Cisco Secure Access Documentation Changes

Cisco Secure Access
Updated November 2, 2026

Topics included

1 Change log overview....4
What the change log includes....5
Access the legacy Secure Access Help change log....5

2 November 2026 updates....6
Cisco Secure Access Documentation Changes 2026-11-02....7

3 October 2026 updates....36
Cisco Secure Access Documentation Changes 2026-10-26....37
Cisco Secure Access Documentation Changes 2026-10-19....48
Cisco Secure Access Documentation Changes 2026-10-12....62
Cisco Secure Access Documentation Changes 2026-10-05....90

4 September 2026 updates....96
Cisco Secure Access Documentation Changes 2026-09-28....97
Cisco Secure Access documentation changes 2026-09-21....104

1 Change log overview

Topics:

- What the change log includes
- Access the legacy Secure Access Help change log

Explains how the change log compares Secure Access Help snapshots and reports page counts, additions, removals, and links to changed content.

What the change log includes

Identifies the snapshot dates, page counts, added or removed pages, and content details included in each Secure Access Help change-log entry.

A change-log entry is a record of changes to the Cisco Secure Access Help (https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html). It compares the current snapshot with the previous snapshot and links to affected pages. The change log is generated weekly, except during holidays.

Each change-log entry includes:

- Generation date
- Previous snapshot date used as the comparison baseline
- Number of pages checked
- Number of pages changed since the previous snapshot
- Number of pages added since the previous snapshot
- Number of pages removed since the previous snapshot
- Added or removed text, with a link to each affected page

Access the legacy Secure Access Help change log

Provides access to the legacy Secure Access Help change log for documentation published before Secure Access Help moved to Cisco.com.

Cisco Secure Access Help has moved to Cisco.com. If you need to access the legacy change log, see https://securitydocs.cisco.com/docs/csa/changelog/170171.dita.

2 November 2026 updates

Topics:

- Cisco Secure Access Documentation Changes 2026-11-02

Lists the Secure Access Help updates published during November 2026 and groups them by dated change-log entry.

Cisco Secure Access Documentation Changes 2026-11-02

Lists changes to Cisco Secure Access documentation published on November 2, 2026.

Summary

- Document URL: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html
- Snapshot date: 2026-11-02
- Pages checked: 466
- Pages changed: 48
- Pages added: 2
- Pages removed: 0

Changed Pages

Limitations and range limits

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/introduction-secure-access-intro/limitations_and_range_limits.html

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

Endpoint Data Center Selection

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/introduction-secure-access-intro/Endpoint_Data_Center_Selection.html

- Removed: It uses the public IP of the client (embedded in EDNS Client Subnet data) as well as the org ID (implicitly looked up via network registration, or gathered explicitly if embedded in the FQDN).
- Removed: For geolocation, a dynamic lookup is performed against IP-to-location services to detect the source country of the user.
- Removed: You can ues GeoLB to apply the following:
- Added: You can use GeoLB to apply the following:
- Removed: Country Ring-fencing: Keeping user traffic within national borders or preferred neighboring countries where possible.
- Removed: Note This is a best-effort feature, and subject to the accuracy of the geolocation of the public IP of the client.

Security Insights Dashboard

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/dashboards-overview-intro/security-insights-dashboard.html

- Removed: Threat
- Added: Threats
- Added: Set Background Theme
- Added: Set the user interface theme to light theme, dark theme, or to adopt the theme your browser uses.

- Removed: Threat Tab
- Removed: The Threat tab of the Security Insights dashboard helps you identify where Secure Access blocks threats, where policy allows threats, and which rules, destinations, categories, or users require follow-up.
- Added: Threats Tab
- Added: The Threats tab of the Security Insights dashboard helps you identify where Secure Access blocks threats, where policy allows threats, and which rules, destinations, categories, or users require follow-up.
- Added: Set Background Theme
- Added: This procedure describes how to set the user interface theme of Secure Access to light theme, dark theme, or to adopt the theme your browser uses.
- Added: Most integrated products and platform pages in Secure Access use the theme you set.
- Added: Procedure
- Added: From the home page of Security Cloud Control or any integrated product page, click the user menu and select Edit user settings
- Added: In the System settings area, choose from:
- Added: Light theme
- Added: Dark theme
- Added: System theme - The system theme adopts the theme your browser uses.
- Added: Here is an example of Security Cloud Control using the dark theme:

Routing Options and Guidelines for Network Tunnel Groups

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/manage-network-infrastructure-intro/routing-options-and-guidelines.html

- Added: BGP route filtering per network tunnel group
- Added: BGP route filtering per network tunnel group (NTG) is a Cisco Secure Access feature that enables administrators to control, from the cloud and client, which routes are accepted from or advertised to each BGP-enabled NTG.
- Added: This allows for granular security, compliance, and optimization without editing filters on individual branch devices.
- Added: By default, Cisco Secure Access advertises all known routes to all BGP-enabled NTGs and accepts all prefixes from branch peers.
- Added: This can lead to excessive routing table entries, security risks, and operational complexity.
- Added: Route filtering per NTG solves these problems by allowing centralized, per-peer control over which IP prefixes are accepted or advertised, using simple cloud-based configuration.
- Added: Benefits
- Added: Centralizes control with a single interface for route filtering across multiple NTGs.
- Added: Reduces operational overhead by eliminating per-device BGP filter management.
- Added: Improves security and compliance by isolating sensitive or rogue routes.
- Added: Optimizes routing behavior and network performance by selective advertisement.
- Added: Sample use cases
- Added: Some of the use cases for the route filtering feature include:

- Added: Selective advertisement: Only advertise necessary routes to certain branches.
- Added: Partner route protection: Prevent overlap or rogue routes from external partners.
- Added: Region-based segmentation: Restrict route propagation to NTGs in a specific geography.
- Added: Compliance assurance: Ensure sensitive subnets are never advertised to unauthorized branches.
- Added: Types of route filtering
- Added: Filtering can be applied in two directions:
- Added: Client or Ingress filtering: controls which routes received from branches are accepted into Secure Access.
- Added: Cloud or Egress filtering: controls which routes Secure Access advertises to branch devices.
- Added: Filter modes
- Added: Equal to: Filters only the specified prefix match.
- Added: For example, 10.10.5.0/24.
- Added: Less than: Filters the specified prefix and any sub-prefixes under it.
- Added: For example, /24 rule applies also to /25, and /26 within that /24 subnet.
- Added: BGP route filter parameters and limits
- Added: This section lists the parameters, match options, limits, and supported values for BGP route filters per network tunnel group in Cisco Secure Access.
- Added: Table 4.
- Added: Route filter parameters
- Added: Parameter
- Added: Description
- Added: Allowed Values
- Added: Default
- Added: Direction
- Added: Filter direction: ingress (client) or egress (cloud)
- Added: ingress, egress
- Added: -
- Added: Prefix/Subnet
- Added: IP prefix in CIDR notation to filter
- Added: IPv4 or IPv6 prefix
- Added: For example, 10.10.5.0/24
- Added: -
- Added: Match Mode
- Added: How the prefix is matched
- Added: Equal to
- Added: Less than

- Added: Equal to
- Added: Action
- Added: Permit (allow) or deny (block)
- Added: Allow, Deny
- Added: Depends on the direction
- Added: Target NTGs
- Added: One or more NTGs by name where the filter needs to be applied
- Added: Multi-select
- Added: -
- Added: Table 5.
- Added: Route filter limits
- Added: Limit
- Added: Value
- Added: Maximum filters per organization
- Added: 1000
- Added: Bulk action limit
- Added: Up to 5 per operation
- Added: Supported tunnel types
- Added: BGP-enabled NTGs only
- Added: Propagation Delay
- Added: 1 – 2 minutes
- Added: This is the time for a new filter to take effect.
- Added: Restrictions for BGP route filtering per NTG
- Added: You cannot configure the BGP route filtering feature on static NTGs, and on NTGs with multi-region backhaul (MRB) enabled.
- Added: Key considerations
- Added: Filtering and summarization: Plan the interaction between filters and route summarization.
- Added: Filtering is always evaluated before summarization and may prevent a summary from being advertised if all child prefixes are filters out or denied.
- Added: Allowed overlapping filters:
- Added: Overlapping filters that have different prefix length, say less than /24 and /23, where the more specific prefix takes priority.
- Added: Overlapping filters that have the same prefix length, say /24 and /24, only if there are no overlapping NTGs
- Added: Filter modification: You can modify the filter action while editing the rule.
- Added: You cannot change the filter from client filter to cloud filter or the other way around by editing.
- Added: Review the impact of filter changes using the per-NTG and global route tables before and after deployment.

- Added: Configure BGP route filters per NTG
- Added: Use this procedure to configure BGP route filters per NTG to control which routes are accepted from or advertised to BGP peers.
- Added: Before you begin
- Added: Ensure you have at least one BGP-enabled NTG in Cisco Secure Access.
- Added: Verify that you have sufficient privileges to modify Traffic Management and route filters.
- Added: Decide which prefixes, and match modes you want to allow or deny.
- Added: Procedure
- Added: Navigate to Connect> Traffic Management> Route Filters in the Secure Access UI.
- Added: Choose the filter type:
- Added: Choose Client filters for ingress filters that control which routes are accepted from the branch.
- Added: They support both allow and deny filter actions.
- Added: Choose Cloud filters for egress filters that control which routes are advertised to the branch.
- Added: They support only deny filter action.
- Added: Click Add Filter.
- Added: A side panel Add client filter or Add cloud filter opens.
- Added: Figure 1.
- Added: Add client filter panel
- Added: Enter a filter name.
- Added: Specify the Subnet/Prefix.
- Added: Enter the prefix in CIDR notation.
- Added: For example, 10.10.5.0/24.
- Added: Select a match mode: Less than or Equal to.
- Added: Set the Action as Allow or Deny.
- Added: Allow: Permits only the specified NTGs.
- Added: By default, it denies all other NTGs in this case.
- Added: Deny: Blocks only the specified NTGs.
- Added: By default, it allows all other NTGs in this case.
- Added: Select the target NTGs by name.
- Added: You can select multiple NTGs.
- Added: Review your settings.
- Added: Click Save.
- Added: (Optional) Apply a bulk action.
- Added: You can select up to five filters and choose Change Action or Delete.
- Added: (Optional) Apart from the steps listed above, you can also apply route filters while creating a new NTG.

- Added: Navigate to Secure Access> Connections> Network Connections> Network Tunnel Groups> Add a Network Tunnel Group to create a new NTG.
- Added: In the Route Filters section, select the subnets to be filtered.
- Added: Select the filter actions to be applied.
- Added: Click Save.
- Added: Verify BGP route filtering configuration
- Added: Procedure
- Added: Navigate to Connect> Traffic Management> Route Filters> Client Filters> or> Cloud Filters to check the filter status after adding a new filter.
- Added: The table lists the newly created filter.
- Added: Hover over the respective subnet entry for the filter to view the status.
- Added: The initial status shows as In Progress, Filter is being created.
- Added: At this stage, you cannot edit the filter.
- Added: You can either delete the filter or view the details.
- Added: Click on the ellipses (…) on the right corner of the filter table to perform these actions, if required.
- Added: After a few minutes, the filter status finally changes to Active when all the NTGs have the rule configured.
- Added: Click on the respective filter subnet listed in the Route Filters table to view the route filter information and filter action details.
- Added: Figure 2.
- Added: Route filter details
- Added: View Network Tunnel Group Details to check the pre- and post-filter route count for client or cloud routes.
- Added: Navigate to Secure Access> Connections> Network Tunnel Groups> <NTG-name>> Routing> Client Routes> or> Cloud Routes to verify if the intended prefixes are shown as allowed or denied in the route table per NTG.
- Added: Verify that the denied routes do not appear in the client or cloud route tables accordingly.
- Added: Use the audit and log features to verify filter propagation, especially after bulk changes or when route counts are unexpectedly low.

Configure Tunnels with Cisco Catalyst SD-WAN

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccess-Help/network-tunnels-by-device-info/configure-tunnels-with-cisco-catalyst-sd-wan.html

- Removed: Under SIG Provider select Device Types, click the Genric radio button.
- Added: Under SIG Provider select Device Types, click the Generic radio button.
- Removed: In the API url endpoint, enter the API URL for the SIG endpoint of the tunnel.
- Added: In the API URL endpoint, enter the API URL for the SIG endpoint of the tunnel.
- Removed: IKE ID for local End point: Tuneel Group ID on SSE page.
- Added: IKE ID for local End point: Tunnel Group ID on SSE page.

Configure Automatic Tunnels with Catalyst SD-WAN

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccess-Help/network-tunnels-by-device-into/configure_automatic_tunnels_with_catalyst_sd-wan_overview.html

- Removed: Comand Line Interface (CLI) Commands
- Added: Command Line Interface (CLI) Commands

Manage Resource Connectors and Connector Groups

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccess-Help/resource-connectors-groups-into/manage_resource_connectors_and_connector_groups.html

- Added: Standard_D4as_v5 (4 vCPU, 16 GiB)
- Removed: Note: For Disks, Networking, Management, Monitoring, and Tags, you can modify the settings for you cloud environment or keep the default selections.
- Added: Note: For Disks, Management, Monitoring, and Tags, you can modify the settings for you cloud environment or keep the default selections.
- Added: Click the Networking tab and check the Enable accelerated networking checkbox.
- Added: This supports the Standard_D4as_v5 instance type.
- Added: Note: Enable Accelerated Networking on the connector VM's network interface.
- Added: In the Azure portal, select Enable accelerated networking on the Networking tab when you create the VM.
- Added: Accelerated Networking improves network throughput and reduces CPU load on the connector.
- Added: To enable it on an existing connector VM use the following steps:
- Added: Stop the VM so that its status is Stopped.
- Added: Restarting the VM is not enough.
- Added: Open the VM's network interface, then enable Accelerated networking.
- Added: Start the VM.
- Added: You can confirm the setting with the Azure CLI: az network nic show -g -n --query enableAcceleratedNetworking.
- Added: The output is true when Accelerated Networking is enabled.

Troubleshoot Resource Connectors and Connector Groups

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccess-Help/resource-connectors-groups-into/troubleshoot_resource_connectors_and_connector_groups.html

- Added: Note: If you are using Standard_D4as_v5 instance type and intend to enable Accelerated Networking, rebooting does not push changes.
- Added: Enable Accelerated Networking on the connector VM's network interface.
- Added: In the Azure portal, select Enable accelerated networking on the Networking tab when you create the VM.
- Added: Accelerated Networking improves network throughput and reduces CPU load on the connector.
- Added: To enable it on an existing connector VM:
- Added: Stop the VM so that its status is Stopped.
- Added: Restarting the VM is not enough.
- Added: Open the VM's network interface, then enable Accelerated networking.

- Added: Start the VM.
- Added: You can confirm the setting with the Azure CLI: az network nic show -g <resource-group> -n <nic-name> --query enableAcceleratedNetworking.
- Added: The output is true when Accelerated Networking is enabled.

About Key Admin API Keys

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/manage-api-keys-intro/add_keyadmin_api_keys.html

- Removed: In the dialog window, click Delete to confim the removal of the Key Admin API key.
- Added: In the dialog window, click Delete to confirm the removal of the Key Admin API key.

Manage User Authentication Profiles

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/user-auth-profiles-intro/manage_user_authentication_profiles.html

- Removed: Note When you add the Cisco User Management Connector application to your IdP, the connector app only suppports SAML.
- Added: Note When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML.

Configure Integrations with SAML Identity Providers

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saml-identity-providers-intro/configure_integrations_with_saml_identity_providers.html

- Removed: SAML transfers data between the identity provider and the sevice provider; authentication is required to protect both the user's identity and the user's access to resources through single sign-on actions.
- Added: SAML transfers data between the identity provider and the service provider; authentication is required to protect both the user's identity and the user's access to resources through single sign-on actions.
- Removed: If applicable, add IdP metdata to Secure Access.
- Added: If applicable, add IdP metadata to Secure Access.
- Removed: To reconfigure SAML in Secure Accss, upload IdP metadata containing at least one public key.
- Added: To reconfigure SAML in Secure Access, upload IdP metadata containing at least one public key.
- Removed: Without SAML 2.0 the serice provider does not verify incoming SAML responses are signed with the configured IdP and this can open your environment to malicious attacks.
- Added: Without SAML 2.0 the service provider does not verify incoming SAML responses are signed with the configured IdP and this can open your environment to malicious attacks.

Configure Microsoft Entra ID for SAML

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saml-identity-providers-intro/configure_microsoft_entra_id_for_saml.html

- Removed: Note When you add the Cisco User Management Connector application to your IdP, the connector app only suppports SAML.
- Added: Note When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML.

Configure Okta for SAML

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saml-identity-providers-intro/configure_okta_for_saml.html

- Removed: Note When you add the Cisco User Management Connector application to your IdP, the connector app only suppports SAML.
- Added: Note When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML.

Configure AD FS for SAML

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saml-identity-providers-intro/configure_ad_fs_for_saml.html

- Removed: Note When you add the Cisco User Management Connector application to your IdP, the connector app only suppports SAML.
- Added: Note When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML.

Configure Duo Security for SAML

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saml-identity-providers-intro/configure_duo_security_for_saml.html

- Removed: Note When you add the Cisco User Management Connector application to your IdP, the connector app only suppports SAML.
- Added: Note When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML.

Configure Ping Identity for SAML

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saml-identity-providers-intro/configure_ping_identity_for_saml.html

- Removed: Note When you add the Cisco User Management Connector application to your IdP, the connector app only suppports SAML.
- Added: Note When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML.

Configure OpenAM for SAML

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saml-identity-providers-intro/configure_openam_for_saml.html

- Removed: Note When you add the Cisco User Management Connector application to your IdP, the connector app only suppports SAML.
- Added: Note When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML.

Manage Global Settings for Access Rules

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/access-policies-intro/manage_global_settings_for_access_rules.html

- Added: Disable Decryption for Specific sources
- Added: Configure Decryption for Specific Sources
- Added: To exclude specific internet traffic from decryption, add source IP addresses or Classless Inter-Domain Routing (CIDR) blocks.

- Added: This setting applies to internet access rules.
- Added: Before you begin
- Added: You must have Full Admin user role.
- Added: For more information, see Manage Accounts.
- Added: Procedure
- Added: Click Rule Defaults and Global Settings, and then select the Global Settings tab.
- Added: Under Disable decryption for specific sources, click Add/edit sources.
- Added: In the Disable decryption for specific sources panel, enter the source IP addresses or CIDR blocks in the Add sources field.
- Added: Click + Add.
- Added: The source count updates and the added sources appear in the list.
- Added: (Optional) In the Search sources field, enter an IP address or CIDR block to filter the list.
- Added: (Optional) To modify an existing entry, click the Edit (pencil) icon next to the source.
- Added: (Optional) To remove a source, click the Delete (trash can) icon next to the source.

Manage Destination Lists

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-saas-resource-intro/manage_destination_lists.html

- Removed: Click Canel if you want the destination list to remain.
- Added: Click Cancel if you want the destination list to remain.

Manage Content Category Lists

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-saas-resource-intro/manage-content-categories.html

- Removed: Use the followng procedure to permanently delete a content category list from your organization.
- Added: Use the following procedure to permanently delete a content category list from your organization.

Troubleshoot Private Access Rules

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/private-access-rules-intro/troubleshoot_private_access_rules.html

- Added: Use Events to investigate browser-based ZTA connections.

Manage IPS Profiles

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/ips-profiles-intro/manage_ips_profiles.html

- Removed: Click Add and enter a name for your custom signature list and choose either Detection or Prevention for Intrusion System Mode.
- Added: Click + IPS Profile and enter a name for your custom signature list and choose either Detection or Prevention for Intrusion System Mode.

Manage Client-Based Zero Trust Access in Secure Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/zero-trust-access-intro/manage-client-based-zta-overview.html

- Removed: Note: While you can sustain multiple site environments note that having duplicate destinations assocaited with a resource connector may affect mobile functionality with Secure Private Access.
- Added: Note: While you can sustain multiple site environments note that having duplicate destinations associated with a resource connector may affect mobile functionality with Secure Private Access.
- Removed: Block HTTPS Pages with Zero Trust Access
- Added: Block Experience with ZTA
- Added: Default Block Action
- Added: ZTA blocks traffic through a combination of traffic steering, rules attributed to the access policy, and enforcement modes.
- Added: Where traffic steering and interception determines if ZTA should handle a traffic request before the request is authorized, either by a destination match or exclusion configured as part of your traffic steering, the access policy evaluates if traffic should be permitted post-interception based on explicit rules, matching criteria in rules, or specific rule order.
- Added: Intercepted traffic that doesn't explicitly match any custom access policy rules is default blocked by the system policy.
- Added: This specific case triggers a ZTA remediation flow to evaluate and identify the reason for denied access.
- Added: If this occurs for multiple requests simultaneously, the system can experience overwhelming load due to the expensive nature of the remediation flow.
- Added: In such a scenario, remediation is throttled at an organization level during this increased window and a generic Access was blocked by the default rule block reason is reported in the Activity Search logs.
- Added: Block Enforcement Pages
- Removed: 5 minutes
- Added: 1 minute
- Added: General policy and posture based blocks
- Added: 30 seconds
- Added: Process
- Removed: MDM Enrollment
- Added: Certificate Enrollment
- Added: Android
- Added: ChromeOS
- Added: For more information about MDM enrollment and recommended configuration guidelines, see Configure iOS Settings in Mobile Device Manager (MDM)and Configure Android Settings in MDM respectively.
- Added: Traffic Steering: Secure Internet Access for all internet destinations
- Added: iOS
- Added: Android
- Added: ChromeOS
- Added: iOS 26.5
- Added: Note: Trusted server probes do not support certificate hash checks; only the first probe URL is used.
- Added: Trusted Network Detection (Secure Internet Access and Secure Private Access)

- Added: iOS
- Added: Android
- Added: ChromeOS
- Added: All versions.
- Added: Note iOS does not support virtual interface detection, and multiple interface evaluation matches network fingerprint rules against a single OS-preferred adapter.
- Added: Pause ZTA with Cisco Secure Client
- Added: Android
- Added: ChromeOS
- Added: All versions.
- Added: Note: For information on known issues in Client compatibility see the Secure Client Release Notes.

Manage Zero Trust Access Posture Profiles

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/zero-trust-access-intro/manage_zero_trust_access_posture_profiles.html

- Removed: Module name—The name of the posture profile integration for broswer used.
- Added: Module name—The name of the posture profile integration for browser used.

Manage Endpoint Security

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/endpoint-security-intro/manage_endpoint_security.html

- Added: Note Edge for Business Posture enforcement checks are only applicable for clients connecting from clients running Windows OS due to restrictions by the MS Edge for Business Connector.

Deploy VAs in Hyper-V for Windows 2012 or Higher

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_hyper-v_for_windows_2012_or_higher.html

- Removed: The two files, dynamic and forwarder-va. must be renamed per the VA that is being installed.
- Added: The two files, dynamic and forwarder-va must be renamed per the VA that is being installed.

Deploy VAs in KVM

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_kvm.html

- Removed: To successfully deploy a virtual appliance in a KVM envinronment, follow the steps as they are listed below:
- Added: To successfully deploy a virtual appliance in a KVM environment, follow the steps as they are listed below:

Deploy VAs in Alibaba Cloud

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_alibaba_cloud.html

- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Added: Note: You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Added: A VA running version 3.6.1 or above.

Manage Notification Pages

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/notification-pages-intro/manage_notification_pages.html

- Removed: Note: You can allow users to directly contact their administrators by enabling Allow blocked users to contact an adminstrator.
- Added: Note: You can allow users to directly contact their administrators by enabling Allow blocked users to contact an administrator.

Manage the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/manage-data-protection-policies.html

- Removed: text/plain
- Added: text/plain**
- Removed: text/plain
- Added: text/plain**
- Added: ** Plain text files, such as plain text.txt and UNIX_SCRIPT, as well as JSON files, are not supported when the file type is used as the only matching criterion.
- Added: They are supported only when combined with other matching criteria.

Add a SaaS API Rule to the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/add-a-saas-api-rule.html

- Removed: For the next step in the process, see Create a DLP SaaS API Rule Step 3 – Select Files Controls
- Added: For the next step in the process, see Create a DLP SaaS API Rule Step 3 – Select Platform and Tenant
- Removed: Create a DLP SaaS API Rule Step 3 – Select Files Controls
- Removed: This is the third step in the process to add a SaaS API rule to a DLP policy, in which you select the files controls to apply to the rule.
- Added: Create a DLP SaaS API Rule Step 3 – Select Platform and Tenant
- Added: This is the third step in the process to add a SaaS API rule to a DLP policy, in which you select one platform and tenant for the rule.
- Removed: For the next step in the process, see Create a DLP SaaS API Rule Step 4 – Select Platform and Tenant
- Added: For the next step in the process, see Create a DLP SaaS API Rule Step 4 – Select Files Controls
- Added: Create a DLP SaaS API Rule Step 4 – Select Files Controls
- Added: This is the fourth step in the process to add a SaaS API rule to a DLP policy, in which you select the files controls to apply to the rule.
- Added: For the previous step in the process, see Create a DLP SaaS API Rule Step 3 – Select Platform and Tenant
- Removed: Create a DLP SaaS API Rule Step 4 – Select Platform and Tenant
- Removed: This is the fourth step in the process to add a SaaS API rule to a DLP policy, in which you select one platform and tenant for the rule.
- Removed: For the previous step in the process, see Create a DLP SaaS API Rule Step 3 – Select Files Controls
- Removed: For the previous step in the process, see Create a DLP SaaS API Rule Step 4 – Select Platform and Tenant

- Added: For the previous step in the process, see Create a DLP SaaS API Rule Step 4 – Select Files Controls

Add an AI Guardrails Rule to the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/add_an_ai_guardrails_rule_to_the_data_loss_prevention_policy.html

- Removed: For each application you can scan one of three traffic options: Prompt (from your system to the AI application), Response (from the AI application to your system), or Prompt & Response.
- Added: For each application (except Microsoft Copilot), you can scan one of three traffic options: Prompt (from your system to the AI application), Response (from the AI application to your system), or Prompt & Response.
- Added: Tip: At this time, Microsoft Copilot is only supported in the Prompt direction.

