without entering edit mode.
   - To delete a rule you no longer need, select the rule and click the remove button in the **Actions** pane.
   - To move a rule within the policy, select the rule in the access control table and click the up or down arrow at the end of the rule row to move the rule.
7. In the **Order** field, select the position for the rule within the policy. Network traffic is evaluated against the list of rules in numerical order, from 1 to the "last" rule.

   Rules are applied on a first-match basis. Rules with highly specific traffic matching criteria must appear before policies with general criteria that would otherwise apply to the matching traffic.

   The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.
8. Enter the rule name. You can use alphanumeric characters, spaces, and the special characters: + . _ -

> **Note**
>
> The **Name** of the access control rule is used as the name of the rule in Security Cloud Control while the **Remark** field is treated as the name of the rule in the Meraki dashboard. The two fields are not dependent on each other.

9. Select the action to apply if the network traffic is matched by the rule:
   - **Block**: Drop the traffic unconditionally. The traffic is not inspected.
   - **Allow**: Allow the traffic subject to the intrusion and other inspection settings in the policy.

> **Note**
>
> You can only set or modify the rule action. You cannot change the default policy action from Security Cloud Control.

10. Define the traffic matching criteria by using any combination of attributes in these tabs.
    - **Source**: Click the **Source** tab and add or remove networks (which includes networks and continents) or ports from which the network traffic originated. The default value is "Any."
    - **Destination**: Click the **Destination** tab and add or remove networks (which includes networks and continents), or ports on which the traffic arrives. The default value is "Any."

> **Note**
>
> The source and destination networks must be within one of the configured VLAN subnets, or if a VLAN subnet is not manually configured, the default VPN subnet. Deploying a rule that includes an invalid source or destination network will fail.

11. Click **Save**.
12. Review and deploy the changes you made now, or wait and deploy multiple changes at once.

Meraki templates

An overview of meraki templates, including what it is, when to use it, and key considerations for administrators.

A Meraki template is a network configuration that you can share with multiple sites or networks. You can bind individual site networks to a template network. Any changes you make to a single template automatically update all bound networks. You can view bound networks as bound devices in Security Cloud Control. This configuration is ideal for applying a single policy across multiple networks in different locations.

For more information about configuring more than one network to a single template, refer to Managing Multiple Networks with Configuration Templates.. For detailed information about Meraki templates, template planning, and setup, refer to Meraki Templates Best Practices.

Manage Meraki templates in the same way as you manage Meraki devices. First, configure your template with the Meraki dashboard, then onboard it to Security Cloud Control. When you onboard a template to Security Cloud Control, any existing rules or groups of IPs are read into Security Cloud Control and translated into objects. After syncing, view the template name and the number of associated networks (as bound devices) in the **Device Details** pane on the **Security Devices** page. You can also manage, modify, and deploy the policies associated with the template and the bound networks from Security Cloud Control. For more information about onboarding Meraki templates to Security Cloud Control, refer to Onboard Meraki Template.

Part X

Manage AWS VPC

Topics:

- Onboard AWS VPC
- Configure AWS VPC

37 Onboard AWS VPC

Topics:

- Supported devices, software, and hardware for Security Cloud Control Firewall Management
- Onboard an AWS VPC

This chapter provides the steps to connect to the Amazon Virtual Private Cloud.

Supported devices, software, and hardware for Security Cloud Control Firewall Management

Provides an overview of devices supported by Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management is a cloud-based management solution enabling the management of security policies and device configurations across multiple security platforms.

This section describes the supported device types, software, hardware, and constraints for managing firewall, cloud, SD-WAN, Cisco IOS, Cisco Umbrella, and management center integrations in Security Cloud Control Firewall Management.

Support scope

Security Cloud Control Firewall Management is a cloud-based management solution for security policies and device configurations across multiple security platforms. The source identifies support for these management areas:

- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Catalyst SD-WAN Manager
- Cisco Secure Firewall Management Center, on-premises
- Cisco Meraki MX
- Cisco IOS devices
- Cisco Umbrella
- AWS Security Groups

Security Cloud Control Firewall Management documentation identifies the devices, software, and hardware that Security Cloud Control Firewall Management supports. If the documentation does not explicitly claim support for a software version or device type, Security Cloud Control Firewall Management does not support it.

Cisco secure firewall ASA

Cisco Adaptive Security Appliance (ASA) is a security device that integrates firewall, VPN, and intrusion prevention capabilities. Security Cloud Control supports ASA device management to streamline configuration management and support regulatory compliance across the network infrastructure.

Cisco secure firewall threat defense

Cisco Secure Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It includes security functions such as intrusion prevention, application control, URL filtering, and advanced malware protection.

A Secure Firewall Threat Defense device can be deployed on ASA hardware appliances, Cisco firewall hardware appliances, and virtual environments. You can manage threat defense devices through management interfaces such as Cisco Firewall Management Center, Security Cloud Control, and Firewall Device Manager.

Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It offers comprehensive security functions, including intrusion prevention, application control, URL filtering, advanced malware protection, and so on. An FTD can be deployed on ASA hardware appliances, and Cisco firewall hardware appliances, and in virtual environments. Managing threat defense devices is possible through various management interfaces, such as Cisco Firewall Management Center, Security Cloud Control Firewall Management, and Firewall Device Manager.

For more information on software and hardware compatibility, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Firewall Device Manager is a web-based management interface explicitly designed for threat defense device management. It provides a simplified approach for configuring and monitoring threat defense devices, making it ideal for smaller-scale deployments or organizations preferring an intuitive interface.

FDM offers basic configuration capabilities for network settings, access control policies, NAT rules, VPN configuration, monitoring, and basic troubleshooting. Typically accessed through a web browser, FDM is directly available on the FTD device, eliminating the need for additional management servers or appliances.

Cisco Catalyst SD-WAN manager

Security Cloud Control offers centralized management for Catalyst SD-WAN and Branch WAN environments, allowing organizations to efficiently configure, monitor, and enforce security policies across their networks. This integration also facilitates advanced troubleshooting, rule optimization, and change management on the Catalyst SD-WAN Manager.

For more information on software and hardware compatibility, see Cisco Catalyst SD-WAN Device Compatibility.

Cisco secure firewall management center

Security Cloud Control Firewall Management simplifies the management of on-premises Firewall Management Center by establishing a secure integration, discovering security devices, and enabling centralized policy management. Security policies such as firewall rules, VPN settings, and intrusion prevention policies can be efficiently managed and deployed across all devices under FMC.

Cisco Meraki MX

The Cisco Meraki MX appliance is an enterprise-grade security and SD-WAN next-generation firewall appliance for decentralized deployments. Security Cloud Control Firewall Management supports management of layer 3 network rules on Meraki MX devices.

When you onboard a Meraki device to Security Cloud Control Firewall Management, Security Cloud Control Firewall Management communicates with the Meraki dashboard to manage that device. Security Cloud Control Firewall Management transfers configuration requests to the Meraki dashboard, and the Meraki dashboard applies the new configuration to the device.

Security Cloud Control Firewall Management support for Cisco Meraki MX includes centralized policy management, backup and restore, monitoring and reporting, compliance checking, and automation capabilities.

Cisco IOS devices

Cisco IOS software manages network functions such as routing, switching, and other networking protocols. Cisco IOS includes features and commands to configure and maintain Cisco network devices.

Cisco umbrella

Security Cloud Control Firewall Management manages Cisco Umbrella through integrations such as the Umbrella ASA Integration. This integration lets administrators include Cisco Adaptive Security Appliance (ASA) devices in their Umbrella configuration by using per-interface policies.

The integration enables ASA devices to redirect DNS queries to Umbrella and use Umbrella DNS security, web filtering, and threat intelligence capabilities.

AWS security groups

Security Cloud Control Firewall Management provides a simplified management interface for Amazon Web Services (AWS) Virtual Private Clouds (VPCs). Source-backed capabilities include monitoring AWS Site-to-Site VPN connections, tracking changes to AWS devices, and viewing AWS Site-to-Site VPN tunnels.

ASA support specifics

Lists the constraints and limitations for Security Cloud Control Firewall Management support of ASA platforms.

Security Cloud Control Firewall Management support for ASA has these constraints:

- Security Cloud Control Firewall Management can manage all ASA platforms that run currently supported code versions, including ASAv instances.
- Security Cloud Control Firewall Management does not support ASA Services Module (ASASM).
- Security Cloud Control Firewall Management does not test end-of-life ASA code versions and does not recommend them for production.
- Use currently supported ASA code versions for optimal results.
- ASA 8.3 is not supported with the new policy view.
- Security Cloud Control Firewall Management does not manage the ASA FirePOWER module because the module runs a different operating system from ASA. Manage the ASA FirePOWER module separately with Secure Firewall Management Center or ASDM.
- End-of-life code and hardware might continue to work with Security Cloud Control Firewall Management. Because end-of-life code and hardware are not part of Security Cloud Control Firewall Management testing, correct operation with end-of-life software and hardware is not guaranteed or assured.

  Refer to the version download page for Cisco "suggested release" or "gold star" versions.
- ASA versions 8.x, 9.1, and 9.2 do not support TLS 1.2 on the management plane and are considered insecure for ASA software management.

For a full discussion of ASA, ASDM, and hardware compatiblity, see the Cisco Secure Firewall ASA Compatibility guide.

Cloud device support specifics

Provides software and device type support information for cloud-based devices.

This table describes software and device type support for cloud-based devices. Read the affiliated links for more information about onboarding and feature functionality for the device types in the table.

Device Types	Notes
Meraki Security Appliance • MX Series • Meraki Templates	Meraki MX devices and the Meraki dashboard receive regular software updates through the Meraki cloud. Security Cloud Control Firewall Management works with the latest version of the Meraki dashboard to manage layer 3 network rules enforced by Meraki MX devices. Register the MX device to the Meraki dashboard, or create the template in the Meraki dashboard, before onboarding it to Security Cloud Control Firewall Management. For more information, refer to Managing Meraki with Security Cloud Control. You must register an MX device to, or create a template in, the Meraki dashboard before onboarding it to Security Cloud Control Firewall Management.
Amazon Web Services VPC	AWS VPC receives updates through the AWS console. Refer to AWS documentation for more information about the platform and available services. Launch an AWS VPC in the AWS console before onboarding it to Security Cloud Control Firewall Management.

Device Types	Notes
Google Cloud Platform	Google Cloud Platform (GCP) receives updates through the GCP console. Refer to Google Cloud documentation for more information about the platform and available services.
Microsoft Azure	Azure receives updates through the Azure console. Refer to Azure documentation for more information about the platform and available services.

Switching and routing support specifics

Provides Cisco IOS software and device type support information for devices specific to switching and routing.

This table describes Cisco IOS software and device type support for devices specific to switching and routing. Read the affiliated links for more information about onboarding and feature functionality for the device types in the table.

Devices Types	Notes
Cisco IOS	Security Cloud Control supports devices running Cisco IOS version 12.4 or later.

Onboard an AWS VPC

Learn how to onboard an AWS VPC in Security Cloud Control Firewall Management so you can manage VPC details, security groups, and site-to-site VPN connectivity.

To onboard an AWS VPC to Security Cloud Control Firewall Management, follow this procedure.

Before you begin

Note

Security Cloud Control Firewall Management does not support peered AWS VPCs. If you attempt to onboard a peered VPC referencing a security group that is defined on the peer VPC, the onboarding process fails.

Before onboarding your Amazon Web Services (AWS) Virtual Private Cloud (VPC) to Security Cloud Control Firewall Management, review these prerequisites:

- To onboard an AWS VPC, you need the access key and secret access key for the VPC. Both credentials are generated using the Identity and Access Management (IAM) console. For more information about security credentials, refer to Understanding and Getting your Security Credentials.
- Configure IAM permissions to allow Security Cloud Control to communicate with your AWS VPC. For more information about changing permissions for an IAM user, refer to Changing Permissions for an IAM User. See this example for required permissions.

```
"cloudformation:CreateStack",
"cloudformation:CreateStackInstances",
"cloudformation:DescribeStackInstance",
```

```
"cloudformation:DescribeStackResource",
"cloudformation:DescribeStackResources",
"cloudformation:DescribeStacks",
"ec2:AllocateAddress",
"ec2:AllocateHosts",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2:AssociateSubnetCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateInternetGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:DescribeAddresses",
"ec2:DescribeAddressesAttribute",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeInstanceStatus",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpcs",
"ec2:DescribeVpnGateways",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySecurityGroupRules",
"ec2:ModifySubnetAttribute",
"ec2:RunInstances",
"sts:GetCallerIdentity"
```

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click  to begin onboarding the device.

4. Click the **AWS VPC** tile.
5. Enter these details in the **Account** page.
   a) Enter the Access Key ID and Secret Access Key to connect to the AWS account. The generated list of names is retrieved from the AWS VPC to which you supplied login credentials.
   b) Click **Connect**.
6. Enter these details in the **VPC** page.
   a) Select a region from the drop-down menu. Choose the region where the VPC is located.
   b) Click **Select**.
   c) Use the drop-down menu to select the correct AWS VPC. The generated list of names is retrieved from the AWS VPC to which you supplied login credentials.

      Note

      AWS VPC IDs names are unique; there cannot be two or more instances with the same ID.

   d) Click **Select**.
7. Enter these details in the **Name** page.
   a) Enter a name to be shown in the Security Cloud Control UI.
   b) Click **Continue**.
8. (Optional) Enter a label for the device in the **Labels** page, and click **Continue**.

   Note

   If you create labels for an AWS VPC, the tables are not automatically synchronized with your device. You must manually recreate the labels as tags in the AWS console. For more information about labels and tags in AWS VPC, refer to Labels and tags in AWS VPC.

After successful onboarding, the Configuration Status changes to 'Synced,' and Connectivity changes to 'Online' on the **Security Devices** page.

38 Configure AWS VPC

Topics:

- Manage AWS VPCs with Security Cloud Control Firewall Management
- Update AWS VPC connection credentials
- Monitor AWS VPC tunnels using AWS transit gateway
- View AWS VPC tunnel history
- AWS VPC Policy

This chapter provides steps to configure Amazon Virtual Private Cloud.

Manage AWS VPCs with Security Cloud Control Firewall Management

An overview of managing AWS VPCs in Security Cloud Control Firewall Management, including onboarding, security groups, shared objects, VPN tunnel monitoring, and change tracking.

Use Security Cloud Control Firewall Management to manage AWS VPCs

Security Cloud Control Firewall Management provides a simplified management interface for your Amazon Web Services (AWS) Virtual Private Clouds (VPCs). You can manage your AWS VPCs and their components in the same interface you manage your other devices.

Use Security Cloud Control Firewall Management to perform these tasks:

- Onboard an AWS VPC on page 689
- View VPC Details
- Work with Security Groups
- Monitor AWS Site-to-Site VPN Connections
- Monitoring Changes to AWS Devices

These are common AWS features that Security Cloud Control Firewall Management expects to support in the future:

- Showing the relationship of load balancers (elastic, network, and application load balancers) to the security group.
- Showing the relationship of autoscaling groups to a security group.

You cannot manage these aspects of security groups with Security Cloud Control Firewall Management:

- Creating Security Groups.
- Linking Security Groups to instances.
- Assigning Security Groups to load balancers.
- VPC peering.

Onboard AWS VPCs

Start by onboarding the AWS VPC using the onboarding wizard for Security Cloud Control Firewall Management. For more information about onboarding an AWS VPC, refer to Onboard an AWS VPC .

Note that if an AWS VPC contains tags, these tags are imported into Security Cloud Control Firewall Management when you onboard the device. Security Cloud Control Firewall Management represents the tags as **labels**. Unlike security cloud objects or rules, labels are not automatically synchronized to the AWS VPC. For more information about labels and filtering, refer to Labels and Filtering.

Handle AWS VPC login credentials and permissions through the Security Cloud Control Firewall Management console. Without the correct credentials or permissions, Security Cloud Control Firewall Management cannot communicate with the AWS VPC. For more information, refer to Update AWS VPC connection credentials on page 696 and Changing Permissions for an IAM User .

View AWS VPC details

After onboarding the AWS VPC, you can view its ID, region, security groups, and the rules and objects assigned to those security groups.

Work with Security Groups

Security groups are a collection of rules that govern inbound and outbound network traffic for all AWS instances and other entities associated with the security group. When you onboard an AWS VPC to Security Cloud Control Firewall Management, the security groups are stored in Security Cloud Control Firewall Management as security group objects.

Using Security Cloud Control Firewall Management you can perform these tasks:

- Create new rules in a security group.
- Check for changes, edit, and delete rules in a security group.

At this time, you cannot create new security groups in a VPC. For more information, refer to Manage AWS VPC Security Groups Rules

Share Objects between AWS and other managed devices

Security Cloud Control Firewall Management supports the use of objects in rules. Objects are containers for values. For example, you can create a network object containing the IP address of a resource and assign it a meaningful name. You can then use that object in access rules as part of the source or destination, instead of using the resource's literal IP address. You can also reuse that object in different rules. If you change the value of the object once, any rule that uses that object starts using the new value.

After onboarding an AWS VPC, Security Cloud Control Firewall Management translates AWS concepts into security group objects, network objects, and service objects found in existing security group rules.

Network objects and service objects (also called port objects) can be shared between AWS VPCs and other devices managed using Security Cloud Control Firewall Management. Security group objects are unique to AWS.

Monitor Changes to AWS VPCs and AWS Security Groups

Change Log

The change log continuously captures configuration changes as they are made in Security Cloud Control Firewall Management. This view includes changes across all supported devices and services. The change log offers these features:

- Side-by-side comparison of changes made to device configuration.
- Plain English labels for all change log entries.
- Records onboarding and removal of devices.
- Detection of policy change conflicts occurring outside of Security Cloud Control Firewall Management.
- Answers who, what, and when during an incident investigation or troubleshooting.

Change Request Management

Change request management allows you to associate a change request and its business justification, opened in a third-party ticketing system, with an event in the Change Log. Use change request management to create a change request in Security Cloud Control Firewall Management, identify it with a unique name, enter a description of the change, and associate the change request with change log events. You can later search the Change Log for the change request name.

Support for common managerial tasks

Security Cloud Control Firewall Management supports these common management tasks for AWS security groups:

- Bulk deploy device configurations on page 824
- Read all device configurations on page 815
- Detecting Out-of-Band Changes
- Conflict Detection

- Resolve Configuration Conflicts

Update AWS VPC connection credentials

Configure updated AWS VPC connection credentials so Security Cloud Control Firewall Management can continue communicating with onboarded AWS resources.

This task ensures continuous communication between Security Cloud Control Firewall Management and onboarded AWS resources when new access keys and secret access keys are created for the AWS VPC connection.

If you create a new access key and secret access key to connect to the AWS VPC, you must update the connection credentials in Security Cloud Control Firewall Management. To do this, first update the credentials in the AWS console. Next, update the credentials in the Security Cloud Control Firewall Management console by using this procedure. For more information, refer to *Managing Access Keys for IAM Users* (https://docs.AWS.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) or *Creating, Disabling, and Deleting Access Keys for Your AWS Account Root User* (https://docs.AWS.amazon.com/general/latest/gr/managing-AWS-access-keys.html).

You **cannot** change the access key or secret access key from Security Cloud Control Firewall Management. You must manually manage the connection credentials using the AWS console or the AWS CLI console.

> **Note**
>
> If multiple AWS VPCs are onboarded to your Security Cloud Control Firewall Management tenant, you must update the credentials for one device at a time.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab, and then click **AWS VPC**.
4. Select the AWS VPC whose connection credentials you want to update.

   Use the filter and search functionalities to find the required device.
5. Under **Device Actions**, click **Update Credentials**.
6. Enter the new **Access Key** and **Secret Access Key**, which you want to use to connect to the AWS VPC.
7. Click **Update**.

   > **Note**
   >
   > If Security Cloud Control fails to sync the device, the connectivity status in Security Cloud Control may display "Invalid Credentials." If this occurs, you may have entered an invalid username and password combination. For more information about troubleshooting invalid credentials, refer to Troubleshoot invalid credentials on page 1094

The AWS VPC connection credentials are updated successfully, and Security Cloud Control Firewall Management can continue communicating with the onboarded AWS resources using the new credentials.

Monitor AWS VPC tunnels using AWS transit gateway

Learn how to monitor AWS VPC tunnel connectivity in Security Cloud Control Firewall Management using AWS Transit Gateway and run on-demand checks for active or idle VPN tunnel status.

Amazon Web Services (AWS) Transit Gateway acts as a cloud router. It connects enterprise virtual private clouds (VPCs) to AWS VPCs through a central hub, which allows for simplified peering relationships.

Security Cloud Control Firewall Management allows you to monitor the connection status of your onboarded AWS VPCs using AWS Transit Gateway.

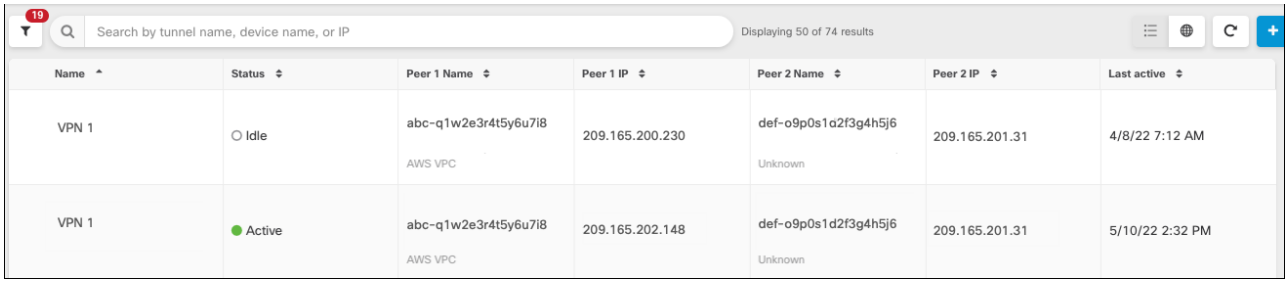
Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.

   The **VPN Tunnels** page displays the connection status for all network tunnels managed by your Security Cloud Control tenant. The connection status for the VPN tunnel can be active or idle.
3. Select a VPC, and then under **Actions**, click **Check Connectivity**. This triggers a real-time connectivity check against the tunnel and identifies whether the tunnel is currently active or idle. If you do not click the on-demand connectivity check link, a check across all tunnels on all onboarded devices occurs every ten minutes.

   Note

   Security Cloud Control prompts a notification if the connection of a VPN tunnel goes down. No notification appears when the link comes back up.



View AWS VPC tunnel history

Learn how to view AWS VPC tunnel history in Security Cloud Control Firewall Management by filtering the Change Log for a specific AWS VPC.

To view a history of changes made to AWS VPC tunnels, follow these steps.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Events & Logs** > **Logs** > **Change Log**.
3. On the **Change Log** page, click the filter icon, select the **Filter by device** tab, and then click **AWS VPC** .
4. Select the AWS VPC whose history you want to review, and click **OK**.

Related Information

Change logs in Security Cloud Control on page 1038

AWS VPC Policy

Learn how to manage AWS VPC policies and security group rules in Security Cloud Control Firewall Management to define inbound and outbound traffic, update rules, and deploy policy changes to selected AWS VPCs.

Security Cloud Control Firewall Management enables you to keep security policies consistent across any Amazon Web Services (AWS) Virtual Private Cloud (VPC) associated with your AWS account. You can also use Security Cloud Control Firewall Management to share objects across multiple device types. See these topics for more information.

AWS VPC Security Groups Rules

AWS security groups are collections of rules that govern inbound and outbound network traffic to all AWS EC2 instances, and other entities, associated with the security group. Similar to the Amazon Web Services (AWS) console, Security Cloud Control displays each rule individually.

If your SDC has Internet access, you can create and manage AWS Virtual Private Cloud (VPC) rules for these environments:

- A security group allowing information to or from another security group within the same AWS VPC.
- A security group allowing to or from an IPv4 or IPv6 address.

When creating a rule in Security Cloud Control that contains an AWS security group, keep these limitations in mind:

- For a rule allowing inbound traffic, the source can be one or more security group objects in the same AWS VPC, an IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address. Inbound rules can have only **one** security group object as the destination.
- For a rule allowing outbound traffic, the destination can be one or more security group objects in the same AWS VPC, a prefix list ID, an IPv4 or IPv6 CIDR block, a single IPv4 or IPv6 address. Outbound rules can have only **one** security group object as the source.
- Security Cloud Control translates rules that contain multiple entities, such as more than one port or subnet, into separate rules before deploying them to an AWS VPC.
- When you add or remove rules, the changes are automatically applied to all AWS entities associated with the security group.
- An AWS security group is limited to hosting a maximum of 60 inbound rules and 60 outbound rules. This limit is enforced separately for IPv4 rules and IPv6 rules; any additional rules created in Security Cloud Control are inclusive to the total number of rules. You cannot exceed the 60-rule limit by onboarding to Security Cloud Control.

Warning

If you edit an existing rule, the system deletes the edited rule and creates a new rule with the updated details. As a result, traffic that depends on the rule may be dropped briefly during the update process. This does not occur if you create a brand new rule.

For more information about the types of rules you can create from the AWS console, refer to AWS Security Group Object.

Create a Security Group Rule

By default, Amazon Web Services (AWS) Virtual Private Cloud (VPC) blocks all network traffic. As a result, any rules are automatically configured to **Allow** traffic. You cannot edit this action.

Note

When you create a new security group rule, you must associate it with a security group.

The AWS console does not support rules that contain more than one source or destination. This means that if you deploy a single security group rule that contains more than one entity, Security Cloud Control converts the rule into separate rules before deploying it to the AWS VPC. For example, if you create an inbound rule that allows traffic from two port ranges into one cloud security group object, Security Cloud Control converts it into two separate rules. One allows traffic from the first port range to the security group, and the other allows traffic from the second port range to the security group.

Use this procedure to create a security group rule:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Template** tab.
4. Click the **AWS** tab, and select the AWS VPC device template whose access control policy you want to edit.
5. In the Management pane, select **Policy**.



6. Click the blue plus button next to the security group you wish to add the rule to.



7. Click **Inbound** or **Outbound**.

   Inbound rules: The source network can contain one or multiple IPv4 addresses, IPv6 addresses, or cloud security group objects. The destination network **must** be defined as a single cloud security group object.

   Outbound rules: The source network **must** be defined as a single cloud security group object. The destination network can contain one or multiple IPv4 addresses, IPv6 addresses, or security group objects.

8. Enter the rule name. You can use alphanumeric characters, spaces, and the special characters plus, period, underscore, and hyphen.

9. Define the traffic matching criteria by using any combination of attributes in the following tabs.

   Source : Click the **Source** tab and add or remove networks (which includes networks and continents). You cannot define a port or port range as the source.

   Destination: Click the **Destination** tab and add or remove networks (which includes networks and continents), or ports on which the traffic arrives. The default value is "Any."

   > **Note**
   >
   > If no network object is defined, it will be translated into two rules in the AWS Console: one for IPv4 (0.0.0.0/0) and one for IPv6 (::0/0).

10. Click **Save**.
11. Review and deploy the changes you made immediately, or wait and deploy multiple changes at once.

    > **Caution**
    >
    > If the deploy fails, Security Cloud Control tries to restore the AWS VPC to its previous state. This is done on a "best-effort" basis. Because AWS does not maintain a "state," this rollback attempt might fail. If this happens, log in to the AWS management console and manually restore the AWS VPC configuration and then read the changes into Security Cloud Control.

Edit a Security Group Rule

Use this procedure to edit an access control rule for an AWS VPC using Security Cloud Control:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab to locate the device, or click the **Templates** tab to locate the model device.
4. Click the **AWS** tab and select the AWS VPC whose access control policy you want to edit.
5. In the **Management** pane, select **Policy**.
6. To edit an existing security group rule, select the rule and click the edit icon in the **Actions** pane. You can also make simple edits inline without entering edit mode. For more information about rule limitations and exceptions, refer to AWS VPC Security Group Rules.
7. Click **Save**.
8. Review and deploy the changes you made immediately, or wait and deploy multiple changes at once.

> **Caution**
>
> If the deployment fails, Security Cloud Control tries to restore the AWS VPC to its previous state. This is done on a "best-effort" basis. Because AWS does not maintain a "state," this rollback attempt might fail. If this happens, log in to the AWS management console and manually restore the AWS VPC configuration. Then poll for differences between the AWS VPC device configuration and the configuration in Security Cloud Control.

Delete a Security Group Rule

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab to locate the device, or click the **Templates** tab to locate the model device.
4. Click the **AWS** tab and select the AWS VPC whose access control policy you want to edit.
5. In the **Management** pane, select **Policy**.
6. To delete a security group rule you no longer need, select the rule and click the delete icon in the **Actions** pane.
7. Review and deploy the changes you made immediately, or wait and deploy multiple changes at once.

> **Caution**
>
> If the deployment fails, Security Cloud Control tries to restore the AWS VPC to its previous state. This is done on a "best-effort" basis. Because AWS does not maintain a "state," this rollback attempt might fail. If this happens, log in to the AWS management console and manually restore the AWS VPC configuration. Then poll for differences between the AWS VPC device configuration and the configuration in Security Cloud Control.

Part XI

Manage Cisco IOS

Topics:

- Onboard Cisco IOS Devices
- Configure Cisco IOS

Cisco IOS devices are network devices running Cisco's Internetwork Operating System (IOS), such as routers and switches. Security Cloud Control explicitly supports Cisco IOS devices for centralized policy and configuration management. Cisco IOS devices are onboarded similarly using SSH but are recognized as a specific device type with tailored management capabilities within Security Cloud Control.

39 Onboard Cisco IOS Devices

Topics:

- Onboard a Cisco IOS Device

This chapter provides information for onboarding Cisco IOS devices.

Cisco IOS devices are network devices running Cisco's Internetwork Operating System (IOS), for example, routers and switches. Security Cloud Control explicitly supports Cisco IOS devices for centralized policy and configuration management. Cisco IOS devices are onboarded similarly using SSH but are recognized as a specific device type with tailored management capabilities within Security Cloud Control.

Onboard a Cisco IOS Device

Learn how to onboard a Cisco IOS device. You can onboard a live Cisco device running Cisco IOS (Internetwork Operating System).

You can onboard a live Cisco device running Cisco IOS (Internetwork Operating System).

Onboard a Cisco IOS Device

Before you begin

Before you begin, ensure that all prerequisites are met.

- Your Cisco IOS server must support ciphers that are compatible with Security Cloud Control. Currently, Security Cloud Control supports a limited set of ciphers for onboarding Cisco IOS devices. Supported ciphers are `aes128-ctr`, `aes192-ctr`, `aes256-ctr`, `aes128-gcm`, `aes128-gcm@openssh.com`, `aes256-gcm`, `aes256-gcm@openssh.com`.

  Log in to your Secure Device Connector (SDC) and run the command `ssh -vv <ip_address>` to view the ciphers your server supports.

- You must have an active on-premises Secure Device Connector (SDC) in your network to add a Cisco IOS device.

  For more information about SDCs and deployment scenarios, refer to Secure Device Connector on page 75.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click **Security Devices**
3. Click the blue add button  to begin onboarding the device.
4. Click the **Integrations** tile.

   If the tile is grayed out, there is no active Secure Device Connector deployed in your network for your Security Cloud Control tenant.

5. Enter these details in the **Locate Device** page.
   a) Select **IOS** from the drop-down list under **Create Integrations**.
   b) Click the Secure Device Connector on page 75 button and select the SDC in your network that this device will communicate with. The default SDC appears. To choose a different SDC, click the SDC name.
   c) Enter a name for the device.
   d) Enter the device location (FQDN or IPv4).
   e) Enter the port number. The default connection port is 22.
   f) Click **Next**.
6. Enter these details in the **SSH Fingerprint** page.
   a) Enter the device administrator name and password.

> **Note**
>
> Currently, Security Cloud Control does not support connections using public key authentication.

b) If you have set an enable password on the device, enter it in the **Enable Password** field.
c) Click **Next**.
You can download and review the SSH fingerprint by clicking the copy icon.

7. (Optional) Enter a label for the device in the **Done** page. For more information about labels and label groups, refer to Labels and Label Groups.
8. Click **Go to Security Devices** to return to the **Security Devices** page.

After successful onboarding, the Configuration Status changes to 'Synced,' and Connectivity changes to 'Online.'

To write a note about the device, enter it in the **Device Notes** page for the device. For more information about the notes page, refer to Device Notes.

Create and Import an ASR or ISR Model

When you onboard a Cisco Integrated Services Router (ISR) or Aggregation Services Router (ASR) device to Security Cloud Control, the device's running configuration is represented as a Cisco IOS model. This model is a copy of the device configuration and is used to centrally manage supported security settings, such as firewall and VPN policies. You can download the Cisco IOS model as a text file and import it into another tenant that you manage to replicate or reuse the configuration.

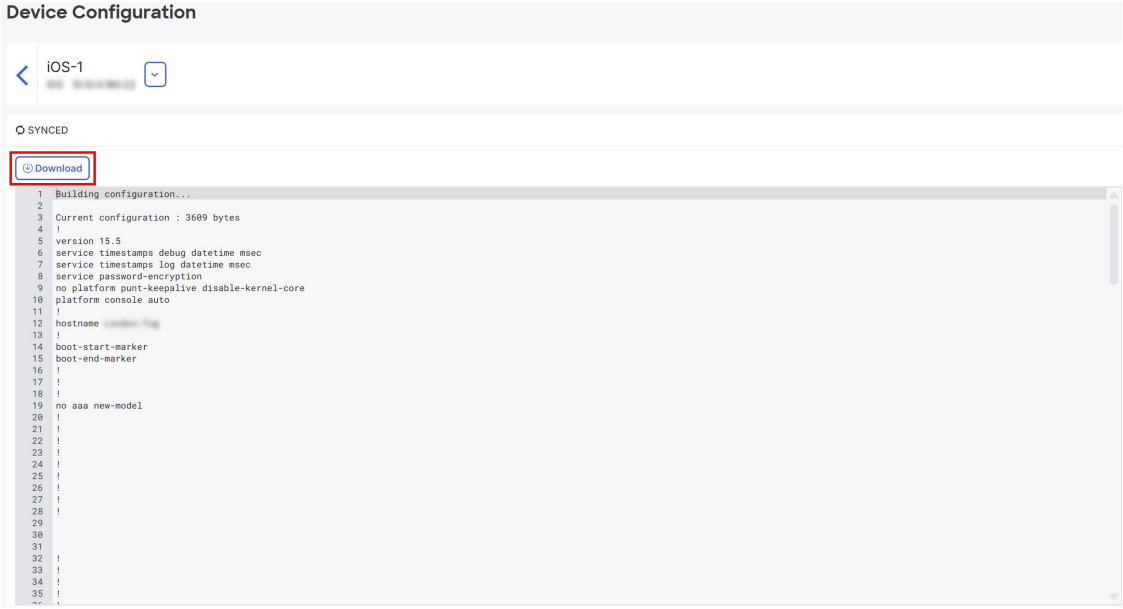
Download ASR or ISR Configuration

You can download the configuration for an onboarded Integrated Services Router (ISR) or Aggregation Services Router (ASR) device from Security Cloud Control and use it to bootstrap the device or save its current managed configuration locally.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click **Security Devices**.
3. Click the **Devices** tab.
4. Click the **IOS** tab and select a device.
5. Click **Configuration** under the **Management** section.
6. Click **Download** to download the device configuration to your local computer.



Import ASR or ISR Configuration

You can import an Integrated Services Router (ISR) or Aggregation Services Router (ASR) configuration file into Security Cloud Control without onboarding a physical device. Uploading a text-based configuration file creates a model device in Security Cloud Control. You can use this model for analysis, labeling, and policy management. After you import and process the configuration, the model appears in the Security Devices list for further use.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click **Security Devices**.
3. Click the blue add (+) button to import the configuration.
4. Click the **Import** tile.
5. Enter these details in the **Configuration for Model Device** page.
   a) Enter a name for the device.
   b) Select the **Device Type** as **ASR** or **ISR**.
   c) Click **Browse** and select the configuration file (text format) to upload.
   d) Click **Upload**.
6. Once the configuration is verified, you are prompted to label the device or service. For more information about labels and label groups, refer to Labels and Label Groups.
7. After labeling your model device, you can view it in the **Security Devices** list.

> **Note**
>
> The system may take some time to analyze the configuration, depending on its size and the number of devices or services.

Configuration import for offline device management

Explains how to import configuration files for offline device management, allowing analysis and optimization of device settings without live network access.

Configuration import for offline device management is a feature that

- allows you to review, analyze, and optimize device settings without requiring access to a live device in your network
- creates models that represent copies of device configurations for policy review, planning, and reuse, and
- processes uploaded configuration files so they appear in the **Security Devices** list for labeling, reviewing, and managing like other supported devices.

Supported device types

You can import the configurations for these device types into Security Cloud Control Firewall Management:

- Adaptive Security Appliance (ASA): You can upload an ASA configuration file to create an ASA model for offline review and management. For more information, refer to Create and Import an ASA Model.
- Cisco IOS devices such as Aggregation Services Routers (ASRs) and Integrated Services Routers (ISRs): You can upload a text-based running configuration file to create an IOS model for offline analysis and reuse. For more information, refer to Create and Import an ASR or ISR Model.

40 Configure Cisco IOS

Topics:

- Manage IOS Devices with Security Cloud Control
- Use the Security Cloud Control Command Line Interface Tool

This chapter provides steps to configure Cisco IOS.

Manage IOS Devices with Security Cloud Control

Learn how to manage IOS devices with Security Cloud Control. Cisco IOS devices are network devices, such as routers and switches, that run Cisco's Internetwork Operating System (IOS).

Cisco IOS devices are network devices, such as routers and switches, that run Cisco's Internetwork Operating System (IOS). Security Cloud Control supports Cisco IOS devices for centralized policy and configuration management.

You can onboard Cisco IOS devices using SSH. The system recognizes them as a specific device type with tailored management capabilities within Security Cloud Control. Cisco IOS devices include routers and switches that run IOS or IOS XE and have dedicated SSH management support.

You can use these features for IOS devices.

- Onboard Integrations. To onboard the device, enter the username and password of a user with high privileges stored on the IOS device.
- View Device Configuration File on page 712. You can view the device configuration file.
- Reading changes from firewalls on page 817. When you check for changes in the configuration file from the Cisco IOS device, it will be saved in the database of Security Cloud Control.
- Out-of-band changes on devices on page 831. When you enable Conflict Detection, Security Cloud Control checks the device every 10 minutes for configuration changes. If a change occurs, the device status changes to Conflict Detected, and you can then resolve the conflict.
- Use the Security Cloud Control Command Line Interface Tool on page 712. You can issue all IOS commands to the device through Security Cloud Control's command line interface.
- You can turn individual CLI commands and groups of commands into editable and reusable macros. Security Cloud Control provides system-defined macros. You can also create your own macros for frequently performed tasks.
- Detect and manage SSH fingerprint changes. When the device credentials or properties change and the SSH fingerprint changes, Security Cloud Control prompts you to review and accept the new fingerprint.
- Change logs in Security Cloud Control on page 1038. The change log records all commands issued to the IOS device.

Use the Security Cloud Control Command Line Interface Tool

Learn how to use the Security Cloud Control command line interface tool. Use the Security Cloud Control command line interface (CLI) to manage or troubleshoot IOS and other device types.

Use the Security Cloud Control command line interface (CLI) to manage or troubleshoot IOS and other device types.

For more information, refer to the Security Cloud Control configuration guideUse the Security Cloud Control Command Line Interface Tool (CLI) on page 861.

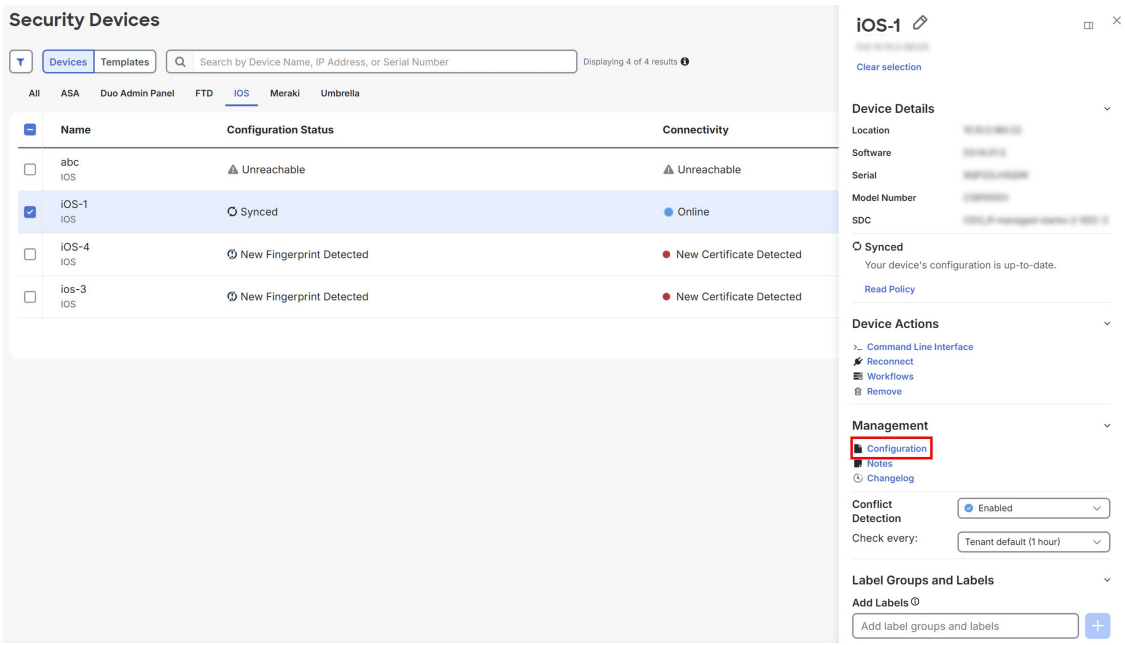
View Device Configuration File

You can view the configuration file using Security Cloud Control.

> **Note**
>
> Cisco IOS devices have read-only configurations.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click **Security Devices**.
3. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
4. Click the appropriate device type tab.
5. Select the device or model whose configuration you want to view.
6. Click **Configuration** under the **Management** section.



After you complete these steps, you can see the full configuration file.

Part XII

Manage Network Devices with Generic SSH Access

Topics:

- Onboard an SSH Device
- Configure SSH Devices

Generic SSH refers to the use of the Secure Shell (SSH) protocol as a standard method to securely access and manage network devices remotely. Devices such as Linux servers, Unix-based systems, or third-party network appliances accessible using SSH. It provides encrypted communication, replacing less secure protocols like Telnet. These devices are accessible using SSH that can be onboarded and managed through Security Cloud Control by specifying the device's IP or FQDN, SSH port, and login credentials.

41 Onboard an SSH Device

Topics:

- How to onboard an SSH device

Learn how to onboard an SSH device to Security Cloud Control using an on-premises Secure Device Connector, supported SSH ciphers, device credentials, fingerprint verification, and optional configuration commands.

How to onboard an SSH device

Onboard an SSH device to Security Cloud Control using SSH integration and Secure Device Connector. Configure the device connection and credentials to manage it from Security Cloud Control.

Generic SSH refers to the use of the Secure Shell (SSH) protocol as a standard method to securely access and manage network devices remotely. Devices such as Linux servers, Unix-based systems, or third-party network appliances accessible using SSH. It provides encrypted communication, replacing less secure protocols like Telnet. These devices are accessible using SSH that can be onboarded and managed through Security Cloud Control by specifying the device's IP or FQDN, SSH port, and login credentials.

You can use the username and password of a highly privileged user stored on the SSH device to onboard the device.

Before you begin

Before you begin, make sure you have met these prerequisites:

- Ensure that the ciphers your Cisco SSH device supports are supported by Security Cloud Control. At this time, Security Cloud Control supports a limited set of ciphers for onboarding Cisco SSH devices. The supported ciphers are: `aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm, aes128-gcm@openssh.com, aes256-gcm, aes256-gcm@openssh.com`. To determine the ciphers your server supports, log in to your SDC and run this command: `ssh -vv <ip_address>`.
- You must have an on-premises Secure Device Connector (SDC) in your network to onboard a Cisco IOS device.

  See About for a discussion of SDCs and links to deployment scenarios.
- Before you onboard your device, review Connect to Security Cloud Control.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the blue plus button  to onboard a device.
3. Click the **Integrations** tile. If it is grayed-out, it means you do not have an active Secure Device Connector deployed in your network and used by your Security Cloud Control tenant.
4. Click the About button and select the SDC in your network that this device will communicate with. The default SDC is displayed but you can change it by clicking the SDC name.
5. Give the device a name.
6. In the Integrations drop-down menu, select **Generic SSH**.
7. Enter the device's location as either the FDQN or IPv4 address. The default SSH port is 22.
8. Click **Go**. Security Cloud Control locates the device and prepares to integrate the configuration.
9. **Download** the SSH fingerprint and save locally. If you've never connected to this device through SSH before, this fingerprint allows you to confirm the device.
10. Enter the Username and Password login credentials for the device you are onboarding. Security Cloud Control cannot successfully read the existing configuration without the correct login information.
11. (Optional) Enter the **Enable Password** if you've previously configured one for this device.
12. (Optional) Select a Configuration Command from the drop-down menu, or enter a custom command in the textbox. This command will be used as the configuration for the device; if OOB is enabled, Security Cloud Control checks for changes and you can view the current value of this in the Configuration page. Note that you can change this command once the device is successfully onboarded to Security Cloud Control.
13. Click **Connect**.

> **Note**
>
> If the login credentials were incorrect, you will be prompted to review the connection details. Here you can re-enter the login information. If you exit the review without correcting the credentials, the device has an integration instance in the **Security Devices** page but the device is not onboarded or synchronized.

14. (Optional) Add labels to this device.
15. Click **Continue**.
16. The device onboards to Security Cloud Control. Click **Finish**.
17. Return to the **Security Devices** page. After the device has been successfully onboarded, you will see that the Configuration Status is "Synced" and the Connectivity state is "Online."

> **Note**
>
> Once a device is onboarded, you can change the configuration command to be executed. You can use a custom command or create a macro.

18. (Optional) If you want you can write a note about the device by typing it in the device's notes page.

42 Configure SSH Devices

Topics:

- Managing SSH Devices with Security Cloud Control
- Use the Security Cloud Control Command Line Interface Tool

This chapter provides steps to configure SSH devices.

Managing SSH Devices with Security Cloud Control

Learn how to manage Generic SSH devices in Security Cloud Control, including onboarding, viewing configurations, using CLI commands and macros, detecting out-of-band changes, managing SSH fingerprint changes, and reviewing Change Log activity.

Generic SSH devices include any other SSH-capable devices not running Cisco IOS, managed using a generic SSH interface. Devices such as Linux servers, Unix-based systems, or third-party network appliances accessible using SSH. Generic SSH refers to the use of the Secure Shell (SSH) protocol as a standard method to securely access and manage network devices remotely. These devices are accessible using SSH that can be onboarded and managed through Security Cloud Control by specifying the device's IP or FQDN, SSH port, and login credentials.

These are the features we support for those devices:

- Onboard a SSH Device: You can use the username and password of a highly privileged user stored on the SSH device to onboard the device.
- View Device Configuration File: You can view the device configuration file.
- Review policy and configuration changes from device: When you read the configuration file from the SSH device, it will be saved in Security Cloud Control's database.
- Out-of-band change detection: When you enable Conflict Detection, Security Cloud Control checks the device every 10 minutes for changes to the device's configuration. If there is a change, the device's status will change to Conflict Detected and you will be able to resolve the conflict.
- Use the Security Cloud Control Command Line Interface Tool on page 722: You can issue all SSH device commands to the device through Security Cloud Control's command line interface.
- Individual CLI commands and groups of commands can be turned into editable and reusable "macros." You can use the system-defined macros provided by Security Cloud Control and create your own macros for tasks you perform often.
- Detect and manage SSH fingerprint changes: If any credentials or properties of the device change, and that causes a change to the SSH fingerprint, Security Cloud Control detects that change and gives you a chance to review and accept the new fingerprint.
- Change Log: The change log captures all the commands you issue to the SSH device.

Use the Security Cloud Control Command Line Interface Tool

Learn how to use the Security Cloud Control command line interface tool to manage and troubleshoot supported device types.

You can use the Security Cloud Control command line interface (CLI) for managing or troubleshooting many device types.

For more information, see Use the Security Cloud Control Command Line Interface Tool (CLI) on page 861.

View a Device's Configuration File

For devices that store the entire configuration in a single configuration file, you can view the configuration file using Security Cloud Control.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

3. Click the device type tab for a device type.
4. Select the device or model whose configuration it is you want to view.
5. In the **Management** pane on the right, click **Configuration**.
   The full configuration file is displayed.

Part XIII

Establish Secure Connections

Topics:

- Establish Site-to-Site VPN connection using Security Cloud Control Firewall Management
- Establish Remote Access VPN connection using Security Cloud Control Firewall Management
- Configure Firewall for Universal Zero Trust Network Access

43 Establish Site-to-Site VPN connection using Security Cloud Control Firewall Management

Topics:

- Introduction to Site-to-Site Virtual Private Network
- Site-to-Site VPN concepts
- Site-to-Site VPN configuration for FDM-Managed
- Site-to-Site VPN Configuration for Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense
- Site-to-Site VPN for Secure Firewall ASA
- Monitor ASA Site-to-Site Virtual Private Networks

Introduction to Site-to-Site Virtual Private Network

Learn how site-to-site VPN tunnels connect networks across locations and how Security Cloud Control Firewall Management supports IPsec VPN configuration for managed device pairs.

A site-to-site VPN tunnel connects networks in different geographic locations. You can create site-to-site IPsec connections between managed devices and between managed devices and other Cisco or third-party peers that comply with all relevant standards. These peers can have any mix of inside and outside IPv4 and IPv6 addresses. Site-to-site tunnels are built using the Internet Protocol Security (IPsec) protocol suite and Internet Key Exchange version 2 (IKEv2). After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

Simplifying Site-to-Site VPNs with Security Cloud Control Firewall Management

Site-to-Site VPNs are a reliable solution for securely connecting multiple networks over the internet. To make this process easier and more efficient, Security Cloud Control Firewall Management provides a **consolidated Site-to-Site VPN wizard**. This intuitive tool is designed to simplify the creation and management of secure VPN tunnels while reducing the complexity involved in traditional VPN configurations.

The Site-to-Site VPN wizard provides a single, unified interface for configuring VPN tunnels across a variety of managed devices. This consistency ensures a streamlined experience for administrators, regardless of the specific device or network environment. By offering a centralized and intuitive configuration process, the wizard helps organizations enhance operational efficiency, reduce errors, and maintain a high level of security in their network infrastructure.

The table below specifies the permitted site-to-site VPN configurations for the managed devices.

	FDM-managed	Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense	Secure Firewall ASA	Multicloud Defense
FDM-managed	Yes	No	No	No
Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense	No	Yes	Yes	Yes
Secure Firewall ASA	No	Yes	Yes	Yes
Multicloud Defense	No	Yes	Yes	No

Site-to-Site VPN concepts

An overview of site-to-site VPN topology, IKE and IPsec settings, pre-shared keys, encryption domains, VTI limits, and extranet devices.

VPN Topology

To create a new site-to-site VPN topology you must provide a unique name, specify a topology type, choose the IKE version that is used for IPsec IKEv1 or IKEv2, or both and authentication method. Once configured, you deploy the topology to ASAFTD.

IPsec and IKE Protocols

In Security Cloud Control, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

Authentication VPN Tunnels

For authentication of VPN connections, configure a pre-shared key in the topology on each device. Pre-shared keys allow a secret key, used during the IKE authentication phase, to be shared between two peers.

Virtual Tunnel Interface (VTI)

Security Cloud Control does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on FTD. Devices with configured VTI tunnels can be onboarded to Security Cloud Control but it ignores the VTI interfaces. If a security zone or static route references a VTI, Security Cloud Control reads the security zone and static route without the VTI reference.

VPN Encryption Domain

There are two methods to define the VPN's encryption domain: route-based or policy-based traffic selectors.

- **Policy-Based**: The encryption domain is set to allow any traffic which enters the IPSec tunnel. IPSec Local and remote traffic selectors are set to 0.0.0.0. This means that any traffic routed into the IPSec tunnel is encrypted regardless of the source/destination subnet. ASA supports policy-based VPN with crypto maps.
- **Route-Based**: The encryption domain is set to encrypt only specific IP ranges for both source and destination. It creates a virtual IPsec interface, and whatever traffic enters that interface is encrypted and decrypted. ASA supports route-based VPN with the use of Virtual Tunnel Interfaces (VTIs).

About Extranet Devices

You can add non-Cisco or unmanaged Cisco devices to a VPN topology as "Extranet" devices with either static or dynamic IP addresses.

- Non-Cisco Device: You cannot use Security Cloud Control to create and deploy configurations to non-Cisco devices.
- Unmanaged Cisco Device: Cisco device not managed by your organization, such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.

Encryption and Hash Algorithms Used in VPN

Because a VPN tunnel typically traverses a public network, most likely the Internet, you need to encrypt the connection to protect the traffic. You define the encryption and other security techniques to apply using IKE policies and IPsec proposals.

If your device license allows you to apply strong encryption, there is a wide range of encryption and hash algorithms, and Diffie-Hellman groups, from which to choose. However, as a general rule, the stronger the encryption that you apply to the tunnel, the worse the system performance. Find a balance between security and performance that provides sufficient protection without compromising efficiency.

We cannot provide specific guidance on which options to choose. If you operate within a larger corporation or other organization, there might already be defined standards that you need to meet. If not, take the time to research the options.

The following topics explain the available options:

Deciding Which Encryption Algorithm to Use

When determining which encryption algorithms to use for the IKE policy or IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN.

For IKEv2, you can configure multiple encryption algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

For IPsec proposals, the algorithm is used by the Encapsulating Security Protocol (ESP), which provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP.

If your device license qualifies for strong encryption, you can choose from the following encryption algorithms. If you are not qualified for strong encryption, you can select DES only.

- AES-GCM - (IKEv2 only.) Advanced Encryption Standard in Galois/Counter Mode is a block cipher mode of operation providing confidentiality and data-origin authentication and provides greater security than AES. AES-GCM offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance. GCM is a mode of AES that is required to support NSA Suite B. NSA Suite B is a set of cryptographic algorithms that devices must support to meet federal standards for cryptographic strength.
- AES-GMAC - (IKEv2 IPsec proposals only.) Advanced Encryption Standard Galois Message Authentication Code is a block cipher mode of operation providing only data-origin authentication. It is a variant of AES-GCM that allows data authentication without encrypting the data. AES-GMAC offers three different key strengths: 128-, 192-, and 256-bit keys.
- AES - Advanced Encryption Standard is a symmetric cipher algorithm that provides greater security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance.
- DES - Data Encryption Standard, which encrypts using 56-bit keys, is a symmetric secret-key block algorithm. If your license account does not meet the requirements for export controls, this is your only option. It is faster than 3DES and uses fewer system resources, but it is also less secure. If you do not need strong data confidentiality, and if system resources or speed is a concern, choose DES.
- 3DES - Triple DES, which encrypts three times using 56-bit keys, is more secure than DES because it processes each block of data three times with a different key. However, it uses more system resources and is slower than DES.
- NULL - A null encryption algorithm provides authentication without encryption. This is typically used for testing purposes only.

Deciding Which Hash Algorithms to Use

In IKE policies, the hash algorithm creates a message digest, which is used to ensure message integrity. In IKEv2, the hash algorithm is separated into two options, one for the integrity algorithm, and one for the pseudo-random function (PRF).

In IPsec proposals, the hash algorithm is used by the Encapsulating Security Protocol (ESP) for authentication. In IKEv2 IPsec Proposals, this is called the integrity hash. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP-, and there is also an -HMAC suffix (which stands for "hash method authentication code").

For IKEv2, you can configure multiple hash algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

You can choose from the following hash algorithms:

- SHA (Secure Hash Algorithm) - Standard SHA (SHA-1) produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. However, it is also more resource-intensive than MD5. For implementations that require the highest level of security, use the SHA hash algorithm.

- The following SHA-2 options, which are even more secure, are available for IKEv2 configurations. Choose one of these if you want to implement the NSA Suite B cryptography specification.
  - SHA-256 - Specifies the Secure Hash Algorithm SHA-2 with the 256-bit digest.
  - SHA-384 - Specifies the Secure Hash Algorithm SHA-2 with the 384-bit digest.
  - SHA-512 - Specifies the Secure Hash Algorithm SHA-2 with the 512-bit digest.
- MD5 (Message Digest 5) - Produces a 128-bit digest. MD5 uses less processing time for overall faster performance than SHA, but it is considered to be weaker than SHA.
- Null or None (NULL, ESP-NONE) - (IPsec Proposals only.) A null Hash Algorithm; this is typically used for testing purposes only. However, you should choose the null integrity algorithm if you select one of the AES-GCM/GMAC options as the encryption algorithm. Even if you choose a non-null option, the integrity hash is ignored for these encryption standards.

Deciding Which Diffie-Hellman Modulus Group to Use

You can use the following Diffie-Hellman key derivation algorithms to generate IPsec security association (SA) keys. Each group has different size modules. A larger modulus provides higher security but requires more processing time. You must have a matching modulus group on both peers.

If you select AES encryption, to support the large key sizes required by AES, you should use Diffie-Hellman (DH) Group 5 or higher. IKEv1 policies do not support all of the groups listed below.

To implement the NSA Suite B cryptography specification, use IKEv2 and select one of the elliptic curves Diffie-Hellman (ECDH) options: 19, 20, or 21. Elliptic curve options and groups that use 2048-bit modulus are less exposed to attacks such as Logjam.

For IKEv2, you can configure multiple groups. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

- 2 - Diffie-Hellman Group 2: 1024-bit modular exponential (MODP) group. This option is no longer considered good protection.
- 5 - Diffie-Hellman Group 5: 1536-bit MODP group. Formerly considered good protection for 128-bit keys, this option is no longer considered good protection.
- 14 - Diffie-Hellman Group 14: 2048-bit modular exponential (MODP) group. Considered good protection for 192-bit keys.
- 19 - Diffie-Hellman Group 19: National Institute of Standards and Technology (NIST) 256-bit elliptic curve modulo a prime (ECP) group.
- 20 - Diffie-Hellman Group 20: NIST 384-bit ECP group.
- 21 - Diffie-Hellman Group 21: NIST 521-bit ECP group.
- 24 - Diffie-Hellman Group 24: 2048-bit MODP group with 256-bit prime order subgroup. This option is no longer recommended.

Deciding Which Authentication Method to Use

You can use the following methods to authenticate the peers in a site-to-site VPN connection.

Preshared Keys

Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase. For IKEv1, you must configure the same preshared key on each peer. For IKEv2, you can configure unique keys on each peer.

Preshared keys do not scale well compared to certificates. If you need to configure a large number of site-to-site VPN connections, use the certificate method instead of the preshared key method.

Site-to-Site VPN configuration for FDM-Managed

Learn how to create and manage site-to-site VPN tunnels between FDM-managed devices or extranet peers in Security Cloud Control.

Security Cloud Control supports these aspects of site-to-site VPN functionality on FDM-managed devices:

- Both IPsec IKEv1 & IKEv2 protocols are supported.
- Automatic or manual pre-shared keys for authentication.
- IPv4 and IPv6. All combinations of inside and outside are supported.
- IPsec IKEv2 site-to-site VPN topologies provide configuration settings to comply with Security Certifications.
- Static and dynamic interfaces.
- Support for the dynamic IP address for the extranet device as an endpoint.

Configure Site-to-Site VPN Connections with Dynamically Addressed Peers

Security Cloud Control allows you to create a site-to-site VPN connection between peers when one of the peers' VPN interface IP address is not known or when the interface obtains its address from a DHCP server. Any dynamic peer whose preshared key, IKE settings, and IPsec configurations match with another peer can establish a site-to-site VPN connection.

Consider two peers, A and B. The static peer is a device whose IP address of its VPN interface is fixed and a dynamic peer is a device whose IP address of the VPN interface is not known or has a temporary IP address.

The following use cases describe different scenarios for establishing a secure site-to-site VPN connection with dynamically-addressed peers:

- A is a static peer, and B is a dynamic peer or conversely.
- A is a static peer, and B is a dynamic peer with a resolved IP address from the DHCP server or conversely. You can select **Bind VPN to the assigned IP** to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.
- A and B are dynamic with resolved IP addresses from the DHCP server. In such a case, you must select **Bind VPN to the assigned IP** for at least one peer to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.
- A is a dynamic peer, and B is an extranet device with a static or dynamic IP address.
- A is a dynamic peer with a resolved IP address from the DHCP server, and B is an Extranet device with a static or dynamic IP address. You can select **Bind VPN to the assigned IP** to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.

Important

If you select **Bind VPN to the assigned IP**, the VPN binds statically to the DHCP assigned IP address. However, this dynamic interface can receive many new IP addresses after the peer restarts. Although the VPN tunnel updates the new IP address, the other peer is not updated with the new configuration. You must deploy the site-to-site configuration again for out-of-band changes on the other peer.

> **Note**
>
> If the IP address of the interface is changed by using a local manager like Firewall Device Manager, the **Configuration Status** of that peer in Security Cloud Control shows "Conflict Detected". When you resolve this out-of-band change, the **Configuration Status** of the other peer changes to the "Not Synced" state. You must deploy the Security Cloud Control configuration to the device which is in "Not Synced" state.

Typically, the dynamic peer must be the one that initiates the connection as the other peer would not know the IP address of the dynamic peer. When the remote peer attempts to establish the connection, the other peer validates the connection using the preshared key, IKE settings, and IPsec configurations.

Because the VPN connection is established only after the remote peer initiates the connection, any outbound traffic that matches access control rules that allow traffic in the VPN tunnel will be dropped until that connection is established. This ensures that data does not leave your network without the appropriate encryption and VPN protection.

> **Note**
>
> A site-to-site VPN connection cannot be configured in the following scenarios:

- If both peers have DHCP assigned IP addresses.
  - **Workaround**: You can configure a site-to-site VPN, if one of the peers has a resolved IP address from the DHCP server. In such a case, you must select **Bind VPN to the assigned IP** to configure site-to-site VPN.
- If a device has more than one dynamic peer connection.
  - **Workaround**: You can configure a site-to-site VPN by performing the following steps:
    - Consider three devices A, B, and C.
    - Configure site-to-site VPN connection between A (static peer) and B (dynamic peer).
    - Configure site-to-site VPN connection between A and C (dynamic peer) by creating an Extranet device. Assign the static VPN interface IP address of A to the Extranet device and establish a connection with C.

FDM-Managed Device Site-to-Site VPN Guidelines and Limitations

- Security Cloud Control does not support a crypto-acl to design the interesting traffic for S2S VPN. It only supports protected networks.
- Security Cloud Control does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to Security Cloud Control but it ignores the VTI interfaces. If a security zone or static route references a VTI, Security Cloud Control reads the security zone and static route without the VTI reference. Security Cloud Control support for VTI tunnels is coming soon.
- Whenever IKE ports 500/4500 are in use or when there are some PAT translations that are active, the site-to-site VPN cannot be configured on the same ports as it fails to start the service on those ports.
- Transport mode is not supported only tunnel mode. IPsec tunnel mode encrypts the entire original IP datagram which becomes the payload in a new IP packet. Use tunnel mode when the firewall is protecting traffic to and from hosts

positioned behind a firewall. Tunnel mode is the normal way regular IPsec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.

- For this release, only PTP topology is supported, containing one or more VPN tunnels. Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.

Create a Site-To-Site VPN Tunnel Between FDM-managed Devices

Note that an FDM-managed device has the capability to establish a secure VPN tunnel either with another FDM-managed device or with an extranet device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Click the **Create Tunnel** () icon and then click **Site-to-Site VPN**.
4. In the **Peer Selection** area, provide the following information:
   - **Configuration Name**: Enter a unique topology name.

     We recommend naming your topology to indicate that it is an FDM-managed device VPN, and its topology type.
   - **Peer 1**: Click the **FDM** tab and select an FDM-managed device.
   - **Peer 2**: Click the **FDM** tab and select an FDM-managed device.

     If you choose an extranet device, select **Static** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.

     > **Note**
     >
     > If one or both endpoint devices have dynamic IP addresses, see Configure Site-to-Site VPN Connections with Dynamically-Addressed Peers for additional instructions.

5. Click **Next**.
6. In the **Peer Details** area, provide the following information:
   - **VPN Access Interface**: Select the interface to establish a connection between peer 1 and peer 2.
   - **Routing**: Click **Add Networks** and select one or more protected networks to establish a site-to-site tunnel between the protected networks of peer 1 and peer 2
   - (Optional) **NAT Exempt Interface**: Select **NAT Exempt** for peer 1 and peer 2 to exempt the VPN traffic from NAT policies on the local VPN access interface. It must be configured manually for individual peers. If you do not want NAT rules to apply to the local network, select the interface that hosts the local network. This option works only if the local network resides behind a single routed interface (not a bridge group member). If the local network is behind more than one routed interface or one or more bridge group members, you must manually create the NAT exempt rules.
7. Click **Next**.
8. In the **IKE Settings** area, choose the IKE versions to use during Internet Key Exchange (IKE) negotiations and specify the privacy configurations: For more information on the IKE policies, see Configuring the Global IKE Policy.

> **Note**
>
> IKE policies are global to a device and apply to all VPN tunnels associated with it. Therefore, adding or deleting policies affect all VPN tunnels in which this device is participating.

a. Select either or both options as appropriate.

> **Note**
>
> By default, **IKEV Version 2** is enabled.

b. Click **Add IKEv2 Policies** to select the IKEv2 policies for peer 1 and peer 2.

c. The **Local Pre-Shared Key** and **Remote Pre-Shared Key** for the participating devices are auto-genreated. Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase.

d. Click **IKE Version 1** to enable it.

e. Click **Add IKEv1 Policies** to select the IKEv1 policies for peer 1 and peer 2.

f. The **IPEv1 Pre-Shared Key** is auto-generated.

9. Click **Next**.
10. In the **IPSec Settings** area, specify the IPSec configurations for peer 1 and peer 2. The corresponding IKEV proposals are available depending on the selection that is made in the **IKE Settings** step.

    For more information on the IPSec settings, see the IPsec proposal and IKE policy objects on page 154.

    a. Click **Add IKEv2 IPSec Proposals** and select the IKEv2 proposals you want for peer 1 and peer 2.

    b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see Deciding Which Diffie-Hellman Modulus Group to Use.

    c. Click **Next**.

11. In the **Finish** area, you will find a summary of the configurations you have completed.

    Read the configuration and then click **Submit** if you're satisfied.

Configure Networking for Protected Traffic Between the Site-To-Site Peers

After completing the configuring of the Site-To-Site connection, make sure that you perform the following configuration for VPN to function on all targeted devices.

Procedure

1. Configure AC policies:

Configure AC policies for permitting bidirectional traffic between the protected networks behind both peers. These policies help the packets to traverse to the intended destination without being dropped.

> **Note**
>
> You must create AC policies for incoming and outgoing traffic on both peers.

a. In the Security Cloud Control navigation bar at the left, click **Policies** and select the option that you want.

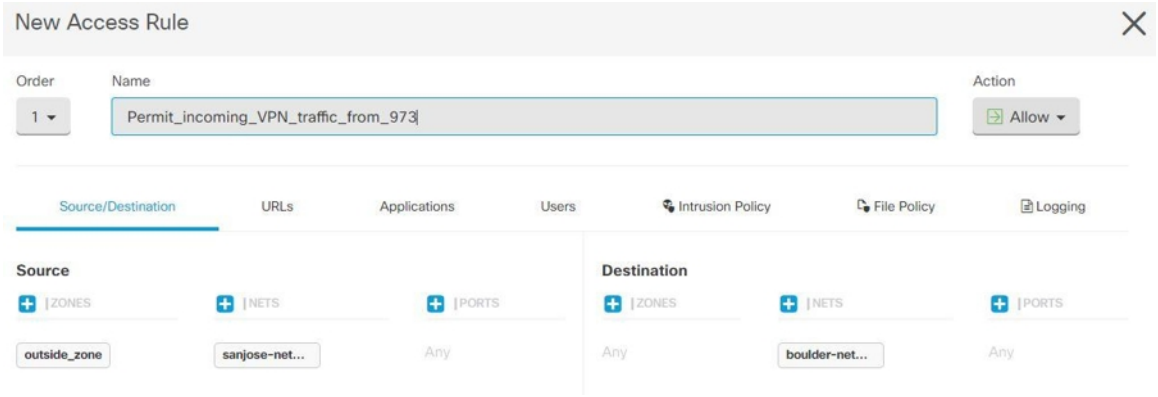
b. Create policies for incoming and outgoing traffic on both peers.

The following example shows steps for creating AC policies on both peers.

Consider two FDM-managed devices 'FTD_BGL_972' and 'FTD_BGL_973' with Site-To-Site VPN connection between two protected networks 'boulder-network' and 'sanjose-network' respectively.

Creating the AC policy for permitting incoming traffic:

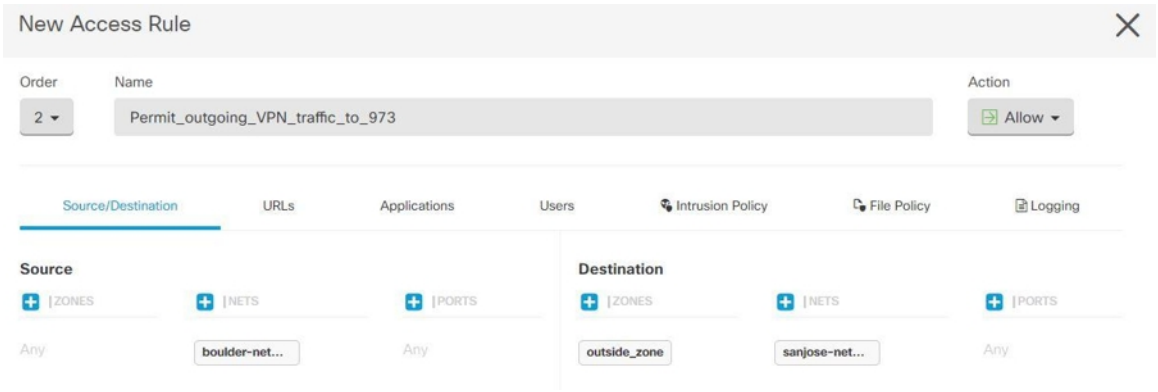
The policy 'Permit_incoming_VPN_traffic_from_973' is created on the 'FTD_BGL_972' device for allowing incoming traffic from the peer ('FTD_BGL_973').



- **Source Zone**: Set the zone of the peer device from which the network traffic originates. In this example, the traffic is originating from FTD_BGL_973 and reaching FTD_BGL_972.
- **Source Network**: Set the protected network of the peer device from which the network traffic originates. In this example, traffic is originating from 'sanjose-network' which is the protected network behind the peer device (FTD_BGL_973).
- **Destination Network**: Set the protected network of the device on which the network traffic arrives. In this example, traffic is arriving at 'boulder-network' which is the protected network behind the peer device (FTD_BGL_972). **Note**: The remaining fields can have the default value ("Any").
- Set **Action** to **Allow** for allowing the traffic subject to the intrusion and other inspection settings in the policy.

Creating the AC policy for permitting outgoing traffic:

The policy 'Permit_outgoing_VPN_traffic_to_973' is created on the 'FTD_BGL_972' device for permitting outgoing traffic to the peer ('FTD_BGL_973').



- **Source Network**: Set the protected network of the peer device from which the network traffic originates. In this example, traffic is originating from 'boulder-network' which is the protected network behind the peer device (FTD_BGL_972).
- **Destination Zone**: Set the zone of the peer device on which the network traffic arrives. In this example, the traffic is arriving from FTD_BGL_972 and reaching FTD_BGL_973.
- **Destination Network**: Set the protected network of the peer on which the network traffic arrives. In this example, traffic is arriving on 'sanjose-network' which is the protected network behind the peer device (FTD_BGL_972). **Note**: The remaining fields can have the default value ("Any").
- Set **Action** to **Allow** for allowing the traffic subject to the intrusion and other inspection settings in the policy.

After creating AC policies on one device, you must create similar policies on its peer.

2. If NAT is configured on either of the peer devices, you need to configure the NAT exempt rules manually. See Exempting Site-to-Site VPN Traffic from NAT.
3. Configure routing for receiving the return VPN traffic on each peer.
   a. **Gateway**-Select the network object that identifies the IP address for the gateway to the destination network. Traffic is sent to this address.
   b. **Interface**-Select the interface through which you want to send traffic. In this example, the traffic is sent through 'outside' interface.
   c. **Destination Networks**-Select one or network objects, that identify the destination network. In this example, the destination is 'sanjose-network' which is behind peer (FTD_BGL_973).

   After configuring routing settings on one device, you must configure similar settings on its peer.

Edit an Existing Security Cloud Control Site-To-Site VPN

The advanced configuration wizard is used by default to modify an existing site-to-site VPN configuration.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Select the desired site-to-site VPN tunnel that you want to edit.
4. In the **Actions** pane, click **Edit**.

Note

Alternatively, you can perform the following to edit the configuration:

a. Open the VPN page and click **Global View** button in the filter panel (for more information, see Global View).

The illustration of all site-to-site VPN tunnels available across all devices appears.

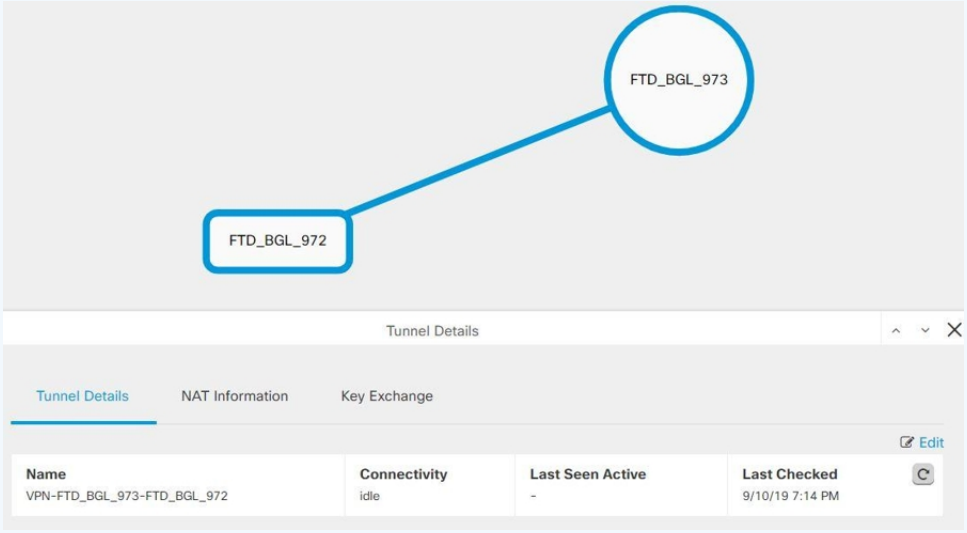
To edit the configuration, one of the peers must be FDM-managed device.

b. Select a device by clicking the box.

c. Click **View details** to view its peers.

d. Click the peer device to view the tunnel details.

You can view the tunnel details, NAT information, and key exchange information pertaining to the device.



e. Click **Edit** in **Tunnel Details**.

5. In the **Peer Devices** section, you can modify the following device configurations: Configuration Name, VPN Access Interface, and Protected Networks.

Note

You cannot change the participating devices.

6. In the **IKE Settings** section, you can modify the following IKEv2 policies configurations:

a. Click the blue plus button for the respective device and select new IKEv2 policies. To delete an existing IKEv2 Policy, hover-over the selected policy and click the **x** icon.

b. Modify the **Pre-Shared Key** for the participating devices. If the pre-shared keys are different for endpoint devices, click the blue settings button and enter the appropriate pre-shared keys for the devices.

c. Click **Next**.

7. In the **IPSec Settings** section, you can modify the following IPSec configurations:

   a. Click the blue plus  button to select new IKEv2 proposals. To delete an existing IKEv2 Proposal, hover-over the selected proposal and click the **x** icon.

   b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**.

   c. Click **Edit VPN**, and then **Finish**.

The Point to point VPN is modified and updated with all the changes you have made.

Delete a Security Cloud Control Firewall Management Site-To-Site VPN Tunnel

Learn how to delete a site-to-site VPN tunnel from the Security Cloud Control VPN page.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. Select the desired site-to-site VPN tunnel that you want to delete.
4. In the **Actions** pane on the right, click **Delete**.

The selected site-to-site VPN tunnel is deleted.

Exempt Site-to-Site VPN Traffic from NAT

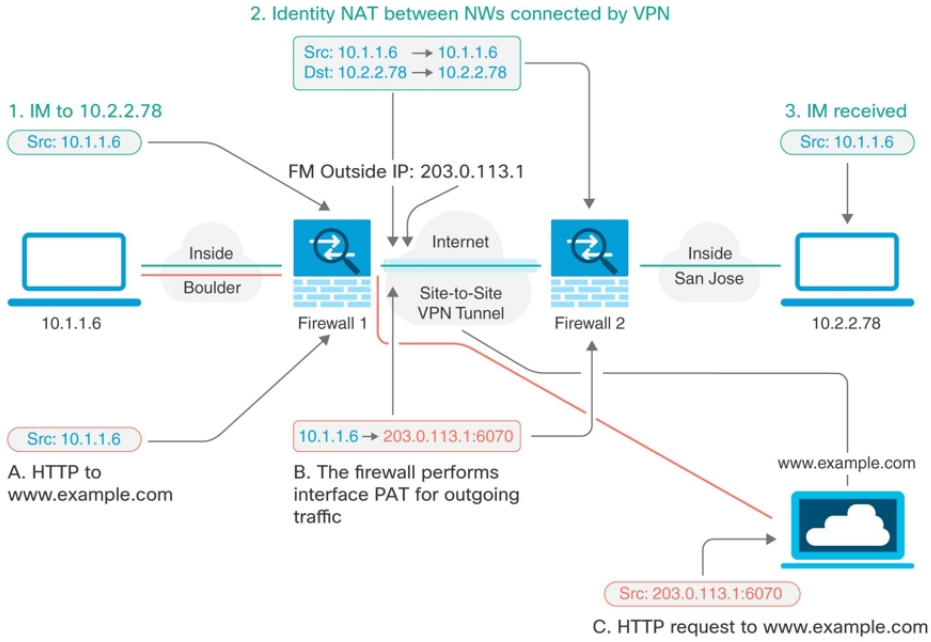
When you have a site-to-site VPN connection defined on an interface, and you also have NAT rules for that interface, you can optionally exempt the traffic on the VPN from the NAT rules. You might want to do this if the remote end of the VPN connection can handle your internal addresses.

When you create the VPN connection, you can select the **NAT Exempt** option to create the rules automatically. However, this works only if your local protected network is connected through a single routed interface (not a bridge group member). If instead, the local networks in the connection reside behind two or more routed interfaces or one or more bridge group members, you need to configure the NAT exempt rules manually.

To exempt VPN traffic from NAT rules, you create an identity manual NAT rule for the local traffic when the destination is the remote network. Then, apply NAT to the traffic when the destination is anything else (for example, the Internet). If you have more than one interface for the local network, create rules for each interface. Also, consider the following suggestions:

- If there is more than one local network in the connection, create a network object group to hold the objects that define the networks.
- If you are including both IPv4 and IPv6 networks in the VPN, create separate identity NAT rules for each.

Consider the following example, which shows a site-to-site tunnel connecting the Boulder and San Jose offices. For traffic that you want to go to the Internet (for example from 10.1.1.6 in Boulder to www.example.com), you need a public IP address provided by NAT to access the Internet. The below example uses interface Port Address Translation (PAT) rules. However, for traffic that you want to go over the VPN tunnel (for example from 10.1.1.6 in Boulder to 10.2.2.78 in San Jose), you do not want to perform NAT; you need to exempt that traffic by creating an identity NAT rule. Identity NAT translates an address to the same address.



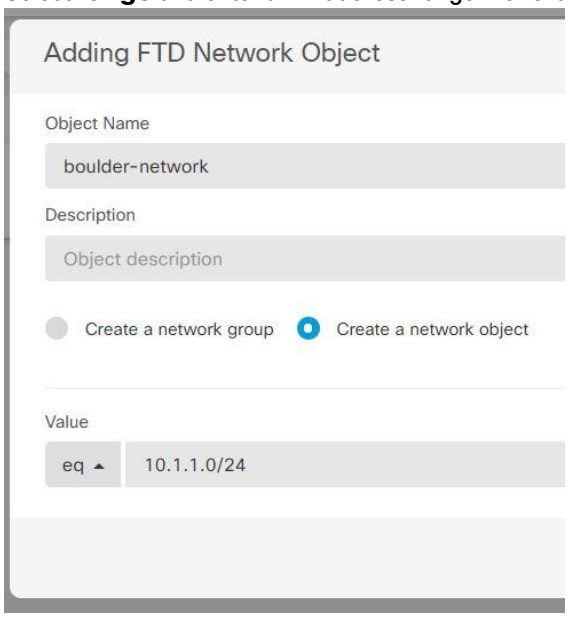
The following example explains the configuration for Firewall1 (Boulder). The example assumes that the inside interface is a bridge group, so you need to write the rules for each member interface. The process is the same if you have a single or multiple routed inside interfaces.

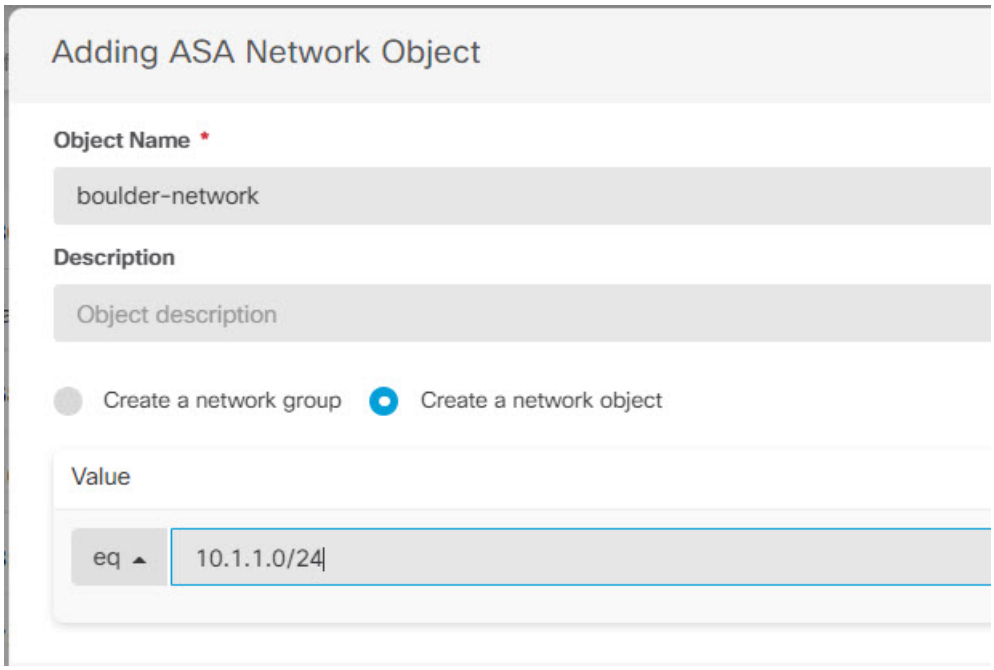
> **Note**
>
> This example assumes IPv4 only. If the VPN also includes IPv6 networks, create parallel rules for IPv6. Note that you cannot implement IPv6 interface PAT, so you need to create a host object with a unique IPv6 address to use for PAT.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Create objects to define the various networks.
   a. In the left pane, click **Objects**.
   b. Click the blue plus button to create an object.
   c. Click **FTD** > **Network**.
   d. Click **ASA** > **Network**.
   e. Identify the Boulder inside network.
   f. Enter an object name (for example, boulder-network).
   g. Select **Create a network object**.
   h. In the Value section:
      - Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.

- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.





i. Click **Add**.

j. Click the blue plus button  to create an object.

k. Define the inside San Jose network.

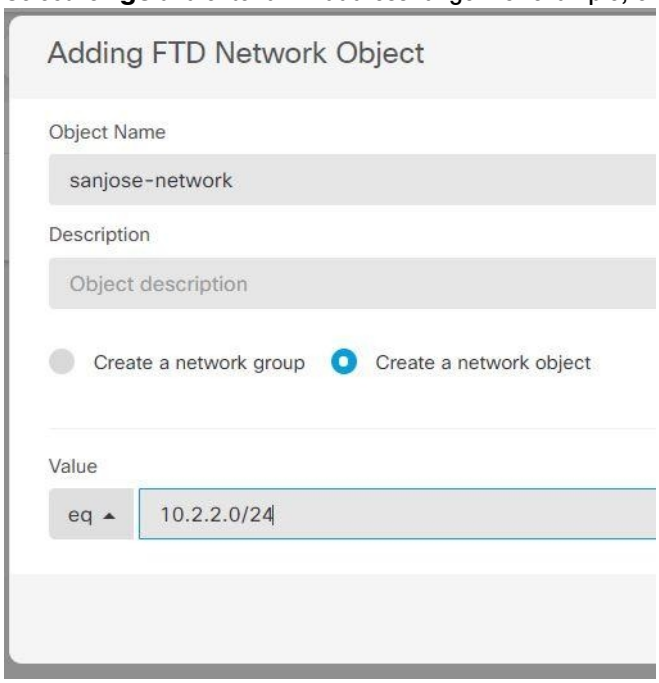
l. Enter the object name (for example, san-jose).

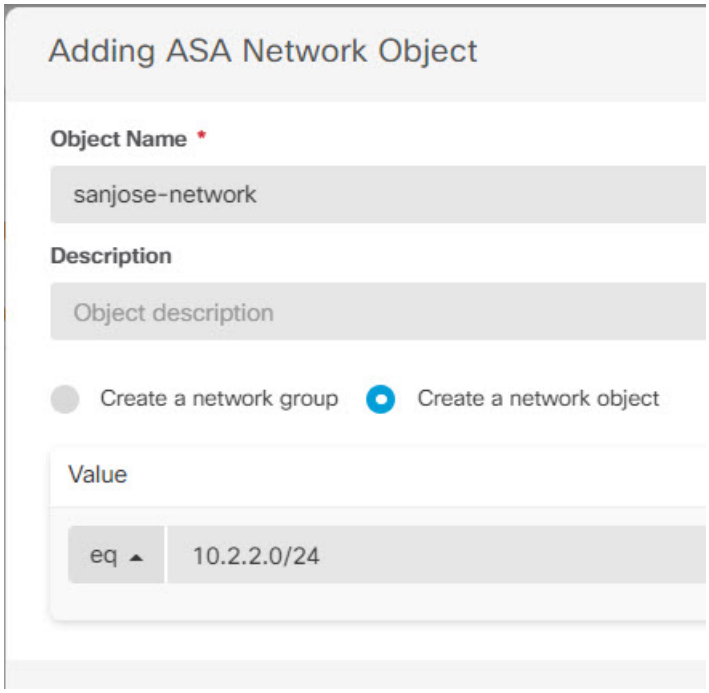
m. Select **Create a network object**.

n. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.

- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.





o. Click **Add**.

3. Configure manual identity NAT for the Boulder network when going over the VPN to San Jose on Firewall1 (Boulder).

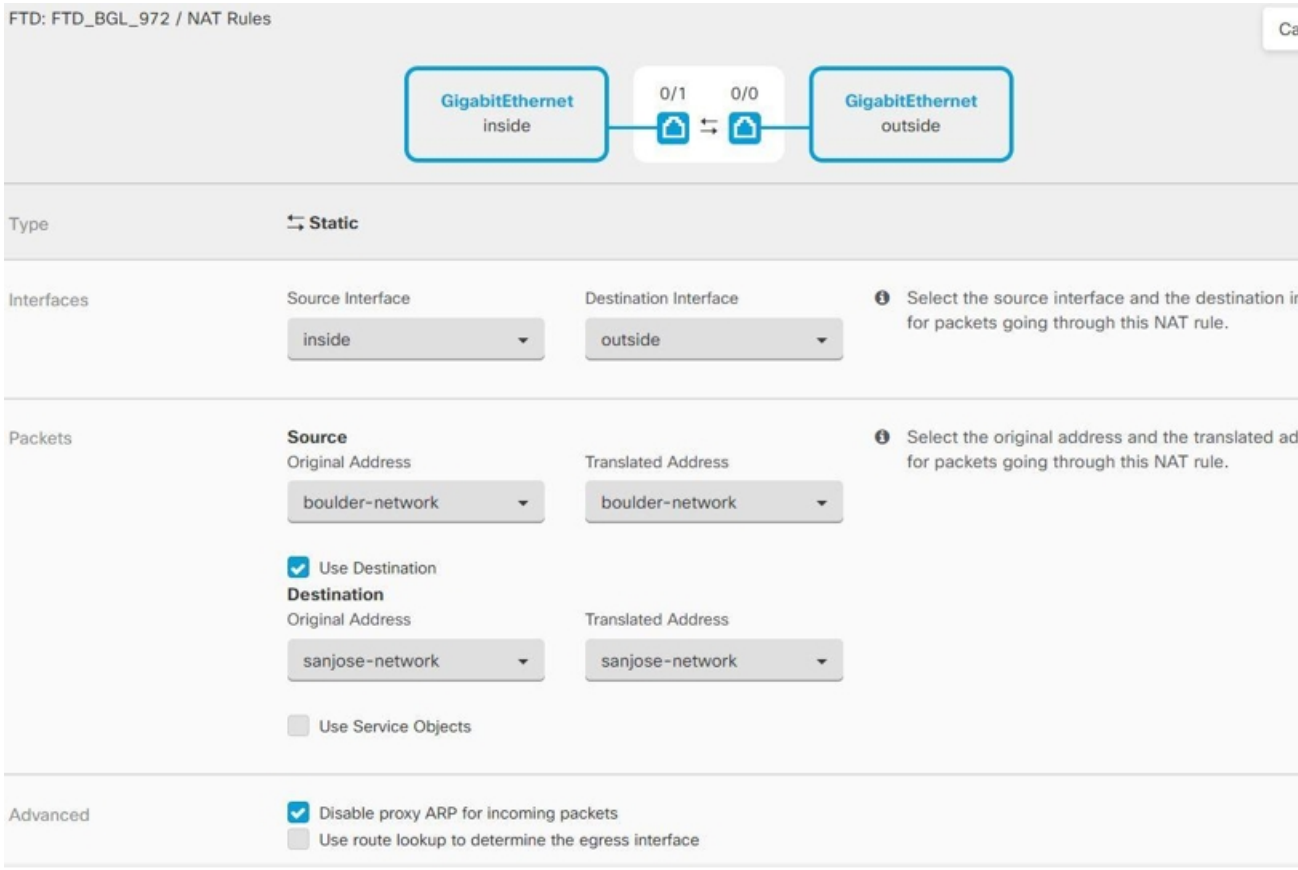
a. In the left pane, click **Security Devices** > **All Devices**.

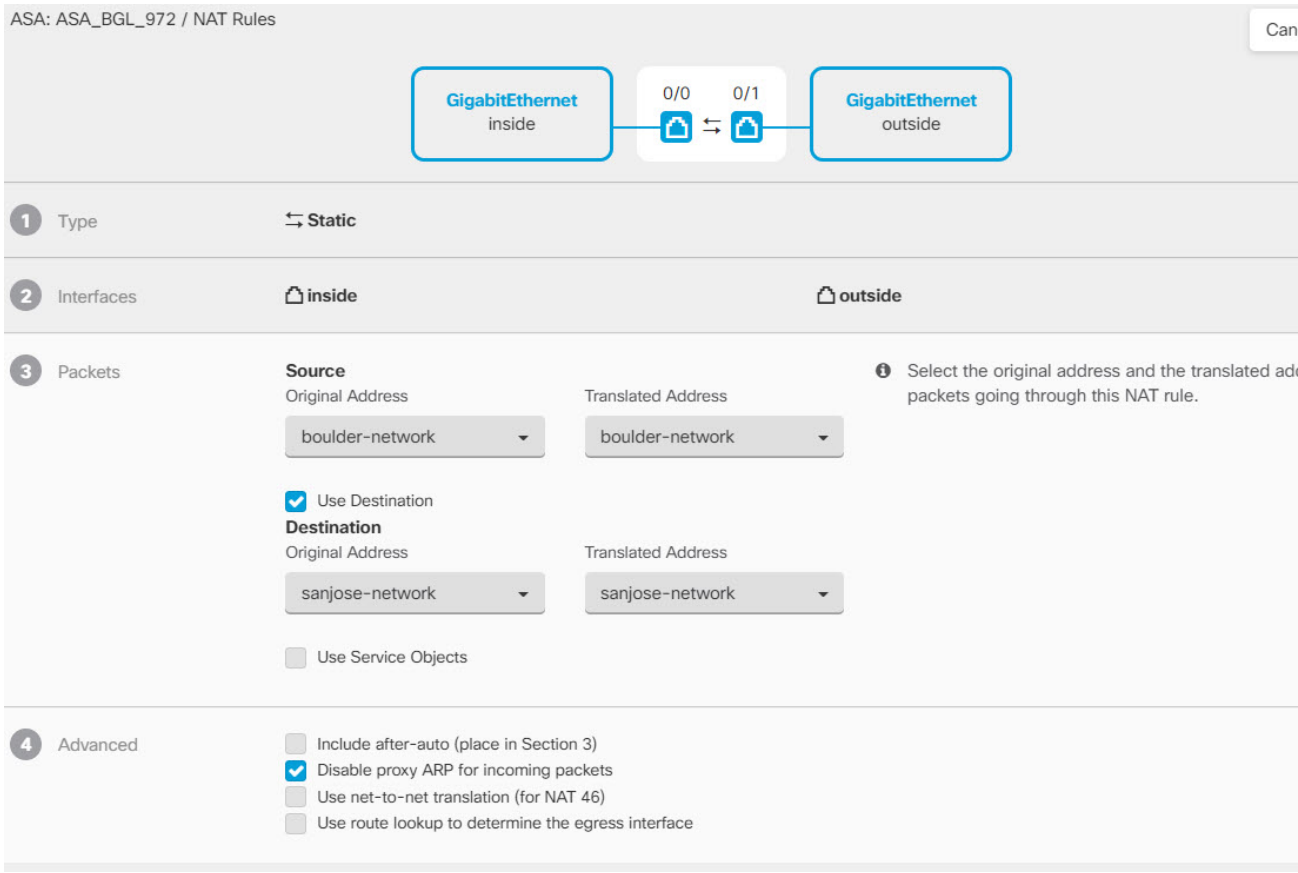
b. Use the filter to find the device for which you want to create the NAT rule.

c. In the Management area of the details panel, click **NAT** NAT.

d. Click + **> Twice NAT**.

- In section 1, select **Static.** Click **Continue**.
- In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.
- In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'boulder-network'.
- Select **Use Destination**.
- Select **Destination Original Address** = 'sanjose-network' and **Source Translated Address** = 'sanjose-network'. **Note**: Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank. This rule configures identity NAT for both source and destination.





- Select **Disable proxy ARP for incoming packets**.
- Click **Save**.
- Repeat the process to create equivalent rules for each of the other inside interfaces.

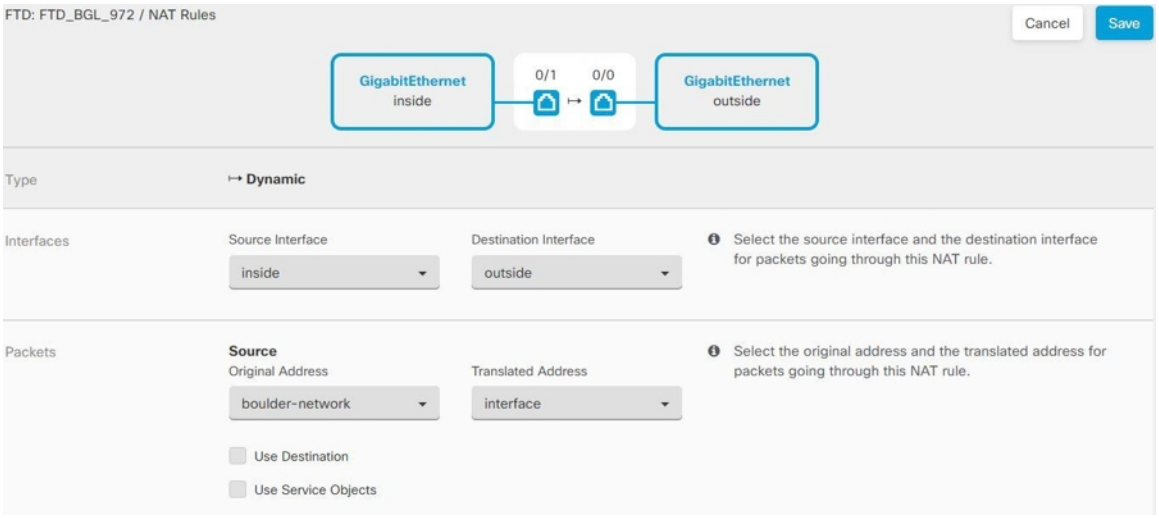
4. Configure manual dynamic interface PAT when going to the Internet for the inside Boulder network on Firewall1 (Boulder). **Note**: There might already be dynamic interface PAT rules for the inside interfaces, covering any IPv4 traffic, as these are created by default during initial configuration. However, the configuration is shown here for completeness. Before completing these steps, check whether a rule already exists that covers the inside interface and network, and skip this step if it does.

