Cisco Secure Access for Government Help

Cisco Secure Access
Updated November 18, 2026

Part I

Cisco Secure Access for Government Help

Topics:

- Welcome to Cisco Secure Access for Government
- Secure Access Single Sign-On Authentication
- Get Started
- Quickstarts
- Secure Access Integration with Protective DNS
- Limitations and Range Limits
- Network Requirements for Secure Access
- Manage Network Connections
- Manage Network Tunnel Groups
- Network Tunnel Configuration
- Provision Users and Groups from Active Directory
- Manage End-User Connectivity
- Manage Users, Groups, and Endpoint Devices
- Configure Integrations with SAML Identity Providers
- Manage Virtual Private Networks
- Traffic Steering for Zero Trust Access Client-Based Connections
- Manage Internet Security
- Manage PAC Files
- Manage Registered Networks
- Manage Internal Networks
- Manage Destination Lists
- Manage Application Lists
- Manage Content Category Lists
- Manage Tenant Control Profiles
- Manage Roaming Devices
- Manage Private Resources
- Manage Connections to Private Destinations
- Manage the Access Policy
- Get Started With Internet Access Rules
- Get Started With Private Access Rules
- Manage Endpoint Security
- Manage Zero Trust Access Posture Profiles

- Manage VPN Connection Posture Profiles
- Manage IPS Profiles
- Manage Security Profiles
- Threat Categories
- Manage File Inspection and File Analysis
- Manage File Type Controls
- Manage Notification Pages
- Manage Traffic Decryption
- Manage Certificates
- Manage the Data Loss Prevention Policy
- Manage Data Classifications
- Built-in Data Identifiers
- Manage SaaS API Data Loss Prevention
- Manage Cloud Malware Protection
- Manage Logging
- Manage API Keys
- Manage Accounts
- Manage Domains
- Manage Resources
- Manage DNS Servers

1 Welcome to Cisco Secure Access for Government

Topics:

- Sign into Secure Access with Security Cloud Sign On
- Find Your Organization ID
- Determine Your Current Package
- Contact Cisco Secure Access Support

Introduces welcome to cisco secure access for government. Secure Access is Cisco's cloud-based platform that provides you with multiple levels of defense against internet-based threats.

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

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

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

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

Sign into Secure Access

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

Find Your Organization

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

Determine Your Current Package

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

Contact Support

- For more information, see Contact Cisco Secure Access Support.

Sign into Secure Access with Security Cloud Sign On

Provides instructions for sign into secure access with security cloud sign on. Cisco Secure Access supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access console. An administrator signs in to Secure Access using Cisco Security Cloud Single Sign On (SCSO).

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

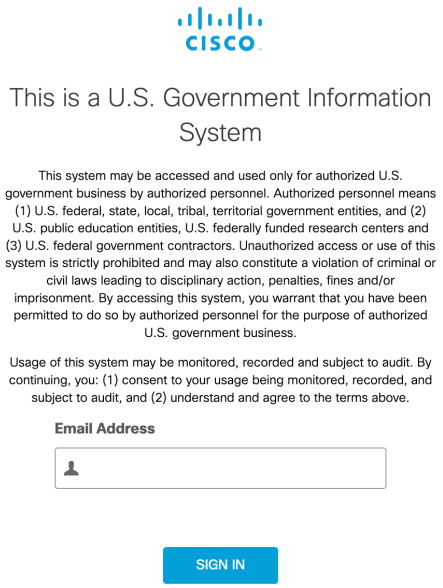
Sign in to Secure Access through the Cisco Security Cloud Sign-On (SCSO) portal. If you do not have an SCSO account, follow the steps to Configure Single Sign-On Authentication.

Before you begin

- A valid Secure Access account. For more information, see Manage Accounts.
- A Cisco Security Cloud Sign-On (SCSO) account. For more information, see Configure Single Sign-On Authentication.

Procedure

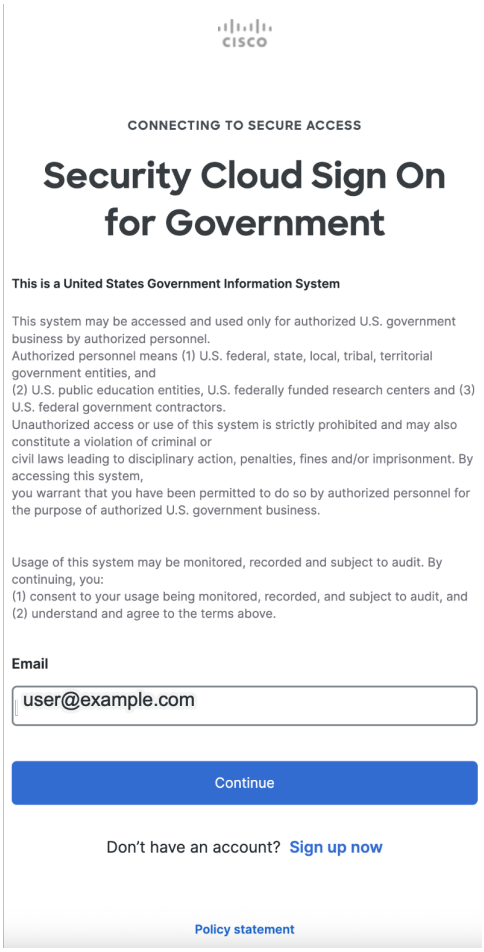
1. Navigate to your Secure Access organization at https://dashboard.secureaccessfed.cisco/org<*orgId*>.



2. Enter the email address where you received the invitation to join a Secure Access organization, then click **SIGN IN**.

   Secure Access uses single sign-on authentication through **Security Cloud Sign On**. Your Secure Access account and the SCSO account must use the same email address.

3. In **Security Cloud Sign On for Government**, enter the email address and click **Continue**.



4. In the next window, enter password and click **Continue** to sign in to Secure Access after SSO authentication.

Find Your Organization ID

Provides instructions for find your organization id. Every Secure Access organization (Org) is a separate instance of Secure Access. Organizations are identified by their account name and a unique numeric organization ID (Org ID).

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

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

Before you begin

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

Procedure

---

1. Sign in to Secure Access.
2. Check the URL in the browser's address bar: `<https://dashboard.secureaccessfed.cisco/org>\<_orgId_>` where `orgId` is your unique Secure Access organization ID.

3. Navigate to the name of your user account, and expand your username to view the organizations where the username is a member. Confirm that you are signed in to the correct Secure Access organization. Your organization name is listed under your account name.
4. Click **Switch Organizations** to change to another Secure Access organization.
5. Locate **System Status**–the overall health status of Secure Access.

Determine Your Current Package

Provides instructions for determine your current package. Within your Cisco Secure Access subscription, the Secure Access package determines the features available to you and your level of support. Your current package is listed on the Cisco Secure Access Subscription page.

Within your Cisco Secure Access subscription, the Secure Access package determines the features available to you and your level of support. Your current package is listed on the Cisco Secure Access Subscription page.

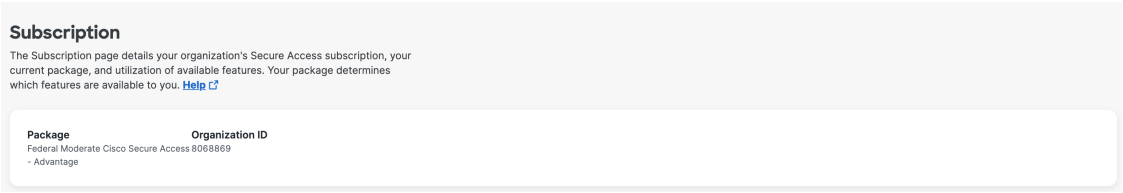
For more information about your current package, contact your sales representative.

Before you begin

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

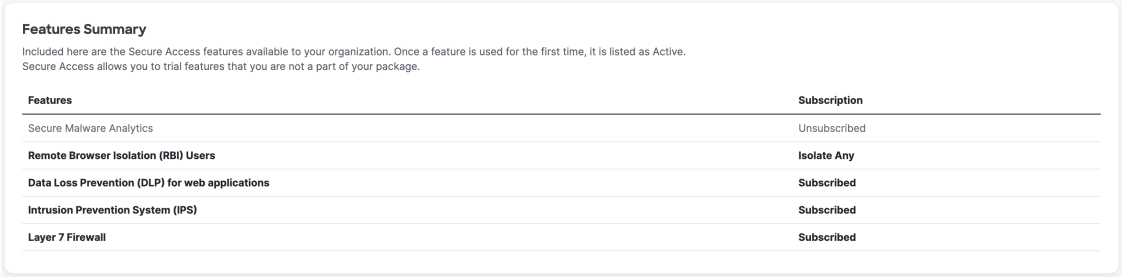
Procedure

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



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

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



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

Contact Cisco Secure Access Support

Describes contact cisco secure access support. Support for Secure Access can be reached through Cisco Support at https://mycase.frmod.cisco

Support for Secure Access can be reached through Cisco Support at https://mycase.frmod.cisco

2 Secure Access Single Sign-On Authentication

Topics:

- Configure Single Sign-On Authentication
- Troubleshoot Single Sign On Authentication

Introduces secure access single sign-on authentication. Cisco Secure Access supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access console. An administrator signs in to Secure Access from Cisco Security Cloud Single Sign On (SCSO).

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

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

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

Note

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

Configure Single Sign-On Authentication

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

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

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

Before you begin

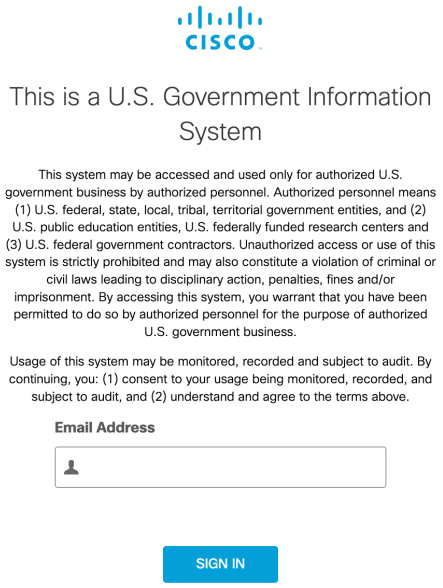
- A valid Secure Access account. For more information, see Manage Accounts.
- **Add Your Organization's Identity Provider in Security Cloud Sign On**–You can add an SAML identity provider (IdP) in SCSO for Secure Access. Once you add an IdP and provision user accounts in Security Cloud Sign On, administrators in your organization are not required to complete the **Sign Up Now** steps. For more information, see Cisco Security Cloud Sign On Identity Provider Integration Guide.
- **Add Administrators to Secure Access**–A Cisco Secure Access administrator can add additional administrators to their Secure Access organization (Org) and assign a role to the new administrator's account. To establish an account, provide the email address of the new administrator and choose the Secure Access role for the account. For more information, see Manage Accounts.

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

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

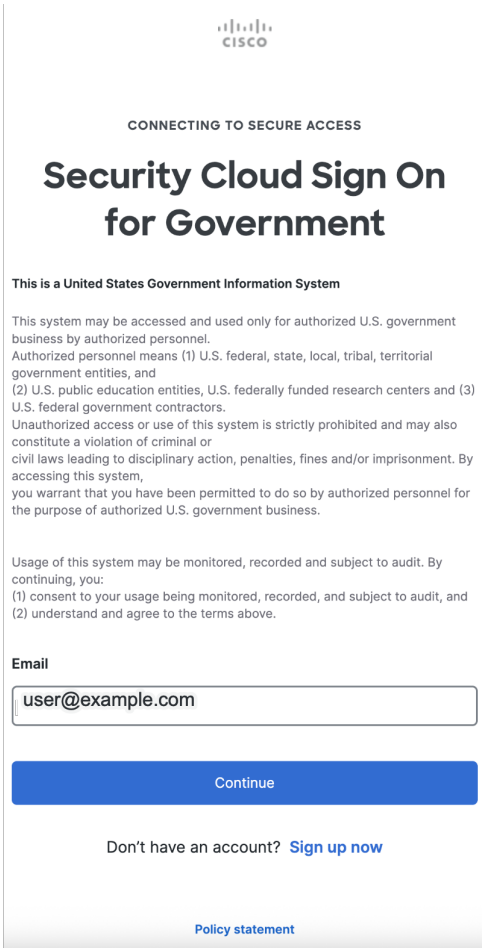
Procedure

1. Navigate to your Secure Access organization at https://dashboard.secureaccessfed.cisco/org<*orgId*>.



2. Enter the email address where you received the invitation to join a Secure Access organization, then click **SIGN IN**.
3. In **Security Cloud Sign On for Government**, enter the email address and click **Continue**.

   Secure Access uses single sign-on authentication through **Security Cloud Sign On**. Your Secure Access account and the SCSO account must use the same email address.



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

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

5. Once you receive an email from Secure Access inviting you to create an SCSO account, click the link in the email and follow the instructions to set up your SCSO account with your IdP. For more information, see Security Cloud Sign On Quickstart Guide.
6. Follow the steps to sign in to your Secure Access Org. For more information, see Sign In to Secure Access with Security Cloud Sign On.

Troubleshoot Single Sign On Authentication

Describes troubleshooting single sign on authentication. If you are unable to sign in to Secure Access through Cisco Security Cloud Sign On, contact Support.

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

3 Get Started

Topics:

- Begin Secure Access Onboarding Workflow
- Step 1 – Configure Network Connections
- Step 2 – Configure Access to Resources
- Step 3 - Configure End User Connectivity
- Step 4 – Configure Endpoints and Network Sources
- Secure Access Overview Dashboard

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

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

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

Prerequisites

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

What's Next

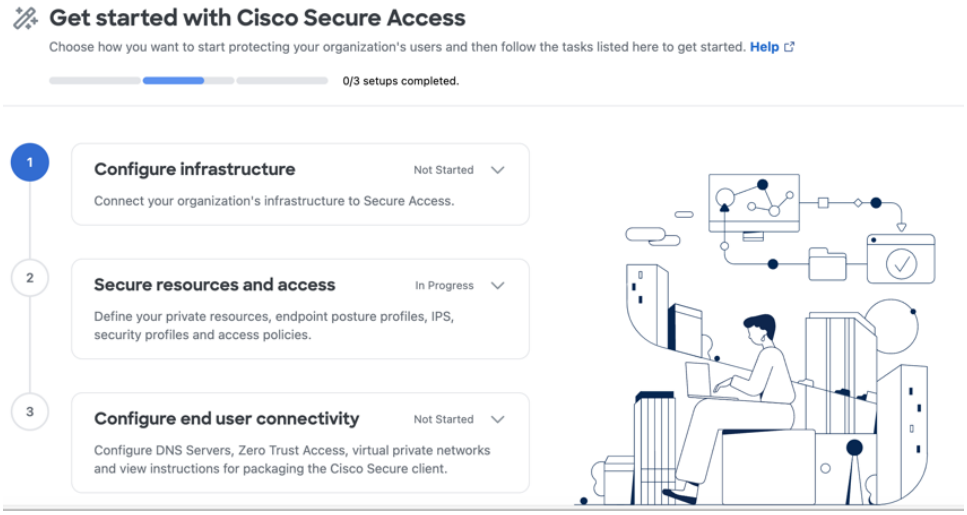
- Begin the **Get Started with Cisco Secure Access** workflow. Provision your organization's network connections and users and groups, and set up integrations with SAML identity providers (IdPs). For more information, see Begin Secure Access Onboarding Workflow.

Begin Secure Access Onboarding Workflow

Describes begin secure access onboarding workflow. The Get Started with Cisco Secure Access workflow guides you through the initial setup of Secure Access. Sign in to Secure Access and navigate to Workflows.

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

After you establish network connections, begin the **Secure resources and access** step in the Get Started workflow. **Secure resources and access** includes: designing endpoint posture profiles, IPS and security profiles, and policy rules. Then, in the **Configure end user connectivity** step, define traffic patterns for remote user connections to resources–configure DNS servers, Zero Trust, virtual private networks (VPNs), and internet security settings.



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

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

Step 1 – Configure Network Connections

Describes step 1 - configure network connections. The Get Started with Cisco Secure Access workflow guides you through the tasks in the Configure Infrastructure step–configure Network Tunnel Groups and establish network tunnels to Secure Access.

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

Prerequisites

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

Task 1 – Add Network Connections

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

- Manage Network Tunnels

Task 2 – Provision Users and Groups

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

- Import Users and Groups from CSV File
- Provision Users and Groups from Okta
- Provision Users and Groups from Azure
- Provision Users and Groups from Active Directory

Task 3 – Configure Integrations with SAML Identity Providers

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

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

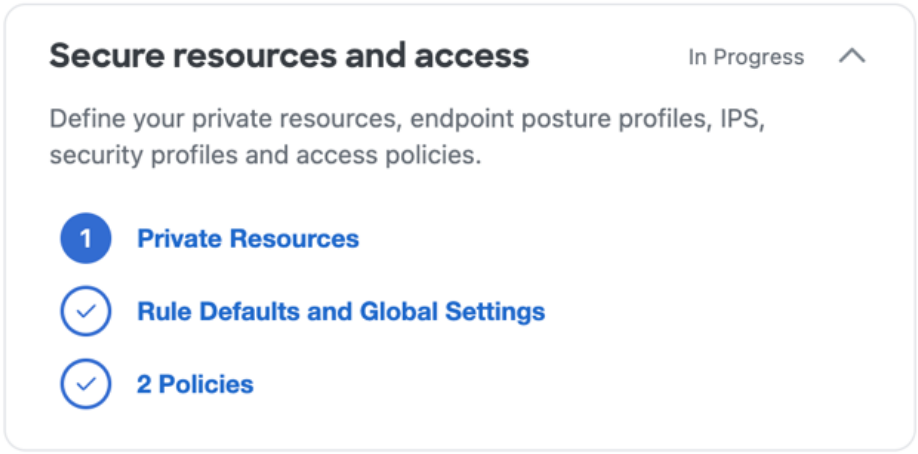
What's Next

- Step 2 – Configure Access to Resources

Step 2 – Configure Access to Resources

Describes step 2 – configure access to resources. The Get Started with Secure Access workflow guides you through the tasks in the Secure Resources and Access step—secure your private resources, enable access controls on resources, and create policy rules. For more information, see Manage Private Resources.

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



Prerequisites

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

Task 1 – Set Up Private Resources

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

- Manage Private Resources

Task 2 – Configure Rule Defaults and Global Settings

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

Manage Rule Defaults

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

Manage Global Settings

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

Global Settings:

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

Default Settings:

- Default Settings for Private Access Rules

- Default Settings for Internet Access Rules

Task 3 – Add a Policy Rule

Configure and add rules to the Secure Access policy.

- Manage the Access Policy

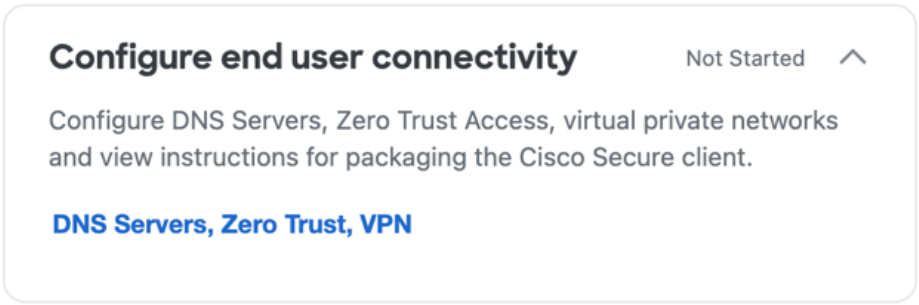
What's Next

- Step 3 – Configure End User Connectivity

Step 3 - Configure End User Connectivity

Describes step 3 – configure end user connectivity. The Get Started with Secure Access workflow guides you through the tasks in the Configure End User Connectivity step–configure DNS servers, internet security, virtual private networks (VPNs), and Zero Trust (ZT) access for user devices.

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



Prerequisites

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

Task 1 - Configure Zero Trust

Configure connections to private resources from user devices.

- Manage Traffic Steering for Cisco Secure Client Connections

Task 2 - Configure Virtual Private Networks

Set up virtual private networks (VPNs) settings.

- Manage Virtual Private Networks

Task 3 - Configure Internet Security

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

- Add DNS Servers

- Manage Internet Security

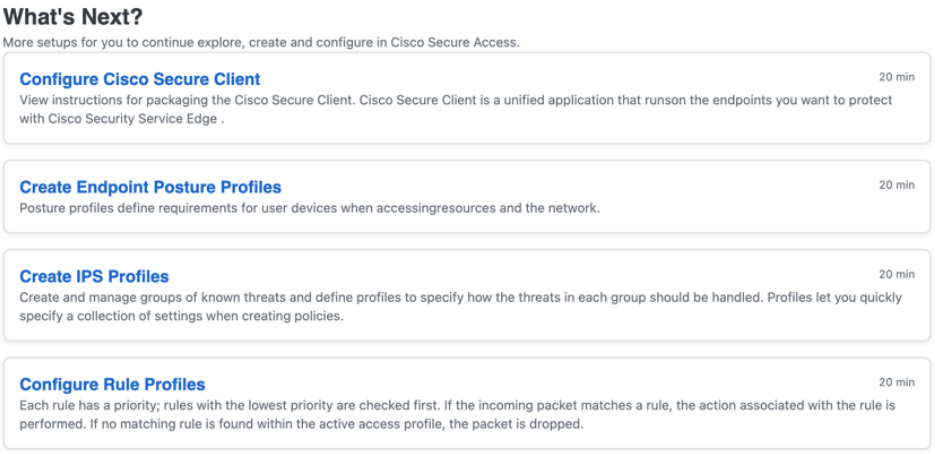
What's Next

- Step 4 – Configure Endpoints and Network Sources

Step 4 – Configure Endpoints and Network Sources

Describes step 4 – configure endpoints and network sources. The Get Started with Secure Access workflow guides you through the tasks in the What's Next step—configure your organization's user devices, add registered and internal networks to Secure Access, and configure IPS and endpoint posture profiles in policy rules.

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



Prerequisites

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

Add Networks to Secure Access

- Manage Registered Networks
- Manage Internal Networks

Set Up the Cisco Secure Client

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

Add IPS Profiles

- Manage IPS Profiles

Configure Rule Profiles

- Manage the Access Policy

Secure Access Overview Dashboard

Describes secure access overview dashboard. The Cisco Secure Access Overview dashboard lists the latest information about your organization. The Overview dashboard displays information about your organization's traffic and the amount of data transferred over your connections and correlates this with security events.

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

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

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

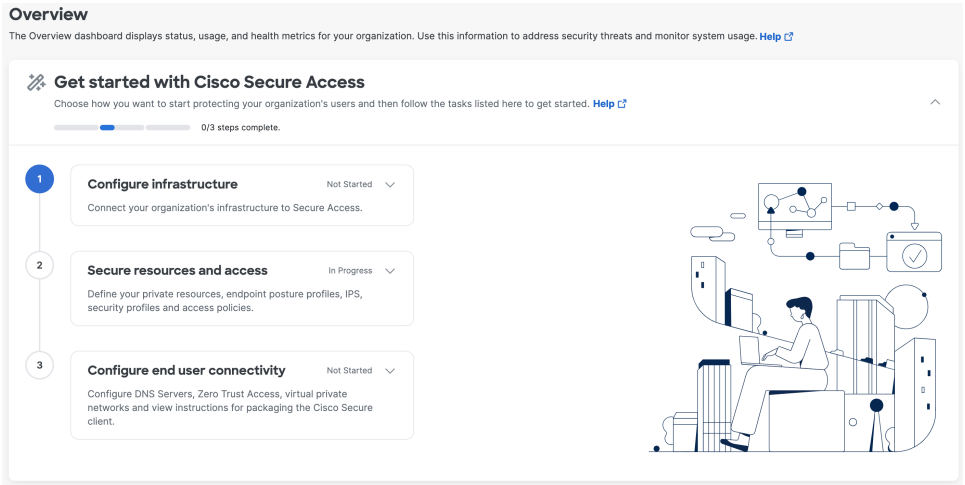
Prerequisites

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

Get Started Workflow

Describes get started workflow. The Getting Started with Secure Access workflow describes the first configuration steps required to begin protecting your systems with Secure Access.

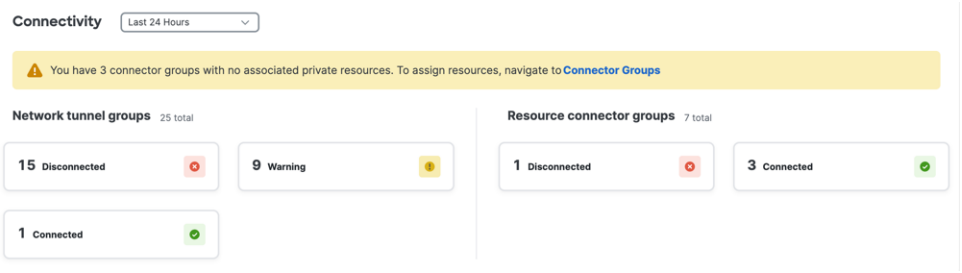
The **Getting Started with Secure Access** workflow describes the first configuration steps required to begin protecting your systems with Secure Access.



Connectivity

Describes connectivity. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

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

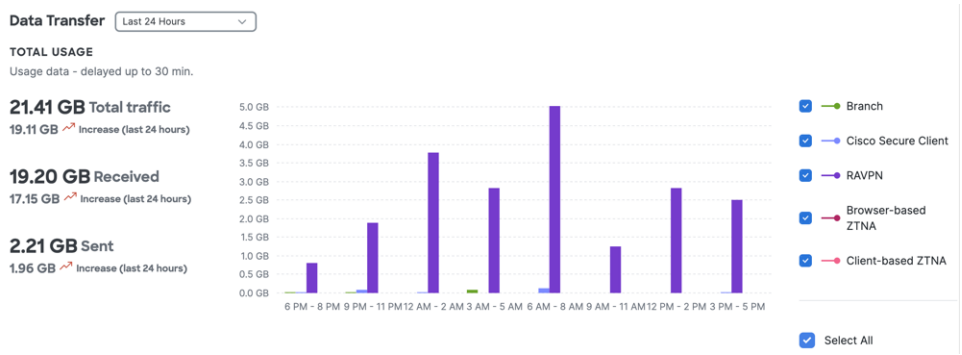


Data Transfer

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

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

- **Branch**
- **Cisco Secure Client**
- **Remote access virtual private network (RAVPN)**
- **Browser-based Zero Trust Network Access (ZTNA)**
- **Client-based Zero Trust Network Access (ZTNA)**



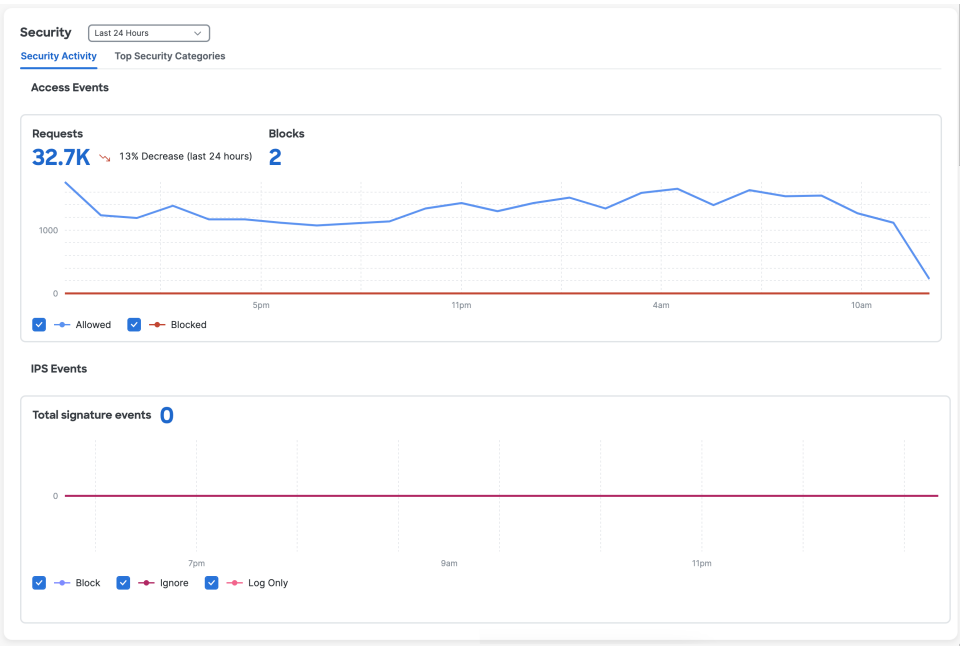
Security

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

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

Security Activity

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



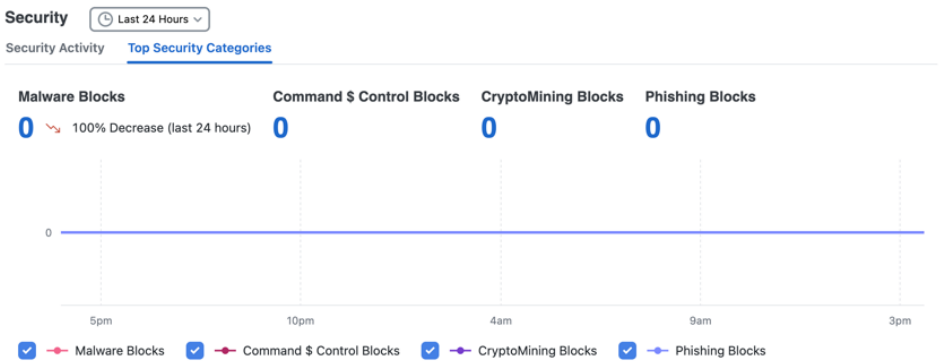
The **Security** > **Security Activity** > **IPS Events** section displays an expiry banner when a certificate for Private Resource Decryption has expired or will expire within 90 days.



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

Top Security Categories

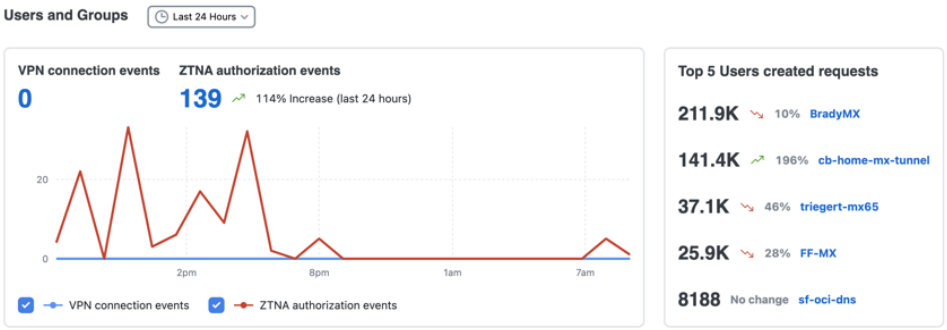
The Top Security Categories displays the number of requests to the top security categories.



Users and Groups

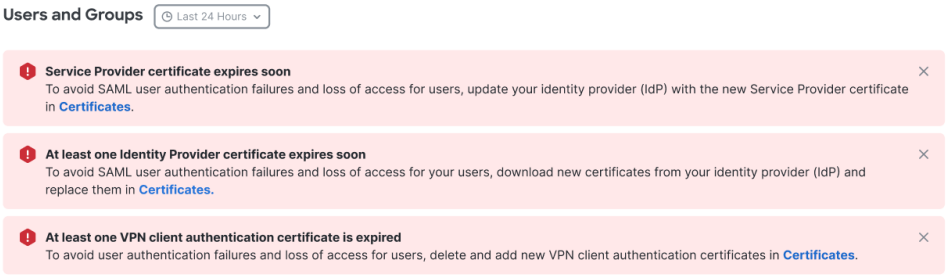
Describes users and groups. The Users and Groups section displays the number of virtual private network (VPN) connections and Zero Trust Network Access authorization events over time. This section also lists the top users in your organization who made the greatest number of requests in the selected time period.

The Users and Groups section displays the number of virtual private network (VPN) connections and Zero Trust Network Access authorization events over time. This section also lists the top users in your organization who made the greatest number of requests in the selected time period.



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

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



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

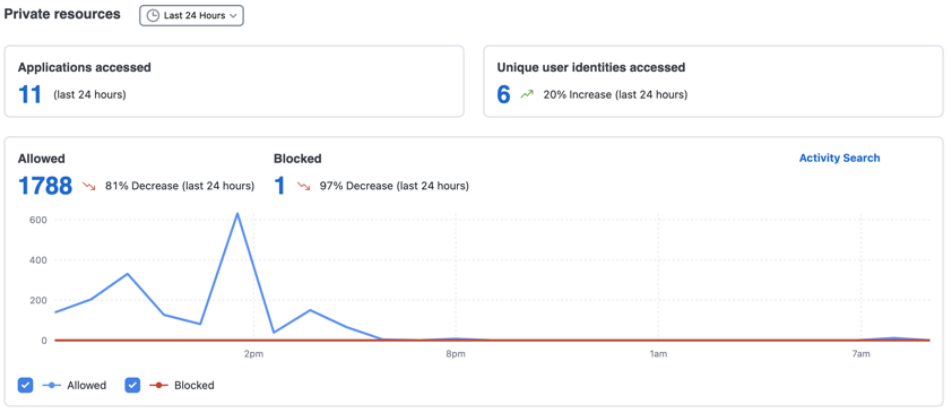
- Manage SAML Certificates for Service Providers
- Manage SAML Certificates for Identity Providers
- VPN Certificates for User and Device Authentication

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

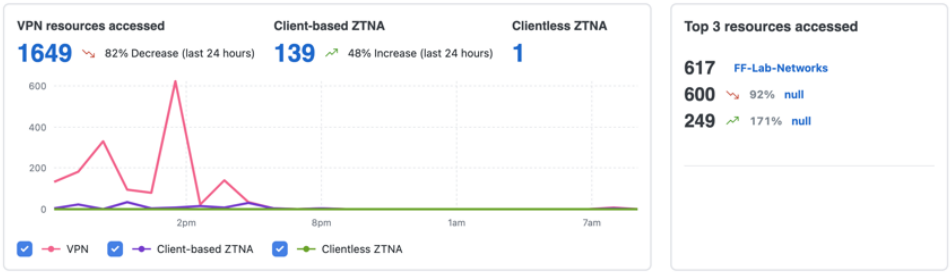
Private Resources

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

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



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



4 Quickstarts

Topics:

- Quickstart – Cisco Secure Client with Zero Trust Access
- Quickstart – Cisco Secure Client with Virtual Private Network
- Quickstart – Cisco Secure Client with Internet Security
- Quickstart – Browser with SAML Authentication
- Quickstart – Bring Your Own Device with Zero Trust

Introduces quickstarts. Quickstart tasks are designed as individual onboarding workflows. A workflow describes how to connect users in your organization securely to private, Software as a Service (SaaS), and public internet resources using various deployments.

Quickstart tasks are designed as individual onboarding workflows. A workflow describes how to connect users in your organization securely to private, Software as a Service (SaaS), and public internet resources using various deployments.

A user device can connect securely to resources through the following types of deployments:

- Cisco Secure Client deployed with Zero Trust (ZT). For more information, see Quickstart – Cisco Secure Client with Zero Trust.
- Cisco Secure Client deployed with virtual private networks (VPNs). For more information, see Quickstart – Cisco Secure Client with Virtual Private Network.
- Cisco Secure Client deployed with Internet Security. For more information, see Quickstart – Cisco Secure Client with Internet Security.
- A browser on a user device with a deployed PAC file. Configure a Secure Access Security profile and enable SAML authentication. For more information, see Quickstart – Browser with SAML Authentication.
- An unmanaged device connecting with Zero Trust (ZT). For more information, see Quickstart – Bring Your Own Device with Zero Trust.

Prerequisites

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

Quickstart – Cisco Secure Client with Zero Trust Access

Provides instructions for quickstart - cisco secure client with zero trust access. The Cisco Secure Client with Zero Trust Access connects user devices securely to private resources in on-premises data centers managed by your organization and resources in private and public clouds.

The Cisco Secure Client with Zero Trust Access connects user devices securely to private resources in on-premises data centers managed by your organization and resources in private and public clouds. Cisco Secure Access Zero supports visibility into user and device identities, network connectivity, and security posture.

User devices must have the Cisco Secure Client with Zero Trust Access deployed and configure a Secure Access Zero Trust Access endpoint posture profile. Users are members of the organization who manages their devices. An administrator must configure the Zero Trust Access endpoint posture profiles in Secure Access and apply a policy rule that includes the Zero Trust Access profiles to the user devices.

The procedure to start onboarding user devices in an organization with the Secure Client and Zero Trust Access should take no more than ten minutes.

Before you begin

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

Procedure

1. Deploy network connectors in Secure Access.
   - Deploy network tunnel groups in Secure Access. For more information, see Manage Network Tunnel Groups.
   - Configure a network tunnel on a network device from within your data center or public network. For more information, see Device Compatibility and Network Tunnels.
2. Provision users and groups in Secure Access. For more information, see Manage Users, Groups, and Endpoint Devices.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create Zero Trust (ZT) posture profiles for the user devices in the organization. For more information, see Manage Zero Trust Access Posture Profile.
5. Create a policy rule or add an ZT posture profile to an existing Secure Access rule. For more information, see Manage the Access Policy.
6. Deploy Cisco Secure Client with Zero Trust on user devices.
   - Download Cisco Secure Client
   - Install the Cisco Secure Client
   - Invite Users to Enroll in Zero Trust Access for Secure Client

What to do next

Test Your Connectivity

- Check that you can reach private resources protected by Secure Access.

Quickstart – Cisco Secure Client with Virtual Private Network

Provides instructions for quickstart – cisco secure client with virtual private network. Cisco Secure Client with VPN connects user devices securely to private resources in data centers managed by your organization and software as a service (SaaS) resources in private and public clouds.

Cisco Secure Client with VPN connects user devices securely to private resources in data centers managed by your organization and software as a service (SaaS) resources in private and public clouds. The procedure to start onboarding user devices in an organization with the Cisco Secure Client and VPN access should take no more than ten minutes.

A VPN provides a point-to-point, private network between a user device and a resource where the traffic sent over the network is encrypted and the IP address of the source is hidden.

User devices must have the Secure Client deployed with the VPN module and VPN XML metadata file, and configure a Secure Access VPN endpoint posture profile. Users are members of the Secure Access organization that manages their devices. An administrator must configure the network connections–Network Tunnel Groups

–for the organization.

Before you begin

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

Procedure

1. Deploy network connectors in Secure Access.
   - Deploy network tunnel groups in Secure Access. For more information, see Manage Network Tunnel Groups.
   - Configure a network tunnel on a network device from within your data center or public network. For more information, see Device Compatibility and Network Tunnels.
2. Provision users and groups in Secure Access. For more information, see Manage Users, Groups, and Endpoint Devices.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create a VPN endpoint posture profile for the user devices. For more information, see Add a VPN Connection Posture Profile.
5. Create a policy rule or add a VPN endpoint posture profile for the user devices to an existing Secure Access rule. For more information, see Manage the Access Policy.
6. Deploy Cisco Secure Client with VPN on user devices in the organization.
   - Download Cisco Secure Client
   - Download the VPN XML File
   - Install the Cisco Secure Client

What to do next

Test Your Connectivity

- Check that you can reach private, SaaS, and internet resources protected by Secure Access.

Quickstart – Cisco Secure Client with Internet Security

Provides instructions for quickstart - cisco secure client with internet security. Full Admin user role. For more information, see Manage Accounts.

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

The Cisco Secure Client with Internet Security–DNS-layer security and secure web gateway (SWG)–connects user devices securely to internet resources. The procedure to start onboarding user devices in an organization with the Cisco Secure Client and Internet Security access should take no more than ten minutes.

User devices must have the Cisco Secure Client deployed with the Umbrella module. Users are members of the organization that manages their devices. An administrator must configure the network connections–Network Tunnel Groups– and add Registered Networks and Internal Networks to their Secure Access organization.

Procedure

1. Deploy network connectors in Secure Access.
   - Deploy network tunnel groups in Secure Access. For more information, see Manage Network Tunnel Groups.
   - Configure a network tunnel on a network device from within your data center or public network. For more information, see Device Compatibility and Network Tunnels.
2. Provision users and groups in Secure Access. For more information, see Manage Users, Groups, and Endpoint Devices.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create a Web posture profile for the user devices. For more information, see Add a Security Profile.
5. Create a policy rule or add a Security profile for the user devices to an existing Secure Access rule. For more information, see Manage the Access Policy.
6. Deploy Cisco Secure Client with Umbrella on user devices in the organization.
   - Download Cisco Secure Client
   - Download the OrgInfo.json File
   - Install the Cisco Secure Client

What to do next

Test Your Connectivity

- Check that you can reach internet resources protected by Secure Access.

Quickstart – Browser with SAML Authentication

Provides instructions for quickstart - browser with saml authentication. This Quickstart guide describes how to connect user devices securely to internet resources from a browser. The onboarding procedure should take no more than ten minutes.

This Quickstart guide describes how to connect user devices securely to internet resources from a browser. The onboarding procedure should take no more than ten minutes.

User devices must have a browser installed and configure a Secure Access Security profile. Users are members of the organization that manages their devices.

Before you begin

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

Procedure

1. Provision users and groups in Secure Access. For more information, see Manage Users, Groups, and Endpoint Devices.
2. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
3. Create a Secure Access Security profile that includes the user devices. For more information, see Add a Security Profile.
4. Set up a Secure Access PAC file. For more information, see Manage PAC Files.
5. Create a policy rule or add a Security profile to an existing Secure Access rule. For more information, see Manage the Access Policy.

What to do next

Test Your Connectivity

- Check that you can reach internet resources protected by Secure Access.

Quickstart – Bring Your Own Device with Zero Trust

Provides instructions for quickstart – bring your own device with zero trust. Full Admin user role. For more information, see Manage Accounts.

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

Cisco Secure Access Zero Trust Access can connect unmanaged devices securely to private resources in on-premises data centers managed by your organization and in private and public clouds. Secure Access ZT provides visibility into user and device identities, supports network connectivity, and manages the security posture of unmanaged devices.

Bring your own devices (BYODs) are devices that are not managed by your organization, but are devices that are permitted by your organization to connect to certain private resources. An administrator shares an organization's private resource URL to the user of a BYOD device. An administrator must include the BYOD device in the Secure Access ZT endpoint posture profile and users of the devices are members of the organization.

The procedure to start onboarding unmanaged devices with Secure Access Zero Trust in an organization should take no more than ten minutes.

Procedure

1. Deploy network connectors in Secure Access.
   - Deploy network tunnel groups in Secure Access. For more information, see Manage Network Tunnel Groups.
   - Configure a network tunnel on a network device from within your data center or public network. For more information, see Device Compatibility and Network Tunnels.
2. Provision users and groups in Secure Access. For more information, see Manage Users, Groups, and Endpoint Devices.

3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create Zero Trust (ZT) posture profiles for the user devices in the organization. For more information, see Manage Zero Trust Access Posture Profile.
5. Provide Secure Access private resource URLs to users on unmanaged devices.
6. Create a policy rule or add an ZT posture profile to an existing Secure Access rule. For more information, see Manage the Access Policy.

What to do next

Test Your Connectivity

- Check that you can reach private resources protected by Secure Access.

5 Secure Access Integration with Protective DNS

Topics:

- Secure Access Integration with Protective DNS

Describes the purpose and procedures for secure access integration with protective dns and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Secure Access Integration with Protective DNS

Describes secure access integration with protective dns. Secure Access for Government (SAGov) now supports direct integration with Protective DNS (PDNS), enabling your organization to comply with government mandates and strengthen security across all user and device locations.

Secure Access for Government (SAGov) now supports direct integration with Protective DNS (PDNS), enabling your organization to comply with government mandates and strengthen security across all user and device locations. This integration provides centralized, policy-driven DNS protection and visibility, leveraging government-approved cloud resolvers and the latest threat intelligence.

Key Benefits

- Meet government PDNS mandates with cloud-delivered security
- Benefit from advanced threat intelligence, powered by Cisco Talos and real-time DNS data
- Apply consistent DNS policy enforcement across on-premises, remote, and mobile users

How the Integration Works

When integrated, Secure Access directs DNS requests from your network—across on-premises, remote, and mobile environments—to a specialized set of U.S.-based DNS resolvers. These resolvers forward your organization's DNS queries to Protective DNS for evaluation and policy enforcement. DNS responses return through Secure Access, where organizational DNS policies are applied before being delivered to users and devices.

This architecture helps ensure:

- Compliance with Protective DNS mandates
- Centralized enforcement and reporting for DNS activity
- Protection from threats such as malware, phishing, and command-and-control domains

Procedure for Integrating Secure Access with Protective DNS

Provides instructions for procedure for integrating secure access with protective dns. Configure the SSE Source Set in Protective DNS. Log in to the Protective DNS management portal.

Procedure

1. Configure the SSE Source Set in Protective DNS.
   a) Log in to the Protective DNS management portal.
   b) Navigate to **My Organization**.
   c) Under **Authorized Sources**, select **Add New**.
   d) In the Add New Source window:
      1. Set the **Type** to **SSE Provider**.
      2. Select **Cisco** as the Secure Service Edge (SSE) Provider.
      3. Use an existing Source Set or create a new one.
      4. Optionally, provide a description indicating which user groups will use this Source Set.
      5. Create a separate Source Set for each Secure Access Organization ID if required.
   e) Click **Save**. The new Source Set will appear in the Authorized Sources list with a unique IPv6 address.

2. Notify Cisco of Source Set IPv6 Address and Organization ID.

   For backend setup, provide Cisco with:

   - The IPv6 address of your new Source Set
   - Your Secure Access Organization ID

   To submit this information:

   a. Locate the Source Set configuration in your Authorized Sources table.

   b. Find your Secure Access Organization ID. For more information, see Find Your Organization ID.

   c. Email your Cisco Secure Access Customer Success Manager (CSM) with the Source Set IPv6 address and your Organization ID. If you do not know who your CSM is mail your Cisco Account Manager so the information can be properly forwarded.

      Important

      Wait for Cisco's confirmation that the backend configuration is complete, before moving to the next step.

3. Validate Protective DNS Integration.

   To confirm integration and content blocking, on a client device configured to use Secure Access for Government DNS resolvers, run: `nslookup heartbeat.protectivedns.net`

   The result should show the PDNS lander address, confirming that DNS traffic is being processed by Protective DNS.

   Note

   Secure Access applies DNS policies to all queries. Blocked requests are immediately dropped and will not be forwarded to PDNS. Requests permitted or denied by Secure Access policies may not appear in the Protective DNS UI, but will be recorded in the Secure Access logs.

6 Limitations and Range Limits

Topics:

- Limitations and Range Limits

Describes the purpose and procedures for limitations and range limits and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Limitations and Range Limits

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

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

- Internet Protocol Versions
- Users and Groups
- Data Retention
- Reports
- Access Policy
- Cisco Secure Client

Internet Protocol Versions

Secure Access supports IPv4 and IPv6 to accommodate different network environments. The dashboard and wizards guide you in selecting the appropriate protocol based on your requirements.

Protocol configuration types

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

Upstream Connectivity and Protocol Handling

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

Important

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

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

Table 1: Internet Protocol support by Function

Function in Secure Access	Client-to-Cloud Connection (Ingress)	Cloud-to-Destination Forwarding (Egress)
Remote Access VPN	IPv4, Pure IPv6, or Dual stack	IPv4 and IPv6 traffic forwarding (No IPv6 to IPv4 fallback)
IPsec tunnel (Network Tunnel Group)	IPv4, Pure IPv6, or Dual stack	IPv4 and IPv6 traffic forwarding (No IPv6 to IPv4 fallback)

Function in Secure Access	Client-to-Cloud Connection (Ingress)	Cloud-to-Destination Forwarding (Egress)
Roaming Security Module	IPv4 or Pure IPv6	IPv4 or Pure IPv6
DNS	IPv4, Pure IPv6, or Dual stack	IPv4 or Pure IPv6

Users and Groups

- You can import no more than 200 Groups into a Secure Access organization.
- For access to private applications, configure the user and private applications to use the same data center.

Data Retention

- DNS logs–Summary data (such as queries per identity or domain) is available for one calendar year.
- DNS, Web proxy, firewall logs–Data retained for 30 days.

Reports

Feature	Limit
• Total Requests • Top Destinations • Top Categories • Top Identities	Data available for one calendar year.
• Activity Search • Security Activity	Data retained for 30 days.
• Activity Volume	Data retained for one calendar year.
• Admin Audit Log	Data retained for one calendar year. You can access data in 90-day increments.
Scheduled Report (email attachment)	Accepts up to 10,000 rows of data.
Exported Report (CSV export)	Exports no more than 1,000,000 rows of data.

Access Policy

- The Secure Access Unified Policy Framework supports 5000 rules.

Cisco Secure Client

- Secure Access checks the Cisco Secure Client Zero Trust Access (ZTA) posture profile every 30 minutes.
- Secure Access applies private application configuration changes to the Cisco Secure Client every 30 minutes.

7 Network Requirements for Secure Access

Topics:

- Network Requirements for Secure Access

Describes the purpose and procedures for network requirements for secure access and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Network Requirements for Secure Access

Describes network requirements for secure access. This document describes the network configurations that support connections to the Secure Access cloud services and other Secure Access services and applications

This document describes the network configurations that support connections to the Secure Access cloud services and other Secure Access services and applications

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

Secure Access DNS Resolvers

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

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

IPv4	Port/Protocol	Description
18.252.251.72	53 TCP/UDP	Primary
18.254.118.193	53 TCP/UDP	Secondary

Best Practices

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

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

Cisco Secure Client

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

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

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

Cisco Secure Client and External DNS Resolution

Describes cisco secure client and external dns resolution. In normal circumstances, the Cisco Secure Client Umbrella Roaming Security module functions only on networks where external DNS resolution exists.

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

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

- **devices.api.secureaccessfed.cisco**
- **crl3.digicert.com**
- **crl4.digicert.com**
- **ocsp.digicert.com**
- **debug.umbrellagov.com**–This domain can receive a response to a TXT record query. The Cisco DNS resolvers must answer this DNS request.

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

Secure Access Encrypted DNS Queries

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

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

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

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

IPv4	Port/Protocol	Description
18.252.251.72	443 TCP/UDP	Primary
18.254.118.193	443 TCP/UDP	Secondary

Secure Access DNS, Web, and Block Pages

Describes secure access dns, web, and block pages. Required by applications or devices connecting to the Secure Access DNS-layer security, including Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security).

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

We recommend that you allow all traffic on ports 80 and 443 over TCP for the Secure Access DNS-layer, internet security, and Block Page services.allow the following CIDRs and/or domains in your firewalls on ports 80 and 443 over TCP.

- block.umbrellagov.com

- phish.umbrellagov.com
- malware.umbrellagov.com
- block.secureaccessfed.cisco
- phish.secureaccessfed.cisco
- malware.secureaccessfed.cisco

IP	Ports/Protocol
18.252.84.15	80/443 TCP
18.254.162.83	80/443 TCP
18.254.77.32	80/443 TCP
16.64.101.72	80/443 TCP
16.64.116.188	80/443 TCP
16.64.19.231	80/443 TCP
16.64.3.101	80/443 TCP
16.64.34.204	80/443 TCP
16.64.44.65	80/443 TCP
16.64.58.196	80/443 TCP
16.64.77.81	80/443 TCP
16.64.88.211	80/443 TCP
18.252.224.185	80/443 TCP
18.252.236.99	80/443 TCP
18.252.86.49	80/443 TCP
18.253.205.239	80/443 TCP
18.253.45.107	80/443 TCP
18.253.87.126	80/443 TCP
18.253.94.118	80/443 TCP
18.254.225.10	80/443 TCP
18.254.233.234	80/443 TCP
18.254.71.48	80/443 TCP
182.30.49.246	80/443 TCP
182.30.95.86	80/443 TCP

Secure Access DNS and Web – Client Configuration Services

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

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

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

Domains	Port/Protocol	Description
gateway.id.secureaccessfed.cisco	443/TCP	Configuration
devices.api.secureaccessfed.cisco	443/TCP	Configuration

The Cisco Secure Client Umbrella Roaming Security module uses HTTP (80/TCP) and HTTPS (443/TCP) to communicate with Secure Access for the following uses:

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

IP Ranges	Ports	Protocol
18.252.251.72	53/443	UDP & TCP
18.254.118.193	53/443	UDP & TCP

Windows Only

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

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

Secure Access DNS and Web – Client Sync Services

Describes secure access dns and web - client sync services. Required by devices or applications that are protected by Secure Access DNS or Web security. Includes Cisco Secure Client deployments with the Umbrella Roaming Security module.

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

Domains	Port/Protocol	Description
devices.api.secureaccessfed.cisco	443/TCP	Syncing data

The **devices.api.secureaccessfed.cisco** domain resolves to multiple IP addresses, all within the 146.112.63.0/24 IP range. We recommend that you add this entire range. The IP addresses for **devices.api.secureaccessfed.cisco** are Anycast and may change.

Secure Access DNS and Web – Client Certificate Revocation Services

Describes secure access dns and web - client certificate revocation services. Required by devices or applications that are protected by Secure Access DNS or Web security. Includes the Secure Access Active Director (AD) Connector and Cisco Secure Client deployments with the Umbrella Roaming Security module.

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

Domains	Port/Protocol	Description
crl3.digicert.com	80/TCP	CRL
crl4.digicert.com	80/TCP	CRL
ocsp.digicert.com	80/TCP	OCSP

Note

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

Cisco Secure Client and Captive Portal Detection

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

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

- **msftconnecttest.com**
- **msftncsi.com**

Note

The **msftconnecttest.com** and **msftncsi.com** domains have dynamic IP addresses.

Cisco Secure Client and Device Hostnames

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

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

Transport Layer Security Protocol Requirements

Describes transport layer security protocol requirements. The Secure Access Transport Layer Security (TLS) Protocol Network Information. Ensure that the operating systems of the devices in the organization support at a minimum TLS 1.2.

The Secure Access Transport Layer Security (TLS) Protocol Network Information.

Ensure that the operating systems of the devices in the organization support at a minimum TLS 1.2. The TLS 1.0 and TLS 1.1 protocols contain security vulnerabilities and do not support modern cryptographic algorithms.

TLS 1.2 Support in Windows

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

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

TLS 1.2 Support in macOS

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

Secure Access Secure Web Gateway Services

Describes secure access secure web gateway services. Required by the Secure Access Network Tunnel and PAC file deployments, and Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules.

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

Egress IP Addresses for the Secure Web Gateway

This topic describes the egress IP addresses used for public web traffic in the Government environment.

All public web traffic through the secure web gateway egresses from the SWG account using the following NAT gateway IP addresses:

- 18.254.231.190
- 18.253.158.121
- 18.254.222.101

Ingress IP Addresses for the Secure Web Gateway

Describes ingress ip addresses for the secure web gateway. To enable connections to the Secure Access Secure Web Gateway, allow the following CIDRs and/or domains in your firewalls on ports 80 and 443 over TCP.

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

- swg.secureaccessfed.cisco
- 18.252.203.75
- 18.254.63.241
- 18.253.118.199

Egress IP addresses

This topic lists the egress IP addresses required for web and non web traffic in the Cisco Secure Access for Government environment.

All public web and non web traffic egresses from the Cisco Secure Access for Government environment using the following IP addresses.

If you connect to services that implement IP allow listing, provide these IP addresses to ensure connectivity:

- 18.254.231.190

- 18.253.158.121
- 18.254.222.101

Secure Access SaaS Tenants

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

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

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

Microsoft 365

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

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

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

Secure Access SAML Gateway Services

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

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

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

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

Unless noted, send **gateway.id.secureaccessfed.cisco** requests to the SWG, not directly to the internet.

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

Active Directory Federation Service SAML Identity Provider

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

Secure Access SAML Identity Provider Domains

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

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

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

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

Azure AD SAML Identity Provider

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

Domain	Port/Protocol
portal.azure.com	80/443 TCP
login.live.com	80/443 TCP
login.microsoftonline.com	80/443 TCP
msauth.net	80/443 TCP
msftauth.net	80/443 TCP

Secure Access SAML Gateway Client Certificate Revocation Services

Describes secure access saml gateway client certificate revocation services. Required by Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules, and Secure Access integrations with SAML identity providers (IdPs).

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

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

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

Secure Access VPN Services

Describes secure access vpn services. Required by Cisco Secure Client deployments with the Virtual Private Network (VPN) module. The Cisco Secure Client VPN module uses HTTPS to communicate with the Secure Access VPN client head end services.

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

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

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

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

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

Secure Access VPN Client Certificate Revocation Services

Describes secure access vpn client certificate revocation services. Required by Cisco Secure Client deployments with the Virtual Private Network (VPN) module.

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

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

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

Secure Access Zero Trust Client-Based Enrollment Services

Describes secure access zero trust client-based enrollment services. Required by Cisco Secure Client deployments with the Zero Trust module. The Cisco Secure Client Zero Trust module uses HTTPS to communicate with the Secure Access Zero Trust device enrollment services.

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

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

Domain	Ports/Protocol
ztna.secureaccessfed.cisco	443 TCP
acme.secureaccessfed.cisco	443 TCP

Domain	Ports/Protocol
devices.api.secureaccessfed.cisco	443 TCP
sseposture.secureaccessfed.cisco	443 TCP

Secure Access Zero Trust Client-Based Proxy Services

Describes secure access zero trust client-based proxy services. Required by Cisco Secure Client deployments with the Zero Trust module. The Cisco Secure Client Zero Trust module uses HTTPS to communicate with the client-based Secure Access Zero Trust proxy services.

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

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

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

Known Network Restrictions for Zero Trust Clients

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

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

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

Describes secure access zero trust client-based proxy – client certificate revocation services. Required by Cisco Secure Client deployments with the Zero Trust module.

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

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

Domains	Port/Protocol
*.ztna.secureaccessfed.cisco	443 TCP

Secure Access Zero Trust Proxy Services – Unmanaged Devices

Describes secure access zero trust proxy services – unmanaged devices. Required by devices that are on an organization's network, connect to Secure Access with Zero Trust, and do not have the Cisco Secure Client deployed.

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

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

Domains	Port/Protocol
*.ztna.secureaccessfed.cisco	443 TCP

8 Manage Network Connections

Topics:

- Manage Network Connections

Describes the purpose and procedures for manage network connections and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Network Connections

Describes managing network connections. Configure Network Tunnel Groups to route traffic from remote and on-premises users to the internet and to private destinations managed by your organization, and to route branch-to-branch traffic.

Configure Network Tunnel Groups to route traffic from remote and on-premises users to the internet and to private destinations managed by your organization, and to route branch-to-branch traffic.

For connections to configured private resources, Secure Access supports directing user traffic through Network Tunnel Groups, which involve virtual machine instances deployed on your network.

You can configure one or more Network Tunnel Groups as needed.

IPsec Network Tunnels

Describes ipsec network tunnels. Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels.

Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels. Network devices that are capable of establishing IPsec IKEv2 tunnels forward traffic to one of the Secure Access data centers where the tunnel head end is located. For more information, see Manage Network Tunnel Groups.

User devices can read, write, and update private resources by setting up virtual private networks (VPNs) or zero trust network access (ZTNA) connections to Secure Access through IPsec network tunnels.

> **Note**
>
> If a private resource is served by multiple tunnel groups and more than one is available, traffic will be routed according to your configured priorities and policies.

Network Connection Method

Describes network connection method. Traffic from remote users to private destinations is directed using Network Tunnels, which are deployed in Network Tunnel Groups.

Traffic from remote users to private destinations is directed using Network Tunnels, which are deployed in Network Tunnel Groups.

You can configure one or more Network Tunnel Groups for your resources, based on your organization's requirements. For more information about traffic handling and configuration, see [Manage Network Connections].

Network Tunnels (Deployed in Network Tunnel Groups)

Describes network tunnels (deployed in network tunnel groups). Characteristics of network tunnel groups: Can route internet-bound traffic as well as traffic to private resources.

Characteristics of network tunnel groups:

- Can route internet-bound traffic as well as traffic to private resources.
- Support VPN, branch-to-branch, and Zero trust network access (client-based and browser-based) connections.
- Require networking devices on your network that can initiate IPSec tunnels. See Device Compatibility and Network Tunnels.
- Network routing configuration is required.

- Extend your network to the Secure Access cloud.
- Many supported virtual and hardware platforms, simplifying connections to your existing environment. You may be able to use existing infrastructure, without deploying additional devices.

For more information, see Manage Network Tunnel Groups and subtopics.

9 Manage Network Tunnel Groups

Topics:

- Device Compatibility and Network Tunnels
- Add a Network Tunnel Group
- Delete a Network Tunnel Group
- Edit a Network Tunnel Group
- View Network Tunnel Group Details
- Supported IPsec Parameters

Introduces managing network tunnel groups. Tunnels and tunnel groups are core concepts in managing connections between your data centers and Cisco Secure Access.

Tunnels and tunnel groups are core concepts in managing connections between your data centers and Cisco Secure Access.

- Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels.
- Network devices that are capable of establishing IPsec tunnels forward traffic to one of the Secure Access data centers where the tunnel head end is located.
- User devices can read, write, and update private resources by setting up virtual private networks (VPNs) or zero trust network access (ZTNA) connections to Secure Access through these IPsec tunnels.
- A network tunnel group provides the framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources.

Device Compatibility and Network Tunnels

Describes device compatibility and network tunnels. Secure Access connects and secures traffic from IPsec tunnels established by various network devices. A network device must have the capability to configure an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel and connect to Secure Access.

Secure Access connects and secures traffic from IPsec tunnels established by various network devices. A network device must have the capability to configure an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel and connect to Secure Access.

IPsec Tunnel Requirements

IPsec tunnels for Secure Access must have an MTU that is no larger than 1390 bytes. Secure Access automatically clamps the TCP MSS to 1350 or below.

Fragmented packets in underlay or overlay are dropped. Slightly larger MTU and MSS may work depending on your IPsec configuration. For more information about establishing tunnels to Secure Access, see the tunnel configuration topics found in Network Tunnel Configuration.

Supported Devices for Setting Up IPsec Tunnels

Secure Access integrates with network devices that can create compatible IPsec tunnels. We provide guides to configure tunnels from various network devices. For devices where the setup is not documented, we cannot guarantee that the device can establish an IPsec tunnel to Secure Access.

Platform	Software Version
Cisco Meraki MX - Configure Tunnels with Meraki MX	15.3
Cisco Catalyst SD-WAN - Configure Tunnels with Cisco Catalyst SD-WAN	18.4.5+, 19.2.3+
Cisco ISR-G2 - Configure Tunnels with Cisco ISR	15.4M3
Cisco ASA - Configure Tunnels with Cisco Adaptive Security Appliance (ASA)	Cisco ASA v9.8
Cisco FTD - Configure Tunnels with Cisco Secure Firewall	6.4+ (6.7 when using VTI)

Add a Network Tunnel Group

Provides instructions for adding a network tunnel group. Configure network tunnel groups in Cisco Secure Access to provide high availability and redundancy for IPsec tunnels connected to data center hubs.

This task describes how to configure network tunnel groups in Cisco Secure Access to provide high availability and redundancy for IPsec tunnels connected to data center hubs.

Network tunnel groups enable high-availability connectivity by allowing multiple IPsec tunnels to share primary and secondary hub sites. Any network device capable of establishing an IPsec tunnel can join a network tunnel group using the credentials generated during deployment.

Regardless of your network device type, the setup process follows these three steps:

1. **Configure and deploy the tunnel group:** In Secure Access, define the tunnel group attributes and deploy the group. Upon deployment, the tunnel group status changes from **Unestablished** to **Inactive**.
2. **Configure tunnels on your network device:** Configure the primary and secondary tunnels on your network device to send traffic to Secure Access. Associate these tunnels with the deployed tunnel group using the required attributes, including the tunnel ID, tunnel passphrase, and the Secure Access data center IP address.

3. **Enable traffic flow and monitor status:** Once user devices are configured to connect through the tunnel, Secure Access logs the traffic and the tunnel status changes to Active. You can monitor the status of tunnel groups and individual tunnels, as well as view related events, on the Secure Access **Status** page, Secure Access Overview and Activity Search.

Follow these detailed steps to add a network tunnel group in Secure Access.