Discovery Scan

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/discovery_scan.html

- Removed: Note that the cancelation of a scan might take a few minutes.
- Added: Note that the cancellation of a scan might take a few minutes.

SaaS API Data Loss Prevention

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saas-api-data-loss-prevention-intro.html

- Added: Enable SaaS API Data Loss Prevention for GitHub Tenants
- Added: Explains how SaaS API Data Loss Prevention (DLP) policies are applied to GitHub tenants to identify and protect sensitive data by scanning various content types.

Cloud Malware Protection

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/cloud-malware-protection-intro.html

- Removed: Enable Cloud Malware Protection
- Removed: Provides instructions for completing the Enable Cloud Malware Protection workflow in Cisco Secure Access.
- Removed: It explains the sequence of actions and relevant settings presented in the procedure.
- Removed: Revoke Authorization for a Platform
- Removed: Provides instructions for completing the Revoke Authorization for a Platform workflow in Cisco Secure Access.
- Removed: It explains the sequence of actions and relevant settings presented in the procedure.
- Added: Enable Cloud Malware Protection for GitHub Tenants
- Added: Configure cloud malware protection for GitHub to monitor repository files for security threats and ensure compliance.
- Removed: Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants
- Removed: Describes Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants in Cisco Secure Access and explains Limitations.
- Removed: It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Manage Cloud Malware Protection

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/cloud-malware-protection-intro/manage_cloud_malware_protection.html

- Removed: The system will remove all collaborators and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permisson set for the quarantine app.
- Added: The system will remove all collaborators and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permission set for the quarantine app.
- Added: Enable Cloud Malware Protection
- Added: Enable Cloud Malware Protection so that Secure Access scans your environment's cloud platforms for malicious files and any other risks.
- Added: When Cloud Malware Protection finds malicious files, the information is presented in the Cloud Malware Report.
- Added: Before you begin
- Added: Full Admin user role.
- Added: For more information, see Manage Accounts.
- Added: Procedure
- Added: Navigate to Admin> Authentication.
- Added: In the Platforms section, expand a platform.
- Added: Click Authorize New Instance to add an instance of this platform to your Secure Access environment.
- Added: You can authorize more than one instance of the same platform.
- Added: What to do next
- Added: Secure Access redirects you to the platform's OAuth login page.
- Added: Follow the instructions for the platform that you selected to authorize access to Secure Access:
- Added: AWS S3
- Added: Azure Storage
- Added: Box
- Added: Confluence
- Added: Dropbox
- Added: Google
- Added: Jira
- Added: Microsoft 365
- Added: Salesforce
- Added: ServiceNow
- Added: Slack
- Added: Webex Teams
- Added: Revoke Authorization for a Platform
- Added: After authorizing a platform in your Secure Access environment, you can revoke authorization at any time.

- Added: Before you begin
- Added: Full Admin user role.
- Added: For more information, see Manage Accounts.
- Added: Procedure
- Added: Navigate to Admin> Authentication.
- Added: Under Platforms, click the platform that you wish to revoke.
- Added: Choose the instance to revoke and click Revoke.
- Added: Click Revoke again to complete the process.

Enable Cloud Access Security Broker Features for Google Drive

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccess-Help/cloud-malware-protection-intro/enable_cloud_access_security_broker_features_for_google_drive.html

- Added: Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants
- Added: Secure Access supports two Cloud Access Security Broker (CASB) features for Microsoft 365:
- Added: Cloud Malware protection for OneDrive, SharePoint Online, and Outlook sites within your Microsoft 365 deployment.
- Added: Note on running both Microsoft 365 and Cloud Malware: Microsoft 365 and Cloud Malware both protect users against malware.
- Added: However, their functionalities are not redundant.
- Added: Microsoft 365 might discover malware that Cloud Malware does not find.
- Added: Cloud Malware also finds malware that Microsoft 365 overlooks.
- Added: There is value to running Microsoft 365 and Cloud Malware simultaneously.
- Added: CASB detection of third-party cloud applications that have been granted OAuth-based permission to access a user's protected resources on Microsoft 365 Sharepoint Online and OneDrive.
- Added: For more information, see Third-Party Apps Report.
- Added: You can enable CASB features for authorized tenants that use the following Microsoft 365 applications:
- Added: Sharepoint Online
- Added: OneDrive
- Added: Outlook (For Cloud Malware protection only and for the primary inbox only.
- Added: For outgoing mail you can enable Data Loss Prevention; see Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants.)
- Added: Note You cannot add an application to an existing tenant.
- Added: If you have an existing Microsoft 365 tenant that uses one or two of these applications and you wish to add another application to that tenant, you must first revoke authorization for the existing tenant, then create a new tenant using all the desired applications.
- Added: Limitations
- Added: A tenant the fails to authenticate cannot be deleted.
- Added: Secure Access Cloud Malware attempts to quarantine a file will fail if that file has been locked by Microsoft 365.

- Added: This may occur if Microsoft 365 Advanced Threat Protection (ATP) has detected malware in the file.
- Added: In such a case, the lock placed by ATP take precedence over Umbrella's ability to detect or remediate DLP violations in malware.
- Added: Prerequisites for Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants
- Added: Full Admin user role.
- Added: For more information, see Manage Accounts.
- Added: Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Added: The user performing the installation must use a service account with a Microsoft 365 Global Admin and active license
- Added: Audit log must be enabled for Microsoft 365.
- Added: For more information, refer to Microsoft Technical documentation and search for Turn auditing on or off.
- Added: Sharepoint Online and OneDrive must be enabled for the organization.
- Added: The following IP addresses must be allowed if there are Firewall rules that prevent third-party applications:
- Added: 146.112.161.0/24
- Added: 146.112.163.0/24
- Added: 146.112.165.0/24
- Added: 146.112.167.0/24
- Added: Users must have the following API permissions for Microsoft:
- Added: API/ Permissions Name
- Added: Type
- Added: Description
- Added: Admin Consent Required
- Added: Microsoft Graph
- Added: 1.
- Added: Directory.AccessAsUser.All
- Added: Delegated
- Added: Access directory as the signed-in user
- Added: Yes
- Added: 2.
- Added: Directory.Read.All
- Added: Application
- Added: Read directory data
- Added: Yes
- Added: 3.
- Added: Files.Read.All

- Added: Delegated
- Added: Read all files that user can access
- Added: No
- Added: 4.
- Added: Files.Read.All
- Added: Application
- Added: Read files in all site collections
- Added: Yes
- Added: 5.
- Added: Sites.Read.All
- Added: Delegated
- Added: Read items in all site collections
- Added: No
- Added: 6.
- Added: User.Read
- Added: Delegated
- Added: Sign in and read user profile
- Added: No
- Added: 7.
- Added: User.Read.All
- Added: Application
- Added: Read all users' full profiles
- Added: Yes
- Added: Microsoft 365 Management APIs
- Added: 1.
- Added: ActivityFeed.Read
- Added: Application
- Added: Read activity data for the Organization
- Added: Yes
- Added: SharePoint
- Added: 1.
- Added: Site.FullControl.All
- Added: Application
- Added: Full control of all site collections
- Added: Yes

- Added: 2.
- Added: User.Read.All
- Added: Application
- Added: Read user profiles
- Added: Yes
- Added: Authorize a Tenant
- Added: Procedure
- Added: Navigate to Admin> Authentication.
- Added: Click to expand Microsoft 365 in the list of Platforms.
- Added: Click Authorize New Tenant in the Cloud Access Security Broker subsection to add a Microsoft 365 tenant to your Secure Access environment.
- Added: Check the boxes to confirm that you meet all three Authentication Requirements in the Microsoft 365 Authorization Prerequisites dialog, then click Next.
- Added: Create a name for your tenant, then click Next.
- Added: Select one or both Cloud Access Security Broker (CASB) features to authenticate: Cloud Malware and Third-Party Apps.
- Added: If you choose to authorize for Cloud Malware protection, you must also select a Response Action for Umbrella to apply to Microsoft 365 files found with malware.
- Added: Choose Monitor to cause Umbrella to log files detected with malware.
- Added: You will be able to manually quarantine these files from the Cloud Malware report.
- Added: Choose Quarantine to:
- Added: Move the file into a folder named Cisco_Quarantine_Malware in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Microsoft 365 admin.
- Added: Replace the file in its original location with a text file named filename.ppt_Cisco_Quarantined.txt explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.
- Added: Note: If you choose Quarantine this will apply only to rules applied to Sharepoint and OneDrive; Secure Access Cloud Malware supports monitoring Outlook messages in the primary inbox, but cannot quarantine them.
- Added: For more information on Cloud Malware monitoring and quarantine features, see Manage Cloud Malware Protection.
- Added: For more information on Third-Party Apps detection features, see Third-Party Apps Report.
- Added: After making your selections, click Next.
- Added: Define the message to appear in the Tombstone File when files are quarantined.
- Added: A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report.
- Added: In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step.
- Added: You determine the contents of this tombstone file:
- Added: To Use the Default Tombstone Template:

- Added: Click Default.
- Added: To preview the content of the tombstone text, click on Preview Default Tombstone.
- Added: You can review the text, but you cannot change it.
- Added: Click CLOSE to close the preview.
- Added: To Use a Custom Tombstone Template:
- Added: Click Custom.
- Added: From the drop-down list, select an existing custom template, or choose Create new tombstone Template.
- Added: If you select an existing custom template, you can click PREVIEW AND EDIT to review and change the template.
- Added: When you choose to create or edit a custom template for for tombstone text you will see one of these two dialogs, which are almost identical:
- Added: The Edit Custom Tombstone Template includes a DELETE link which you can use to delete a custom template that is no longer needed.
- Added: You cannot delete a template that is in use by any rule.
- Added: To create a new template or change an existing template:
- Added: Enter a unique Custom Template Name.
- Added: Enter the text of the tombstone file in the Message Body text box.
- Added: The text can include the following variables, which you must enclose in braces ({}):
- Added: {eventId} - The unique identifier the system generates for the policy violation event.
- Added: {detectedTimestamp} - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
- Added: {actorName} - Name of the user whose action triggered the violation.
- Added: (The system gets this from the tenant associated with the violation.
- Added: Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- Added: {actorEmail} - Email address of the user whose action triggered the violation.
- Added: (The system gets this from the tenant associated with the violation.
- Added: Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
- Added: {fileName} - Name of the data file that triggered the violation.
- Added: {ruleName} - Name of the rule that was triggered.
- Added: {matchedClassifications} - The data classifications associated with the violation.
- Added: (See Manage Data Classifications.)
- Added: {fileOwnerName} - Name of the file owner.
- Added: (The system gets this from the tenant associated with the violation.
- Added: Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- Added: {fileOwnerEmail} - Email address of the file owner.

- Added: (The system gets this from the tenant associated with the violation.
- Added: Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- Added: {fileLocation} - The file URL.
- Added: Note The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.
- Added: Click SAVE to complete the changes.
- Added: Click Next to procede to Integration.
- Added: At the Integration step, click Next.
- Added: You are redirected to the Microsoft 365 login page.
- Added: Log into Microsoft 365 with admin credentials to authorize your Microsoft 365 account as a Secure Access CASB.
- Added: You are redirected to Secure Access, which displays a message when the authorization is complete.
- Added: It can take up to 24 hours for the CASB integration status in Secure Access to show that authorization is complete.
- Added: Click Done to complete.
- Added: Edit a Tenant
- Added: You can change the protection type or Response Action you have selected for a tenant.
- Added: Procedure
- Added: Navigate to Admin> Authentication.
- Added: Click to expand Microsoft 365 in the list of Platforms.
- Added: In the Cloud Access Security Broker subsection, from the Edit column, click Edit.
- Added: You can edit any tenant.
- Added: Choose to authorize your Microsoft 365 tenant for Cloud Malware protection, or detection of third-party cloud applications, or both.
- Added: If you choose to authorize for Cloud Malware protection, you must also select a Response Action for Umbrella to apply to Microsoft 365 files found with malware.
- Added: Choose Monitor to cause Umbrella to log files detected with malware.
- Added: You will be able to manually quarantine these files from the Cloud Malware report.
- Added: Choose Quarantine to:
- Added: Move the file into a folder named Cisco_Quarantine_Malware in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Microsoft 365 admin.
- Added: Replace the file in its original location with a text file named filename.ppt_Cisco_Quarantined.txt explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.
- Added: Note If you choose Quarantine this will apply only to rules applied to Sharepoint and OneDrive; Secure Access supports monitoring outgoing Outlook messages, but cannot quarantine them.
- Added: For more information on Cloud Malware monitoring and quarantine features, see Manage Cloud Malware Protection.

- Added: For more information on Third-Party Apps detection features, see Third-Party Apps Report.
- Added: Change the message to appear in the Tombstone File when files are quarantined.
- Added: A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report.
- Added: In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step.
- Added: You determine the contents of this tombstone file:
- Added: To Use the Default Tombstone Template:
- Added: Click Default.
- Added: To preview the content of the tombstone text, click on Preview Default Tombstone.
- Added: You can review the text, but you cannot change it.
- Added: Click CLOSE to close the preview.
- Added: To Use a Custom Tombstone Template:
- Added: Click Custom.
- Added: From the drop-down list, select an existing custom template, or choose Create new tombstone Template.
- Added: If you select an existing custom template, you can click PREVIEW AND EDIT to review and change the template.
- Added: When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:
- Added: The Edit Custom Tombstone Template includes a DELETE link which you can use to delete a custom template that is no longer needed.
- Added: You cannot delete a template that is in use by any rule.
- Added: To create a new template or change an existing template:
- Added: Enter a unique Custom Template Name.
- Added: Enter the text of the tombstone file in the Message Body text box.
- Added: The text can include the following variables, which you must enclose in braces ({}):
- Added: {eventId} - The unique identifier the system generates for the policy violation event.
- Added: {detectedTimestamp} - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
- Added: {actorName} - Name of the user whose action triggered the violation.
- Added: (The system gets this from the tenant associated with the violation.
- Added: Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- Added: {actorEmail} - Email address of the user whose action triggered the violation.
- Added: (The system gets this from the tenant associated with the violation.
- Added: Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
- Added: {fileName} - Name of the data file that triggered the violation.

- Added: {ruleName} - Name of the rule that was triggered.
- Added: {matchedClassifications} - The data classifications associated with the violation.
- Added: (See Manage Data Classifications.)
- Added: {fileOwnerName} - Name of the file owner.
- Added: (The system gets this from the tenant associated with the violation.
- Added: Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- Added: {fileOwnerEmail} - Email address of the file owner.
- Added: (The system gets this from the tenant associated with the violation.
- Added: Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- Added: {fileLocation} - The file URL.
- Added: Note The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.
- Added: Click SAVE to complete the changes.
- Added: Click Next to procede to Integration.
- Added: At the Integration step, click Next.
- Added: The new Response Action is displayed.
- Added: Note For tenants authorized only for CASB detection of third-party applications, no Response Action is shown.
- Added: Revoke Authorization
- Added: Procedure
- Added: Under Action, click Revoke.
- Added: You can revoke any authorized tenant.
- Added: Confirm to proceed.
- Added: The selected account is not authorized.

Manage Internet Security

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-security-intro/manage_internet_security.html

- Added: Internet Security Bypass Limits
- Added: When configuring domains and IP addresses in the Internet Security Bypass list, adhere to the following organization capacity limits:
- Added: List Type
- Added: Standard Limit (Default)
- Added: Extended Limit (On Request)
- Added: Internal and External Domains (Combined)
- Added: 5,000
- Added: 9,000

- Added: IP Addresses
- Added: 5,000
- Added: 9,000
- Added: Internal domains and external domains share a single combined limit per organization.
- Added: By default, you can configure up to 5,000 total domains.
- Added: If your organization requires additional capacity (up to 9,000 domains), contact your Cisco representative or Cisco Support to request an increase.
- Added: Caution: While organizations with extended limits can configure up to 9,000 domain entries, deploying very large bypass lists to roaming devices running Cisco Secure Client increases local memory usage and configuration payload size.
- Added: For optimal client performance and stability, keep active domain entries consolidated.
- Removed: Third Party VPN compatibility
- Added: Third Party VPN Compatibility
- Removed: This setting requires that you have the Trusted Network Detection (TND) setting enabled in the AnyConnect virutal private network (VPN) profile for the user devices.
- Added: This setting requires that you have the Trusted Network Detection (TND) setting enabled in the AnyConnect virtual private network (VPN) profile for the user devices.

Manage CA Certificates for VPN Connections and Zero Trust Access Enrollment

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/certificates-into/manage_ca_certificates_for_vpn_connections_and_zero_trust_access_enrollment.html

- Removed: The location where you can check the revocation of the certifcate.
- Added: The location where you can check the revocation of the certificate.

Set up the Zero Trust Access App for iOS Devices

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/client-based-za-mobile-into/set_up_the_zero_trust_access_app_for_ios_devices.html

- Removed: Configure iOS Settings in MDM
- Removed: We strongly recommend configuring the following settings in your Mobile Device Manager (MDM) to support the full range of functionality and features that Secure Access has to offer.
- Removed: For information on how to implement these changes in your particular MDM, consult your MDM documentation.
- Added: Configure iOS Settings in Mobile Device Manager (MDM)
- Added: At this time, Apple iOS 5.1.19 supports certificate-based zero touch enrollment through the ManagedApp tool.
- Added: Administrators can use a compatible EMM solution with Declarative Device Management (DDM) support for managed applications to provision the enrollment choice configuration and enrollment certificate identity to ZTA.
- Added: For more information specifically on Apple managed apps, search for "Apple's guidance for configuring managed apps".
- Added: Use the following configurations for certificate-based zero touch enrollment:
- Added: The device runs iOS 18.4 or later, which supports the ManagedApp configuration and credential delivery used by this feature.

- Added: ZTA 5.1.19 or later is deployed as a managed app.
- Added: The EMM solution supports Apple's DDM managed application configuration and credential provisioning.
- Added: General DDM support alone does not establish support for these capabilities.
- Added: A valid ZTA enrollment choice file is configured for certificate-based enrollment, and a certificate identity matching its certificate selection requirements is available.
- Added: Using the EMM solution, provision the certificate identity and enrollment choice configuration to the managed ZTA app.
- Added: A certificate identity includes the certificate and its associated private key.

Download the OrgInfo.json File

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/secure-client-windows-mac-linux-intro/procedure_1753019861337_6546.html

- Removed: Copy your OrgInfo.json file to either the location of the Cisco Secure Client install directory or the Profiles\\secureaccess directory on the local system.
- Removed: When you deploy the OrgInfo.json file for the first time, the Cisco Secure Client copies the OrgInfo.json file to the data subdirectory (/secureaccess/data), which also contains several registration files.
- Added: Copy your OrgInfo.json file to either the location of the Cisco Secure Client install directory or the Profiles\\umbrella directory on the local system.
- Added: When you deploy the OrgInfo.json file for the first time, the Cisco Secure Client copies the OrgInfo.json file to the data subdirectory (/umbrella/data), which also contains several registration files.
- Removed: %ProgramData%\\Cisco\\Cisco Secure Client\\SecureAccess
- Added: %ProgramData%\\Cisco\\Cisco Secure Client\\Umbrella
- Removed: Alternatively, before installing the Cisco Secure Client, copy the OrgInfo.json file to \\Profiles\\secureaccess.
- Removed: The Secure Access module installer is located in \\Profiles\\secureacces.
- Added: Alternatively, before installing the Cisco Secure Client, copy the OrgInfo.json file to \\Profiles\\Umbrella.
- Added: The Secure Access module installer is located in \\Profiles\\Umbrella.
- Removed: /opt/cisco/secureclient/secureaccess/
- Added: /opt/cisco/secureclient/umbrella/

Manage Internet Security on Cisco Secure Client

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-security-secure-client-intro/manage-cisco-secure-client-internet-security.html

- Added: Internet Security Bypass Sizing: Cisco Secure Access supports up to 5,000 combined domain entries (and up to 9,000 entries upon request to your Cisco representative or Cisco Support).
- Added: While large lists are supported, maintaining consolidated domain lists is recommended for optimal performance and reduced memory utilization on roaming devices running Cisco Secure Client.
- Added: For more information, see Manage Internet Security Bypass.
- Added: The Umbrella Roaming Security Module for Cisco Secure Client is not supported on Windows Server.
- Removed: The Cisco Secure Client Umbrella Roaming Security module is not compatible with other DNS serving software.
- Removed: You should not install the Cisco Secure Client Umbrella module on a device that serves DNS requests.

- Added: The Umbrella Roaming Security Module for Cisco Secure Client is not supported on Windows Server and is incompatible with other DNS-serving software.
- Added: Do not install the module on a device that serves DNS requests.
- Added: The module's dnscryptproxy subprocess encrypts DNS traffic and listens on UDP and TCP port 53.
- Added: This port usage conflicts with the Windows DNS Server service.
- Added: The module is also generally incompatible with other software that binds to UDP or TCP port 53 on localhost, regardless of the operating system.

Manage Logging

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/logging-intro/manage_logging.html

- Added: A custom certificate is required only for logging Web DLP violation evidence to your own Amazon S3 bucket.
- Added: Endpoint DLP, Email DLP, and SaaS API DLP violation events continue to be logged to your S3 bucket without a custom certificate.
- Added: Web DLP violation evidence logging is not supported for organizations using a shared certificate (Secure Access Root Cert), due to potential security vulnerabilities.
- Added: Endpoint DLP, Email DLP, and SaaS API DLP violation events continue to be logged to your S3 bucket.

Log Formats and Versioning

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/logging-intro/log_formats_and_versioning.html

- Removed: Note: The Event Correlation ID is not used in ZTNA, as its functionality is covered by the Transaction ID field.
- Added: For a browser-based connection, the authorization, establishment, and termination records share the same Transaction ID.
- Added: In Events, use the Event ID to display these records.
- Added: Note
- Added: The Event Correlation ID is not used in ZTNA, as its functionality is covered by the Transaction ID field.
- Added: Note:
- Removed: ZTA flow logs show traffic events in client-based and browser-based ZTA sessions that take place after successful authentication.
- Added: ZTA flow logs show traffic after successful authentication for clientbased and browserbased sessions.
- Added: For browserbased access, each TCP connection has establishment and termination records.
- Added: Match Transaction IDs to correlate these records with authorization logs.
- Added: One application session can use several connections.
- Added: Use log format version 10 or later.
- Removed: "2025-10-02 23:52:53","network@example.com","network@example.com, Network.
- Removed: AD Computer","Networks","ts-auto.com","1234567","1254367","Gd2o4Dr9PBERUpOwAneaKbBqA6D4lo","45937","45873","147","56","TERMINATED","App did not respond","CLAP","129","CONN_FAILURE","453","7756","1.1.1.1","3000","256","4001","FTD","12321321312","","

- Added: "2026-08-28 12:34:56","alice@example.com","alice@example.com","managed-device-123","AD Users","Managed Devices","10001","","zta-host","vm-dc-123","999","888","777","666","555","444","TERMINATED","Timeout","CLAP","CONN_FAILURE","1024","2048","100","443","333","8080","Enforcement Point","ftd-123","FTD Device"
- Added: For browser-based flow records, the timestamp identifies establishment or termination according to Connection Status.
- Added: Termination is not necessarily application logout.
- Added: For browser-based ZTA, Connected marks establishment; Terminated marks closure.
- Added: For browserbased ZTA, final totals are available at termination.
- Added: For browser-based ZTA, final totals are available at termination.
- Removed: However, it can be found in the ZTA logs using the same transaction ID..
- Added: However, it can be found in the ZTA logs using the same transaction ID.
- Added: source ip
- Added: The source IP address of the client endpoint for the Zero Trust Access flow.
- Added: v18
- Added: destination ip
- Added: The destination IP address for the flow.
- Added: v18
- Added: application protocol
- Added: The application layer protocol used by the flow.
- Added: Example: HTTPS.
- Added: v18

Security Activity Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/activity-reports-intro/security-activity-report.html

- Added: The Security Activity report shows security activity over time and matching events in a table.
- Added: Use Search Security Activity, Event type, Response, and Filters above the chart to refine the results.

Events Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/events-report-intro/events-report-overview.html

- Removed: Status: Action taken (Allowed, Blocked, or Isolated).
- Added: Status: Action taken (Allowed, Blocked, Isolated, Connected, or Disconnected).
- Added: Browser-based authorization records are ZTA Clientless; TCP connection records are ZTA Clientless Flow.
- Added: Browser-based flows can have statuses such as Connected or Disconnected.
- Added: For browser-based events, select ZTA Clientless.
- Added: View Browser-based ZTA Flow Events
- Added: Use the Events report to investigate browser-based Zero Trust Access (ZTA) connections to a private resource.

- Added: Authorization records show the access decision.
- Added: Flow records show when an underlying TCP connection is established and terminated.
- Added: Related records share an Event ID.
- Added: An application session can use several TCP connections.
- Added: Each connection has its own lifecycle records.
- Added: Connection timestamps do not necessarily identify the times that a user signs in to or signs out of an application.
- Added: Procedure
- Added: Choose Monitor> Reports> Events.
- Added: Choose the time range to investigate, for example, Last 30 minutes.
- Added: Select ZTA Clientless.
- Added: To narrow the results, filter by the destination private resource.
- Added: Authorization records appear as ZTA Clientless.
- Added: Connection lifecycle records appear as ZTA Clientless Flow.
- Added: Click the arrow next to an event to open the Event Details card.
- Added: Review the available source, connection, security control, and destination information.
- Added: Click the Event ID value and choose Search.
- Added: Remove unrelated filters if they exclude records that you need for the investigation.
- Added: The report displays the authorization record and the related Connected and Disconnected flow records for that connection.
- Added: Compare the Time values on the matching Connected and Disconnected rows to determine when the connection was active.
- Added: Use the event row timestamps for this comparison.
- Added: The Session end time field in the detail card can be blank.
- Added: If a matching Disconnected record has not appeared, the connection might still be open.
- Added: Connected records remain in the report after their corresponding Disconnected records appear.
- Added: Note: Connections can overlap.
- Added: Do not add connection durations together to calculate the duration of an application session.
- Added: Expand the Disconnected flow record.
- Added: Under Security Controls> ZTA clientless flow, review Session Bytes Received and Session Bytes Sent.\
- Added: Final byte totals are available when the connection disconnects.
- Added: They are not available in its Connected record.
- Added: Review Reason Code in the event table or Reason in the Connection card for available closure information.
- Added: A normal closure can populate these fields.
- Added: A populated reason does not necessarily indicate a failed connection.
- Added: For example, an RDP End session action can be followed by close_event=local_close and local_close_reason=triggered_delayed_close_timeout.