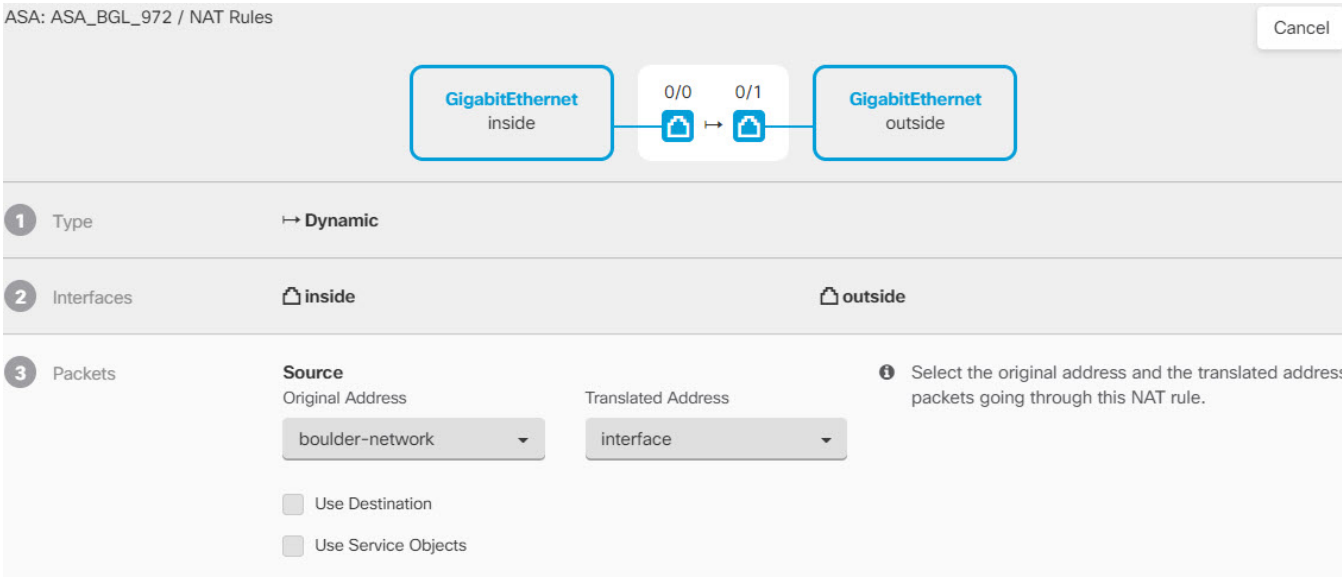
   a. Click + **> Twice NAT**.

   b. In section 1, select **Dynamic.** Click **Continue**.

   c. In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.

d. In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'interface'.





e. Click **Save**.

f. Repeat the process to create equivalent rules for each of the other inside interfaces.

5. Deploy configuration changes to Security Cloud Control. For more information, see Deploy configuration changes made using the Security Cloud Control GUI on page 819.
6. If you are also managing Firewall2 (San Jose), you can configure similar rules for that device.
   - The manual identity NAT rule would be for 'sanjose-network' when the destination is boulder-network. Create new interface objects for the Firewall2 inside and outside networks.
   - The manual dynamic interface PAT rule would be for 'sanjose-network' when the destination is "any."

Site-to-Site VPN Configuration for Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense

Learn how to create site-to-site VPN tunnels for Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense devices with supported peers.

You can create site-to-site IPsec connections between a Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense device and the following devices:

- Firewall Threat Defense
- Secure Firewall ASA
- Multicloud Defense

Create a Site-to-Site VPN Tunnel Between Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense Devices

Use the following procedure to create a site-to-site VPN tunnel between two Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center.

Before you begin

There should not be any pending deployments on the Firewall Threat Defense device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Click the **Create Tunnel** () icon and then click **Site-to-Site VPN**.
4. In the **Peer Selection** area, provide the following information:
   - **Configuration Name**: Enter a unique topology name.

     We recommend naming your topology to indicate that it is a Firewall Threat Defense device VPN, and its topology type.
   - **Peer 1**: Click the **FTD** tab and select a Firewall Threat Defense device.
   - **Peer 2**: Click the **FTD** tab and select a Firewall Threat Defense device.

     If you choose an extranet device, select **Static** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.
5. Click **Next**.
6. In the **Peer Details** area, provide the following information:
   - **VPN Access Interface**: Select the interface for both peer 1 and peer 2 to establish a connection between them.
   - **LAN Interfaces**: Select the interface for both peer 1 and peer 2 that controls the LAN subnet. You can select multiple interfaces
   - **Routing**: Click **Add Networks** and select one or more protected networks for peer 1 and peer 2 to establish a site-to-site tunnel between between them.

7. Click **Next**.
8. In the **IKE Settings** area, choose the IKE versions to use during Internet Key Exchange (IKE) negotiations and specify the privacy configurations: For more information on the IKE policies, see Configuring the Global IKE Policy.

   > **Note**
   >
   > IKE policies are global to a device and apply to all VPN tunnels associated with it. Therefore, adding or deleting policies affect all VPN tunnels in which this device is participating.

   a. Select either or both options as appropriate.

      > **Note**
      >
      > By default, **IKEV Version 2** is enabled.

   b. Click **Add IKEv2 Policies** to select the IKEv2 policies for peer 1 and peer 2.

   c. The **Local Pre-Shared Key** and **Remote Pre-Shared Key** for the participating devices are auto-genreated. Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase.

   d. Click **IKE Version 1** to enable it.

   e. Click **Add IKEv1 Policies** to select the IKEv1 policies for peer 1 and peer 2.

   f. The **IPEv1 Pre-Shared Key** is auto-generated.

9. Click **Next**.
10. In the **IPSec Settings** area, specify the IPSec configurations for peer 1 and peer 2. The corresponding IKEV proposals are available depending on the selection that is made in the **IKE Settings** step.

    For more information on the IPSec settings, see the About IPSec Proposals.

    a. Click **Add IKEv2 IPSec Proposals** and select the IKEv2 proposals you want for peer 1 and peer 2.

    b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see Encryption and Hash Algorithms Used in VPN on page 729.

    c. Click **Next**.

11. In the **Finish** area, you will find a summary of the configurations you have completed.

    Read the configuration and then click **Submit** if you're satisfied.

12.
13. Perform the following steps to deploy the configuration to a Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense device:
    a) Choose **Administration** > **Integrations** > **Firewall Management Center**.
    b) Ensure the check box corresponding to **Cloud-Delivered FMC** is checked and in the **Actions** pane on the right, click **Deployment**.
    c) Select the device participating in the site-to-site VPN configuration and click **Deploy**.

d) Choose **Devices** > **VPN** > **Site To Site**. You can see the same VPN topology that was configured in Security Cloud Control.

Create a Site-to-Site VPN Tunnel Between Cloud-Delivered Firewall Management Center-Managed Firewall Threat Defense and Multicloud Defense

> **Note**
>
> If you are a new customer and you want to use Security Cloud Control to configure a site-to-site VPN between Multicloud Defense and a Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense device, contact Cisco Technical Assistance Center (Cisco TAC) to enable this feature. To manually configure a site-to-site VPN between ASA and Multicloud Defense, you can configure the VPN in the Multicloud Defense application and also on the Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense device manually, and bring up the site-to-site VPN.

You can create site-to-site IPsec connections between a Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense and Multicloud Defense from the Security Cloud Control dashboard that complies with all relevant standards. After the VPN connection is established, the hosts behind the firewall can connect to the hosts behind the gateway through the secure VPN tunnel.

Multicloud Defense currently supports Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and Oracle OCI cloud accounts.

Use the following procedure to create a VPN tunnel between a Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense device and Multicloud Defense from the Security Cloud Control dashboard:

Before you begin

Ensure that the following prerequisites are met:

- The Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense device must not have any pending changes.
- The Multicloud Defense must be onboarded to Security Cloud Control. See Connect Cloud Account.
- The Multicloud Defense Gateway must be in the **Active** state.
- The Multicloud Defense Gateway must be VPN enabled. See Enable VPN within the gateway.
- Read the Multicloud Defense Gateway prerequisites and limitations for more information.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation pane, choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Click the **Create Tunnel** (+) icon and then click **Site-to-Site VPN**.
4. In the **Peer Selection** area, provide the following information:
   - **Configuration Name**: Enter a unique topology name.
   - **Peer 1**: Click the **FTD** tab and select a Firewall Threat Defense device.
   - **Peer 2**: Click the Multicloud Defense tab and select the gateway you want.

If you choose an extranet device, select **Static** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.

5. Click **Next**.
6. In the **Peer Details** area, provide the following information:
   - **VPN Access Interface**: Select the interface for Firewall Threat Defense to establish a connection with the gateway.
   - **Public IP (optional)**: Specify the public IP address of the NAT that maps to the outside interface of the selected Firewall Threat Defense.
   - **Routing**: Click **Add Networks** and select one or more protected networks from Firewall Threat Defense to create a site-to-site tunnel between the selected networks and the Multicloud Defense Gateway
7. Click **Next**.
8. In the **Tunnel Details** area, provide the following information:
   - **Virtual Tunnel Interface IP**: Specify the addresses for the new **Virtual Tunnel Interfaces** on the peer. You can assign any unused IP address that is currently not used on this device.
   - **Autonomous System Number**: Specify the autonomous system number of the network.
9. Click **Next**.
10. In the **IKE Settings** area, click **Add IKEv2** and add the IKE version for the Internet Key Exchange (IKE) negotiations and specify the privacy configurations.

    Security Cloud Control generates a default **Local Pre-Shared Key**. This is a secret key string that is configured on the peers. IKE uses this key during the authentication phase. It is used to verify each other when establishing a tunnel between the peers.
11. Click **Next**.
12. In the **IPSec Settings** area, click **Add IKEv2 IPSec Proposals** and select the IKE IPSec configuration. The proposals are available depending on the selection that is made in the **IKE Settings** step. See Configuring IPSec Proposals.
13. Click **Next**.
14. In the **Finish** area, review the configuration and continue further only if you're satisfied with the configuration.
15. Click **Submit**.

    The configurations are pushed to the Multicloud Defense Gateway.
16. Perform the following steps to deploy the configuration to a Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense device:
    a) Choose **Administration** > **Integrations** > **Firewall Management Center**.
    b) Ensure the check box corresponding to **Cloud-Delivered FMC** is checked and in the **Actions** pane on the right, click **Deployment**.
    c) Select the device participating in the site-to-site VPN configuration and click **Deploy**.
    d) Choose **Devices** > **VPN** > **Site To Site**. You can see the same VPN topology that was configured in Security Cloud Control.

Create a Site-to-Site VPN Between Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense and Secure Firewall ASA

Before you begin

There should not be any pending deployments on the Firewall Threat Defense device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation pane, choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Click the **Create Tunnel** () icon and then click **Site-to-Site VPN**.
4. In the **Peer Selection** area, provide the following information:
   - **Configuration Name**: Enter a unique topology name.

     We recommend naming your topology to indicate that it is a Firewall Threat Defense device VPN, and its topology type.
   - **Peer 1**: Click the **FTD** tab and select a Firewall Threat Defense device.
   - **Peer 2**: Click the **ASA** tab and select a Secure Firewall ASAdevice.

     If you choose an extranet device, select **Static** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.
5. Click **Next**.
6. In the **Peer Details** area, provide the following information:
   - **VPN Access Interface**: Select the interface for both peer 1 and peer 2 to establish a connection between them.
   - **LAN Interfaces**: Select the interface for both peer 1 and peer 2 that controls the LAN subnet. You can select multiple interfaces
   - **Routing**: Click **Add Networks** and select one or more protected networks for peer 1 and peer 2 to establish a site-to-site tunnel between between them.
7. Click **Next**.
8. In the **Tunnel Details** area, provide the following information:
   - **Virtual Tunnel Interface IP**: Specify the address for the new **Virtual Tunnel Interfaces** for Secure Firewall ASA. Security Cloud Control provides a sample address for Secure Firewall ASA which you can change if it causes conflict. You can assign any unused IP address that is currently not used on this device.
9. Click **Next**.
10. In the **IKE Settings** area, choose the IKE versions to use during Internet Key Exchange (IKE) negotiations and specify the privacy configurations: For more information on the IKE policies, see Configuring the Global IKE Policy.

> **Note**
>
> IKE policies are global to a device and apply to all VPN tunnels associated with it. Therefore, adding or deleting policies affect all VPN tunnels in which this device is participating.

a. Select either or both options as appropriate.

> **Note**
>
> By default, **IKEV Version 2** is enabled.

b. Click **Add IKEv2 Policies** to select the IKEv2 policies for peer 1 and peer 2.

c. The **Local Pre-Shared Key** and **Remote Pre-Shared Key** for the participating devices are auto-genreated. Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase.

d. Click **IKE Version 1** to enable it.

e. Click **Add IKEv1 Policies** to select the IKEv1 policies for peer 1 and peer 2.

f. The **IPEv1 Pre-Shared Key** is auto-generated.

11. Click **Next**.
12. In the **IPSec Settings** area, specify the IPSec configurations for peer 1 and peer 2. The corresponding IKEV proposals are available depending on the selection that is made in the **IKE Settings** step.

    For more information on the IPSec settings, see the About IPSec Proposals.

    a. Click **Add IKEv2 IPSec Proposals** and select the IKEv2 proposals you want for peer 1 and peer 2.

    b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see Deciding Which Diffie-Hellman Modulus Group to Use.

13. Click **Next**.
14. In the **Finish** area, you will find a summary of the configurations you have completed.

    Read the configuration and then click **Submit** if you're satisfied.

15. Perform the following steps to deploy the configuration to a Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense device:
    a) Choose **Administration** > **Integrations** > **Firewall Management Center**.
    b) Ensure the check box corresponding to **Cloud-Delivered FMC** is checked and in the **Actions** pane on the right, click **Deployment**.
    c) Select the device participating in the site-to-site VPN configuration and click **Deploy**.
    d) Choose **Devices** > **VPN** > **Site To Site**. You can see the same VPN topology that was configured in Security Cloud Control.

Site-to-Site VPN for Secure Firewall ASA

Learn how to create site-to-site VPN tunnels for Secure Firewall ASA devices, including ASA-to-ASA, ASA-to-extranet, and ASA-to-Multicloud Defense connections.

Security Cloud Control supports these aspects of site-to-site VPN functionality on Secure Firewall ASA devices:

- Both IPsec IKEv1 & IKEv2 protocols are supported.
- Automatic or manual pre-shared keys for authentication.
- IPv4 and IPv6. All combinations of inside and outside are supported.
- IPsec IKEv2 site-to-site VPN topologies provide configuration settings to comply with Security Certifications.
- Static and dynamic interfaces.
- Support the static or dynamic IP address for the extranet device as an endpoint.

Configure Site-to-Site VPN Connections with Dynamically Addressed Peers

Security Cloud Control allows you to create a site-to-site VPN connection between peers when one of the peers' VPN interface IP address is not known or when the interface obtains its address from a DHCP server. Any dynamic peer whose preshared key, IKE settings, and IPsec configurations match with another peer can establish a site-to-site VPN connection.

Consider two peers, A and B. The static peer is a device whose IP address of its VPN interface is fixed and a dynamic peer is a device whose IP address of the VPN interface is not known or has a temporary IP address.

The following use cases describe different scenarios for establishing a secure site-to-site VPN connection with dynamically-addressed peers:

- A is a static peer, and B is a dynamic peer or conversely.
- A is a static peer, and B is a dynamic peer with a resolved IP address from the DHCP server or conversely.
- A is a dynamic peer, and B is an extranet device with a static or dynamic IP address.
- A is a dynamic peer with a resolved IP address from the DHCP server, and B is an Extranet device with a static or dynamic IP address.

Note

If the IP address of the interface is changed by using a local manager like Adaptive Security Device Manager (ASDM), the **Configuration Status** of that peer in Security Cloud Control shows "Conflict Detected". When you resolve this out-of-band change, the **Configuration Status** of the other peer changes to the "Not Synced" state. You must deploy the Security Cloud Control configuration to the device which is in "Not Synced" state.

Typically, the dynamic peer must be the one that initiates the connection as the other peer would not know the IP address of the dynamic peer. When the remote peer attempts to establish the connection, the other peer validates the connection using the preshared key, IKE settings, and IPsec configurations.

Because the VPN connection is established only after the remote peer initiates the connection, any outbound traffic that matches access control rules that allow traffic in the VPN tunnel will be dropped until that connection is established. This ensures that data does not leave your network without the appropriate encryption and VPN protection.

Note

A site-to-site VPN connection cannot be configured in the following scenario:

If a device has more than one dynamic peer connection.

- Consider three devices A, B, and C.
- Configure site-to-site VPN connection between A (static peer) and B (dynamic peer).
- Configure site-to-site VPN connection between A and C (dynamic peer) by creating an Extranet device. Assign the static VPN interface IP address of A to the Extranet device and establish a connection with C.

Secure Firewall ASA Site-to-Site VPN Guidelines and Limitations

- Security Cloud Control does not support a crypto-acl to design the interesting traffic for S2S VPN. It only supports protected networks.
- Whenever IKE ports 500/4500 are in use or when there are some PAT translations that are active, the site-to-site VPN cannot be configured on the same ports as it fails to start the service on those ports.
- Transport mode is not supported only tunnel mode. IPsec tunnel mode encrypts the entire original IP datagram which becomes the payload in a new IP packet. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind a firewall. Tunnel mode is the normal way regular IPsec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- For this release, only PTP topology is supported, containing one or more VPN tunnels. Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.

Guidelines for Virtual Tunnel Interfaces

- VTIs are only configurable in IPsec mode. To terminate GRE tunnels on an Secure Firewall ASA is unsupported.
- You can use dynamic or static routes for traffic using the tunnel interface.
- The MTU for VTIs is automatically set, according to the underlying physical interface. However, if you change the physical interface MTU after the VTI is enabled, you must disable and reenable the VTI to use the new MTU setting.
- If Network Address Translation has to be applied, the IKE and ESP packets will be encapsulated in the UDP header.
- IKE and IPsec security associations will be re-keyed continuously regardless of data traffic in the tunnel. This ensures that VTI tunnels are always up.
- Tunnel group name must match what the peer will send as its IKEv1 or IKEv2 identity.
- For IKEv1 in LAN-to-LAN tunnel groups, you can use names which are not IP addresses, if the tunnel authentication method is digital certificates and/or the peer is configured to use aggressive mode.
- VTI and crypto map configurations can co-exist on the same physical interface, provided the peer address configured in the crypto map and the tunnel destination for the VTI are different.
- By default, all traffic through VTI is encrypted.
- By default, the security level for VTI interfaces is 0.
- Access list can be applied on a VTI interface to control traffic through VTI.
- Only BGP is supported over VTI.

- If Secure Firewall ASA is terminating IOS IKEv2 VTI clients, disable the config-exchange request on IOS, because Secure Firewall ASA cannot retrieve the mode-CFG attributes for this L2L session initiated by an IOS VTI client.
- IPv6 is not supported.

Create a Site-to-Site VPN Tunnel Between Secure Firewall ASA

Use the following procedure to create a site-to-site VPN tunnel between two ASAs or an ASA with an Extranet device:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.
3. Click the **Create Tunnel** () icon and then click **Site-to-Site VPN**.
4.
5. In the **Peer Selection** area, provide the following information:
   - **Configuration Name**: Enter a unique topology name.
   - **Peer 1**: Click the **ASA** tab and select a Secure Firewall ASA device.
   - **Peer 2**: Click the **ASA** tab and select a Secure Firewall ASAdevice.

     If you choose an extranet device, select **Static** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.
6. Click **Next**.
7. In the **Peer Details** area, provide the following information:
   - Select one of the options to create a new **Policy Based** or **Route Based** site-to-site VPN.
   - **VPN Access Interface**: Select the interface for both peer 1 and peer 2 to establish a connection between them.
   - (Applicable to Route Based) **LAN Interfaces**: Select the interface for both peer 1 and peer 2 that controls the LAN subnet. You can select multiple interfaces
   - **Routing**: Click **Add Networks** and select one or more protected networks for peer 1 and peer 2 to establish a site-to-site tunnel between between them.
   - (Applicable to Policy Based) **NAT Exempt**: Select to exempt the VPN traffic from NAT policies on the local VPN access interface. It must be configured manually for individual peers. If you do not want NAT rules to apply to the local network, select the interface that hosts the local network. This option works only if the local network resides behind a single routed interface (not a bridge group member). If the local network is behind more than one routed interface or one or more bridge group members, you must manually create the NAT exempt rules. For information on manually creating the required rules, see Exempt ASA Site-to-Site VPN Traffic from NAT.
8. Click **Next**.
9. (Applicable to Route Based) In the **Tunnel Details**, the **VTI Address** fields are automatically filled once the peer devices are configured in the previous step. If necessary, you can manually enter an IP address that will be used as the new VTI.
10. In the **IKE Settings** area, choose the IKE versions to use during Internet Key Exchange (IKE) negotiations and specify the privacy configurations: For more information on the IKE policies, see Global IKE policies on page 157.

> **Note**
>
> IKE policies are global to a device and apply to all VPN tunnels associated with it. Therefore, adding or deleting policies affect all VPN tunnels in which this device is participating.

a. Select either or both options as appropriate.

> **Note**
>
> By default, **IKEV Version 2** is enabled.

b. Click **Add IKEv2 Policies** to select the IKEv2 policies for peer 1 and peer 2.

c. The **Local Pre-Shared Key** and **Remote Pre-Shared Key** for the participating devices are auto-genreated. Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase.

d. Click **IKE Version 1** to enable it.

e. Click **Add IKEv1 Policies** to select the IKEv1 policies for peer 1 and peer 2.

f. The **IPEv1 Pre-Shared Key** is auto-generated.

11. Click **Next**.
12. In the **IPSec Settings** area, specify the IPSec configurations for peer 1 and peer 2. The corresponding IKEV proposals are available depending on the selection that is made in the **IKE Settings** step.

    For more information on the IPSec settings, see the Global IKE policies on page 157.

    a. Click **Add IKEv2 IPSec Proposals** and select the IKEv2 proposals you want for peer 1 and peer 2.

    b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see Encryption and Hash Algorithms Used in VPN on page 729.

13. In the **Finish** area, review the configuration and continue further only if you're satisfied with the configuration.

    By default, the **Deploy changes to ASA immediately** check box is checked to deploy the configurations immediately to the ASA device after clicking **Submit**.

    If you want to review and deploy the configurations manually later, then uncheck this check box.

You are directed to the VPN Tunnels page that shows the newly configured site-to-site VPN tunnel. The changes are staged and must be deployed manually. A routing policy is created to route the VTI traffic automatically between the devices over the VTI tunnel. To see this policy, select the device from the **Security Devices** page and choose **Configuration** > **Diff**.

Create a Site-to-Site VPN Between ASA and Multicloud Defense Gateway

> **Note**
>
> If you are a new customer and you want to use Security Cloud Control to configure a site-to-site VPN between Multicloud Defense and an ASA device, contact Cisco Technical Assistance Center (Cisco TAC) to enable this feature.
>
> To manually configure a site-to-site VPN between ASA and Multicloud Defense, you can configure the VPN in the Multicloud Defense application and also on the ASA device manually, and bring up the site-to-site VPN.

You can create site-to-site IPsec connections between an ASA and a Multicloud Defense Gateway that complies with all relevant standards. After the VPN connection is established, the hosts behind the firewall can connect to the hosts behind the gateway through the secure VPN tunnel.

Multicloud Defense currently supports Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and Oracle OCI cloud accounts.

Use the following procedure to create a VPN tunnel between an ASA device that is managed by Security Cloud Control and Multicloud Defense Gateway from the Security Cloud Control dashboard:

Before you begin

Ensure that the following prerequisites are met:

- The ASA device must not have any pending changes.
- Create a BGP profile in the ASA console prior to creating a VPN tunnel. See *Configure ASA Border Gateway Protocol* for more information.
- The Multicloud Defense Gateway must be in the **Active** state.
- The Multicloud Defense Gateway must be VPN enabled. See Enable VPN within the gateway.
- Read the ASA site-to-site VPN limitations and guidelines for more information.
- Read the Multicloud Defense Gateway prerequisites and limitations for more information.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Click the **Create Tunnel** () icon and then click **Site-to-Site VPN**.
4. In the **Peer Selection** area, provide the following information:
   - **Configuration Name**: Enter a unique topology name.
   - **Peer 1**: Click the **ASA** tab and select a Secure Firewall ASA device.
   - **Peer 2**: Click the **Multicloud Defense** tab and select a multicloud gateway.

     If you choose an extranet device, select **Static** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.
5. Click **Next**.

6. In the **Peer Details** area, provide the following information:
   - **VPN Access Interface**: Select the interface for Secure Firewall ASA to establish a connection with Multicloud Defense Gateway.
   - **LAN Interfaces**: Select the interface for Secure Firewall ASA that controls the LAN subnet. You can select multiple interfaces
   - **Public IP (optional)**: Specify the public IP address of the NAT that maps to the outside interface of the selected Secure Firewall ASA.
   - **Routing**: Click **Add Networks** and select one or more protected networks for Secure Firewall ASA to establish a site-to-site tunnel with Multicloud Defense Gateway.
7. Click **Next**.
8. In the **Tunnel Details** area, provide the following information:
   - **Virtual Tunnel Interface IP**: Specify the addresses for the new **Virtual Tunnel Interfaces** on the peers. Security Cloud Control provides a sample address for Secure Firewall ASA which you can change if it causes conflict. You can assign any unused IP address that is currently not used on this device.
   - **Autonomous System Number** (Peer 1): If the Secure Firewall ASA device does not have an autonomous system number configured, Security Cloud Control will suggest one for the device, which can be modified. If the device already has an autonomous system number configured, the current value will be displayed and cannot be modified.
   - **Autonomous System Number** (Peer 2): If a BGP profile is assigned to the Multicloud Defense Gateway, the autonomous number associated with the profile is displayed, which cannot be modified. See Add a Multicloud Defense Gateway.
9. Click **Next**.
10. In the **IKE Settings** area, Security Cloud Control generates a default **Local Pre-Shared Key**. This is a secret key string that is configured on the peers. IKE uses this key during the authentication phase. It is used to verify each other when establishing a tunnel between the peers.
11. In the **Finish** area, review the configuration and continue further only if you're satisfied with the configuration.

    By default, the **Deploy changes to ASA immediately** check box is checked to deploy the configurations immediately to the ASA device after clicking **Submit**.

    If you want to review and deploy the configurations manually later, then uncheck this check box.
12. Click **Submit**.

    The configurations are pushed to the Multicloud Defense Gateway.

The VPN page in Security Cloud Control shows the site-to-site tunnel created between the peers. You will be able to see the corresponding tunnel in the Multicloud Defense Gateway portal.

Exempt Site-to-Site VPN Traffic from NAT

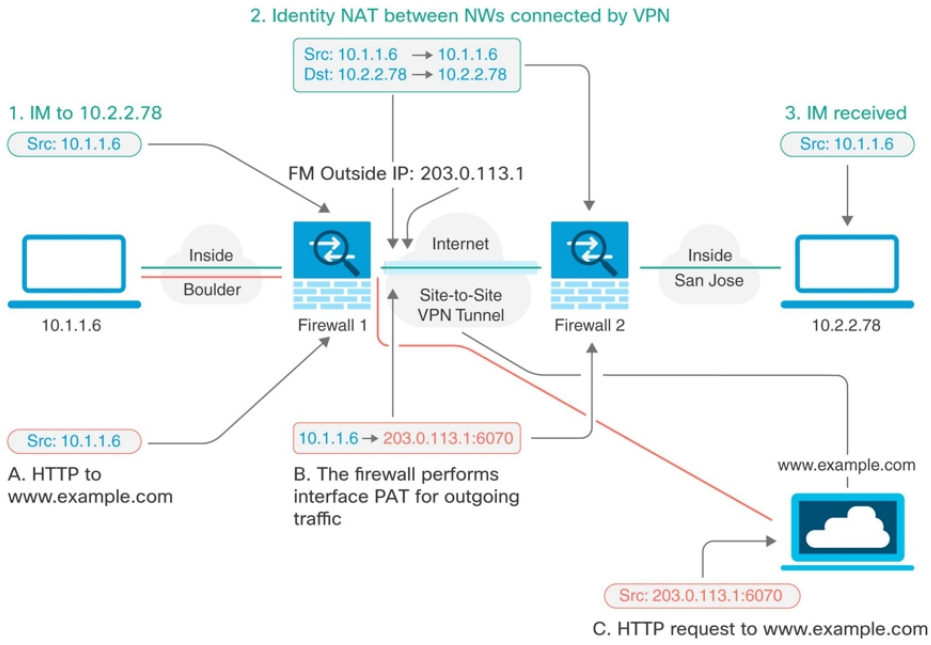
When you have a site-to-site VPN connection defined on an interface, and you also have NAT rules for that interface, you can optionally exempt the traffic on the VPN from the NAT rules. You might want to do this if the remote end of the VPN connection can handle your internal addresses.

When you create the VPN connection, you can select the **NAT Exempt** option to create the rules automatically. However, this works only if your local protected network is connected through a single routed interface (not a bridge group member). If instead, the local networks in the connection reside behind two or more routed interfaces or one or more bridge group members, you need to configure the NAT exempt rules manually.

To exempt VPN traffic from NAT rules, you create an identity manual NAT rule for the local traffic when the destination is the remote network. Then, apply NAT to the traffic when the destination is anything else (for example, the Internet). If you have more than one interface for the local network, create rules for each interface. Also, consider the following suggestions:

- If there is more than one local network in the connection, create a network object group to hold the objects that define the networks.
- If you are including both IPv4 and IPv6 networks in the VPN, create separate identity NAT rules for each.

Consider the following example, which shows a site-to-site tunnel connecting the Boulder and San Jose offices. For traffic that you want to go to the Internet (for example from 10.1.1.6 in Boulder to www.example.com), you need a public IP address provided by NAT to access the Internet. The below example uses interface Port Address Translation (PAT) rules. However, for traffic that you want to go over the VPN tunnel (for example from 10.1.1.6 in Boulder to 10.2.2.78 in San Jose), you do not want to perform NAT; you need to exempt that traffic by creating an identity NAT rule. Identity NAT translates an address to the same address.



The following example explains the configuration for Firewall1 (Boulder). The example assumes that the inside interface is a bridge group, so you need to write the rules for each member interface. The process is the same if you have a single or multiple routed inside interfaces.

Note

This example assumes IPv4 only. If the VPN also includes IPv6 networks, create parallel rules for IPv6. Note that you cannot implement IPv6 interface PAT, so you need to create a host object with a unique IPv6 address to use for PAT.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Create objects to define the various networks.
   a. In the left pane, click **Objects**.

b. Click the blue plus button to create an object.

c. Click **FTD** > **Network**.

d. Click **ASA** > **Network**.

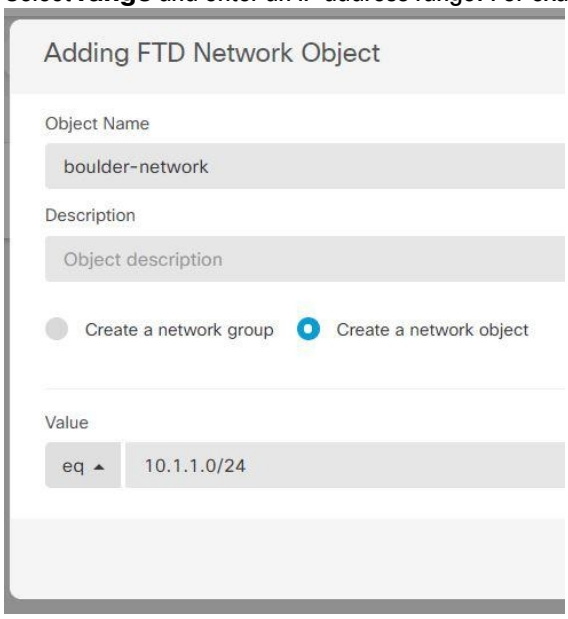
e. Identify the Boulder inside network.

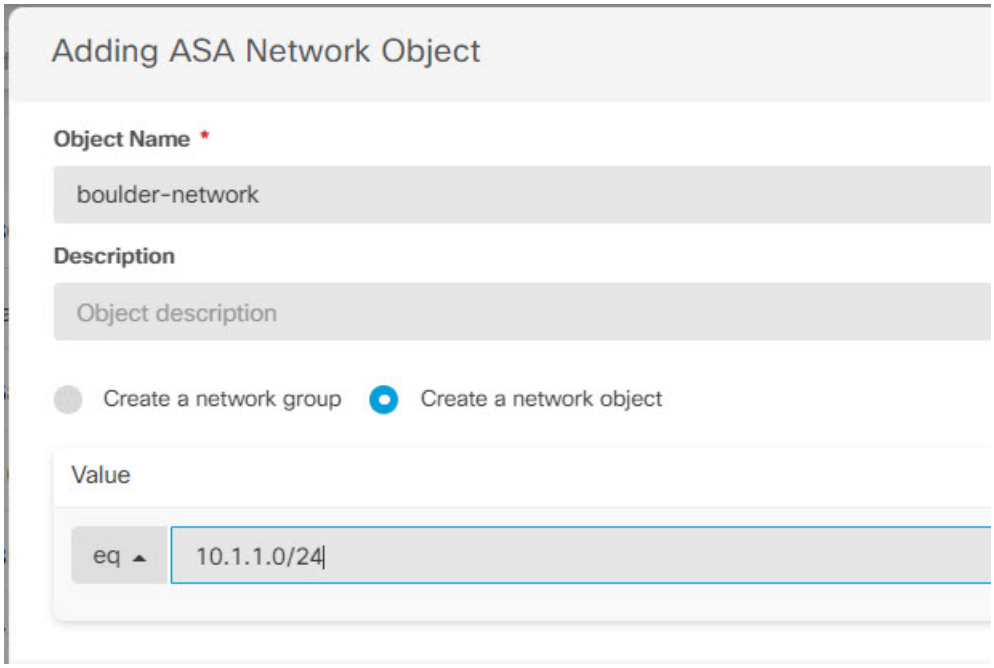
f. Enter an object name (for example, boulder-network).

g. Select **Create a network object**.

h. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.
- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.





i. Click **Add**.

j. Click the blue plus button to create an object.

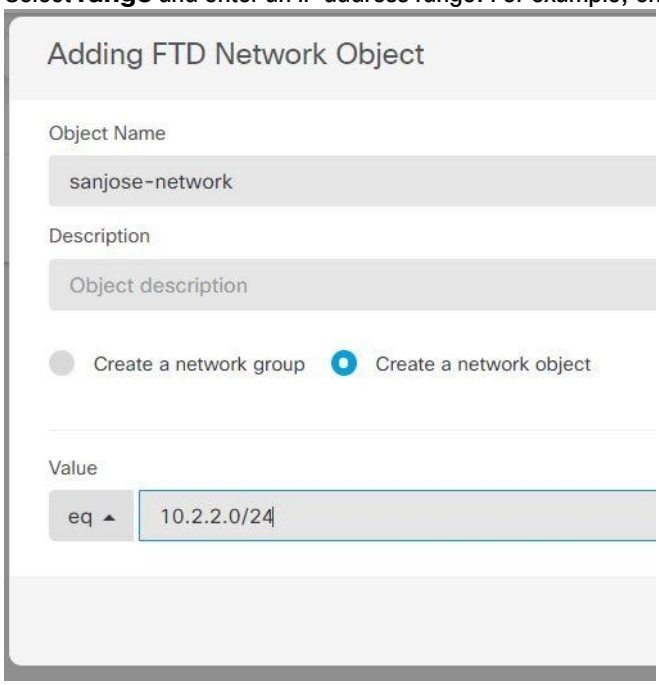
k. Define the inside San Jose network.

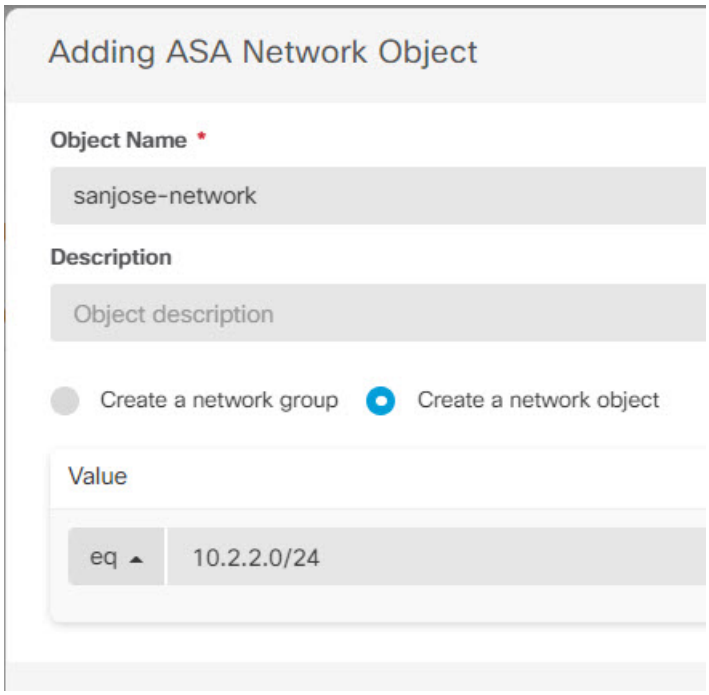
l. Enter the object name (for example, san-jose).

m. Select **Create a network object**.

n. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.
- Select **range** and enter an IP address range. For example, enter the network address as `10.1.1.0/24`.





o. Click **Add**.

3. Configure manual identity NAT for the Boulder network when going over the VPN to San Jose on Firewall1 (Boulder).

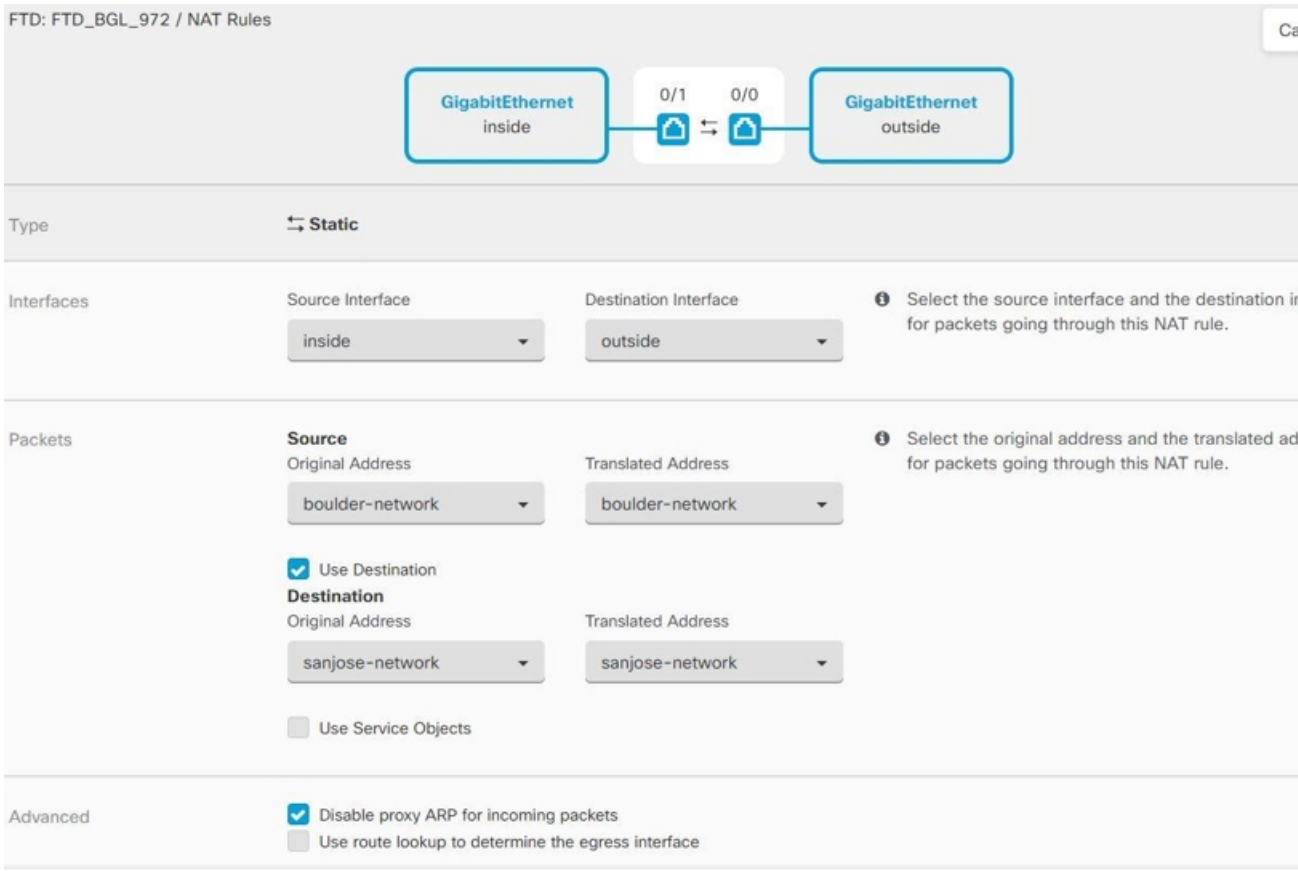
a. In the left pane, click **Security Devices** > **All Devices**.

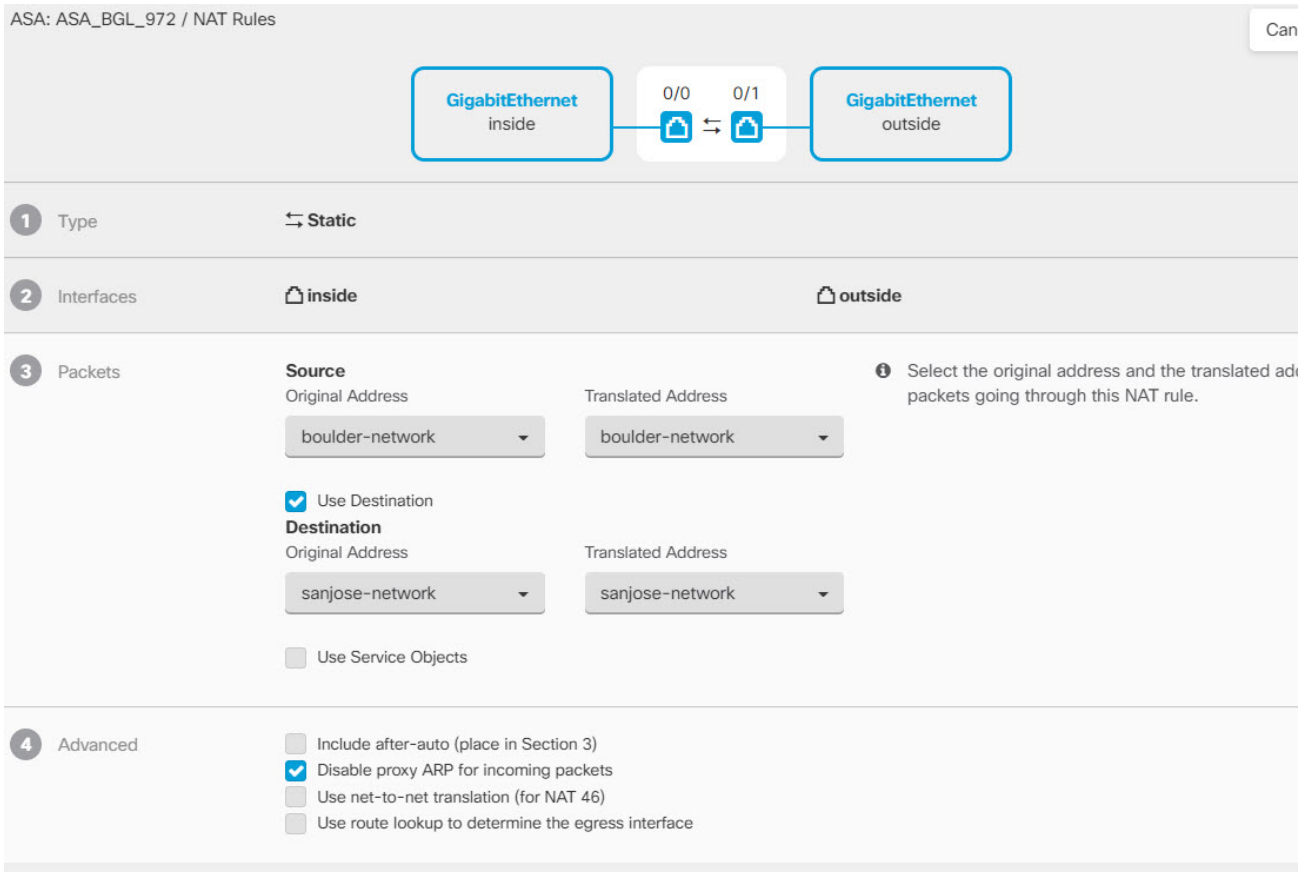
b. Use the filter to find the device for which you want to create the NAT rule.

c. In the Management area of the details panel, click **NAT** NAT.

d. Click + **> Twice NAT**.

- In section 1, select **Static.** Click **Continue**.
- In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.
- In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'boulder-network'.
- Select **Use Destination**.
- Select **Destination Original Address** = 'sanjose-network' and **Source Translated Address** = 'sanjose-network'. **Note:** Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank. This rule configures identity NAT for both source and destination.





- Select **Disable proxy ARP for incoming packets**.
- Click **Save**.
- Repeat the process to create equivalent rules for each of the other inside interfaces.

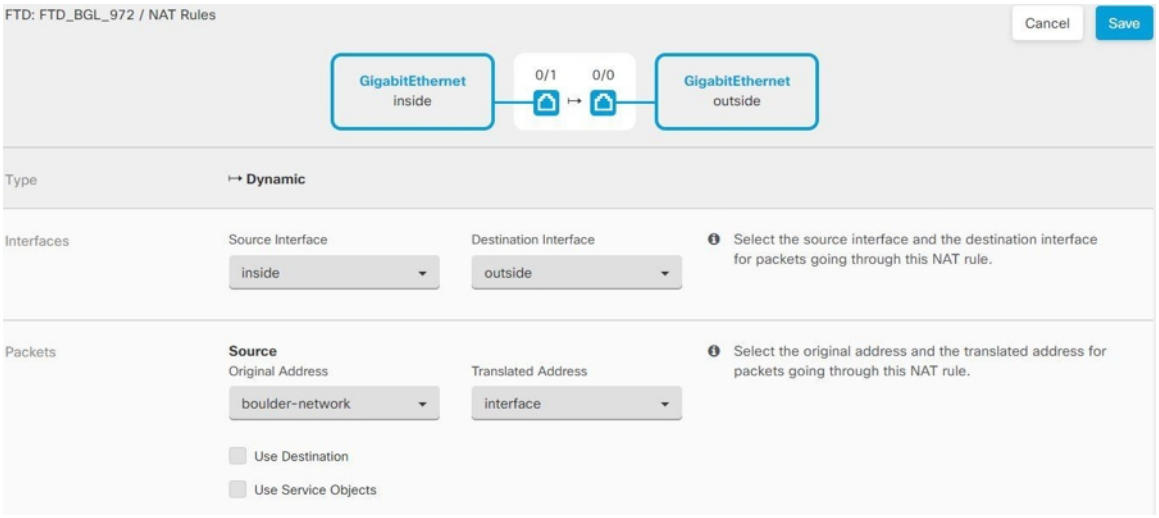
4. Configure manual dynamic interface PAT when going to the Internet for the inside Boulder network on Firewall1 (Boulder). **Note**: There might already be dynamic interface PAT rules for the inside interfaces, covering any IPv4 traffic, as these are created by default during initial configuration. However, the configuration is shown here for completeness. Before completing these steps, check whether a rule already exists that covers the inside interface and network, and skip this step if it does.

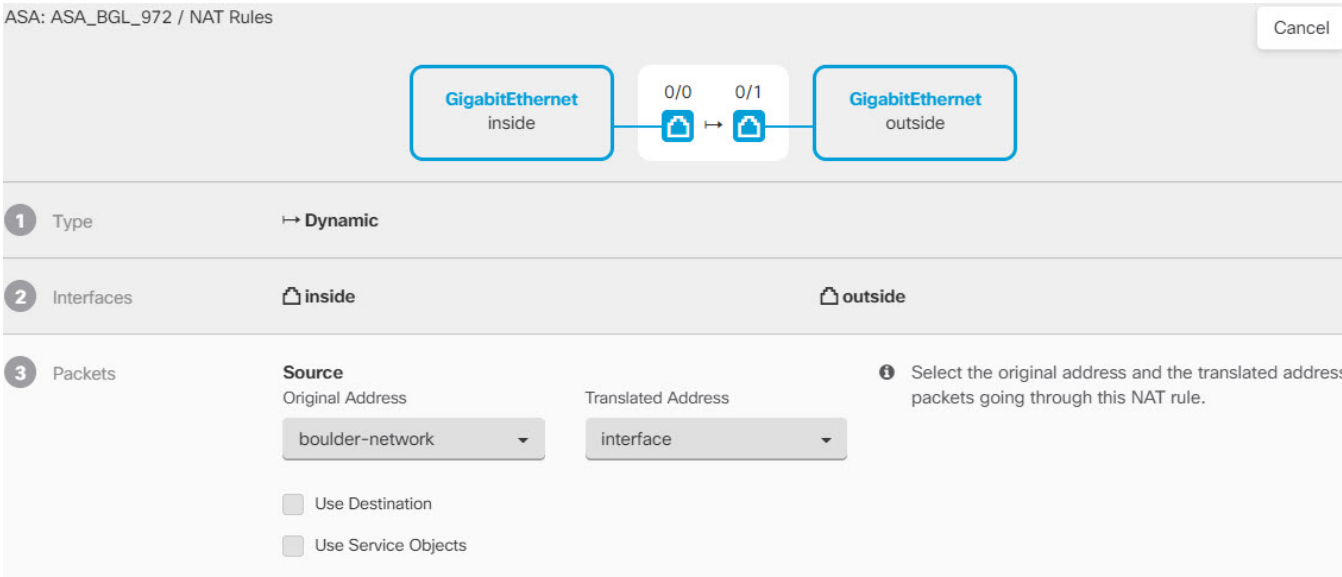
   a. Click + **> Twice NAT**.

   b. In section 1, select **Dynamic.** Click **Continue**.

   c. In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.

d. In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'interface'.





e. Click **Save**.

f. Repeat the process to create equivalent rules for each of the other inside interfaces.

5. Deploy configuration changes to Security Cloud Control. For more information, see Deploy configuration changes made using the Security Cloud Control GUI on page 819.
6. If you are also managing Firewall2 (San Jose), you can configure similar rules for that device.
   - The manual identity NAT rule would be for 'sanjose-network' when the destination is boulder-network. Create new interface objects for the Firewall2 inside and outside networks.
   - The manual dynamic interface PAT rule would be for 'sanjose-network' when the destination is "any."

Monitor ASA Site-to-Site Virtual Private Networks

Learn how to monitor ASA site-to-site VPN tunnels, check connectivity, review dashboard status, identify issues, and view tunnel details.

Security Cloud Control allows you to monitor already existing site-to-site VPN configurations on onboarded ASA devices. It doesn't allow you to modify or delete the site-to-site configuration.

Security Cloud Control allows you to monitor already existing site-to-site VPN configurations on onboarded AWS devices. It doesn't allow you to modify or delete the site-to-site configuration.

Security Cloud Control allows you to monitor, modify, and delete existing or newly created site-to-site VPN configurations on onboarded FDM-managed devices.

Check Site-to-Site VPN Tunnel Connectivity

Use the **Check Connectivity** button to trigger a real-time connectivity check against the tunnel to identify whether the tunnel is currently active or idle. Unless you click the on-demand connectivity check button, a check across all tunnels, available across all onboarded devices, occurs once an hour.

Note

- Security Cloud Control runs this connectivity check command on the ASAFTD to determine if a tunnel is active or idle:

```
show vpn-sessiondb l2l sort ipaddress
```

- Model ASA device(s) tunnels will always show as **Idle**.

To check tunnel connectivity from the VPN page:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Search and filter the list of tunnels for your site-to-site VPN tunnel and select it.
4. In the Actions pane at the right, click **Check Connectivity**.

Site-To-Site VPN Dashboard

Security Cloud Control provides a consolidated information about site-to-site VPN connections created in the tenant.

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Site to Site VPN**. The **Site-to-Site VPN** provides the information in the following widgets:

   - **Sessions & Insights**: Displays a bar graph representing Active VPN Tunnels and Idle VPN Tunnels, each in appropriate colors.

- **Issues**: Shows the total number of tunnels detected with issues.
- **Pending Deploy**: Shows the total number of tunnels with pending deployment.

By clicking on a value in the pie chart or any link in the widget, the site-to-site VPN listing page is displayed with a filter based on the selected value. For instance, in the **VPN Tunnel Status** widget, on clicking the **Active VPN Tunnels**, you will be directed to the site-to-site VPN listing page with the **Active** status filter applied, showing only the active tunnels.

Identify VPN Issues

Security Cloud Control can identify VPN issues on ASAFTD. (This feature is not yet available for AWS VPC site-to-site VPN tunnels.) This article describes:

- Find VPN Tunnels with Missing Peers
- Find VPN Peers with Encryption Key Issues
- Find Incomplete or Misconfigured Access Lists Defined for a Tunnel
- Find Issues in Tunnel Configuration

  Resolve Tunnel Configuration Issues on page 767

Find VPN Tunnels with Missing Peers

The "Missing IP Peer" condition is more likely to occur on ASA devices than FDM-managed devices.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. Select **Table View**.
4. Open the Filter panel by clicking the filter icon .
5. Check **Detected Issues**.
6. Select each device reporting an issue ⚠ and look in the Peers pane at the right. One peer name will be listed. Security Cloud Control reports the other peer name as, "[Missing peer IP.]"

Find VPN Peers with Encryption Key Issues

Use this approach to locate VPN Peers with encryption key issues such as:

- IKEv1 or IKEv2 keys are invalid, missing, or mismatched
- Obsolete or low encryption tunnels

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. Select **Table View**.

4. Open the Filter panel by clicking the filter icon .
5. Select each device reporting an issue ⚠ and look in the Peers pane at the right. The peer information will show you both peers.
6. Click on **View Peers** for one of the devices.
7. Double-click the device reporting the issue in the Diagram View.
8. Click **Key Exchange** in the Tunnel Details panel at the bottom. You will be able to view both devices and diagnose the key issue from that point.

Find Incomplete or Misconfigured Access Lists Defined for a Tunnel

The "incomplete or misconfigured access-list" condition could only occur on ASA devices.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. Select **Table View**.
4. Open the Filter panel by clicking the filter icon .
5. Select each device reporting an issue ⚠ and look in the Peers pane at the right. The peer information shows you both peers.
6. Click on **View Peers** for one of the devices.
7. Double-click the device reporting the issue in the Diagram View.
8. Click **Tunnel Details** in the Tunnel Details panel at the bottom. You will see the message, "Network Policy: Incomplete"

Find Issues in Tunnel Configuration

The tunnel configuration error can occur in the following scenarios:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn't match the other VPN tunnel, the "IKE value Mismatch" message appears.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. Select **Table View**.
4. Open the Filter panel by clicking the filter icon .
5. In the **Tunnel Issues**, click **Detected Issues** to view the VPN configuration reporting errors. You can view the configuration reporting issues ⚠.
6. Select the VPN configuration reporting issues.
7. In the **Peers** pane on the right, the ⚠ icon appears for the peer having the issue. Hover over the ⚠ icon to see the issue and resolution.

Next Step: Resolve Tunnel Configuration Issues.

Resolve Tunnel Configuration Issues

This procedure attempts to resolve these tunnel configuration issues:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn't match the other VPN tunnel, the "IKE value Mismatch" message appears.

See Find Issues in Tunnel Configuration for more information.

Procedure

---

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab and select the device associated with the VPN configuration reporting an issue.
4. Accept the device changes.
5. In the left pane, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.
6. Select the VPN configuration reporting this issue.
7. In the **Actions** pane, click the **Edit** icon.
8. Click **Next** in each step until you click the **Finish** button in step 4.
9. Preview and deploy configuration changes for all devices on page 817.

Search and filter site-to-site VPN tunnels

Learn how to search and filter site-to-site VPN tunnels in Security Cloud Control Firewall Management.

Use the filter sidebar  in combination with the search field to focus your search of VPN tunnels presented in the VPN tunnel diagram.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Click the filter icon  to open the filter pane.
4. Use these filters to refine your search:
   - **Filter by Device**: Click **Filter by Device**, select the device type tab, and check the devices you want to find by filtering.
   - **Tunnel Issues**: Indicates whether issues have been detected on either side of the tunnel. For example, a device may be missing an associated interface, peer IP address, access list, or may have IKEv1 proposal mismatches. (Detecting tunnel issues is not yet available for AWS VPC VPN tunnels.)
   - **Devices/Services**: Filters by type of device.
   - **Status**: Indicates tunnel status, which can be active or idle.

- **Active**: An open session exists in which network packets traverse the VPN tunnel, or a successful session was established that has not timed out yet. The "Active" status indicates that the tunnel is operational and relevant.
- **Idle**: Security Cloud Control is unable to discover an open session for this tunnel. The tunnel may either be not in use or there is an issue with this tunnel.

- **Onboarded**: Devices could be managed by Security Cloud Control or not managed (unmanaged) by Security Cloud Control.
  - **Managed**: Filters by devices that Security Cloud Control manages.
  - **Unmanaged**: Filters by devices that Security Cloud Control does not manage.

- **Device Types**: Indicates whether either side of the tunnel is a live (connected) or model device.

5. You can also search the filtered results by device name or IP address by entering that information in the search bar. The search is case-insensitive.

Onboard an Unmanaged Site-to-Site VPN Peer

Security Cloud Control will discover a site-to-site VPN tunnel when one of the peers is onboarded. If the second peer is not managed by Security Cloud Control, you can filter the list of VPN tunnels to find the unmanaged device and onboard it:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. Select **Table View**.
4. Open the filter panel by clicking .
5. Check **Unmanaged**.
6. Select a tunnel from the table from the results.
7. In the **Peers** pane on the right, click **Onboard Device** and follow the instructions on the screen.

Viewing AWS Site-to-Site VPN Tunnels

AWS site-to-site VPN connects your Virtual Private Cloud (VPC) to your enterprise network through a secure tunnel.

All site-to-site VPN configuration occurs in the AWS Management Console. Once you onboard your VPC, Security Cloud Control is able to display the site-to-site VPN connections maintained by your AWS VPC and display them on the VPN Tunnels page so that you can manage them along with all your other site-to-site connections. Each VPN connection from your network to your VPC is made up of two separate VPN tunnels.

From the VPN Tunnels page in Security Cloud Control, you can view information about all your managed VPN peers, filter and search for the site-to-site VPN peers of the VPC, and onboard unmanaged VPN peers.

Security Cloud Control polls the AWS Management Console every 10 minutes looking for changes to the site-to-site VPN configuration. If Security Cloud Control finds that there has been a change, it polls for changes in that configuration and stores the changes in its database. Security Cloud Control administrators will then be able to view the new configurations in Security Cloud Control.

Amazon Web Services (AWS) Reference Material

AWS Virtual Private Network Documentation

View IKE Object Details of Site-To-Site VPN Tunnels

You can view the details of the IKE objects configured on the peers/devices of the selected tunnel. These details appear in a tree structure in a hierarchy based on the priority of the IKE policy object.

> **Note**
>
> Extranet devices don't show the IKE Objects details.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. In the **VPN Tunnels** page, click the name of the VPN tunnel that connects the peers.
4. Under **Relationships** on the right, expand the object that you want to see its details.

View Last Successful Site-to-Site VPN Tunnel Establishment Date

This information typically provides the date and time when the VPN tunnel was last successfully established, ensuring connectivity between the two sites. Accessing this data can help you monitor VPN health and troubleshoot any connectivity issues that might arise.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. The **VPN Tunnels** page displays all the site-to-site VPN tunnels configured across your managed devices. You can click a tunnel to view more details in the right pane.

   > **Note**
   >
   > Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel.

   The **Last Active** field shows the date and time the VPN tunnel was successfully established.

View Site-to-Site VPN Tunnel Information

The site-to-site VPN table view is a complete listing of all site-to-site VPN tunnels available across all devices onboarded to Security Cloud Control. A tunnel only exists once in this list. Clicking on a tunnel listed in the table provides an option in the right side bar to navigate directly to a tunnel's peers for further investigation.

In cases where Security Cloud Control does not manage both sides of a tunnel, you can click Onboard Device to open the main onboarding page an onboard the unmanaged peer. In cases where Security Cloud Control manages both side of a tunnel, the Peer 2 column contains the name of the managed device. However, in the case of an AWS VPC, the Peer 2 column contains the IP address of the VPN gateway.

To view site-to-site VPN connections in the table view:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN** to open the VPN page.
3. The **VPN Tunnels** page displays all the site-to-site VPN tunnels configured across your managed devices. You can click on a tunnel to view more details in the right pane.

> **Note**
>
> Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel.

Site-to-Site VPN Global View

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **Network Connections** > **Site to Site VPN**.
3. Click the **Global view** button.
4. Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.
5. Select one of the peers represented in the Global View.
6. Click **View Details**.
7. Click the other end of the VPN tunnel and Security Cloud Control displays Tunnel Details, NAT Information, and Key Exchange information for that connection:
   - **Tunnel Details**-Displays the name and connectivity information about the tunnel. Clicking the Refresh icon updates the connectivity information for the tunnels.
   - **Tunnel Details specific to AWS connections**-Tunnel details for AWS site-to-site connections are slightly different than for other connections. For each connection from the AWS VPC to your VPN gateway, AWS creates two VPN tunnels. This is for high availability.
     - The name of the tunnel represents the name of the VPC your VPN gateway is connected to. The IP address named in the tunnel is the IP address that your VPN gateway knows as the VPC.

  - If the Security Cloud Control Connectivity status shows **active**, the AWS tunnel state is **Up**. If the Security Cloud Control Connectivity state is **inactive**, the AWS tunnel state is **Down**.

- **NAT Information**-Displays the type of NAT rule being used, original and translated packet information, and provides links to the NAT table to view the NAT rule for that tunnel. (Not yet available for AWS VPC site-to-site VPN.)
- **Key Exchange**-Displays the cryptographic keys in use by the tunnel and key-exchange issues. (Not yet available for AWS VPC site-to-site VPN.)

Site-to-Site VPN Tunnels Pane

The Tunnels pane displays a list of all the tunnels associated with a particular VPN gateway. For site-to-site VPN connections between your VPN gateway and an AWS VPC, the tunnels pane shows all the tunnels from your VPN gateway to the VPC. Since each site-to-site VPN connection between your VPN gateway and an AWS VPC has two tunnels, you will see double the number of tunnels you normally would for other devices.

VPN Gateway Details

Displays the number of peers connected to the VPN gateway and the IP address of the VPN gateway. This is only visible in the VPN Tunnels page.

View Peer

After you select a site-to-site VPN peer pair, the peers pane lists the two devices in the pair and allows you to click **View Peer** for one of the devices. By clicking **View Peer**, you see any other site-to-site peer that device is associated with. This is visible in the Table view and in the Global view.

44 Establish Remote Access VPN connection using Security Cloud Control Firewall Management

Topics:

- Introduction to Remote Access Virtual Private Network
- Configure Remote Access Virtual Private Network for ASA

Introduction to Remote Access Virtual Private Network

Learn how remote access VPN helps users securely connect to your network from outside the office using supported computers or mobile devices.

Remote Access virtual Private Network (RA VPN) capability enables users to connect to your network from a location outside the physical office premises. This means that they can use a computer or a supported iOS/Android device that is connected to the internet and access your network resources securely. This feature is particularly useful for mobile workers who need to connect from their home network or a public Wi-Fi network while ensuring that their data remains safe and protected.

Configure Remote Access Virtual Private Network for ASA

Learn how to configure ASA remote access VPN in Security Cloud Control, including new configurations and VPN settings discovered from onboarded ASA devices.

The ASA creates a remote access virtual private network (VPN) by creating a secure connection across a TCP/IP network (such as the Internet) that users see as a private connection. It can create single-user-to-LAN connections and LAN-to-LAN connections.

The secure connection is called a tunnel, and the ASA uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The ASA functions as a bidirectional tunnel endpoint: it can receive plain packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination.

Security Cloud Control provides an intuitive user interface for configuring a new remote access Virtual Private Network. It also allows you to quickly and easily configure remote access VPN connection for multiple Adaptive Security Appliance (ASA) devices onboarded in Security Cloud Control.

Security Cloud Control allows you to configure the remote access VPN configuration on ASA devices from scratch. It also allows you to manage the remote access VPN settings that have already been configured using another ASA management tool, such as the Adaptive Security Defense Manager (ASDM) or Cisco Security Manager (CSM). When you onboard an ASA device that already has remote access VPN settings, Security Cloud Control automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. This default configuration can contain all the connection profile objects that are defined on the device. If you want to understand the RAVPN attributes that are read into Security Cloud Control, see the Read RA VPN Configuration of an Onboarded ASA Device section. Otherwise, you can start performing steps described in the "End-to-End Remote Access VPN Configuration Process for ASA" section.

End-to-End Remote Access VPN Configuration Process for ASA

This section provides the end-to-end procedure for configuring remote access VPN on an ASA device onboarded to Security Cloud Control.

To enable remote access VPN for your clients, you need to configure several separate items. The following procedure provides the end-to-end process.

Procedure

1. Configure the identity source used for authenticating remote users.

   You can use the following sources to authenticate users attempting to connect to your network using remote access VPN. Additionally, you can use client certificates for authentication, either alone or in conjunction with an identity source.

   See Configure Identity Sources for ASA for more information.

- Active Directory identity realm: As a primary authentication source. The user accounts are defined in your Active Directory (AD) server. See Configuring AD Identity Realms. See Create or Edit an ASA Active Directory Realm Object.
- RADIUS server group: As a primary or secondary authentication source, and for authorization and accounting. See Create or Edit an ASA RADIUS Server Object or Group.
- Local Identity Source (the local user database): As a primary or fallback source. You can define users directly on the device and not use an external server. If you use the local database as a fallback source, ensure that you define the same usernames/passwords as the ones described in the external server. **Note**: You can create user accounts directly on the ASA device only from the Adaptive Security Device Manager (ASDM). See the "Configure Local User Groups" section in the Objects for Access Control" chapter of the Cisco ASA Series Firewall ASDM Configuration Guide, X.Y.

2. (optional) Create RA VPN group policies. The group policy defines user-related attributes. You can configure group policies to provide differential access to resources based on group membership. Alternatively, use the default policy for all connections.
3. Create ASA Remote Access VPN Configuration on page 775.
4. Configure ASA Remote Access VPN Connection Profile on page 779.
5. (optional) Exempt Remote Access VPN Traffic from NAT on page 793.
6. Review and deploy configuration changes to the devices.

Important

If you change the Remote Access VPN configuration by using a local manager like Adaptive Security Device Manager (ASDM), the **Configuration Status** of that device in Security Cloud Control shows "Conflict Detected". See Out-of-Band Changes on an ASA Device. You can Resolve Configuration Conflicts on this ASA.

Once the remote access VPN configuration is downloaded to the ASA devices, the users can connect to your network from a remote location using a computer or other supported iOS or Android device connected to the Internet. You can monitor live AnyConnect remote access VPN sessions from all onboarded ASA remote access VPN head-ends in your tenant.

See Monitoring Remote Access Virtual Private Network.

Create ASA Remote Access VPN Configuration

Security Cloud Control allows you to add one or more Adaptive Security Appliance (ASA) devices to the remote access VPN configuration wizard and configure the VPN interfaces, access control, and NAT exemption settings associated with the devices. Therefore, each remote access VPN configuration can have connection profiles and group policies shared across multiple ASA devices that are associated with the remote access VPN configuration. Further, you can enhance the configuration by creating connection profiles and group policies.

You can either onboard an ASA device that has already been configured with remote access VPN settings or a new device without remote access VPN settings. See Onboard a Secure Firewall ASA on page 260. When you onboard an ASA device that already has remote access VPN settings, Security Cloud Control automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. Also, this default configuration can contain all the connection profile objects that are defined on the device. See Read RA VPN Configuration of an Onboarded ASA Device for more information. Security Cloud Control allows you to delete the default configuration.

Important

- You are not allowed to add ASA and FTD in the same Remote Access VPN Configuration.
- An ASA device cannot have more than one remote access VPN Configuration.

Before you begin

Before adding the ASA device to the remote access VPN configuration, the following prerequisites must be met on the ASA device:

- License requirements.

  Device must be enabled for export-controlled functionality.

  To view the license summary of your ASA device, execute the show license summary command in the ASA command-line interface.

  To use the Security Cloud Control ASA CLI interface, see Use the command line interface.

  - Example of export-controlled functionality enabled in the license summary :

  ```
  Registration: Status: REGISTERED Smart Account: Cisco SVS temp-request access
  licensing@cisco.com Export-Controlled Functionality: ALLOWED

  Last Renewal Attempt: None

  Next Renewal Attempt: Jun 08 2021 09:46:22 UTC
  ```

  The 'Export-Controlled Functionality' property must be in the 'Allowed' state for creating or editing the VPN configuration.

  If this property is in the 'Not Allowed' state, Security Cloud Control displays an error message ('remote access VPN cannot be configured for devices which are not export compliant.') when you are creating or modifying the VPN configuration and doesn't allow remote access VPN configuration on the device.

- Device Identity Certificates.

  Certificates are required to authenticate connections between the clients and the ASA device. Before starting the VPN configuration, ensure that the identity certificate is already present on the ASA device.

  To determine whether or not the certificate is present on the device, execute the **show crypto CA Certificates** command in the ASA command-line interface.

  To use the Security Cloud Control ASA CLI interface, see ASA command line interface on page 303.

  If the identity certificate is not present or you want to enroll in a new certificate, install them on ASA using Security Cloud Control. See ASA Certificate Management.

  The usage of digital certificates in remote access VPN context is explained in Remote Access VPN Certificate-Based Authentication on page 792.

- Outside interfaces.

  The outside interfaces must be configured already on the ASA device. **You need to use either ASDM or ASA CLI to configure interfaces**. To know configure interfaces using ASDM, see the "Interfaces" book of the Cisco ASA Series General Operations CLI Configuration Guide, X.Y.

- Download the AnyConnect packages and upload them to a remote server. Later, use the remote access VPN wizard or ASA File Management wizard to upload the AnyConnect software packages from the server to ASAs. See Manage AnyConnect Software Packages on an ASA Device for instructions.

- There are no configuration deployments pending.

- If you are using the local database for authentication Add user accounts to the local database using ASDM or ASA CLI.

  To add user accounts using ASDM, see the "Add a User Account to the Local Database" section in the "AAA Servers and the Local Database" book of the Cisco ASA Series VPN CLI Configuration Guide, X.Y.

  To add user accounts using ASA CLI, execute **username[***username***] password [***password***] privilege [***priv_level***]** command.

- ASA changes are synchronized to Security Cloud Control.

  1. In the left pane, click **Security Devices** and search for one or more ASA devices to be synchronized.
  2. Select one or more devices and then click **Check for changes**. Security Cloud Control communicates with one or more FTD devices to synchronize the changes.

- Remote access VPN configuration group policy objects are consistent.
  - Ensure that all inconsistent group policy objects are resolved as they cannot be added to the remote access VPN configuration. Either address the issue or remove inconsistent group policy objects from the **Objects** page. For more information see, Resolve Duplicate Object Issues and Resolve Inconsistent Object Issues.

Procedure

1. Onboard a Secure Firewall ASA on page 260.
2. From the Security Cloud Control Home page, click **Firewall**.
3. In the left pane, click **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM**.
4. Click the blue plus  button to create a new remote access VPN configuration.
5. Enter a name for the Remote Access VPN configuration.
6. Click the blue plus  button to add ASA devices to the configuration.

   You can add the device details and configure network traffic-related permissions that are associated with the device.

   a. Provide the following device details:
      - **Device**: Select an ASA device that you want to add and click **Select**. **Important**: You are not allowed to add ASA and FTD in the same Remote Access VPN Configuration.
      - **Certificate of Device Identity**: Select the internal certificate used for establishing the identity of the device. This establishes the device identity for AnyConnect clients when they make a connection to the device. Clients must accept this certificate to complete a secure VPN connection.
      - **Outside Interface**: Select the interface to which users connect when making the remote access VPN connection. Although this is normally the outside (internet-facing) interface, choose whichever interface is between the device and the end-users you are supporting with this connection profile.

      > **Attention**
      >
      > You cannot create or modify remote access VPN configuration for devices that are not export compliant. You must license the ASA device with export-controlled functionality enabled and try again.

   b. Click **Continue** to configure the traffic permissions.

- **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**: Decrypted traffic is subjected to Access Control Policy inspection by default. Enabling this option bypasses the decrypted traffic option bypasses the access control policy inspection, but the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic.

  Note that if you select this option, the system configures the sysopt connection permit-vpn command, which is a global setting. This will also impact the behavior of site-to-site VPN connections.

  If you do not select this option, it might be possible for external users to spoof IP addresses in your remote access VPN address pool, and thus gain access to your network. This can happen because you will need to create access control rules that allow your address pool to have access to internal resources. If you use access control rules, consider using user specifications to control access, rather than source IP address alone.

  The downside of selecting this option is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic. This also means that no connection events will be generated for the traffic, and thus statistical dashboards will not reflect VPN connections.

- **NAT Exempt**: NAT exemption exempts addresses from translation and allows both translated and remote hosts to initiate connections with your protected hosts. Configure NAT Exempt to exempt traffic to and from the remote access VPN endpoints from NAT translation. See Exempt Remote Access VPN Traffic from NAT on page 793.

c. Click **OK**.

The **AnyConnect Packages Detected** shows the AnyConnect packages that are already available on the device.

There are two options to upload AnyConnect package to ASA from remote access VPN wizard:

- (Option 1): Select a package from Security Cloud Control's repository. The ASA must have access to the internet.
- (Option 2): Specify the ftp/http/https/scp/smb/tftp URL location where the AnyConnect package is preloaded.

See Upload new AnyConnect Software Packages for instructions.

> **Note**
>
> Note: If you want to replace an existing package, see Replace an Existing AnyConnect Package.

7. Click **OK**.

The ASA VPN configuration is created.

Modify ASA Remote Access VPN Configuration

You can modify the name and the device details of an existing remote access VPN configuration.

Procedure

1. Select the configuration to be modified and under **Actions**, click **Edit**.

- Modify the name if required.

- Click the blue plus  button to add a new device
- Click to perform the following on the ASA device.
  - Click **Edit** to modify the existing remote access VPN configuration.
  - Click **Remove** to remove the ASA device from the remote access VPN configuration. All connection profiles and remote access VPN settings associated with that device except the group policies are deleted. You can remove the group policies explicitly from the objects page.

    Note

    You cannot remove the ASA if that is the only device using the configuration. Alternatively, you can remove the remote access VPN configuration.

2. Deploy Configuration Changes.

   You can also search for remote access VPN configuration by typing the name of the configuration or device.

Configure ASA Remote Access VPN Connection Profile

A Remote Access VPN connection profile defines the characteristics that allow external users to create a VPN connection to the system using the AnyConnect client. Each profile defines the AAA servers and certificates used for authenticating users, the address pools for assigning users IP addresses, and the group policies that define various user-oriented attributes.

You can create multiple profiles within the remote access VPN configuration if you need to provide variable services to different user groups, or if you have various authentication sources. For example, if your organization merges with a different organization that uses different authentication servers, you can create a profile for the new group that uses those authentication servers.

A remote access VPN connection profile allows your users to connect to your inside networks when they are on external networks, such as their home network. Create separate profiles to accommodate different authentication methods.

Before you begin

Create ASA Remote Access VPN Configuration on page 775.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM**. You can click a VPN configuration to view the summary information on how many connection profiles and group policies are currently configured.

> **Note**
>
> To know the group policies assigned to the device, in **Actions**, click **Group Policies**. Group Policies assigned to connection profiles are automatically added to the list and cannot be removed.

If the group policy you need does not yet exist, click + and select from the list. You can create additional group policies to provide the services you require. See Create ASA RA VPN group policies.

3. Click the connection profile and under **Actions** in the sidebar at the right, click **Add Connection Profile**.
4. Configure the basic connection attributes.
   - **Connection Profile Name**: The name for this connection, up to 50 characters without spaces. For example, MainOffice.

     > **Note**
     >
     > The name you enter here is what users will see in the connection list in the AnyConnect client. Choose a name that will make sense to your users.

   - **Group Alias, Group URL**: Aliases contain alternate names or URLs for a specific connection profile. VPN users can choose an alias name in the AnyConnect client in the list of connections when they connect to the ASA device. The connection profile name is automatically added as a group alias. You can also configure the list of group URLs, which your endpoints can select while initiating the Remote Access VPN connection. If users connect using the group URL, the system will automatically use the connection profile that matches the URL. This URL would be used by clients who do not yet have the AnyConnect client installed. Add as many group aliases and URLs as required. These aliases and URLs must be unique across all connection profiles defined on the device. Group URLs must start with **https://**.
   - For example, you might have the alias Contractor and the group URLhttps://ravpn.example.com/contractor. Once the AnyConnect client is installed, the user would simply select the group alias in the AnyConnect VPN drop-down list of connections.

5. Configure the primary and optionally, secondary identity sources. These options determine how remote users authenticate to the device to enable the remote access VPN connection. The simplest approach is to use AAA only and then select an AD realm or use the LocalIdentitySource. You can use the following approaches for **Authentication Type**:
   - **AAA Only**: Authenticate and authorize users based on username and password. For details, see Configure AAA for a Connection Profile on page 781.
   - **Client Certificate Only**: Authenticate users based on client device identity certificate.
   - **AAA and ClientCertificate**: Use both username/password and client device identity certificate.

6. Configure the address pool for clients. The address pool defines the IP addresses that the system can assign to remote clients when they establish a VPN connection. For more information, see Configure Client Address Pool Assignment.
7. Click **Continue**.
8. Select the **Group Policy** to use for this profile from the list and click **Select**.

The group policy sets terms for user connections after the tunnel is established. The system includes a default group policy named 'DfltGrpPolicy'. You can create additional group policies to provide the services you require. See Create ASA RA VPN group policies.

9. Click **Continue**.
10. Review the summary. First, verify that the summary is correct. You can see what end-users need to do to initially install the AnyConnect software and test that they can complete a VPN connection. Click  to copy the instructions to the clipboard, and then distribute them to your users.
11. Click **Done**.
12. Perform step 5 of End-to-End Remote Access VPN Configuration Process for ASA.

Configure AAA for a Connection Profile

Authentication, Authorization, and Accounting (AAA) servers use username and password to determine if a user is allowed access to the remote access VPN. If you use RADIUS servers, you can distinguish authorization levels among authenticated users, to provide differential access to protected resources. You can also use RADIUS accounting services to keep track of usage.

When configuring AAA, you must configure a primary identity source. Secondary and fallback sources are optional. Use a secondary source if you want to implement dual authentication, for example, using RSA tokens or DUO.

Primary Identity Source Options

- **Primary Identity Source for User Authentication**: Authentication provides a way to identify a user, typically by having the user enter a valid username and valid password before access is granted. The primary identity source used for authenticating remote users. End-users must be defined in this source or the optional fallback source to complete a VPN connection. Select one of the following:
  - An Active Directory (AD) identity realm.
  - A RADIUS server group.
  - LocalIdentitySource (the local user database): You can define users directly on the device and not use an external server.

    You can click Identity Source to create new identity sources.

- **Fallback Local Identity Source**: If the primary source is an external server, you can select the LocalIdentitySource as a fallback in case the primary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the external server.
- **Strip options**: A realm is an administrative domain. Enabling the following options allows the authentication to be based on the username alone. You can enable any combination of these options. However, you must select both check boxes if your server cannot parse delimiters.
  - **Strip Identity Source Server from Username**: Whether to remove the identity source name from the username before passing the username on to the AAA server. For example, if you select this option and the user enters domain\username as the username, the domain is stripped off from the username and sent to the AAA server for authentication. By default, this option is unchecked.
  - **Strip Group from Username**: Whether to remove the group name from the username before passing the username on to the AAA server. This option applies to names given in the username@domain format; the option strips the domain and @ sign. By default, this option is unchecked.

Secondary Identity Source

- **Secondary Identity Source for User Authorization**: The optional second identity source. If the user successfully authenticates with the primary source, the user is prompted to authenticate with the secondary source. You can select an AD realm, RADIUS server group, or the local identity source.
- **Advanced options**: Click the **Advanced** link and configure the following options:
  - **Fallback Local Identity Source for Secondary**: If the secondary source is an external server, you can select the LocalIdentitySource as a fallback in case the secondary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the secondary external server.
  - **Use Primary Username for Secondary Login**: By default, when using a secondary identity source, the system will prompt for both username and password for the secondary source. If you select this option, the system prompts for the secondary password only and uses the same username for the secondary source that was authenticated against the primary identity source. Select this option if you configure the same usernames in both the primary and secondary identity sources.
    - **Username for Session Server**: After successful authentication, the username is shown in events and statistical dashboards, is used for determining matches for a user- or group-based SSL decryption and access control rules and is used for accounting. Because you are using two authentication sources, you need to tell the system whether to use the Primary or Secondary username as the user identity. By default, the primary name is used.
    - **Password Type**: How to obtain the password for the secondary server. The default is **Prompt**, which means the user is asked to enter the password. Select **Primary Identity Source Password** to automatically use the password entered when the user authenticated to the primary server. Select **Common Password** to use the same password for every user, then enter that password in the **Common Password** field.
  - **Authorization Server**: The RADIUS server group that has been configured to authorize remote access, VPN users. After authentication is complete, authorization controls the services and commands available to each authenticated user. Authorization works by assembling a set of attributes that describe what the user is authorized to perform, their actual capabilities, and restrictions. Were you not to use authorization, authentication alone would provide the same access to all authenticated users.

    Note that if the system obtains authorization attributes from the RADIUS server that overlap those defined in the group policy, the RADIUS attributes override the group policy attributes.

    You can click Create RADIUS Server Group to create new server groups.
  - **Accounting Server**: (Optional.) The RADIUS server group to use to account for the remote access VPN session. Accounting tracks the services users are accessing as well as the number of network resources they are consuming. The ASA device reports user activity to the RADIUS server. Accounting information includes when sessions start and stop, usernames, the number of bytes that pass through the device for each session, the service used, and the duration of each session. You can then analyze the data for network management, client billing, or auditing. You can use accounting alone or together with authentication and authorization.

    You can click Create RADIUS Server Group to create new server groups.

Configure Certificate Authentication for a Connection Profile

> **Note**
>
> This section is not applicable for **Authentication Type** as **AAA Only**.

You can use certificates installed on the client device to authenticate remote access VPN connections.

When using client certificates, you can still configure a secondary identity source, fallback source, and authorization and accounting servers. These are AAA options; for details, see Configure ASA Remote Access VPN Connection Profile on page 779.

The following are the certificate-specific attributes. You can configure these attributes separately for primary and secondary identity sources. Configuring a secondary source is optional.

- **Username from Certificate**: Select one of the following:
  - **Map Specific Field**: Use the certificate elements in the order of **Primary Field** and **Secondary Field**. The defaults are CN (Common Name) and OU (Organizational Unit). Select the options that work for your organization. The fields are combined to provide the username, and this is the name used in events, dashboards, and for matching purposes in SSL decryption and access control rules.
  - **Use entire DN (distinguished name) as username**: The system automatically derives the username from the DN fields.
- **Advanced options** (not applicable for **Authentication Type** as **Client Certificate Only**): Click the **Advanced** link and configure the following options:
  - **Prefill username from certificate on user login window**: Whether to fill in the username field with the retrieved username when prompting the user to authenticate.
  - **Hide username in login window**: If you select the **Prefill** option, you can hide the username, which means the user cannot edit the username in the password prompt.

Configure Client Address Pool Assignment

There must be a way for the system to provide an IP address to endpoints that connect to the remote access VPN. The AAA server can provide these addresses, a DHCP server, an IP address pool configured in the group policy, or an IP address pool configured in the connection profile. The system tries these resources in that order and stops when it obtains an available address, which it then assigns to the client. Thus, you can configure multiple options to create a failsafe in case of an unusual number of concurrent connections.

Use one or more of the following methods to configure the address pool for a connection profile.

- **IPv4 Address Pool** and **IPv4 Address Pool**: First, create up to six network objects that specify subnets. You can configure separate pools for IPv4 and IPv6. Then, select these objects in the **IPv4 Address Pool** and **IPv6 Address Pool** options, either in the group policy or in the connection profile. You do not need to configure both IPv4 and IPv6, configure the addressing scheme you want to support. You also do not need to configure the pool in both the group policy and the connection profile. The group policy overrides the connection profile settings, so if you configure the pools in the group policy, leave the options empty in the connection profile. Note that the pools are used in the order in which you list them.

  To create new IPv4 or IPV6 address pools, see Create IP Address Pool.
- **DHCP Servers**: First, configure a DHCP server with one or more IPv4 address ranges for the remote access VPN (you cannot configure IPv6 pools using DHCP). Then, create a host network object with the IP address of the DHCP server. You can then select this object in the **DHCP Servers** attribute of the connection profile.

You can configure more than one DHCP server. If the DHCP server has multiple address pools, you can use the **DHCP Scope** attribute in the group policy that you attach to the connection profile to select which pool to use. Create a host network object with the network address of the pool. For example, if the DHCP pool contains 192.168.15.0/24 and 192.168.16.0/24, setting the DHCP scope to 192.168.16.0 will ensure that an address from the 192.168.16.0/24 subnet will be selected.

Manage AnyConnect Software Packages on ASA Devices

You can perform one of the following steps to upload an AnyConnect package using the remote access VPN wizard:

- Upload the package from the Security Cloud Control repository.
- Upload the package from the server using HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

Upload an AnyConnect Package from Security Cloud Control Repository

The remote access VPN Configuration wizard presents AnyConnect packages per operating system from the Security Cloud Control repository, which you can select and upload to device. Make sure that the device has access to the internet and proper DNS configuration.

> **Note**
>
> If the desired package is unavailable in the presented list or the device has no access to the internet, you can upload the package using the server where the AnyConnect packages are preloaded.

Procedure

1. Click on the field that corresponds to an operating system and select an AnyConnect package.
2. Click  to upload the package. If the checksum doesn't match, the AnyConnect package upload fails. You can see the device's workflow tab for more details about the failure.

Upload an AnyConnect Package to ASA from Server

Download the AnyConnect client software packages to your computer and upload them to a remote server accessible from ASAs. Later, use the RA VPN wizard or ASA File Management wizard to upload the AnyConnect software packages from that server to ASAs. DNS must be configured correctly on the device for URLs that use a domain name.

The ASA RA VPN wizard supports uploading packages using HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

The syntax of supported protocols for uploading the file:

Protocol	Syntax	Example
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	ftp://user:NKT9g78RgRmWGHe@ftp.test.com/img-0001.jpg
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/filename]	scp://root:cisco123@10.10.16.6//root/events_send.py

Before you begin

Make sure that you download the "AnyConnect Headend Deployment Package" for your desired operating systems. Always download the latest AnyConnect version to ensure that you have the latest features, bug fixes, and security patches. Regularly update the packages on the device.**Important**

If you choose to upload the package using the ASA File Management wizard, do not modify the package's name after downloading them.

Note

You can upload one AnyConnect package per Operating System (OS): Windows, Mac, and Linux. You cannot upload multiple versions for a given OS type.

Procedure

1. Download the AnyConnect packages from https://software.cisco.com/download/home/283000185.
   - Make sure you accept the EULA and have K9 (encrypted image) privileges.
   - Select the "AnyConnect Headend Deployment Package" package for your operating system. The package name will be similar to "anyconnect-win-4.7.04056-webdeploy-k9.pkg." There are separate headend packages for Windows, macOS, and Linux.
2. Upload the AnyConnect packages to a remote server. Ensure that there is a network route from the ASA device and the server.

   The ASA RA VPN wizard supports uploading packages HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

   Important

   If you are uploading the AnyConnect package to an HTTPS server, ensure that the following steps are performed:

   - Upload the trusted CA certificate of that server on the ASA device.
   - Install the trusted CA certificate on the HTTPS server.
3. The remote server's URL must be a direct link without prompting for authentication. If the URL is pre-authenticated, you can download the file by specifying the RA VPN wizard's URL.
4. If the remote server IP address is NATed, you have to provide the NATed public IP address of the remote server location.

Upload new AnyConnect Packages to ASA

You can either use the remote access VPN wizard or ASA File Management wizard to upload the AnyConnect software packages to ASAs.

Use the following procedure to upload new AnyConnect packages to an ASA device from an HTTP or HTTPS server:

Procedure

1. In the **AnyConnect Package Detected**, you can upload separate packages for Windows, Mac, and Linux endpoints.
2. In the corresponding platform field, specify the server's paths where the AnyConnect packages compatible for Windows, Mac, and Linux are pre-uploaded. Examples of server paths: 'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg', 'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.
3. Click to upload the package. Security Cloud Control validates if the path is reachable and the specified filename is a valid package. When the validation is successful, the names of the AnyConnect packages appear. As you add more ASA devices to the remote access VPN configuration, you can upload the AnyConnect packages to them.
4. Click **OK**. The AnyConnect packages are added to the remote access VPN configuration.
5. Continue to Create an ASA RA VPN Configuration from step 5 onwards.

   To complete a VPN connection, your users must install the AnyConnect client software on their workstation. For more information, see How Users Can Install the AnyConnect Client Software on ASA.

Upload AnyConnect Packages using File Management Wizard

Use the File Management wizard to upload AnyConnect packages to a single or multiple ASA devices from an HTTP, HTTPS, TFTP, FTP, SMB, or SCP server. When you want to push AnyConnect packages to multiple ASA devices simultaneously, the bulk upload comes in handy.

For more information, see ASA File Management.

Important

If you choose to upload the package using the ASA File Management wizard, do not modify the package's name after downloading them.

Once the upload is complete, open the ASA RA VPN Configuration wizard and notice that the packages are auto-detected. If you upload multiple packages for an OS version, the wizard lists them in a drop-down allowing you to select one among them. Then, you can create the RA VPN configuration and deploy them to the devices.

Replace an AnyConnect Package

If the AnyConnect packages are already present on the devices, you can see them in the remote access VPN wizard. You can see all the available AnyConnect packages for an operating system in a drop-down list. You can select an existing package from the list and replace it with a new one but can't add a new package to the list.

Note

If you want to replace an existing package with a new one, ensure that the new AnyConnect package is uploaded already to a server on the network that the ASA can reach.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM**.

3. Select the remote access VPN configuration to be modified, and under **Actions**, click **Edit**.
4. In **AnyConnect Packages Detected**, click icon appearing beside the existing AnyConnect package. If there are multiple versions of AnyConnect package for an operating system, select the package you want to replace from the list and click **Edit**. The existing package disappears from the corresponding field.
5. Specify the server's path where the new AnyConnect package is preloaded and click to upload the package.
6. Click **OK**. The new AnyConnect package is added to the remote access VPN configuration.
7. Continue to Create ASA Remote Access VPN Configuration on page 775 from step 6 onwards.

Delete an AnyConnect Package

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM**.
3. Select the remote access VPN configuration to be modified, and under **Actions**, click **Edit**.
4. In **AnyConnect Packages Detected**, click icon appearing beside the AnyConnect package that you want to delete. If there are multiple versions of AnyConnect package for an operating system, select the package you want to delete from the list. The existing package disappears from the corresponding field.

   Note

   Click **Cancel** to stop the delete operation and retain the existing package,

5. Click **OK**. The device's **Configuration Status** is in 'Not Synced' state.

   Note

   If you want to undo the delete action at this stage, go to **Security Devices** page and click **Discard Changes** to retain the existing AnyConnect package.

6. Review and deploy configuration changes to the devices.

Manage and Deploy Pre-existing ASA Remote Access VPN Configuration

When you onboard an ASDM managed ASA device that already has remote access VPN settings, it discovers and displays the existing remote access VPN configurations. Security Cloud Control automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. There are some remote access VPN configurations that aren't read or supported in the Security Cloud Control but can be configured in the Security Cloud Control command-line interface.

> **Note**
>
> This section doesn't cover every supported or unsupported configuration in Security Cloud Control. Instead, it only describes the most commonly used ones.

To see the remote access VPN configurations from an onboarded ASA, perform the following steps:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM**.
3. Click the remote access VPN configuration corresponding to the onboarded ASA device. Security Cloud Control automatically creates a "**Default_RA_VPN_Configuration**" and associates the ASA device with this configuration. You can delete the default configuration. The ASA remote access VPN configurations that are read in Security Cloud Control are classified as follows:
   - Device settings
   - Connection profiles
   - Group policies

Device Settings

The RA VPN configurations associated with the onboarded ASA device appear in **Default_RA_VPN_Configuration**. You need to click on this configuration to see the name of the ASA device (in the **Devices** pane on the right) associated with that configuration. You can also see the AnyConnect packages present in the ASA devices by clicking the edit button.

Connection Profile

Security Cloud Control supports and reads the connection profiles defined in "AnyConnect Client VPN Access" of the ASA device. It does not support the "Clientless SSL VPN Access" configuration.

To see the connection profile attributes, perform the following:

Procedure

1. Expand **Default_RA_VPN_Configuration**.
2. Click one of the connection profiles that you want and click **Edit**.

All the basic and advanced ASA RA VPN attributes can be seen in the **Connection Profile name and details** of the Security Cloud Control RA VPN configuration page.

> **Note**
>
> You can delete the default configuration (Select the default RA VPN configuration and in the **Actions** pane on the right, click **Remove**).

Primary Identity Source

- Security Cloud Control reads the **Connection Aliases** and **Group URLs** attributes as **Group Alias** and **Group URL**.

  > **Note**
  >
  > - The connection profiles configured with SAML, Multiple certificates and AAA, and Multiple certificates aren't read.
  > - The authentication server group with the interface and server group is not supported.

- Security Cloud Control supports the AnyConnect connection profiles configured with "AAA", "AAA and certificate", and "Certificate only" authentication methods in **Primary Identity Source**.
- The **AAA Server Group** is read in Security Cloud Control as **Primary Identity Source for User Authentication** in**Primary Identity Source** (You can see this attribute by selecting **AAA** or **AAA and Client Certificate** as the **Authentication Type**).
  - If the **AAA Server Group** has been configured something other than LOCAL, Security Cloud Control reads and displays this attribute in the **Fallback Local Identity Source** field under **Primary Identity Source**. (You can see this attribute by selecting **AAA** as the authentication type).

    To learn more about the server group attributes read in Security Cloud Control, see AAA Server Groups.

Secondary Identity Source

The **Secondary Identity Source** displays the secondary authentication attributes of the ASA device. To see these attributes, select **AAA** or **AAA and Client Certificate** as the authentication type, and click **View Secondary Identity Source**.

- The **Secondary Identity Source for User Authentication** displays the secondary authentication **Server Group** attribute.
  - If the **Server Group** has been configured something other than LOCAL, Security Cloud Control reads and displays this attribute in the **Fallback Local Identity Source for Secondary**field under **Secondary Identity Source**.
- Security Cloud Control doesn't support the **Attribute Server** and **Interface-Specific Authorization Server Groups** attributes.

To learn more about the server group attributes read in Security Cloud Control, see AAA Server Groups.

Authorization Server

- The **Authorization Server** displays the authorization **Server Group** attribute.

- Security Cloud Control doesn't support the authorization server group with interface and server group.

To learn more about the RADIUS server group attributes read in Security Cloud Control, see RADIUS Server Groups.

Accounting Server

The **Accounting Server** displays the accounting **Server Group** attribute. To learn more about the server group attributes read in Security Cloud Control, see RADIUS Server Groups.

Client Address Pool Assignment

Security Cloud Control reads the **Client Address Assignment attributes** (**DHCP Servers**, **Client Address Pools**, and **Client IPv6 Address Pools**) as objects. (You can see these attributes in **Client Address Pool Assignment**). The DHCP server details are read as literals.

> **Note**
>
> Security Cloud Control doesn't support the IP address pools assigned on specific interfaces. However, these attributes can be seen in the ASA command-line interface (CLI).