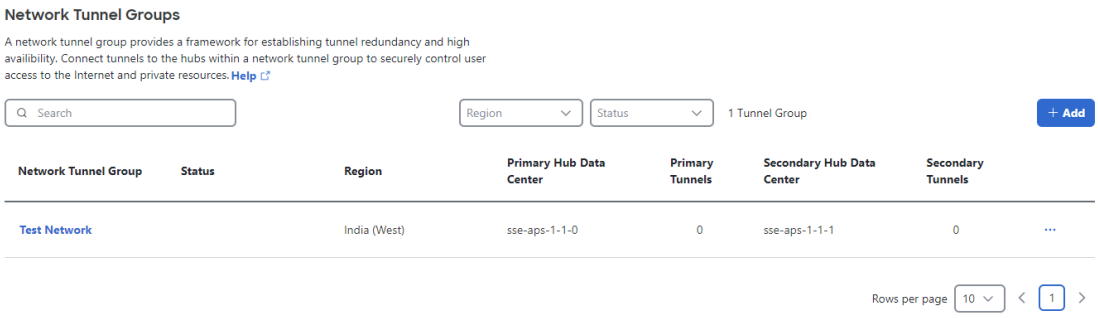
Before you begin

Ensure that your account has the Full Admin role in Secure Access. For more information, refer to Manage Accounts.

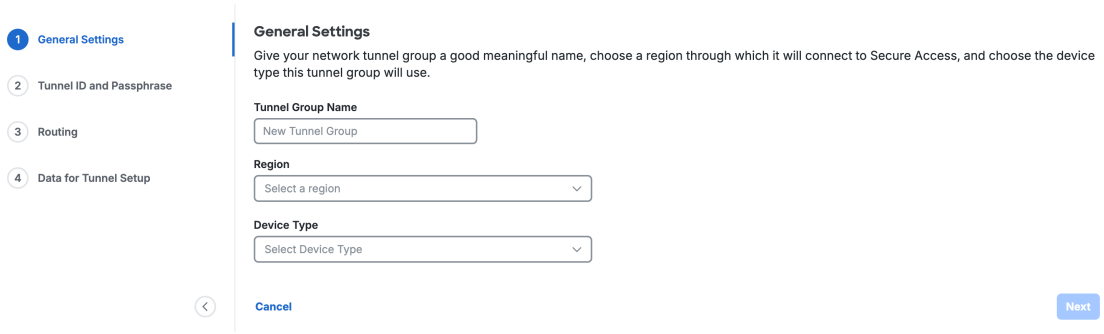
Procedure

Step 1 - General Settings

1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
2. Click **Add**.



3. Enter the **General Settings** for your tunnel group:
   - **Tunnel Group Name**: Enter a meaningful name for the tunnel group.
   - **Region**: Select a Secure Access region from the dropdown list.
   - **Device Type**: Choose the network device type from the dropdown list.
   - Click **Next**.



Step 2 - Tunnel ID and Passphrase–Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

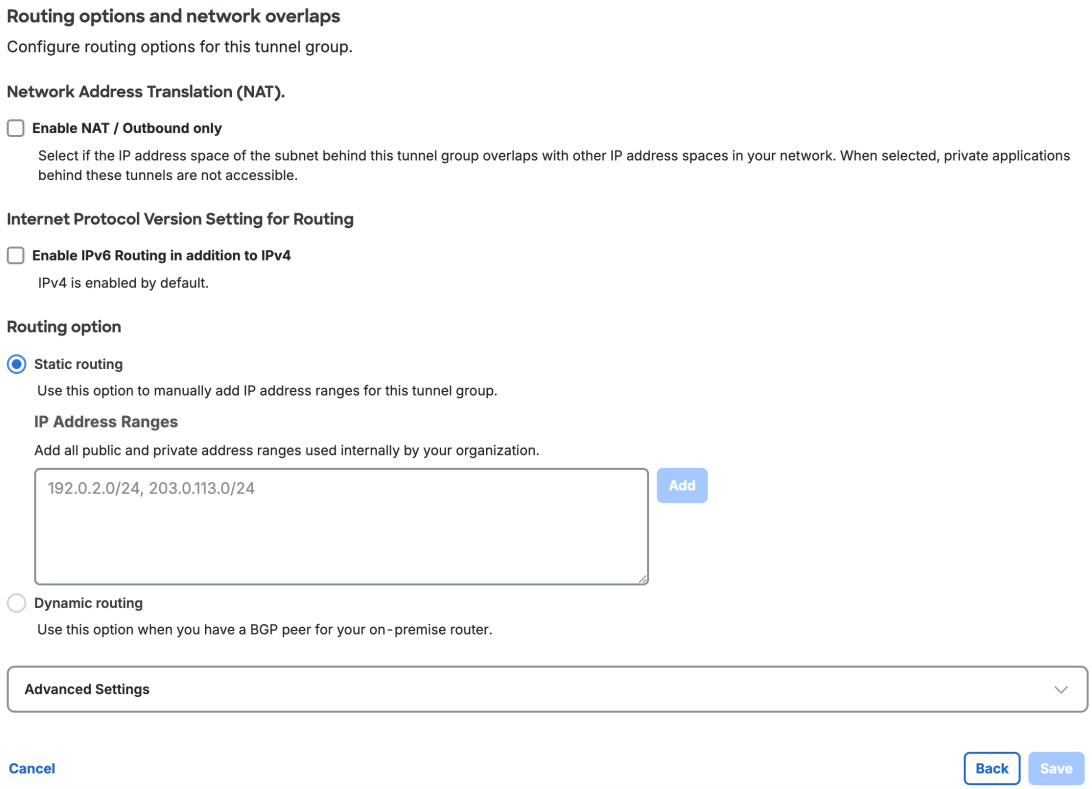
4. Enter the **Tunnel ID**.
   - Tunnel ID may be an email address or a primary and secondary pair of IP addresses.
   - Tunnel ID format requirements vary based on the device type selected in **Step 1 - General Settings**:

Device Type	Tunnel ID Format
Meraki MX	Email
Catalyst SDWAN	Email
ISR	Email
ASA	Email OR IP address (primary and secondary)
AWS	IP address (two each for primary and secondary)
AZURE	IP address (primary and secondary)
FTD	Email OR IP address (primary and secondary)
Other	Email OR IP address (primary and secondary)

- Email tunnel ID requires the format `<tunnel name>@<org><hub>.secureaccessfed.cisco`. Use the name you assigned to the tunnel group in **Step 1 - General Settings**.
- IP address Tunnel IDs require both a primary and a secondary IP address.
- IP address Tunnel IDs support both IPv4 and IPv6.

5. Enter a tunnel **Passphrase** between 16 and 64 characters in length. The passphrase must contain at least one upper case letter, one lower case letter, and one number. The passphrase cannot include any special characters.
6. Reenter your passphrase to confirm.
7. Click **Next** to continue.

Step 3 - Routing – Configure routing options and network overlaps for this tunnel group.



8. Select **Enable NAT / Outbound only** if the IP address space behind this tunnel group overlaps with other IP address spaces in your network. NAT mapping translates real IP prefixes to unique mapped prefixes to resolve address conflicts and enable routing between branch sites, partner networks, and cloud applications.

a) Check the box to enable NAT and reveal the **Source Mappings** and **Destination NAT Mappings** sections.
b) Review the **Source Mappings** tiles.

Source mapping tiles display the translation behavior for source IP addresses in each traffic direction.

- **Site → Secure Access** – Source addresses are automatically translated to the Secure Access NAT subnet. This mapping is not configurable. To request a change to the source translation pool, contact Cisco Secure Access Support.
- **Secure Access → Site** – By default, source addresses are translated to the Secure Access NAT subnet. Override this default by enabling **Translate to Secure Access NAT subnet** and entering a custom IP prefix range. This mapping applies to all destination NAT mappings.

> **Note**
>
> When no destination mappings are configured, the **Secure Access → Site** source mapping has no effect. In this state, the NTG performs outbound-only NAT.

c) Configure **Destination NAT Mappings**.

Destination NAT mappings translate destination IP addresses for traffic between your network and external destinations. You can create up to 100 mappings per direction in each NTG.

Click + Add Mappings and configure the following fields:

- **Name** – Enter a name that clearly identifies the mapping.
- **Direction**:
  - **Secure Access → Site** – Translates destination IP addresses in the **Original CIDR** for inbound traffic to devices on your network. Sources send traffic to the **Translated CIDR** to reach destinations on your network.
  - **Site → Secure Access** – Translates destination IP addresses in the **Original CIDR** for outbound traffic from devices on your network. Devices send traffic to the **Translated CIDR** to reach cloud, branch, or partner destinations.
- **Original CIDR** – The untranslated IP address range.
- **Translated CIDR** – The translated IP address range.
- **Description** – (Optional) Additional context for the mapping. Limited to 200 characters.
- **Summary** – Displays a description of the translation in this format: `Traffic destined to [Original CIDR] is translated to [Translated CIDR] in a 1-1 NAT translation.`

d) Click the **checkmark** on the right side of the row to save the mapping.

Important

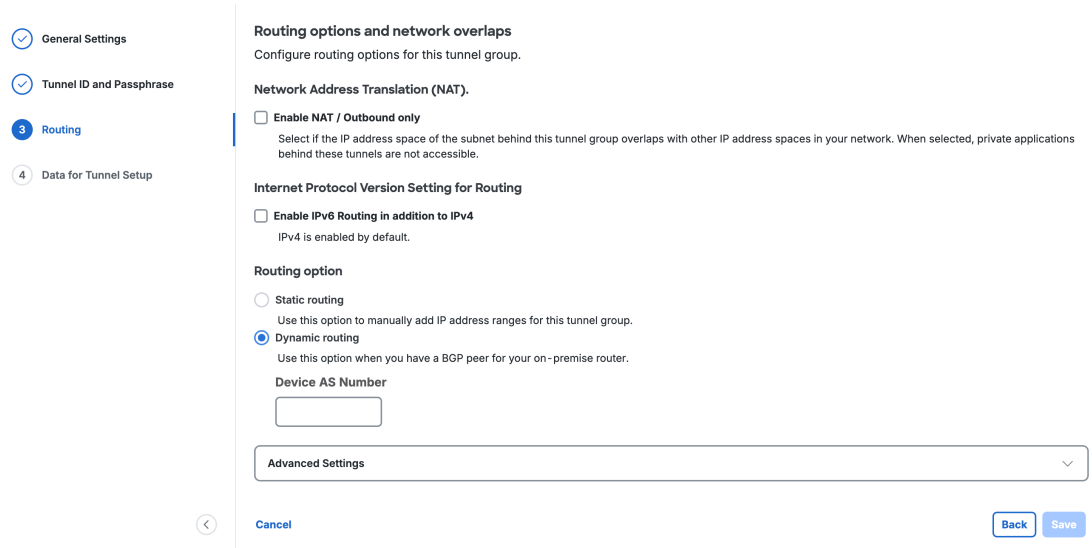
- NAT mappings in the **Site → Secure Access** direction support overlapping mapped IP addresses between NTGs.
- NAT mappings in the **Secure Access → Site** direction do not support overlapping mapped IP addresses between NTGs. Each NTG must use unique mapped IP address ranges to avoid routing errors.

> **Note**
>
> When configuring private resources and access rules for NAT-mapped destinations, use the **Translated CIDR** for **Secure Access → Site** mappings and the **Original CIDR** for **Site → Secure Access** mappings.

> **Note**
>
> Enabling NAT disables the static and dynamic routing options for the NTG.

9. **Internet Protocol Version Setting for Routing**: Choose whether to **Enable IPv6 Routing in addition to IPv4**.
10. Choose a **Routing option** for this network tunnel group.
    a. Choose **Static routing** to manually add IPv4 and IPv6 address ranges for this tunnel group. You should add all public and private address ranges used internally by your organization.
    b. Choose **Dynamic routing** when you have a BGP peer for your on-premise router.

> **Note**
>
> You'll need the router's autonomous system (AS) number to use dynamic routing.



    c. Click **Next**.

11. Expand **Advanced Settings** for additional dynamic routing options.
    - **Multihop BGP**: Enables BGP peers to establish a connection when not directly connected.
      - Enter the **IP Ranges** from where BGP peering sessions will originate, then click **Add**
      - (Optional) Enter the **Hop count** to limit the number of hops over which the BGP multihop session is established. The hop count equates to the time to live (TTL) parameter. The range is 1 to 254 hops, with a default value of 1. The hop count is disabled until IP addresses are entered.

- **Multi-region backhaul** supports a customer backhaul network that spans multiple Secure Access regions. Enable this setting for each network tunnel group connected to your backhaul.

> **Attention**
>
> **The Multi-Region Backhaul feature is currently controlled by a feature flag and is not available or enabled by default.** To request access to this feature, please contact Cisco Secure Access Support.

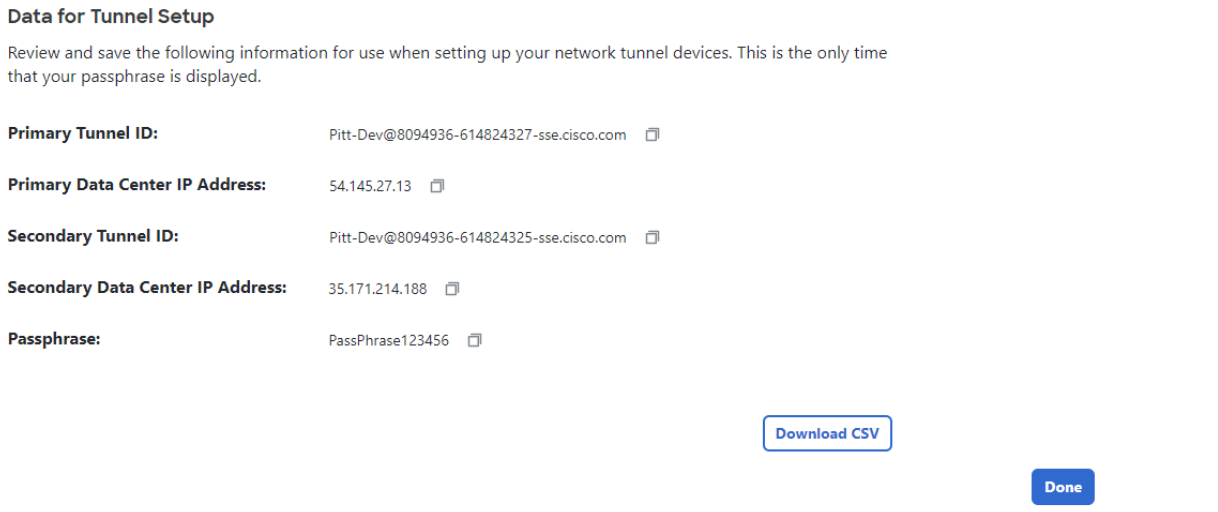
> **Note**
>
> Overlapping prefixes advertised to Secure Access from multiple customer Network Tunnel Groups are supported by Secure Access BGP only when MRB is enabled on those Network Tunnel Groups. When MRB is not enabled, overlapping prefixes should not be advertised across multiple Network Tunnel Groups.

- **Block default route advertisement** – Blocks the advertisement of the default route in dynamic routing mode. Advertising default routes via BGP is not supported and can lead to traffic disruptions.

Step 4 - Data for Tunnel Setup

12. Review the network tunnel information for completeness. Click the **Download CSV** button to save your tunnel setup information. You can use the information to configure and deploy a tunnel in a network device.

> **Note**
>
> This is the only time that your passphrase is displayed.



Once the tunnel group is deployed, the initial state of the tunnel group changes from **Unestablished** to **Inactive**.

What to do next

After you configure the tunnel group, perform the following tasks to ensure a robust environment:

- **Configure primary and secondary tunnels:** Configure your network devices to connect to both primary and secondary tunnels to ensure redundancy. For more information, refer to Network Tunnel Configuration and Establish a Tunnel.
- **Enable user connectivity:** Configure user computers to connect securely through the tunnel and send traffic to Secure Access.
- **Verify tunnel status:** Once Secure Access receives traffic, the tunnel status changes to Active. Navigate to the **Overview** page to confirm the status of your configured tunnel.
- **Monitor traffic:** Use the Overview page and Activity Search Report to monitor tunnel traffic events.

Delete a Network Tunnel Group

Describes deleting a network tunnel group. Once a network tunnel group is added to Cisco Secure Access, you can remove the deployed tunnel group from your organization.

Once a network tunnel group is added to Cisco Secure Access, you can remove the deployed tunnel group from your organization.

Procedure for Delete a Network Tunnel Group

Provides instructions for procedure for delete a network tunnel group. It also identifies related requirements, procedures, and operational considerations.

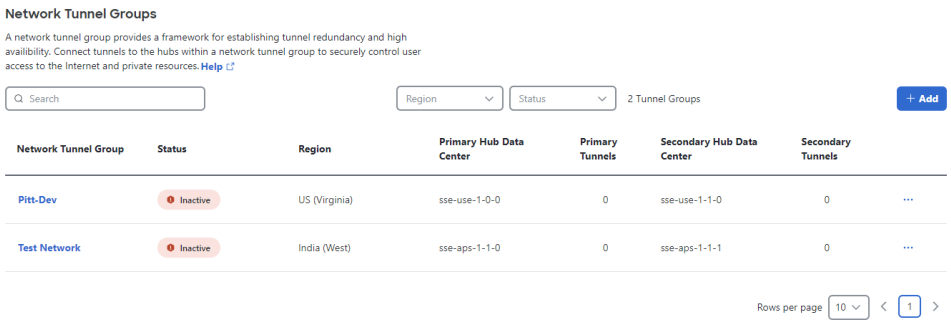
Delete a network tunnel group from Secure Access.

Before you begin

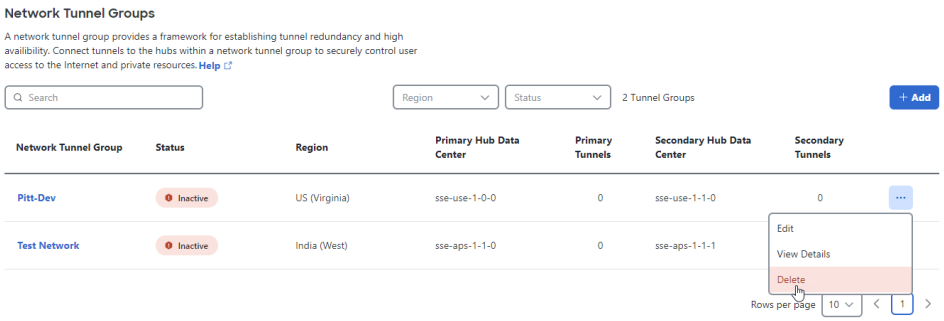
Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.



2. From the list of network tunnel groups, expand a tunnel.
3. Click the ellipsis (**...**), and then choose **Delete**.



4. After the delete is completed, verify that the tunnel group is not present in the list of network tunnel groups.

Edit a Network Tunnel Group

Describes editing a network tunnel group. Once a network tunnel group is added to Cisco Secure Access, you can edit the configuration attributes of the deployed tunnel group.

Once a network tunnel group is added to Cisco Secure Access, you can edit the configuration attributes of the deployed tunnel group.

Procedure for Editing a Network Tunnel Group

Provides instructions for editing a network tunnel group. Edit the configuration attributes of a deployed network tunnel group in Secure Access.

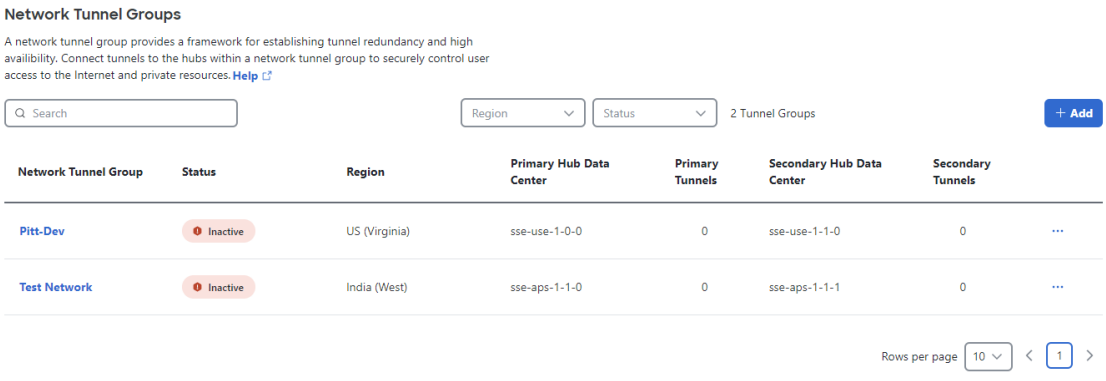
Edit the configuration attributes of a deployed network tunnel group in Secure Access.

Before you begin

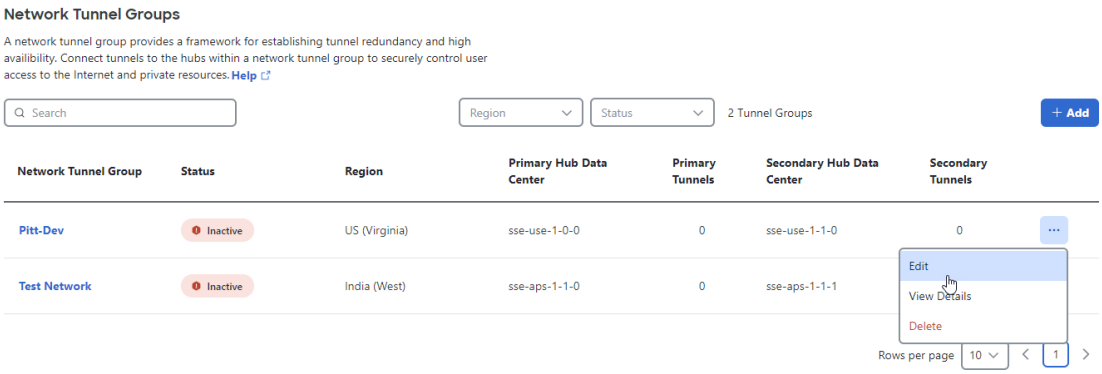
Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

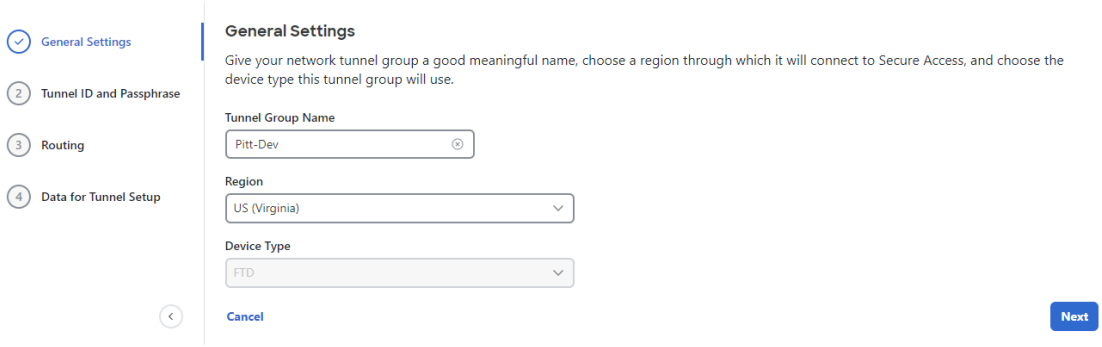
1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.



2. From the list of network tunnel groups, expand a tunnel group.
3. Click the ellipsis (**...**), and then choose **Edit**.



4. Navigate through the settings to edit **Tunnel Group Name**, **Region**, **Device Type**, **Tunnel ID**, **Passphrase**, or **Routing** configuration attributes.



5. Click **Save**.

View Network Tunnel Group Details

Describes viewing network tunnel group details. Once a network tunnel group is added to Cisco Secure Access, you can view the configuration attributes of a deployed tunnel group.

Once a network tunnel group is added to Cisco Secure Access, you can view the configuration attributes of a deployed tunnel group. You can also edit the attributes of a network tunnel group and view information about the network tunnels associated with the selected tunnel group.

Secure Access also lists the status of your organization's network tunnels and information about the attributes of the deployed tunnel groups in **Overview** > **Connectivity**.

Procedure for Viewing Network Tunnel Group Details

Provides instructions for procedure for viewing network tunnel group details. View the details of a deployed network tunnel group in Secure Access.

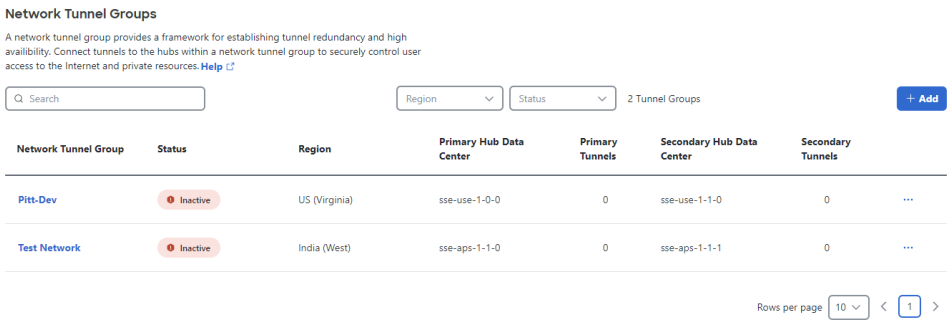
View the details of a deployed network tunnel group in Secure Access.

Before you begin

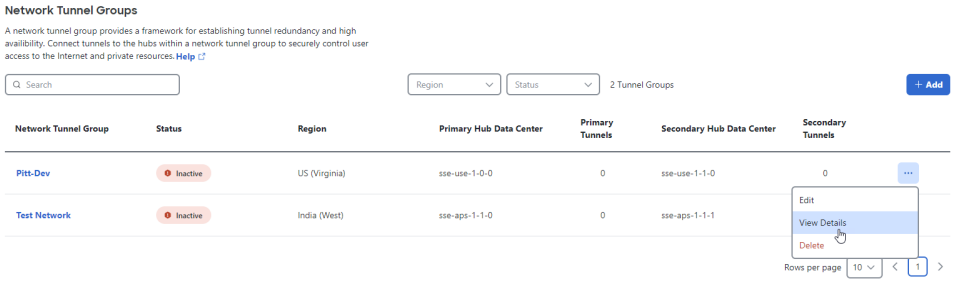
A minimum role of Read Only in Secure Access. For more information, For more information, see Manage Accounts.

Procedure

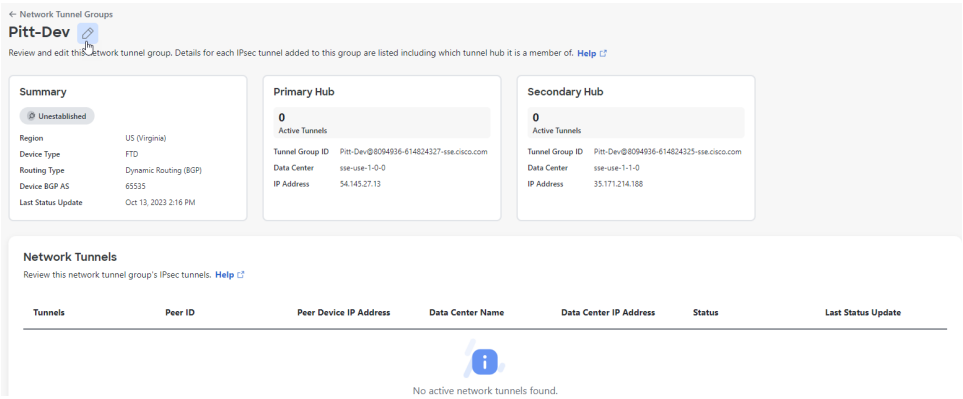
1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.



2. From the list of network tunnel groups, expand a tunnel group.
3. Click the ellipsis (**...**), and then choose **View Details**.



4. Review the **Summary** details for the selected network tunnel group. You can also view the **Primary Hub** and **Secondary Hub** details.



5. (Optional) Click the pencil icon next to the network tunnel group name to edit the tunnel group attributes. See Edit a Network Tunnel Group

---

Supported IPsec Parameters

Describes supported ipsec parameters. Cisco Secure Access uses the IPsec protocol for tunneling traffic. IPsec has multiple components and one of the core components is Internet Key Exchange (IKE). IKE manages negotiation with peers, authentication, and certificate exchanges.

Cisco Secure Access uses the IPsec protocol for tunneling traffic. IPsec has multiple components and one of the core components is Internet Key Exchange (IKE). IKE manages negotiation with peers, authentication, and certificate exchanges. IKE maintains the session by using Dead Peer Detection (DPD) as per RFC 5996. Secure Access supports IKEv2, which is faster and more secure than IKEv1.

Secure Access supports the configuration of certain IPsec parameters to deploy a network tunnel. Even if a device can establish an IPsec tunnel to Secure Access, we do not guarantee that the tunnel is compatible. For example, if the tunnel

enables Perfect Forward Secrecy (PFS), you can establish a tunnel, but in the event of reconnection, the tunnel may fail to rekey and lose service. We recommend that you test the tunnel connectivity thoroughly before putting any tunnel into production.

Components	IKEv2 (Phase I) (no IKEv1 support)	ESP (Phase II)
Encryption	**AES-256-16 (GCM)**, AES-256-8 (GCM), AES-128-16 (GCM), AES-128-8 (GCM), AES-128(CBC), AES-256(CBC)	**AES-256-16(GCM)**, AES-128-16(GCM), AES-256(CBC), AES-128(CBC), NULL(GCM) - AES-256 GMAC, NULL(GCM) - AES-192 GMAC, NULL(GCM) - AES-128 GMAC NULL(CBC)
Hashing	**SHA256**, SHA1	**SHA256**, SHA1
DH Group	**20**, **19**, 15 14	**20**, **19**, 15, 14
Authentication	**Pre-Shared Key (PSK)**	N/A
Protocol	N/A	ESP in UDP (NAT-T) (Port - UDP 4500)
Total Child SAs Supported	N/A	1
Lifetime	Based on client settings (IKE default is 4 hours)	Based on client settings (Child SA default is one hour)
Perfect Forward Secrecy (PFS)	N/A	Allowed (Ciphers configured with both PFS and non-PFS.) **Note:** If the remote end prefers to negotiate PFS, it has to set the child rekey timer lower than the head end and/or allow both PFS and non-PFS. Reason: CNHE prefers non-PFS. We configured both, but if the other side wants PFS, we can negotiate.
DPD Timeouts	30 seconds (back_off = 2, retransmit timeout = 2, retries = 5)	N/A
IP fragmentation	Not supported	Not supported
IKE Fragmentation (RFC 7383)	Enabled	N/A
Extended Sequence Number (ESN)	N/A	Allowed and preferred

Recommendations are in **Bold**.

Note

Secure Access routing platforms are optimized for Galois/Counter Mode (GCM) encryption. Thus, we recommend that you use GCM encryption for maximum throughput. Using cipher block chaining (CBC) may result in lower throughput. Performance is subject to hardware and configurations.

10 Network Tunnel Configuration

Topics:

- Network Tunnel Configuration

Describes the purpose and procedures for network tunnel configuration and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Network Tunnel Configuration

Describes network tunnel configuration. You can establish an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel from a network device deployed in your environment to Cisco Secure Access. IPsec tunnels created for Secure Access accept traffic on all ports and protocols with a throughput of 1GB.

You can establish an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel from a network device deployed in your environment to Cisco Secure Access. IPsec tunnels created for Secure Access accept traffic on all ports and protocols with a throughput of 1GB.

Establish a Tunnel

Describes establishing a tunnel. You can establish an IPsec IKEv2 tunnel on a supported network device to the Secure Access head end of the tunnel. Use the tunnel passphrase credentials that you generated in Secure Access to configure the IPsec tunnel .

You can establish an IPsec IKEv2 tunnel on a supported network device to the Secure Access head end of the tunnel. Use the tunnel passphrase credentials that you generated in Secure Access to configure the IPsec tunnel .

The network device – tunnel configuration guides describe the steps to configure tunnels from a network device to Secure Access. The sample commands in the guides use the `<secure_access_dc_ip>` variable to represent the public IP address of the Secure Access data center.

Maximum Transmission Unit (MTU) Size

Describes maximum transmission unit (mtu) size. IPsec tunnels for Secure Internet Access must have an MTU no larger than 1280 bytes, with an MSS no larger than 1240 bytes. Fragmented packets in underlay or overlay are dropped.

IPsec tunnels for Secure Internet Access must have an MTU no larger than 1280 bytes, with an MSS no larger than 1240 bytes. Fragmented packets in underlay or overlay are dropped. Slightly larger MTU and MSS may work depending on your specific IPsec configuration.

Tunnel Size

Describes tunnel size. Secure Access supports the following tunnel size ranges: The maximum concurrent load for a tunnel is 1 Gbps throughput in either direction.

Secure Access supports the following tunnel size ranges:

- The maximum concurrent load for a tunnel is 1 Gbps throughput in either direction.
- There are no restrictions on throughput measured in packets per second.
- There are no restrictions on the number of users per tunnel.

If you exceed the throughput limit your tunnel may have degraded performance including increased latency and packet loss.

Client Reachable Prefixes

Describes client reachable prefixes. Secure Access expects a private RFC 1918 address as the source IP for outbound packets. If you use non-RFC 1918 addresses, you can add them under Client Reachable Prefixes when configuring your tunnel.

Secure Access expects a private RFC 1918 address as the source IP for outbound packets. If you use non-RFC 1918 addresses, you can add them under Client Reachable Prefixes when configuring your tunnel. This overrides the default behavior, which allows all traffic destined for RFC 1918 addresses to return through the tunnel. For information about address allocation and private networks, see RFC 1918.

Secure Access supports the following options for client-reachable prefixes:

- Static IP addresses, which must be globally unique in the customer org; i.e. no other network tunnel group can be configured with the same address.
- BGP-based dynamic routing. BGP dynamic routing enables advertisement of self-service (private) network prefixes to physical network devices that support BGP such as routers, and removes the dependency on static routes.

Note: After updating client reachable prefixes for an established tunnel, wait at least five minutes, disconnect and shut down the tunnel for at least 10 seconds, and then reconnect the tunnel.

Throughput and Multiple Tunnels

Describes throughput and multiple tunnels. Each tunnel is limited to approximately 1 Gbps. To achieve higher throughput, you can establish multiple tunnels. If you set up multiple tunnels, we recommend that you divide the traffic between the tunnels by assigning traffic through policy-based routing.

Each tunnel is limited to approximately 1 Gbps. To achieve higher throughput, you can establish multiple tunnels. If you set up multiple tunnels, we recommend that you divide the traffic between the tunnels by assigning traffic through policy-based routing.

If you set up multiple tunnels, we recommend that you divide the traffic between the tunnels either through load balancing with ECMP (Equal-cost multi-path routing) or assigning traffic through policy-based routing. The number of supported ECMP tunnels is 10. For information about ECMP, see RFC 2991.

> **Note**
>
> To protect against a loss of connectivity, you should set up redundant tunnel headends for a network tunnel group and monitor your IPSec tunnels. You'll need to update their local routing to send traffic to the secondary headend when the primary is unreachable.

Configure Tunnels with Cisco ISR

Describes configuring tunnels with cisco isr. Follow the steps in this guide to connect a Cisco ISR-G2, ISR4K, or CSR router through an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel to Cisco Secure Access.

Follow the steps in this guide to connect a Cisco ISR-G2, ISR4K, or CSR router through an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel to Cisco Secure Access.

Prerequisites

The following prerequisites must be met for the tunnel to work successfully.

Licensing and Hardware

Describes licensing and hardware. A valid Cisco Secure Access account. A Cisco Secure Access organization ID. For more information, see Find Your Organization ID.

- A valid Cisco Secure Access account.
- A Cisco Secure Access organization ID. For more information, see Find Your Organization ID.
- A router (ISR-G2, ISR4K, or CSR) with a security K9 license to establish an IPsec tunnel.

> **Note**
>
> An HSEC license is required to get high-throughput internet bandwidth for SLVPN tunnel setup.

Network Access

Describes network access. You must select a Secure Access data center IP address when creating the IPsec tunnel.

- You must select a Secure Access data center IP address when creating the IPsec tunnel. In the sample commands, `<sse_dc_ip>` refers to this IP address. We recommend choosing the IP address based on the data center located closest to your device.
- Open UDP ports `500` and `4500` before connecting to the tunnel.

Cisco router (ISR-G2, ISR4K, or CSR) devices do not require public static IPv4 addresses configured on the interface that connects to the public internet and Secure Access. You can deploy these devices behind a NAT device. This is because we can specify a text as its IKE ID. This ID in combination with the PSK is used to successfully authenticate the Cisco router (ISR-G2, ISR4K, or CSR) devices with Secure Access.

Text as an IKE ID also allows multiple tunnels to be established from the same Cisco router device with a single IP address. This provides an opportunity to increase bandwidth by increasing the number of tunnels.

Configure Tunnels in Secure Access

Provides instructions for configuring tunnels in secure access. Follow the steps in Add Network Tunnel Group. The new tunnel appears in the Secure Access dashboard with a status of UnEstablished. The tunnel status is updated once it is fully configured and connected with the Cisco ISR.

Procedure

Follow the steps in Add Network Tunnel Group.

What to do next

The new tunnel appears in the Secure Access dashboard with a status of *UnEstablished*. The tunnel status is updated once it is fully configured and connected with the Cisco ISR.

Configure ISR (G2, 4K) or CSR

Provides instructions for configuring isr (g2, 4k) or csr. Follow these steps to connect the Cisco router to Secure Access.

Follow these steps to connect the Cisco router to Secure Access.

Procedure

1. Configure the IKEv2 proposal.

   ISR routers support a default proposal and policy for IKEv2, with a predefined encryption, integrity, and DH group. These values change across different software versions. You can either use the default proposal or you can create your own proposal. Your proposal needs to be attached to the policy with matching parameters. Create an IKEv2 keyring profile and configure the peer address and pre-shared key, associate the keyring profile to the IKEv2 profile, set the local identity as email and configure the IKE ID (email) which you get from the Tunnel Configuration dashboard.

For example, the default IKE proposal of an ISR running 16.11.01a:

```
ISR-4221#sh ver
Cisco IOS XE Software, Version 16.11.01a

ISR-4221#show crypto ikev2 proposal sse-prop
 IKEv2 proposal: sse-prop
     Encryption : AES-GCM-256
     Integrity  : none
     PRF        : SHA256
     DH Group   : DH_GROUP_256_ECP/Group 19 DH_GROUP_384_ECP/Group 20
```

2. Define the IKEv2 Keyring and IKEv2 profile.

   Create your IKEv2 keyring and IKEv2 profile with the [sse_dc_ip] of the Secure Access data center closest to your location. Then associate the IKEv2 keyring to the IKEv2 profile.

   Replace [Portal_Tunnel_ID] and [Portal_Tunnel_Passphrase] with the Tunnel ID and Passphrase you configured in section Add Network Tunnel Group.

```
crypto ikev2 keyring sse-kr
  peer sse
  address \[sse_dc_ip\]
  pre-shared-key \[sse-tunnel-psk\]
!
crypto ikev2 profile sse-profile
  match identity remote address 16.64.116.188
  255.255.0.0
  identity local email \[sse-email\]
  authentication remote pre-share
  authentication local pre-share
  keyring local sse-kr
  dpd 10 3 periodic
!
```

3. Define the IPSec transform-set, profile, and policy.

   Create the transform-set and IPsec profile. Then associate the transform-set and IKEv2 Profile with the IPSec profile. Refer to Supported IPsec Parameters for the recommended algorithms.

```
crypto ipsec transform-set sse-ts esp-gcm 256
mode tunnel

crypto ipsec profile sse
 set transform-set sse-ts
 set ikev2-profile sse-profile

crypto ikev2 policy sse
 match address local \[Router_WAN_IP\]
 proposal sse-proposal
```

4. Create the tunnel interface.

   Define the static tunnel interface with the peer IP as the Secure Access VPN headend IP and associate the IPsec profile under the tunnel. Make sure the tunnel interface does not contain NAT related commands; traffic sent to Secure Access should not have NAT applied.

```
interface Tunnel1
 ip unnumbered \[interface-name\]
 ip tcp adjust-mss 1280
 tunnel source \[interface-name\]
```

```
 tunnel mode ipsec ipv4
 tunnel destination \[sse_dc_ip\]
 tunnel protection ipsec profile sse
```

5. Configure routing rules.

   Define the traffic which needs to be tunneled to the CDFW. Based on the requirements, these ACL rules can be modified.

   The route-map needs to be associated with the LAN interface of the router where the device receives the traffic.

   In the following examples, `192.168.20.0/24` is the LAN subnet, and `GigabitEthernet` is the LAN interface.

```
ip access-list extended traffic-to-sse
  permit ip \[lan-ip\] any
!
route-map sse-route-map permit 10
  match ip address traffic-to-sse
  set interface Tunnel1
!
interface GigabitEthernet \[lan-interface-name\]
 ip policy route-map sse-route-map
```

Test Your Configuration

Describes testing your configuration. Use the following command to verify the tunnel status on your ISR. show crypto session detail and the output must show the tunnel status as UP-ACTIVE.

Check Tunnel Status

Use the following command to verify the tunnel status on your ISR.

`show crypto session detail` and the output must show the tunnel status as **UP-ACTIVE**.

Substitute the IP address of the Secure Access data center nearest your location for `\[sse_dc_ip\]`.

```
ISR#show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update

Interface: Tunnel1
Profile: sse
Uptime: 14:53:47
Session status: UP-ACTIVE
Peer: \[sse_dc_ip\] port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: \[sse_dc_ip\]
      Desc: (none)
  Session ID: 1
  IKEv2 SA: local 10.10.10.201/4500 remote \[sse_dc_ip\]/4500 Active
          Capabilities:DFNXU connid:4 lifetime:09:06:13
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4608000/2499
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/2499
```

Manually Trigger the Tunnel

Describes manually trigger the tunnel. Should the tunnel not come up immediately, or should it need to be manually triggered for any reason, select the tunnel interface, and issue the shutdown and no shutdown commands.

Should the tunnel not come up immediately, or should it need to be manually triggered for any reason, select the tunnel interface, and issue the `shutdown` and `no shutdown` commands.

```
ISR(config)#int T1
ISR(config-if)#shutdown
ISR(config-if)#no shutdown
```

Verify Tunnel Status

Describes verifying tunnel status.

Verify the tunnel status with `show crypto session remote <Headend IP> detail`. See the example output.

```
ISR#show crypto session remote 146.112.66.2 detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Tunnel1
Profile: sse
Uptime: 00:39:11
Session status: UP-ACTIVE
Peer: 192.0.2.0 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 192.0.2.0
      Desc: (none)
  Session ID: 1
  IKEv2 SA: local 192.0.2.0/4500 remote 146.112.66.2/4500 Active
          Capabilities:DN connid:3 lifetime:23:20:49
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4607996/1248
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4607997/1248
```

Configure Tunnels with Cisco Secure Firewall

Describes configuring tunnels with cisco secure firewall. Cisco Secure Firewall is a family of threat-focused next-generation firewalls. It can be managed centrally through Cisco Secure Firewall Management Center or through the on-box manager Firepower Device Manager (FDM).

Cisco Secure Firewall is a family of threat-focused next-generation firewalls. It can be managed centrally through Cisco Secure Firewall Management Center or through the on-box manager Firepower Device Manager (FDM). This guide covers the steps to configure site to site VPN between FTD devices and Secure Access through the Cisco Secure Firewall Management Center centralized manager.

Until version 6.7, FTD only supports policy-based VPN (Crypto-map). Version 6.7+ supports Virtual tunnel interface (VTI), version 7.1+ supports IKE identity and policy-based routing (PBR) through graphic interface.

Configure Firepower Policy-based VPN

Describes configuring firepower policy-based vpn. The Firepower configuration process consists of the following steps. Add Network Object Add Traffic Selector ACL

The Firepower configuration process consists of the following steps.

1. Add Network Object
2. Add Traffic Selector ACL
3. Configure Site-to-Site VPN
4. Configure NAT Policy
5. Configure Access Policy

To start the configuration, log in to your Cisco Secure Firewall Management Center web interface at its IP address or FQDN; for example, `https://FMC_IP_OR_FQDN`.

Configure Tunnels in Secure Access

Describes configuring tunnels in secure access. Firepower authenticates to the Secure Access IPsec headend by using a Pre-Shared Key (PSK) and IKEv2 IP identity.

Firepower authenticates to the Secure Access IPsec headend by using a Pre-Shared Key (PSK) and IKEv2 IP identity.

Follow the steps in Add Network Tunnel Group to add an FTD device to Secure Access.

The new tunnel appears in Secure Access with a status of *UnEstablished*. The tunnel status is updated once the first IKEv2 INIT message containing the tunnel identity is received in one of the Secure Access data centers.

> **Note**
>
> Secure Access does not support dynamic IP addresses for ASA and Firepower devices.

Add Network Object

Provides instructions for adding network object. Create a network object type “Group”. You will use this object in NAT configuration as well as in the Access Control List (ACL) in the IKEv2 traffic selector.

Create a network object type “Group”. You will use this object in NAT configuration as well as in the Access Control List (ACL) in the IKEv2 traffic selector. Using a group object simplifies the task of bypassing encryption and provides NAT for the bypassed traffic.

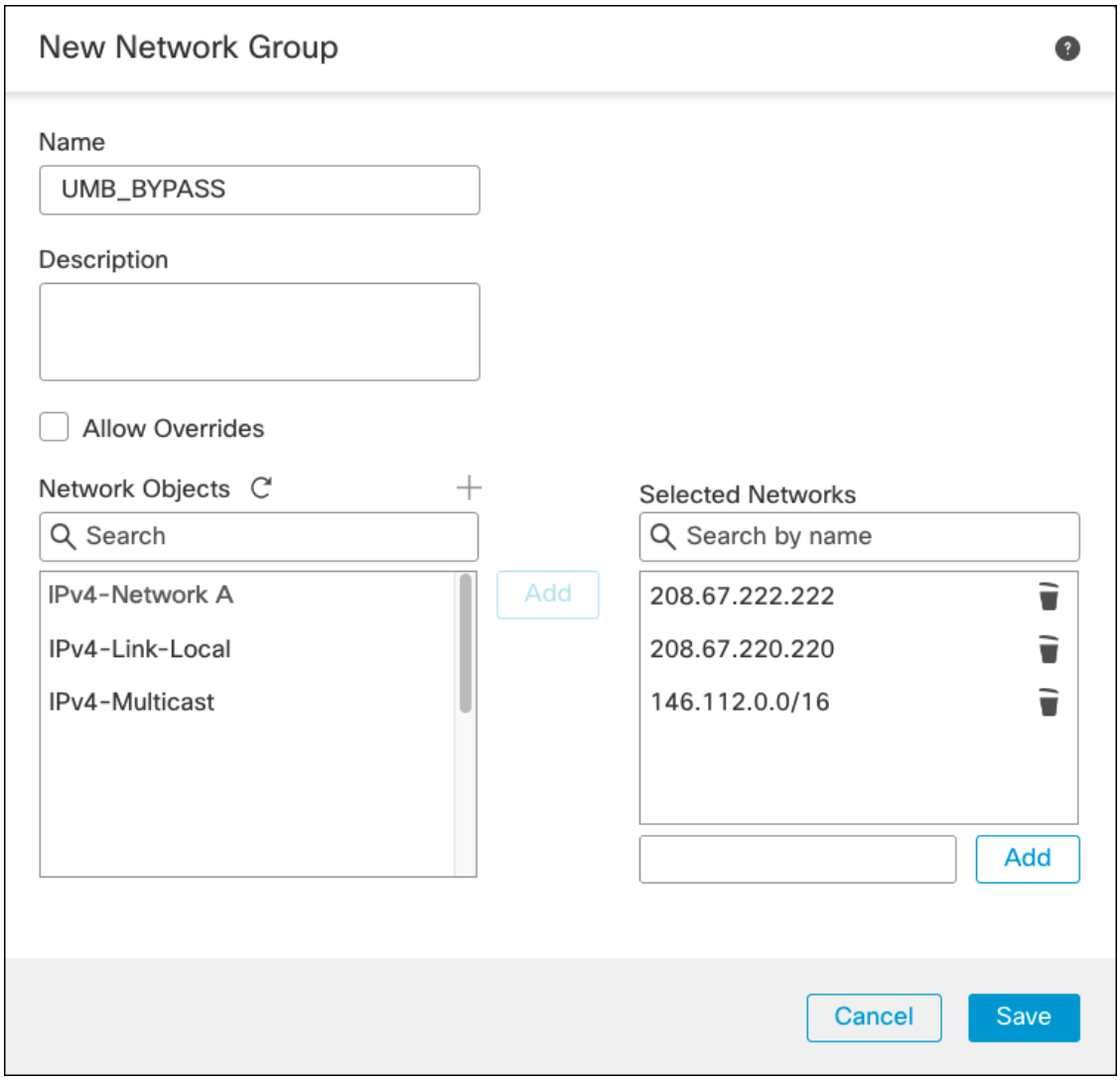
> **Note**
>
> Public IP traffic from SIG users will appear to come from the address ranges 146.112.0.0/16 and 155.190.0.0/16. Depending on your organization, you may be required to inform service providers that you access through the Secure Access service of these additional IP address ranges. For example, some service providers require prior knowledge of the IP address ranges used before allowing access to their service.

Procedure

1. Navigate to **Objects** > **Object Management** > **Network** > **Add Network** > **Add Group**.

2. Add the Secure Access resolvers IP address so the DNS queries are not sent through the tunnel.

   Currently, if the DNS queries are sent through the tunnel it will be NATed to 146.112.0.0/16 IP range and queries will not be linked to the user's dashboard. By bypassing the traffic to the Secure Access resolvers it is possible to add a public IP address to the dashboard (network deployment) and retrain DNS visibility and enforcement capabilities.



3. Optionally, add 146.112.0.0/16 as a network. Web traffic from endpoints with PAC file or Cisco Secure Client as well as proxy chaining traffic can then go outside the IPSec tunnel and achieve higher throughput.

Add Traffic Selector ACL

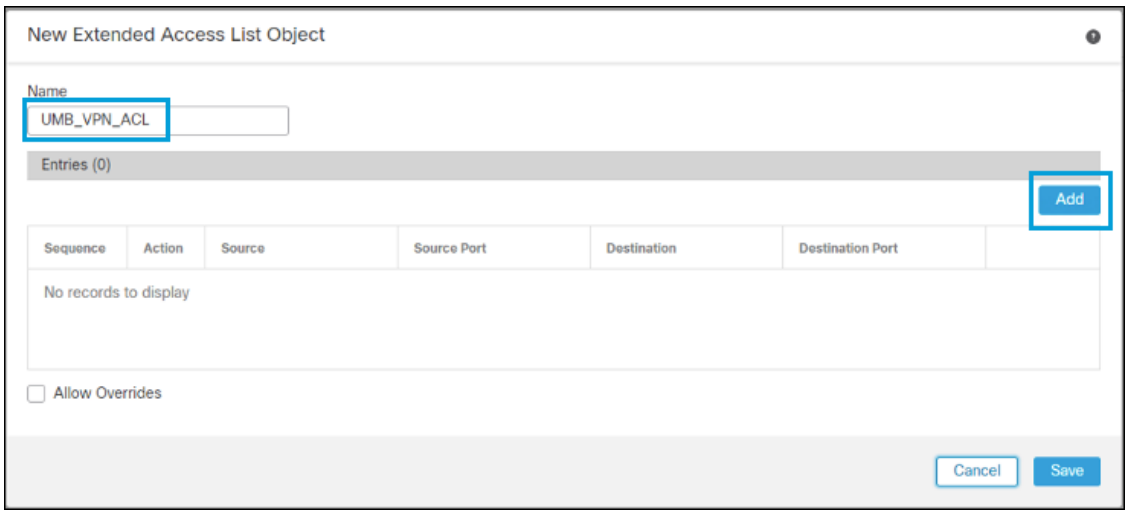
Provides instructions for adding traffic selector acl. This ACL is used in the IKEv2 security association negotiation as well as when Firepower makes decisions about when to encrypt traffic. It does not encrypt traffic denied in the ACL when the deny statement comes before the permit statement.

This ACL is used in the IKEv2 security association negotiation as well as when Firepower makes decisions about when to encrypt traffic. It does not encrypt traffic denied in the ACL when the `deny` statement comes before the `permit` statement.

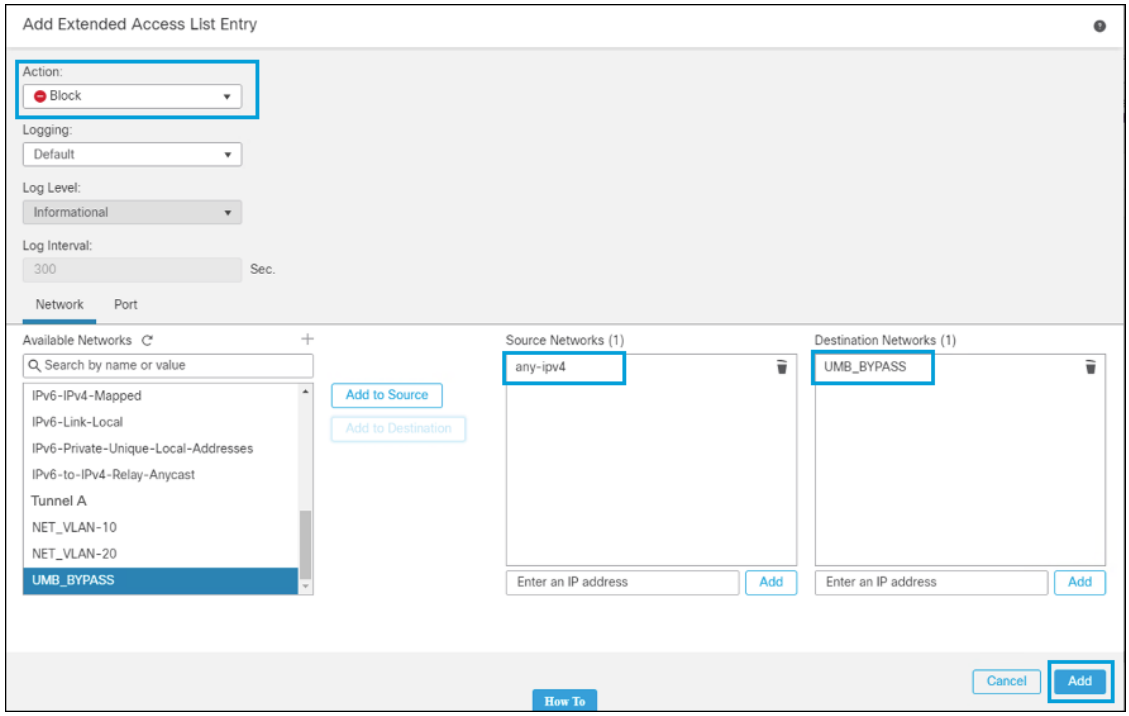
Procedure

1. Navigate to **Objects** > **Object Management** > **Access List** > **Extended** > **Add Extended Access List**.

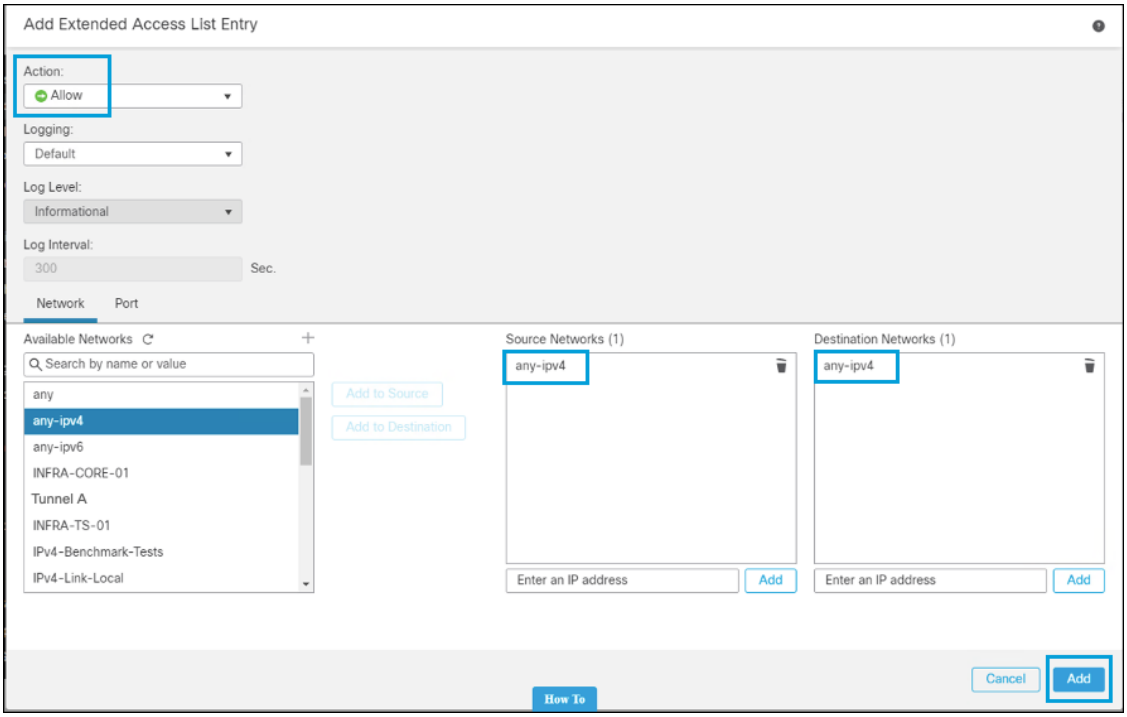
2. Enter a name for the ACL and then click **Add** to add the Access Control Entries (ACE).



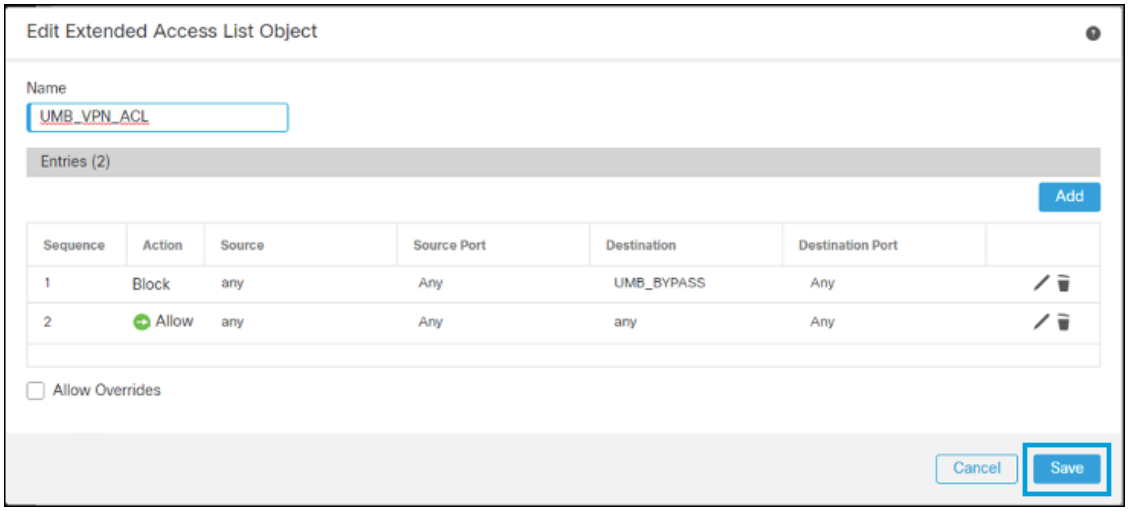
   a. The first entry denies traffic to the network object type group containing the Secure Access resolvers. Optionally, traffic to the `146.112.0.0/16` and `155.190.0.0/16` subnets can also be denied.



   b. The second entry allows traffic from any IPv4 address to any IPv4 address. This is also the entry IKEv2 uses to negotiate the IPSec Security Association (traffic selector).



3. After you have added the entries, click **Save**.

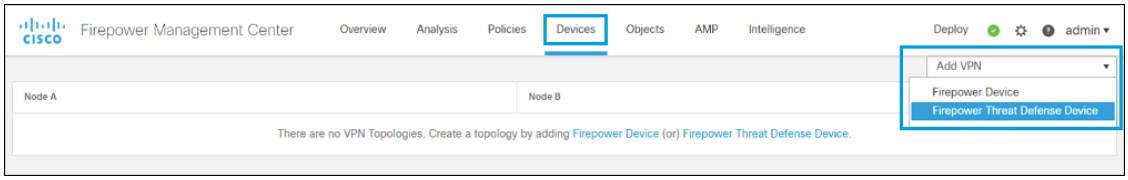


Configure Site-to-Site VPN

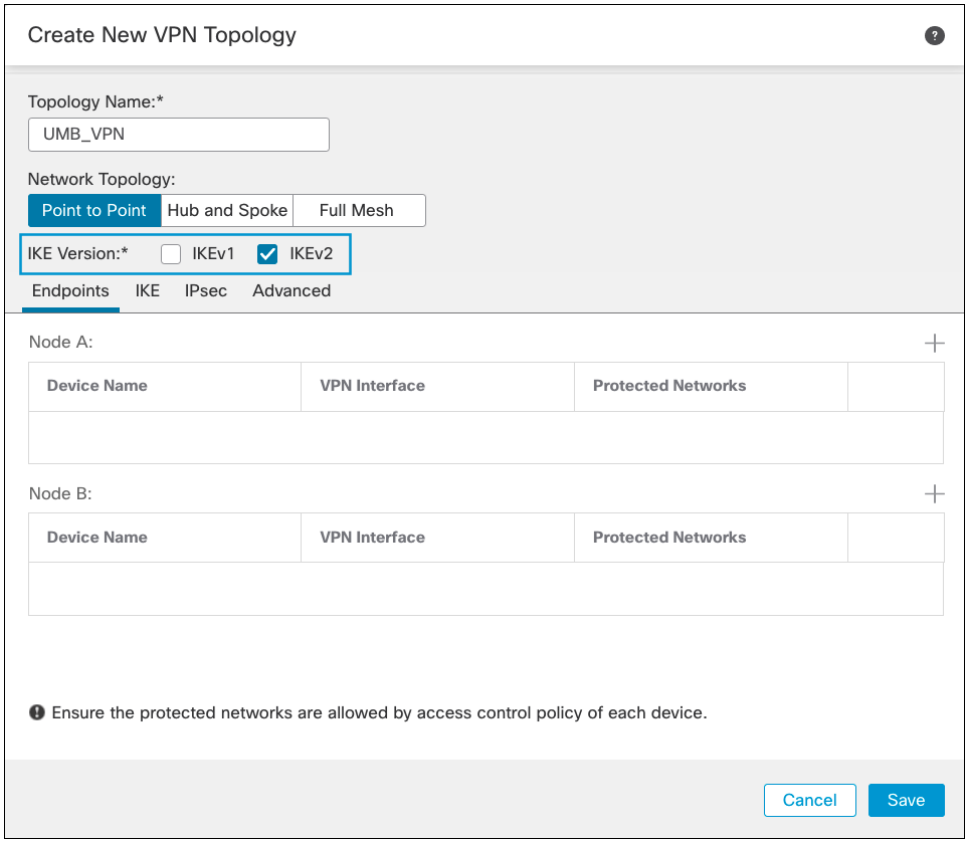
Describes configuring site-to-site vpn.

You can now configure the site-to-site VPN.