- Added: Other browser connections can remain open while the application page is loaded.
- Added: Closing the browser tab can close those connections and produce close_event=remote_close.

Microsoft Edge for Business Third-Party Integration

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/secure-access-integrations-intro/ms_edge_for_business_thrid_party_integration.html

- Removed: In your Secure Access organization, view the third-party integrations configured for Microsft Edge for Business.
- Added: In your Secure Access organization, view the third-party integrations configured for Microsoft Edge for Business.
- Removed: Name—The name of the Third-party Integration for Microsft Edge for Business.
- Added: Name—The name of the Third-party Integration for Microsoft Edge for Business.
- Removed: Module name—The name of the Third-party Integration for Microsft Edge for Business.
- Added: Module name—The name of the Third-party Integration for Microsoft Edge for Business.
- Removed: Organizations can edit a Third-party Integration for Microsft Edge for Business in Secure Access.
- Added: Organizations can edit a Third-party Integration for Microsoft Edge for Business in Secure Access.

Integrate ISE (Identity Services Engine) with Secure Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/secure-access-integrations-intro/integrate-ise.html

- Removed: We strongly recommend modifying or creating a private access rule to further incorprate this successful integration.
- Removed: You can now include private IP addresss from the security group tag (SGT) originating from the ISE appliction as either the source or the destination.
- Added: We strongly recommend modifying or creating a private access rule to further incorporate this successful integration.
- Added: You can now include private IP address from the security group tag (SGT) originating from the ISE application as either the source or the destination.

Added Pages

- Enable SaaS API Data Loss Prevention for GitHub Tenants: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/saas-api-data-loss-prevention-intro/enable_saas_api_data_loss_prevention_for_github.html
- Enable Cloud Malware Protection for GitHub Tenants: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/cloud-malware-protection-intro/enable_cloud_malware_for_github.html

Removed Pages

No pages were removed.

3 October 2026 updates

Topics:

- Cisco Secure Access Documentation Changes 2026-10-26
- Cisco Secure Access Documentation Changes 2026-10-19
- Cisco Secure Access Documentation Changes 2026-10-12
- Cisco Secure Access Documentation Changes 2026-10-05

Lists the Secure Access Help updates published during October 2026 and groups them by dated change-log entry.

Cisco Secure Access Documentation Changes 2026-10-26

Lists changes to Cisco Secure Access documentation published on October 26, 2026.

Summary

- Document URL: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html
- Snapshot date: 2026-10-26
- Pages checked: 467
- Pages changed: 17
- Pages added: 1
- Pages removed: 1

Changed Pages

About this content

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html

- Removed: Network Connectivity Log
- Removed: Provides an overview of Network Connectivity Log in Cisco Secure Access, including Network Connectivity Log.
- Removed: It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.
- Added: Network Connectivity Monitoring
- Added: Provides an overview of network connectivity monitoring in Cisco Secure Access, including how to use network tunnel logs and resource connector logs to track infrastructure health, monitor state changes, and troubleshoot connectivity issues.

Security Insights Dashboard

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/dashboards-overview-intro/security-insights-dashboard.html

- Added: Failed Private Resource Access Attempts – Detect when an end user makes an unusually high number of failed attempts to access private resources through client-based ZTNA.

Manage Behaviour Analytics Configuration

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/advanced-user-config-intro/manage_behaviour_analytics_configuration.html

- Added: Note Changes to UEBA configurations appear in the Admin Audit Log.
- Added: Entries identify UEBA as the feature and the anomaly type as the component.
- Added: Update entries show the changed property and its previous and new values.
- Added: For more information, see Admin Audit Log Report.
- Removed: User activity from a city or source IP address that was not observed for that user during the previous 30 days.
- Added: User activity from a city or source IP address that is not in that user's rolling 60-day location history.

- Added: Note The system starts to generate alerts only after seven days of configuration.
- Added: Failed Private Resource Access Attempts
- Added: An unusually high number of failed attempts to access private resources.
- Added: An AI-based user baseline and a configured minimum number of failed attempts per hour.
- Added: The following table lists the traffic types that each UEBA component analyzes.
- Added: Traffic type
- Added: UEBA components
- Added: Secure Web Gateway (SWG) web traffic
- Added: File Operations; High-Risk Country File Activities; Impossible Travel; Anomalous MCP Activity; Unseen Location Activity; Traffic Spike and Destination Monitoring
- Added: DLP events
- Added: DLP Violation Spike
- Added: Client-based ZTNA traffic
- Added: Failed Private Resource Access Attempts
- Added: AD user; web traffic, ZTNA (client-based)
- Removed: Select the required file activities from the following optons:
- Added: Select the required file activities from the following options:
- Removed: UEBA supports only Secure Internet Access traffic paths and does not support Secure Private Access.
- Removed: AD user; web traffic only
- Added: Configure Analytics for Failed Private Resource Access Attempts
- Added: Failed Private Resource Access Attempts identifies an unusually high number of failed attempts to access private resources.
- Added: It analyzes client-based Zero Trust Network Access (ZTNA) traffic only.
- Added: Your organization must use client-based ZTNA to use this analytics.
- Added: Secure Access generates alerts for authentication failures and access-policy rule denials.
- Added: It does not generate alerts for DNS resolution, profile configuration, device posture, or protocol mismatch failures.
- Added: The analytics uses an AI-based user baseline.
- Added: Secure Access generates an alert when activity is anomalous for the user and meets the configured minimum threshold.
- Added: To configure Failed Private Resource Access Attempts, perform these steps:
- Added: Before you begin
- Added: Procedure
- Added: Navigate to Connect> Users, Groups, and Endpoint Devices> Configuration management> Behaviour analytics.
- Added: On the Failed Private Resource Access Attempts tile, click Edit.
- Added: Click the Status toggle to enable it.

- Added: Enter a value in Alert threshold.
- Added: Note The alert threshold acts as a minimum activity level for generating an alert.
- Added: If activity is anomalous but stays below the threshold, no alert is generated.
- Added: Note The alert threshold value is optional and can be any number between 0 and 10,000.
- Added: Click Save.
- Added: Note Secure Access can take up to seven days after you enable this analytics to generate the first alert.
- Added: It suppresses repeated alerts for the same user for 60 minutes.
- Added: What to do next
- Added: To receive notifications, create a behavior analytics alert rule for Failed Private Resource Access Attempts.
- Added: To know more, see Add and Edit Alert Rules for Behavior Analytics

Manage the Access Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/access-policies-intro/manage-access-policy.html

- Removed: For users implementing Kerberos authentication with AD, we recommend reviewing the appropriate Microsoft documentation about configuring the correct ports and private resources to plan for for AD communication. to understand how to optimize the location of a domain controller, see this documentation.
- Added: For users implementing Kerberos authentication with AD, we recommend reviewing the appropriate Microsoft documentation about configuring the correct ports and private resources to plan for for AD communication.
- Added: To understand how to optimize the location of a domain controller, see this documentation.

Rule Defaults: Default Settings for Access Rules

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/access-policies-intro/rule_defaults_default_settings_for_access_rules.html

- Added: Configure Access Rule Editing Sessions
- Added: Use the editing-session settings to control how long an administrator can lock and edit an access rule, and to determine whether they can extend the active session.
- Added: Before you begin
- Added: You must have the Full Admin user role to configure rule defaults and global settings.
- Added: For more information, see Manage Accounts.
- Added: Procedure
- Added: In the global settings panel, locate the Editing sessions.
- Added: In the Session duration section, enter the number of minutes that an access rule remains locked for an editing session before it expires.
- Added: To allow administrators to extend a session, enable the Extend session toggle button, and then enter the number of minutes to add under minutes added per extension.
- Added: Note You can extend an editing session only once.
- Added: The maximum extension duration is 40 minutes.
- Added: Click Save.

- Added: While editing a rule, the Internet Access Rule and Private Access Rule page both shows the remaining time at the top and bottom.
- Added: Click Extend session before the time expires to extend the session.
- Added: If another admin opens the rule during an active session, Secure Access displays a dashboard notification and opens the rule in preview mode.
- Added: To take over editing, click Take Over Editing, and then click Yes, take over.
- Added: This action ends the current administrator's session and discards any unsaved changes.

Add an Internet Access Rule

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-access-rules-intro/add_an_internet_access_rule.html

- Removed: Navigate to a rule, and then click on the horizontal elipsis (…) to expand the rule menu.
- Added: Navigate to a rule, and then click on the horizontal ellipsis (…) to expand the rule menu.

Manage Destination Lists

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-saas-resource-intro/manage_destination_lists.html

- Removed: Added a URL to an allow list.
- Removed: URLs in allow lists are not currently supported.
- Removed: Consider adding the domain only instead.
- Removed: Remove the URL and replace it with the domain for that URL.

Traffic Steering for Zero Trust Access Client-Based Connections

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/zero-trust-access-intro/traffic_steering_for_zero_trust_access_client-based_connections.html

- Removed: dentity workflows that depend on Kerberos service discovery while working remotely through ZTA after sign-in.
- Added: Identity workflows that depend on Kerberos service discovery while working remotely through ZTA after sign-in.
- Removed: You can configure a ZTA profile to either permenantly or temporarily pause ZTA enforcement and still utlize the traffic steering configured for a specific profile with the Enable Cisco Secure Client end user pause function.
- Added: You can configure a ZTA profile to either permanently or temporarily pause ZTA enforcement and still utilize the traffic steering configured for a specific profile with the Enable Cisco Secure Client end user pause function.
- Removed: Note You can enable the pause functionality for both Secure Private Access and Secure Internet Access indepently of each other; both of these configruable settings are available in their repsective steps when editing or creating a profile.
- Added: Note You can enable the pause functionality for both Secure Private Access and Secure Internet Access independently of each other; both of these configurable settings are available in their respective steps when editing or creating a profile.
- Removed: Check the About icon inside your Cisco Secure Client module to view the Secure Client UI verison.
- Added: Check the About icon inside your Cisco Secure Client module to view the Secure Client UI version.
- Removed: Microsoft documents specific SRV DNS records for you, see 6.3.2.3 SRV Records sepcifically for more information.

- Added: Microsoft documents specific SRV DNS records for you, see 6.3.2.3 SRV Records specifically for more information.
- Removed: For users implementing Kerberos authentication with AD, we recommend reviewing the appropriate Microsoft documentation about configuring the correct ports and private resources to plan for for AD communication. to understand how to optimize the location of a domain controller, see this documentation.
- Added: For users implementing Kerberos authentication with AD, we recommend reviewing the appropriate Microsoft documentation about configuring the correct ports and private resources to plan for for AD communication.
- Added: To understand how to optimize the location of a domain controller, see this documentation.

Get Started with Virtual Appliances

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/get_started_with_virtual_appliances.html

- Removed: Encryption is established with a probe sent on port 53 (UDP/TCP) to 208.67.220.220 and 208.67.222.222 and if you have a firewall or IPS/IDS doing deep packet inspection and expecting to see only DNS traffic, the probe may fail.
- Added: Encryption is established with a probe sent on port 53 (UDP/TCP) to the following addresses:
- Added: IPv4: 18.252.251.72 and 18.254.118.193
- Added: IPv6: 2600:1f15:ef3:1800::aaaa and 2600:1f15:ef3:1801::bbbb
- Added: If you have a firewall or IPS/IDS doing deep packet inspection and expecting to see only DNS traffic, the probe may fail.
- Removed: The VA, when deployed, will forward all externally-bound DNS requests to the Secure Access DNS resolvers, 208.67.222.222 and 208.67.220.220.
- Added: The VA, when deployed, will forward all externally-bound DNS requests to the Secure Access DNS resolvers, 18.252.251.72 and 18.254.118.193 or 2600:1f15:ef3:1800::aaaa and 2600:1f15:ef3:1801::bbbb.

Configure Virtual Appliances

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/configure_virtual_appliances.html

- Removed: Your password must be at least eight characters long, include at least one lowercase character, one uppercase character, one digit, and one special character.
- Added: Your password must be at least 15 characters long, include at least one lowercase character, one uppercase character, one digit, and one special character.
- Removed: For example, if your Org ID is 2406960, the default password for the VA would be Umbrella2406960.
- Added: For example, if your Org ID is 2406960, the default password for the VA would be Umbrella2406960!.
- Removed: Configuring an IPv6 address is optional and will not overwrite the IPv4 address configuration.
- Added: Configuring an IPv6 address is optional and does not replace the IPv4 configuration.
- Added: In addition to static IPv6 configuration, the VA supports dynamic IPv6 addressing through DHCPv6 or Stateless Address Autoconfiguration (SLAAC) when the network provides the required service or router advertisements.
- Added: Configure NAT64 Prefixes
- Added: You can configure NAT64 prefixes on the VA.
- Added: The prefix must be a valid IPv6 CIDR prefix with host bits set to zero.
- Added: config va nat64prefixes add 64:ff9b::/96

- Added: config va nat64prefixes remove 64:ff9b::/96
- Added: config va nat64prefixes show
- Added: The VA supports up to eight configured NAT64 prefixes
- Added: You can configure NTP servers by using IPv4 or IPv6 addresses.
- Added: Use either IPv4 or IPv6, not both.
- Added: config ntp add 2001:db8::123
- Added: config ntp remove 2001:db8::123
- Added: config ntp show
- Added: NTP over TLS also supports IPv6 server addresses:
- Added: config ntp tls add 2001:db8::123
- Added: config ntp tls remove 2001:db8::123
- Added: config ntp tls enable config ntp tls disable
- Added: config ntp tls ca <certificate>
- Added: You can configure NTP servers by using IPv4 or IPv6 addresses.
- Added: Use either IPv4 or IPv6, not both.
- Added: When you configure an IPv6 log export destination, enclose the IPv6 address in square brackets before specifying the port.
- Added: config logexport destination [2001:db8::50]:514 udp
- Added: config logexport destination [2001:db8::50]:514 tcp
- Added: config logexport destination [2001:db8::50]:6514 tls
- Added: For DMZ deployment, configure two interfaces on the VA before you enable DMZ mode.
- Added: To enable DMZ mode, enter
- Added: config va dmz
- Added: enable
- Added: .
- Added: To disable DMZ mode, enter
- Added: config va dmz
- Added: disable
- Added: .
- Added: To check the current DMZ mode, enter
- Added: config va
- Added: show
- Added: .

Local DNS Forwarding

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/local_dns_forwarding.html

- Added: Example:
- Added: config localdns add 2001:db8:300::53 corp.example.com
- Added: You can configure IPv4 or IPv6 local DNS servers.
- Added: The VA must have an IPv6 address configured before you add an IPv6 local DNS target.

Add a SaaS API Rule to the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/add-a-saas-api-rule.html

- Removed: Note: When you select Confluence or Jira, each of the tenants you have established for that platform will appear; you must choose one.
- Added: When you select Confluence or Jira, each of the tenants you have established for that platform will appear; you must choose one.
- Removed: The Resource Labels area appears only if you have selected AWS or Azure for Platform.
- Added: The Resource Labels area appears only if you have selected AWS, or Azure for Platform.

Monitor Secure Access with Alert Rules

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/monitor-alert-rules-intro/monitor_secure_access_with_alert_rules.html

- Added: Add and Edit Alert Rules for Resource Connectors
- Added: Manage Alert Rules for Destination Lists
- Added: Failed Private Resource Access Attempts
- Removed: However, for Behavior analytics alert rules, Secure Access generates alerts only for the first alert rule created for each alert type.
- Added: However, for Behavior analytics alert rules, Secure Access generates only 25 alerts in an hour for the first alert rule created for each alert type.
- Added: Failed Private Resource Access Attempts – Alert when an end user makes an unusually high number of failed attempts to access private resources through client-based ZTNA.
- Added: Add and Edit Alert Rules for Resource Connectors
- Added: Secure Access checks the status of resource connectors and resource connector groups at regular intervals.
- Added: When a resource connector is disconnected or an issue meets alert conditions, Secure Access delays raising the alert for 10 minutes.
- Added: If alert conditions are still met after 10 minutes, Secure Access raises the alert.
- Added: This delay avoids unnecessary alerts caused by transient network disruptions and connector flapping.
- Added: Note When you edit an alert rule, Secure Access dismisses any active alerts for that rule.
- Added: After you add an alert rule, Secure Access begins to monitor the conditions defined for the alert.
- Added: You can view the alerts generated by Secure Access for the Behavior analytics alert rules in the organization.
- Added: In Secure Access, navigate to the toolbar at the top of your browser window.
- Added: Click the bell icon to open the Alerts drop-down menu.

- Added: Secure Access displays the alerts generated for the configured alert rules.
- Added: For information about viewing alerts in Secure Access, see Monitor Alerts From Secure Access.
- Added: Before you begin
- Added: Before creating or editing alert rules for Resource Connectors, ensure you meet the following requirements:
- Added: You must have Full Administrator role in Cisco Secure Access.
- Added: For more information, see Manage Accounts.
- Added: At least one resource connector group and active resource connector must be deployed in your organization.
- Added: Valid email addresses or distribution lists must be identified for alert notifications.
- Added: Procedure
- Added: In the Cisco Secure Access navigation menu, navigate to Monitor> Alert Rules.
- Added: Choose one of the following actions to open the alert rule wizard:
- Added: To create a new alert rule, click Add Rule.
- Added: To update an existing alert rule, locate the rule in the table, click More Options (…), and select Edit.
- Added: In the General Settings tab, specify the rule identity and severity:
- Added: In the Alert rule name field, enter a unique, descriptive name for the alert rule.
- Added: From the Category drop-down list, select Resource Connector.
- Added: From the Alert type drop-down list, select the condition you want to monitor.
- Added: Table 1.
- Added: Resource Connector Alert Types
- Added: Alert Type
- Added: Trigger Condition
- Added: Resource connector software updates
- Added: Resource connector update started
- Added: Alert on an over-the-air (OTA) software update beginning on a resource connector during its scheduled maintenance window.
- Added: Resource connector update succeeded
- Added: Alert on a software update completing successfully and the resource connector restarting with the updated software image.
- Added: Resource connector update failed
- Added: Alert on a resource connector software update failure, requiring verification of outbound firewall access to Cisco update repositories.
- Added: Resource connector certificate & security
- Added: Resource connector certificate renewal failed
- Added: Alert on the failure of automatic TLS client certificate renewal between the resource connector and Cisco cloud services.
- Added: Resource connector certificate expiring soon

- Added: Alert on a resource connector TLS client certificate approaching expiration within 10 days.
- Added: Resource connector certificate expired
- Added: Alert on a resource connector TLS client certificate expiring, resulting in tunnel authentication termination.
- Added: Resource connector software vulnerability detected
- Added: Alert on a security vulnerability detected in the running resource connector software package.
- Added: Resource connector host OS vulnerability detected
- Added: Alert on a security vulnerability detected in the underlying host operating system of the resource connector.
- Added: Resource connector connectivity & sync
- Added: Resource connector tunnel disconnected
- Added: Alert on a resource connector tunnel remaining disconnected for 10 or more consecutive minutes.
- Added: Resource connector tunnel reconnected
- Added: Alert on a previously disconnected resource connector tunnel successfully restoring connection to Cisco Secure Access.
- Added: Resource connector configuration out of sync
- Added: Alert on the local configuration metadata on a resource connector failing to match cloud tenant records.
- Added: Resource connector end-of-support
- Added: Resource connector software image end of support
- Added: Alert on a running resource connector software image reaching End-of-Support (EoS).
- Added: Resource connector host OS end of support
- Added: Alert on the underlying host operating system of a resource connector reaching End-of-Support (EoS).
- Added: Resource connector group connectivity
- Added: Resource connector group disconnected
- Added: Alert on all resource connectors within a connector group disconnecting simultaneously, interrupting ZTNA access to associated private resources.
- Added: Resource connector group partially reconnected
- Added: Alert on at least one resource connector reconnecting in a previously offline group, indicating degraded operational capacity.
- Added: Resource connector group performance
- Added: Resource connector group overloaded
- Added: Alert on active connection load or bandwidth throughput exceeding capacity thresholds for a resource connector group.
- Added: Configure rule severity and description:
- Added: From the Severity level drop-down list, select the severity level: High, Medium, Low, or Info.
- Added: (Optional) In the Description field, enter or edit the remediation description (maximum 150 characters).
- Added: Click Next.
- Added: In the Alert Conditions tab, specify the trigger scope for the alert rule:

- Added: Choose one of the following trigger options:
- Added: Trigger notifications for all regions and connector groups: To trigger alerts for every region and connector group.
- Added: Trigger only for selected regions and connector groups: To limit the alert rule to targeted regions and/or connector groups.
- Added: Select the Regions affected check box, and then from the Select regions drop-down list, choose one or more cloud regions.
- Added: Select the Connector groups affected check box, and then from the Select connector groups drop-down list, choose one or more resource connector groups.
- Added: Click Next.
- Added: In the Notifications tab, enable the notifications for the alert rule.
- Added: You can enable Webhook notifications and Email notifications
- Added: Secure Access always enables in-product notifications.
- Added: For more information about in-product notifications, see Monitor Alerts from Secure Access.
- Added: Choose Web notifications to configure push notifications to a third-party product or service.
- Added: You can choose from a list of configured webhooks or add a new webhook.
- Added: Click on the Select a webhook drop-down menu and then choose a webhook from the list of configured webhooks.
- Added: Click + Configure a new webhook.
- Added: After you complete the configuration of the new webhook, click Save.
- Added: Complete the configuration of the webhook and add the webhook in the organization.
- Added: You can add at most 10 webhooks.
- Added: For information about webhooks, see Manage Webhooks for Third-Party Integrations.
- Added: Click Email notifications to configure notifications to a list of email recipients.
- Added: You can configure and send a test notification to the list of email recipients.
- Added: Add a comma-separated list of email addresses.
- Added: Note
- Added: You are limited to 50 email addresses.
- Added: (Optional) Enter an email address, and then click Send.
- Added: Secure Access sends a test alert to evaluate that the email address receives the alert.
- Added: In the Summary tab, review the configured general settings, alert conditions, and notifications, then click Save.
- Added: The alert rule is saved and listed in the Alert Rules table.
- Added: Cisco Secure Access continuously evaluates connector status against the configured conditions and delivers notifications when matching events occur.
- Added: What to do next
- Added: After configuring alert rules, you can:

- Added: Filter active and dismissed alerts in the notification drawer.
- Added: For more information, see Monitor Alerts From Secure Access.
- Added: Click Dismiss on an alert card to clear acknowledged notifications.
- Added: For more information, see Monitor Alerts From Secure Access.
- Added: Toggle the rule status to Disable in the Alert Rules table to suspend notifications without deleting the rule configuration.
- Added: For more information, see Manage Alert Rules.

Report Scheduling

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/monitor-with-reports-intro/schedule-reports.html

- Removed: Network Connectivity Log –Lists events for each tunnel within your Network Tunnel Groups.
- Removed: This log provides key details to help you troubleshoot connectivity issues, monitor tunnel activity, and confirm that traffic is securely transmitted between devices and Secure Access.
- Added: Network Connectivity Monitoring –Lists events for network tunnel groups and resource connectors to help you monitor connectivity, track state changes, and troubleshoot issues to ensure that traffic is securely transmitted between your environment and Secure Access.

Activity Search Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/activity-reports-intro/activity-search-report.html

- Added: When a DNS event is evaluated and resolved by underlying platform security settings rather than a user-defined policy rule, Secure Access displays one of the following system-generated descriptions:
- Added: Block due to security setting (0): Access was blocked by a DNS security policy rather than an explicit access rule.
- Added: Allow with domain on global allow list (9223372036854775807): Access was allowed because the requested domain is explicitly permitted on your Global Allow List.
- Added: No action with default rule not defined (9223372036854775806): No action occurs because the traffic does not match any user-defined rule and a default catch-all rule does not exist.
- Added: Error due to invalid policy (9223372036854775805): An error occurred during evaluation due to an invalid policy configuration.
- Added: Note System-generated policy names appear as plain text in the report and do not contain a clickable link to the Access Policy page.
- Added: Note: System-generated DNS rules (such as Block due to security setting (0)) are triggered by global security settings rather than user-defined rules.
- Added: These specific activity records do not contain a link to the Access Policy page.

Admin Audit Log Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/admin-audit-log-intro/admin_audit_log_report.html

- Removed: Policies, Identities, or Block Pages that were Changed
- Added: Policies, Identities, Block Pages, or User and Entity Behavior Analytics (UEBA) Configurations that were Updated

Network Connectivity Monitoring

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-connectivity-log-intro.html

- Removed: Network Connectivity Log
- Removed: Provides an overview of Network Connectivity Log in Cisco Secure Access, including Network Connectivity Log.
- Removed: It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.
- Removed: Network Connectivity Log
- Removed: Use this procedure to view, search, and export Network Connectivity Log entries for detailed visibility into network tunnel activity and connectivity issues.
- Added: Network Connectivity Monitoring
- Added: Provides an overview of network connectivity monitoring in Cisco Secure Access, including how to use network tunnel logs and resource connector logs to track infrastructure health, monitor state changes, and troubleshoot connectivity issues.
- Added: Network Connectivity Monitoring
- Added: This topic provides an overview of network connectivity monitoring, including how to use network tunnel logs and resource connector logs to ensure secure traffic transmission.