AAA Server Groups

Security Cloud Control represents an LDAP Server Group and its associated LDAP Servers as an **Active Directory Realm** object. For Active Directory (AD), a realm is equivalent to an Active Directory domain. Note that Security Cloud Control does read the AD password for AD realm objects that are already present.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation bar on the left, choose **Objects**.
3. Apply the **Active Directory Realms** filter to see this object.
4. Select the **Active Directory Realm** object that you want and click **Edit** to see its details.

   You can see that the AD realm contains the associated AD server and its configuration. If there are multiple Active Directory (AD) servers for the AD realm, the AD servers need to be duplicates of each other and support the same AD domain. Therefore, the basic realm properties such as **Directory name**, **Directory Password**, and **Base Distinguished Name** must be the same across all AD servers associated with that AD realm. Security Cloud Control displays a warning message in the Active Directory Realm object if these properties aren't the same. You have to correct these properties to make them consistent across the AD servers. If you continue without addressing this warning, Security Cloud Control uses one of the AD server properties and applies it to other servers in that realm object.

RADIUS Server Group

The AAA RADIUS Server Group attributes of the ASA device are read in Security Cloud Control as RADIUS Server Group objects.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.

3. Apply the **RADIUS Server Group** filter to see this object.
4. Select the object that you want and then click **Edit** to see its details.
    - The **Enable dynamic authorization** in ASA is read in Security Cloud Control as **Dynamic Authorization (for RA VPN only)**.
    - The **Depletion** option in **Reactivation Mode** is read in Security Cloud Control, and therefore the **Dead Time** value associated with depletion time is read in Security Cloud Control. However, the **Timed** attribute is not read in Security Cloud Control.
    - Security Cloud Control doesn't support **Accounting Mode**, **Timed**, **Enable interim accounting update**, **Enable interim accounting update**, and **Use authorization only mode**.

RADIUS Server

When Security Cloud Control reads the Radius Servers from ASA, it creates a Radius server object specifies the name as "Name of the Radius server group_server name or IP address".

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Apply the **RADIUS Server** filter to see this object.
4. Select the object that you want and then click **Edit** to see its details.

Group Policy

In the **Group Policy** section, click the drop-down to view the group policies associated with the device.

> ⚠ **Attention**
>
> Security Cloud Control reads the group policies configured with tunneling protocol as **SSL VPN Client**.

Security Cloud Control reads most of the group policy attributes configured in ASA. The information is displayed across the tabs in the RA VPN Group policy wizard. To see the details of group policies read from the ASA device, you need to perform the following:

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Objects**.
3. Filter for **RA VPN Group Policy**.
4. Select the group policy associated with that device and click **Edit**.

Note

Security Cloud Control doesn't support the Standard Access Control Lists (ACL) defined in the split tunneling in the ASA device. It supports the Extended Access Control Lists (ACL) and reads them as ACLs in the ASA policies.

To see the policies, on the navigation bar, you can click **Policies** > **ASA Access Policies**.

To select the extended ACLs, perform the following:

- Click the **Split Tunneling** tab.
- Based on whether the traffic in ASA uses IPv4 or IPv6 addresses, select "Allow specified traffic over tunnel" or "Exclude networks specified below" from the corresponding drop-down list. Select the extended ACLs that are imported from ASA.

Remote Access VPN Certificate-Based Authentication

The remote access VPN uses digital certificates for authenticating secure gateways and AnyConnect clients (endpoints) in the following scenarios:

Important

Security Cloud Control handles the installation of digital certificates on the VPN headends (ASA FTD). It does not handle the installation of certificates on the AnyConnect client device. The administrator of your organization must handle it.

- Identify and authenticate the VPN headend device (ASA FTD):

  VPN headends require an identity certificate to identify and authenticate themselves when the AnyConnect client requests a VPN connection. Using Security Cloud Control, you must install the identity certificate on the device. See Installing an Identity Certificate Using PKCS12 or Certificate And Key. It is not mandatory to install the issuer's CA certificate on the AnyConnect client.

  While creating the Remote Access VPN configuration from Security Cloud Control, assign the enrolled identity certificate to the outside interface of the device and download the configuration to the device. The identity certificate becomes fully operational on the outside interface of the device.

  When the AnyConnect client attempts to connect to VPN, the device authenticates itself by presenting its identity certificate to the AnyConnect client. The AnyConnect client verifies this identity certificate with its trusted CA certificate and trusts the certificate and thereby the device. If the CA certificate isn’t installed on the AnyConnect client, the user must manually trust the device when prompted.

- Identify and authenticate the AnyConnect client:

> **Note**
>
> This applies when you use "Client Certificate Only" or "AAA and Client Certificate" as the authentication method in the connection profile of remote access VPN configuration. It does not apply for "AAA Only".

Once the device is trusted, the AnyConnect client needs to authenticate itself to complete the VPN connection. You must install an identity certificate on the AnyConnect client and using Security Cloud Control, install a trusted CA certificate on the device. These certificates must be issued from the same certificate authority. See Installing Trusted CA Certificate in ASA.

The AnyConnect client presents its identity certificate and the device verifies this certificate with its trusted CA certificate and establishes the VPN connection.

Exempt Remote Access VPN Traffic from NAT

Configure NAT Exempt to exempt traffic to and from the remote access VPN endpoints from NAT translation. If you do not exempt VPN traffic from NAT, ensure that the existing NAT rules for the outside and inside interfaces do not apply to the remote access VPN pool of addresses. NAT exempt rules are manual static identity NAT rules for a given source/destination interface and network combination, but they are not reflected in the NAT policy, they are hidden. If you enable NAT Exempt, you must also configure the following.

- **Inside Interfaces**: Select the interfaces for the internal networks remote users will be accessing. NAT rules are created for these interfaces.
- **Inside Networks**: Select the network objects that represent internal networks remote users will be accessing. The networks list must contain the same IP types as the address pools you are supporting.

Before you begin

Create ASA network objects that match the configuration of the local IP address pools used in the connection profile and group policy of that device. These network objects must be assigned as the destination address and translated address when configuring the NAT rule.

See Create an ASA Network Object on page 113.

Procedure

1. In the left pane, click **Security Devices**.
2. Use the filter and search field to find the ASA device for which you want to create the NAT rule.
3. In the **Management** area of the details panel, click **NAT** NAT.
4. Click + > **Twice NAT**.
   a. In section 1, select **Static.** Click **Continue**.
   b. In section 2, select **Source Interface** = 'any' and **Destination Interface** = 'any'.Click **Continue**.
   c. In section 3, select **Source Original Address** = 'any' and **Source Translated Address** = 'any'.
   d. Select **Use Destination**.
      1. **Destination Original Address** and **Source Translated Address**: Click **Choose** in the drop-down and select the network objects that match the configuration of the local IP address pools. In the below example, 'IPV4_Object' is the network object with the same configuration as the IPv4 address pool object used in the

connection profile and group policy settings of the ASA (BGL_ASA1_SH) device.



2. Select **Disable proxy ARP for incoming packets**.
3. Click **Save**.
4. Repeat the process (from step 4) to create equivalent rules for each of the other network objects equivalent to IP address pools.

5. Review and deploy configuration changes to the devices.

Install the AnyConnect Client Software on ASA

To complete a VPN connection, your users must install the AnyConnect client software. You can use your existing software distribution methods to install the software directly. Or, you can have users install the AnyConnect client directly from the ASA device.

> **Note**
>
> Users must have Administrator rights on their workstations to install the software.

If you decide to have users initially install the software from the ASA device, inform users to perform the following steps:

> **Note**
>
> Android and iOS users should download AnyConnect from the appropriate App Store.

Procedure

1. Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. You identify this interface when you configure the remote access VPN. The system prompts the user to log in.
2. Log into the site. Users are authenticated using the directory server configured for the remote access VPN. Log in must be successful to continue. If the login is successful, the system determines if the user already has the required

version of the AnyConnect client. If the AnyConnect client is absent from the user's computer or is down-level, the system automatically starts installing the AnyConnect software. When the installation is finished, AnyConnect completes the remote access VPN connection.

Modify ASA Remote Access VPN Configuration

When ASA devices are onboarded to Security Cloud Control, it discovers and displays the pre-existing remote access VPN configurations from onboarded ASA devices. For more information, see Manage and Deploy Pre-existing ASA Remote Access VPN Configuration.

You can modify these configurations and download the new configuration to the device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM**.
3. If you want to add or remove group policies to the VPN configuration, click the VPN configuration associated with the onboarded ASA device. In the Actions pane on the left, click **Group Policies**.
   a) Click the blue + icon and configure the selections and click **Select**.
   b) Click Save. You can also Create new RAVPN group policy.
4. Click the VPN configuration, and in the **Actions** pane, click **Edit**.

   The wizard lists the ASA device associated with the configuration.

   a) You can modify the following details in the same fashion as it was created:
      - Change the name of the remote access VPN configuration.
      - Click the three dots appearing in the row that shows the device details and click **Edit**.

   For more information, see Create ASA Remote Access VPN Configuration on page 775
5. Click **OK**.
6. Preview and deploy configuration changes for all devices on page 817

Modify ASA Connection Profile

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM**.
3. Expand the VPN configuration associated with the onboarded ASA device, and select a connection profile.
4. Under **Actions**, click **Edit**.
5. Edit the values in the same fashion as it was created and click **Done**.

   For more information, see Configure ASA Remote Access VPN Connection Profile on page 779
6. Preview and deploy configuration changes for all devices on page 817

Upload RA VPN AnyConnect Client Profile

The Remote Access VPN AnyConnect Client Profile is a group of configuration parameters stored in a file. There are different AnyConnect client profiles containing configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, AMP Enabler, ISE posture, Network Visibility, Customer Feedback Experience profiles, Umbrella roaming security, and Web Security.

Security Cloud Control allows uploading of these profiles as objects which can be used in the group policy later.

- **AnyConnect VPN Profile** – AnyConnect client profiles are downloaded to clients along with the VPN AnyConnect client software. These profiles define many client-related options, such as auto-connect on startup and auto-reconnect, and whether the end-user can change the option from the AnyConnect client preferences and advanced settings. Security Cloud Control supports the XML file format.
- **AMP Enabler Service Profile** – The profile is used for the AnyConnect AMP Enabler. The AMP Enabler and this profile are pushed to the endpoints from FDM-managed device when a remote access VPN user connects to the VPN. Security Cloud Control supports XML and ASP file formats.
- **Feedback Profile** – You can add a Customer Experience Feedback profile and select this type to receive information about the features and modules customers have enabled and used. Security Cloud Control supports the FSP file format.
- **ISE Posture Profile** – Choose this option if you add a profile file for the AnyConnect ISE Posture module. Security Cloud Control supports XML and ISP file formats.
- **Network Access Manager Service Profile** – Configure and add the NAM profile file using the Network Access Manager profile editor. Security Cloud Control supports XML and NSP file formats.
- **Network Visibility Service Profile** – Profile file for AnyConnect Network Visibility module. You can create the profile using the NVM profile editor. Security Cloud Control supports XML and NVMSP file formats.
- **Umbrella Roaming Security Profile** – You must select this file type if you deploy the Umbrella Roaming Security module. Security Cloud Control supports XML and JSON file formats.
- **Web Security Service Profile** – Select this file type when you add a profile file for the Web security module. Security Cloud Control supports XML, WSO, and WSP file formats.

Before you begin

Use the suitable GUI-based AnyConnect profile editors to create the profiles you need. You can download the profile editors from Cisco Software Download Center in the AnyConnect Secure Mobility Client category and install the AnyConnect "Profile Editor - Windows / Standalone installer (MSI)." The profile editor installer contains stand-alone versions of the profile editors. The installation file is for Windows only and has the file name anyconnect-profileeditor-win-<version>-k9.msi, where <version> is the AnyConnect version. For example, anyconnect-profileeditor-win-4.3.04027-k9.msi. You must also install Java JRE 1.6 (or higher) before installing the profile editor.

Except for the Umbrella Roaming Security profile editor, this package contains all the profile editors required for creating the modules. For detailed information, see the *AnyConnect Profile Editor* chapter in the appropriate release of the Cisco AnyConnect Secure Mobility Client Administrator Guide for details. Download the Umbrella Roaming Security profile separately from the Umbrella dashboard. For detailed information, see the "Download the AnyConnect Roaming Security Profile from the Umbrella Dashboard" section of the "Umbrella Roaming Security" chapter in the Cisco Umbrella User Guide.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Objects**.

3. Click the blue plus  button.
4. Click **RA VPN Objects (ASA & FDM)** > **AnyConnect Client Profile**.
5. In the **Object Name** field, enter a name for the AnyConnect client profile.
6. Click **Browse** and select the file you created using the Profile Editor.
7. Click **Open** to upload the profile.
8. Click **Add** to add the object.
   - Associate the client modules with the AnyConnect VPN profile in the RA VPN group policies window. See Create New FTD RA VPN Group Policies.

> **Note**
>
> The client module association is supported by all ASA versions and FDM running software version 6.7 or later.

Verify ASA Remote Access VPN Configuration

After you configure the remote access VPN and deploy the configuration to the device, verify that you can make remote connections.

Procedure

1. From an external network, establish a VPN connection using the AnyConnect client. Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. If necessary, install the client software and complete the connection. See How Users Can Install the AnyConnect Client Software. If you configured group URLs, also try those URLs.
2. In the **Security Devices** page, select the device (FTD or ASA) you want to verify and click **Command Line Interface** under **Device Actions**.
3. Use the **show vpn-sessiondb** command to view summary information about current VPN sessions.

4. The statistics should show your active AnyConnect Client session, and information on cumulative sessions, the peak concurrent number of sessions, and inactive sessions. Following is sample output from the command.

```
> show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client          :      1 :         49 :           3 :        0
  SSL/TLS/DTLS             :      1 :         49 :           3 :        0
Clientless VPN             :      0 :          1 :           1
  Browser                  :      0 :          1 :           1
----------------------------------------------------------------------------


  Total Active and Inactive    :      1             Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  ----------------------------------------------------------------------------

  ----------------------------------------------------------------------------
  Tunnels Summary
  ----------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
  Clientless                 :      0 :          1 :               1
  AnyConnect-Parent          :      1 :         49 :               3
  SSL-Tunnel                 :      1 :         46 :               3
  DTLS-Tunnel                :      1 :         46 :               3
  ----------------------------------------------------------------------------
  Totals                     :      3 :        142
  ----------------------------------------------------------------------------

  ----------------------------------------------------------------------------
  IPv6 Usage Summary
  ----------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
  AnyConnect SSL/TLS/DTLS    :        :            :
    Tunneled IPv6            :      1 :         20 :           2
  ----------------------------------------------------------------------------
```

5. Use the **show vpn-sessiondb anyconnect** command to view detailed information about current AnyConnect VPN sessions. Detailed information includes encryption used, bytes transmitted and received, and other statistics. If you use your VPN connection, you should see the bytes transmitted/received numbers change as you re-issue this command.
6. Use the **show vpn-sessiondb anyconnect** command to view detailed information about current AnyConnect VPN sessions. Detailed information includes encryption used, bytes transmitted and received, and other statistics. If you use your VPN connection, you should see the bytes transmitted/received numbers change as you re-issue this command.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

View ASA Remote Access VPN Configuration Details

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM**
3. Click on a VPN configuration object present. The group shows summary information on how many connection profiles and group policies are currently configured.
   - Expand the remote access VPN configuration to view all connection profiles associated with them.
     - Click the add + button to add a new connection profile.
     - Click the view button () to open a summary of the connection profile and connection instructions. Under **Actions**, you can click **Edit** to modify the changes.
   - You can click one of the following options under **Actions** to perform additional tasks:
     - Click **Group Policies** to assign/add group policies.
     - Click a configuration object or connection profile that you no longer need and click **Remove** to delete.

45 Configure Firewall for Universal Zero Trust Network Access

Topics:

- Universal Zero Trust Network Access
- Onboard Applications in Security Cloud Control
- Enable Cloud-Delivered Firewall Management Center Center in Security Cloud Control
- Configure Security Devices

Configure universal zero trust network access (universal ZTNA) on a Firewall Threat Defense device and associate private resources. universal ZTNA enables traffic inspection and secure access to the resources.

Universal Zero Trust Network Access

An overview of Universal Zero Trust Network Access in Security Cloud Control, including identity-based access to private resources, Secure Access integration, Secure Client enforcement, and Threat Defense policy protection.

Universal Zero Trust Network Access (universal ZTNA) enables administrators to specifically allow access to internal network resources according to user identity including user trust and posture, without granting access to the entire network as with Remote Access VPN. Universal ZTNA is a client-based ZTNA solution that enables users to securely access internal resources and applications regardless of their location, whether remote or on-premises.

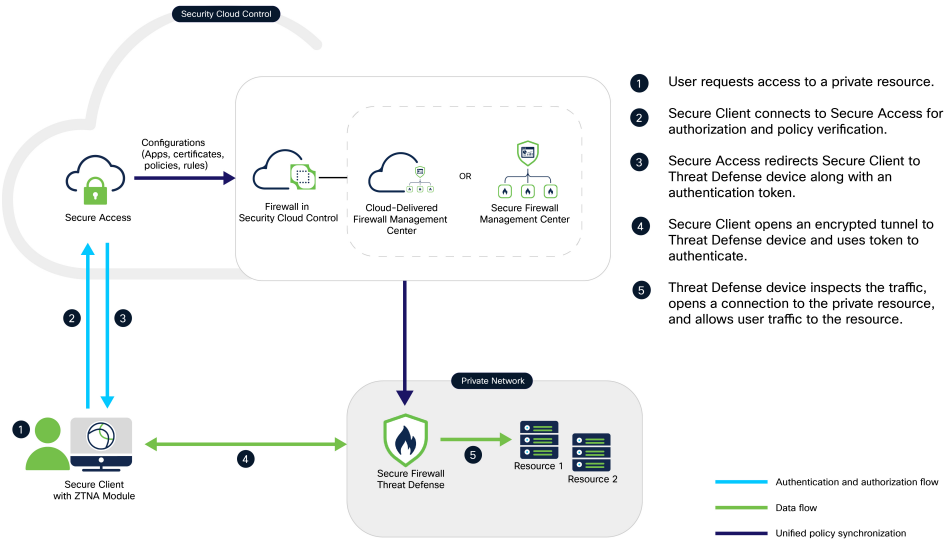
Because universal ZTNA does not assume that access granted to one application implicitly authorizes access to other applications, the network attack surface is reduced.

Universal ZTNA ensures least-privileged, per-application, per-user access with strong authentication, posture validation, and comprehensive traffic inspection. It secures applications effectively across hybrid environments.

Components of Universal ZTNA

A new configuration of universal ZTNA consists of Security Cloud Control Firewall Management (formerly called Cisco Defense Orchestrator), and Secure Access, both provisioned on the Security Cloud Control platform. Security Cloud Control Firewall Management manages the Firewall Threat Defense devices through the Secure Firewall Management Center.

Figure 21: Components of Universal ZTNA



- **Security Cloud Control Firewall Management**: Manages the configuration and deployment of universal ZTNA policies to the Firewall Threat Defense devices. The Threat Defense devices protect on-premises resources by enforcing universal ZTNA policies. Threat Defense inspects traffic and enforces intrusion prevention system (IPS), file, and malware policies on the traffic.
- **Secure Access**: Secure Access defines the access policies, posture, and security profiles for the user. It enforces the policies for user traffic through the cloud.
- **Security Cloud Control platform**: Security Cloud Control provides a unified secure management plane for both Secure Access and Firewall, simplifying the administration of universal ZTNA policies across them.
- **Secure Client**: The Secure Client is installed on the end user's device. It acts as the enforcement point that intercepts connection requests to protected internal resources, enabling secure, identity-based access.

The following sections describe how to enable universal ZTNA on a Threat Defense device. For the complete configuration of universal ZTNA, refer to the *Universal Zero Trust Network Access Configuration Guide*.

Onboard Applications in Security Cloud Control

The first step to configuring a universal ZTNA is to onboard both Secure Firewall and Secure Access on the Security Cloud Control platform.

The core elements of universal ZTNA are the Security Cloud Control Firewall Management and Secure Access applications. The first step to configuring universal ZTNA is to onboard both these applications to the Security Cloud Control platform.

1. If you have purchased a subscription for the products, claim the subscription in Security Cloud Control and activate both the products. For information on claiming a subscription and activating products in Security Cloud Control, see the Security Cloud Control Administration Guide.
2. Configure user management in Secure Access—configure users and groups, either manually or integrate an identity provider.
3. Configure one or more trusted networks through Secure Access. We recommend having one default trusted network. A default trusted network is automatically assigned to a universal ZTNA-enabled Firewall Threat Defense device.
4. Update Secure Access with the CA certificate for the universal ZTNA user.

Enable Cloud-Delivered Firewall Management Center Center in Security Cloud Control

Learn how to enable Cloud-Delivered Firewall Management Center in Security Cloud Control for universal ZTNA, including provisioning the instance and tracking its status until it becomes active.

To configure universal ZTNA, first enable the Cloud-Delivered Firewall Management Centerin Cisco Security Cloud Control. After you enable it, configure the associated Secure Firewall Threat Defense devices. The devices can then use the networks, private resources, and policies needed to configure and manage universal ZTNA.

Procedure

1. From the Security Cloud Control menu, click **Administration** > **Integrations** > **Firewall Management Center**.
2. Click **Enable Cloud-Delivered FMC**.

   Security Cloud Control starts provisioning the instance. This process takes a few minutes to complete. You can track the progress in the **Status** column of **Cloud-Delivered FMC**.

   After the provisioning is complete, the status changes to **Active**.

   Onboard the Firewall Threat Defense devices to the . To learn how to onboard a Threat Defense device, see *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center*

Configure Security Devices

Configure Cisco Firewall Threat Defense devices for Universal Zero Trust Network Access to secure the private resources and enforce identity-based access rules.

All Firewall Threat Defense devices associated with the Cloud-Delivered Firewall Management Center that you onboarded to Security Cloud Control are *security devices* to which you can:

- Associate private resources, which are internal applications you want to protect with identity-based access control, IPS, malware, and other protections.

- Deploy Secure Access access rules. Security devices are responsible for enforcing access rules for on-premises users, remote users, or both.

Perform these steps to enable **universal zero trust network access settings** on the Threat Defense devices. These steps include configuring the device FQDN, inside interface, outside interface, and PKCS12 certificate to enable universal ZTNA on the devices.

Before you begin

You must know the name of each device's internal and external network interfaces:

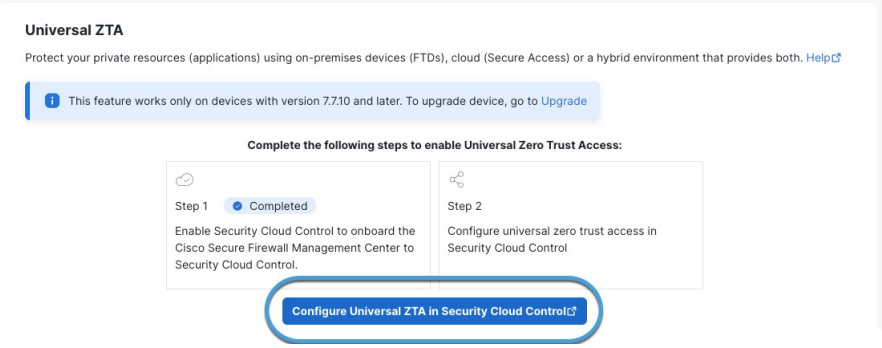
- The internal interface (also referred to as the *DMZ* interface) is used to apply access rules to on-premises users.
- The external interface is used to apply access rules to remote users.

You can choose internal, external, or both types of interfaces for each security device.

Procedure

1. In the Cloud-Delivered Firewall Management Center, click **Policies** > **Security policies** > **Zero Trust Application**.
2. Click **Configure Universal ZTA in Security Cloud Control**.

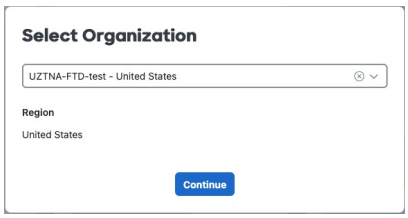
   This figure shows an example.



3. When prompted, log in to Security Cloud Control.
4. When prompted, select your organization from the drop-down list and click **Continue**.

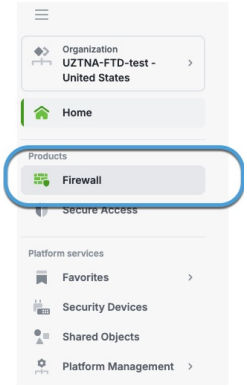
   Select an organization that has both Secure Access and Secure Firewall micro applications configured.

   This figure shows an example.



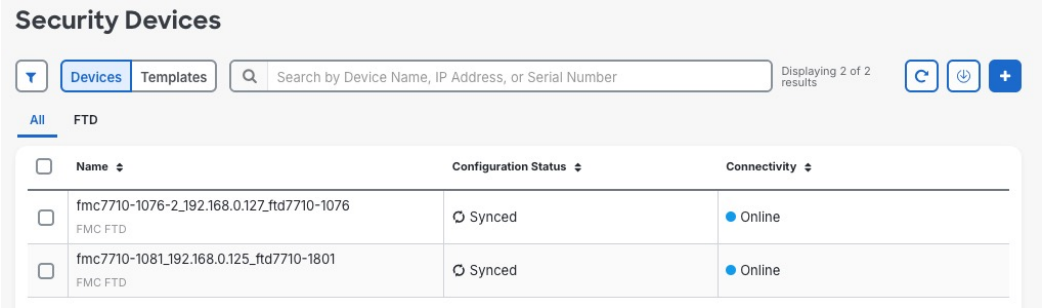
5. In Security Cloud Control, in the Products section, click **Firewall**.

   This figure shows an example.



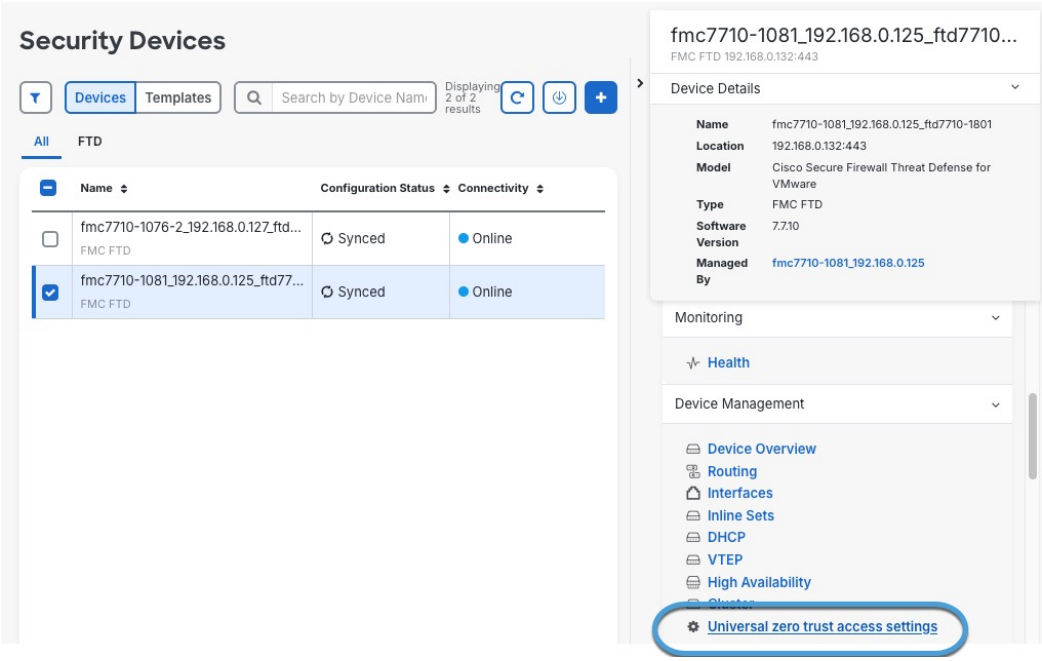
6. In the Manage section, click **Security Devices**.

   The **Security Devices** page displays the available security devices.

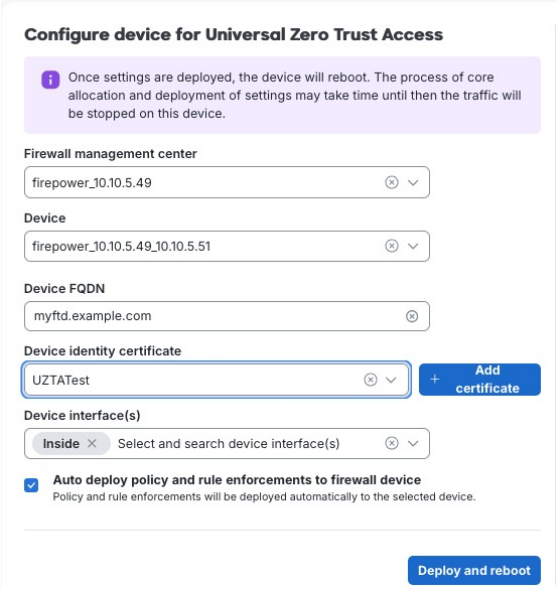


7. Select the check box next to a device to add to the universal zero trust network access configuration.
8. In the right pane, click **Device Management** > **Universal zero trust access settings**.

   This figure shows an example.



9. Enter or edit the following information on the **Configure device for Universal Zero Trust Access** page.



This table describes the configurations to enable universal ZTNA on the device.

Item	Description
Firewall management center	From the drop-down list, click the name of a Cloud-Delivered Firewall Management Center to use for policy deployment, monitoring, and other tasks.
Device	From the drop-down list, click the name of a device to use for rule deployment and enforcement.
Device FQDN	Enter the security device's fully qualified domain name (FQDN). The FQDN is also referred to as the TLS/SSL certificate's Common Name. Secure Access redirects the clients to the resource that is represented by this FQDN. Ensure that the device FQDN *exactly matches* the Common Name (CN) of the device identity certificate and must also match a Subject Alternative Name (SAN) in the certificate.

Item	Description
Device identity certificate	The **Device identity certificate** must have a Common Name that: • *Exactly matches* the value you enter in the **Device FQDN** field. • Matches a Subject Alternative Name (SAN) in the certificate. From the drop-down list, click the name of an existing identity certificate from the list. Click **Add certificate** and add an identity certificate in **.p12** format (also referred to as PKCS#12; see this article on ssl.com). **Note** Universal ZTNA supports only the PKCS#12 format of certificate enrollment. In the provided fields, enter a **Name** to identify the certificate. Then copy/paste, drag/drop, or upload the certificate and private key. If the certificate is encrypted, enter its password in the provided field. You can optionally use a wildcard certificate as discussed in What is a Wildcard Certificate? on ssl.com.
Device Interface(s)	From the drop-down list, select the check box next to any of the following types of interfaces. • Internal network interface (or DMZ): deploys access rules for on-premises users only. • External network interface: deploys access rules for remote users only. • Both types of interfaces: deploys access rules for either on-premises or remote users.

Item	Description
Auto deploy policy and rule enforcements to firewall device	Select the check box to automatically deploy access rules to the device after they are updated on Secure Access. On the device, the Auto deploy feature selectively deploys only the Universal ZTNA access policy. It does not impact other changes or configurations on the Firewall Management Center. **Note** If there are other interdependent policies on the device (which are interlinked with the Universal ZTNA access policy), the Firewall configuration status displays an error message. The deployment then stops. In such cases, you should manually deploy the Universal ZTNA access policy from the Firewall Management Center.

10. Click **Deploy and Reboot**.

    The device reboots to reallocate the system resources for universal ZTNA components.

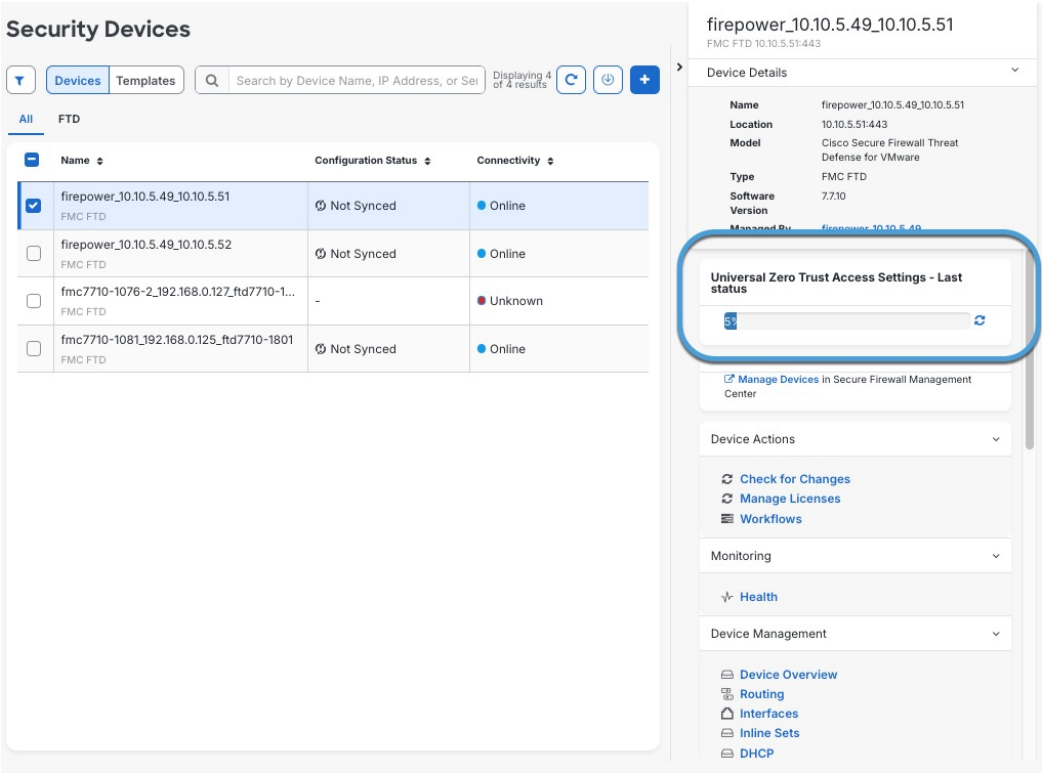
    Note

    The device takes several minutes to reboot, during which time all traffic handled by the device is disrupted.

    If you deploy a High Availability (HA) pair of devices, both devices reboot simultaneously.

11. On the **Security Devices** page, select the check box next to the device to which you just deployed the Universal ZTNA configuration.

    The right pane displays the deployment status, as shown in the figure.



For additional information, click **Device Actions** > **Workflows** in the right pane.

After the deployment completes, you can view the completion status in the **Universal Zero trust Access Settings - Last status** tab for the device.

Universal ZTNA-enabled Firewall Threat Defense device is connected to Secure Access.

What to do next:

Check the availability of the Threat Defense device under Secure Access by clicking **Security Cloud Control** > **Secure Access** > **Connect** > **Network Connections** > **FTD**.

Part XIV

Device Operations

Topics:

- Manage device configuration
- Manage onboarded device settings
- Use the Security Cloud Control Command Line Interface Tool (CLI)
- Manage CLI Templates
- Migrate Firewalls with the Migration Tool in Security Cloud Control

46 Manage device configuration

Topics:

- Read, discard, and deploy configuration changes
- Synchronizing configurations between Security Cloud Control and device

Learn how Security Cloud Control reads, compares, discards, accepts, and deploys device configuration changes to keep managed device configurations synchronized and resolve pending or conflicting changes.

To manage a device, Security Cloud Control stores a copy of the device configuration in its local database. When Security Cloud Control reads a configuration from a managed device, it copies and saves the configuration.

Security Cloud Control also reads and saves a copy of a device configuration when the device is onboarded. Each of these actions serves a specific purpose.

- **Discard Changes**: This action is available when a device configuration status is "Not Synced." In the **Not Synced** state, there are changes to the device configuration pending on Security Cloud Control. This option allows you to undo all pending changes. The pending changes are deleted and Security Cloud Control overwrites its copy of the configuration with the copy of the configuration stored on the device.
- **Check for Changes**: This action is available if the device configuration status is "Synced." Click **Check for Changes** to instruct Security Cloud Control to compare its copy of the device configuration with the copy stored on the device. If a difference is detected, Security Cloud Control immediately overwrites its copy of the device configuration with the copy stored on the device.
- **Review Conflict** and **Accept Without Review**: If you have enabled Conflict Detection on a device, Security Cloud Control checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, Security Cloud Control notifies you by displaying the "Conflict Detected" configuration status.
  - **Review Conflict**: Click **Review Conflict** to review changes made directly on a device and accept or reject them.
  - **Accept Without Review**: This action overwrites the copy of the device configuration on Security Cloud Control with the latest copy of the configuration stored on the device. Security Cloud Control does not prompt you to confirm the differences in the two copies of the configuration before taking the overwriting action.

Read All: This is a bulk operation. You can select any number of devices in any state and click **Read All** to overwrite all the device configurations stored on Security Cloud Control with the configurations stored on the devices.

- **Deploy Changes**: When you make changes to a device configuration, Security Cloud Control saves your changes to its copy of the configuration. These changes remain **Pending** in Security Cloud Control until you deploy them to the device. If there are pending changes that have not been deployed, the device is in the **Not Synced** configuration state.

  Pending configuration changes do not affect network traffic. They take effect only after Security Cloud Control deploys them to the device.

  When Security Cloud Control deploys changes to a device configuration, only the elements that were changed are overwritten. The entire device

configuration file is not overwritten. You can deploy changes to one device or multiple devices simultaneously.

- **Discard All**: This option appears after you click **Preview and Deploy...**. When you click **Preview and Deploy...**, Security Cloud Control displays a preview of the pending changes in Security Cloud Control. You can delete all pending changes from Security Cloud Control without deploying them to the selected devices by clicking **Discard All**. Unlike "Discard Changes," deleting the pending changes completes the operation.

> **Note**
>
> You can schedule deployments or recurring deployments. For more information about scheduling an automatic deployment, refer to Schedule an automatic deployment on page 827.

Read, discard, and deploy configuration changes

Describes how to read, discard, and deploy configuration changes to effectively manage and apply network configuration modifications.

Read all device configurations

Configure multiple devices to overwrite Security Cloud Control's copy of device configurations with the local device configurations using the Read All link.

This task allows you to synchronize device configurations when changes have been made to devices outside of Security Cloud Control, ensuring that Security Cloud Control's copy matches the device's local configuration.

If a configuration change is made to a device outside of Security Cloud Control, the device configuration stored on Security Cloud Control and the device's local copy of its configuration are no longer the same. You many want to overwrite Security Cloud Control's copy of the device's configuration with the configuration stored on the device to make the configurations the same again. You can perform this task on many devices simultaneously using the **Read All** link.

For more information about how Security Cloud Control manages the two copies of the device configuration, refer to Reading, Discarding, Checking for, and Deploying Configuration Changes.

Here are three configuration statuses where clicking **Read All** will overwrite Security Cloud Control's copy of the device's configuration with the device's copy of the configuration.

- **Conflict Detected**: If conflict detection is enabled, Security Cloud Control polls the devices it manages every 10 minutes for changes made to their configurations. If Security Cloud Control finds that the configuration on the device has changed, Security Cloud Control displays a "Conflict detected" configuration status for the device.
- **Synced**: If the device is in a synced state, and you click **Read All**, Security Cloud Control immediately checks the devices to determine if there have been any changes made to its configurations directly. After clicking **Read All**, Security Cloud Control confirms your intent to overwrite its copy of the device's configuration and then Security Cloud Control performs the overwrite.
- **Not Synced**: If the device is in the **Not Synced** state, and you click **Read All**, Security Cloud Control warns you that there are pending changes made to the device's configuration using Security Cloud Control and that proceeding with the **Read All** operation will delete those changes and then overwrite Security Cloud Control's copy of the configuration with the configuration on the device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab.
4. Click the appropriate device type tab.
5. (Optional) Create a change request label to identify the results of this bulk action easily in the change log.
6. Select the devices whose configurations you want to save in Security Cloud Control.

   Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.

   Security Cloud Control warns you if there are configuration changes staged on Security Cloud Control for any of the devices you selected and asks if you want to continue with the bulk reading configurations action.
7. Click **Read All** to continue.
8. Look at the notifications tab for the progress of the **Read All** configurations operation.

9. If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

The device configurations are read from the selected devices and Security Cloud Control's copy of the configurations is updated to match the local device configurations.

Configuration reading from ASA to Security Cloud Control

Explains how Security Cloud Control reads and maintains copies of device configurations for management purposes.

Configuration reading is a management process that

- enables Security Cloud Control to maintain its own copy of the ASA running configuration file for device management
- occurs during device onboarding when Security Cloud Control reads and saves a copy of the device configuration file for the first time, and
- provides options to **Check for Changes**, **Accept without Review**, or **Read Configuration** when reading configurations from an ASA.

When Security Cloud Control needs to read ASA configurations

Security Cloud Control needs to read an ASA configuration in these circumstances:

- When deployment of configuration changes to the ASA fails and the device state is not listed or **Not Synced**.
- When device onboarding fails and the device state is **No Config**.
- When changes are made to the device configuration outside of Security Cloud Control and those changes have not yet been polled or detected. In this case, the device state is **Synced** or **Conflict Detected**.

In these cases, Security Cloud Control needs a copy of the last known configuration stored on the device.

For more information, refer to Reading, Discarding, Checking for, and Deploying Configuration Changes.

Read configuration changes on ASA device

Configure manual synchronization of your ASA device with Security Cloud Control to resolve onboarding or deployment failures.

This task enables you to manually synchronize your ASA device with Security Cloud Control to resolve onboarding or deployment failures.

Use this procedure when you need to resolve onboarding failures or deployment issues by reading configuration changes directly from your ASA device.

Follow these steps to read configuration changes on your ASA device:

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab.
4. Click the appropriate device type tab.
5. Select the device that Security Cloud Control has recently failed to onboard, or select the device where Security Cloud Control could not deploy a change.
6. Click **Read Configuration** in the **Synced** pane.

This option overwrites the configuration currently saved to Security Cloud Control.

The device configuration is read from the ASA device and synchronized with Security Cloud Control, resolving onboarding or deployment failures.

Reading changes from firewalls

Explains how Security Cloud Control manages device configurations by reading and saving configuration files from Cisco IOS devices or SSH devices.

Reading changes from firewalls is a configuration management process that

- requires Security Cloud Control to maintain its own copy of the device configuration file
- involves onboarding the device when Security Cloud Control first reads and saves its configuration file, and
- replaces the existing copy in the database when checking the configuration from the device.

Configuration change management processes

When you check the configuration from the device, Security Cloud Control saves a new copy of the device configuration file and replaces the copy in its database.

Related processes include:

- Detecting changes made directly to the Cisco IOS or SSH device outside of Security Cloud Control
- Undoing configuration changes that have been started on Security Cloud Control but not deployed to the IOS or SSH device

For more information about these processes, refer to:

- Reading, Discarding, Checking for, and Deploying Configuration Changes
- Check for Changes
- Discard Changes

Preview and deploy configuration changes for all devices

Configure deployment of pending configuration changes to managed devices in Security Cloud Control, track deployment progress, and verify results in jobs or event logs.

This task allows you to deploy pending configuration changes to managed devices in Security Cloud Control and verify the deployment results.

Security Cloud Control informs you when you have made a configuration change to a device in your organization, but you have not deployed that change, by displaying an orange dot on the deploy icon . Each device affected by these changes displays a status of "Not Synced" in the **Security Devices** page. Click **Deploy** to review which devices have pending changes and deploy the changes to those devices.

This deployment method is available for all supported devices.

You can use this deployment method for a single configuration change. Alternatively, you can wait and deploy multiple changes at once.

This deployment method is only available when Security Cloud Control Firewall Management has been onboarded to Security Cloud Control.

Procedure

1. In the menu bar of Security Cloud Control click the **Deploy** button .
2. Select the devices with changes you want to deploy. If a device displays a yellow caution triangle, you cannot deploy changes to that device. Hover your pointer over the yellow caution triangle to see the reason.
3. (Optional) If you want to see more information about a pending change, click the **View Detailed Change log** link to open the change log associated with that change. Click the **Deploy** icon to return to the **Devices with Pending Changes** page.
4. Click **Deploy Now** to deploy the changes immediately to the devices that you selected. You will see the progress in the Active jobs indicator in the Jobs tray.
5. (Optional) After the deployment has finished, in the **Platform menu**, click Firewall, and then select **Events & Logs** > **Events** > **Jobs**. You will see a recent "Deploy Changes" job showing the results of the deployment.

Configuration changes are successfully deployed to the selected devices. The deployment status can be monitored through the Jobs tray and verified in the Events & Logs section.

Deploy configuration changes from Security Cloud Control to ASA

Explains how to deploy configuration changes from Security Cloud Control to your ASA device, including staging updates, modifying the running configuration, and saving to the startup configuration.

A configuration deployment is a network management process that

- transfers staged configuration changes from Security Cloud Control to the running configuration of an ASA device
- updates only the modified configuration elements without overwriting the entire configuration file, and
- allows changes to take effect on network traffic passing through the device.

Why does Security Cloud Control deploy changes to an ASA

When you manage and make changes to a device configuration with Security Cloud Control, Security Cloud Control saves those changes to its own copy of the configuration file. Those changes are considered staged on Security Cloud Control until they are deployed to the device. Staged configuration changes have no effect on the network traffic running through the device. Only after Security Cloud Control deploys the changes to the device do they have an effect on the traffic running through the device. When Security Cloud Control deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. These actions do not overwrite the entire configuration file on your device.

The ASA has a running configuration file (sometimes called the running config) and a startup configuration file (sometimes called the startup config). The configuration stored in the running config file is enforced on traffic passing through the ASA. After you change the running config and confirm the device behaves as you want, deploy those changes to the startup config. When you reboot the ASA, it starts using the startup config as its configuration starting point. If you do not save your changes to the startup config, you lose them when you reboot the ASA.

Deploying changes from Security Cloud Control to an ASA writes those changes to the running configuration file. When you are satisfied with how those changes affect the device, deploy them to the startup configuration file.

You can start deployments for one device or several devices simultaneously. You can schedule single or recurring deployments for a device.

If you use the command line interface on Security Cloud Control to make a change to an ASA, those changes are not staged on Security Cloud Control. They are deployed directly to the running configuration of the ASA. When you make changes that way, your device remains synced with Security Cloud Control.

Deploy configuration changes

Configure deployment of configuration changes to your ASA using Security Cloud Control.

This task enables you to update your device configuration via the GUI or Device Configuration page to ensure your network remains secure.

This section assumes you are using Security Cloud Control's GUI or editing the Device Configuration page to make changes to an ASA configuration file, and not using Security Cloud Control's CLI interface or CLI macro interface.

Follow these steps to update an ASA configuration:

Procedure

1. Make changes on Security Cloud Control using one of these methods:
   - The Security Cloud Control GUI
   - The device configuration on the **Device Configuration** page
2. After you make your changes, return to the **Security Devices** page and select **Preview and Deploy...** to apply the change to the device.

   Further you can:

   When Security Cloud Control updates an ASA's running configuration with the one staged on Security Cloud Control or changes the configuration on Security Cloud Control with the running configuration stored on the ASA, it attempts to change only the relevant lines of the configuration file. These selective changes occur only if the configuration aspect can be managed by the Security Cloud Control GUI. If the desired configuration change cannot be made using the Security Cloud Control GUI, Security Cloud Control attempts to overwrite the entire configuration file.

   Here are two examples:

   - You **can** create or change a network object using the Security Cloud Control GUI. If Security Cloud Control needs to deploy that change to an ASA's configuration, it would overwrite the relevant lines of the running configuration file on the ASA when the change occurs.
   - You **cannot** create a new local ASA user using the Security Cloud Control GUI but you can create one by editing the ASA's configuration on the Device Configuration page. If you add a user on the Device Configuration page, and you deploy that change to the ASA, Security Cloud Control will try to save that change to the ASA's running configuration file by overwriting the entire running configuration file.

The configuration changes are deployed to your device and your network configuration is updated according to the changes made through the two-step deployment process.

Deploy configuration changes made using the Security Cloud Control GUI

Configure deployment of configuration changes made via the Security Cloud Control GUI to your ASA.

This task allows you to apply configuration changes from Security Cloud Control to your device's running configuration.

Use this procedure to review pending updates, check synchronization status, and apply changes effectively after making configuration modifications through the Security Cloud Control GUI.

Procedure

1. When you make a configuration change using Security Cloud Control GUI and save it, the change is stored in the version of the ASA's running configuration file kept in Security Cloud Control.

2. Return to the device on the **Security Devices** page.
3. Click the **Devices** tab. The device status now displays **Not synced**.
4. Choose one of these methods to deploy the changes.

   - Click the **Deploy** icon ( ) at the top right of the screen. A review screen appears so you can examine your changes. Select the device you modified, expand it to review the changes, and click **Deploy now** to deploy the changes.

     Note

     If you see a yellow warning triangle next to your device on the **Devices with Pending Changes** screen, you cannot deploy changes to it. Hover over the warning triangle to learn why you cannot deploy changes.

   - In the **Not Synced** pane, click **Preview and Deploy...**

     a. Review the commands that will change the ASA configuration file.

     b. If you are satisfied with the commands, choose a **Configuration Recovery Preference**.

        Note

        If you choose **Let me know and I will restore the configuration manually**, click **View Manual Synchronization Instructions** before continuing.

     c. Click **Apply Changes to Device**.

     d. Click **OK** to acknowledge the success message.

The configuration changes are successfully deployed to your ASA and the device status returns to synced.

Schedule automatic deployments

Explains how to configure automatic deployment of configuration changes to devices in your tenant.

Schedule automatic deployments is a configuration feature that enables your tenant to deploy changes automatically either to a single device or to all devices with pending changes.

Deployment scheduling information

For more information about the deployment scheduling feature, refer to scheduling automatic deployments.

Deploy configuration changes using Security Cloud Control's CLI interface

Configure device settings by deploying configuration changes directly through the command line interface in Security Cloud Control.

This task allows you to deploy configuration changes to devices using the CLI interface, enabling direct command execution for configuration management and device updates.

Use the CLI interface when you need to make configuration changes to devices through direct command entry. This method is useful for single commands, batch operations, or applying configuration file sections.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab.
4. Click the appropriate device type tab.
5. Select the device whose configuration you want to change.
6. Click **>_Command Line Interface** in the **Actions** pane.
7. If there are any commands in the command line interface table, click **Clear** to remove them.
8. In the top box of the command line interface table, enter your commands at the command prompt. You can run a single command, several commands in a batch by entering each command on its own line, or entering a section of configuration file as a command.

   A single command creating the network object "albany":

   ```
   object network albany
   host 209.165.30.2
   ```

   Multiple commands sent together:

   ```
   object network albany
   host 209.165.30.2
   object network boston
   host 209.165.40.2
   object network cambridge
   host 209.165.50.2
   ```

   A section of a running configuration file entered as a command:

   ```
   interface GigabitEthernet0/5
    nameif guest
    security-level 0
    no ip address
   ```

   Note

   Security Cloud Control does not require you to move between EXEC mode, Privileged EXEC mode, and Global Configuration mode. It interprets the command you enter in the proper context.

9. After you have entered your commands, click **Send**.

   After Security Cloud Control has successfully deployed the changes to the ASA's running config file, you receive the message, Done!

10. After you send the command, you may see the message, "Some commands may have made changes to the running config." This message includes two links.
    - Click **Deploy to Disk** to save the changes made by this command, and any other change in the running config, to the ASA's startup config.

- Click **Dismiss** to dismiss the message.

The configuration changes are deployed to the device's running configuration. If you choose to deploy to disk, the changes are also saved to the startup configuration.

Deploy configuration changes by editing the device configuration

Configure configuration changes by editing the Device Configuration in Security Cloud Control. This procedure allows you to modify the ASA running configuration directly.

This task allows you to deploy configuration changes by directly editing the device configuration in Security Cloud Control, enabling direct modification of the ASA running configuration.

> ⚠ **Caution**
>
> This procedure is for advanced users who are familiar with the syntax of an ASA configuration file. This method makes changes directly to the running configuration file stored on Security Cloud Control.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**
3. Click the appropriate device type tab.
4. Select the device whose configuration you want to change.
5. Click **View Configuration** in the **Actions** pane.
6. Click **Edit**.
7. Make your changes to the running configuration and **Save** them.
8. Return to the **Security Devices** page. In the Not Synced pane, click **Preview and Deploy...**
9. In the **Device Sync** pane to review the changes.
10. Click **Replace Configuration** or **Apply Changes to Device** depending on the kind of change it is.

The configuration changes are deployed to the device and the device configuration is updated with your modifications.

Deploy configuration changes for a shared object on multiple devices

Configure deployment of changes to a policy or object shared by two or more devices.

This task enables you to efficiently modify and deploy configuration changes to multiple devices that share a common policy or object, ensuring consistent updates across your network infrastructure.

Use this procedure when you are making changes to a policy or object shared by two or more devices. You can change a common policy on however many devices use it.

Procedure

---

1. Open and edit the Policies page or the Objects page containing the shared object you want to edit.
2. Review the shared device list and confirm that you want to make the changes on all the devices mentioned.

3. Click **Confirm**.
4. Click **Save**.
5. Click the **Deploy** icon and deploy your changes to the affected devices.

The configuration changes are deployed to all devices that share the modified policy or object, ensuring consistent updates across your network infrastructure.

Deploy changes to a device

Configure deployment of configuration changes to a single FTD, Meraki, or AWS VPC device.

Deploy saved configuration changes from Security Cloud Control to the actual device.

Use this procedure to deploy changes to a single FTD, Meraki, or AWS VPC device.

Procedure

---

1. When you make a configuration change for a device using Security Cloud Control and save it, that change is saved in the Security Cloud Control instance of the device configuration.
2. From the Security Cloud Control Home page, click **Firewall**.
3. Choose **Security Devices**.
4. Click the **Devices** tab.
5. Click the appropriate device type tab. The configuration status of the device will display "Not synced" after you make changes.
6. To deploy the changes, select one of these methods:
   - Select the device and in the "Not Synced" pane, and click **Preview and Deploy**. On the Pending Changes screen, review the changes. If you are satisfied with the pending version, click **Deploy Now**.

     After the changes are deployed successfully, you can view the change log to confirm.
   - Click the **Deploy** icon. For more information, refer to Preview and deploy configuration changes for all devices on page 817.

The configuration changes are deployed to the selected device and the device status updates to reflect successful synchronization.

Cancelling changes

Describes what happens when you cancel the deployment of changes from Security Cloud Control to a device.

Cancelling changes is a deployment control action that

- stops the deployment process when you click **Cancel** during deployment
- prevents changes from being deployed to the device
- keeps changes in a pending state on Security Cloud Control for future editing and deployment to FDM-managed device.

Discarding changes

Describes the process of removing uncommitted configuration changes in device management.

Discarding changes is a configuration management action that removes all uncommitted modifications made to device configurations and reverts the system to the last deployed state.

Change discarding behavior

When you click **Discard all** while previewing changes, the system performs these actions:

- Deletes the changes you made
- Deletes any other changes that other users made but did not deploy to the device
- Reverts Security Cloud Control pending configuration to the last read or deployed configuration before any changes were made

Bulk deploy device configurations

Configure bulk deployment to apply configuration changes to multiple devices simultaneously when you have made changes by editing shared objects.

Use bulk deployment to efficiently apply configuration changes to multiple devices at once, particularly when you have modified shared objects that affect several devices.

If you have made changes to multiple devices, for instance by editing a shared object, you can apply those change to all of the affected devices at once.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select all of the devices for which you have made configuration changes on Security Cloud Control. These devices should show "Not Synced" status.
5. Deploy the changes using one of these methods:
   - Click the  button at the top-right of the screen to view the **Devices with Pending Changes** window. This gives you a chance to review the pending changes on the devices you selected before you deploy them. Click **Deploy Now** to deploy the changes.

     > **Note**
     >
     > If you see a yellow warning triangle next to a device on the **Devices with Pending Changes** screen, you cannot deploy a change to that device. Hover your mouse over the warning triangle for information about why changes cannot be deployed to that device.

   - Click **Deploy All** on the details pane. Review any warnings and click **OK**. The bulk deployment starts immediately without a review of the changes.
6. (Optional) Click the Jobs icon  in the navigation bar to view the results of the bulk deploy.

Configuration changes are deployed to all selected devices simultaneously, and the deployment status can be monitored through the Jobs interface.

Preview and deploy On-Premises Firewall Management Center configurations

Configure deployment of configuration changes made in Security Cloud Control to your On-Premises Firewall Management Center, ensuring the updates are pushed and synchronized efficiently.

This task allows you to deploy configuration changes made in Security Cloud Control to your On-Premises Firewall Management Center and ensures configuration synchronization between systems.

If you have made configuration changes to an object, such as changing a value or adding an override to an object, you can deploy all those changes at once to your On-Premises Firewall Management Center.

> **Note**
>
> This task deploys configuration changes only to On-Premises Firewall Management Center. To deploy these changes to your Firewall Threat Defense devices, you must deploy these changes manually from your On-Premises Firewall Management Center. For more information, see Configuration Deployment in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Firewall Management Center**
3. Click the **FMC** tab.
4. Select the On-Premises Firewall Management Center where you want to preview and deploy changes.

   > **Note**
   >
   > Security Cloud Control identifies when your On-Premises Firewall Management Center is out of sync and displays the status as **Not Synced**.

5. Click **Preview and Deploy** on the details pane.
6. Review any warnings. To deploy immediately, click **Deploy Now**. If you do not want to proceed, click **Discard All**.
7. Alternatively, click the download button at the top-right corner of the screen to open the **Devices with Pending Changes** window. Select the devices, review the pending changes on the selected devices, and then deploy them.
8. Click **Deploy Now** to deploy the changes.

The configuration changes are deployed to your On-Premises Firewall Management Center and the system status shows as synchronized. You must manually deploy these changes to your managed Firewall Threat Defense devices from your On-Premises Firewall Management Center.

Scheduled automatic deployments

Describes a Security Cloud Control feature that allows you to schedule configuration changes to be deployed to devices at a convenient time.

A scheduled automatic deployment is a Security Cloud Control feature that

- allows you to make configuration changes to one or more devices and schedule the deployment at a convenient time
- deploys all staged changes saved on Security Cloud Control at the specified date and time, and
- requires enabling the scheduling option in the **Tenant Settings** tab before use.

Deployment requirements and behavior

You can only schedule deployments if you Enable scheduled automatic deployments on page 52 in the **Tenant Settings** tab of the Settings page. Once this option is enabled, you can create, edit, or delete scheduled deployments.

If there were changes made directly to the device that have not been read to Security Cloud Control, the scheduled deployment will be skipped until that conflict is resolved. The Jobs page will list any instance where a scheduled deployment fails. If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

You can also view and delete scheduled deployments from the Jobs page.

Caution

If you schedule a new deployment for multiple devices, and some of those devices already have deployments scheduled, the new scheduled deployment overwrites the existing scheduled deployments.

Note

When you create a scheduled deployment, the schedule is created in your local time, not in the time zone of the device. Scheduled deployments *do not* automatically adjust for daylight savings time.

Enable scheduled automatic deployments

Configure the option to schedule automatic deployments to conveniently plan single or recurring updates for your devices.

Enable the option to schedule automatic deployments to automate deployment workflows and ensure updates occur at optimal times.

Enabling the option to schedule automatic deployments allows you to schedule future deployments at a date and time when it is convenient. Once you enable this option, you can schedule a single automatic deployment or set up recurring automatic deployments.

Changes you make on Security Cloud Control for a device are not automatically deployed to the device if it has pending changes . If a device is not in the **Synced** state, such as **Conflict Detected** or **Not Synced**, scheduled deployments are not executed. The jobs page lists any instance where a scheduled deployment fails.

If you turn off **Enable the Option to Schedule Automatic Deployments**, all scheduled deployments are deleted.

Important

If you use Security Cloud Control to create more than one scheduled deployment for a device, the new deployment overwrites the existing deployment. If you create more than one scheduled deployment for a device using the API, you **must** delete the existing deployment before scheduling the new deployment.

Follow these steps to enable scheduled automatic deployments:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Turn on the **Enable the option to schedule automatic deployments** toggle button to enable it.

The option to schedule automatic deployments is now enabled, allowing you to schedule single or recurring automatic deployments for your devices.

Schedule an automatic deployment

Configure a one-time or recurring automatic deployment schedule for ASA and FDM-managed devices to align with your maintenance window.

Schedule automatic deployments to streamline the deployment process and align with maintenance windows. This can be configured as a single event or a recurring event for convenience.

The deployment schedule can be a single event or a recurring event. You may find recurring automatic deployments a convenient way to line up recurring deployments with your maintenance window.

Important

This procedure applies only to ASAs and FDM-managed devices.

To schedule deployments for Secure Firewall Threat Defense devices managed by on-premises Firewall Management Center or Cloud-Delivered Firewall Management Center, see Scheduling.

Note

If you schedule a deployment for a device that has an existing deployment scheduled, the new scheduled deployment overwrites the existing deployment.

Follow these steps to schedule a one-time or a recurring deployment for a single device:

Procedure

1. From the Security Cloud Control home page, choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select one ore more devices.

5. In the Device Details pane, locate the Scheduled Deployments tab and click **Schedule**.
6. Select when the deployment should occur.
   - For a one-time deployment, click the **Once on** option to select a date and time from the calendar.
   - For a recurring deployment, click the **Every** option. You can choose either a daily or once a week deployment. Select the **Day** and **Time** the deployment should occur.
7. Click **Save**.

The automatic deployment is scheduled according to your selected configuration. The system will execute deployments at the specified time intervals.

Edit a scheduled deployment

Configure the recurrence, date, or time settings for an existing scheduled deployment in Security Cloud Control.

Edit the timing parameters of scheduled deployments to ensure device configurations are deployed at the most appropriate times for your network operations.

Use this procedure when you need to modify the scheduling parameters of an existing deployment to better align with maintenance windows or operational requirements.

Before you begin

Follow these steps to edit a scheduled deployment:

Procedure

---

1. From the Security Cloud Control home page, choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select one or more devices.
5. In the **Device Details** pane, locate the Scheduled Deployments tab and click **Edit**.



6. Edit the recurrence, date, or time of a scheduled deployment.
7. Click **Save**.

The scheduled deployment is updated with your new timing parameters and will execute according to the modified schedule.

Delete a scheduled deployment

Configure the deletion of a scheduled deployment for one or more devices in CDO.

This task allows you to remove scheduled deployments that are no longer needed or need to be rescheduled.

Use this procedure when you need to cancel or remove a previously scheduled deployment from your devices.

> **Note**
>
> If you schedule a deployment for multiple devices, and then change or delete the schedule for some of the devices, the original scheduled deployment for the remaining devices will be preserved.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select one or more devices.
5. In the **Device Details** pane, locate the **Scheduled Deployments** tab and click **Delete** .

- Reading, Discarding, Checking for, and Deploying Configuration Changes
- Read all device configurations on page 815
- Deploy configuration changes from Security Cloud Control to ASA on page 818
- Preview and deploy configuration changes for all devices on page 817

The scheduled deployment is deleted from the selected devices.

Check for configuration changes

Verify if the device's configuration has been changed directly on the device and differs from the configuration stored on Security Cloud Control.

Check for configuration changes to determine if the device's configuration has been modified directly on the device and no longer matches the copy stored on Security Cloud Control.

Use **Check for Changes** to determine if the device's configuration has been changed directly on the device and it is no longer the same as the copy of the configuration stored on Security Cloud Control. You will see the this option when the device is in the "Synced" state.

Procedure

1. From the Security Cloud Control home page, choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select the device, whose configuration you suspect may have been changed directly on the device.
5. Click **Check for Changes** in the Synced pane on the right.
6. The behavior that follows is slightly different depending on the device:

- For FTD Meraki AWS device if there has been a change to the device's configuration, you will receive the message:

```
Reading the policy from the device. If there are active deployments on the
device, reading will start after they are finished.
```

- Click **OK** to continue. The configuration on the device will overwrite the stored configuration on Security Cloud Control.
- Click **Cancel** to cancel the action.

- For ASA IOS SSH device:

a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on Security Cloud Control. The configuration labeled **Found on Device** is the configuration saved on the ASA.

b. Select either:

1. **Reject** the out-of-band changes to keep the "Last Known Device Configuration."
2. **Accept** the out-of-band changes to overwrite the device's configuration stored in Security Cloud Control with the configuration found on the device.

c. Click **Continue**.

The system compares configurations and presents options to either accept or reject the changes found on the device.

Discard configuration changes

Configure Security Cloud Control to undo all undeployed configuration changes made to a device's configuration.

Use this task to discard undeployed configuration changes and restore synchronization between Security Cloud Control and the device configuration.

Click **Discard Changes** when you want to "undo" all the *undeployed* configuration changes you made to a device's configuration using Security Cloud Control. When you click **Discard Changes**, Security Cloud Control *completely overwrites* its local copy of a device's configuration with the configuration stored on the device.

When you click **Discard Changes**, your device's configuration status is in a **Not Synced** state. After you discard your changes, the copy of the configuration on Security Cloud Control will be the same as the copy of the configuration on the device and the configuration status in Security Cloud Control will return to Synced.

Follow these steps to discard all of your undeployed configuration changes for a device:

Procedure

---

1. From the Security Cloud Control home page, choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select the device you have been making configuration changes to.
5. Click **Discard Changes** in the **Not Synced** pane on the right.
   - For FDM-managed devices-Security Cloud Control warns you that "Pending changes on Security Cloud Control will be discarded and the Security Cloud Control configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
   - For Meraki devices-Security Cloud Control deletes the change immediately.
   - For AWS devices-Security Cloud Control displays what you are about to delete. Click **Accept** or **Cancel**.

The device configuration status returns to Synced, and the configuration copy on Security Cloud Control matches the configuration on the device.

Discard On-Premises Firewall Management Center configuration changes

Configure Security Cloud Control to discard all configuration changes made for an On-Premises Firewall Management Center, ensuring the configuration matches the version stored on the managed device.

This task allows you to undo all configuration changes made in Security Cloud Control and restore the configuration to match what is stored on the device.

Use this procedure when you need to undo all configuration changes you made in Security Cloud Control, such as changes to objects shared between your Security Cloud Control and On-Premises Firewall Management Center. When you perform this task, Security Cloud Control *completely overwrites* its local configuration copy with the configuration stored on the device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Firewall Management Center**.
3. Click the **FMC** tab.
4. Select the On-Premises Firewall Management Center for which you want to discard changes.
5. Click **Discard Changes** in the **Not Synced** pane.

   When you click **Discard Changes**, your On-Premises Firewall Management Center configuration status changes to **Not Synced**. After you discard your changes, the configuration copy stored in Security Cloud Control matches the configuration on On-Premises Firewall Management Center. The status in Security Cloud Control then returns to **Synced**.

All configuration changes are discarded and the local configuration copy in Security Cloud Control matches the configuration stored on the On-Premises Firewall Management Center. The status returns to **Synced**.

Out-of-band changes on devices

Explains configuration changes made directly on network devices without using Security Cloud Control and how these changes create conflicts between device and cloud configurations.

Out-of-band changes are configuration modifications that

- are made directly on the device without using Security Cloud Control
- may be made using the device's command-line interface over an SSH connection or by using a local manager like the Adaptive Security Device Manager (ASDM) for the ASA, the FDM for the FDM-managed device, or for an On-Premises Firewall Management Center on the On-Premises Firewall Management Center user interface, and
- cause a conflict between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

Detecting out-of-band changes on devices

If Conflict Detection is enabled for an ASA, or an FDM-managed device, a Cisco IOS device, or an On-Premises Firewall Management Center, Security Cloud Control checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of Security Cloud Control.

If Security Cloud Control finds that there are changes to the device's configuration that are not stored on Security Cloud Control, it changes the **Configuration Status** of that device to the "Conflict Detected" state.

When Security Cloud Control detects a conflict, one of these conditions is likely:

- There have been configuration changes made to the device directly that have not been saved to Security Cloud Control's database.
- In the case of an FDM-managed device, there may be "pending" configuration changes on the FDM-managed device that have not been deployed.
- In the case of an On-Premises Firewall Management Center, there may be changes made, for instance, to objects outside Security Cloud Control, which are pending to be synchronized with Security Cloud Control or changes made in Security Cloud Control which are pending to be deployed to the On-Premises Firewall Management Center.

Synchronizing configurations between Security Cloud Control and device

Explains how to synchronize configurations between Security Cloud Control and device.

Configuration synchronization is a process that maintains consistency between device configurations stored in Security Cloud Control and configurations stored locally on devices.

Configuration conflicts

In the **Security Devices** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Premises Firewall Management Center that you manage using Security Cloud Control, navigate **Administration** > **Integrations** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on Security Cloud Control and the configuration stored locally on the device are the same.
- When a device is **Not Synced**, the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device. Deploying your changes from Security Cloud Control to the device changes the configuration on the device to match Security Cloud Control's version.
- Changes made to devices outside of Security Cloud Control are called **out-of-band changes**. When out-of-band changes are made, you'll see the device state change to "Conflict Detected," if conflict detection is enabled for the device. Accepting the out-of-band changes, changes the configuration on Security Cloud Control to match the configuration on the device.

Conflict detection

Describes a monitoring feature that identifies unauthorized configuration changes made to devices outside of the management platform.

Conflict detection is a monitoring feature that

- polls devices at regular intervals to identify configuration changes made outside of Security Cloud Control
- changes the device configuration status to **Conflict Detected** when out-of-band changes are identified, and
- stops polling when there are staged changes and the device is in **Not Synced** state for On-Premises Firewall Management Center devices.

Out-of-band changes and conflict states

Changes made to a device outside of Security Cloud Control are called "out-of-band" changes.

In the case of an On-Premises Firewall Management Center that is managed by Security Cloud Control, if there are changes that are staged and the device is in **Not Synced** state, Security Cloud Control stops polling the device to check for changes. When there are changes made outside Security Cloud Control which are pending to be synchronized with Security Cloud Control and changes made in Security Cloud Control which are pending to be deployed to the On-Premises

Firewall Management Center, Security Cloud Control declares the On-Premises Firewall Management Center to be in the **Conflict Detected** state.

Once this option is enabled, you can configure how often conflicts or OOB changes are detected per device. See Schedule polling for device changes on page 838 for more information.

Enable conflict detection

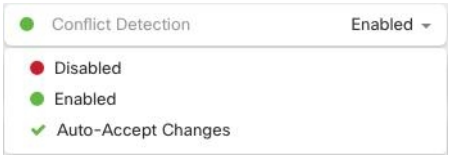
Configure conflict detection to alert you when changes have been made to a device outside of Security Cloud Control.

Enable conflict detection to receive alerts when changes are made to a device outside of Security Cloud Control.

Enabling conflict detection alerts you to instances where changes have been made to a device outside of Security Cloud Control.

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab.
3. Select the appropriate device type tab.
4. Select the device or devices for which you want to enable conflict detection.
5. In the **Conflict Detection** box at the right of the device table, select **Enabled** from the list.



Conflict detection is enabled for the selected devices and will alert you to external changes made to those devices.

Enable conflict detection for an On-Premises Firewall Management Center

Configure conflict detection for an On-Premises Firewall Management Center that you manage using Security Cloud Control.

Enable conflict detection to monitor changes made outside Security Cloud Control and changes made in Security Cloud Control that require synchronization.

Enabling conflict detection for an On-Premises Firewall Management Center keeps you informed when there are changes made outside Security Cloud Control that are pending synchronization with Security Cloud Control, and when there are changes made in Security Cloud Control that are pending deployment to On-Premises Firewall Management Center.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Firewall Management Center**.
3. From the list, select the On-Premises Firewall Management Center for which you want to enable conflict detection.
4. In the **Conflict Detection** box on the right pane, select **Enabled** from the list.

> **Note**
>
> Unlike other devices managed by Security Cloud Control, for an On-Premises Firewall Management Center, you can either enable or disable conflict detection; you cannot opt to auto-accept changes.

Conflict detection is now enabled for the On-Premises Firewall Management Center, and you will receive notifications when changes require synchronization.

Auto-accept changes

Describes a feature that automatically updates Security Cloud Control configuration when out-of-band changes are made directly to managed devices.

Auto-accept changes is a configuration management feature that

- automatically accepts any change made directly to a managed device without using Security Cloud Control
- enhances conflict detection by checking for out-of-band changes every 10 minutes, and
- updates Security Cloud Control's local version of the device configuration automatically without prompting.

How auto-accept changes works

Changes made directly to a device without using Security Cloud Control are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

If you have auto-accept changes enabled on your device, Security Cloud Control checks for changes every 10 minutes to determine if there have been any out-of-band changes made to the device's configuration. If there have been configuration changes, Security Cloud Control automatically updates its local version of the device's configuration without prompting you.

> **Note**
>
> Security Cloud Control will ***not*** automatically accept a configuration change if there are configuration changes made on Security Cloud Control that have not yet been deployed to the device. Follow the prompts on the screen to determine your next action.

To use auto-accept changes, you first enable the tenant to display the auto-accept option in the Conflict Detection menu on the **Security Devices** page; then, you enable auto-accept changes for individual devices. For On-Premises Firewall Management Center, you can do this from the **Services** page by navigating **Administration** > **Integrations** > **Firewall Management Center** and selecting the FMC.

If you want Security Cloud Control to detect out-of-band changes but give you the option to accept or reject them manually, enable Conflict detection on page 832 instead.

Configure auto-accept changes

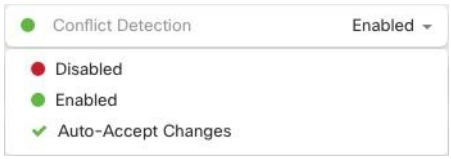
Configure the auto-accept changes feature to automatically accept out-of-band changes detected on security devices.

This task enables automatic acceptance of out-of-band changes on security devices, reducing manual intervention when configuration changes are detected.

When devices are managed through Security Cloud Control, out-of-band changes can occur when configurations are modified directly on the device. The auto-accept feature automatically incorporates these changes without requiring manual review.

Procedure

1. Log in to Security Cloud Control using an account with Admin or Super Admin privileges.
2. From the Security Cloud Control Home page, click **Firewall**.
3. Choose **Administration** > **General Settings**.
4. In the **Tenant Settings** area, click the toggle to **Enable the option to auto-accept device changes**. This enables the Auto-Accept Changes menu option to appear in the Conflict Detection menu on the **Security Devices** page.
5. In the left pane, click **Security Devices** and select the device for which you want to automatically accept out-of-band changes.
6. In the **Conflict Detection** menu, select **Auto-Accept Changes** in the drop-down menu.



The device is now configured to automatically accept out-of-band changes. When configuration changes are detected on the device, they will be automatically incorporated without requiring manual review or approval.

Disable auto-accept changes for all devices on the tenant

Configure tenant settings to disable the auto-accept changes option for all devices, requiring manual review of device conflicts before acceptance.

This task disables the auto-accept changes feature for all devices on your tenant, ensuring that all device conflicts require manual review before acceptance into Security Cloud Control.

When the auto-accept changes option is enabled, device conflicts are automatically accepted without manual review. Disabling this feature provides greater control over device changes by requiring explicit approval for each conflict.

Procedure

1. Log-in to Security Cloud Control using an account with Admin or Super Admin privileges.
2. From the Security Cloud Control Home page, click **Firewall**.
3. Choose **Administration** > **General Settings**.
4. In the **Tenant Settings** area, disable the "**Enable the option to auto-accept device changes**" by sliding the toggle to the left so it shows a grey X.

> **Note**
>
> Disabling "Auto-Accept" will require you to review each device conflict before you can accept it into Security Cloud Control. This includes devices previously configured to auto-accept changes.

The auto-accept changes feature is disabled for all devices on your tenant. The Auto-Accept Changes option in the Conflict Detection menu is no longer available, and all device conflicts will require manual review before acceptance.

Resolve configuration conflicts

Explains how to resolve configuration conflicts that occur on devices during configuration management and deployment processes.

This section explains how to resolve configuration conflicts that occur on the device.

Resolve the not synced status

Configure a device with a "Not Synced" Configuration Status to resolve synchronization issues between Security Cloud Control and the device.

This task helps you resolve synchronization conflicts when a device shows "Not Synced" status, allowing you to either deploy pending changes or revert to the device's current configuration.

Use this procedure when a device displays a "Not Synced" Configuration Status, indicating there are differences between the configuration stored in Security Cloud Control and the running configuration on the device.

Procedure

---

1. Choose **Security Devices**.

   > **Note**
   >
   > For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.
4. Select the device reported as Not Synced.
5. In the **Not synced** panel to the right, select either of the following:
   - **Preview and Deploy...** -If you want to push the configuration change from Security Cloud Control to the device, preview and deploy the changes you made now, or wait and deploy multiple changes at once.
   - **Discard Changes** -If you do **not** want to push the configuration change from Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This

option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

The device synchronization status is resolved. If you selected Preview and Deploy, your changes are pushed to the device. If you selected Discard Changes, the configuration in Security Cloud Control is updated to match the device's running configuration.

Resolve the conflict detected status

Configure conflict resolution to synchronize device configurations between Security Cloud Control and live devices when conflicts are detected.

This task resolves configuration conflicts that occur when changes are made directly to a device without using Security Cloud Control.

Security Cloud Control allows you to enable or disable conflict detection on each live device. If Conflict detection on page 832 is enabled and there was a change made to the device's configuration without using Security Cloud Control, the device's configuration status will show **Conflict Detected**.

Before you begin

Follow these steps to resolve a **Conflict Detected** status:

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.

   > **Note**
   >
   > For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

3. Click the **Devices** tab to locate your device.
4. Click the appropriate device type tab.
5. Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.
6. In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.
   - The panel labeled "Last Known Device Configuration" is the device configuration stored on Security Cloud Control.
   - The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.
7. Resolve the conflict by selecting one of the following:
   - **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration.

> **Note**
>
> As Security Cloud Control does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

- **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on Security Cloud Control.

> **Note**
>
> All configuration changes, rejected or accepted, are recorded in the change log.

The conflict status is resolved and the device configuration is synchronized between Security Cloud Control and the device.

Schedule polling for device changes

Configure Security Cloud Control to customize schedule polling for device changes by defining specific polling intervals per device when conflict detection or auto-accept is enabled.

Optimize Security Cloud Control by customizing schedule polling for device changes. This overrides the tenant default, ensuring precise monitoring of device configuration changes across your network for efficient, automated device management and synchronization.

If you enable Conflict detection on page 832 or **Enable the option to auto-accept device changes** from the **Settings** page, Security Cloud Control polls the device at the default interval to check for configuration changes made outside Security Cloud Control. You can set how often Security Cloud Control polls for changes for each device. This customization can be applied to multiple devices.

If you do not configure a selection for a device, the interval is automatically configured for "tenant default".

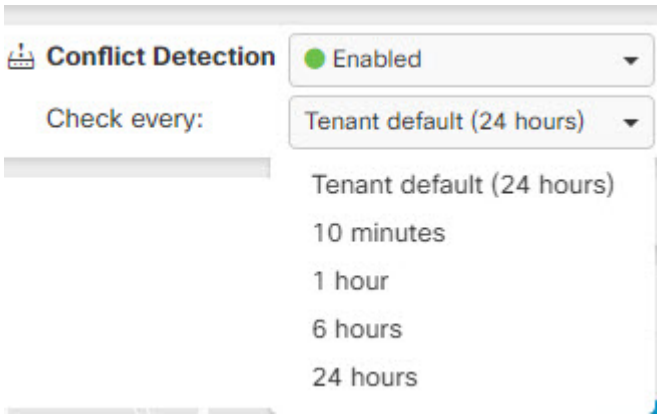
> **Note**
>
> If you set a custom interval per device on the **Security Devices** page, it overrides the polling interval selected as the Default Conflict Detection Interval on the **General Settings** page.

After you enable **Conflict Detection** from the **Security Devices** page or **Enable the option to auto-accept device changes** from the **Settings** page, you can schedule how often Security Cloud Control polls your devices with this procedure.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.

2. Choose **Security Devices**.
3. Click the **Devices** tab to locate your device.
4. Click the appropriate device type tab.
5. Select the devices where you want to enable conflict detection.
6. Next to **Conflict Detection**, click the drop-down menu for **Check every** and select the polling interval you want.



The selected devices are now configured with the custom polling interval for conflict detection, overriding the tenant default settings.

Schedule a security database update

Describes how to schedule a security database update on the device to ensure current threat protection and security policy enforcement.

This section provides information about scheduling a security database update on the device.

Create a scheduled security database update

Configure a scheduled task to automatically check and update security databases for an FTD device at specified intervals.

Create a scheduled task to ensure security databases are automatically updated on a regular basis to maintain device protection.

Use the following procedure to create a scheduled task to check and update the security databases for an FDM-managed device:

Procedure

1. In the navigation bar, click **Security Devices**.
2. Click the **Devices** tab to locate your device.
3. Click the **FTD** tab.
4. Select a device.
5. In the **Actions** pane, locate the **Security Database Updates** section and click the**add +** button.

> **Note**
>
> If there is an existing scheduled task for the selected device, click the edit icon to create a new task. Creating a new task will overwrite the existing one.

6. Configure the scheduled task with the following:
   - **Frequency** . Choose for the update to occur daily, weekly, or monthly.
   - **Time**. Choose the time of day. Note that the time displayed is UTC.
   - **Select Days.** Choose which day(s) of the week you want the update to occur.
7. Click **Save**.

The device's Configuration Status will change to "Updating Databases".

Edit a scheduled security database update

Configure the schedule for an existing security database update task for an FDM-managed device.

Edit an existing scheduled task to modify the frequency, time, and days for security database updates on an FDM-managed device.

Use this procedure to edit an existing scheduled task to check and update the security databases for an FDM-managed device.

Procedure

---

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate your device.
3. Click the **FTD** tab.
4. Select a device.
5. In the **Actions** pane, locate the **Security Database Updates** section and click the edit icon .
6. Edit the scheduled task with the following:
   - **Frequency**. Choose for the update to occur daily, weekly, or monthly.
   - **Time**. Choose the time of day. Note that the time displayed is UTC.
   - **Select Days.** Choose which day(s) of the week you want the update to occur.
7. Click **Save**.

The device's Configuration Status will change to "Updating Databases".

47 Manage onboarded device settings

Topics:

- Change a device's IP address in Security Cloud Control Firewall Management
- Change a device's name in Security Cloud Control Firewall Management
- Export a list of devices and services
- Export device configuration
- External links for devices
- Bulk reconnect devices to Security Cloud Control Firewall Management
- Moving devices between organizations
- Device certificate expiry detection
- Write a device note
- Delete a device from Security Cloud Control Firewall Management
- Back up Firewall Threat Defense devices
- Manage Firewall Threat Defense devices through Security Cloud Control Firewall Management
- Filter security devices by hardware end-of-life status
- Security Cloud Control Firewall Management labels and filtering
- Use Security Cloud Control Firewall Management search functionality

This chapter provides guidance on managing the device settings of the onboarded device.

Change a device's IP address in Security Cloud Control Firewall Management

Configure a device's IP address in Security Cloud Control Firewall Management when the device's network address changes.

Update the IP address stored in Security Cloud Control Firewall Management to match a device's new IP address without changing the device's configuration.

When you onboard an device to Security Cloud Control Firewall Management using an IP address, Security Cloud Control Firewall Management stores that IP address in its database and communicates with the device using that IP address. If the IP address of the device changes, you can update the IP address stored in Security Cloud Control Firewall Management to match the new address. Changing the device's IP address on Security Cloud Control Firewall Management does not change device's configuration.

To change the IP address, Security Cloud Control uses to communicate with a device, follow this procedure:

Procedure

1. Choose **Security Devices**
2. Click the **Devices** tab to locate the device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required device.
4. Select the device whose IP address it is you want to change.
5. Above the **Device Details** pane, click the edit button next to the device's IP address.

6. Enter the new IP address in the field and click the blue check button.

   No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

The IP address stored in Security Cloud Control Firewall Management is updated to the new address, and Security Cloud Control will communicate with the device using the new IP address.

Change a device's name in Security Cloud Control Firewall Management

Configure a device's name in Security Cloud Control Firewall Management without changing the device configuration itself.

Change device names to improve organization and identification in your inventory without affecting the actual device configuration.

All devices, models, templates, and services are given a name when they are onboarded or created in Security Cloud Control Firewall Management. You can change that name without changing the configuration of the device itself.

Procedure

1. Choose **Security Devices**.
2. Click the **Device** tab to locate the device.
3. Select the device whose name it is you want to change.

4. Above the **Device Details** pane, click the edit button next to the device's name.

5. Enter the new name in the field and click the blue check button.

   No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

The device appears with its new name in your inventory, while maintaining its synchronized configuration status.

Export a list of devices and services

Configure the export of your list of devices and services in Security Cloud Control Firewall Management to a comma-separated value (.CSV) file.

Export your list of devices and services to a comma-separated value (.CSV) file that can be opened in spreadsheet applications for sorting and filtering.

This article explains how to export your list of devices and services to a comma-separated value (.CSV) file. Once in that format, you can open the file in a spreadsheet application such as Microsoft Excel to sort and filter the items in your list.

The export button is available in both the Devices and Templates tab. You can also export details from devices under the selected device type tab.

Before you export your list of devices and services, look at the filter pane and determine if the **Security Devices** page is displaying the information you want to export. Clear all filters to view all managed devices and services, or apply filters to display a subset of your devices and services. The export function includes only the information currently displayed in the **Security Devices** page.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
4. Click the appropriate device type tab to export details from devices under that tab or click **All** to export details from all devices.

   You can use the filter and search functionalities to find the required device.

5. Click **Export list to CSV**.

6. If prompted, save the .CSV file.
7. Open the .CSV file in a spreadsheet application to sort and filter the results.

The device and service information is exported to a .CSV file that can be opened and manipulated in spreadsheet applications for sorting and filtering purposes.

Export device configuration

Configure device configuration export in Security Cloud Control Firewall Management.

Export a device's configuration to a JSON file for backup, analysis, or migration purposes.

You can only export one device configuration at a time.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
4. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required device.
5. Select the device you want so it is highlighted.
6. In the **Actions** pane, select **Export Configuration**.
7. Select **Confirm** to save the configuration as a JSON file.

The device configuration is exported and saved as a JSON file to your local system.

External links for devices

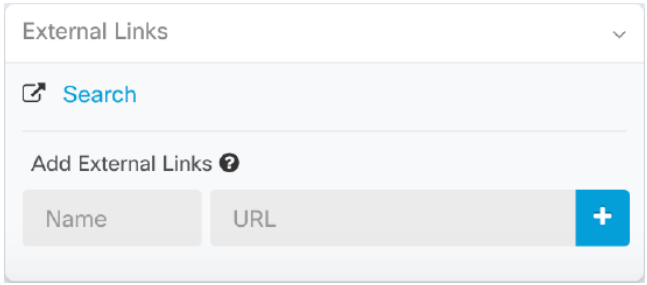
Explains external links for devices in Security Cloud Control Firewall Management.

An external link is a hyperlink feature that

- creates connections to external resources and associates them with managed devices
- enables convenient access to device local managers (Adaptive Security Device Manager (ASDM) for ASA), documentation, corporate wikis, or any chosen URL, and
- allows multiple link associations with devices and the same link with multiple devices simultaneously.

External link properties

You can associate as many external links with a device as you want. You can also associate the same link with multiple devices at the same time.



The links you create can reach anywhere, but your company's security requirements do not change. For example, if you ordinarily need to be connected to your corporate network, by being on-premises or through a VPN connection to reach

a particular URL, those requirements remain. If your company blocks specific URLs, those URLs continue to be blocked. URLs that are not restricted continue to not be restricted.

The {location} variable can be incorporated in your URLs. This variable will be populated with the IP address of your device. For example:

```
https://{location}
```

should reach the ASDM for your ASAor the FDM of your FDM-managed device.

Create an external link from your device

Configure external links from your device for related settings, requirements, and user workflow access.

This task enables you to create external links from your device that provide quick access to related settings, requirements, and user workflow information.

External links allow you to associate URLs with specific devices or model devices in your inventory, providing convenient access to related documentation or resources.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
4. Click the appropriate device type tab.
5. Select a device or model.

   You can use the filter and search functionalities to find the required device.
6. Enter a name for the link in the details pane under the **External Links** section.
7. Enter the URL for the link in the URL field. You need to specify the full URL. For example, for Cisco, enter http://www.cisco.com.
8. Click + to associate the link with the device.

The external link is now associated with the selected device and appears in the External Links section of the device details pane.

Create an External Link to ASDM FDM

Configure an external link to ASDMFDM for convenient access to device management.

Create an external link to provide convenient access to the Adaptive Security Device Manager (ASDM) of your ASA the Firepower Device Manager (FDM) of your FDM-managed device directly from Security Cloud Control.

This external link provides a convenient way to open the Adaptive Security Device Manager (ASDM) of your ASA the Firepower Device Manager (FDM) of your FDM-managed device, directly from Security Cloud Control.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required device.

4. Select a device or model.
5. In the details pane, on the right, go to the **External Links** section.
6. Enter a name for the link such as ASDM FDM.
7. Enter https://{location} in the URL field. The {location} variable will be populated with the IP address of your device.
8. Click the + box.

The external link is created and you can now access ASDMFDM directly from Security Cloud Control.

Create an external link for multiple devices

Configure external links for multiple devices to enable quick access to external resources or device management interfaces.

Create external links for multiple devices to provide quick access to external resources or device management interfaces directly from the device inventory.

External links allow you to create shortcuts to external resources associated with your devices, such as device management interfaces or external documentation. You can apply the same external link to multiple devices simultaneously.

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required devices.
4. Select multiple devices or models.
5. In the details pane, on the right, go to the **External Links** section.
6. Enter a name for the link.
7. Enter the URL you want to reach using one of these methods:
   - Enter

     ```
     https://{location}
     ```

     in the URL field. The {location} variable will be populated with the IP address of your device. This creates an automatic link to the ASDM for your device.
   - Enter the URL for the link in the URL field. You need to specify the full URL, for example, for Cisco enter http://www.cisco.com.
8. Click + to associate the link with the device.

The external link is created and associated with all selected devices. The link appears in the External Links section for each device and can be accessed by clicking on the link name.

Edit or delete external links

Configure external link settings by editing or deleting existing links for devices and model devices.

Edit or delete external links to manage device and model device configurations in Cisco Defense Orchestrator.

Use this procedure when you need to modify or remove external links associated with devices or model devices in your inventory.

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required device.

4. Select a device or model.
5. In the details pane, go to the **External Links** section.
6. Mouse-over the name of the link to reveal the edit and delete icons.
7. Click the appropriate icon to edit or delete the external link and confirm your action.

The external link is successfully edited or deleted from the device or model device configuration.

Edit or delete external links for multiple devices

Configure external link settings for multiple devices by editing or deleting existing links in the device inventory.

This task allows you to modify or remove external links from multiple devices simultaneously, providing efficient management of device connections across your network inventory.

External links provide additional connectivity and reference points for devices in your network. When managing multiple devices, you may need to update or remove these links to maintain accurate device configurations and improve network organization.

Follow these steps to edit or delete external links for multiple devices:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required devices.

4. Select multiple devices or models.
5. In the details pane, on the right, go to the **External Links** section.
6. Mouse-over the name of the link to reveal the edit and delete icons.
7. Click the appropriate icon to edit or delete the external link and confirm your action.

The external links for the selected devices are updated or removed based on your chosen action. The changes are applied immediately to all selected devices.

Bulk reconnect devices to Security Cloud Control Firewall Management

Configure bulk reconnection of multiple managed devices to Security Cloud Control Firewall Management at the same time.

This task allows administrators to attempt to reconnect multiple managed devices to Security Cloud Control Firewall Management simultaneously to restore management capabilities.

Security Cloud Control Firewall Management allows an administrator to attempt to reconnect more than one managed device to Security Cloud Control Firewall Management at the same time. When a device Security Cloud Control Firewall Management manages is marked "unreachable," Security Cloud Control Firewall Management can no longer detect out of band configuration changes or manage the device. There could be many different reasons for the disconnect. Attempting to reconnect the devices is a simple first step in restoring Security Cloud Control Firewall Management's management of the device.

> **Note**
>
> If you are reconnecting devices having new certificates, Security Cloud Control Firewall Management automatically reviews and accepts the new certificates on the devices and continues to reconnect with them. However, if you are reconnecting with only one device, Security Cloud Control Firewall Management prompts you to review and accept the certificate manually to continue to reconnect with it.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate devices.
3. Click the appropriate device type tab.

   Use the filter to look for devices whose connectivity status is "unreachable."
4. From the filtered results, select the devices you want to attempt to reconnect.
5. Click **Reconnect** . Notice that Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.
6. Look at the **notifications** tab for the progress of the bulk device reconnect action.

   > **Tip**
   >
   > If a reconnect failure was caused because the device's certificate or credentials have changed, you will have to reconnect to those devices individually to add the new credentials and accept the new certificate.

The selected devices are reconnected to Security Cloud Control Firewall Management, restoring management capabilities and allowing detection of configuration changes.

Moving devices between organizations

Explains the process and requirements for moving devices between organizations in Security Cloud Control Firewall Management.

Moving devices between organizations is a process that:

- requires removing devices from the current Security Cloud Control Firewall Management organization
- involves re-onboarding the devices to the new organization, and
- cannot be performed through direct migration between organizations.

Device migration requirements

After onboarding devices to a Security Cloud Control Firewall Management organization, you cannot migrate the devices from one Security Cloud Control Firewall Management organization to another. If you want to move your devices to a new organization, you need to remove the devices from the old tenant and re-onboard them to the new organization.

Device certificate expiry detection

Explains device certificate expiry detection functionality in Security Cloud Control Firewall Management.

Device certificate expiry detection is a monitoring feature that

- actively monitors the expiration status of management certificates and Cisco Secure Client certificates
- notifies users when these certificates are nearing their expiration date or have expired, and
- prevents disruptions in device operations due to certificate expiry.

Certificate monitoring scope and functionality

The management certificate is used for accessing FDM-managed and ASA devices from Security Cloud Control Firewall Management, while the Cisco Secure Client (formerly AnyConnect) is necessary for using virtual private network features on ASA, FDM-managed, and FTD devices from Security Cloud Control Firewall Management.

The management certificate expiry check applies to ASA and FDM-managed devices, while the Secure Client certificate expiry check applies to ASA, FDM-managed, and FTD devices.

View certificate expiry notifications

In the top right corner, click the **Notifications** ( ) icon to view the most recent alerts that have occurred or affected the devices you have onboarded to your tenant. The **High Priority** section displays the certificate expiration notifications.

These notifications are sent 30, 14, and 7 days before the certificate expiration date and then every day thereafter until the certificate either expires or is renewed with a valid certificate. You can also subscribe to receive these notifications by email on the **Notification Settings** section of the user preferences page. For more information, see User Notification Preferences.

Write a device note

Configure a device note in Security Cloud Control Firewall Management.

This task allows you to create a single, plain-text note file for a device to document important information or configuration details.

Use this procedure to create a single, plain-text, note file for a device.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.
4. Select the device or model you want to create a note for.
5. In the **Management** pane on the right, click **Notes**. Notes.
6. Click the editor button on the right and select the Default text editor, Vim, or Emacs text editors.

7. Edit the Notes page.
8. Click **Save**.

   The note is saved in the tab.

The device note is successfully created and saved, allowing you to document important information about the device for future reference.

Delete a device from Security Cloud Control Firewall Management

Configure device removal by deleting a device from Security Cloud Control Firewall Management.

This task removes a device from your security management platform to free up licensing or decommission unused devices.

Use this procedure when you need to permanently remove a device from your security infrastructure management. The device will no longer be monitored or managed after deletion.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Select the device you want to delete.
4. Click **Remove** in the **Device Actions** pane.
5. To confirm device removal, click **OK**.

   To keep the device onboarded, click **Cancel**.

   > **Note**
   >
   > Both devices in an FDM-managed high-availability (HA) pair must be deleted simultaneously. Click the FDM-managed HA pair name instead of selecting individual peers.

The device is permanently removed from Security Cloud Control Firewall Management and is no longer managed or monitored by the platform.

Back up Firewall Threat Defense devices

Configure backups for Firewall Threat Defense devices managed by Security Cloud Control Firewall Management.

Back up Firewall Threat Defense devices to ensure configuration data can be restored if needed.

Different backup procedures apply depending on how your Firewall Threat Defense devices are managed - through Cloud-Delivered Firewall Management Center, on-premises On-Premises Firewall Management Center, or Firewall Device Managers.