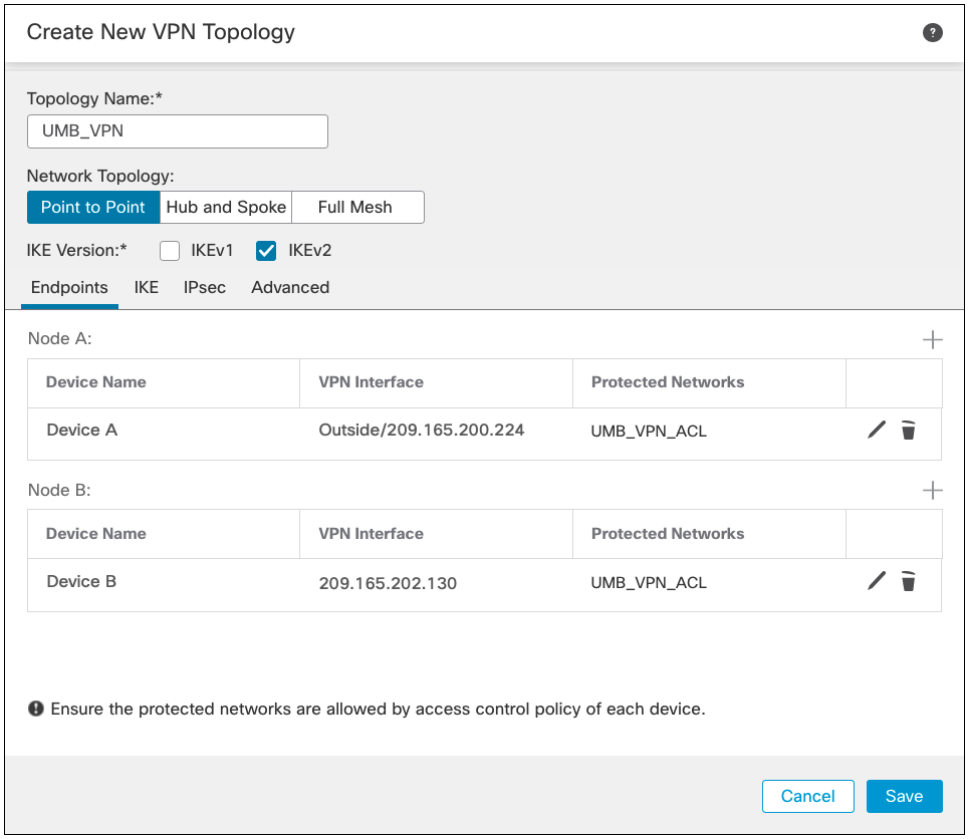
1. Navigate to **Devices** > **VPN** > **Site to Site** > **Add VPN** > **Firepower Threat Defense Device**.



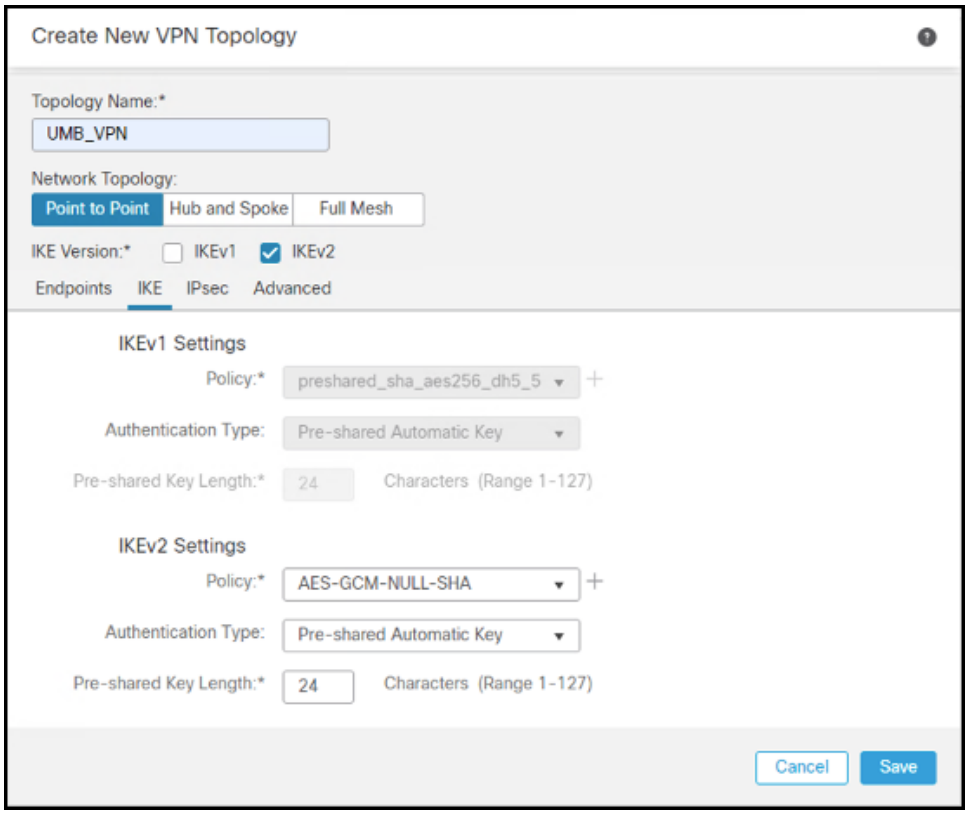
2. Enter a name for the topology. Check IKEv2 box (Secure Access supports IKEv2 only). For more information about supported protocols, see Supported IPSec Parameters.



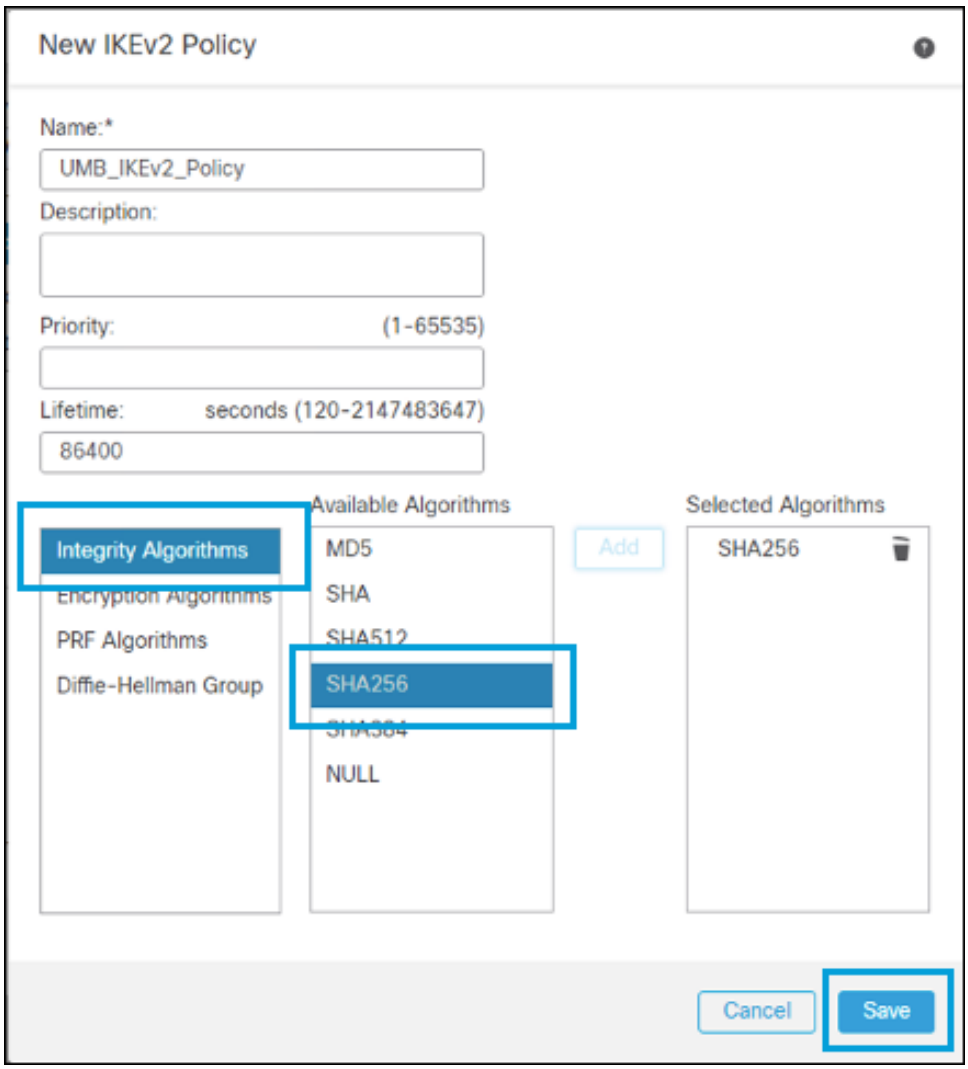
3. Add two peers: the local peer (FTD device) and the remote peer (Secure Access).
   a. Click **Add** for Node A and select the FTD device as the local peer and the interface sourcing the IPSec connection. The IP address is automatically populated.
   b. Under **Protected Networks**, select **Access List (Extended)**, and then select the ACL you created in the **Traffic Selector ACL**. Click **OK**.
   c. Click **Add** for Node B to add the remote peer.
   d. Select **Extranet** and enter a name. Select **Static**, and enter one of the Secure Access datacenter IP addresses. Then select the same ACL, then click **OK**.



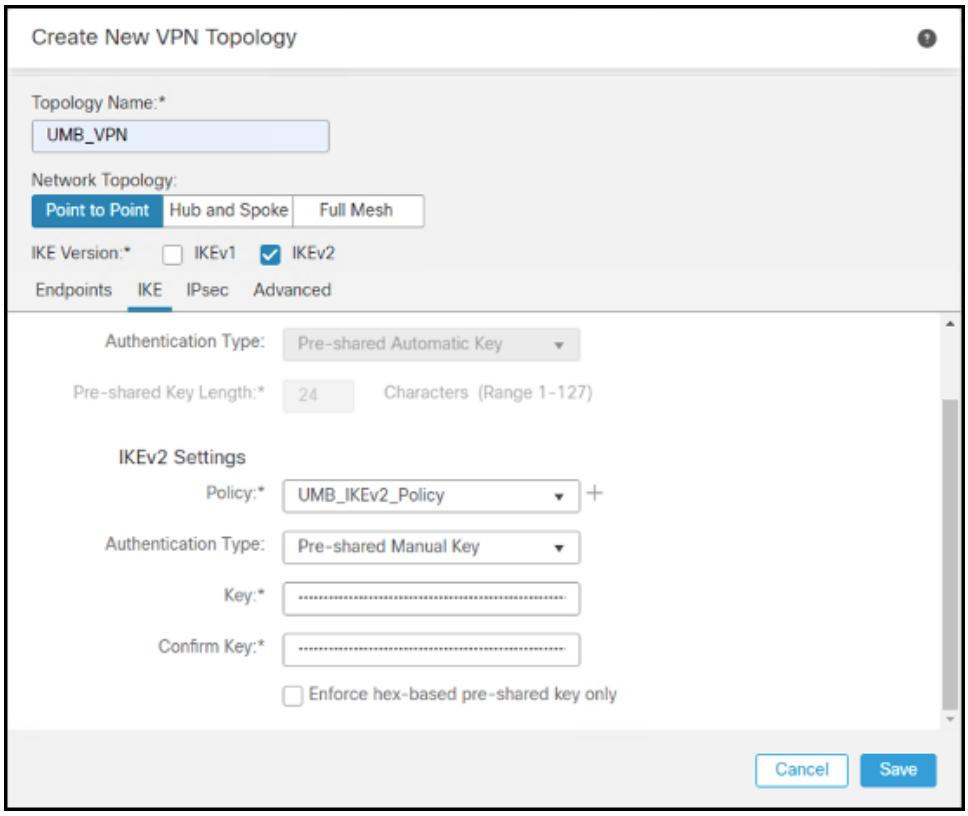
4. Click the **IKE** tab to add a new IKEv2 Policy containing the desired crypto algorithms. For more information about encryption supported by Secure Access, see Supported IPsec Parameters.



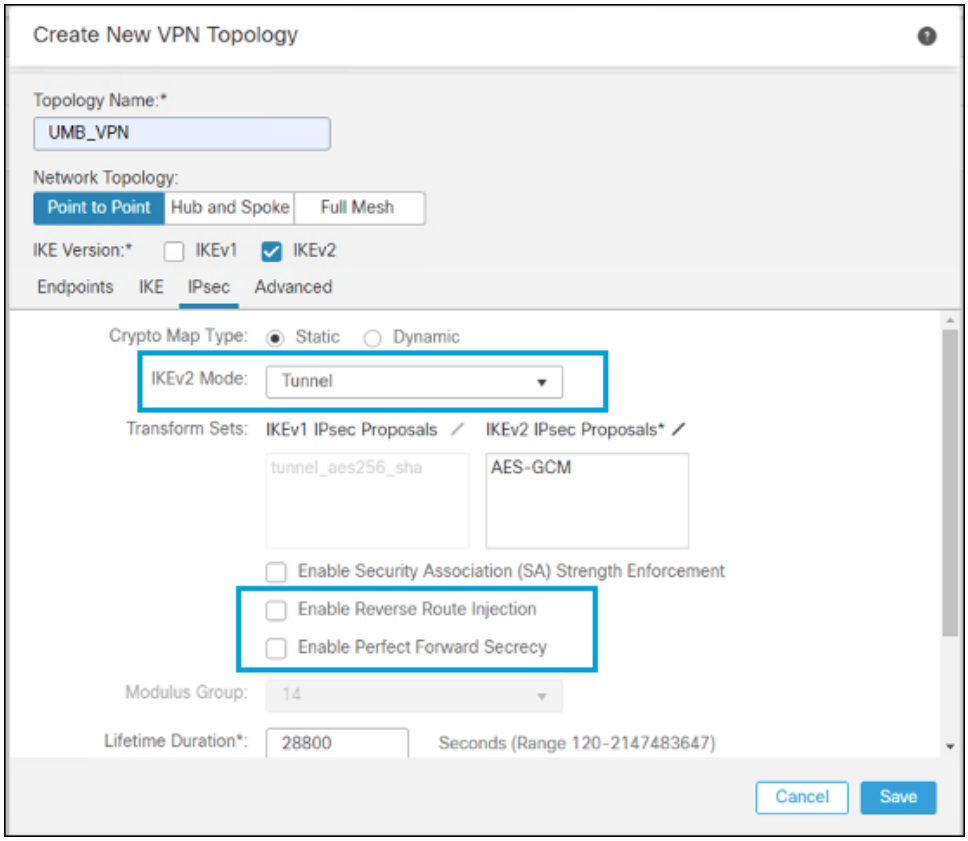
5. Enter a name for the IKEv2 policy, then select the parameters from the Supported IPsec Parameters.



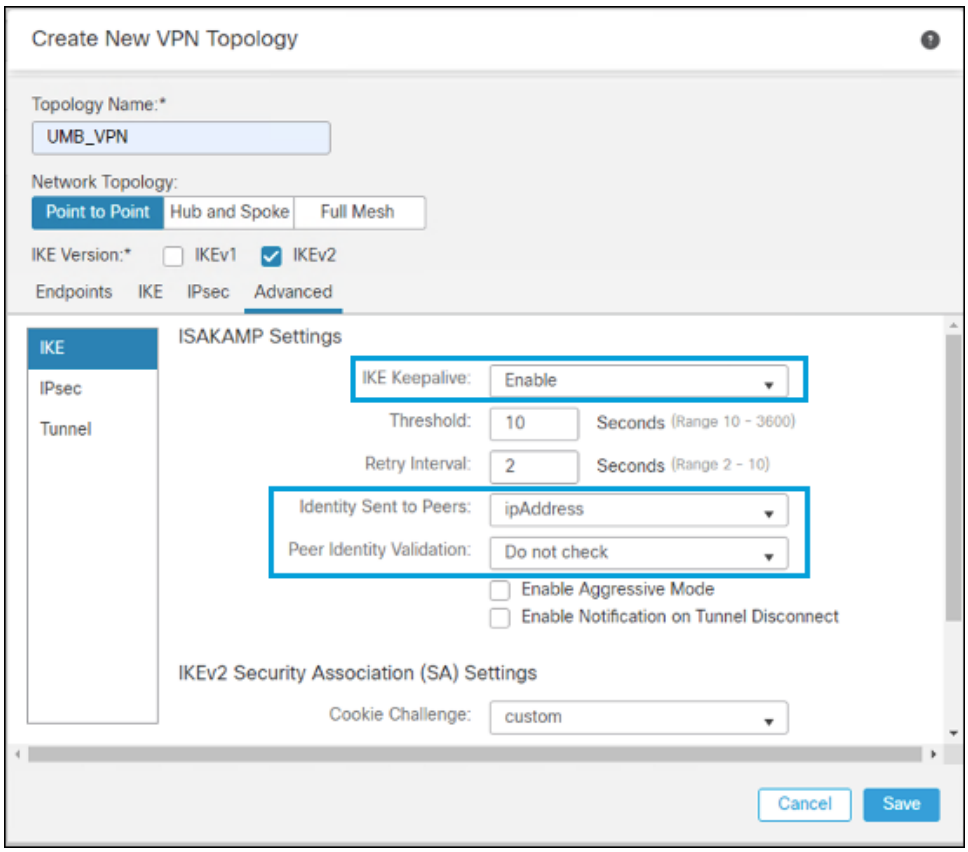
6. After saving the IKEv2 Policy, select it. Choose **Pre-shared Manual Key** from the **Authentication** drop-down menu and enter the key.



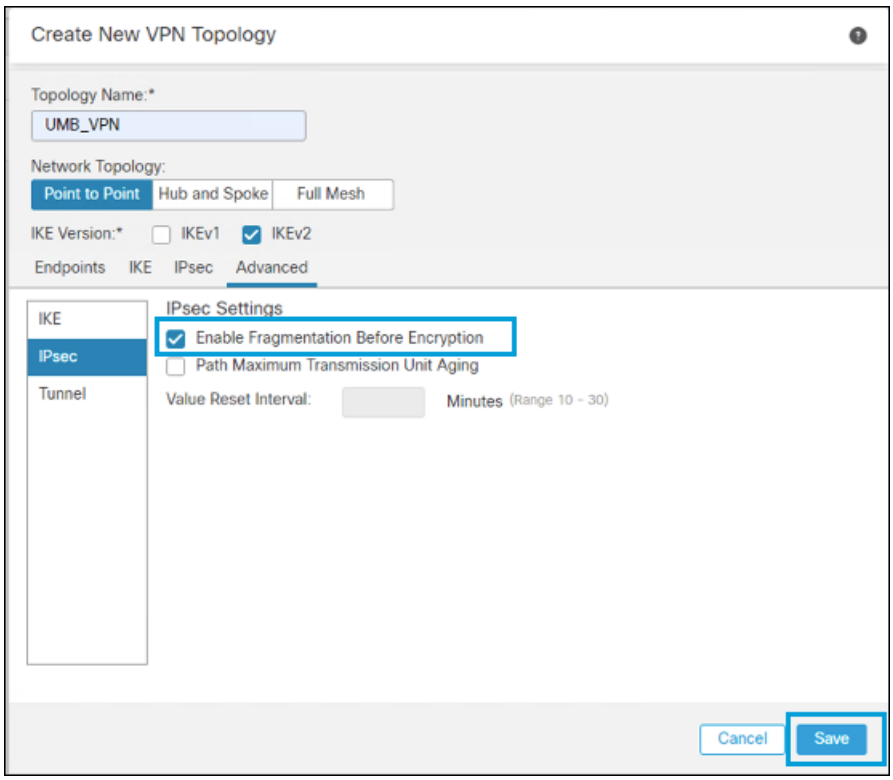
7. Under **IPSec Configuration**, add a new **IKEv2 IPsec Proposal** with your crypto algorithms or select an existing profile. Select **Tunnel** for **IKEv2 Mode** and uncheck **Enable Reverse Route Injection** and **Enable Perfect Forward Secrecy**.



8. In the **Advanced** tab under IKE, enable **IKE Keepalive**. Select **ipAddress** as the **Identity Sent to Peers**, and disable **Peer Identity Validation**.



9. Under **IPSec**, select **Enable Fragmentation Before Encryption**, then click **Save**.



Configure NAT Policy

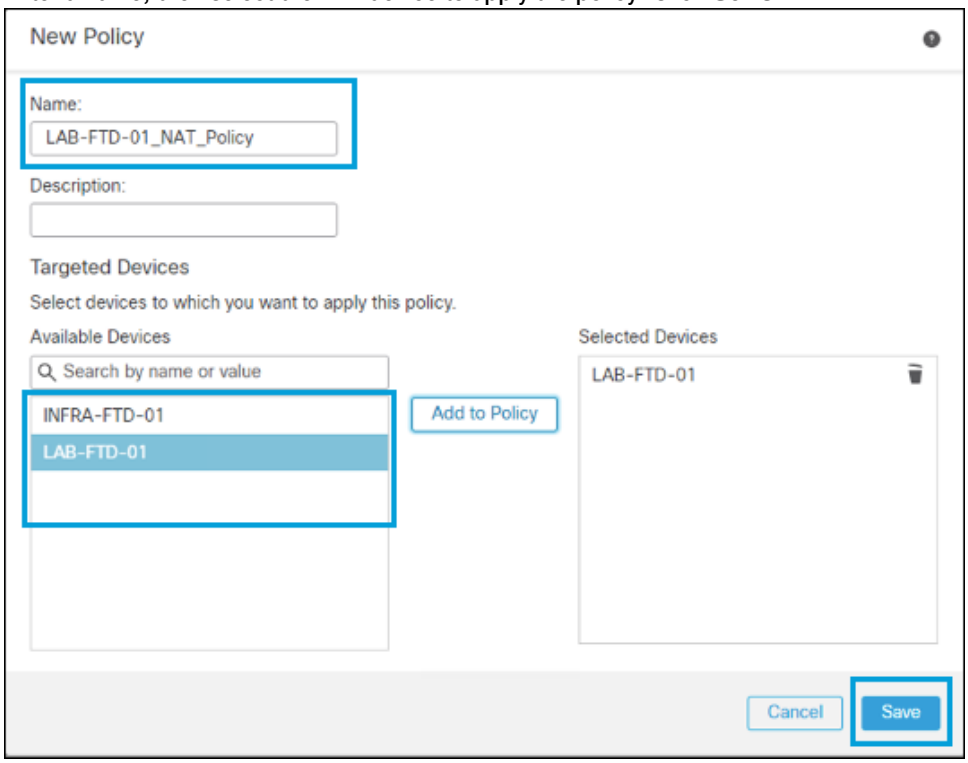
Describes configuring nat policy. If a NAT policy currently exists in the Firepower device, this policy must be changed to exempt traffic going through the tunnel from being NATed.

If a NAT policy currently exists in the Firepower device, this policy must be changed to exempt traffic going through the tunnel from being NATed. Secure Access requires the source of the connection to be the client's original private IP address – the public IP is not currently supported.

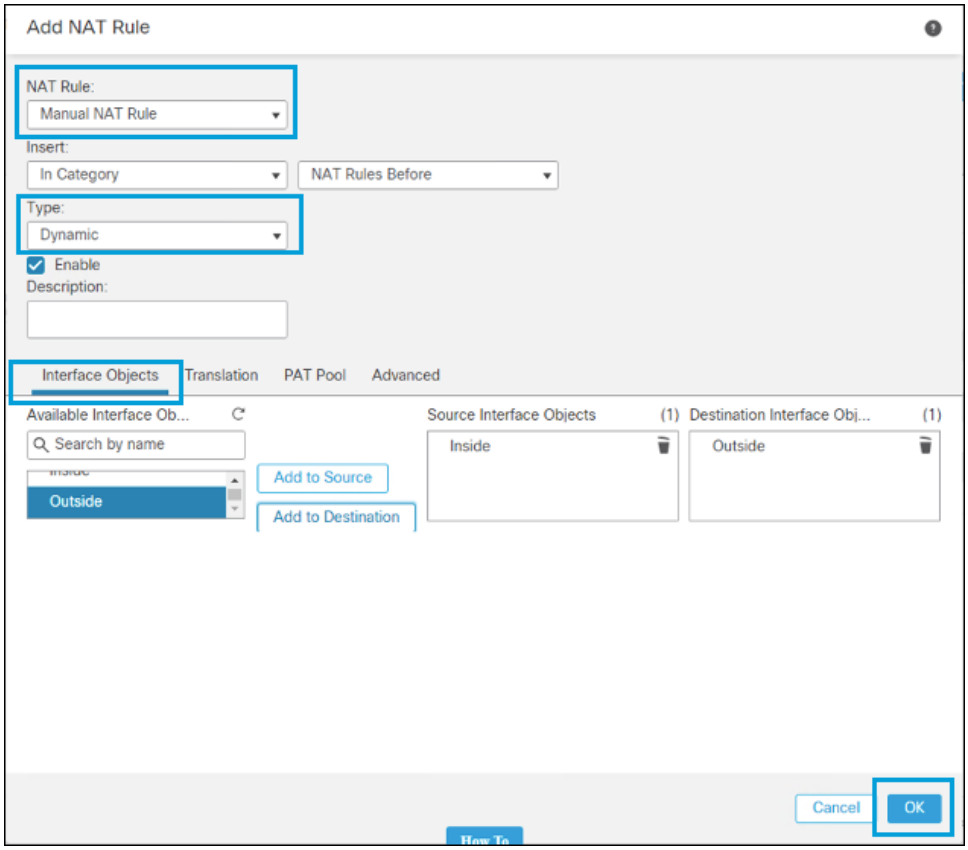
If you use the public IP in your internal network, you must NAT the traffic to a private IP address pool before sending the traffic to Secure Access, as most of the traffic goes through the Secure Access IPSec tunnel. It is easier to create NAT for the traffic not going through the tunnel and use no NAT for all other traffic.

In this example, the network object containing the Secure Access resolvers' IP address is referred to in the NAT statement. All traffic sourced from the internal network with a destination matching the network object will have the source IP NATed to the firewall interface address. All other traffic does not match the NAT statement, and so is forwarded to Secure Access without being NATed.

1. In Cisco Secure Firewall Management Center, navigate to **Devices** > **NAT** > **New Policy** > **Threat Defense NAT**.
2. Enter a name, then select the FTD device to apply the policy. Click **Save**.



3. Click **Add Rule**.
4. Select **Manual** for **NAT Rule**, then select **Dynamic** for type. In **Interface Objects**, choose **Inside** for the **Source** and **Outside** for **Destination**.

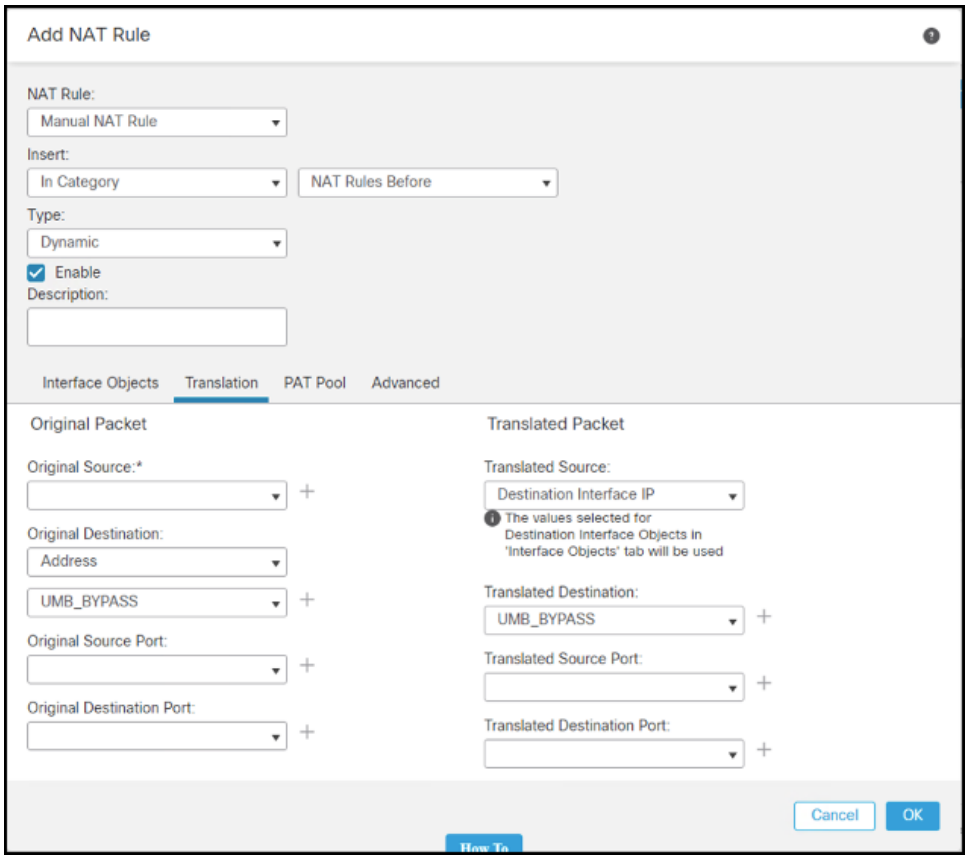


5. Under **Translations**, select a network object containing the internal subnet as the **Original Source**. Specify the Secure Access bypass network object you previously created as the **Original Destination**.

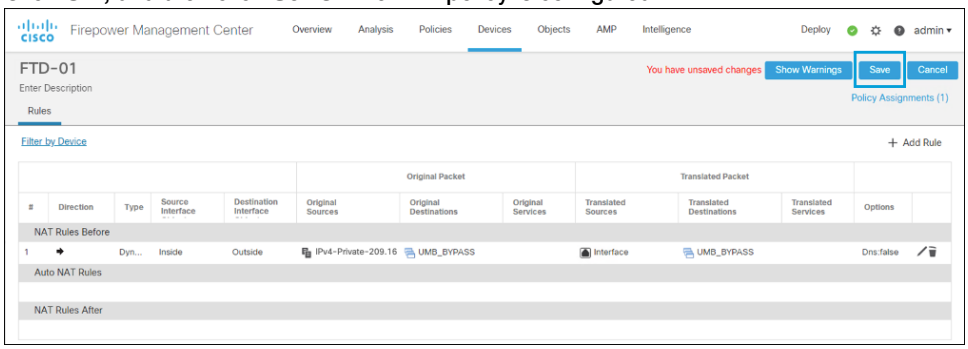
> **Note**
>
> This object contains the Secure Access resolvers' IP address, as well as (optionally) the `146.112.0.0/16` and `155.190.0.0/16` networks, plus any other traffic you may want to exempt from the tunnel. Using this object facilitates the configuration, because when hosts and subnets are added or removed from the object, both the IPsec traffic selector and NAT statement are updated.

6. Select **Destination Interface IP** as the **translated source**, and the same object as the **translated destination**.

   This ensures that the internal network is NATed to the interface IP address only when the destination is the network object containing the resolver's IP address. Other destinations do not match the NAT statement.



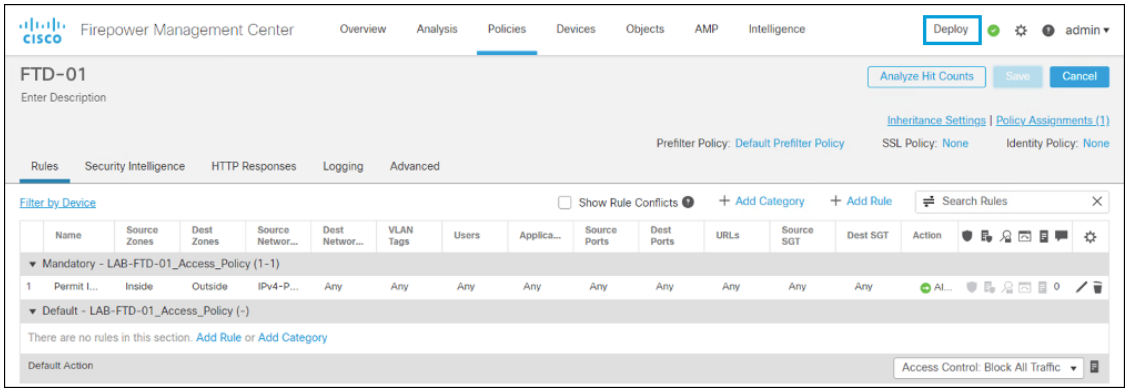
7. Click **OK**, and then click **Save**. The NAT policy is configured.



Configure Access Policy

Describes configuring access policy. The Access Policy in Firepower combines all the other policies (SSL Decryption, DNS, Pre-filter, Identity). At a minimum, an entry permitting inside traffic going out should exist. In production environments, you normally add more specific access entries.

The Access Policy in Firepower combines all the other policies (SSL Decryption, DNS, Pre-filter, Identity). At a minimum, an entry permitting inside traffic going out should exist. In production environments, you normally add more specific access entries.



Note

Deployment Not Automatic

A policy configured in Cisco Secure Firewall Management Center is not automatically applied to FTD devices. The configuration must be enabled by clicking **Deploy** in the top configuration bar.

Configure Firepower VTI, PBR, and Per Tunnel Identity

Describes configuring firepower vti, pbr, and per tunnel identity. At a high level, the Firepower configuration process consists of the following steps.

At a high level, the Firepower configuration process consists of the following steps.

1. Configure Site-to-Site VPN
2. Configure Policy-based Routing
3. Configure Access Policy

To start the configuration, log in to your Cisco Secure Firewall Management Center web interface at its IP address or FQDN; for example, ***https://FMC_IP_OR_FQDN***.

Configure Tunnels in Secure Access

Describes configuring tunnels in secure access. From Firepower 7.1+, FTD can authenticate to Secure Access by using a Pre-Shared Key (PSK) and IP or FQDN IKEv2 identity. If the Firepower is behind a NAT device, FQDN identity is the only possible option.

From Firepower 7.1+, FTD can authenticate to Secure Access by using a Pre-Shared Key (PSK) and IP or FQDN IKEv2 identity. If the Firepower is behind a NAT device, FQDN identity is the only possible option.

Virtual tunnel interface is available from Firepower 6.7+ with Policy Based Routing (PBR) through FlexConfig. Firepower 7.1+ adds Per Tunnel Identity and Policy Based Routing via graphic interface.

Follow the steps in Add Network Tunnel Group to add Firepower VTI and PBR to Secure Access.

Note: When supported by the device, FQDN is always the preferred option.

The new tunnel appears in Secure Access with a status of *UnEstablished*. The tunnel status is updated once the first IKEv2 INIT message containing the tunnel identity is received in one of the Secure Access data centers.

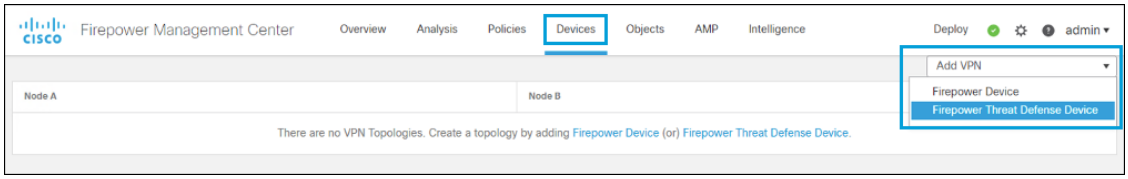
Configure Site-to-Site VPN

Provides instructions for configuring site-to-site vpn. It also identifies related requirements, procedures, and operational considerations.

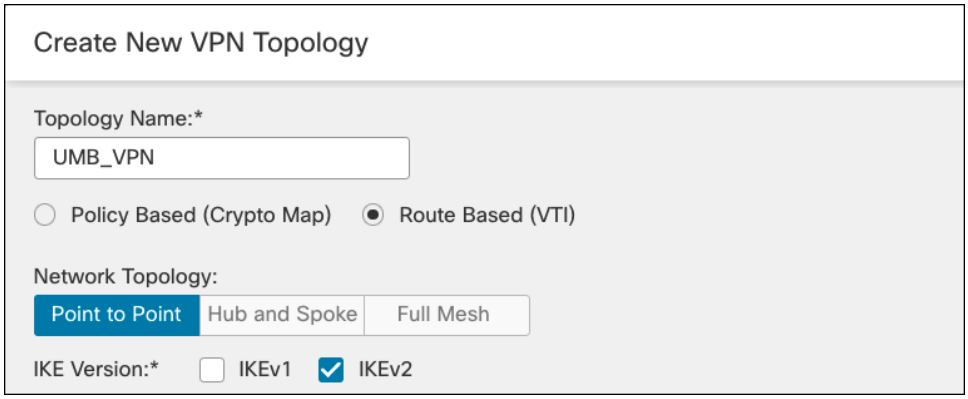
You can now configure the site-to-site VPN.

Procedure

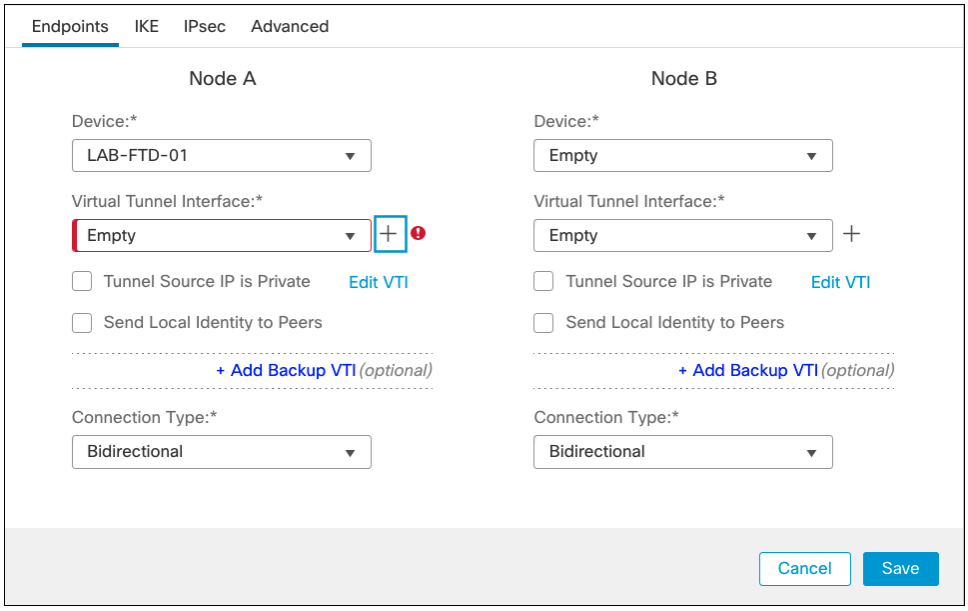
1. Navigate to **Devices** > **VPN** > **Site to Site** > **Add VPN** > **Firepower Threat Defense Device**.



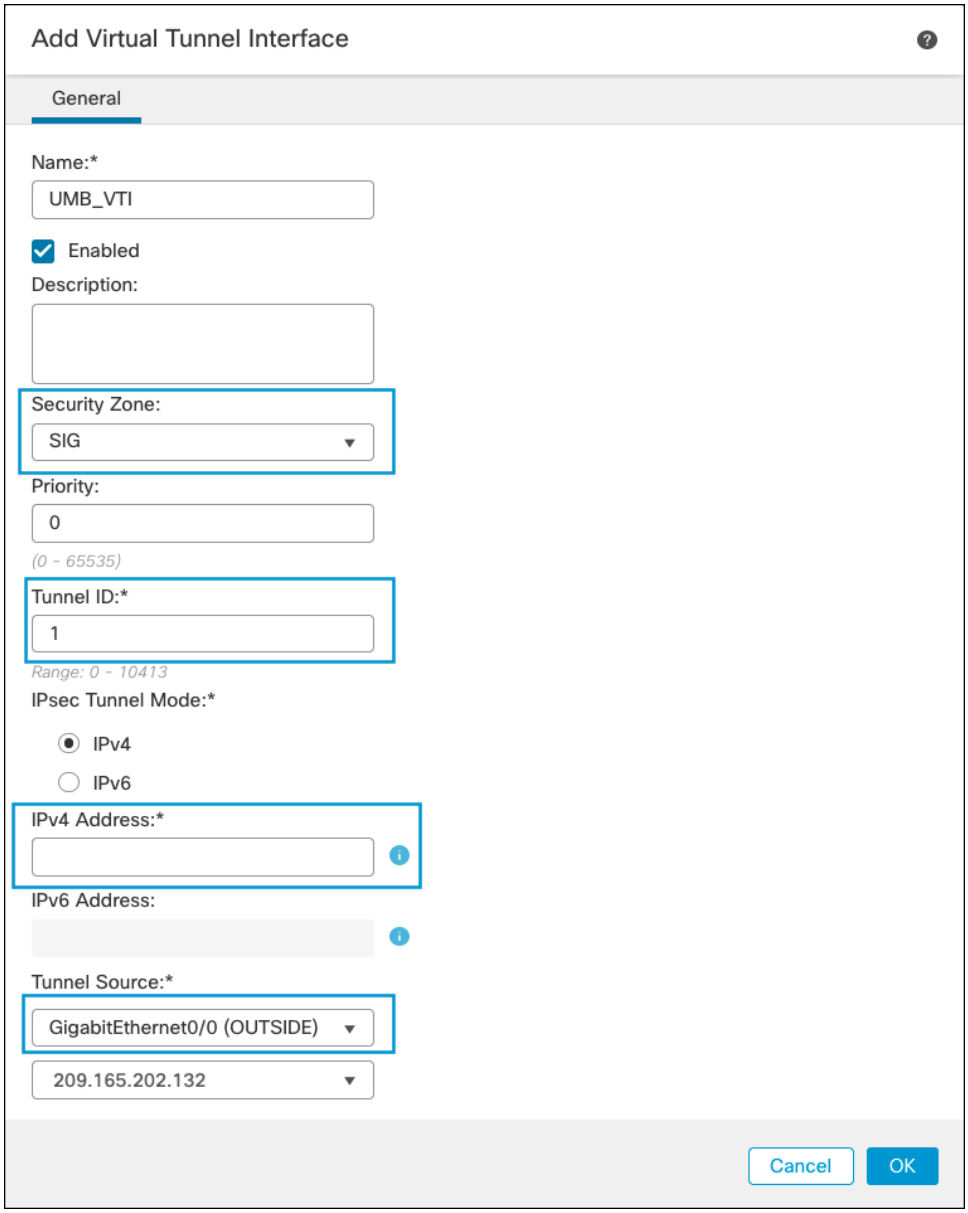
2. Enter a name for the topology, select **Route Based (VTI)**, and check IKEv2 box. For more information about supported protocols, see Supported IPSec Parameters.



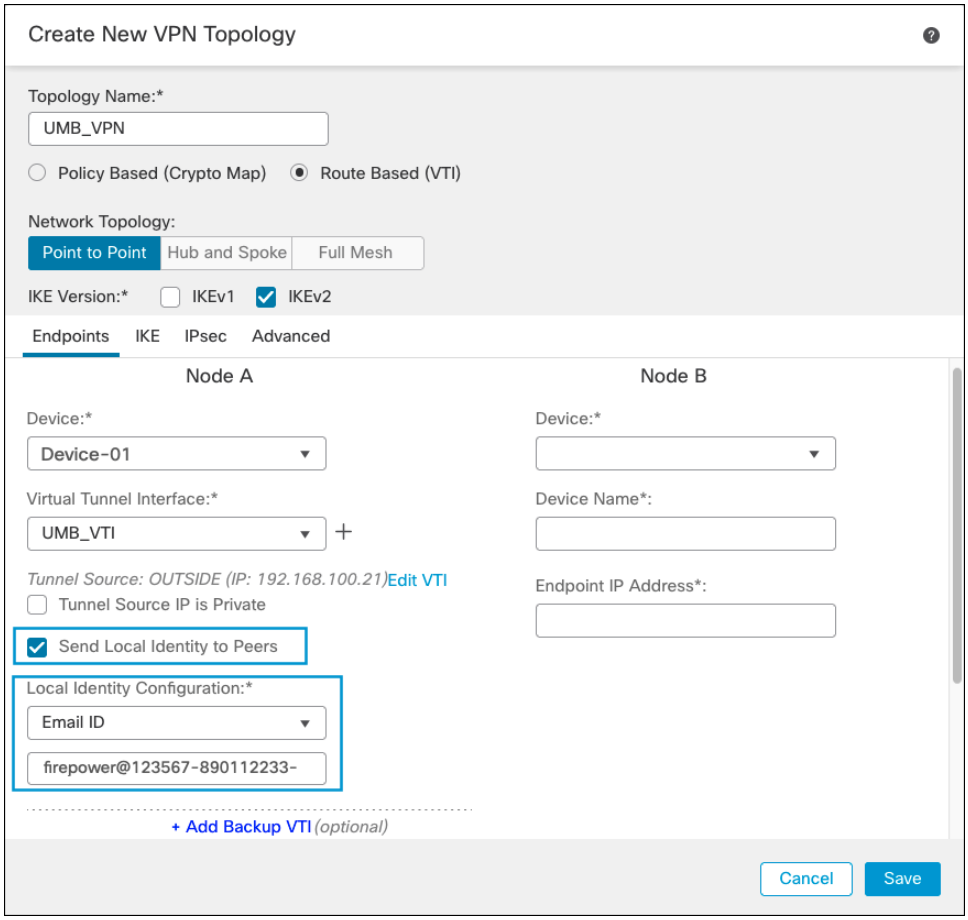
3. Choose a Firepower device from the **Device** drop-down list for Node A and click **Add** to add a Virtual Tunnel Interface.



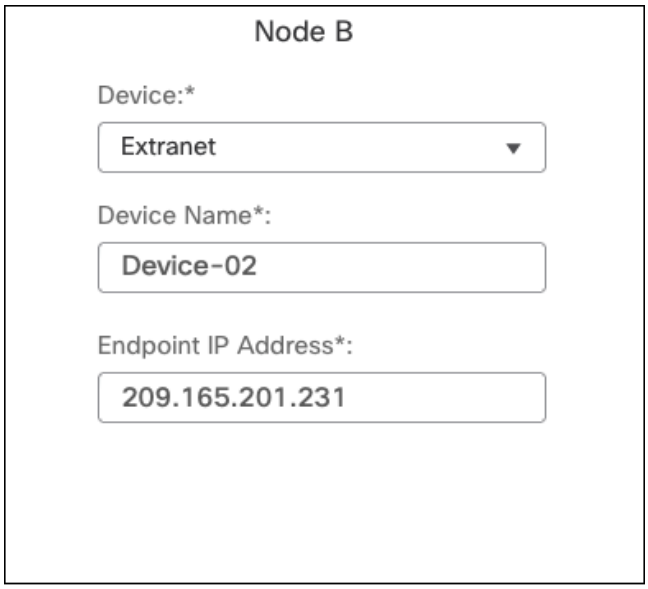
4. Enter a name for the VTI, choose an existing Security Zone or create a new for the tunnel, enter a Tunnel ID and an IP address (a /30 subnet to accommodate local device and remote IP), and select the **OUTSIDE** interface as tunnel source. Then click **Ok**.



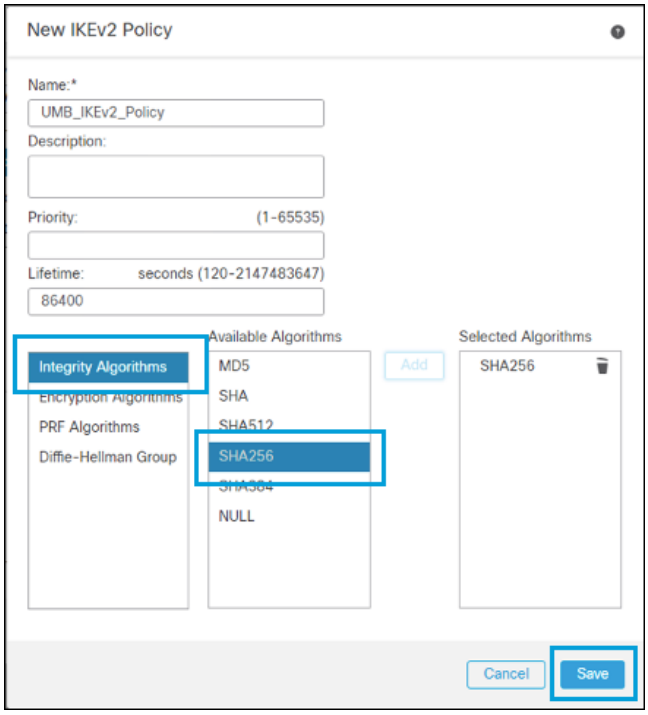
5. Select the VTI you just created, and under **Send Local Identity to Peers** select **Email ID** and type the previous created tunnel FQDN.



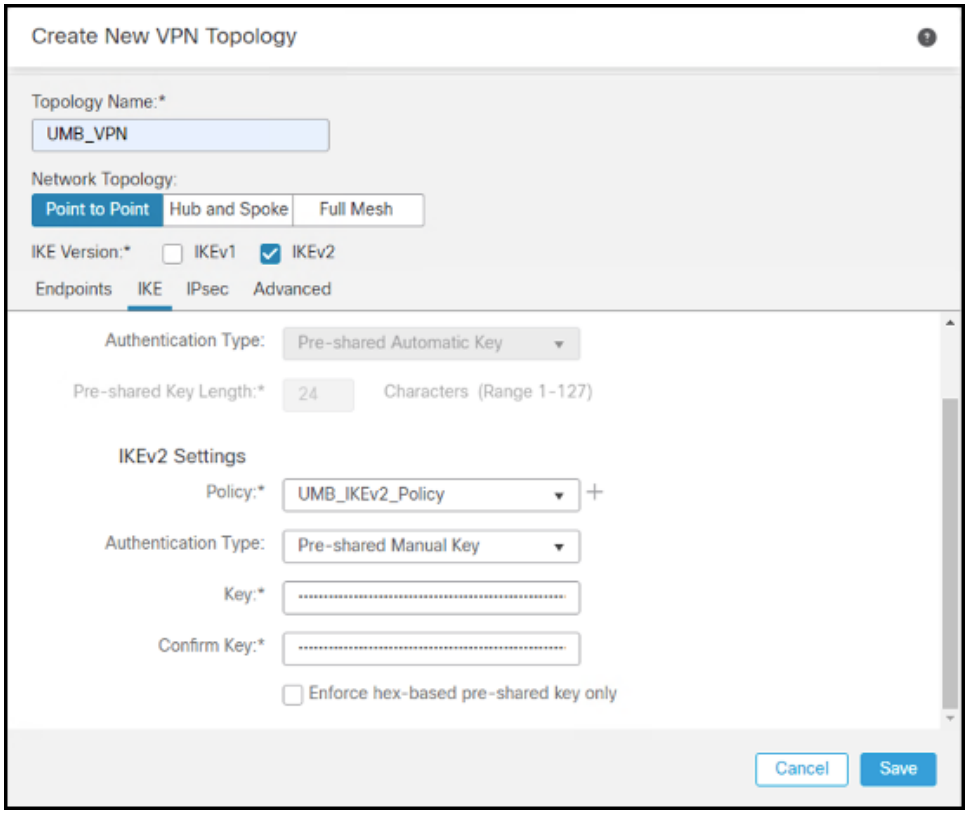
6. Under Node B, choose **Extranet** as the device, enter a name and IP address of a Secure Access data center.



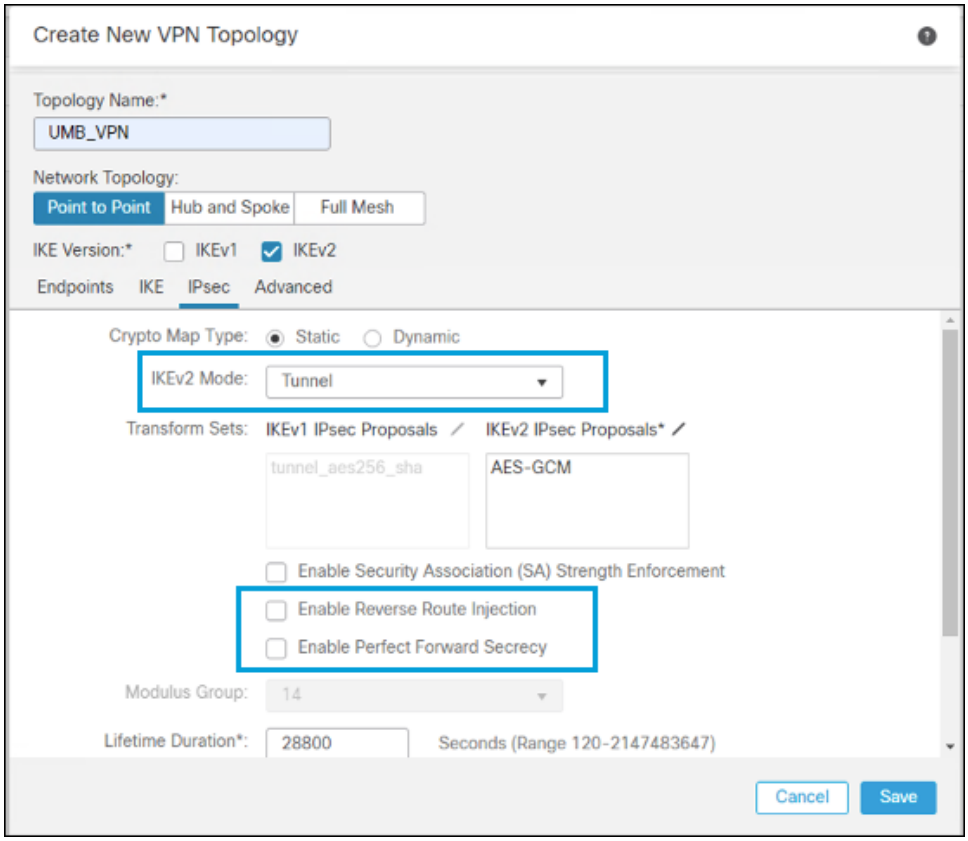
7. Enter a name for the IKEv2 policy, then select the parameters from the list.



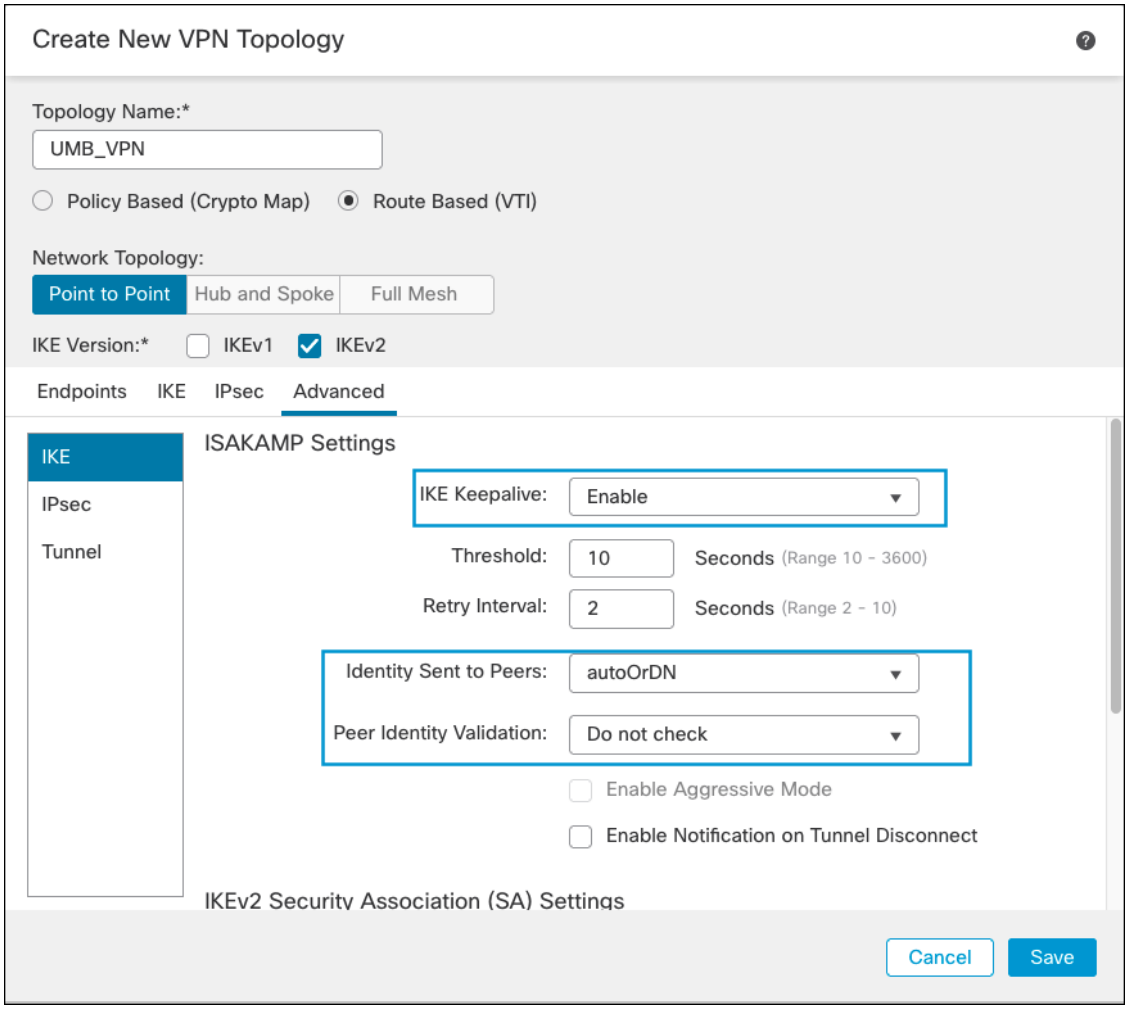
8. After saving the IKEv2 Policy, select it. Choose **Pre-shared Manual Key** from the **Authentication** drop-down list and enter the key.



9. Under **IPSec Configuration**, add a new **IKEv2 IPsec Proposal** with your crypto algorithms or select an existing profile. Select **Tunnel** for **IKEv2 Mode** and uncheck **Enable Reverse Route Injection** and **Enable Perfect Forward Secrecy**.



10. In the **Advanced** tab under IKE, enable **IKE Keepalive**. Select **autoOrDN** as the **Identity Sent to Peers**, and disable **Peer Identity Validation**. Then click **Save**.

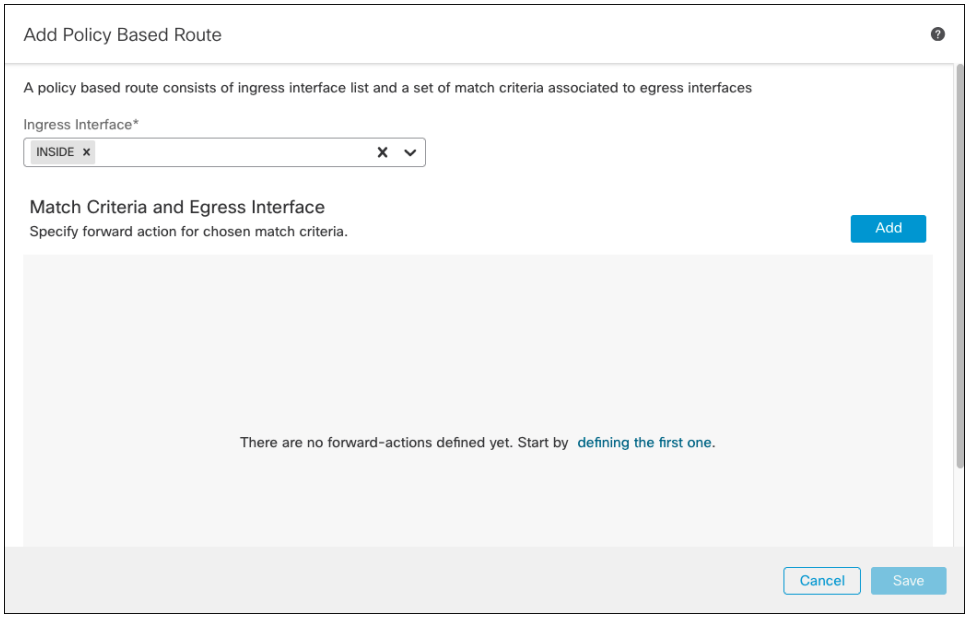


Configure Policy-based Routing

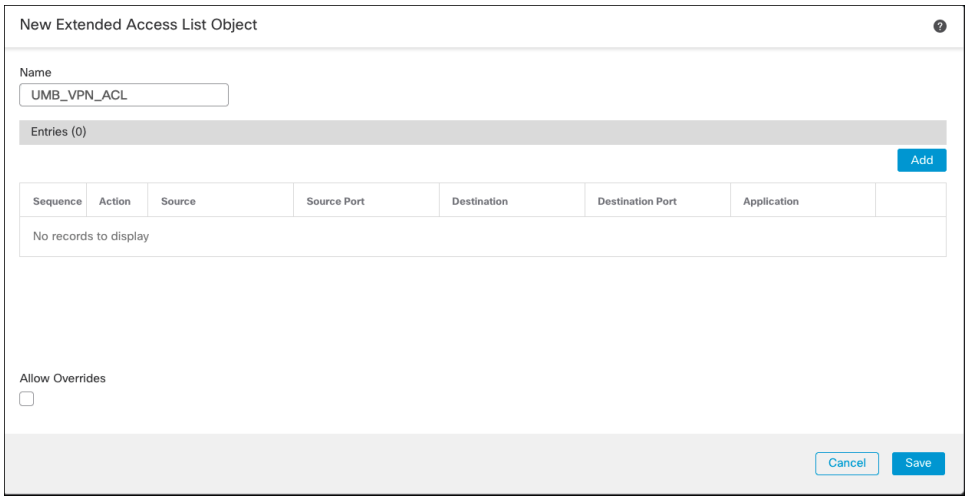
Provides instructions for configuring policy-based routing. Navigate to Devices Device Management and click the name of the device to edit.

Procedure

1. Navigate to **Devices** > **Device Management** and click the name of the device to edit.
2. Under **Routing** > **Policy Based Routing**, click **Add** to add a new policy
3. Choose the **Inside** for the Ingress Interface (user's facing interface where PBR will be applied) and click **Add**.

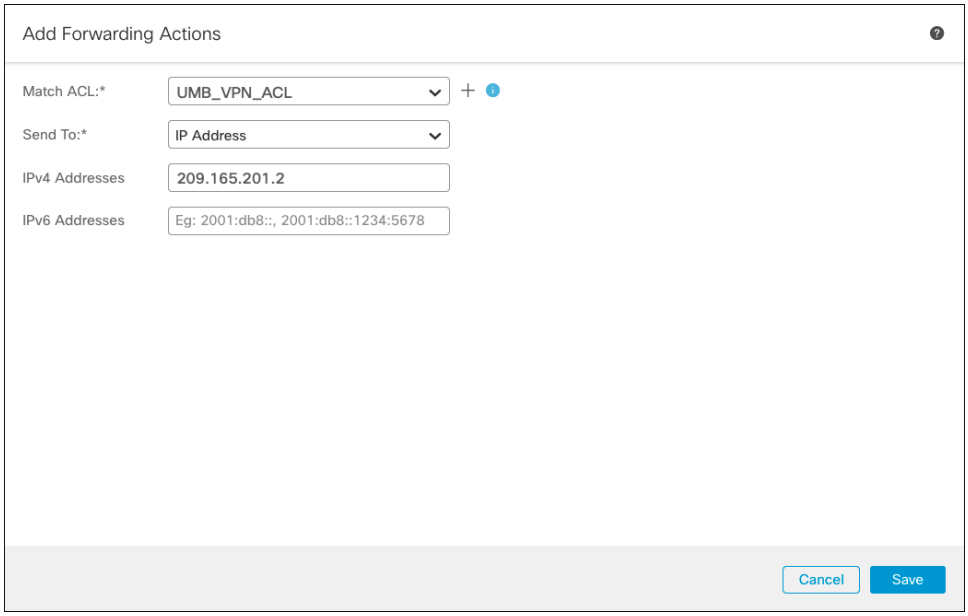


4. Choose the existing extended ACL, and click **Add**.



Alternatively, if you are creating a new ACL, enter a name and add Access Control Entries (ACE) matching the traffic that should be redirected to Secure Access.

5. Click **Save** to add the access entries.
6. Under **Match ACL**, choose the newly created ACL and under **Send To** choose **IP Address**. Type the IP address in the same subnet previously used for VTI and click **Save**



7. Click **Save** to save the configuration and deploy.

Configure Access Policy

Describes configuring access policy. If not yet allowed by the access policy, add an access entry allowing traffic from inside the network to the Secure Access tunnel.

If not yet allowed by the access policy, add an access entry allowing traffic from inside the network to the Secure Access tunnel.

Troubleshooting

Describes troubleshooting. Cisco Secure Firewall Management Center has a VPN troubleshooting tab where VPN-related events are displayed. If you need to send VPN debug messages to Cisco Secure Firewall Management Center, change the logging level in the Platform Settings policy.

Cisco Secure Firewall Management Center has a VPN troubleshooting tab where VPN-related events are displayed. By default, only error messages are sent from FTD to Cisco Secure Firewall Management Center, as LINA code (ASA) is responsible for the IPSec tasks the same commands available for troubleshooting the ASA devices are available in FTD.