Added Pages

- Network Connectivity Monitoring: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-connectivity-log-intro/c_network_connectivity_monitoring.html

Removed Pages

- https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-connectivity-log-intro/network_connectivity_log.html

Cisco Secure Access Documentation Changes 2026-10-19

Lists changes to Cisco Secure Access documentation published on October 19, 2026.

Summary

- Document URL: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html
- Snapshot date: 2026-10-19
- Pages checked: 467
- Pages changed: 26
- Pages added: 0
- Pages removed: 0

Changed Pages

Limitations and range limits

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/introduction-secure-access-intro/limitations_and_range_limits.html

- Removed: Single Stack versus Dual Stack
- Removed: The terms "single stack" and "dual stack" refer to how a client or network device is configured:
- Removed: Single stack: A configuration that uses only one IP version (IPv4 or IPv6) for communication.
- Removed: Dual stack: A configuration that supports both IPv4 and IPv6.
- Removed: Secure Access receives traffic from any client configured with single stack IPv4, dual stack, or single stack IPv6 (via Remote Access VPN (RAVPN) or IPsec tunnels).
- Removed: Upstream connectivity and fallback: For upstream connectivity to web servers and internet-hosted resources, Secure Access connects using either IPv4 or IPv6.
- Added: Protocol Configuration Type
- Added: Pure IPv6 stack: A configuration where the entire communication path, including tunnels and end to end traffic, is strictly IPv6.
- Added: Dual stack: A configuration where tunnel endpoints communicate over IPv6, while the encapsulated internal traffic flows as IPv4.
- Added: Upstream connectivity and protocol handling: For upstream connectivity to web servers and internet-hosted resources, Secure Access connects using either IPv4 or IPv6 depending on the client configuration and destination resource.
- Removed: Dual stack configurations provide backward compatibility.
- Removed: If a session transaction cannot be completed using IPv6, the system falls back to IPv4.
- Removed: Clients configured exclusively for single stack IPv6 cannot perform this fallback.
- Removed: In these scenarios, the inability to connect to an IPv4-only resource is a limitation of the client configuration rather than the Secure Access service.
- Removed: See the table below for what type of internet protocol is supported.
- Removed: Note that this table is not all-encompassing.
- Added: Secure Access does not support automatic IPv6 fallback to IPv4.
- Added: If an upstream session or resource connection fails over IPv6, the system does not fall back or translate the request to IPv4.
- Added: Clients attempting to reach IPv4-only resources over a pure IPv6 connection or unresolvable IPv6 path will fail to connect.
- Added: Ensure your network routing and client configurations support the intended protocol end-to- end.
- Added: The following table outlines internet protocol and configuration support across Secure Access functions:
- Removed: IPv4
- Removed: IPv6
- Added: Client-to-Cloud Connection (Ingress)
- Added: Cloud-to-Destination Forwarding (Egress)
- Removed: Dual stack
- Removed: IPv6 traffic forwarding
- Added: IPv4, pure IPv6, or Dual stack
- Added: IPv4 and IPv6 traffic forwarding (No IPv6 to IPv4 fallback)

- Removed: Dual stack
- Removed: IPv6 traffic forwarding
- Added: IPv4, pure IPv6, or Dual stack
- Added: IPv4 and IPv6 traffic forwarding (No IPv6 to IPv4 fallback)
- Removed: Dual stack
- Removed: Dual stack
- Added: IPv4 or pure IPv6
- Added: IPv4 or pure IPv6
- Removed: Single stack
- Added: IPv4 or pure IPv6
- Removed: Dual stack
- Removed: Supported
- Added: IPv4, pure IPv6, or Dual stack
- Added: IPv4 or pure IPv6

Manage Connections to Private Destinations

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/connections-private-destinations-intro/manage_connections_to_private_destinations.html

- Removed: Does not require SRV DNS records.
- Removed: Examples: Active Directory, Kerberos, SCCM.

AD Integration with Virtual Appliances

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/provisioning-active-dir-intro/ad_integration_with_virtual_appliances.html

- Removed: You must have at least one virutal appliance already associated with your Active Directory Connector server and account.
- Added: You must have at least one virtual appliance already associated with your Active Directory Connector server and account.
- Removed: You must have at least one virutal appliance already associated with your Active Directory Connector server and account.
- Added: You must have at least one virtual appliance already associated with your Active Directory Connector server and account.
- Removed: You must have at least one virutal appliance already associated with your Active Directory Connector server and account.
- Added: You must have at least one virtual appliance already associated with your Active Directory Connector server and account.

Add an Internet Access Rule

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-access-rules-intro/add_an_internet_access_rule.html

- Added: Yes

- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes

- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Added: Yes
- Removed: In an internet access rule, add as destinations any applications from the tables under Advanced Application Controls, or a configured application list that includes any of the those applications.
- Removed: The Advanced Application Controls option will appear:
- Added: When you create or edit an internet access rule, you can add specific applications or application lists as destinations.
- Added: You can select applications from the Advanced Application Controls tables or use a configured application list.
- Removed: Click Edit.
- Removed: In the pane on the left, select the types of activities to block.
- Removed: (Optional) Filter the list in the main pane by clicking All categories and choosing a category.
- Removed: In the main pane, select the activities to block for each application in the list.
- Removed: (Optional) If you filtered the list, choose a different category, then select the activities to block for that category.
- Removed: Repeat as needed for each category in the All categories list.
- Removed: Click Save.
- Added: When creating or editing an internet access rule, enter the application name in the To text box, and select the Application categories check box.
- Added: Note You can select all applications or a single application in the To text box.
- Added: Click Block actions to restrict specific activities.
- Added: In the left pane, select the types of actions to block.
- Added: (Optional) Filter the list in the main pane by clicking All categories and choosing a specific category.
- Added: In the main pane, select the Activities to block for each application in the list.
- Added: (Optional) If you filtered the list, choose a different category, and then select the activities to block for that category.
- Added: Repeat this process for each category as needed.
- Added: Click Done to apply your changes.

Add a Private Access Rule

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/private-access-rules-intro/add_a_private_access_rule.html

- Removed: Navigate to a rule, and then click on the horizontal elipsis (…) to expand the rule menu.

- Added: Navigate to a rule, and then click on the horizontal ellipsis (…) to expand the rule menu.

Security Profiles for Internet Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/security-profiles-intro/security_profiles_for_internet_access.html

- Removed: Follow the steps in this procedure to configure the settings on the security profile.
- Removed: Navigate to Decryption, and then click Edit.
- Added: Navigate to Decryption.
- Removed: Navigate to SSO Authentication, navigate to Single Sign-On (SSO), and then click Edit.
- Added: Navigate to SSO Authentication.
- Removed: For Threat Categories, click Edit.
- Added: Click the Threat Categories dropdown and expand your setting to open the dialog box.
- Removed: For SafeSearch, click Edit.
- Removed: Enable this option to filter out offensive, explicit, unsafe, and harmful search results in Google, YouTube, Yahoo, and Bing.
- Removed: AI Supply Chain Blocking
- Removed: Control access to AI models by selecting AI supply chains to block.
- Removed: Once enabled, select AI model categories to block.
- Removed: For more information, see AI Supply Chain Report.
- Removed: Procedure
- Removed: For AI Supply Chain Blocking, click Edit.
- Removed: Enable this option to control end user access to files that can pose AI supply chain risk to security and compliance.
- Removed: Select one or more AI model categories to block:
- Removed: Prohibited Suppliers—Restrict AI models sourced from banned or untrusted suppliers.
- Removed: Code Execution—Prevent AI models that may introduce or exploit vulnerabilities in your environment.
- Removed: Copyleft License—Block AI models licensed under copyleft licensing agreements.
- Removed: Click Save.
- Removed: What to do next
- Removed: Note: Decryption is required for AI Supply Chain Blocking to work properly.
- Removed: For more information, see Enable or Disable Decryption.
- Added: Enable the SafeSearch to filter out offensive, explicit, unsafe, and harmful search results in Google, YouTube, Yahoo, and Bing.
- Removed: Navigate to End-User Notifications.

Manage Threat Categories

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/threat-categories-intro/manage_threat_categories.html

- Removed: Navigate to Secure> Settings> Threat Categories and click Add.

- Added: Navigate to Secure> Settings> Threat Categories and click Add Threat Category.
- Removed: Select security categories.
- Added: Select Security Categories.
- Added: Select Security Feeds.

Manage Traffic Decryption

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/traffic-decryption-intro/manage_traffic_decryption.html

- Removed: Under IP/CIDR, to add multiple IP addresses and CIDRs manually, click the Manual radio button, enter the IP addess and CIDR, then click Add to exempt IP addresses and CIDRs from HTTPS inspection, and then click Save.
- Added: Under IP/CIDR, to add multiple IP addresses and CIDRs manually, click the Manual radio button, enter the IP address and CIDR, then click Add to exempt IP addresses and CIDRs from HTTPS inspection, and then click Save.

Manage Client-Based Zero Trust Access in Secure Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/zero-trust-access-intro/manage-client-based-zta-overview.html

- Added: Customers that are new to ZTA now experience the broad match policy enforcement model to provide a more consistent, reliable, and efficient security enforcement experience.
- Added: This update streamlines our infrastructure to ensure greater system stability while establishing a unified foundation for future platform enhancements.
- Added: Note: While you can sustain multiple site environments note that having duplicate destinations assocaited with a resource connector may affect mobile functionality with Secure Private Access.
- Added: Cached Block Verdict Types for ZTA
- Added: The Zero Trust Access module caches blocked verdicts to reduce the load from client interception and cloud enforcement.
- Added: Blocked Verdict Types and Cache Intervals
- Added: Block Type
- Added: Verdict Cache Interval
- Added: Verdict Cache Scope
- Added: Geolocation-based
- Added: 5 minutes
- Added: Global
- Added: No matching access policy rule
- Added: 1 minute
- Added: Global
- Added: Explicit block rule
- Added: 5 minutes
- Added: Process
- Added: Time-based
- Added: 5 minutes

- Added: Global
- Added: DNS errors
- Added: 1 minute
- Added: Global
- Added: Resource matching or definition issue
- Added: 5 minutes
- Added: Global
- Added: This function is only available on desktop platforms running Client version 5.1.17 and later.
- Added: For more information about supported features on desktop and mobile platforms, see Zero Trust Access Requirements and Limitations.
- Removed: Note Virtual interfact detection is only supported with version 5.1.13 and later.
- Added: Note Virtual interface detection is only supported with version 5.1.13 and later.
- Added: Table 6.

Get Started with Virtual Appliances

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/get_started_with_virtual_appliances.html

- Removed: Ensure your Virtual Appliance (VA) complies with Secure Access requirements annd prerequisites prior to onboarding them.
- Added: Ensure your Virtual Appliance (VA) complies with Secure Access requirements and prerequisites prior to onboarding them.
- Removed: Secure Access supports the folowing KVM Linux versions:
- Added: Secure Access supports the following KVM Linux versions:

Manage VAs in Secure Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/manage-vas-in-secure-access.html

- Removed: Locate a Virtual Appliance and click the ellipsis (...), and then seelect Reset Password.
- Added: Locate a Virtual Appliance and click the ellipsis (...), and then select Reset Password.

Deploy VAs in KVM

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_kvm.html

- Added: Describes Deploy VAs in KVM in Cisco Secure Access and explains Prerequisites and Configure Authentication for the Virtual Appliances.
- Added: It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.
- Added: Deploy Cisco Secure Access Virtual Appliances (VAs) in KVM.
- Added: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Added: It is critical that these VAs are not cloned or copied in any way.
- Added: Configure and set up each VA manually.

- Added: Prerequisites
- Added: Full Admin user role.
- Added: For more information, see Manage Accounts.
- Added: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Added: A Linux system with qemu-utils package installed.
- Added: Only VAs running 2.5 or above can be deployed in KVM.
- Added: Virtual Appliance deployments in KVM are supported with specific Red Hat Linux and Ubuntu Linux versions only.
- Added: KVM on Ubuntu Linux (supported LTS versions)
- Added: KVM on Red Hat Linux (supported versions)
- Added: Configure Authentication for the Virtual Appliances
- Added: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.
- Added: Secure Access enables the Download Components only after the API keys for the VAs are configured.
- Added: For more information, see Configure Authentication for Virtual Appliances.
- Added: Procedure for Deploying VAs in KVM
- Added: Prerequisites
- Added: Full Admin user role.
- Added: For more information, see Manage Accounts.
- Added: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Added: A Linux system with qemu-utils package installed.
- Added: Only VAs running 2.5 or above can be deployed in KVM.
- Added: Virtual Appliance deployments in KVM are supported with specific Red Hat Linux and Ubuntu Linux versions only.
- Added: KVM on Ubuntu Linux (supported LTS versions)
- Added: KVM on Red Hat Linux (supported versions)
- Added: To successfully deploy a virtual appliance in a KVM envinronment, follow the steps as they are listed below:
- Added: Step 1 – Download and Extract the KVM Installer
- Added: Step 2 – Launch the Virtual Appliance on KVM
- Added: Step 1 – Download and Extract the KVM Installer
- Added: Procedure
- Added: Navigate to Connect> DNS Forwarders and click Download Components.
- Added: Click Download next to VA for KVM.
- Added: Secure Access generates and downloads a.tar file unique to your deployment.
- Added: This tar file includes:
- Added: A zip file containing the KVM-compatible virtual hard disk images (.qcow2 format) and configuration files

- Added: A signature file
- Added: A Cisco public certificate to validate the signature
- Added: A readme file
- Added: Extract the contents of the tar file using the tar -xvf <tar filename> -C <Destination folder> command.
- Added: Verify the integrity of the downloaded file by following the signature validation instructions in the readme file.
- Added: On a successful verification, the message Verified OK is displayed.
- Added: Extract the.zip file.
- Added: The extracted contents include the Virtual Hard Disks folder, the Virtual Machines folder, and a configuration file.
- Added: The Virtual Hard Disks folder contains the KVM-compatible.qcow2 files (namely, dynamic.qcow2 and forwarder-va.qcow2).
- Added: Step 2 – Launch the Virtual Appliance on KVM
- Added: Procedure
- Added: Open the Virtual Machine Manager on your Linux system running KVM and click Create a new virtual machine.
- Added: In the first step of the wizard, choose Import existing disk image.
- Added: Provide the existing storage path to your forwarder-va.qcow2.
- Added: Set the OS type to Linux and click Forward.
- Added: Set the memory and CPU settings to at least 1 CPU and 1 GB RAM and click Forward.
- Added: In the last step of the wizard, select Customize configuration before install and then click Finish.
- Added: Select Add Hardware.
- Added: Select Storage, add or create custom storage, add the dynamic disk, and then click Finish.
- Added: You should then see two disks.
- Added: Click Begin installation to create the VA.
- Added: If your network supports DHCP, the VA will get auto-configured with a DHCP IP address and will register to Umbrella using this IP.
- Added: You can configure the VA on KVM through two mechanisms:
- Added: Press Ctrl+B on the VA console and entering the Configuration mode.
- Added: Or
- Added: Initiate an SSH connection to the DHCP IP—this IP can be retrieved in Secure Access—and enter Configuration mode.
- Added: What to do next
- Added: You can now configure the VA.
- Added: For information about configuring VAs, see Configure Virtual Appliances.

Manage File Inspection and File Analysis

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/file-inspection-analysis-intro/manage_file_inspection_and_file_analysis.html

- Removed: bat, bz2, chm, dll, doc, docx, eml, exe, gz, hta, hwp, hwt, hwpx, iso, jar, jtd, jtt, jtdc, jttc, lnk, msg, msi, mhtml, rar v5, rtf, xls, xlsx, ppt, pptx, pdf, ps1, sep, slk, swf, tar, vbe, vbn, vbs, wsf, xml, xps, xz, zip, 7-zip
- Added: bat, bz2, chm, dll, doc, docx, exe, gz, hta, hwp, hwt, hwpx, iso, jar, jtd, jtt, jtdc, jttc, lnk, msg, msi, mhtml, rar v5, rtf, xls, xlsx, ppt, pptx, pdf, ps1, sep, slk, swf, tar, vbe, vbn, vbs, wsf, xml, xps, xz, zip, 7-zip

Enable File Type Controls

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/file-type-controls-intro/enable_file_type_controls.html

- Removed: Navigate to Security and Acceptable Use Controls, navigate to File Type Blocking, and then click Edit.
- Added: Navigate to Security and Acceptable Use Controls, navigate to File Type Blocking.

Manage Notification Pages

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/notification-pages-intro/manage_notification_pages.html

- Removed: Note The notification pages described in this section do not apply to private access rules in the Access policy.
- Added: Note: The notification pages described in this section do not apply to private access rules in the Access policy.
- Removed: Note You can pin a specific column or re-arrange columns in your desired layout by clicking on the Settings gear icon.
- Added: Note: You can pin a specific column or re-arrange columns in your desired layout by clicking on the Settings gear icon.
- Removed: Note You can View or Edit the Default Settings End User Notification Page, but you cannot Delete it.
- Added: Note: You can View or Edit the Default Settings End User Notification Page, but you cannot Delete it.
- Removed: Note
- Removed: The value of the user input field is a case-insensitive string.
- Added: Note: The value of the user input field is a case-insensitive string.

Add a Real Time Rule to the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/add_a_real_time_rule_to_the_data_loss_prevention_policy.html

- Removed: Note Policies based on the Executables file type group, specifically those targeting.exe files, do not apply to the Endpoint DLP channel.
- Removed: Additionally, exe file-type-based policies do not apply to the Endpoint DLP channel.
- Added: Note Within the Paste to Application, ChatGPT (Desktop) is available under AI Apps and MS Teams is available under Collaboration; both require Endpoint DLP for Windows version 1.8.0.376 or later.

Add an Email Rule to the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/t_add-an-email-rule.html

- Removed: The rule will search for any of the configured label names in document properties of email attachements.
- Added: The rule will search for any of the configured label names in document properties of email attachments.

Manage Certificates for Private Resource Decryption

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/certificates-intro/manage_certificates_for_private_resource_decryption.html

- Removed: Secure Access uses decryption to inspect traffic with Intrusion Prevention (IPS) and the Data Loss Prevention policy or validate a custome domain.
- Added: Secure Access uses decryption to inspect traffic with Intrusion Prevention (IPS) and the Data Loss Prevention policy or validate a custom domain.

Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/secure-client-windows-mac-linux-intro/get-started-cisco-secure-client.html

- Added: Note If you are using Cisco Secure Client with Secure Web Gateway (SWG), Cisco recommends disabling the QUIC protocol in your browser settings (for example, Google Chrome, Microsoft Edge, or Firefox) to prevent issues with browser services like search, Gmail, or YouTube.
- Added: For more information, see Disable QUIC Protocol to Ensure Compatibility with AnyConnect SWG.

Manage Zero Trust Access using Cisco Secure Client

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/za-secure-client-intro/manage_zero_trust_access_using_cisco_secure_client.html

- Removed: Now continue to the SSO authetnication enrollment procedure.
- Added: Now continue to the Enroll Devices in Zero Trust Access Using SSO Authentication.

Manage Endpoint Data Loss Prevention Using Cisco Secure Client for Windows and Mac

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/edp-secure-client-intro/c_Manage_EDLP_Using_Cisco_Secure_Client__1.html

- Added: Media/Portable Devices: Prevents sensitive files from being exfiltrated to Android phones and cameras.
- Removed: Disk space: Atleast 1 GB of free disk space available
- Added: Disk space: At least 1 GB of free disk space available

Cisco Endpoint Diagnostic Tool

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/endpoint-diagnostic-tool-intro/t_client_endpoint_diagnostic_tool.html

- Removed: Donot close CEDT while the diagnostic run is paused.
- Added: Do not close CEDT while the diagnostic run is paused.

Log Formats and Versioning

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/logging-intro/log_formats_and_versioning.html

- Removed: The UTC time the event occured in milliseconds. (e.g., 2017-10-02 23:52:53).
- Removed: Note: Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.
- Added: The UTC time the event occurred in milliseconds. (e.g., 2017-10-02 23:52:53).
- Added: Note
- Added: Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.

- Removed: timestamp,policy identity label,internal client ip,external client ip,destination ip,content type,action,url,referer,user agent,status code,request size,response size,response body size,sha–sha256,categories,av detections,puas,amp disposition,AMP malware name,amp score,policy identity type,blocked categories,identities,identity types,request method,dlp status,certificate errors,file name,ruleset id,rule ID,destination list ids,isolate action,file action,warn status,forwarding method,producer,msp organization id,geo location of blocked destination countries,application ids,hostname,data center,egress,server name,time based rule,security overridden,detected response file type,warn categories,organization id,application entity name,application entity category, egress ip,ai model name,ai suply chain categories,event correlation id,isolation profile id,source country
- Added: timestamp,policy identity label,internal client ip,external client ip,destination ip,content type,action,url,referer,user agent,status code,request size,response size,response body size,sha–sha256,categories,av detections,puas,amp disposition,AMP malware name,amp score,policy identity type,blocked categories,identities,identity types,request method,dlp status,certificate errors,file name,ruleset id,rule ID,destination list ids,isolate action,file action,warn status,forwarding method,producer,msp organization id,geo location of blocked destination countries,application ids,hostname,data center,egress,server name,time based rule,security overridden,detected response file type,warn categories,organization id,application entity name,application entity category, egress ip,ai model name,ai supply chain categories,event correlation id,isolation profile id,source country

Activity Search Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/activity-reports-intro/activity-search-report.html

- Removed: Connection Staus
- Added: Connection Status

Data Loss Prevention Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/dlp-report-intro/data_loss_prevention_report.html

- Removed: The exact fields displayed varies depending upon the platform associated with the event.
- Added: The fields displayed vary depending on the platform associated with the event.
- Removed: File Name–The name of the email fle that triggered the violation.
- Removed: Subject–The subject line of the email that tirggered the violation.
- Added: File Name–The name of the email that triggered the violation.
- Added: Subject–The subject line of the email that triggered the violation.
- Removed: Endpoint API Events
- Added: Endpoint DLP Events
- Removed: Detected–The date and time the content was detected.
- Removed: Action –The action triggered by the rule when a violation is detected.
- Removed: File Name–The name of the file or attachment where a classification match was found.
- Removed: This includes attachments to email messages, Jira pages and comments, and Confluence pages, but not attachments to comments on Confluence pages.
- Removed: If content is found in a message, post, or form data, this field name displays Message, Content, or Form.
- Removed: For Salesforce chatter posts, this field name displays Chatter Post.
- Removed: For Salesforce sObjects, this field name displays SObject followed by object name.
- Removed: For Confluence and Jira pages, this field name displays the title of the page.

- Removed: For comments on Confluence and Jira pages, this field name displays Comment followed by Page title.
- Removed: Identity –The identity that made the request.
- Removed: Application–The application where the file was uploaded or posted.
- Removed: Application Category–The category for the application where the file was uploaded or posted.
- Removed: Destination URL–The URL of the destination for the event.
- Removed: Rule–The rule that triggered the event.
- Removed: Severity–The severity of the rule that triggered the event.
- Removed: File Label–File label names in the file's document properties.
- Removed: This includes Microsoft Office Document Properties, and AdobePDF Document Properties.
- Removed: For Microsoft 365 or Box tenants this includes Microsoft Office sensitivity labels.
- Removed: Within the Box application these are referred to as classification labels.
- Removed: If no labels are detected, this field displays Unclassified.
- Removed: Direction–Direction of traffic.
- Added: File Name–The name of the file on the endpoint that triggered a classification match:
- Added: For the printer channel, it holds file name - printing application, for example, allow-824.txt - Notepad.
- Added: For clipboard channel, it holds application filename reading from clipboard (PID), for example, chrome.exe (9096).
- Added: Application–Available only for the Application File Access and Paste to Applications channels..
- Added: Destination URL–This field contains the endpoint channel for the event such as BLUETOOTH or NETWORK SHARE.
- Added: Device Type–The category of the destination device, for example, USB, printer, network device, application file access, media devices, or media portable devices.
- Added: Device Name–The human-readable display name of the device.
- Added: Manufacturer–The device manufacturer name.
- Added: Model–The hardware model name of the device.
- Added: Serial Number–The hardware serial number of the device.
- Added: Vendor ID–The USB vendor ID.
- Added: Product ID–The USB product ID.
- Added: Instance ID– The OS device instance ID or hardware ID.
- Added: Raw Device Path–The raw OS-level device path.
- Added: Removable–Indicates whether the device is removable.
- Added: File System–The file system type of the device.
- Added: Media Type– The physical media category of the device, for example, removable, SD, HDD, or virtual.
- Added: Bus Type–The bus interface type of the device.
- Added: First Observed–The ISO-8601 or epoch time stamp indicating when the device was first observed.
- Added: Mount Options– The OS mount options for the device volume.

- Added: Volume UUID–The UUID of the mounted volume.
- Added: Mount Path–The file system path where the device is mounted.
- Added: Volume Label–The display label of the mounted volume.
- Added: Share Name– The network share name.
- Added: Server FQDN– The fully qualified domain name of the file server.
- Added: Protocol–The network protocol used to access the share.
- Added: Print Server–The hostname or IP address of the print server.
- Added: Print Type–The type of the printer, for example, local, network, virtual.
- Added: Print To File–Indicates whether the print job was directed to a file.
- Added: IP Address–The IP address of the device.
- Added: Hostname– The hostname of the device.
- Removed: Remove all collaborators, and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permisson set for the quarantine app.
- Added: Remove all collaborators, and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permission set for the quarantine app.
- Removed: Threshold Severity Represents the total number of occurances of a data identifier that must be detected in a document for Secure Access to generate an incident.
- Added: Threshold Severity Represents the total number of occurrences of a data identifier that must be detected in a document for Secure Access to generate an incident.

Events Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/events-report-intro/events-report-overview.html

- Removed: Update a saved search: If you modify the filters in an applied saved search, click the Update saved search button that apears to save your changes to the current saved search.
- Added: Update a saved search: If you modify the filters in an applied saved search, click the Update saved search button that appears to save your changes to the current saved search.