Procedure

1. For Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center, access the management interface.
   - In the Security Cloud Control left pane, choose **Administration** > **Firewall Management Center**.
   - Choose **Cloud-delivered FMC** under the **FMC** tab.
   - Click **Devices** on the right pane to navigate to the Cloud-Delivered Firewall Management Center.
   - Continue to follow the steps in Back Up a Threat Defense Device from Cloud-delivered Firewall Management Center.
2. For Firewall Threat Defense devices managed by On-Premises Firewall Management Center onboarded to Security Cloud Control Firewall Management, access the management center.
   - In the Security Cloud Control left pane, choose **Administration** > **Firewall Management Center**.
   - Choose the On-Premises Firewall Management Center whose Firewall Threat Defense devices you want to back up.
   - Click **FMC Cross Launch URL** on the right pane to navigate to the On-Premises Firewall Management Center or manually log in to the On-Premises Firewall Management Center.
   - Continue to follow the steps in *Back up a Device from the Management Center* in the Cisco Secure Firewall Management Center Administration Guide.
3. For Firewall Threat Defense devices managed by Firewall Device Managers onboarded to Security Cloud Control Firewall Management, use the FDM backup procedure.

   Follow the steps in Back up an FDM-managed Device.

Device configuration backups are created and available for restoration when needed. The backup location depends on the management type used for your devices.

Manage Firewall Threat Defense devices through Security Cloud Control Firewall Management

Configure Firewall Threat Defense device management through Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management provides a unified interface to manage Firewall Threat Defense devices, both in hardware and virtual formats.

Firewall Threat Defense devices associated with these three management applications can be managed on the Security Cloud Control platform:

- Secure Firewall Device Manager
- Secure Firewall Management Center
- Secure Cloud-Delivered Firewall Management Center

Procedure

1. Log in to the Security Cloud Control platform.

2. In the left pane, click **Security Devices**.
3. Click the **FTD** tab.
4. Click  at the top-left corner.

   Under **Devices/Services**, the filter pane provides filters that display Firewall Threat Defense devices based on the management application through which they are accessed from Security Cloud Control.

   - **FDM**: Firewall Threat Defense device managed by Firewall Device Manager
   - **FMC-FTD**: Firewall Threat Defense devices managed by Firewall Management Center
   - **FTD**: Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center

5. To view the Firewall Threat Defense devices under a management application, check the corresponding check box.

The Firewall Threat Defense devices associated with the selected management application are displayed.

Filter security devices by hardware end-of-life status

Configure the Hardware End-of-Life filter to identify devices nearing or reaching their last day of hardware support in Security Cloud Control.

Use the Hardware End-of-Life filter to identify devices that are approaching or have reached their hardware end-of-life date for support planning and risk mitigation. This helps ensure you maintain supported hardware configurations and avoid operational and security risks associated with unsupported devices.

Running unsupported hardware may pose operational and security risks because Cisco no longer provides software updates, security patches, or technical support after the EoL date.

> **Note**
>
> The Hardware EoL filter currently supports Firewall Threat Defense devices managed by On-Premises Firewall Management Center and Cloud-Delivered Firewall Management Center, and ASA devices.

Procedure

---

1. In the **Devices** tab, click the filter icon.
2. From the list of available filters, under **Device End-of-Life**, select **Hardware End-of-Life**.

   The list now displays all devices that are approaching or have reached their hardware end-of-life.

3. Select a device to view more information on the right pane.
4. Scroll down to the **Device End of Life** section to view the following details:

   - The exact end-of-life date.
   - Remaining time until the last day of support.

5. Click **Know more**.

   You can view a detailed page that provides the following information:

- Cisco's recommended replacement devices with product specifications, along with links to view the official data sheets.
- Guidance on submitting a request through the Contact Cisco page and options to connect directly with Cisco experts.
- Information on Cisco's product recycling program.

6. Click **Export** to download the device report in CSV format for offline analysis.

You have successfully filtered devices by hardware end-of-life status and can now view devices that require attention for support planning. You can also access detailed replacement information and export device reports for further analysis.

Security Cloud Control Firewall Management labels and filtering

Explains how to use Security Cloud Control Firewall Management labels to group devices and objects, create label groups, and filter device or object tables by assigned labels.

A label is a grouping mechanism that

- groups devices or objects for organizational purposes
- can be applied to one or more devices during onboarding or any time after onboarding
- enables filtering of device table or objects table contents using the corresponding label, and
- allows creation of label groups using the syntax group name:label.

Label application and filtering information

You can apply labels to objects after creating them. Once you apply labels to devices and objects, you can filter the contents of the device table or objects table using the corresponding label.

> **Note**
>
> A label that is applied to a device is not extended to its associated objects, and a label applied to a shared object is not extended to its associated objects.

You can create a label group by using the syntax group name:label, for example, Region:East or Region:West. If you create these two labels, the group label would be Region and you could choose from East or West in that group.

Apply labels to devices and objects

Configure labels for devices and objects to organize and categorize them within the inventory and objects management interface.

Applying labels helps organize and categorize devices and objects for easier identification and management within the system.

Labels provide a way to group and identify devices and objects based on their function, location, or other relevant criteria. You can apply labels to both devices in the inventory and objects in the objects management interface.

Procedure

1. In the left pane, click **Security Devices**.
2. In the left pane, click **Objects**.
3. Click the **Devices** tab to locate a device or the **Templates** tab to locate the model device.
4. Click the appropriate device type tab.
5. Select one or more devices.
6. In the **Add Groups and Labels** field on the right, specify a label for the devices.
7. Click the + icon.

The label is applied to the selected devices or objects and can be used for filtering and organizing items in the interface.

Labels and tags in AWS VPC

Explains how AWS VPC tags are represented as Security Cloud Control labels and the synchronization behavior between AWS and Security Cloud Control.

Labels and tags in AWS VPC are metadata management features that

- enable AWS VPC tags to be read and copied to Security Cloud Control's database during onboarding
- represent AWS tags as Security Cloud Control labels viewable on the **Security Devices** page, and
- require manual synchronization between Security Cloud Control and AWS console for any modifications.

Label synchronization behavior

When you onboard an AWS VPC to Security Cloud Control, Security Cloud Control reads all AWS VPC tags as part of the configuration. That is, they are copied from AWS and stored in Security Cloud Control's database. These tags are represented as Security Cloud Control labels, which can be viewed on the **Security Devices** page, just like labels on any other device type.

If you delete the existing labels or create new labels from Security Cloud Control, these changes are not synchronized to the AWS VPC. You must manually make the same changes using the AWS console. VPC Tags that are created or modified in the AWS console after the AWS VPC has been onboarded will not be stored in Security Cloud Control's copy of the configuration or detected as an out-of-band change.

Filters on security devices, policies, and objects page

Describes how to filter devices, policies, and objects by attributes such as device type, status, version, connector, management application, and labels.

Filters on security devices, policies, and objects page are navigation tools that

- help you find specific devices and objects by filtering based on various criteria
- allow filtering by attributes such as device type, hardware version, software version, Snort version, configuration status, connection state, conflict detection, Secure Device Connector, and labels, and
- are accessible through the filter icon in the left pane of the Security Devices, Policies, and Objects pages.

Filter functionality by device type

On the **Security Devices** page, the filter panel lets you filter devices by criteria such as device type, hardware version, software version, Snort version, configuration status, connection state, conflict detection, Secure Device Connector, and labels. You can apply filters within the selected device type tab.

When the **FTD** tab is open, the filter panel also lets you filter FTD devices by the management application that Security Cloud Control uses to access them.

To filter, click  in the left-hand pane of the Security Devices, Policies, and Objects tabs.

> **Note**
>
> When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from Security Cloud Control.
>
> - FDM: Devices managed using FTD API or Firewall Device Manager.
> - FMC-FTD: Devices managed using Firepower Management Center.
> - FTD: Devices managed using FTD Management.

Use Security Cloud Control Firewall Management search functionality

Explains how to search in Security Cloud Control Firewall Management using page-level search and global search to find devices, policies, objects, VPN entries, change logs, and jobs across your tenant.

The Security Cloud Control Firewall Management search functionality is a platform feature that

- provides a highly efficient search function that makes it easy to find anything you need,
- includes a search bar on each page that is tailored to the content of that page, and
- offers global search that allows for a comprehensive search across the entire tenant.

Search functionality benefits

This search functionality saves time and effort, as you can quickly locate the necessary information.

Use page level search

Configure page-level search to find specific items on Security Devices, Policies, Objects, VPN, Change Log, and Jobs pages.

Use page-level search to quickly locate specific devices, policies, objects, VPN configurations, or change log entries within the interface.

The page-level search enables you to search specific items on the Security Devices, Policies, Objects, VPN, Change Log, and Jobs pages.

- In the **Security Devices** space, you can simply start typing in the search bar, and devices that fit the search criteria will be displayed. You can type any partial part name of the device, IP address, or the serial number of the physical device to find the device.
- In the **Policies** space, you can search policies by their name, components or objects used in them.

- In the **Objects** space, you can search for an object by typing any partial part of the name of the object, or partial IP Address, port, or protocols.
- In the **VPN** space, you can search by tunnel name, device name, and IP address used in the VPN policies.
- In the **Change log** space, you can search logs based on events, device names, or actions.

Procedure

1. Navigate to the search bar near the top of the interface.
2. Type the search criteria into the Search Bar and the corresponding results will be displayed.

The search results display items that match your criteria, allowing you to quickly locate and select the specific device, policy, object, VPN configuration, or change log entry you need.

Global search

Describes a centralized search functionality that allows users to quickly locate and navigate to onboarded devices, objects, and policies in Security Cloud Control.

A global search is a centralized search functionality that

- allows you to search for onboarded devices and associated objects available within Security Cloud Control
- enables you to navigate to device and object pages directly from search results, and
- provides quick location and navigation to devices managed by Security Cloud Control.

Global search indexing options and supported entities

- Full Indexing–Requires that you invoke the full indexing process. This process scans all the devices and objects in the system and displays them in the search index only after you invoke the indexing. To invoke full indexing, you must have administrative privileges.

  For more information, see Initiate full indexing on page 857.

- Incremental Indexing–An event-based indexing process where the search index automatically updates each time that a device or an object is added, modified, or deleted.

The information that you enter in the search field is not case-sensitive. You can perform a global search using these entities:

- Device Name–Supports partial device names, URL, IP address, or range.
- Object Types–Supports object name, object descriptions, and configured values.
- Policy Types–Supports policy name, policy description, rule name, and rule comments.

  Cloud-Delivered Firewall Management Center and on-premises Firewall Management Center managed in Security Cloud Control support these policy types:

  - Access Control Policy
  - Prefilter Policy
  - Threat Defense NAT Policy

When you type a search expression, the interface begins to display search results and you do not need to press *Enter* to execute a search.

The search results display all devices and objects that match your search terms. If your search term matches more than one device or object, the results appear under categories such as devices, objects, and connected_fmc.

By default, the first item in the search result is highlighted and the related information for that item appears in the right pane. You can scroll through the search results and click any item to view the corresponding information. You can click the arrow icon besides the item to navigate to the corresponding page.

Note

Currently, Security Cloud Control supports global search for ASA, Cloud-Delivered Firewall Management Center, on-premises Firewall Management Center managed by Security Cloud Control, Firewall Threat Defense, and Meraki.

Global search is only available when Security Cloud Control Firewall Management has been onboarded to Security Cloud Control.

Note

- Global search does not display duplicate search results. For objects, the unique identifier of the shared object is used to navigate to the Object view.
- If you delete a device from Security Cloud Control, all associated objects are removed from the global search index.
- If you delete an object from the policy and retain the device before you initiate full indexing, the object remains in the global search index because it is associated with the device.

Initiate full indexing

Configure full indexing for global search functionality.

Initiate full indexing to enable global search capabilities for your tenant.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Administration** > **General Settings**.
3. In Global Search, click **Initiate Full Indexing** to trigger indexing.



> **Note**
>
> Initiating full indexing clears existing indexing of the Security Cloud Control tenant.

4. Click **here** to view the global search workflow.

Full indexing is initiated and global search functionality becomes available for your tenant.

Perform a global search

Configure global search to locate devices, objects, and policies across your Security Cloud Control environment.

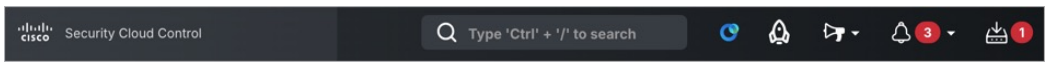
Use global search to quickly locate and navigate to specific devices, objects, policies, and Cloud-Delivered Firewall Management Center items across your environment.

Procedure

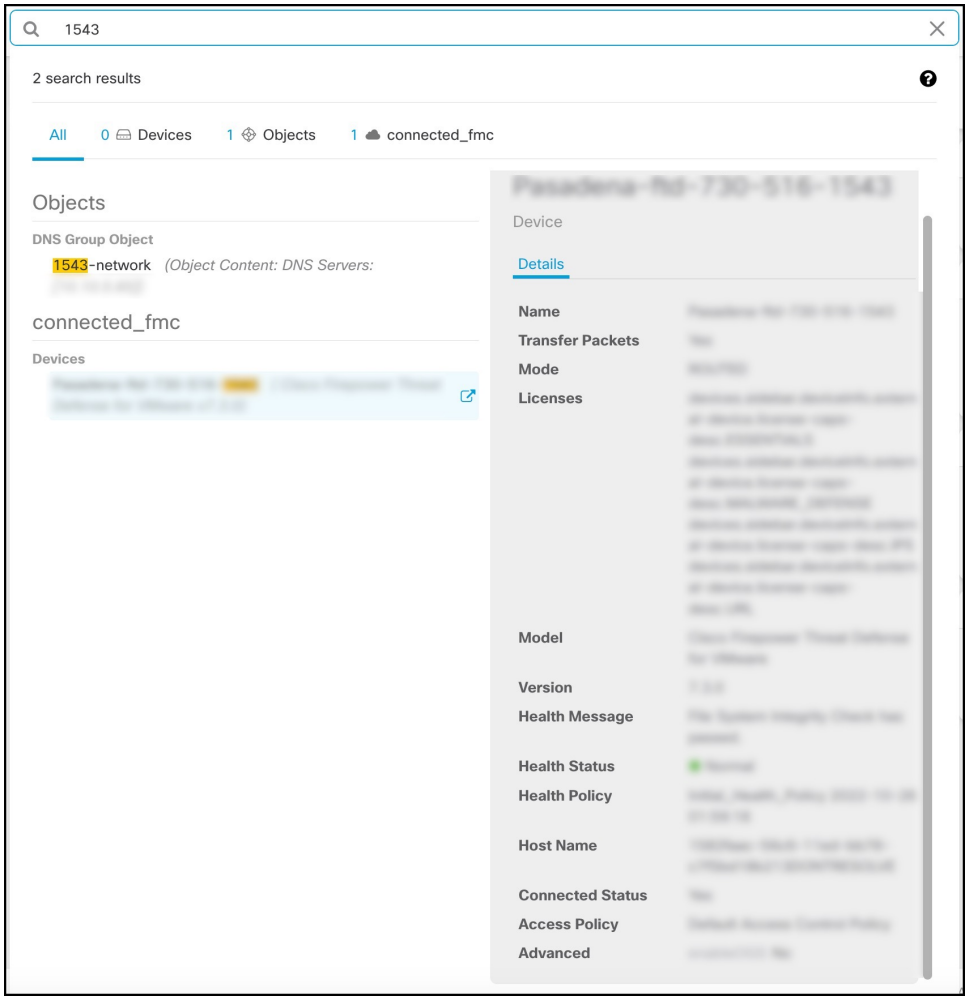
---

1. Log into Security Cloud Control.
2. Click the search icon in the Security Cloud Control page and enter the search strings in the search field that appears.

   Alternatively, you can press and hold the **Ctrl** key and the **/** key simultaneously on Windows, or the **Command** key and **/** key on Mac, to open the search bar.

   The search results display a list of possible items as you begin entering the search strings. The search results appear under four categories: All, Devices, Objects, Policies, and Cloud-Delivered Firewall Management Center. The right pane displays information for a selected search result.



3. From the search result, select a device or an object, and click the arrow icon to navigate from the search results to the corresponding device and object page. From the search result, select an item, and click the arrow icon to navigate from the search results to the corresponding page.

> **Note**
>
> Selecting a search result for devices in the Cloud-Delivered Firewall Management Center, allows you to navigate to the Cloud-Delivered Firewall Management Center user interface within Security Cloud Control.

4. Click **X** to close the search bar.

You have successfully performed a global search and navigated to the desired device, object, or policy page. The search bar is now closed.

48 Use the Security Cloud Control Command Line Interface Tool (CLI)

Topics:

- Use the command line interface on a single device
- Use the bulk command line interface
- Run a CLI macro
- Export command line interface results

You can use the Command Line Interface tool for managing or troubleshooting devices. The commands supported with this tool depend on the type of device. For the ASA, for example, you can use the full CLI. But for the Firewall Threat Defense, command support is limited to select **show** commands.

You can send commands to a single device or to multiple devices simultaneously.

See the following supported device types:

- ASA

  Commands are entered directly in global configuration mode. For detailed ASA CLI documentation, see ASA Command Line Interface Documentation on page 305.

- Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense

  Your command will be sent to either the Firewall Threat Defense CLI or the diagnostic CLI, depending on which command it is. Supported commands for Firewall Threat Defense are shown onscreen. These commands are a subset of commands that you can enter at the CLI. In addition, you cannot filter **show** command by piping the output (|) like you can directly at the CLI or in the Threat Defense CLI tool in the Cloud-Delivered Firewall Management Center.

  For diagnostic CLI output, see the ASA command reference guide.

  For Firewall Threat Defense CLI documentation, see Cisco Firepower Threat Defense Command Reference.

- FDM-managed Firewall Threat Defense

  Commands are entered at the Firewall Threat Defense CLI. You cannot access other modes. For Firewall Threat Defense CLI documentation, see Cisco Firepower Threat Defense Command Reference.

- Cisco IOS

  Commands are entered in user EXEC mode. You need to enter **enable** followed by **configure terminal** to execute them in Global Configuration mode. For Cisco IOS CLI documentation, see Networking Software (IOS & NX-OS) for your IOS version.

- SSH

Use the command line interface on a single device

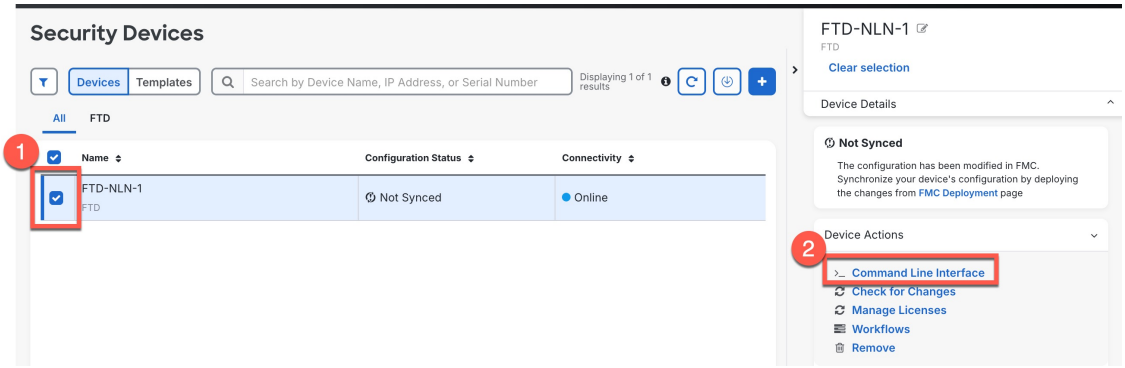
Configure the command line interface on a single device for ASA devices, including interface names, security levels, IP addressing, VLANs, and enablement options.

Use the Command Line Interface to execute commands directly on a single device and manage device configurations efficiently.

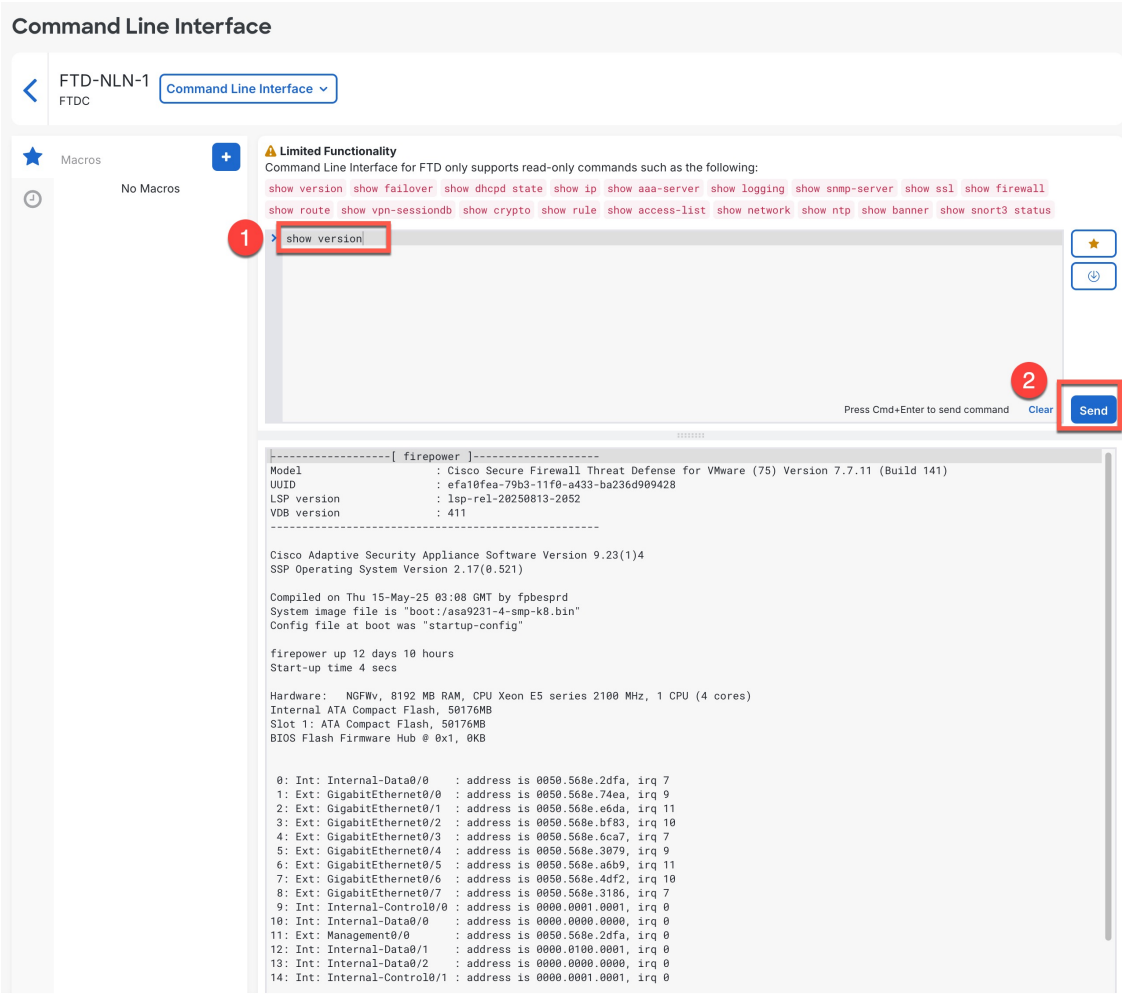
When you select a single device, you can enter one or more commands. You can also view and use command history to rerun a set of commands.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.
3. Click the **Devices** tab.
4. Select the device, and in the **Device Actions** pane, click **>_Command Line Interface.**



5. Enter one or more commands in the command pane, and click **Send**.



If there are limitations on the commands you can run, they appear in the area above the command pane.

The response to your commands is displayed in the response pane. If there is no output for a command (either it was executed successfully, or there was no output to show), you will see **Done!** in the results pane.

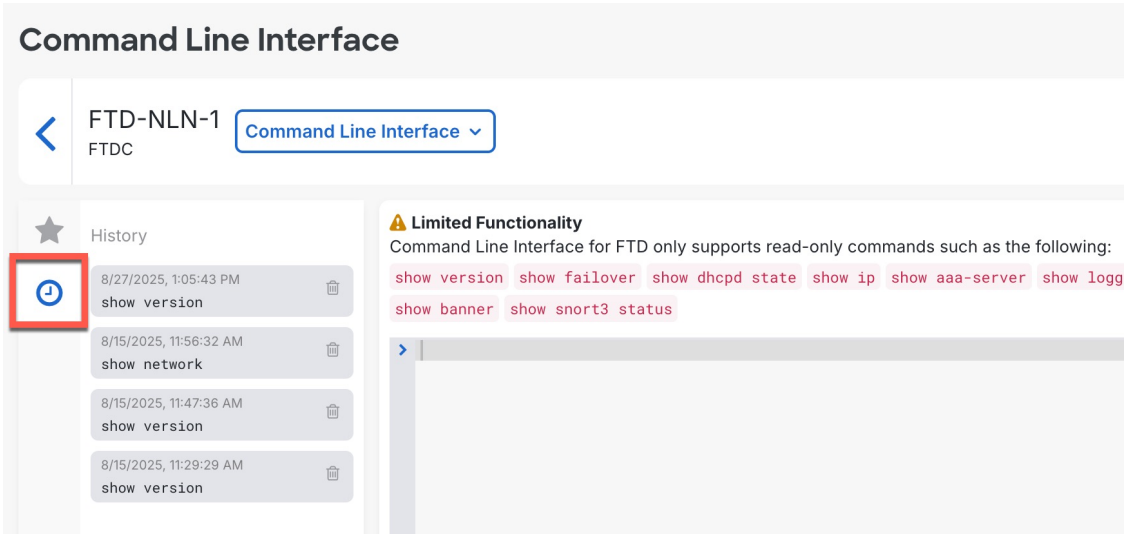
> **Note**
>
> If you enter a very long list of commands, you may exceed the limitations of Security Cloud Control's interface with the device. If you see an error, you can add extra blank lines between groups of commands so Security Cloud Control can send the commands in batches.

Example

This ASA example sends a batch of commands that creates three network objects and a network object group that contains those network objects.



6. After you send commands, Security Cloud Control records that command in the **History** pane. You can rerun the commands saved in the **History** pane or use the commands as a macro.
   a) Click the clock icon to open the **History** pane.



   b) Select the command in the **History** pane that you want to modify or resend.
   c) Reuse the command as it is or edit it in the command pane and click **Send**.

You can successfully execute commands on the selected device and reuse command history for efficient device management.

Use the bulk command line interface

Configure CLI commands to send to multiple same-type devices in Security Cloud Control, compare command responses by device or result, and reuse command history for repeated bulk tasks.

Send CLI commands to multiple devices of the same type at once for efficient bulk device management.

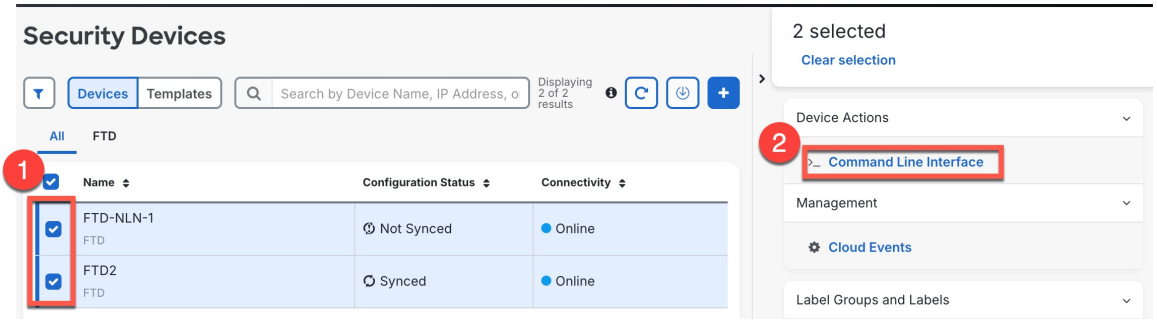
Use the bulk Command Line Interface to execute commands across multiple devices simultaneously rather than configuring each device individually.

Procedure

1. In the left pane, click **Security Devices**.

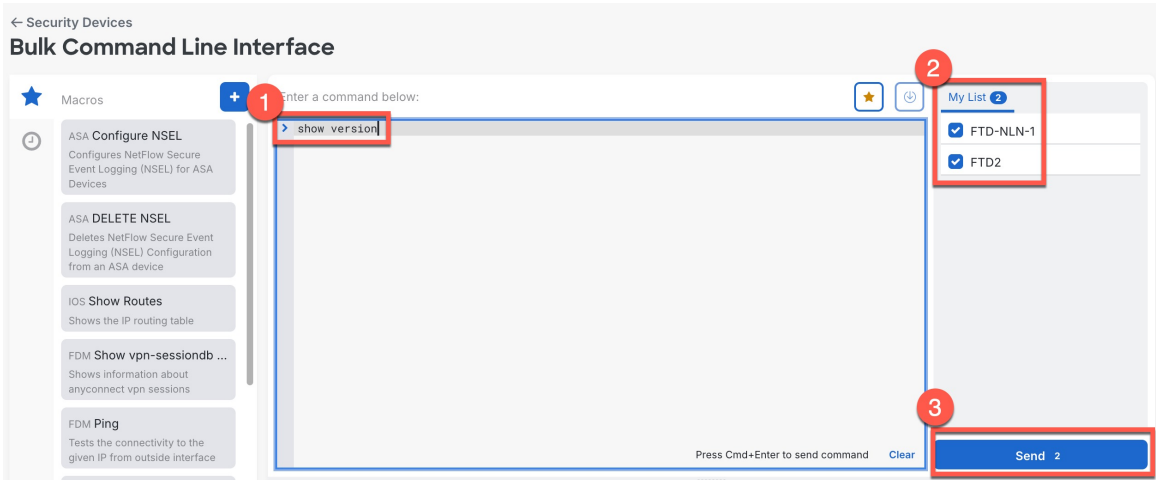
2. Click the **Devices** tab.
3. Select multiple devices of the same type, and in the **Device Actions** pane on the right, click **>_Command Line Interface**.

Figure 22: Open the command line interface



4. Enter one or more commands in the command pane, check or uncheck devices you want to send the commands to in the **My List** field, and click **Send**.

Figure 23: Command line interface



Note

If you enter a very long list of commands, you may exceed the limitations of Security Cloud Control's interface with the device. If you see an error, you can add extra blank lines between groups of commands so Security Cloud Control can send the commands in batches.

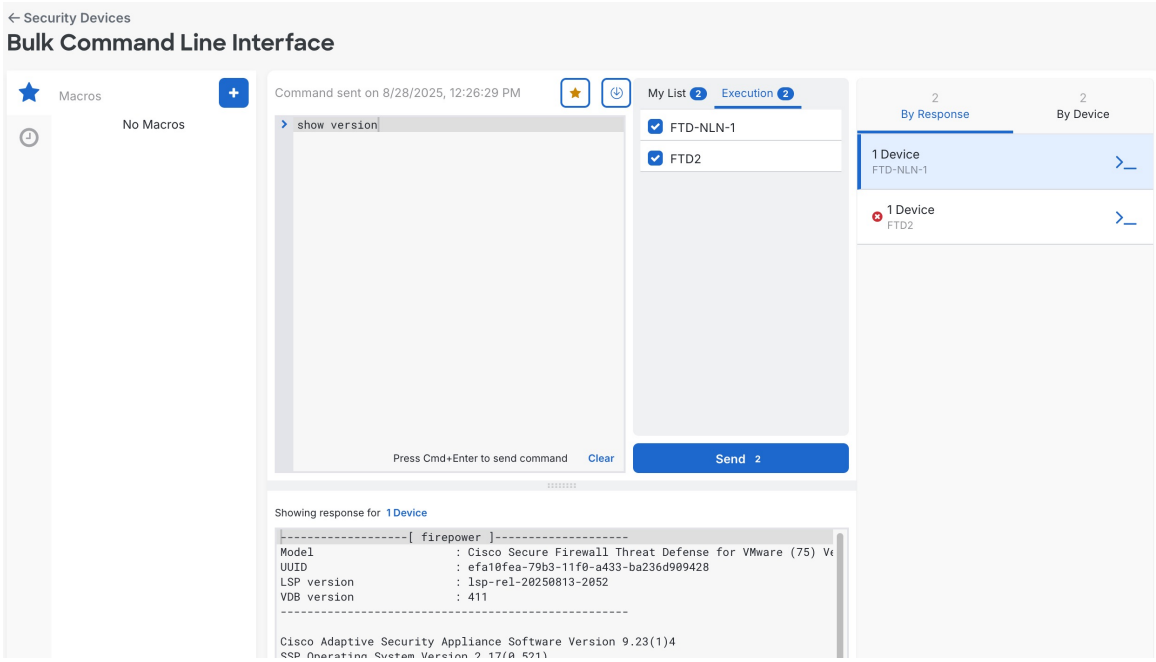
Note

For the ASA, if any of the selected devices are not synced, only certain commands are allowed: **show**, **ping**, **traceroute**, **vpn-sessiondb**, **changeto**, **dir**, **write**, and **copy**.

5. View the device output.

The **Execution** tab shows the devices where the commands were sent; this list should match the selected devices in **My List**.

Figure 24: Command line interface



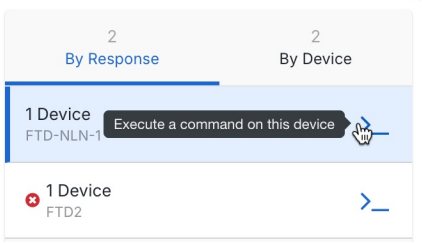
If there is no output for a command (either it was executed successfully, or there was no output to show), you will see `Done!` in the results pane.

The devices' response to the commands are displayed below in the response pane. If the response was the same for more than one device, the response pane displays the message "Showing Responses for X devices." Click **X Devices** to show all the devices that returned the same response in a pane to the right. Click **View Device** to go to that device in **Inventory**.

On the **By Response** tab, devices with identical responses are consolidated in a single row. Click a different row to show the response from other devices.

To re-run the command on the selected devices, click the prompt symbol to the right of the device row, and then click **Send**. You can change the commands you want to send or check and uncheck devices in the **My List** tab.

Figure 25: Execute a command

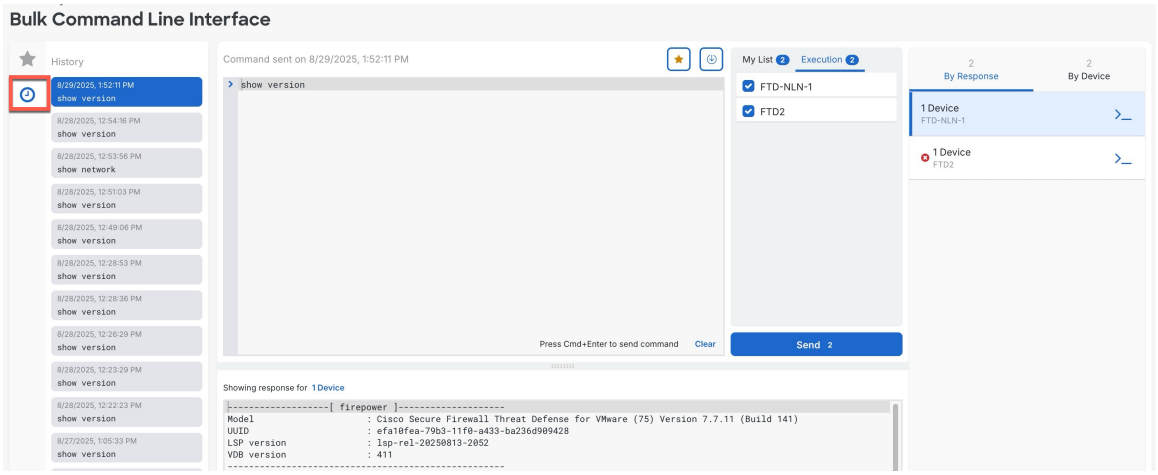


Click the **By Device** tab, and select a device to show only that device's command response.

6. After you send commands, Security Cloud Control records that command in the **History** pane. You can rerun the commands saved in the history pane or use the commands as a macro. The commands in the history pane are associated with the original devices on which they were run.

   a) Click the clock icon to open the **History** pane.

   Figure 26: History pane



b) Select the command in the **History** pane that you want to modify or resend.

Note that the command you pick is associated with specific devices (shown on the **Execution** tab) and not necessarily the ones you chose in the first step.

c) Click the **My List** tab to check or uncheck additional devices.

d) Reuse the command as it is or edit it in the command pane, and click **Send**.

Commands are sent to the selected devices and responses are displayed in the interface. Command history is saved for future reuse across the same device types.

Run a CLI macro

Configure CLI macros in Security Cloud Control to reuse prepared commands, define parameters, apply them to matching devices, and save configuration changes.

Run CLI macros to execute prepared commands on one or more devices of the matching type, with the ability to define parameters for customized execution.

A CLI macro is a fully-formed CLI command ready to use on one or more devices of the matching type.

For some device types, Security Cloud Control provides system-defined macros. System-defined macros cannot be edited or deleted.

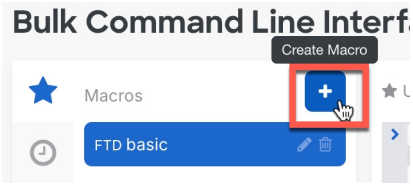
Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Select one or more devices of the same type, and in the **Device Actions** pane on the right, click **>_Command Line Interface**.

   You cannot create macros without first choosing a device.
4. Create a macro for this device type if one does not already exist.
   a) Add a macro in one of the following ways:

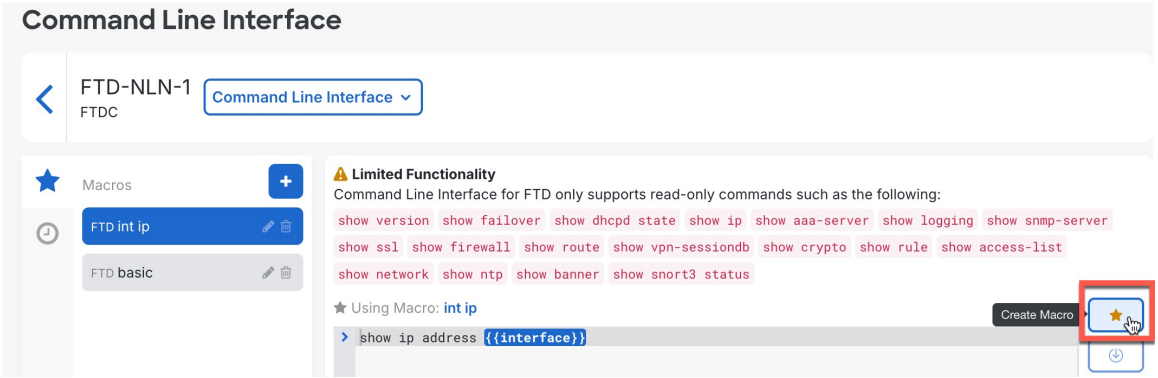
   - New macro–On the **Macros** tab (★), create a new macro by clicking the **Create Macro** (+) button.

   Figure 27: Create new macro



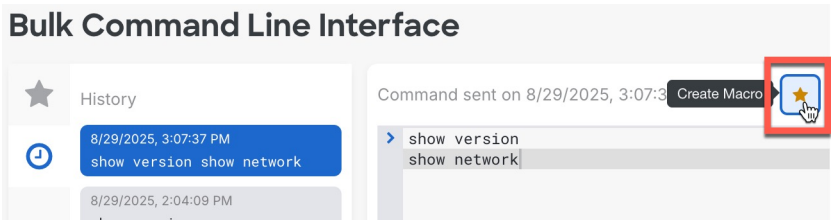
- From an existing macro–On the **Macros** tab (★), create a macro starting with the same commands by selecting a macro and then clicking the **Create Macro** (★) button.

Figure 28: Create macro from existing



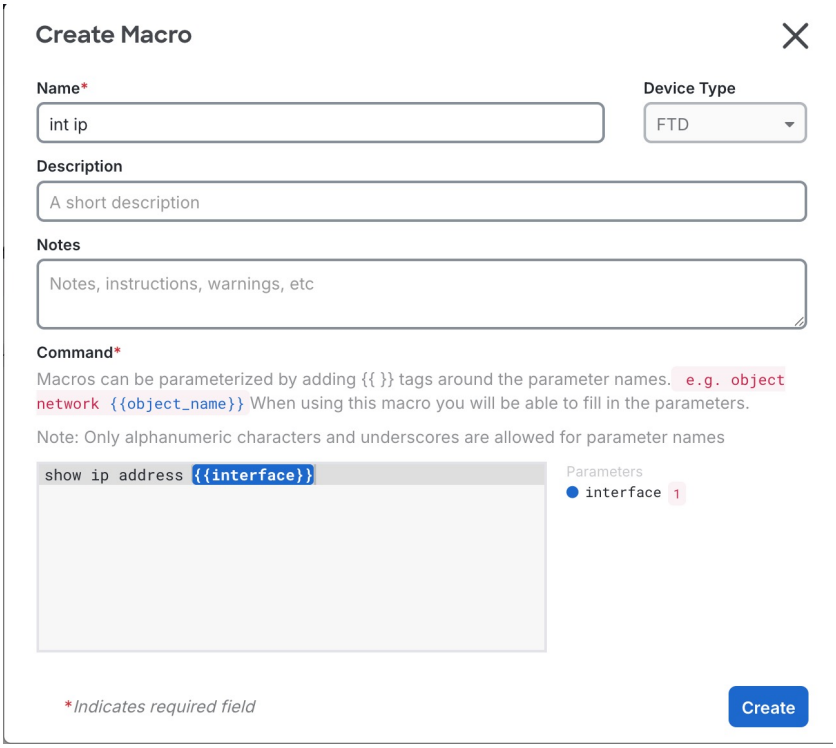
- From history–On the **History** tab (🕘), select a command you already ran, and then click **Create Macro** (★) button.

Figure 29: Create macro from history



b) Give the macro a unique name and provide an optional description and notes.

Figure 30: Create macro



c) Enter the commands in the **Command** field. For variables, enter the parameter surrounded by double curly brackets: **{{***parameter***}}**.

You will define the parameter before you run the macro.

```
> show running-config | grep {{username}}
```

You can name your parameters anything you want.

d) Click **Create**.

5. Click the star ★ to open the **Macros** tab, and select a macro from the list.

You can edit or delete a macro using the icons next to the macro name.

6. Run the macro one of two ways:

- If the macro has no parameters to define, click **Send**. The response to the command appears in the response pane. You're done.
- If the macro contains parameters, such as the Configure DNS macro below, click **>_ View Parameters.**



a) In the **Parameters** pane, fill in the values for the parameters in the **Parameters** fields.



b) Click **Send**.

7. Save configuration changes if you made any.

   After you send the command you may see the message, "Some commands may have made changes to the running config" along with two links.

   - Clicking **Write to Disk** saves the changes made by this command, and any other change that in the running config, to the device's startup config.
   - Clicking **Dismiss**, dismisses the message and does not save the configuration. You may lose the configuration changes if you reboot the device.

The CLI macro runs on the selected devices with the specified parameters, and any configuration changes can be saved to the device's startup configuration.

Export command line interface results

Configure export of Security Cloud Control CLI command results to a CSV file for offline filtering, sorting, and review by device, date, user, command, and output.

This task allows you to export CLI command results to a CSV file for offline analysis and record keeping.

You can export the results of CLI commands to a comma separated value (.CSV) file, so you can filter and sort the information in it. The exported information contains the following categories:

- Device
- Date
- User
- Command
- Output

Procedure

---

1. Run your commands according to Use the command line interface on a single device on page 862, Use the bulk command line interface on page 864, or Run a CLI macro on page 867, or choose a command from the **History** pane ( ).

2. Click the **Export results** () button.
3. Give the .CSV file a descriptive name and save the file to your local file system.

   When reading the command output in the .CSV file, expand all the cells to see all the results of the command.

The CLI command results are exported to a CSV file that you can open and analyze using spreadsheet applications for filtering, sorting, and offline review.

49 Manage CLI Templates

Topics:

- CLI templates
- Create a CLI template
- Edit a CLI template
- Export a CLI template
- Delete a CLI template

This chapter contains the following sections:

CLI templates

Explains CLI templates in Security Cloud Control, including how reusable command templates can be parameterized and exported for consistent configuration across multiple devices.

A CLI template is a predefined or user-created script that

- can be customized and exported to configure a wide range of devices
- allows you to parameterize the commands predefined for various scenarios, and
- enables you to quickly configure and provision a device.

CLI template capabilities

CLI templates in Security Cloud Control can be used for Cisco ASA and Cisco IOS devices, but are not limited to these. These templates allow you to configure devices even before onboarding them to Security Cloud Control or other platforms.

CLI Templates in Security Cloud Control allow you to:

- Create and access device configurations without onboarding a device
- Export the entire or partial device configurations
- Edit and remove device configurations

Create a CLI template

Configure a CLI template in Security Cloud Control by naming the template, entering configuration commands, adding parameter tags, and saving it for reuse.

Create a CLI template to standardize and reuse configuration commands across multiple devices.

Use this procedure to create a CLI template.

Procedure

1. Log into Security Cloud Control.
2. In the Security Cloud Control platform menu, choose **Products** > **Firewall**.
3. From the left pane, choose **Administration** > **Integrations** > **CLI Templates**.
4. On the **CLI Templates** page, click .
5. Give the template a unique name in the **Name** field.
6. (Optional) Provide a **Description** and **Notes** for the template.
7. In the **Command** field, enter your configuration commands to create a new template.

   You can add parameters in the template by adding {{}} tags around the parameter names. Only alphanumeric characters and underscores are allowed for parameter names.
8. Click **Create**.

The CLI template is created and saved for reuse across multiple devices with the specified configuration commands and parameters.

Edit a CLI template

Configure how to edit a CLI template in Security Cloud Control by selecting an existing template, updating its details or commands, adding parameters, and saving the changes.

Edit a CLI template to update template details, modify configuration commands, or add parameters as needed.

Use this procedure to edit a CLI template.

Procedure

1. Log into Security Cloud Control.
2. In the Security Cloud Control platform menu, choose **Products** > **Firewall**.
3. From the left pane, choose **Administration** > **Integrations** > **CLI Templates**.
4. On the **CLI Templates** page, select the template you want to edit.
5. Click the  icon on the selected CLI template.
6. On the **Edit Template** page, edit the **Name**, **Description**, and **Notes**, as required.
7. In the **Command** field, edit your configuration commands, as required.

   You can add parameters within the template by adding {{}} tags around the parameter names. Only alphanumeric characters and underscores are allowed for parameter names.
8. Click **Save**.

The CLI template is updated with your changes and is ready to be used for device configuration.

Export a CLI template

Configure the export of a CLI template in Security Cloud Control by entering required parameter values, reviewing the template, and downloading it as a .txt file for device configuration.

Export a CLI template as a .txt file to use for device configuration.

You can export a CLI template as a .txt file and use it to configure a device.

Procedure

1. Log into Security Cloud Control.
2. In the Security Cloud Control platform menu, choose **Products** > **Firewall**.
3. From the left pane, choose **Administration** > **Integrations** > **CLI Templates**.
4. On the **CLI Templates** page, select the template that you want to export.
5. Click **>_View Parameters**.
6. On the **Parameters** page, enter the values.
7. Click **Review**. Note that all the parameters must have values before exporting.
8. Click **Export results**.

   The .txt file with the template name is downloaded to your system.

The CLI template is exported as a .txt file and downloaded to your system for device configuration.

Delete a CLI template

Configure the deletion of a CLI template in Security Cloud Control by selecting an existing template from the CLI Templates page and removing it.

Delete a CLI template that is no longer needed or required for configuration management.

Use this procedure to delete a CLI template.

Procedure

1. Log into Security Cloud Control.
2. In the Security Cloud Control platform menu, choose **Products** > **Firewall**.
3. From the left pane, choose **Administration** > **Integrations** > **CLI Templates**.
4. On the **CLI Templates** page, select the template that you want to delete.
5. Click the icon on the selected CLI template.
6. Click **Remove**.

The CLI template is permanently deleted from the system.

50 Migrate Firewalls with the Migration Tool in Security Cloud Control

Topics:

- Firewall migration tool guide audience
- Firewall migration tool in Security Cloud Control
- Migrate Secure Firewall ASA to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control
- Migrate Microsoft Azure Native Firewall with the Firewall Migration Tool in Security Cloud Control
- Migrate FDM-Managed Device to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control
- Migrate Check Point Firewall to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control
- Migrating Check Point Firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control
- Migrate Fortinet Firewall with the Firewall Migration Tool in Security Cloud Control
- Migrating Fortinet firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control
- Migrate Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control
- Migrate Secure Firewall ASA to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control
- Migrate Palo Alto Networks Firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control
- Related documentation

This chapter provides steps for migrating Cisco firewalls and third-party firewalls to Security Cloud Control using Secure Firewall migration tool.

Firewall migration tool guide audience

Describes who should use the Firewall Migration Tool guide, including users migrating Secure Firewall ASA, FDM-managed threat defense, or third-party firewall configurations to Cisco Secure Firewall Threat Defense managed byCloud-Delivered Firewall Management Center.

The Firewall Migration Tool guide is a documentation resource that assists specific users in migrating firewall configurations to Cisco Secure Firewall Threat Defense.

Target audience

This guide is for you if you use Security Cloud Control to manage your Secure Firewall ASA devices and FDM-managed threat defense devices or you use third-party firewalls such as Palo Alto Networks, Check Point, and Fortinet firewalls and you want to move into the Cisco Secure Firewall Threat Defense. You can migrate all your existing firewall configurations to a threat defense device managed by your Cloud-Delivered Firewall Management Center using the Secure Firewall migration tool in Security Cloud Control. This document describes what you need to do to migrate your configurations.

Firewall migration tool in Security Cloud Control

Explains the Firewall Migration Tool hosted on Security Cloud Control and how to access it.

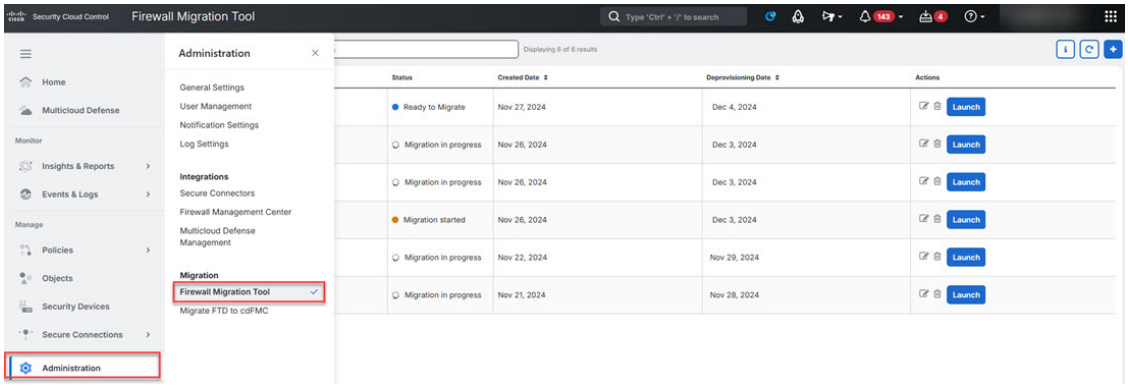
The Firewall Migration Tool in Security Cloud Control is a cloud-based migration service that

- extracts device configurations from source devices or uploaded configuration files
- migrates validated configurations to Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant, and
- eliminates the need to download and maintain the desktop version of the Secure Firewall migration tool.

Migration workflow and supported configurations

When you initialize a new migration in **Administration** > **Migration** > **Firewall Migration Tool** and **Launch** it, a cloud instance of the migration tool opens in a new browser tab and enables you to perform your migration tasks using a guided workflow.

The migration tool supports most configurations; unsupported configurations must be manually configured in the Cloud-Delivered Firewall Management Center. See Supported configurations on page 879.



You can migrate Cisco and third-party firewall configurations to Secure Firewall Threat Defense devices:

- Cisco Secure Firewall ASA
- Secure Firewall Threat Defense managed by Firewall Device Manager

- Check Point firewall
- Palo Alto Networks firewall
- Fortinet firewall

Important

You need an admin or a super admin user role in Security Cloud Control to be able to use the Firewall migration tool.

Supported configurations

Lists all the configurations supported by the Cisco Secure Firewall Migration Tool hosted on Security Cloud Control.

The migration tool supports the configurations that enable you to migrate network objects, services, access rules, NAT configurations, routing, interfaces, VPN settings, and dynamic routing protocols from source firewalls to the management center.

The migration tool supports these configurations:

- Network objects and groups
- Service objects, except those configured for a source and destination
- Referenced ACL and NAT rules
- Service object groups

> **Note**
>
> Nested service object group contents are broken down to individual objects before being migrated, because the cloud-delivered management center does not support nesting.

- IPv4 and IPv6 FQDN objects and groups
- IPv6 conversion (interface, static routes, objects, ACL, and NAT)
- Access rules applied to ingress interfaces
- Global ACLs
- Auto NAT, manual NAT, and object NAT
- Static routes, equal-cost multipath (ECMP) routes, and policy-based routing (PBR)
- Physical interfaces
- Sub-interfaces
- Port channels
- Virtual tunnel interface
- Bridge groups in transparent mode
- IP SLA objects - the migration tool creates them, maps them with static routes, and migrates them
- Time-based objects

- Site-to-site VPN
  - Site-to-Site VPN–When the Firewall migration tool detects crypto-map configuration in the source ASA, FDM-managed device, Palo Alto Networks firewall, or Fortinet firewall, the Secure Firewall migration tool migrates it AS a point-to-point topology to the management center VPN
  - Crypto-map (static/dynamic)-based VPN from ASA, FDM-managed devices, Palo Alto Networks firewall, and Fortinet firewall
  - Route-based (VTI) ASA and FDM VPN
  - Certificate-based VPN migration from ASA, FDM-managed device, Palo Alto Networks firewall, Fortinet firewall

    Important

    If you have site-to-site VPN configurations in your source ASA, FDM-managed device, Palo Alto Networks firewall, or Forinet firewall, ensure that their device trustpoint or certificates are configured manually in the cloud-delivered FMC.

- Remote-access VPN
  - SSL and IKEv2 protocols
  - Authentication methods–AAA only, client certificate only, SAML, AAA, and client certificate
  - AAA–Radius, local, LDAP, and AD
  - Connection profiles, group policy, dynamic access policy, LDAP attribute map, and certificate map
  - Standard and extended ACL
  - Custom attributes and VPN load balancing

  Important

  If you have configured remote-access VPN in your source firewall, ensure these tasks are performed:
  - Configure the ASA,FDM-managed device, Palo Alto Networks, and Fortinet firewall trustpoints manually on the management center AS PKI objects
  - Retrieve AnyConnect packages, Hostscan files (dap.XML, data.XML, hostscan package), external browser package, and AnyConnect profiles from the source ASA and FDM-managed device
  - Upload all AnyConnect packages and profiles to the management center

- Dynamic route objects, BGP, and EIGRP
  - Policy list
  - Prefix list
  - Community list
  - Autonomous system (AS) path
  - Route map

> **Note**
>
> The migration tool analyzes all objects and object groups based on both their name and configuration, and reuses objects that have the same name and configuration; however, XML profiles in remote access VPN configurations are validated only using their name.

Refer to *Cisco Secure Firewall Migration Tool Compatibility Guide* for more information.

Licenses

Lists the license requirements for accessing and using the Secure Firewall migration tool.

The Secure Firewall migration tool does not require any additional license to be accessed from Security Cloud Control.

However, you need to have a Security Cloud Control base subscription and licenses for the Firewall Threat Defense features you want to migrate.

Initialize a new migration instance

Configure a new migration instance in the Firewall migration tool hosted in Security Cloud Control.

This task creates a new migration instance that allows you to migrate firewall configurations using the Firewall migration tool.

The Firewall migration tool enables you to create up to 10 migrations and launch all of them concurrently. Each migration instance opens up in a new browser tab. If there are several users provisioned on your tenant, note that you can launch only migrations that you created.

Procedure

1. Log in to your Security Cloud Control tenant.
2. From the Security Cloud Control Home page, click **Firewall**.
3. Choose **Administration** > **Migration** > **Firewall Migration Tool**.
4. Click the blue plus button to initialize a new migration instance.

   > **Note**
   >
   > The Firewall migration tool enables you to create up to 10 migrations and launch all of them concurrently–each migration instance opens up in a new browser tab. However, if there are several users provisioned on your tenant, note that you can launch only migrations that you created.

   If you want to initialize a new migration instance when you already have 10 migrations, delete one of the existing migration instances.
5. Security Cloud Control generates a name for your migration automatically; you can use the auto-generated name or change it to suit your needs.
6. Click **OK** and wait until you see the status change from **Initializing** to **Ready to Migrate**.

Security Cloud Control also notifies you with a new announcement on the **Notifications** pane when your migration is ready.

7. On the new migration, click **Launch**.

   The migration tool opens in a new browser tab and does not require any authentication.

   > **Note**
   >
   > Migrations in Security Cloud Control are valid for seven days from the date of being created, after which they are automatically deprovisioned. This ensures that Security Cloud Control resources are freed up from time to time. You can check the dates in the **Created Date** and **Deprovisioning Date** columns.

   Security Cloud Control displays the status of all the migrations in the **Status** column; you can filter out the migrations based on the their statuses. You can also select a migration to see migration details, such as date and time of creation, date and time of start, source and destination device names, and created by on the right pane. Note that when several users are provisioned on your Security Cloud Control tenant, you can only launch migrations you created.

The Firewall migration tool opens in a new browser tab and is ready for use. The migration instance is now initialized and you can begin configuring your firewall migration.

Delete a migration instance

Configure the deletion of a migration instance to manually deprovision your migration before automatic deprovisioning occurs.

Delete a migration instance when you want to manually deprovision your migration before Security Cloud Control automatically deprovisions it, such as after your migration tasks are finished.

You can delete a migration instance to manually control the deprovisioning process rather than waiting for automatic deprovisioning.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Migration** > **Firewall Migration Tool**.
3. On the migration you want to delete, click **Delete** under the **Actions** pane.
4. Confirm your action by clicking **Delete**.

The migration instance is deleted and deprovisioned.

Demo mode in secure firewall migration tool

Explains the demo mode feature in Secure Firewall Migration Tool, which allows trying a hands-on demo migration using dummy devices and visualizing how the actual migration flow behaves.

Demo mode is a Secure Firewall Migration Tool feature that

- provides an opportunity to perform a demo migration using dummy devices and visualize how an actual migration flow would look like
- allows leveraging the whole feature set of the Secure Firewall Migration Tool, except pushing of configurations, and

- enables a trial run of the end-to-end migration procedure before performing your actual migration.

Demo mode access and workflow

When you launch the Secure Firewall Migration tool and are on the **Select Source Configuration** page, you can choose to start performing a migration using **Start Migration** or enter the **Demo Mode**.

The migration tool triggers the demo mode based on the selection you make in the **Source Firewall Vendor** drop-down; you can also upload a configuration file or connect to a live device and continue with the migration. You can proceed performing the demo migration by selecting demo source and target devices such as demo FMC, demo FTD devices, or Multicloud Defense.

> ⚠ **Caution**
>
> Choosing **Demo Mode** erases existing migration workflows, if any. If you use the demo mode while you have an active migration in **Resume Migration**, your active migration is lost and needs to be restarted from first, after you use the demo mode.

Migrate Secure Firewall ASA to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control

Learn how to migrate Secure Firewall ASA configurations to Secure Firewall Threat Defense using the Firewall Migration Tool in Security Cloud Control, including source selection, interface mapping, validation, and deployment.

The Secure Firewall migration tool in Security Cloud Control lets you to migrate configurations from live ASA devices that are managed by Security Cloud Control or using a configuration file extracted from an ASA device. To read more about the Secure Firewall ASA configurations supported for migration, see ASA Configuration Support in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book.

Select Source Configuration

After launching your migration instance from Security Cloud Control, choose **Cisco ASA** in **Select Source Configuration** and click **Start Migration**. You can either manually upload an ASA configuration file or choose any one of the Security Cloud Control-managed ASA devices listed on the **Connect to ASA** pane. If you are trying to select a Security Cloud Control-managed device, note that devices having **Configuration Status** as **Synced** are only listed by the migration tool; if you do not see the device you want to migrate in the list, check if the device configuration changes are up-to-date and synced with Security Cloud Control. Note that one ASA device can be selected as the source device by more than one user at the same time and the confuguration extraction takes place seamlessly. If you have one or more security contexts configured on your ASA device, the migration tool allows you to choose which context you want to migrate; you can also merge all your contexts to a single instance and then migrate them. Refer Select the ASA Primary Security Context for more information.

The migration tool parses the device configuration and displays a summary containing the parsed configurations. Click **Next**.

Select Target

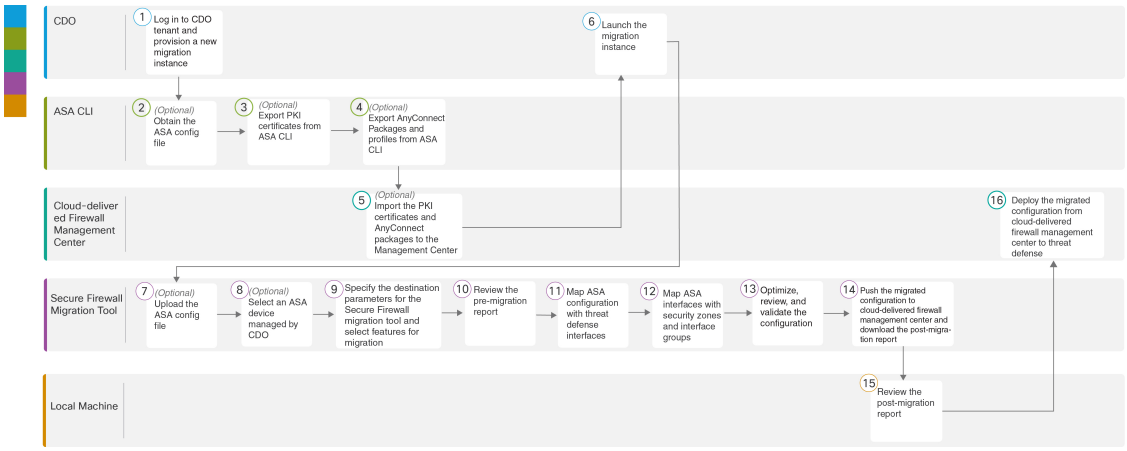
In the **Select Target** page, the Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant is selected by default, and the Firewall Threat Defense devices managed by that management center are listed. You can choose the Firewall Threat Defense device you wish to migrate your ASA configuration to or choose to **Proceed without FTD**. Note that the threat defense devices listed are displayed either as **In Use** or **Available** based on whether the device is being used in another migration instance. However, you can perform an override by clicking **Change Device Status**, selecting the device from the **In Use** list, and clicking **Continue**, which will make the device available for being selected as the target.

> **Caution**
>
> Changing the device status from **In Use** to **Available** impacts the ongoing migration instance that is using the device already. We recommend that you exercise caution when doing this.

Choosing **Proceed without FTD** pushes only NAT objects, ACLs, and port objects to the Cloud-Delivered Firewall Management Center. For more information about the commonly used ASA features and their equivalent threat defense features, see Cisco Secure Firewall ASA to Threat Defense Feature Mapping guide.

The flowchart that follows illustrates the step-by-step procedure for migrating an ASA to Firewall Threat Defense using the Firewall migration tool in Security Cloud Control.

Figure 31: End-to-End Procedure for ASA to FTD Migration with Firewall Migration Tool in Security Cloud Control



To perform the procedure with more detailed steps, continue to Obtain the ASA Configuration File in the Migrating Cisco Secure Firewall ASA to Threat Defense with the Migration Tool guide.

	Workspace	Steps
1	Security Cloud Control	Log in to your Security Cloud Control tenant, navigate **Administration** > **Migration** > **Firewall Migration Tool**, and click the blue plus button to start provisioning a new migration instance.
2	ASA CLI	(Optional) Obtain the ASA configuration file: To obtain the ASA config file from ASA CLI, see Obtain the ASA Configuration File. If you intend to select a Security Cloud Control-managed ASA device in the **Select Source Configuration**, skip to Step 3.
3	ASA CLI	(Optional) Export public key infrastructure (PKI) certificates from ASA CLI: This step is required only if you are planning to migrate site-to site VPN and RAVPN configurations from ASA to threat defense. To export the PKI certificates from ASA CLI, see Export PKI Certificate from ASA and Import into Management Center. If you do not have remote-access VPN configurations on your device or you are not planning to migrate site-to-site VPN and remote-access VPN, skip to Step 7.

	Workspace	Steps
4	ASA CLI	(Optional) Export AnyConnect packages and profiles from ASA CLI: This step is required only if you are planning to migrate remote-access VPN features from ASA to threat defense. To export AnyConnect packages and profiles from ASA CLI, see Retrieve AnyConnect Packages and Profiles.
5	Cloud-Delivered Firewall Management Center	(Optional) Import the PKI certificates and AnyConnect packages to the management center: To import the PKI certificates to management center, see Step 2 in Export PKI Certificate from ASA and Import into Management Center and Retrieve AnyConnect Packages and Profiles.
6	Security Cloud Control	Ensure that the status of the migration instance you created is **Ready to Migrate** and click **Launch**; the Secure Firewall Migration Tool opens in a new browser tab.
7	Secure Firewall Migration Tool	(Optional) Upload the ASA config file obtained from ASA CLI, see Upload the ASA Configuration File. If you are planning to migrate configuration from an ASA device managed by Security Cloud Control, skip to Step 8.
8	Secure Firewall Migration Tool	From the list of ASA devices shown, that are managed by your Security Cloud Control tenant, select the device whose configuration you want to migrate. If you have configured more than one security context on your ASA device, select the context you wish to migrate or choose to merge all the contexts to a singe instance in the **Primary Context Selection**drop-down. See Select the ASA Primary Security Context for more information.
9	Secure Firewall Migration Tool	On the **Select Target** page, the Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant is selected by default.
10	Secure Firewall Migration Tool	Select a target device from the list of threat defense devices managed by your Cloud-Delivered Firewall Management Center or choose **Proceed without FTD** and proceed.
11	Secure Firewall Migration Tool	Download the pre-migration report and review it for a detailed summary of the parsed configuration. For detailed steps, see Review the Pre-Migration Report.
12	Secure Firewall Migration Tool	**Map FTD Interface** with the ASA configuration. Because the names of physical and port channel interfaces on your ASA and threat defense devices are not always the same, you can select to which interface in the target threat defense device you want an ASA interface to get mapped. For more information, see Map ASA Configurations with Secure Firewall Device Manager Threat Defense Interfaces.
13	Secure Firewall Migration Tool	Map ASA interfaces to existing threat defense security zones and interface groups. See Map ASA Interfaces to Security Zones and Interface Groups for detailed steps.
14	Secure Firewall Migration Tool	**Optimize, Review and Validate Configuration** with caution and ensure ACLs, objects, NAT, interfaces, routes, site-to-site VPN, and remote-access VPN rules are configured as intended for the destination threat defense device. See Optimize, Review and Validate the Configuration.
15	Secure Firewall Migration Tool	Once your configuration validation is a success, **Push Configuration** to the Cloud-Delivered Firewall Management Center. For more information, see Push the Migrated Configuration to Management Center.

	Workspace	Steps
16	Local Machine	Download the post-migration report and review it. To know more on what information the post-migration report contains, see Review the Post-Migration Report and Complete the Migration.
17	Cloud-Delivered Firewall Management Center	Deploy the newly migrated configuration to the threat defense device.

Migrate Microsoft Azure Native Firewall with the Firewall Migration Tool in Security Cloud Control

Configure Microsoft Azure Native Firewall configurations to migrate to Secure Firewall Threat Defense using the Firewall Migration Tool in Security Cloud Control.

This task allows migrating configurations from Azure firewall to threat defense devices managed by your Cloud-Delivered Firewall Management Center. You can manually derive the configuration file from your Azure firewall and upload it to the migration tool to begin your migration.

The Firewall migration tool in Security Cloud Control enables configuration upload, target selection, validation, and deployment. To learn about supported Azure firewall configurations, see Azure Configuration Support.

Procedure

1. On the **Select Source Configuration** page, choose **Microsoft Azure** and click **Start Migration**.
2. Click **Upload** to choose the Azure configuration file and click **Next**.
3. In the **Select Target** page, select the Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant.

   The threat defense devices managed by that management center are listed. You can choose the threat defense device you wish to migrate the configuration to, and proceed with the migration.

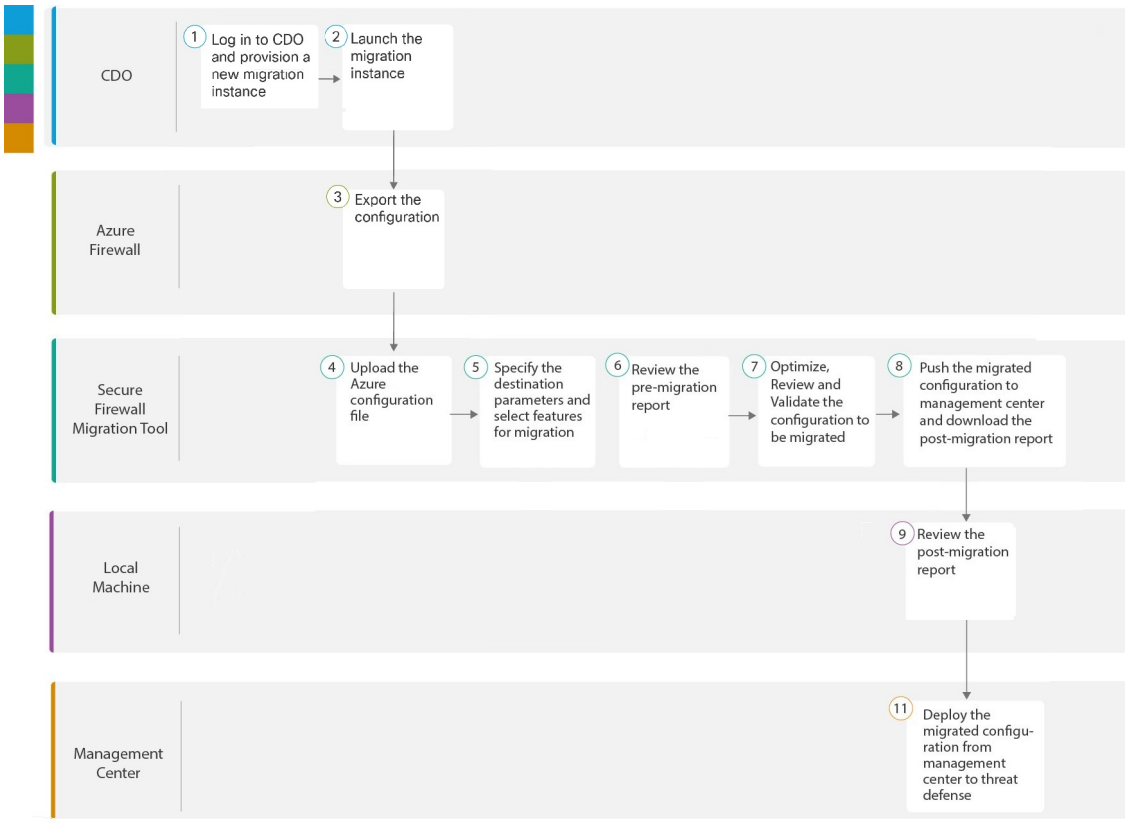
   The threat defense devices listed are displayed either as **In Use** or **Available** based on whether the device is being used in another migration instance. However, you can perform an override by clicking **Change Device Status**, selecting the device from the **In Use** list, and clicking **Continue**, which will make the device available for being selected as the target. Choosing **Proceed without FTD** pushes only NAT objects, ACLs, and port objects to the Cloud-Delivered Firewall Management Center. For more information about the commonly used ASA features and their equivalent threat defense features, see Cisco Secure Firewall ASA to Threat Defense Feature Mapping guide.

   > ⚠ **Caution**
   >
   > Changing the device status from **In Use** to **Available** impacts the ongoing migration instance that is using the device already. We recommend that you exercise caution when doing this.

   The flowchart that follows illustrates the step-by-step procedure for migration of Azure firewall configurations to threat defense devices:

To perform the procedure with more detailed steps, continue to Export the Configuration from Microsoft Azure Native Firewall in *Migrating Microsoft Azure Native Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool* guide.

Figure 32: Fortinet firewall to multicloud defense End-to-End migration



	Workspace	Steps
1	Security Cloud Control	Log in to your Security Cloud Control tenant, and in the left pane, click **Administration** > **Migration** > **Firewall Migration Tool** and click the blue plus button to start provisioning a new migration instance.
2	Security Cloud Control	After your migration instance is ready, click **Launch** and choose **Microsoft Azure**.
3	Azure Firewall	Export the Azure configuration to the local system. To export the configuration from Azure firewall, see Export the Configuration from Microsoft Azure Native Firewall.
4	Secure Firewall Migration Tool	Upload the Azure configuration file exported from Azure firewall, see Upload the Microsoft Azure Configuration File.
5	Secure Firewall Migration Tool	In this step, you can specify the destination parameters for the migration. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool.
6	Secure Firewall Migration Tool	Navigate to where you downloaded the pre migration report and review the report. For detailed steps, see Review the Pre-Migration Report.

	Workspace	Steps
7	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. For detailed steps, see Optimize, Review and Validate the Configuration to be Migrated.
8	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to management center and allows you to download the post-migration report. For detailed steps, see Push the Migrated Configuration to Management Center.
9	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
10	Cloud-Delivered Firewall Management Center	Deploy the migrated configuration from the Cloud-Delivered Firewall Management Center to threat defense.

The Microsoft Azure Native Firewall configuration is successfully migrated to Secure Firewall Threat Defense, with the configuration validated and deployed through the Firewall Migration Tool.

Migrate FDM-Managed Device to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control

Learn how to migrate FDM-managed device configurations to Secure Firewall Threat Defense using the Firewall Migration Tool in Security Cloud Control , including source selection, configuration upload, validation, and deployment.

You can migrate FDM-managed device configurations using configuration files or by simply selecting the FDM-managed devices that are onboarded to Security Cloud Control . To read more about the FDM-managed device configurations supported for migration, see FDM-Managed Device Configuration Support in *Migrating an FDM-Managed Device to Secure Firewall Threat Defense with the Migration Tool* book.

Select Source Configuration

After launching your migration instance from Security Cloud Control , choose **Cisco Secure Firewall Device Manager** in **Select Source Configuration** and choose from of the following options:

- **Migrate Firepower Device Manager (Shared Configurations Only)**
- **Migrate Firepower Device Manager (Includes Device & Shared Configurations)**
- **Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)**

On clicking **Continue** , the migration tool enables you to either manually upload an FDM-managed device configuration file or choose any one of the FDM-managed devices onboarded to Security Cloud Control , which are listed on the **Connect to FDM** pane and click **Next** .

Select Target

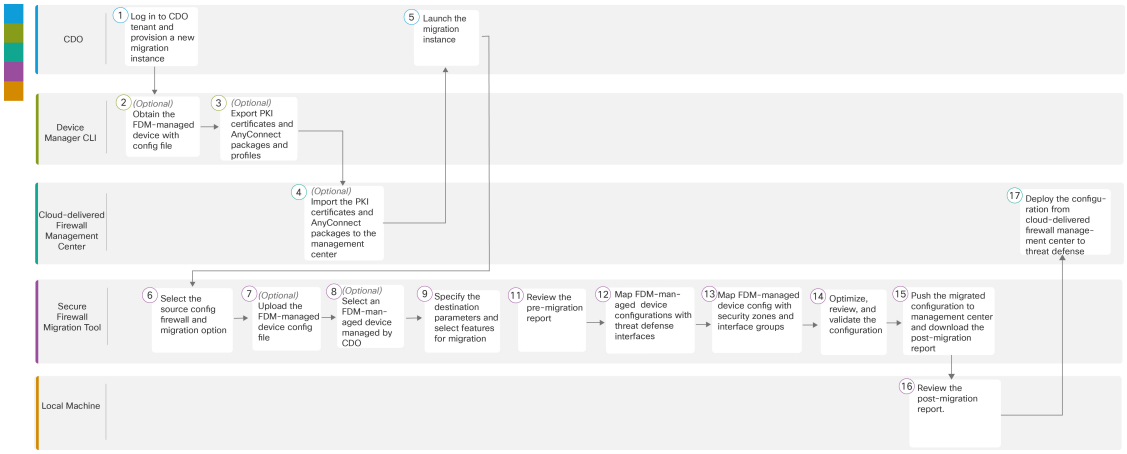
In the **Select Target** page, the Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant is selected by default, and the Firewall Threat Defense devices managed by that management center are listed. You can choose the Firewall Threat Defense device you wish to migrate the configuration to, and proceed with the migration.

Note that the threat defense devices listed are displayed either as **In Use** or **Available** based on whether the device is being used in another migration instance. However, you can perform an override by clicking **Change Device Status** , selecting the device from the **In Use** list, and clicking **Continue** , which will make the device available for being selected as the target.

> **Caution**
>
> Changing the device status from **In Use** to **Available** impacts the ongoing migration instance that is using the device already. We recommend that you exercise caution when doing this.

The flowchart that follows illustrates the step-by-step procedure for migrating an FDM-managed device using the Firewall migration tool in Security Cloud Control .

Figure 33: End-to-End Procedure for FDM-Managed Devices to FTD Migration with the Firewall Migration Tool in Security Cloud Control



To perform the procedure with more detailed steps, continue to Obtain the FDM-managed Device Configuration File in the Migrating an FDM-managed Device to Secure Firewall Threat Defense with the Migration Tool guide.

	Workspace	Steps
1	Security Cloud Control	Log in to your Security Cloud Control tenant, and in the left pane, click **Administration** > **Migration** > **Firewall Migration Tool** , and click the blue plus button to start provisioning a new migration instance.
2	Device Manager CLI	(Optional) Obtain the FDM-managed device configuration file: To obtain the FDM-managed device config file from device manager CLI, see Obtain the FDM-Managed Device Configuration File . If you intend to select a Security Cloud Control -managed FDM device in the **Select Source Configuration** , skip to Step 3.
3	Device Manager CLI	(Optional) Export PKI certificates and AnyConnect packages and profiles: This step is required only if you are planning to migrate site-to site VPN and remote-access VPN features from an FDM-managed device to threat defense. To export the PKI certificates from device manager CLI, see Step 1 in Export PKI Certificate from and Import into Firewall Management Center . To export AnyConnect packages and profiles from device manager CLI, see Step 1 in Retrieve AnyConnect Packages and Profiles . If you are not planning to migrate site-to-site VPN and remote-access VPN configurations, skip to Step 7.

	Workspace	Steps
4	Cloud-Delivered Firewall Management Center	(Optional) Import the PKI certificates and AnyConnect packages to management center: To import the PKI certificates to management center, see Step 2 in Export PKI Certificate from and Import into Firewall Management Center and Retrieve AnyConnect Packages and Profiles .
5	Security Cloud Control	Ensure that the status of the migration instance you created is **Ready** and click **Launch** ; the Secure Firewall Migration Tool opens in a new browser tab.
6	Secure Firewall Migration Tool	To select the source configuration firewall and migration option, see Select the Source Configuration Firewall and Migration .
7	Secure Firewall Migration Tool	(Optional) Upload the FDM-managed device config file obtained from device manager CLI, see Upload the FDM-Managed Device Configuration File . If you are migrating configuration from an FDM-managed device onboarded to Security Cloud Control , skip to Step 8.
8	Secure Firewall Migration Tool	From the list of FDM-managed devices shown, that are managed by your Security Cloud Control tenant, select the device whose configuration you want to migrate.
9	Secure Firewall Migration Tool	On the **Select Target** page, the Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant is selected by default.
10	Secure Firewall Migration Tool	Select a target device from the list of threat defense devices managed by your Cloud-Delivered Firewall Management Center or choose **Proceed without FTD** and proceed.
11	Secure Firewall Migration Tool	Download the pre-migration report and review it for a detailed summary of the parsed configuration. For detailed steps, see Review the Pre-Migration Report .
12	Secure Firewall Migration Tool	**Map FTD Interface** with the FDM-managed device configuration. Because the names of physical and port channel interfaces on your FDM and threat defense devices are not always the same, you can select to which interface in the target threat defense device you want an FDM-managed device interface to get mapped. For more information, see Map FDM-managed Device Configurations with Secure Firewall Device Manager Threat Defense Interfaces .
13	Secure Firewall Migration Tool	Map FDM-managed device interfaces to existing threat defense security zones and interface groups. See Map FDM-managed Interfaces to Security Zones and Interface Groups for detailed steps.
14	Secure Firewall Migration Tool	**Optimize, Review and Validate Configuration** with caution and ensure ACLs, objects, NAT, interfaces, routes, site-to-site VPN, and remote-access VPN rules are configured as intended for the destination threat defense device. See Optimize, Review and Validate the Configuration .
15	Secure Firewall Migration Tool	Once your configuration validation is a success, **Push Configuration** to the Cloud-Delivered Firewall Management Center . For more information, see Push the Migrated Configuration to Management Center .
16	Local Machine	Download the post-migration report and review it. To know more on what information the post-migration report contains, see Review the Post-Migration Report and Complete the Migration .
17	Cloud-Delivered Firewall Management Center	Deploy the newly migrated configuration to the threat defense device.

Troubleshoot FDM-managed Migration Issues

If you encounter a migration-blocking error when trying to migrate an FDM-managed device, try the following troubleshooting steps:

- Ensure that your target On-Premises Firewall Management Center 's network connectivity is up.
- Ensure that the FDM-managed that you are trying to migrate is not manage by the target On-Premises Firewall Management Center already.

Resume Migration

If you have started a migration from Security Cloud Control and wish to continue later, you can simply close the Firewall migration tool tab. When you want to continue with the migration, you can log in to Security Cloud Control and in **Firewall Migration Tool** click **Launch** on the migration you want to continue. The migration tool detects that you were migrating and lets you continue from where you left off. However, for the migration tool to detect that you have an ongoing migration, you must at least perform up to parsing of the source configuration. If you leave off a migration before performing this step, you can still launch the same migration from Security Cloud Control but you must start the migration from the first.

A Firewall Migration Tool is a tool that migrates FDM-managed device configurations, supports configuration file uploads, and facilitates source and target device selection.

- migrates FDM-managed device configurations
- supports configuration file uploads, and, and
- facilitates source and target device selection.

Migrate Check Point Firewall to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control

Learn how to migrate Check Point firewall configurations to Secure Firewall Threat Defense using the Firewall Migration Tool in Security Cloud Control , including version selection, configuration upload or extraction, interface mapping, validation, and deployment.

You can migrate your Check Point Firewall configurations to threat defense either by manually extracting the configuration from your firewall or using the configuration extractor that comes inbuilt with the migration tool. To know the Check Point configurations that are supported, see Check Point Configuration Support .

Select Source Configuration

In the **Source Firewall Vendor** drop-down, choose **Check Point (r80-r81)** or **Check Point (r75-r77)** based on the firewall version you want to migrate. You can manually upload an extracted firewall configuration using **Manual Configuration Upload** or use the **Live Connect** option to connect to the Check Point Security Gateway to export the configuration file.

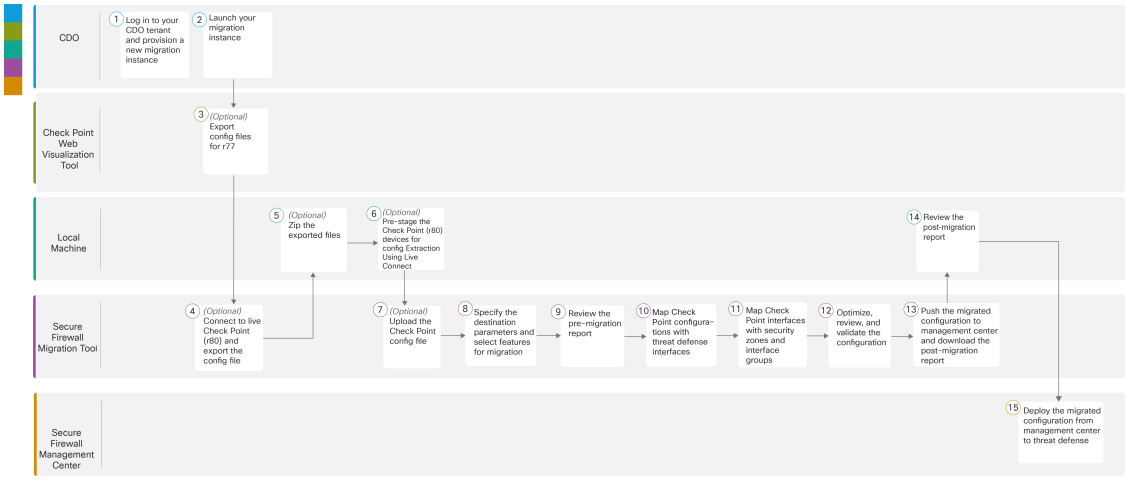
> **Note**
>
> You can use **Live Connect** only when you have selected Check Point (r80-81) and **Configuration Extractor** only when you have selected Check Point (r75-r77).

Select Target

In the **Select Target** page, the Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant is selected by default, and the Firewall Threat Defense devices managed by that management center are listed. You can choose the Firewall Threat Defense device you wish to migrate the configuration to, and proceed with the migration.

Note that the threat defense devices listed are displayed either as **In Use** or **Available** based on whether the device is being used in another migration instance. However, you can perform an override by clicking **Change Device Status** , selecting the device from the **In Use** list, and clicking **Continue** , which will make the device available for being selected as the target. Choosing **Proceed without FTD** pushes only NAT objects, ACLs, and port objects to the Cloud-Delivered Firewall Management Center . For more information about the commonly used ASA features and their equivalent threat defense features, see Cisco Secure Firewall ASA to Threat Defense Feature Mapping guide.

> **Caution**
>
> Changing the device status from **In Use** to **Available** impacts the ongoing migration instance that is using the device already. We recommend that you exercise caution when doing this.



To perform the migration with more detailed steps, continue to Export the Check Point Configuration Files in *Migrating Check Point Firewall to Secure Firewall Threat Defense with the Migration Tool* book.

	Workspace	Steps
1	Security Cloud Control	Log in to your Security Cloud Control tenant, and in the left pane, click **Administration** > **Migration** > **Firewall Migration Tool** and click the blue plus button to start provisioning a new migration instance.

	Workspace	Steps
2	Security Cloud Control	Launch your migration instance from Security Cloud Control and choose **Check Point (r75–r77)** or **Check Point (r80–r81)** in the **Source Firewall Vendor** drop-down, based on your requirement.
3	Check Point Web Visualization Tool	(Optional) Export the Check Point configuration file for r77: To export the Check Point configuration files for r77, see Export the Check Point Configuration Files for r77 . If you intend to export configuration files for r80 using Secure Firewall migration tool live connect feature, skip to step 6.
4	Secure Firewall Migration Tool	(Optional) Connect to live Check Point (r80) and export the config file: To export the Check Point configuration files for r80 using live connect feature, see Export the Check Point Configuration Files for r80 .
5	Local Machine	(Optional) Zip the exported files: select all the exported configuration files for r77 and compress them to a zip file. For detailed steps, see Zip the Exported Files .
6	Local Machine	Pre-stage the Check Point (r80) devices for config extraction: You must configure the credentials on Check Point (r80) devices before using Live Connect. For pre-staging credentials on Check Point (r80) devices, see Pre-Stage the Check Point Devices for Configuration Extraction Using Live Connect . This step is required only if you are planning to migrate configuration files for r80 devices.
7	Secure Firewall Migration Tool	(Optional) Upload the Check Point config file .
8	Secure Firewall Migration Tool	Specify the destination parameters for the Secure Firewall Migration Tool.
9	Secure Firewall Migration Tool	Navigate to where you downloaded the pre-migration report and review the report.
10	Secure Firewall Migration Tool	The Secure Firewall migration tool allows you to map the Check Point configuration with threat defense interfaces. For detailed steps, see Map Check Point Configurations with Secure Firewall Device Manager Threat Defense Interfaces .
11	Secure Firewall Migration Tool	To ensure that the Check Point configuration is migrated correctly, map the Check Point interfaces to the appropriate threat defense interface objects, security zones, and interface groups. For more information, see Map Check Point Interfaces to Security Zones and Interface Groups .
12	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. For detailed steps, see Optimize, Review and Validate the Configuration to be Migrated .
13	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to the Cloud-Delivered Firewall Management Center and allows you to download the post-migration report.
14	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration .
15	Cloud-Delivered Firewall Management Center	Deploy the migrated configuration from the Cloud-Delivered Firewall Management Center to threat defense.

Migrating Check Point Firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control

Describes how to migrate Check Point firewall configurations to Cisco Multicloud Defense using the Firewall Migration Tool in Security Cloud Control, including source selection, configuration upload, validation, and migration completion.

Migrating Check Point Firewall to Multicloud Defense with the Firewall Migration Tool is a configuration transformation process that

- converts Check Point firewall configurations to Multicloud Defense format using the Secure Firewall migration tool hosted on Security Cloud Control,
- supports Check Point r80-r81 configurations with comprehensive validation and optimization steps, and
- delivers migrated configurations directly to Multicloud Defense for gateway configuration.

Migration workflow overview

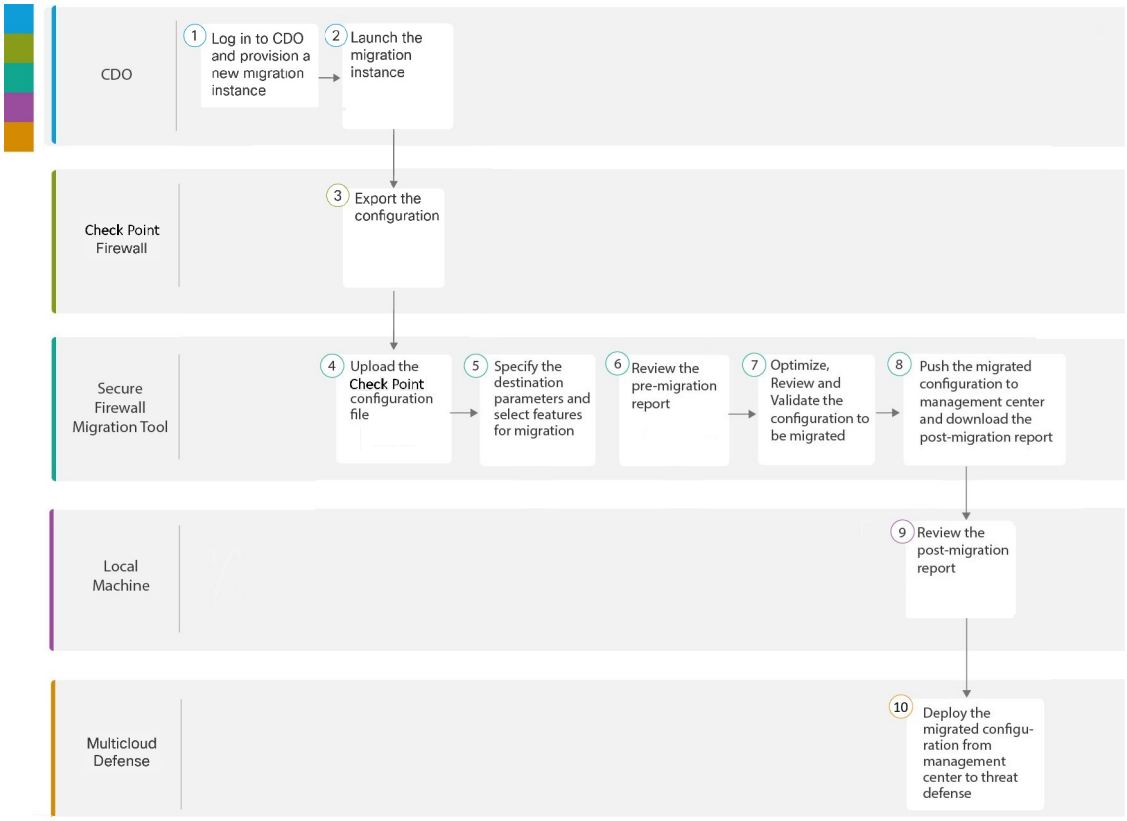
The migration process includes selecting source and target configurations, uploading Check Point configuration files, and completing validation steps.

To read more about the supported configurations for this migration, see Check Point Firewall Configuration Support for Multicloud Defense in Migrating Check Point Firewall to Cisco Multicloud Defense with the Migration Tool guide.

The migration includes two main configuration selection steps:

- **Source configuration selection**: In the **Source Firewall Vendor** drop-down, choose **Check Point (r80-r81)** and start the migration. Upload the configuration extracted from a Check Point (r80) to the Firewall Migration Tool. To extract configuration from a Check Point (r80) using the Secure Firewall migration tool, proceed to Export the Check Point Configuration Files for r80 in *Migrating Check Point Firewall to Cisco Multicloud Defense with the Migration Tool* guide.
- **Target selection**: On the **Select Target** page, choose **Multicloud Defense**. To know more about the prerequisites and the steps involved, see Specify Destination Parameters for Multicloud Defense in the *Migrating Check Point Firewall to Cisco Multicloud Defense with the Migration Tool* guide.

Figure 34: Check point firewall to multicloud defense End-to-End migration



The migration process consists of multiple steps across different workspaces:

	Workspace	Steps
1	Security Cloud Control	Log in to your Security Cloud Control tenant, and in the left pane, click **Administration** > **Migration** > **Firewall Migration Tool** and click the blue plus + button to start provisioning a new migration instance.
2	Security Cloud Control	After your migration instance is ready, click **Launch** and choose **Check Point (r80-r81)**.
3	Check Point Firewall	Export the Configuration File: To export the configuration from Check Point Networks Firewall, see Export the Check Point Configuration Files for r80.
4	Secure Firewall Migration Tool	Upload the configuration to the Firewall Migration tool. For more information, see Upload the Check Point Configuration File.
5	Secure Firewall Migration Tool	During this step, you can specify the destination parameters for Multicloud Defense. For detailed steps, see Specify Destination Parameters for Multicloud Defense.
6	Secure Firewall Migration Tool	Navigate to where you downloaded the pre migration report and review the report. For detailed steps, see Review the Pre-Migration Report.
7	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct. For detailed steps, see Optimize, Review, and Validate the Configuration to be Migrated.
8	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to Multicloud Defense and allows you to download the post-migration report. For detailed steps, see Push the Configuration to Multicloud Defense.

	Workspace	Steps
9	Secure Firewall Migration Tool	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
10	Multicloud Defense	Verify the migrated configurations and use them as required in configuring gateways.

Migrate Fortinet Firewall with the Firewall Migration Tool in Security Cloud Control

Configure Fortinet firewall configuration migration to Secure Firewall Threat Defense using the Firewall Migration Tool in Security Cloud Control, including configuration upload, interface mapping, validation, and deployment.

The Firewall migration tool allows migrating configurations from Fortinet firewall to threat defense devices managed by your Cloud-Delivered Firewall Management Center.

You can manually derive the configuration file from your Fortinet firewall and upload it to the migration tool to begin with your migration. To learn about supported Fortinet firewall configurations, see Fortinet Configuration Support.

Procedure

1. On the **Select Source Configuration** page, choose **Fortinet (5.0+)** and click **Start Migration**.
2. Click **Upload** to choose the Fortinet configuration file and click **Next**.
3. In the **Select Target** page, choose the threat defense device you wish to migrate the configuration to.

   The Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant is selected by default, and the Firewall Threat Defense devices managed by that management center are listed.

   The threat defense devices listed are displayed either as **In Use** or **Available** based on whether the device is being used in another migration instance. However, you can perform an override by clicking **Change Device Status**, selecting the device from the **In Use** list, and clicking **Continue**, which will make the device available for being selected as the target.

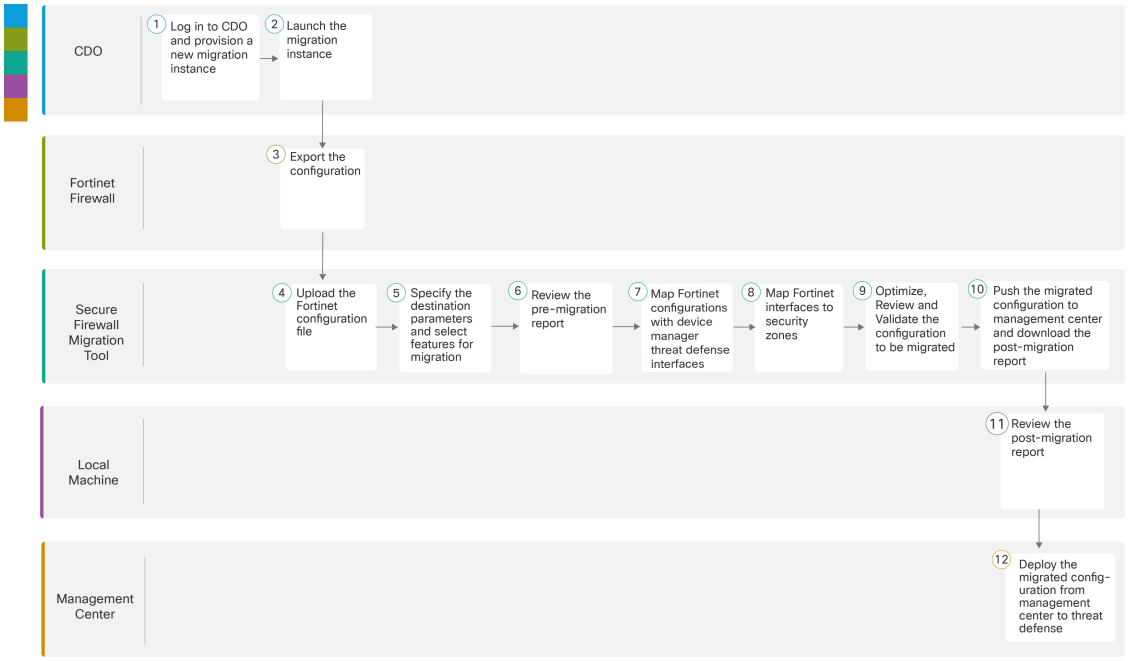
   Choosing **Proceed without FTD** pushes only NAT objects, ACLs, and port objects to the Cloud-Delivered Firewall Management Center. For more information about the commonly used ASA features and their equivalent threat defense features, see Cisco Secure Firewall ASA to Threat Defense Feature Mapping guide.