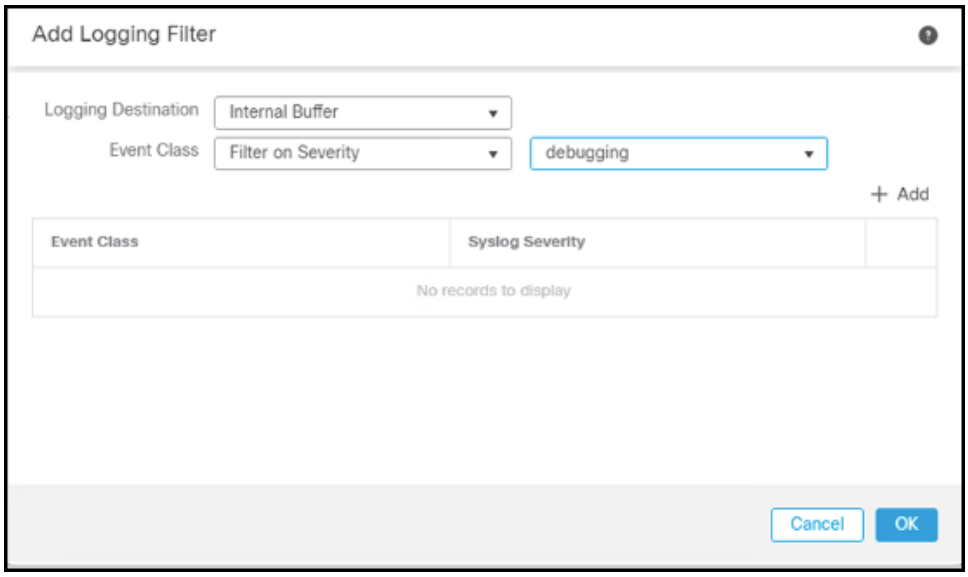
If you need to send VPN debug messages to Cisco Secure Firewall Management Center, change the logging level in the Platform Settings policy. This policy is configured and added in **Devices > Platform Settings**. VPN logging to Cisco Secure Firewall Management Center is in the Syslog section of the Platform Settings policy from the Logging Setup tab. It is also possible to send logging messages to other destinations, such as the FTD device internal buffer.

Enable Logging for Debugging

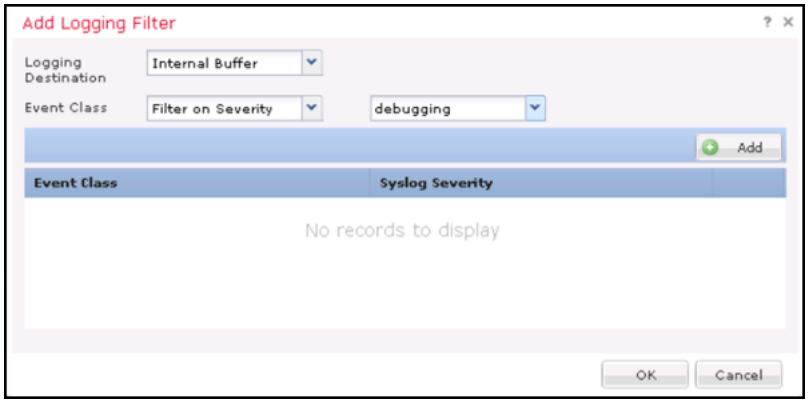
Provides instructions for enabling logging for debugging. In Cisco Secure Firewall Management Center, navigate to DevicesPlatform Settings. Under Basic Logging Settings, add a logging destination. Page displaying logging filter setup with logging destination option

Procedure

1. In Cisco Secure Firewall Management Center, navigate to **Devices** > **Platform Settings**.
2. Under **Basic Logging Settings**, add a logging destination.



3. Under **Logging Destinations** tab, click **Add**, then select **Internal Buffer** (or another logging destination). Set the logging level to **Debugging**.



When logging is enabled, you can enable IKEv2 debug, SSH to FTD. Then enter type `debug crypto ikev2 platform` and `debug crypto ikev2 protocol`. These two debugging options provide detailed information about IKEv2 negotiation.

```
Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

> debug crypto ikev2
  ha         debug the ikev2 ha
  platform   debug the ikev2 platform
  protocol   debug the ikev2 protocol
  timers     debug the ikev2 timers

> debug crypto ikev2 platform
> debug crypto ikev2 protocol
>
```

4. After enabling debugging in the FTD device, return to Cisco Secure Firewall Management Center and navigate to **Devices** > **VPN** > **Troubleshooting**. IKEv2 negotiation debugging information is available.

What to do next

If debug destination internal buffer was configured, going back to the FTD device via SSH is also possible. This enables you to see debug messages in the FTD terminal.

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 145 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, 197 messages logged
 Bytes rcv: 24260, Reason: Internal Error
%FTD-7-609002: Teardown local-host identity:188.40.190.251 duration 0:02:54
%FTD-7-609002: Teardown local-host Outside:146.112.97.2 duration 0:02:54
%FTD-7-710005: UDP request discarded from 0.0.0.0/68 to Outside:255.255.255.255/
7
%FTD-7-710005: UDP request discarded from 0.0.0.0/68 to Inside:255.255.255.255/6
```

To access the LINE portion of the code, enter the command `system support diagnostic-cli`.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

FF-FTD-01# show ver
FF-FTD-01# show version
--------------[ FF-FTD-01.sig.local ]---------------
Model                     : Cisco Firepower Threat Defense for VMWare (75) Versio
n 6.5.0 (Build 115)
UUID                      : 567ce6e8-deb6-11e9-9e95-b425c64212f5
Rules update version      : 2019-08-12-001-vrt
VDB version               : 327
-----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.13(1)
SSP Operating System Version 2.7(1.105)

Compiled on Thu 19-Sep-19 17:23 PDT by builders
System image file is "boot:/asa9131-0-smp-k8.bin"
Config file at boot was "startup-config"
```

Configure Tunnels with Meraki MX

Describes configuring tunnels with meraki mx. Follow these steps to connect a Cisco Meraki MX/Z4 series device to Cisco Secure Access through a Meraki Third Party (non-Meraki) VPN Tunnel (NMVPN) configuration.

Follow these steps to connect a Cisco Meraki MX/Z4 series device to Cisco Secure Access through a Meraki Third Party (non-Meraki) VPN Tunnel (NMVPN) configuration.

- The two primary uses cases for Secure Access with Meraki Networks are secure internet access and remote access to private applications.
- To connect to Secure Access, a NMVPN must be established to a Secure Access Network Tunnel Group (NTG).
- With this configuration in place, internet-bound traffic from Meraki branches will be secured through Secure Access.
- The same tunnels can be used to securely connect remote users of AnyConnect VPN and Client/Clientless Zero Trust Access modules in the Secure Client to private applications on Meraki networks.

Caveats and Considerations

Provides instructions for caveats and considerations. This section discusses important caveats and considerations associated with the Meraki Third Party (non-Meraki) VPN tunnel configuration to Secure Access.

This section discusses important caveats and considerations associated with the Meraki Third Party (non-Meraki) VPN tunnel configuration to Secure Access.

Before you begin

- A Cisco Meraki MX/Z4 device (running MX 18.107+ firmware).
- A valid Cisco Secure Access account.
- A network tunnel group configured on Cisco Secure Access; see Add a Network Tunnel Group.

Procedure

1. There is no stateful failover to a Secure Access secondary tunnel.
   - The MX only supports active/cold standby to a single headend.
   - Traffic from a failed site is required to reestablish the tunnel.
2. Only static routing is supported; BGP is not supported.
3. Requires traffic to be generated from the LAN side of an MX through the non-Meraki VPN to establish connection.
   - Remote application access on Meraki networks through an MX is not possible until traffic is initiated from the application side of the MX through the non-Meraki VPN.
   - Traffic will also need to be consistently generated from the LAN side of the MX over each non-Meraki VPN to keep the tunnel from timing out.
4. ECMP/Load balancing is not supported. Only a single IPSec tunnel is supported between a single Meraki network and a Secure Access network tunnel group.
5. A unique public uplink IP is required for each network.
   - The public uplink IP is used as the MX peer device IP, and this cannot be changed.
6. In the Secure Access dashboard, the network tunnel group will display the status as .

> **Warning**
>
> This is because the Meraki network cannot build a standby tunnel to the Secondary Hub in the network tunnel group that is provided for intra-region redundancy.

Supported Use Cases and Requirements

Describes supported use cases and requirements. The following sections describe supported use cases for Meraki Third Party (non-Meraki) VPN tunnel configuration to Secure Access.

The following sections describe supported use cases for Meraki Third Party (non-Meraki) VPN tunnel configuration to Secure Access.

Remote Access VPN and ZTA

Describes remote access vpn and zta. The Meraki networks will need to be tagged. Use the Umbrella IKEv2 configuration. No default exit hub.

- The Meraki networks will need to be tagged.
- Use the Umbrella IKEv2 configuration.
- No default exit hub.
- No spokes.

Branch-to-Branch through Secure Access

Provides instructions for branch-to-branch through secure access. One of the following options is required to enable Secure Access policy enforcement to apply to branch-to-branch communication. Otherwise, all traffic will traverse Meraki AutoVPN between Meraki networks directly.

One of the following options is required to enable Secure Access policy enforcement to apply to branch-to-branch communication. Otherwise, all traffic will traverse Meraki AutoVPN between Meraki networks directly.

Procedure

1. Each network hosting applications is in a separate org; or
2. All networks are in a single org.

> **Note**
>
> If this is the case, contact Support to have hub-to-hub communication turned off.

Secure Internet Access with Non-Meraki VPN

Describes secure internet access with non-meraki vpn. The following are requirements for this configuration: No AutoVPN default route. Local route configuration 0.0.0.0/0.

The following are requirements for this configuration:

- No AutoVPN default route.
- Local route configuration 0.0.0.0/0.

Step 1: Add a Network Tunnel Group in Secure Access

Provides instructions for step 1: add a network tunnel group in secure access. Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels.

Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels.

Tunnels and tunnel groups are core concepts in managing connections between your data centers and Cisco Secure Access. A network tunnel group provides the framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources.

Procedure

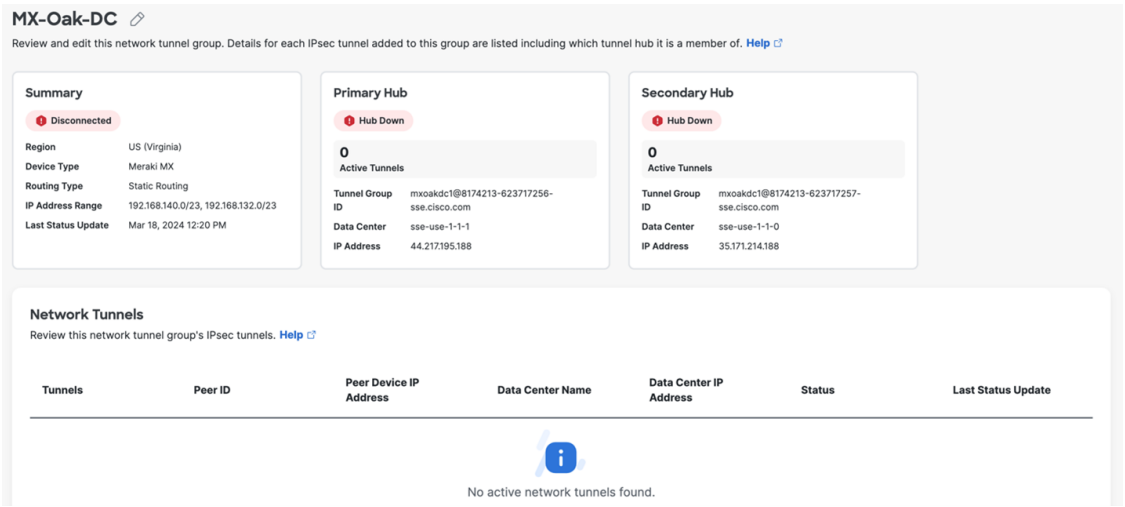
1. Follow the steps in Add a Network Tunnel Group.
2. Make note of the **Tunnel ID** and **Passphrase** you enter when configuring the network tunnel group. These values are needed when you configure your Meraki IPsec tunnel.

   > **Note**
   >
   > Secure Access provides the option to download a CSV file with the network tunnel group details.

3. Remember to select **Static routing** under routing options. Only static routing is supported.

What to do next

The new network tunnel group appears in the Secure Access dashboard as **Disconnected**, and with the **Primary Hub** and **Secondary Hub** status showing as **Hub Down**. The network tunnel group status is updated once it is fully configured and connected with Meraki MX.



See the Verification and Troubleshooting section for additional information about how to evaluate the network tunnel group status.

Step 2: Configure a Tunnel in Meraki MX

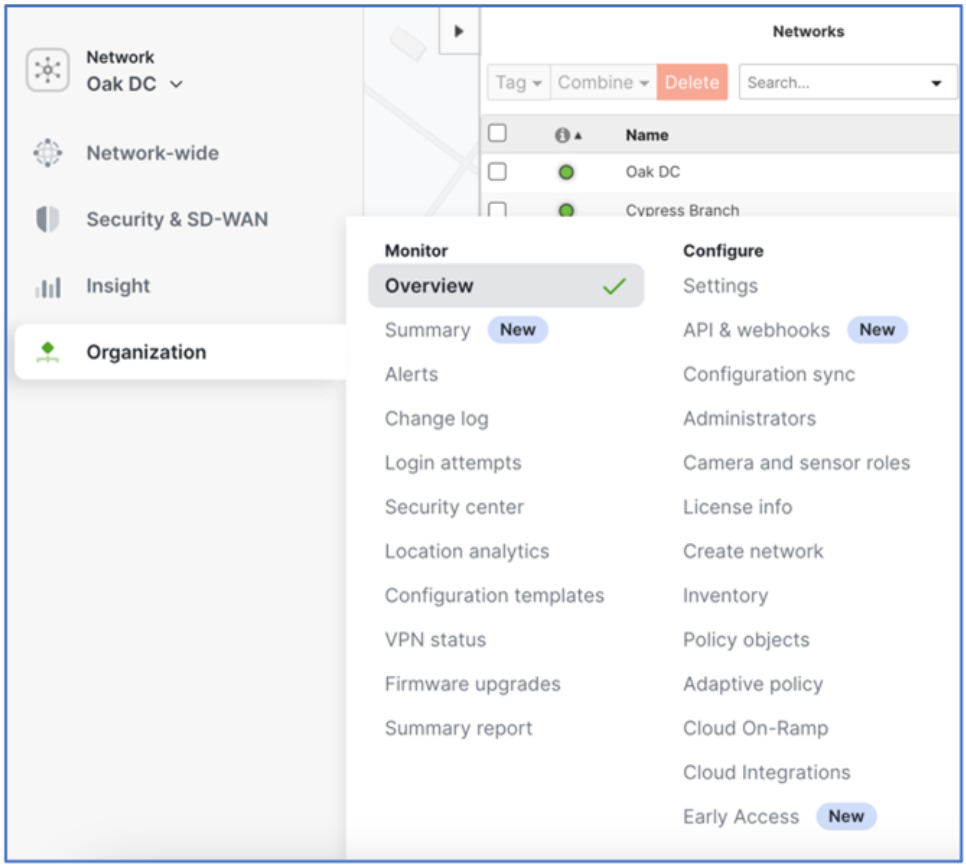
Provides instructions for step 2: configure a tunnel in meraki mx. Configure a Meraki Third Party (non-Meraki) VPN tunnel to connect a Meraki MX/Z4 series device to Cisco Secure Access.

Configure a Meraki Third Party (non-Meraki) VPN tunnel to connect a Meraki MX/Z4 series device to Cisco Secure Access.

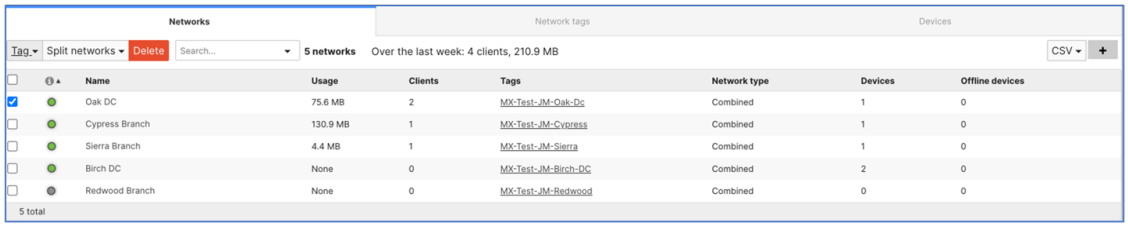
Procedure

1. In the Meraki MX dashboard, navigate to the **Organization** > **Monitor** > **Overview** page.

   If the page is not expanded by default, expand the **Networks** list by clicking the left-facing arrow at the top of the network list.

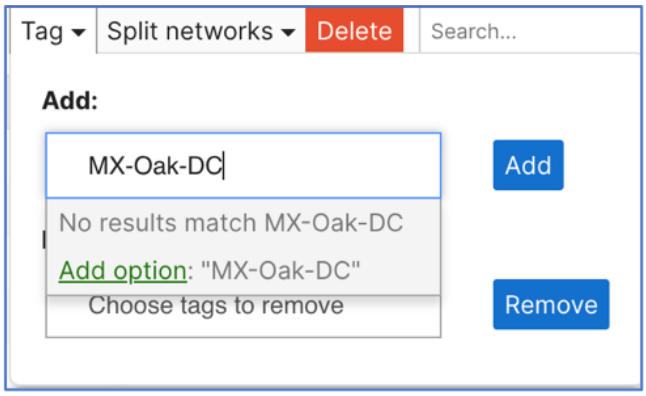


2. Select the desired network from the networks **Name** list. Select only the network that will connect to the Secure Access Network Tunnel Group.

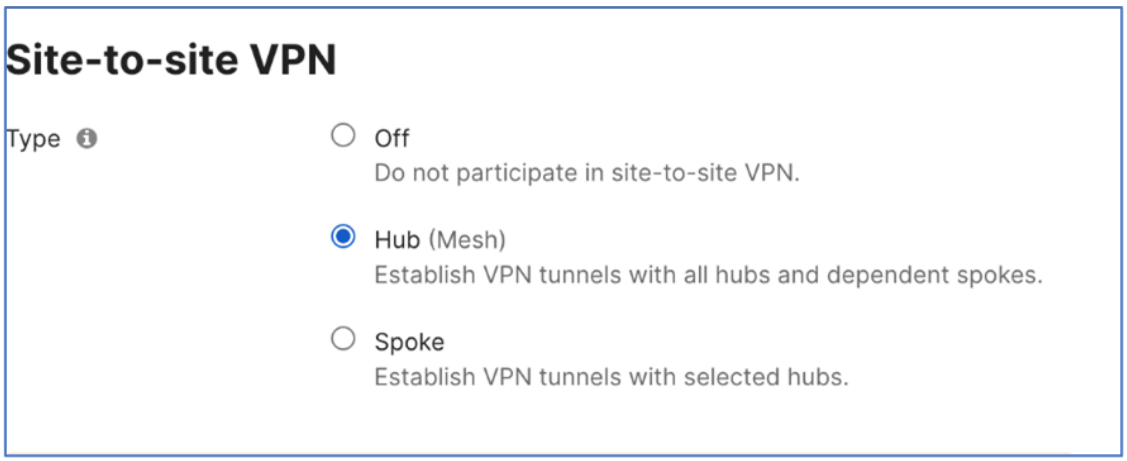


3. Add a Network tag to the selected network. Select the **Tag** dropdown menu from the top left. A tag can be created by typing into the field and then clicking **Add**.

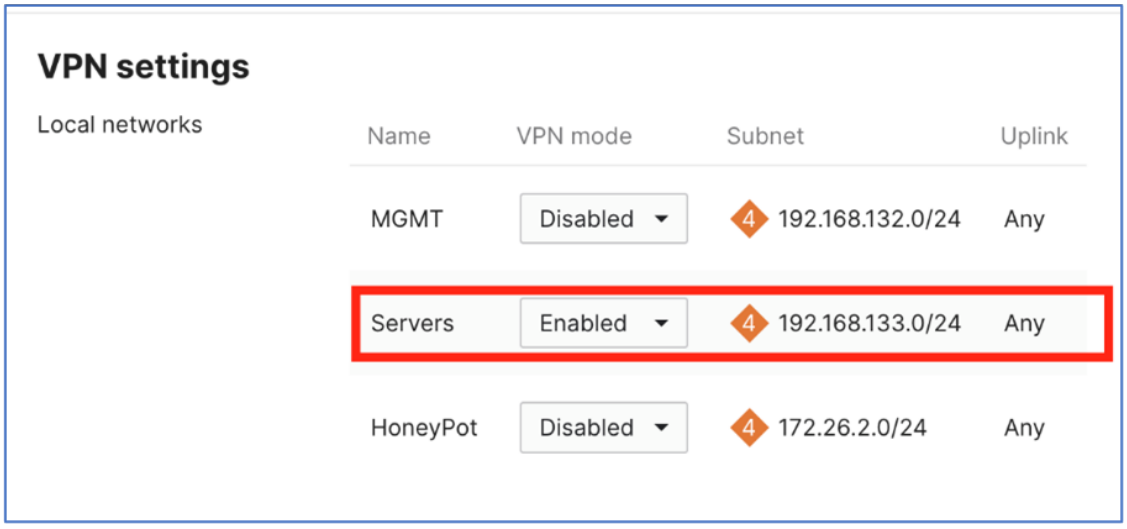
> **Note**
>
> It is recommended that the same name is used for the Meraki Network Tag as the Secure Access Network Tunnel Group.



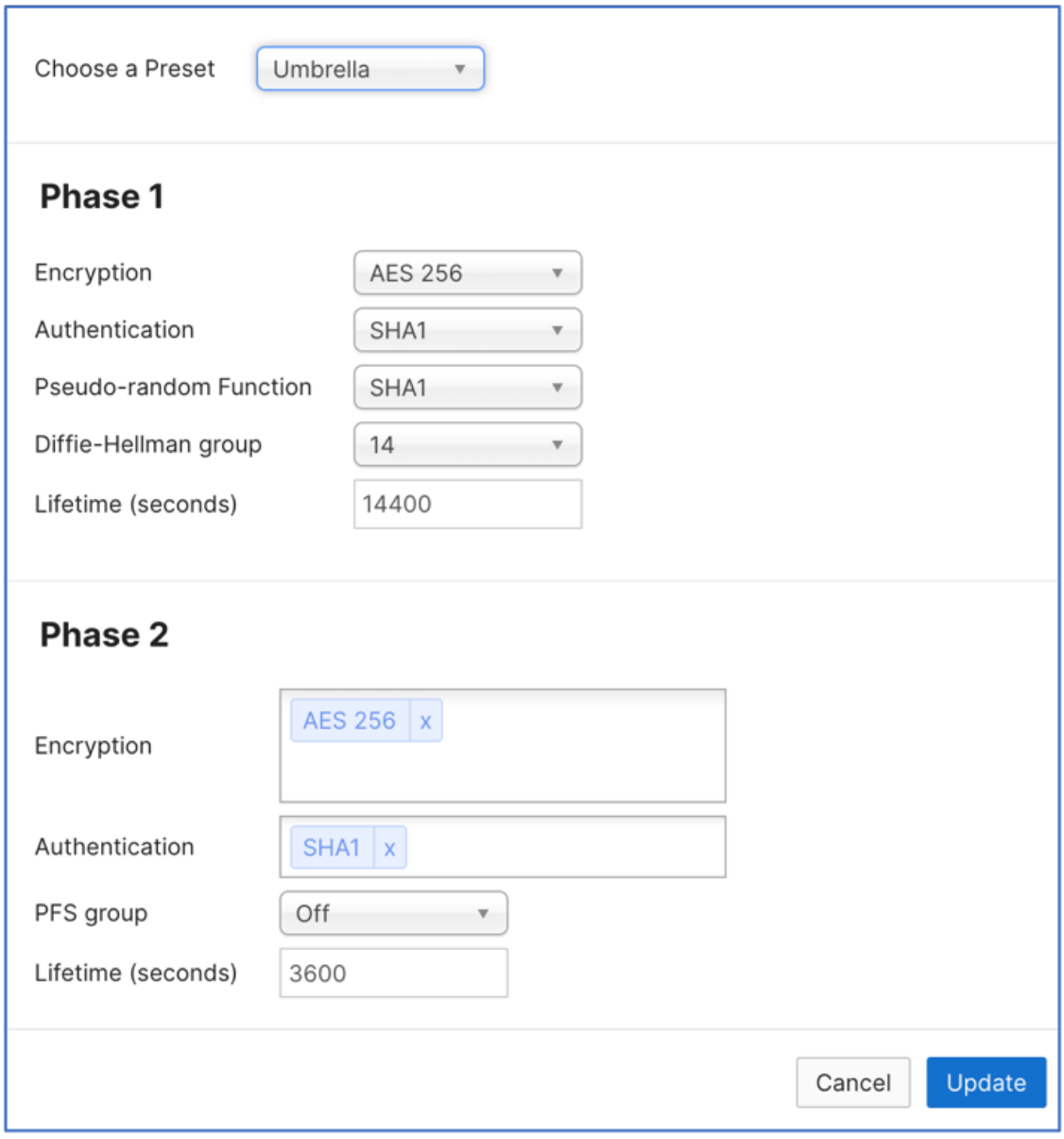
4. While in the Meraki dashboard, navigate to **Security & SD-WAN** > **Site-to-site VPN**, and choose **Hub (Mesh)**.



5. Next, in the same section, find the **VPN settings** and choose **Enabled** for the VLANs that will use the new Secure Access network tunnel group.



6. Scroll down to find **Organization-wide settings** to locate the **Non-Meraki VPN Peers** section. Click **Add a peer** and then add the tunnel ID and tunnel passphrase that you created in Step 1: Add a Network Tunnel Group in Secure Access.
7. Configure the IPsec parameter settings:
   - **Name**–Provide a meaningful name for the tunnel.
   - **IKE Version**–Select IKEv2.
   - **IPsec policies** Choose the predefined Umbrella configuration; see Supported IPsec Parameters.



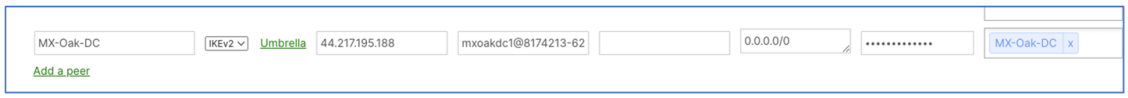
   - **Public IP**–IP address to connect to Secure Access Network Tunnel Group Primary Data Center IP.
   - **Local ID**–The Primary Tunnel ID for the Network Tunnel Group.
   - **Remote ID**–Leave this blank.
   - **Private subnets**–There are 2 common configurations for Private Subnets:

- If the desired behavior is to use Secure Internet Access and Secure Private Access to access applications on tunnel-enabled vlans/subnets, then the only entry here should be 0.0.0.0/0. This will route all traffic to Secure Access for either Secure Internet Access, Remote Access VPN, or ZTA clients.
- If only Remote Private Application access is required, then all subnets that are used by the Secure Access infrastructure must be entered:
  a. CGNAT 100.64.0.0/10
  b. RA VPN and Management IP Pool subnets.

- **Preshared secret**–This is the **Passphrase** for the Network Tunnel Group created in Secure Access.
- **Availability**–Enter the Network tag you defined earlier for the MX appliance that builds the tunnels to Secure Access.

Important

Do not leave this field blank. Ideally this field should match the Network tag entered in Step 3 above. Leaving this field blank, "All Networks", or entering a tag that is associated with multiple networks could cause one or more tunnels to become unstable. This could lead to unexpected behavior and cause an NMVPN tunnel to not be established.



8. Click **Save**.

   Upon completion of these steps, you should have a functioning tunnel routing your traffic as intended.

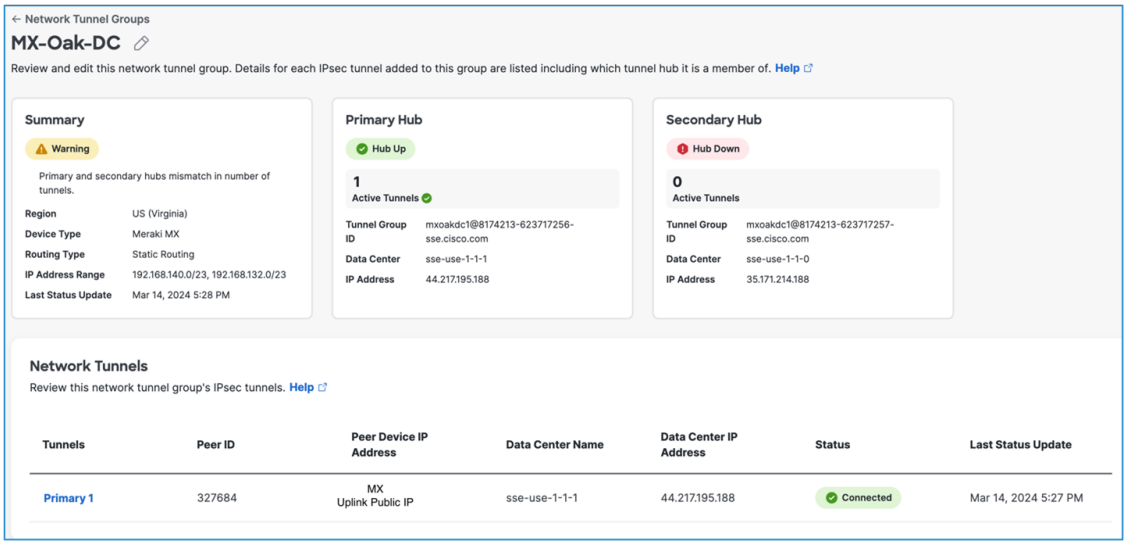
Verification and Troubleshooting

Provides instructions for verification and troubleshooting. The Secure Access Network Tunnel Group will move from Disconnected Status to Warning. This change could take several minutes and may require a test ping described in step 2 below.

Procedure

---

1. The Secure Access Network Tunnel Group will move from **Disconnected** Status to **Warning**. This change could take several minutes and may require a test ping described in step 2 below.



Note

Network Tunnel Group Status

The Network Tunnel Group will never move from a **Warning** status to **Connected**. This is because the Network Tunnel Group is designed to have a Primary and Secondary tunnel connected to each Hub for failover. Traffic will pass to the **Primary Hub** even if the Network Tunnel Group status is **Warning**.

2. Run `ping` tests from the new VLAN to the internet. For more information, see Using the Ping Live Tool.
3. Check the status of the VPN tunnel. For more information, see VPN Status Page.
4. Follow the VPN troubleshooting procedures. For more information, see Troubleshooting Non-Meraki Site-to-site VPN.

What to do next

Note

Cisco Meraki does not support policy based routing. It is not possible to do client side routing to determine if specific traffic belongs inside or outside the tunnel. However, it is possible to choose if an entire VLAN is tunneled to Secure Access.

Optional Configurations

Provides instructions for optional configurations. To create a VLAN for the subnet to redirect to Secure Access, see Configuring VLANs on the MX Security Appliance.

Procedure

---

1. To create a VLAN for the subnet to redirect to Secure Access, see Configuring VLANs on the MX Security Appliance.
2. To create a new SSID for the VLAN, see Configuring Simple Guest and Internal Wireless Networks.

Configure Tunnels with Cisco Adaptive Security Appliance

Describes configuring tunnels with cisco adaptive security appliance. Follow the steps in this guide to connect a Cisco Adaptive Security Appliance (ASA) firewall through an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel to Cisco Secure Access.

Follow the steps in this guide to connect a Cisco Adaptive Security Appliance (ASA) firewall through an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel to Cisco Secure Access.

Licensing and Hardware

Describes licensing and hardware. A valid Cisco Secure Access account. A Cisco Secure Access organization ID. For more information, see Find Your Organization ID.

- A valid Cisco Secure Access account.
- A Cisco Secure Access organization ID. For more information, see Find Your Organization ID.
- ASA Base or Security Plus license to establish an IPsec tunnel.
- A Cisco ASA router with a security K9 license to establish an IPsec tunnel. Other devices may work but have not been tested.

Network Access

Describes network access. When you add a network tunnel, we recommend that you choose the IP address based on the data center located closest to you.

- When you add a network tunnel, we recommend that you choose the IP address based on the data center located closest to you.
- Open UDP ports 500 and 4500.

Cisco ASA version 9.16 or lower devices require static public routable IPv4 address(es) configured on the interface that connects to the public internet and the Cisco Secure Access data center. This static public routable IPv4 address **must not be subject to a NAT**. **If NAT is present, the tunnel will fail**. This is because Cisco ASA IKEv2 PSK authentication automatically uses this directly configured IPv4 address as its IKE ID. This ID in combination with the PSK is used to successfully authenticate the ASA with Secure Access.

ASA 9.17 or above supports per tunnels identity and IKEv2 FQDN identity. Now that the ASA can be behind NAT, configure the tunnel in Secure Access as follows:

- Tunnel type: **Other**
- Authentication: **FQDN**
- ASA IPsec profile configuration should include the extra command with tunnel identity (set ikev2 local-identity email-id xxxxxxx@xxxxxxxxx-xxxxxxx.sse.com)

Note

A unique set of network tunnel credentials must be used for each IPsec tunnel. Using unique credentials for every tunnel prevents inadvertent outages should one tunnel get re-routed to a nearby data center through Anycast failover. You can create multiple tunnels as long as each tunnel connects to a unique network/IP on your ASA. Organizations have a default limit of 50 network tunnels. To increase this limit, contact support or your account manager. For more information, see Throughput and Multiple Tunnels.

Configure Tunnels in Secure Access

Provides instructions for configuring tunnels in secure access. Follow the steps in Add Network Tunnel Group. The new tunnel appears in the Secure Access dashboard with a status of UnEstablished. The tunnel status is updated once it is fully configured and connected with the ASA.

Procedure

Follow the steps in Add Network Tunnel Group.

What to do next

The new tunnel appears in the Secure Access dashboard with a status of *UnEstablished*. The tunnel status is updated once it is fully configured and connected with the ASA.

Configure ASA

Provides instructions for configuring asa. Configure the IKEv2 policy. Define the settings according to the supported IPsec parameters. Choose the policy number based on your ASA's existing policies.

Procedure

1. Configure the IKEv2 policy. Define the settings according to the supported IPsec parameters. Choose the policy number based on your ASA's existing policies.
   - Replace the default device name called `outside` with the name configured on your device. The device name refers to the public facing interface which the VPN uses to connect.

```
crypto ikev2 policy 10
  encryption aes-gcm-256
  integrity null
  group 19
  lifetime seconds 86400
crypto ikev2 enable outside
```

2. Configure the Group Policy and Tunnel Group parameters.
   - Enter the IP of a Secure Access data center.
   - Replace `\[Portal_Tunnel_Passphrase\]` with the Passphrase you configured in the previous section, Add Network Tunnel Group.

```
group-policy sse-policy internal
group-policy sse-policy attributes
```

```
   vpn-tunnel-protocol ikev2

tunnel-group <sse_dc_ip> type ipsec-l2l
tunnel-group <sse_dc_ip> general-attributes
  default-group-policy sse-policy
tunnel-group <sse_dc_ip> ipsec-attributes
  ikev2 remote-authentication pre-shared-key 0 \[Portal_Tunnel_Passphrase\]
  ikev2 local-authentication pre-shared-key 0 \[Portal_Tunnel_Passphrase\]
```

> **Note**
>
> Validate that the command crypto isakmp identity is set to the default value "**auto**" to determine the correct ID Method for ISAKMP Peers.

3. Configure IPsec proposal and profile parameters.
   - Define the settings according to the Supported IPsec parameters.

```
crypto ipsec ikev2 ipsec-proposal Secure-Access-Ipsec-Proposal
  protocol esp encryption aes-gcm-256
  protocol esp integrity sha-1

crypto ipsec profile Secure Access
  set ikev2 ipsec-proposal Secure Access-Ipsec-Proposal
  !
  !Note: below command applies for v9.17+ only
  set ikev2 local-identity email-id asav917a@6484741-576683214-sse.com
```

4. Create a virtual tunnel interface (VTI).
   - Enter the IP of a Secure Access data center.
   - Replace the Sample IP with any non-existing IP address that is not being used for a VLAN, subnet or existing VLAN connection in your network.

```
interface Tunnel1
   nameif vti
   ip address x.x.x.1 255.255.255.0 An unused range
   tunnel source interface outside
   tunnel destination<sse_dc_ip>
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile sse
```

5. Configure policy-based routing. In the following examples, the LAN subnet is `192.168.20.0/24` and the LAN interface is `GigabitEthernet1/2`.
   - Configure PBR to send the internal traffic through the tunnel interface to reach the Secure Access data center.
   - Set the IP address in `next-hop` to the same subnet assigned to the VTI.

What to do next

```
access-list ACL-sse line 1 extended permit ip 192.168.20.0 255.255.255.0 any4


route-map sse-PBR permit 10
  match ip address ACL-sse
  set ip next-hop x.x.x.2

interface GigabitEthernet1/2
  policy-route route-map sse-PBR
```

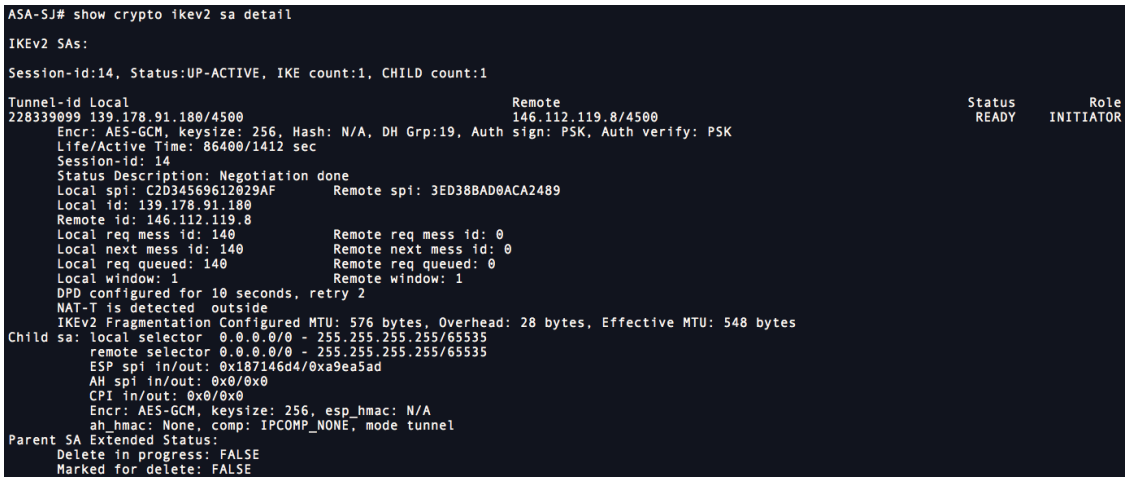
Test and Verify

Describes testing and verify. ASA CLI You can verify the ASA tunnel status to Secure Access by using these commands:

ASA CLI

You can verify the ASA tunnel status to Secure Access by using these commands:

```
show crypto ikev2 sa detail
show crypto ipsec sa detail
```



```
ASA-SJ# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:14, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                    Remote                                    Status         Role
228339099 139.178.91.180/4500                      146.112.119.8/4500                         READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:19, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1412 sec
      Session-id: 14
      Status Description: Negotiation done
      Local spi: C2D34569612029AF       Remote spi: 3ED38BAD0ACA2489
      Local id: 139.178.91.180
      Remote id: 146.112.119.8
      Local req mess id: 140            Remote req mess id: 0
      Local next mess id: 140           Remote next mess id: 0
      Local req queued: 140             Remote req queued: 0
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is detected  outside
      IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes, Effective MTU: 548 bytes
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x187146d4/0xa9ea5ad
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 256, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
Parent SA Extended Status:
      Delete in progress: FALSE
      Marked for delete: FALSE
```

```
ASA-SJ#  show crypto ipsec sa detail
interface: vti
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: 139.178.91.180

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 146.112.119.8


      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts invalid pad (rcv): 0,
      #pkts invalid ip version (rcv): 0,
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 139.178.91.180/4500, remote crypto endpt.: 146.112.119.8/4500
      path mtu 1500, ipsec overhead 63(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 0A9EA5AD
      current inbound spi : 187146D4

    inbound esp sas:
      spi: 0x187146D4 (410076884)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
         slot: 0, conn_id: 17, crypto-map: __vti-crypto-map-5-0-1
         sa timing: remaining key lifetime (kB/sec): (4331520/27282)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x0A9EA5AD (178169261)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
         slot: 0, conn_id: 17, crypto-map: __vti-crypto-map-5-0-1
         sa timing: remaining key lifetime (kB/sec): (4008960/27282)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Use the following command to simulate a packet from the inside interface, with a specific source IP address and port and a specific destination IP address and port. The response indicates whether the packet flows through the tunnel.

```
packet-tracer input inside tcp 192.168.20.13 3520 72.163.4.161 443 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f8d35d7da90, priority=1, domain=permit, deny=false
```

```
     hits=3848, user_data=0x0, cs_id=0x0, l3_type=0x8
     src mac=0000.0000.0000, mask=0000.0000.0000
     dst mac=0000.0000.0000, mask=0100.0000.0000
     input_ifc=inside, output_ifc=any

Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map sse-pbr permit 10
 match ip address pbr-sse
 set ip next-hop 11.11.11.12
Additional Information:
 Matched route-map sse-pbr, sequence 10, permit
 Found next-hop 11.11.11.12 using egress ifc vti

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f8d34b62c90, priority=0, domain=nat-per-session, deny=false
     hits=459, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0,
protocol=6
     src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
     dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
     input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f8d35d85db0, priority=0, domain=inspect-ip-options, deny=true
     hits=456, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
     src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
     dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
     input_ifc=inside, output_ifc=any



Phase: 5
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7f8d35dfabc0, priority=70, domain=encrypt, deny=false
     hits=152, user_data=0x78dc, cs_id=0x0, reverse, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
     dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
     input_ifc=any, output_ifc=vti

Phase: 6
Type: VPN
Subtype: ipsec-tunnel-flow
```

```
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x7f8d36c3cd90, priority=69, domain=ipsec-tunnel-flow, deny=false
     hits=152, user_data=0x84dc, cs_id=0x0, reverse, flags=0x0, protocol=0
     src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
     dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
     input_ifc=vti, output_ifc=any



Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x7f8d34b62c90, priority=0, domain=nat-per-session, deny=false
     hits=461, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0,
protocol=6
     src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
     dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
     input_ifc=any, output_ifc=any

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x7f8d35e547a0, priority=0, domain=inspect-ip-options, deny=true
     hits=291, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
     src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
     dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
     input_ifc=vti, output_ifc=any



Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 547, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_encrypt
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
```

```
snp_fp_ipsec_tunnel_flow
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat



Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: vti
output-status: up
output-line-status: up
Action: allow
```

Configure Tunnels with Catalyst SD-WAN cEdge and vEdge

Describes configuring tunnels with catalyst sd-wan cedge and vedge. Follow these steps to add a tunnel to connect a Cisco Catalyst SD-WAN (formerly known as Viptela) cEdge or vEdge device to Cisco Secure Access security services.

Follow these steps to add a tunnel to connect a Cisco Catalyst SD-WAN (formerly known as Viptela) cEdge or vEdge device to Cisco Secure Access security services.

For more information about Cisco Catalyst SD-WAN cEdge and vEdge devices and related topics, see Cisco's SD-WAN product documentation.

Configure Tunnel in Secure Access

Describes configuring tunnel in secure access. Before you configure the tunnel in the Cisco Catalyst SD-WAN (vManage) template for the device, add a network tunnel group to Secure Access. A tunnel group configuration includes: tunnel ID, tunnel passphrase, and optionally IP address ranges.

Before you configure the tunnel in the Cisco Catalyst SD-WAN (vManage) template for the device, add a network tunnel group to Secure Access. A tunnel group configuration includes: tunnel ID, tunnel passphrase, and optionally IP address ranges. When you add a network tunnel group, choose a tunnel ID and create a pre-shared key (PSK). Use the tunnel ID and passphrase to define the tunnel configuration in the feature template for the cEdge or vEdge device.

For more information, see Add Network Tunnel Group.

Prerequisites

- You must enable NAT in the feature template that faces the internet.
- You can access the Cisco Catalyst SD-WAN (vManage) console with a web browser. By default, the HTTPS port is 8443, but this may vary based on how your Cisco Catalyst SD-WAN (vManage) is configured.

> **Note**
>
> If you get a "Not Secure" warning when accessing the link, you can ignore it. When the Cisco Catalyst SD-WAN (vManage) login screen appears, enter your credentials.

Configure Cisco Catalyst SD-WAN Templates

Describes configuring cisco catalyst sd-wan templates. In Cisco Catalyst SD-WAN (vManage), all the features are configured through templates. Once the Cisco Catalyst SD-WAN cEdge or vEdge devices are registered with Cisco Catalyst SD-WAN (vManage), you cannot configure anything through the CLI.

In Cisco Catalyst SD-WAN (vManage), all the features are configured through templates. Once the Cisco Catalyst SD-WAN cEdge or vEdge devices are registered with Cisco Catalyst SD-WAN (vManage), you cannot configure anything through the CLI.

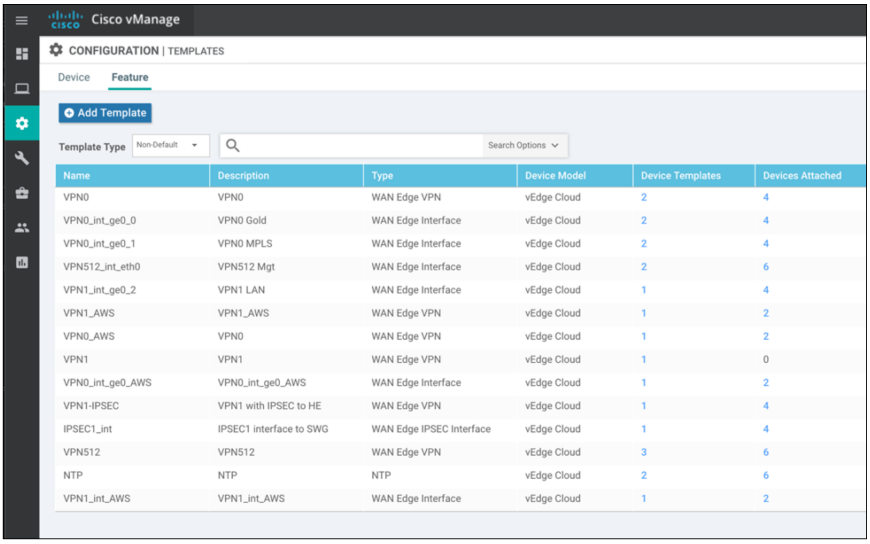
You can use the Cisco Catalyst SD-WAN (vManage) **Device** and **Feature** Templates to establish a tunnel from the device. First define the device template and then the feature template.

Define the Feature Template

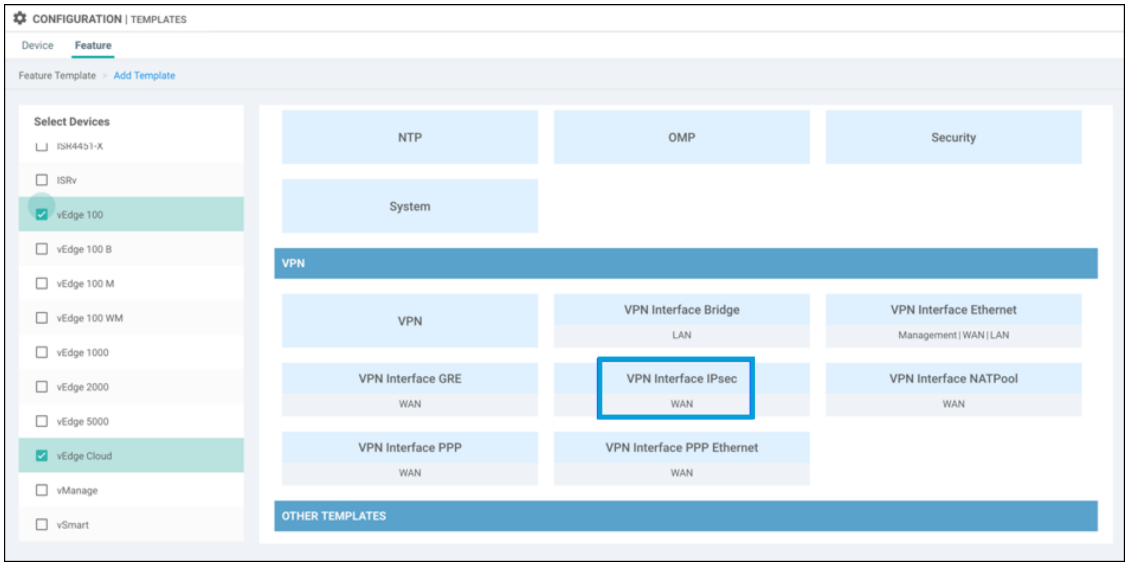
Provides instructions for defining the feature template. Log into the Cisco Catalyst SD-WAN (vManage) console and navigate to Configuration Templates .

Procedure

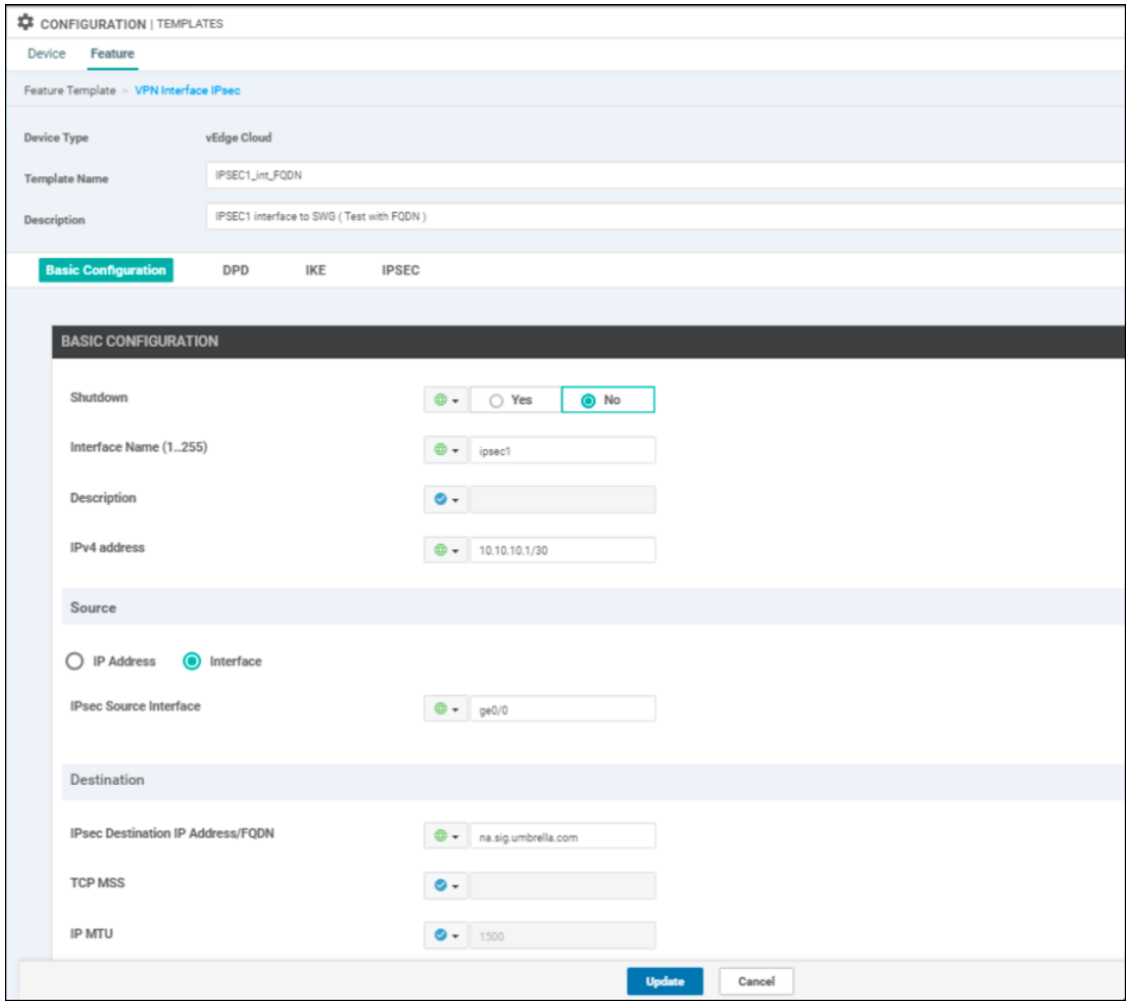
1. Log into the Cisco Catalyst SD-WAN (vManage) console and navigate to **Configuration** > **Templates**.
2. Confirm that the **Feature Templates** tab is selected, then click **Add Template**.



3. Under **Select Services** select device types, then choose **VPN Interface IPSec WAN**.



4. Configure Tunnel Parameters:
   a. Choose a template name and description for the Tunnel interface.
   b. Under **Basic Configuration**, set **Shutdown** to the global option and choose **NO**.
   c. Choose the **Interface Name** from 1 to 255. For example,`ipsec1`.
   d. Configure the IPv4 address by selecting the Global attribute and set the IP.
   e. Set the IPSec Source Interface to `ge0/0`. This must be the WAN interface in VPN 0, which has the internet connectivity.
   f. Set the IPSec Destination to the closest data center).

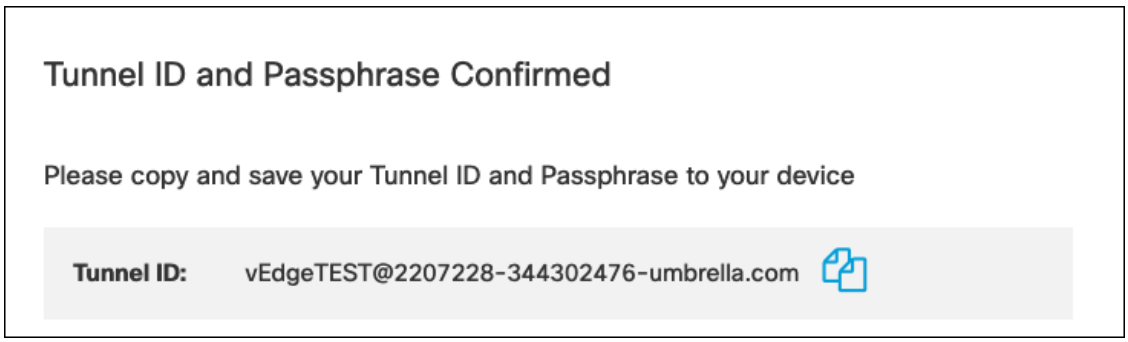


g. **Dead Peer Detection Value:** Leave this at the default setting unless you have a specific requirement otherwise.

5. Choose the **Global Attribute** to change any IKE and IPSec defaults:

IKE Settings

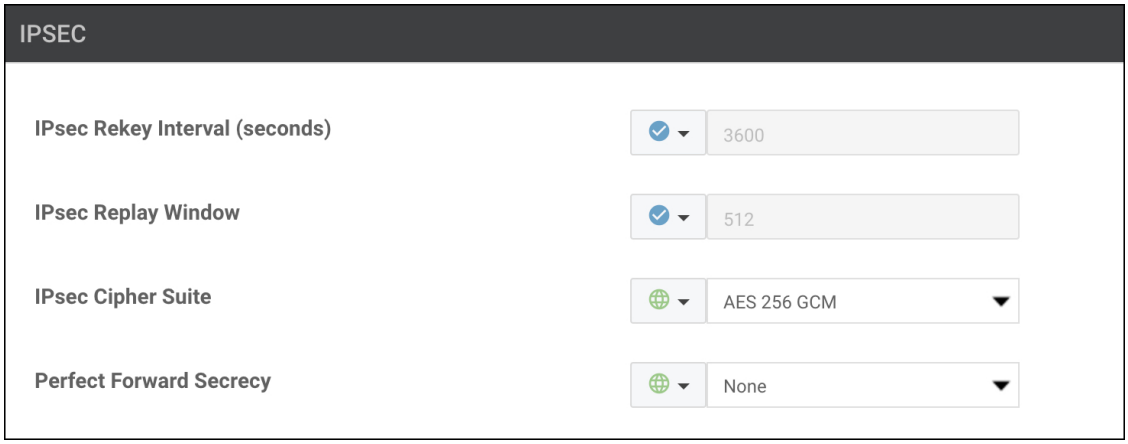
- Set the IKE Version to 2.
- Set the IKE Rekey Interval to 28800.
- Leave the default Cipher Suite, which is AES-256-CBC-SHA1.
- Set the IKE DH Group to 14 2048-bit Modulus.



IPsec Settings

- Leave the IPsec Rekey Interval & Replay Window values at their defaults.
- Use the default Cipher Suite `AES 256 GCM`.
- Set the Perfect Forward Secrecy value to "NONE".

> **Note**
>
> Cipher Suite Encryption
>
> If performance is an issue with the default cipher, both `AES 256 CBC SHA1` and `Null SHA1` are also supported. You can test these to determine whether one offers better performance for a particular platform. Note that `Null SHA1` isn't necessarily faster than the default `AES 256 GCM` because of the cost of the SHA1 hashing. In addition, `Null SHA1` is not recommended due to security concerns of unencrypted transport.



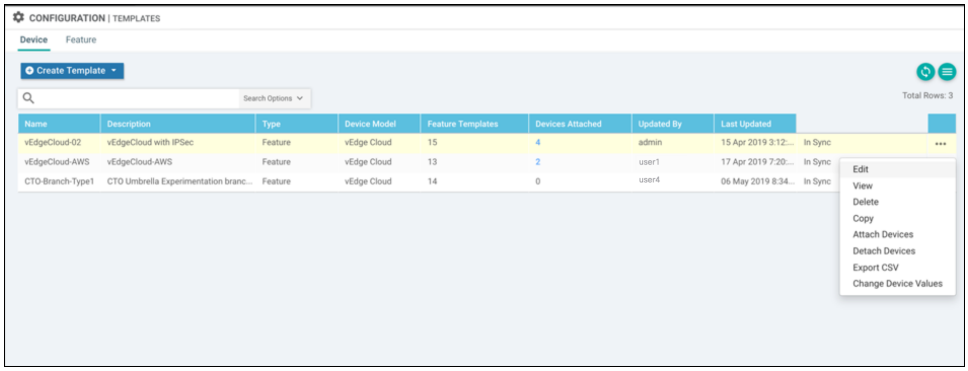
6. Click **Update** to save the configuration template.

Add the IPsec Interface Template

Provides instructions for adding the ipsec interface template. Navigate to Configuration Templates Device and then choose the device template for the CDFW tunnel.

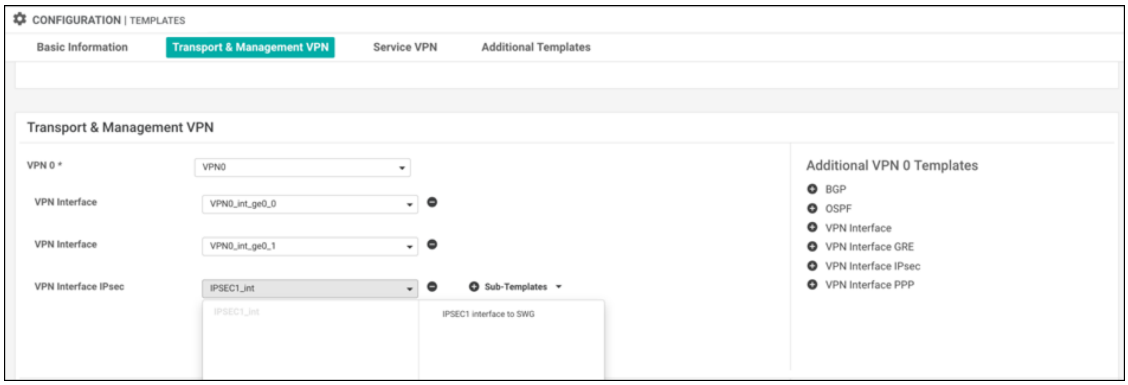
Procedure

1. Navigate to **Configuration** > **Templates** > **Device** and then choose the device template for the CDFW tunnel.
2. Select **Edit** from the rightmost dropdown menu.

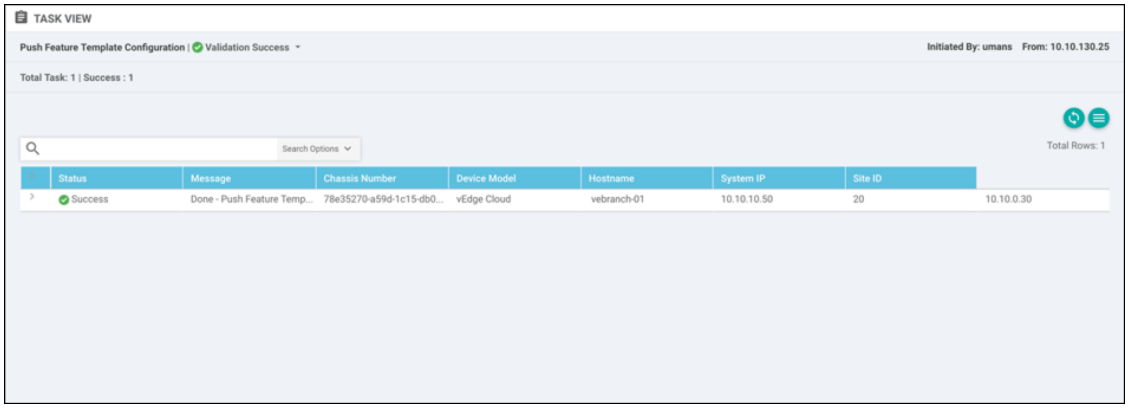


3. Add the VPN IPSec tunnel interface in the **VPN 0 Transport & Management VPN** section.

   Choose the VPN Interface IPSec that you added as part of the feature template.



4. Click **Update**. A success message appears.



Configure Static Routes

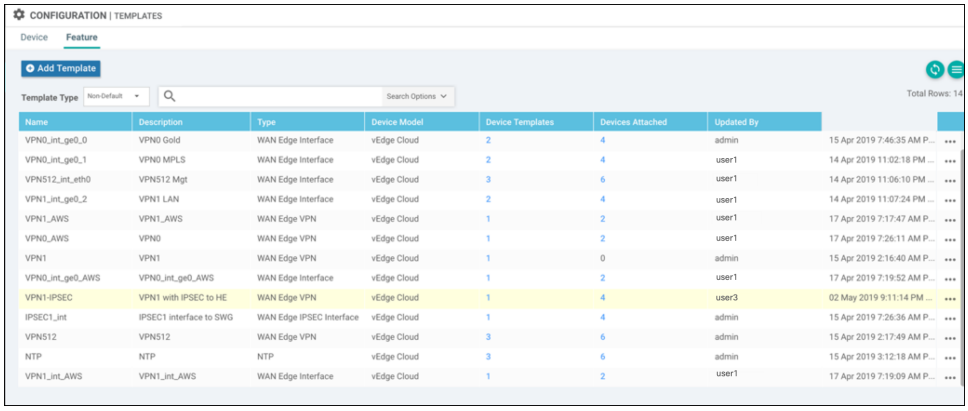
Provides instructions for configuring static routes. After configuring a template, you need to add static routes from the service VPN to redirect the traffic through the IPSec tunnel to CDFW headend.

After configuring a template, you need to add static routes from the service VPN to redirect the traffic through the IPSec tunnel to CDFW headend.

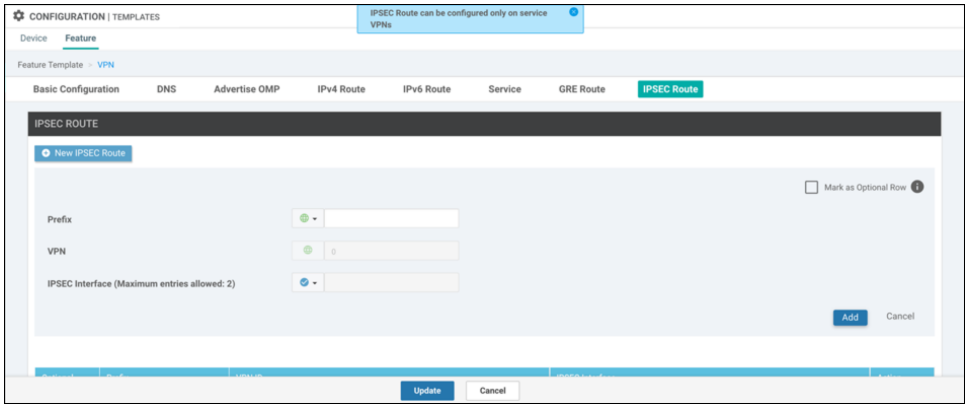
Procedure

---

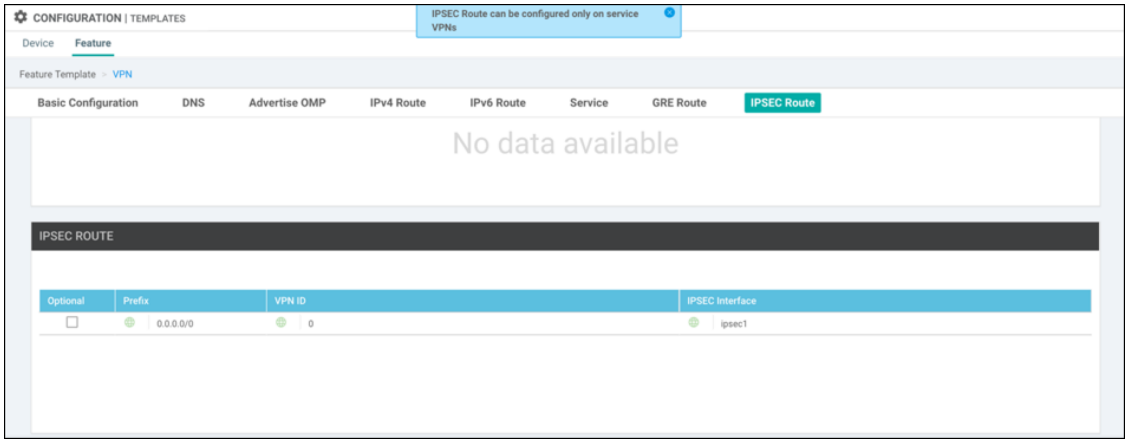
1. Navigate to **Configuration** > **Templates** > **Feature**.
2. Right-click the right most column, then edit the template to add *IPSec route 0.0.0.0/0 via IPSec1 Tunnel interface*.



3. Add one more IPsec Tunnel interface (for example, IPSec2), and set that as the secondary tunnel interface.



In this example, the default IPsec route is set to the **ipsec1** tunnel interface.



4. Save configuration changes.

Verify Tunnel Status

Provides instructions for verifying tunnel status. Log into the Cisco Catalyst SD-WAN (vManage) console and navigate to Monitor Network vEdge Device .

Procedure

---

1. Log into the Cisco Catalyst SD-WAN (vManage) console and navigate to **Monitor** > **Network** > **vEdge** > **Device**.

2. Choose a device, then choose **Interface** to check the status of the IPSec tunnel for **ipsec1**.

What to do next

Alternatively, the following is an example of checking the tunnel status through the CLI.