Cisco Secure Access Documentation Changes 2026-10-12

Lists changes to Cisco Secure Access documentation published on October 12, 2026.

Summary

- Document URL: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html
- Snapshot date: 2026-10-12
- Pages checked: 467
- Pages changed: 8
- Pages added: 8
- Pages removed: 0

Changed Pages

Security Insights Dashboard

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/dashboards-overview-intro/security-insights-dashboard.html

- Removed: Use the period switcher (24 hours, 7 days, 30 days, 60 days) at the top right.
- Added: Use the period switcher (24 hours, 7 days, 30 days) at the top right.
- Added: The default selection is Last 24 hours.
- Removed: Top Data Flows
- Added: Data Loss Prevention Violation Breakdown
- Removed: Rules with 0 Hits – Rules that have never matched traffic; candidates for review or removal.
- Added: Rules with 0 Hits – Rules that have never matched threats in the past 24 hours.
- Added: This time frame is always 24 hours.

Virtual Appliances

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro.html

- Added: Deploy VAs in Hyper-V for Windows 2012 or Higher
- Added: Describes Deploy VAs in Hyper-V for Windows 2012 or Higher in Cisco Secure Access.
- Added: Deploy Cisco Secure Access Virtual Appliances in Microsoft Hyper-V for Windows Server 2012 or higher.
- Added: Deploy VAs in VMware
- Added: Describes Deploy VAs in VMware in Cisco Secure Access and explains Prerequisites and Configure Authentication for the Virtual Appliances.
- Added: It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.
- Added: Deploy VAs in Microsoft Azure
- Added: Describes Deploy VAs in Microsoft Azure in Cisco Secure Access.
- Added: Deploy Cisco Secure Access Virtual Appliances (VAs) in Microsoft Azure.
- Added: Deploy VAs in Amazon Web Services
- Added: Describes Deploy VAs in Amazon Web Services in Cisco Secure Access.
- Added: Deploy Cisco Secure Access Virtual Appliances (VAs) in Amazon Web Services.
- Added: Deploy VAs in Google Cloud Platform
- Added: Describes Deploy VAs in Google Cloud Platform in Cisco Secure Access.
- Added: Deploy Cisco Secure Access Virtual Appliances (VAs) in Google Cloud Platform.
- Added: Deploy VAs in KVM
- Added: Describes Deploy VAs in KVM in Cisco Secure Access and explains Prerequisites and Configure Authentication for the Virtual Appliances.
- Added: It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Added: Deploy VAs in Nutanix
- Added: Provides instructions for completing the Deploy VAs in Nutanix workflow in Cisco Secure Access.
- Added: It explains the sequence of actions and relevant settings presented in the procedure.
- Added: Deploy VAs in Alibaba Cloud
- Added: Describes Deploy VAs in Alibaba Cloud in Cisco Secure Access.
- Added: This guide describes how to deploy Cisco Secure Access Virtual Appliances in the Alibaba Cloud environment.

Deploy Virtual Appliances

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_virtual_appliances.html

- Removed: Deploy VAs in Hyper-V for Windows 2012 or Higher
- Removed: Deploy Cisco Secure Access Virtual Appliances in Microsoft Hyper-V for Windows Server 2012 or higher.
- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Configure and set up each VA manually.
- Removed: Prerequisites
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: One of the following Windows Server operating systems:
- Removed: Windows Server 2012, SP1, or R2 (Standard or Datacenter), 2016 or 2019 with Hyper-V role.
- Removed: Hyper-V Server 2012, 2012 R2, 2016 or 2019.
- Removed: Basic knowledge of Hyper-V.
- Removed: Note Secure Access does not support Virtual Appliances that are deployed using System Center Virtual Machine Manager (SCVMM).
- Removed: Configure Authentication for the Virtual Appliances
- Removed: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.
- Removed: Secure Access enables the Download Components only after the API keys for the VAs are configured.
- Removed: For more information, see Configure Authentication for Virtual Appliances.
- Removed: Procedure for Deploying VAs in Hyper-V for Windows 2012 or Higher
- Removed: Step 1 – Download and Extract the Hyper-V Installer
- Removed: Step 2 – Import the Virtual Appliance
- Removed: Step 3 – Copy and Rename Image Files
- Removed: Step 4 – Select Network Adapter
- Removed: Step 5 – Select Hard Drive
- Removed: Step 6 – Power on the Virtual Machine

- Removed: Step 7 – Repeat for the Second Virtual Appliance
- Removed: Step 1 – Download and Extract the Hyper-V Installer
- Removed: Procedure
- Removed: Navigate to Connect> DNS Forwarders and click Download Components.
- Removed: Click Download next to VA for Hyper-V.
- Removed: Secure Access generates and downloads a tar file unique to your deployment.
- Removed: This tar file includes:
- Removed: a zip file containing the virtual hard disks that need to be deployed on Hyper-V
- Removed: a signature file
- Removed: a Cisco public certificate to validate the signature
- Removed: a readme file
- Removed: Extract the contents of the tar file using the command tar -xvf <tar filename> -C <Destination folder>.
- Removed: To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file.
- Removed: When successful, you will see a message saying “Verified OK."
- Removed: Extract the.zip file.
- Removed: You'll find two folders– Virtual Hard Disks and Virtual Machines –and a config file.
- Removed: Step 2 – Import the Virtual Appliance
- Removed: Tip Using Windows 2012 R2 or Higher Versions
- Removed: Microsoft has introduced a "Generation 2" style of VM profile on Hyper-V for Windows 2012 R2 and higher versions.
- Removed: As a result, the import steps below will fail with the error: "Hyper-V did not find virtual machines to import from location [path]"
- Removed: You will need to create a new virtual machine as "Generation 1", then skip to 3.
- Removed: Copy and Rename Image Files.
- Removed: For more information about Generation 1 vs.
- Removed: Generation 2, see Generation 2 Virtual Machine Overview.
- Removed: Note Step 2 in this procedure applies to Windows 2012 only, and not Windows 2012 R2.
- Removed: Procedure
- Removed: Select your Hyper-V server, right-click its name and select Import Virtual Machine from the menu.
- Removed: Navigate to the extraction folder from your download, select that folder to import, and then click Next.
- Removed: Select forwarder-va as the virtual machine to import and click Next.
- Removed: Select Copy the virtual machine (create a new unique ID) and click Next.
- Removed: Choose destination folders to install to.
- Removed: By default, these are the Hyper-V Configuration folders, but you can choose another folder.

- Removed: Note If selecting a different folder, pick a drive with sufficient space and create a folder with a specific name for the virtual machine, such as \opendnsforwarder-1.
- Removed: This can be helpful to ensure you're able to distinguish between the two virtual appliances in your file structure.
- Removed: Click Finish.
- Removed: Step 3 – Copy and Rename Image Files
- Removed: Procedure
- Removed: In Windows Explorer, navigate to the \Virtual Hard Disks subfolder within the extracted download folder created in Step 1.
- Removed: Copy the two files from that location to the Virtual Machine Configuration Folder you specified in the previous step.
- Removed: The two files, dynamic and forwarder-va. must be renamed per the VA that is being installed.
- Removed: For example, rename:
- Removed: dynamic to Dynamic-VA-1
- Removed: and
- Removed: forwarder-va to Forwarder-VA-1
- Removed: If configuring your second VA, change the number accordingly.
- Removed: This can help ease the management of multiple virtual appliances and avoids conflicts between filenames when configuring your second VA.
- Removed: Step 4 – Select Network Adapter
- Removed: Procedure
- Removed: In the Hyper-V Manager, select the virtual machine you've created, right-click and choose Settings.
- Removed: Under Hardware, select Network Adapter, and then assign a virtual switch that has internet access.
- Removed: Step 5 – Select Hard Drive
- Removed: Procedure
- Removed: In Settings for Hardware, select the hard drives.
- Removed: Ideally, they should be under the same IDE controller.
- Removed: For hard drive settings, browse to the Virtual Machine Configuration Folder and the first hard drive should be set to the forwarder file (Forwarder-va) and the second hard drive should be set to the dynamic (Dynamic) file.
- Removed: Click Apply.
- Removed: Step 6 – Power on the Virtual Machine
- Removed: If all is well, you'll see the Virtual Appliance console screen.
- Removed: For information about configuring VAs, see Configure Virtual Appliances.
- Removed: Step 7 – Repeat for the Second Virtual Appliance
- Removed: Two VAs are required per Umbrella site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Each VA must be set up and configured manually.

- Removed: To build your second VA, repeat procedures starting at 2.
- Removed: Import Virtual Appliance.
- Removed: Deploy VAs in VMware
- Removed: Deploy Cisco Secure Access Virtual Appliances (VAs) in VMware.
- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Configure and set up each VA manually.
- Removed: Prerequisites
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: Basic knowledge of VMware ESXi.
- Removed: For more information, see the VMware documentation.
- Removed: Configure Authentication for the Virtual Appliances
- Removed: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.
- Removed: Secure Access enables the Download Components button only after the API keys for the VAs are configured.
- Removed: For more information, see Configure Authentication for Virtual Appliances.
- Removed: Procedure for Deploying VAs in VMware
- Removed: Step 1 – Download OVF Template
- Removed: Step 2 – Deploy OVF Template
- Removed: Step 3 – Deploy a Second Virtual Appliance
- Removed: Step 4 – Power on the Virtual Machines
- Removed: Step 1 – Download OVF Template
- Removed: Procedure
- Removed: Navigate to Connect> DNS Forwarders and click Download Components.
- Removed: Click Download next to VA for VMWare ESXi.
- Removed: Umbrella generates and downloads a.tar file unique to your deployment.
- Removed: This tar file includes:
- Removed: an.ovf template containing the virtual hard disks that need to be deployed on VMware
- Removed: a signature file
- Removed: a Cisco public certificate to validate the signature
- Removed: a readme file
- Removed: Extract the contents of the tar file using the command tar –xvf <tar filename> -C <Destination folder>.

- Removed: To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file.
- Removed: On successful signature validation, you should see a message saying “Verified OK."
- Removed: Step 2 – Deploy OVF Template
- Removed: Procedure
- Removed: Log into your VMware vSphere client and select the File tab.
- Removed: Click Deploy OVF Template, choosing the downloaded.ova template.
- Removed: Follow the deployment wizard prompts, but be sure to follow these steps:
- Removed: For the source, browse to the.ova file you just downloaded.
- Removed: Specify a unique name and location for your VA.
- Removed: Select the disks appropriate to your environment.
- Removed: It is recommended to select Thin Provision for the disk format, but it is not mandatory.
- Removed: Select or map a network.
- Removed: Click Finish.
- Removed: The system begins to deploy the VA.
- Removed: During the deployment, subsequent prompts update you about the status of the deployment.
- Removed: Step 3 – Deploy a Second Virtual Appliance
- Removed: While the first VA is deploying, repeat the previous two steps to configure your second VA.
- Removed: Note Two VAs are required per Umbrella site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Each VA must be set up and configured manually.
- Removed: Step 4 – Power on the Virtual Machines
- Removed: If the deployment succeeded, you'll see the VA console screen.
- Removed: For information about configuring VAs, see Configure Virtual Appliances.
- Removed: Deploy VAs in Microsoft Azure
- Removed: Deploy Cisco Secure Access Virtual Appliances (VAs) in Microsoft Azure.
- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Configure and set up each VA manually.
- Removed: Prerequisites
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: If you use the VA on Azure as a DNS server for your on-premise endpoints, then DNS traffic from these endpoints should not traverse through a Network Address Translation (NAT) device en route to the VA.

- Removed: The VA should receive DNS packets with the source IP as the internal IP of the endpoints.
- Removed: An ExpressRoute or dedicated MPLS or site-to-site VPN connection from your on-premise environment to Azure will meet this requirement.
- Removed: A system running Windows 10 with the Hyper-V role enabled to convert VHD images to an Azure-acceptable format.
- Removed: Only VAs running version 2.4 or above can be deployed in Microsoft Azure.
- Removed: Configure Authentication for the Virtual Appliances
- Removed: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.
- Removed: Secure Access enables the Download Components button only after the API keys for the VAs are configured.
- Removed: For more information, see Configure Authentication for Virtual Appliances.
- Removed: Procedure for Deploying VAs in Microsoft Azure
- Removed: Before you begin
- Removed: Add internal.cloudapp.net to the internal domains list for VAs.
- Removed: Unless you are using your own DNS server in Azure, you should configure 168.63.129.16 as the local DNS server in the VA settings.
- Removed: This is the virtual IP used by Azure for recursive and local DNS queries.
- Removed: Procedure
- Removed: Step 1 – Prepare the Virtual Appliance Image on Azure.
- Removed: This is a one time task.
- Removed: Step 2 – Launch the Virtual Appliance on Azure.
- Removed: Perform this task for each VA after you have performed the one-time task of preparing the VA image.
- Removed: Step 1 – Prepare the Virtual Appliance Image on Azure
- Removed: This is a one-time task to create an image in Azure that can be used to launch multiple VAs.
- Removed: Note Generation 2 VMs are not supported for VA deployments.
- Removed: Procedure
- Removed: Navigate to Connectors> DNS Forwarders and click Download Components.
- Removed: Click Download next to VA for Hyper-V.
- Removed: Umbrella generates and downloads to your computer a.tar file unique to your deployment.
- Removed: This tar file includes:
- Removed: a.zip file containing the virtual hard disks that need to be deployed on Azure
- Removed: a signature file
- Removed: a Cisco public certificate to validate the signature
- Removed: a readme file
- Removed: Extract the contents of the tar file using the command tar -xvf <tar filename> -C <Destination folder>.
- Removed: To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file.

- Removed: On successful signature validation, you should see a message saying “Verified OK."
- Removed: Extract the downloaded zip file.
- Removed: You'll find two folders– Virtual Hard Disks and Virtual Machines –and a config file.
- Removed: Open Windows PowerShell as Administrator, navigate to the Virtual Hard Disks folder, and convert the vhd files (forwarder and dynamic) in their respective folders to a fixed type format acceptable by Azure.
- Removed: To convert and resize the forwarder file, run the following commands:
- Removed: Convert-VHD -Path .\forwarder-va.vhd -DestinationPath forwarder-fixed.vhd -VHDType fixed
- Removed: Resize-VHD .\forwarder-fixed.vhd -SizeBytes 8GB
- Removed: To convert and resize the dynamic file, run the following commands:
- Removed: Convert-VHD -Path .\dynamic.vhd -DestinationPath dynamic-fixed.vhd -VHDType fixed
- Removed: Resize-VHD .\dynamic-fixed.vhd -SizeBytes 30MB
- Removed: Conversion free disk space requirements
- Removed: Conversion requires at least 9GB of free disk space to create the modified disks.
- Removed: The new forwarder-fixed.vhd will consume approximately 8GB of space.
- Removed: Machines with less than 9GB of space will fail to convert with a red error message.
- Removed: Upload the forwarder-fixed.vhd and dynamic-fixed.vhd to a blob in your Azure storage account using the Azure portal or the AZ CLI.
- Removed: Note This is a one-time upload.
- Removed: Create an image in Azure from these virtual hard disks using the Azure portal.
- Removed: Use the forwarder-fixed.vhd as the OS disk (OS type: Linux) and the dynamic-fixed.vhd as the data disk.
- Removed: Note Ensure that Host caching for both the OS disk and data disk is set to Read/write.
- Removed: Since second generation VMs are not supported for VA deployments, ensure that you set VM Generation to Gen 1.
- Removed: Once the VA image is created in Azure, use this image to launch multiple VAs.
- Removed: For more information, see Step 2: Launch the Virtual Appliance on Azure.
- Removed: Step 2 – Launch the Virtual Appliance on Azure
- Removed: Note Before performing this task, you must complete the one-time task of preparing the virtual appliance image on Azure.
- Removed: For more information, see Step 1: Prepare the Virtual Appliance Image on Azure.
- Removed: Procedure
- Removed: Use the Azure portal to launch Secure Access VAs in Azure using the VA image you created in Step 1: Prepare the Virtual Appliance Image on Azure:
- Removed: Choose a VM size with at least one VCPU and 1024 MB RAM.
- Removed: Note VM sizes above eight VCPUs are not supported.
- Removed: For the Administrator account, set the Authentication type to Password.
- Removed: Note It is a security risk to specify a public IP address for the VA, and is not recommended except in case of SNAT port exhaustion issues.

- Removed: If you need to configure a public IP for the VA on Azure for these issues, ensure that inbound access from the Internet is not permitted.
- Removed: For more information, see Troubleshoot Intermittent DNS Resolution Failures on a VA Deployed in Azure.
- Removed: Provide the username as vmadmin and enter a password that meets complexity requirements.
- Removed: Note The admin-password you create here is not actually set on the VA.
- Removed: You may also use the Azure Cloud Shell to launch VAs in Azure using the VA images you created in Step 1: Prepare the Virtual Appliance Image on Azure.
- Removed: VM sizes above eight VCPUs are not supported.
- Removed: You may specify the static IP as part of the command.
- Removed: For example:
- Removed: az vm create --resource-group MyResourceGroup --size Standard_B2s --name UmbrellaVA
- Removed: --image VAImage --authentication-type password --admin-username vmadmin
- Removed: --admin-password <password> --vnet-name MyVnet --subnet MySubnet
- Removed: --private-ip-address 10.0.0.1
- Removed: In Secure Access, navigate to Connector> DNS Forwarders.
- Removed: Secure Access displays your list of deployed VAs.
- Removed: Use the same image to launch multiple VAs as required.
- Removed: Provide a different name and different static IP for each VA.
- Removed: Note If you do not specify the private IP address, the VA will automatically pull a DHCP IP and register to Umbrella with this IP address.
- Removed: This IP address will be listed as the VA name in Secure Access.
- Removed: What to do next
- Removed: Tip Diagnostic Settings
- Removed: It is not recommended to turn on Diagnostic Settings (Guest-level monitoring) or install any extension for a VA on Azure.
- Removed: Enabling diagnostics results in huge log files being generated on the VA, which causes the VA to run out of disk space.
- Removed: If your VA on Azure is reporting disk space issues, navigate to the Settings> Extensions page against your VA on the Azure portal and remove any extensions.
- Removed: Also, navigate to the Monitoring> Diagnostic Settings page against your VA on the Azure portal and verify that Guest-level monitoring is turned off.
- Removed: Deploy VAs in Amazon Web Services
- Removed: Deploy Cisco Secure Access Virtual Appliances (VAs) in Amazon Web Services.
- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Configure and set up each VA manually.
- Removed: Prerequisites

- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: If you are using the VA on Amazon Web Services as a DNS server for your on-premise endpoints, then DNS traffic from these endpoints should not traverse through a Network Address Translation (NAT) device en route to the VA.
- Removed: The VA should receive DNS packets with the source IP as the internal IP of the endpoints.
- Removed: An AWS Direct Connect or dedicated MPLS or VPN connection from your on-premise environment to AWS will meet this requirement.
- Removed: Only VAs running version 2.6 or above can be deployed in AWS.
- Removed: Configure Authentication for the Virtual Appliances
- Removed: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.
- Removed: Secure Access enables the Download Components button only after the API keys for the VAs are configured.
- Removed: For more information, see Configure Authentication for Virtual Appliances.
- Removed: Procedure for Deploying VAs in Amazon Web Services
- Removed: Prepare the Virtual Appliance Amazon Machine Image.
- Removed: This is a one time task.
- Removed: Launch the Virtual Appliance on Amazon Web Services.
- Removed: Perform this task for each VA after you have performed the one-time task of preparing the VA image.
- Removed: Step 1 – Prepare the Virtual Appliance Amazon Machine Image
- Removed: Note This is a one-time task to create an Amazon Machine Image (AMI) that can be used to launch multiple VAs.
- Removed: Procedure
- Removed: Navigate to Connect> DNS Forwarders and click Download Components.
- Removed: Click Download for VA for Hyper-V.
- Removed: Secure Access generates and downloads a.tar file to your computer unique to your deployment.
- Removed: This.tar file includes:
- Removed: a.zip file containing the virtual hard disks that need to be deployed on AWS
- Removed: a signature file
- Removed: a Cisco public certificate to validate the signature
- Removed: a readme file
- Removed: Extract the contents of the tar file using the command tar -xvf <tar filename> -C <Destination folder>.
- Removed: To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file.
- Removed: On successful signature validation, you see a message saying “Verified OK.“
- Removed: Extract the.zip file.

- Removed: You'll find two folders– Virtual Hard Disks and Virtual Machines –and a config file.
- Removed: Follow the steps provided by AWS to (optionally) create an S3 bucket and to create the vmimport service role.
- Removed: Upload the downloaded vhd files (forwarder-va.vhd and dynamic.vhd) to the S3 bucket.
- Removed: This should be the same S3 bucket as specified in the role-policy.json file.
- Removed: Use the AWS CLI to import the image.
- Removed: Create a file locally named "containers.json" for importing the image.
- Removed: The following is an example of a containers.json file.
- Removed: Specify the S3 bucket where you have saved the vhd images in this file.
- Removed: \[
- Removed: {
- Removed: "Description": "Forwarder",
- Removed: "Format": "vhd",
- Removed: "UserBucket": {
- Removed: "S3Bucket": "va-vhd-bucket",
- Removed: "S3Key": "forwarder-va.vhd"
- Removed: }
- Removed: },
- Removed: {
- Removed: "Description": "Dynamic",
- Removed: "Format": "vhd",
- Removed: "UserBucket": {
- Removed: "S3Bucket": "va-vhd-bucket",
- Removed: "S3Key": "dynamic.vhd"
- Removed: }
- Removed: }
- Removed: \]
- Removed: You must use the.vhd files to create the Amazon Machine Image and not the.ova file.
- Removed: Creating the AMI using the.ova file will result in the VA not being able to register to Umbrella.
- Removed: Use the AWS CLI command import-image to create import tasks:
- Removed: aws ec2 import-image --description "Umbrella VA" --license-type BYOL --disk-containers "file://containers.json"
- Removed: Note the AMI ID and verify that the import has been completed through the describe-import-image-tasks command:
- Removed: aws ec2 describe-import-image-tasks --import-task-ids <AMI ID>
- Removed: Once the VA Amazon Machine Image is created, use this image to launch multiple VAs.

- Removed: For more information, see Step 2.
- Removed: Launch the Virtual Appliance on Amazon Web Services.
- Removed: Step 2 – Launch the Virtual Appliance on Amazon Web Services
- Removed: Note Before performing this task, you must complete the one-time task of preparing the virtual appliance image on AWS.
- Removed: Tip Nitro based instance types and instance types that enable the Elastic Networking Adapter (ENA) are currently not supported.
- Removed: Refer to AWS documentation to determine if the instance type is Nitro based or uses ENA.
- Removed: Procedure
- Removed: Use the AWS console to launch Secure Access VA instances in AWS using the VA image you created in Step 1.
- Removed: Prepare the Virtual Appliance Image on Amazon Web Services.
- Removed: Choose a VM size with at least 1 VCPU and 1 GB RAM.
- Removed: Note Specifying a public IP address for the VA is a security risk and is not a supported configuration.
- Removed: In Secure Access, navigate to Connectors> DNS Forwarders.
- Removed: You should see the VA listed here with the dynamic IP address as its name.
- Removed: You can now configure the VA.
- Removed: For more information and the procedure, see Enter Configuration Mode on a VA Deployed in Azure, AWS, or Google Cloud Platform.
- Removed: Tip Route 53 Resolver can also be used to apply network-level protection to your AWS workloads.
- Removed: See How to Point AWS to Umbrella with New Route 53 Feature for more information.
- Removed: For a VA deployed on AWS, in addition to configuring the IP of the VA via the VA command line, you will also need to assign this IP to the VA instance through the AWS console.
- Removed: If this IP is different from the DHCP IP assigned by AWS, you can add it as the secondary IP for the instance.
- Removed: Deploy VAs in Google Cloud Platform
- Removed: Deploy Cisco Secure Access Virtual Appliances (VAs) in Google Cloud Platform.
- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Configure and set up each VA manually.
- Removed: Prerequisites
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: If you are using the VA on Google Cloud Platform (GCP) as a DNS server for your on-premise endpoints, then DNS traffic from these endpoints should not traverse through a Network Address Translation (NAT) device en route to the VA.
- Removed: The VA should receive DNS packets with the source IP as the internal IP of the endpoints.