   > ⚠ **Caution**
   >
   > Changing the device status from **In Use** to **Available** impacts the ongoing migration instance that is using the device already. We recommend that you exercise caution when doing this.

4. Follow the migration workflow using the table and flowchart provided.

   The flowchart that follows illustrates the step-by-step procedure for migration Fortinet firewall configurations to threat defense devices:

   To perform the procedure with more detailed steps, continue to Export Fortinet Firewall Configuration from Fortinet Firewall GUI in Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool guide.



	Workspace	Steps
1	Security Cloud Control	Log in to your Security Cloud Control tenant, and in the left pane, click **Administration** > **Migration** > **Firewall Migration Tool**, and click the blue plus button to start provisioning a new migration instance.
2	Security Cloud Control	After your migration instance is ready, click **Launch** and choose **Fortinet (5.0+)**.
3	Fortinet Firewall	Export the Fortinet configuration to the local system. To export the configuration from Fortinet firewall, see Export the Configuration from Fortinet Firewall.
4	Secure Firewall Migration Tool	Upload the Fortinet config file exported from Fortinet firewall, see Upload the Fortinet Configuration File.
5	Secure Firewall Migration Tool	In this step, you can specify the destination parameters for the migration. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool. .
6	Secure Firewall Migration Tool	Navigate to where you downloaded the pre migration report and review the report. For detailed steps, see Review the Pre-Migration Report.
7	Secure Firewall Migration Tool	To ensure that the Fortinet configuration is migrated correctly, map the Fortinet interfaces to the appropriate threat defense interface objects, security zones, and interface groups. For detailed steps, see Map Fortinet Firewall Configurations with Secure Firewall Device Manager Threat Defense Interfaces.
8	Secure Firewall Migration Tool	Map the Fortinet interfaces to the appropriate security zones, see Map Fortinet Interfaces to Security Zones for detailed steps.
9	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. For detailed steps, see Optimize, Review and Validate the Configuration to be migrated.

	Workspace	Steps
10	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to the Cloud-Delivered Firewall Management Center and allows you to download the post-migration report. For detailed steps, see Push the Migrated Configuration to Management Center.
11	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
12	Management Center	Deploy the migrated configuration from the Cloud-Delivered Firewall Management Centerto threat defense.

The Fortinet firewall configuration is successfully migrated to the Secure Firewall Threat Defense device through the management center.

Migrating Fortinet firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control

Describes how to migrate Fortinet firewall configurations to Cisco Multicloud Defense using the Firewall Migration Tool in Security Cloud Control, including source selection, configuration upload, validation, and migration completion.

The Secure Firewall migration tool hosted on Security Cloud Control lets you migrate configurations from Fortinet firewall to Multicloud Defense. To read more about the supported configurations for this migration, see Fortinet Firewall Configuration Support for Multicloud Defense in *Migrating Fortinet Firewall to Cisco Multicloud Defense with the Migration Tool* guide.

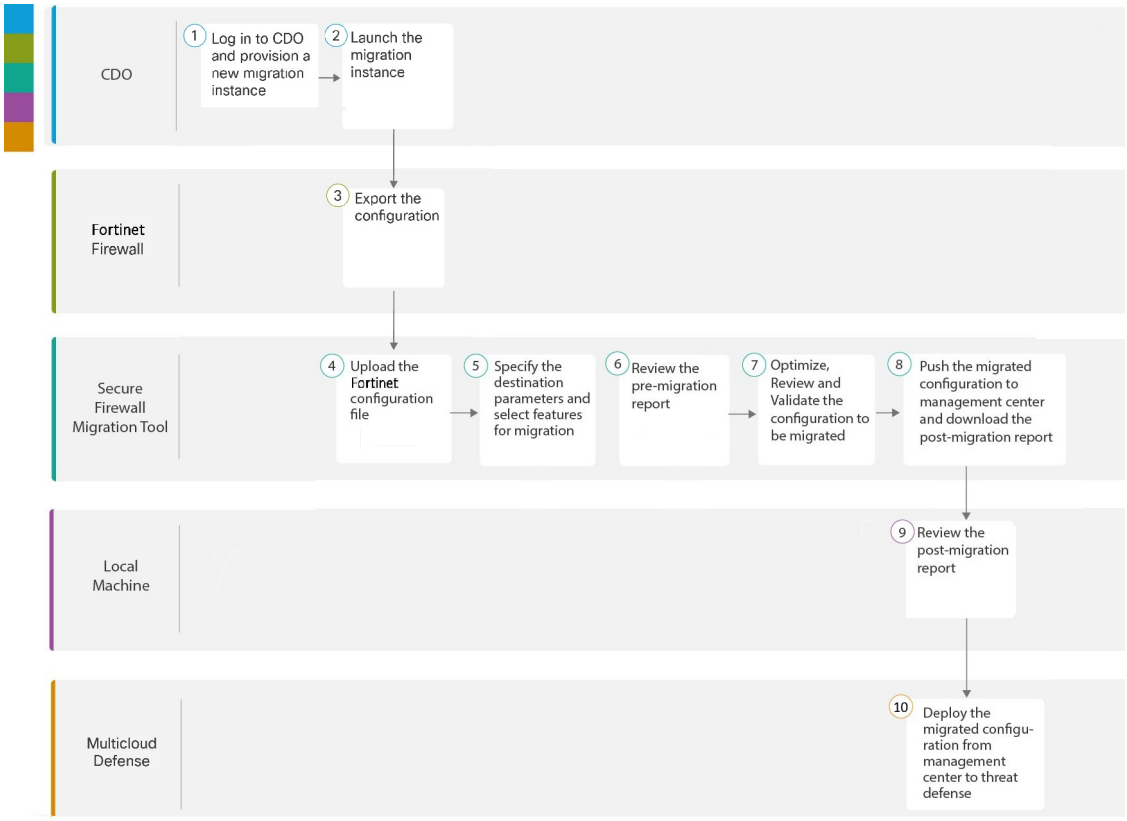
Summary

The key components involved in the Fortinet firewall to Multicloud Defense migration process are:

- **Fortinet Firewall (5.0+)**: Source system containing the configuration to be migrated
- **Firewall Migration Tool**: Tool hosted on Security Cloud Control that processes and transforms configurations
- **Multicloud Defense**: Target platform where migrated configurations are deployed
- **Configuration Files**: Exported source configuration and migration reports

Workflow

Figure 35: Fortinet firewall to multicloud defense End-to-End migration



These are the stages of migrating Fortinet firewall configurations to Multicloud Defense:

1. The system administrator logs in to Security Cloud Control and provisions a new migration instance.
   - Log in to your Security Cloud Control tenant
   - In the left pane, click **Administration** > **Migration** > **Firewall Migration Tool**
   - Click the blue plus button to start provisioning a new migration instance

   The migration instance is ready for configuration.
2. The administrator selects the source firewall configuration type and exports the configuration from Fortinet firewall.
   - After the migration instance is ready, click **Launch** and choose **Fortinet (5.0+)**
   - Export the configuration file from Fortinet Networks Firewall as described in Export the Configuration from Fortinet Firewall

   You can migrate configurations from your Fortinet firewall by choosing **Fortinet (5.0+)** in the **Source Firewall Vendor** drop-down and uploading the extracted configuration file to Firewall Migration Tool. To read about the Fortinet firewall configurations that are supported for migration, see Supported Software Versions for Migration in the *Migrating Fortinet Firewall to Cisco Multicloud Defense with the Migration Tool* guide.

   The source configuration is available for upload to the migration tool.
3. The administrator uploads the configuration to the Firewall Migration tool and selects Multicloud Defense as the target.
   - Upload the configuration to Firewall Migration tool as described in Upload the Fortinet Configuration File
   - Choose **Multicloud Defense** as the target
   - Specify the destination parameters as described in Specify Destination Parameters for Multicloud Defense

On the **Select Target** page, choose **Multicloud Defense**. To know more about the prerequisites and the steps involved, see Specify Destination Parameters for Multicloud Defense in the *Migrating Fortinet Firewall to Cisco Multicloud Defense with the Migration Tool* guide.

The tool generates a pre-migration report for review.

4. The administrator reviews the pre-migration report to understand what will be migrated.
   - Navigate to where you downloaded the pre migration report
   - Review the report as described in Review the Pre-Migration Report

   The administrator can proceed with optimization and validation.
5. The administrator optimizes, reviews, and validates the configuration to ensure accuracy before migration.
   - Optimize and review the configuration carefully
   - Validate that the configuration is correct as described in Optimize, Review, and Validate the Configuration to be Migrated

   The configuration is ready to be pushed to Multicloud Defense.
6. The migration tool sends the migrated configuration to Multicloud Defense and generates a post-migration report.
   - Push the configuration to Multicloud Defense as described in Push the Configuration to Multicloud Defense
   - Download the post-migration report

   This step in the migration process sends the migrated configuration to Multicloud Defense and allows you to download the post-migration report.
7. The administrator reviews the post-migration report and verifies the migrated configurations in Multicloud Defense.
   - Navigate to where you downloaded the post migration report and review the report as described in Review the Post-Migration Report and Complete the Migration
   - Verify the migrated configurations in Multicloud Defense
   - Use the configurations as required in configuring gateways

   The migration is complete and configurations are available for use in Multicloud Defense.

	Workspace	Steps
1	Security Cloud Control	Log in to your Security Cloud Control tenant, and in the left pane, click **Administration** > **Migration** > **Firewall Migration Tool** and click the blue plus  button to start provisioning a new migration instance.
2	Security Cloud Control	After your migration instance is ready, click **Launch** and choose **Fortinet (5.0+)**.
3	Fortinet Firewall	Export the Configuration File: To export the configuration from Fortinet Networks Firewall, see Export the Configuration from Fortinet Firewall.
4	Secure Firewall Migration Tool	Upload the configuration to Firewall Migration tool. For more information, see Upload the Fortinet Configuration File.
5	Secure Firewall Migration Tool	Choose Multicloud Defense as the target and specify the destination parameters. For more information, see Specify Destination Parameters for Multicloud Defense.

	Workspace	Steps
6	Secure Firewall Migration Tool	Navigate to where you downloaded the pre migration report and review the report. For more information, see Review the Pre-Migration Report.
7	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct. For detailed steps, see Optimize, Review, and Validate the Configuration to be Migrated.
8	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to Multicloud Defense and allows you to download the post-migration report. For detailed steps, see Push the Configuration to Multicloud Defense.
9	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
10	Multicloud Defense	Verify the migrated configurations and use them as required in configuring gateways.

Migrate Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Firewall Migration Tool in Security Cloud Control

Configure migration of Palo Alto Networks firewall configurations to Secure Firewall Threat Defense using the Firewall Migration Tool in Security Cloud Control, including configuration upload, interface mapping, validation, and deployment.

This task enables you to migrate Palo Alto Networks firewall configurations to Secure Firewall Threat Defense using the Firewall Migration Tool, preserving your security policies while transitioning to Cisco's threat defense platform.

You can migrate configurations from your Palo Alto Networks firewall by choosing **Palo Alto Networks (6.1+)** in the **Source Firewall Vendor** drop-down and manually uploading the derived configuration file to Firewall Migration Tool. To read about the Palo Alto Networks firewall configurations that are supported for migration and the limitations around them, see Guidelines and Limitations in the *Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool* book.

Procedure

1. Log in to your Security Cloud Control tenant, and in the left pane, click **Administration** > **Migration** > **Firewall Migration Tool**, and click the blue plus  button to start provisioning a new migration instance.
2. Launch the migration instance from Security Cloud Control and choose **Palo Alto Networks (6.1+)**.
3. Export the Configuration File from your Palo Alto Networks Firewall.

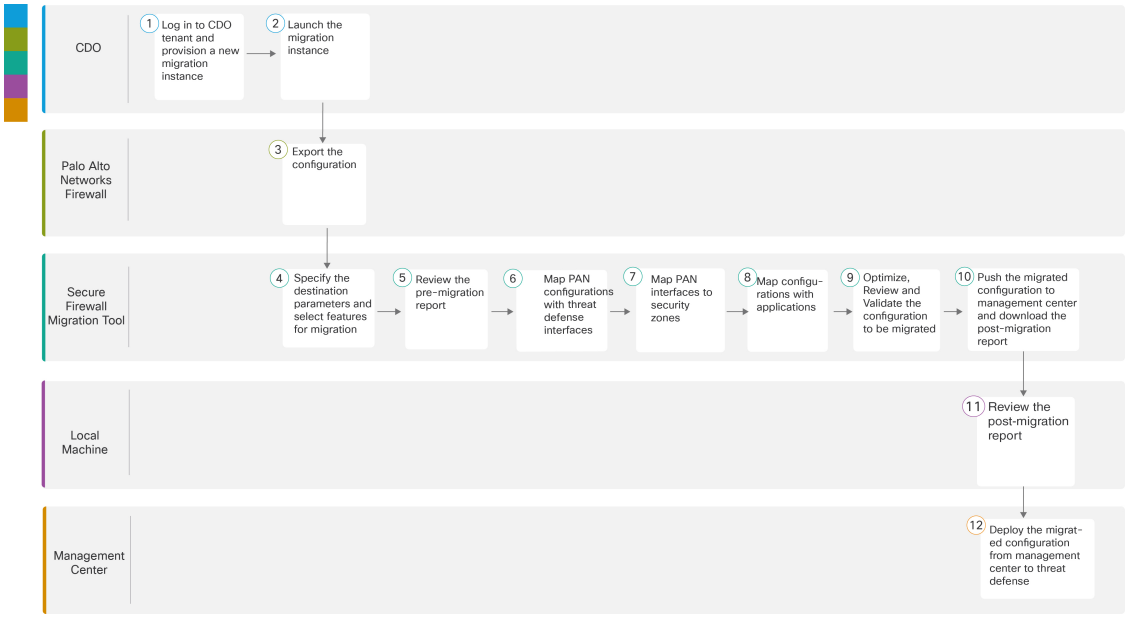
   To export the configuration from Palo Alto Networks Firewall, see Export the Configuration from Palo Alto Networks.
4. Select the target threat defense device for migration.

   In the **Select Target** page, the Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant is selected by default, and the Firewall Threat Defense devices managed by that management center are listed. You can choose the Firewall Threat Defense device you wish to migrate the configuration to, and proceed with the migration.

   Note that the threat defense devices listed are displayed either as **In Use** or **Available** based on whether the device is being used in another migration instance. However, you can perform an override by clicking **Change Device Status**, selecting the device from the **In Use** list, and clicking **Continue**, which will make the device available for being selected as the target. Choosing **Proceed without FTD** pushes only NAT objects, ACLs, and port objects

to the Cloud-Delivered Firewall Management Center. For more information about the commonly used ASA features and their equivalent threat defense features, see Cisco Secure Firewall ASA to Threat Defense Feature Mapping guide.

> **Caution**
>
> Changing the device status from **In Use** to **Available** impacts the ongoing migration instance that is using the device already. We recommend that you exercise caution when doing this.



5. Specify the destination parameters for the migration.

   For detailed steps, see Specify the destination parameters for the migration.

6. Review the pre-migration report.

   Navigate to where you downloaded the pre migration report and review the report. For detailed steps, see Review the Pre-Migration Report.

7. Map PAN interfaces to threat defense interface objects, security zones, and interface groups.

   To ensure that the PAN configuration is migrated correctly, map the PAN interfaces to the appropriate threat defense interface objects, security zones, and interface groups. For detailed steps, see Map PAN Firewall Configurations with Secure Firewall Management Center Threat Defense Interfaces.

8. Map PAN interfaces to security zones.

   For detailed steps, see Map PAN interfaces to security zones.

9. Map PAN configuration to corresponding target applications.

   For detailed steps, see Map Configurations with Applications.

10. Optimize, review, and validate the configuration.

    Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. For detailed steps, see Optimize, Review and Validate the Configuration to be Migrated.

11. Push the migrated configuration to Cloud-Delivered Firewall Management Center.

This step in the migration process sends the migrated configuration to management center and allows you to download the post-migration report. For detailed steps, see Push the Migrated Configuration to Cloud-Delivered Firewall Management Center.

12. Review the post-migration report.

    Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.

13. Deploy the migrated configuration from the Cloud-Delivered Firewall Management Center to threat defense.

Your Palo Alto Networks firewall configuration has been successfully migrated to Secure Firewall Threat Defense. The migrated configuration is now deployed and active on your target threat defense device.

Migrate Secure Firewall ASA to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control

Configure Cisco Secure Firewall ASA configurations to migrate to Cisco Multicloud Defense using the Firewall Migration Tool in Security Cloud Control.

The Secure Firewall migration tool in Security Cloud Control lets you to migrate configurations from live ASA devices that are managed by Security Cloud Control or using a configuration file extracted from an ASA device.

To read more about the Secure Firewall ASA configurations supported for migration, see ASA Configuration Support in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book.

Before you begin

In the left pane, navigate to **Administration** > **Migration** > **Firewall Migration Tool** and provision a new migration instance.

Follow these steps to migrate Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Firewall Migration Tool:

Procedure

1. Launch your migration instance from Security Cloud Control.
2. Choose **Cisco ASA (8.4+)** in **Select Source Configuration** and click **Start Migration**.
3. Upload an ASA configuration file manually or choose any one of the Security Cloud Control-managed ASA devices listed on the **Connect to ASA** pane.

   Note

   If you are trying to select a Security Cloud Control-managed device, note that devices having **Configuration Status** as **Synced** are only listed by the migration tool; if you do not see the device you want to migrate in the list, check if the device configuration changes are up-to-date and synced with Security Cloud Control. Note that one ASA device can be selected as the source device by more than one user at the same time and the confuguration extraction takes place seamlessly.

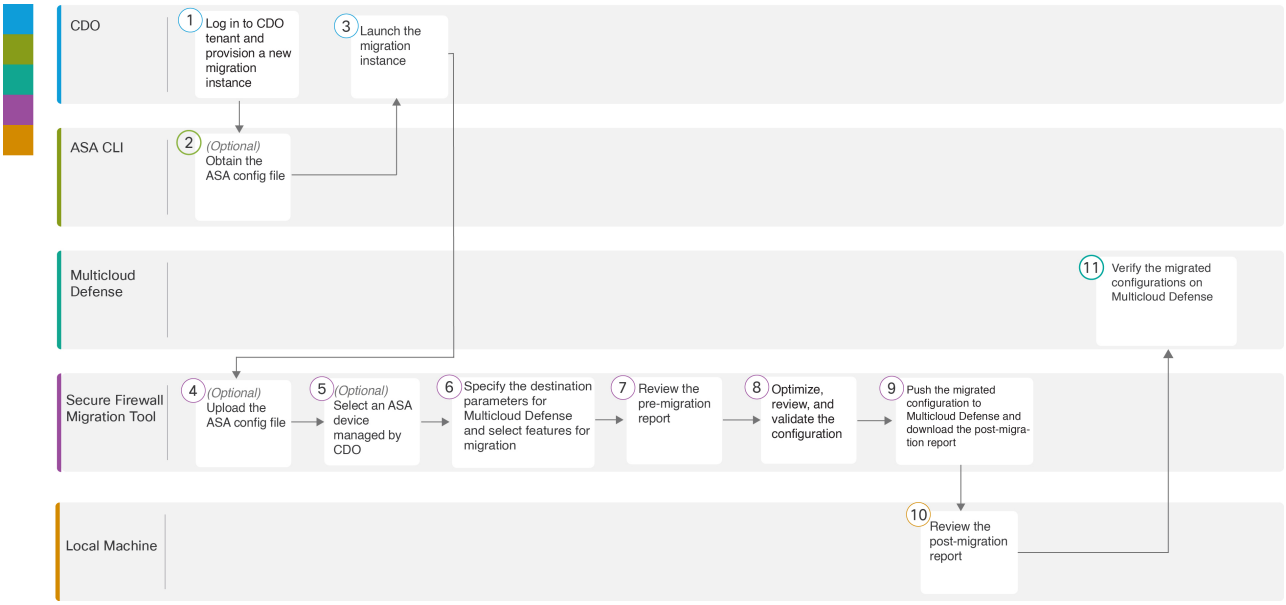
   If you have one or more security contexts configured on your ASA device, the migration tool allows you to choose which context you want to migrate; you can also merge all your contexts to a single instance and then migrate them. Refer Select the ASA Primary Security Context for more information.

4. Verify the parsed configuration summary and click **Next**.

5. On the **Select Target** page, choose **Multicloud Defense**.

   To know more about the prerequisites and the steps involved, see Specify Destination Parameters for Multicloud Defense in *Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool* guide.

Figure 36: ASA to Multicloud Defense End-to-End Migration



	Workspace	Steps
1	Security Cloud Control	In the left pane, navigate to **Administration** > **Migration** > **Firewall Migration Tool** and provision a new migration instance.
2	Secure Firewall ASA CLI	Obtain the ASA configuration file: To obtain the ASA config file from ASA CLI, see Obtain the ASA configuration file.
3	Security Cloud Control	Click **Launch** under **Actions** to open the migration tool in a different browser tab.
4	Secure Firewall migration tool	Upload the ASA config file obtained from ASA CLI, see Upload the ASA Configuration File. If you are planning to connect to live ASA, skip to step 6.
5	Secure Firewall migration tool	If you want to connect in real time to an ASA already managed by Security Cloud Control, choose from the list of ASA devices.
6	Secure Firewall migration tool	Specify the destination parameters for Multicloud Defense. See Specify Destination Parameters for more information.
7	Secure Firewall migration tool	Navigate to where you downloaded the pre migration report and review it. See Review the Premigration Report for more information.
8	Secure Firewall migration tool	Optimize and review the configuration carefully and validate that it is correct. See Optimize, Review, and Validate for more information.
9	Secure Firewall migration tool	Push the configuration to Multicloud Defense. See Push the Configuration to Multicloud Defense for more information.

	Workspace	Steps
10	Local machine	Download the postmigration report for verifying how the migration went. See Review the Postmigration Report for more information.
11	Multicloud Defense	Verify the migrated configurations on Multicloud Defense and use them as required in configuring your gateways.

The ASA configuration is successfully migrated to Cisco Multicloud Defense, and you can verify the migrated configurations on the Multicloud Defense platform.

Migrate Palo Alto Networks Firewall to Multicloud Defense with the Firewall Migration Tool in Security Cloud Control

Configure migration of Palo Alto Networks firewall configurations to Cisco Multicloud Defense using the Firewall Migration Tool in Security Cloud Control, including source selection, configuration upload, validation, and migration completion.

This task allows you to migrate configurations from Palo Alto Networks firewall to Multicloud Defense using the Secure Firewall migration tool hosted on Security Cloud Control.

The Secure Firewall migration tool hosted on Security Cloud Control lets you migrate configurations from Palo Alto Networks firewall to Multicloud Defense. To read more about the supported configurations for this migration, see PAN Firewall Configuration Support for Multicloud Defense in *Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool* guide.

Before you begin

Follow these steps to migrate Palo Alto Networks firewall configurations to Multicloud Defense:

Procedure

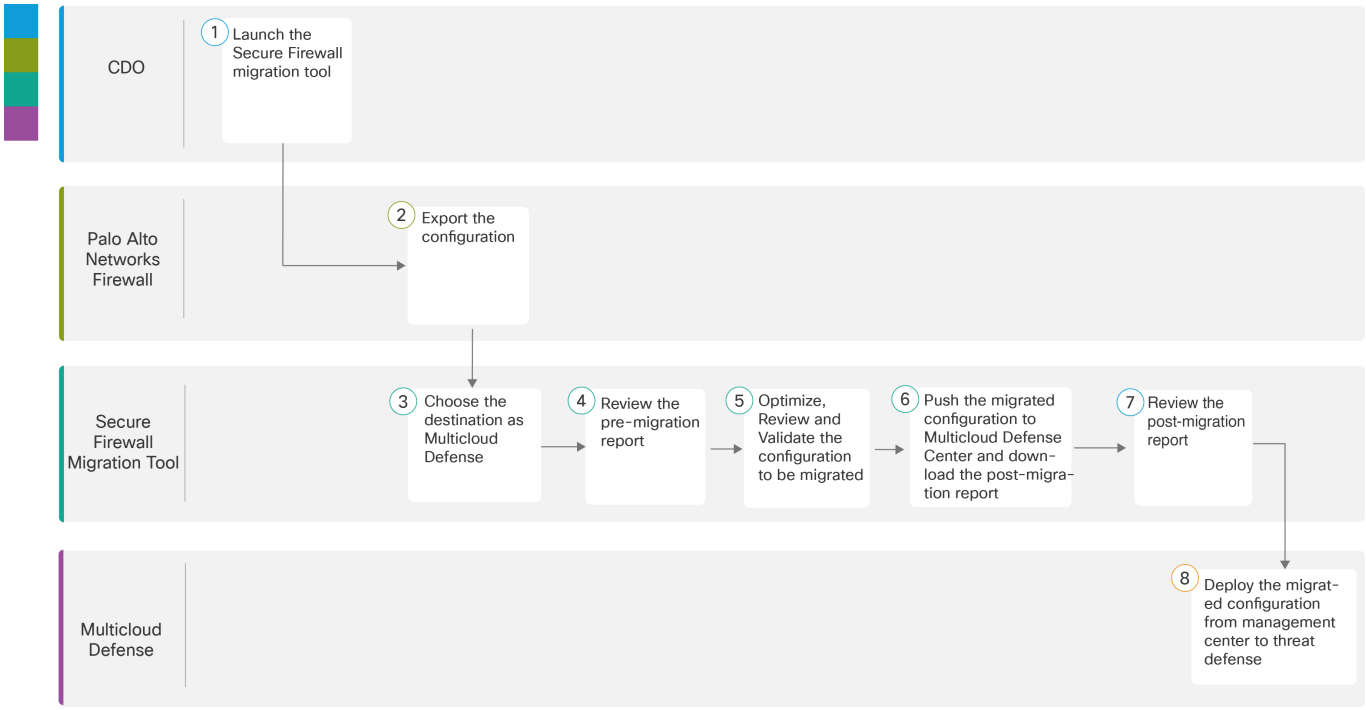
1. In the left pane, navigate to **Administration** > **Migration** > **Firewall Migration Tool**, provision a new migration instance, and click **Launch**.
2. Export the configuration from your Palo Alto Networks Firewall.

   For detailed steps to export the configuration from Palo Alto Networks Firewall, see Export the Configuration from Palo Alto Networks Firewall.
3. Select the source configuration by choosing **Palo Alto Networks (6.1+)** in the **Source Firewall Vendor** drop-down and upload the extracted configuration file to Firewall Migration Tool.

   To read about the Palo Alto Networks firewall configurations that are supported for migration and the limitations around them, see Guidelines and Limitations in the *Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool* book.
4. On the **Select Target** page, choose **Multicloud Defense** and specify the destination parameters.

   To know more about the prerequisites and the steps involved, see Specify Destination Parameters for Multicloud Defense in *Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool* guide. For more detailed steps specific to Palo Alto Networks migration, see Specify Destination Parameters for Multicloud Defense.

   Figure 37: Palo Alto Networks firewall to Multicloud Defense End-to-End Migration



5. Navigate to where you downloaded the pre migration report and review the report.

   For more information, see Review the Premigration Report.

6. Optimize and review the configuration carefully and validate that it is correct.

   For detailed steps, see Optimize, Review, and Validate.

7. Push the migrated configuration to Multicloud Defense and download the post-migration report.

   This step in the migration process sends the migrated configuration to Multicloud Defense and allows you to download the post-migration report. For detailed steps, see Push the Configuration to Multicloud Defense.

8. Navigate to where you downloaded the post migration report and review the report.

   For detailed steps, see Review the Postmigration Report.

9. Verify the migrated configurations in Multicloud Defense and use them as required in configuring gateways.

Your Palo Alto Networks firewall configuration is successfully migrated to Multicloud Defense and is ready for use in configuring gateways.

Related documentation

Provides information on the various guides about the Secure Firewall migration tool.

To know more about migrating third-party firewalls using the Secure Firewall migration tool in Security Cloud Control, see the following documents based on your requirement:

- To know about the latest features and release-specific information around the Firewall migration tool, see Cisco Secure Firewall Migration Tool Release Notes.

> **Note**
>
> Security Cloud Control hosts the latest version of the Secure Firewall migration tool.

- To migrate configurations from a Check Point firewall to threat defense, start from Export the Check Point Configuration Files in Migrating a Check Point Firewall to Threat Defense guide.
- To migrate configurations from a Palo Alto Networks firewall to threat defense, start from Export the Configuration from Palo Alto Networks Firewall in Migrating a Palo Alto Networks Firewall to Threat Defense guide.
- To migrate configurations from a Fortinet firewall to threat defense, start from Export the Configuration from Fortinet Firewall in Migrating a Fortinet Firewall to Threat Defense guide.

Important

Unlike ASA and FDM-managed device migrations, you can only upload a manually extracted configuration file for migrating a third-party firewall configuration to threat defense.

If you wish to read overall information about the Secure Firewall migration tool and all related documentation, see Cisco Secure Firewall Migration Tool.

Part XV

Monitor and Analyze

Topics:

- Events in Security Cloud Control
- Security Analytics and Logging Licenses
- Secure Event Connectors
- Monitor Catalyst SD-WAN Events
- View Events in Security Cloud Control Firewall Management
- Integrate Security Cloud Control with Splunk
- Use Cisco Secure Cloud Analytics Portal
- Monitor Remote Access Virtual Private Network Sessions from Secure Firewall ASA and Firewall Threat Defense
- Monitor and report change logs, workflows, and jobs
- Smart Licensing Dashboard

51 Events in Security Cloud Control

Topics:

- Security Analytics and Logging (SaaS) in Security Cloud Control
- Event types in Security Cloud Control
- Troubleshoot network problems using security and analytics logging events
- Caution: maintain active Cisco security analytics and logging subscription

Learn how Security Analytics and Logging captures firewall events in Security Cloud Control, including supported event types, event filtering, and event data retention after deprovisioning.

This chapter provides information about Security Analytics and Logging (SaaS) in Security Cloud Control.

Security Analytics and Logging (SaaS) in Security Cloud Control

Explains how Cisco Security Analytics and Logging (SAL) collects and centralizes firewall security events in the cloud, enabling unified visibility and filtering through Security Cloud Control.

Cisco Security Analytics and Logging (SAL) is a software as a service product that

- captures supported types of security events from all firewall devices
- stores events in the Security Analytics and Logging cloud, and
- provides unified visibility through the **Event Logging** page in Security Cloud Control.

Integration capabilities

Terminology Note: In this documentation, when Cisco Security Analytics and Logging (a software as a service product) is used with Security Cloud Control for security event monitoring and analysis, you will see this integration referred to as Cisco Security Analytics and Logging (SaaS) or SAL (SaaS).

The **Event Logging** page allows you to search, filter and analyze the security event data to understand which security rules are being triggered in your network.

Event types in Security Cloud Control

Secure Logging Analytics (SaaS) enables you to filter and analyze security events from ASA, FTD, and devices by event types such as AAA, BotNet, Firewall Traffic, Intrusion, and AI Defense. These filters help monitor network activity, detect threats, and enforce security policies for comprehensive security visibility.

When filtering the security events logged in Secure Logging Analytics (SaaS), you can choose from a list of ASA, FTD, and event types that Security Cloud Control supports. From the Security Cloud Control menu, navigate **Analytics** > **Event Logging** and click the filter icon to choose events. These event types represent groups of syslog IDs. The table that follows shows which syslog IDs are included in which event type. To learn more about a specific syslog ID, you can search for it in the Cisco ASA Series Syslog Messages or the Cisco Secure Firewall Threat Defense Syslog Messages guides.

Some syslog events have the additional attribute "EventName." You can filter the events table to find events using the EventName attribute by filtering by attribute:value pairs.

See Event Name Attributes for Syslog Events.

Some syslog events will have the additional attributes "EventGroup" and "EventGroupDefinition". You will be able to filter the events table to find events using these additional attributes by filtering by attribute:value pairs.

The NetFlow events are different from syslog events. The **NetFlow** filter searches for all NetFlow event IDs that resulted in an NSEL record. Those NetFlow event IDs are defined in the Cisco ASA NetFlow Implementation Guide.

The following table describes the event types that Security Cloud Control supports and lists the syslog or NetFlow event numbers that correspond to the event types:

Filter Name	Description	Corresponding Syslog Event or Netflow Event
AAA	These are events that the system generates when failed or invalid attempts happen to authenticate, authorize, or use up resources in the network, when AAA is configured.	109001-109035 113001-113027

Filter Name	Description	Corresponding Syslog Event or Netflow Event
BotNet	These events get logged when a user attempts to access a malicious network, which might contain a malware-infected host, possibly a BotNet, or when the system detects traffic to or from a domain or an IP address in the dynamic filter block list.	338001-338310
Failover	These events get logged when the system detects errors in stateful and stateless failover configurations or errors in the secondary firewall unit when a failover occurs.	101001-101005, 102001, 103001-103007, 104001-104004, 105001-105048 210001-210022 311001-311004 709001-709007
Firewall Denied	These events get generated when the firewall system denies traffic of a network packet for various reasons, ranging from a packet drop because of the security policy to a drop because the system received a packet with the same source IP and destination IP, which could potentially mean an attack on the network. Firewall Denied events may be contained in a NetFlow and may be reported with NetFlow event IDs as well as syslog IDs.	106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027
Firewall Traffic	These are events that get logged depending on the various connection attempts in the network, user identities, time stamps, terminated sessions, and so on. Firewall Traffic events may be contained in a NetFlow and may be reported with NetFlow event IDs as well as syslog IDs.	106001-106100, 108001-108007, 110002-110003 201002-201013, 209003-209005, 215001 302002-302304, 302022-302027, 303002-303005, 313001-313008, 317001-317006, 324000-324301, 337001-337009 400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001 500001-500005, 508001-508002 607001-607003, 608001-608005, 609001-609002, 616001 703001-703003, 726001

Filter Name	Description	Corresponding Syslog Event or Netflow Event
IPsec VPN	These events are logged in an IPsec VPN-configured firewall when mismatches occur in IPsec security associations or when the system detects an error in the IPsec packets it receives.	402001-402148, 602102-602305, 702304-702307
NAT	These events are logged in a NAT-configured firewall when NAT entries are created or deleted and when all the addresses in a NAT pool are used up and exhausted.	201002-201013, 202001-202011, 305005-305012
SSL VPN	These events are logged in an SSL VPN-configurated firewall when WebVPN sessions get created or terminated, user access errors, and user activities.	716001-716060, 722001-722053, 723001-723014, 724001-724004, 725001-725015
NetFlow	These events are logged around the IP network traffic as network packets enter and exit the interfaces, timestamps, user identities, and the amount of data transferred.	0, 1, 2, 3, 5

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Connection	You can generate events for connections as users generate traffic that passes through the system. Enable connection logging on access rules to generate these events. You can also enable logging on Security Intelligence policies and SSL decryption rules to generate connection events. Connection events contain data about the detected sessions. The information available for any individual connection event depends on several factors, but in general includes: • Basic connection properties: timestamp, source and destination IP address, ingress and egress zones, the device that handled the connection, and so on. • Additional connection properties discovered or inferred by the system: applications, requested URLs, or users associated with the connection, and so on. • Metadata about why the connection was logged: which configuration handled the traffic, whether the connection was allowed or blocked, details about encrypted and decrypted connections, and so on.	430002, 430003
Intrusion	The system examines the packets that traverse your network for malicious activity that could affect the availability, integrity, and confidentiality of a host and its data. When the system identifies a possible intrusion, it generates an intrusion event, which is a record of the date, time, type of exploit, and contextual information about the source of the attack and its target. Intrusion events are generated for any intrusion rule set to block or alert, regardless of the logging configuration of the invoking access control rule.	430001

Filter Name	Description	Corresponding Syslog Event or Netflow Event
File	File events represent files that the system detected, and optionally blocked, in network traffic based on your file policies. You must enable file logging on the access rule that applies the file policy to generate these events. When the system generates a file event, the system also logs the end of the associated connection regardless of the logging configuration of the invoking access control rule.	430004
Malware	The system can detect malware in network traffic as part of your overall access control configuration. AMP for Firepower can generate a malware event, containing the disposition of the resulting event, and contextual data about how, where, and when the malware was detected. You must enable file logging on the access rule that applies the file policy to generate these events. The disposition of a file can change, for example, from clean to malware or from malware to clean. If AMP for Firepower queries the AMP cloud about a file, and the cloud determines the disposition has changed within a week of the query, the system generates retrospective malware events.	430005
Security Intelligence	Security Intelligence events are a type of connection event generated by the Security Intelligence policy for each connection that is blocked or monitored by the policy. All Security Intelligence events have a populated Security Intelligence Category field. For each of these events, there is a corresponding "regular" connection event. Because the Security Intelligence policy is evaluated before many other security policies, including access control, when a connection is blocked by Security Intelligence, the resulting event does not contain the information that the system would have gathered from subsequent evaluation, for example, user identity.	430002, 430003

Filter Name	Description	Corresponding Syslog Event or Netflow Event
AI Defense	AI Defense events provide a detailed record of activities within your AI environment, capturing interactions such as prompts submitted, responses generated, and any triggered AI Defense policy violations. These events include key information like timestamps, the application and AI model involved, the specific rule triggered, and the action taken. These event logs enable you to monitor AI usage in real time, detect threats, and enforce security policies effectively.	

Troubleshoot network problems using security and analytics logging events

Troubleshoot network problems using security and analytics logging events by reviewing symptoms, configuration details, likely causes, and corrective actions for managed devices.

This task helps network operations teams investigate and resolve user access issues by analyzing security and analytics logging events to identify which firewall rules OR policies are preventing network access.

Here is a basic framework you can use to troubleshoot network problems using the Events Viewer.

This scenario assumes that your network operations team has had a report that a user can't access a resource on the network. Based on the user reporting the issue and their location, the network operations team has a reasonable idea of which firewall controls their access to resources.

> **Note**
>
> This scenario also assumes that an FDM-managed device is the firewall managing the network traffic. Security Analytics and Logging does not collect logging information from other device types.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Events & Logs** > **Events** > **Event Logging**.
3. Click the **Historical** tab.
4. Start filtering events by **Time Range**. By default, the Historical tab shows the last hour of events. If that is the correct time range, enter the current date and time as the **End** time. If that is not the correct time range, enter a start and end time encompassing the time of the reported issue.
5. Enter the IP address of the firewall that you suspect is controlling the user's access in the **Sensor ID** field. If it could be more than one firewall, filter events using **attribute:value** pairs in the search bar. Make two entries and combine them with an OR statement. For example: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.
6. Enter the user's IP address in the **Source IP** field in the Events filter bar.
7. If the user can't access a resource, try entering that resource's IP address in the **Destination IP** field.

8. Expand the events in the results and look at their details. Here are some details to look at:
    - **AC_RuleAction** - The action taken (Allow, Trust, Block) when the rule was triggered.
    - **FirewallPolicy** - The policy in which the rule that triggered the event resides.
    - **FirewallRule** - The name of the rule that triggered the event. If the value is Default Action then it was the default action of the policy that triggered the event and not one of the rules in the policy.
    - **UserName** - The user associated with the initiator IP address. The Initiator IP address is the same as the Source IP address.
9. If the rule action is preventing access, look at the FirewallRule and FirewallPolicy fields to identify the rule in the policy that is blocking access.

You have identified the specific firewall rule OR policy that is preventing user access to network resources. Use this information to modify the appropriate firewall configuration to resolve the connectivity issue.

Caution: maintain active Cisco security analytics and logging subscription

Outlines the consequences of allowing your Cisco Security Analytics and Logging (SaaS) subscription to lapse and the critical timelines for data retention.

Maintain an active Cisco Security Analytics and Logging (SaaS) subscription to prevent data loss and preserve your ability to monitor, analyze, and respond to security threats using stored firewall events and behavioral analytics.

If you allow your Cisco Security Analytics and Logging (SaaS) paid subscription to lapse, collection of new events stops immediately. After 90 days from expiry, you will no longer be able to view or query your existing event data. You have 180 days to renew your subscription.

If you allow the 180-day grace period to lapse, the system purges all of your event data. You can no longer view security events on the **Event Logging** page, nor have dynamic entity modeling (DEM) behavioral analytics applied to your security events and network flow data.

52 Security Analytics and Logging Licenses

Topics:

- Security Analytics and Logging licenses

Learn how Security Analytics and Logging licensing works in Security Cloud Control, including subscriptions, free trials, ingest rates, storage usage, retention, alerts, and license management.

This chapter provides information on Security Analytics and Logging licenses.

Security Analytics and Logging licenses

Lists Security Analytics and Logging subscription options for managing firewall logs in Security Cloud Control, including per-device licenses and customizable log storage and retention.

Security Analytics and Logging subscriptions offer flexible options for managing firewall logs in Security Cloud Control, including per-device licenses and customizable log storage and retention. Choose between Essentials, Advantage, and Premier tiers to meet operational and compliance requirements, with retention periods up to five years and storage capacities up to 40 TB.

Security Analytics and Logging subscription overview

You can combine SAL with your Security Cloud Control subscription. When managing your firewalls with Security Cloud Control, you can obtain Security Analytics and Logging entitlement in these ways:

- Device management with unlimited logging: This option provides a per-device license. It includes device management capabilities for your firewall device and unlimited log storage for a rolling period of 90 days.
- Device management only with optional cloud logging: This option involves purchasing a per-device license for management only. You can then add Security Analytics and Logging as a separate cloud logging subscription. This allows you to customize logging data storage and log retention based on your specific operational and compliance needs.

90-day free trial

To accurately estimate your daily ingest rate, log in to Security Cloud Control and navigate to the **Events & Logs** > **Events** > **Event Logging** tab to request a 90-day trial. You can purchase the desired subscription plan to continue the service by reviewing the instructions in the Security Cloud Control Firewall Management Ordering Guide.

Security Analytics and Logging paid subscription tiers

If you choose not to use device management with unlimited logging option, you can purchase logging capacity separately. This standalone Security Analytics and Logging subscription provides greater flexibility, longer default retention, and increased storage entitlements. The default minimum retention period for these subscription tiers is 1 year.

Select these flexible Security Analytics and Logging subscription tiers if:

- You have already purchased your firewall devices as part of a different order.
- You have specific logging estimates and want to buy a tier based on a fixed amount of ingest, storage, and logging retention.
- You want a log retention period that is more than 90 days.

Security Analytics and Logging subscription is categorized into three tiers—Essentials, Advantage, and Premier. This table lists the storage capacities and log retention periods for each tier.

Description	Retention Period	Storage Limit	Subscription Term
Cisco SAL Essentials Subscriptions	1, 2, or 3 years	5 TB	0 to 5 years
Cisco SAL Advantage Subscriptions	1, 2, or 3 years	10 TB	0 to 5 years
Cisco SAL Premier Subscriptions	1, 2, or 3 years	40 TB	0 to 5 years

For more information about the subscription plans, refer to the Security Cloud Control Firewall Management Ordering Guide.

> **Note**
>
> For paid subscriptions, Security Analytics and Logging automatically manages your event data to ensure that it aligns with your licensed retention period. Security Analytics and Logging removes event data that is older than your specified retention period on a daily basis, and ensures that you always retain access to all event data within your full retention period.

Estimate your daily ingest rate

Purchase a subscription plan that matches the number of events the Cisco cloud receives from your onboarded firewall devices on a daily basis. This is called your *daily ingest rate*. You can use the Logging Volume Estimator tool to estimate your daily ingest rate and as that rate changes you can update your subscription plan.

Subscribing to a Security Analytics and Logging license

Describes the process for subscribing to a Security Analytics and Logging license, including starting a trial, purchasing a subscription, claiming licenses, and maintaining renewal.

Security Analytics and Logging trial provides full feature access for 90 days, allowing you to evaluate event logging performance, estimate daily ingest rates, and determine storage requirements. Gain valuable insights to select the optimal subscription and ensure continuous access to your firewall security data in the Cisco cloud.

Purchase a data storage plan that matches the daily event volume your onboarded security devices send to Cisco cloud. This volume is referred to as your daily ingest rate. Before making a purchase, participate in a free trial of Security Analytics and Logging to accurately estimate your daily ingest rate.

Summary

The key components involved in the Security Analytics and Logging subscription process are:

- Customer: Starts trial, evaluates performance, and determines subscription requirements
- Cisco representative or authorized partner: Facilitates subscription purchase
- Security Cloud Control administrator: Claims and activates subscription
- Trial period: 90 days with full feature access for evaluation
- Grace periods: 90 days for trial data retention, 180 days for paid subscription data retention

Workflow

These are the stages of subscribing to a Security Analytics and Logging license:

1. The customer starts a Security Analytics and Logging trial subscription to evaluate requirements and performance.
   - With this trial plan, you gain access to all Security Analytics and Logging features for 90 days.
   - During the 90-day trial period, your onboarded firewalls send events to Security Analytics and Logging. Monitor your event ingestion rates, understand your storage requirements, and evaluate performance. This data helps you to plan and select the most appropriate paid subscription.
   - If you activate a paid Security Analytics and Logging subscription while a trial is active, Security Cloud Control replaces the trial license for the product instance with the paid license and ends the trial.

- If you choose not to apply the paid subscription to the trial, event ingestion automatically stops after 90 days. After this, you cannot access Security Analytics and Logging features. However, your existing log data remains in the Security Analytics and Logging cloud for an additional 90 days from the trial expiry date.

> **Note**
>
> If you do not subscribe to a paid Security Analytics and Logging license within this 90-day grace period, all your trial data is permanently deleted.

This stage enables the customer to gain hands-on experience with Security Analytics and Logging capabilities and accurately determine their subscription requirements.

2. The customer orders a paid Security Analytics and Logging subscription based on trial insights.
   - Use the insights that you gained from your trial (daily ingest rate, required retention, storage volume) to determine the most suitable Security Analytics and Logging subscription plan.
   - Work with your Cisco representative or authorized partner to purchase the appropriate Security Analytics and Logging subscription.

   This stage ensures the customer selects a subscription plan that matches their actual usage requirements and establishes the commercial relationship.
3. The Security Cloud Control administrator claims the Security Analytics and Logging subscription to activate it.

   After you purchase a new Security Analytics and Logging subscription, you receive a claim code to activate it within Security Cloud Control. A welcome email containing your subscription claim code is automatically sent to the Provisioning Contact you specified during the purchasing process. If you included an End Customer contact, they also receive a copy. You will receive this email on the requested start date of your subscription.

   A Security Cloud Control administrator uses the claim code to activate the subscription for their organization. For detailed instructions on claiming and activating subscriptions, refer to Claim a Subscription.

   This stage completes the activation process and makes the paid subscription services available to the organization.
4. The customer maintains their Security Analytics and Logging subscription through timely renewal.

   Maintaining an active Security Analytics and Logging subscription ensures continuous logging and access to your historical data.
   - If your Security Analytics and Logging subscription expires without renewal, event ingestion from your firewalls stops immediately.
   - You can continue to view and search existing event data for 90 days after the subscription expires. After 90 days, event data is no longer accessible.
   - Your existing data remains in the Security Analytics and Logging cloud for a 180-day grace period from the subscription expiry date.
   - If the Security Analytics and Logging subscription is not renewed within this 180-day grace period, all your event data is permanently deleted from the Security Analytics and Logging cloud.

   This stage ensures continuous service availability and prevents data loss through proactive subscription management.

Result

The subscription process results in continuous access to Security Analytics and Logging logging services, properly sized to match actual usage requirements, with established renewal processes to prevent service interruption and data loss.

View Security Analytics and Logging license information

Configure monitoring of your Security Analytics and Logging license to track storage limits and retention periods. The dashboard helps you optimize event data management, prevent overages, and maintain compliance within your Security Cloud Control subscription.

Monitor your Security Analytics and Logging license to track storage limits and retention periods to optimize event data management and prevent overages.

View your Security Analytics and Logging license information such as the entitled monthly storage limit and the event storage retention period. If you do not have a separate Security Analytics and Logging license and data plan, you see the 90-day rolling data storage details in the licensing information.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Logging Settings**.
3. Click **View Logging Storage Usage**.

> **Tip**
>
> Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** and then click the **View Dashboard** button to view the Security Analytics and Logging license information.
>
> The **Event Logging Overview** dashboard provides a comprehensive overview of your Security Analytics and Logging license subscription:
>
> - **Retention policy**: Displays the event log retention period according to your subscription. Event data that is older than your retention period is removed daily, and you always retain access to all event data within your full retention period.
> - **Storage capacity**: Displays the total entitled data under your Security Analytics and Logging license, the amount of storage currently used, and the remaining available storage.

The Security Analytics and Logging license information is displayed, showing your entitled monthly storage limit, event storage retention period, and current usage details.

View Security Analytics and Logging Storage usage and event ingest rate

Configure insights into storage usage and event trends in Security Cloud Control with interactive dashboards.

Gain insights into storage usage and event trends in Security Cloud Control with interactive dashboards. Regular analysis helps you optimize event logging, adjust storage settings, prevent overages, and maintain efficient compliance and performance across your security environment.

View the current Security Analytics and Logging storage utilization and analyze event logging trends. You can analyze the storage utilization trends by event type, device type, and individual devices to gain deeper insights into storage utilization patterns. Use the data visualizations for quick and easy analysis. This helps you assess the current storage capacity and take measures to reduce the logging rate if the storage utilization approaches the limits that are specified in your Security Analytics and Logging license.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Logging Settings**.
3. Click **View Logging Storage Usage**.

> **Tip**
>
> Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** from the left navigation bar, and then click the **View Dashboard** button to view the Security Analytics and Logging storage usage and event ingestion trends.

4. Use these dashboards to customize and analyze storage utilization and gain insights into event logging trends in your firewall deployment:
   - **Usage Trends**: Displays the event logging storage usage for the last 12 months. Hover over a bar to see the data usage for the corresponding month.
   - **Events per second (EPS) trends**: Displays the event ingest rate for the onboarded devices. Customize your events per second trends view for a specific time period or device to get more granular data. You can filter the data for the past 1 week, 2 weeks, 3 weeks, or 1 month.

     > **Note**
     >
     > The device drop-down list displays the managed firewall devices that are sending events to the Cisco Security Cloud.

   - **Utilization by event type trends**: Displays event data storage used, in bytes per day, for different event types. Use this widget to monitor storage use by event types and identify surges, if any, or unusual changes in storage use for specific event types. This insight enables you to adjust logging settings for a specific event type and manage storage use.
   - **Utilization by device type trends**: Displays event data storage used, in bytes per day, for each managed device type. Use this widget to monitor storage use by the device type and identify surges, if any, or unusual changes in storage use for a specific type of device.
   - **Utilization by device trends**: Displays event data storage used, in bytes per day, for each security device that sends events to Security Cloud Control. This widget focuses on devices with storage use exceeding the average bytes per second value, showing only the top five devices to improve usability. Use this widget to monitor storage use for each device and identify surges or unusual changes. This insight allows you to adjust logging settings for specific devices and manage storage use effectively.

You can view storage utilization and event logging trends across multiple dashboards, allowing you to monitor usage patterns and make informed decisions about storage settings and event logging configurations.

Monitor Security Analytics and Logging service availability

Verify Security Analytics and Logging service availability, review FTD device event logging status, and check when Security Analytics and Logging last received events from managed Firewall Threat Defense devices.

Monitor the availability and health of Security Analytics and Logging(SaaS) service, review Firewall Threat Defense device event logging status, and determine when Security Analytics and Logging last received events from managed devices.

> **Note**
>
> The **Service Status** tab currently supports Firewall Threat Defense devices.

Before you begin

Enable the managed Firewall Threat Defense devices to send events to the Security Analytics and Logging cloud so you can view meaningful device logging status and last-event details.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Logging Settings**.
3. Click **View Logging Storage Usage**.

   > **Tip**
   >
   > Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** and then click the **View Dashboard** button to view the Security Analytics and Logging service status.

4. Click the **Service Status** tab.
5. Review the **SAL Service Availability** widget to check the current Security Analytics and Logging service status.

   If the Security Analytics and Logging service status displays **Degraded**, your Security Analytics and Logging service is affected and event ingestion might be delayed or disrupted.
6. Check the **Last Event Received** widget to determine when Security Analytics and Logging last received an event from a device.
7. Review the **Firewall Logging Status** widget to check Firewall Threat Defense device event logging status.
   - **Connected**: Indicates the number of Firewall Threat Defense devices that are enabled to send events to the Security Analytics and Logging.
   - **Disabled**: Indicates the number of Firewall Threat Defense devices that are disabled from sending events to the Security Analytics and Logging.
8. In the **Firewall Details** list, check when each Firewall Threat Defense device last sent an event to Security Analytics and Logging.

   Use this information along with **SAL Service Availability** and **Last Event Received** widgets to identify whether events might be delayed or not ingested.

If Firewall Threat Defense devices are disabled from sending events, review the device logging configuration. If the Security Analytics and Logging service status is **Unavailable** or **Degraded**, or if event ingestion appears delayed or disrupted, contact Cisco TAC for assistance.

You have reviewed the Security Analytics and Logging service status, device logging configuration, and last event timestamps to ensure proper event ingestion and identify any potential issues with the service or device connectivity.

Extend event storage duration and increase event storage capacity

Configure your Security Analytics and Logging license to extend event storage from the default 90 days to up to three years and increase storage capacity for long-term data retention and compliance.

Upgrade your Security Analytics and Logging license to extend event storage from the default 90 days to up to three years. Enhancing storage capacity ensures long-term data retention, compliance, and improved security visibility for network monitoring.

Perform this task when your organization needs increased event storage or retention.

Procedure

---

1. Log in to your account on Cisco Commerce.
2. Select your Security Cloud Control PID.
3. Follow the prompts to upgrade the duration or capacity of your storage.

   The increased cost will be prorated based on the term remaining on your existing license. See the Guidelines for Quoting Cisco Defense Orchestrator Products for detailed instructions.

Your Security Analytics and Logging license is upgraded with extended event storage duration and increased storage capacity based on your selected options.

View Security Analytics and Logging alerts

Configure real-time alerts for Security Analytics and Logging configuration and event issues on firewall devices. Addressing notifications promptly helps prevent data loss, maintain compliance, and ensure reliable security monitoring for your network.

Monitor and address Security Analytics and Logging configuration and event issues to maintain security compliance and prevent data loss.

View alerts and notifications for the Security Analytics and Logging configurations and event settings for the managed firewall devices.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Logging Settings**.
3. Click the **View Logging Storage Usage** button.

> **Tip**
>
> Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** from the left navigation bar, and then click **View Dashboard** to view the Security Analytics and Logging license information.

The **Alerts and Notifications** section displays alerts about the settings that impact event logging. These alerts enable you to take action to resolve any issues. Some of these settings include:

- Sending events to cloud setting is disabled.
- Sending events to the cloud setting is disabled at device level.
- Secure Event Connector becomes unavailable.
- Increase in events ingestion rate.
- Security Analytics and Logging license is expired or the allotted data storage is exceeded.

The **Alerts and Notifications** section displays current alerts for Security Analytics and Logging configurations and event settings, enabling you to identify and resolve issues that may impact event logging.

Frequently asked questions about Security Analytics and Logging license

Lists common questions about Security Analytics and Logging data allotment, storage management, license expiration, and retention periods.

Learn which events count toward your Security Analytics and Logging data allotment, how to manage storage limits, what happens if your license expires, and how retention periods affect long-term data storage. Gain practical tips to optimize storage and maintain continuous access to your security event data.

Which data gets counted against my Security Analytics and Logging allotment?

All events sent to the Cisco cloud directly or to the Secure Event Connector accumulate in Security Analytics and Logging and count against your data allotment.

Filtering the events viewer does not decrease the number of stored events in Security Analytics and Logging. It only reduces the number of events you see in the events viewer.

We're using up our storage allotment quickly. what should i do?

Here are two approaches to address that problem:

- Request more storage.
- Consider reducing the number of rules that log events. You can log events from SSL policy rules, security intelligence rules, access control rules, intrusion policies, and file and malware policies. Review your current logging settings to determine if you need to log events from all the rules and policies that you have configured.

What happens to my data if my Security Analytics and Logging license expires?

If your paid Security Analytics and Logging license expires, event ingestion from your firewalls stops immediately. However, your existing data remains accessible in the Security Analytics and Logging cloud for a 180-day grace period. If you renew your paid license during this grace period, your service continues without interruption. If you do not renew within these 180 days, all your data is permanently deleted.

If I purchase a Security Analytics and Logging subscription with a 1-year retention period and a 5-year term, will my data be stored for all 5 years?

The retention period defines how long each log is stored. With a 1-year retention period, only the most recent 1-year log data is available at any given time. Log data older than 1 year is overwritten or deleted when new data is collected. A 5-year term means that data for that duration will continue to be ingested, but the retention limit is applicable to the log data itself.

53 Secure Event Connectors

Topics:

- Secure event connectors
- Secure event connector installation
- Secure event connector removal
- Finding your device's TCP, UDP, and NSEL port used for secure logging analytics (SaaS)

Learn how Secure Event Connectors collect firewall events for Security Analytics and Logging, including connector installation options, AWS deployment, SEC identification, event port lookup, and removal workflows.

This chapter provides information about secure event connectors.

Secure event connectors

Describes Secure Event Connectors for ASA devices, including SEC destinations, ports, severity levels, custom event lists, and cloud event delivery.

A Secure Event Connector (SEC) is a component of the Security Analytics and Logging SaaS solution that

- receives events from ASA , and FDM-managed devices
- forwards events to the Cisco cloud for centralized analysis, and
- enables display of events on the **Event Logging** page in Security Cloud Control.

SEC deployment options

The SEC is installed on a Secure Device Connector deployed in your network, on its own Security Cloud Control Connector virtual machine deployed in your network, or on an AWS Virtual Private Cloud (VPC).

Secure Event Connector ID location:

1. From the Security Cloud Control menu on the left, choose **Administration** > **Secure Connectors**.
2. Click the SEC you wish to identify.
3. The SEC ID is the ID listed above the Tenant ID in the Details pane.

> **Note**
>
> You may need the ID of the SEC when working with Cisco Technical Assistance Center (TAC) or other Security Cloud Control Support.

Secure event connector installation

Describes the installation of Secure Event Connectors, including SEC destinations, ports, severity levels, custom event lists, and cloud event delivery.

A Secure Event Connector installation is a deployment process that enables installation of SECs on a tenant with or without an SDC configuration.

Installation options

You can install one SEC on the same virtual machine as a Secure Device Connector, if you have one; or you can install the SEC on it's own Security Cloud Control Connector virtual machine that you maintain in your network.

Install a secure event connector on an SDC virtual machine

Configure a Secure Event Connector (SEC) on the same virtual machine as a Secure Device Connector to receive and forward security events to the Cisco cloud.

The purpose of this task is to install a Secure Event Connector on an existing SDC virtual machine to enable centralized event logging and analysis.

The Secure Event Connector (SEC) receives events from ASA and FDM-managed devices and forwards them to the Cisco cloud. Security Cloud Control displays the events on the **Event Logging** page enabling you to analyze the security events from all devices in one place.

You can install one SEC on the same virtual machine as a Secure Device Connector, if you have one; or you can install the SEC on it's own Security Cloud Control Connector virtual machine that you maintain in your network.

This article describes installing an SEC on the same virtual machine as an SDC. If you want to install more SECs see Installing an SEC using a Security Cloud Control image on page 933 or SEC installation using VM images on page 939.

Before you begin

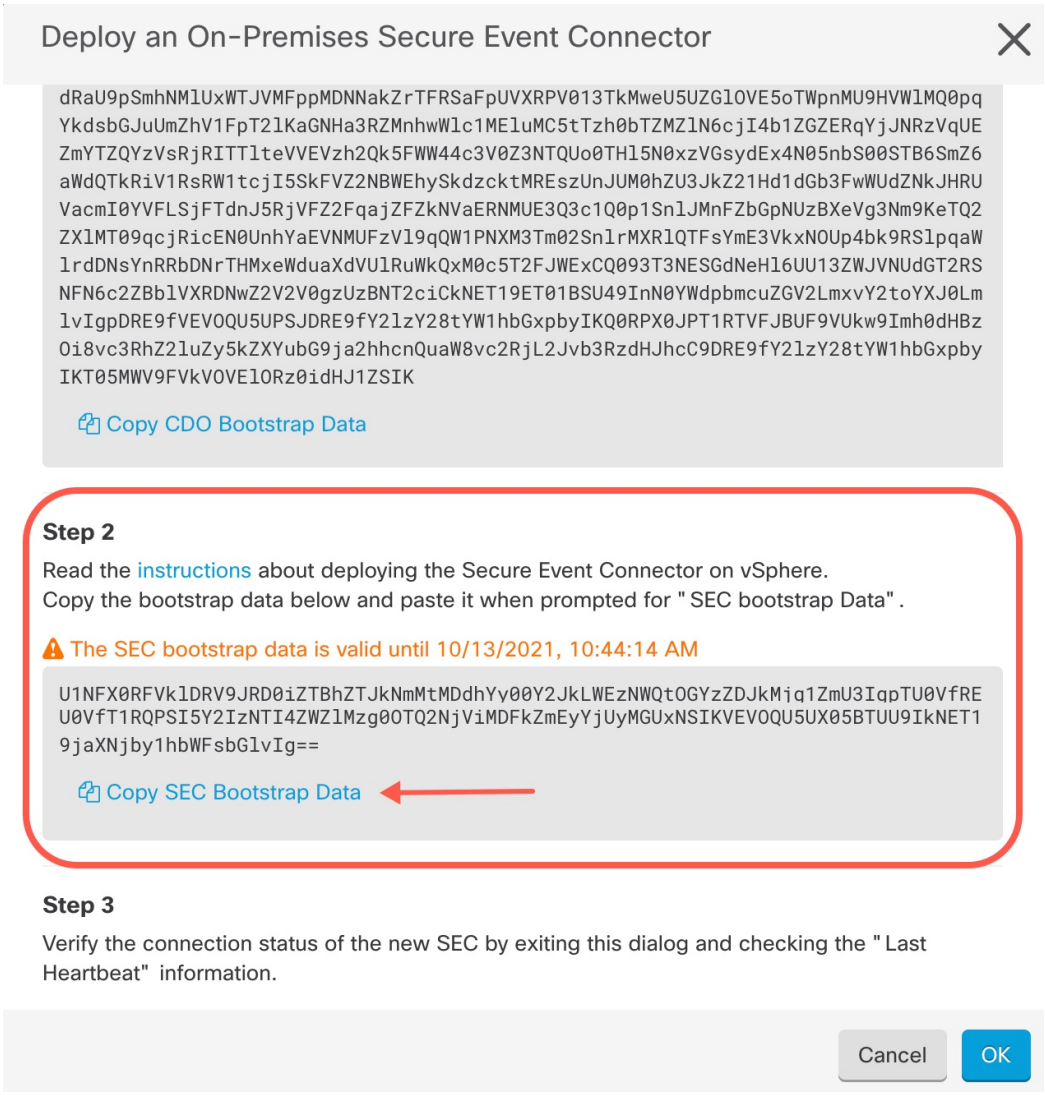
- Purchase the Cisco Security and Analytics Logging license. If you want to try Cisco Security and Analytics Logging out first, log in to Security Cloud Control, and on the main navigation bar, choose **Events & Logs** > **Events** > **Event Logging** and click **Request Trial**.
- Make sure your SDC has been installed. For more information, see Deploy a VM for running the secure device connector and secure event connector on page 78.
- Make sure the SDC is communicating with Security Cloud Control:
  1. In the left pane, click **Administration** > **Secure Connectors**.
  2. Make sure that the SDC's last heartbeat was less than 10 minutes prior to the installation of the SEC and that the SDC's status is active.
- System Requirements - Assign additional CPUs and memory to the virtual machine running the SDC:
  - CPU: Assign an **additional** 4 CPUs to accommodate the SEC to make a total of 6 CPU.
  - Memory: Assign an **additional** 8 GB of memory for the SEC to make a total of 10 GB of memory.

    After you have updated the CPU and memory on the VM to accommodate the SEC, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.

Follow these steps to install a Secure Event Connector on an SDC virtual machine:

Procedure

1. Log in to Security Cloud Control. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Administration** > **Secure Connectors**.
3. Click the  icon and then click **Secure Event Connector**.
4. Skip Step 1 of the wizard and go to Step 2. In step 2 of the wizard, click the link to **Copy SEC Bootstrap Data**.



5. Open a terminal window and log into the SDC as the "cdo" user.
6. Once logged in, switch to the "SDC" user. When prompted for a password, enter the password for the "cdo" user.

Example

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

7. At the prompt, run the **SEC.sh setup** script:

Example

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

8. At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

Example

```
Please copy the bootstrap data from Setup Secure Event Connector page of
Security Cloud Control: KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the SEC.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "SEC-health-check."



If you receive a message that the registration failed or that the SEC onboarding failed, go to Troubleshooting Secure Event connector Onboarding Failures.

9. Determine if the VM on which the SDC and SEC are running needs additional configuration:
   - If you installed your SDC on your own virtual machine, continue with Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created on page 946.
   - If you installed your SDC using a Security Cloud Control image, continue to "What to do Next."

The Secure Event Connector is now installed on your SDC virtual machine and is ready to receive events from ASA devices and forward them to the Cisco cloud for analysis in the Event Logging page.

Installing an SEC using a Security Cloud Control image

Describes the process for installing a Secure Event Connector (SEC) using a Security Cloud Control image to forward events from ASA and FTD devices to the Cisco cloud.

Installing an SEC using a Security Cloud Control image is a deployment process that

- enables the Secure Event Connector (SEC) to forward events from ASA and FTD devices to the Cisco cloud for viewing in the **Event Logging** page
- allows installation of multiple SECs on a tenant to distribute event forwarding workload across different locations, and
- requires a two-part process involving Security Cloud Control Connector installation and SEC configuration.

Installation process

Installing an SEC is a two-part process:

1. Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image on page 934 You need one Security Cloud Control Connector for every SEC you install. The Security Cloud Control Connector is different than a Secure Device Connector (SDC).
2. Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine on page 947.

> **Note**
>
> If you want to create a Security Cloud Control Connector by creating your own VM, see Install Multiple SECs for Your Tenant Using a VM Image you Create.

What to do next:

Continue with Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image on page 934

Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image

Configure a Security Cloud Control Connector using a VM image to support a Secure Event Connector installation.

Install a Security Cloud Control Connector on a virtual machine to provide the platform for deploying a Secure Event Connector that will handle security event logging and analytics.

This task is performed when you need to set up a Security Cloud Control Connector as the foundation for a Secure Event Connector deployment in your network infrastructure.

Before you begin

- Purchase the Cisco Security and Analytics Logging license.

  If you would rather, you can request a trial version of Security Analytics and Logging by logging in to Security Cloud Control, and on the main navigation bar, choose **Events & Logs** > **Events** > **Event Logging** and click **Request Trial**.

- Security Cloud Control requires strict certificate checking and does not support Web/Content Proxy inspection between the Security Cloud Control Connector and the Internet. If using a proxy server, disable inspection for traffic between the Security Cloud Control Connector and Security Cloud Control.
- **The** Security Cloud Control **Connector installed in this process must have full outbound access to the Internet on TCP port 443.**
- **Review** Connect to Security Cloud Control using Secure Device Connector **to ensure proper network access for the** Security Cloud Control **Connector.**
- Security Cloud Control supports installing its Security Cloud Control Connector VM OVF image using the vSphere web client or the ESXi web client.
- Security Cloud Control does not support installing the Security Cloud Control Connector VM OVF image using the VM vSphere desktop client.
- ESXi 5.1 hypervisor.
- System requirements for a VM intended to host only a Security Cloud Control Connector and an SEC:
  - VMware ESXi host needs 4 vCPU.
  - VMware ESXi host needs a minimum of 8 GB of memory.
  - VMware ESXi requires 64GB disk space to support the virtual machine depending on your provisioning choice.
- Gather this information before you begin the installation:
  - Static IP address you want to use for your Security Cloud Control Connector VM.
  - Passwords for the **root** and Security Cloud Control users that you create during the installation process.

- The IP address of the DNS server your organization uses.
- The gateway IP address of the network the SDC address is on.
- The FQDN or IP address of your time server.

- The Security Cloud Control Connector virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.

Follow these steps to install a Security Cloud Control Connector using a VM image:

Procedure

1. Log on to the Security Cloud Control tenant you are creating the Security Cloud Control Connector for.
2. From the Security Cloud Control Home page, click **Firewall**.
3. In the left pane, click **Administration** > **Secure Connectors**.
4. Click the + icon and then click **Secure Event Connector**.
5. In Step 1, click **Download the Security Cloud Control Connector VM image**. This is a special image that you install the SEC on. Always download the Security Cloud Control Connector VM to ensure that you are using the latest image.



6. Extract all the files from the .zip file. They will look similar to these:
   - Security Cloud Control-SDC-VM-ddd50fa.OVF
   - Security Cloud Control-SDC-VM-ddd50fa.mf
   - Security Cloud Control-SDC-VM-ddd50fa-disk1.vmdk
7. Log on to your VMware server as an administrator using the vSphere Web Client.

> **Note**
>
> Do not use the VM vSphere desktop client.

8. Deploy the on-premises Security Cloud Control Connector virtual machine from the OVF template by following the prompts. (You will need the .OVF, .mf, and .vdk files to deploy the template.)
9. When the setup is complete, power on the VM.
10. Open the console for your new Security Cloud Control Connector VM.
11. Login as the Security Cloud Control user. The default password is **adm123**.
12. At the prompt type **sudo SDC-onboard setup**

Example

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

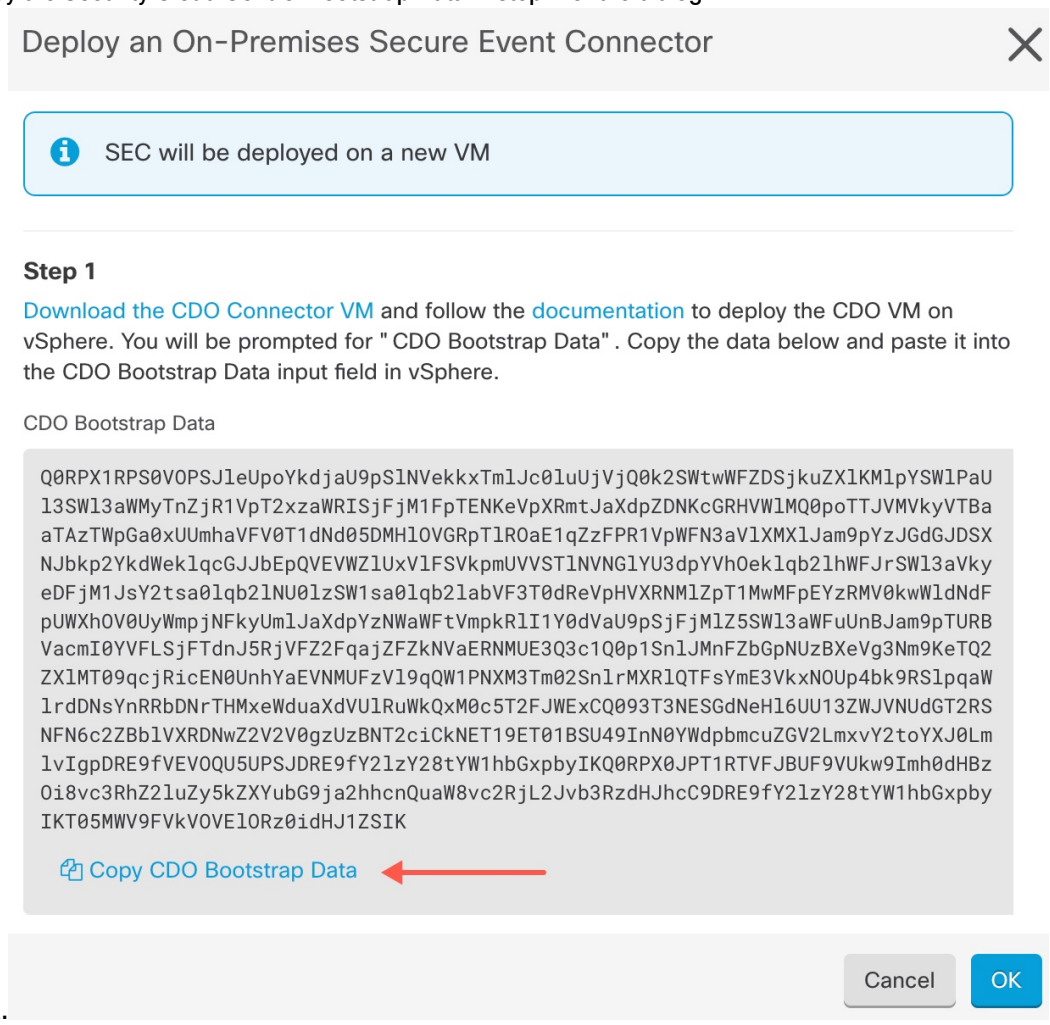
13. When prompted, enter the default password for the Security Cloud Control user: **adm123**.
14. Follow the prompts to create a new password for the **root** user.
15. Follow the prompts to create a new password for the Security Cloud Control user.
16. Follow the prompts to enter your Security Cloud Control domain information.
17. Enter the static IP address you want to use for the Security Cloud Control Connector VM.
18. Enter the gateway IP address for the network on which the Security Cloud Control Connector VM is installed.
19. Enter the NTP server address or FQDN for the Security Cloud Control Connector.
20. When prompted, enter the information for the Docker bridge or leave it blank if it is not applicable and press <Enter>.
21. Confirm your entries.
22. When prompted "Would you like to setup the SDC now?" enter **n**.
23. Create an SSH connection to the Security Cloud Control Connector by logging in as the Security Cloud Control user.
24. At the prompt type **sudo SDC-onboard bootstrap**

Example

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

25. When prompted, enter the Security Cloud Control user's password.
26. When prompted, return to Security Cloud Control and copy the Security Cloud Control bootstrap data, then paste it into your SSH session. To copy the Security Cloud Control bootstrap data:
    a. Log into Security Cloud Control.
    b. In the left pane, click **Administration** > **Secure Connectors**.
    c. Select the Secure Event Connector which you started to onboard. The status should show, "Onboarding."
    d. In the **Actions** pane, click **Deploy an On-Premises Secure Event Connector**.

e. Copy the Security Cloud Control Bootstrap Data in step 1 of the dialog box.



27. When prompted, **Would you like to update these settings?** enter **n**.
28. Return to the **Deploy an On-Premises Secure Event Connector** dialog in Security Cloud Control and click **OK**. In the **Secure Connectors** page, you will see your Secure Event Connector is in the yellow Onboarding state.

    Continue to Install the Secure Event Connector on the Security Cloud Control Connector VM on page 937.

Your Security Cloud Control Connector VM is successfully installed and configured, with the Secure Event Connector in an onboarding state ready for the next installation phase.

Install the Secure Event Connector on the Security Cloud Control Connector VM

Configure the Secure Event Connector on the Security Cloud Control Connector VM by deploying and setting up the connector using bootstrap data.

This task enables secure event logging by installing and configuring the Secure Event Connector on your Security Cloud Control Connector VM to establish communication between on-premises devices and the cloud-based logging service.

The Secure Event Connector enables secure logging analytics for your security devices by creating a secure tunnel between your on-premises environment and the cloud logging service. This connector must be properly installed and configured to ensure events are successfully transmitted and logged.

Before you begin

You should have installed Security Cloud Control Connector VM as described inInstall a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image on page 934 .

Follow these steps to install the Secure Event Connector on the Security Cloud Control Connector VM:

Procedure

1. Log in to Security Cloud Control. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Administration** > **Secure Connectors**.
3. Select the Security Cloud Control Connector that you onboarded above. In the Secure Connectors table, it will be called a Secure Event Connector and it should still be in the "Onboading" status.
4. Click **Deploy an On-Premises Secure Event Connector** in the Actions pane on the right.
5. In **step 2** of the wizard, click the link to **Copy SEC bootstrap data**.
6. Create an SSH connection to the Security Cloud Control Connector and log in as the **CDO** user.
7. Once logged in, switch to the **sdc** user. When prompted for a password, enter the password for the "Security Cloud Control" user. Here is an example of those commands:

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

8. At the prompt, run the SEC.sh setup script:

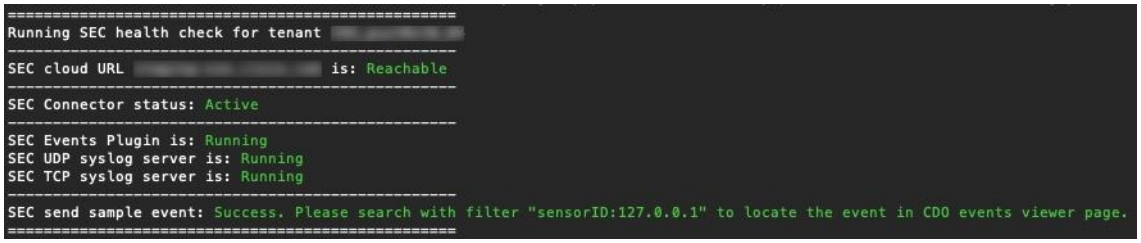
```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

9. At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE

RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the SEC.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "SEC-health-check."



If you receive a message that the registration failed or that the SEC onboarding failed, go to Troubleshoot SEC onboarding failures on page 1081.

If you receive the success message return to Security Cloud Control and click **Done on the Deploy an ON-Premise Secure Event Connector** dialog box.

Return to Implement secure logging analytics (SaaS) for ASA devices on page 329 .

The Secure Event Connector is successfully installed and configured on the Security Cloud Control Connector VM. The connector establishes a secure communication channel for event logging, and a health check event appears in the Event Log confirming proper operation.

Deploy secure event connector on ubuntu virtual machine

Configure the Secure Event Connector deployment on an Ubuntu virtual machine using the bootstrap data from CDO.

Deploy the Secure Event Connector on your Ubuntu VM to enable event collection and management through CDO.

The Secure Event Connector allows you to collect and forward security events from your network devices to CDO for centralized monitoring and analysis. This deployment process requires bootstrap data from CDO to establish the secure connection.

Before you begin

You should have installed Secure Device Connector on your Ubuntu VM as described in Deploy a VM for running the secure device connector and secure event connector on page 78.

Follow these steps to deploy Secure Event Connector on Ubuntu Virtual Machine:

Procedure

1. Log on to Security Cloud Control.
2. From the Security Cloud Control Home page, click **Firewall**.
3. From the left pane, **Administration** > **Secure Connectors**.
4. Click the  icon and then click **Secure Event Connector**.
5. Copy the SEC bootstrap data in step 2 on the window to a notepad.
6. Execute the following commands:

```
[sdc@vm]:~$sudo su sdc
```

```
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```

When prompted, enter the SEC bootstrap data that you have copied.

```
sdc@vm:~/toolkit$ ./sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of
CDO:
Successfully on-boarded SEC
```

It may take a few minutes for the Secure Event Connector to become "Active" in Security Cloud Control.

The Secure Event Connector is successfully deployed and becomes "Active" in CDO, enabling event collection and forwarding from your network devices.

SEC installation using VM images

Describes the process of installing a Secure Event Connector using your own virtual machine image to forward events from ASA and FTD devices to the Cisco cloud.

A SEC installation using VM images is a deployment method that

- forwards events from ASA and FTD to the Cisco cloud so that you can view them in the **Event Logging** page in Security Cloud Control

- allows installation of multiple Secure Event Connectors on your tenant to direct events from your ASAs and FDM-managed devices to any of the SECs you install, and
- enables distribution of event forwarding work across different regions by having SECs installed in different locations.

Installation process requirements

Installing multiple SECs using your own VM image requires completion of these steps:

1. Install a Security Cloud Control Connector to Support an SEC Using Your VM Image on page 940
2. Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created on page 946
3. Install the Secure Event Connector

> **Note**
>
> Using a Security Cloud Control VM image for the Security Cloud Control Connector is the easiest, most accurate, and preferred method of installing a Security Cloud Control connector. If you want to use that method, see Installing an SEC using a Security Cloud Control image on page 933.

Continue to Install a Security Cloud Control Connector to Support an SEC Using Your VM Image on page 940 to begin the installation process.

Install a Security Cloud Control Connector to Support an SEC Using Your VM Image

To install and configure a Secure Event Connector (SEC) on a virtual machine so it can securely transmit event data to Cisco Security Analytics and Logging (SaaS). This ensures proper integration and secure communication between your organization's environment and Cisco's security analytics platform.

The Security Cloud Control Connector VM is a virtual machine on which you install an SEC. The purpose of the Security Cloud Control Connector is solely to support an SEC for Cisco Security Analytics and Logging (SaaS) customers.

This is the first of three steps you need to complete in order install and configure your Secure Event Connector (SEC). After this procedure, you need to complete the following procedures:

- Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created on page 946
- Install the Secure Event Connector

Before you begin

- Purchase a Security and Analytics Logging (SaaS) subscription plan. For more information about the subscription plans, refer to the Security Cloud Control Firewall Management Ordering Guide .

  If you would rather, you can request a trial version of Security Analytics and Logging by logging in to Security Cloud Control , and on the main navigation bar, choose **Events & Logs** > **Events** > **Event Logging** and click **Request Trial** .
- Security Cloud Control requires strict certificate checking and does not support a Web/Content Proxy between the Security Cloud Control Connector and the Internet.
- **The Security Cloud Control Connector must have full outbound access to the Internet on TCP port 443.**

- **Review** Connect to Security Cloud Control using Secure Device Connector **to ensure proper network access for the Security Cloud Control Connector.**
- VMware ESXi host installed with vCenter web client or ESXi web client.

> **Note**
>
> We do not support installation using the vSphere desktop client.

- ESXi 5.1 hypervisor.
- Ubuntu 22.04 and Ubuntu 24.04.
- System requirements for a VM to host only a Security Cloud Control Connector and an SEC:
  - CPU: Assign 4 CPUs to accommodate the SEC.
  - Memory: Assign 8 GB of memory for the SEC.
  - Disk Space: 64 GB
- Users performing this procedure should be comfortable working in a Linux environment and using the **vi** visual editor for editing files.
- Gather this information before you begin the installation:
  - Static IP address you want to use for your Security Cloud Control Connector.
  - Passwords for the **root** and **Security Cloud Control** users that you create during the installation process.
  - The IP address of the DNS server your organization uses.
  - The gateway IP address of the network the Security Cloud Control Connector address is on.
  - The FQDN or IP address of your time server.
- The Security Cloud Control Connector virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.
- **Before you get started** : Do not copy and paste the commands in this procedure into your terminal window, type them instead. Some commands include an "n-dash" and in the cut and paste process, these commands can be applied as an "m-dash" and that may cause the command to fail.

Procedure

1. Log on to Security Cloud Control .
2. From the Security Cloud Control Home page, click **Firewall**.
3. From the left pane, **Administration** > **Secure Connectors** .
4. Click the + icon and then click **Secure Event Connector** .
5. Using the link provided, copy the SEC Bootstrap Data in step 2 of the "Deploy an On-Premises Secure Event Connector" window.
6. Once installed, configure basic networking such as specifying the IP address for the Security Cloud Control Connector, the subnet mask, and gateway.
7. Configure a DNS (Domain Name Server) server.
8. Configure a NTP (Network Time Protocol) server.

9. Install an SSH server for easy interaction with Security Cloud Control Connector's CLI.
10. Install the **AWS CLI package** (https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html)

> **Note**
>
> Do not use the `--user` flag.

11. Install the **Docker CE packages** (https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce)

> **Note**
>
> Use the "Install using the repository" method.

12. Start the Docker service and enable it to start on boot:

```
                        [root@sdc-vm ~]#
                        systemctl start docker
 [root@sdc-vm ~]#
                        systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service
 to /usr/lib/systemd/system/docker.service.
```

13. Create two users: **Security Cloud Control** and **sdc.** The Security Cloud Control user will be the one you log-into to run administrative functions (so you don't need to use the root user directly), and the sdc user will be the user to run the Security Cloud Control Connector docker container.

```
                        [root@sdc-vm ~]#
                        useradd
                        Security Cloud Control
 [root@sdc-vm ~]#
                        useradd sdc -d /usr/local/
                        Security Cloud Control
```

14. Configure the sdc user to use crontab:

```
                        [root@sdc-vm ~]#
                        touch /etc/cron.allow
[root@sdc-vm ~]#
                        echo "sdc" >> /etc/cron.allow
```

15. Set a password for the Security Cloud Control user.

```
                        [root@sdc-vm ~]#
                        passwd
```

```
                        Security Cloud Control
Changing password for user
                        Security Cloud Control
                        .
New password:
                        <type password>
Retype new password:
                        <type password>
passwd: all authentication tokens updated successfully.
```

16. Add the Security Cloud Control user to the "wheel" group to give it administrative (sudo) privileges.

```
                        [root@sdc-vm ~]#
                        usermod -aG wheel
                        Security Cloud Control
 [root@sdc-vm ~]#
```

17. When Docker is installed, there is a user group created. Depending on the version of CentOS/Docker, this may be called either "docker" or "dockerroot". Check the /etc/group file to see which group was created, and then add the sdc user to this group.

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

18. If the `/etc/docker/daemon.json` file does not exist, create it, and populate with the contents below. Once created, restart the docker daemon.

> **Note**
>
> Make sure that the group name entered in the "group" key matches the group you found in the /etc/group file .

```
                         [root@sdc-vm ~]#
                        cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "
                        docker
                        "
}
[root@sdc-vm ~]#
                        systemctl restart docker
[root@sdc-vm ~]#
```

19. If you are currently using a vSphere console session, switch over to SSH and log in as the **Security Cloud Control** user. Once logged in, change to the **sdc** user. When prompted for a password, enter the password for the **Security Cloud Control** user.

```
                        [
                        Security Cloud Control
                        @sdc-vm ~]$
                        sudo su sdc
[sudo] password for
                        Security Cloud Control
                        : <
                        type password for
                        Security Cloud Control
                        user
                        >
[sdc@sdc-vm ~]$
```

20. Change directories to **/usr/local/** Security Cloud Control **.**
21. Create a new file called **bootstrapdata** and paste the bootstrap data from Step 1 of the deployment wizrd into this file. **Save** the file. You can use **vi** or **nano** to create the file.
22. The bootstrap data comes encoded in base64. Decode it and export it to a file called **extractedbootstrapdata**

```
                         [sdc@sdc-vm ~]$
                        base64 -d /usr/local/
                        Security Cloud Control
                        /bootstrapdata > /usr/local/
                        Security Cloud Control
                        /extractedbootstrapdata
[sdc@sdc-vm ~]$
```

Run the cat command to view the decoded data. The command and decoded data should look similar to this:

```
                        [sdc@sdc-vm ~]$
                        cat /usr/local/
                        Security Cloud Control
                        /extractedbootstrapdata
                        Security Cloud Control
                        _TOKEN="<token string>"
                        Security Cloud Control
                        _DOMAIN="www.defenseorchestrator.com"
                        Security Cloud Control
                        _TENANT="<tenant-name>"
<
                        Security Cloud Control
                        _URL>/sdc/bootstrap/
                        Security Cloud Control

_acm="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

23. Run the following command to export the sections of the decoded bootstrap data to environment variables.

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > secenv &&
source secenv
[sdc@sdc-vm ~]$
```

24. Download the bootstrap bundle from Security Cloud Control .

```
                         [sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $
                        Security Cloud Control
                        _TOKEN" "$
                        Security Cloud Control
                        _BOOTSTRAP_URL" -o $
                        Security Cloud Control
                        _TENANT.tar.gz
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$
                        ls -l /usr/local/
                        Security Cloud Control
                        /*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/
                        Security Cloud Control
                        /

                            Security Cloud Control
                            _<tenant_name>
```

25. Extract the Security Cloud Control Connector tarball, and run the bootstrap_sec_only.sh file to install the Security Cloud Control Connector package.

```
                         [sdc@sdc-vm ~]$
                        tar xzvf /usr/local/
                        Security Cloud Control
                        /tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$
                        /usr/local/
                        Security Cloud Control
                        /bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/
                        Security Cloud Control
                        /toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/
                        Security Cloud Control
                        /toolkit/toolkit.log
```

```
0 2 * * * sleep 30 && /usr/local/
                        Security Cloud Control
                        /toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/
                        Security Cloud Control
                        /toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

Continue to Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created on page 946 .

Your Secure Event Connector (SEC) is installed on your VM image, configured to securely forward events to Cisco Security Analytics and Logging (SaaS), and ready for ongoing maintenance and updates.

Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created

Configure additional firewall settings on your CentOS 7 virtual machine to allow events to reach the SEC.

This configuration ensures that events can reach the SEC when you have installed your Security Cloud Control Connector on your own CentOS 7 virtual machine.

This is the second of three steps you need to complete in order to install and configure your SEC. If you have not already, complete Install a Security Cloud Control Connector to Support an SEC Using Your VM Image on page 940 before making these configuration changes.

After you complete one of the additional configuration changes described here, complete Install the Secure Event Connector

Before you begin

You must have installed your Security Cloud Control Connector on your own CentOS 7 virtual machine.

Follow these steps to configure additional settings for your SDC and Security Cloud Control Connector:

Procedure

---

1. Choose one of the following configuration procedures:
   - Disable the firewalld service on the CentOS 7 VM (matches the configuration of the Cisco-provided SDC VM)
   - Allow the firewalld service to run and add firewall rules to allow event traffic to reach the SEC (more granular approach)
2. If you chose to disable the firewalld service, log into the CLI of the SDC VM as the "Security Cloud Control" user.
3. Stop the firewalld service and ensure that it will remain disabled upon subsequent reboots of the VM.

   If you are prompted, enter the password for the **Security Cloud Control** user.

   Example

   ```
   [Security Cloud Control@SDC-VM ~]$ sudo systemctl stop firewalld
   Security Cloud Control@SDC-VM ~]$ sudo systemctl disable firewalld
   ```

4. Restart the Docker service to re-insert Docker-specific entries into the local firewall.

Example

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart docker
```

5. If you chose to allow the firewalld service to run, log into the CLI of the SDC VM as the "Security Cloud Control" user.
6. Add local firewall rules to allow incoming traffic to the SEC from the TCP, UDP, or NSEL ports you configured.

   See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging for the ports used by your SEC. If prompted, enter the password for the **Security Cloud Control** user. You may need to specify different port values.

   Example

```
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
 --add-port=10125/tcp
Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
 --add-port=10025/udp
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
 --add-port=10425/udp
```

7. Restart the firewalld service to make the new local firewall rules both active and persistent.

   Example

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart firewalld
```

You have successfully configured the firewall settings on your CentOS 7 virtual machine to allow events to reach the SEC. Next, continue to Install the Secure Event Connector.

Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine

Configure the Secure Event Connector (SEC) on your Security Cloud Control Connector Virtual Machine by completing the onboarding process.

This procedure completes the installation and configuration of your Secure Event Connector (SEC) on your virtual machine, enabling secure event logging and analytics capabilities.

This is the final step in a three-part process to deploy a Secure Event Connector. The SEC enables secure event logging and analytics for your devices managed through Security Cloud Control.

Before you begin

This is the third of three steps you need to complete in order to install and configure your Secure Event Connector (SEC). If you have not already, complete the following tasks before continuing with this procedure:

- Install a Security Cloud Control Connector to Support an SEC Using Your VM Image on page 940.
- Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created on page 946.

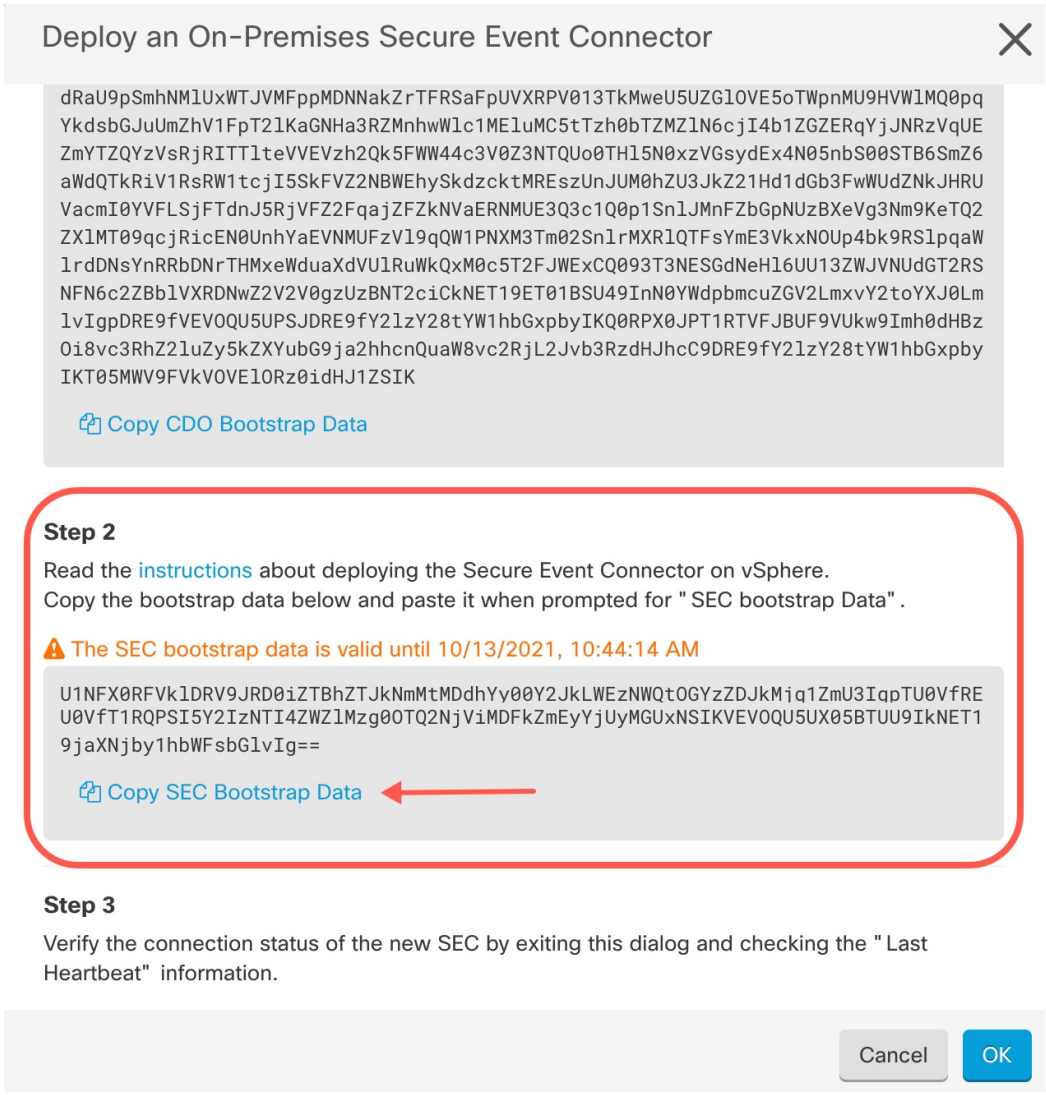
Follow these steps to install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine:

Procedure

---

1. Log in to Security Cloud Control. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, **Administration** > **Secure Connectors**.

3. Select the Security Cloud Control Connector that you installed using the procedure in the prerequisites above. In the Secure Connectors table, it will be displayed as Secure Event Connector.
4. Click **Deploy an On-Premises Secure Event Connector** in the **Actions** pane on the right.
5. In **step 2** of the wizard, click the link to **Copy SEC Bootstrap Data**.