```
BR9-vEC1# show ipsec ike sessions | tab
                                                
```

11 Provision Users and Groups from Active Directory

Topics:

- Prerequisites for AD Connectors
- Connect Multiple Active Directory Domains
- Change the Connector Account Password
- Manage AD Components
- Manage AD Connectors
- AD Connector Communication Flow and Troubleshooting
- Connect Active Directory to Secure Access
- AD Integration with Virtual Appliances

Introduces provisioning users and groups from active directory. Provisioning users and groups from Active Directory (AD) requires a Cisco AD Connector deployment. The Cisco AD connector securely retrieves non-sensitive user and group information from the AD domain controller and communicates that information to Secure Access.

Provisioning users and groups from Active Directory (AD) requires a Cisco AD Connector deployment. The Cisco AD connector securely retrieves non-sensitive user and group information from the AD domain controller and communicates that information to Secure Access. Once your users and groups are integrated into Secure Access, you can create and enforce AD group-based access rules and view AD user-based reports.

Prerequisites for AD Connectors

Describes prerequisites for ad connectors. To integrate your organization's identities from Microsoft Active Directory (AD) with Cisco Secure Access, deploy the Cisco AD Connector in your environment.

To integrate your organization's identities from Microsoft Active Directory (AD) with Cisco Secure Access, deploy the Cisco AD Connector in your environment.

This guide describes the Windows Server, user account in the AD domain, and network requirements to deploy the AD Connector. You must meet these requirements before you deploy the AD Connector.

Connector Server

You must configure a server that is a member of the AD domain with the following environment:

- Windows Server 2012, 2012 R2, 2016, 2019, 2022, or 2025 with the latest service packs and 100MB free hard disk drive space.

> **Note**
>
> Windows Server Service packs prior to SP2 are not supported.

- .NET Framework 4.5 or above.
- If a local anti-virus application is running, allow the **CiscoAuditClient.exe** and **CiscoAuditService.exe** processes to run on the system.

You can deploy the AD Connector directly on the domain controller. In this case, the domain controller must meet all prerequisites for the Connector server. Only one AD Connector is required to provision identities from an AD domain. If you require high-availability of the AD Connector, deploy a second AD Connector.

Outbound Network Access to Secure Access

The server where you install the AD Connector requires outbound access on certain domains and URLs. If you are using a transparent HTTP web proxy, ensure that these domains and URLs on port 80/443 are excluded from the proxy, and not subject to authentication.

- For syncing, allow traffic on 443 (TCP) to **devices.api.secureaccessfed.cisco**.
- For Windows to perform Certificate Revocation List and Code-Signing checks, allow access to additional URLs on port 80/443 (TCP). For a complete list of ports, see AD Connector Communication Flow and Troubleshooting.

Connector Account

To deploy the AD Connector, create a new user account in the AD domain. This account should have:

- The logon name (**sAMAccountName**) set to **Cisco_Connector**. You can use a custom username, but you must configure it with the required permissions.
- Select **Password never expires**.

> **Note**
>
> Passwords can not include backslashes, quotations (single or double), greater-than or less-than chevron brackets (**< >**), or colons.

- Assign **Read** and **Replicating Directory Changes** permissions. Alternatively, you can make the AD Connector account a member of the built-in **Enterprise Read-only Domain Controllers** group, which will automatically assign these permissions.
  - The AD Connector does an initial synchronization of the AD structure to Secure Access. After this, it detects changes to the AD structure and communicates these changes only. The detection of changes requires the **Replicating Directory Changes** permission. The AD Connector cannot function without this permission.
  - The **Replicating Directory Changes** permission is different from the **Replicating Directory Changes All** permission, which enables the retrieval of password hashes. The AD Connector does not read password hashes. Thus, the AD Connector does not require the **Replicating Directory Changes All** permission.

Connect Multiple Active Directory Domains

Describes connecting multiple active directory domains. To import users and groups from multiple Active Directory (AD) domains or multiple AD forests, register a domain controller or domain in Cisco Secure Access for each AD domain that needs to integrate with Secure Access.

To import users and groups from multiple Active Directory (AD) domains or multiple AD forests, register a domain controller or domain in Cisco Secure Access for each AD domain that needs to integrate with Secure Access. We recommend that you deploy a separate Cisco AD Connector for each AD domain. For more information, see Connect Active Directory to Secure Access.

If you wish to use the same Cisco AD Connector to provision users and groups from multiple AD domains, ensure that the connector account is created with the same **sAMAccountName** name and password across all of your domains. This feature is not enabled by default. Contact Support to have the feature enabled. For more information, see Contact Cisco Secure Access Support.

> **Note**
>
> If you have groups in an AD domain that have member users in another AD domain, Secure Access requires that you deploy a single Cisco AD Connector for multiple AD domains.

Change the Connector Account Password

Provides instructions for changing the connector account password. Administrative privileges on the user device. Install and set up the Cisco AD Connector on a server in your organization. For more information, see Connect Active Directory to Secure Access.

- Administrative privileges on the user device.
- Install and set up the Cisco AD Connector on a server in your organization. For more information, see Connect Active Directory to Secure Access.

For regulatory compliance, you may need to change the password of the Cisco Active Directory (AD) Connector account. You can modify this password without impacting the functionality of the Cisco AD Connector.

Changing the password on the Cisco AD Connector ensures that the AD connector can communicate with Microsoft AD using the new credentials. If the AD Connector account password is not correct, the Cisco AD Connector is unable to subscribe to login events and AD changes. If the password is not changed, Secure Access can not identify DNS requests with the AD users or groups accurately, and can not sync user and group changes from AD.

Procedure

1. Sign in to the account from any system that is a member of the domain and then set the new password.
2. Stop the **Cisco AD Connector** service.
3. Navigate to `C:\Program Files (x86)\Cisco\Cisco AD Connector` and run the file `CiscoPasswordManager.exe`. If you see any errors, you may need to run this utility as an administrator.
4. When prompted, add your new password.
5. Start the **Cisco AD Connector** service.
6. Repeat steps 2 and 3 for each deployed Cisco AD Connector.

Manage AD Components

Describes managing ad components. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft AD. After you add the AD Connector and the AD components–AD domain controllers and AD domains–in your environment, you can manage these AD components in Secure Access.

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft AD. After you add the AD Connector and the AD components–AD domain controllers and AD domains–in your environment, you can manage these AD components in Secure Access.

This guide describes how to add, remove, and view AD components, and manage Sites for your deployed AD components.

- Add AD Components in Secure Access
- Manage Sites for AD Components
- View AD Components in Secure Access
- Delete AD Components

Add AD Components in Secure Access

Describes adding ad components in secure access. The integration of Active Directory (AD) with Cisco Secure Access requires that you add either AD domains or domain controllers in the organization's environment and register these AD components in Secure Access.

The integration of Active Directory (AD) with Cisco Secure Access requires that you add either AD domains or domain controllers in the organization's environment and register these AD components in Secure Access.

This guide describes the steps to add domain controllers or domains in Secure Access and configure the communications between the AD components and the Cisco AD Connector.

Support for Multiple AD Domains and AD Forests

To integrate multiple AD domains or AD forests with Secure Access through integrations with domain controllers, deploy an AD Connector (with an additional AD Connector for redundancy) for each AD domain that integrates with Secure Access.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

Add your AD domain controllers or domains to Secure Access. After you add the AD components you can view them in Secure Access.

- Verify Auditing of Logon Events on Domain Controllers
- Download the Windows Configuration Script for Domain Controllers
- Run the Windows Configuration Script for the Domain Controllers
- Add a Domain Controller in Secure Access
- Add a Domain in Secure Access

Verify Auditing of Logon Events on Domain Controllers

Describes verifying auditing of logon events on domain controllers. The AD integration with domain controllers requires each domain controller to audit logon events.

The AD integration with domain controllers requires each domain controller to audit logon events.

On each domain controller (excluding read-only domain controllers), enable the **Audit account logon events** to include `Success` and `Failure` if it is set to `No Auditing`.

By default, this group policy is set to log `Success` logon events and you should not modify it. Secure Access requires the **Audit account logon events** setting so that it knows whether a user has logged in successfully and can then compare that login to subsequent events generated by that user.

If the Audit Policy is not set, the **Windows Configuration Script for Domain Controller** script displays this error message:

```
"ERROR: "

------------------------------------------------------------------------


Your Group Policy for this Domain Controller is set to NOT audit successful
logon events!

You MUST edit the following Group Policy for all DCs:


Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit logon events


Define that policy to audit Success attempts, gpupdate, and re-run this script!
```

Download the Windows Configuration Script for Domain Controllers

Provides instructions for downloading the windows configuration script for domain controllers. The Windows Configuration Script automates the permissions for the Cisco_Connector user.

The Windows Configuration Script automates the permissions for the **Cisco_Connector** user.

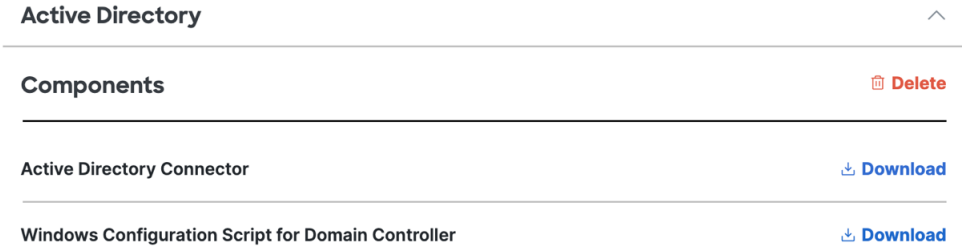
In Secure Access, download the `Windows Configuration Script for Domain Controller` script to the domain controllers in your environments.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users**, click **Configuration Management** > **Integrate directories**, and then click **Active Directory**.
2. After an initial AD deployment, navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users**, click **Configuration Management**, and expand **Active Directory**.
3. For **Windows Configuration Script for Domain Controller**, click **Download**.



4. Download and save the configuration script to a location on the machine where you plan to run it.

> **Note**
>
> The configuration script is written in Visual Basic Script and is in plain text.

Run the Windows Configuration Script for the Domain Controllers

Provides instructions for running the windows configuration script for the domain controllers. Run the Windows Configuration Script for Domain Controller on all of the domain controllers at each site, (excluding read-only domain controllers (RODCs)) for each domain that will integrate with Secure Access.

Run the **Windows Configuration Script for Domain Controller** on all of the domain controllers at each site, (excluding read-only domain controllers (RODCs)) for each domain that will integrate with Secure Access. The configuration script prepares the domain controllers to communicate with the AD Connector.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

1. As an administrator, open an elevated command prompt.

Before running the script, you must create the **Cisco_Connector** user. Also, there are several Group Policies that affect system operation that may need manual configuration. The script displays the status of these settings and, if needed, provides instructions on how to change them.

2. Locate the `Windows Configuration Script for Domain Controller` file and run the script in the command prompt.
3. Substitute the Windows configuration script filename (including the `.wsf` file extension) in the **cscript** command.

```
cscript forcenonva=true <Windows Configuration Script filename with extension>
 or cscript forcenonva=true <Windows Configuration Script filename with
extension> --username <sAMAccountName for custom user>
```

Important

The script displays your current configuration, then offers to auto-configure the domain controller. If the auto-configure steps are successful, the script offers to registers the domain controller with Secure Access. Registration only occurs if you accept this offer.

Repeat the steps to add your domain controllers in Secure Access. It is essential that each domain controller in each AD domain environment has the configuration script run on it in order for the service to work as expected, both for high availability and overall reliability.

Note

The configuration script is not an application or service. If you change the IP address or hostname of the domain controller, remove the previous instance of the domain controller and re-register the domain controller.

Add a Domain Controller in Secure Access

Provides instructions for adding a domain controller in secure access. Choose the domain controller component type and set up the domain controller to sync with Secure Access.

Choose the domain controller component type and set up the domain controller to sync with Secure Access.

For LDAP or LDAPS AD queries, AD integration requires that you register an AD domain controller or AD domain in Secure Access. The Cisco AD Connector performs an LDAP sync against this domain controller or domain to retrieve the Users and Groups. The Cisco AD Connector server communicates with the domain controller on port 389 over TCP for LDAP sync or port 636 over SSL for LDAP.

The Cisco AD Connector can only retrieve users and groups from a single domain controller. If you register multiple domain controllers in Secure Access, the Cisco AD Connector only attempts to perform an LDAP sync against the first domain controller in the list. Ensure that the domain controller you are registering is not subject to any AD replication delays. Read-only Domain Controller (RODC) registrations are supported for retrieval of users and groups.

If you need to periodically bring down your domain controller for maintenance or updates or your domain controllers are behind a load balancer that does not support LDAP queries, we recommend that you register the domain instead.

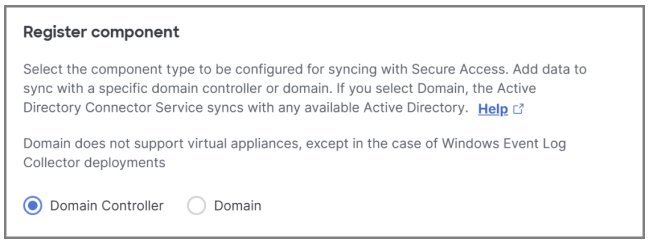
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

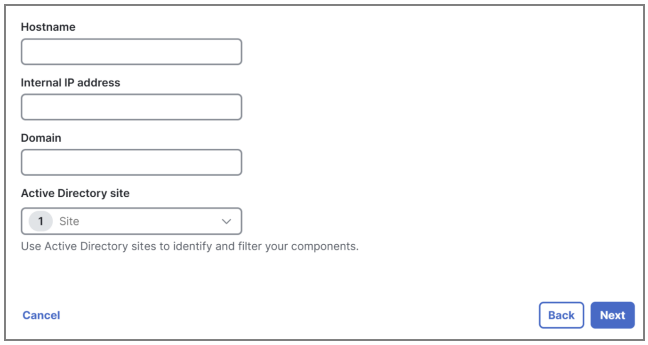
Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users**, click **Configuration Management** > **Integrate directories**, and then click **Active Directory**.
2. Click **Next**, and then choose **Domain Controller**.

   Register the domain controller with Secure Access.



3. Enter the details for the domain controller.
   - **Hostname**–The hostname of the server where the domain controller is deployed.
   - **Internal IP address**–The private IP address of the server where the domain controller is deployed. This field becomes available based on the IP version selection.
   - **Domain**–The domain where the domain controller receives the events.
4. For **Active Directory site**, choose a Site to associate with the domain controller.



5. Click **Next**, and then follow the instructions to install the AD Connector.

Add a Domain in Secure Access

Provides instructions for adding a domain in secure access. Full Admin user role. For more information, see Manage Accounts. For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

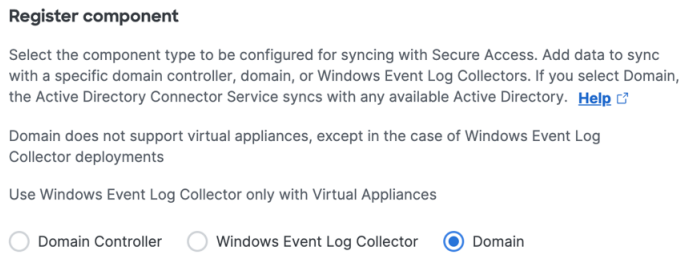
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

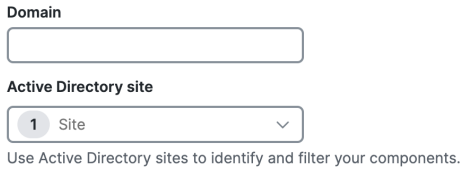
Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users**, click **Configuration Management** > **Integrate directories**, and then click **Active Directory**.

2. Click **Next**, and then choose **Domain**.Register the AD domain with Secure Access.



3. For **Domain**, enter the domain name.
4. For **Active Directory site**, choose a Site to associate with the AD domain.



5. Click **Next**, and then follow the instructions to install the Cisco AD Connector.

Manage Sites for AD Components

Provides instructions for managing sites for ad components. The Cisco Active Directory (AD) Connector and the organization's AD domains and domain controllers integrate Cisco Secure Access with your instance of Microsoft AD.

The Cisco Active Directory (AD) Connector and the organization's AD domains and domain controllers integrate Cisco Secure Access with your instance of Microsoft AD. After you add an AD component in Secure Access, you can select a Secure Access Site for the AD Component.

This guide describes how to manage your Secure Access Sites for the deployed AD components in your organization.

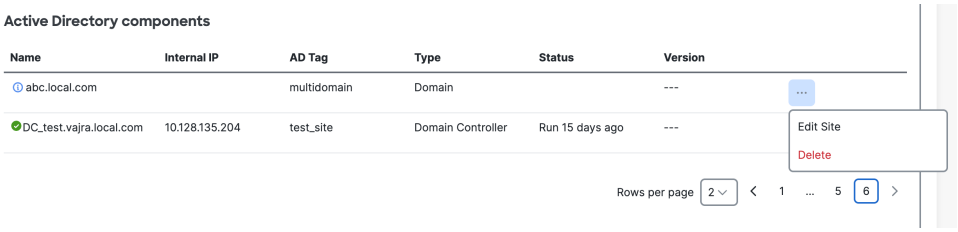
Manage a Site for an AD component that is deployed in your on-premises environment.

Before you begin

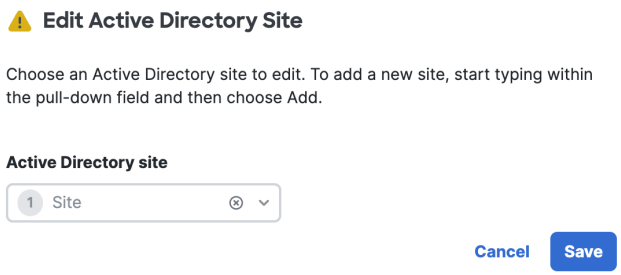
- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, click **Configuration management**, and then expand **Active Directory**.
2. For **Active Directory components**, locate an installed AD component, and then click the ellipsis (**...**).
3. Click **Edit Site**.



4. Choose a Site for the AD component, and then click **Save**.



View AD Components in Secure Access

Provides instructions for viewing ad components in secure access. The integration of Active Directory (AD) with Cisco Secure Access requires that you add the organization's AD components on Secure Access and integrate a Cisco AD Connector. Once these AD components are added, you can view them in Secure Access.

The integration of Active Directory (AD) with Cisco Secure Access requires that you add the organization's AD components on Secure Access and integrate a Cisco AD Connector. Once these AD components are added, you can view them in Secure Access. You can also view the AD Connector deployments in Secure Access.

This guide describes how to view the AD components that you registered with Secure Access and the AD Connectors, which you deployed in your environments.

In Secure Access, view the AD components and AD Connectors that you deployed.

It can take up to four hours for large numbers of AD user and group objects to synchronize for the first time.

Seeing your groups listed means the domain controllers have automatically synchronized user and computer group memberships with Secure Access through the AD Connector successfully. Any subsequent changes should also sync successfully.

> **Note**
>
> If the AD Connector does not appear in Secure Access and you have met the network requirements, check that the AD Connector server is not missing the DigiCert CA. If a certificate error is presented, download and install the latest DigiCert Global Root CA from DigiCert and restart the Cisco Active Directory Service. If it does not appear, contact Cisco Secure Access Support.

Before you begin

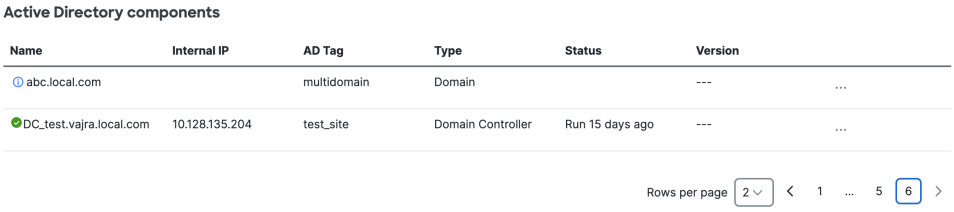
- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connectors.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, click **Configuration management**, and then expand **Active Directory**.



2. For **Active Directory components**, view the properties of the installed AD components.
   - **Name**–The hostname of the Windows computer where you installed the AD Component.
   - **Internal IP**–The internal IP address of the AD component.
   - **AD Tag**–The unique label that identifies the Site associated with the AD component.
   - **Type**–The type of AD component, either **Domain Controller**, **Domain**, or **AD Connector**.
   - **Status**–The state of the AD component.
   - **Version**–The version of the AD component.



Delete AD Components

Describes deleting ad components. After you register the Active Directory (AD) components in Secure Access, you can delete a single AD component or remove all AD components for the organization.

After you register the Active Directory (AD) components in Secure Access, you can delete a single AD component or remove all AD components for the organization. When the AD components (Cisco AD Connector, and AD domain or domain controller) are deleted, you can no longer protect and monitor the users and groups in the organization that you provisioned from AD.

This guide describes the steps to remove a single AD component that you added to Secure Access or the integration of AD (all AD components) with Secure Access.

Remove a single AD component for the organization or delete all AD components that you registered with Secure Access.

- Delete an AD Component
- Remove All AD Components

Delete an AD Component

Provides instructions for deleting an ad component. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

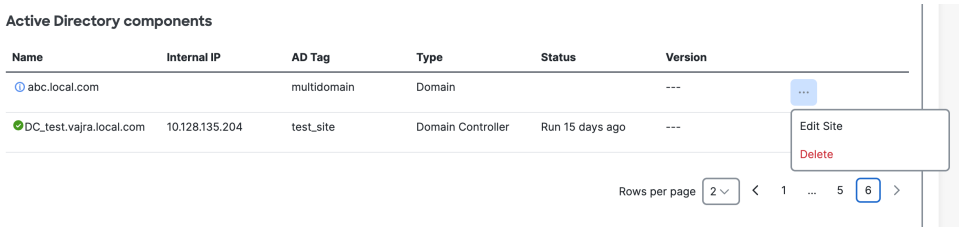
Delete a single AD component that was added in Secure Access.

Before you begin

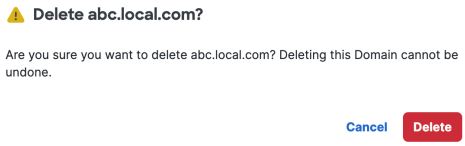
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, click **Configuration management**, and then expand **Active Directory**.
2. For **Active Directory components**, locate an installed AD component, and then click the ellipsis (**...**).
3. Click **Delete**.



4. Click **Delete** to confirm the removal of the AD component in Secure Access.



Remove All AD Components

Provides instructions for removing all ad components. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

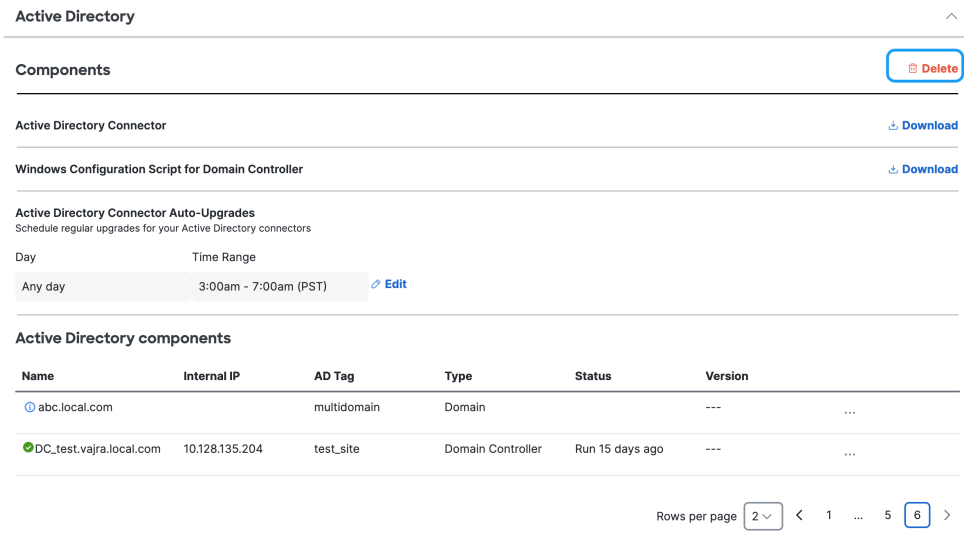
Remove all AD components for the organization in Secure Access.

Before you begin

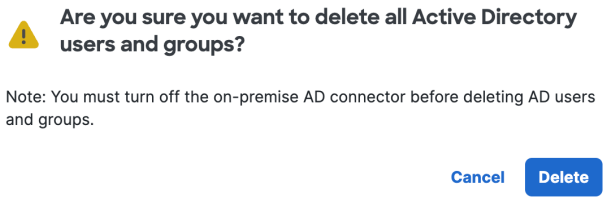
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, click **Configuration management**, and then expand **Active Directory**.
2. For **Active Directory components**, click **Delete**.



3. Click **Delete**, to confirm the removal of all registered AD components in Secure Access and remove the users and groups that were provisioned for AD.



Manage AD Connectors

Describes managing ad connectors. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft Active Directory (AD).

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft Active Directory (AD). Before you can provision users, groups, and endpoint devices from AD to Secure Access, complete the setup of the AD components, register the AD Components in Secure Access, and install the Cisco AD Connector in the organization's environment.

How to Connect Active Directory to Secure Access

The deployment of the AD Connector has various components and configuration settings. You can configure the Cisco AD Connector to provision users and groups from Microsoft AD using LDAP or LDAPS (domain controller or domain), or LDAP Interchange Format (LDIF) source files.

1. Add domain controllers or domains in Secure Access for LDAP or LDAPS deployments. For more information, see Add AD Components to Secure Access.
2. (Optional) Configure authentication for the AD Connectors in your environment. For more information, see Configure Authentication for AD Connectors and VAs.
3. (Optional) Configure updates for the AD Connectors in your environment. For more information, see Configure Updates on AD Connectors.
4. Download the AD Connector software package and install it on your AD server. For more information, see Connect Active Directory to Secure Access.

5. (Optional) Configure the provisioning of users, groups, and endpoint devices with LDIF source files. For more information, see Deploy LDIF Files for AD Connector.
6. (Optional) Change the AD Connector account password. For more information, see Change the Connector Account Password.
7. View the installed AD components in Secure Access and verify that users and groups begin to sync with Secure Access. For more information, see View AD Components in Secure Access.

Configure Authentication for AD Connectors and VAs

Describes configuring authentication for ad connectors and vas. Cisco Secure Access communicates with the deployed Cisco Active Directory (AD) Connectors in your environments. Secure Access makes software syncs and health checks to the AD Connectors and requires that API requests from the AD Connectors use authentication.

Cisco Secure Access communicates with the deployed Cisco Active Directory (AD) Connectors in your environments. Secure Access makes software syncs and health checks to the AD Connectors and requires that API requests from the AD Connectors use authentication. For information about deploying the Cisco AD Connector, see Connect Active Directory to Secure Access.

To manage the authentication of the communications from the AD Connectors to Secure Access, we recommend that you configure API key credentials for your AD Connector deployments. Your API key credentials apply to all AD Connectors and Secure Access Virtual Appliances that are deployed in your environment.

For more information about authentication and deploying Virtual Appliances, see Configure Authentication for Virtual Appliances.

> **Note**
>
> The API key authentication is available for Secure Access Virtual Appliances version 3.7.0 and newer and the Cisco AD Connector version 1.14.4 or newer. The API keys apply to the Virtual Appliances and the Cisco AD Connectors in the organization.

How to Set Up Your API Credentials

Describes how to set up your api credentials. Create a Secure Access Key Admin API key and secret. Then, use the Secure Access Key Admin API credentials to generate your Secure Access client API key credentials.

Create a Secure Access Key Admin API key and secret. Then, use the Secure Access Key Admin API credentials to generate your Secure Access client API key credentials.

The Secure Access client API key and secret are stored in the AD Connectors that you deploy in your environments. The generated API credentials (key and secret) apply to all AD Connectors in the organization.

AD Connectors use the organization's Secure Access client API key credentials to generate an OAuth 2.0 access token, which authorizes API requests from the AD Connectors to Secure Access. The access token is included in every API request from the AD Connector to Secure Access.

Important

Secure Access client API key credentials are valid for 90 days.

- Step 1 – Create the Key Admin API Key Credentials
- Step 2 – Add the Key Admin API Key Credentials

Step 1 – Create the Key Admin API Key Credentials

Provides instructions for step 1 – create the key admin api key credentials. Full Admin user role. For more information, see Manage Accounts. Cisco AD Connector version 1.14.4 or newer.

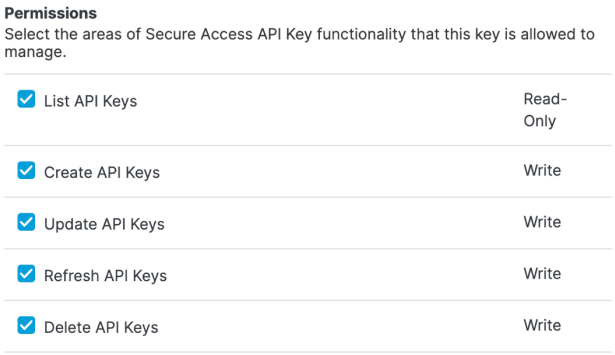
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Create a Secure Access Key Admin API key. For more information, see Add Key Admin API Keys.
2. Select each type of permission for the key.

> **Note**
>
> Save your Key Admin API key and secret and use these credentials to configure the authentication for the AD Connectors in the organization.



Step 2 – Add the Key Admin API Key Credentials

Provides instructions for step 2 – add the key admin api key credentials. Add the Secure Access Key Admin API key and secret to the AD Connector in Users, Groups, and Endpoint Devices Configuration Management API Authentication . Then, generate a Secure Access client API key and secret.

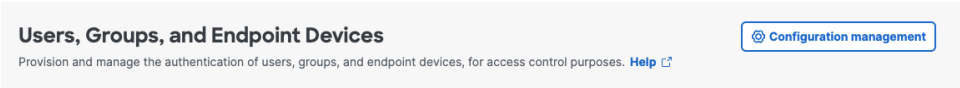
Add the Secure Access Key Admin API key and secret to the AD Connector in **Users, Groups, and Endpoint Devices** > **Configuration Management** > **API Authentication**. Then, generate a Secure Access client API key and secret.

Before you begin

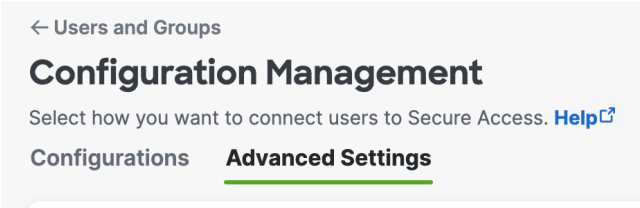
- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and then click **Configuration management**.

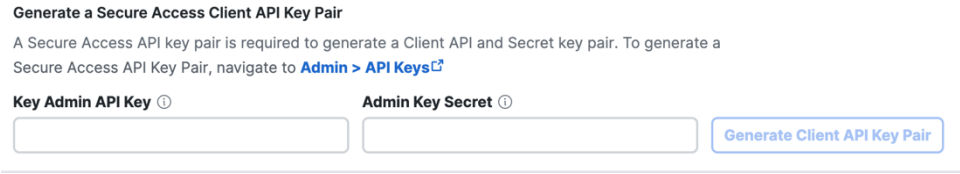


2. Click **Advanced Settings**.



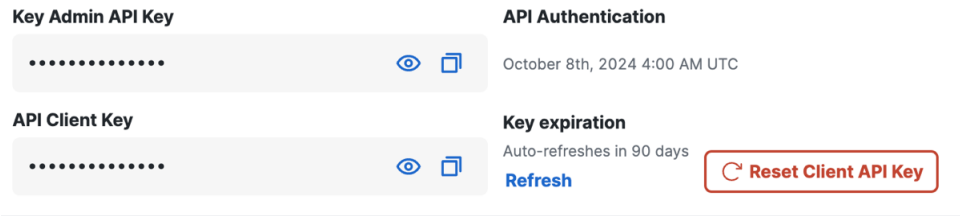
3. For **Key Admin API Key**, add the Key Admin API key, and for **Key Admin Key Secret**, add the Key Admin API key secret.

   For information about creating the Key Admin API key, see Step 1 - Create the Key Admin API Key Credentials.



4. After you add the Key Admin API key and secret, click **Generate Client API Key Pair**.
5. Save the Secure Access client API key and secret.

   Secure Access updates the client API key and secret automatically every 90 days.



Refresh Client API Key and Secret

Provides instructions for refresh client api key and secret. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

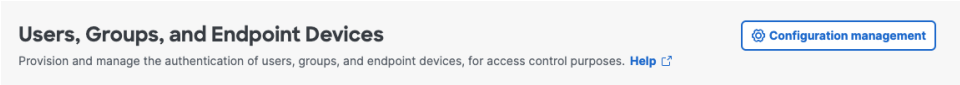
Refresh your Secure Access client API key and secret.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

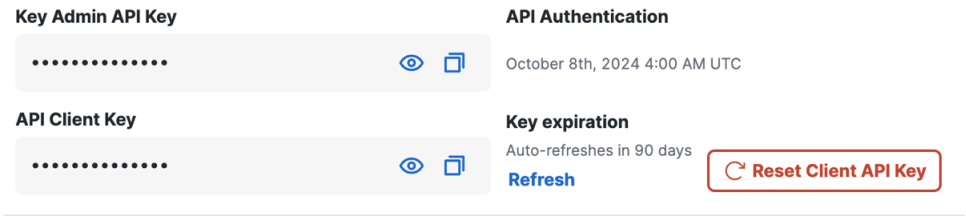
Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and then click **Configuration management**.

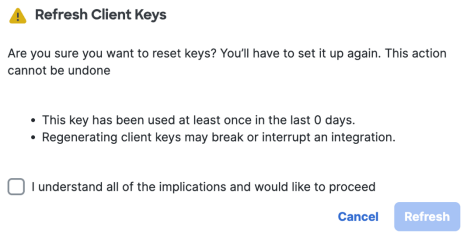


2. Click **Advanced Settings**.

3. Click **Refresh**.
   Secure Access refreshes the client API key and secret.



4. For **Refresh Client Keys**, check the box to confirm the deletion of the client API key and secret.



5. Click **Refresh**.

Reset Client API Key

Provides instructions for resetting client api key. Delete your Secure Access Key Admin API key and Secure Access client API key.

Delete your Secure Access Key Admin API key and Secure Access client API key.

Important

After you delete the Key Admin API key and client API key, existing AD Connector deployments may continue to use the stored Secure Access client API key and secret for up to 90 days.

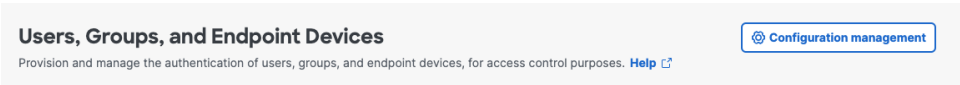
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

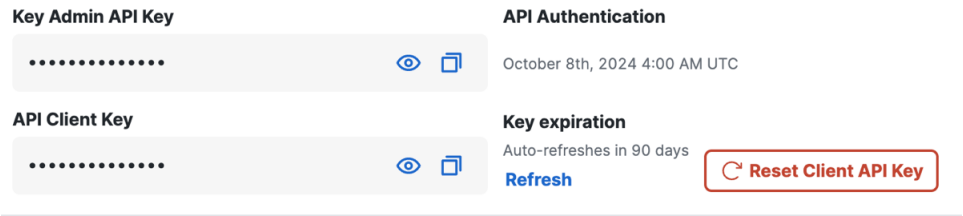
Procedure

---

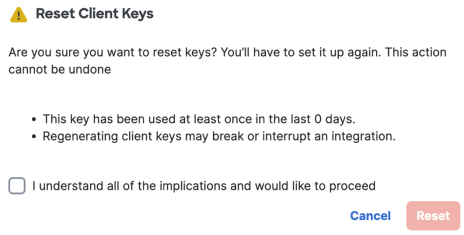
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and then click **Configuration management**.



2. Click **Advanced Settings**.
3. Click **Reset Client API Key**.



4. For **Reset Client Keys**, check the box to confirm the deletion of both the Key Admin API key and client API key for the AD Connectors in the organization.



5. Click **Reset**.

Configure Updates on AD Connectors

Provides instructions for configuring updates on ad connectors. You can schedule the date and time that Cisco Secure Access updates the Active Directory (AD) Connector software on your deployed Cisco AD Connectors. When scheduled, Secure Access checks if an AD Connector has the latest version of the software.

You can schedule the date and time that Cisco Secure Access updates the Active Directory (AD) Connector software on your deployed Cisco AD Connectors. When scheduled, Secure Access checks if an AD Connector has the latest version of the software.

If a new version is available, Secure Access removes the installed AD Connector software from your systems and deploys the latest version of the AD Connector.

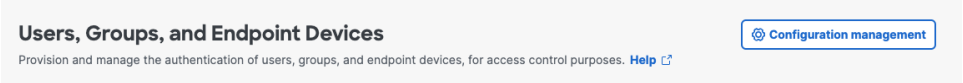
Select the day and time to update your deployed AD Connectors automatically.

Before you begin

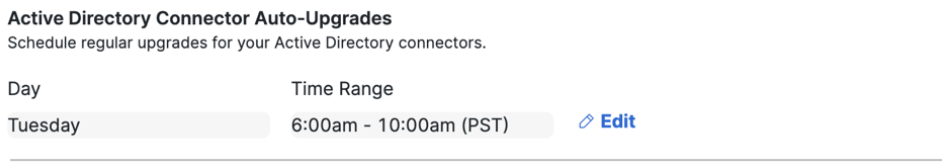
- Full Admin user role. For more information, see Manage Accounts.
- Deploy an AD Connector in your environment. For more information, see Connect Active Directory to Secure Access.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and then click **Configuration management**.

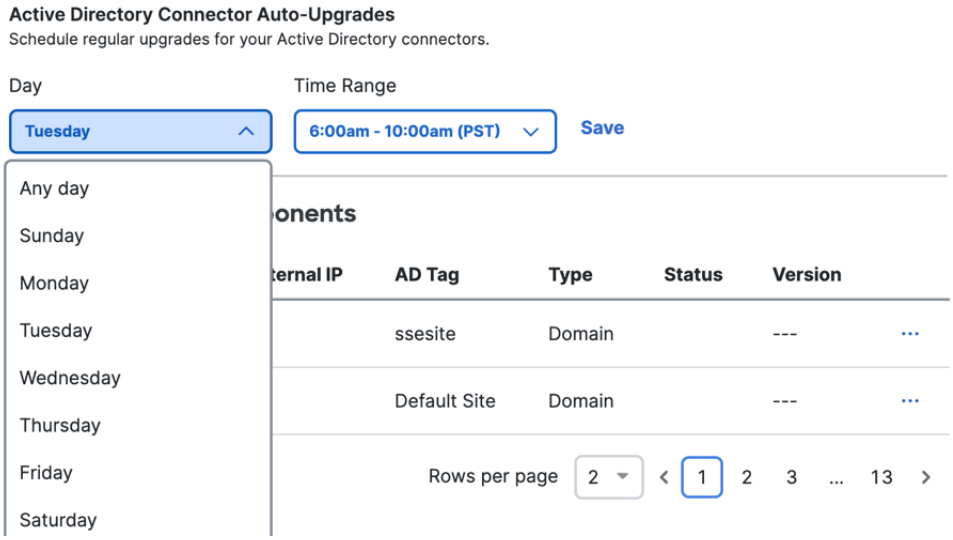


2. For **Provisioning**, expand **Active Directory**.
3. Navigate to **Active Directory Connector Auto-Upgrades**, and then click **Edit**.



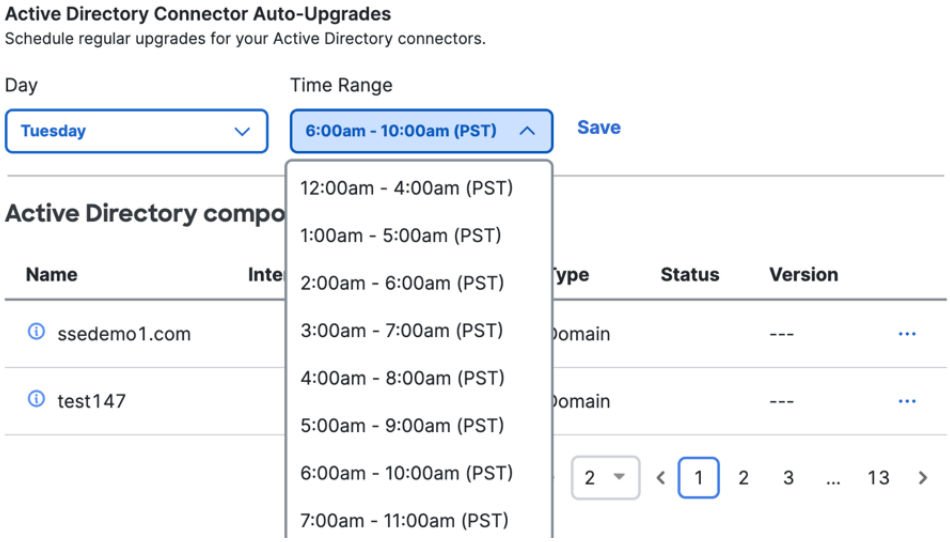
4. For **Day**, choose the day of the week to update the AD Connector software.

> **Note**
>
> The default **Day** is **Any day**–On every day of the week, if a software update is available, Secure Access attempts to redeploy the AD Connectors with the latest version of the software.



5. For **Time Range**, choose the four-hour time period to update the AD Connectors on the scheduled day.

> **Note**
>
> The default **Time Range** is **2:00 am - 6:00 am PST**.



6. Click **Save**.

Connect Active Directory to Secure Access

Describes connecting active directory to secure access. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft Active Directory (AD).

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft Active Directory (AD). Before you can provision users, groups, and endpoint devices from AD to Secure Access, register the AD Components in the environment (domain controller or domain) to Secure Access. Then, download the Cisco AD Connector software package and install the AD Connector in the organization's environment.

This guide describes the steps to install the Cisco AD Connector for LDAP or LDAPS, and provision users and groups from your instance of Microsoft AD to Secure Access.

Step 1 – Download the Active Directory Connector

Provides instructions for step 1 - download the active directory connector. Download the Cisco AD Connector from Secure Access to your server.

Download the Cisco AD Connector from Secure Access to your server.

Note

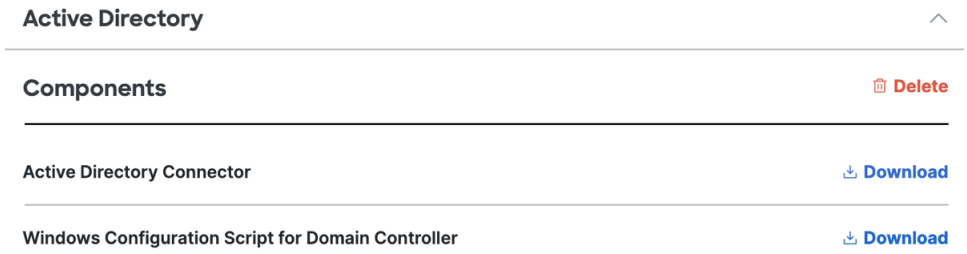
When you download the Cisco AD Connector software package, and if you did not configure API key credentials for the AD Connectors, Secure Access displays a warning message. We recommend that you configure API keys for your AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Set up the AD Connector server, user account, and environment for deploying the AD Connector. For more information, see Prerequisites for AD Connectors.
- Add the AD components in Secure Access. For more information, see Add AD Components in Secure Access.
- (Optional) Configure Authentication for AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.
- (Optional) Configure software updates on the AD Connector. For more information, see Configure Updates on AD Connectors.

Procedure

1. Configure a server to run the Cisco AD Connector, and then sign in to Secure Access on that server.
2. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and then click **Configuration management**.
3. Under **Directories**, expand **Active Directory**.
4. For **Active Directory Connector**, click **Download** to save the Cisco AD connector software package to the server. The deployment package is named: `CiscoAuditClient_vX.X.X.zip`.



Note

You must download the ZIP file to the local machine where you plan to run it, or copy it locally from another machine. We do not recommend that you install the Cisco AD Connector from a network drive or run the `setup.msi` directly from the compressed file.

Step 2 - Install the Active Directory Connector

Provides instructions for step 2 - install the active directory connector. As an administrator, extract the contents of the Cisco AD Connector ZIP file to a folder on the server, and then navigate to that folder.

As an administrator, extract the contents of the Cisco AD Connector ZIP file to a folder on the server, and then navigate to that folder.

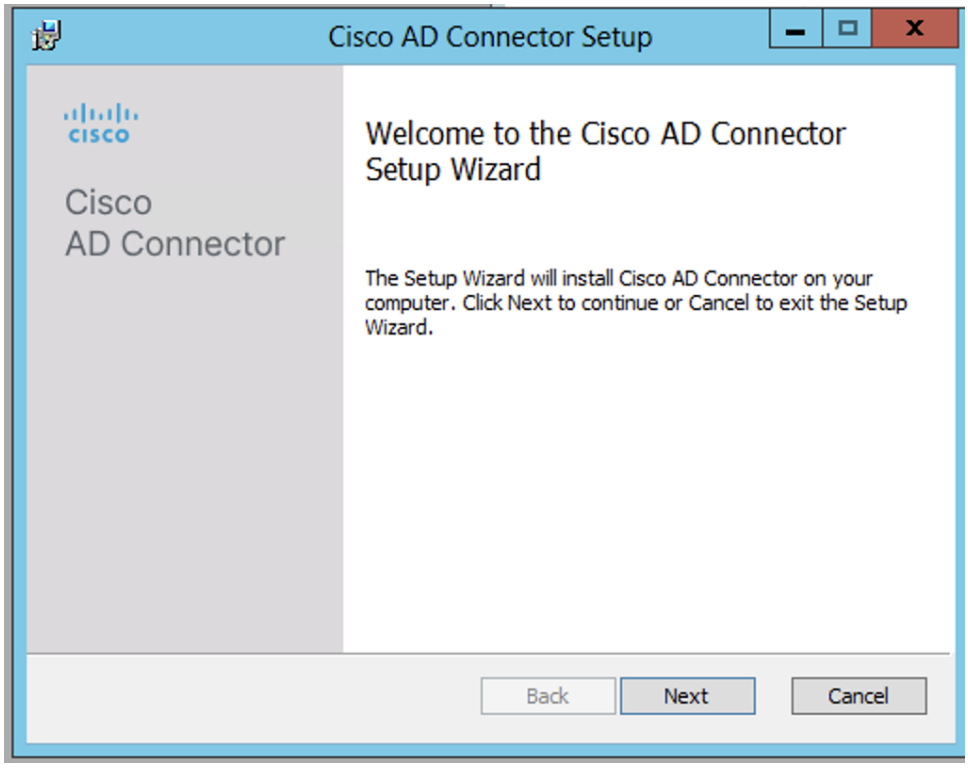
> **Note**
>
> If you run the AD Connector installer from the root directory of your server, you may encounter installation errors.

Before you begin

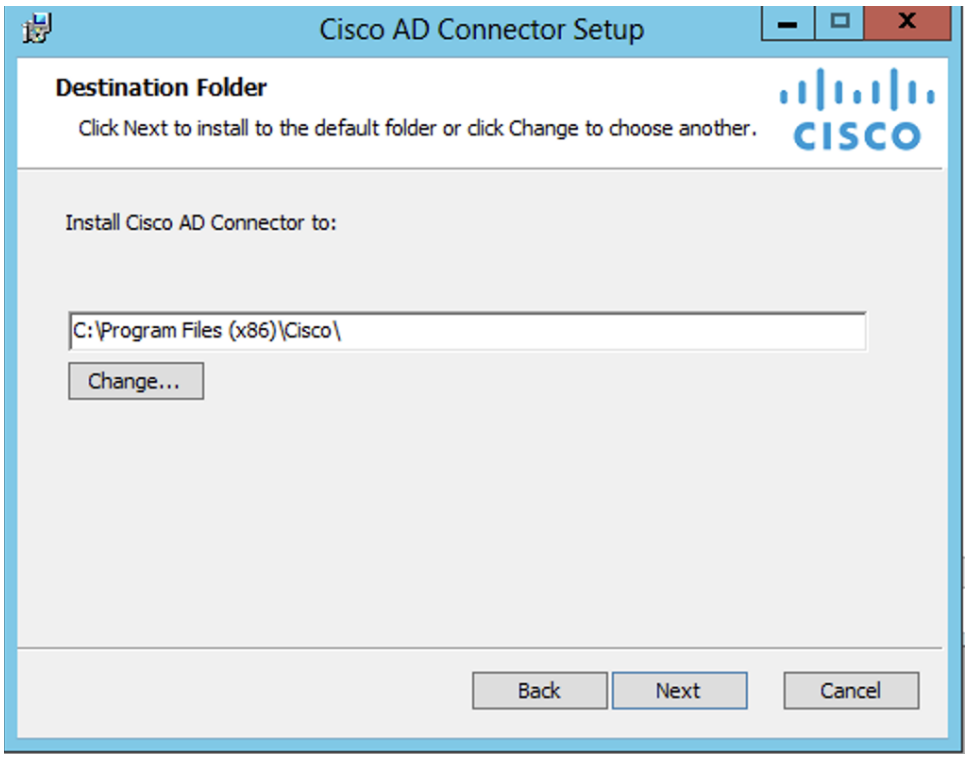
- Full Admin user role. For more information, see Manage Accounts.
- Set up the AD Connector server, user account, and environment for deploying the AD Connector. For more information, see Prerequisites for AD Connectors.
- Add the AD components in Secure Access. For more information, see Add AD Components in Secure Access.
- (Optional) Configure Authentication for AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.
- (Optional) Configure software updates on the AD Connector. For more information, see Configure Updates on AD Connectors.

Procedure

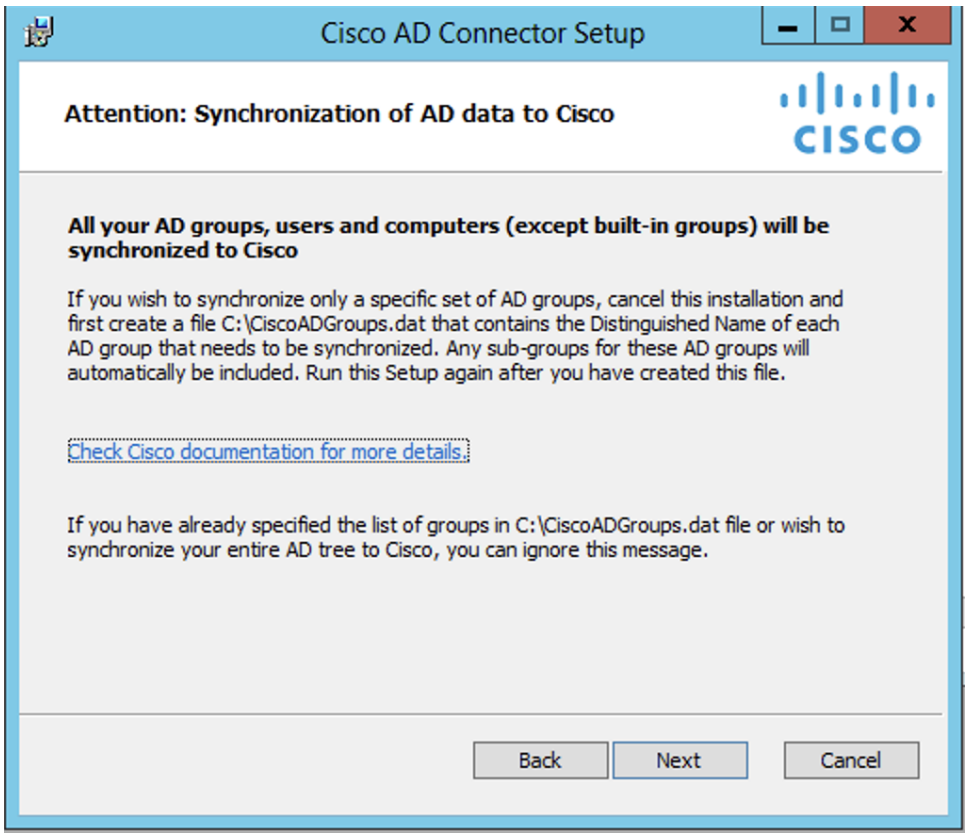
1. Run **setup.msi**, and then in the **Cisco AD Connector Setup** wizard, click **Next**.



2. Choose the directory on the server to install the Cisco AD Connector.



3. Confirm that you permit your AD Users and Groups to sync to Secure Access from the Cisco AD Connector.



4. Add your Active Directory credentials. Enter the **Username** of the Connector user (**Cisco_Connector** or custom username) and the **Password**.

5. Follow the remaining prompts in the setup, and when finished click **Finish**.

(Optional) Specify AD Groups in Selective Sync File

Describes (optional) specify ad groups in selective sync file. You can specify the AD Groups for the purpose of creating Access rules in Secure Access. Users and computers belonging to these Groups synchronize to Secure Access.

You can specify the AD Groups for the purpose of creating Access rules in Secure Access. Users and computers belonging to these Groups synchronize to Secure Access.

Supported Organizational Units

```
CN=My Group,OU=Organizational Unit,DC=sample,DC=local
```

Unsupported Organizational Units