- Removed: A Google Cloud Interconnect or dedicated MPLS or site-to-site VPN connection from your on-premise environment to GCP meets this requirement.
- Removed: A Linux system with the qemu-utils package installed, on which you can run qemu-img and tar commands.
- Removed: Only VAs running version 2.6 or above can be deployed in GCP.
- Removed: Configure Authentication for the Virtual Appliances
- Removed: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.
- Removed: Secure Access enables the Download Components button only after the API keys for the VAs are configured.
- Removed: For more information, see Configure Authentication for Virtual Appliances.
- Removed: Procedure
- Removed: Step 1 – Prepare the Virtual Appliance Instance Template on GCP.
- Removed: This is a one time task.
- Removed: Step 2 - Launch the Virtual Appliance on Google Cloud Platform.
- Removed: Perform this task for each VA after you have performed the one-time task of preparing the VA image.
- Removed: Step 1 – Prepare the Virtual Appliance Instance Template on GCP
- Removed: Note This is a one-time task to create an Instance Template that can be used to launch multiple virtual appliances in GCP.
- Removed: Procedure
- Removed: Navigate to Deployments> Configuration> Sites and Active Directory and click Download Components.
- Removed: Click Download for VA for Hyper-V.
- Removed: Secure Access generates and downloads a.tar file unique to your deployment.
- Removed: This.tar file includes:
- Removed: .zip file containing the virtual hard disks that need to be deployed on Google Cloud Platform
- Removed: Signature file
- Removed: Cisco public certificate to validate the signature
- Removed: README file
- Removed: Extract the contents of the tar file using the command tar -xvf <tar filename> -C <Destination folder>.
- Removed: To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file.
- Removed: When successful, you should see a message saying “Verified OK."
- Removed: Extract the.zip file.
- Removed: The.zip file contains two folders– Virtual Hard Disks and Virtual Machines –and a config file.
- Removed: Use the qemu-img convert commands to convert each of the VHD files to RAW format and resize them to a multiple of 1 GB.
- Removed: qemu-img convert -f vpc -O raw forwarder-va.vhd forwarder-va.raw
- Removed: qemu-img resize forwarder-va.raw -f raw 7G
- Removed: qemu-img convert -f raw -O raw dynamic.vhd dynamic.raw

- Removed: qemu-img resize dynamic.raw -f raw 1G
- Removed: Tar each raw file.
- Removed: Note GCP requires that each file be renamed as disk.raw before you tar it.
- Removed: GCP also requires tar to use the oldgnu format.
- Removed: mv forwarder-va.raw disk.raw
- Removed: tar --format=oldgnu -Sczf forwarder-va.tar.gz disk.raw
- Removed: mv disk.raw forwarder-va.raw
- Removed: mv dynamic.raw disk.raw
- Removed: tar --format=oldgnu -Sczf dynamic.tar.gz disk.raw
- Removed: mv disk.raw dynamic.raw
- Removed: Create a bucket in GCP Storage Engine or use an existing bucket and then upload both the forwarder-va.tar.gz and dynamic.tar.gz files to this bucket.
- Removed: Create two images in Google Compute Engine: one with source as the forwarder-va.tar.gz file and the other with source as the dynamic.tar.gz file.
- Removed: Each image is created with roughly the same size as its respective.tar.gz file (7 GB or 1 GB).
- Removed: Create an Instance Template in the Google Compute Engine using the forwarder image as the boot image and the dynamic image attached as a data disk.
- Removed: Choose a machine type with at least 1 vCPU and 1 GB memory.
- Removed: To select the 'forwarder' image as the boot disk, choose Change on the boot disk, and then choose the forwarder image from the Custom Images category.
- Removed: Note Do not click Create.
- Removed: Click Disks, Add new disk to attach the dynamic disk to the instance template.
- Removed: You must create a new disk with the source as the 'dynamic' image you created earlier.
- Removed: Failure to do so results in your VA not registering with Umbrella.
- Removed: Note Google Cloud does not allow you to create a disk of size less than 10 GB from the dynamic image.
- Removed: After you have added the new disk created from the dynamic image, you can click on Create to create the VA Instance template.
- Removed: Once the VA Instance template is created, use this image to launch multiple VAs.
- Removed: For more information, see Step 2.
- Removed: Launch the Virtual Appliance on Google Cloud Platform.
- Removed: Step 2 – Launch the Virtual Appliance on Google Cloud Platform
- Removed: Note Before performing this task, you must complete the one-time task of preparing the virtual appliance instance template
- Removed: Procedure
- Removed: Create VA instances based on the template.
- Removed: The VA will automatically pull a DHCP IP and register to Secure Access with this IP address.
- Removed: Note Specifying a public IP address for the VA is a security risk and is not a supported configuration.

- Removed: In Secure Access, navigate to Connectors> DNS Forwarders.
- Removed: You should see the VA listed here with the dynamic IP address as its name.
- Removed: You can now configure the VA.
- Removed: For information about configuring VAs, see Configure Virtual Appliances.
- Removed: Deploy VAs in KVM
- Removed: Deploy Cisco Secure Access Virtual Appliances (VAs) in KVM.
- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Configure and set up each VA manually.
- Removed: Prerequisites
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: A Linux system with qemu-utils package installed.
- Removed: Only VAs running 2.5 or above can be deployed in KVM.
- Removed: Virtual Appliance deployments in KVM are supported with specific Red Hat Linux and Ubuntu Linux versions only.
- Removed: KVM on Ubuntu Linux (supported LTS versions)
- Removed: KVM on Red Hat Linux (supported versions)
- Removed: Configure Authentication for the Virtual Appliances
- Removed: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.
- Removed: Secure Access enables the Download Components only after the API keys for the VAs are configured.
- Removed: For more information, see Configure Authentication for Virtual Appliances.
- Removed: Procedure for Deploying VAs in KVM
- Removed: Prerequisites
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: A Linux system with qemu-utils package installed.
- Removed: Only VAs running 2.5 or above can be deployed in KVM.
- Removed: Virtual Appliance deployments in KVM are supported with specific Red Hat Linux and Ubuntu Linux versions only.
- Removed: KVM on Ubuntu Linux (supported LTS versions)
- Removed: KVM on Red Hat Linux (supported versions)
- Removed: To successfully deploy a virtual appliance in a KVM envinronment, follow the steps as they are listed below:

- Removed: Step 1 – Download and Extract the KVM Installer
- Removed: Step 2 – Launch the Virtual Appliance on KVM
- Removed: Step 1 – Download and Extract the KVM Installer
- Removed: Procedure
- Removed: Navigate to Connect> DNS Forwarders and click Download Components.
- Removed: Click Download next to VA for KVM.
- Removed: Secure Access generates and downloads a.tar file unique to your deployment.
- Removed: This tar file includes:
- Removed: A zip file containing the KVM-compatible virtual hard disk images (.qcow2 format) and configuration files
- Removed: A signature file
- Removed: A Cisco public certificate to validate the signature
- Removed: A readme file
- Removed: Extract the contents of the tar file using the tar -xvf <tar filename> -C <Destination folder> command.
- Removed: Verify the integrity of the downloaded file by following the signature validation instructions in the readme file.
- Removed: On a successful verification, the message Verified OK is displayed.
- Removed: Extract the.zip file.
- Removed: The extracted contents include the Virtual Hard Disks folder, the Virtual Machines folder, and a configuration file.
- Removed: The Virtual Hard Disks folder contains the KVM-compatible.qcow2 files (namely, dynamic.qcow2 and forwarder-va.qcow2).
- Removed: Step 2 – Launch the Virtual Appliance on KVM
- Removed: Procedure
- Removed: Open the Virtual Machine Manager on your Linux system running KVM and click Create a new virtual machine.
- Removed: In the first step of the wizard, choose Import existing disk image.
- Removed: Provide the existing storage path to your forwarder-va.qcow2.
- Removed: Set the OS type to Linux and click Forward.
- Removed: Set the memory and CPU settings to at least 1 CPU and 1 GB RAM and click Forward.
- Removed: In the last step of the wizard, select Customize configuration before install and then click Finish.
- Removed: Select Add Hardware.
- Removed: Select Storage, add or create custom storage, add the dynamic disk, and then click Finish.
- Removed: You should then see two disks.
- Removed: Click Begin installation to create the VA.
- Removed: If your network supports DHCP, the VA will get auto-configured with a DHCP IP address and will register to Umbrella using this IP.
- Removed: You can configure the VA on KVM through two mechanisms:

- Removed: Press Ctrl+B on the VA console and entering the Configuration mode.
- Removed: Or
- Removed: Initiate an SSH connection to the DHCP IP—this IP can be retrieved in Secure Access—and enter Configuration mode.
- Removed: What to do next
- Removed: You can now configure the VA.
- Removed: For information about configuring VAs, see Configure Virtual Appliances.
- Removed: Deploy VAs in Nutanix
- Removed: Deploy Cisco Secure Access Virtual Appliances in Nutanix.
- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Removed: It is critical that these VAs are not cloned or copied in any way.
- Removed: Configure and set up each VA manually.
- Removed: Before you begin
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: Virtual Appliance deployments are supported on the current LTS version of Nutanix AHV only.
- Removed: Configure Authentication for the Virtual Appliances
- Removed: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.
- Removed: Secure Access enables the Download Components button only after the API keys for the VAs are configured.
- Removed: For more information, see Configure Authentication for Virtual Appliances.
- Removed: Procedure
- Removed: Navigate to Connectors> DNS Forwarders and click Download Components.
- Removed: Click Download for VA for hyper-V.
- Removed: Secure Access generates and downloads to your computer a.tar file unique to your deployment.
- Removed: This tar file includes:
- Removed: a.zip file containing the virtual hard disks that need to be deployed on Nutanix
- Removed: a signature file
- Removed: a Cisco public certificate to validate the signature
- Removed: a readme file
- Removed: Extract the contents of the tar file.
- Removed: To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file.
- Removed: When successful, a message saying Verified OK will appear.
- Removed: Run:

- Removed: tar -xvf <tar filename> -C <Destination folder>
- Removed: Extract the downloaded zip file.
- Removed: You will find two folders– Virtual Hard Disks and Virtual Machines –and a config file.
- Removed: Navigate to the Virtual Hard Disks folder and find the forwarder-va.vhd and dynamic.vhd files.
- Removed: Log into the Nutanix AHV console, navigate to Settings> Image Configuration, and create two images (VAForwarder and VADynamic) by uploading the forwarder-va.vhd and dynamic.vhd respectively.
- Removed: Create a new VM with at least 1 VCPU (1 core), 1 GB RAM, and 1 NIC.
- Removed: Add a new disk using the VAForwarder image.
- Removed: Choose the operation Clone from Image Service and Bus Type as SCSI.
- Removed: Remove the CD-ROM.
- Removed: Add another disk using the VADynamic image with operation as Clone from Image Service and Bus Type as SCSI.
- Removed: Note The disk order is important.
- Removed: The VAForwarder should be Disk 0, the VADynamic should be Disk 1.
- Removed: You can now power on the VA and configure it using either the console or by initiating an SSH connection to the VA.
- Removed: For information about configuring VAs, see Configure Virtual Appliances.
- Removed: For more information about how to enhance throughput of the VA on Nutanix, see Enabling RSS Virtio-Net Multi-Queue by Increasing the Number of VNIC Queues.
- Removed: Deploy VAs in Alibaba Cloud
- Removed: This guide describes how to deploy Cisco Secure Access Virtual Appliances in the Alibaba Cloud environment.
- Removed: Note You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site.
- Removed: It is critical that these VAs are not cloned or copied.
- Removed: Configure and set up each VA manually.
- Removed: Prerequisites
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Removed: For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Removed: An Alibaba account.
- Removed: Create your account at https://www.alibaba.com/.
- Removed: A qemu-utils package installed, such as Homebrew, to run the qemu-img and tar commands.
- Removed: Only VAs running version 3.6.1 or above can be deployed in Alibaba.
- Removed: An SSH client (for example, PuTTY on Windows or Terminal on Macintosh) to access the VA console.
- Removed: Configure Authentication for the Virtual Appliances
- Removed: Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.

- Removed: Secure Access enables the Download Components only after the API keys for the VAs are configured.
- Removed: For more information, see Configure Authentication for Virtual Appliances.
- Removed: Procedure
- Removed: Download and Extract the Hyper-V Installer.
- Removed: This is a one time task.
- Removed: Alibaba Cloud Setup
- Removed: Create a Custom Image.
- Removed: Perform this task for each VA after performing the one-time task of preparing the VA images.
- Removed: Deploy the Secure Access VAs from the Imported Custom Image
- Removed: First-time Login to Secure Access VA
- Removed: Related Topics
- Removed: Dual-NIC Support on the Secure Access VA
- Removed: IP Addressing
- Removed: Anycast Configuration Support
- Removed: DNS Performance on Alibaba ECS Instances
- Removed: Extensions on Alibaba ECS Instances
- Removed: Download and Extract the Hyper-V Installer
- Removed: Procedure
- Removed: Navigate to Connectors> DNS Forwarders and click Download Components.
- Removed: Click Download for VA for Hyper-V.
- Removed: Secure Access generates and downloads a tar file unique to your deployment.
- Removed: This tar file includes:
- Removed: a zip file containing the virtual hard disks that need to be deployed on Hyper-V
- Removed: a signature file
- Removed: a Cisco public certificate to validate the signature
- Removed: a readme file
- Removed: Extract the contents of the tar file using the command tar -xvf <tar filename> -C <Destination folder>.
- Removed: To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file.
- Removed: When successful, there will be a message saying “Verified OK."
- Removed: Extract the.zip file.
- Removed: You'll find two folders– Virtual Hard Disks and Virtual Machines –and a config file.
- Removed: In Windows Explorer, navigate to the Virtual Hard Disks subfolder within the extracted download folder created in Step 1.
- Removed: Note the two VA files, dynamic and forwarder-va.

- Removed: Convert the forwarder-va.vhd file to.raw format:
- Removed: qemu-img convert -f vpc -O raw forwarder-va.vhd forwarder-va.raw
- Removed: Zip the forwarder-va.raw file.
- Removed: Note Alibaba only allows for 5Gb uploads.
- Removed: Alibaba Cloud Setup
- Removed: This section describes the configuration requirements within Alibaba Cloud to support deploying the Secure Access VA instances to your virtual private cloud (VPC).
- Removed: For more details on setting up a VPC and other components, please refer to Alibaba's Cloud Documentation here.
- Removed: Create an Alibaba Virtual Private Cloud (VPC)
- Removed: Create a Bucket for the Umbrella VAs
- Removed: Configure a ZIP Package Decompression Rule
- Removed: Upload the Secure Access VHD Images to the OSS Bucket
- Removed: Create an Alibaba Virtual Private Cloud (VPC)
- Removed: A virtual private cloud (VPC) is required to deploy your Alibaba Cloud resources, such as Secure Access VAs.
- Removed: Procedure
- Removed: Log in to your Alibaba Cloud Account and log on to the VPC console.
- Removed: In the top navigation bar, select the region where you want to deploy the VPC.
- Removed: Note The VPC and the cloud resources that you want to deploy in the VPC must belong to the same region.
- Removed: On the VPCs page, click Create VPC.
- Removed: On the Create VPC page, set the required parameters and click OK.
- Removed: What to do next
- Removed: To find more information about this, please click here.
- Removed: Create a Bucket for the Secure Access VAs
- Removed: An Object Storage Service (OSS) bucket is needed.
- Removed: Alibaba OSS is a secure, cost-effective, and highly reliable cloud storage service that allows for the storage of large amounts of data.
- Removed: Procedure
- Removed: On the Alibaba Cloud Console home page, select Object Storage Service (OSS).
- Removed: In the left-side navigation pane, click Buckets.
- Removed: On the Buckets page, click Create Bucket.
- Removed: In the Create Bucket panel, enter the Bucket Name and Region.
- Removed: The bucket must be in the same region as the VPC in which the Secure Access VAs are to be deployed.
- Removed: Keep the default settings for other parameters or configure the parameters after the bucket is created.
- Removed: Click OK.

- Removed: After the bucket is created, the Created message is displayed.
- Removed: Configure a ZIP Package Decompression Rule
- Removed: Alibaba Cloud accepts uploads of objects up to 5 GB in size using the OSS console.
- Removed: Because the Secure Access Forwarder VA is larger than 5 GB, the forwarder-va.vhd file needs to be converted to.raw format and then compressed to a zip file, as described in Download and Extract the Hyper-V Installer.
- Removed: Procedure
- Removed: In the left navigation pane of the OSS console, click Buckets.
- Removed: On the Buckets page, find and click the desired bucket.
- Removed: In the left navigation tree, choose Data Processing> Decompress ZIP Package.
- Removed: Click Start Activation and follow the prompts.
- Removed: Once activation is complete, go to the bucket and click Decompress ZIP Package.
- Removed: In the Decompress ZIP Package panel, configure the following parameters:
- Removed: Service Authorization - Authorize Function Compute to read data from and write data to OSS and to execute functions.
- Removed: Click Authorize.
- Removed: Complete authorization on the page that appears.
- Removed: Authorize Trigger - Authorize OSS to access Function Compute.
- Removed: Click Authorize.
- Removed: Complete authorization on the page that appears.
- Removed: If OSS is authorized to access Function Compute, the Trigger Role parameter is displayed instead of the Authorize Trigger parameter.
- Removed: Destination Directory - To store the objects extracted from a ZIP package in a subdirectory that has the same name as the package in the destination directory, select Add the compressed object name to the destination directory.
- Removed: Click OK.
- Removed: What to do next
- Removed: Now that the bucket is created, click Go to Bucket.
- Removed: Alternatively, click Buckets in the left-side navigation pane and click the name of the created bucket.
- Removed: Upload the Secure Access VHD Images to the OSS Bucket
- Removed: Upload the Secure Access VHD images that were downloaded in Download and Extract the Hyper-V Installer to your bucket.
- Removed: Procedure
- Removed: Select your bucket, choose Files> Upload, and click here to upload.
- Removed: Select the compressed forwarder-va zip file on your local drive.
- Removed: Wait for the automatic decompression to be triggered before continuing.
- Removed: The forwarder-va.raw file should be seen in the table on the Upload page if it is uploaded successfully.
- Removed: Select the dynamic.vhd on your local drive.

- Removed: Given the small size of this file, no conversion or compression is required.
- Removed: The file will be displayed in the table on the Upload page if it is uploaded successfully.
- Removed: Click View Details, the click Copy File URL.
- Removed: This URL is needed in later steps when creating a custom image.
- Removed: Create a Custom Image
- Removed: Procedure
- Removed: Select the Alibaba Elastic Compute Service (ECS).
- Removed: Select Instances & Images> Images> Custom Images.
- Removed: Click Import Image.
- Removed: Paste the forwarder-va.raw URL in the Import Image window.
- Removed: See Upload the Secure Access VHD Images to the OSS Bucket for where to find the URL.
- Removed: Note If the following error is seen, ECS does not have access to the OSS resources.
- Removed: Enable access by clicking the here hyperlink shown.
- Removed: If necessary, click Confirm Authorization Policy.
- Removed: Repeat the Import Image action and fill the necessary fields as below.
- Removed: Check the Configure Disk Attributes box and adjust the Disk SizeGiB setting.
- Removed: Note Make sure that the forwarder-va.raw disk size is 6.5 GB.
- Removed: Repeat for the dynamic.vhd file.
- Removed: Note Make sure that the dynamic.vhd disk size is 20 MB.
- Removed: If the image is successfully created, the following window is shown.
- Removed: Note that if the forwarder-va.vhd is uploaded instead of.raw image, or if the size is not supported, the following error is shown.
- Removed: Deploy the Secure Access VAs from the Imported Custom Image
- Removed: An Elastic Compute Service (ECS) image provides the information that is required to create an ECS instance.
- Removed: An image must be specified when creating an ECS instance.
- Removed: An image is a copy of data from one or more disks.
- Removed: An instance image can contain data from only the system disk or from both the system disk and data disks.
- Removed: Procedure
- Removed: Navigate to Elastic Compute Service> Instances.
- Removed: Click Create Instance.
- Removed: Complete the following Basic Configuration settings:
- Removed: Select the Region and zone.
- Removed: Select a region that is close to your geographical location to reduce latency.
- Removed: After an instance is created, the region and the zone of the instance cannot be changed.
- Removed: Select the Instance type.

- Removed: Different instance types have different CPU, RAM and throughput capacity.
- Removed: Note It is recommended to have an instance type having a minimum capability of ecs.c6.xlarge for optimal DNS performance, with enhanced clock speed as the VA is a DNS proxy.
- Removed: Select the Custom image, Duration and click Next.
- Removed: Note The System Disk size increase will not help scale the VA as dynamic disk size change is not supported.
- Removed: The VA only supports a 7 GB system and 1 GB data disk.
- Removed: Select the VPC and VSwitch as per the topology.
- Removed: In this example, default values are selected.
- Removed: The Virtual Appliance will have a private IP with which it will be registered with the dashboard.
- Removed: Specify the private IP so that it does not change on power cycle.
- Removed: If a Security Group has already been created, the same can be reused.
- Removed: This example proceeds with basic configuration and enable the ports later as per VA pre-requisites.
- Removed: Alibaba cloud does not support password setting for users other than "root", so the vmadmin password cannot be set through the Cloud and it has to be Set Later through SSH or console access.
- Removed: Select the Resource Group in the next window.
- Removed: In this example, the Default Resource Group is used.
- Removed: Click Create Order and proceed.
- Removed: Once the subscription is created, the instance will show up on the ECS console.
- Removed: What's Next
- Removed: Go to the newly created instance and edit Security Group rules; see the virtual appliances (VA) network requirements.
- Removed: The vmadmin password can be reset by doing remote SSH via the public IP as port 3389 is allowed by default.
- Removed: If the instance does not have a public IP, a Bastion host has to be created in the same region to access it via Private IP as per Alibaba documentation.
- Removed: Please note that connecting to the VA through the Alibaba Cloud workbench will fail due to the change password prompt, so the first time password reset has to happen via SSH.
- Removed: Once the password is reset, the Alibaba workbench can be used to login to the console.
- Removed: After the password is set, you can SSH to the VA via the ECS Workbench as well.
- Removed: First-time Login to Secure Access VA
- Removed: There are three ways to do the first-time login to the Secure Access VA:
- Removed: Procedure
- Removed: If the VA has a public IP associated, use the default vmadmin/<orgid> credentials and reset the password.
- Removed: If the VA is inside private network, create another OAM VM (not the Alibaba bastion) inside the same network and SSH through the private IP using the vmadmin/<orgid> credentials and reset the password.
- Removed: ECS instances can also be added to a Bastion host enterprise edition available on the Alibaba cloud; refer to the following guidelines.

- Removed: When doing so, please note that the password should be reset from the ECS instance UI also before trying to login through the Bastion.
- Removed: Please note that even though the instance password is reset through UI, it won't apply to the instance as we do not have a root account.
- Removed: Related Topics
- Removed: Dual-NIC Support on the VA
- Removed: IP Addressing
- Removed: Anycast Configuration Support
- Removed: DNS Performance on Alibaba ECS Instances
- Removed: Extensions on Alibaba ECS Instances
- Removed: Dual-NIC Support on the VA
- Removed: In the Alibaba Cloud elastic network interfaces (ENIs) are logical networking components that represent virtual NICs, providing network connectivity and IP addresses for Elastic Compute Service (ECS) instances deployed in virtual private clouds (VPCs).
- Removed: The Secure Access VA supports a dual-NIC configuration.
- Removed: This dual-NIC configuration is intended to enable DMZ deployment of a VA for traffic segregation with one network interface being used for outbound communication and the other network interface used for internal communication.
- Removed: There is no change to existing behavior if the VA is deployed with a single NIC.
- Removed: Configuring more than two NICs on the VA is not supported.
- Removed: For more information about Secure Access Dual-NIC support and how to configure Alibaba ENIs, see the following:
- Removed: Configure Dual-NIC Support on the VA
- Removed: Elastic Network Interfaces
- Removed: Note: Do not connect more than one ENI the same VSwitch.
- Removed: Network issues will result.
- Removed: IP Addressing
- Removed: General Guidelines
- Removed: The Secure Access VA supports both IPv4 and IPv6 addressing (dual stack).
- Removed: However there are some observations on the Alibaba cloud regarding IP addressing:
- Removed: While the Alibaba ECS ENI supports multiple private IP address, please note that the Secure Access VA only supports a single IPv4 or Single IPv4 + IPv6 pair per ENI.
- Removed: One private IPv4 and one private IPv6 address can be added to the Secure Access VA.
- Removed: The Alibaba Cloud is not supporting public IPv6 address to ECS instances.
- Removed: An IPv6 gateway can be set up at the VPC level and establish connectivity to Secure Access global IPv6 resolvers.
- Removed: However, it has been observed during testing that IPv6 packets are not getting a response even after setting up the gateway.
- Removed: This has been observed in the Germany Frankfurt Region.

- Removed: Support for IPv6 Addressing
- Removed: The following are observations regarding IPv6 addressing on the Alibaba Cloud:
- Removed: The IPv6 address range should be enabled on the VSwitch.
- Removed: By default, when creating an Elastic Compute Service (ECS) instance, an IPv4 address instead of an IPv6 address is assigned to the instance.
- Removed: To have the instance communicate over IPv6, configure an IPv6 address for the instance.
- Removed: IPv6 addressing is not supported on every ECS instance types.
- Removed: It depends on system resources selected during deployment.
- Removed: Refer to ECS instance type family.
- Removed: See Configure IPv6 addresses for information on how to configure an IPv6 address for the instance.
- Removed: Anycast Configuration Support
- Removed: The Umbrella VA enables the use of Anycast DNS addressing within an enterprise.
- Removed: The VA currently supports enabling Anycast using the BGP protocol.
- Removed: This requires support for BGP on the VA's neighboring router, or any router that is reachable from the VA within 255 hops.
- Removed: See the Configure Anycast topic for information about how to configure Anycast on the VA.
- Removed: In addition, keep the following in mind when configuring Anycast on the Alibaba cloud:
- Removed: Configure an additional route on the VSwitch for the Anycast IP address for packets with the destination IP as Anycast.
- Removed: The Anycast IP/network can be routed only per single ECS or ENI per VSwitch, where the next hop is the VA instance on which Anycast is enabled and 10.0.0.5 is the Anycast IP.
- Removed: Note VAs participating in anycast DNS should belong to different VSwitches or different networks; the following image shows the route table of a VSwitch configured with an Anycast route.
- Removed: DNS Performance on Alibaba ECS Instances
- Removed: Different instance types have different CPU, RAM and throughput capacity.
- Removed: Latency and throughput testing was performed on the following instances using dnsperf.
- Removed: The results captured after running the test for 1 minute are collected in the following table.
- Removed: From these statistics, it is recommended to have an instance type having a minimum capability of ecs.c6.xlarge for optimal DNS performance.
- Removed: Refer to the Alibaba Cloud Instance family documentation for information on instance configurations.
- Removed: Instance Type
- Removed: Maximum DNS Throughput
- Removed: ecs.c6.large
- Removed: 2000 qps
- Removed: ecs.c6.xlarge
- Removed: 5000 qps
- Removed: ecs.c6.2xlarge

- Removed: 10000 qps
- Removed: ecs.hfc6.large
- Removed: 2200 qps
- Removed: ecs.g6e.large
- Removed: 3000 qps
- Removed: Extensions on Alibaba ECS Instances
- Removed: Alibaba ECS instance supports installing agents/plugins for monitoring purpose, example CloudMonitor argusagent.
- Removed: It is not recommended to do so as it puts the VA under risk for root partition exhaustion.
- Removed: On a newly deployed VA instance, the memory usage is 66% due to the aliyun default packages installation.