6. Connect to the Secure Connector using SSH and log in as the Security Cloud Control user.
7. Once logged in, switch to the **sdc** user. When prompted for a password, enter the password for the "Security Cloud Control" user. Here is an example of those commands:

Example

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

8. At the prompt, run the SEC.sh setup script:

Example

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

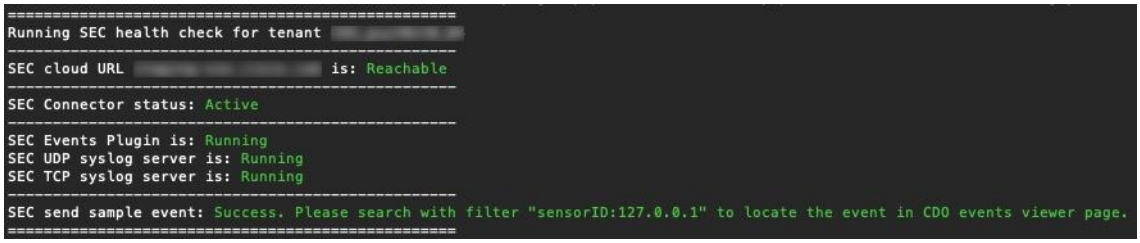
9. At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

Example

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:

 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the SEC.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "SEC-health-check."



If you receive a message that the registration failed or that the SEC onboarding failed, go to Troubleshooting Secure Event Connector Onboarding Failures.

If you receive the success message, click **Done** in the **Deploy an ON-Premise Secure Event Connector** dialog box.You have finished installing an SEC on a your VM image.

The Secure Event Connector is successfully installed and configured on your virtual machine. The SEC performs health checks and sends a sample event to verify proper operation.

Install a secure event connector on an AWS VPC using a terraform module

Configure deployment of a secure event connector on your AWS VPC using a Terraform module.

This task enables you to deploy a secure event connector on your AWS VPC infrastructure using Terraform automation, allowing for secure log collection and transmission to Security Cloud Control.

Use this procedure when you need to establish a secure event connector in an AWS VPC environment for centralized logging and analytics. The Terraform module automates the deployment process and ensures proper security configurations.

Before you begin

- To perform this task, you must enable SAL on your Security Cloud Control tenant. This section presumes that you have a SAL license. If you do not have one, purchase the Cisco Security and Analytics Logging, Logging and Troubleshooting license.
- Ensure you have a new SEC installed. To create a new SEC, see Install a secure event connector on an SDC virtual machine on page 930.
- When installing the SEC, make sure you take a note of the Security Cloud Control bootstrap data and SEC bootstrap data.

Follow these steps to install a secure event connector on an AWS VPC using a Terraform module:

Procedure

1. Go to Secure Event Connector Terraform Module on the Terraform Registry and follow the instructions to add the SEC Terraform module to your Terraform code and apply.
2. Ensure that you print the **instance_id** and **sec_fqdn** outputs, because you will need them later in the procedure.

   > **Note**
   >
   > To troubleshoot your SEC, you must connect to your SEC instance using the AWS Systems Manager Session Manager (SSM). See the AWS Systems Manager Session Manager documentation to know more about connecting to an instance using SSM.

   Ports to connect to the SDC instance using SSH are not exposed for secuirty reasons.

3. To enable sending of logs from your ASA to the SEC, obtain the certificate chain of the SEC you created and remove the leaf certificate by running this command with the output from Step 3:

   ```
   rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect
   <FQDN>:10125 < /dev/null | awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{
   if(/BEGIN CERTIFICATE/){a++}; out="/tmp/cert_chain.pem"; if(a > 1) print
   >>out}'
   ```

4. Copy the contents of **/tmp/cert_chain.pem** to your clipboard.
5. Take a note of the IP address of the SEC using this command:

   ```
   nslookup <FQDN>
   ```

6. Log in to Security Cloud Control and start adding a new trustpoint object.

   See Adding a Trusted CA Certificate Object for more information. Ensure you uncheck the **Enable CA flag in basic constraints extension** checkbox in **Other Options** before clicking **Add**.

7. Click **Add**, copy the CLI commands generated by Security Cloud Control in the **Install Certificate** page, and click **Cancel**.
8. Below **enrollment terminal**, add **no CA-check** in a text clipboard.
9. SSH into your ASA device or use the ASA CLI option in Security Cloud Control and execute these commands:

   ```
   DataCenterFW-1> en
   Password: ****************
   DataCenterFW-1# conf t
   DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
   DataCenterFW-1(config)# wr mem
   Building configuration...
   Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
   ```

   What to do next: You can check if your SEC is receiving packets using AWS SSM:

   You should now see logs similar to this:

   ```
   time="2023-05-10T17:13:46.135018214Z" level=info
   msg="[ip-10-100-5-19.ec2.internal][util.go:67 plugin.createTickers:func1]
   Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
   ```

The secure event connector is successfully deployed on your AWS VPC and configured to receive logs from your ASA device. The SEC will begin processing and forwarding security events to Security Cloud Control for analysis and monitoring.

Secure event connector removal

Describes how to remove the Secure Event Connector, including SEC destinations, ports, severity levels, custom event lists, and cloud event delivery.

Secure Event Connector removal is a process that

- deletes the Secure Event Connector from the Secure Device Connector
- prevents the use of Secure Logging Analytics (SaaS), and
- is not reversible once completed.

Removal process

Warning

This procedure deletes the Secure Event Connector from the Secure Device Connector. Doing so will prevent you from using Secure Logging Analytics (SaaS). It is not reversible. If you have any questions or concerns, contact Security Cloud Control support before taking this action.

Removing the Secure Event Connector from your Secure Device Connector is a two-step process:

1. Remove SEC from Security Cloud Control.
2. Remove SEC files from the SDC.

What to do next: Continue to Remove SEC from Security Cloud Control

Remove an SEC from Security Cloud Control

Configure the removal of a Secure Event Connector from your Security Cloud Control management interface.

This task removes an SEC (Secure Event Connector) from your Security Cloud Control management system when it is no longer needed or when troubleshooting connectivity issues.

Use this procedure when you need to disconnect and remove a Secure Event Connector from your Security Cloud Control environment. This is typically done during device decommissioning or when reconfiguring your security infrastructure.

Before you begin

See Secure event connector removal on page 951.

Procedure

1. Log in to Security Cloud Control.
2. From the Security Cloud Control Home page, click **Firewall**.
3. From the left pane, choose **Administration** > **Secure Connectors**.
4. Select the row with the device type, **Secure Event Connector**.

> **Warning**
>
> Be careful NOT to select your Secure Device Connector.

5. In the **Actions** pane, click **Remove**.
6. Click **OK** to confirm.

   Continue to Remove a secure event connector from the secure device connector VM on page 952.

The Secure Event Connector is successfully removed from Security Cloud Control and no longer appears in the connector list.

Remove a secure event connector from the secure device connector VM

Configure the removal of a Secure Event Connector from your SDC virtual machine using command line interface.

Remove the Secure Event Connector from your Secure Device Connector virtual machine to complete the SEC removal process.

This is the second part of a two part procedure to remove the Secure Event Connector from your SDC. See Secure event connector removal on page 951 before you begin.

Procedure

---

1. Open your virtual machine hypervisor and start a console session for your SDC.
2. Switch to the SDC user using the command **sudo su SDC**.

   Example

   ```
   [cdo@sdc]$ sudo su sdc
   ```

3. Remove the SEC from the SDC virtual machine using one of the following commands:
   - If you want to use the tenant selector (or if there's only one tenant on the VM):

     ```
     [sdc@tenant toolkit]$ sdc eventing delete
     ```

   - If you want to specify the tenant directly in the command arguments:

     ```
     [sdc@tenant toolkit]$ sdc eventing delete CDO_{tenant-name}
     ```

4. Confirm your intention to remove the SEC files.

The Secure Event Connector is successfully removed from the Secure Device Connector virtual machine.

Finding your device's TCP, UDP, and NSEL port used for secure logging analytics (SaaS)

Configure your device to find the TCP, UDP, and NSEL ports used for secure logging analytics (SaaS) for ASA devices, including SEC destinations, ports, severity levels, custom event lists, and cloud event delivery.

This task helps you identify the correct TCP, UDP, and NSEL ports that your Secure Event Connector (SEC) uses to receive events from your ASA or FDM-managed devices for Secure Logging Analytics (SaaS).

Secure Logging Analytics (SaaS) allows you to send events from your ASA or FDM-managed devices to certain UDP, TCP, or NSEL ports on the Secure Event Connector (SEC). The SEC then forwards those events to the Cisco cloud.

If these ports aren't already in use, the SEC makes them available to receive events and the Secure Logging Analytics (SaaS) documentation recommends using them when you configure the feature.

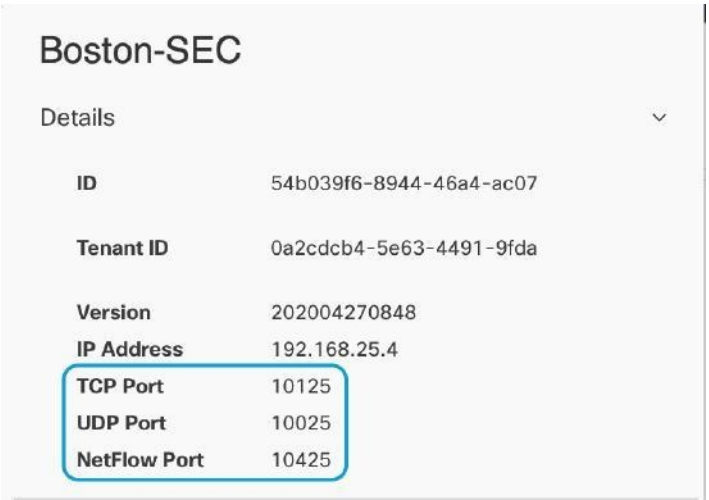
- TCP: 10125
- UDP: 10025
- NSEL: 10425

If those ports are already in use, before you configure Secure Logging Analytics (SaaS), look at your SEC device details to determine what ports it is actually using to receive events.

Follow these steps to find the port numbers the SEC uses:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. From the left pane, click **Administration** > **Integrations** > **Firewall Management Center** and then click the **Secure Connectors** tab.
3. In the **Secure Connectors** page, select the SEC you want to send events to.
4. In the **Details** pane, you will see the TCP, UDP, and NetFlow (NSEL) port you should send events to.



The Details pane displays the specific TCP, UDP, and NetFlow (NSEL) ports that your SEC is configured to use for receiving events from your devices.

54 Monitor Catalyst SD-WAN Events

Topics:

- Security Analytics and Logging for Catalyst SD-WAN
- How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management
- Requirements and guidelines for SD-WAN integration
- View Catalyst SD-WAN events in Security Cloud Control Firewall Management

This chapter covers information on how to share events from your Cisco Catalyst SD-WAN Manager and view them in Security Cloud Control.

Security Analytics and Logging for Catalyst SD-WAN

Describes how Catalyst SD-WAN integrates advanced firewall and security features for centralized policy enforcement and secure cloud access. Explains how onboarding devices to Security Cloud Control enables centralized monitoring and analysis of connection events.

Security Analytics and Logging for Catalyst SD-WAN is a security management solution that

- integrates advanced firewall and security features directly into the SD-WAN fabric
- enables centralized policy enforcement and secure cloud access through Direct Internet Access (DIA) and Direct Cloud Access (DCA)
- provides centralized monitoring and analysis of connection events when devices are onboarded to Security Cloud Control, and
- supports threat hunting and comprehensive security management across distributed networks.

Security capabilities

The Secure Router integrates firewall capabilities into its architecture, ensuring robust security across distributed networks.

- Catalyst SD-WAN integrates security features directly into the SD-WAN fabric, enabling secure Direct Internet Access (DIA) and Direct Cloud Access (DCA).
- It includes next-generation firewall, integrated intrusion prevention capabilities, and URL filtering.
- The Catalyst SD-WAN platform enables you to enforce centralized policies for all users, extending enterprise VPN architectures into your private cloud.

Onboard Catalyst SD-WAN Manager to Security Cloud Control to manage the security capabilities of managed devices.

- Onboarded Catalyst SD-WAN devices send connection events to Security Analytics and Logging for storage in the cloud data store.
- Security Analytics and Logging enables you to view connection events from all Catalyst SD-WAN devices in one centralized location–the **Event Logging** page in Security Cloud Control.
- On the **Event Logging** page, you can view, filter, and search for events to perform threat hunting and analyze security rules triggered in your network.

How Catalyst SD-WAN router shares events with Security Cloud Control Firewall Management

Describes how Catalyst SD-WAN event flow enables automated sharing of security events with Security Cloud Control, allowing seamless data export, cloud storage, and enrichment for enhanced threat detection.

This process describes how Catalyst SD-WAN shares security events with Security Cloud Control Firewall Management in Security Cloud Control. This integration streamlines event visibility and analysis, empowering SOC analysts to monitor network activity and enhance threat detection using Catalyst SD-WAN security data in real time.

Summary

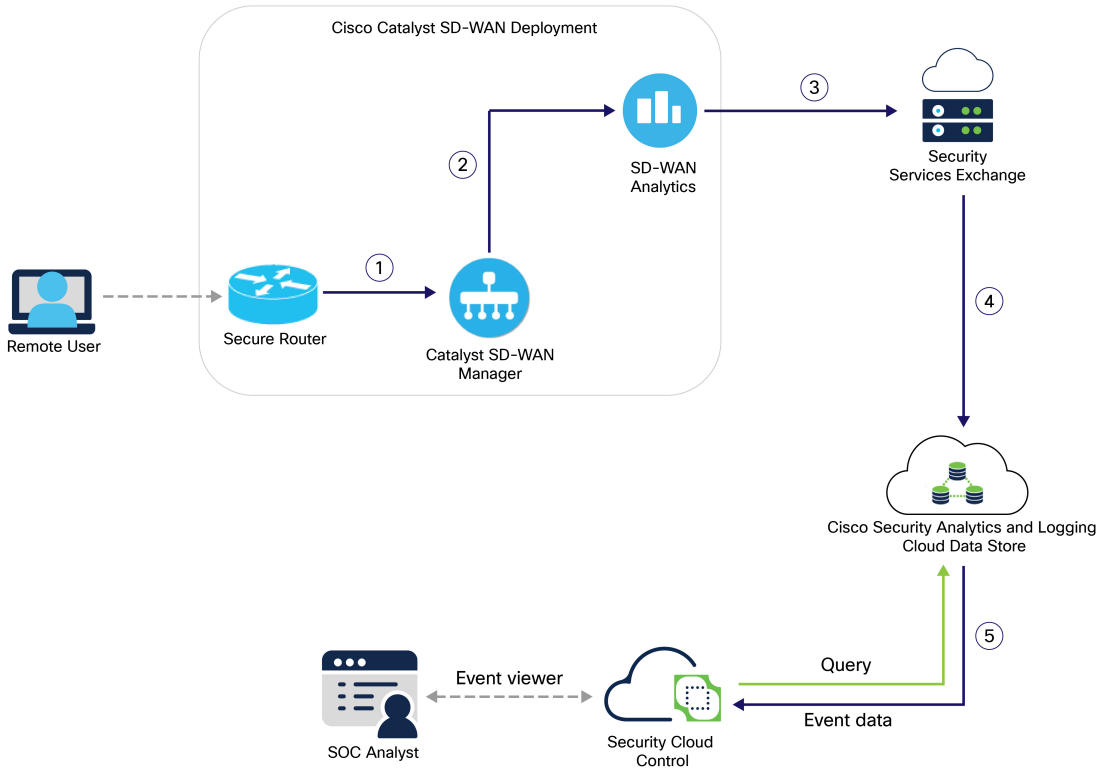
The key components involved in the event sharing process are:

- Catalyst SD-WAN device: Generates event logs for network traffic and exports data to PSV files
- Catalyst SD-WAN Manager: Receives event data from SD-WAN devices and forwards to analytics cloud

- SD-WAN Analytics cloud: Stores event data and notifies Security Services Exchange
- Security Services Exchange: Downloads event data and converts from PSV to JSON format
- Security Analytics and Logging (SaaS): Processes, classifies, and enriches event data for SOC analysts

Workflow

Figure 38: Event flow from Catalyst SD-WAN to Security Cloud Control



These stages describe how security events flow from Catalyst SD-WAN to Security Cloud Control:

1. A remote user accesses the network, and the Catalyst SD-WAN device generates an event log for the corresponding traffic. The device then exports the event data to a PSV file and sends it to Catalyst SD-WAN Manager.
2. Catalyst SD-WAN Manager sends the event data to the SD-WAN Analytics cloud.
3. SD-WAN Analytics stores the event data in cloud to make it accessible for Security Services Exchange and notifies Security Services Exchange.

   After receiving the notification from SD-WAN Analytics cloud, Security Services Exchange downloads the event data from SD-WAN AWS cloud.
4. Security Services Exchange converts the event data from PSV to JSON format and sends it to Cisco Security Analytics and Logging (SaaS).
5. Security Analytics and Logging (SaaS) processes the event data using various services to classify and enrich it for use by Security Cloud Control.

   Security Analytics and Logging (SaaS) stores the event data in the cloud data store. The event viewer queries this data store to provide security operations center (SOC) analysts with relevant event data.

Requirements and guidelines for SD-WAN integration

Outlines the requirements and guidelines for onboarding Catalyst SD-WAN Manager to Security Cloud Control for centralized visibility of connection events.

Onboard the Catalyst SD-WAN Manager to the Security Cloud Control organization where you want to view the security events.

Onboard the SD-WAN Analytics services to your Catalyst SD-WAN Manager and enable data collection.

Ensure you have a Security Cloud Control Firewall Management organization with a valid Security Analytics and Logging subscription plan.

Note that this integration supports only viewing the connection events from your Catalyst SD-WAN devices in Security Cloud Control.

Ensure that you have a Security Analytics and Logging subscription plan that reflects the number of events the Cisco cloud receives from your on-boarded Catalyst SD-WAN devices on a daily basis. This is called your *daily ingest rate*. You can use the Logging Volume Estimator tool to estimate your daily ingest rate and as that rate changes you can update your data plan.

If you do not have a Security Analytics and Logging plan subscribed, you can request a 90-day trial by logging in to Security Cloud Control and navigating to **Events & Logs** > **Events** > **Event Logging** tab. You can accurately estimate your daily ingest rate and purchase the desired subscription plan by following the instructions in the Security Cloud Control Firewall Management Ordering Guide.

View Catalyst SD-WAN events in Security Cloud Control Firewall Management

Configure filtering for Catalyst SD-WAN connection events in the event logging page to quickly identify network activity and security events.

This task enables you to streamline event analysis, enhance threat detection, and maintain compliance by filtering specific network events.

Network administrators should perform this task regularly for effective security monitoring. Use this feature to focus on relevant connection events and improve your network security posture.

Before you begin

Ensure that you have met all the requirements described in Requirements and guidelines for SD-WAN integration on page 632.

Follow these steps to view Catalyst SD-WAN events in Security Cloud Control Firewall Management:

Procedure

1. In the navigation pane, choose **Events & Logs** > **Events** > **Event Logging**.
2. Click the filter (▼) icon.
3. Scroll to the **Catalyst SD-WAN Events** section and check the **Connection** check box.

The event logging page displays filtered Catalyst SD-WAN connection events, allowing you to focus on relevant network activity and security events for analysis.

55 View Events in Security Cloud Control Firewall Management

Topics:

- View live events
- View historical events
- Customize the events view
- Show and hide columns on the event logging page
- Change the time zone for the event timestamps
- Create and save customizable event filters
- Event logging page search and filter functionality
- Event attributes in security analytics and logging

Learn how to view live and historical events in Security Cloud Control Firewall Management, customize event views, adjust timestamps, filter and search events, and review Security Analytics and Logging attributes.

This chapter provides information on how to view live and historical events in Security Cloud Control Firewall Management.

View live events

Configure the Live events page to view the most recent 500 events that match your filter and search criteria.

View live events to monitor the most recent activity including event details, device status, and reporting views for follow-up actions.

The Live events page shows the most recent 500 events that match the filter and search criteria you entered. If the Live events page displays the maximum of 500 events, and more events stream in, Security Cloud Control displays the newest live events, and transfers the oldest live events to the Historical events page, keeping the total number of live events at 500. That transfer takes roughly a minute to perform. If no filtering criteria is added, you will see all the latest Live 500 events generated by rules configured to log events.

The event timestamps are shown in UTC.

Changing the filtering criteria, whether live events are playing or paused, clears the events screen and restarts the collection process.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click the **Live** tab.

The Live events page displays the most recent 500 events matching your criteria, with event timestamps shown in UTC.

Play/pause live events

Explains the functionality for controlling live event streaming, including play and pause capabilities, auto-pause features, and event reporting mechanisms.

A play/pause live events feature is a streaming control mechanism that

- allows users to "play" ▶ or "pause" ⏸ live events as they stream in
- displays events matching filtering criteria in the Events viewer when playing, and
- stops updating the Live events page when paused until restarted.

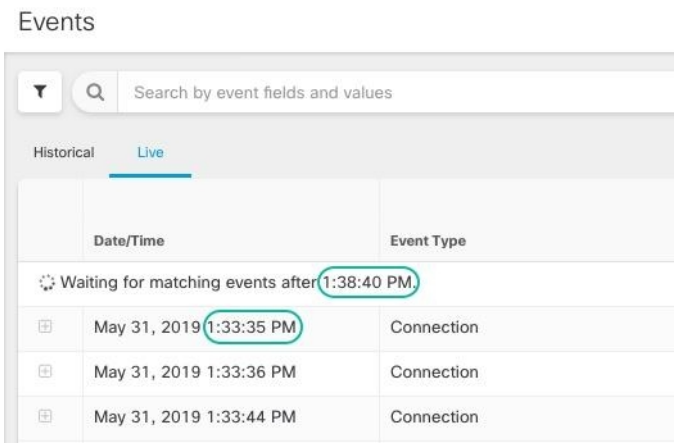
Live event streaming behavior

If live events are "playing," Security Cloud Control displays events that match the filtering criteria specified in the Events viewer in the order they are received. If events are paused, Security Cloud Control does not update the Live events page until you restart playing live events. When you restart playing events, Security Cloud Control begins populating events in the Live page from the point at which you restarted playing events. It doesn't back-fill the ones you missed.

To view all the events that Security Cloud Control received whether you played or paused live event streaming, click the **Historical** tab.

Auto-pause live events: After displaying events for about 5 consecutive minutes, Security Cloud Control warns you that it is about to pause the stream of live events. At that time, you can click the link to continue streaming live events for another 5 minutes or allow the stream to stop. You can restart the live events stream when you are ready.

Receiving and reporting events: There may be a small lag between the Secure Event Connector or the Security Service Exchange receiving events and Security Cloud Control posting events in the Live events viewer. You can view the gap on the Live page. The time stamp of the event is the time it was received by Secure Event Connector or the Security Service Exchange.



View historical events

Configure access to view historical events including event details, device status, reporting views, and follow-up actions.

View historical events to access events older than the most recent 500 that have been transferred from the Live events page to the Historical events table.

The Live events page shows the most recent 500 events that match the filter and search criteria you entered. Events older than the most recent 500 are transferred to the Historical events table. That transfer takes roughly a minute to perform. You can then filter all the events you have stored to find events you're looking for.

Note

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation pane, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click the **Historical** tab. By default, when you open the Historical events table, the filter is set to display the events collected within the last hour.

   The event attributes are largely the same as what is reported by Firepower Device Manager (FDM) or the Adaptive Security Device Manager (ASDM).

   - For a complete description of Firepower Threat Defense event attributes, see Cisco FTD Syslog Messages.
   - For a complete description of ASA event attributes, see Cisco ASA Series Syslog Messages.

The Historical events table displays filtered events, allowing you to review and analyze historical event data based on your specified criteria.

Customize the events view

Configure the events view including event details, device status, reporting views, and follow-up actions.

Customize the events view to display only the columns and information that are relevant to your monitoring and analysis needs. This allows you to optimize the view for better performance and easier data interpretation.

Any changes made to the Event Logging page are automatically saved for when you navigate away from this page and come back at a later time.

> **Note**
>
> The Live and Historical events view have the same configuration. When you customize the events view, these changes are applied to both the Live and Historical view.

Procedure

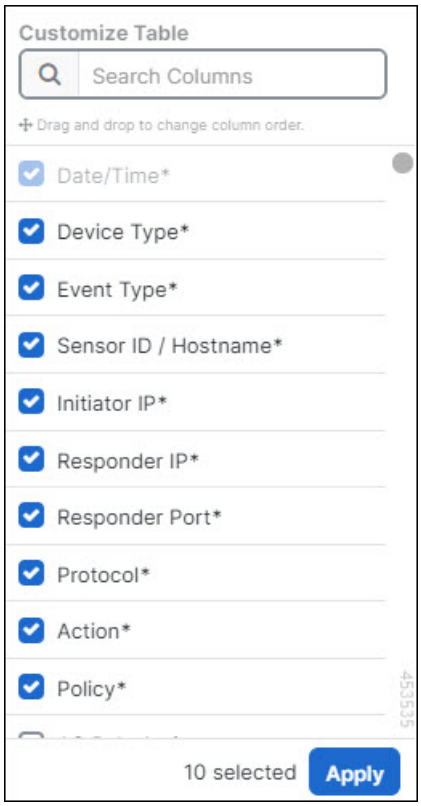
1. Click the column filter icon located to the right of the columns.

   You can modify the event view for both live and historical events to only include column headers that apply to the view you want.

2. Select or deselect the columns you want.

   Columns with asterisks are provided within the event table by default, although you can remove them at any time.

   Figure 39: Show or hide columns



3. Click **Apply**.
4. Search for additional columns not part of the default list and add them to the event view.

You can search for more columns, which are not part of the default list, and add them to the event view for both live and historical events. Note that adding many columns for customizing the table may reduce performance. Consider using fewer columns for faster data retrieval.

Alternatively, click the **+** icon next to an event to expand it and view the hidden columns. Note that some of the event fields displayed when you expand an event can have a different name compared to the corresponding column name. To correlate the events fields displayed when you expand an event to the corresponding column name, see Correlate Threat Defense Event Fields and Column Names.

5. Reorder the columns by dragging and dropping them in the column filter menu.

   Click the column filter icon located to the right of the columns to view the list of selected columns. Then, drag and drop the columns into the order you want. The column at the top of the list in the drop-down menu appears as the left-most column in the event table.

The events view is customized with your selected columns and preferred order. These settings are automatically saved and will persist when you navigate away from and return to this page.

Correlate Firewall Threat Defense event fields and column names

Lists Firewall Threat Defense event fields that have differing column names and provides a comparison between the event field and the respective column name.

On the Security Cloud Control **Event Logging** page, you can click on any event to expand its details and view all the associated event fields. Note that the names of some event fields may differ from those of the column headers in the Security Cloud Control event viewer where the values of these fields are displayed.

Table 49: Firewall Threat Defense Event Field and the Corresponding Security Cloud Control Column Name

Security Cloud Control Column Name	FTD Event Field
Date/Time	Timestamp
Detection Type	ClientAppDetector
Encrypted Visibility Fingerprint	EVE_Fingerprint
Encrypted Visibility Process Name	EVE_Process
Encrypted Visibility Process Confidence Score	EVE_ProcessConfidencePct
Encrypted Visibility Threat Confidence	EVE_ThreatConfidenceIndex
Encrypted Visibility Threat Confidence Score	EVE_ThreatConfidencePct
MITRE	MitreAttackGroups
NAT Source IP	NAT_InitiatorIP
NAT Source Port	NAT_InitiatorPort
Rule Group	SnortRuleGroups

Show and hide columns on the event logging page

Learn how to show and hide columns on the event logging page.

-

The **Event Logging** page displays events sent to the Cisco cloud from configured ASA and FDM-managed devices.

You can show or hide columns on the **Event Logging** page by using the Show/Hide widget with the table:

Before you begin

-

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Events & Logs** > **Events** > **Event Logging** .
3. Scroll to the far right of the table and click the column filter icon .
4. Check the columns you want to see and uncheck the columns you want to hide.

Other users logging into the tenant will see the same columns you chose to show until columns are shown or hidden again.

This table describes the default column headers:

Column Header	Description
Date/Time	The time the device generated the event. By default, event timestamps are displayed in your Local time zone. To view event timestamps in UTC, see Change the time zone for the event timestamps on page 966
Device Type	ASA (Adaptive Security Appliance) FTD (Firepower Threat Defense)

Column Header	Description

Event Type	This composite column can have any of the following:
	• **FTD Event Types**
	  • Connection: Displays connection events from access control rules.
	  • File: Displays events reported by file policies in access control rules.
	  • Intrusion: Displays events reported by intrusion policy in access control rules.
	  • Malware: Displays events reported by malware policies in access control rules.
	• **ASA Event Types** : These event types represent groups of syslog or NetFlow events. See ASA Event Types for more information about which syslog ID or which NetFlow ID is included in which group.
	  • Parsed Events: Parsed syslog events contain more event attributes than other syslog events and Security Cloud Control is able to return search results based on those attributes more quickly. Parsed events are not a filtering category; however, parsed event IDs are displayed in the Event Types column in *italics* . Event IDs that are not displayed in italics are not parsed.
	  • ASA NetFlow Event IDs: All Netflow (NSEL) events from ASA appear here.

Sensor ID / Hostname	The Sensor ID is the IP address from which events are sent to Security Service Exchange or Secure Event Connector. This is typically the management interface on the threat defense or the ASA.
Initiator IP	This is the IP address of the source of the network traffic. The value of the Initiator address field corresponds to the value of the InitiatorIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.
Responder IP	This is the destination IP address of the packet. The value of the Destination address field corresponds to the value in the ResponderIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.
Port	The port or ICMP code used by the session **responder** . The value of the destination port corresponds to the value of the **ResponderPort** in the event details.
Protocol	It represents the protocol in the events.

Column Header	Description
Action	Specifies the security action defined by the rule. The value you enter must be an exact match to what you want to find; however, the case doesn't matter. Enter different values for connection, file, intrusion, malware, syslog, and NetFlow event types: • For connection event types, the filter searches for matches in the AC_RuleAction attribute. Those values could be Allow, Block, Trust. • For file event types, the filter searches for matches in the FileAction attribute. Those values could be Allow, Block, Trust. • For intrusion event types, the filter searches for matches in the InLineResult attribute. Those values could be Allowed, Blocked, Trusted. • For malware event types, the filter searches for matches in the FileAction attribute. Those values could be Cloud Lookup Timeout. • For syslog and NetFlow events types, the filter searches for matches in the Action attribute.
Policy	The name of the policy that triggered the event. Names will be different for ASA and FDM-managed devices.

Refer to Event logging page search and filter functionality on page 967.

Change the time zone for the event timestamps

Configure the time zone display for event timestamps on the Event Logging page.

This task allows you to switch between UTC and local time zone display for event timestamps to match your preferred time reference.

Change the time zone display for event timestamps on the Security Cloud Control **Event Logging** page.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. From the left pane, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click the **UTC Time** or **Local Time** button on the top right side of the **Event Logging** page to display the event timestamps in the selected time zone.

   By default, event timestamps are displayed in your local time zone.

Event timestamps are now displayed in your selected time zone (UTC or local time) throughout the Event Logging page.

Create and save customizable event filters

Configure custom filters for frequently used filter criteria in Secure Logging Analytics (SaaS).

Create and save custom filters to quickly access frequently used filter criteria for event logging analysis.

If you are a Secure Logging Analytics (SaaS) customer, you can create and save custom filters that you use frequently.

The elements of your filter are saved to a filter tab as you configure them. Whenever you return to the Event Logging page, these searches will be available to you. They will not be available to other Security Cloud Control users of the tenant. They will not be available to you on a different tenant, if you manage more than one tenant.

> **Note**
>
> Be aware that when you are working in a filter tab, if you modify any filter criteria, those changes are saved to your custom filter tab automatically.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. From the main menu, choose **Events & Logs** > **Events** > **Event Logging**.
3. Clear the Search field of any values.
4. Above the event table, click the blue plus button to add a View tab.

   Filter views are labeled "View 1", "View 2", "View 3" and so on until you give them a name.

5. Select a view tab.
6. Open the filter bar and select the filters attributes you want in your custom filter.

   See Event logging page search and filter functionality on page 967. Remember that only filter attributes are saved in the custom filter.

7. Customize the columns you want to show in the event logging table.

   See Show and hide columns on the event logging page on page 964 for a discussion of showing and hiding columns.

8. Double-click the filter tab with the "View X" label and rename it.
9. (Optional) Now that you have created a custom filter, you can fine tune the results displayed on the Event Logging page, without changing the custom filter, by adding search criteria to the Search field.

   See Event logging page search and filter functionality on page 967.

You have successfully created and saved a custom event filter that will be available to you whenever you return to the Event Logging page.

Event logging page search and filter functionality

Describes how to search and filter events using the event logging page functionality.

Event logging page search and filter functionality is a data management feature that

- enables you to search and filter historical and live event tables for specific events using the same mechanisms as other information in Security Cloud Control,
- limits what displays on the **Event Logging** page as you add filter criteria, and
- allows you to combine filtering and searching mechanisms where search finds values from filtered event results.

Event logging search and filter options

These are the options to conduct a search for event logs:

- Search events using the events logging page on page 974
- Search historical events in the background on page 976

Filtering works the same way for live events as it does for historical events with the exception that live events cannot be filtered by time.

Learn about these filtering methods:

- Filter live or historical events on page 968
- Filter only NetFlow events on page 970
- Filter for ASA or FDM-Managed Device Syslog Events but not ASA NetFlow Events on page 970
- Combine filter elements on page 970

Filter live or historical events

Configure event filtering to display a subset of events in the Event Logging page based on specific criteria.

Filter events to view specific subsets of live or historical events in the Event Logging page, which helps in analyzing security events more effectively.

This procedure explains how to use event filtering to see a subset of events in the **Event Logging** page. If you find yourself repeatedly using certain filter criteria, you can create a customized filter and save it. See Customizable Event Filters for more information.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation bar, choose **Events & Logs** > **Events** > **Event Logging**
3. Click either the **Historical** or **Live** tab.
4. Click the filter icon ( ). Click the pin icon ( ) to pin the **Filter** pane and keep it open.
5. Click a view tab that has no saved filter elements.



6. Select the event details you want to filter by:
   - **FTD Events**:
     - Connection: Displays connection events from access control rules.
     - File: Displays events reported by file policies in access control rules.
     - Intrusion: Displays events reported by intrusion policy in access control rules.

  - Malware: Displays events reported by malware policies in access control rules.

- **ASA Events**: These event types represent groups of syslog or NetFlow events.

  See Security Cloud Control Event Types for more information about events.

  - Parsed Events: Parsed syslog events contain more event attributes than other syslog events and Security Cloud Control is able to return search results based on those attributes more quickly. Parsed events are not a filtering category; however, parsed event IDs are displayed in the Event Types column in *italics*. Event IDs that are not displayed in italics are not parsed.

- **Time Range**: Click the Start or End time fields to select the beginning and end of the time period you want to display. The time stamp is displayed in the local time of your computer.
- **Action**: Specifies the security action defined by the rule. The value you enter must be an exact match to what you want to find; however, the case doesn't matter. Enter different values for connection, file, intrusion, malware, syslog, and NetFlow event types:
  - For connection event types, the filter searches for matches in the AC_RuleAction attribute. Those values could be Allow, Block, Trust.
  - For file event types, the filter searches for matches in the FileAction attribute. Those values could be Allow, Block, Trust.
  - For intrusion event types, the filter searches for matches in the InLineResult attribute. Those values could be Allowed, Blocked, Trusted.
  - For malware event types, the filter searches for matches in the FileAction attribute. Those values could be Cloud Lookup Timeout.
  - For syslog and NetFlow events types, the filter searches for matches in the Action attribute.
- **Sensor ID / Hostname**: The Sensor ID is the management IP address from which events are sent to the Secure Event Connector or Security Service Exchange.

  For an FDM-managed device, the Sensor ID is typically the IP address of the device's management interface.
- **IP addresses**
  - **Initiator**: This is the IP address of the source of the network traffic. The value of the Initiator address field corresponds to the value of the InitiatorIP field in the event details. You can enter a single address, such as `10.10.10.100`, or a network defined in CIDR notation such as `10.10.10.0/24`.
  - **Responder**: This is the destination IP address of the packet. The value of the Destination address field corresponds to the value in the ResponderIP field in the event details. You can enter a single address, such as `10.10.10.100`, or a network defined in CIDR notation such as `10.10.10.0/24`.
- **Ports**
  - **Initiator**: The port or ICMP type used by the session initiator. The value of the source port corresponds to the value fo the InitiatorPort in the event details. (Add a range - starting port ending port and space in between or both initiator and responder)
  - **Reponder**: The port or ICMP code used by the session responder. The value of the destination port corresponds to the value of the ResponderPort in the event details.
- **NetFlow**: ASA NetFlow events are different than syslog events. The NetFlow filter searches for all NetFlow events IDs that resulted in an NSEL record. Those "NetFlow event IDs" are defined in the Cisco ASA NetFlow Implementation Guide.

7. (Optional) Save your filter as a custom filter by clicking out of the view tab.

The Event Logging page displays only the events that match your selected filter criteria. You can further refine your search by adjusting the filter parameters or save the filter configuration for future use.

Filter only NetFlow events

Configure the Event Logging filter to display only ASA NetFlow events in the analytics dashboard.

Filter the Event Logging table to display only ASA NetFlow events, removing other event types from view for focused analysis.

This procedure finds only ASA NetFlow events in the Event Logging interface.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. From the left menu, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click the Filter icon and pin the filter open.
4. Check **Netflow** ASA Event filter.
5. Clear all other ASA Event filters.

   Only ASA NetFlow events are displayed in the Event Logging table.

The Event Logging table displays only ASA NetFlow events, with all other event types filtered out.

Filter for ASA or FDM-Managed Device Syslog Events but not ASA NetFlow Events

Configure filters to display only ASA or FTD syslog events while excluding NetFlow events from the event logging interface.

This task allows you to isolate syslog events for troubleshooting and analysis by filtering out NetFlow events that may clutter the event view.

This procedure finds only syslog events by ensuring NetFlow events are excluded from both the general filter settings and the ASA Events filter tree.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click the Filter icon and pin the filter open.
4. Scroll to the bottom of the **Filter** pane and make sure the **Include NetFlow events** filter is **unchecked**.
5. Scroll back up to the ASA Events filter tree, and make sure the **NetFlow** box is **unchecked**.
6. Select the rest of your ASA or FTD filter criteria.

The event logging interface now displays only ASA or FTD syslog events with NetFlow events excluded from the view.

Combine filter elements

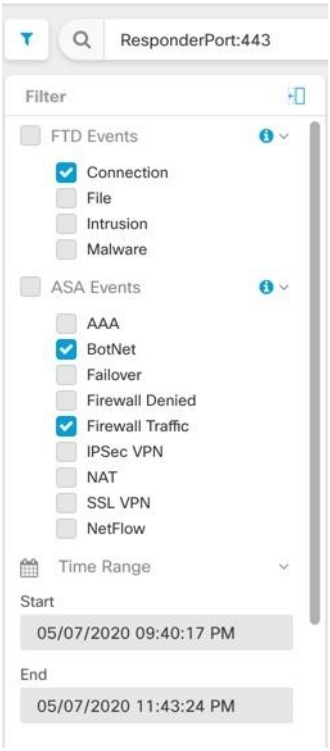
Explains how to combine filter elements to create complex search criteria for event filtering in Security Cloud Control.

Combine filter elements is a filtering mechanism that

- follows standard filtering rules where categories are "AND-ed" AND values within categories are "OR-ed"
- allows combination of filters with custom search criteria
- applies "OR" logic to device event filters, AND
- enables filtering by historical events within a time range.

Filter combination behavior

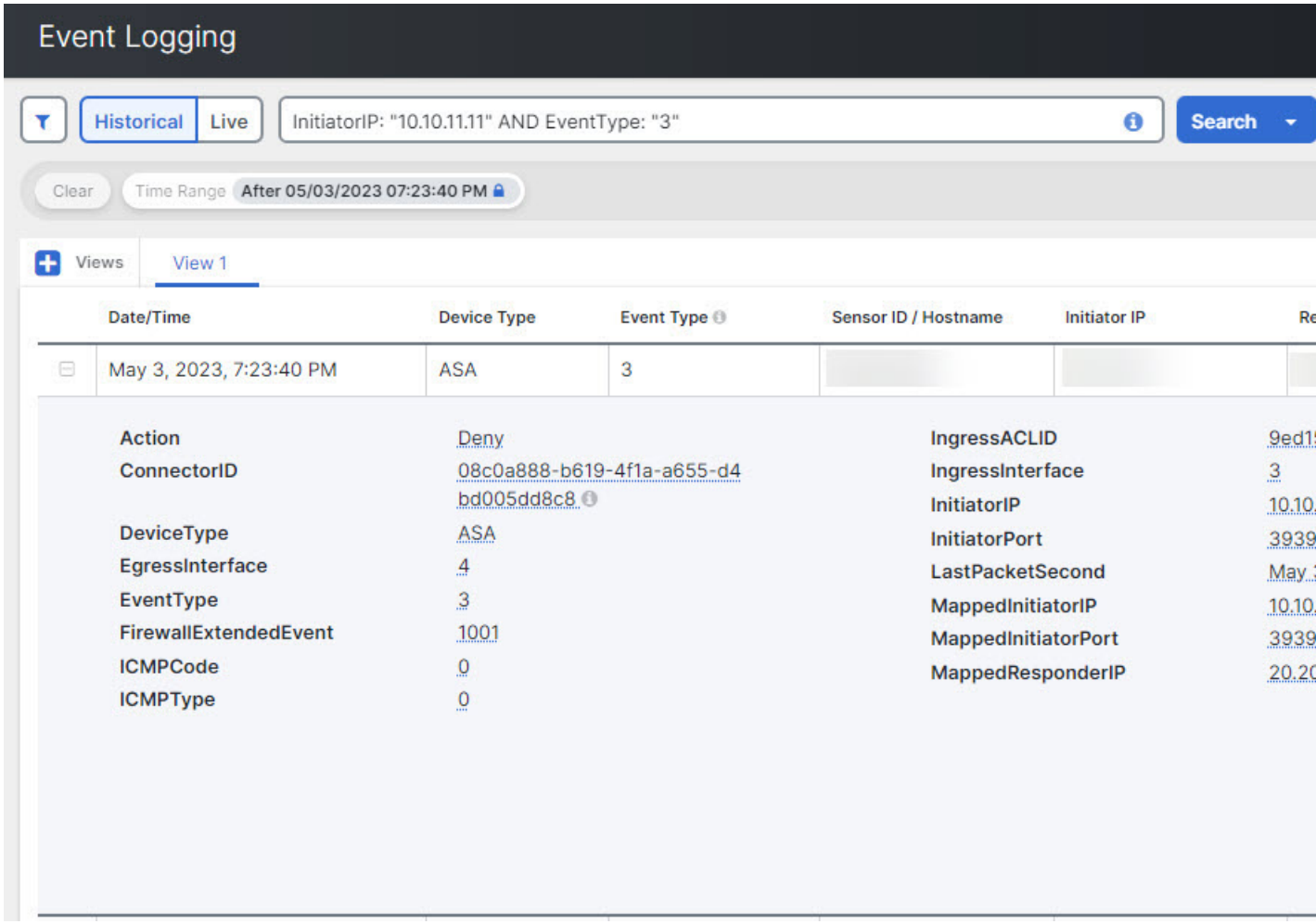
Filtering events generally follows the standard filtering rules in Security Cloud Control: The filtering categories are "AND-ed" AND the values within the categories are "OR-ed." You can also combine the filter with your own search criteria. In the case of event filters; however, the device event filters are also "OR-ed."



With this filter in use, Security Cloud Control would display Firewall Threat Defense device connection events **OR** ASA BotNet **OR** Firewall Traffic events, **AND** those events that occurred between the two times in the time range, **AND** those events that also contain the ResponderPort 443. You can filter by historical events within a time range. The live events page always displays the most recent events.

Search for specific attribute: value pairs

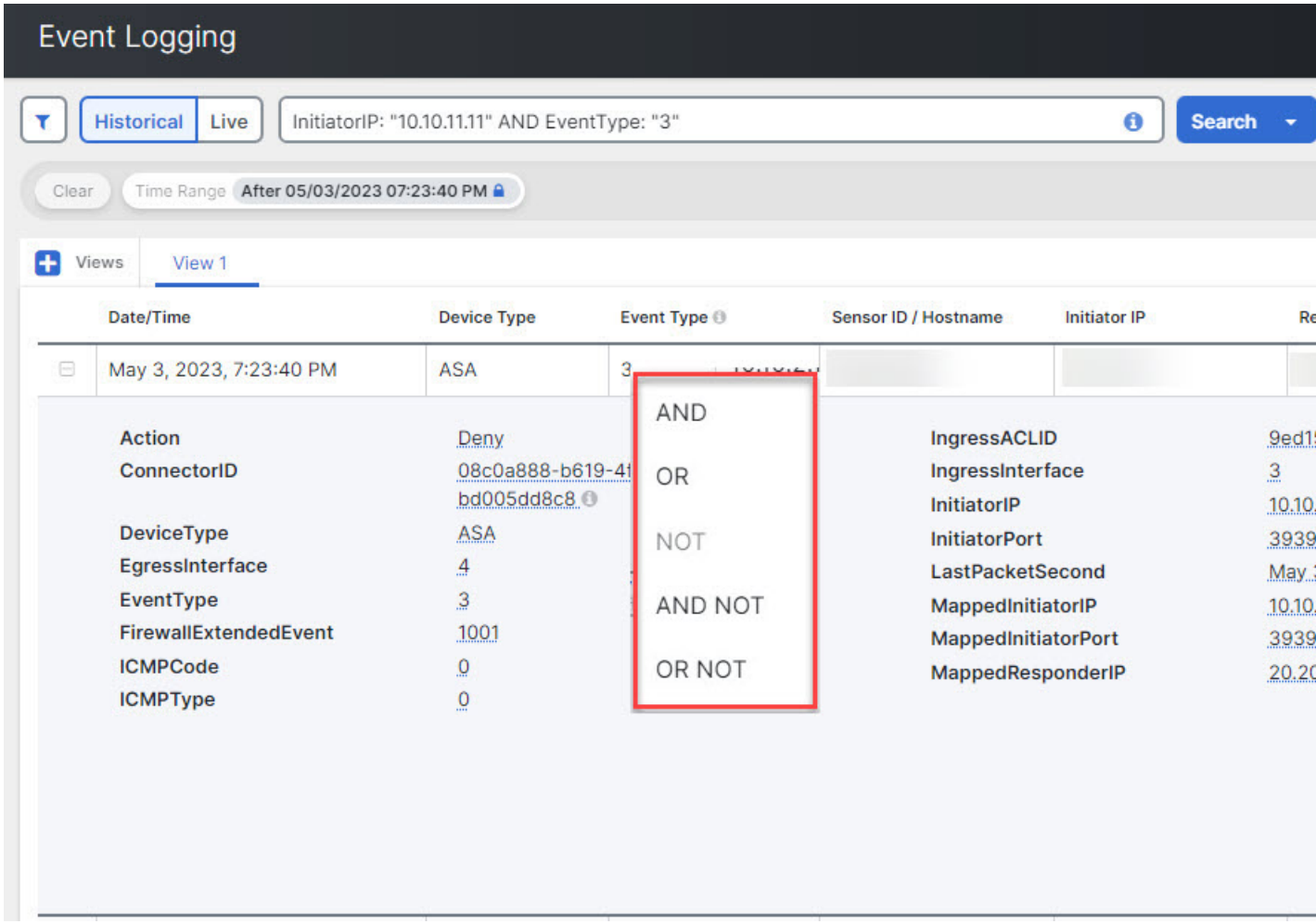
You can search for live OR historical events by entering an event attribute AND a value in the search field. The easiest way to do this is to click the attribute in the Event Logging table that you want to search for, AND Security Cloud Control enters it in the Search field. The events you can click on will be blue when you roll over them.



In this example, the search started by rolling over the InitiatorIP value of 10.10.11.11 AND clicking it. Initiator IP AND it's value were added to the search string. Next, Event Type, 3 was rolled-over AND clicked AND added to the search string AND an AND was added by Security Cloud Control. So the result of this search will be a list of events that were initiated from 10.10.11.11 AND that are 3 event types.

Notice the magnifying glass next to the value 3 in the example above. If you roll-over the magnifying glass, you could also choose an AND, OR, AND NOT, OR NOT operator to go with the value you want to add to the search.

In the example below, "OR" is chosen. The result of this search will be a list of events that were initiated from 10.10.11.11 OR are a 106023 event type. Note that if the search field is empty AND you right click a value from the table, only NOT is available as there is no other value.



As long as you rollover a value AND it is highlighted blue, you can add that value to the search string.

AND, OR, NOT, AND NOT, OR NOT filter operators behavior:

- **AND**: Use the AND operator in the filter string, to find events that include all attributes. The AND operator cannot begin a search string.
- **OR**: Use the OR operator in the filter string, to find events that include any of the attributes. The OR operator cannot begin a search string.
- **NOT**: Use this only at the beginning of a search string to exclude events with certain attributes.
- **AND NOT**: Use the AND NOT operator in the filter string to exclude events that contain certain attributes. AND NOT cannot be used at the beginning of a search string.
- **OR NOT**: Use the OR NOT operator to include search results that exclude certain elements. The OR NOT operator cannot be used at the beginning of a search string.

Filter operator examples

AND example:

For example, the search string below will search for events that contain the TCP protocol AND that originated from InitiatorIP address 10.10.10.43, AND that were sent from the Initiator port 59614. One would expect that with each additional AND statement, the number of events that meet the criteria would be small AND smaller.

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

OR example:

For example, the search string below will display events in the event viewer that include events that include the TCP protocol, OR that originated from InitiatorIP address 10.10.10.43, OR that were sent from the Initiator port 59614. One would expect that with each additional OR statement, the number of events that meet the criteria would be bigger AND bigger.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

NOT example:

For example, this search string would exclude any event with the InitiatorIP 192.168.25.3 from the results.

```
NOT InitiatorIP: "192.168.25.3"
```

AND NOT example:

For example, this filter string will display events with the InitiatorIP 192.168.25.3 but NOT those whose ResponderIP address is also 10.10.10.1.

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

You can also combine NOT AND AND NOT to exclude several attributes. For example this filter string, will exclude events with InitiatorIP 192.168.25.3 AND events with ResponderIP 10.10.10.1

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

OR NOT example:

For example, this search string will find events with the Protocol of TCP, OR that have the InitiatorIP of 10.10.10.43, OR those NOT from InitiatorPort 59614.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

You could also think of it this way: Search for (Protocol: "TCP") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614").

Wildcard searches:

Use an asterisk (*) to represent a wildcard in the value field of an **attribute:value** search to find results within events. For example, this filter string,

```
URL:*feedback*
```

will find strings in the URL attribute field of events that contain the string **feedback**.

Related information:

- Show AND Hide Columns on the Event Logging Page
- Event Attributes in Security Analytics AND Logging

Search events using the events logging page

Configure event searches and reports using the Event Logging page to find logged events and generate historical reports.

This task allows you to search all logged events and find the information you need using the search and report capabilities in the Event Logging page.

Use the search and report capabilities in the **Event Logging** page to search all logged events and find the information you need. Note that you can generate reports only for historical events.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation bar, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click either the **Historical** or **Live** tab.
4. Type the search query in the search bar and click **Search** to execute the search.

   Alternatively, click the search box to choose from a list of **Sample Filters** to quickly search for events. Use the sample filters to quickly populate a search query in the search bar and then modify it to match your specific needs. Find more information about using the sample filters in Use sample filters to search events on page 975.
5. (optional)To run a search in the background and generate a report while you move away from the search page, do these steps:
   a) Type your search query and choose **Schedule Report** from the **Search** drop-down list.
   b) Click **Generate Report**.

      The search is queued, and you are notified when it is complete. You can run multiple searches in the background.

      For more information about scheduling a report, refer to Schedule to generate a search report in the background on page 976
6. (Optional) If you want to view and manage your search reports, click **Reports**.

   From this view, you can do these actions:

   - The **Reports** page allows you to view, download, or delete the search reports.
   - Click **Schedule a Report** to generate a one-time report or to schedule a recurring report.
   - Click **View Notification Settings** to navigate to the **Notification Preferences** page to view or modify your notification settings.

   You can convert any one-time report into a recurring report schedule if you need recurring searches. For more information, refer to Schedule to generate a search report in the background on page 976.

You have successfully searched for events and can view the results in the Event Logging page. Any scheduled reports will run in the background and notify you when complete.

Use sample filters to search events

Configure sample filters to construct common search queries quickly without requiring you to type the full query.

Sample filters allow you to construct common search queries quickly without requiring you to type the full query.

You can select a filter and modify the query parameters to fit your specific needs when searching for events.

Procedure

1. In the **Event Logging** page, click the search bar.

   A list of **Sample Filters** appears below the search bar.
2. Choose a filter from the drop-down list.

   The search bar automatically populates with the corresponding search query.
3. Modify the values in the predefined query to refine your search.

   Examples

- To search for events related to a specific website, select **Wildcard URL**. The search bar displays **URL: " *.sharepoint.com"** . You can then change sharepoint.com to any other domain you wish to investigate.
- To search for events involving a specific device, select **Specific Host**. The search bar displays **InitiatorIP: " 192.168.55.55" OR ResponderIP: " 192.168.55.55"** . Change 192.168.55.55 to the IP address of the device you want to monitor.

4. Click **Search**.

The search results display events that match your filter criteria, allowing you to analyze specific network activity OR investigate particular devices OR websites.

Search historical events in the background

Describes how Security Cloud Control enables background event log searches and report generation based on defined search criteria.

A background historical event search is a feature that allows you to define search criteria and search for event logs based on that criteria, with the **Reports** feature enabling you to perform the event log searches in the background and generate reports.

Background search capabilities

The background search functionality provides these capabilities:

- You receive a notification when the report generation is complete, based on your configured notification preferences.
- You can view, download, or delete the reports from the **Reports** page.
- You can schedule to generate either a one-time report or a recurring report.
- Navigate to the **Notification Settings** page to view or modify the subscription options.

Schedule to generate a search report in the background

Configure scheduled event log searches in the background to generate reports for historical events at specified intervals.

Use the **Report** feature to run one-time or scheduled event log searches in the background and generate reports for analysis and compliance purposes.

You can modify or cancel the scheduled report at any time. You can also modify a one-time search query to be a recurring search.

- You can schedule to generate reports only for historical events.
- You can opt to get alerts on reports that have started, completed, or have failed.

Before you begin

Follow these steps to schedule a search and generate report:

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation bar, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click the **Historical** tab to view historical events.
4. Type the search query in the search bar.
5. Click the **Search** drop-down and choose **Schedule Report**.

6. (Optional) Enter a name for the report to identify it.
7. The **Generate report now** check box is checked by default. When checked, the report generation starts upon saving.
8. Check the **Setup recurring schedule** check box and configure these settings:
   - **Search Logs for the Last**: Specify how far back you want to search through.
   - **Frequency**: Specify how frequent you want the scheduled search to occur and the time at which you want it to run.
9. Confirm the scheduled search criteria at the bottom of the window. Click **Schedule and Generate Now**. If you did not opt for the search to start immediately, click **Schedule Report**.

   Scheduled search reports are available to view for up to seven days before Security Cloud Control automatically deletes them.

The scheduled search is created and will generate reports according to the specified frequency. If you opted to generate the report immediately, the initial report generation begins upon saving.

Download a search report

Configure the download of search reports and scheduled queries in CSV format from the analytics interface.

Download search results and scheduled queries in CSV format for local storage and analysis before they are automatically removed after seven days.

Search results and schedules queries are stored for seven days before Security Cloud Control automatically removes them. You can download a copy of the search report in CSV format.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the navigation bar, choose **Events & Logs** > **Events** > **Event Logging**.
3. Click **Reports**.
4. In the **Actions** column, click **Download** next to the report to download it. The report file in CSV format is automatically downloaded to the default storage location on your local drive.
5. (Optional) To view the search query and download the report, follow these steps:
   a) click **Queries** tab.
   b) Expand the report to see the search query details.
   c) Click **View Reports** next to the report you want to view and download.
   d) Click **Download**.

The search report is downloaded in CSV format to your local drive's default storage location, allowing you to analyze the data before it is automatically removed from the system.

Event attributes in security analytics and logging

Describes event attributes in security analytics and logging including event details, device status, reporting views, and follow-up actions.

Event attributes in Security Analytics and Logging are data elements that

- provide detailed information about security events and logging activities

- are largely the same as what is reported by Firepower Device Manager (FDM) and Adaptive Security Device Manager (ASDM), and
- include parsed events and additional attributes for filtering Event Logging table contents using attribute:value pairs.

Event attribute descriptions

The event attribute descriptions used by Security Cloud Control are largely the same as what is reported by Firepower Device Manager (FDM) and Adaptive Security Device Manager (ASDM).

- For a complete description of FDM-managed device event attributes, see Cisco Firepower Threat Defense Syslog Messages.
- For a complete description of Adaptive Security Appliance (ASA) event attributes, see Cisco ASA Series Syslog Messages.

Some ASA syslog events are "parsed" and others have additional attributes which you can use when filtering the contents of the Event Logging table using attribute:value pairs. See these additional topics for other important attributes of syslog events:

- Parsed ASA Syslog Events
- EventGroup and EventGroupDefinition Attributes for Some Syslog Messages
- Event Name Attributes for Syslog Events
- Time Attributes

EventGroup and EventGroupDefinition attributes for some syslog messages

Lists the EventGroup and EventGroupDefinition attributes that appear on some syslog events, which you can use to filter the events table.

Some syslog events will have the additional attributes "EventGroup" and "EventGroupDefinition". You will be able to filter the events table to find events using these additional attributes by filtering by attribute:value pairs. For example, you could filter for Application Firewall events by entering `apfw:415*` in the search field of the Event Logging table.

Syslog message classes and associated message ID numbers

EventGroup	EventGroupDefinition	Syslog Message ID Numbers (first 3 digits)
aaa/auth	User Authentication	109, 113
acl/session	Access Lists/User Session	106
apfw	Application Firewall	415
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
citrix	Citrix Client	723
clst	Clustering	747
cmgr	Card Management	323
config	Command Interface	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776

EventGroup	EventGroupDefinition	Syslog Message ID Numbers (first 3 digits)
dap	Dynamic Access Policies	734
EAP, eapoudp	EAP or EAPoUDP for Network Admission Control	333, 334
EIGRP	EIGRP Routing	336
email	E-mail Proxy	719
ipaa/envmon	Environment Monitoring	735
ha	Failover	101, 102, 103, 104, 105, 210, 311, 709
idfw	Identity-based Firewall	746
ids	Intrusion Detection System	733
ids/ips	Intrusion Detection System / Intrusion Protection System	400
ikev2	IKEv2 Toolkit	750, 751, 752
IP	IP Stack	209, 215, 313, 317, 408
ipaa	IP Address Assignment	735
ips	Intrusion Protection System	401, 420
ipv6	IPv6	325
l4tm	Block lists, Allow lists, grey lists	338
lic	Licensing	444
MDM-proxy	MDM Proxy	802
nac	Network Admission Control	731, 732
VPN/nap	IKE and IPsec / Network Access Point	713
NP	Network Processor	319
OSPF	OSPF Routing	318, 409, 503, 613
passwd	Password Encryption	742
pp	Phone Proxy	337
RIP	RIP Routing	107, 312
rm	Resource Manager	321
sch	Smart Call Home	120
session	User Session	108, 201, 202, 204, 302, 303, 304, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
session/natpat	User Session/NAT and PAT	305
SNMP	SNMP	212
ssafe	ScanSafe	775

EventGroup	EventGroupDefinition	Syslog Message ID Numbers (first 3 digits)
SSL/NP SSL	SSL Stack/NP SSL	725
svc	SSL VPN Client	722
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711, 741
tre	Transactional Rule Engine	780
ucime	UC-IME	339
tag-switching	Service Tag Switching	779
td	Threat Detection	733
vm	VLAN Mapping	730
vpdn	PPTP and L2TP Sessions	213, 403, 603
VPN	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
VXLAN	VXLAN	778
webfo	WebVPN Failover	721
webvpn	WebVPN and AnyConnect Client	716
session/natpat	User Session / NAT and PAT	305

EventName Attributes for Syslog Events

Some syslog events will have the additional attribute "EventName". You will be able to filter the events table to find events using the EventName attribute by filtering by attribute:value pairs. For example, you could filter events for a "Denied IP packet" by entering **EventName:"Denied IP Packet"** in the search field of the Event Logging table.

Syslog Event ID and Event Names Tables

AAA Syslog Event IDs and Event Names

EventID	EventName
109001	AAA Begin
109002	AAA Failed
109003	AAA Server Failed
109005	Authentication Success
109006	Authentication Failed
109007	Authorization Success

EventID	EventName
109008	Authorization Failed
109010	AAA Pending
109011	AAA Session Started
109012	AAA Session Ended
109013	AAA
109014	AAA Failed
109016	AAA ACL not found
109017	AAA Limit Reach
109018	AAA ACL Empty
109019	AAA ACL error
109020	AAA ACL error
109021	AAA error
109022	AAA HTTP limit reached
109023	AAA auth required
109024	Authorization Failed
109025	Authorization Failed
109026	AAA error
109027	AAA Server error
109028	AAA Bypassed
109029	AAA ACL error
109030	AAA ACL error
109031	Authentication Failed
109032	AAA ACL error
109033	Authentication Failed
109034	Authentication Failed
109035	AAA Limit Reach
113001	AAA Session limit reach
113003	AAA overridden
113004	AAA Successful
113005	Authorization Rejected

EventID	EventName
113006	AAA user locked
113007	AAA User unlocked
113008	AAA successful
113009	AAA retrieved
113010	AAA Challenge received
113011	AAA retrieved
113012	Authentication Successful
113013	AAA error
113014	AAA error
113015	Authentication Rejected
113016	AAA Rejected
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected
113020	AAA error
113021	AAA Logging Fail
113022	AAA Failed
113023	AAA reactivated
113024	AAA Client certification
113025	AAA Authentication fail
113026	AAA error
113027	AAA error

Botnet Syslog Event IDs and Event Names

EventID	EventName
338001	Botnet Source Block List
338002	Botnet Destination Block List
338003	Botnet Source Block List
338004	Botnet Destination Block List
338101	Botnet Source Allow List

EventID	EventName
338102	Botnet destination Allow List
338202	Botnet destination Grey
338203	Botnet Source Grey
338204	Botnet Destination Grey
338301	Botnet DNS Intercepted
338302	Botnet DNS
338303	Botnet DNS
338304	Botnet Download successful
338305	Botnet Download failed
338306	Botnet Authentication failed
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client
338310	Botnet dyn filter failed

Failover Syslog Event IDs and Event Names

EventID	EventName
101001	Failover Cable OK
101002	Failover Cable BAD
101003	Failover Cable not connected
101004	Failover Cable not connected
101005	Failover Cable reading error
102001	Failover Power failure
103001	No response from failover mate
103002	Failover mate interface OK
103003	Failover mate interface BAD
103004	Failover mate reports failure
103005	Failover mate reports self failure
103006	Failover version incompatible
103007	Failover version difference

EventID	EventName
104001	Failover role switch
104002	Failover role switch
104003	Failover unit failed
104004	Failover unit OK
106100	Permit/Denied by ACL
210001	Stateful Failover error
210002	Stateful Failover error
210003	Stateful Failover error
210005	Stateful Failover error
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error
210010	Stateful Failover error
210020	Stateful Failover error
210021	Stateful Failover error
210022	Stateful Failover error
311001	Stateful Failover update
311002	Stateful Failover update
311003	Stateful Failover update
311004	Stateful Failover update
418001	Denied Packet to Management
709001	Failover replication error
709002	Failover replication error
709003	Failover replication start
709004	Failover replication complete
709005	Failover receive replication start
709006	Failover receive replication complete
709007	Failover replication failure
710003	Denied access to Device

Firewall Denied Syslog Event IDs and Event Names

EventID	EventName
106001	Denied by Security Policy
106002	Outbound Deny
106006	Denied by Security Policy
106007	Denied Inbound UDP
106008	Denied by Security Policy
106010	Denied by Security Policy
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP
106014	Denied Inbound ICMP
106015	Denied by Security Policy
106016	Denied IP Spoof
106017	Denied due to Land Attack
106018	Denied outbound ICMP
106020	Denied IP Packet
106021	Denied TCP
106022	Denied Spoof packet
106023	Denied IP Packet
106025	Dropped Packet failed to Detect context
106026	Dropped Packet failed to Detect context
106027	Dropped Packet failed to Detect context
106100	Permit/Denied by ACL
418001	Denied Packet to Management
710003	Denied access to Device

Firewall Traffic Syslog Event IDs and Event Names

EventID	EventName
108001	Inspect SMTP
108002	Inspect SMTP

EventID	EventName
108003	Inspect ESMTP Dropped
108004	Inspect ESMTP
108005	Inspect ESMTP
108006	Inspect ESMTP Violation
108007	Inspect ESMTP
110002	No Router found
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length
209005	Fragment IP discard
302003	H245 Connection Start
302004	H323 Connection start
302009	Restart TCP
302010	Connection USAGE
302012	H225 CALL SIGNAL CONN
302013	Built TCP
302014	Teardown TCP
302015	Built UDP
302016	Teardown UDP
302017	Built GRE
302018	Teardown GRE
302019	H323 Failed
302020	Built ICMP
302021	Teardown ICMP
302022	Built TCP Stub
302023	Teardown TCP Stub
302024	Built UDP Stub
302025	Teardown UDP Stub
302026	Built ICMP Stub
302027	Teardown ICMP Stub

EventID	EventName
302033	Connection H323
302034	H323 Connection Failed
302035	Built SCTP
302036	Teardown SCTP
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped
303005	Inspect FTP reset
313001	ICMP Denied
313004	ICMP Drop
313005	ICMP Error Msg Drop
313008	ICMP ipv6 Denied
324000	GTP Pkt Drop
324001	GTP Pkt Error
324002	Memory Error
324003	GTP Pkt Drop
324004	GTP Version Not Supported
324005	GTP Tunnel Failed
324006	GTP Tunnel Failed
324007	GTP Tunnel Failed
337001	Phone Proxy SRTP Failed
337002	Phone Proxy SRTP Failed
337003	Phone Proxy SRTP Auth Fail
337004	Phone Proxy SRTP Auth Fail
337005	Phone Proxy SRTP no Media Session
337006	Phone Proxy TFTP Unable to Create File
337007	Phone Proxy TFTP Unable to Find File
337008	Phone Proxy Call Failed
337009	Phone Proxy Unable to Create Phone Entry
400000	IPS IP options-Bad Option List

EventID	EventName
400001	IPS IP options-Record Packet Route
400002	IPS IP options-Timestamp
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID
400006	IPS IP options-Strict Source Route
400007	IPS IP Fragment Attack
400008	IPS IP Impossible Packet
400009	IPS IP Fragments Overlap
400010	IPS ICMP Echo Reply
400011	IPS ICMP Host Unreachable
400012	IPS ICMP Source Quench
400013	IPS ICMP Redirect
400014	IPS ICMP Echo Request
400015	IPS ICMP Time Exceeded for a Datagram
400017	IPS ICMP Timestamp Request
400018	IPS ICMP Timestamp Reply
400019	IPS ICMP Information Request
400020	IPS ICMP Information Reply
400021	IPS ICMP Address Mask Request
400022	IPS ICMP Address Mask Reply
400023	IPS Fragmented ICMP Traffic
400024	IPS Large ICMP Traffic
400025	IPS Ping of Death Attack
400026	IPS TCP NULL flags
400027	IPS TCP SYN+FIN flags
400028	IPS TCP FIN only flags
400029	IPS FTP Improper Address Specified
400030	IPS FTP Improper Port Specified
400031	IPS UDP Bomb attack

EventID	EventName
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request
400035	IPS DNS Zone Transfer
400036	IPS DNS Zone Transfer from High Port
400037	IPS DNS Request for All Records
400038	IPS RPC Port Registration
400039	IPS RPC Port Unregistration
400040	IPS RPC Dump
400041	IPS Proxied RPC Request
400042	IPS YP server Portmap Request
400043	IPS YP bind Portmap Request
400044	IPS YP password Portmap Request
400045	IPS YP update Portmap Request
400046	IPS YP transfer Portmap Request
400047	IPS Mount Portmap Request
400048	IPS Remote execution Portmap Request
400049	IPS Remote execution Attempt
400050	IPS Statd Buffer Overflow
406001	Inspect FTP Dropped
406002	Inspect FTP Dropped
407001	Host Limit Reach
407002	Embryonic limit Reached
407003	Established limit Reached
415001	Inspect Http Header Field Count
415002	Inspect Http Header Field Length
415003	Inspect Http body Length
415004	Inspect Http content-type
415005	Inspect Http URL length
415006	Inspect Http URL Match

EventID	EventName
415007	Inspect Http Body Match
415008	Inspect Http Header match
415009	Inspect Http Method match
415010	Inspect transfer encode match
415011	Inspect Http Protocol Violation
415012	Inspect Http Content-type
415013	Inspect Http Malformed
415014	Inspect Http Mime-Type
415015	Inspect Http Transfer-encoding
415016	Inspect Http Unanswered
415017	Inspect Http Argument match
415018	Inspect Http Header length
415019	Inspect Http status Matched
415020	Inspect Http non-ASCII
416001	Inspect SNMP dropped
419001	Dropped packet
419002	Duplicate TCP SYN
419003	Packet modified
424001	Denied Packet
424002	Dropped Packet
431001	Dropped RTP
431002	Dropped RTCP
500001	Inspect ActiveX
500002	Inspect Java
500003	Inspect TCP Header
500004	Inspect TCP Header
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped
509001	Prevented No Forward Cmd

EventID	EventName
607001	Inspect SIP
607002	Inspect SIP
607003	Inspect SIP
608001	Inspect Skinny
608002	Inspect Skinny dropped
608003	Inspect Skinny dropped
608004	Inspect Skinny dropped
608005	Inspect Skinny dropped
609001	Built Local-Host
609002	Teardown Local Host
703001	H225 Unsupported Version
703002	H225 Connection
726001	Inspect Instant Message

Identity Based Firewall Syslog Event IDs and Event Names

EventID	EventName
746001	Import started
746002	Import complete
746003	Import failed
746004	Exceed user group limit
746005	AD Agent down
746006	AD Agent out of sync
746007	Netbios response failed
746008	Netbios started
746009	Netbios stopped
746010	Import user failed
746011	Exceed user limit
746012	User IP add
746013	User IP delete
746014	FQDN Obsolete

EventID	EventName
746015	FQDN resolved
746016	DNS lookup failed
746017	Import user issued
746018	Import user done
746019	Update AD Agent failed

IPSec Syslog Event IDs and Event Names

EventID	EventName
402114	Invalid SPI received
402115	Unexpected protocol received
402116	Packet doesn't match identity
402117	Non-IPSEC packet received
402118	Invalid fragment offset
402119	Anti-Replay check failure
402120	Authentication failure
402121	Packet dropped
426101	cLACP Port Bundle
426102	cLACP Port Standby
426103	cLACP Port Moved To Bundle From Standby
426104	cLACP Port Unbundled
602103	Path MTU updated
602104	Path MTU exceeded
602303	New SA created
602304	SA deleted
702305	SA expiration - Sequence rollover
702307	SA expiration - Data rollover

NAT Syslog Event ID and Event Names

EventID	EventName
201002	Max connection Exceeded for host
201003	Embryonic limit exceed
201004	UDP connection limit exceed
201005	FTP connection failed

EventID	EventName
201006	RCMD connection failed
201008	New connection Disallowed
201009	Connection Limit exceed
201010	Embryonic Connection limit exceeded
201011	Connection Limit exceeded
201012	Per-client embryonic connection limit exceeded
201013	Per-client connection limit exceeded
202001	Global NAT exhausted
202005	Embryonic connection error
202011	Connection limit exceeded
305005	No NAT group found
305006	Translation failed
305007	Connection dropped
305008	NAT allocation issue
305009	NAT Created
305010	NAT teardown
305011	PAT created
305012	PAT teardown
305013	Connection denied

SSL VPN Syslog Event IDs and Event Names

EventID	EventName
716001	WebVPN Session Started
716002	WebVPN Session Terminated
716003	WebVPN User URL access
716004	WebVPN User URL access denied
716005	WebVPN ACL error
716006	WebVPN User Disabled
716007	WebVPN Unable to Create
716008	WebVPN Debug
716009	WebVPN ACL error
716010	WebVPN User access network
716011	WebVPN User access
716012	WebVPN User Directory access

EventID	EventName
716013	WebVPN User file access
716014	WebVPN User file access
716015	WebVPN User file access
716016	WebVPN User file access
716017	WebVPN User file access
716018	WebVPN User file access
716019	WebVPN User file access
716020	WebVPN User file access
716021	WebVPN user access file denied
716022	WebVPN Unable to connect proxy
716023	WebVPN session limit reached
716024	WebVPN User access error
716025	WebVPN User access error
716026	WebVPN User access error
716027	WebVPN User access error
716028	WebVPN User access error
716029	WebVPN User access error
716030	WebVPN User access error
716031	WebVPN User access error
716032	WebVPN User access error
716033	WebVPN User access error
716034	WebVPN User access error
716035	WebVPN User access error
716036	WebVPN User login successful
716037	WebVPN User login failed
716038	WebVPN User Authentication Successful
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied
716041	WebVPN ACL hit count
716042	WebVPN ACL hit
716043	WebVPN Port forwarding
716044	WebVPN Bad Parameter
716045	WebVPN Invalid Parameter
716046	WebVPN connection terminated

EventID	EventName
716047	WebVPN ACL usage
716048	WebVPN memory issue
716049	WebVPN Empty SVC ACL
716050	WebVPN ACL error
716051	WebVPN ACL error
716052	WebVPN Session Terminated
716053	WebVPN SSO Server added
716054	WebVPN SSO Server deleted
716055	WebVPN Authentication Successful
716056	WebVPN Authentication Failed
716057	WebVPN Session terminated
716058	WebVPN Session lost
716059	WebVPN Session resumed
716060	WebVPN Session Terminated
722001	WebVPN SVC Connect request error
722002	WebVPN SVC Connect request error
722003	WebVPN SVC Connect request error
722004	WebVPN SVC Connect request error
722005	WebVPN SVC Connect update issue
722006	WebVPN SVC Invalid address
722007	WebVPN SVC Message
722008	WebVPN SVC Message
722009	WebVPN SVC Message
722010	WebVPN SVC Message
722011	WebVPN SVC Message
722012	WebVPN SVC Message
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address

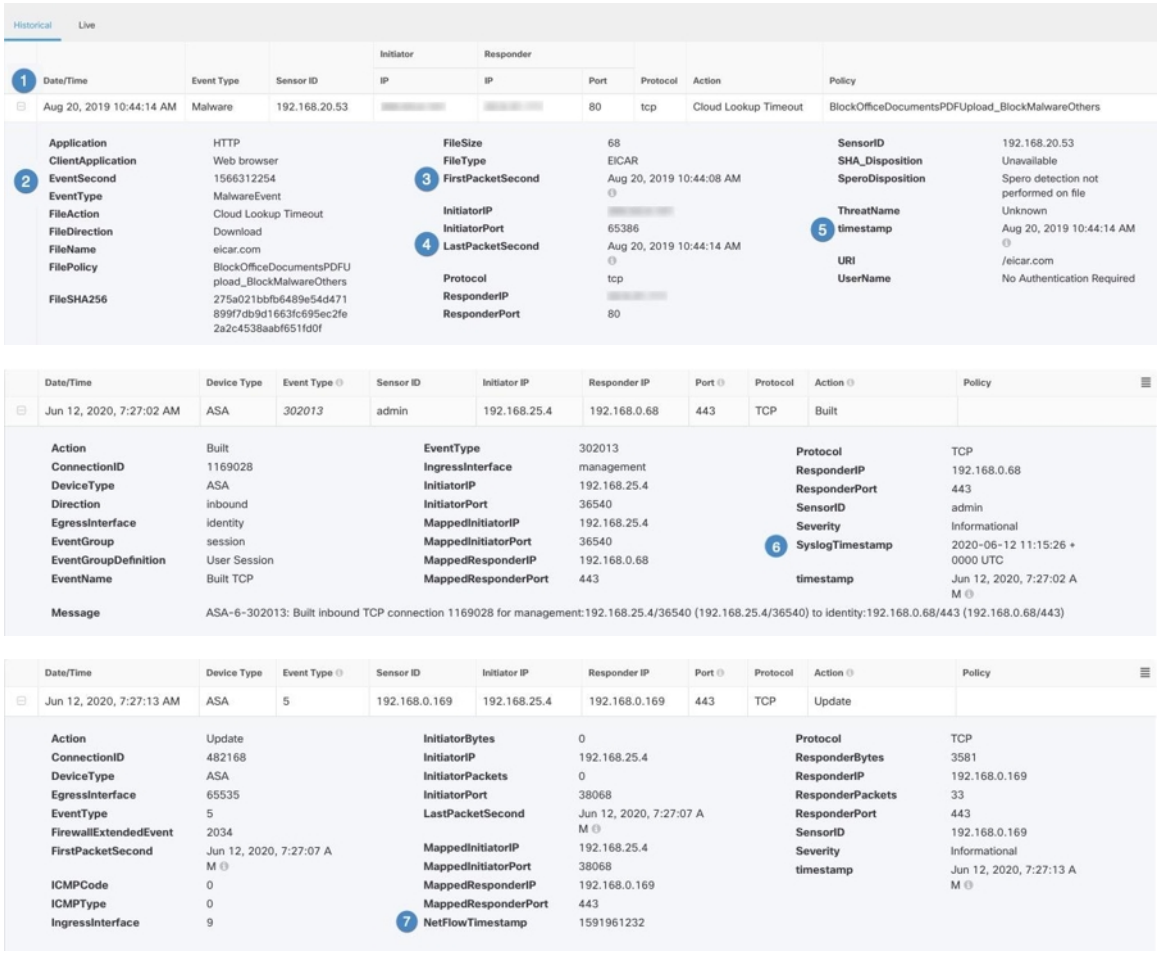
EventID	EventName
722021	WebVPN Memory issue
722022	WebVPN SVC connection established
722023	WebVPN SVC connection terminated
722024	WebVPN Compression Enabled
722025	WebVPN Compression Disabled
722026	WebVPN Compression reset
722027	WebVPN Decompression reset
722028	WebVPN Connection Closed
722029	WebVPN SVC Session terminated
722030	WebVPN SVC Session terminated
722031	WebVPN SVC Session terminated
722032	WebVPN SVC connection Replacement
722033	WebVPN SVC Connection established
722034	WebVPN SVC New connection
722035	WebVPN Received Large packet
722036	WebVPN transmitting Large packet
722037	WebVPN SVC connection closed
722038	WebVPN SVC session terminated
722039	WebVPN SVC invalid ACL
722040	WebVPN SVC invalid ACL
722041	WebVPN SVC IPv6 not available
722042	WebVPN invalid protocol
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection Up
723002	WebVPN Citrix connection Down

EventID	EventName
723003	WebVPN Citrix no memory issue
723004	WebVPN Citrix bad flow control
723005	WebVPN Citrix no channel
723006	WebVPN Citrix SOCKS error
723007	WebVPN Citrix connection list broken
723008	WebVPN Citrix invalid SOCKS
723009	WebVPN Citrix invalid connection
723010	WebVPN Citrix invalid connection
723011	WebVPN citrix Bad SOCKS
723012	WebVPN Citrix Bad SOCKS
723013	WebVPN Citrix invalid connection
723014	WebVPN Citrix connected to Server
724001	WebVPN Session not allowed
724002	WebVPN Session terminated
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL handshake Started
725002	SSL Handshake completed
725003	SSL Client session resume
725004	SSL Client request Authentication
725005	SSL Server request authentication
725006	SSL Handshake failed
725007	SSL Session terminated
725008	SSL Client Cipher
725009	SSL Server Cipher
725010	SSL Cipher
725011	SSL Device choose Cipher
725012	SSL Device choose Cipher
725013	SSL Server choose cipher
725014	SSL LIB error
725015	SSL client certificate failed

Time attributes in a syslog event

Provides information about the different time-stamps in the Event Logging page to help you filter and find events of interest.

Understanding the purposes of the different time-stamps in the Event Logging page will help you filter and find the events that interest you.



Number	Label	Description
1	Date/Time	The time the Secure Event Connector (SEC) processed the event. This may not be the same as the time the firewall inspected that traffic. Same value as timestamp.
2	EventSecond	Equals with LastPacketSecond.

Number	Label	Description
3	FirstPacketSecond	The time at which the connection opened. The firewall inspects the packet at this time. The value of the FirstPacketSecond is calculated by subtracting the ConnectionDuration from the LastPacketSecond. For connection events logged at the beginning of the connection, the value of FirstPacketSecond, LastPacketSecond, and EventSecond will all be the same.
4	LastPacketSecond	The time at which the connection closed. For connection events logged at the end of the connection, LastPacketSecond and EventSecond will be equal.
5	timestamp	The time the Secure Event Connector (SEC) processed the event. This may not be the same as the time the firewall inspected that traffic. Same value as Date/Time.
6	Syslog TimeStamp	Represents the syslog originated time if 'logging timestamp' is used. If the syslog does not have this info, the time the SEC received the event is reflected.
7	NetflowTimeStamp	The time at which the ASA finished gathering enough flow records/events to fill a NetFlow packet to then send them off to a flow collector.

56 Integrate Security Cloud Control with Splunk

Topics:

- Splunk Federated Search Integration with Cisco Security Analytics and Logging

Connect Cisco Security Cloud Control with Splunk to investigate firewall activity across your security environment. Choose the integration that fits your workflow: use **Splunk Federated Search** to query historical events stored in Cisco Security Analytics and Logging from Splunk,.

- Splunk Federated Search: Search and analyze events in Cisco Security Analytics and Logging directly from Splunk Cloud Platform without ingesting the data into Splunk. Set up the connection, check its status, and troubleshoot or disconnect it from Security Cloud Control.

  For more information click: Splunk Federated Search Integration with Cisco Security Analytics and Logging

Splunk Federated Search Integration with Cisco Security Analytics and Logging

Describes the integration between Splunk Federated Search and Cisco Security Analytics and Logging for searching firewall events across multiple Splunk deployments.

Splunk Federated Search integration with Cisco Security Analytics and Logging is a cloud-based integration that

- enables Splunk administrators to search Cisco Secure Firewall Threat Defense events stored in Cisco Security Analytics and Logging without direct ingestion into Splunk Cloud Platform
- allows viewing analytics, running reports, and investigating incidents directly from the Splunk Cloud Platform interface, and
- provides federated search capabilities across multiple Splunk deployments or environments from a single search interface.

Integration details

Terminology Note: In this document, "Cisco Security Analytics and Logging" refers specifically to Cisco Security Analytics and Logging (SaaS), which is a cloud-based platform that serves as a central repository for aggregated security event data.

Splunk Federated Search is a feature that is available in both Splunk Cloud Platform and Splunk Enterprise. You can use Splunk Federated Search to search and analyze data across multiple Splunk deployments or environments from a single search interface. For more information, see Splunk Federated Search.

Using the Splunk Federated Search feature, Cisco Security Analytics and Logging can be added as a dataset in the Splunk Cloud Platform. This integration enables Splunk administrators to search the Cisco Secure Firewall Threat Defense events stored in Cisco Security Analytics and Logging, without having to ingest them into the Splunk Cloud Platform directly. Splunk administrators can also view analytics, run reports, and investigate incidents directly from the Splunk Cloud Platform interface. For more information on the logs stored in Cisco Security Analytics and Logging, see Security Analytics and Logging (SaaS) in Security Cloud Control.

Benefits of Splunk Federated Search integration with Cisco Security Analytics and Logging:

- Accelerated security investigations: Run federated queries on historical firewall logs without any storage overhead.
- Wider data coverage: Enable the Splunk Cloud Platform users to leverage data stored in Cisco Security Analytics and Logging for security investigation, operational monitoring, and business intelligence.
- End-to-end visibility: Correlate real-time alerts with historical data seamlessly.
- Statistical analysis over time: Analyze large historical datasets for trends and threat patterns.
- Compliance readiness: Maintain searchable, long-term logs to meet audit and regulatory needs.
- Operational efficiency: Enable SecOps teams to access logs directly, eliminating the need for NetOps teams to provide access.

Region compatibility for tenant mapping

Each Cisco SAL tenant belongs to a Cisco Security Cloud Control region. Each Splunk Cloud Platform deployment runs in an AWS region. Splunk software supports a tenant mapping only when the deployment's AWS region corresponds to the tenant's Cisco Security Cloud Control region.

Table 50:

Cisco Security Cloud Control region	Corresponding Splunk Cloud Platform deployment AWS regions
https://us.manage.security.cisco.com/	us-east-1 (N. Virginia), us-west-2 (Oregon)
https://eu.manage.security.cisco.com/	eu-central-1 (Frankfurt), eu-north-1 (Stockholm), eu-south-1 (Milan), eu-west-1 (Ireland), eu-west-2 (London), eu-west-3 (Paris)
https://apj.manage.security.cisco.com/	ap-northeast-1 (Tokyo), ap-northeast-2 (Seoul), ap-southeast-1 (Singapore), ap-southeast-3 (Jakarta)
https://in.manage.security.cisco.com/	ap-south-1 (Mumbai)
https://aus.manage.security.cisco.com/	ap-southeast-2 (Sydney)

How Splunk Federated Search Integrates with Cisco Security Analytics and Logging

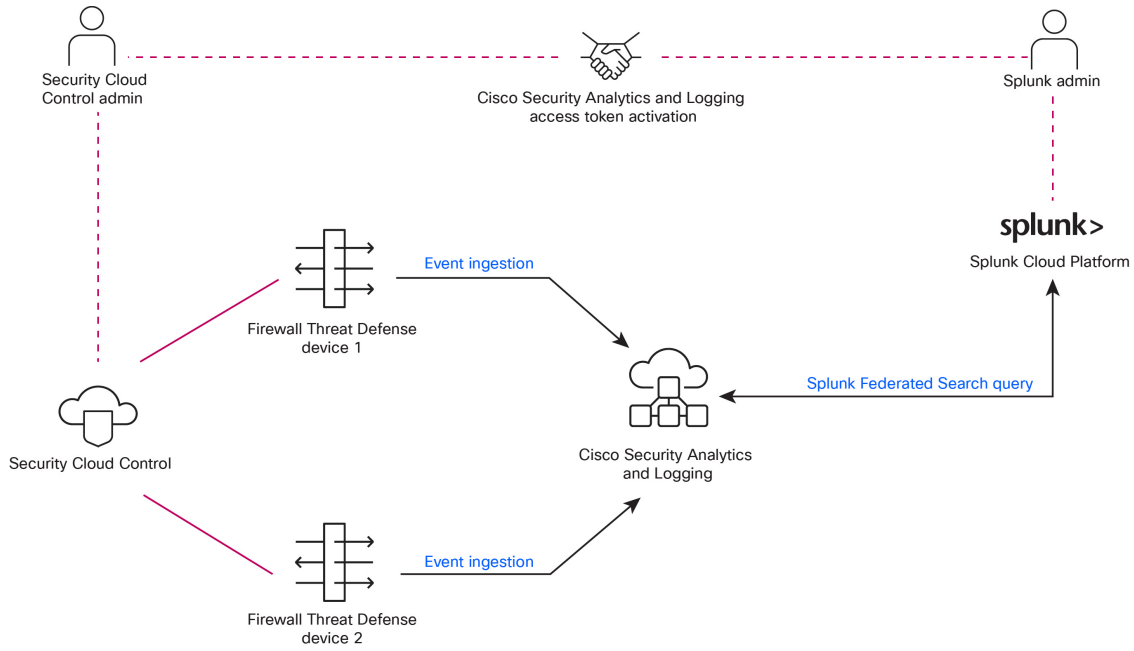
Describes the integration topology between Splunk Federated Search and Cisco Security Analytics and Logging within the Security Cloud Control platform, showing information flow and component interactions.

Splunk Federated Search integration with Cisco Security Analytics and Logging is a cloud-native security architecture that

- enables federated search queries from Splunk Cloud Platform to access security event data in Cisco Security Analytics and Logging without local data ingestion
- leverages token-based authentication to authorize data access between the platforms, and
- centralizes security event visibility through Security Cloud Control for unified security management across hybrid and multicloud environments.

Integration components and data flow

This topology shows the flow of information and interactions between the following components:



- **Security Cloud Control**: A unified, cloud-native security management interface designed to centralize and simplify the management of Cisco security solutions across hybrid and multicloud environments. It leverages Cisco Security Analytics and Logging to provide visibility into security events and trends.
- **Cisco Security Analytics and Logging**: This cloud-based platform serves as a central repository for aggregated security event data from various sources, including the Cisco Secure Firewall Threat Defense devices. It ingests event logs from these devices and allows Splunk Federated Search to query this event data.
- **Security Cloud Control admin**: This administrator manages the Security Cloud Control platform, overseeing the configuration and operational status of security devices like firewalls. They are responsible for setting up the necessary integrations, including the activation of the access token for Cisco Security Analytics and Logging.
- **Cisco Security Analytics and Logging token activation**: A access token-based mechanism is employed to authenticate and authorize Splunk and Cisco Security Analytics and Logging service interactions. It ensures that event data in Cisco Security Analytics and Logging can be queried by Splunk Federated Search.
- **Splunk admin**: This administrator is responsible for managing the Splunk environment and leveraging its capabilities for security analysis. The admin configures and initiates federated searches to query and retrieve security event data from external platforms, such as Cisco Security Analytics and Logging, without needing to ingest all data locally.
- **Splunk Federated Search** query: This refers to the query initiated from Splunk Cloud platform to access and analyze data residing in Cisco Security Analytics and Logging. All Firewall Threat Defense security events can be queried from the Splunk Cloud Platform.
- **Splunk Cloud Platform**: This represents the Splunk Security Information and Event Management (SIEM) platform, which utilizes its federated search capability to integrate with Cisco Security Analytics and Logging. This integration allows the security teams to query event data from Cisco Security Analytics and Logging without needing to ingest data locally.

How Splunk Federated Search integration works with Cisco Security Analytics and Logging

Describes the workflow of Splunk Federated Search integration with Cisco Security Analytics and Logging in Security Cloud Control.

This integration allows organizations to leverage both Splunk Cloud Platform capabilities and Cisco Security Analytics and Logging data through federated search functionality.

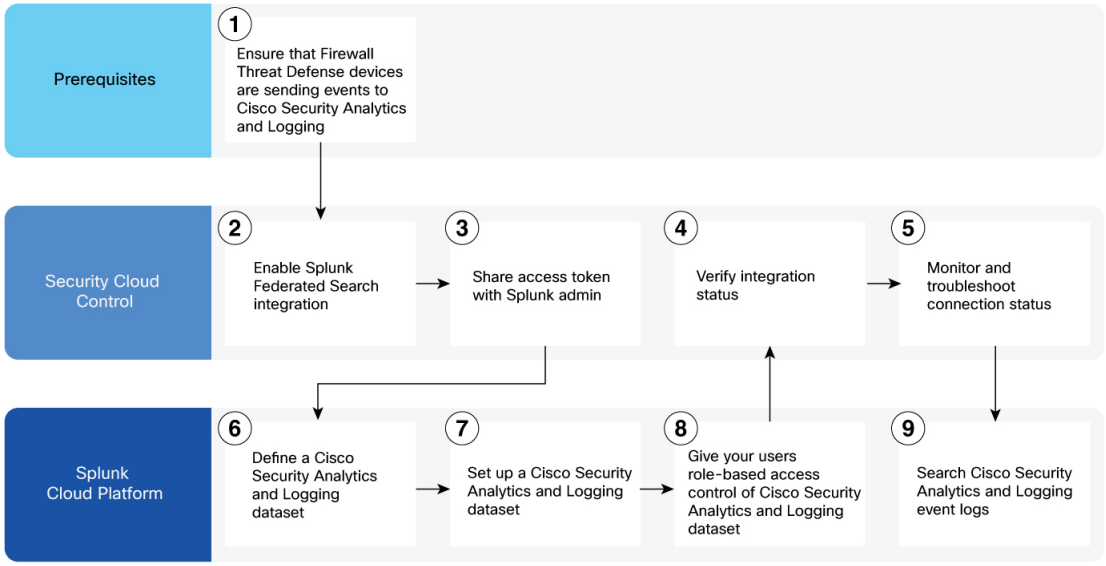
Summary

The key components involved in the Splunk Federated Search integration process are:

- Firewall Threat Defense devices: Generate security events and send them to Cisco Security Analytics and Logging
- Security Cloud Control: Manages the integration configuration and provides access tokens for Splunk
- Splunk Cloud Platform: Configures dataset and role-based access controls
- Splunk administrators: Configure the Splunk side of the integration and manage user access

Workflow

The completed integration enables users to perform federated searches of Cisco Security Analytics and Logging data directly from the Splunk Cloud Platform interface, providing unified access to security event data across both platforms.



These stages describe how the Splunk Federated Search integration with Cisco Security Analytics and Logging works:

1. Prerequisites phase: Firewall Threat Defense devices send security events to Cisco Security Analytics and Logging.
   - Ensure that Firewall Threat Defense devices managed on the Security Cloud Control platform are sending intrusion, file and malware, and connection events to Cisco Security Analytics and Logging. For more information, see About Security Analytics and Logging (SaaS) in Security Cloud Control.

2. Integration enablement phase: Security Cloud Control administrator enables the integration and shares access credentials.
   - Enable Splunk Federated Search integration. For more information, see Enable Splunk Federated Search Integration with Cisco Security Analytics and Logging on page 1006.
   - Share the access token with the Splunk admin. For more information, see Enable Splunk Federated Search Integration with Cisco Security Analytics and Logging on page 1006.

3. Splunk configuration phase: Splunk Cloud Platform administrator configures the federated search components.
   - Define a Cisco Security Analytics and Logging dataset. For more information, see Splunk Federated Search for Cisco Analytics and Logging (SAL) - Splunk Side.

- Set up a Cisco Security Analytics and Logging dataset. For more information, see Splunk Federated Search for Cisco Analytics and Logging (SAL) - Splunk Side.
- Give your users role-based access control of Cisco Security Analytics and Logging datasets. For more information, see Splunk Federated Search for Cisco Analytics and Logging (SAL) - Splunk Side.

4. Verification and monitoring phase: Security Cloud Control administrator verifies integration status and monitors ongoing operations.
   - Verify the integration status. For more information, see Verify Connection Status of Splunk Federated Search with Cisco Security Analytics and Logging on page 1008.
   - Monitor and troubleshoot the connection status. For more information, see Monitor and Troubleshoot Connection Status of Splunk Federated Search with Cisco Security Analytics and Logging on page 1009.
5. Operational phase: Users search Cisco Security Analytics and Logging event logs through Splunk Cloud Platform.
   - Search Cisco Security Analytics and Logging event logs. For more information, see Search your Cisco Firewall datasets.

Requirements for Splunk Federated Search Integration with Cisco Security Analytics and Logging

Outlines the prerequisites and limitations for integrating Splunk Federated Search with Cisco Security Analytics and Logging.

Prerequisites

Ensure you meet these requirements before initiating the Splunk Federated Search integration with Cisco Security Analytics and Logging.

- You must have Super Admin user role in Security Cloud Control platform to initiate the Splunk Federated Search integration with Cisco Security Analytics and Logging by generating the access token. Users without Super Admin privileges can only view the Splunk Federated Search integration flow.
- Ensure that the Firewall Threat Defense devices deployed on the Security Cloud Control platform are sending intrusion, file and malware, and connection events to Cisco Security Analytics and Logging.

Limitation

By default, only up to 30 days of log data from Cisco Security Analytics and Logging is available for federated search.

Enable Splunk Federated Search Integration with Cisco Security Analytics and Logging

Configure an access token to enable Splunk administrator access to Cisco Security Analytics and Logging data through the Splunk Cloud Platform integration.

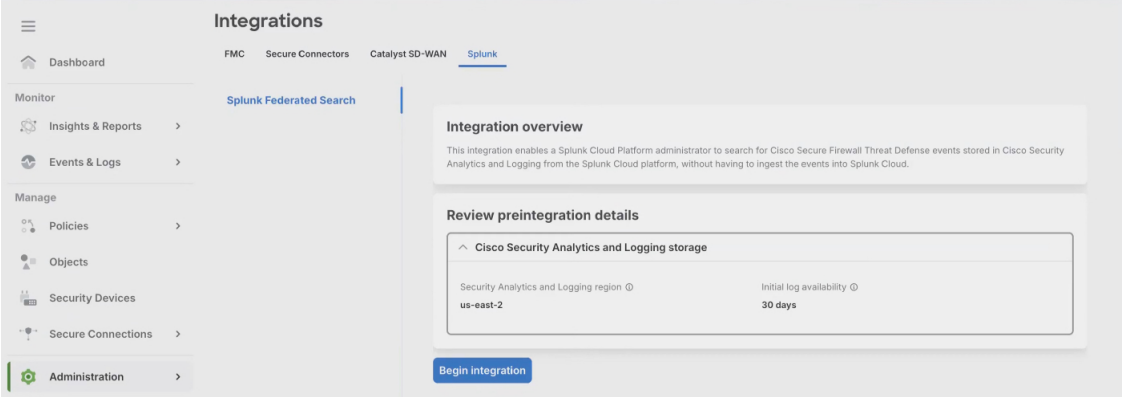
Generate a secure access token that authenticates and authorizes interactions between the Splunk Cloud Platform and the Cisco Security Analytics and Logging service for data access.