```
OU=My OU,OU=Organizational Unit,DC=sample,DC=local
```

Sample File Entries

```
CN=Engineering,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Sales,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Marketing,CN=Builtin,DC=ciscoumbrella,DC=com
```

Total Number of Groups Selected for Synchronization

Groups specified in the selective sync file and all of their subgroups should not exceed 15,000. Also, these Groups should not be nested within more than five OU levels. Selective synchronization fails in both cases.

> **Note**
>
> If you can not meet either of these requirements, we recommend that you do not use the selective sync file. Instead, you can do a full AD tree synchronization.

Rename Selective Sync File After Upgrading to AD Connector v1.14.4

Describes rename selective sync file after upgrading to ad connector v1.14.4. If you use selective sync and upgrade the Cisco AD Connectors to v1.14.4 or later, you must rename the current selective sync file C:\CiscoUmbrellaADGroups.dat to C:\CiscoADGroups.dat.

If you use selective sync and upgrade the Cisco AD Connectors to v1.14.4 or later, you must rename the current selective sync file **C:\CiscoUmbrellaADGroups.dat** to **C:\CiscoADGroups.dat**.

> **Note**
>
> The selective sync file–previously named **CiscoUmbrellaADGroups.dat**–is not recognized by the Cisco AD Connector v1.1.4.4 or later.

After you rename the selective sync file, Secure Access automatically reads the selective sync file (**C:\CiscoADGroups.dat**) and syncs the Users in the specific Groups from AD to Secure Access. You are not required to restart the AD Connector service.

Create AD Groups in a Selective Sync File

Provides instructions for creating ad groups in a selective sync file. Full Admin user role. For more information, see Manage Accounts. Set up the AD Connector server, user account, and environment for deploying the AD Connector. For more information, see Prerequisites for AD Connectors.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Set up the AD Connector server, user account, and environment for deploying the AD Connector. For more information, see Prerequisites for AD Connectors.
- Add the AD components in Secure Access. For more information, see Add AD Components in Secure Access.
- (Optional) Configure Authentication for AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.
- (Optional) Configure software updates on the AD Connector.

Procedure

1. Identify the AD Groups of interest. Users and computers belonging to these Groups synchronize to Secure Access. For each sub-tree, only the parent group needs to be specified. All AD groups, users, and computers that are part of this parent group are automatically included.

> **Note**
>
> If you enabled **Selective Sync**, AD Users and Computers that are not members of Groups specified in **CiscoADGroups.dat** or their subgroups are not synchronized to Secure Access and are completely exempt from Secure Access access rules and reports.

> **Note**
>
> When configuring **Selective Sync** for **Cisco AD Connector**, do not use top-level built-in groups such as **Domain Users** or **Domain Computers** in the group filter. These built-in primary groups typically include most or all identities in the domain. In multi-domain environments, their use may result in users and computers from all domains being synchronized unintentionally. To maintain precise and predictable control over which identities are synchronized, create and use dedicated custom groups for selective sync instead.

2. Create a **CiscoADGroups.dat** file in the **C:** drive of each machine where the connector is installed. The connector only reads the **C:\CiscoADGroups.dat** file. If the file is incorrectly named or is not present in the **C:** drive, all groups are imported to Secure Access.
3. List the AD groups that need to be synchronized in `distinguished name` (DN) format in this file.
4. Ensure that there are no blank lines anywhere in the file.

> **Note**
>
> If you are running multiple AD Connectors, the file **C:\CiscoADGroups.dat** should be present on each system running the AD Connector and should be identical on each system.

Deploy LDIF Files for AD Connector

Describes deploying ldif files for ad connector. The Cisco Active Directory (AD) Connector integrates with Cisco Secure Access to provision the organization's users and groups from AD. You can install and configure the AD Connector to provision users and groups using LDAP Interchange Format (LDIF) source files.

The Cisco Active Directory (AD) Connector integrates with Cisco Secure Access to provision the organization's users and groups from AD. You can install and configure the AD Connector to provision users and groups using LDAP Interchange Format (LDIF) source files. Once you deploy the LDIF files on your server, the AD Connector syncs the users and groups in your organization with Secure Access.

For information about deploying the AD Connector with LDAP or LDAPS, see Connect Active Directory to Secure Access.

Best Practices for LDIF Source Deployments

- Do not combine manually provisioned (CSV file) users and groups with LDIF-based sourcing deployments. If you use both deployment methods, you may add duplicate users and groups in your organization.
- To migrate from the manually provisioned users and groups to LDIF-based sourcing, delete the CSV file with the users and groups that you uploaded to Secure Access.

- If you have multiple Active Directory deployments and choose to manually provision users and groups, we recommend that you deploy the AD Connector with LDIF source files.
- Once you provision users and groups with LDIF-based sourcing, we do not recommend that you delete the deployment and provision the users and groups using another deployment method.
- LDIF-based sourcing does not require Secure Access Domain Controllers.

Requirements

Requirements for deploying LDIF source files on your server:

- LDIF can support multiple domains.
- Create the LDIF files in the **Text** document format.

Known Limitations

- No support for selective groups-only sync.
- No support for incremental sync.

Download, install, and configure the Cisco AD Connector. Then, deploy the LDIF source files.

- Step 1 – Download the Active Directory Connector
- Step 2 – Install the Cisco AD Connector
- Step 3 – Deploy the LDIF Source Files

Step 1 – Download the Active Directory Connector

Provides instructions for step 1 – download the active directory connector. Download the Cisco AD Connector from Secure Access to your server.

Download the Cisco AD Connector from Secure Access to your server.

When you download the Cisco AD Connector software package, and if you did not configure API key credentials for the AD Connectors, Secure Access displays a warning message. We recommend that you configure API keys for your AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.

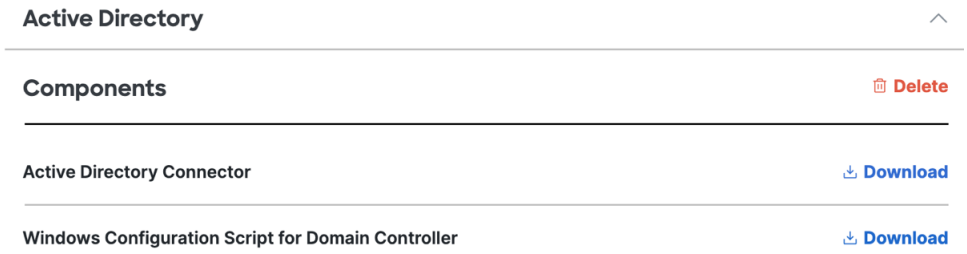
> **Note**
>
> You must download the ZIP file to the local machine where you plan to run it, or copy it locally from another machine. We do not recommend that you install the Cisco AD Connector from a network drive or run the `setup.msi` directly from the compressed file.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about network requirements, and connector user account and server prerequisites, see Prerequisites for AD Connectors.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Configure a server to run the Cisco AD Connector, and then sign in to Secure Access on that server.
2. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and then click **Configuration management**.
3. Navigate to **Directories**, expand **Active Directory**.
4. For **Active Directory Connector**, click **Download** to save the Cisco AD connector software package to the server. The software package is named: `CiscoAuditClient_vX.X.X.zip`.



Step 2 – Install the Cisco AD Connector

Provides instructions for step 2 – install the cisco ad connector. As an administrator, extract the contents of the ZIP file that you downloaded to a folder and then navigate to that folder.

As an administrator, extract the contents of the ZIP file that you downloaded to a folder and then navigate to that folder.

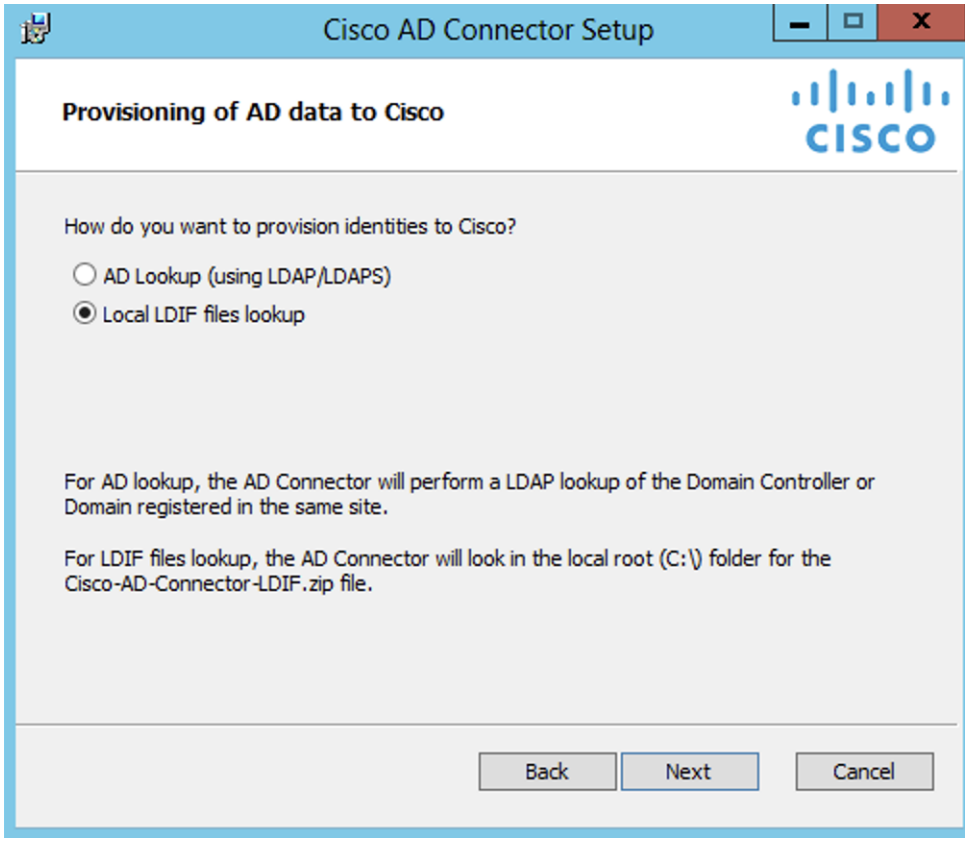
If you run the Cisco AD Connector installer files from the root directory of your device, you may encounter installation errors.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about network requirements, and connector user account and server prerequisites, see Prerequisites for AD Connectors.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Run `setup.msi`.
2. Enter the username of the Connector user (**Cisco_Connector** or custom username) and the password.
   For more information, see Prerequisites for AD Connectors.
3. Select **Local LDIF files lookup**, and then click **Next**.
4. Follow the prompts in the setup, and then click **Finish**.



Step 3 – Deploy the LDIF Source Files

Provides instructions for step 3 - deploy the ldif source files. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Deploy the LDIF source files on your server.

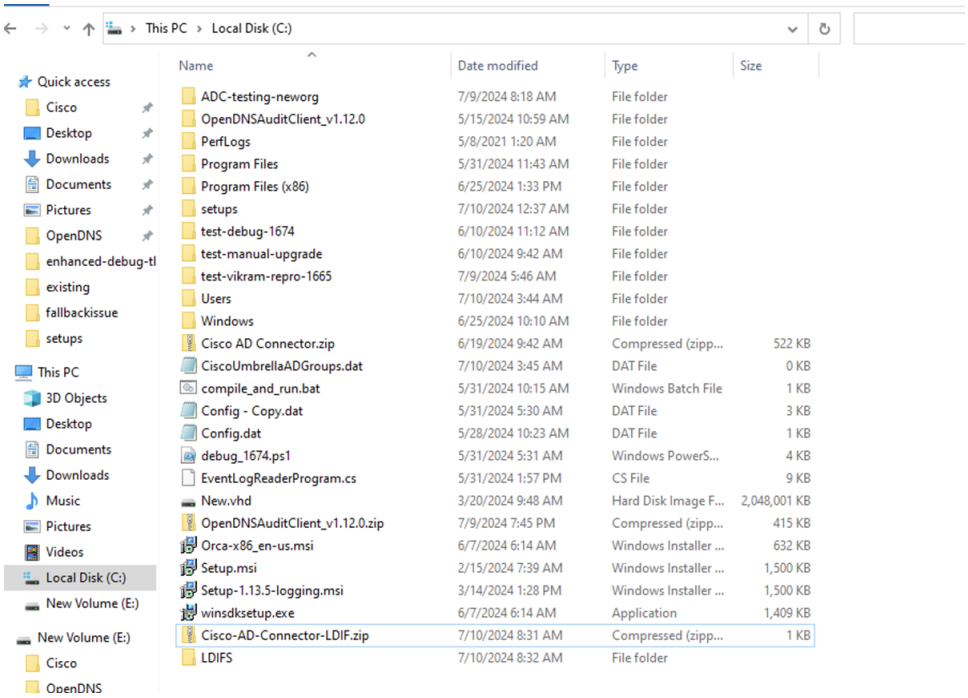
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about network requirements, and connector user account and server prerequisites, see Prerequisites for AD Connectors.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Navigate to the **C:** drive on your server.
2. Generate the LDIF files for the users and groups in your organization, and zip the files into a file. Name the file **Cisco-AD-Connector-LDIF.zip**.
   - Base-64 encode the value of the **objectGUID** fields.
   - Use two colons (**::**) to separate the **objectGUID** fields.
   - For users, create an `UserStruct.ldif` file. The supported fields are:
     - **dn**, **objectGUID**, **sAMAccountName**, **userPrincipalName**, **memberOf**, and **primaryGroupID**.

- For groups, create a **GroupStruct.ldif** file. The supported fields are:
  - **dn**, **objectGUID**, **sAMAccountName**, **userPrincipalName**, **memberOf**, and **primaryGroupToken**.



Troubleshooting

Describes troubleshooting. Various configuration conditions of the AD Connector with LDIF source files can result in provisioning errors. You uploaded an Cisco-AD-Connector-LDIF.zip file with users and groups in a particular set of domains.

Various configuration conditions of the AD Connector with LDIF source files can result in provisioning errors.

Scenario 1

- You uploaded an `Cisco-AD-Connector-LDIF.zip` file with users and groups in a particular set of domains. Later, you uploaded another `Cisco-AD-Connector-LDIF.zip` file (with a different set of domains) and expected only the identities from these domains to be present. However, the identities from the domain of the previous upload were retained and not removed.

Possible Cause: This configuration is not supported.

Solution: Raise a request with Cisco Support.

Scenario 2

The `Cisco-SSE-AD-Connector-LDIF.zip` file is not found. The Cisco AD Connector can not sync the users and groups with Secure Access.

Solution: Ensure that the `Cisco-AD-Connector-LDIF.zip` file is located under the `C:\` drive on the server.

Scenario 3

If one or both of the LDIF source files (`UserStruct.ldif` and `GroupStruct.ldif`) are not present or empty, then the Cisco AD Connector can not sync the users and groups with Secure Access.

Solution: Verify the contents in the `Cisco-AD-Connector-LDIF.zip` file and upload the file to the `C:\` drive on the server.

Scenario 4

Ensure that all fields in the LDIF source files are valid with no inappropriate values. The **dn** field is required and should contain appropriate values.

Analyze Logs

You can find the Cisco AD Connector logs on the server in the `C:\Program Files (x86)\Cisco\CiscoAD Connector\v1.14.4` folder. The log files are:

- For errors–`CiscoAuditClient.error.log`.
- For all events–`CiscoAuditClient.log`.

Change the Connector Account Password

Provides instructions for changing the connector account password. For regulatory compliance, you may need to change the password of the Cisco Active Directory (AD) Connector account. You can modify this password without impacting the functionality of the Cisco AD Connector.

For regulatory compliance, you may need to change the password of the Cisco Active Directory (AD) Connector account. You can modify this password without impacting the functionality of the Cisco AD Connector.

Changing the password on the Cisco AD Connector ensures that the AD connector can communicate with Microsoft AD using the new credentials. If the AD Connector account password is not correct, the Cisco AD Connector is unable to subscribe to login events and AD changes.

> **Note**
>
> If the password is not changed, Secure Access can not identify DNS requests with the AD users or groups accurately, and can not sync user and group changes from AD.

Before you begin

- Administrative privileges on the server where you will install the AD Connector.
- Install and set up the AD Connector on a server in your organization. For more information, see Connect Active Directory to Secure Access.

Procedure

1. Sign in to the account from any system that is a member of the domain and then set the new password.
2. Stop the **Cisco AD Connector** service.
3. Navigate to `C:\Program Files (x86)\Cisco\CiscoADConnector` and run the file `CiscoPasswordManager.exe`.

   You may need to run this utility as an administrator.

4. When prompted, add your new password.
5. Start the **Cisco Active Directory Service** service.

What to do next
Repeat steps 2 and 3 for each deployed AD Connector.

AD Connector Communication Flow and Troubleshooting

Describes ad connector communication flow and troubleshooting. The Cisco Active Directory (AD) Connector is a Windows application and service that communicates with Cisco Secure Access and AD domain controllers. The Cisco AD Connector only syncs the required AD User and Group attributes with Secure Access.

The Cisco Active Directory (AD) Connector is a Windows application and service that communicates with Cisco Secure Access and AD domain controllers. The Cisco AD Connector only syncs the required AD User and Group attributes with Secure Access.

The following information describes the communication flow between a Cisco AD Connector and AD domain controllers, the attributes that sync between AD, the AD Connector, and Secure Access, and the steps that you can take to troubleshoot your Cisco AD Connector deployment.

- Communication Flow
- Troubleshooting

Communication Flow

Describes communication flow. The Cisco AD Connector first attempts to communicate to the AD domain controller over secure lightweight directory access protocol (LDAPS) on port 646.

1. The Cisco AD Connector first attempts to communicate to the AD domain controller over secure lightweight directory access protocol (LDAPS) on port 646. If unsuccessful, the Cisco AD Connector falls back to communicating over LDAP on port 389 using first Kerberos authentication and if that does not succeed, NTLM authentication (Windows NT LAN Manager) over LDAP.
2. The Cisco AD Connector retrieves the AD Users and Groups details only.

   Note

   If there are updates to the Users and Groups, the Cisco AD Connector sends the AD data every five to seven minutes using an HTTPS connection on TCP port 443. However, it can take an hour or longer for changes to reflect in Secure Access.

   Secure Access stores the required attributes from each object, including:

   - `sAMAccountName`–The username that you use to sign into the Cisco AD Connector.
   - `dn`–The distinguished name.
   - `userPrincipalName`–The user's principal name.
   - `memberOf`–The groups that include the user.
   - `objectGUID`–The group ID of the object. This property is sent to Secure Access as a hash.

- `primaryGroupId`–The primary group ID that is available for Users and Groups.
- `primaryGroupToken`–The primary group token that is available only for Groups. Passwords or password hashes are not retrieved. Secure Access uses the `primaryGroupToken` data in the access policy and configuration and reporting. This data is also required for each user or per-computer filtering.

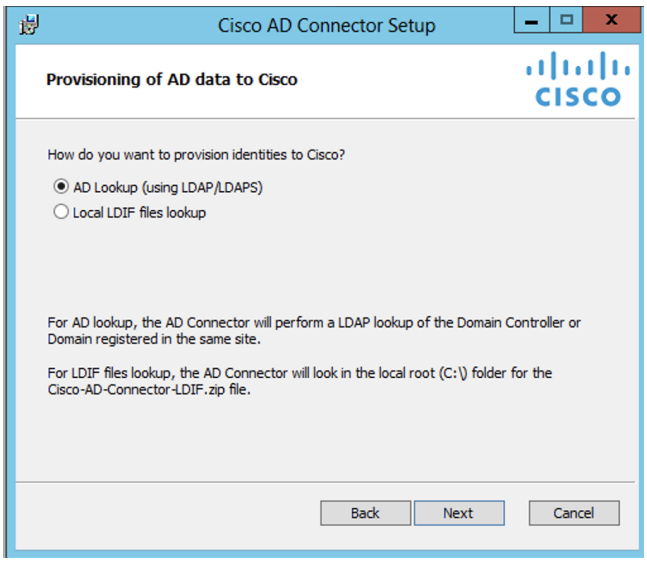
3. The Cisco AD Connector stores the AD User and Group data locally in `.ldif` files.

   The local AD User and Groups data is contained within this folder: `C:\\Program Files (x86)\\Cisco\\Cisco AD Connector\\ADSync`.

   Review the files in the `.ldif` files in the **ADSync** directory to confirm that the Cisco AD Connector synchronized the AD Users and Groups data to Secure Access.

   Note

   When you install the Cisco AD Connector, you have the option to turn off the local storage of `.ldif` files.



Troubleshooting

Describes troubleshooting. Recommendations for troubleshooting the communications with the Cisco AD Connector. The following firewall or access control (ACL) requirements ensure that a Cisco AD Connector can communicate with Secure Access and domain controllers.

Recommendations for troubleshooting the communications with the Cisco AD Connector.

Network Requirements

The following firewall or access control (ACL) requirements ensure that a Cisco AD Connector can communicate with Secure Access and domain controllers. For more information, see Network Requirements for Secure Access.

Port and Protocol	Source	Destination	Note
443/TCP	AD Connector	**devicesapisecureaccessfedcisco**	• Initial registration with the Secure Access • Automatic updates • Health status reporting in Secure Access
80/TCP	AD Connector	**ocsp.digicert.com** **crl3.digicert.com** **crl4.digicert.com**	• Check for certificate revocations through the Online Certificate Status Protocol (OCSP) and certificate revocation lists (CRLs).
389/TCP 636/TCP	AD Connector	Domain controller or domain	• Sync with LDAP/LDAPS

Note

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

If you experience any issues communicating with Secure Access, we recommend that you check for any Layer-7 application proxies, which may block or drop data sent to Secure Access. A common case is the **inspect** feature on Cisco devices that act on protocols such as DNS, HTTP, or HTTPS. For more information, see Cisco Security Appliance Command Line Configuration Guide, Version 7.2.

Restart the Active Directory Connector

You can restart the Cisco AD Connector by restarting the **Cisco AD Connector** service on the AD Connector server. Restarting the Cisco AD Connector triggers a full synchronization of the AD Users and Groups, not only the changes from the previous sync to Secure Access.

If your Cisco AD Connector is not in the **Okay** state, contact Support. For more information, see Contact Cisco Secure Access Support.

Connect Active Directory to Secure Access

Describes connecting active directory to secure access. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your users and groups, which are deployed in Microsoft AD. Before you can provision users and groups from Active Directory, you must connect your instance of AD to Secure Access.

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your users and groups, which are deployed in Microsoft AD. Before you can provision users and groups from Active Directory, you must connect your instance of AD to Secure Access.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Configure a Connector Server.

- Allow Outbound Network Access to Secure Access.
- Create the Connector Account.

Configure a Connector Server

You must configure a server that is a member of the AD domain with the following environment:

- Windows Server 2012, 2012 R2, 2016, 2019 or 2022 with the latest service packs and 100MB free hard disk drive space.
- .NET Framework 4.5 or newer.
- If a local anti-virus application is running, allow the `CiscoAuditClient.exe` and `CiscoAuditService.exe` processes.

You may deploy the Cisco AD Connector directly on the domain controller. In this case, the domain controller must meet all prerequisites. Only one Cisco AD Connector is required to provision users and groups from an AD domain. For redundancy, add an optional second connector.

Allow Outbound Network Access to Secure Access

The Cisco AD Connector server requires outbound access to certain URLs. If you use a transparent HTTP web proxy, ensure that the following URLs on port 80/443 are excluded from the proxy, and not subject to authentication:

- 443 (TCP) to **devices.api.secureaccessfed.cisco** to sync the AD Users and Groups.
- Access to additional URLs on port 80/443 (TCP) for Windows to perform Certificate Revocation List and Code-Signing checks. For a complete list of ports, see AD Connector Communication Flow and Troubleshooting.

Create the Connector Account

When you deploy the Cisco AD Connector, you must create a new user account in the AD domain. This account must have these attributes:

- Set the account name (**sAMAccountName**) to **Cisco_Connector**.

  > **Note**
  >
  > You can sign in with a custom username that has the required permissions.

- Select **Password never expires**.

  > **Note**
  >
  > Passwords must not include backslashes, quotations (single or double), greater-than or less-than chevron brackets (< >), or colons.

- Assign **Read** and **Replicating Directory Changes** permissions.

  Alternately, you can make the Cisco AD Connector account a member of the built-in **Enterprise Read-only Domain Controllers** group, which automatically assigns these permissions.

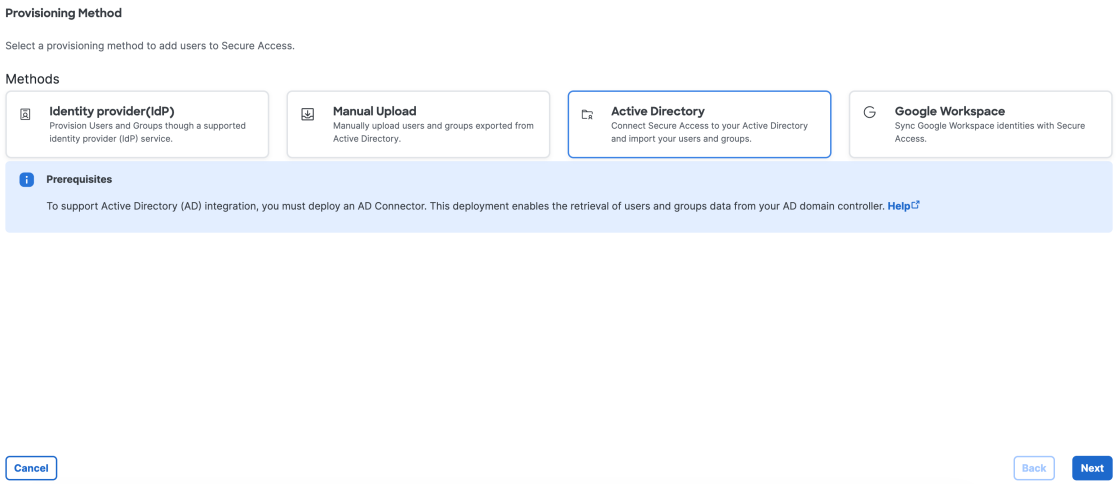
> **Note**
>
> The Cisco AD Connector does an initial synchronization of the AD structure to Secure Access. After the sync, it detects changes to the AD structure and communicates these changes only. The detection of the changes requires the **Replicating Directory Changes** permission. The Cisco AD Connector can not function without this permission. The **Replicating Directory Changes** permission is different from the **Replicating Directory Changes All** permission, which enables retrieval of password hashes. The Cisco AD Connector does not read password hashes and thus does not require the **Replicating Directory Changes All** permission.

Step 1 – Choose a Provisioning Method

Provides instructions for step 1 – choose a provisioning method. Navigate to Connect Users, Groups, and Endpoint Devices Users and click Provision Users, or navigate to Connect Users, Groups, and Endpoint Devices Groups and click Provision Groups.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users** and click **Provision Users**, or navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Groups** and click **Provision Groups**.
2. For **Provisioning Method**, click **Active Directory**.
3. Click **Next**.



Step 2 – Register a Domain Controller or Domain in Secure Access

Describes step 2 – register a domain controller or domain in secure access. Choose the AD component type and configure the component to sync with Secure Access.

Choose the AD component type and configure the component to sync with Secure Access.

Active Directory integration requires that you register an AD domain controller or AD domain in Secure Access. The Cisco AD Connector performs an LDAP sync against this domain controller or domain to retrieve the Users and Groups. The Cisco AD Connector server communicates with the domain controller on port 389 over TCP for LDAP sync or port 636 over SSL for LDAP.

The Cisco AD Connector can only retrieve users and groups from a single domain controller. If you register multiple domain controllers in Secure Access, the Cisco AD Connector only attempts to perform an LDAP sync against the first domain controller in the list. Ensure that the domain controller you are registering is not subject to any AD replication delays. Read-only Domain Controller (RODC) registrations are supported for retrieval of users and groups.

If you need to periodically bring down your domain controller for maintenance or updates or your domain controllers are behind a load balancer that does not support LDAP queries, we recommend that you register the domain instead.

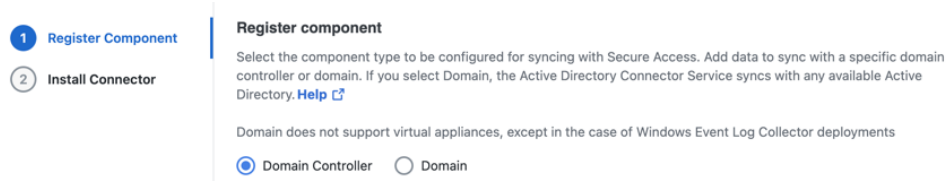
- Register a Domain Controller
- Register a Domain

Register a Domain Controller

Provides instructions for register a domain controller. Choose Domain Controller to register the AD domain controller component.

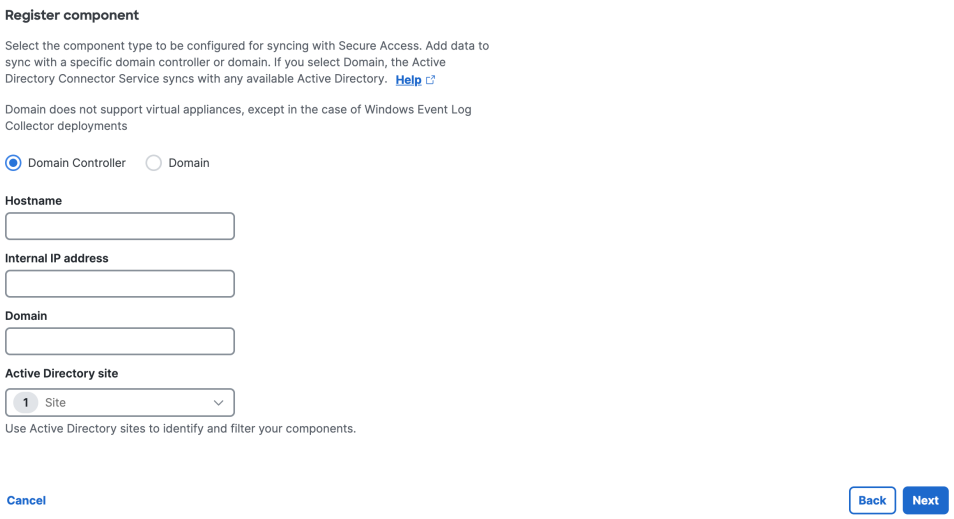
Procedure

1. Choose **Domain Controller** to register the AD domain controller component.



2. Enter the **hostname**, **internal IP address**, and **domain** of the domain controller. Choose an **Active Directory site** to identify the AD component.

   The Active Directory connector attempts to connect to your newly added domain controller. If all the required permissions have been configured, you should not experience any issues. If there are errors, review Prerequisites or contact Support.



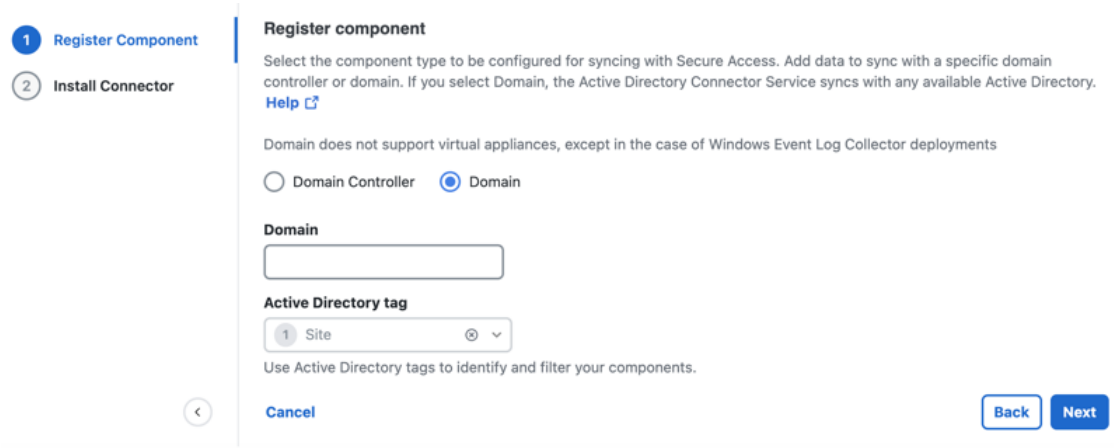
3. Click **Next** and then follow the instructions in Step 3 – Install the Cisco AD Connector.

Register a Domain

Provides instructions for register a domain. Choose Domain to register the AD domain component. For Domain, enter the domain name. Choose an Active Directory tag to identify the AD component.

Procedure

1. Choose **Domain** to register the AD domain component.
2. For **Domain**, enter the domain name. Choose an **Active Directory tag** to identify the AD component.
3. Click **Next**, and then follow the instructions in Step 3 – Install the Cisco AD Connector.



Step 3 – Download the Cisco AD Connector from Secure Access

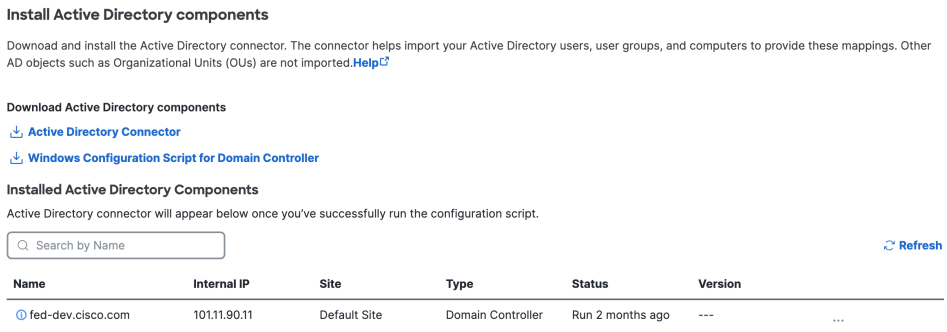
Provides instructions for step 3 – download the cisco ad connector from secure access. Download the Cisco AD connector to your server.

Download the Cisco AD connector to your server.

Procedure

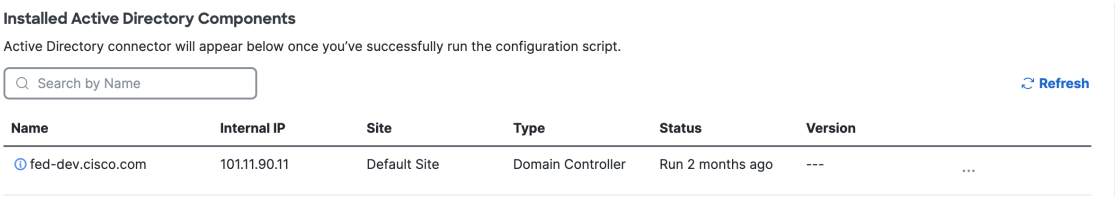
1. In the **Install Connector** page, click **Active Directory Connector** to save the Cisco AD connector deployment package to the server.

   The deployment package is named: **OpenDNS-Windows-Service.zip**.



> **Note**
>
> You must download the ZIP file to the local machine where you plan to run it, or copy it locally from another machine. We do not recommend that you install the Cisco AD Connector from a network drive or run the `setup.msi` directly from the compressed file.

2. Once you've successfully run the configuration script (see, Install the Cisco AD Connector, the Active Directory connector will appear in **Installed Active Directory Components**. Enter text for an AD component in the search bar to query for an installed AD component or click the ellipsis (**...**) to edit or delete the AD component.



   - **Name**–The hostname of the Windows computer where you installed the AD Controller.
   - **Internal IP**–The internal IP address of the AD Controller.
   - **Site**–The site associated with the AD component.
   - **Type**–The type of AD component, either Domain Controller or Domain.
   - **Status**–The state of the AD component.
   - **Version**–The version of the AD component.

   The status of your domain controller and connectors should change from **Inactive** to **Active** (green). If the configured domain controller or connectors are not active after a period of time, contact Secure Access Support.

   It can take up to four hours for large numbers of AD user, computer and group objects to synchronize for the first time. During this time, the connector status icon may appear as red until the initial sync is complete. After the sync completes, the connector status icon is labeled as **Active** (green).

   Seeing your groups listed means the domain controllers have automatically synchronized user and computer group memberships with Secure Access through the connector successfully. Any subsequent changes should also sync successfully.

   > **Note**
   >
   > If the connector does not appear in Secure Access and port 443 is confirmed to be open to **devices.api.secureaccessfed.cisco**, **crl4.digicert.com**, and **ocsp.digicert.com**, the connector server may be missing the DigiCert CA. To confirm, visit `https://devices.api.secureaccessfed.cisco/v2/OnPrem.Asset`. If a certificate error is presented, download and install the latest DigiCert Global Root CA from DigiCert and restart the Connector service. If it does not appear, contact Support.

Step 4 - Install the Cisco AD Connector

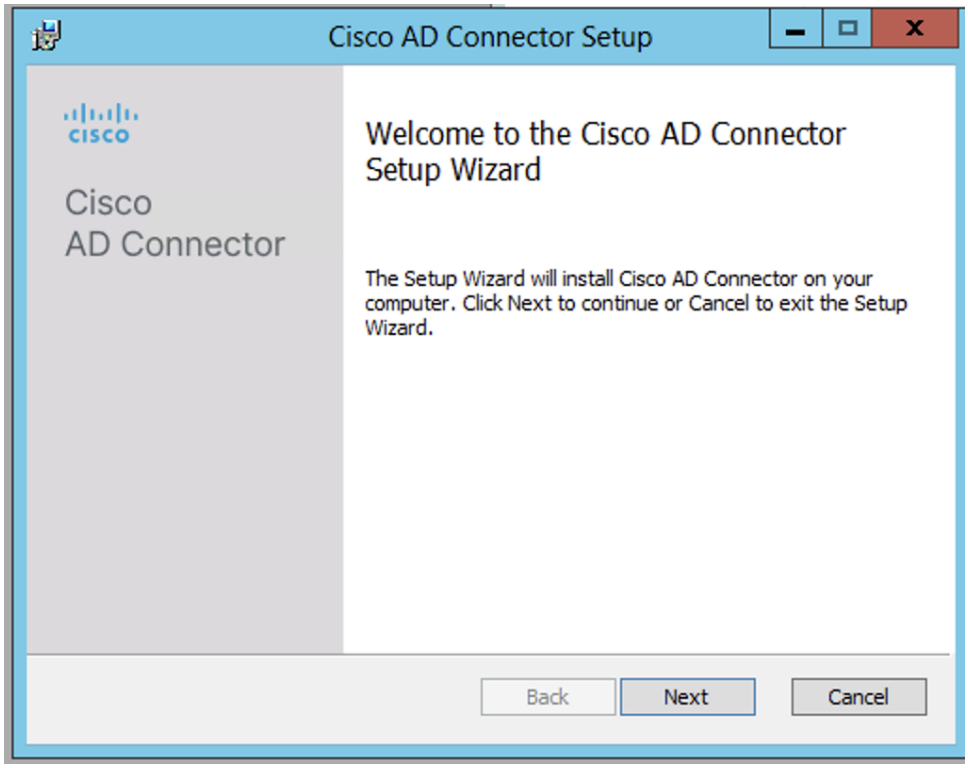
Provides instructions for step 4 - install the cisco ad connector. As an administrator, extract the contents of the OpenDNS-Windows-Service ZIP file that you downloaded from Secure Access to a folder on the server, and then navigate to that folder.

As an administrator, extract the contents of the **OpenDNS-Windows-Service** ZIP file that you downloaded from Secure Access to a folder on the server, and then navigate to that folder.

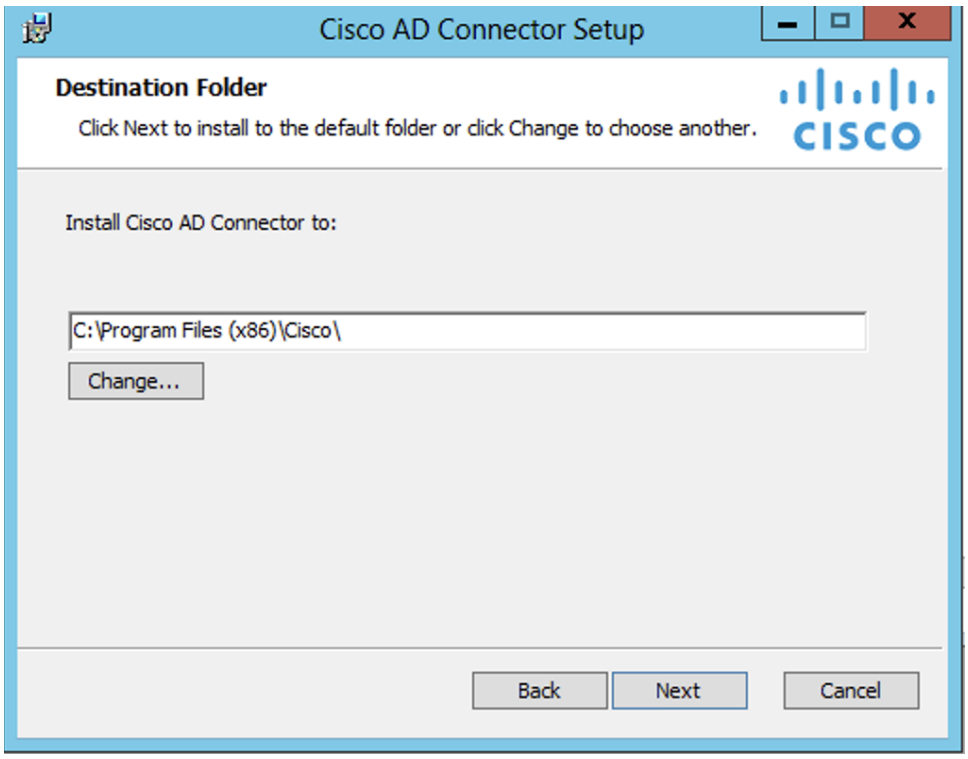
> **Note**
>
> If you run the AD Connector installer files from the root directory of your server, you may encounter installation errors.

Procedure

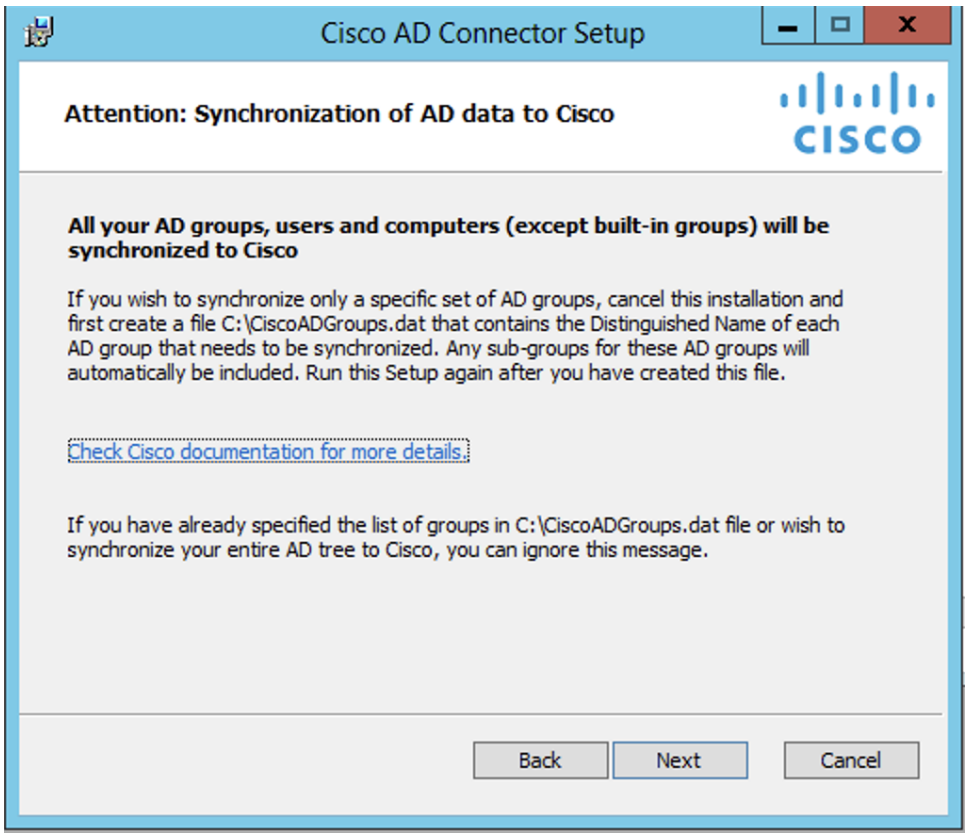
1. Run `setup.msi`, and then in the **Cisco Connector Setup** wizard, click **Next**.



2. Choose the directory on the server to install the Cisco AD Connector.



3. Confirm that you permit your AD Users and Groups to sync to Secure Access from the Cisco AD Connector.



4. Add your Active Directory credentials. Enter the **Username** of the Connector user (**Cisco_Connector** or custom username) and the **Password**. For more information, see Prerequisites.

5. Follow the remaining prompts in the setup and when finished, click **Close**.

Best Practices for Synchronizing Active Directory Groups and Organizational Units

Describes best practices for synchronizing active directory groups and organizational units. To enable efficient and secure integration between Cisco Secure Access and your Active Directory environment, it is important to carefully select and configure the AD Groups and Organizational Units (OUs) to be synchronized.

To enable efficient and secure integration between Cisco Secure Access and your Active Directory environment, it is important to carefully select and configure the AD Groups and Organizational Units (OUs) to be synchronized. The following sections outline the key considerations and requirements for defining groups of interest, supported and unsupported OUs, file configuration, and synchronization limits.

Specify AD Groups of Interest

Optionally, you can specify the AD Groups of interest for the purpose of creating access rules in Secure Access.

1. Identify the AD Groups of interest. Users and computers belonging to these Groups synchronize to Secure Access.

   For each sub-tree, only the parent group needs to be specified. All AD groups, users, and computers that are part of this parent group are automatically included.

   > **Note**
   >
   > If you enabled **Selective Sync**, AD Users and Computers that are not members of Groups specified in **CiscoADGroups.dat** or their subgroups are not synchronized to Secure Access and are completely exempt from Secure Access access rules and reports.

2. Create a **CiscoADGroups.dat** file in the **C:** drive of each machine where the connector is installed.

   The connector only reads the **C:\CiscoADGroups.dat** file. If the file is incorrectly named or is not present in the **C:** drive, all groups are imported to Secure Access.

3. List the AD groups that need to be synchronized in `distinguished name` (DN) format in this file.

Supported Organizational Units

```
CN=My Group,OU=Organizational Unit,DC=sample,DC=local
```

Unsupported Organizational Units

```
OU=My OU,OU=Organizational Unit,DC=sample,DC=local
```

Sample File Entries

```
CN=Engineering,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Sales,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Marketing,CN=Builtin,DC=ciscoumbrella,DC=com
```

1. Ensure that there are no blank lines anywhere in the file.

> **Note**
>
> If you are running multiple connectors, the file **C:\CiscoADGroups.dat** should be present on each system running the connector and should be identical on each system.

Total Number of Groups Selected for Synchronization

The total number of Groups selected for synchronization—Groups specified in the selective sync file and all of their subgroups—should not exceed 15,000. Also, these Groups should not be nested within more than five OU levels. Selective synchronization fails in both cases. If you can not meet either of these requirements, we recommend that you do not use the selective sync file. Instead, you can do a full AD tree synchronization.

AD Integration with Virtual Appliances

Describes ad integration with virtual appliances. The integration of Microsoft Active Directory (AD) with Cisco Secure Access Virtual Appliances (VAs) provides AD user, group, or computer name information for each applicable DNS request. Secure Access VAs forward DNS requests at the site.

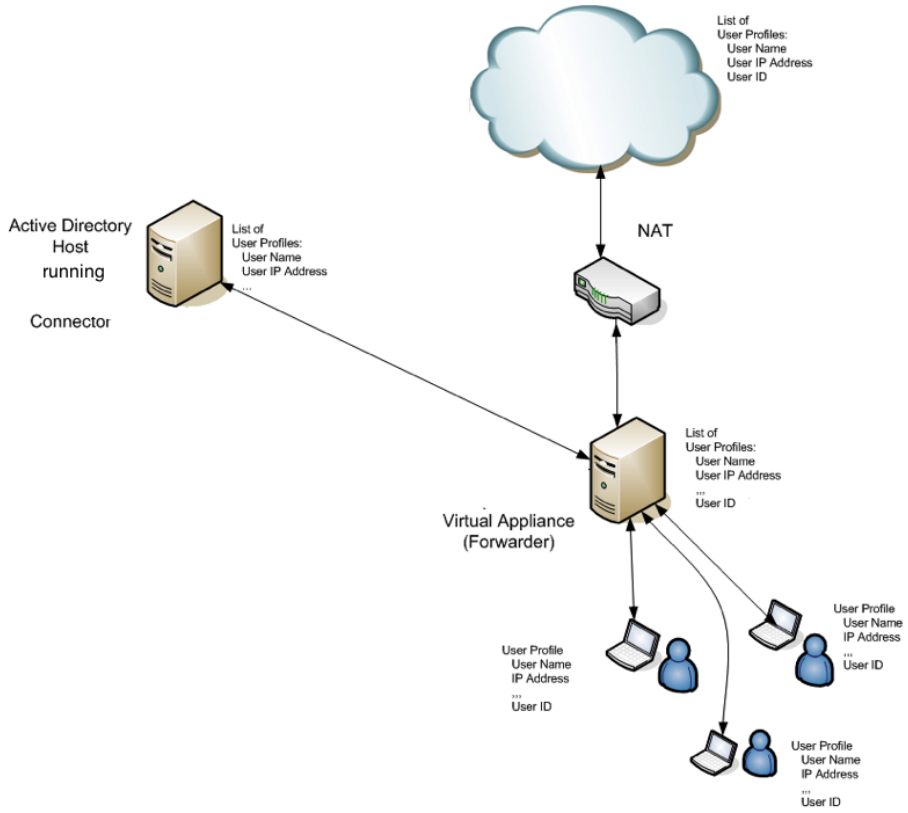
The integration of Microsoft Active Directory (AD) with Cisco Secure Access Virtual Appliances (VAs) provides AD user, group, or computer name information for each applicable DNS request. Secure Access VAs forward DNS requests at the site.

An AD site in the context of this guide means an independent location with its own domain controllers, DNS servers, and connection to the internet. For information about Secure Access Sites, see Manage Sites for AD Components and Manage Site for Virtual Appliance.

For an overview of the network topology, as well as the flow of traffic with the VA, see AD Connector Communication Flow and Troubleshooting.

Network Diagram for VA Deployments

The client computers at each AD site must be set to use the VA at their respective site as their DNS resolvers. The VA can then route DNS queries to their appropriate IP address for both internal and external resources. The VA also communicates with the AD environment to query for a list of user information to match to clients.



How to Set Up AD Components with VAs

1. Review the requirements for setting up the AD components in your environment. For more information, see Prerequisites for AD Connectors and VAs.
2. Prepare your AD Environment. For more information, see Prepare Your AD Environment.
3. Install the AD Connectors. For more information, see Connect Active Directory to VAs.
4. View the installed AD components. For more information, see View AD Components..
5. View the provisioned AD users and groups in Secure Access. For more information, see View User Details and View Group Details.

Prerequisites for AD Connectors and VAs

Describes prerequisites for ad connectors and vas. To support the integration of Active Directory (AD) with Secure Access, review and meet the requirements for the Connector server and account, and AD deployments with Secure Access virtual appliances.

To support the integration of Active Directory (AD) with Secure Access, review and meet the requirements for the Connector server and account, and AD deployments with Secure Access virtual appliances.

Connector Server

You must configure a server that is a member of the AD domain with the following environment:

- Windows Server 2012, 2012 R2, 2016, 2019, or 2022 with the latest service packs and 100MB free hard disk drive space. Service packs prior to SP2 are not supported.
- .NET Framework 4.5 or above.

- If a local anti-virus application is running, allow the **CiscoAuditClient.exe** and **CiscoAuditService.exe** processes to run on the system.

The Connector may be deployed directly on the domain controller. In this case, the domain controller must meet all prerequisites listed above. Only one connector is required to provision identities from an AD domain, with an optional second connector for redundancy if required.

Guidelines for AD Deployments with Secure Access Virtual Appliances

- For troubleshooting, install the **AD Domain Services Snap-ins and Command-line Tools** feature through the **<!DOCTYPE concept PUBLIC " -//CISCO//DTD DITA 1.3 Concept v1.0//EN" "cisco-concept.dtd" []>** > **Remote Server Administration Tools** > **Role Administration Tools** > **AD DS & AD LDS Tools** > **AD DS Tools**.
- If you are deploying AD with Virtual Appliances through the integration with domain controllers, you must deploy one AD Connector for each AD domain (with an optional second connector for each AD domain).
- If you have already deployed a centralized Windows Event Log Collector to which all domain controllers forward login events, and you wish to deploy AD integration with Virtual Appliances using this Windows Event Log Collector, you will need to deploy a single AD connector for all AD domains, with an optional second connector for redundancy.

Outbound Network Access to Secure Access

The Connector server requires outbound access on certain domains and URLs. If you are using a transparent HTTP web proxy, ensure that these domains and URLs on port 80/443 are excluded from the proxy, and not subject to authentication.

- For syncing, allow traffic on 443 (TCP) to **devices.api.secureaccessfed.cisco**.
- For Windows to perform Certificate Revocation List and Code-Signing checks, allow access to additional URLs on port 80/443 (TCP). For a complete list of ports, see AD Connector Communication Flow and Troubleshooting.

Connector Account

To deploy the Connector, create a new user account in the AD domain. This account should have:

- The logon name (sAMAccountName) set to **Cisco_Connector**. You can use a custom username, but you must configure it with the required permissions.
- Select `Password never expires`.

> **Note**
>
> Passwords can not include backslashes, quotations (single or double), greater-than or less-than chevron brackets (**< >**), or colons.

- Assign `Read` and `Replicating Directory Changes` permissions. Alternatively, you can make the Connector account a member of the built-in `Enterprise Read-only Domain Controllers` group which will automatically assign these permissions.

> **Note**
>
> The Connector does an initial synchronization of the AD structure to Secure Access. After this, it detects changes to the AD structure and communicates these changes only. The detection of changes requires the `Replicating Directory Changes` permission, so the Connector cannot function without this permission. The `Replicating Directory Changes` permission is different from the `Replicating Directory Changes All` permission which enables the retrieval of password hashes. The Connector does not read password hashes and hence does not require the `Replicating Directory Changes All` permission.

Guidelines for AD Deployments with Secure Access Virtual Appliances

- The Connector account (**Cisco_Connector** or custom username) must be a member of the following built-in groups on each AD domain:
  - Enterprise Read-only Domain Controllers
  - Event Log Readers

> **Note**
>
> In a parent/child domain scenario, the `Enterprise Read-only Domain Controller` only exists in the parent domain. In this case, follow the instructions listed here to provide the required permissions for the Connector account. You must add other missing groups.

Prepare Your AD Environment

Describes prepare your ad environment. The integration of Active Directory (AD) with a Secure Access Virtual Appliance (VA) requires that you register the deployed AD domain controllers or the Windows Event Log Collector and AD domains in Secure Access. You must also deploy the Cisco AD Connector.

The integration of Active Directory (AD) with a Secure Access Virtual Appliance (VA) requires that you register the deployed AD domain controllers or the Windows Event Log Collector and AD domains in Secure Access. You must also deploy the Cisco AD Connector. For information about the AD Connector, see Manage AD Connectors.

You must have at least one VA deployed in the environment. For information about the Secure Access VAs, see Get Started with Virtual Appliances.

This guide describes how to register AD domain controllers or a centralized Windows Event Log Collector and AD domains in Secure Access.

To integrate AD with a Secure Access VA, complete one of the procedures-->:

- Integrate AD with Domain Controllers

About the AD Connector and Logon Events

Describes about the ad connector and logon events. For each end-user on the AD domains, the AD Connector forwards the logon events to the deployed VAs.

For each end-user on the AD domains, the AD Connector forwards the logon events to the deployed VAs. The AD Connector can read logon events for users from the AD domain controllers at the site or a centralized Windows Event Log Collector. You can use an existing deployment of a centralized Windows Event Log Collector where domain controllers forward

logon events for multiple AD domains or AD forests. For more information, see Support for Multiple AD Domains and AD Forests.

The domain controller or centralized Windows Event Log Collector record logon events by end users. The user's IP and username are made available through the AD Connector to the VA. The VA is a conditional DNS forwarder. The VA forwards DNS requests to the Secure Access DNS resolvers or, if bypass domains have been configured, forwards DNS requests to the organization's internal DNS servers. Secure Access applies the access rules in the policy to the DNS traffic and displays the end user identity information with the request in the reports and logs.

Note

You must deploy the VA, AD Connector, and domain controllers or centralized Windows Event Log Collector at the same Site registered with Secure Access.

Prerequisites

Describes prerequisites. Full Admin user role. For more information, see Manage Accounts. For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.
- Deploy at least one Secure Access Virtual Appliance. For more information, see Get Started with Virtual Appliances.

Additional Prerequisites for the Windows Event Log Collector

- The Cisco AD Connector account (**Cisco_Connector** or custom account as configured) should be added to the local Event Log Readers group on the Windows Event Log Collector machine.
- On the Windows Event Log Collector machine, enable these firewall rules, which allow the server where you deployed the AD Connector to read the Windows event logs:
  - **Remote Event Log Management (NP-In)**
  - **Remote Event Log Management (RPC)**
  - **Remote Event Log Management (RPC-EPMAP)**
- Review all network access requirements. For more information, see AD Connector Communication Flow and Troubleshooting.

Integrate AD with Domain Controllers

Describes integrating ad with domain controllers. Download the Windows Configuration script from Secure Access, and then run the script to add an AD domain controller in Secure Access.

Download the Windows Configuration script from Secure Access, and then run the script to add an AD domain controller in Secure Access.

- Support for Multiple AD Domains and AD Forests
- Verify Auditing of Logon Events on Domain Controllers
- Download the Windows Configuration Script for Domain Controllers
- Run the Configuration Script on the Domain Controllers

- Add a Domain Controller in Secure Access
- View the Registered AD Components in Secure Access

Support for Multiple AD Domains and AD Forests

Describes support for multiple ad domains and ad forests. Using domain controllers, you can integrate multiple AD domains or AD forests with Secure Access. For each AD domain that integrates with Secure Access, deploy the Cisco AD Connector plus an additional AD Connector for redundancy.

Using domain controllers, you can integrate multiple AD domains or AD forests with Secure Access. For each AD domain that integrates with Secure Access, deploy the Cisco AD Connector plus an additional AD Connector for redundancy.

Verify Auditing of Logon Events on Domain Controllers

Describes verifying auditing of logon events on domain controllers. The AD integration with domain controllers requires each domain controller to audit logon events.

The AD integration with domain controllers requires each domain controller to audit logon events.

On each domain controller (excluding read-only domain controllers), enable the **Audit account logon events** to include `Success` and `Failure` if it is set to `No Auditing`.

By default, this group policy is set to log `Success` logon events and you should not modify it. Secure Access requires the **Audit account logon events** setting so that it knows whether a user has logged in successfully and can then compare that logon to subsequent events generated by that user.

If the Audit Policy is not set, the **Windows Configuration Script for Domain Controller** displays this error message:

```
"ERROR: "

-------------------------------------------------------------------------------


Your Group Policy for this Domain Controller is set to NOT audit successful
logon events!

You MUST edit the following Group Policy for all DCs:

Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit logon events

Define that policy to audit Success attempts, gpupdate, and re-run this script!
```

Download the Windows Configuration Script for Domain Controllers

Provides instructions for downloading the windows configuration script for domain controllers. The Windows Configuration Script automates the permissions for the Cisco_Connector user.

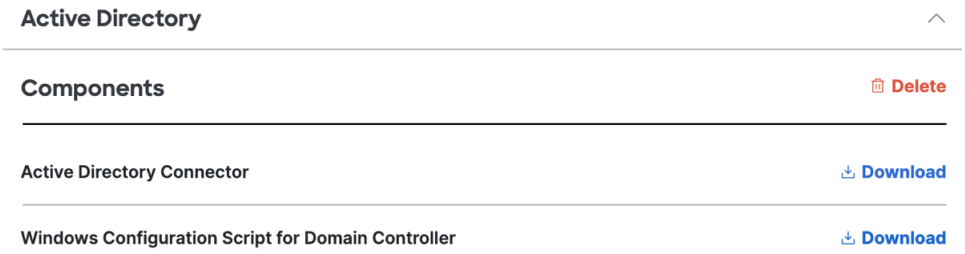
The Windows Configuration Script automates the permissions for the **Cisco_Connector** user.

In Secure Access, download the **Windows Configuration Script for Domain Controller** script to the domain controllers in your environments.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users**, click **Configuration Management** > **Integrate directories**, and then click **Active Directory**.
2. After an initial AD deployment, navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users**, click **Configuration Management**, and expand **Active Directory**.

3. For **Windows Configuration Script for Domain Controller**, click **Download**.



4. Download and save the configuration script to a location on the machine where you plan to run it.

> **Note**
>
> The configuration script is written in Visual Basic Script and is in plain text.

Run the Windows Configuration Script for the Domain Controllers

Provides instructions for running the windows configuration script for the domain controllers. Run the Windows Configuration Script for Domain Controller script on all of the domain controllers at each site, (excluding read-only domain controllers (RODCs)) and for each domain that will integrate with Secure Access.

Run the **Windows Configuration Script for Domain Controller** script on all of the domain controllers at each site, (excluding read-only domain controllers (RODCs)) and for each domain that will integrate with Secure Access. The configuration script prepares the domain controllers to communicate with the AD Connector. When you run the script, the domain controller should register with Secure Access.

> **Note**
>
> The script displays your current configuration, and then offers to auto-configure the domain controller. If the auto-configure steps are successful, the script offers to registers the domain controller with Secure Access. Registration only occurs if you accept this offer.

Repeat the steps to add your domain controllers in Secure Access. It is essential that each domain controller in each AD domain environment has the configuration script run on it in order for the service to work as expected, both for high availability and overall reliability.

> **Note**
>
> The configuration script is not an application or service. If you change the IP address or hostname of the domain controller, remove the previous instance of the domain controller and re-register the domain controller.

Procedure

1. As an administrator, open an elevated command prompt.

> **Note**
>
> Before running the script, you must create the `Cisco_Connector` user account. Also, there are several Group Policies that affect system operation that may need manual configuration. The script displays the status of these settings and, if needed, provides instructions on how to change them.

2. Locate the **Windows Configuration Script for Domain Controller** file and run the script in the command prompt.

> **Note**
>
> Substitute the Windows configuration script filename (including the `.wsf` file extension) in the `cscript` command.

```
cscript <Windows Configuration Script filename with extension> or cscript
<Windows Configuration Script filename with extension> --username
<sAMAccountName for custom user>
```

Add a Domain Controller in Secure Access

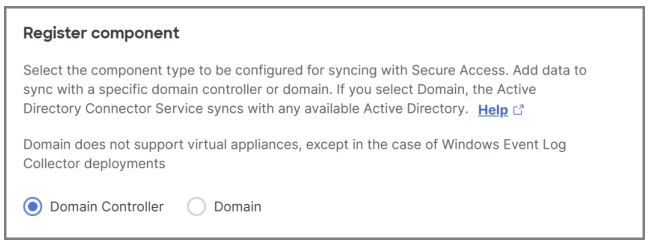
Provides instructions for adding a domain controller in secure access. If the script did not register the domain controller with Secure Access, then add the information for each domain controller in Secure Access.

> **Note**
>
> The configuration script attempts to automatically register the domain controller with Secure Access. This requires the domain controller to support outbound connectivity to Secure Access. If your domain controller can support outbound connectivity to the Internet, ensure that network connectivity requirements are met for the domain controller to automatically register with Secure Access. For more information, see AD Connector Communication Flow and Troubleshooting.

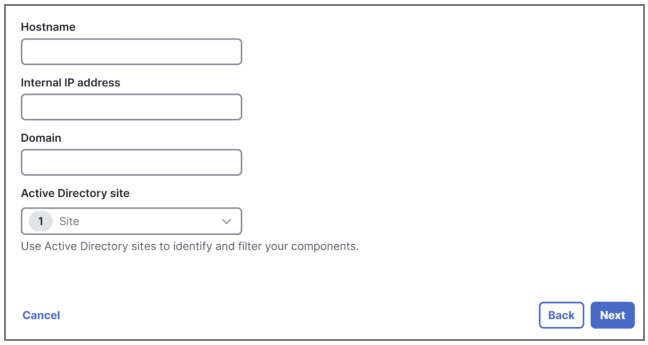
If the script did not register the domain controller with Secure Access, then add the information for each domain controller in Secure Access. After you add the domain controller, the domain controller syncs with Secure Access and you can view the status of the domain controller.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users**, click **Configuration Management** > **Integrate directories**, and then click **Active Directory**.
2. Click **Next**, and then choose **Domain Controller**.



3. Enter the details for the domain controller.
   - **Hostname**–The hostname of the server where the domain controller is deployed.
   - **Internal IP address**–The private IP address of the server where the domain controller is deployed. This field becomes available based on the IP version selection.
   - **Domain**–The domain where the domain controller receives the events.
4. For **Active Directory site**, choose a Secure Access site to associate with the domain controller, and then click **Next**.



5. Deploy the AD Connector.
   For more information, see Connect Active Directory to VAs.
6. On **Installed Active Directory components**, click **Done**.

View the Registered AD Components in Secure Access

Describes viewing the registered ad components in secure access. You can view the status for each deployed AD component in Secure Access. Secure Access displays the hostname of the server where the domain controller is deployed and where you ran the configuration script.

You can view the status for each deployed AD component in Secure Access. Secure Access displays the hostname of the server where the domain controller is deployed and where you ran the configuration script. If you configured multiple sites and deployed VAs, make sure that the AD server is in the same site as the VAs that will receive DNS queries from the users in that AD domain.

For information about viewing the deployed AD components, see View AD Components in Secure Access.

Connect Active Directory to VAs

Describes connecting active directory to vas. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft AD. Before you can provision users and groups from Active Directory, connect your instance of AD to Secure Access by deploying an AD Connector.

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft AD. Before you can provision users and groups from Active Directory, connect your instance of AD to Secure Access by deploying an AD Connector.

Install the AD Connector in the same Site as your deployed Secure Access Virtual Appliances.

The Cisco Active Directory (AD) Connector monitors one or more domain controllers in your environment.

- The AD Connector listens to user and computer logins through the security event logs, and then transmits IP-to-user and IP-to-computer mappings to your deployed Secure Access Virtual Appliances (VAs).
- The AD Connector synchronizes user-to-group, computer-to-group and group-to-group memberships with Secure Access, which enables you to create and enforce group-based settings and view user, computer, and group-based reports.

The AD Connector helps import your Active Directory (AD) users, groups and computers to provide these mappings.

> **Note**
>
> Only one AD Connector is required for each Secure Access Site. For redundancy, add an optional second AD Connector. If you are onboarding multiple AD domains through domain controller integrations, one AD Connector is required per AD domain per Umbrella site, with an optional second connector for redundancy if required.

This guide describes the steps to install the Cisco AD Connector for LDAP or LDAPS, and provision users and groups from your instance of Microsoft AD to Secure Access.

How to Configure the Setup of the AD Connector

Provides instructions for how to configure the setup of the ad connector. The deployment of the AD Connector has various components. You can configure the Cisco AD Connector to provision users and groups from Microsoft AD using LDAP or LDAPS (domain controller or domain).

The deployment of the AD Connector has various components. You can configure the Cisco AD Connector to provision users and groups from Microsoft AD using LDAP or LDAPS (domain controller or domain).

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors and VAs.
- (Optional) Configure Authentication for the AD Connectors and VAs.
- Add the AD components in Secure Access. For more information, see Prepare Your AD Environment.

Procedure

1. (Optional) Configure authentication for the AD Connectors and Secure Access Virtual Appliances (VAs) in your environment.
   For more information, see Configure Authentication for AD Connectors and VAs
2. Download the AD Connector ZIP file from Secure Access.
3. Add a domain controller or domain in Secure Access for LDAP or LDAPS deployments.
   For more information, see Prepare Your AD Environment.
4. Install and configure the AD Connector on your server.
5. Verify that the AD Connector begins to provision users and groups in Secure Access.

(Optional) Specify AD Groups in Selective Sync File

Describes (optional) specify ad groups in selective sync file. You can specify the AD Groups for the purpose of creating access rules in Secure Access. Users and computers belonging to these Groups synchronize to Secure Access.

You can specify the AD Groups for the purpose of creating access rules in Secure Access. Users and computers belonging to these Groups synchronize to Secure Access.

Rename Selective Sync File After Upgrading to AD Connector v1.14.4

If you use selective sync and upgrade the Cisco AD Connectors to v1.14.4 or later, you must rename the current selective sync file `C:\CiscoUmbrellaADGroups.dat` to `C:\CiscoADGroups.dat`.

> **Note**
>
> The selective sync file–previously named `CiscoUmbrellaADGroups.dat`–is not recognized by the Cisco AD Connector v1.1.4.4 or later.

After you rename the selective sync file, Secure Access automatically reads the selective sync file (`C:\CiscoADGroups.dat`) and syncs the Users in the specific Groups from AD to Secure Access. You are not required to restart the AD Connector service.

Create AD Groups in a Selective Sync File

1. Identify the AD Groups of interest. Users and computers belonging to these Groups synchronize to Secure Access. For each sub-tree, only the parent group needs to be specified. All AD groups, users, and computers that are part of this parent group are automatically included.

   > **Note**
   >
   > If you enabled `Selective Sync`, AD Users and Computers that are not members of Groups specified in `CiscoADGroups.dat` or their subgroups are not synchronized to Secure Access and are completely exempt from Secure Access access rules and reports.

2. Create a `CiscoADGroups.dat` file in the `C:\` drive of each machine where the connector is installed. The connector only reads the `C:\CiscoADGroups.dat` file. If the file is incorrectly named or is not present in the `C:\` drive, all groups are imported to Secure Access.
3. List the AD groups that need to be synchronized in `distinguished name` (DN) format in this file.
4. Ensure that there are no blank lines anywhere in the file.

> **Note**
>
> If you are running multiple AD Connectors, the file `C:\CiscoADGroups.dat` should be present on each system running the connector and should be identical on each system.

Supported Organizational Units

```
CN=My Group,OU=Organizational Unit,DC=sample,DC=local
```

Unsupported Organizational Units