Add a SaaS API Rule to the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/add-a-saas-api-rule.html

- Added: Note: A maximum of 1,000 users can be added as exclusions in a policy.

Set up the Zero Trust Access App for iOS Devices

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/client-based-za-mobile-intro/set_up_the_zero_trust_access_app_for_ios_devices.html

- Removed: Configure a client-based posture profile that includes iOS devices and supported iOS versions: Navigate to Secure> Endpoit Posture Profiles.
- Added: Configure a client-based posture profile that includes iOS devices and supported iOS versions: Navigate to Secure> Endpoint Posture Profiles.

Log Formats and Versioning

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/logging-intro/log_formats_and_versioning.html

- Removed: This field is currently used to identify YouTube channel names only.
- Added: This field is used exclusively for YouTube Tenant Control.
- Removed: This field is currently used to identify YouTube categories only.
- Added: This field is used exclusively for YouTube Tenant Control.

App Discovery Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/app-reports-intro/app-discovery-report.html

- Removed: View DNS requests and traffic by App Risk.
- Added: View Network activity by app risk.
- Removed: Select Web and review Traffic (bytes in and out) by App Risk for the last 30 days.
- Added: Toggle between DNS requests, Web traffic and Firewall events (bytes in and out) by App Risk for the last 30 days.
- Removed: Filter by label.
- Added: View by label.

- Removed: Filter by date.
- Added: Select all–Selects all app types
- Added: Filter by usage date.
- Removed: Navigate to Reporting> Core Reports> App Discovery and click one of the app labels to open the Apps Grid.
- Added: Navigate to Monitor> Reports> App Discovery and click one of the app labels to open the Apps Grid.
- Removed: Hover over the Risk Score icon to display the Risk Summary for the app.
- Removed: Note If you apply a Custom risk score to an App, it will be noted in the Apps Grid display as shown below:
- Added: Note If you apply a Custom risk score to an App, it will be noted in the Apps Grid display.
- Removed: Click the Download CSV icon to download this information as a CSV file.
- Removed: Click Attributes.
- Added: Click Security attributes.
- Added: Click Web traffic & DNS.
- Added: This pane displays the total and blocked DNS, web, and firewall traffic observed for this application (in bytes).
- Removed: You have two choices:
- Removed: To change the risk score for an app from the Apps Grid, hover over the risk score for an app to view its Risk Summary.
- Removed: From the Risk Summary, click on CHANGE RISK SCORE to display the Risk Score Change dialog.
- Added: From the Risk Summary, click on Change to display the Risk Score Change dialog.
- Removed: Click SAVE.
- Added: Click Save.
- Removed: To change the label for an app from the Apps Grid, hover over its label to view the label menu.
- Removed: To change the label for an app from its Details page, click the name of the app on the Apps Grid, then on the Details page hover over the label to view the Label menu.
- Added: To change the label for an app from the Apps Grid, click… and Change label.
- Added: To change the label for an app from its Details page, click the name of the app on the Apps Grid, then on the Details page, click Change against Label to view the Label menu.
- Added: Unreviewed–The app is not reviewed to be used in your environment.
- Removed: Choose an app to control and click Control this app.
- Added: Choose an app to control and click Add to application list.
- Removed: Details include the total and blocked traffic in bytes.
- Removed: Navigate to the Identities section of the app details and view the total Traffic and Blocked Traffic.
- Added: Navigate to the Identities section of the app details and view the total Web Traffic.

About the Remote Access Log Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/remote-access-log-intro/remote-access-log-report.html

- Removed: For failed posture checks, the Remote Acess Logs now provide a section in the details panel that include the status, the region, the affected posture profile, and any detected errors such as a disabled firwall or a missing executionable file. an example of such failure is shown here:
- Added: For failed posture checks, the Remote Access Logs now provide a section in the details panel that include the status, the region, the affected posture profile, and any detected errors such as a disabled firewall or a missing executionable file.

Added Pages

- Deploy VAs in Hyper-V for Windows 2012 or Higher: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_hyper-v_for_windows_2012_or_higher.html
- Deploy VAs in VMware: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_vmware.html
- Deploy VAs in Microsoft Azure: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_microsoft_azure.html
- Deploy VAs in Amazon Web Services: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_amazon_web_services.html
- Deploy VAs in Google Cloud Platform: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_google_cloud_platform.html
- Deploy VAs in KVM: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_kvm.html
- Deploy VAs in Nutanix: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_nutanix.html
- Deploy VAs in Alibaba Cloud: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/virtual-appliances-intro/deploy_vas_in_alibaba_cloud.html

Cisco Secure Access Documentation Changes 2026-10-05

Lists changes to Cisco Secure Access documentation published on October 5, 2026.

Summary

- Document URL: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html
- Snapshot date: 2026-10-05
- Pages checked: 459
- Pages changed: 5
- Pages added: 0
- Pages removed: 0

Changed Pages

Manage Client-Based Zero Trust Access in Secure Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/zero-trust-access-intro/manage-client-based-zta-overview.html

- Removed: Table of supported ZTA Functionality and Required Versioning
- Removed: ZTA Functionality
- Removed: Supported Platforms
- Removed: Minimum Secure Client Version Required
- Removed: SAML Enrollment
- Removed: Android
- Removed: ChromeOS
- Removed: All versions.
- Removed: Zero Touch Enrollment
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: 5.1.9+
- Removed: Certificate-based Enrollment
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: 5.1.9+
- Removed: Step-up Authentication
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: ChromeOS
- Removed: All versions.
- Removed: Trusted Network Detection (Secure Internet Access and Secure Private Access)
- Removed: Windows
- Removed: MacOS
- Removed: mobile iOS 5.1.18+
- Removed: Linux
- Removed: 5.1.10+
- Removed: Note Virtual interfact detection is only supported with version 5.1.13 and later.
- Removed: Trusted Network Detection (DNS Server or DNS Domain)
- Removed: Windows
- Removed: MacOS
- Removed: Linux

- Removed: 5.1.10+
- Removed: Posture Profiles
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: iOS
- Removed: Android
- Removed: ChromeOS
- Removed: All versions.
- Removed: Posture Profiles with DNS-over-HTTPS (DoH)
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: 5.1.8+
- Removed: Posture Profiles with Duo Desktop
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: All versions.
- Removed: Posture Profile with Duo Desktop
- Removed: Windows
- Removed: MacOS
- Removed: All versions.
- Removed: Pause ZTA with Cisco Secure Client
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: 5.1.13+
- Removed: Custom ZTA Profiles
- Removed: Windows
- Removed: MacOS
- Removed: iOS
- Removed: Android
- Removed: ChromeOS
- Removed: All versions.

- Removed: Traffic Steering: Secure Private Access
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: iOS
- Removed: Android
- Removed: ChromeOS
- Removed: All versions.
- Removed: Traffic Steering: Secure Private Access (DNS)
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: 5.1.16+
- Removed: Traffic Steering: Secure Internet Access for specific internet destinations
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: iOS
- Removed: Android
- Removed: ChromeOS
- Removed: All versions.
- Removed: Traffic Steering: Secure Internet Access for all internet destinations
- Removed: Windows
- Removed: MacOS
- Removed: Mobile iOS 26.5
- Removed: Linux
- Removed: Desktop 5.1.11+
- Removed: Mobile iOS 5.1.18+
- Removed: Traffic Steering: Universal ZTNA (cloud or local)
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: 5.1.11+
- Removed: Traffic Steering: Universal ZTNA (local only)
- Removed: Windows

- Removed: MacOS
- Removed: Linux
- Removed: 5.1.11+
- Removed: Network Location Objects
- Removed: Windows
- Removed: MacOS
- Removed: Linux
- Removed: Android (Generic)
- Removed: Desktop 5.1.19
- Removed: Android (Generic) 5.1.18
- Added: Cached Block Verdict Types
- Added: 5.1.17+
- Added: MDM Enrollment
- Added: 5.1.19+
- Removed: Table 6.

Manage the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/manage-data-protection-policies.html

- Added: Monitoring DLP Rules That Use Only File Size Without Data Classification
- Added: When a DLP rule is configured using File Control with a custom File Size threshold and no Data Classification, and the action is set to Monitor, uploads for certain MIME types are not logged intentionally.
- Added: This exclusion applies to these MIME types:
- Added: text/plain
- Added: application/octet-stream
- Added: application/json
- Added: application/x-ndjson
- Added: application/reports+json
- Added: application/dns-message
- Added: application/protobuf
- Added: application/x-protobuf
- Added: message/ohttp-req
- Added: application/csp-report
- Added: The Block action logs all uploads regardless of MIME type.
- Added: This behavior is intended and applies only to file-size-only rules, without Data Classification.

Set up the Zero Trust Access App for iOS Devices

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/client-based-za-mode-intro/set_up_the_zero_trust_access_app_for_ios_devices.html

- Removed: Configure a client-based posture profile that includes iOS devices and supported iOS versions: Navigate to Secure> Endpoint Posture Profiles.
- Added: Configure a client-based posture profile that includes iOS devices and supported iOS versions: Navigate to Secure> Endpoit Posture Profiles.

Manage Endpoint Data Loss Prevention Using Cisco Secure Client for Windows and Mac

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/edp-secure-client-intro/c_Manage_EDLP_Using_Cisco_Secure_Client__1.html

- Removed: The Endpoint DLP module uses information from the choice file to enroll itself to the Secure Access cloud using the user identity certificate and additional device information.
- Removed: Ensure you store the choice file in a secure location.
- Removed: The Endpoint DLP module uses information from the enrollment choice file and the user identity certificate, along with device information, to enroll the device choice file in Secure Access cloud.
- Removed: Store the choice file in a secure location.
- Removed: The Endpoint DLP module uses information from the enrollment choice file and the user identity certificate, along with device information, to enroll the device in Secure Access cloud.
- Removed: Store the choice file in a secure location.

About the Remote Access Log Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/remote-access-log-intro/remote-access-log-report.html

- Added: For failed posture checks, the Remote Acess Logs now provide a section in the details panel that include the status, the region, the affected posture profile, and any detected errors such as a disabled firwall or a missing executionable file. an example of such failure is shown here:

4 September 2026 updates

Topics:

- Cisco Secure Access Documentation Changes 2026-09-28
- Cisco Secure Access documentation changes 2026-09-21

Lists the Secure Access Help updates published during September 2026 and groups them by dated change-log entry.

Cisco Secure Access Documentation Changes 2026-09-28

Lists changes to Cisco Secure Access documentation published on September 28, 2026.

Summary

- Document URL: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html
- Snapshot date: 2026-09-28
- Pages checked: 459
- Pages changed: 8
- Pages added: 2
- Pages removed: 0

Changed Pages

Manage the Access Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/access-policies-intro/manage-access-policy.html

- Added: For users implementing Kerberos authentication with AD, we recommend reviewing the appropriate Microsoft documentation about configuring the correct ports and private resources to plan for for AD communication. to understand how to optimize the location of a domain controller, see this documentation.

Manage Client-Based Zero Trust Access in Secure Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/zero-trust-access-intro/manage-client-based-zta-overview.html

- Added: Multi-site Environments
- Added: If you organization has multiple Active Directory sites then the IP address of the client (the LDAP source IP) can affect the resultant selection of AD Site and therefore the selected domain controllers.
- Added: Consider the IP address of the client in different deployment modes:
- Added: Network Tunnels - In Network Tunnel mode the client IP will be affected by NAT.
- Added: The source IP will be replaced with an IP address from the CGNAT IP address range.
- Added: Therefore clients will typically be associated with the “Default Site” in Active Directory.
- Added: The Domain Controllers in the default site must be accessible in the Access Policy.
- Added: Resource Connectors - In Resource Connector mode the client IP will be affected by NAT.
- Added: The source IP will be the Resource Connector IP address.
- Added: The IP address of the resource connector(s) should be assigned to an appropriate AD Site in Active Directory Sites & Services.
- Added: The Domain Controllers in this site must be accessible in the Access Policy.
- Removed: Traffic Steering: Secure Internet Access for specific interenet destinations
- Added: Traffic Steering: Secure Internet Access for specific internet destinations
- Removed: Traffic Steering: Secure Internet Access for specific interenet destinations

- Removed: Traffic Steering: Secure Internet Access for all interenet destinations
- Added: Traffic Steering: Secure Internet Access for specific internet destinations
- Added: Traffic Steering: Secure Internet Access for all internet destinations
- Removed: Traffic Steering: Secure Internet Access for specific interenet destinations
- Added: Traffic Steering: Secure Internet Access for specific internet destinations
- Removed: Traffic Steering: Secure Internet Access for all interenet destinations
- Added: Traffic Steering: Secure Internet Access for all internet destinations

Traffic Steering for Zero Trust Access Client-Based Connections

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/zero-trust-access-intro/traffic_steering_for_zero_trust_access_client-based_connections.html

- Added: If you are implementing Kerberos authentication wit Active Directory (AD), we strongly recommend adding the AD DNS SRV recorcd names to the DNS Steering you just created.
- Added: For more information from Microsoft, see How to verify that SRV DNS records have been created for a domain controller for more information.
- Added: Microsoft documents specific SRV DNS records for you, see 6.3.2.3 SRV Records sepcifically for more information.
- Removed: Full Admin user role.
- Removed: For more information, see Manage Accounts.
- Added: Zero Trust Access profiles provides distinct access experiences for different users and groups.
- Added: You can view, edit, and delete the profiles for private and internet access.
- Added: Wildcard matching in ZTA profiles does not include exact-domain matchinng; it can represent only one token and cannot represent multiple tokens.
- Added: When you add a domain like google.com to an allow list, it implicitly allows all subdomains like *.google.com, but if you want to block only a specific subdomain such as news.google.com, you must add the entire FQDN as your DNS steering destination.
- Added: For users implementing Kerberos authentication with AD, we recommend reviewing the appropriate Microsoft documentation about configuring the correct ports and private resources to plan for for AD communication. to understand how to optimize the location of a domain controller, see this documentation.
- Added: Be aware of the ZTA limitations when creating a profile.
- Added: See Limitations and Range Limits for more information.
- Added: You must be a Full Admin to proceed with this procedure.
- Added: See Manage Accounts for more information.
- Added: Zero Trust Access profiles are an ordered list where the order of profiles determines their priority.
- Added: The last profile in the list is always the Default ZTA Profile.
- Added: A user's Zero Trust Access client receives settings from the first matching Zero Trust Access profile in profile order.
- Added: The profile must match both the user's membership and the endpoint operating system.
- Added: Default profile includes all users in the org and all client Zero Trust Access enabled private and internet resources.

- Added: Use the following procedure to modify the user's access:

Add a Real Time Rule to the Data Loss Prevention Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/data-loss-prevention-intro/add_a_real_time_rule_to_the_data_loss_prevention_policy.html

- Added: Note: Files encrypted with Digital Rights Management (DRM) or Microsoft Sensitivity Labels cannot be decrypted for deep content inspection or text extraction.
- Added: Because content cannot be extracted from encrypted files, DLP content and pattern-matching rules cannot be evaluated against the file body.
- Added: As a result, these files are allowed by default unless explicitly governed by supported metadata or transport-level policies.

Endpoint Data Loss Prevention using Cisco Secure Client

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/edlp-secure-client-intro.html

- Added: Troubleshoot Endpoint Data Loss Prevention for Linux
- Added: This concept describes how to locate Endpoint DLP logs and troubleshoot common enrollment errors on Linux devices.
- Added: Uninstall Cisco Secure Client Endpoint DLP on Linux
- Added: Use this procedure to uninstall the Cisco Secure Client - Endpoint Data Loss Prevention (DLP) module from your Linux device.
- Added: This guide provides the specific command-line instructions required to remove the software from both Ubuntu and Enterprise Linux distributions effectively.

Manage Endpoint Data Loss Prevention Using Cisco Secure Client for Windows and Mac

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/edp-secure-client-intro/c_Manage_EDLP_Using_Cisco_Secure_Client__1.html

- Removed: Versions: macOS 15, macOS 26
- Added: Versions: macOS 15, macOS 26, macOS 27
- Removed: Step 4 - Deployment on user devices
- Removed: Step 4 - Install the User Certificate and Enrollment Choice File on User Devices for macOS
- Removed: Step 4 - Install the User Certificate and Enrollment Choice File on User Devices for Linux
- Added: Step 4 - Install the User Certificate and Enrollment Choice File on User Devices
- Added: Step 4a - Install the User Certificate and Enrollment Choice File on User Devices for Windows
- Added: Step 4b - Install the User Certificate and Enrollment Choice File on User Devices for macOS
- Added: Step 4c - Install the User Certificate and Enrollment Choice File on User Devices for Linux
- Removed: Step 4 - Install the User Certificate and Enrollment Choice File on User Devices for Windows
- Added: Step 4 - Install the User Certificate and Enrollment Choice File on User Devices
- Added: The Endpoint DLP module uses information from the choice file to enroll itself to the Secure Access cloud using the user identity certificate and additional device information.
- Added: Ensure you store the choice file in a secure location.
- Added: Step 4a - Install the User Certificate and Enrollment Choice File on User Devices for Windows

- Removed: Step 4 - Install the User Certificate and Enrollment Choice File on User Devices for macOS
- Added: Step 4b - Install the User Certificate and Enrollment Choice File on User Devices for macOS
- Removed: Step 4 - Install the User Certificate and Enrollment Choice File on User Devices for Linux
- Added: Step 4c - Install the User Certificate and Enrollment Choice File on User Devices for Linux

Cisco Endpoint Diagnostic Tool

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/endpoint-diagnostic-tool-intro/t_client_endpoint_diagnostic_tool.html

- Removed: Use the Cisco Endpoint Diagnostic Tool (CEDT) to collect diagnostic data from your macOS or Windows endpoint.
- Removed: This tool helps you troubleshoot issues related to Cisco Secure Access modules.
- Removed: It gathers system information, application logs, and network diagnostic data relevant only to Cisco Secure Access components.
- Removed: CEDT automatically detects installed Cisco Secure Access modules on your system, including Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), and Remote Access Virtual Private Network (RAVPN).
- Removed: This data helps Cisco Technical Assistance Center (TAC) engineers analyze your endpoint connectivity and configuration issues.
- Added: Use the Cisco Endpoint Diagnostic Tool (CEDT) to collect diagnostic data from macOS or Windows endpoints and troubleshoot Cisco Secure Access modules.
- Added: CEDT provides these capabilities:
- Added: System scanning: Detects installed Cisco Secure Access modules.
- Added: Application logs: Collects diagnostic logs generated by client software and the service infrastructure.
- Added: System data: Securely collects and encrypts system data related only to Cisco Secure Access diagnostics.
- Added: Network diagnostics: Collects network diagnostic data relevant to Cisco Secure Access components.
- Added: CEDT packages the collected data into a diagnostic archive that you can save locally or upload directly to a Cisco TAC support case.
- Added: The tool does not capture personal data.
- Added: CEDT automatically detects installed Cisco Secure Access modules and displays each module with its version number.
- Added: The detected components can include Zero Trust Access (ZTNA), Secure Web Gateway (SWG), Remote Access VPN (RAVPN), and Common System Information.
- Added: Install Google Chrome if you plan to run HAR capture.
- Added: CEDT does not currently support HAR capture inFirefox or Safari.
- Added: System Data Collected
- Added: The tool collects this system data, organized by category.
- Added: No personal data of any kind is captured.
- Added: General System Information
- Added: Data
- Added: macOS

- Added: Windows
- Added: OS, hardware, CPU, RAM, storage
- Added: system_profiler SPSoftwareDataType SPHardwareDataType
- Added: systeminfo, WMI classes(Win32_OperatingSystem,Win32_ComputerSystem,Win32_BIOS)
- Added: Kernel parameters
- Added: sysctl-a
- Added: N/A
- Added: Network Configuration
- Added: Data
- Added: macOS
- Added: Windows
- Added: Network interfaces & IP addresses
- Added: ifconfig-a
- Added: ipconfig/all
- Added: Routing table
- Added: netstat--rn
- Added: netsat-rn
- Added: DNS configuration
- Added: scutil--dns
- Added: (include in ipconfig/all)
- Added: Network services
- Added: networksetup-listallnetworkservices
- Added: netsh interface show interface
- Added: WiFi profiles
- Added: N/A
- Added: netsh wlan show profiles
- Added: Product Information
- Added: Data
- Added: macOS
- Added: Windows
- Added: Cisco preferences/config files
- Added: /Library/Preferences/com.cisco*
- Added: Registry exports (HKLM\SOFTWARE\Cisco, HKCU\SOFTWARE\Cisco, acsock service)
- Added: Installation directions
- Added: 1s-1as/opt/cisco

- Added: %ProgramFiles%\Cisco,%ProgramFiles(x86)%\Cisco%ProgramData%\Cisco
- Added: Running Cisco processes
- Added: ps aux \|grep -i cisco
- Added: tasklist\|findstr/icisco, WMI Win32_Process
- Added: Installed Cisco products
- Added: mdfind for Cisco apps
- Added: WMI Win32_Product(Vendor Cisco)
- Added: Application logs
- Added: Cisco Secure Client log directories
- Added: %ProgramData%\Cisco\Cisco Secure Client\Logs
- Added: Event logs
- Added: N/A
- Added: Windows Event Log (Cisco Secure Client - Zero Trust Access, Application provider *Cisco*)
- Added: Crash reports
- Added: ~/Library/Logs/DignosticReports/Cisco*
- Added: N/A
- Removed: The welcome screen scans the system and lists installed Cisco Secure Access modules, such as Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), and Remote Access Virtual Private Network (RAVPN).
- Removed: The Common System Information checkbox is enabled by default.
- Added: On the welcome screen, review the detected modules and their version numbers.
- Added: CEDT can display Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), Remote Access Virtual Private Network (RAVPN) and Common System Information.
- Added: Select or deselect the modules that you want to diagnose, and then click Let's Start.
- Added: On the Diagnostic Data Collection screen, select the connectivity tests to run.
- Added: DNS Lookup–Tests DNS resolution for specified hosts.
- Added: You can specify custom resolver IP addresses.CEDT saves the consolidated results in dns/dns_lookups.txt.
- Added: Packet Capture – Captures network packets for a specified duration.
- Added: This test requires administratorprivileges.
- Added: Ping Hosts–Pings specified hosts to verify connectivity.
- Added: Policy Test Output–Tests policy enforcement for up to 10 specified URLs throughpolicy.test.sse.cisco.com.
- Added: The results include structured policy output and automatically captured HARdata.
- Added: Network Speed Test–Measures download speed, upload speed, latency, and jitter throughspeed.test.sse.cisco.com.
- Added: CEDT saves the results in JSON and text-summary formats.
- Added: URL Reachability–Uses HTTP GET requests to test up to 20 URLs, with a 30-second timeout for eachURL.

- Added: The results include reachability, HTTP status, response time, content length, resolved IP address,TLS version, and timestamp.
- Added: Select the data-collection and debugging options to include.
- Added: HAR Capture—Records browser-session network data.
- Added: CEDT currently supports Google Chrome only.
- Added: DART Bundle Collection—Collects a DART bundle from Cisco Secure Client, including logs from allinstalled modules.
- Added: Reserved IP—Runs reserved-IP traceroute or tracert and DNS diagnostics.
- Added: Enable Debug Flags—Collects detailed endpoint-activity logs.
- Added: This option is available only when at leastone detected Cisco Secure Access product is selected.
- Added: DebugView Capture—Enables debug logging for the Windows Secure Endpoint Connector.
- Added: This optionis available only on Windows.
- Removed: Configure the settings displayed on the screen as required for the selected diagnostic tests.
- Removed: Example: If you selected DNS Lookup, enter the DNS Lookup Settings, such as Hosts to look up and Resolver IPs (optional).
- Added: Configure the settings for each selected test.
- Added: CEDT displays settings only for the tests that you selected.
- Added: For DNS Lookup, enter one or more hostnames and, optionally, custom resolver IP addresses.
- Added: For Packet Capture, select the interfaces, packet count, and capture duration.
- Added: For Ping Hosts, enter one or more hosts.
- Added: For URL Reachability, enter the URLs to test.
- Added: HTTP uses port 80 and HTTPS uses port 443 by default.Include the port in the URL when you use a nonstandard port.
- Added: For Policy Test Output, enter up to 10 host URLs.
- Added: For HAR Capture, enter the target URLs and ensure that Google Chrome is installed.
- Added: Configure any selected KDF, reserved-IP, performance, certificate-store, or debug-page-load settings.
- Removed: If you selected network diagnostic options such as Packet capture or Debug flags, the Diagnostics Paused window appears.
- Removed: This pause allows you to trigger the issue while detailed logging is active, ensuring the support team receives comprehensive data for effective troubleshooting.
- Added: If CEDT pauses during advanced troubleshooting, reproduce the issue while detailed logging is active.
- Added: Donot close CEDT while the diagnostic run is paused.
- Added: Click Continue after you reproduce the issue.
- Added: Reconnect to the VPN.
- Added: Open the internal application that is failing.
- Added: Repeat the steps that cause the error.
- Removed: Click Continue to collect the diagnostic files and turn logging back to normal.

- Removed: Enter the Case ID and Token, and then click Upload to send the diagnostic archive to your Cisco Technical Assistance Center (TAC) case.
- Added: Wait for all selected diagnostic tasks to complete.
- Added: The progress bar displays the overall status.
- Added: Do not close CEDT while diagnostics are running.
- Added: When the run completes, review the archive filename, file size, and SHA-256 checksum.
- Added: To upload the archive directly, enter the Cisco TACCase ID and Token, and then click Upload to send the diagnostic archive to your Cisco Technical Assistance Center (TAC) case.
- Added: To retain the archive without uploading it, click Skip.
- Added: After a successful upload, click Run Again to start another diagnostic run or click Close to exit CEDT.