Use this procedure to generate the access token that can be copied and shared with the Splunk administrator to enable access to Cisco Security Analytics and Logging data. The secure access token is automatically generated and is used to authenticate and authorize interactions between the Splunk Cloud Platform and the Cisco Security Analytics and Logging service. These tokens are generated per tenant and can be renewed manually.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. From the left pane, choose **Administration** > **Integrations** > **Splunk** > **Splunk Federated Search**.

3. Under the **Splunk Federated Search** tab, review the preintegration details and click **Begin integration**.



The initial log availability is up to 30 days, that is, up to 30 days of firewall event data is available for Splunk Federated Search.

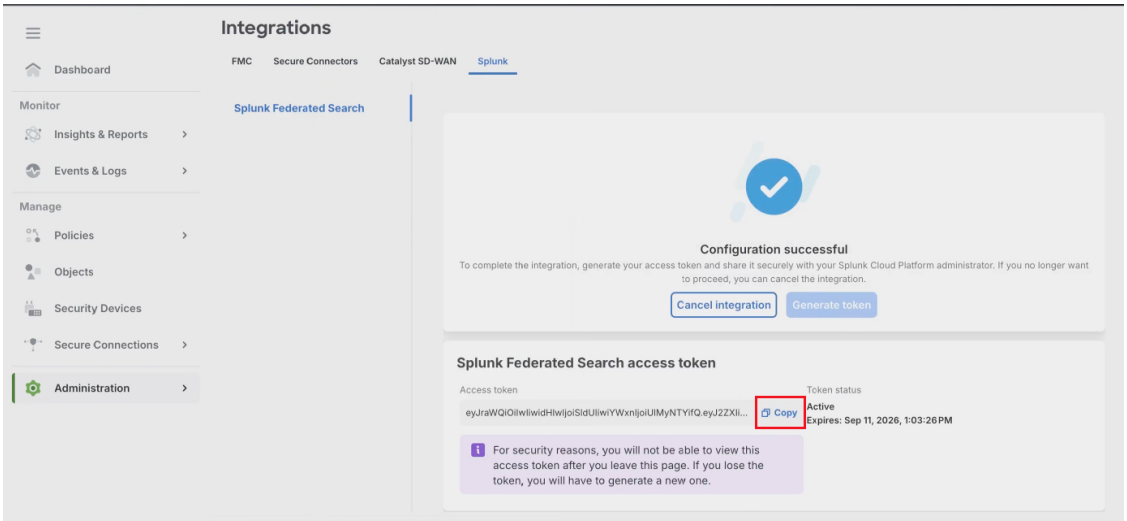
> **Note**
>
> This step may take a few minutes to complete. The time taken depends on the volume of event data stored in Cisco Security Analytics and Logging.

You can click **Cancel integration** to cancel the integration at this stage. No changes will be made to your Cisco Security Analytics and Logging environment and access will not be granted to Splunk Cloud Platform if you cancel the integration.

4. After you see the **Configuration successful** message, click **Generate token**.

   If you see the **Configuration failed** message, click **Retry setup**.

5. From the **Splunk Federated Search access token** section, copy the access token and share it with the Splunk administrator.



This access token is valid for 7 days (168 hours) from the time it is generated. The Splunk administrator must create the dataset before the access token expires.

> **Note**
>
> If you leave this page without copying the displayed access token, the access token is lost and you must regenerate a new access token by clicking **Regenerate token**.

You have successfully generated an access token that enables Splunk administrator access to Cisco Security Analytics and Logging data through the Splunk Cloud Platform integration.

What to do next

Follow the steps in Splunk Federated Search for Cisco Analytics and Logging (SAL) - Splunk Side to:

1. Define a Cisco Security Analytics and Logging dataset.
2. Set up a Cisco Security Analytics and Logging dataset.
3. Give your users role-based access control of Cisco Security Analytics and Logging datasets.

Verify Connection Status of Splunk Federated Search with Cisco Security Analytics and Logging

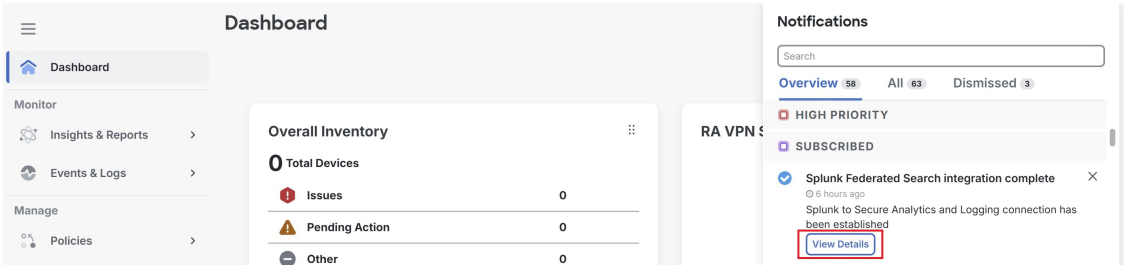
Verify the connection status between Splunk Federated Search and Cisco Security Analytics and Logging through the notifications interface.

This task helps you check whether the integration between Splunk Federated Search and Cisco Security Analytics and Logging is functioning properly and monitor any connection issues.

Use this procedure to verify the connection status of Splunk Federated Search with Cisco Security Analytics and Logging.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the top-right corner, click the **Notifications** ( ) icon to view the status of your connection.
3. Click **View details** to monitor the connection status on the **Splunk Federated Search** tab under **Integrations**.



You can view the current connection status and monitor any integration issues between Splunk Federated Search and Cisco Security Analytics and Logging.

Monitor and Troubleshoot Connection Status of Splunk Federated Search with Cisco Security Analytics and Logging

Configure monitoring and troubleshooting for the connection status between Splunk Federated Search and Cisco Security Analytics and Logging after integration is complete.

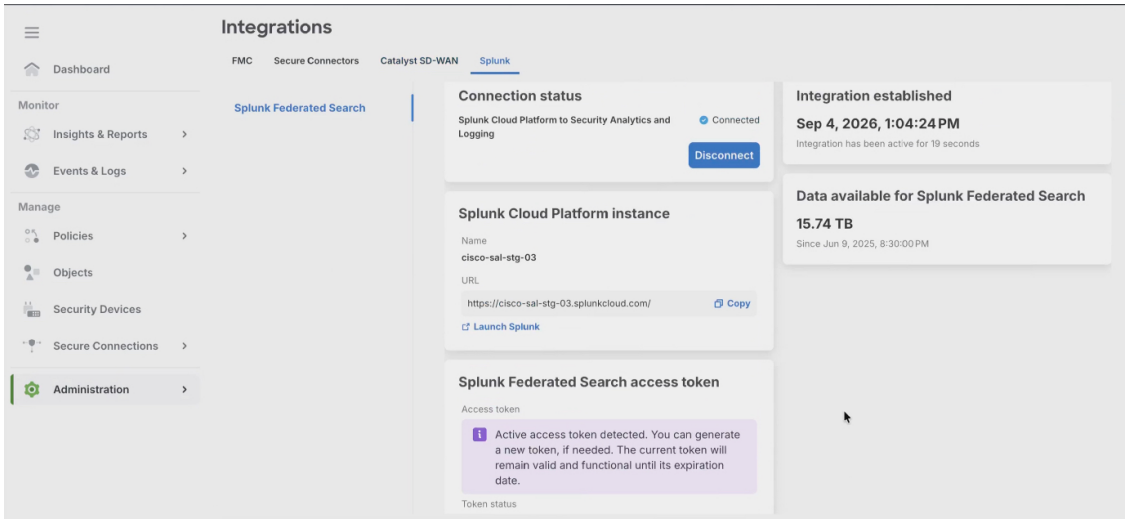
This task enables you to monitor the integration status and troubleshoot connectivity issues between Splunk Federated Search and Cisco Security Analytics and Logging.

After the integration is complete, use this procedure to monitor and troubleshoot the connection status of Splunk Federated Search with Cisco Security Analytics and Logging.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Splunk** > **Splunk Federated Search**.

   The table shows the sections displayed under the **Splunk Federated Search** tab after the integration is complete.



Section	Description
Connection Status	**Splunk to Security Analytics and Logging**: Indicates the current state of connectivity between Splunk Cloud Platform and Cisco Security Analytics and Logging.
Integration established	The date and time at which the integration was completed, displayed in local time.
Splunk Cloud Platform instance	**Name**: Name of the Splunk Cloud instance. **URL**: URL of the Splunk Cloud instance for federated search for Cisco Security Analytics and Logging.
Data available for Splunk Federated Search	Amount of data, typically measured in gigabytes (GB) or terabytes (TB), which can be queried with Splunk Federated Search.

Section	Description
Splunk Federated Search access token	• **Access token**: If the access token is active, no access token is displayed here. Click **Regenerate token** if you still want to generate a new token. If you generate a new token, the current token will remain valid and functional until its expiration date. • **Token status**: Status of the access token. It can be either **Active** or **Expired**. • **Generated by**: Email address of the user who generated the access token. • **Expires**: Date and time when the access token expires.

Troubleshooting

- What should I do if the connection status shows disconnected?

  If the connection status shows **Disconnected**, go back to the **Integrations** page to restart integration.

- What should I do if the Splunk instance URL does not launch?

  If the Splunk instance URL does not launch, contact your Splunk administrator or Splunk Support.

- The data available for Splunk Federated Search is zero. What should I do?

  If the data volume shows zero, it means no data is currently available for federated search. In such cases, you should verify whether the firewall events are flowing into the **Events and Logs** page in the Security Cloud Control platform. For existing customers, federated search up to 30 days of historical events. The actual period depends on the retention and onboarding configuration.

You can view the connection status, integration details, and troubleshoot any issues with the Splunk Federated Search integration.

What to do next:

Search Cisco Security Analytics and Logging event logs. For more information, see Search your Cisco Firewall datasets.

Disconnect Splunk Federated Search

Configure the disconnection of Splunk Federated Search integration with Cisco Security Analytics and Logging to revoke access while preserving data.

Disconnect the integration of Splunk Federated Search with Cisco Security Analytics and Logging when you no longer need federated search capabilities.

You can disconnect the integration of Splunk Federated Search with Cisco Security Analytics and Logging in Security Cloud Control at any time. After you disconnect, Splunk Cloud Platform will no longer have access to the Cisco Security Analytics and Logging data, and Splunk Cloud Platform users will not be able to perform a federated search.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **Integrations** > **Splunk Federated Search**.
3. In the **Splunk Federated Search** tab, click **Disconnect** under **Connection status**.

> **Note**
>
> If Cisco Security Analytics and Logging is disconnected from Splunk Federated Search, no data will be deleted or lost; only the access is revoked. You can reconnect at any time.

The Splunk Federated Search integration is successfully disconnected. Splunk Cloud Platform no longer has access to Cisco Security Analytics and Logging data, and federated search is disabled.

57 Use Cisco Secure Cloud Analytics Portal

Topics:

- Provision a Cisco secure cloud analytics portal
- Review sensor health and Security Cloud Control integration status in Secure Cloud Analytics
- Cisco secure cloud analytics sensor deployment for total network analytics and reporting
- Cisco Secure Cloud Analytics alerts from Security Cloud Control
- Cisco secure cloud analytics and dynamic entity modeling
- Alerts based on firewall events
- Modify alert priorities

This chapter provides information about Cisco Secure Cloud Analytics portal.

Provision a Cisco secure cloud analytics portal

Configure a Cisco Secure Cloud Analytics portal to view alerts and monitor network flow data after purchasing the required license.

Provision a Cisco Secure Cloud Analytics portal to view Secure Cloud Analytics alerts and monitor network analytics after deploying and configuring the Secure Event Connector (SEC).

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

If you purchase a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, after you deploy and configure the Secure Event Connector (SEC), you must associate a Secure Cloud Analytics portal with your Security Cloud Control portal to view Secure Cloud Analytics alerts. When you purchase the license, if you have an existing Secure Cloud Analytics portal, you can provide the Secure Cloud Analytics portal name and immediately link it to your Security Cloud Control portal.

Otherwise, you can request a new Secure Cloud Analytics portal from the Security Cloud Control UI. The first time you access Secure Cloud Analytics alerts, the system takes you to a page to request the Secure Cloud Analytics portal. The user that requests this portal is granted administrator permission in the portal.

Procedure

1. In the left pane, click **Analytics** > **Secure Cloud Analytics** to open the Secure Cloud Analytics UI in a new window.
2. Click **Start Free Trial** to provision a Secure Cloud Analytics portal and associate it with your Security Cloud Control portal.

   Note

   After you request the portal, the provisioning may take up to several hours.

   What to do next:

   - If you purchased a **Logging Analytics and Detection** license, your configuration is complete. If you want to view the status of your Security Cloud Control integration or sensor health from the Secure Cloud Analytics portal UI, see Review sensor health and Security Cloud Control integration status in Secure Cloud Analytics on page 363 for more information. If you want to work with alerts in the Secure Cloud Analytics portal, see Cisco Secure Cloud Analytics alerts from Security Cloud Control on page 364 and Working with Alerts Based on Firepower Events for more information.
   - If you purchased a **Total Network Analytics and Monitoring** license, deploy one or more Secure Cloud Analytics sensors to your internal network to pass network flow data to the cloud. If you want to monitor cloud-based network flow data, configure your cloud-based deployment to pass flow data to Secure Cloud Analytics. See Cisco secure cloud analytics sensor deployment for total network analytics and reporting on page 363 for more information.

Ensure that your portal is provisioned before moving on to the next step.

1. In the left pane, click **Analytics** > **Secure Cloud Analytics** to open the Secure Cloud Analytis UI in a new window.
2. You have these options:

- If you requested a Secure Cloud Analytics portal, and the system states it is still provisioning the portal, wait and try to access the alerts later.
- If the Secure Cloud Analytics portal is provisioned, enter your **Username** and **Password**, then click **Sign in**.

> **Note**
>
> The administrator user can invite other users to create accounts within the Secure Cloud Analytis portal. See Cisco Secure Cloud Analytics alerts from Security Cloud Control on page 364 for more information.

Review sensor health and Security Cloud Control integration status in Secure Cloud Analytics

Configure visibility into sensor health and Security Cloud Control integration status in Secure Cloud Analytics for ASA devices, including ASA integration with Cisco Umbrella and secure internet gateway use cases.

This task allows you to monitor the operational status of your sensors and Security Cloud Control integration to ensure proper connectivity and configuration.

Sensor Status

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

In the Secure Cloud Analytics web UI, you can view your Security Cloud Control integration status and your configured sensors from the Sensor List page. The Security Cloud Control integration is the read-only *connection-events* sensor. Stealthwatch Cloud provides an overall health of your sensors in the main menu:

- green cloud icon ( ) - connectivity established with all sensors, and Security Cloud Control if configured
- yellow cloud icon ( ) - connectivity established with some sensors, or Security Cloud Control if configured, and one or more sensors is not configured properly
- red cloud icon ( ) - connectivity lost with all configured sensors, and Security Cloud Control if configured

Per sensor or Security Cloud Control integration, a green icon signifies connectivity established, and a red icon signifies connectivity lost.

Procedure

1. In the Secure Cloud Analytics portal UI, select **Settings** ( ) > **Sensors**.
2. Select **Sensor List**.

The Sensor List page displays the status of all configured sensors and Security Cloud Control integration, allowing you to identify any connectivity or configuration issues.

Cisco secure cloud analytics sensor deployment for total network analytics and reporting

Explains Cisco Secure Cloud Analytics sensor deployment for total network analytics and reporting, including configuration options for on-premises and cloud-based environments.

Cisco Secure Cloud Analytics sensor deployment for total network analytics and reporting is a network monitoring solution that

- deploys sensors within on-premises networks to pass network flow data to the cloud for analysis
- configures cloud-based deployments to pass network flow log data to Secure Cloud Analytics for analysis, and
- requires a Total Network Analytics and Monitoring license for provisioning a Secure Cloud Analytics portal.

Secure cloud analytics sensor overview and deployment

Required License: Total Network Analytics and Monitoring

If you obtain a **Total Network Analytics and Monitoring** license, after you provision a Secure Cloud Analytics portal, you can:

- Deploy and configure a Secure Cloud Analytics sensor within your on-premises network to pass network flow data to the cloud for analysis.
- Configure your cloud-based deployment to pass network flow log data to Secure Cloud Analytics for analysis.

Firewalls at your network perimeter gather information about traffic between your internal network and external networks, while Secure Cloud Analytics sensors gather information about traffic within your internal network.

Note

FDM-managedSecure Firewall Threat Defense devices may be configured to pass NetFlow data. When you deploy a sensor, do not configure it to pass NetFlow data from any of your FDM-managedSecure Firewall Threat Defense devices which you also configured to pass event information to Security Cloud Control.

See the Secure Cloud Analytics Sensor Installation Guide for sensor deployment instructions and recommendations.

See the Secure Cloud Analytics Public Cloud Monitoring Guides for cloud-based deployment configuration instructions and recommendations.

Note

You can also review instructions in the Secure Cloud Analytics portal UI to configure sensors and your cloud-based deployment.

See the Secure Cloud Analytics Free Trial Guide for more information about Secure Cloud Analytics.

Next steps:

- Continue with Cisco Secure Cloud Analytics alerts from Security Cloud Control on page 364.

Cisco Secure Cloud Analytics alerts from Security Cloud Control

Describes how to view Cisco Secure Cloud Analytics alerts from Security Cloud Control, including symptoms, checks, likely causes, and corrective actions for managed devices.

Cisco Secure Cloud Analytics alerts from Security Cloud Control are security notifications that

- are generated from firewall event data and network flow data
- require cross-launching from Security Cloud Control to the Secure Cloud Analytics portal for review, and
- display in the Security Analytics menu with a badge showing the number of open alerts.

License requirements and access methods

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

While you can review your firewall events on the Events logging page, you cannot review Cisco Secure Cloud Analytics alerts from the Security Cloud Control portal UI. You can cross-launch from Security Cloud Control to the Secure Cloud Analytics portal using the Security Analytics menu option, and view alerts generated from firewall event data (and from network flow data if you enabled **Total Network Analytics and Monitoring**). The Security Analytics menu option displays a badge with the number of Secure Cloud Analytics alerts in an open workflow status, if 1 or more are open.

If you use a Security Analytics and Logging license to generate Secure Cloud Analytics alerts, and you provisioned a new Secure Cloud Analytics portal, log into Security Cloud Control, then cross-launch to Secure Cloud Analytics using Cisco Security Cloud Sign On. You can also directly access your Secure Cloud Analytics portal through its URL.

See Cisco Security Cloud Sign On for more information.

Invite users to join your secure cloud analytics portal

Configure user access to your Secure Cloud Analytics portal by inviting users via email to join and create their Cisco Security Cloud Sign On credentials.

Invite other users by email to join your Secure Cloud Analytics portal and enable them to create Cisco Security Cloud Sign On credentials for cross-launch access from Security Cloud Control to Secure Cloud Analytics.

The initial user to request the Secure Cloud Analytics portal provision has administrator privileges in the Secure Cloud Analytics portal. That user can invite other users by email to join the portal. If these users do not have Cisco Security Cloud Sign On credentials, they can create them using the link in the invite email. Users can then use Cisco Security Cloud Sign On credentials to log in during the cross-launch from Security Cloud Control to Secure Cloud Analytics.

Before you begin

Follow these steps to invite other users to your Secure Cloud Analytics portal by email:

Procedure

1. Log into your Secure Cloud Analytics portal as an administrator.
2. Select **Settings** > **Account Management** > **User Management**.
3. Enter an **Email** address.
4. Click **Invite**.

The invited user receives an email invitation to join the Secure Cloud Analytics portal and can create Cisco Security Cloud Sign On credentials if needed.

Cross-launch from Security Cloud Control to Secure Cloud Analytics

Configure cross-launching to view security alerts from Security Cloud Control in Secure Cloud Analytics.

This task enables you to access and view security alerts through the integrated interface between Security Cloud Control and Secure Cloud Analytics.

To view security alerts from Security Cloud Control:

Procedure

1. Log into the Security Cloud Control portal.
2. In the left pane, choose **Analytics** > **Secure Cloud Analytics**.
3. In the Secure Cloud Analytics interface, select **Monitor** > **Alerts**.

You can now view and monitor security alerts from the Secure Cloud Analytics interface.

Cisco secure cloud analytics and dynamic entity modeling

Describes Cisco Secure Cloud Analytics and dynamic entity modeling, including translated addresses, rule behavior, interface scope, and policy impact.

Cisco Secure Cloud Analytics is a software as a service (SaaS) solution that

- monitors your on-premises and cloud-based network deployments by gathering information about your network traffic from sources including firewall events and network flow data,
- creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns, and
- generates alerts using this information combined with other sources of threat intelligence, such as Talos, which constitute a warning that there is behavior that may be malicious in nature.

License requirements

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

Dynamic entity modeling overview:

Dynamic entity modeling tracks the state of your network by performing a behavioral analysis on firewall events and network flow data. In the context of Secure Cloud Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they take on your network.

Secure Cloud Analytics, integrated with a **Logging Analytics and Detection** license, can draw from firewall events and other traffic information in order to determine the types of traffic the entity usually transmits. If you purchase a **Total Network Analytics and Monitoring** license, Secure Cloud Analytics can also include NetFlow and other traffic information in modeling entity traffic. Secure Cloud Analytics updates these models over time, as the entities continue to send traffic, and potentially send different traffic, to keep an up-to-date model of each entity.

From this information, Secure Cloud Analytics identifies:

- Roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Cloud Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- Observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, or a remote access session established with another entity. If you integrate with Security Cloud Control, these facts can be obtained from firewall events. If you also purchase a **Total Network Analytics and Monitoring** license, the system can also obtain facts from NetFlow, and generate observations from both firewall events and NetFlow. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

Alerts and analysis process

Based on the combination of roles, observations, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system. Note that one alert may represent multiple observations. If a firewall logs multiple connection events related to the same connection and entities, this may result in only one alert.

For example, a New Internal Device observation on its own does not constitute possible malicious behavior. However, over time, if the entity transmits traffic consistent with a Domain Controller, then the system assigns a Domain Controller role to the entity. If the entity subsequently establishes a connection to an external server that it has not established a connection with previously, using unusual ports, and transfers large amounts of data, the system would log a New Large Connection (External) observation and an Exceptional Domain Controller observation. If that external server is identified as on a Talos watchlist, then the combination of all this information would lead Secure Cloud Analytics to generate an alert for this entity's behavior, prompting you to take further action to research, and remediate malicious behavior.

When you open an alert in the Secure Cloud Analytics web portal UI, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about the entities involved, including the traffic that they transmitted, and external threat intelligence if it is available. You can also see other observations and alerts that entities were involved with, and determine if this behavior is tied to other potentially malicious behavior.

Note

When you view and close alerts in Secure Cloud Analytics, you cannot allow or block traffic from the Secure Cloud Analytics UI. You must update your firewall access control rules to allow or block traffic, if you deployed your devices in active mode, or your firewall access control rules if your firewalls are deployed in passive mode.

Alerts based on firewall events

Describes the workflow for working with alerts based on firewall events, including event details, device status, reporting views, and follow-up actions.

An alert based on firewall events is a security notification that

- generates from observations produced by firewall event data
- follows a workflow based on status changes from open to closed
- allows assignment, tagging, and investigation to help identify and resolve potential security issues, and
- requires a Logging Analytics and Detection or Total Network Analytics and Monitoring license.

Alert workflow process

When the system generates an alert, the default status is Open, and no user is assigned. When you view the Alerts summary, all open alerts are displayed by default, as these are of immediate concern.

> **Note**
>
> If you have a **Total Network Analytics and Monitoring** license, your alerts can be based on observations generated from NetFlow, observations generated from firewall events, or observations from both data sources.

As you review the Alerts summary, you can assign, tag, and update status on alerts as an initial triage. You can use the filters and search functionality to locate specific alerts, or display alerts of different statuses, or associated with different tags or assignees. You can set an alert's status to Snoozed, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove Snoozed status from an alert, to display it as an open alert again. As you review alerts, you can assign them to yourself or another user in the system. Users can search for all alerts assigned to their username.

From the Alerts summary, you can view an alert detail page. This page allows you to review additional context about the supporting observations that resulted in this alert, and additional context about the entities involved in this alert. This information can help you pinpoint the actual issue, in order to further research the issue on your network, and potentially resolve malicious behavior.

As you research within the Secure Cloud Analytics web portal UI, in Security Cloud Control, and on your network, you can leave comments with the alert that describe your findings. This helps create a record for your research that you can reference in the future.

If you complete your analysis, you can update the status to Closed, and have it no longer appear by default as an open alert. You can also re-open a closed alert in the future if circumstances change.

These general guidelines and suggestions for investigating alerts use the additional context that Secure Cloud Analytics provides when it logs an alert to help guide your investigation.

These steps are meant to be neither comprehensive, nor all-inclusive. They merely offer a general framework with which to start investigating an alert.

You can take these steps when you review an alert:

1. Best practice for triaging open alerts on page 368
2. Snooze alerts for later analysis on page 369
3. Update the alert for further investigation on page 369
4. Review the alert and start your investigation on page 370
5. Examine the entity and users on page 371
6. Best practice for remediating issues using secure cloud analytics on page 372
7. Update and close the alert on page 373

Best practice for triaging open alerts

Outlines the systematic approach for investigating and prioritizing open alerts, particularly when multiple alerts require attention.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

Triage the open alerts, especially if more than one have yet to be investigated:

- See Monitoring Secure Cloud Analytics Alerts Generated from FTD Events for more information on cross-launching from Security Cloud Control to Secure Cloud Analytics, and viewing alerts.
- Have you configured this alert type as high priority?

- Did you set a high sensitivity for the affected subnet?
- Is this unusual behavior from a new entity on your network?
- What is the entity's normal role, and how does the behavior in this alert fit that role?
- Is this an exceptional deviation from normal behavior for this entity?
- If a user is involved, is this expected behavior from the user, or exceptional?
- Is protected or sensitive data at risk of being compromised?
- How severe is the impact to your network if this behavior is allowed to continue?
- If there is communication with external entities, have these entities established connections with other entities on your network in the past?

If this is a *high* priority alert, consider quarantining the entity from the internet, or otherwise closing its connections, before continuing your investigation.

Snooze alerts for later analysis

Configure alert snoozing to temporarily hide lower-priority alerts from the active alert list for later review.

Snooze alerts when they are of lesser priority, as compared to other alerts, allowing you to focus on more critical alerts while preserving lower-priority alerts for future analysis.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

For example, if your organization is repurposing an email server as an FTP server, and the system generates an Emergent Profile alert (indicating that an entity's current traffic matches a behavior profile that it did not previously match), you can snooze this alert as it is intended behavior, and revisit it at a later date. A snoozed alert does not show up with the open alerts; you must specifically filter to review these snoozed alerts.

Follow these steps to snooze an alert:

Procedure

1. Click **Close Alert**.
2. In the Snooze this alert pane, select a snooze period from the drop-down.
3. Click **Save**.

   When you are ready to review these alerts, you can unsnooze them. This sets the status to Open, and displays the alert alongside the other Open alerts.

   Unsnooze a snoozed alert:

   - From a snoozed alert, click **Unsnooze Alert**.

The alert is snoozed for the selected period and removed from the active alerts view until the snooze period expires or you manually unsnooze it.

Update the alert for further investigation

Configure alert assignment and tagging to enable further investigation and tracking of security events.

Update alerts with assignment and categorization information to enable effective investigation and establish tracking patterns for security events.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

Open the alert detail and prepare to assign and categorize the alert for investigation.

Procedure

1. Select **Monitor** > **Alerts**.
2. Click an alert type name.

What to do next:

Based on your initial triage and prioritization, assign the alert and tag it:

a. Select a user from the **Assignee** drop-down to assign the alert, so a user can start investigating.

b. Select one or more **Tags** from the drop-down to add tags to the alert, to better categorize your alert's for future identification, as well as to try and establish long-term patterns in your alerts.

c. Enter a **Comment on this alert**, then click **Comment** to leave comments as necessary to track your initial findings, and assist the person assigned to the alert. The alert tracks both system comments and user comments.

The alert is assigned to a specific user with appropriate tags and comments, enabling organized investigation and tracking of security events.

Review the alert and start your investigation

Configure your investigation process by reviewing alert details and analyzing supporting observations to determine if source entity behavior indicates malicious activity.

Review the alert detail to understand why Secure Cloud Analytics generated an alert and examine supporting observations to understand what these observations mean for the source entity.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

If you are reviewing an assigned alert, review the alert detail to understand why Secure Cloud Analytics generated an alert. Review the supporting observations to understand what these observations mean for the source entity.

Note that if the alert was generated based on firewall events, the system does not note that your firewall deployment was the source of this alert.

View all of the supporting observations for this source entity to understand its general behavior and patterns, and see if this activity may be part of a longer trend:

Procedure

1. From the alert detail, click the arrow icon () next to an observation type to view all logged observations of that type.
2. Click the arrow icon () next to **All Observations for Network** to view all logged observations for this alert's source entity.

Download the supporting observations in a comma-separated value file, if you want to perform additional analysis on these observations:

- From the alert detail, in the Supporting Observations pane, click **CSV**.

From the observations, determine if the source entity behavior is indicative of malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet.

View additional context surrounding the source entity from a source entity IP address or hostname, including other alerts and observations it may be involved in, information about the device itself, and what type of session traffic it is transmitting:

- Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
- Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
- Select **Device** from the IP address or hostname drop-down to view information about the device.
- Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that the source entity in Secure Cloud Analytics is always internal to your network. Contrast this with the Initiator IP in a firewall event, which indicates the entity that initiated a connection, and may be internal or external to your network.

From the observations, examine information about other external entities. Examine the geolocation information, and determine if any of the geolocation data or Umbrella data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior.

Review the context for an external entity IP address or hostname with which the source entity established a connection:

- Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
- Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
- Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
- Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
- Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
- Select **Talos Intelligence** from the IP address or hostname drop-down to view information about this information on Talos's website.
- Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
- Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that connected entities in Secure Cloud Analytics are always external to your network. Contrast this with the Responder IP in a firewall event, which indicates the entity that responded to a connection request, and may be internal or external to your network.

Leave comments as to your findings.

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Examine the entity and users

Configure examination procedures for source entities and users involved in firewall-based security alerts to identify potential malicious activity or unauthorized access.

Perform detailed examination of source entities and users following alert review to identify potential security threats, malware, vulnerabilities, or unauthorized activities that triggered the alert.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

After you review the alert in the Secure Cloud Analytics portal UI, you can perform an additional examination on a source entity directly, any users that may have been involved with this alert, and other related entities.

Procedure

1. Examine the source entity location and access logs

   Determine where the source entity is on your network, physically or in the cloud, and access it directly. Locate the log files for this entity. If it is a physical entity on your network, access the device to review the log information, and see if there is any information as to what caused this behavior. If it is a virtual entity, or stored in the cloud, access the logs and search for entries related to this entity. Examine the logs for further information on unauthorized logins, unapproved configuration changes, and the like.

2. Examine the entity for malware and vulnerabilities

   Examine the entity. Determine if you can identify malware or a vulnerability on the entity itself. See if there has been some malicious change, including if there are physical changes to a device, such as a USB stick that is not approved by your organization.

3. Investigate user involvement

   Determine if a user on your network, or from outside your network, was involved. Ask the user what they were doing if possible. If the user is unavailable, determine if they were supposed to have access, and if a situation occurred that prompted this behavior, such as a terminated employee uploading files to an external server before leaving the company.

4. Enter a **Comment on this alert**, then click **Comment**

   Leave comments as to your findings from the alert detail.

You have examined the source entity, users, and related components to identify potential security threats and documented your findings in the alert comments for future reference and investigation tracking.

Best practice for remediating issues using secure cloud analytics

Outlines remediation actions for malicious behavior detected through Secure Cloud Analytics alerts.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

If malicious behavior caused the alert, remediate the malicious behavior.

- If a malicious entity or user attempted to log in from outside your network, update your firewall rules and firewall configuration to prevent the entity or user from accessing your network.
- If an entity attempted to access an unauthorized or malicious domain, examine the affected entity to determine if malware is the cause. If there are malicious DNS redirects, determine if other entities on your network are affected, or part of a botnet. If this is intended by a user, determine if there is a legitimate reason for this, such as testing firewall settings. Update your firewall rules and firewall configuration to prevent further access to the domain.
- If an entity is exhibiting behavior that is different from the historical entity model behavior, determine if the behavior change is intended. If it is unintended, examine whether an otherwise authorized user on your network is responsible for the change. Update your firewall rules and firewall configuration to address unintended behavior if it involves connections with entities that are external to your network.
- If you identify a vulnerability or exploit, update or patch the affected entity to remove the vulnerability, or update your firewall configuration to prevent unauthorized access. Determine if other entities on your network may similarly be affected, and apply the same update or patch to those entities. If the vulnerability or exploit currently does not have a fix, contact the appropriate vendor to let them know.

- If you identify malware, quarantine the entity and remove the malware. Review the firewall file and malware events to determine if other entities on your network are at risk, and quarantine and update the entities to prevent this malware from spreading. Update your security intelligence with information about this malware, or the entities that caused this malware. Update your firewall access control and file and malware rules to prevent this malware from infecting your network in the future. Alert vendors as necessary.
- If malicious behavior resulted in data exfiltration, determine the nature of the data sent to an unauthorized source. Follow your organization's protocols for unauthorized data exfiltration. Update your firewall configuration to prevent future data exfiltration attempts by this source.

Update and close the alert

Configure alert tags and close alerts after completing your security investigation in Secure Cloud Analytics.

Update alerts with relevant tags and close them after completing your security investigation to maintain accurate alert tracking and provide feedback on alert usefulness.

This task is part of a workflow defined in Alerts based on firewall events on page 367.

Add additional tags based on your findings:

Procedure

1. In the Secure Cloud Analytics portal UI, select **Monitor** > **Alerts**.
2. Select one or more **Tags** from the drop-down.

Add final comments describing the results of your investigation, and any remediation steps taken:

- From an alert's detail, enter a **Comment on this alert**, then click **Comment**.

Close the alert, and mark it as helpful or not helpful:

1. From an alert's detail, click **Close Alert**.
2. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. Note that this does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
3. Click **Save**.

Reopen a closed alert

If you discover additional information related to a closed alert, or want to add more comments related to that alert, you can reopen it, changing the status to Open. You can then make changes as necessary to the alert, then close it again when your additional investigation is complete.

Reopen a closed alert:

- From a closed alert's detail, click **Reopen Alert**.

Modify alert priorities

Configure alert priorities to adjust system sensitivity for generating alerts based on your network environment requirements.

Modifying alert priorities allows you to customize how sensitive the system is to generating alerts of specific types, emphasizing certain alerts that are of concern in your network environment.

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Alert types come with default priorities, which affect how sensitive the system is to generating alerts of this type. Alerts default to *low* or *normal* priority, based on Cisco intelligence and other factors. Based on your network environment, you may want to reprioritize alert types, to emphasize certain alerts that you are concerned with. You can configure any alert type to be *low*, *normal*, or *high* priority.

Procedure

1. Select **Monitor** > **Alerts**.
2. Click the settings drop-down icon (), then select **Alert Types and Priorities**.
3. Click the edit icon () next to an alert type and select *low*, *medium*, or *high* to change the priority.

The alert priority is modified according to your selection, affecting the system's sensitivity to generating alerts of that type.

58 Monitor Remote Access Virtual Private Network Sessions from Secure Firewall ASA and Firewall Threat Defense

Topics:

- Remote access VPN session monitoring

This chapter details remote access monitor VPN for Secure Firewall ASA and Firewall Threat Defense.

Remote access VPN session monitoring

Explains how to monitor Remote Access VPN sessions in Security Cloud Control Firewall Management for ASA and FDM-managed devices, including live and historical AnyConnect session data, dashboards, search and filters, customized views, CSV exports, and session disconnection.

Remote access VPN session monitoring is a Security Cloud Control Firewall Management capability that

- provides secure connection monitoring for remote users, such as mobile users or telecommuters
- enables you to determine quickly whether remote access VPN problems exist and where they exist, and
- allows you to disconnect remote access VPN sessions as needed.

Remote access VPN monitoring capabilities

You can monitor remote access VPN sessions from ASA, FTDs managed using Cloud-Delivered Firewall Management Center, and FDM-managed devices.

The Remote Access Virtual Private Monitoring page provides this information:

- A list of active and historical sessions for up to a year.
- Shows intuitive graphical visuals to provide at-a-glance views from all active VPN headends managed by Security Cloud Control Firewall Management.
- The live session screen shows the most used operating system and VPN connection profile in the Security Cloud Control Firewall Management tenant. It also shows the average session duration and data uploaded and downloaded.

  Note

  The data upload and download statistics won't include the data from FTDs managed using Cloud-Delivered Firewall Management Center.

- Filtering capabilities to narrow your search based on criteria such as device type, device names, session length, and the amount of data transmitted and received.

Note

The **Data TX** and **Data RX** information are not available for FTDs managed using Cloud-Delivered Firewall Management Center.

Monitor live AnyConnect remote access VPN sessions

Configure monitoring for real-time data from active AnyConnect remote access VPN sessions on your devices.

Monitor real-time data from active AnyConnect remote access VPN sessions to track current connectivity and session status.

You can monitor real-time data from active AnyConnect remote access VPN sessions on the devices. This data is automatically refreshed every 10 minutes. If you want to retrieve the latest list of sessions at any point, you click the reload icon appearing on the right corner of the screen.

When you migrate a Firewall Threat Defense device running any version from 7.7.x to 10.0.x to Cloud-Delivered Firewall Management Center Version 10.1.91, active remote access VPN sessions with Azure AD integration are not displayed in the monitoring dashboard. You can view the active sessions from the Firewall Threat Defense device CLI.

Before you begin

- Onboard the remote access VPN head-ends to Security Cloud Control.
- Ensure that the connectivity status of the devices you want to monitor live data is "Online" on the **Security Devices** page.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Reports & Analytics** > **Remote Access Monitoring**.
3. Click **RA VPN**.
4. Click **Live**.

   You can search and filter RA VPN sessions to narrow down your search based on criteria such as device type, session length, and upload and download data range.

   > **Note**
   >
   > The **Data TX** and **Data RX** information are not available for FTD.

The live AnyConnect remote access VPN sessions are displayed with real-time data that refreshes automatically every 10 minutes.

View live remote access VPN data

Provides dashboard and tabular views of live Remote Access VPN session data from all active VPN headends.

The live data is presented both in the dashboard and tabular form.

Dashboard view

You have to click the **Show Charts View** icon appearing at the top right corner of the screen to see the dashboard.

The dashboard provides at-a-glance views from all active VPN headends managed by Security Cloud Control.

- **Breakdown (All Devices)**: Shows a total number of live sessions. It also shows a pie chart that is divided into four arc lengths. It illustrates the percentage of VPN sessions of the top three devices with the highest number of sessions. The remaining arc length represents the aggregate of other devices.
- Shows most used operating system and connection profile in the Security Cloud Control tenant.
- Shows average session duration and data uploaded and downloaded.
- **Active Sessions by Country**: Shows an interactive heat map of the location of the users connected to your RA VPN headends.

- Countries from which users have connected are shown in progressively darker shades of blue, depending on the relative proportion of the sessions established from that country – the darker the blue color means more sessions are established from that country.
- The legend at the bottom of the map provides a scale that indicates the correlation between the number of sessions in a country and the shade of blue used to color the country.
- Hover the mouse pointer on the map to see the country's name and the total number of active user sessions established from that country.
- Hover the mouse pointer on the table to see the country's location and the total number of active user sessions on the map.

Tabular view

Click the **Show Tabular View** icon on the top right corner of the screen to view the data in tabular format.

The tabular form provides a complete list of VPN users connected presently.

- The **Location** column shows the location of all the users connected to the VPN headends by geolocating their public IP addresses. Click a row to view the user details. On clicking the location link in the left pane, the location of the user is shown on the Google map.

  Important

  Security Cloud Control applies a standard filter to the live data and represents them on the dashboard. You can apply new filters only when tabular data is shown, since the custom filters are not supported in the visual dashboard view. Click **Clear** to remove all filters you have applied. You cannot remove the standard filter.

You can use Search and Filter RA VPN Sessions functionalities to narrow down your search based on criteria such as device type, session length, and upload and download data range. Note that a maximum of 10,000 results can be displayed at once.

A green dot with an **Active** label in the status column indicates an active VPN user's session.

Monitor historical AnyConnect remote access VPN sessions

Configure monitoring for historical data from AnyConnect Remote Access VPN sessions recorded over the past year.

Monitor historical data from AnyConnect Remote Access VPN sessions to analyze VPN usage patterns and session data recorded over the past 1 year.

You can monitor the historical data from AnyConnect Remote Access VPN sessions recorded over the past 1 year.

Before you begin

- Onboard the RA VPN head-ends to Security Cloud Control.

Follow these steps to monitor Historical AnyConnect Remote Access VPN Sessions:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Reports & Analytics** > **Remote Access Monitoring**.
3. Click **RA VPN**.
4. Click **Historical**.

- Remote Access VPN Session data is stored and available to query for 1 year.
- You can use Search and Filter RA VPN Sessions functionalities to narrow down your search based on criteria such as device type, session length, and upload and download data range.
- The **Data TX** and **Data RX** information are not available for Secure Firewall Threat Defense.

You can now view and monitor historical AnyConnect Remote Access VPN session data, with options to search and filter based on various criteria.

View historical remote access VPN data

Provides historical Remote Access VPN data in both dashboard and tabular formats to monitor VPN sessions and user connections.

The historical data is presented both in the dashboard and tabular form.

Dashboard view

You have to click the **Show Charts View** icon appearing at the top right corner of the screen to see the dashboard. You will see the dashboard view along with the tabular view.

The dashboard provides at-a-glance views from all active VPN headends managed by Security Cloud Control. It provides a bar graph showing the VPN sessions recorded for all devices in the last 24 hours, 7 days, and 30 days. You can select the duration from the drop-down. You can hover over on individual bars to see the date and the total number of sessions on that day.

Tabular view

You have to click the **Show Tabular View** icon appearing at the top right corner of the screen to see only the tabular view. The tabular form provides a complete list of VPN users connected over the last year.

The **Location** column shows the location of all the users connected to the VPN headends by geolocating their public IP addresses. Click a row to view the user details. On clicking the location link in the left pane, the location of the user is shown on the Google map.

Important

Security Cloud Control applies a standard filter to the historical data and represents them on the dashboard. You can apply new filters only when tabular data is shown, since the dashboard is not supported for custom filters. Clearing the newly applied filters relaunches the dashboard (On the screen, click **Clear** to remove manually applied filters). You cannot remove the standard filter.

You can use Search and Filter RA VPN Sessions functionalities to narrow down your search based on criteria such as session date and time range, session length, and upload and download data range. Note that a maximum of 10,000 results can be displayed at once.

A green dot with an **Active** label in the status column indicates an active VPN user's session.

Search and filter remote access VPN sessions

Configure search and filter functionality to find remote access VPN sessions based on device criteria, session parameters, and data transfer metrics.

This task enables you to locate specific remote access VPN sessions efficiently using search and filter capabilities to analyze session data and troubleshoot connectivity issues.

Use search and filter functionality to find remote access VPN sessions when you need to monitor or analyze specific session data. The filter functionality is available for both live and historical views, allowing you to examine sessions over the last three months.

Procedure

1. Use the search bar to find remote access VPN sessions by device name, IP address, or serial number.

   Start typing in the search bar, and remote access VPN sessions that fit the search criteria will be displayed. Search is not case-sensitive.

2. Use the filter sidebar to find remote access VPN sessions based on specific criteria.
   - **Filter by Devices**: Select one or all devices from the **All Types** tab to view sessions from selected devices. The window also categorizes the devices based on their type and displays them under the corresponding tabs.
   - **Sessions Time Range** (Applicable only for historical data): View historical sessions from a specified date and time range. Note that you can view data recorded over the last three months.
   - **Sessions Length**: View sessions based on a specified session's duration length. Set the time unit (hours, minutes, or seconds) and specify the minimum and maximum duration length by moving the slider. You can also specify the length in the provided fields.
   - **Upload (TX)**: View sessions based on a specified amount of data uploaded or transferred to the secured network. Set the unit (GB, MB, or KB) and select the range by moving the slider accordingly. You can also specify the values in the available fields.
   - **Download (RX)**: View sessions based on a specified amount of data downloaded or received from the secured network. Set the unit (GB, MB, or KB) and select the range by moving the slider accordingly. You can also specify the values in the available fields.

     Note

     The **Upload (TX)** and **Download (RX)** options do not apply to FTD.

Remote access VPN sessions matching your search criteria or filter parameters are displayed, allowing you to analyze specific session data based on your requirements.

Customize the remote access VPN monitoring view

Configure the remote access VPN monitoring view to display only the column headers that are relevant to your monitoring requirements.

Customize the remote access VPN monitoring view to display only relevant column headers for your specific monitoring needs.

You can modify the remote access VPN monitoring view in both live and historical modes. Security Cloud Control remembers your selection the next time you sign in to Security Cloud Control.

Procedure

1. Click the column filter icon located to the right of the columns.

2. Select or deselect the columns you want to display in the view.

The remote access VPN monitoring view displays only the selected column headers. Your column selection preferences are saved for future sessions.

Export remote access VPN sessions to a CSV file

Export the remote access VPN sessions of one or more devices to a comma-separated value (.CSV) file for analysis in spreadsheet applications.

Export remote access VPN sessions to analyze session data in a spreadsheet application and to create sortable and filterable reports for monitoring purposes.

You can export the remote access VPN sessions of one or more devices to a comma-separated value (.CSV) file. You can open the .CSV file in a spreadsheet application such as Microsoft Excel to sort and filter the items on your list. This information helps you to analyze the remote access VPN sessions. Every time you export the sessions, Security Cloud Control creates a new .CSV file, where the file created has a date and time in its name.

Security Cloud Control can export a maximum of 100,000 active sessions to the CSV file. If the total number of sessions from all devices exceeds the maximum limit, you can use the **View By Device** filter and generate reports for individual devices.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Insights & Reports** > **Reports & Analytics** > **Remote Access Monitoring**.
3. In the **View By Devices** area, select one of the following:
   - **All Devices** to export active sessions from all devices listed below it.
   - Click on a device that you want to export sessions of that device.
4. Click the icon on the top right corner. Security Cloud Control exports the rules you see on the screen to a .CSV file.
5. Open the .CSV file in a spreadsheet application to sort and filter the results.

The remote access VPN sessions are exported to a .CSV file with a timestamp in the filename, ready for analysis in your spreadsheet application.

View the remote access VPN dashboard

Configure access to the Remote Access VPN Dashboard to view consolidated information about remote access VPN connections from ASA, Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense, and FDM-managed devices.

This task allows you to access the Remote Access VPN Dashboard, which provides consolidated information about remote access VPN connections from multiple device types.

Security Cloud Control provides a consolidated information about remote access VPN connections from ASA, Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense, and FDM-managed devices.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.

2. In the left pane, click **Secure Connections** > **Remote Access VPN**.

The Remote Access VPN Dashboard displays the following information:

- **VPN Tunnel Status**: Displays a pie chart representing the active and idle VPN tunnels, each in appropriate colors. This chart shows the top ten number of remote access VPN sessions by headends.
- **Statistics**: Shows the average session duration and data uploaded and downloaded.

Disconnect Remote Access VPN Sessions of an ASA User

Configure termination of all active remote access VPN sessions for users on ASA devices.

This task terminates all active remote access VPN sessions to manage user access and maintain security compliance on your device.

You can terminate all active remote access VPN sessions of all users on the ASA device. You can perform this task in both live and historical modes.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **VPN** > **Remote Access VPN Monitoring**.
3. In the **View By Devices** area, click on the ASA device that you want to end all active sessions on that device.
4. Click **Terminate All Sessions** appearing in the top-right corner.
5. Click **Yes, Terminate All Sessions** to confirm your selection.

All active remote access VPN sessions for the selected device are terminated and users are disconnected.

Disconnect all active RA VPN sessions of a user

Configure the termination of all active RA VPN sessions for a specific user on your security device.

Use this task to terminate all of a user's active Remote Access VPN sessions on a security device.

Security Cloud Control terminates all of the user's active RA VPN sessions on that ASASecure Firewall Cloud Native device when you disconnect a user. You can perform this task in both live and historical modes.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **VPN** > **Remote Access VPN Monitoring**.
3. Search for a user whose sessions you want to disconnect. You can type the search criteria into the **Search** bar.
4. Click on an active session, and in the **Actions** pane on the right, click the **Terminate all RA VPN sessions for this user** link.

All active RA VPN sessions for the selected user are terminated on the device.

Disconnect Remote Access VPN Sessions on FDM-Managed Device

Configure remote access VPN session termination on FDM-managed devices using CLI commands.

This task allows you to terminate remote access VPN sessions for specific users on an FDM-managed device when the Security Cloud Control interface does not provide this capability.

Currently, it is not possible to terminate remote access VPN sessions on an FDM-managed device using the Security Cloud Control interface. Instead, you can connect to the Firewall Threat Defense CLI using SSH and disconnect the desired user. You can perform this task on an online FDM-managed device onboarded to Security Cloud Control.

Procedure

1. Log on to Firewall Device Manager and use the device CLI as explained in the **Logging Into the Command Line Interface (CLI)** section of the "Getting Started" chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.
2. Execute the **VPN-sessionsdb logoff {name}** command and replace **name** with the user name. This command terminates all sessions for the username that you specify.

The remote access VPN sessions for the specified user are terminated.

Disconnect remote access VPN sessions on FTD

Configure the termination of active remote access VPN sessions on Cloud-Delivered Firewall Management Center managed FTD devices.

Terminate active remote access VPN sessions on Cloud-Delivered Firewall Management Center managed FTD to manage network access and security.

You can terminate active remote access VPN sessions on Cloud-Delivered Firewall Management Center managed FTD. This task can be performed in live mode.

Security Cloud Control provides a VPN Sessions Manager user role to allow users to view and terminate VPN sessions. See User Roles for more information.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Secure Connections** > **End User Connections** > **Remote Access VPN** > **Firewall Threat Defense**.
3. In the tabular view, find the session you wish to terminate using the search and filter options and click on it.
4. In the **Actions** pane on the right, perform the action you want:
   - **Terminate session**: Disconnect the selected session on the device.
   - **Terminate all of this user's sessions**: Disconnect all sessions of the user on the device.
   - **Terminate all sessions on this device**: Disconnect all user sessions on the device.
5. Click **Terminate Session(s)** to confirm your selection.

After a session is terminated, the session is immediately disconnected from the VPN headend. However, Security Cloud Control does not immediately query the device to retrieve the list of live sessions. Therefore, you might still see the terminated session after you've chosen to terminate it. To see the latest list of sessions from the device, click the **Reload** icon.

Note

If you have terminated a session, you may have to wait a while before clicking on the **Reload** button, as the Cloud-Delivered Firewall Management Center can take a while before it reflects the updated list of live sessions.

59 Monitor and report change logs, workflows, and jobs

Topics:

- Change logs in Security Cloud Control
- Change log entries after deploying to an ASA
- Change log entries after reading changes from an ASA
- View change log differences
- Change request management
- Export the change log
- Monitoring Jobs in Security Cloud Control
- Monitor workflows in Security Cloud Control

Describes how to monitor and report change logs, workflows, and jobs to track configuration changes, bulk device operations, and device communication processes for understanding network security posture.

Security Cloud Control effectively monitors configuration change logs, bulk device operations, and the process that runs when communicating with devices. This helps you understand how your network's existing policies influence its security posture.

Change logs in Security Cloud Control

Explains how to use change logs in Security Cloud Control to review configuration changes, track who made them and when, identify conflict entries, compare differences, and export log data for troubleshooting or reporting.

A change log is a configuration tracking feature that

- captures configuration changes made in Security Cloud Control, providing a single view that includes changes in all the supported devices and services
- provides a side-by-side comparison of changes made to device configuration
- records onboarding and removal of devices, and
- detects policy change conflicts occurring outside Security Cloud Control.

Change log management capabilities

Change logs provide these capabilities for configuration management and troubleshooting:

- Provides labels for all change log entries
- Provides answers about who, what, and when during an incident investigation or troubleshooting
- Enables downloading of the complete change log, or only a portion of it, as a CSV file

> **Note**
>
> Changes made in Cloud-Delivered Firewall Management Center are not reflected in the change log.

Change log capacity: Security Cloud Control retains the change log information for one year and deletes data older than a year.

There is a difference between the change log information stored in Security Cloud Control's database and what you see in an exported change log. See Export the change log on page 1048 for more information.

Change log entries: A change log entry reflects the changes to a single device configuration, an action performed on a device, or the change made to a device outside Security Cloud Control:

- For change log entries that contain configuration changes, you can view details about the change by clicking anywhere in the corresponding row.
- For out-of-band changes made outside Security Cloud Control and are detected as conflicts, the **System User** is reported as the **Last User**.
- Security Cloud Control closes a change log entry after a device's configuration on Security Cloud Control is synced with the configuration on the device, or when a device is removed from Security Cloud Control. Configurations are considered to be in sync after they read the configuration from the device to Security Cloud Control or after deploying the configuration from Security Cloud Control to the device.
- Security Cloud Control creates a new change log entry immediately after completing an existing entry, irrespective of whether the change was a success or failure. Additional configuration changes are added to the new change log entry that opens.
- Events are displayed for read, deploy, and delete actions for a device. These actions close a device's change log.

- A change log is closed after Security Cloud Control is in sync with the configuration on the device (either by reading or deploying), or when Security Cloud Control no longer manages the device.
- If a change is made to the device outside of Security Cloud Control, a *Conflict detected* entry is included in the change log.

Pending and completed change log entries: Change logs have a status of either Pending or Completed. As you make changes to a device's configuration using Security Cloud Control, these changes are recorded in a Pending change log entry. Activities that complete a Pending change log:

- Reading a configuration from a device to Security Cloud Control
- Deploying changes from Security Cloud Control to a device
- Deleting a device from Security Cloud Control
- Running a CLI command that updates the running configuration file

This image shows a Pending change log entry in an ASA. This is denoted by the open circle next to the timestamp.



Search and filter change log entries: You can search and filter change log entries. Use the search field to find events. Use the filter ( ) to find the entries that meet the criteria you specify. You can also combine the two tasks by filtering the change log and adding a keyword to the search field to find an entry within the filtered results.

- Manage device configuration on page 813
- Change request management on page 1042
- Export the change log on page 1048

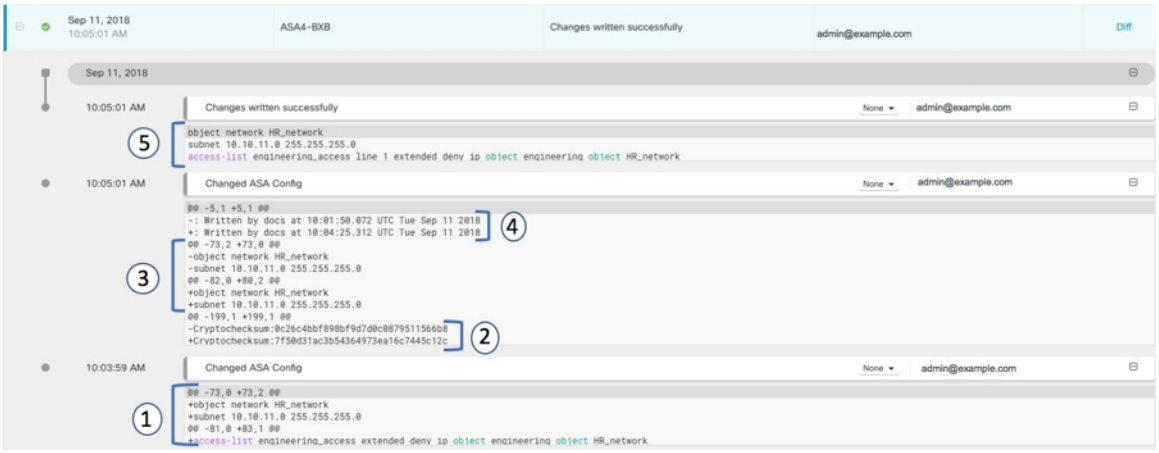
Change log entries after deploying to an ASA

Provides information about interpreting change log entries created after deploying configuration changes to a Secure Firewall ASA, including how Security Cloud Control records completed deployments and tracks device updates.

A checkmark on the header indicates that the change log is complete. The change log displays the most recent entries first followed by the older entries below in a chronological order. You can sort these entries.

Click the Diff link in the change log entry row to view a side-by-side comparison of the changes in the context of the running configuration file.

The explanations for the different changes are shown below.



Number in illustration	Explanation
1	This is the change that admin@example.com made at 10:03:59 AM on September 11, 2018. **1.** The "HR_network" object was added. **2.** The initial network address (10.10.11.0) and subnet mask (255.255.255.0) were added to the HR_network object. **3.** A rule was added to the "engineering_access" network policy denying addresses in the "engineering" network from reaching the "HR_network"
2	The checksum of the running configuration file was recalculated by the ASA and changed. The old value was *removed* and the new value was *added*.
3	The ASA moves the object to a different location in the running configuration file than where Security Cloud Control placed it. **Note** You don't always see this kind of an entry.
4	The record of the last time the running configuration file was updated. The old timestamp is removed and the new timestamp is added. This change was made by the ASA.
5	These are the commands sent by Security Cloud Control to the ASA to make the configuration changes.

Change log entries after reading changes from an ASA

Explains how change log entries capture out-of-band changes detected on a Secure Firewall ASA, including accepted, reviewed, or rejected changes and the resulting conflict details in Security Cloud Control.

A change log entry after reading changes from an ASA is a record that

- captures out-of-band changes detected on a Secure Firewall ASA device
- includes accepted, reviewed, or rejected changes with resulting conflict details

- records the time when the configuration conflict was detected.

Change log entry process and status messages

When Security Cloud Control detects a change on an ASA that it manages, it opens a change log entry and records the time when the configuration conflict was detected. You see this change log entry when Security Cloud Control detects a conflict:



If you accept the changes, or review and accept the changes, that change is added to the change log entry and the entry is completed.



This entry shows the Conflict Detected change and the deletion of a rule that prevents addresses in the engineering network from reaching the HR_network. The change log entry also shows a change with the message *Successfully imported out-of-band changes.* If the admin chooses to reject the out-of-band change, the change log will display the message *Successfully rejected out-of-band changes on the device* along with what was rejected. Out-of-band changes refers to the changes made to the ASA device directly without using Security Cloud Control.

View change log differences

Configure a side-by-side comparison view to examine added, modified, deleted, and message entries for device configuration changes in the change log.

View change log differences to analyze configuration changes made to devices by examining before and after states of the running configuration file.

Change log differences provide a detailed comparison between the original and modified configuration files, helping you understand what changes were made to device configurations. The side-by-side view highlights additions, modifications, and deletions in the running configuration.

Procedure

1. Click **Diff** in the change log.

   A side-by-side comparison of the changes in the running configuration file of the device opens.

   The **Original Configuration** column shows the running configuration file before a change was written to the ASA device. The **Modified Configuration** column shows the running configuration file after the change was written.

2. Follow the lines across from the left to the right column to see the changes.

In the comparison view, you can see additions such as the *HR_network* object and the access rule preventing addresses in the *engineering* network to reach addresses in the *HR_network* network. The **Original Configuration** column highlights rows that provide reference points for understanding the changes in the **Modified Configuration** column.



3. Click **Previous** and **Next** to move through the changes in the file.

You can view and analyze the configuration differences between the original and modified device configurations, understanding exactly what changes were made during the configuration update process.

Change request management

Explains how change request management enables linking business justifications to change log events through third-party ticketing systems.

Change request management is a functionality that

- enables the linking of a **Change Request** and its business justification to a **Change Log** event
- opens the **Change Request** in a third-party ticketing system, and
- allows creation of a **Change Request** in Security Cloud Control and associates it with change log events.

Change request management usage

Use **Change Request Management** to create a **Change Request** in Security Cloud Control and associate it with change log events. You can search for this change request by **Name** within the change log.

> **Note**
>
> In Security Cloud Control, **Change Request Tracking** and **Change Request Management** refer to the same functionality.

Enable change request management

Configure change request tracking to monitor and manage configuration changes across your organization.

Enable change request tracking to provide visibility and control over configuration changes made by all users in your organization.

Enabling change request tracking affects all users of your organization.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Enable the **Change Request Tracking** toggle button. 

   When enabled, the **Change Request** menu appears at the bottom-left corner and the **Change Request** drop-down list is available in the **Change Log** page.

Change request tracking is now enabled for your organization. The Change Request menu is available at the bottom-left corner, and the Change Request drop-down list appears in the Change Log page.

Create a change request

Configure a change request to track and manage device configuration changes in your organization.

Create a change request to organize and track configuration changes that will be made to devices in your network, ensuring proper documentation and oversight of modifications.

Change requests provide a structured way to group related configuration changes and maintain an audit trail of modifications. Once created, all subsequent changes will be associated with the active change request until it is cleared or disabled.

Procedure

1. In Security Cloud Control, click the **Create Change Request** (**+**) icon in the **Change Request** menu at the bottom-left corner.
2. Enter a **Name** and **Description**.

   Ensure that the **Name** corresponds to a **Change Request** name that your organization intends to use, and that the **Description** describes the purpose of the change.

> **Note**
>
> You cannot modify the name of a **Change Request** after you create it.

3. Click **Save**.

> **Note**
>
> When a **Change Request** is saved, Security Cloud Control associates all the new changes with the corresponding **Change Request** name. This association continues until you either disable change requests or clear the change request details from the menu.

The change request is created and becomes the active change request. All subsequent configuration changes will be associated with this change request until you disable change request management or clear the change request details.

Associate a change request with a change log event

Configure the association between a change request and a change log event to track configuration changes.

Associate change requests with change log events to maintain an audit trail and track the reasons for configuration changes.

Use this procedure when you need to link a change request to a specific change log event to document the authorization and rationale for configuration changes.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
3. Expand the change log to view the events you want to associate with a **Change Request**.
4. Click the drop-down list adjacent to the corresponding change log entry.

> **Note**
>
> The latest change requests are displayed at the top of the change request list.

5. Select a change request and click **Select**.

The change request is now associated with the change log event, creating a traceable link between the authorization and the configuration change.

Search for change log events with change requests

Configure search parameters to find change log events that are associated with specific change requests in the system.

This task helps you locate specific change log events by searching for associated change request names, allowing you to track changes and their corresponding documentation.

Use this procedure when you need to find change log events that are linked to particular change requests for auditing, tracking, or analysis purposes.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
3. In the change log search field, enter the name of a change request to find the associated change log events.

   Security Cloud Control highlights the change log events that are exact matches.

The system displays change log events that match your search criteria, with exact matches highlighted for easy identification.

Search for a change request

Configure a search to locate change requests by name or keywords in the change request system.

Enable users to quickly locate existing change requests by searching through names and descriptions using partial matches.

Use this search functionality when you need to find specific change requests among multiple entries in the system.

Procedure

1. In Security Cloud Control, click the **Create Change Request** (**+**) icon in the **Change Request** menu at the bottom-left corner.
2. Enter the name of the **Change Request** or a relevant keyword in the search field. As you enter a value, the results that partially match your input, appear in both the **Name** and **Description** fields.

The system displays change requests that match your search criteria in both the name and description fields, allowing you to locate the desired change request quickly.

Filter change requests

Configure filters to search and view specific change requests in the Change Log table.

Filter change requests to quickly locate and review specific configuration changes or events in your security environment.

Use the filter functionality in the Change Log to narrow down the list of change requests based on specific criteria. This helps you efficiently review and manage configuration changes across your devices.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
3. Click the filter icon to view all the options.

4. In the search field, enter the name of a **Change Request**.

   As you enter a value, the results that partially match your entry appear.

5. Select a change request by checking the corresponding check box.

   The matches appear in the **Change Log** table. Security Cloud Control highlights the change log events that are exact matches.

The Change Log table displays only the filtered change requests that match your search criteria, with exact matches highlighted for easy identification.

Clear the change request toolbar

Configure the change request toolbar to avoid automatic association of change log events with an existing change request.

Clear the change request toolbar to prevent change log events from being automatically associated with an existing change request.

When you need to avoid automatic association of change log events with an existing change request, clear the information in the change request toolbar.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. Click the **Create Change Request** (**+**) icon in the **Change Request** menu at the bottom-left corner.
3. Click **Clear**.

   The **Change Request** menu now displays **None**.

The change request toolbar is cleared and displays **None**, ensuring that change log events will not be automatically associated with any existing change request.

Clear a change request associated with a change log event

Configure the disassociation of change requests from change log events to remove unwanted connections between these items.

This task allows you to remove the association between a change request and a change log event when the connection is no longer needed or was created in error.

Use this procedure when you need to disassociate change requests from change log events in the Change Log interface. This helps maintain accurate tracking and organization of changes.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
3. Expand the **Change Log** to view the events that you want to disassociate from **Change Requests**.
4. Click the drop-down list adjacent to the corresponding change log entry.
5. Click **Clear**.

The change request is successfully disassociated from the selected change log event, and the connection between them is removed.

Delete a change request

Configure the deletion of a change request to remove it from the change request list while preserving it in the change log.

Delete a change request to remove it from the active change request list when it is no longer needed.

Deleting a **Change Request** removes it from the change request list, but not from the **Change Log**.

Procedure

1. Click the **Create Change Request** (**+**) icon in the **Change Request** menu at the bottom-left corner.
2. Select the change request and click the bin icon to delete it.
3. Click the check mark to confirm.

The change request is removed from the change request list but remains available in the change log for historical reference.

Disable change request management

Configure your account to disable Change Request Management or Change Request Tracking features.

This task disables Change Request Management functionality for your account when it is no longer needed or desired.

Disabling **Change Request Management** or **Change Request Tracking** affects all users of your account.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Administration** > **General Settings**.
3. Disable the **Change Request Tracking** toggle button.

Change Request Management and Change Request Tracking features are disabled for all users in your account.

Manage change requests and associate change log events

Configure change request management to track changes made to firewall devices and associate them with external tickets or change requests.

This task helps you track changes made to firewall devices and associate them with change requests to resolve tickets maintained in external systems. You can create change requests, associate change log events with them, and search for events related to specific change requests.

These use cases assume that you have enabled Change Request Management. You can use change request management in various scenarios to maintain audit trails and associate firewall changes with external ticketing systems.

Procedure

1. Track changes made to the firewall device to resolve a ticket maintained in an external system.

   This use case describes a scenario where you want to make changes to a firewall device to resolve a ticket maintained in an external system and want to associate the change log events resulting from these firewall changes to a change request.

a. Create a change request on page 1043.

b. Use the ticket name or number from the external system as the name of the change request and add the justification for the change and other relevant information in the **Description** field.

c. Ensure that the new change request is visible in the change request toolbar.

d. Make the changes to the firewall device.

e. In the navigation pane, click **Change Log** and find the change log events that are associated with your new change request.

f. Clear the change request toolbar on page 1046 to avoid automatic association of change log events with an existing change request.

2. Manually update individual change log events after changes are made to the firewall device.

   This use case describes a scenario where you have made changes to a firewall device to resolve a ticket that is maintained in an external system, but forgot to use the Change Request Management feature to associate change requests with the change log events. You want to update the change log events with the ticket number.

   a. Create a change request on page 1043: Use the ticket name or number from the external system as the name of the change request. Use the **Description** field to add the justification for the change and other relevant information.

   b. In the navigation pane, click **Change Log** and search for the change log events that are associated with the changes.

   c. Associate a change request with a change log event on page 1044.

   d. Clear the change request toolbar on page 1046 to avoid automatic association of change log events with an existing change request.

3. Search for change log events associated with a change request.

   This use case describes a scenario where, you want to find out what change log events were recorded in the change log because of the work done to resolve a ticket maintained in an external system.

   a. In the navigation pane, click **Change Log.**

   b. Search for change log events that are associated with change requests using one of these methods:

      - In the **Change Log** search field, enter the exact name of the change request to find change log events associated with that change request. Security Cloud Control highlights change log events that are exact matches.
      - Filter change requests on page 1045 to find the change log events.

   c. View each change log to find the highlighted change log events showing the associated change request.

You have successfully managed change requests and associated change log events with external tickets. The change log now contains trackable events linked to your change requests, providing an audit trail for firewall modifications.

Export the change log

Configure the export of all or selected change log data to a CSV file so you can filter, sort, and retain change records for reporting or analysis.

Export change log data to a comma-separated value (.CSV) file to enable filtering, sorting, and analysis of change records outside of the system.

You can export all or a subset of the Security Cloud Control change log to a comma-separated value (.CSV) file so that you can filter and sort the information, as required.

To export the change log to a .CSV file, follow this procedure:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
3. Find the changes you want to export by doing one of the following tasks:
   - Use the filter ( ) and the search field to find what you want to export. For example, filter by device to see only the changes for your selected device or devices.
   - Clear all the filters and search criteria in the change log. This allows you to export the entire change log.

> **Note**
>
> Security Cloud Control retains 1 year of change log data. It is recommended to filter the change log contents and download the results to a .CSV file rather than downloading the entire change log history for a year.

4. Click the export icon at the top right corner of the page.
5. Save the .CSV file to your local file system, with a descriptive name.

The change log data is exported to a CSV file on your local system, allowing you to perform additional filtering, sorting, and analysis as needed.

Differences between change log capacity in Security Cloud Control and size of an exported change log

Explains the differences between the change log information that Security Cloud Control stores in its database and the information included in an exported change log.

Change log capacity differences are data storage variations that

- distinguish between the complete change log information stored in Security Cloud Control's database and the subset of information included in exported files
- result from different storage requirements for database operations versus export functionality, and
- affect file sizes when users export change log data.

Change log storage structure

For every change log, Security Cloud Control stores two copies of the device's configuration–the *starting* configuration and either the *ending* configuration in the case of a closed change log or the *current* configuration in the case of an open change log. This allows Security Cloud Control to display configuration differences side by side. In addition, Security Cloud Control tracks and stores every step (*change event*) with the username that made the change, the time the change was made, and other details.

However, when you export the change log, the export does not include the two complete copies of the configuration. It only includes the *change events*, which makes the export file much smaller than the change log that Security Cloud Control stores.

Security Cloud Control stores change log information for a year. This includes two copies of the configuration.

Monitoring Jobs in Security Cloud Control

Explains how to monitor bulk operations in Security Cloud Control, review job progress and device-level results, search or filter jobs by action, user, or status, and reinitiate or cancel bulk actions.

Jobs monitoring in Security Cloud Control is a management interface that

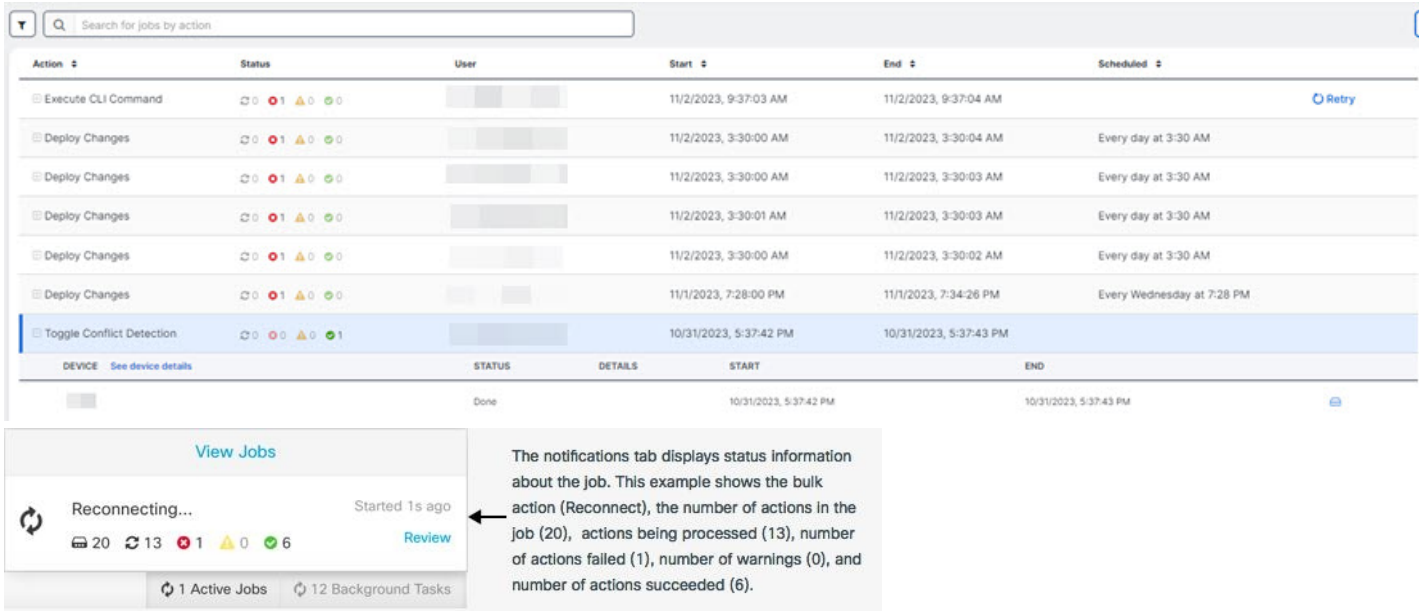
- provides an overview of the progress of bulk operations, such as reconnecting multiple devices, reading configurations from multiple devices, or upgrading multiple devices simultaneously
- uses color-coded rows along with the status of individual actions, indicating if they have succeeded or failed, and
- displays results for each of the devices affected by the bulk operation when a row is expanded.

Job access methods

You can reach the **Jobs** page in two different ways:

- In the **Notifications** tab, when there is a new Job notification, click the **Review** link. You will be redirected to the **Jobs** page and see the specific job represented by the notification.
- In the left pane, click **Events & Logs** > **Events heading** > **Jobs**. This table shows a complete list of the bulk actions performed in Security Cloud Control.

One row in the table represents a single bulk operation. This one bulk operation may have been, for example, an attempt to reconnect 20 devices. Expanding a row in the **Jobs** page displays the results for each of the devices affected by the bulk operation.



When you're on the **Jobs** page, you can filter and search by different actions, the users who performed them, and the action status.

Reinitiate a bulk action

Configure a bulk action retry to address failed actions in a previously executed bulk operation.

This task allows you to retry failed actions within a bulk operation without re-running the entire job.

After reviewing the **Jobs** page, if you find that one or more actions in a bulk action have failed, you can retry the bulk action after making the necessary corrections. Note that Security Cloud Control will re-run the job only for the failed actions.

Procedure

1. In the **Jobs** page, select the row that indicates a failed action.
2. Click the **Retry** (↻) icon.

The system retries only the failed actions from the original bulk operation, and the job status updates accordingly.

Cancel a bulk action

Configure the cancellation of bulk actions that are currently in progress on multiple devices.

Cancel bulk actions that are currently in progress when you need to stop ongoing operations on multiple devices that may be taking longer than expected or are no longer needed.

You can cancel the bulk actions that are currently in progress on multiple devices. For example, if you have tried to reconnect four managed devices, and three of them have successfully reconnected, but the fourth device is still neither connected nor disconnected, you can cancel the bulk action.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Events & Logs** > **Events heading** > **Jobs**.
3. Identify the running bulk action and click the **Cancel** link on the right side.

> **Note**
>
> If any part of the bulk action is successful, it cannot be undone. Any ongoing action will be cancelled.

The bulk action is cancelled, stopping any ongoing operations while preserving any successfully completed portions of the action.

Monitor workflows in Security Cloud Control

Explains how to monitor Security Cloud Control workflows, troubleshoot failed device or connector tasks, export workflow details for TAC analysis, and copy stack traces for unresolved errors.

Workflow monitoring is a Security Cloud Control capability that

- tracks every process that Security Cloud Control runs when communicating with devices, Secure Device Connector (SDC), or Secure Event Connector (SEC), and when applying ruleset changes to devices,
- creates an entry in the workflow table for every step and displays its outcome, and
- contains information pertaining only to the action performed by Security Cloud Control and not the device it is interacting with.

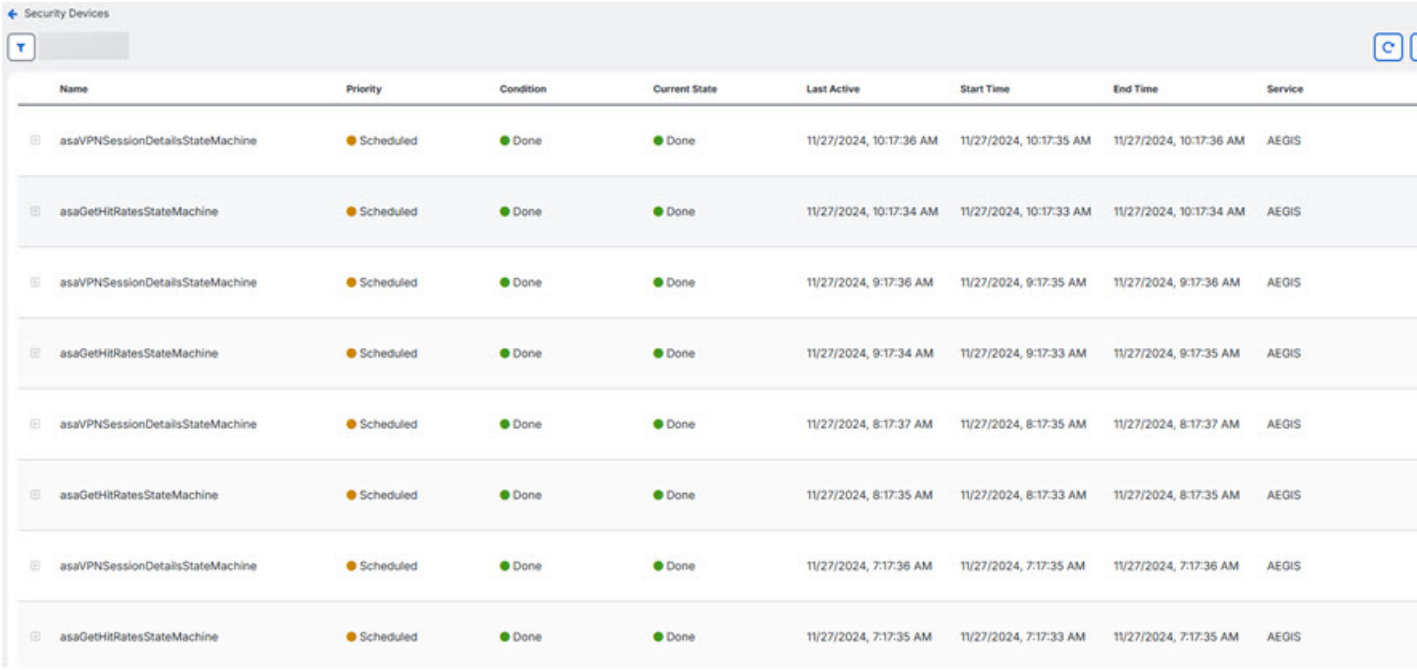
Workflow error reporting and troubleshooting

Security Cloud Control reports an error when it fails to perform a task on a device. Navigate to the **Workflows** page to see the step where the error occurred, for more details.

This page also helps you determine and troubleshoot errors or share information with TAC, when required.

To navigate to the **Workflows** page, in the left pane, click **Security Devices** and, click the **Devices** tab. Click the appropriate device type tab to locate the device and select the device you want. Under the **Devices and Actions** in the right pane, click **Workflows**.

Figure 40: Workflows page with entries in the workflow table



Export device workflows:

- You can download the complete workflow information to a JSON file and provide it when the TAC team asks for further analysis. To export the workflow information, select the corresponding device and, navigate to its **Workflows** page and click the export ( ) icon appearing at the top-right corner.

Copy stack trace:

- If you have an error you cannot resolve and you approach TAC, they may ask you for a copy of the stack trace. To collect the stack trace for the error, click the **Stack Trace** link and click **Copy Stacktrace** to copy the stacks appearing on the screen, to a clipboard.

60 Smart Licensing Dashboard

Topics:

- Smart licensing dashboard
- View smart licensing dashboard

This concept explains how the Smart Licensing Dashboard provides centralized management, real-time insights, and efficient planning for license usage and compliance for Secure Firewall ASAs and Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

The Smart Licensing Dashboard provides centralized management, real-time insights, and efficient planning for license usage and compliance for Secure Firewall ASAs and Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

Smart licensing dashboard

Explains how the Smart Licensing Dashboard provides centralized management, real-time insights, and efficient planning for license usage and compliance for Secure Firewall ASAs and Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

A Smart Licensing Dashboard is a management interface that

- provides visibility into the license usage and compliance status of Secure Firewall ASAs and Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices
- enables comprehensive license tracking and compliance monitoring, and
- displays details for all smart accounts, virtual accounts, and licenses associated with your current tenant.

Smart licensing dashboard benefits

The Smart Licensing Dashboard provides these benefits:

- **Comprehensive License Visibility:** You can see which smart account and virtual account your licenses originate from, providing clear traceability of license sources.
- **Detailed License Consumption Tracking:** You can see how many licenses you are consuming along with availability, usage, and expiration dates for each license type.
- **Compliance Monitoring:** You can view the compliance status of each license, which helps ensure that you remain within your licensed entitlements and avoid out-of-compliance issues.

> **Note**
>
> - Smart licenses are managed using smart accounts. Each smart account can have multiple virtual accounts. As a smart account owner, you can move licenses between these virtual accounts.
> - This dashboard displays the details of all the smart accounts, virtual accounts, and licenses associated only with your current tenant.

View smart licensing dashboard

Configure the Smart Licensing Dashboard to view detailed information about your licenses and compliance status of your Secure Firewall ASAs and Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

View detailed information about your licenses and compliance status of your devices on the Smart Licensing Dashboard.

The **Smart Licensing Dashboard** displays detailed information about your licenses. The dashboard shows the compliance status (**In compliance**, **Out of compliance**, or **Unknown**), the number of licenses purchased, and the number currently in use, along with the count of active licenses within your tenant. It also displays the type of licenses associated with onboarded devices (**Term**, **Unlicensed**, or **Perpetual**) as well as the start and expiration dates for each term license.

Note

- Firepower chassis devices: Licensing for chassis devices is managed on the chassis, not on the ASA.
- Multi-context devices in a non-admin context: Licensing for multi-context devices is managed in the admin context, not in a non-admin context.

For these devices, the dashboard displays the licensing status and compliance status as **Unknown** and excludes them from the **In this tenant** count.

Procedure

1. Choose **Insights & Reports** > **Reports & Analytics** > **Smart Licensing Dashboard**.

   The table provides details about the information displayed on the page.

Column name	Description
Virtual account name	Name of the virtual account.
Compliance status	Compliance status of the virtual account.

2. Click the virtual account name to view its details.

   The table provides details about the information displayed on the page.

Column name	Description
License name	Name of the smart license.
Type	Type of license associated with the devices onboarded to your tenant: **Term**, **Unlicensed**, or **Perpetual**.
Purchased	Number of smart licenses that you purchased.
In use	Number of smart licenses that are currently in use.
In this tenant	Number of smart licenses being used in the selected tenant.
Available	Number of smart licenses that are currently available for use.
Dates	Start and expiration dates for term licenses.
Compliance status	Compliance status–**In compliance**, **Out of compliance**, or **Unknown**.

   Use the search fields in this page to filter by license name, status, or type.

3. Click the download button to export the table to a CSV file.

You can view detailed licensing information including compliance status, license types, purchased and available licenses, and export the data to a CSV file for further analysis.

Part XVI

Troubleshoot

Topics:

- Troubleshooting
- FAQ and support

61 Troubleshooting

Topics:

- Troubleshoot a Secure Firewall ASA device
- Troubleshoot a secure device connector
- Secure event connector troubleshooting
- Troubleshoot Security Cloud Control
- Device connectivity states

This chapter details how to troubleshoot errors that may occur when working with various components in Security Cloud Control Firewall Management.

Troubleshoot a Secure Firewall ASA device

Explains how to troubleshoot common device issues including connectivity problems, configuration errors, synchronization failures, and deployment challenges to ensure proper device functionality.

ASA fails to reconnect to Security Cloud Control after reboot

Describes a connection issue where ASA devices fail to reconnect to Security Cloud Control after a reboot due to cipher suite incompatibility.

An ASA reconnection failure is a connectivity issue that

- occurs when an ASA device fails to reconnect to Security Cloud Control after a reboot
- happens because the ASA has fallen back to using an OpenSSL cipher suite that is not supported by Security Cloud Control's Secure Device Connector (SDC), and
- requires troubleshooting to test for the cipher suite issue and apply remediation steps.

Symptoms

- ASA reboots and Security Cloud Control and the ASA fail to reconnect. Security Cloud Control displays the message, "Failed to reconnect."
- When attempting to onboard an ASA, Security Cloud Control displays the message: *Certificate could not be retrieved for <ASA_IP_Address>*.

Disable ASA client-side certificate authentication for onboarding

Configure ASA to disable client-side certificate authentication to resolve onboarding issues with Security Cloud Control.

Disable client-side certificate authentication on ASA to enable successful onboarding to Security Cloud Control.

Environment: ASA is configured with client-side certificate authentication.

Solution: Disable client-side certificate authentication.

Details: ASAs support credential-based authentication as well as client-side certificate authentication. Security Cloud Control cannot connect to ASAs that use client-side certificate authentication. Before onboarding your ASA to Security Cloud Control, make sure it does not have client-certificate authentication enabled by using this procedure:

Procedure

1. Open a terminal window and connect to the ASA using SSH.
2. Enter global configuration mode.
3. At the hostname (config)# prompt, enter this command:

   no ssl certificate-authentication interface*interface-name***port 443**

   The interface name is the name of the interface Security Cloud Control connects to.

Client-side certificate authentication is disabled on the ASA, allowing successful onboarding to Security Cloud Control.

Determine the OpenSSL cipher suite used by your ASA

Verify the OpenSSL cipher suite being used by your ASA to ensure compatibility with the SDC.

This task helps you identify whether the OpenSSL cipher suite on your ASA is compatible with the Secure Device Connector (SDC).

Use this procedure to identify the OpenSSL cipher suite being used by your ASA. If the cipher suite named in the command output is not in the list of supported cipher suites, the SDC doesn't support that cipher suite and you will need to update the cipher suites on your ASA.

Procedure

1. Open a console window on a computer that can reach the SDC.
2. Connect to your SDC using SSH. You can log in as a regular user such as Security Cloud Control or SDC or some other user you created. You don't need to be logged in as root.

   Tip

   To find your SDC IP address:

   a. Open Security Cloud Control.

   b. From the user menu, select Secure Device Connectors.

   c. Click the SDC displayed in the table. The IP address of the SDC is displayed in the details pane for the device.

3. At the command prompt enter: **openssl s_client -showcerts -connect** *ASA_IP_Address*:**443**
4. Look for these lines in the command output.

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

   In this example, the cipher suite being used by the ASA is `DES-CB3-SHA`.

The command output displays the OpenSSL cipher suite being used by your ASA, allowing you to verify its compatibility with the SDC.

Cipher suites supported by Security Cloud Control's Secure Device Connector

Lists the cipher suites supported by Security Cloud Control's Secure Device Connector for secure communications.

Security Cloud Control's Secure Device Connector uses node.js which only accepts the latest and most secure ciphers. As a result, Security Cloud Control's SDC only supports this list of ciphers:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

If the cipher suite you use on your ASA is not in this list, SDC does not support it and you will need to Update your ASA's cipher suite on page 394.

Update your ASA's cipher suite

Configure TLS cipher suites on an ASA device to enhance security by specifying supported encryption protocols.

Update the TLS cipher suites on your ASA to ensure secure communication by configuring specific encryption protocols that meet your security requirements.

You need to modify the TLS cipher suite configuration when strengthening the security posture of your ASA device or when compliance requirements mandate specific encryption standards.

Procedure

1. Connect to the ASA using SSH.
2. Once connected to the ASA, elevate your privileges to global configuration mode.

   Your prompt should look like this: asaname(config)#
3. At the prompt, enter a command similar to this:

   Example

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256
 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA256"
```

   Note

   The cipher suites this command configures your ASA to support are contained between quotes and after the word custom. In this command, the cipher suites specified begin with `ECDHE-RSA-AES128-GCM-SHA256` and end with `DHE-RSA-AES256-SHA256`. When you enter the command on your ASA, remove any cipher suites you know your ASA will not support.
4. After you submit the command, enter write memory at the prompt to save the local configuration.

   Example

```
asaname(config)#write memory
```

The ASA is now configured with the specified TLS cipher suites, and the configuration has been saved to memory.

Troubleshoot ASA using CLI commands

Provides important commands to troubleshoot the ASA and test basic connectivity using the CLI interface.

This section discusses some of the important commands you may want to use to troubleshoot the ASA and test basic connectivity. See CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide to learn about other troubleshooting scenarios and CLI commands. In the 'System Administration' section, navigate to the 'Testing and Troubleshooting' chapter.

You can use the Security Cloud Control CLI interface available for each ASA device to execute these commands.

See ASA command line interface on page 303 to learn about how to use the CLI interface in Security Cloud Control.

NAT policy settings

Some of the important commands to determine the NAT settings are as follows:

- To determine NAT policy statistics, use **show NAT**.
- To determine the NAT pools, including the addresses and ports allocated, and how many times they were allocated, use **show NAT pool**.

For more commands related to NAT, see CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, and navigate to the 'Network Address Translation (NAT)' chapter.

Test basic connectivity: pinging addresses

You can ping the ASA device using the **ping <IP address>** command using the ASA CLI interface.

Display the routing table

Use the **show route** command to view the entries in the routing table.

ciscoasa# show route

Example output for a routing table of an ASA:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF

Gateway of last resort is 192.168.0.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, management
C 10.0.0.0 255.0.0.0 is directly connected, Outside
L 10.10.10.1 255.255.255.255 is directly connected, Outside
C 192.168.0.0 255.255.255.0 is directly connected, management
L 192.168.0.118 255.255.255.255 is directly connected, management
```

Monitor switch ports

- **show interface**

  Displays interface statistics.

- **show interface IP brief**

  Displays interface IP addresses and status.

- **show ARP**

Shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds.

Example output of ARP entries:

```
management 10.10.32.129 0050.568a.977b 0
management 10.10.32.136 0050.568a.5387 21
LANFAIL 20.20.21.1 0050.568a.4d70 96
outsi 10.10.16.6 0050.568a.e6d3 3881
outsi 10.10.16.1 0050.568a.977b 5551
```

Troubleshoot missing information on the RA VPN monitoring page

Configure the outside interface for Webvpn to resolve missing information on the remote access VPN monitoring page.

This task resolves issues where information is missing on the RA VPN monitoring page by enabling the outside interface for Webvpn on an ASA device.

This issue may occur if the outside interface is not enabled for Webvpn when configuring remote access VPN on an ASA device.

Procedure

1. In the left pane, click **Security Devices** and then click the **ASA** tab.
2. Select the RA VPN headend ASA device that is having issues.
3. In the **Management** pane on the right, click **Configuration**.
4. Click **Edit** and search for 'webvpn'.
5. Press **Enter** and add **enable** *interface_name*.

   Here, the interface_name is the name of the outside interface to which users connect when making the remote access VPN connection. Although this is normally the outside (internet-facing) interface, choose whichever interface is between the device and the end-users you are supporting with this connection profile.

   #### Example

   For example:

   ```
   webvpn
   enable outside
   ```

6. Click **Save**.
7. Preview and deploy the configuration to the device.

The outside interface is now enabled for Webvpn, and information should appear correctly on the RA VPN monitoring page.

ASA real-time logging

Describes a logging feature that displays recent logged data from ASA devices with specific data limits and configuration changes.

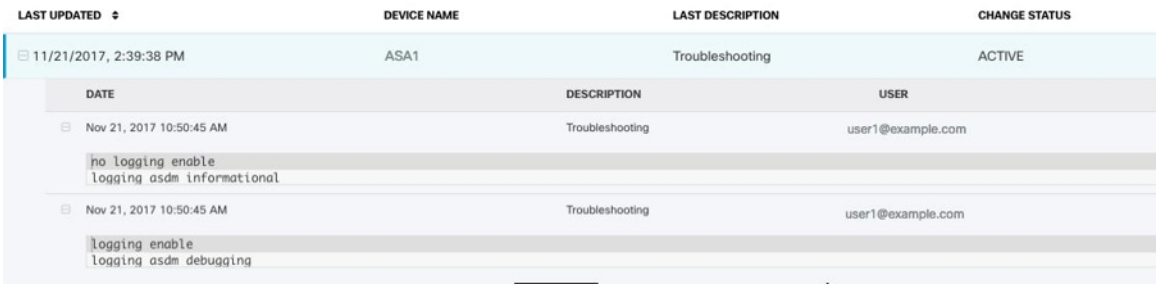
ASA real-time logging is a logging feature that

- displays the last 20 seconds of logged data or the last 10 KB of logged data, whichever limit is reached first
- temporarily changes the existing logging configuration to request debugging-level data during data retrieval, and
- returns the logging configuration to its previous state after data collection completes.

Real-time logging operation

When Security Cloud Control retrieves the real-time data, it reviews the existing logging configuration on your ASDM, changes it to request debugging-level data, and then returns the logging configuration to your configuration. The logging Security Cloud Control displays reflects any logging filters you may have set in ASDM.

You can see the commands that Security Cloud Control sends to perform logging by reviewing the change log. The first entry (on the bottom) indicates that Security Cloud Control "turned on" logging with the logging enable command and changed the ASDM logging level to debugging. The second entry (on the top) shows that the logging configuration was returned to its previous state. Logging was "turned off" with the no logging enable command and the ASDM logging level was returned to informational.



View ASA real-time logs

Configure real-time log viewing for ASA devices to monitor and troubleshoot network activity.

View real-time logging data from ASA devices to monitor network activity and troubleshoot issues as they occur.

Real-time logs provide immediate visibility into ASA device activity, allowing you to monitor traffic, security events, and system status in real time. You can apply filters to refine the log data and focus on specific events or criteria.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the appropriate device type tab and select the device for which you want to view real-time data.
3. Click **Troubleshoot** Troubleshoot .
4. (Optional) Before clicking View Real-time Log, you can define a filter in the left pane to refine the results of your logging search.
5. Click **View Real-time Log**.

   Security Cloud Control retrieves the real-time logging data based on your filtering criteria and displays it.
6. To see an additional 20 seconds of logged data or the last 10 KB of logged data, click **View Real-Time Log** again.

Real-time logging data is displayed based on your filtering criteria, allowing you to monitor ASA device activity and troubleshoot issues as they occur.

ASA packet tracer

Explains a network troubleshooting tool that sends synthetic packets to evaluate routing configuration, NAT rules, and policy configurations on ASA devices.

ASA Packet Tracer is a network troubleshooting tool that

- sends synthetic packets into the network to evaluate how existing routing configuration, NAT rules, and policy configurations affect that packet
- works on live, online ASA devices either physical or virtual, and
- evaluates packets based on the saved configuration on the ASA, not staged changes.

Troubleshooting use cases

Use this tool to troubleshoot these kinds of issues:

- Users report that they cannot reach resources that they should be able to.
- Users report that they can reach resources they should not be able to.
- Test a policy to determine if it works as you expect.

Packet tracer can be used on a live, online, ASA device either physical or virtual. Packet Tracer does not work on ASA model devices. Packet tracer evaluates packets based on the saved configuration on the ASA. Staged changes on Security Cloud Control are not evaluated by packet tracer.

We consider it a best-practice to run packet tracer on an ASA that is in the synced state. Though packet tracer will run if the device is not synced, you could encounter some unexpected results. For example, if you deleted a rule in the staged configuration on Security Cloud Control, and this same rule was triggered on the ASA during packet tracing, Security Cloud Control won't be able to show you the result of the packet's interaction with that rule.

As packet tracer sends the packet through the routing configuration, NAT rules, and security policies of your ASA, it displays the packet's status at each step. If the packet is allowed by the policy it receives a green checkmark. If a packet is denied and dropped, Security Cloud Control displays a red X.

Packet tracer also displays a real time log of the result of the packet trace. In the example below, you can see where a rule denied a tcp packet.



Troubleshoot an ASA device security policy

Configure packet tracer to troubleshoot security policies on ASA devices by virtually sending packets through the device.

Use packet tracer to troubleshoot security policies by simulating packet flow through your ASA device to identify potential connectivity issues and policy violations.

Packet tracer allows you to test how packets traverse through your ASA device's security policies without actually sending real traffic. This helps diagnose connection problems and verify policy configurations.