Network Connectivity Log

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-connectivity-log-intro/network_connectivity_log.html

- Removed: The exported CSV file of Network Connectivity Logs includes the following columns: Network Tunnel Group, Data Center, IP Address, Hub Type, Region, Severity, Service, Device Type, Details, and Time (UTC).
- Removed: Use filters to refine results and help identify security.
- Added: The exported CSV file of Network Connectivity Log includes the following columns: Network Tunnel Group, Data Center, IP Address, Hub Type, Region, Severity, Service, Device Type, Details, and Time (UTC).
- Added: Use filters to refine results and identify connectivity or configuration issues.
- Removed: Any filters applied in the Network Connectivity Logs view, such as network tunnel group, event details, or identities, are reflected in the scheduled report, ensuring only relevant data is included.
- Added: Any filters applied in the Network Connectivity Log view, such as network tunnel group, event details, or identities, are reflected in the scheduled report, ensuring only relevant data is included.

Added Pages

- Troubleshoot Endpoint Data Loss Prevention for Linux: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/edp-secure-client-intro/troubleshoot-endpoint-data-loss-prevention-for-linux.html
- Uninstall Cisco Secure Client Endpoint DLP on Linux: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/edp-secure-client-intro/uninstall-cisco-secure-client-endpoint-dlp-on-linux.html

Cisco Secure Access documentation changes 2026-09-21

Lists changes to Cisco Secure Access documentation published on September 21, 2026.

Summary

- Document URL: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html
- Snapshot date: 2026-09-21
- Pages checked: 457
- Pages changed: 22

- Pages added: 0
- Pages removed: 0

Changed Pages

About this content

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html

- Removed: Endpoint Data Loss Prevention using Ciso Secure Client
- Added: Endpoint Data Loss Prevention using Cisco Secure Client

Endpoint Data Center Selection

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/introduction-secure-access-intro/Endpoint_Data_Center_Selection.html

- Removed: Secure Access - Local data residency deployments: With these deployments, data in the control, management, and data planes remains in a specific region rather than using a global cloud.
- Removed: The features are comparable to standard Secure Access.
- Added: Secure Access - Local data residency deployments: In these deployments, data in the control, management, and data planes remain within a specific region rather than in a global cloud.
- Added: The core security features are comparable to standard Secure Access.
- Added: For data processing details, see the Cisco Secure Access with Local Data Residency Offer Disclosure on the Cisco Trust Portal.

Network Tunnel Groups

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/manage-network-infrastructure-intro/manage-network-tunnel-groups.html

- Added: Step 1 - General Settings
- Added: Step 2 - Tunnel ID and Passphrase—Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.
- Added: If you opted to configure a backup primary or secondary region, you must also enter the IP addresses for both data centers within that region.
- Added: Step 3 - Routing – Configure routing options and network overlaps for this tunnel group.
- Added: Step 4 - Data for Tunnel Setup

Configure Tunnels with Cisco ISR

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-tunnels-by-device-intro/configure-tunnels-with-cisco-isr.html

- Added: Follow these steps to connect the Cisco ISR (G2, 4K) or CSR router to Secure Access.

Enroll Meraki SD-WAN Sites with Meraki Auto-VPN Tunnels

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-tunnels-by-device-intro/enroll-meraki-sd-wan-sites-with-meraki-auto-vpn-tunnels.html

- Added: Enrolling a Meraki Site
- Added: Perform the following steps to enroll a Meraki site.
- Added: For more information, refer to Cisco SASE: Sites Connectivity.

Site-to-Site VPN tunnels with Microsoft Azure

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-tunnels-by-device-intro/configure-site-to-site-vpn-azure.html

- Added: Component 1: Create a VPN Gateway in Microsoft Azure
- Added: Note The Azure S2S IPsec tunnel is sourced from the VPN Gateway.
- Added: If you have already deployed a VPN Gateway in your Azure environment, skip ahead to Component 2.
- Added: Component 2: Create a network tunnel group in Secure Access
- Added: Create a network tunnel group in Secure Access with the following configuration.
- Added: For a more detailed procedure, see Add a Network Tunnel Group.
- Added: Component 3: Create two local network gateways in Azure with S2S connections
- Added: Create and configure two local network gateways in Azure, then connect them to Secure Access.
- Added: The local network gateway acts as the remote site connected by tunnel to the Secure Access DC.
- Added: Component 4: Create a static route table in Azure
- Added: Add a table of branch routes and internet routes to the primary VPN gateway and associate the route table with any required subnets.
- Added: For more information, see Azure: Create, change, or delete a route table.
- Added: Component 1: Create a VPN Gateway in Microsoft Azure
- Added: Note The Azure S2S IPsec tunnel is sourced from the VPN Gateway.
- Added: If you have already deployed a VPN Gateway in your Azure environment, you can skip this section.
- Added: Component 2: Create a network tunnel group in Secure Access.
- Added: Configure a network tunnel group in Secure Access.
- Added: For a more detailed procedure, see Add a Network Tunnel Group.
- Added: Component 3: Create two local network gateways in Azure with S2S connections.
- Added: Create and configure two local network gateways in Azure, then connect them to Secure Access.
- Added: The local network gateway acts as the remote site connected by tunnel to the Secure Access DC.
- Added: Component 4: Verify tunnel status in Azure and Secure Access.

Configure a Site-to-Site VPN tunnel with Amazon Web Services

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-tunnels-by-device-intro/configure-site-to-site-vpn-aws.html

- Added: Component 1: Create a VPC with two subnets in AWS—In your AWS dashboard, create a VPC with two subnets.
- Added: Skip this step if you already have a VPC.
- Added: For more information, refer to Create a VPC
- Added: Component 2: Create a Transit Gateway in AWS—Create a transit gateway in AWS with an attachment to your Amazon VPC.
- Added: For more information, refer to Connect your VPC to other VPCs and networks using a transit gateway, Create a transit gateway using Amazon VPC Transit Gateways, and Create a VPC attachment using Amazon VPC Transit Gateways.

- Added: Component 3: Create two placeholder Customer Gateways in AWS—Create two customer gateways with S2S connections.
- Added: For more information, refer to Get started with AWS Site-to-Site VPN, Step 1: Create a customer gateway and Step 5: Create a VPN connection.
- Added: Note These gateways will act as temporary placeholders that provide outside IP addresses required by the Secure Access network tunnel group configuration in the next step.
- Added: The network tunnel group will provide the Secure Access BGP ASN and public IP addresses for the Secure Access Peer IP address DCs that you will use to create two new customer gateways in AWS.
- Added: Component 4: Create a Site-to-Site VPN connection for each customer gateway
- Added: Component 5: Create a network tunnel group in Secure Access—For a more detailed procedure, refer to Add a Network Tunnel Group.
- Added: Component 6: Replace the placeholder customer gateways in AWS—Configure two more customer gateways in AWS to connect to the Secure Access DC IPs.
- Added: These will replace the placeholder customer gateways that you created for Component 3.
- Added: Note It is not possible to update the placeholder customer gateways.
- Added: You must create new customer gateways with the DC IPs from Secure Access, then modify the VPN connection in AWS to target the new customer gateways.
- Added: Before you begin, you will need this information from Secure Access:
- Added: The DC IP addresses for the primary and secondary tunnel from Component 4.
- Added: You can also find this information in Secure Access by navigating to Connect> Network Connections> Network Tunnel Groups and clicking the network tunnel group name for details.
- Added: The Peer (Secure Access) BGP AS number for the network tunnel group.
- Added: Find this information in Secure Access by navigating to Connect> Network Connections> Network Tunnel Groups and clicking the network tunnel group name for details.
- Added: Component 7: Verify tunnel status in AWS and Secure Access—In the left navigation menu of the AWS VPC dashboard, navigate to Virtual private network (VPN) and click Site-to-Site VPN connections.
- Added: Click the VPN ID of each VPN connection to confirm that the State is Available and that the Status of both tunnels is Up.
- Added: This example shows VPN connection 1 is Available and both tunnels are Up:
- Added: VPN connection 2 is also Available and both tunnels are Up.
- Added: Note that each tunnel has a unique Outside IP Address.
- Added: Tunnel 1 has the same Inside IPv4 CIDR range for each VPN connection, and Tunnel 2 has the same Inside IPv4 CIDR range for each VPN connection.
- Added: Component 8: Modify subnet routing tables to send traffic to the AWS Transit Gateway—To send traffic from the AWS VPC to the AWS transit gateway, modify the routing table of each subnet to target the Transit gateway ID.
- Added: For more information, refer to Change a subnet route table.

Manage Resource Connectors and Connector Groups

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/resource-connectors-groups-into/manage_resource_connectors_and_connector_groups.html

- Added: 208.67.222.222 Note The Resource Connector uses the Cisco OpenDNS resolver (208.67.222.222) as a fallback mechanism.

- Added: This is optional and is only utilized if your configured DNS server becomes non-functional.
- Added: If you do not wish to use this fallback, it is not required for standard operations.
- Added: 208.67.222.222
- Added: TCP/53, UDP/53

Provision Users, Groups, and Endpoint Devices from Active Directory

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/provisioning-active-directory/provision_users_groups_and_endpoint_devices_from_active_directory.html

- Added: Delete one AD component
- Added: Delete all AD components

Manage Destination Lists

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-saas-resource-intro/manage_destination_lists.html

- Removed: Table 1.

Manage Virtual Private Networks

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/vpns-and-proxies-intro/manage-virtual-private-networks.html

- Added: Note Proxy Override Settings manage proxy behavior once the VPN tunnel is active.
- Added: These settings are independent of the Cisco Secure Client proxy settings configured in Step 4 of the Add VPN Profiles Step 4 – Cisco Secure Client Configuration procedure, which specifically govern the client's VPN connection.

Manage Notification Pages

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/notification-pages-intro/manage_notification_pages.html

- Added: Note You can pin a specific column or re-arrange columns in your desired layout by clicking on the Settings gear icon.
- Added: Note You can View or Edit the Default Settings End User Notification Page, but you cannot Delete it.
- Removed: Click +Add, or expand the setting you want to edit.
- Added: Click + Add notification page, or expand the setting you want to edit.
- Removed: If this is a new configuration, name this set of notification pages.
- Removed: Click Allow blocked users to contact an admin from the block page.
- Added: If this is a new configuration, name this set of notification pages using a maximum of 128 characters.
- Added: Enable Show diagnostic information that Cisco TAC may need for troubleshooting, such as organization ID, origin ID, query string, and server name.
- Added: Disabling diagnostic fields may limit support effectiveness..
- Removed: Images larger than 125 x 70 pixels will be cropped and resized.
- Added: Images larger than 600 x 200 pixels will be cropped and resized.
- Added: You can select your desired logo position.
- Removed: Specify your custom message.

- Removed: You can adjust the size of text, as well as bold, italicize, underline, or strikethrough it.
- Removed: You can also add hyperlinks, numbered lists, and bulleted lists.
- Removed: You can also use the following variables within your message.
- Removed: [domain]—Substitutes the domain name that the end-user tried to browse to.
- Removed: [client_ip]—Substitutes the external IP address of the client that is hitting the block page.
- Added: Enter your custom message.
- Added: You can change the size and formatting of your text.
- Added: Add bold, italic, underline, and strikethrough styles.
- Added: You can also include hyperlinks, numbered lists, and bulleted lists.
- Added: You can include the following variables within your message.
- Added: [domain]—Displays the domain that triggered the block and warn page.
- Added: [rule_name]—Displays the name of the rule that triggered the block or warn page.
- Added: [url_category]—Displays the URL category associated with the blocked or warned destination.
- Added: [client_ip]—Displays the client IP address associated with the request.
- Added: [public_ip]—Displays the public source IP address of the client.
- Added: [user_agent]—Displays information about the browser or client that made the request.
- Added: You can redirect users to the URL of your choice by clicking on the radio button and entering the URL.
- Added: Note: You can allow users to directly contact their administrators by enabling Allow blocked users to contact an adminstrator.
- Added: You can change the size and formatting of your text.
- Added: Add bold, italic, underline, and strikethrough styles.
- Added: You can also include hyperlinks, numbered lists, and bulleted lists.
- Added: You can include the following variables within your message.
- Added: [domain]—Displays the domain that triggered the block and warn page.
- Added: [rule_name]—Displays the name of the rule that triggered the block or warn page.
- Added: [url_category]—Displays the URL category associated with the blocked or warned destination.
- Added: [client_ip]—Displays the client IP address associated with the request.
- Added: [public_ip]—Displays the public source IP address of the client.
- Added: [user_agent]—Displays information about the browser or client that made the request.
- Removed: Navigate to a notification page and expand the setting.
- Added: Navigate to a notification page and click Edit.

Built-in Data Identifiers

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/built-in-data-identifiers-intro/built-in_data_identifiers.html

- Removed: The built-in data identifiers are available as an Excel table here.
- Removed: The table is updated frequently, so be sure to download the most recent version.

- Added: The built in data identifiers are available as a PDF document here.

Set up the Zero Trust Access App for iOS Devices

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/client-based-za-mode-into/set_up_the_zero_trust_access_app_for_ios_devices.html

- Removed: We strongly recommend consulting your MDM documentation for setting options and configurable components.
- Added: We strongly recommend configuring the following settings in your Mobile Device Manager (MDM) to support the full range of functionality and features that Secure Access has to offer.
- Added: For information on how to implement these changes in your particular MDM, consult your MDM documentation.
- Added: "enrollment_choice": <enrollment choice file content>.
- Added: This allows you to deploy a different enrollment choice file instead of the default file.
- Added: "DeviceUniqueIdentifier": <device UDID>.
- Added: This allows the admin to set a unique device ID to the enrolled device into each connection request to the private resource to assist in identify the user's device.

Set up the Zero Trust Access App for Android on Samsung Devices

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/client-based-za-mode-into/set_up_the_zero_trust_access_app_for_android_on_samsung_devices.html

- Removed: Configure Android Settings in Seucre Access
- Added: Configure Android Settings in Sucre Access

Manage Zero Trust Access using Cisco Secure Client

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/za-secure-client-into/manage_zero_trust_access_using_cisco_secure_client.html

- Removed: C:\\ProgramData\\Cisco\\Cisco Secure Client\\ZTA\\enrollments
- Added: C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices

Endpoint Data Loss Prevention using Cisco Secure Client

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/edlp-secure-client-intro.html

- Removed: Endpoint Data Loss Prevention using Ciso Secure Client
- Added: Endpoint Data Loss Prevention using Cisco Secure Client

Onboard Experience Insights

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/experience-insights-intro/onboard-experience-insights.html

- Added: Step 1: ThousandEyes integration
- Added: Experience Insights requires the integration of your ThousandEyes account.
- Added: Note OAuth 2.0 with ThousandEyes
- Added: ThousandEyes uses the OAuth 2.0 protocol to grant Secure Access limited access to your ThousandEyes data.
- Added: For more information, see OAuth 2.0 with ThousandEyes.
- Added: Step 2: Account group configuration

- Added: Step 3: Default test target
- Added: Step 4: Unified collaboration application
- Added: Step 5: ThousandEyes agent
- Added: Endpoints must be registered to your Secure Access organization to be monitored for performance.
- Added: When you deployed Cisco Secure Client to your endpoints, the ThousandEyes Endpoint Agent was installed.
- Added: The ThousandEyes Endpoint Agent will register to your Secure Access organization automatically once your endpoints have connected to VPN, ZTA, or Roaming Module.

Log Formats and Versioning

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/logging-intro/log_formats_and_versioning.html

- Removed: v17—The same fields as version 16, but the v17 log format introduces Resource Connector logs and adds the following new fields to the existing logs:
- Added: v17—The same fields as version 16, but the v17 log format introduces Data Loss Prevention (DLP) logs and adds the following new fields to the existing logs:
- Removed: Data Loss Prevention (DLP) logs: taac tenant id, taac profile id, match excerpts, match violation starts, match violation ends, email sender, email recipients, email attachments, email id, email vendor id
- Added: DLP logs: taac tenant id, taac profile id, match excerpts, match violation starts, match violation ends, email sender, email recipients, email attachments, email id, and email vendor id.
- Removed: timestamp,policy identity label,internal client ip,external client ip,destination ip,content type,action,url,referer,user agent,status code,request size,response size,response body size,sha—sha256,categories,av detections,puas,amp disposition,AMP malware name,amp score,policy identity type,blocked categories,identities,identity types,request method,dlp status,certificate errors,file name,ruleset id,rule ID,destination list ids,isolate action,file action,warn status,forwarding method,producer,msp organization id,geo location of blocked destination countries,application ids,hostname,data center,egress,server name,time based rule,security overridden,detected response file type,warn categories,organization id,application entity name,application entity category, egress ip,ai model name,ai suply chain categories,event correlation id,isolation profile id,us
- Added: timestamp,policy identity label,internal client ip,external client ip,destination ip,content type,action,url,referer,user agent,status code,request size,response size,response body size,sha—sha256,categories,av detections,puas,amp disposition,AMP malware name,amp score,policy identity type,blocked categories,identities,identity types,request method,dlp status,certificate errors,file name,ruleset id,rule ID,destination list ids,isolate action,file action,warn status,forwarding method,producer,msp organization id,geo location of blocked destination countries,application ids,hostname,data center,egress,server name,time based rule,security overridden,detected response file type,warn categories,organization id,application entity name,application entity category, egress ip,ai model name,ai suply chain categories,event correlation id,isolation profile id,source country
- Removed: It refers to the specific name of an application entity within a system.
- Removed: For example, the YouTube Channel "Cisco".
- Added: The specific name of an application entity within the system.
- Added: This field is currently used to identify YouTube channel names only.
- Removed: It represents the classification grouping of application entities based on shared characteristics or functions.
- Removed: For example, the YouTube Category "Networking".
- Added: The classification grouping of application entities based on shared characteristics.
- Added: This field is currently used to identify YouTube categories only.

- Removed: Reserved
- Removed: This field is currently not used.
- Added: egress port
- Added: The egress port number of the network where the request originated.
- Removed: Egress port
- Removed: The source port number used by Secure Access ZTA for a session as it exits the Secure Access ZTA infrastructure toward the destination application.
- Removed: For network tunnel backhauls, the destination network sees this port as the source port of the connection.
- Removed: For Resource Connector backhauls, this field does not represent the source port seen by the destination network.
- Added: zta source port
- Added: The port number used by the Zero Trust proxy service to connect to an unmanaged device requesting a connection to a private resource.

Monitor Secure Access with Reports

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/monitor-with-reports-intro/monitor_secure_access_with_reports.html

- Removed: However, the 'time out' is not reflected in the dashboard.
- Removed: Instead, status is set to "Generating..." and persists.
- Removed: The report remains in this state without resolution.
- Added: However, the timeout is not reflected in the dashboard.
- Added: Instead, status is set to Generating... and persists.
- Removed: If this situation occurs, re-run the report export with a shorter date range, or more filters applied.
- Added: If this situation occurs, rerun the report export with a shorter date range, fewer rows, or more detailed filters.
- Added: For Remote Access Logs, the selected time range and applied filters are used for the export, including filters selected from the filter menu or added from a table value.

About the Remote Access Log Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/remote-access-log-intro/remote-access-log-report.html

- Removed: The Remote Access Log report lists users that have remotely connected to Secure Access and requested access to destinations.
- Removed: Some relevant fields to aid debugging and trouble-shooting remote access sessions include:
- Removed: Display Username for Failed Events – Significantly improves how quickly issues can be tracked and addressed.
- Removed: ASA Syslog Message ID Extraction Support – Offers detailed insights by identifying the specific sys-log messages used in the remote access logs.
- Removed: Device ID – Includes the device ID with every event, providing critical help to network administrators in numerous ways.
- Removed: Failed Events for Posture – Provides vital information for effective triage during failed connection attempts.
- Added: The Remote Access Log report lists connection events for users who connect remotely to Secure Access.

- Added: Use the report to investigate connection activity, troubleshoot failed sessions, and identify access issues.
- Added: Some relevant fields include:
- Added: Display username for failed events – Helps you identify the affected user.
- Added: ASA syslog message ID – Helps you identify the syslog message associated with the event.
- Added: Device ID and device name – Helps you identify the endpoint.
- Added: Machine name – Identifies the client machine when the value is returned for the event.
- Added: Endpoint posture information – Provides posture details for failed events when posture data is returned.
- Added: Connection information – Includes the VPN profile, session type, IP addresses, operating system, and Secure Client version.
- Added: Use the time-range control and the filter menu to refine the report.
- Added: Depending on the selected time range and the data returned for that period, you can filter by user, country, region, posture profile, session type, device name, machine name, IP address, VPN profile, reason code, and Security Group Tag information.
- Added: Some filters provide fixed choices, some provide values found in the report data, and some accept a value that you enter.
- Added: You can also hover over a supported value in a table column and select the search control to add that value to the applied filters.
- Added: Use table settings to change the visible columns or table density.
- Added: The report supports sorting for supported columns, including User, Region, and VPN Profile.
- Added: Select a row to expand its details.
- Added: The expanded area can include Source, Endpoint Posture, Connection, and Tunnels information.
- Added: Endpoint Posture details can include the posture attributes evaluated for the event and the posture profile used for the evaluation.
- Added: If the posture profile is linked, select the link to open that posture profile.
- Removed: You can use filters to refine results and help identify security issues that require attention.
- Removed: Access Allowed
- Added: Status
- Added: Connected
- Added: Disconnected
- Added: Failed
- Added: Warning: User
- Added: Machine Name
- Added: Device Name
- Added: IP Address
- Added: Country
- Added: VPN Profile
- Added: Posture Profile

- Added: Region
- Added: Session Type
- Added: Reason Code
- Added: IKEv2 Check
- Added: Access Allowed Geocompliance Service Unavailable
- Added: IP Assignment Failed
- Added: Unknown
- Removed: DDNS Update Failed
- Removed: Geocompliance Service Unavailable
- Removed: IKEV2 Check
- Removed: Static IP Addr Assignment Fail
- Removed: Identities lets you filter by connection events with Security Group Tags (SGT) you have configured rules to traffic originating from IP addresses in network segments that include SGTs.
- Removed: When present, SGTs will be appended to the User column value.
- Added: DDNS update failed
- Added: OS Version
- Added: Client Version
- Added: Security group tag lets you filter by connection events with Security Group Tags (SGT) you have configured rules to traffic originating from IP addresses in network segments that include SGTs.
- Added: When present, SGTs are appended to the User column value.
- Removed: Note Each filter is dynamic, except for Identities, and will only display filter option values that are present in the connection data.
- Removed: If no option values are present in the data for a filter, that filter remains hidden.
- Added: Note Some filters provide fixed options, some display values found in the connection data, and some accept a value that you enter.
- Added: A data-driven filter displays only option values that are present in the connection data for the selected time frame.
- Added: If no option values are present, the filter remains hidden.
- Removed: Option 1: Click the View Details icon (the blue ellipsis at the right end of each row).
- Removed: Option 2: Hover over an Event Details field in any row, then click Read More below the ASA syslog message ID.
- Added: Navigate to Monitor> Reports> Remote Access Logs.
- Added: Click the expand icon at the start of any row.
- Added: This expands the row and displays the event details.
- Removed: Result: The Event Details drawer displays detailed information about an individual event.
- Removed: Extra information is available in the Event Details window:
- Removed: Last Connected– The timestamp when this users was last connected to the machine.

- Removed: Posture profile information– The posture profile associated with the event.
- Added: Result: The event details display in the expanded row as Source, Endpoint Posture, and Connection cards.
- Added: Extra information is available in the event details:
- Added: Last Connected - The timestamp when this user was last connected to the machine.
- Added: Source - The Source card can include Date & Time, User, OS Type & Version, Device Name, Origin ID, Origin type, Country, Public IPv4 address, Public IPv6 address, and Security Group Tag.
- Added: Endpoint Posture - The Endpoint Posture card displays posture information.
- Added: It can show the posture profile applied to the event or indicate that no posture profile is applied.
- Removed: Reason Code– The reason code for VPN incompatibilities.
- Removed: Syslog Information–Syslog information related to the event you are examiningwith timestamps, syslog server IP, and indication of a logging message
- Removed: At the bottom of the Event Details window click View More Details to view VPN specific event details.
- Removed: The following categories is displayed:
- Removed: Duration– The duration of the event.
- Removed: Machine ID– The unique identifier assigned to the client machine.
- Removed: Redirect ACL– The redirect access control l (ACL) that originates from the user or device.
- Removed: Redirect URL–The URL where a user is automatically sent after attempting to access a different URL.
- Removed: Security group Tag– The unique identifier assigned to a device or user, representing their security role or access level within the network.
- Removed: Audit Session ID– The unique identifier generated and associated with a user's process when they successfully log in or connect.
- Removed: Tunnels– How many tunnels are contained within the VPN profile and tunnel information.
- Removed: From your search results, you can click an identity or destination and go to their respective detailed report.
- Added: Connection - The Connection card can include Connection Event, Reason Code, Syslog Info, Region, Internal IPv4 Address, Internal IPv6 Address, Last Connected, VPN Profile, Session Type, and Secure Client Version.
- Added: It can also display session duration, inactivity, redirect, security group tag, and audit session information.
- Added: Reason Code - The reason code for VPN incompatibilities.
- Added: Syslog Information - Syslog information related to the event you are examiningwith timestamps, syslog server IP, and indication of a logging message.
- Added: Review the following additional event details:
- Added: Duration - The duration of the session.
- Added: Inactivity - The amount of time that the session was inactive.
- Added: Redirect ACL - The redirect access control (ACL) that originates from the user or device.
- Added: Redirect URL - The URL where a user is automatically sent after attempting to access a different URL.
- Added: Security Group Tag - The unique identifier assigned to a device or user, representing their security role or access level within the network.
- Added: Audit Session ID - The unique identifier generated and associated with a user's process when they successfully log in or connect.

- Added: Tunnels - Select View tunnels to view tunnel information.
- Added: If the event includes more than one tunnel, select the corresponding tunnel tab to view each tunnel's details.
- Added: From your search results, you can click an identity or destination and go to its detailed report.

Integrate Cisco Identity Intelligence with Secure Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/secure-access-integrations-intro/integrate-cisco-identity-intelligence.html

- Added: Onboarding