Procedure

1. In the left pane, click **Security Devices**.
2. Select your ASA and view troubleshooting details in the **Troubleshooting** pane.

3. In the pane, select the interface and packet type you want to send virtually through your ASA.
4. (Optional) If you want to trace a packet where the security group tag value is embedded in the Layer 2 CMD header (Trustsec), check SGT number and enter the security group tag number, 0-65535.
5. Specify the source and destination. You can specify IPv4 or IPv6 addresses, fully-qualified domain names (FQDN), or security group names or tags if you use Cisco Trustsec. For the source address, you can also specify a username in the format Domain\username.
6. Specify other protocol characteristics:
   - ICMP-Enter the ICMP type, ICMP code (0-255), and optionally, the ICMP identifier.
   - TCP/UDP/SCTP-Enter the source and destination ports by selecting them from the list or entering a value in the port combo box.
   - IP-Enter the protocol number, 0-255.
7. Click **Run Packet Tracer**.
8. Continue with Analyze packet tracer results on page 401.

The packet tracer results display the path the simulated packet takes through your ASA device, showing which security policies are applied and whether the packet is allowed or denied.

Troubleshoot an access rule

Configure packet tracer troubleshooting for a specific access rule in your network policy to analyze traffic flow and rule behavior.

Use packet tracer troubleshooting to analyze how traffic flows through your network policy and identify issues with specific access rules.

When you need to verify that an access rule is working correctly or diagnose traffic flow issues, the packet tracer tool allows you to simulate network traffic and see how it interacts with your configured rules.

Procedure

---

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Policies** > **ASA** > **Access Policies**.
3. Select a policy that is associated with your ASA.
4. Select a rule in the network policy to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane.

   In the values panel of the troubleshoot page, many of the fields are pre-populated with the attributes of the rule you chose.
5. Enter information in the remaining required fields.

   Once you have completed all the required fields the Run Packet Tracer button becomes active.
6. Click **Run Packet Tracer.**
7. Continue with Analyze packet tracer results on page 401.

The packet tracer runs and provides analysis results for the selected access rule, showing how traffic flows through your network policy.

Troubleshoot a NAT rule

Configure troubleshooting for a NAT rule by selecting the rule and running packet tracer analysis to identify configuration issues.

This task enables you to diagnose and resolve issues with NAT rules by using packet tracer functionality to analyze traffic flow and rule behavior.

Use this procedure when you need to troubleshoot NAT rule configuration issues on ASA devices. The troubleshooting process helps identify why traffic is not being translated as expected.

Procedure

1. In the left pane, click **Security Devices** and then click the **ASA** tab.
2. Select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.
3. Select the rule from the NAT Rules table that you want to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. Notice that in the values panel of the Troubleshoot page, many of the fields are pre-populated with the attributes of the rule you chose.
4. Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer becomes active.
5. Click **Run Packet Tracer.**
6. Continue with Analyze packet tracer results on page 401.

The packet tracer runs and provides analysis results that help identify NAT rule issues and traffic flow problems.

Troubleshoot a twice NAT rule

Configure packet tracer troubleshooting for a Twice NAT rule to analyze source and destination packet translations.

Troubleshoot a Twice NAT rule to identify and resolve issues with packet translation by running packet tracer analysis on source or destination packet flows.

Use this procedure when you need to analyze NAT rule behavior and identify potential issues with packet translation in your ASA configuration. For bi-directional Twice NAT rules, you can troubleshoot either source packet translation or destination packet translation.

Procedure

1. In left pane, click **Security Devices**.
2. Click the **ASA** tab, select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.
3. Select the rule from the NAT Rules table that you want to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. For a bi-directional Twice NAT rule, this opens a dropdown where you choose to troubleshoot the source packet translation or the destination packet translation.
4. Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer becomes active.
5. Click **Run Packet Tracer**.

The packet tracer analysis runs and displays the results, showing how the NAT rule processes the specified packet flow and identifying any issues with the translation.

Analyze packet tracer results

Verify packet tracer results to understand why packets are dropped or allowed and take appropriate action based on the findings.

This task helps you understand the reasons behind packet tracer results, whether packets are dropped or allowed, and enables you to make necessary configuration changes to achieve desired access results.

Packet tracer provides detailed information about packet processing decisions. When you run packet tracer, you receive results that show whether packets are allowed or denied, along with the specific rules and policies that influenced these decisions.

Procedure

1. Expand a row in the packet trace table to view detailed rule or logging information.

   Whether the packet is dropped or allowed, you can learn why by expanding a row in the packet trace table and reading the rule or logging information related to that action.

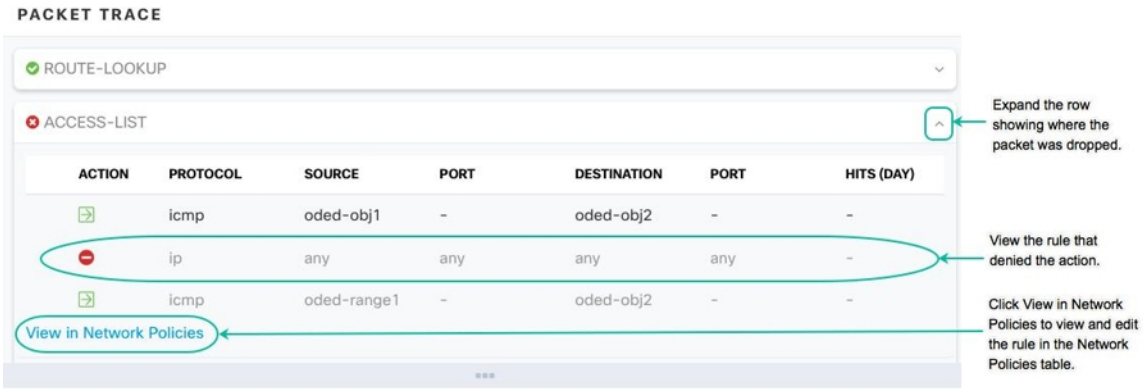
   The expanded view shows the specific access list policy and rules that affected the packet, such as a rule to deny an IP packet coming from any source and going to any destination.

2. If the action is not what you want, click the **View in Network Policies** link to edit the rule.

   This link allows you to immediately access and modify the relevant network policy rule.

3. Deploy the configuration change to the ASA after editing the rule.
4. Re-run packet tracer to verify that you get the expected access results.
5. Review the ASA real-time logging on page 396 from the ASA.

   Along with the packet tracer results, Security Cloud Control displays the real-time logging from the ASA.



You have successfully analyzed the packet tracer results and understand the reasons for packet processing decisions. Any necessary rule modifications have been deployed and verified through re-running packet tracer.

Confirming ASA running configuration size

Verify the size of your ASA running configuration file by copying it to flash memory and checking its file size.

Confirm the size of your running configuration file to ensure it meets system requirements or limitations.

Use this procedure to determine if your ASA running configuration exceeds the 4.5 MB size limit by copying it to flash storage and examining the file properties.

Before you begin

Follow these steps to confirm the size of your running configuration file:

Procedure

1. Access the ASA's command line interface in one of these ways:
   - Open a terminal window and log into your ASA using SSH. Elevate your privilege to "privileged EXEC" mode so you see the prompt with `hostname#`.
   - If you managed to get your ASA onboarded, open the **Security Devices** page, select the device you want to connect to, and click **>_ Command Line Interface** button in the Device Actions pane.
2. At the prompt type `copy running-config flash`
3. When prompted for the Source filename, don't type anything and press <Enter>
4. When prompted for the destination filename, enter a name for the output file. After ASA copies the running configuration the file you specified, it returns you to the privileged EXEC prompt.
5. At the prompt, type `show flash`
6. Look in the length column. If your file is over 4718592 bytes, it is larger than 4.5 MB.

   Here is a sample set of commands and output:

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

You have successfully determined the size of your ASA running configuration file. Files over 4718592 bytes exceed the 4.5 MB limit.

Limitation: large ASA running configuration files

Outlines limitations and solutions when ASA running configuration files exceed size thresholds in Security Cloud Control.

Configuration file size limitations

Be aware that Security Cloud Control cannot predictably manage ASA devices with running configuration files that are 4.5 MB or larger, contain approximately 22,000 lines or more, or have too many access-list entries for a single access group.

This limitation affects ASA onboarding and ongoing management in Security Cloud Control. You may see behavior such as the ASA failing to onboard, Security Cloud Control not displaying all of the configuration defined in the ASA's running configuration file, or Security Cloud Control failing to write to the change log.

When you onboard an ASA to Security Cloud Control, Security Cloud Control stores a copy of the ASA's running configuration file in its database. Large configuration files exceed database storage and processing capabilities.

To confirm the size of your running configuration file, see Confirming ASA running configuration size on page 402. Contact your Cisco account team for help safely reducing the size of your configuration file without disrupting your security policies.

Troubleshoot a secure device connector

Provides troubleshooting guidance for Secure Device Connector issues, including unreachable SDCs, inactive status, IP address changes, device connectivity problems, system time errors, version issues, and AWS certificate or connection errors.

Use these topics to troubleshoot an on-premises Secure Device Connector (SDC).

If none of these scenarios match yours, open a case with Cisco Technical Assistance Center.

Resolve unreachable SDC status

Configure your Secure Device Connector (SDC) to restore communication with Security Cloud Control when the SDC is in unreachable state.

Restore communication between an unreachable SDC and your tenant to enable device management capabilities.

An SDC is in the state "Unreachable" if it has failed to respond to two heartbeat requests from Security Cloud Control in a row. If your SDC is unreachable, your tenant will not be able to communicate with any of the devices you have onboarded.

Security Cloud Control indicates that an SDC is unreachable in these ways:

- You see the message, "Some Secure Device Connectors (SDC) are unreachable. You will not be able to communicate with devices associated with these SDCs." on the Security Cloud Control home page.
- The SDC's status in the Services page is "Unreachable."

Before you begin

Follow these steps to resolve the unreachable SDC issue:

Procedure

1. Check that the SDC virtual machine is running and can reach a Security Cloud Control IP address in your region.

   See Allow inbound access for direct cloud connectivity on page 94.

2. Attempt to reconnect Security Cloud Control and the SDC by requesting a heartbeat manually.

   If the SDC responds to a heartbeat request, it will return to "Active" status. To request a heartbeat manually:

   a. In the left pane, choose **Administration** > **Integrations** > **Secure Connectors**.

   b. Click the SDC that is unreachable.

   c. In the Actions pane, click **Request Heartbeat**.

   d. Click **Reconnect**.

3. If the SDC does not return to the Active status after manually attempting to reconnect it to your tenant, follow the instructions in Troubleshoot SDC status not active on Security Cloud Control after deployment on page 1071.

The SDC returns to "Active" status and communication is restored between the SDC and your tenant, enabling device management capabilities.

Troubleshoot SDC status not active on Security Cloud Control after deployment

Configure troubleshooting steps when SDC status does not become active on Security Cloud Control after deployment.

Resolve connectivity issues when SDC status does not show as active on Security Cloud Control within the expected timeframe.

If Security Cloud Control does not indicate that your SDC is active in about 10 minutes after deployment, connect to the SDC VM using SSH using the `Security Cloud Control` user and password you created when you deployed the SDC.

Procedure

1. In Security Cloud Control, click on the SDC that isn't showing as active, and click **Request Heartbeat**.
2. Ensure that the container is running using the command:

   ```
   docker ps
   ```

3. View the SDC logs and check for errors using the command:

   ```
   SDC show logs
   ```

4. Restart the container using the command:

   ```
   SDC restart
   ```

The SDC status should become active on Security Cloud Control after completing these troubleshooting steps.

Update the changed IP address of the SDC in Security Cloud Control

Configure Security Cloud Control to reflect the updated IP address of an SDC by requesting a heartbeat and refreshing the browser.

This task ensures that Security Cloud Control displays the correct, updated IP address for your Secure Device Connector (SDC) when the IP address has changed.

When an SDC's IP address changes, Security Cloud Control may not immediately reflect this change. You need to manually request a heartbeat to update the displayed information.

Procedure

1. In Security Cloud Control, click on the SDC that isn't showing as active.
2. In the sidebar, click **Request Heartbeat**.
3. Make sure the container is running using the command: `docker ps`
4. View the SDC logs and check for errors using the command `SDC show logs`
5. Restart the container using the command `SDC restart`
6. Refresh your browser to view the updated IP address of the SDC.

The updated IP address of the SDC is now reflected in Security Cloud Control and the SDC shows as active.

Troubleshoot device connectivity with the SDC

Configure a troubleshooting test to verify connectivity from Security Cloud Control through the Secure Device Connector (SDC) to your device.

Test connectivity from Security Cloud Control, through the Secure Device Connector (SDC) to your device.

You may want to test this connectivity if your device fails to onboard or if you want to determine, before on-boarding, if Security Cloud Control can reach your device.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**, and click the **Secure Connectors** tab.
3. Select the SDC.
4. In the **Troubleshooting** pane on the right, click **Device Connectivity**.
5. Enter a valid IP address or FQDN and port number of the device you are attempting to troubleshoot, or attempting to connect to, and click **Go**.

   Security Cloud Control performs the following verifications:

   a) **DNS Resolution** - If you provide a FQDN instead of an IP address, this verifies the SDC can resolve the domain name and acquires the IP address.
   b) **Connection Test** - Verifies the device is reachable.
   c) **TLS Support** - Detects the TLS versions and ciphers that both the device and the SDC support.

      - **Unsupported Cipher** - If there are no TLS version that are supported by both the device and the SDC, Security Cloud Control also tests for TLS versions and ciphers that are supported by the device, but not the SDC.

   d) SSL Certificate - The troubleshoot provides certificate information.
6. If you continue to have issues onboarding or connecting to the device, contact Security Cloud Control support.

The connectivity test completes and displays the results of DNS resolution, connection test, TLS support, and SSL certificate verification between Security Cloud Control and your device through the SDC.

Resolve intermittent or no connectivity with SDC

Configure disk space management for Secure Device Connector to resolve connectivity issues caused by insufficient storage.

This task resolves intermittent or no connectivity issues with Secure Device Connector (SDC) that occur when disk space usage exceeds 80 percent.

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies only to an on-premise SDC and if you are still using CentOS.

Symptom: Intermittent or no connectivity with SDC.

Diagnosis: This problem may occur if the disk space is almost full (above 80%).

Before you begin

Follow these steps to check the disk space usage before performing this task:

1. Open the console for your Secure Device Connector (SDC) VM.
2. Log in with the username **cdo**.

3. Enter the password created during the initial login.
4. First, check the amount of free disk space by typing `df -h` to confirm that there is no free disk space available.

   You can confirm that the disk space was consumed by the Docker. The normal disk usage is expected to be under 2 Gigabytes.
5. To see the disk usage of the **Docker** folder, execute `sudo du -h /var/lib/docker | sort -h`.

   You can see the disk space usage of the **Docker** folder.

Follow these steps to configure Docker log rotation if the disk space usage of the Docker folder is almost full:

Procedure

1. Execute `sudo vi /etc/docker/daemon.json`.
2. Insert the following lines to the file.

   Example

   ```
   {
   "log-driver": "json-file",
   "log-opts": {"max-size": "100m", "max-file": "5" }
   }
   ```

   - Max-size: To force a log rotation once the current file reaches the maximum size.
   - Max-file: To delete excess rotated log files when the maximum limit it reached.
3. Press **ESC** and then type `:wq!` to write the changes and close the file.

   Note

   You can execute `sudo cat /etc/docker/daemon.json` to verify the changes made to the file.
4. Execute `sudo systemctl restart docker` to restart the docker file.

   It will take a few minutes for the changes to take effect. You can execute `sudo du -h /var/lib/docker | sort -h` to see the updated disk usage of the docker folder.
5. Execute `df -h` to verify that the free disk size has increased.
6. Before your SDC status can change from Unreachable to Active, go to the **Secure Connectors** tab which you can navigate to from **Administration** > **Integrations** > **Firewall Management Center** and click **Request Reconnect** from the Actions menu.

The SDC status changes from Unreachable to Active, and connectivity issues are resolved.

Container privilege escalation vulnerability affecting secure device connector: cisco-sa-20190215-runc

Provides information about a high-severity vulnerability in Docker that impacts all Security Cloud Control customers using Secure Device Connector.

The Cisco Product Security Incident Response Team (PSIRT) published the security advisory **cisco-sa-20190215-runc** which describes a high-severity vulnerability in Docker. Read the entire PSIRT team advisory for a full explanation of the vulnerability.

This vulnerability impacts all Security Cloud Control customers:

- Customers using Security Cloud Control's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the Security Cloud Control Operations Team.
- Customers using an SDC deployed on-premise need to upgrade their SDC host to use the latest Docker version. They can do so by using these instructions:
  - Update a Security Cloud Control-Standard SDC Host on page 403
  - Recommendation: migrate SDC from CentOS to ubuntu on page 404
  - Bug tracking on page 405

Update a Security Cloud Control-Standard SDC Host

Configure Docker service updates on your Secure Device Connector host to maintain compatibility with Firewall in Security Cloud Control.

This task updates Docker on your SDC host to ensure continued compatibility and security patching for your Secure Device Connector deployment.

- The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

  For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

  This procedure applies if you are still using CentOS.
- Use these instructions if you deployed an SDC using the Security Cloud Control image.

Procedure

1. Connect to your SDC host using SSH or the hypervisor console.
2. Check the version of your Docker service by running this command:

```
docker version
```

3. If you are running one of the latest virtual machines (VMs) you should see output like this:

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

It's possible you may see an older version here.

4. Run these commands to update Docker and restart the service:

```
> sudo yum update docker-ce
> sudo service docker restart
```

> **Note**
>
> There will be a brief connectivity outage between Security Cloud Control and your devices while the docker service restarts.

5. Run the docker version command again.

   You should see this output:

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

You have successfully upgraded to the latest, patched version of Docker on your SDC host.

Recommendation: migrate SDC from CentOS to ubuntu

Outlines migration guidelines for Secure Device Connector hosts from unsupported CentOS 7 to Ubuntu virtual machines.

Migrate all SDCs from CentOS 7 to an Ubuntu virtual machine. The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

- If you have created your own SDC host you will need to follow the instructions to update based on how you installed Docker. If you used CentOS, yum and Docker-ce (the community edition) the preceding procedure will work.
- If you have installed Docker-ee (the enterprise edtion) or used an alternate method to install Docker, the fixed versions of Docker may be different. You can check the Docker page to determine the correct versions to install: Docker Security Update and Container Security Best Practices.

This procedure applies if you are still using CentOS.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

Bug tracking

Provides information about tracking bugs related to security vulnerabilities and advisory updates.

This reference provides details on how Cisco tracks and updates vulnerability information through bug tracking systems, enabling users to access the latest information on security advisories and associated fixes.

Cisco is continuing to evaluate this vulnerability and will update the advisory as additional information becomes available. After the advisory is marked Final, you can refer to the associated Cisco bug for further details:

CSCvo33929-CVE-2019-5736: runc container breakout

Invalid system time

Configure the system time on your Secure Device Connector to resolve synchronization issues and enable successful migration to the new communication method.

This task corrects system time synchronization issues that prevent successful migration of your Secure Device Connector (SDC) to the new communication method. Proper time synchronization ensures your SDC can communicate effectively with Security Cloud Control.

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies if you are still using CentOS.

- Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

  Note

  If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

- Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because your SDC system time was 15 minutes ahead or behind the AWS system time.

Before you begin

Follow these steps below to correct the system time issue. Once this problem is resolved, you can proceed with the migration.

Procedure

1. Login to your SDC VM throught the VM terminal or by making an SSH connection.
2. At the prompt, enter **sudo SDC-onboard setup** and authenticate.
3. You are now going to respond to the SDC setup questions as if you are were setting up the SDC for the first time. Re-enter all the same passwords and network information as you had before, except take special note of the NTP server address:
   a) Reset the root and Security Cloud Control user passwords with the same passowrds you used to setup the SDC.
   b) When prompted, enter **y** to re-configure the network.
   c) Enter the value for IP address/CIDR as you had before.
   d) Enter the value for the network gateway as you had before.
   e) Enter the value for the DNS Server as you had before.
   f) When prompted for the NTP server, be sure to provide a valid NTP server address, such as **time.AWS.com**.
   g) Review the values you provided and enter **y** if they are correct.
4. Validate that your time server is reachable and synchronized with your SDC by entering **date** at the prompt. The UTC date and time are displayed and you can compare it to your SDC time.

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can complete your SDC migration to the new communication method.

Your SDC system time is now synchronized with the AWS system time, resolving the time synchronization issue that prevented successful migration. The Security Cloud Control operations team can now complete your SDC migration to the new communication method.

Upgrade SDC version lower than 202311****

Upgrade your Secure Device Connector (SDC) to version 202311**** or later to enable communication migration by CDO operations team.

This task upgrades your SDC to the required version so that Security Cloud Control operations can successfully migrate your SDC to the new communication method.

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies if you are still using CentOS.

- Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

  Note

  If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

- Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because your tenant is running a version lower than 202311****.
- The current version of your SDC is listed on the Secure Connectors page by navigating from the Security Cloud Control navigation menu, **Administration** > **Integrations** > **Secure Connectors**. After selecting your SDC, its version number is found in the **Details** pane on the right of the screen.

Follow these steps to upgrade the SDC version to 202311**** or later:

Procedure

---

1. Log in to the SDC VM and authenticate.
2. At the prompt, enter **sudo su - SDC** and authenticate.
3. At the prompt, enter **crontab -r**.

   If you receive the message **no crontab for SDC** you can ignore it and move to the next step.

4. At the prompt, enter **./toolkit/toolkit.sh upgrade**.

   Security Cloud Control will determine if you need an upgrade and upgrade the toolkit. Ensure that no errors were reported in the console.

5. Verify the new version of the SDC:
   a) Log in to Security Cloud Control.
   b) Navigate to the Secure Connectors page by navigating from the Security Cloud Control menu bar, **Tools & Services** > **Secure Connectors**.
   c) Select your SDC and click **Request Heartbeat** in the **Actions** pane.
   d) Validate that the SDC version is 202311**** or later.

   Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can run the migration process again.

Your SDC is upgraded to version 202311**** or later, enabling the Security Cloud Control operations team to successfully migrate your SDC to the new communication method.

Certificate or connection errors with AWS servers

Configure firewall rules and IP addresses to resolve connection issues preventing SDC migration to the new communication method.

This task resolves connection issues that prevent the migration of your Secure Device Connector (SDC) to Security Cloud Control's new communication method.

Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

> **Note**
>
> If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because they experienced a connection issue.

Follow these steps to correct the connection issue:

Procedure

---

1. Create firewall rules that allow outbound proxy connections, on port 443, to the domains in your region:
   - Production tenants in the Australia region:
     - cognito-identity.ap-southeast-2.amazonaws.com
     - cognito-idp.ap-southeast-2.amazonaws.com
     - sns.ap-southeast-2.amazonaws.com
     - sqs.ap-southeast-2.amazonaws.com
   - Production tenants in the India region:
     - cognito-identity.ap-south-1.amazonaws.com
     - cognito-idp.ap-south-1.amazonaws.com

- sns.ap-south-1.amazonaws.com
- sqs.ap-south-1.amazonaws.com

- Production tenants in the US region:
  - cognito-identity.US-west-2.amazonaws.com
  - cognito-idp.US-west-2.amazonaws.com
  - sns.US-west-2.amazonaws.com
  - sqs.US-west-2.amazonaws.com

- Production tenants in the EU region:
  - cognito-identity.EU-central-1.amazonaws.com
  - cognito-idp.EU-central-1.amazonaws.com
  - sns.EU-central-1.amazonaws.com
  - sqs.EU-central-1.amazonaws.com

- Production tenants in the APJ region:
  - cognito-identity.ap-northeast-1.amazonaws.com
  - cognito-idp.ap-northeast-1.amazonaws.com
  - sqs.ap-northeast-1.amazonaws.com
  - sns.ap-northeast-1.amazonaws.com

2. You can determine the full list of IP addresses you need to add to your firewall's "allow list" by using one of the commands below.

> **Note**
>
> The commands below are for users that have **jq** installed. The IP addresses will be displayed in a single list.

- Production tenants in the US region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
 | select( (.service == "AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- Production tenants in the EU region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
 | select( (.service == "AMAZON" ) and .region == "eu-central-1") |
.ip_prefix'
```

- Production tenants in the APJ region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
 | select( (.service == "AMAZON" ) and .region == "ap-northeast-1") |
.ip_prefix'
```

Note

If you don't have **jq** installed, you can use this shortened version of the command:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can complete your SDC migration to the new communication method.

Once the connection issue is resolved, the Security Cloud Control operations team can proceed with the migration of your SDC to the new communication method.

Secure event connector troubleshooting

Describes how to troubleshoot Secure Event Connector issues, including onboarding and registration failures, NSEL data flows, event logging problems, inactive SEC status, missing events, host removal, and health checks.

Secure Event Connector troubleshooting is a diagnostic process that involves identifying and resolving issues with Secure Event Connector functionality and performance.

Support resources

If none of the scenarios described match your issue, open a case with Cisco Technical Assistance Center (TAC) for further assistance.

Troubleshoot SEC onboarding failures

Provides troubleshooting scenarios for a variety of symptoms associated with Secure Event Connector (SEC) onboarding and operational failures.

The troubleshooting scenarios describe a variety of symptoms associated with Secure Event Connector (SEC) onboarding and operational failures. Use this topic to identify and resolve the issue impacting your deployment.

SEC onboarding failed

Symptom: SEC onboarding failed.

Repair: Remove and onboard the SEC again.

> **Tip**
>
> Always use the copy link to copy the bootstrap data when on-boarding an SEC.

> **Note**
>
> If this procedure does not correct the problem, gather the troubleshooting logs and contact your Managed Service Provider or the Cisco Technical Assistance Center.

Downloading, decoding, or extracting bootstrap data failed

Messages:

- **[Error] Downloading the bootstrap package failed.**
- **[Error] Extracting the bootstrap package failed.**
- **[Error] Max retries exceeded for bootstrap download.**

Diagnosis: Decoding bootstrap data failed.

Repair:

- Wait briefly and retry the bootstrap operation.
- Add a new SEC in the UI and attempt to bootstrap the new one instead.

Adequate CPU and memory not available

Message: [Error] Secure Event Connector minimum system requirements not met.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4
 cpus and 8 GB ram required, exiting.
```

Diagnosis: Adequate CPU and memory not available.

Repair: Increase the resources of your virtual machine to meet the minimum required specifications.

Host already has an SEC

Message: [Error] This host currently has an SEC enabled for the same tenant. Please remove the SEC before trying to bootstrap it again.

Diagnosis: SEC already running.

Repair: Ensure that there is no existing operational SEC in your environment. If one is present but not operational, remove it and then re-bootstrap the SEC.

> **Note**
>
> Ensure that you are removing an active SEC. This error message can occur when a bootstrap progresses far enough for the system to assume normal operation but fails to fully complete. As a result, it is possible that a bootstrap error is causing this situation.
>
> To confirm, run the command **sdc eventing healthcheck**. If the health check reports all green, it indicates that the SEC is active and functioning properly. In such a case, removing it would disrupt an operational SEC.

Contact Security Cloud Control Support

If none of the scenarios described above match your issue, open a case with Cisco Technical Assistance Center.

Troubleshoot secure event connector registration failure

Configure troubleshooting procedures to resolve Cisco Secure Event Connector registration failures to the cloud eventing service.

This task helps you identify and resolve common issues that prevent the Secure Event Connector (SEC) from successfully registering to the eventing cloud service.

Symptom: Registration of Cisco Secure Event Connector to cloud eventing service fails.

Diagnosis: These are the most common reasons that the SEC fails to register to the eventing cloud service.

- **The SEC is unable to reach the Eventing cloud service from SEC**

  Repair: Ensure that Internet is accessible on port 443 and DNS is configured correctly.

- **Registration failure due to invalid or expired one-time-password in SEC bootstrapdata**

  Repair:

Procedure

1. SSH to the host VM as the admin user, typically `cdo`.
2. Switch to the `sdc` user usingthe command: `sudo su - sdc`.
3. View the connector log by running command `sdc eventing logs --type connector`.

   > **Note**
   >
   > If the registration has failed due to an invalid token, you see an error message in the log file similar to the example below:
   >
   > ```
   > context:(*contextImpl).handleFailed] registration - CE2001: Registration
   > failed - Failed to register the device because of invalid token. Retry with
   > a new valid token.
   > ```

4. Remove the SEC.

5. Add a new SEC in the UI and re-onboard.

The Secure Event Connector successfully registers to the cloud eventing service and registration failures are resolved.

Collect troubleshooting logs for secure event connector

Configure the Secure Event Connector troubleshooting command to collect logs, configurations, and system information into a compressed archive for diagnosing issues.

The troubleshooting command simplifies the diagnosis of issues by collecting logs, configurations, and limited system information into a single compressed archive.

If you already have a TAC case open, the compressed archive can also be sent directly to your TAC representative.

Before you begin

Follow these steps to collect troubleshooting logs for Secure Event Connector:

Procedure

---

1. SSH to your host using the admin account, typically `cdo`.
2. Switch to the SDC user using the command `sudo su - SDC`
3. Run the appropriate troubleshoot command based on whether you have a TAC case open.

If...	Then...
You do not have a TAC case open	Run the command to gather and compress the troubleshooting bundle: `SDC eventing troubleshoot`
You already have a TAC case open	Request an upload token from your TAC representative and use the command: `SDC eventing troubleshoot --case-number [your-TAC-case-number] --token [the-token-TAC-provided]`

4. If you prefer to retrieve the troubleshooting bundle manually, use SCP or SFTP.

   Locate the absolute path to the bundle provided in the last log entry after running the troubleshoot command. Then, use the following SCP command to download the bundle to your local machine:

```
scp -P [22 or whichever port you SSH on]
        cdo@your-vm-ip:/opt/cdo/.cdo/troubleshooting/cdo_[tenant-name-here]
        -troubleshooting-[timestamp-here].tar.gz
./sec-troubleshooting-bundle.tar.gz
```

> **Note**
>
> Replace `/opt/cdo/.cdo/troubleshooting/cdo_\[tenant-name-here\]-troubleshooting-\[timestamp-here\].tar.gz` with the actual path displayed in the log output.

If you want to decompress the archive to review the logs and system configurations, use the command: `tar xvf ./[sec-troubleshooting-bundle-filename].tar.gz`

The troubleshooting bundle is created as a compressed archive file containing logs, configurations, and system information ready for analysis or TAC submission.

Troubleshooting: SEC status is inactive in Security Cloud Control

Outlines troubleshooting steps when the Secure Event Connector status shows "Inactive" in the Security Cloud Control Secure Connectors page after onboarding.

The Secure Event Connector status shows "Inactive" in the Security Cloud Control Secure Connectors page after onboarding for one of these reasons:

- Heartbeat failed
- Connector registration failed

Heartbeat failed: Request SEC heartbeat and refresh Secure Connector page to see if the status changes to "Active", if not check if the Secure Device Connector registration failed.

Connector registration failed: Refer issue Troubleshooting SEC Registration Failure.

The SEC is online, but there are no events in Security Cloud Control Event Logging Page

Verify the Secure Event Connector configuration when the SEC shows as active but no events appear in the Event Logging page.

This task helps diagnose and resolve issues where the Secure Event Connector appears online in Security Cloud Control but events are not being received or displayed in the Event viewer.

Symptom: The Secure Event Connector shows "Active" in Security Cloud Control Secure Connectors page but you do not see events in Security Cloud Control Event viewer.

Solution or workaround:

Procedure

---

1. SSH to your host using the admin account, typically **cdo**.
2. Switch to the SDC user with the command **sudo su - SDC**.
3. Perform the following checks:
   - Check SEC connector log using the command **SDC eventing logs --type connector -n 100** and ensure the SEC registration was successful.

     If not, see Secure Event Connector Registration failure.

- Check SEC events log using the command **SDC eventing logs --type events -n 200** and ensure that the events are being processed.

  If not, contact Security Cloud Control support.

- Check the SEC supervisor log with **SDC eventing logs --type supervisor -n 100** and ensure the output is as shown below and all processes in **RUNNING** state.

  If not, contact Security Cloud Control support.

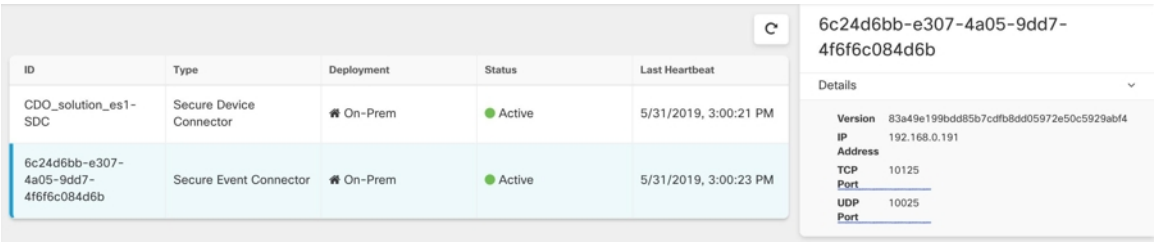
INFO success: estreamer-connector entered RUNNING state, process has stayed up for > than 1 seconds

INFO success: estreamer-plugin entered RUNNING state, process has stayed up for > than 1 seconds

INFO success: estreamer-rsyslog entered RUNNING state, process has stayed up for > than 1 seconds

- Ensure that the firewall rules on the on-premise SDC are not blocking the UDP and TCP ports shown for the SEC on the Secure Connectors page.

  See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging to determine what ports you need to open.



- If you have setup SDC manually using a CentOS 7 VM of your own and have the firewall configured to block incoming requests, you could execute the following commands to unblock the UDP and TCP ports:

firewall-cmd --zone=public --add-port=<udp_port>/UDP --permanent

firewall-cmd --zone=public --add-port=<tcp_port>/TCP --permanent

firewall-cmd --reload

- Using Linux network tools of your choice, check if packets are being received on these ports. If not receiving, re-check the FTD logging configuration.

If none of the above repairs work, raise a support ticket with Security Cloud Control support..

After performing these checks and resolving any identified issues, events should begin appearing in the Security Cloud Control Event viewer. If issues persist, contact support for further assistance.

Remove an SEC from your host

Configure the removal of a Secure Event Connector (SEC) container and its associated files from your Secure Device Connector (SDC) virtual machine.

Remove the SEC container along with its associated files from the Secure Device Connector (SDC) virtual machine to address issues such as Secure Event Connector registration failures or onboarding failures.

The Secure Event Connector (SEC) delete command removes the SEC container along with its associated files from the Secure Device Connector (SDC) virtual machine. This command is typically used to address issues such as Secure Event Connector registration failures or onboarding failures.

Follow these steps to remove an SEC from your host:

Procedure

1. SSH to your host using the admin account, typically `cdo`.
2. Switch to the SDC user with `sudo su - SDC`.
3. Run the command `SDC eventing delete`.

   If applicable, you will be prompted to select the tenant you wish to delete. Follow the on-screen prompts to confirm your selection and fully remove the SEC data from the virtual machine.

The SEC container and its associated files are removed from the SDC virtual machine, resolving registration or onboarding failures.

Use health check to learn the state of your secure event connector

Configure Health Check to monitor and verify the operational state of your Secure Event Connector (SEC).

Use the Health Check script to gather information about the state and operational status of your Secure Event Connector (SEC).

The Secure Event Connector (SEC) Health Check script provides information on the state of your SEC.

Before you begin

Follow these steps to run Health Check:

Procedure

1. SSH to your host using the admin account, typically `cdo`.
2. Switch to the SDC user using the command `sudo su - SDC`
3. Run the command `SDC eventing healthcheck` and, if applicable, select the tenant when prompted.

```
sdc@ci-sdc-4:~$ sdc eventing healthcheck
2025-05-06 16:36:20 [INFO] [ Manual Command ] eventin
2025-05-06 16:36:44 [INFO] Running SEC healthcheck fo


================================================

Running SEC health check for tenant CDO_blum-tenant
--

SEC cloud URL stage-api-sse.cisco.com is: Reachable
SEC Connector status: Eventing subscription not enabl
okSEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
SEC netflow collector is: Running
Skipping SEC test event due to earlier failures
SEC healthcheck failed, please review any errors abov
ok
================================================
```

Values of Health Check output:

- **SEC Cloud URL**: Displays the Security Cloud Control cloud URL and whether or not the SEC can reach Security Cloud Control.
- **SEC Connector**: Will show "Running" if the SEC connector has been onboarded correctly and has started.
- **SEC UDP syslog server**: Will show "Running" if the UDP syslog server is ready to send UDP events.
- **SEC TCP syslog server**: Will show "Running" if the TCP syslog server is ready to send TCP events.
- **SEC Connector status**: Will show Active if the SEC is running and onboarded to Security Cloud Control.
- **SEC Send sample event**: If at the end of the health check, all the status checks are "green," the tool sends a sample event. (If any of the processes are "Down," the tool skips sending the test event.) The sample event shows up in the Event Log as a policy named "SEC-health-check."

The Health Check script displays the operational status of your SEC components and sends a test event if all systems are running correctly.

Troubleshoot Security Cloud Control

Describes how to troubleshoot common issues including login failures, access and certificate problems, and object-related errors to resolve system connectivity and functionality problems.

Troubleshooting access and certificates

Describes common issues related to user access permissions and certificate problems, including authentication failures, expired certificates, and certificate validation errors that may prevent system connectivity.

Troubleshoot User Access with Security Cloud Control

Configure troubleshooting procedures to diagnose and remediate user access issues when users are denied access to resources they should have access to.

This task helps you diagnose and remediate problems when users are denied access to resources that they should have access to.

Consider the case of users being denied access to a resource that they should have access to. Here is an approach you can take to diagnose and remediate that problem.

Procedure

1. Users inform your security team that their access to a resource is blocked. Determine how that resource is typically reached. What is it's IP address? Do you reach it on a specific port? What protocol is used to send information to the resource?
2. In the left pane, click **Security Devices**.
3. Click the **ASA** tab and select the ASA and run packet tracer.

   See ASA Packet Tracer for more instructions.
4. Examine the packet trace table for rules that may have denied access to the resource.
5. After identifying the rule denying access, create a change request label in Security Cloud Control and enable it.

   See Change request management on page 1042. This will help you identify in Change Log policy changes you made to allow access to the resource.
6. Edit the rule from Security Cloud Control to correct the behavior.

   Your ASA is now out of sync with Security Cloud Control.
7. Deploy the changes to the ASA from the **Security Devices** page.

   Security Cloud Control traces packets through the configuration saved on the ASA not a configuration staged on Security Cloud Control. Be aware, you will also be deploying any other configuration changes staged on Security Cloud Control to your ASA.
8. Re-run packet tracer to determine if the policy change provides the desired results. Confirm that your users now have access to the resource.
9. Assuming your users now have access, clear the change request label in Security Cloud Control.

   This prevents unrelated activity from being associated with this fix.

> **Note**
>
> If the change you made doesn't fix the problem or creates some new problems and you want to return to your previous configuration, you can do restore the ASA Configuration.
>
> See Restoring ASA Configurations.

Users should now have access to the resource, and the change request label is cleared to prevent unrelated activity from being associated with this fix.

Resolve new fingerprint detected state

Configure device fingerprint acceptance to resolve the New Fingerprint Detected state and restore device connectivity.

This task resolves the New Fingerprint Detected state that occurs when a device's fingerprint has changed, typically due to certificate updates or device configuration changes.

When a device shows the New Fingerprint Detected state, it indicates that the device's security fingerprint has changed since the last connection. This commonly occurs after device maintenance, certificate renewals, or security updates. The device remains inaccessible until you review and accept the new fingerprint.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select the device in the **New Fingerprint Detected** state.
5. Click **Review Fingerprint** in the New Fingerprint Detected pane.
6. When prompted to review and accept the fingerprint:
   a. Click **Download Fingerprint** and review it.
   b. If you are satisfied with the fingerprint, click **Accept**. If you are not, click **Cancel**.
7. After you resolve the new fingerprint issue, the connectivity state of the device may show **Online** and the Configuration Status may show "Not Synced" or "Conflict Detected." Review Resolve Configuration Conflicts to review and resolve configuration differences between Security Cloud Control and the device.

The device fingerprint is accepted and the device state changes from New Fingerprint Detected to Online. The device is now accessible for management and configuration tasks.

SSL decryption issues

Describes SSL decryption problems that occur when applications use CERTIFICATE pinning techniques to prevent man-in-the-middle attacks.

SSL decryption issues are connectivity problems that

- occur when applications use SSL or CERTIFICATE Authority pinning techniques
- prevent decrypt re-sign from working for mobile apps while browsers continue to function normally, and

- result from hash validation failures when apps receive resigned certificates from Firepower Threat Defense devices.

SSL pinning behavior and identification

Some apps for smart phones and other devices use a technique called SSL (or CERTIFICATE Authority) pinning. The SSL pinning technique embeds the hash of the original SERVER CERTIFICATE inside the APP itself. As a result, when the APP receives the resigned CERTIFICATE from the Firepower Threat Defense device, the hash validation fails and the connection is aborted.

The primary symptom is that users cannot connect to the web site using the site's APP, but they can connect using the web browser, even when using the browser on the same device where the APP fails. For example, users cannot use the Facebook iOS or Android APP, but they can point Safari or Chrome at https://www.facebook.com and make a successful connection.

Because SSL pinning is specifically used to avoid man-in-the-middle attacks, there is no workaround. You must choose between the following options:

If a site works in a browser but not in an APP on the same device, you are almost certainly looking at an instance of SSL pinning. However, if you want to delve deeper, you can use connection events to identify SSL pinning in addition to the browser test.

There are two ways an APP might deal with hash validation failures:

- Group 1 apps, such as Facebook, send an SSL ALERT Message as soon as it receives the SH, CERT, SHD message from the SERVER. The ALERT is usually an "Unknown CA (48)" ALERT indicating SSL Pinning. A TCP Reset is sent following the ALERT message. You should see the following symptoms in the event details:
  - **SSL Flow Flags include ALERT_SEEN.**
  - **SSL Flow Flags do not include APP_DATA_C2S or APP_DATA_S2C.**
  - **SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.**
- Group 2 apps, such as Dropbox, do not send any alerts. Instead they wait until the handshake is DONE and then send a TCP Reset. You should see the following symptoms in the event:
  - **SSL Flow Flags do not include ALERT_SEEN, APP_DATA_C2S, or APP_DATA_S2C.**
  - **SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.**

Device connectivity states

Lists device connectivity states in Security Cloud Control and provides troubleshooting methods for offline devices, insufficient licenses, invalid credentials, onboarding errors, new certificates, and unregistered devices.

You can view the connectivity states of the devices onboarded in your Security Cloud Control tenant. This topic helps you understand the various connectivity states. On the **Security Devices** page, the **Connectivity** column displays the device connectivity states.

When the device connectivity state is 'Online' it means that the device is powered on and connected to Security Cloud Control. The other states described in the table below usually occur when the device is running into problems for various reasons. The table provides the method to recover from such problems. It may be that there is more than one problem causing the connection failure. When you attempt to reconnect, Security Cloud Control will prompt you to fix all of these problems first before performing the reconnect.

Device Connectivity State	Possible Reasons	Resolution
Online	Device is powered on and connected to Security Cloud Control.	NA
Offline	Device is powered down or lost network connectivity.	Check whether the device is offline.
Insufficient licenses	Device doesn't have sufficient licenses.	Troubleshoot Insufficient Licenses
Invalid credentials	Username and password combination used by Security Cloud Control to connect to the device is incorrect.	Troubleshoot Invalid Credentials
Onboarding	Device onboarding is initiated but is not complete.	Check you device's connectivity and ensure you complete the device registration.
Unknown	Device onboarding failed and Security Cloud Control cannot fetch the connectivity state of the device.	On the **Security Devices** page, select the device and choose **Check for Changes** from the right pane, to attempt fetching the latest configuration from the device.
Pending Setup	Device registration has failed.	Troubleshoot Onboarding a Device to the Cloud-delivered Firewall Management Center Using the CLI Registration Key
New Certificate Detected	Certificate on the device has changed. If the device uses a self-signed certificate, then this could have happened due to the device being power cycled.	Troubleshoot New Certificate Issues on page 1094
Device Unregistered	FDM-managed device has been unregistered from Cloud via FDM.	Troubleshoot device unregistered on page 1092
Onboarding Error	Security Cloud Control may have lost connectivity with the device when onboarding it.	Troubleshoot Onboarding Error

Troubleshoot device unregistered

Configure device registration to resolve unregistered device status in the cloud.

Re-register an unregistered FDM-managed device with the cloud to restore connectivity and management capabilities.

The FDM-managed device may have been unregistered from the cloud via Firewall Device Manager.

Before you begin

Perform these steps to register the device again on the cloud:

Procedure

1. In the **Security Devices** page, click the **Devices** tab.

2. Click the **FTD** tab and select the device in the "Device Unregistered" state, and see the error message on the right.
3. If the unregistered device was onboarded using the registration key, Security Cloud Control prompts you to generate a new registration key as the previously applied key has expired.
   a) Click the Refresh button to generate a new registration key and then click the Copy icon .
   b) Log into the Firewall Device Manager of the device you want to reregister with Security Cloud Control.
   c) Under **System Settings**, click **Cloud Services**.
   d) In the Security Cloud Control area, expand **Get Started**.
   e) In the **Registration Key** field, paste the registration key that you generated in Security Cloud Control.
   f) Click **Register** and then **Accept** the Cisco Disclosure. Firewall Device Manager sends the registration request to Security Cloud Control.
   g) Refresh the **Security Devices** page in Security Cloud Control until you see the device's connectivity state changes to "Read Error".
   h) Click **Read Configuration** for Security Cloud Control to read the configuration from the device.
4. If the unregistered device was onboarded using the serial number, Security Cloud Control prompts you to auto-enroll the device from Firewall Device Manager.
   a) Log into the Firewall Device Manager of the device you want to reregister with Security Cloud Control.
   b) Under **System Settings**, click **Cloud Services**.
   c) Select the **Auto-enroll with Tenancy from Security Cloud Control** option and click **Register**.
   d) Refresh the **Security Devices** page in Security Cloud Control until you see the device's connectivity state changes to "Read Error".
   e) Click **Read Configuration** for Security Cloud Control to read the configuration from the device.

The device is successfully re-registered with the cloud and the connectivity state shows "Read Error" indicating the device is ready for configuration reading.

Troubleshoot insufficient licenses

Configure device licensing when the device connectivity status shows "Insufficient License" by generating a new token and applying it to the device.

This task resolves licensing issues when devices show "Insufficient License" status by applying a new license token from Cisco Smart Software Manager.

If the device connectivity status shows "Insufficient License", try these preliminary steps first:

- Wait for some time until the device attains the license. Typically it takes some time for Cisco Smart Software Manager to apply a new license to the device.
- If the device status doesn't change, refresh the Security Cloud Control portal by signing out from Security Cloud Control and signing back to resolve any network communication glitch between license server and device.
- If the portal refresh doesn't change the device status, perform the following:

Procedure

---

1. Generate a new token from Cisco Smart Software Manager and copy it. You can watch the Generate Smart Licensing video for more information.
2. In the left pane, click **Security Devices**.
3. Click the **Devices** tab.
4. Click the appropriate device type tab and select the device with the **Insufficient License** state.
5. In the **Device Details** pane, click **Manage Licenses** appearing in **Insufficient Licenses**. The **Manage Licenses** window appears.

6. In the **Activate** field, paste the new token and click **Register Device**.

   Once the token is applied successfully to the device, its connectivity state turns to **Online**.

The device connectivity status changes from "Insufficient License" to "Online" once the new license token is successfully applied.

Troubleshoot invalid credentials

Configure device reconnection to resolve disconnection issues caused by invalid credentials.

This task helps you restore connectivity to devices that have disconnected due to authentication issues by updating their credentials.

Device disconnections often occur when credentials have been changed directly on the device but not updated in the management interface. This creates an authentication mismatch that prevents proper communication.

Before you begin

Follow these steps to resolve device disconnection due to invalid credentials:

Procedure

---

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab and select the device with the **Invalid Credentials** state.
4. In the **Device Details** pane, click **Reconnect** appearing in **Invalid Credentials**.

   Security Cloud Control attempts to reconnect with your device.

5. When prompted enter the new username and password for the device.
6. Click **Continue**.
7. After the device is online and ready to use, click **Close**.
8. It is likely that because Security Cloud Control attempted to use the wrong credentials to connect to the device, the username and password combination Security Cloud Control should use to connect to the device was changed directly on the device.

   You may now see that the device is "Online" but the configuration state is "Conflict Detected." Use Resolve Configuration Conflicts to review and resolve configuration differences between Security Cloud Control and the device.

The device reconnects successfully with updated credentials and appears as "Online" in the device inventory.

Troubleshoot New Certificate Issues

Resolve issues related to certificates when onboarding devices in Target file not found, including new certificate validation and common certificate error codes. Purpose: Ensure devices with valid certificates are successfully onboarded and synchronized with Target file not found.

Security Cloud Control requires devices to use valid, non-expired SHA-256 certificates with TLS 1.0 or higher. It accepts trusted self-signed certificates or certificates signed by a trusted CA with a complete chain. Certificate checking can be disabled only per ASA device, which reduces security. Common issues include expired certificates, certificates not yet valid, and incomplete chains. Troubleshooting uses openssl to verify certificates and errors. New self-signed certificates after upgrades must be manually accepted unless bulk reconnecting devices. Proper certificate management ensures secure connections.

Security Cloud Control 's Use of Certificates

Security Cloud Control checks the validity of certificates when connecting to devices. Specifically, Security Cloud Control requires that:

1. The device uses a TLS version equal to or greater than 1.0.
2. The certificate presented by the device is not expired, and its issuance date is in the past (i.e. it is already valid, not scheduled to become valid at a later date).
3. The certificate must be a SHA-256 certificate. SHA-1 certificates will not be accepted.
4. One of these conditions is true:
   - The device uses a self-signed certificate, and it is the same as the most recent one trusted by an authorized user.
   - The device uses a certificate signed by a trusted Certificate Authority (CA), and provides a certificate chain linking the presented leaf certificate to the relevant CA.

These are the ways Security Cloud Control uses certificates differently than browsers:

- In the case of self-signed certificates, Security Cloud Control overrides the domain name check, instead checking that the certificate exactly matches the one trusted by an authorized user during device onboarding or reconnection.
- Security Cloud Control does not yet support internal CAs. There is currently no way to check a certificate signed by an internal CA.

  It is possible to disable certificate checking for ASA devices on a per-device basis. When an ASA's certificate cannot be trusted by Security Cloud Control , you will have the option of disabling certificate checking for that device. If you have attempted to disable certificate checking for the device and you are still unable to onboard it, it is likely that the IP address and port you specified for the device is incorrect or unreachable. There is no way to disable certificate checking globally, or to disable certificate checking for a device with a supported certificate. There is no way to disable certificate checking for non-ASA devices.

  When you disable certificate checking for a device, Security Cloud Control will still use TLS to connect to the device, but it will not validate the certificate used to establish the connection. This means that a passive man-in-the-middle attacker will not be able to eavesdrop on the connection, but an active man-in-the-middle could intercept the connection by supplying Security Cloud Control with an invalid certificate.

Identifying Certificate Issues

There are several reasons that Security Cloud Control may not be able to onboard a device. When the UI shows a message that " Security Cloud Control cannot connect to the device using the certificate presented," there is a problem with the certificate. When the UI does not show this message, the problem is more likely related to connectivity problems (the device is unreachable) or other network errors.

To determine why Security Cloud Control rejects a given certificate, you can use the openssl command-line tool on the SDC host or another host that can reach the relevant device. Use the following command to create a file showing the certificates presented by the device:

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

This command will start an interactive session, so you will need to use Ctrl-c to exit after a couple of seconds.

You should now have a file containing output like the following:

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN =
```

```
*.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
   Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB

    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
```

```
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

The first thing to note in this output is the last line, where you see the **Verify return code** . If there is a certificate issue, the return code will be non-zero and there will be a description of the error.

Expand this list of certificate error code to see common errors and how to remediate them

0 X509_V_OK The operation was successful.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT The issuer certificate of an untrusted certificate could not be found.

3 X509_V_ERR_UNABLE_TO_GET_CRL The CRL of a certificate could not be found.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value. This is only meaningful for RSA keys.

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE The CRL signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value. Unused.

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY The public key in the certificate SubjectPublicKeyInfo could not be read.

7 X509_V_ERR_CERT_SIGNATURE_FAILURE The signature of the certificate is invalid.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE The signature of the certificate is invalid.

9 X509_V_ERR_CERT_NOT_YET_VALID The certificate is not yet valid: the notBefore date is after the current time. See Verify return code: 9 (certificate is not yet valid) below for more information.

10 X509_V_ERR_CERT_HAS_EXPIRED The certificate has expired; that is, the notAfter date is before the current time. See Verify return code: 10 (certificate has expired) below for more information.

11 X509_V_ERR_CRL_NOT_YET_VALID The CRL is not yet valid.

12 X509_V_ERR_CRL_HAS_EXPIRED The CRL has expired.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD The certificate notBefore field contains an invalid time.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD The certificate notAfter field contains an invalid time.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD The CRL lastUpdate field contains an invalid time.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD The CRL nextUpdate field contains an invalid time.

17 X509_V_ERR_OUT_OF_MEM An error occurred trying to allocate memory. This should never happen.

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN The certificate chain could be built up using the untrusted certificates but the root could not be found locally.

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE No signatures could be verified because the chain contains only one certificate and it is not self-signed. See "Verify return code: 21 (unable to verify the first certificate)" below for more information. Verify return code: 21 (unable to verify the first certificate) below for more information.

22 X509_V_ERR_CERT_CHAIN_TOO_LONG The certificate chain length is greater than the supplied maximum depth. Unused.

23 X509_V_ERR_CERT_REVOKED The certificate has been revoked.

24 X509_V_ERR_INVALID_CA A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.

25 X509_V_ERR_PATH_LENGTH_EXCEEDED The basicConstraints pathlength parameter has been exceeded.

26 X509_V_ERR_INVALID_PURPOSE The supplied certificate cannot be used for the specified purpose.

27 X509_V_ERR_CERT_UNTRUSTED The root CA is not marked as trusted for the specified purpose.

28 X509_V_ERR_CERT_REJECTED The root CA is marked to reject the specified purpose.

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the -issuer_checks option is set.

30 X509_V_ERR_AKID_SKID_MISMATCH The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the -issuer_checks option is set.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH The current candidate issuer certificate was rejected because its issuer name and serial number were present and did not match the authority key identifier of the current certificate. Only displayed when the -issuer_checks option is set.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.

50 X509_V_ERR_APPLICATION_VERIFICATION An application specific error. Unused.

Certificate Error Codes

Verify return code: 0 (ok) but Security Cloud Control returns certificate error

Once Security Cloud Control has the certificate, it attempts to connect to the URL of the device by making a GET call to "https://<device_ip>:<port>". If this does not work, Security Cloud Control will display a certificate error. If you find that the certificate is valid (openssl returns 0 ok) the problem may be that a different service is listening on the port you're trying to connect to. You can use the command:

```
 curl -k -u <username>:<password>
https://<device_id>:<device_port>/admin/exec/show%20version
```

to determine whether you are definitely talking to an ASA and check if HTTPS server running on the correct port on the ASA:

```
                    # show asp table socket

Protocol         Socket         State         Local Address             Foreign
 Address
SSL              00019b98         LISTEN        192.168.1.5:443
0.0.0.0:*
SSL              00029e18         LISTEN        192.168.2.5:443
0.0.0.0:*
TCP              00032208         LISTEN        192.168.1.5:22
0.0.0.0:*
```

Verify return code: 9 (certificate is not yet valid)

This error means that the issuance date of the certificate provided is in the future, so clients will not treat it as valid. This can be caused by a poorly-constructed certificate, or in the case of a self-signed certificate it can be cause by the device time being wrong when it generated the certificate.

You should see a line in the error including the notBefore date of the certificate:

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

From this error, you can determine when the certificate will become valid.

Remediation

The notBefore date of the certificate needs to be in the past. You can reissue the certificate with an earlier notBefore date. This issue can also arise when the time is not set correctly either on the client or issuing device.

Verify return code: 10 (certificate has expired)

This error means that at least one of the certificates provided has expired. You should see a line in the error including the notBefore date of the certificate:

```
 error 10 at 0 depth lookup:certificate has expired
```

The expiration date is located in the certificate body.

Remediation

If the certificate is truly expired, the only remediation is to get another certificate. If the certificate's expiration is still in the future, but openssl claims that it is expired, check the time and date on your computer. For instance, if a certificate is set to expire in the year 2020, but the date on your computer is in 2021, your computer will treat that certificate as expired.

Verify return code: 21 (unable to verify the first certificate)

This error indicates that there is a problem with the certificate chain, and openssl cannot verify that the certificate presented by the device should be trusted. Let's look at the certificate chain from the example above to see how certificate chains should work:

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
```

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

The certificate chain is a list of certificates presented by the server, beginning with the server's own certificate and then including increasingly higher-level intermediate certificates linking the server's certificate with a Certificate Authority's top-level certificate. Each certificate lists its Subject (the line starting with 's:' and its Issuer (the line starting with 'i').

The Subject is the entity identified by the certificate. It includes the Organization name and sometimes the Common Name of the entity for which the certificate was issued.

The Issuer is the entity that issued the certificate. It also includes an Organization field and sometimes a Common Name.

If a server had a certificate issued directly by a trusted Certificate Authority, it would not need to include any other certificates in its certificate chain. It would present one certificate that looked like:

```
--- Certificate chain 0
s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com i:/C=US/O=Trusted
 Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

Given this certificate, openssl would verify that the ExampleCo certificate for ***.example.com** was correctly signed by the Trusted Authority certificate, which would be present in openssl's built-in trust store. After that verification, openssl would successfully connect to the device.

However, most servers do not have certificates signed directly by a trusted CA. Instead, as in the first example, the server's certificate is signed by one or more intermediates, and the highest-level intermediate has a certificate signed by the trusted CA. OpenSSL does not trust these intermediate CAs by default, and can only verify them if it is given a complete certificate chain ending in a trusted CA.

It is critically important that servers whose certificates are signed by intermediate authorities supply ALL the certificates linking them to a trusted CA, including all of the intermediate certificates. If they don't supply this entire chain, the output from openssl will look something like this:

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1
depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1
CONNECTED(00000003)
---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
 Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
```

```
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
 Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

This output shows that the server only provided one certificate, and the provided certificate was signed by an intermediate authority, not a trusted root. The output also shows the characteristic verification errors.

Remediation

This problem is caused by a misconfigured certificate presented by the device. The only way to fix this so that Security Cloud Control or any other program can securely connect to the device is to load the correct certificate chain onto the device, so that it will present a complete certificate chain to connecting clients.

To include the intermediate CA to the trustpoint follow one of the links below (depending on your case - if CSR was generated on the ASA or not):

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

Resolve new certificate detected

Configure device certificate synchronization when Security Cloud Control detects a new self-signed certificate after a device upgrade.

Resolve the "New Certificate Detected" message that appears as both a Configuration Status and Connectivity status when a device generates a new self-signed certificate after upgrade.

If you upgrade a device that has a self-signed certificate and a new certificate is generated after the upgrade process, Security Cloud Control may generate a "New Certificate Detected" message as both a **Configuration Status** and **Connectivity** status. You must manually confirm and resolve this issue before you can continue managing it from Security Cloud Control. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

> **Note**
>
> When you bulk reconnect devices more than one managed device to Security Cloud Control at the same time, Security Cloud Control automatically reviews and accepts the new certificates on the devices and continues to reconnect with them.

Follow these steps to resolve a new certificate:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.
5. In the action pane, click **Review Certificate**.

   Security Cloud Control allows you to download the certificate for review and accept the new certificate.
6. In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

Security Cloud Control automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the page to see the device once it's synced.

Troubleshoot onboarding error

Configure device onboarding troubleshooting when devices fail to onboard successfully.

Resolve device onboarding errors that prevent devices from being successfully added to the system.

The device onboarding error can occur for various reasons.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the appropriate device type tab and select the device running into this error. In some cases, you will see the error description on the right. Take the necessary actions mentioned in the description.

   Or
3. Remove the device instance from Security Cloud Control and try onboarding the device again.

The device onboarding error is resolved and the device can be successfully onboarded to the system.

Resolve the conflict detected status

Configure conflict resolution to synchronize device configurations between Security Cloud Control and live devices when conflicts are detected.

This task resolves configuration conflicts that occur when changes are made directly to a device without using Security Cloud Control.

Security Cloud Control allows you to enable or disable conflict detection on each live device. If Conflict detection on page 832 is enabled and there was a change made to the device's configuration without using Security Cloud Control, the device's configuration status will show **Conflict Detected**.

Before you begin

Follow these steps to resolve a **Conflict Detected** status:

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. Choose **Security Devices**.

   > **Note**
   >
   > For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

3. Click the **Devices** tab to locate your device.
4. Click the appropriate device type tab.
5. Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.
6. In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.
   - The panel labeled "Last Known Device Configuration" is the device configuration stored on Security Cloud Control.
   - The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.
7. Resolve the conflict by selecting one of the following:
   - **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration.

     > **Note**
     >
     > As Security Cloud Control does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

   - **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on Security Cloud Control.

> **Note**
>
> All configuration changes, rejected or accepted, are recorded in the change log.

The conflict status is resolved and the device configuration is synchronized between Security Cloud Control and the device.

Resolve the not synced status

Configure a device with a "Not Synced" Configuration Status to resolve synchronization issues between Security Cloud Control and the device.

This task helps you resolve synchronization conflicts when a device shows "Not Synced" status, allowing you to either deploy pending changes or revert to the device's current configuration.

Use this procedure when a device displays a "Not Synced" Configuration Status, indicating there are differences between the configuration stored in Security Cloud Control and the running configuration on the device.

Procedure

---

1. Choose **Security Devices**.

   > **Note**
   >
   > For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.
4. Select the device reported as Not Synced.
5. In the **Not synced** panel to the right, select either of the following:
   - **Preview and Deploy...** -If you want to push the configuration change from Security Cloud Control to the device, preview and deploy the changes you made now, or wait and deploy multiple changes at once.
   - **Discard Changes** -If you do **not** want to push the configuration change from Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

The device synchronization status is resolved. If you selected Preview and Deploy, your changes are pushed to the device. If you selected Discard Changes, the configuration in Security Cloud Control is updated to match the device's running configuration.

62 FAQ and support

Topics:

- Security Cloud Control
- FAQ about onboarding devices to Security Cloud Control
- Device types
- Security
- End-of-Support for management of Secure Firewall Threat Defense devices, Version 7.0.x, managed by Cloud-Delivered Firewall Management Center
- Troubleshooting
- Terminologies and definitions used in Zero-Touch Provisioning
- Policy optimization
- Connectivity
- Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI
- About Data Interfaces
- How Security Cloud Control processes personal information
- Contact Security Cloud Control support

This chapter contains the following sections:

Security Cloud Control

Learn how Security Cloud Control helps administrators create, monitor, and maintain consistent security policies across supported devices from a single cloud-based interface.

What is Security Cloud Control?

Security Cloud Control (formerly Cisco Defense Orchestrator) is a cloud-based multi-device manager that allows network administrators to create and maintain consistent security policies across various security devices.

You can use Security Cloud Control to manage these devices:

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Umbrella
- Meraki
- Cisco IOS devices
- Amazon Web Services (AWS) instances
- Devices administered using an SSH connection

Security Cloud Control administrators can monitor and maintain all these device types through a single interface.

FAQ about onboarding devices to Security Cloud Control

Learn about onboarding FAQs for supported device types in Security Cloud Control, including Secure Firewall ASA, Firewall Threat Defense, on-premises Firewall Management Center, Meraki, SSH, and IOS devices.

FAQs About Onboarding Secure Firewall ASA to Security Cloud Control

How do I onboard an ASA using credentials?

You can onboard ASAs one at a time or in a bulk operation. device at a time. When onboarding an ASA that is part of a high-availability pair, use Onboard an ASA Device to onboard only the primary device of the pair. The method of onboarding a security context or admin context is the same for onboarding any other ASA.

How do I onboard more than one ASA at a time?

You can create a list of ASAs using a CSV file, and Security Cloud Control will onboard all the ASAs in the list. See Onboard ASAs in Bulk for instructions on how to bulk onboard ASAs.

What do I do after onboarding my ASAs?

See Managing ASA with Security Cloud Control to get started.

FAQs About Onboarding Secure Firewall Threat Defense to Cloud-Delivered Firewall Management Center

How do I onboard Secure Firewall Threat Defense?

You can onboard an FTD device using a CLI registration key, through zero-touch provisioning, or with a serial number.

What do I do after onboarding my Secure Firewall Threat Defense?

Once the device is sychronized, navigate to **Administration** > **Integrations** > **Firewall Management Center** and select an action from the Actions, Management, or Settings pane to begin configuring your threat defense device in Cloud-Delivered Firewall Management Center. See Cloud-delivered Firewall Management Center Application Page to get started.

How do I troubleshoot my Secure Firewall Threat Defense?

See Troubleshoot Onboarding Secure Firewall Threat Defense.

FAQs About On-Premises Firewall Management Center

This concept explains how you can onboard an On-Premises Firewall Management Center to Security Cloud Control, but device management changes must still be made directly in the On-Premises Firewall Management Center UI.

How do I onboard an On-Premises Firewall Management Center?

You can onboard an On-Premises Firewall Management Center to Security Cloud Control. Onboarding an On-Premises Firewall Management Center also onboards all the devices registered to On-Premises Firewall Management Center. Security Cloud Control does not support creating or modifying objects or policies associated with On-Premises Firewall Management Center or the devices registered to On-Premises Firewall Management Center. You must make these changes in the On-Premises Firewall Management Center UI. For more information, see Onboard an On-Prem Management Center.

FAQs About Onboarding Meraki Devices to Security Cloud Control

How do I onboard a Meraki device?

MX devices can be managed by both Security Cloud Control and the Meraki dashboard. Security Cloud Control deploys configuration changes to the Meraki dashboard, which in turn deploys the configuration securely to the device. See Onboard Meraki MX Devices to get started.

FAQs About Onboarding SSH Devices to Security Cloud Control

How do I onboard an SSH device?

You can use the username and password of a highly privileged user stored on the SSH device to onboard the device with a Secure Device Connector (SDC). See Onboard an SSH Device to get started.

How do I delete a device?

You can delete a device from the **Security Devices** page.

FAQs About Onboarding IOS Devices to Security Cloud Control

How do I onboard a Cisco IOS device?

You can onboard a live Cisco device running Cisco IOS (Internetwork Operating System) with a Secure Device Connector (SDC). See Onboard a Cisco IOS Device to get started.

How do I delete a device?

You can delete a device from the **Security Devices** page.

Device types

Learn about frequently asked questions for device types in Security Cloud Control, including sync and conflict states, deployment behavior, scale limits, and support for ISR, ASR, and SMA devices.

What is Firepower Threat Defense (FTD)

Cisco's next generation firewall software image. It strives to combine the best of Sourcefire next generation firewall services and the ASA platform. It can be installed on a number of different Firepower hardware devices or virtual machines. This is not the same as a ASA FirePOWER module.

See ASA Software and Hardware Support for more information.

What is Firepower?

Firepower is a general term that refers to a group of next generation firewall hardware and software.

When is a device Synced?

When the configuration on Security Cloud Control and the configuration stored locally on the device are the same.

When is a device Not Synced?

When the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device.

When is a device in a Conflict Detected state?

When the configuration on the device was changed outside of Security Cloud Control (out-of-band), and is now different than the configuration stored on Security Cloud Control.

What does it mean to deploy a change to a device?

After you onboard a device to Security Cloud Control, Security Cloud Control maintains a copy of its configuration. When you make a change on Security Cloud Control, Security Cloud Control makes a change to its copy of the device's configuration. When you "deploy" that change back to a device, Security Cloud Control copies the changes you made to the device's copy of its configuration. See these topics:

- Deploy Configuration Changes from Security Cloud Control to an ASA

Are there any scale limitations for device management?

Security Cloud Control's cloud architecture allows it to scale to thousands of devices.

Does Security Cloud Control manage Cisco Integrated Services Routers and Aggregation Services Routers?

Security Cloud Control allows you to create a model device for ISRs and ASRs and import its configuration. You can then create templates based on the imported configurations and export the configuration as a standardized configuration that can be deployed to new or existing ISR and ASR devices for consistent security.

Can Security Cloud Control manage SMA?

No, Security Cloud Control does not currently manage SMA.

Security

Learn about security FAQs, including data protection, multi-factor authentication, OTP login errors, Secure Device Connector usage, private device connectivity, and VPN tunnel status checks.

I received the error "Could not validate your OTP" when logging into Security Cloud Control for the first time

Check that your desktop or mobile device clock is synchronized with a world time server. Clocks being out of sync by less or more than a minute can cause incorrect OTPs to be generated.

Is my device connected directly to Security Cloud Control cloud platform?

Yes. The secured connection is performed using the Security Cloud Control SDC which is used as a proxy between the device and Security Cloud Control platform. Security Cloud Control architecture, designed with security first in mind, enables having complete separation between data traversing back and forth to the device.

How can I connect a device which does not have a public IP address?

You can leverage Security Cloud Control Secure Device Connector (SDC) which can be deployed within your network and doesn't need any outside port to be open. Once the SDC is deployed you can onboard devices with internal (non-internet routable) IP addresses.

See more information here: Secure Device Connector (SDC)

Does the SDC require any additional cost or license?

No.

How can I check the tunnel status? State options

Security Cloud Control performs the tunnel connectivity checks automatically every hour, however ad-hoc VPN tunnel connectivity checks can be performed by choosing a tunnel and requesting to check connectivity. Results may take several seconds to process.

Can I search a tunnel based on the device name as well as its IP address of one of its peers?

Yes. Search and pivot to a specific VPN tunnel details by using available filters and search capabilities on both name and the peers IP addresses.

End-of-Support for management of Secure Firewall Threat Defense devices, Version 7.0.*x*, managed by Cloud-Delivered Firewall Management Center

Learn about FAQs for end-of-support management of Secure Firewall Threat Defense Version 7.0.x devices in Cloud-Delivered Firewall Management Center, including onboarding limits, read-only behavior, upgrade options, and TAC support.

Which version of Secure Firewall Threat Defense devices has Cloud-Delivered Firewall Management Center stopped managing as of December 15, 2025?

Cloud-Delivered Firewall Management Center stopped managing Secure Firewall Threat Defense devices, Version 7.0.*x*, as of December 15, 2025.

Why is this necessary?

This was necessary to ensure compatibility and security for our customers' systems. As we upgrade our systems, it was essential that only the latest version of Secure Firewall Threat Defense devices were supported to maintain reliability and performance.

Can I onboard Version 7.0.*x* devices after December 15, 2025?

No, you can no longer onboard Secure Firewall Threat Defense, Version 7.0.*x,* devices after December 15, 2025.

After December 15, 2025, will I be able to use my existing Secure Firewall Threat Defense 7.0.*x* devices?

Cloud-Delivered Firewall Management Center will not support the management of Secure Firewall Threat Defense devices running Version 7.0.*x* after December 15, 2025. You will not be able to make or deploy changes to Secure Firewall Threat Defense devices running Version 7.0.*x* and earlier except to upgrade or unregister.

> **Note**
>
> Secure Firewall Threat Defense devices running Version 7.0.*x* will still be visible in Cloud-Delivered Firewall Management Center, but in read-only mode only. Changes you make after December 15, 2025 will not be deployed to the devices.

What are the recommended upgrade options?

You are required to upgrade to at least Version 7.2.*x*. The Cisco-suggested version is 7.6.2.

How do I upgrade?

For information about upgrading Secure Firewall Threat Defense devices, refer to Threat defense upgrade guide for Cloud-Delivered Firewall Management Center.

Are there costs associated with upgrade?

There is no addtional cost, unless your hardware must also be upgraded. (The reference to hardware is limited to Cisco Secure ASA 5508-X and Cisco Secure ASA 5516-X running Secure Firewall Threat Defense Version 7.0.*x*). If you must refresh your hardware, reach out to your Cisco account team.

What will happen if I don't upgrade?

From December 15, 2025, you will not be able to make or deploy changes to Secure Firewall Threat Defense devices running Version 7.0.*x* and earlier, except to upgrade or unregister. Failing to upgrade leaves you vulnerable to compatibility issues, security issues, and possible downtime. To minimize disruption, you are required to upgrade now.

Will there be any impact to my existing systems or applications?

Upgrading is unlikely to have any significant impact on your current deployment. If you face any issues during the upgrade process, contact the Cisco Technical Assistance Center (TAC).

For assistance in upgrading, Cisco offers the LevelUp program. You can request assistance using this link.

Can I migrate my existing ASA 5508 and 5516 devices to Cloud-Delivered Firewall Management Center?

We recommend that you do *not* migrate your existing ASA 5508 and ASA 5516 devices to Cloud-Delivered Firewall Management Center because the last supported Secure Firewall Threat Defense version for these ASA devices is 7.0.

In addition, Cisco has stopped support for management of Secure Firewall Threat Defense Version 7.0.x in Cloud-Delivered Firewall Management Center as of December 31, 2025, and the ASA 5508 and 5516 devices cannot be upgraded to Version 7.2.x and later.

Can I manage my device's health in read-only mode after support ends?

After December 15, 2025, you will not be able to deploy device health policy changes, if any, to Secure Firewall Threat Defense devices running Version 7.0.x and earlier. These devices will continue to operate with the previously configured health policies.

What if I'm unsure about how to proceed?

Reach out to Cisco Technical Assistance Center (TAC) (or the Cisco account team) for clarifications.

Troubleshooting

Learn about troubleshooting FAQs for Security Cloud Control, including deployment warnings, out-of-band configuration differences, conflict resolution, and certificate rejection issues.

While performing complete deploy of device configuration from Security Cloud Control to managed device, I get a warning "Cannot deploy changes to device". What can I do to solve that?

If an error occurrs when you deploy a full configuration (changes performed beyond Security Cloud Control supported commands) to the device, click "Check for changes" to pull the latest available configuration from device. This may solve the problem and you will be able to continue making changes on Security Cloud Control and deploy them. In case the issue persist, please contact Cisco TAC from the **Contact Support** page.

While resolving out-of-band issue (changes performed outside of Security Cloud Control; directly to a device), comparing the configuration present in Security Cloud Control that of the device, Security Cloud Control presents additional metadata that were not added or modified by me. Why?

As Security Cloud Control expands its functionality, additional information will be collected from the device's configuration to enrich and maintain all required data for better policy and device management analysis. These are not changes that occurred on managed device but already existing information. Resolving the conflict detected state can be easily solved by checking for changes from the device and reviewing the changes occurred.

Terminologies and definitions used in Zero-Touch Provisioning

Learn about FAQs for zero-touch provisioning terminology in Security Cloud Control, including claimed and parked devices, initial provisioning, and how FTD devices are onboarded through the Cisco Cloud.

- **Claimed** - Used in the context of serial number onboarding in Security Cloud Control. A device is "claimed" if its serial number has been onboarded to a Security Cloud Control tenant.
- **Parked** - Used in the context of serial number onboarding in Security Cloud Control. A device is "parked" if it has connected to the Cisco Cloud, and a Security Cloud Control tenant has not claimed its serial number.
- **Initial provisioning** - Used in the context of the initial FTD setup. During this phase, the device accepts EULA, creates a new password, configures management IP address, sets FQDN, sets DNS servers, and chooses to manage the device locally with FDM.
- **Zero-Touch Provisioning** - It is the process of shipping an FTD from the factory to a customer site (typically a branch office), an employee at the site connects the FTD to their network, and the device contacts the Cisco Cloud. At that point, the device is onboarded to Security Cloud Control tenant if its serial number has already been "claimed," or the FTD is "parked" in the Cisco cloud until a Security Cloud Control tenant claims it.

Policy optimization

Learn about FAQs for policy optimization in Security Cloud Control, including how to identify fully shadowed access rules within the same access group using Network Policy Management.

How can I identify a case when two or more access lists (within the same access group) are shadowing each other?

Security Cloud Control Network Policy Management (NPM) is able to identify and alert the user if within a rule set, a rule higher in order, is shadowing a different rule. User can either navigate between all network policies or filter to identify all shadow issues.

> **Note**
>
> Security Cloud Control supports only fully shadowed rules.

Connectivity

Learn about Security Cloud Control connectivity FAQs, including how to handle SDC IP address changes, update device IP addresses, reconnect managed devices, and meet ASA networking requirements.

The Secure Device Connector changed IP address, but this was not reflected within Security Cloud Control. What can I do to reflect the change?

In order to obtain and update the new Secure Device Connector (SDC) within Security Cloud Control, you will need to restart the container using the following commands:

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$
./cdo/toolkit/toolkit.sh restartSDC <tenant-name>
```

What happens if the IP address used by Security Cloud Control to manage my devices (FTD or ASA) changes?

If the IP address of the device changes for any reason, whether it is a change in the static IP address or a change in the IP address due to DHCP, you can change the IP address that Security Cloud Control uses to connect to the device (see Change a device's IP address in Security Cloud Control Firewall Management on page 842) and then reconnect the device (see Bulk reconnect devices to Security Cloud Control Firewall Management on page 847). When reconnecting the device you will be asked to enter the new IP address of the device as well as re-enter the authentication credentials.

What networking is required to connect my ASA to Security Cloud Control?

- ASDM image present and enabled for ASA.
- Public interface access to 52.25.109.29, 52.34.234.2, 52.36.70.147
- ASA's HTTPS port must be set to 443 or to a value of 1024 or higher. For example, it cannot be set to port 636.
- If the ASA under management is also configured to accept AnyConnect VPN Client connections, the ASA HTTPS port must be changed to a value of 1024 or higher.

Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI

Learn how to complete the initial CLI configuration of a Secure Firewall Threat Defense device, including management networking, data interface access, firewall mode, and manager registration with a CLI registration key.

Connect to the device's CLI to perform initial setup, including setting the management IP address, gateway, and other basic networking settings using the setup wizard. Ensure all DNS and firewall ports are accessible for communication.

The dedicated management interface is a special interface with its own network settings. If you do not want to use the management interface, you can use the CLI to configure a data interface instead.

This configuration is ideal for devices that are going to be onboarded with their CLI registration key.

> **Note**
>
> Do **not** use this configuration procedure for devices that are onboarding with zero-touch provisioning.

Procedure

1. Connect to the device's CLI, either from the console port or using SSH to the management interface. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

   (Firepower and Secure Firewall hardware models) The console port connects to the FXOS CLI. The SSH session connects directly to the Firewall Threat Defense CLI.

2. Log in with the username **admin** and the password **Admin123** .

   At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the Firewall Threat Defense login for SSH.

   > **Note**
   >
   > If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default.
   >
   > For Firepower and Secure Firewall hardware, see the Reimage Procedures in the Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense .
   >
   > For the ISA 3000, see the Cisco Secure Firewall ASA and Threat Defense Reimage Guide .

   Example

```
firepower login:
                          admin
Password:
                          Admin123
Successful login attempts for user 'admin' : 1
[...]
Hello admin. You must change your password.
```

```
Enter new password:
                        ********
Confirm new password:
                        ********
Your password was updated successfully.
[...]
firepower#
```

3. If you connected to FXOS on the console port, connect to the Firewall Threat Defense CLI.

   connect ftd

   Example

   ```
   firepower# connect ftd
   >
   ```

4. The first time you log in to the device, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script.

   > **Note**
   >
   > You cannot repeat the CLI setup wizard unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the threat defense command reference.

   Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

   > **Note**
   >
   > The management interface settings are used even when you enable Firewall Threat Defense access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the management interface DNS servers, and not the data interface DNS servers.

   See the following guidelines:

   - **Configure IPv4 via DHCP or manually?**–If you want to use a data interface for Firewall Threat Defense access instead of the management interface, choose **manual**. Although you do not plan to use the management interface, you must set an IP address, for example, a private address. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
   - **Enter the IPv4 default gateway for the management interface**–If you want to use a data interface for Firewall Threat Defense access instead of the management interface, set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the FMC access data interface.
   - **If your networking information has changed, you will need to reconnect**–If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.

- **Manage the device locally?**–Enter **YES** to configure the device for the device to be managed by either the Cloud-Delivered Firewall Management Center or Secure Firewall Device Manager.

  Manage the device locally?–Enter **NO** to configure the device for remote management with the On-Premises Firewall Management Center.

- **Configure firewall mode?**–We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration. Note that data interface Firewall Threat Defense access is only supported in routed firewall mode.

5. Optional: Configure a data interface for Cloud-Delivered Firewall Management Center access.

   configure network management-data-interface

   You are then prompted to configure basic network settings for the data interface.

   > **Note**
   >
   > You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

   See the following details for using this command. See About Data Interfaces on page 1116 for more informatio.

   - The original management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network {ipv4 | ipv6} manual** command. If you did not already set the management interface gateway to **data-interfaces**, this command will set it now.
   - When you onboard the device for Firewall Threat Defense management through Security Cloud Control, Security Cloud Control discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. You can later make changes to the access interface configuration, but make sure you don't make changes that can prevent the device or Security Cloud Control from re-establishing the management connection. If the management connection is disrupted, the device includes the **configure policy rollback** command to restore the previous deployment.
   - This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

     Also, local DNS servers are only retained if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in Security Cloud Control, including the DNS servers, to match the device configuration.
   - You can change the management interface after you onboard the Firewall Threat Defense for Firewall Threat Defense management through threat defense, to either the management interface or another data interface.
   - The FQDN that you set in the setup wizard will be used for this interface.
   - You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
   - To disable data managemement, enter the **configure network management-data-interface disable** command.

Example

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n)
[n]:

Configuration done with option to allow FMC access from any network, if you
wish to change the FMC access network
use the 'client' option in the command 'configure network
management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n)
[n]:

Configuration done with option to allow FMC access from any network, if you
wish to change the FMC access network
use the 'client' option in the command 'configure network
management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

6. Optional: Limit data interface access to Security Cloud Control on a specific network.

   configure network management-data-interface client *ip_address netmask*

   By default, all networks are allowed.

About Data Interfaces

Learn about data interface, including using management or data interfaces for FTD communication, remote management from outside interfaces, high availability support, and key data interface limitations.

You can use either the dedicated management interface or a regular data interface for communication with the device. Security Cloud Control access on a data interface is useful if you want to manage the FTD remotely from the outside interface, or you do not have a separate management network. Security Cloud Control supports high availability on the FTD managed remotely from the data interface.

FTD management access from a data interface has the following limitations:

- You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the FTD and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using Security Cloud Control. Because the management interface gateway will be changed to be the data interfaces, you also cannot SSH to the management interface from a remote network unless you add a static route for the management interface using the **configure network static-routes** command.

How Security Cloud Control processes personal information

Learn about FAQs for how Security Cloud Control processes personal information, including where to find Cisco's Privacy Data Sheet for details on handling personally identifiable information.

To learn how Security Cloud Control processes your personal identifiable information, see the Security Cloud Control Privacy Data Sheet.

Contact Security Cloud Control support

Learn how to contact Security Cloud Control support, export workflow details, open a Cisco TAC support ticket, and check the Security Cloud Control service status page.

This chapter covers the following sections:

Export The Workflow

We strongly recommend exporting the workflow of a device that is experience issues prior to opening a support ticket. This additional information can help the support team expeditiously identify and correct any troubleshooting efforts.

Use the following procedure to export the workflow:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate your device.
3. Click the appropriate device type tab and select the device you need to troubleshoot.

   Use the **filter** or **search bar** to locate the device you need to troubleshoot. Select the device so it is highlighted.
4. In the **Device Actions** pane, select **Workflows**.
5. Click the **Export** button located at the top right of the page, above the table of events. The file automatically saves locally as a **.json** file. Attach this to any emails or tickets you open with TAC.

Open a Support Ticket with TAC

A customer using a 30-day trial or a licensed Security Cloud Control account can open a support ticket with Cisco's Technical Assistance Center (TAC).

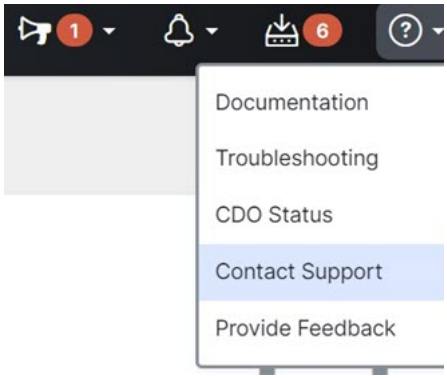
- How Security Cloud Control Customers Open a Support Ticket with TAC.
- How Security Cloud Control Trial Customers Open a Support Ticket with TAC.

How Security Cloud Control Customers Open a Support Ticket with TAC

This section explains how a customer using a licensed Security Cloud Control tenant can open a support ticket with Cisco's Technical Assistance Center (TAC).

Procedure

1. Log in to Security Cloud Control.
2. Next to your tenant name, click the help button and select **Contact Support**.



3. Click **Support Case Manager**.
4. Click the blue **Open New Case** button.
5. Click **Open Case**.
6. Select **Products and Services** and then click **Open Case**.
7. Choose a **Request Type**.
8. Expand **Find Product by Service Agreement** row.
9. Fill in all the fields. Many of the fields are obvious. This is some additional information:
   - **Product Name (PID)** - If you no longer have this number, see the Security Cloud Control Data Sheet.
   - **Product Description** - This is the description of the PID.
   - **Site Name** - Enter your site name. If you are a Cisco Partner opening a case for one of your customers, enter the customer's name.
   - **Service Contract** - Enter your service contract number.
     - **Important**: In order for your case to be associated with your Cisco.com account, you need to associate your contract number to your Cisco.com profile. Use this procedure to associate your contract number to your Cisco.com profile.
       a. Open to Cisco Profile Manager.
       b. Click the **Access Management** tab.
       c. Click **Add Access**.

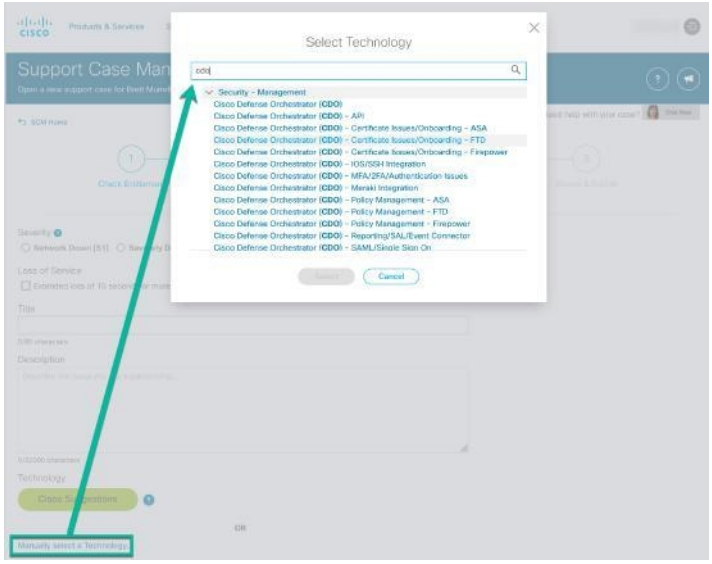
d. Choose **TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com** and click **Go**.

e. Enter service contracts number(s) in the space provided and click **Submit**. You will receive notification via email that the service contract associations have been completed. Service contract association can take up to 6 hours to complete.

Important

Important: If you are not able to access any of the links below, please contact your authorized Cisco partner or re-seller, your Cisco account representative, or the individual in your company who manages Cisco service agreement information.

10. Click **Next.**
11. In the **Describe Problem** screen, scroll down to **Manually select a Technology**, click it, and type **Security Cloud Control** in the search field.
12. Select the category that best matches your request, and click **Select**.



13. Complete the remainder of the service request and click **Submit**.

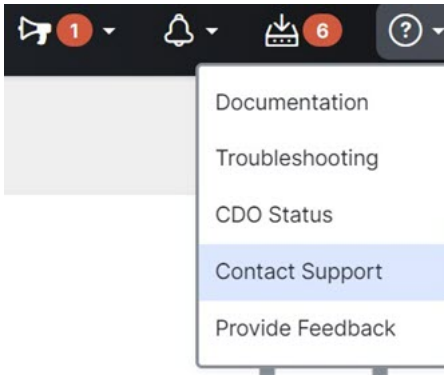
How Security Cloud Control Trial Customers Open a Support Ticket with TAC

This section explains how a customer using a free trial of a Security Cloud Control tenant can open a support ticket with Cisco's Technical Assistance Center (TAC).

Procedure

---

1. Log in to Security Cloud Control.
2. Next to your tenant and account name, click the help button and select **Contact Support**.



3. In the **Enter Issue or request below** field, specify the issue that you are facing or your request and click **Submit**.

   Your request, along with the technical information, will be sent to the support team, and a technical support engineer will respond to your query.

Security Cloud Control Service Status Page

Security Cloud Control maintains a customer-facing service status page that shows you if the Security Cloud Control service is up and any service interruptions it may have had. You can view up-time information with daily, weekly, or monthly graphs.

You can reach the Security Cloud Control status page by clicking **Security Cloud Control Status** in the help menu on any page in Security Cloud Control.

On the status page, you can click the **Subscribe to Updates** to receive a notification if the Security Cloud Control service goes down.

Part XVII

Appendix

Topics:

- Security and Internet Access
- Terraform
- Open Source and 3rd Party License Attribution

63 Security and Internet Access

Topics:

- Internet access requirements

Lists of URLs used by the dynamic attributes connector when communicating with cloud service providers and the Security Cloud Control.

Internet access requirements

Lists specific URIs that require access to the internet when using the dynamic attributes connector.

By default, the dynamic attributes connector is configured to communicate with the Firepower System over the internet using HTTPS on port 443/tcp (HTTPS). If you do not want the dynamic attributes connector to have direct access to the internet, you can configure a proxy server.

This information details the URLs the dynamic attributes connector use to communicate with the Security Cloud Control and with external servers.

Table 51: Dynamic Attributes Connector access requirements

URL	Reason
https://*fmc-ip***/api/fmc_platform/v1/auth/generatetoken**	Authentication
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id***/object/dynamicobjects**	GET and POST dynamic objects
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects/***object-id***/mappings?action=add**	Add mappings
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id*** /object/dynamicobjects/***object-id***/mappings?action=remove**	Remove mappings

Migration from DockerHub to Amazon ECR

Docker images for the Dynamic Attributes Connector are being migrated from Docker Hub to Amazon Elastic Container Registry (Amazon ECR).

To use the new field packages, you must allow access through your firewall or proxy to all of the following URLs:

- https://public.ecr.aws
- https://csdac-cosign.s3.us-west-1.amazonaws.com
- https://d2glxqk2uabbnd.cloudfront.net
- https://d5l0dvt14r5h8.cloudfront.net

  For more information about Amazon Cloudfront URLs, see EKS Anywhere documentation.

Dynamic Attributes Connector Azure access requirements

The dynamic attributes connector calls built-in SDK methods to GET instance information. These methods internally call https://login.microsoft.com (for authentication) and https://management.azure.com (to GET instance information).

64 Terraform

Topics:

- About Terraform

Learn how to automate the setup and management of your Security Cloud Control organization using Terraform providers and modules.

This chapter explains how to set up and manage Security Cloud Control.

About Terraform

Learn how to use Security Cloud Control Terraform providers and modules to manage users, onboard firewall devices, deploy Secure Device and Event Connectors, and maintain repeatable, version-controlled infrastructure configurations.

Security Cloud Control customers can use the Security Cloud Control Terraform provider and Security Cloud Control Terraform modules to rapidly set up their tenants using code that is repeatable and version-controlled. The Security Cloud Control Terraform provider allows users to do the following:

- **Manage** users
- **Onboard** Secure Firewall Threat Defense devices on Cloud-Delivered Firewall Management Centers, Cisco Secure ASA devices, and iOS devices
- **Onboard** secure device connectors on vSphere and AWS
- **Onboard** secure event connectors on AWS

For more information, refer to the following pages:

- Security Cloud Control Terraform Provider page
- Security Cloud Control SDC on vSphere module page
- Security Cloud Control SDC on AWS module page
- Security Cloud Control SEC on AWS module page
- Work through the Devnet learning lab
- Automating Security Infrastructure Management Using the Security Cloud Control Terraform Provider - Learning Lab
- Security Cloud Control automation examples on GitHub

Support

The Security Cloud Control Terraform provider and modules are published as Open Source Software under the Apache 2.0 license. Please file issues on GitHub in the repositories below if you require support:

Module	Repository
Security Cloud Control Terraform Provider	https://github.com/ciscodevnet/terraform-provider-SecurityCloudControl
Security Cloud Control SDC Module (vSphere)	https://github.com/CiscoDevNet/terraform-vsphere-SecurityCloudControl-sdc
Security Cloud Control SDC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-SecurityCloudControl-sdc
Security Cloud Control SEC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-SecurityCloudControl-sec

Contribution to repositories

The Security Cloud Control team welcomes contributions to the repositories above. Please create pull pequests on these GitHub repositories if you wish to contribute to improving the provider and modules.

Related topics

- Deploy an SDC to vSphere Using Terraform
- Deploy an SDC to AWS VPC Using Terraform
- Deploy an SEC to AWS VPC Using Terraform

65 Open Source and 3rd Party License Attribution

Topics:

- Open source and third-party license in SDC

This chapter provides information about open source and third-party license.

Open source and third-party license in SDC

An overview of open-source and third-party license attributions for components included in the Cisco Secure Device Connector (SDC).

Provides an overview of open-source and third-party license attributions for components included in the Cisco Secure Device Connector (SDC).

==========

*** amqplib ***

amqplib copyright (c) 2013, 2014

Michael Bridgen <mikeb@squaremobius.net>

This package, "amqplib", is licensed under the MIT License. A copy maybe found in the file LICENSE-MIT in this directory, or downloaded from

http://opensource.org/licenses/MIT

==========

*** async ***

Copyright (c) 2010-2016 Caolan McMahon

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** bluebird ***

The MIT License (MIT)

Copyright (c) 2013-2015 Petka Antonov

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER

IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** cheerio ***

Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the 'Software'), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** command-line-args ***

The MIT License (MIT)

Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** ip ***

This software is licensed under the MIT License.

Copyright Fedor Indutny, 2012.

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** json-buffer ***

Copyright (c) 2013 Dominic Tarr

Permission is hereby granted, free of charge,to any person obtaining a copy of this software andassociated documentation files (the "Software"), todeal in the Software without restriction, includingwithout limitation the rights to use, copy, modify,merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whomthe Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission noticeshall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIESOF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FORANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THESOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stable-stringify ***

This software is released under the MIT license:

Permission is hereby granted, free of charge, to any person obtaining a copy ofthis software and associated documentation files (the "Software"), to deal inthe Software without restriction, including without limitation the rights touse, copy, modify, merge, publish, distribute, sublicense, and/or sell copies ofthe Software, and to permit persons to whom the Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESSFOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS ORCOPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHERIN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR INCONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stringify-safe ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT,

OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** lodash ***

Copyright JS Foundation and other contributors <https://js.foundation/**>**

Based on Underscore.js, copyright Jeremy Ashkenas,

DocumentCloud and Investigative Reporters & Editors<http://underscorejs.org/**>**

This software consists of voluntary contributions made by manyindividuals. For exact contribution history, see the revision historyavailable at https://github.com/lodash/lodash

The following license applies to all parts of this software except as

documented below:

====

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Samplecode is defined as all source code displayed within the prose of thedocumentation.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

Files located in the node_modules and vendor directories are externallymaintained libraries used by this software which have their ownlicenses; we recommend you read them, as their terms may differ from theterms above.

==========

*** log4js ***

Copyright 2015 Gareth Jones (with contributions from many other people)

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions andlimitations under the License.

==========

*** mkdirp ***

Copyright 2010 James Halliday (mail@substack.net)

This project is free software released under the MIT/X11 license:

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** node-forge ***

New BSD License (3-clause)

Copyright (c) 2010, Digital Bazaar, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or withoutmodification, are permitted provided that the following conditions are met:

*** Redistributions of source code must retain the above copyrightnotice, this list of conditions and the following disclaimer.**

*** Redistributions in binary form must reproduce the above copyrightnotice, this list of conditions and the following disclaimer in thedocumentation and/or other materials provided with the distribution.**

*** Neither the name of Digital Bazaar, Inc. nor thenames of its contributors may be used to endorse or promote productsderived from this software without specific prior written permission.**

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" ANDANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIEDWARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AREDISCLAIMED. IN NO EVENT SHALL DIGITAL BAZAAR BE LIABLE FOR ANYDIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED ANDON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THISSOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

*** request ***

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory

patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

==========

*** rimraf ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** uuid ***

Copyright (c) 2010-2012 Robert Kieffer

MIT License - http://opensource.org/licenses/mit-license.php

==========

*** validator ***

Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** when ***

Open Source Initiative OSI - The MIT License

http://www.opensource.org/licenses/mit-license.php

Copyright (c) 2011 Brian Cavalier

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.==========