```
OU=My OU,OU=Organizational Unit,DC=sample,DC=local
```

Sample File Entries

```
CN=Engineering,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Sales,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Marketing,CN=Builtin,DC=ciscoumbrella,DC=com
```

Total Number of Groups Selected for Synchronization

Groups specified in the selective sync file and all of their subgroups–should not exceed 15,000. Also, these Groups should not be nested within more than five OU levels. Selective synchronization fails in both cases. If you can not meet either of these requirements, we recommend that you do not use the selective sync file. Instead, you can do a full AD tree synchronization.

Procedure

Describes procedure. Download, install, and configure the AD Connector. Step 1 - Set Up Domain Controllers. For more information, see Prepare Your AD Environment. Step 2 - Download the Active Directory Connector Step 3 - Install the Active Directory Connector

Download, install, and configure the AD Connector.

- Step 1 - Set Up Domain Controllers. For more information, see Prepare Your AD Environment.
- Step 2 - Download the Active Directory Connector
- Step 3 - Install the Active Directory Connector

Step 2 – Download the Active Directory Connector

Provides instructions for step 2 - download the active directory connector. Download the AD Connector from Secure Access to your server.

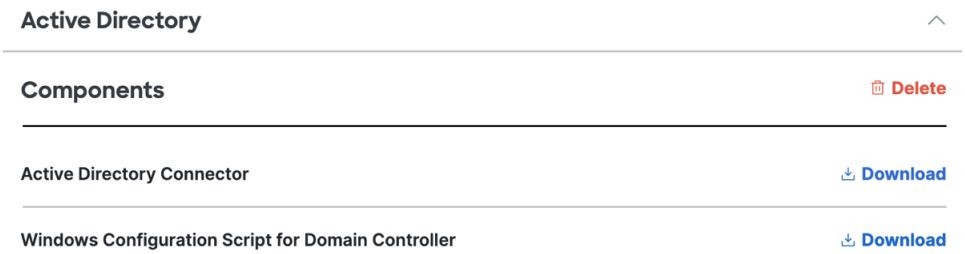
Download the AD Connector from Secure Access to your server.

Note

When you download the AD Connector software package, and if you did not configure API key credentials for the AD Connectors, Secure Access displays a warning message. We recommend that you configure API keys for your AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.

Procedure

1. Configure a server to run the AD Connector, and then sign in to Secure Access on that server.
2. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users** and click **Provision Users**, or navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Groups** and click **Provision Groups**.
3. For **Provisioning Method**, click **Active Directory** or expand **Active Directory**.
4. For **Active Directory Connector**, click **Download** to save the AD Connector deployment package to the server. The deployment package is named: `OpenDNSAuditClient_vX.X.X.zip`.



Note

You must download the ZIP file to the local machine where you plan to run it, or copy it locally from another machine. We do not recommend that you install the AD Connector from a network drive or run `setup.msi` directly from the compressed file.

Step 3 - Install the Active Directory Connector

Provides instructions for step 3 - install the active directory connector. As an administrator, extract the contents of the AD Connector ZIP file to a folder on the server, and then navigate to that folder.

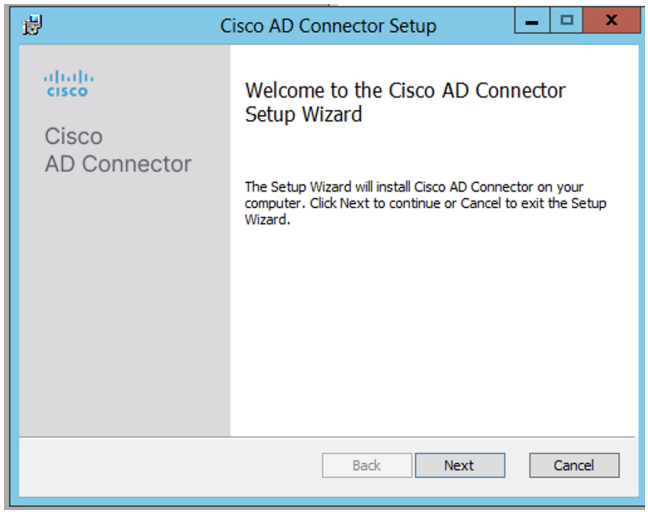
As an administrator, extract the contents of the AD Connector ZIP file to a folder on the server, and then navigate to that folder.

Note

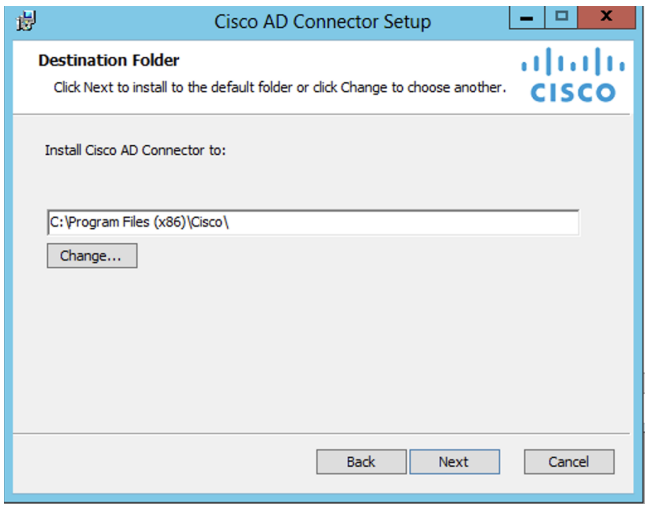
If you run the AD Connector installer from the root directory of your server, you may encounter installation errors.

Procedure

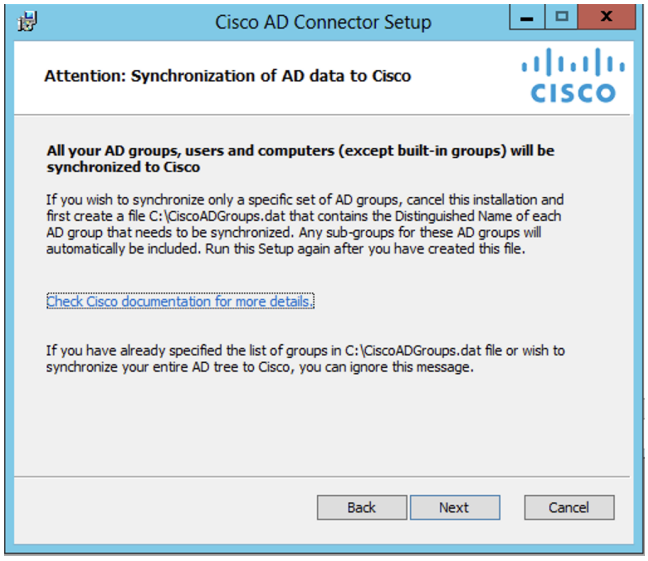
1. Run `setup.msi`, and then in the **Cisco AD Connector Setup** wizard, click **Next**.



2. Choose the directory on the server to install the Cisco AD Connector.



3. Confirm that you permit your AD Users and Groups to sync to Secure Access from the Cisco AD Connector.



4. Add your Active Directory credentials. Enter the **Username** of the Connector user (**Cisco_Connector** or custom username) and the **Password**.

5. Follow the remaining prompts in the setup, and when finished click **Finish**.

What to do next
View the Installed AD Components in Secure Access. For more information, see View AD Components in Secure Access.

Change Connector Account Password

Describes changing connector account password. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- For more information, see Change the Connector Account Password.

Configure Updates to AD Connectors

Describes configuring updates to ad connectors. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- For more information, see Configure Updates on AD Connectors.

Multiple AD Domains with Secure Access Sites

Describes multiple ad domains with secure access sites. Cisco Secure Access Sites let administrators create separate Secure Access deployments. Each Secure Access Site is an isolated deployment where components only communicate with other components in the same Secure Access Site.

Cisco Secure Access Sites let administrators create separate Secure Access deployments. Each Secure Access Site is an isolated deployment where components only communicate with other components in the same Secure Access Site. Secure Access Sites are a container to isolate sections of a large multi-site network into groups which only sync to the other components in the container. For example, Secure Access sites may be North America, Asia, and Europe or Northeast, California, Atlanta office, South Region, and London, and each Secure Access Site may be one or a combination of Active Directory (AD) sites.

This is useful in AD environments containing locations with high-latency connections, or in environments with locations whose internal IP space overlaps.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Active Directory Sites and Secure Access Sites

Describes active directory sites and secure access sites. A site represents a set of computers connected by a high-speed network, such as a local area network (LAN). Typically, all computers in the same physical site reside in the same building or perhaps the same campus network.

A site represents a set of computers connected by a high-speed network, such as a local area network (LAN). Typically, all computers in the same physical site reside in the same building or perhaps the same campus network. AD and Umbrella both use the term "sites", and while related, have slightly different meanings.

Active Directory Sites and Services

- For AD, a site object represents the actual directory data that is replicated between domain controllers.
- AD sites are used to manage the objects that represent the site, and the servers that reside in the site.

Secure Access Sites

- A Secure Access Site refers to a set of components—Virtual Appliances (VAs), Cisco AD Connectors, and domain controllers—that communicate only with each other.
- A Secure Access Site is more than a label and is more like a container. A Secure Access Site is not the same as an AD site. Multiple AD sites can be part of an Secure Access Site, but one AD site should not be split into multiple Secure Access Sites.
- A site must have a minimum of two VAs, and one connector and domain controller for an AD integration.

Because Secure Access Sites act as isolated deployments, each Secure Access Site must have a minimum of two VAs. If AD integration is also being used, each site must additionally contain a minimum of one AD connector and all domain controllers against which a user in that location authenticates.

When to Use Secure Access Sites

- You need to limit WAN traffic between locations and are using AD sites to limit authentication to local servershttp://technet.microsoft.com/en-us/library/cc782048(v=ws.10).aspx.
- Your locations communicate between a NAT device, which causes the internal IP address of an end machine to be lost when communicating between locations.
- Your locations use overlapping internal IP ranges.
- You have locations which have high-latency connections between them—for example, branches in different continents. High latency connections, especially between the connector and the VAs, can result in delays to updates for user mappings.

Caveats

The isolation of the components in a given Secure Access Site means that a specific VA will only be aware of users who have authenticated against domain controllers assigned to the same Secure Access Site. As a result, we do not recommend using multiple Secure Access Sites in a single AD site, even if that AD site spans multiple geographical locations. In such a scenario, users in a location may still authenticate against a DC in a different location, and thus the Secure Access components may miss user mappings.

Use Secure Access Sites

Describes using secure access sites. Configure individual Secure Access Sites as if they are complete deployments. Ensure that there are at least two VAs, one AD server and one AD Connector assigned to each site.

Configure individual Secure Access Sites as if they are complete deployments. Ensure that there are at least two VAs, one AD server and one AD Connector assigned to each site. Verify a complete, functioning deployment at each site before moving on to the next site. For more information, see Manage Site for VA.

Active Directory Only

If you change the location of a Secure Access VA, the AD Connector, or domain controller after you've installed the connector service, you must Stop/Start the AD Connector service on each connector for the Sites through the Services management tool in Windows.

12 Manage End-User Connectivity

Topics:

- Manage End-User Connectivity

Describes the purpose and procedures for manage end-user connectivity and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage End-User Connectivity

Describes managing end-user connectivity. Secure Access provides secure connectivity to the internet and your digital resources. To route network traffic from endpoints securely, you can:

Secure Access provides secure connectivity to the internet and your digital resources. To route network traffic from endpoints securely, you can:

- Manage the DNS servers deployed in your organization
- Manage private resources configured for Zero Trust access
- Manage client IP address ranges and profiles used by virtual private networks (VPNs)
- Protect or bypass traffic to certain internet resources
- Configure comprehensive endpoint internet security settings

DNS Servers

Add DNS servers to resolve DNS requests for certain domains from remote clients. For more information, see Manage DNS Servers.

Traffic Steering for Cisco Secure Client Connections

View traffic steering rules for zero trust connections. Or, for certain private resource configurations, you can specify subdomains to exclude from zero trust access. See Traffic Steering for Client-Based Zero Trust Connections.

Virtual Private Networks Settings and Profiles

Configure VPN settings and profiles. For more information, see Manage Virtual Private Networks.

Internet Security

Steer traffic from endpoints to Secure Access or directly to the internet. For more information, see Manage Internet Security.

13 Manage Users, Groups, and Endpoint Devices

Topics:

- Manage Users, Groups, and Endpoint Devices

Describes the purpose and procedures for manage users, groups, and endpoint devices and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Users, Groups, and Endpoint Devices

Describes managing users, groups, and endpoint devices. Provision users and groups in Cisco Secure Access from your organization's identity provider (IdP) or by importing a comma separated values (CSV) file with the users and groups.

Provision users and groups in Cisco Secure Access from your organization's identity provider (IdP) or by importing a comma separated values (CSV) file with the users and groups. Once you add users and groups to Secure Access, you can protect and monitor the traffic sent from the user devices and manage the resources that are available to the users in your organization. Secure Access supports various methods to provision users and groups.

Provision Users and Groups

- Import Users and Groups from CSV File
- Configure and integrate an identity provider (IdP) with Secure Access. Create an identity provider access token and configure your identity provider.
  - Provision Token for Identity Provider
  - Provision Users and Groups from Okta
  - Provision Users and Groups from Azure
- Provision Users and Groups from Active Directory Federated Services

View Users and Groups in Secure Access

- View User Details
- View Group Details

View User Details

Provides instructions for viewing user details. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

After an administrator provisions users in Secure Access, you can view details about the users and identify the policy rules applied to the users.

View provisioned users and groups in Secure Access.

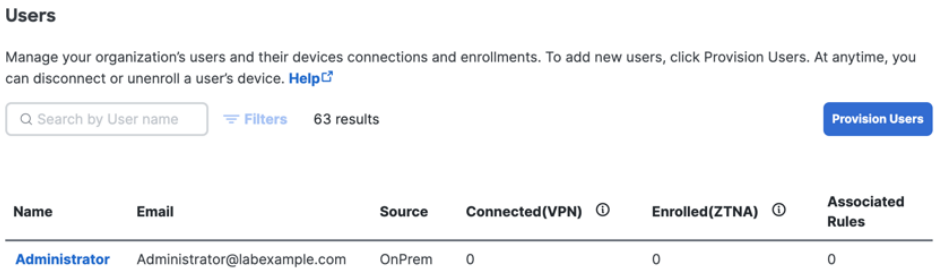
Before you begin

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

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** .
2. Click **Users** to view the users provisioned in the organization.
   - **Name**–The first and last names of the user.
   - **Email**–The email address of the user.
   - **Source**–The method or identity provider used to provision the user.
   - **Connectivity (VPN)**–The number of connections made from virtual private networks (VPNs).

- **Enrolled (ZTNA)**–The number of connections made from a user and device managed by Secure Access Zero Trust Access.
- **Associated Rules**–The Secure Access policy rules that include the user.
- **Source**–The method used to provision the user.



3. Find a user in the organization and click on the **Name** of the user to open the **User Details**.

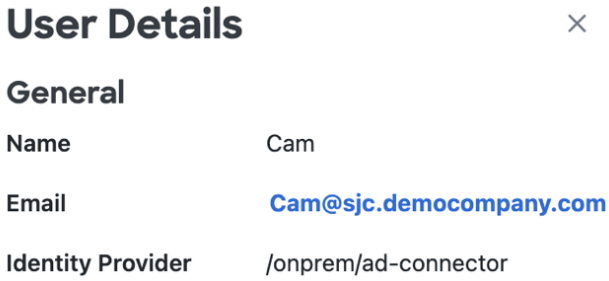
User Details

Describes user details. The information about the user in the organization. Name–The name of the user. Email–The email of the user.

The information about the user in the organization.

General User Details

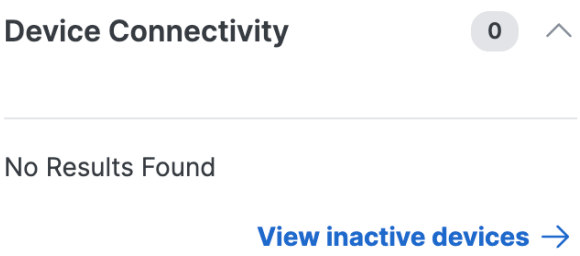
- **Name**–The name of the user.
- **Email**–The email of the user.
- **Identity Provider**–The identity provider that manages the user information.



Device Connectivity

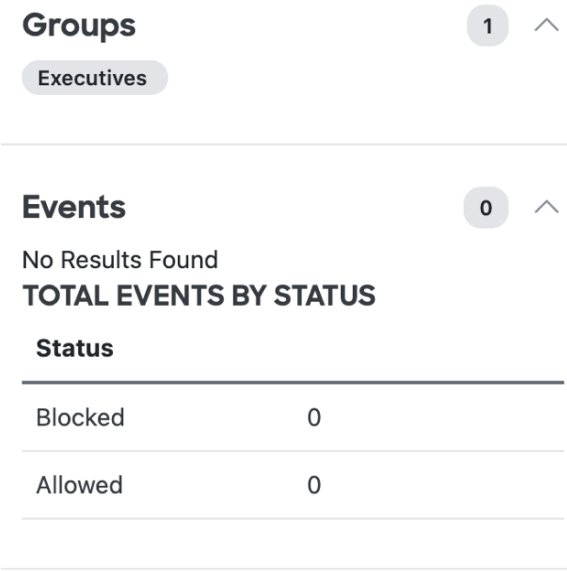
The list of devices associated with the user.

- **Connection**–The type of connection
- **IP address**–The IP address of the device.
- **OS Version**–The version of the device's operating system.



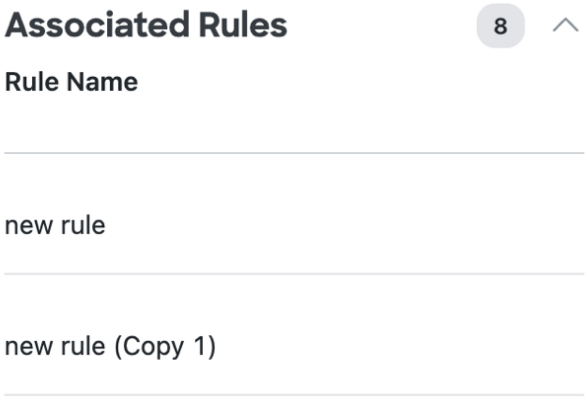
Groups and Events

- **Groups**–The number of groups that include the user and the name of the groups.
- **Events**–The number of events created by the user and the status of the events.



Associated Rules

The Secure Access policy rules applied to the user.



View Group Details

Provides instructions for viewing group details. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

After an administrator provisions groups in Secure Access, you can view the details about the groups and identify the policy rules applied to the groups.

Before you begin

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

Procedure

Navigate to **Connect** > **Users, Groups, and Endpoint Devices** and then click **Groups** to view the groups provisioned in the organization.

- **Name**–The name of the group.
- **Users**–The number users in the group.
- **Associated Rules**–The Secure Access policy rules that include the group.
- **Source**–The method or identity provider used to provision the group.

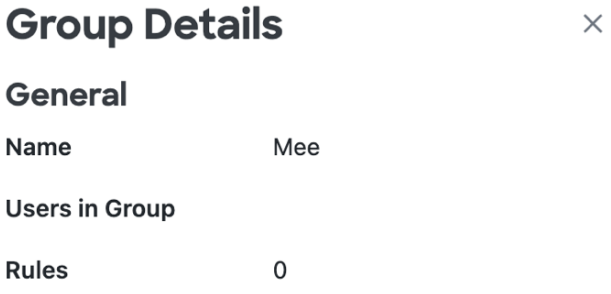
Group Details

Describes group details. The information about the organization's group. Name–The name of the group. Users in Group–The number of users in the group and the label for the group.

The information about the organization's group.

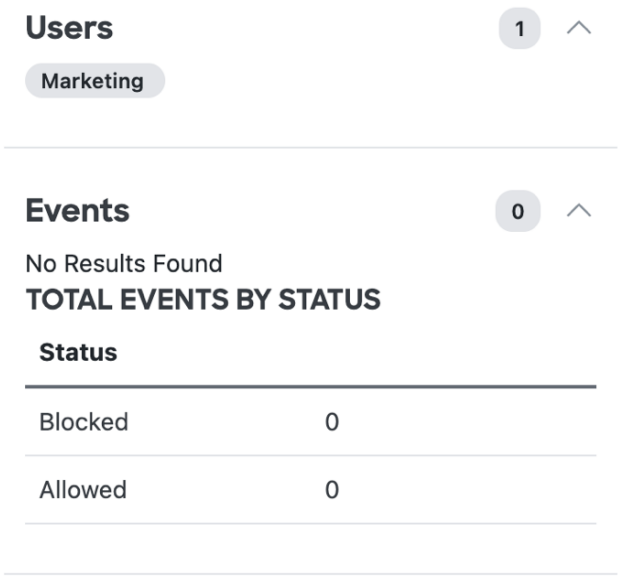
General Group Details

- **Name**–The name of the group.
- **Users in Group**–The number of users in the group and the label for the group.
- **Rules**–The number of rules that include this group.



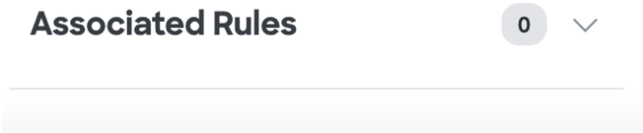
Users and Events

The number of users in the group and the status of the events created by the users.



Associated Rules

The number of Secure Access policy rules applied to the users in the group.



View Organizational Units

Provides instructions for viewing organizational units. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Administrators can use Identity Providers (IdPs) integrated with Secure Access to provision Google Chromebook Organizational Units (OUs) in Secure Access. Once OUs are provisioned, you can view their details and the access rules that apply to users and endpoint devices in those OUs.

View the provisioned groups in Secure Access.

Before you begin

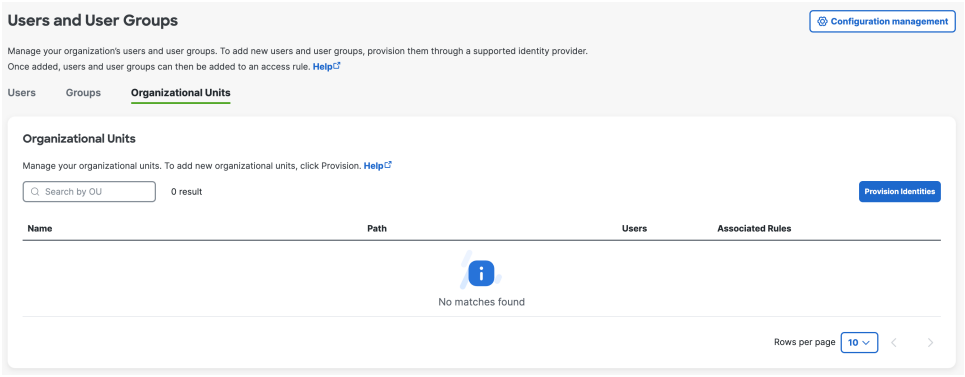
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

Navigate to **Connect** > **Users, Groups, and Endpoint Devices** , then click **Organizational Units**.

Secure Access lists the provisioned OUs.

- **Name**–The name of the OU.
- **Path**–The directory path of the OU.
- **Users**–The number, names, and email addresses of users in the OU.
- **Associated Rules**–The number and names of access rules applied to users in the OU.



Provision Token for Identity Provider

Describes provisioning token for identity provider. Cisco Secure Access uses the System for Cross-domain Identity Management (SCIM) protocol to exchange user and group information with various identity providers (IdPs): Azure, Okta, and other IdPs. You can provision your organization's users and groups into Secure Access through integrations with IdPs.

Cisco Secure Access uses the System for Cross-domain Identity Management (SCIM) protocol to exchange user and group information with various identity providers (IdPs): Azure, Okta, and other IdPs. You can provision your organization's users and groups into Secure Access through integrations with IdPs. In Secure Access, generate a Secure Access SCIM token and get the Secure Access Identity URL. Then, from the IdP add your token and API Identity URL to establish the integration.

Prerequisites

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

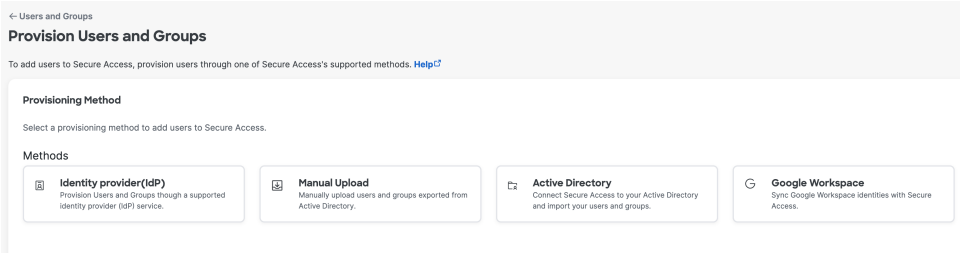
Procedure for Provision Token for Identity Provider

Provides instructions for procedure for provision token for identity provider. Its purpose, requirements, and key details for Cisco Secure Access administrators.

Generate an SCIM token for an IdP and save the token to your local system. Copy and save the Secure Access Identity API URL. Use the Secure Access SCIM token and URL to configure the integration with an IdP.

Procedure

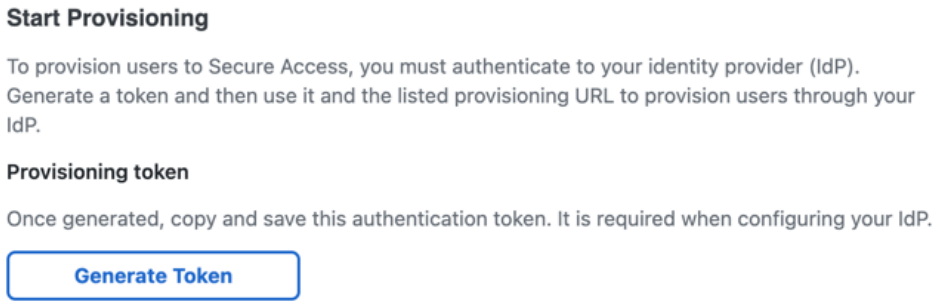
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users** and click **Provision Users** or **Connect** > **Users, Groups, and Endpoint Devices** > **Groups** and click **Provision Groups**.
2. For **Provisioning Method**, click **Identity Provider**.



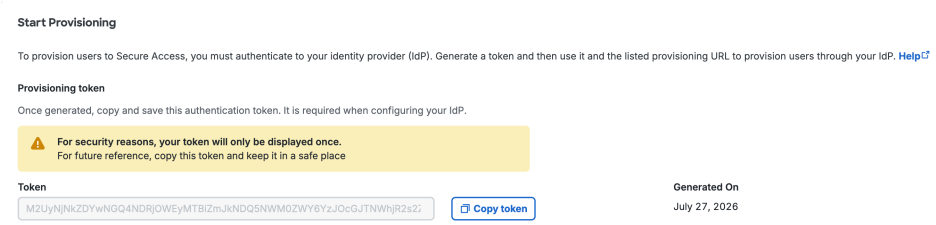
3. Choose an identity provider and then click **Next**.



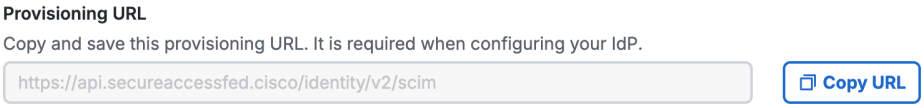
4. Click **Generate Token** to create a provisioning API access token for your integration with the IdP.



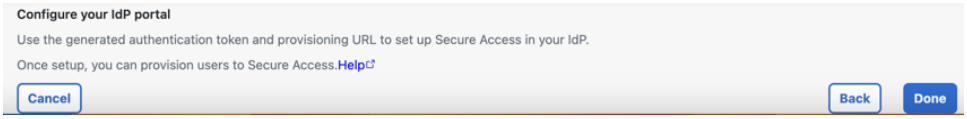
5. Click **Copy token** to copy the generated token. Save the token to your local system.



6. Click **Copy URL** to copy the Secure Access Identity API URL. Save the URL to your local system.



7. Click **Done**.



Configure Identity Providers

Describes configuring identity providers. With your Secure Access SCIM token and Identity API URL, configure a supported IdP to provision users and groups in Secure Access.

With your Secure Access SCIM token and Identity API URL, configure a supported IdP to provision users and groups in Secure Access.

- Provision Users and Groups from Okta
- Provision Users and Groups from Azure

Unenroll Devices for Client-Based Zero Trust Access

Describes unenroll devices for client-based zero trust access. After a user enrolls their device for zero trust access on the Cisco Secure Client, the device appears on Secure Access. The user's device can create secure zero trust sessions and connect to their organization's private resources.

After a user enrolls their device for zero trust access on the Cisco Secure Client, the device appears on Secure Access. The user's device can create secure zero trust sessions and connect to their organization's private resources.

If you need to remove a user device that has zero trust access enabled from the organization, you can unenroll the user's device on Secure Access. The unenroll administrative action has these consequences:

- Prevents new zero trust connections from the device.
  - The user device can not create any new zero trust sessions to private resources.
  - Any existing zero trust connections on the device remain active until the user unenrolls the Zero Trust Access on the Cisco Secure Client.
- Invalidates the devices's zero trust certificate.

Reenroll the User Device on the Secure Client

Describes reenroll the user device on the secure client. After you unenroll a device on Secure Access, the end user can reenroll their device to enable zero trust access from the Cisco Secure Client. For more information, see Invite Users to Enroll in Zero Trust Access for Secure Client.

After you unenroll a device on Secure Access, the end user can reenroll their device to enable zero trust access from the Cisco Secure Client. For more information, see Invite Users to Enroll in Zero Trust Access for Secure Client.

Procedure for Unenroll Devices for Client-Based Zero Trust Access

Provides instructions for procedure for unenroll devices for client-based zero trust access. Its purpose, requirements, and key details for Cisco Secure Access administrators.

Unenroll user devices on Secure Access that have enabled zero trust access on the Secure Client.**Important**

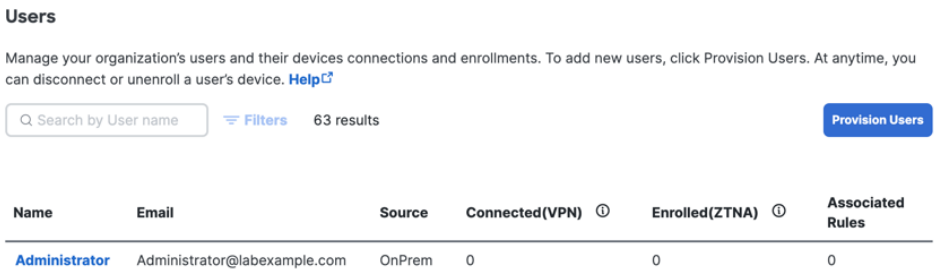
After you unenroll a user device with zero trust access in Secure Access, the device may have active zero trust connections to Secure Access from the Secure Client on the device.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- A user device that has enrolled in zero trust access on the Cisco Secure Client.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** .
2. Click **Users** to view the users provisioned in the organization.
3. Click on the **Name** of a user that has configured **Enrolled (ZTNA)**.



4. For **User Details**, navigate to **Client-based ZTA**, and then click **Unenroll ZTNA**.

5. Click **Unenroll ZTNA**, and then confirm the removal of the user device.

Disconnect Remote Access VPN Sessions

Provides instructions for disconnect remote access vpn sessions. You can disconnect a user's remote access VPN session from Secure Access. The disconnect administrative action has these consequences:

After a user connects to your network on the Cisco Secure Client from a remote location, using a computer or other supported iOS or Android device connected to the Internet, the device appears on Secure Access.

You can disconnect a user's remote access VPN session from Secure Access. The disconnect administrative action has these consequences:

1. Prevents new remote access VPN sessions from the device.

   The user device can not access private resources.

2. Revokes the device's certificate.

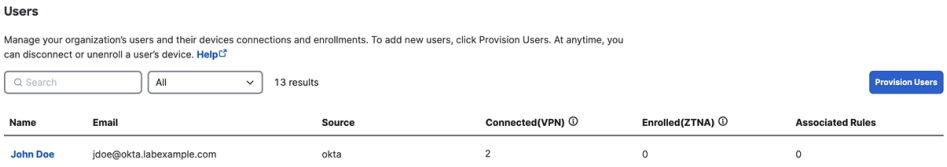
Disconnect users on Secure Access that have established remote access VPN sessions on the Secure Client.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- A user device that has a remote access VPN connection on the Cisco Secure Client to your network from a remote location.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** .
2. Click **Users** to view the users provisioned in the organization.
3. Click on the **Name** of a user that has configured **Connected(VPN)**.



4. For **User Details**, navigate to **Device Connectivity**, and scroll through the device list to find the session you want to disconnect.
5. Under **VPN Access** click **Disconnect device**.
6. Click **Disconnect** to confirm the removal of the user device.

Import Users and Groups from CSV File

Describes importing users and groups from csv file. Secure Access supports provisioning users and groups manually from a comma-separated values (CSV) file. You must export your Microsoft Active Directory (AD) users and groups to a CSV file. We recommend using CSVDE.EXE from a domain controller.

Secure Access supports provisioning users and groups manually from a comma-separated values (CSV) file. You must export your Microsoft Active Directory (AD) users and groups to a CSV file. We recommend using `CSVDE.EXE` from a domain controller.

For each upload, the CSV file can have up to 4000 rows. An import may require ten minutes. Each subsequent CSV file upload replaces the contents of the previous upload. For large numbers of users and groups, we recommend using AD provisioning.

> **Note**
>
> To switch from AD provisioning to CSV import, you must uninstall your Secure Access AD Connectors and delete the AD Connectors in Secure Access. For more information, see Provision Users and Groups from Active Directory.

Prerequisites for Import Users and Groups from CSV File

Describes prerequisites for import users and groups from csv file. Full Admin user role. For more information, see Manage Accounts.

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

CSV File Format

The CSV file must include the users and groups information in a comma delimited format.

Header row:

```
sn,givenName,userPrincipalName,mail,memberOf
```

Object row:

```
"CN=SMUser,CN=Users,DC=mycompany,DC=local",last_name_1,first_name_1,smuser@mycompany.com,smuser@mycompany.com,"CN=Group2,CN=Users,DC=mycompany,DC=com"
```

The following characters are not supported:

```
%<([{\\^-=$!|]})?*+>
```

CSV File Fields

Field	Required	Notes	Supported Number of Characters
DN		"CN=SMUser,CN=Users,DC=mycompany,DC=local"	64
sn	:heavy_check_mark:	The user's surname (family name or last name).	64
givenName	:heavy_check_mark:	The user's given name (legal first name).	64

Field	Required	Notes	Supported Number of Characters
userPrincipalName	:heavy_check_mark:	The `userPrincipalName` corresponds to the principal that Secure Access receives in the SAML assertion, and is often identical to the object's mail attribute. However, this is not always the case. The `userPrincipalName` is constant, but the mail attribute may change. Example: samluser@mycompany.com	64
mail	:heavy_check_mark:	Only valid email addresses. Example: samluser@mycompany.com	256
memberOf		"CN=Group2,CN=Users,DC=mycompany,DC=local"	1024

A user may belong to multiple groups, which are defined in the `memberOf` attribute.

An example value of the `memberOf` field:

```
"CN=Group1,CN=Users,DC=dcloud,DC=local;CN=Group2,CN=Users,
DC=dcloud,DC=local;CN=Group3,CN=Users,DC=dcloud,DC=local;
CN=Group4,CN=Users,DC=dcloud,DC=local"
```

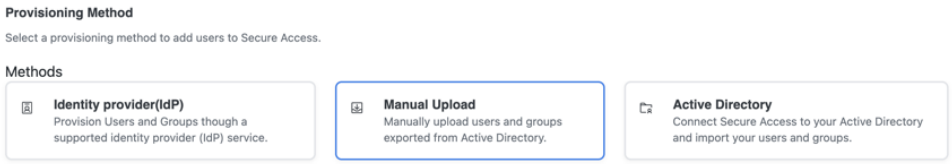
Procedure for Import Users and Groups from CSV File

Provides instructions for procedure for import users and groups from csv file. Its purpose, requirements, and key details for Cisco Secure Access administrators.

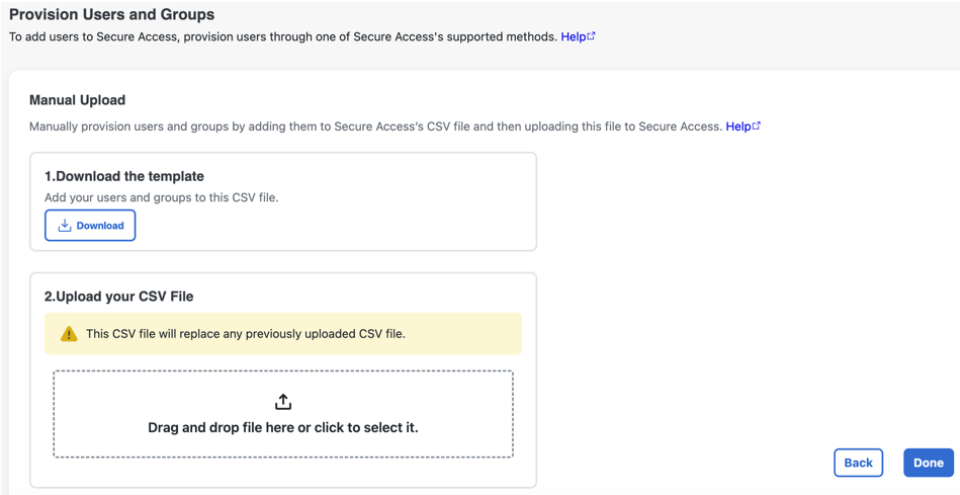
Import users into Secure Access from a comma-separated values (CSV) file.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Users** and click **Provision Users** or **Connect** > **Users, Groups, and Endpoint Devices** > **Groups** and click **Provision Groups**.
2. For **Provisioning Method**, click **Manual Upload** to provision users or groups in your organization.



3. Click **Download** to save the Secure Access import template (CSV file) to your local system.
4. Add users or groups to the Secure Access CSV template file, and then upload the CSV file to Secure Access.



For example:

```
sn,givenName,userPrincipalName,mail,memberOf
last_name1,first_name1,emp20@cisco.com,emp20@cisco.com,adminGroup
last_name2,first_name2,emp2@cisco322.onmicrosoft.com,emp2@cisco322.onmicrosoft.com,adminGroup
last_name3,first_name3,user5@vvaidya.com,user5@vvaidya.com,adminGroup
last_name4,first_name4,employee1@company.com,employee1@company.com,adminGroup
last_name5,first_name5,demouser@company.com,demouser@company.com,adminGroup
```

5. Click **Done**.

View Provisioned Users and Groups in Secure Access

Provides instructions for viewing provisioned users and groups in secure access. Navigate to Connect Users, Groups, and Endpoint Devices to view the users and groups provisioned in your organization.

Procedure

Navigate to **Connect** > **Users, Groups, and Endpoint Devices** to view the users and groups provisioned in your organization.

For more information, see View User Details and View Group Details.

Provision Users and Groups from Okta

Describes provisioning users and groups from okta. Cisco Secure Access supports the provisioning of users and groups from Okta. With your Secure Access System for Cross-domain Identity Management (SCIM) token, configure the Cisco User Management Connector Gov app on the Okta portal.

Cisco Secure Access supports the provisioning of users and groups from Okta. With your Secure Access System for Cross-domain Identity Management (SCIM) token, configure the **Cisco User Management Connector Gov** app on the Okta portal. Once you add users and groups in the app, Okta begins to exchange the user and group information with Secure Access.

> **Note**
>
> You do not need to deploy an on-premises Secure Access Active Directory (AD) Connector.

Prerequisites for Provision Users and Groups from Okta

Describes prerequisites for provision users and groups from okta. Full Admin user role. For more information, see Manage Accounts. A valid Okta subscription.

- Full Admin user role. For more information, see Manage Accounts.
- A valid Okta subscription.
- A valid SCIM token generated in Secure Access. For more information, see Provision Token for Identity Provider.
- No concurrent provisioning of the same users or groups from on-premises AD and Okta. If you are using the on-premises Secure Access AD Connector to import users and groups and choose to import the same users and groups from Okta, ensure that the on-premises Secure Access AD connector is switched off or that the OpenDNS Connector service on the connector machine is stopped.
- For IP-to-user mapping deployments, you must use an on-premises Secure Access AD connector. Okta does not store the private IP to AD user mappings.

Limitations for Provision Users and Groups from Okta

Describes limitations for provision users and groups from okta. Secure Access supports provisioning a maximum of 200 groups from Okta. Any groups beyond this number that are in scope are not provisioned. Secure Access does not restrict the number of users that you can provision from Okta.

- Secure Access supports provisioning a maximum of 200 groups from Okta. Any groups beyond this number that are in scope are not provisioned. Secure Access does not restrict the number of users that you can provision from Okta.
- To ensure that all users are provisioned, assign the `Everyone` group to the **Cisco User Management Connector Gov** app. You can push other additional groups for group-based Secure Access policy enforcement.
- Okta does not support nested groups.
- If you previously imported groups from on-premises AD and push the same groups from Okta, the groups from Okta do not overwrite the groups imported from the on-premises AD. You must reassign any group-based Secure Access policy rules to the groups imported from Okta.
- Provisioning large numbers of users and groups to Secure Access may take several hours.
- After the initial provisioning of users and groups, it can take up to one hour for subsequent changes to users and groups to reflect in Secure Access.
- Concurrent synchronization of the same users and groups from the Secure Access AD Connector and the **Cisco User Management Connector Gov** app is not supported and leads to inconsistent policy enforcement.

Supported Features

Describes supported features. The following Okta provisioning features are supported: Create Users–New users created in Okta are also created in Secure Access.

The following Okta provisioning features are supported:

- **Create Users**–New users created in Okta are also created in Secure Access.
- **Update User Attributes**–Updates to a user's profile through Okta are pushed to Secure Access.

- **Deactivate Users**–Deactivating a user through Okta deactivates the user in Secure Access.
- **Group Push**–Groups in Okta are pushed to Secure Access.

Import the ObjectGUID Attribute from Okta to Secure Access

Provides instructions for importing the objectguid attribute from okta to secure access. You have endpoints that authenticate against on-premises AD and run the Cisco Secure Client.

The on-premises Secure Access AD Connector and the Cisco Secure Client rely on the `objectGUID` attribute for user and group identification. Ensure that the `objectGUID` attribute of users is synchronized from Okta to Secure Access only if either of the following conditions are true:

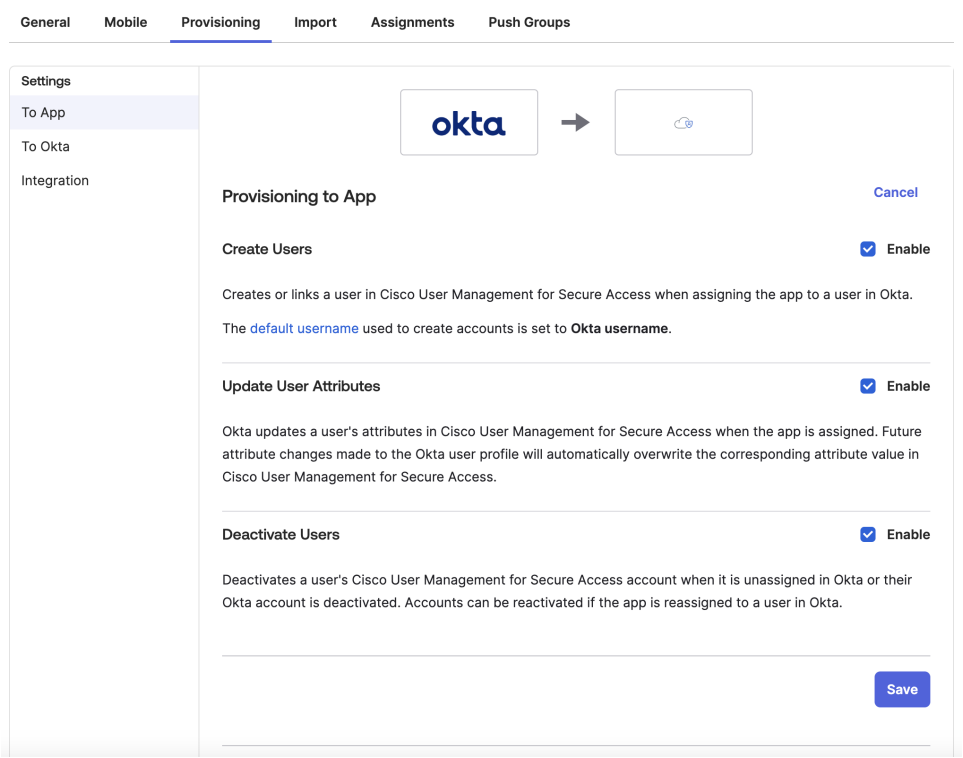
1. You have previously imported AD users to Secure Access using the on-premises Secure Access AD connector, are now importing the same user identities from Okta, and want the previously imported identities to be persisted for policy or reporting purposes.
2. You have endpoints that authenticate against on-premises AD and run the Cisco Secure Client.

> **Note**
>
> Before setting up the import of the `objectGUID`, ensure that the on-premises Secure Access AD Connector that synchronizes these users and groups is switched off or that the OpenDNS Connector service on the connector machine is stopped.

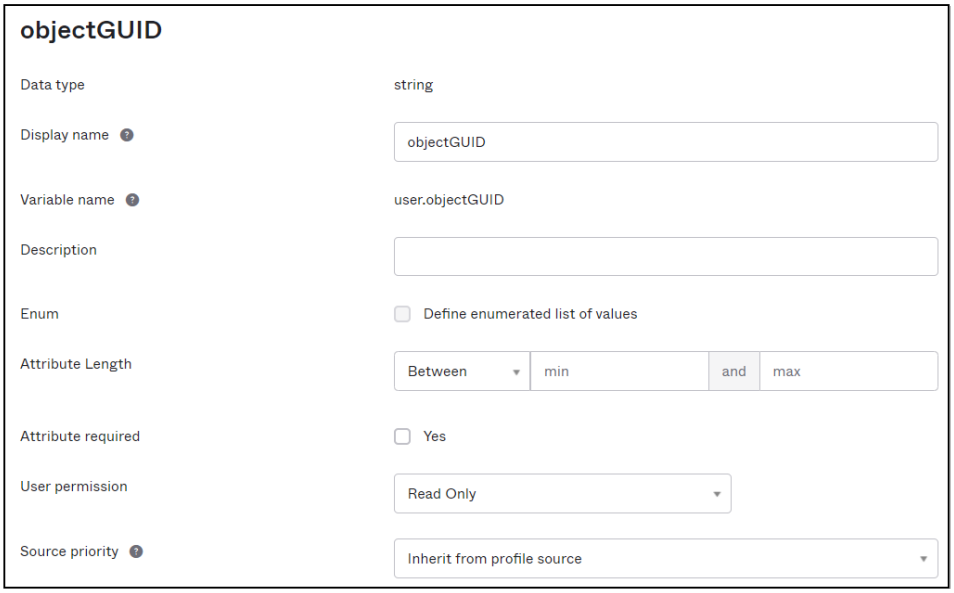
The Okta Active Directory agent does not synchronize the `objectGUID` attribute of users from on-premises AD to Okta by default.

Procedure

1. Navigate to the **Provisioning** tab on the **Cisco User Management Connector Gov** app in Okta.
2. From **Settings** > **To App**, navigate to **Profile Editor**.



3. For **Okta Attribute Mappings**, click **Add Attribute** to create a custom attribute of string type called `objectGUID`.



4. For **Cisco User Management Connector Gov User Profile Mappings**, create a new **User Profile Mapping** for your AD domain that maps the Okta User `appuser.externalId` to the `user.objectGUID` .
5. For **Okta Attribute Mappings**, do a **Force Sync** of attributes to ensure that the `objectGUID` attribute for users is imported from AD.

Configure the Cisco Secure Access App

Describes configuring the cisco secure access app. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Configure the **Cisco User Management Connector Gov** app on the Okta portal.

> **Note**
>
> The **To Okta** setting is not supported on the **Cisco User Management Connector Gov** app.

Step 1 – Add the App to Okta

Provides instructions for step 1 – add the app to okta. Sign in to Okta and add the Cisco User Management Connector Gov app to your instance of Okta.

Procedure

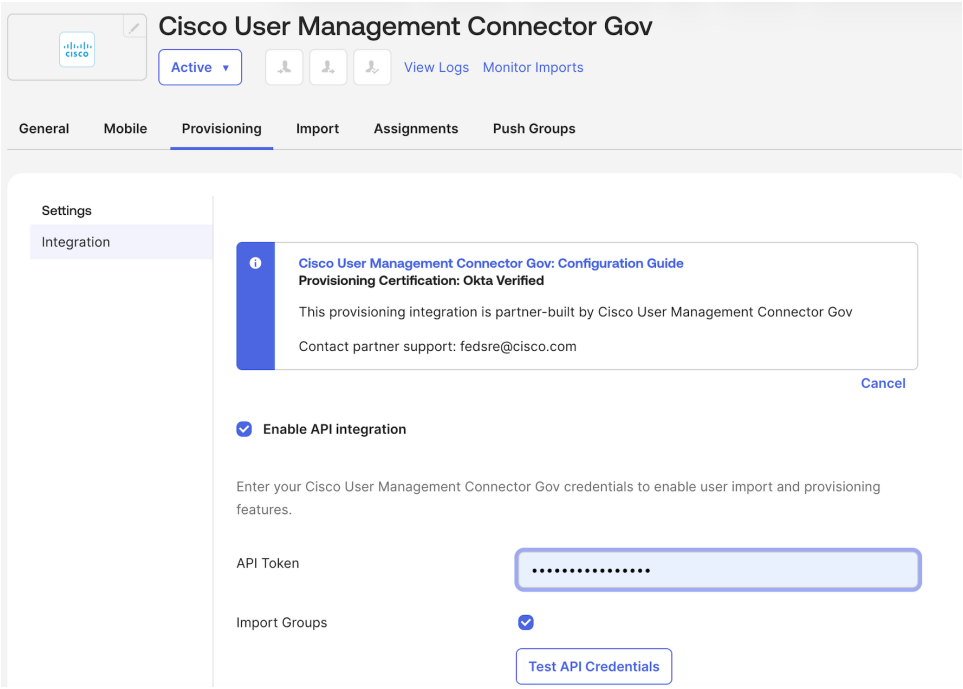
Sign in to Okta and add the **Cisco User Management Connector Gov** app to your instance of Okta.

Step 2 – Add the Secure Access SCIM Token to the App

Provides instructions for step 2 – add the secure access scim token to the app. Navigate to the Provisioning tab on the Cisco User Management Connector Gov app in Okta.

Procedure

1. Navigate to the **Provisioning** tab on the **Cisco User Management Connector Gov** app in Okta.
2. From **Settings** > **Integration**, select **Enable API Integration**, and then add the Secure Access SCIM API token.
3. Click **Test API credentials**, to confirm that you can use your Secure Access SCIM token to connect the Secure Access API with Okta, and then click **Save**.

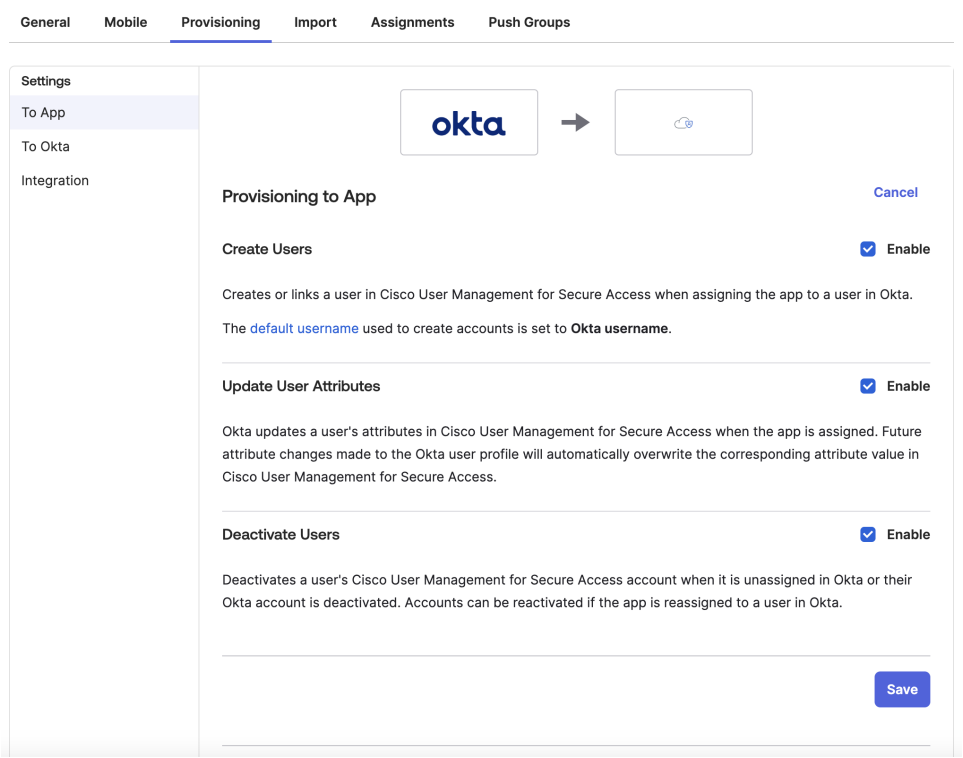


Step 3 – Configure the Required User Options

Provides instructions for step 3 – configure the required user options. Navigate to the Provisioning tab on the Cisco User Management Connector Gov app in Okta.

Procedure

1. Navigate to the **Provisioning** tab on the **Cisco User Management Connector Gov** app in Okta.
2. From **Settings** > **To App**, enable the **Create Users**, **Update User Attributes**, and **Deactivate Users** options. You must select these options to provision users or groups.

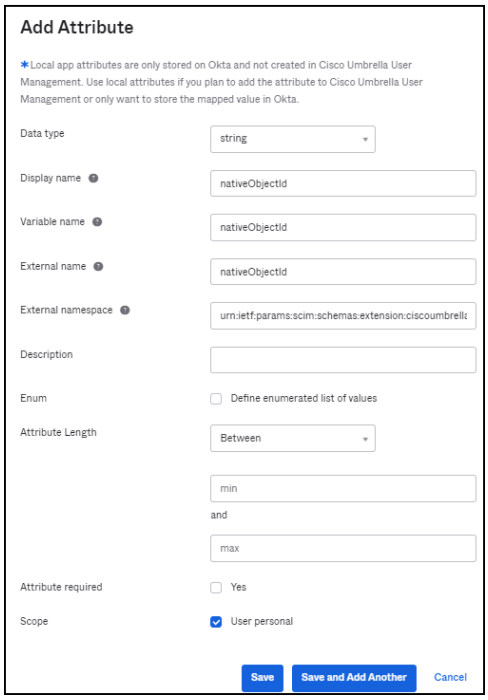


3. Verify that the following attributes are chosen for synchronization to Secure Access. Other attributes are not required. Secure Access does not list the **Given name** and **Family name** attributes for users. Secure Access only lists the **Display name** and **Username** attributes.
   - **Username**
   - **Given name**
   - **Family name**
   - **Display name**
   - **Primary email**

Step 4 – (Optional) Add a New Attribute and Create the User Profile Mapping

Provides instructions for step 4 – (optional) add a new attribute and create the user profile mapping. Its purpose, requirements, and key details for Cisco Secure Access administrators.

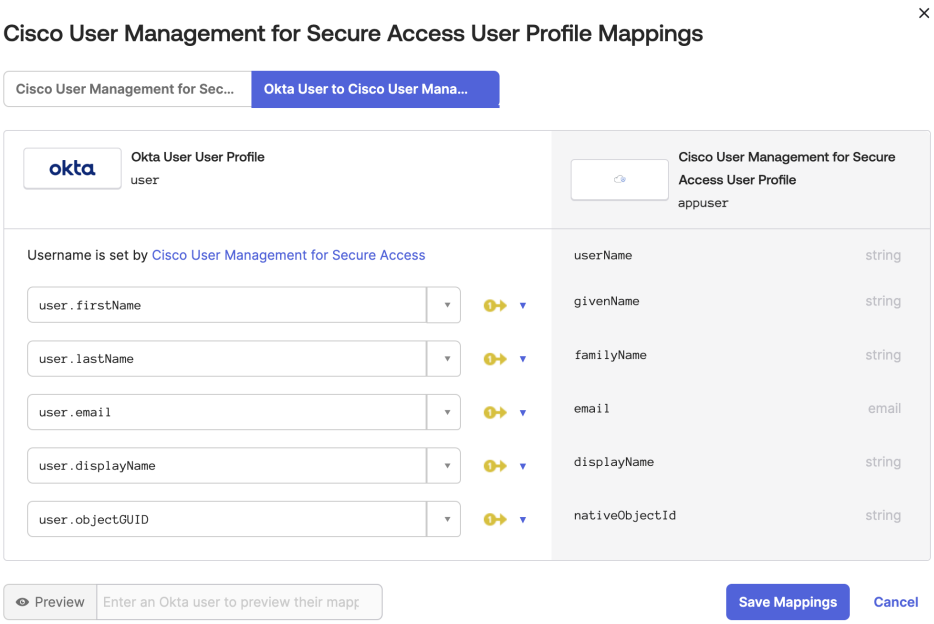
If you need to import the `objectGUID` attribute for users, add a new attribute and map the attributes in the profile mapping.



Procedure

1. Navigate to the **Provisioning** tab on the **Cisco User Management Connector Gov** app in Okta.
2. From **Settings** > **To App**, navigate to **Profile Editor**.
3. Click **Add Attribute**.
   a. Set **Display name**, **Variable name**, and **External name** to `nativeObjectId`.
   b. For **Scope**, click **User personal**.
   c. Set **External namespace** to `urn:ietf:params:scim:schemas:extension:ciscoumbrella:2.0:user`
4. Click **Save**.

   Add the new user profile mapping.
5. Navigate to the **Provisioning** tab on the **Cisco User Management Connector Gov** app in Okta.
6. From **Settings** > **To App**, navigate to **Profile Editor**.
7. For **Cisco User Management Connector Gov User Profile Mappings**, create a new **Okta User Profile** that maps the Okta User to the **Cisco User Management Connector Gov** user. The profile must map the `user.objectGUID` to `nativeObjectId`.
8. Click **Save Mappings** to save the profile mapping. Select the option to **Apply the Mappings to All Users with this Profile**.



Step 5 – Assign Users and Groups in the App

Provides instructions for step 5 - assign users and groups in the app. Its purpose, requirements, and key details for Cisco Secure Access administrators.

Once you complete the provisioning configuration, assign users in the **Cisco User Management Connector Gov** app.

Procedure

1. Navigate to the **Assignments** tab on the **Cisco User Management Connector Gov** app in Okta.

   You can assign individual users or specific groups to the app. To assign all users, assign the `Everyone` group to the app.

   > **Note**
   >
   > Assigning groups to the app does not provision these groups to Secure Access. Okta only provisions users that are members of the assigned groups. Do not manually change the value of the `nativeObjectId` field when assigning any groups and users.

2. Once users and groups are assigned, these users automatically begin to provision to Secure Access. Wait for all users to show up in Secure Access before starting to push groups. This can take time depending on the number of users provisioned. Confirm that all users are provisioned to Secure Access.
3. Navigate to the **Push Groups** tab on the **Cisco User Management Connector Gov** app in Okta.
4. Provision groups and group membership to Secure Access.

   Pushing a group does not sync any users and only provisions the group to Secure Access.

> **Note**
>
> Okta does not recommend pushing groups that are assigned to the app. If you have assigned the **Everyone** group to the app, you should not push the same group.

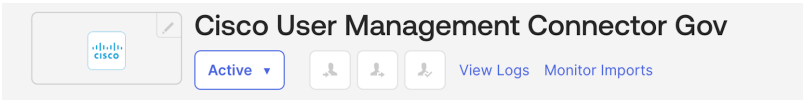
Step 6 – View Logs in the App

Provides instructions for step 6 - view logs in the app. Navigate to View Logs on the Cisco User Management Connector Gov app in Okta.

Procedure

Navigate to **View Logs** on the **Cisco User Management Connector Gov** app in Okta.

The app displays the progress of the provisioning.



View Provisioned Users and Groups in Secure Access

Provides instructions for viewing provisioned users and groups in secure access. Navigate to Connect Users, Groups, and Endpoint Devices to view the users and groups provisioned from Okta.

Procedure

Navigate to **Connect** > **Users, Groups, and Endpoint Devices** to view the users and groups provisioned from Okta.

What to do next

For more information, see View User Details and View Group Details.

Refresh SCIM Token

Describes refresh scim token. Secure Access recommends that you refresh the SCIM token at least once every 180 days. Refresh the token in Secure Access and immediately copy the new token to the Cisco Secure Access app on Okta so that provisioning is not impacted.

Secure Access recommends that you refresh the SCIM token at least once every 180 days. Refresh the token in Secure Access and immediately copy the new token to the Cisco Secure Access app on Okta so that provisioning is not impacted. Refreshing the SCIM token is the full responsibility of the administrator. Secure Access does not perform this action.

Provision Users and Groups from Microsoft Entra ID

Describes provisioning users and groups from microsoft entra id. Cisco Secure Access supports the provisioning of users and groups from Microsoft Entra ID (formerly Azure Active Directory).

Cisco Secure Access supports the provisioning of users and groups from Microsoft Entra ID (formerly Azure Active Directory). With your Secure Access System for Cross-domain Identity Management (SCIM) token, configure the **Cisco User Management for Secure Access** app on the Microsoft Entra ID portal. Once you add users and groups in the app, Microsoft Entra ID begins to exchange the user and group information with Secure Access.

> **Note**
>
> You do not need to deploy an on-premises Secure Access Active Directory (AD) Connector.

Prerequisites for Provision Users and Groups from Microsoft Entra ID

Describes prerequisites for provision users and groups from microsoft entra id. Full Admin user role. For more information, see Manage Accounts.

- Full Admin user role. For more information, see Manage Accounts.
- A valid Microsoft Entra ID subscription with a premium Microsoft Entra IDlicense.
- No concurrent provisioning of the same user or group identities from on-premises AD and Microsoft Entra ID AD. If you are using the on-premises Secure Access AD Connector to import users and groups and choose to import the same users and groups from Microsoft Entra ID, ensure that the on-premises Secure Access AD connector is switched off or that the OpenDNS Connector service on the connector machine is stopped.
- For IP-to-user mapping deployments, you must use an on-premises Secure Access AD connector. Microsoft Entra ID does not store the private IP to Active AD user mappings.
- Import the `ObjectGUID` attribute from Microsoft Entra ID AD to Secure Access. The on-premises Secure Access AD Connector and Cisco Secure Client rely on the `ObjectGUID` attribute for user identification. If all of your endpoints are running the Cisco Secure Client, you do not have to import the `ObjectGUID` attribute from Microsoft Entra ID.
  - Before you set up the import of the `ObjectGUID` attribute, ensure that the on-premises Secure Access AD Connector that is synchronizing these identities is switched off or that the OpenDNS Connector service on the connector machine is stopped.
  - To ensure that the `ObjectGUID` attribute for users is synchronized from Microsoft Entra ID AD to Secure Access, your endpoints must authenticate against on-premises AD and run the Cisco Secure Client.
- If you previously configured a policy against groups imported from on-premises AD, and then choose to import the same groups from Microsoft Entra ID, you must reconfigure the policy to map it to the Microsoft Entra ID groups instead of the on-premises AD groups. In a policy, on-premises AD group names are displayed with the domain name preceding the group name, for example: `Domain1\ADGroup1`. For Microsoft Entra ID, only group names are displayed on the policy page, for example: **ADGroup1**.

Limitations for Provision Users and Groups from Microsoft Entra ID

Describes limitations for provision users and groups from microsoft entra id. You can provision no more than 200 groups from Microsoft Entra ID to Secure Access. Secure Access supports the provisioning of an unlimited number of users from Microsoft Entra ID.

- You can provision no more than 200 groups from Microsoft Entra ID to Secure Access. Secure Access supports the provisioning of an unlimited number of users from Microsoft Entra ID.
- Concurrent synchronization of the same users and groups from the Secure Access AD Connector and the Cisco Secure Access Microsoft Entra ID app is not supported and leads to inconsistent policy enforcement.

- To ensure that all users are provisioned, create a dynamic **All Users** group and assign this group to the Cisco Secure Access app. For more information, see Dynamic Membership Rules for Groups in Microsoft Entra ID Active Directory. You can assign additional groups as required for group-based policy rule enforcement.
- Provisioning large numbers of users and groups to Secure Access may take several hours.
- Microsoft Entra ID does not support nested group memberships for group-based assignment to any SaaS application.

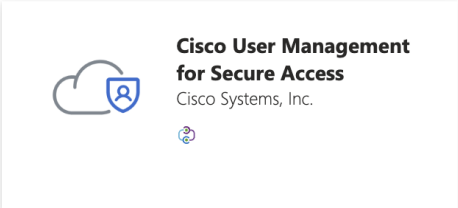
Configure the Cisco User Management for Secure Access App

Provides instructions for configuring the cisco user management for secure access app. Its purpose, requirements, and key details for Cisco Secure Access administrators.

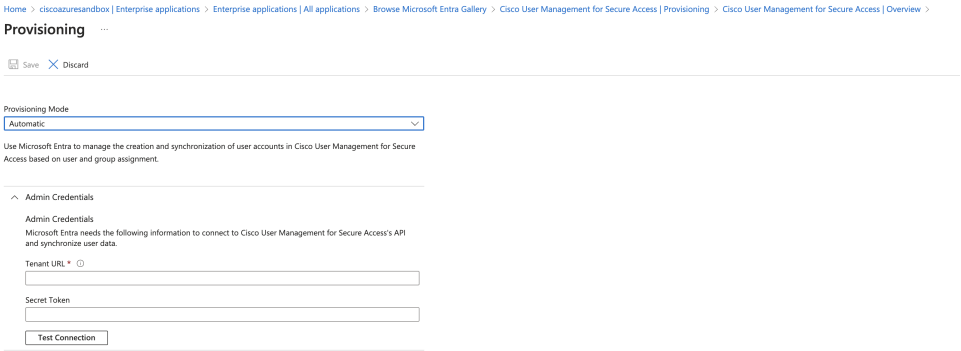
With your Secure Access SCIM token and API Identity URL, set up the Cisco Secure Access app in Microsoft Entra ID AD and provision users and groups. For more information, see Tutorial: Configure Cisco Secure Access User Management for automatic user provisioning.

Procedure

1. Navigate to the **Cisco User Management for Secure Access** app in Microsoft Entra ID AD.



2. Add your Secure Access SCIM API token to the **Secret Token** field.
3. Add the Secure Access API Identity URL to the **Tenant URL** field.
4. Click **Test Connection** to confirm that you can use your Secure Access SCIM token to connect the Secure Access API with Microsoft Entra ID AD.



View Provisioned Users and Groups in Secure Access

Provides instructions for viewing provisioned users and groups in secure access. Navigate to Connect Users, Groups, and Endpoint Devices to view the users and groups provisioned from Microsoft Entra ID.

Procedure

Navigate to **Connect** > **Users, Groups, and Endpoint Devices** to view the users and groups provisioned from Microsoft Entra ID.

What to do next

For more information, see View User Details and View Group Details.

Refresh SCIM Token

Describes refresh scim token. Secure Access recommends that you refresh the SCIM token at least once every 180 days. Refresh the token in Secure Access and immediately copy the new token to the Cisco Secure Access app on Microsoft Entra ID so that provisioning is not impacted.

Secure Access recommends that you refresh the SCIM token at least once every 180 days. Refresh the token in Secure Access and immediately copy the new token to the Cisco Secure Access app on Microsoft Entra ID so that provisioning is not impacted. Refreshing the SCIM token is the full responsibility of the administrator. Secure Access does not perform this action.

14 Configure Integrations with SAML Identity Providers

Topics:

- Configure Integrations with SAML Identity Providers

Describes the purpose and procedures for configure integrations with saml identity providers and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Configure Integrations with SAML Identity Providers

Describes configuring integrations with saml identity providers. Cisco Secure Access enables you to connect securely to the internet, web resources in private and public clouds, your organization's on-premises private resources, and Software as a Service (SaaS) applications.

Cisco Secure Access enables you to connect securely to the internet, web resources in private and public clouds, your organization's on-premises private resources, and Software as a Service (SaaS) applications. To create more granular policy rules and to enable Secure Access to authenticate users connecting from networks or network tunnels or with Zero Trust (ZT), you must integrate a Security Assertion Markup Language (SAML) identity provider (IdP) with Secure Access. The SAML IdP provides single sign-on (SSO) authentication. Secure Access establishes a trust relationship with the IdP.

Secure Access supports Security Assertion Markup Language (SAML) for single sign-on (SSO) authentication of users. Secure Access integrates with various SAML 2.0 IdPs: Azure Active Directory (Azure AD), Duo, Okta, Ping Identity, Active Directory Federation Services (AD FS), and OpenAM.

Once users in your organization are configured to use SSO, the SAML IdP manages all authentication requests. A user authenticates to the SSO IdP, automatically signs in to Secure Access, and is authorized to connect to certain resources.

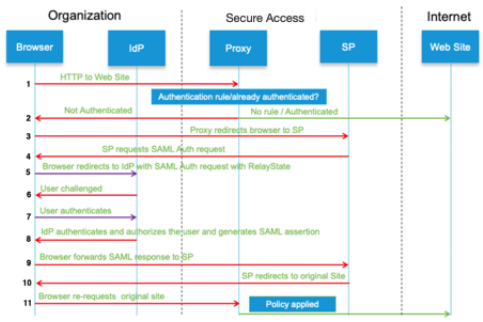
Use Cases

Describes using cases. Secure Access uses SAML authentication to provide seamless connections to web resources and private resources from user devices.

Secure Access uses SAML authentication to provide seamless connections to web resources and private resources from user devices.

Secure Internet Access—Networks and Network Tunnels

- Secure web gateway—The Cisco Secure Access secure web gateway (SWG) uses SAML to authenticate and authorize web requests from user devices sent over networks and network tunnels. Internet traffic is protected by the Secure Access DNS and Web security layers. The Secure Access SWG is not an open proxy. Secure Access must trust the source that forwards web traffic to it, whether the source is a network or network tunnel.
- SAML uses a cookie surrogate. When a browser sends an HTTP request, Secure Access checks if the request contains the HTTP Cookie header. If the cookie is not set, Secure Access can not authenticate the user.
- Web Security SAML Data Flow



Zero Trust Access with the Cisco Secure Client

- Secure Access Zero Trust (ZT) uses SAML to authenticate and authorize requests to an organization's private resources from a user device where the Cisco Secure Client is deployed.

Zero Trust Access with an Unmanaged Device

- Secure Access Zero Trust (ZT) uses SAML to authenticate and authorize requests to an organization's private resources from an unmanaged device.

Configure Identity Providers for SAML Authentication

Describes configuring identity providers for saml authentication. Configure Azure AD for SAML Configure Okta for SAML Configure AD FS for SAML

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

Prerequisites for SAML Authentication

Describes prerequisites for saml authentication. To configure the integration of a Security Assertion Markup Language (SAML) identity provider (IdP) with Cisco Secure Access, you must meet certain requirements.

To configure the integration of a Security Assertion Markup Language (SAML) identity provider (IdP) with Cisco Secure Access, you must meet certain requirements.

Secure Access Service Provider Metadata

Describes secure access service provider metadata. Secure Access Entity ID–saml.fg.id.secureaccessfed.cisco.com Secure Access Entity URL–fg.id.secureaccessfed.cisco.com/gw/auth/acs/response

- Secure Access Entity ID–**saml.fg.id.secureaccessfed.cisco.com**
- Secure Access Entity URL–**fg.id.secureaccessfed.cisco.com/gw/auth/acs/response**

Requirements

Describes requirements. If your organization integrates with AD FS, we recommend that you bypass web traffic to the gateway.id.secureaccessfed.cisco domain on the Secure Access secure web gateway (SWG). Otherwise, send gateway.id.secureaccessfed.cisco requests to the SWG, not directly to the internet.

- If your organization integrates with AD FS, we recommend that you bypass web traffic to the **gateway.id.secureaccessfed.cisco** domain on the Secure Access secure web gateway (SWG). Otherwise, send **gateway.id.secureaccessfed.cisco** requests to the SWG, not directly to the internet. For more information about bypassing domains and Secure Access Web security, see Manage Domains.
- Provision users and groups from your organization in Secure Access. The users and groups must match the identities obtained from SAML. For more information, see Manage Users and Groups.
- Download your identity provider's SAML metadata file in XML format.
- The SAML metadata must have a signing key.
- The SAML identity provider (IdP) must support SAML 2.0 POST profiles.
- Enable cookies for your browser. For more information, see your browser's documentation.

Enable SAML and HTTPS Inspection in the Security Profile

Describes enabling saml and https inspection in the security profile. To obtain the user identity of a device through SAML, you must enable SAML and HTTPS inspection in the Security profile. For more information, see Manage Security Profiles.

- To obtain the user identity of a device through SAML, you must enable SAML and HTTPS inspection in the Security profile. For more information, see Manage Security Profiles.
- HTTPS Inspection enables Secure Access to read the SAML cookie in the Cookie HTTP request header. The SAML cookie acts as the authentication token or surrogate.
- You must install the Cisco Secure Access root certificate on all client machines egressing from networks or network tunnels where SAML is enabled. For more information, see Manage Certificates.

Configure Okta for SAML

Describes configuring okta for saml. Cisco Secure Access uses the Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust Network Access (ZTNA) enabled.

Cisco Secure Access uses the Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust Network Access (ZTNA) enabled.

To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access. Configure Okta for SAML authentication with the Secure Access service provider metadata and then add your Okta SAML metadata to Secure Access.

For information about provisioning users from Okta to Secure Access, see Provision Users and Groups from Okta.

Procedure for Configure Okta for SAML

Describes procedure for configure okta for saml. Step 1 – Choose an Authentication Method Step 2 – Add an Identity Provider Step 3 – Configure the Identity Provider's SAML Metadata

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Configure the Identity Provider's SAML Metadata

Prerequisites

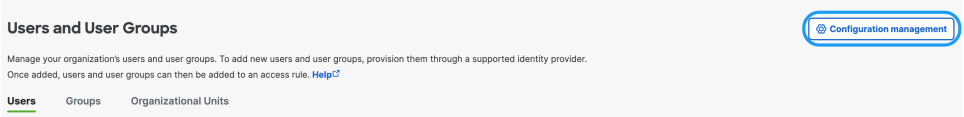
- Full Admin user role. For more information, see Manage Accounts.
- Send **id.secureaccessfed.cisco.com** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Domains.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Domains.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access security profile. For more information, see Manage Security Profiles.
- The IdP SAML metadata must have a signing key.
- Enable cookies on the browsers on user devices. For more information, see your browser's documentation.

Step 1 – Choose an Authentication Method

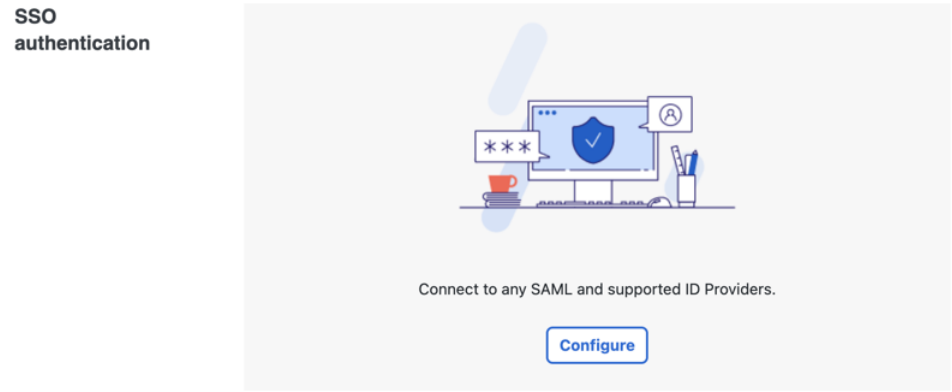
Provides instructions for step 1 – choose an authentication method. Navigate to Connect Users, Groups, and Endpoint Devices and click Configuration Management.

Procedure

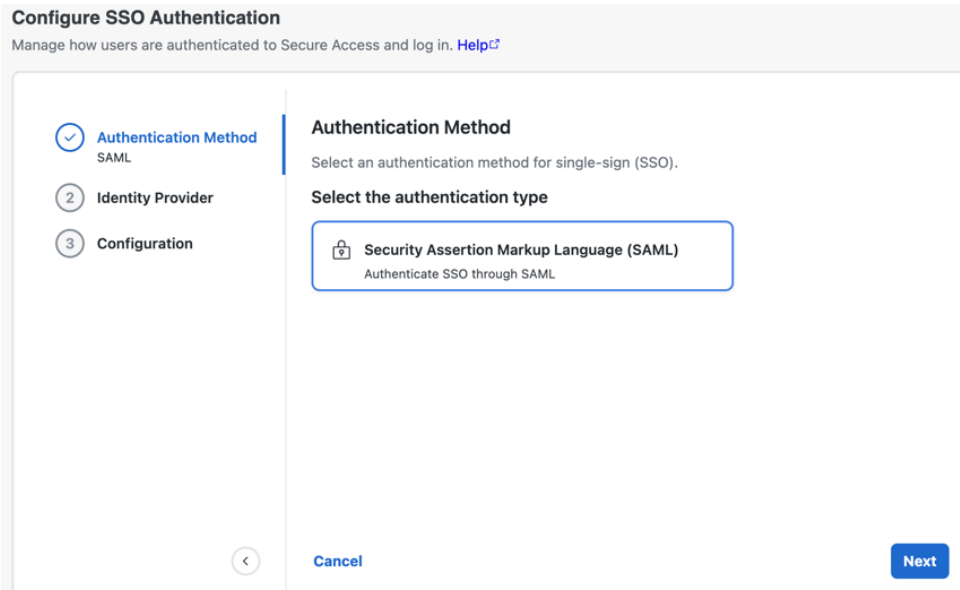
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.



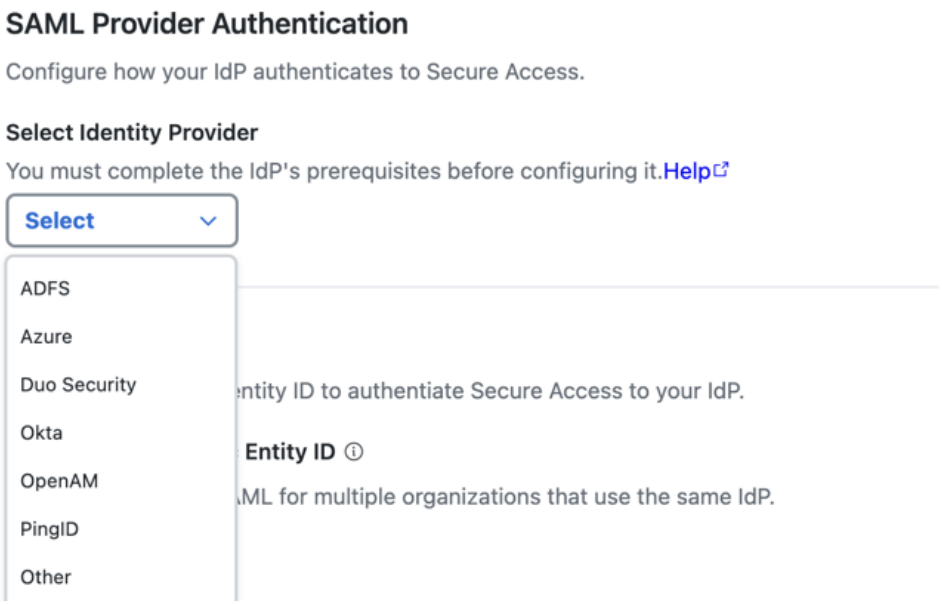
Step 2 – Add an Identity Provider

Provides instructions for step 2 – add an identity provider. In the SSO authentication profile, select the Okta SAML IdP, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.

In the SSO authentication profile, select the Okta SAML IdP, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.

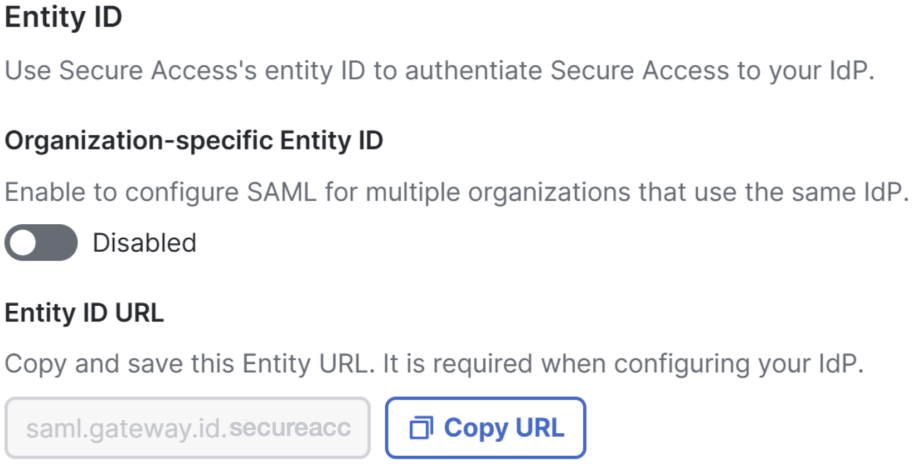
Procedure

1. For **Identity Provider**, choose **Okta**. Secure Access supports various IdPs.



2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security and Zero Trust Network Access (ZTNA) for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**. Secure Access allows you to override the default Secure Access SAML EntityID on a per-Org basis.

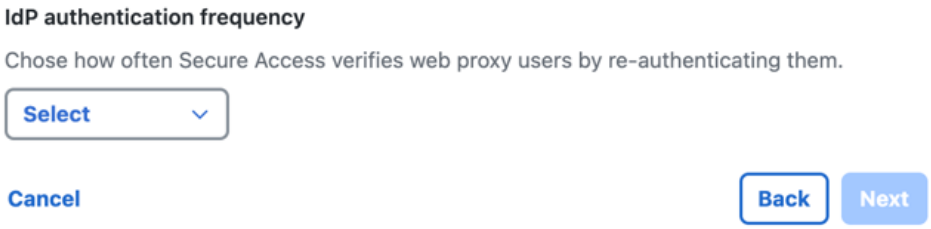
3. For **Entity ID URL**, click **Copy URL** to make a local copy of the Secure Access Entity ID URL. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**.



4. Choose a time interval when a user must authenticate with Secure Access.

   The time intervals are:

- **Daily**
- **Weekly**
- **Monthly**



5. Click **Next**.

Step 3 – Configure the Identity Provider's SAML Metadata

Describes step 3 – configure the identity provider's saml metadata. Download the Cisco_FedSSE_SP_Metadata XML file from Secure Access and use the service provider metadata to configure your instance of Okta.

Download the **Cisco_FedSSE_SP_Metadata** XML file from Secure Access and use the service provider metadata to configure your instance of Okta.

The Secure Access service provider metadata includes the service provider Issuer ID, the assertion consumer endpoint URL, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion.

> **Note**
>
> Okta does not provide the option to directly upload the metadata XML file. You must manually enter the Secure Access service provider metadata. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

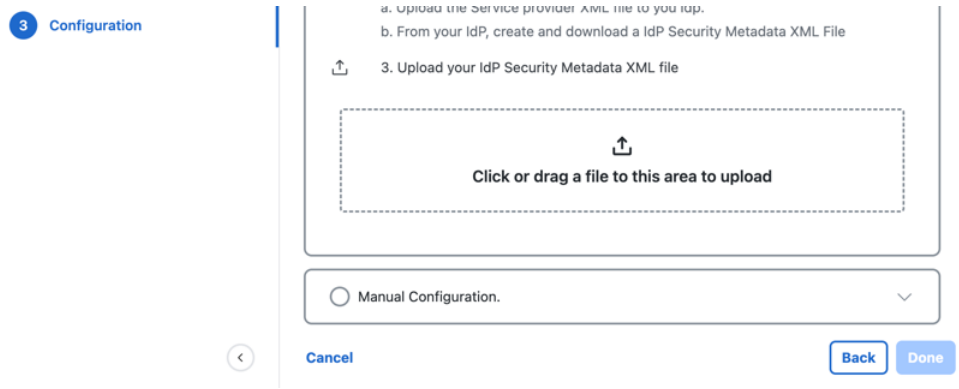
Step 3a – Download the Secure Access Service Provider XML File

Provides instructions for step 3a – download the secure access service provider xml file. Check Manual Configuration, and then click Download service provider XML file to save the Cisco_FedSSE_SP_Metadata XML file to your local device.

Procedure

---

1. Check **Manual Configuration**, and then click **Download service provider XML file** to save the **Cisco_FedSSE_SP_Metadata** XML file to your local device.



2. Open the **Cisco_FedSSE_SP_Metadata** XML file.
3. Copy the certificates from the **Cisco_FedSSE_SP_Metadata** XML file to a new file and save. Use the certificate file in the next step when you create the app integration in Okta.

Step 3b – Add Secure Access Service Provider Metadata to Okta

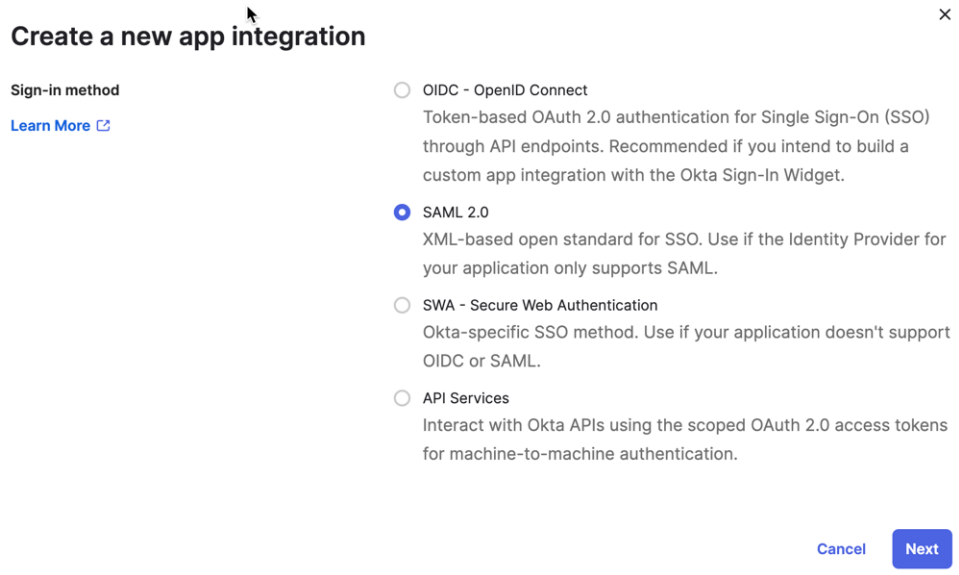
Provides instructions for step 3b – add secure access service provider metadata to okta. You can find the following steps described in the Okta Help.

You can find the following steps described in the Okta Help. For more information, see Create a Basic Custom SAML Application Using SP Metadata File.

You must configure Secure Access as a generic SAML 2.0 application within Okta. Okta does not provide a method to upload Secure Access metadata for automatic configuration. Extract the **EntityID** and **AssertionConsumerService** values from the Secure Access metadata file and add these to the applicable fields in Okta. Contact Okta for assistance.

Procedure

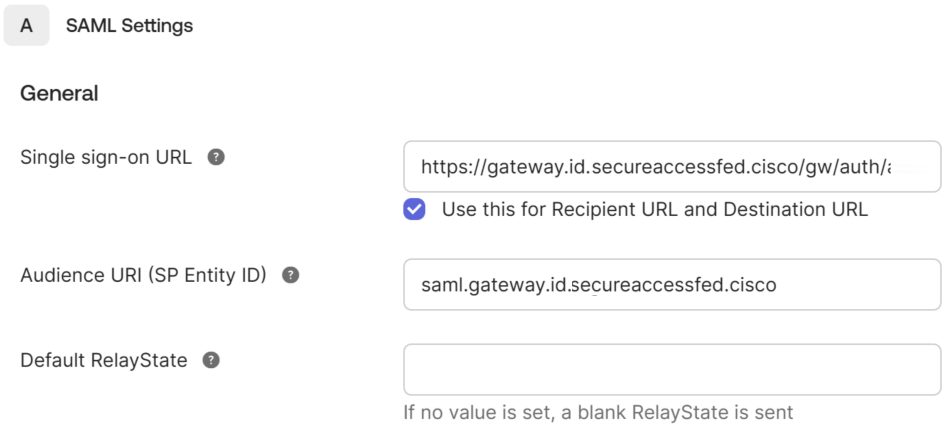
1. Sign in to your instance of Okta, then navigate to **Applications** > **Create a new app integration**.



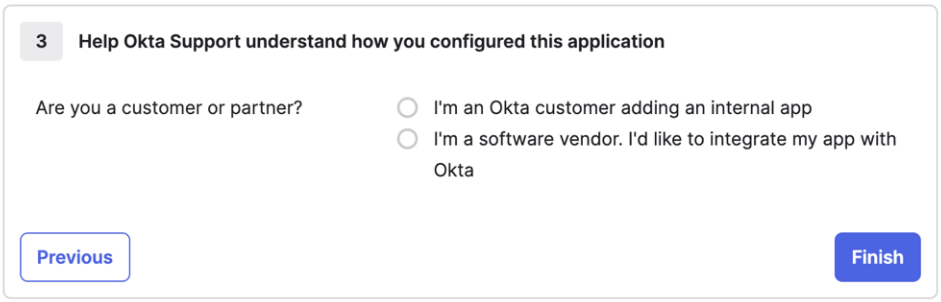
2. Click **SAML 2.0**, and then click **Next**.
3. For **General Settings**, add a name for the app integration, and then click **Next**.
4. For **SAML Settings** > **General**, enter the values from the service provider metadata file that you downloaded in Step 3a – Download the Secure Access Service Provider XML File .

- For **Single sign-on URL**, add the value of the **Location** attribute for the **md:AssertionConsumerService** element. The value should be something like: `gateway.id.secureaccessfed.cisco/gw/auth/acs/response..`
- For **Audience URI (SP Entity ID)**, add the value of the **entityID** element.

  The value should be something like: `saml.gateway.id.secureaccessfed.cisco`.



5. Click **Show Advanced Settings**.
6. For **Signature Certificate**, upload the root certificate that you downloaded from the **Cisco_FedSSE_SP_Metadata** XML file. Click **Preview the SAML Assertion** to show the created metadata file, and then click **Next**.
7. Click **I'm an Okta customer adding an internal app**, and then click **Finish**.



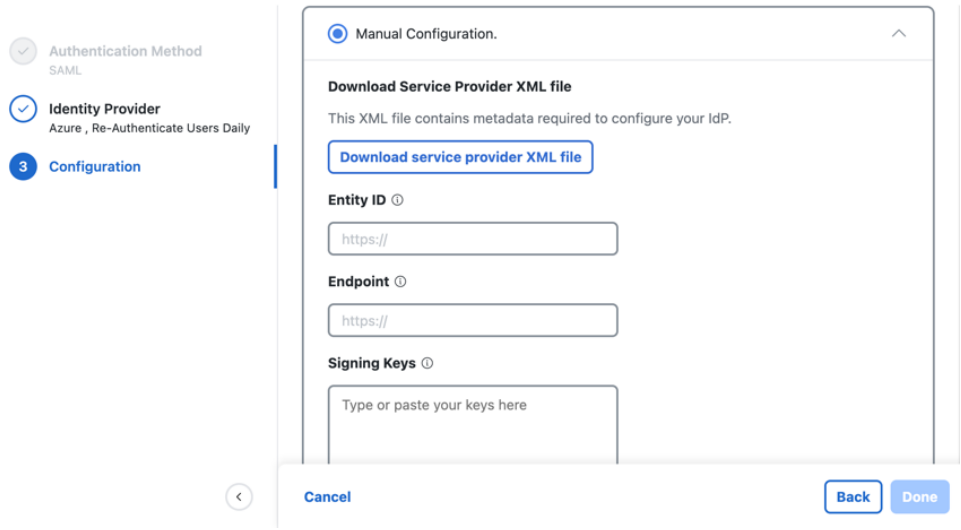
Step 3c - Add the Okta SAML Metadata to Secure Access

Provides instructions for step 3c - add the okta saml metadata to secure access. Complete the manual configuration of Okta in Secure Access. Enter your Okta SAML metadata for the following Secure Access settings:

Complete the manual configuration of Okta in Secure Access. Enter your Okta SAML metadata for the following Secure Access settings:

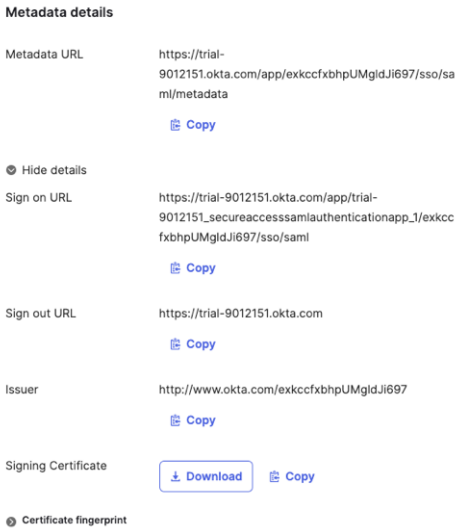
Procedure

1. **Entity ID**–A globally unique name for an identity provider.
2. **Endpoint**–The URL used to communicate with your identity provider.
3. **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
4. **Signed Authentication Request (optional)**–Choose whether to sign the authentication request for the IdP.



What to do next

1. On Okta, navigate to **Sign on** > **Settings** > **Metadata details**.



2. On Okta, copy the value of **Metadata URL**. Navigate to Secure Access and and enter the value in **Entity ID** .
3. On Okta, click **More Details**.
4. On Okta, copy the value of **Sign on URL**. Navigate to Secure Access and enter the value in **Endpoint**.
5. On Okta, copy the value of **Signing Certificate**. Navigate to Secure Access and enter the value in **Signing Keys**.
6. (Optional) Navigate to Secure Access and choose whether to sign the authentication request.
7. On Secure Access, click **Done**.

Test the Identity Provider Integration

Describes testing the identity provider integration. To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

View the SAML Certificates in Secure Access

Describes viewing the saml certificates in secure access. Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Configure AD FS for SAML

Describes configuring ad fs for saml. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure Active Directory Federation Services (AD FS) with Secure Access by uploading the AD FS XML metadata file to Secure Access, or alternatively add the AD FS metadata in Secure Access manually.

For information about provisioning users from AD FS to Secure Access, see Provision Users and Groups from Active Directory.

Procedure for Configure AD FS for SAML

Describes procedure for configure ad fs for saml. Step 1 – Choose an Authentication Method Step 2 – Add an Identity Provider

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- We recommend that you bypass web traffic to the **id.secureaccessfed.cisco.com** domain on the Secure Access secure web gateway (SWG). For more information about domains and the SWG, see Manage Domains.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Domains.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access security profile. For more information, see Manage Security Profiles.
- Download your IdP's metadata file in XML format.
- The IdP SAML XML metadata file must have a signing key.
- Enable cookies on the browsers on user devices. For more information, see your browser's documentation.

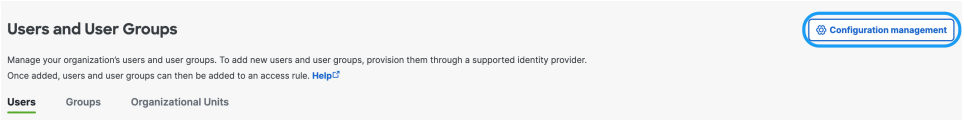
- Enable HTTPS Inspection in the Secure Access Security profile. Secure Access must inspect the Cookie HTTP header to read the SAML cookie. The SAML cookie acts as the authentication token or surrogate. For more information, see Manage Security Profiles.
- You must install the Cisco Secure Access root certificate on all client machines egressing from networks or network tunnels where SAML is enabled. For more information, see Manage Certificates.

Step 1 – Choose an Authentication Method

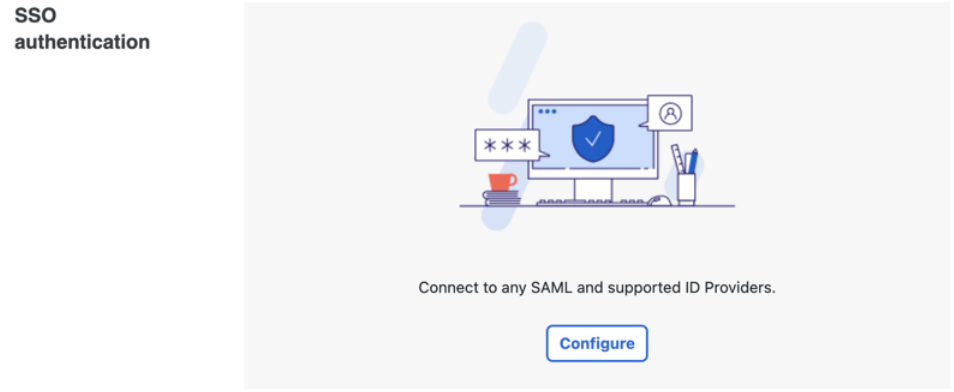
Provides instructions for step 1 – choose an authentication method. Navigate to Connect Users, Groups, and Endpoint Devices and click Configuration Management.

Procedure

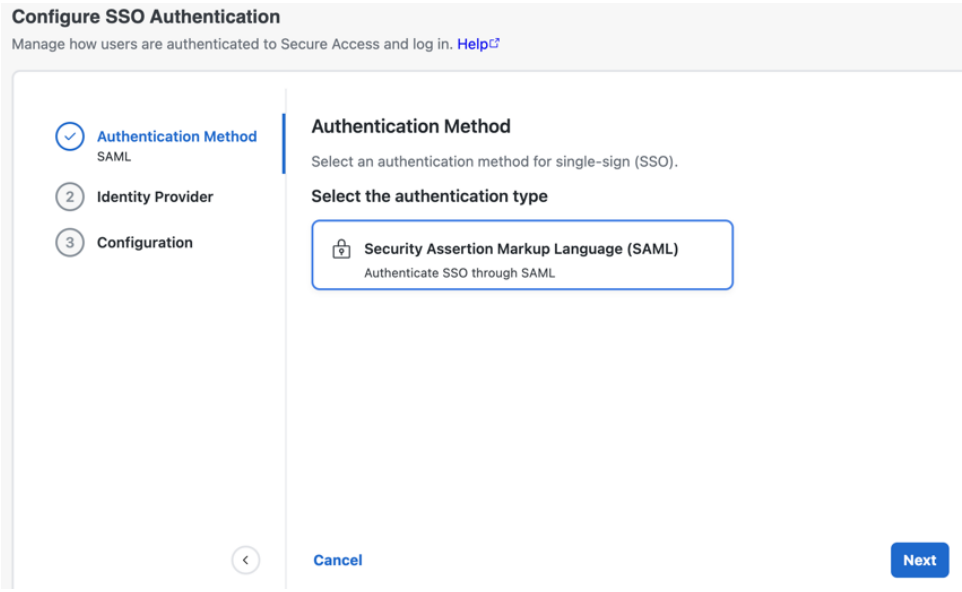
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.

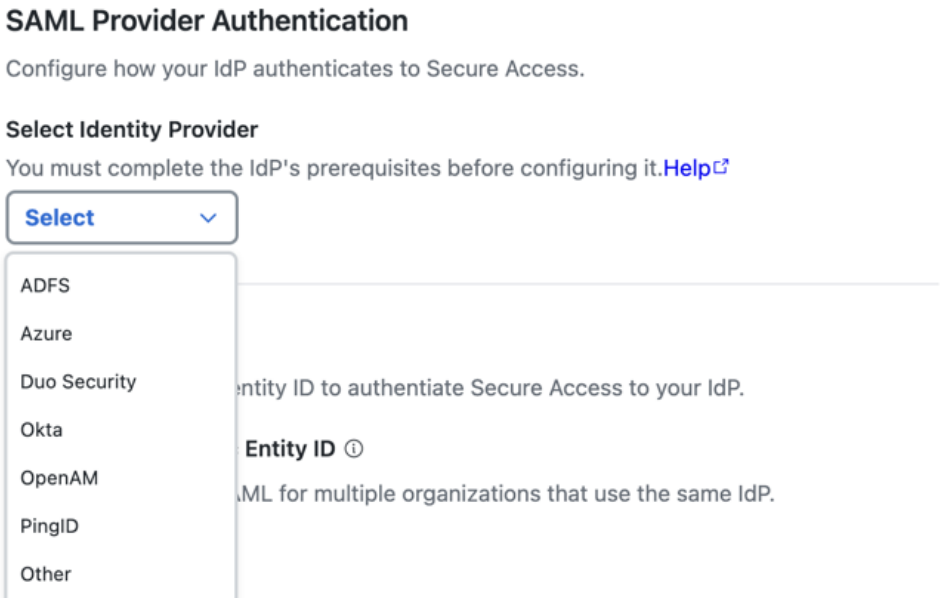


Step 2 – Add an Identity Provider

Provides instructions for step 2 – add an identity provider. For Identity Provider, choose ADFS. Secure Access supports various IdPs.

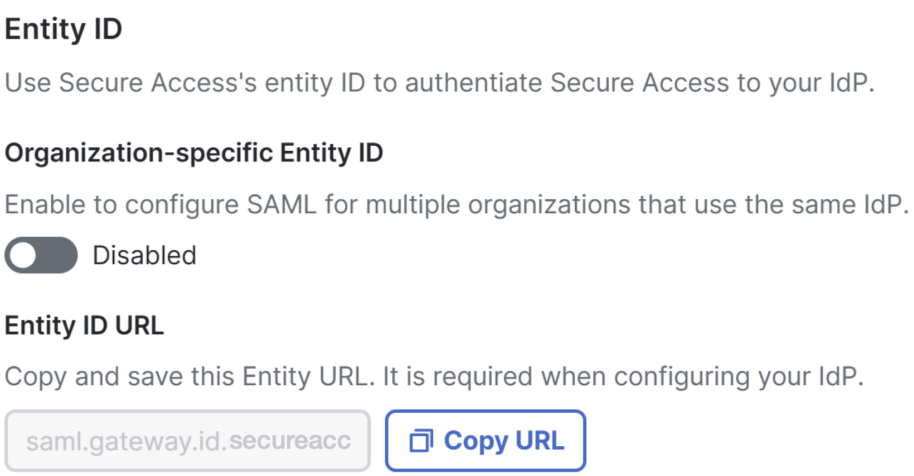
Procedure

1. For **Identity Provider**, choose **ADFS**. Secure Access supports various IdPs.



2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security and Zero Trust (ZT) for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**. Secure Access allows you to override the default Secure Access SAML EntityID on a per-Org basis.

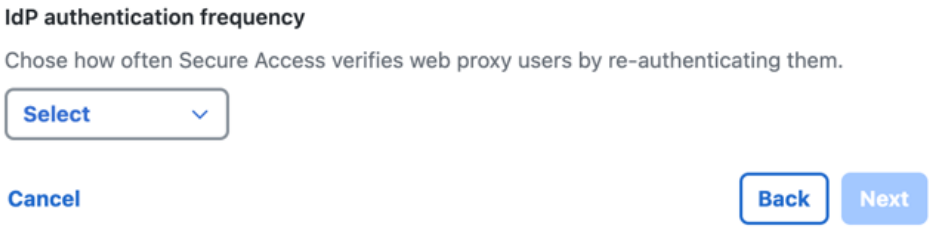
3. For **Entity ID URL**, click **Copy URL** to make a local copy of the Secure Access Entity ID URL. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**.



4. Choose a time interval when a user must authenticate with Secure Access.

The time intervals are:

- **Daily**
- **Weekly**
- **Monthly**



5. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes step 3 – add the identity provider's saml metadata to secure access. Download the Secure Access Metadata XML file and use the service provider file to configure your instance of AD FS. The Secure Access Metadata XML file includes the Secure Access root certificate.

Download the Secure Access Metadata XML file and use the service provider file to configure your instance of AD FS. The Secure Access Metadata XML file includes the Secure Access root certificate. For more information about setting up the service provider metadata in AD FS, see Configure Active Directory Federation Services.

Then, either upload the AD FS SAML metadata XML file to Secure Access or add the SAML metadata directly in Secure Access.

- Step 3a – Upload the Identity Provider's SAML Metadata XML File
- Step 3b – Add the Identity Provider's SAML Metadata

Step 3a – Upload the Identity Provider's SAML Metadata XML File

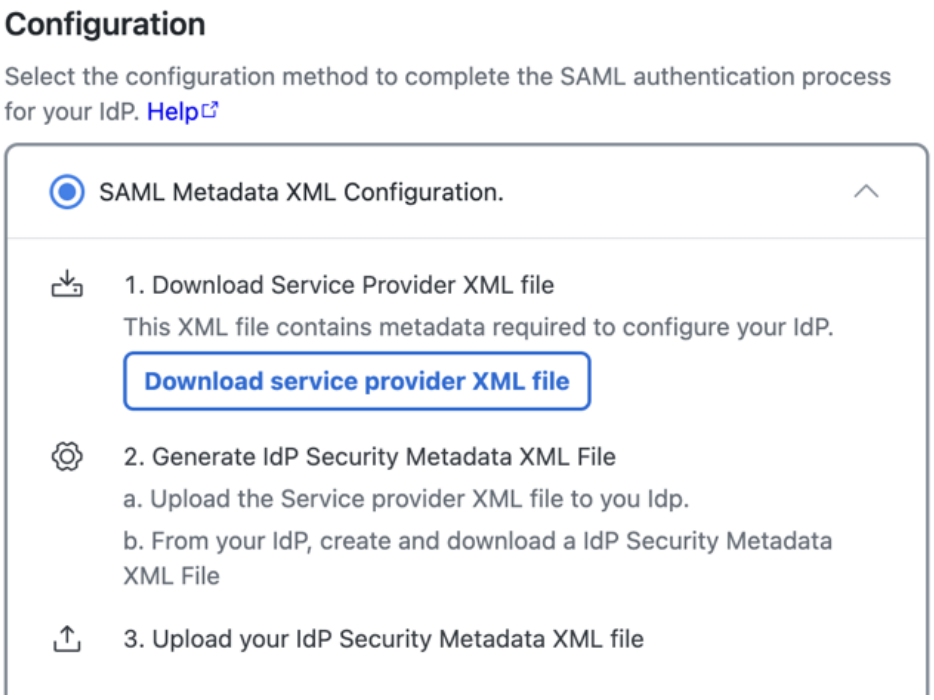
Provides instructions for step 3a – upload the identity provider's saml metadata xml file. Download the Secure Access Metadata XML file, configure the SAML IdP, and then upload the IdP's metadata XML file to Secure Access.

Download the Secure Access Metadata XML file, configure the SAML IdP, and then upload the IdP's metadata XML file to Secure Access.

Procedure

---

1. Check **SAML Metadata XML Configuration**.



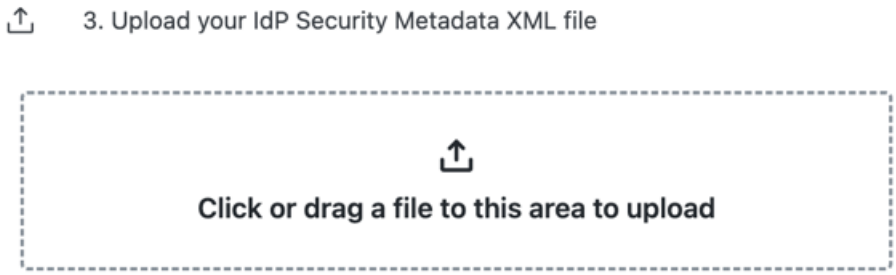
2. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

3. Configure your AD FS instance with the Secure Access SAML metadata. Follow the steps in Configure Active Directory Federation Services.
4. Upload the configured IdP Metadata XML file to Secure Access, and then click **Done**.

   The IdP's Metadata XML file contains the IdP's root certificate, which is required to integrate the IdP with Secure Access.



Step 3b – Add the Identity Provider's SAML Metadata

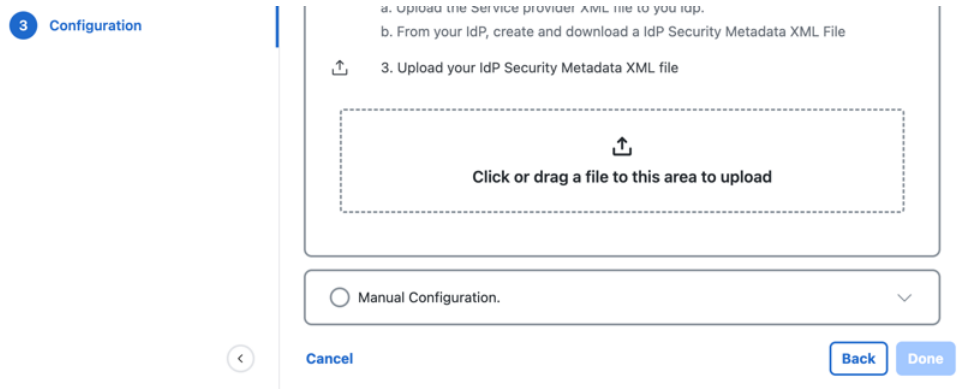
Provides instructions for step 3b – add the identity provider's saml metadata. Download the Secure Access Metadata XML file, configure the SAML IdP, and then add the IdP's metadata in Secure Access.

> **Note**
>
> If you uploaded your IdP's SAML Metadata XML file to Secure Access, you do not have to complete the following steps.

Download the Secure Access Metadata XML file, configure the SAML IdP, and then add the IdP's metadata in Secure Access.

Procedure

1. Check **Manual Configuration**.

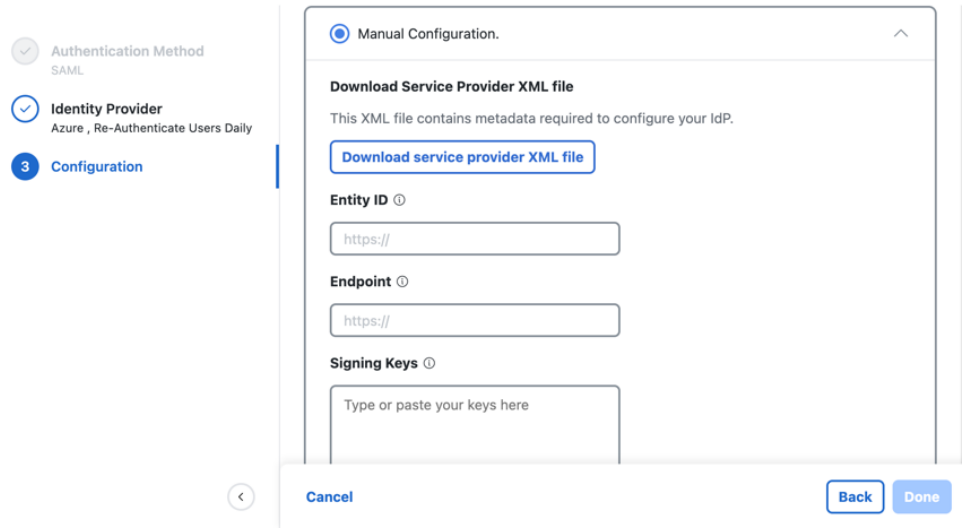


2. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP signing certificate, refer to your vendor's documentation.

3. Configure your AD FS instance with the Secure Access SAML metadata. Follow the steps in Configure Active Directory Federation Services.
4. Enter the identity provider's metadata, and then click **Done**.
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
   - **Signed Authentication Request (optional)**–Choose whether you can sign the authentication request for the IdP.

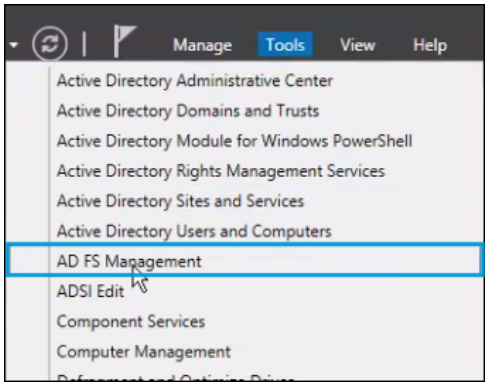


Configure Active Directory Federation Services

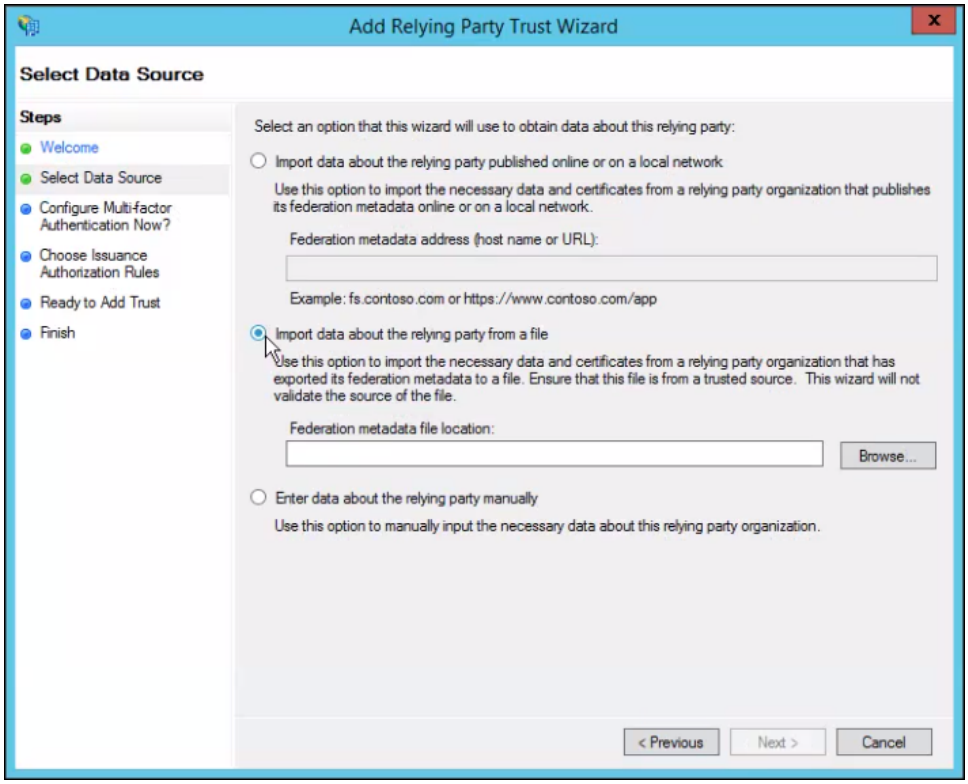
Provides instructions for configuring active directory federation services. Log into AD FS and navigate to Server Manager Tools AD FS Management

Procedure

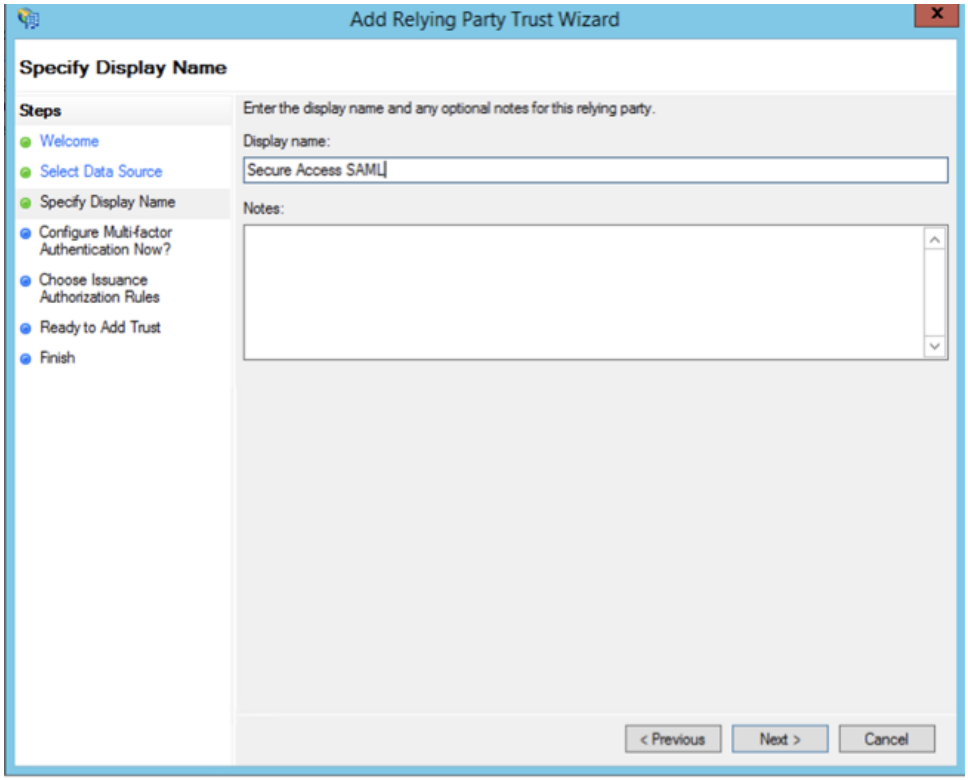
1. Log into AD FS and navigate to **Server Manager** > **Tools** > **AD FS Management**
2. In the AD FS Manager, right-click on **Trust Relationships** and navigate to **Relying Party Trusts** > **Add Relying Party Trust** and select **Start**.



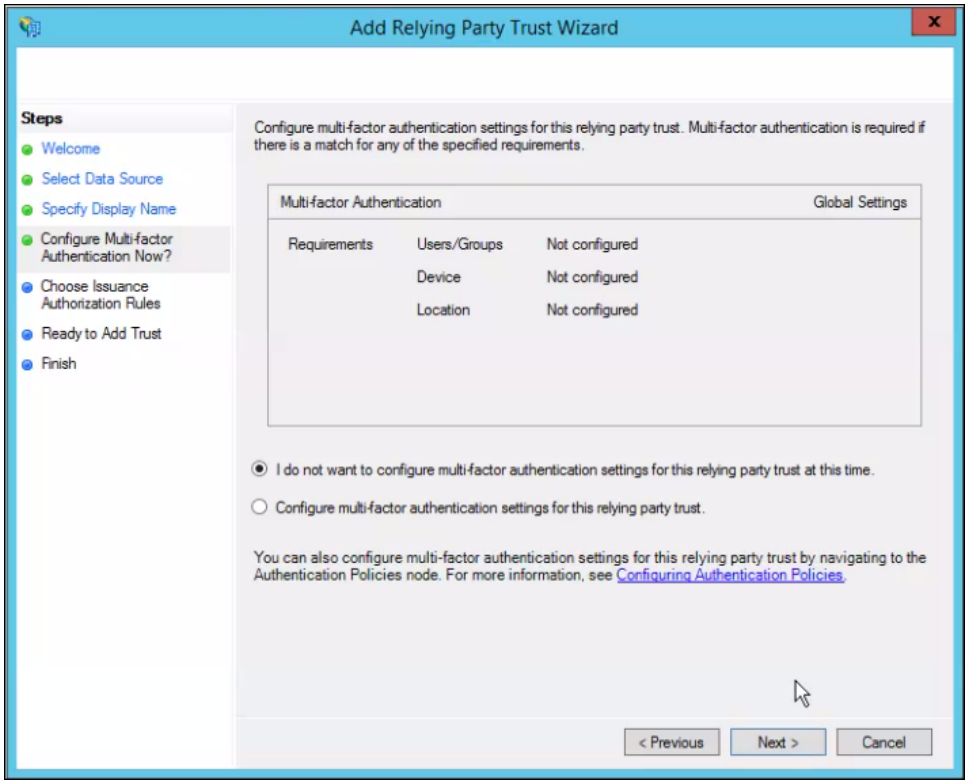
3. Choose **Import data about the relying party from a file** and browse for the **metadata.xml** file downloaded from Secure Access.



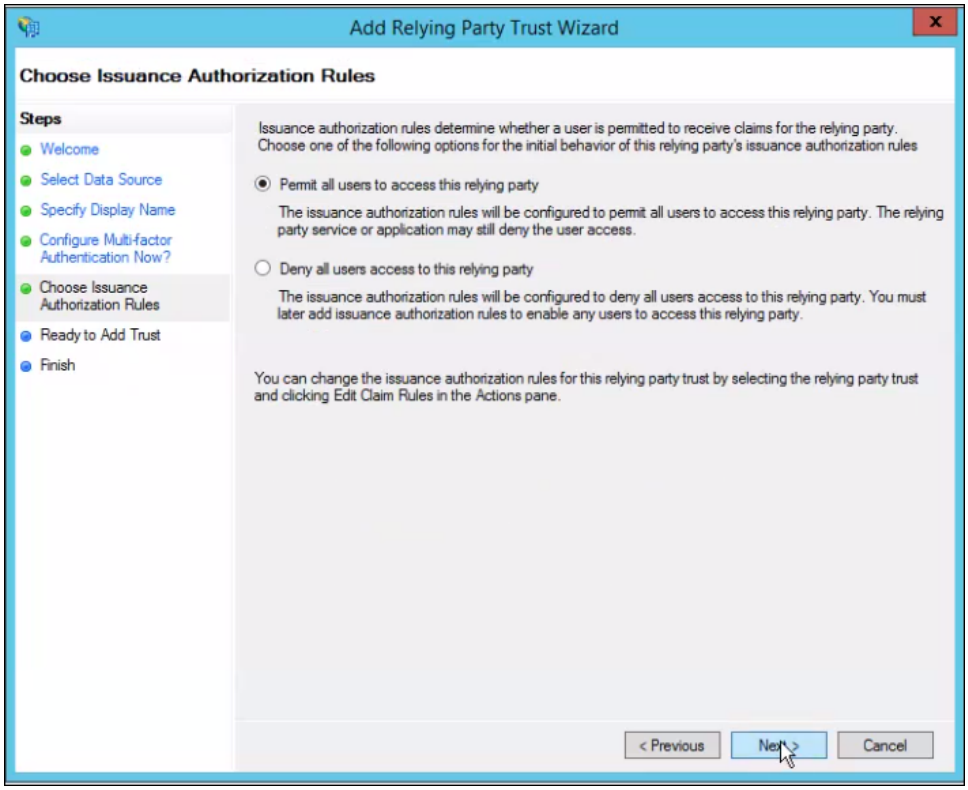
4. For **Display name**, provide a meaningful name for the trust connection, and then click **Next**.



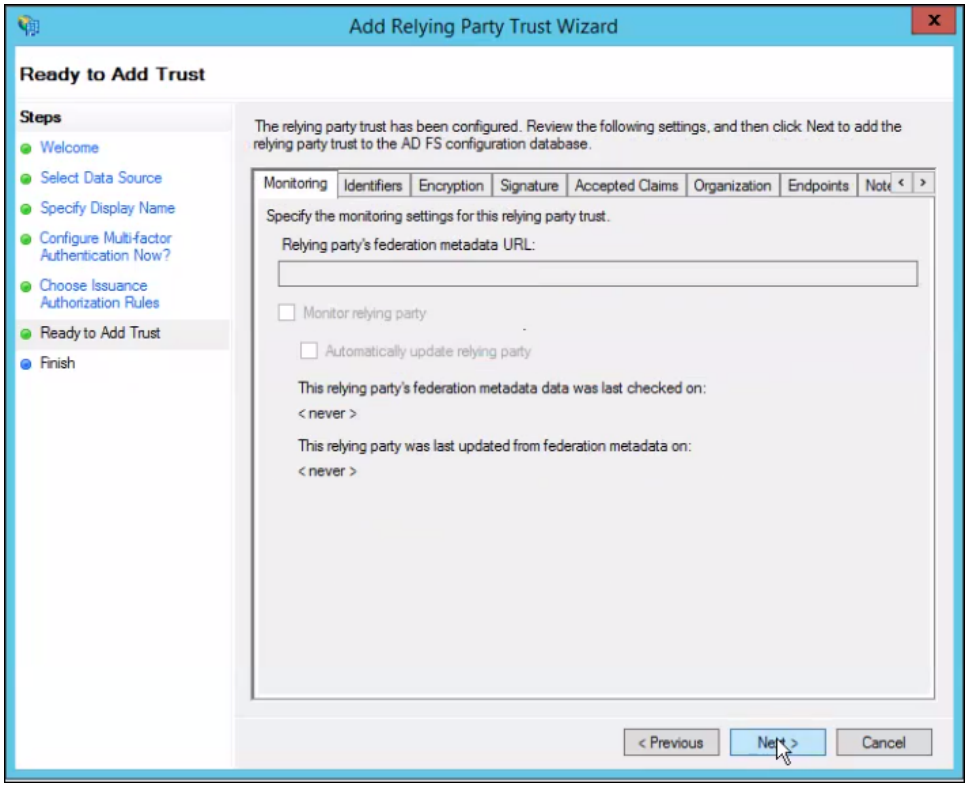
5. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time** and click **Next**.



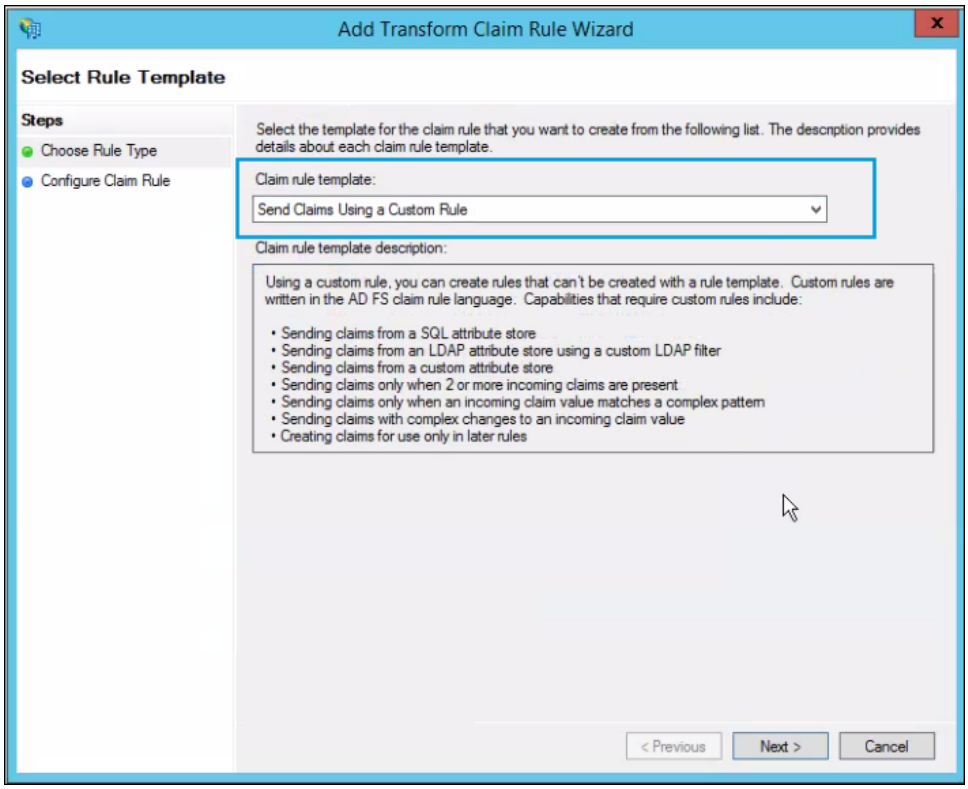
6. Select **Permit all users to access relying party** and click **Next**.



7. Verify settings and click **Next**.



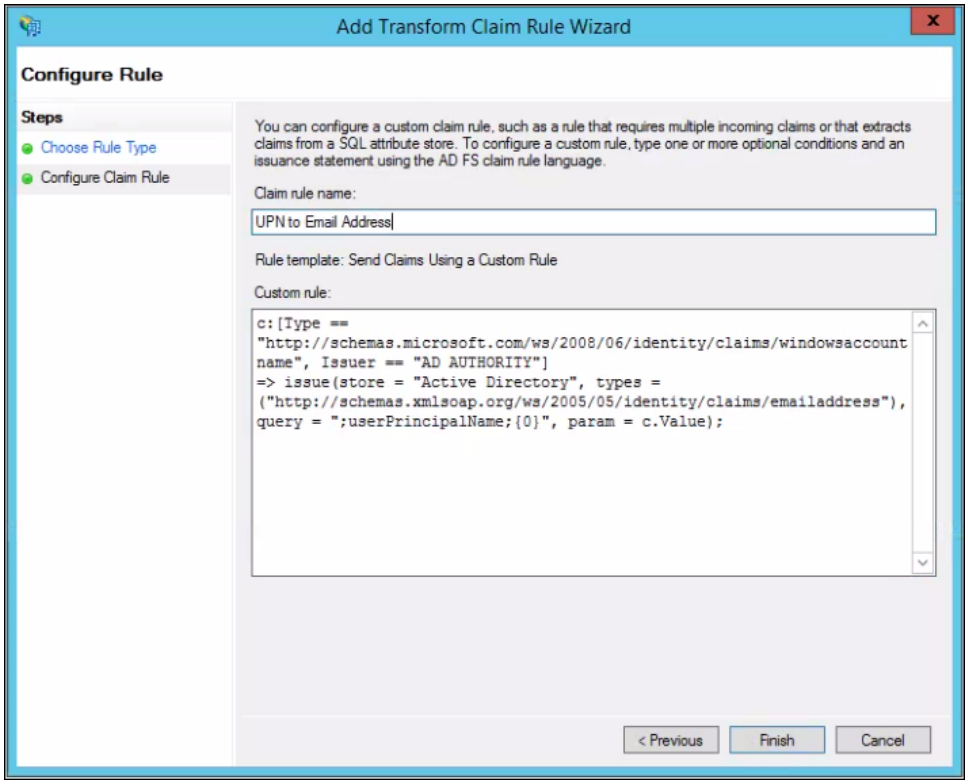
8. Right-click on the recently created relaying party and select **Edit Claim Rules**.



9. Under **Issuance Transform Rules**, click **Add Rule**, then choose **Send Claims Using a Custom Rule** with the following configuration:

```
c:\[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
 Issuer == "AD AUTHORITY"\]

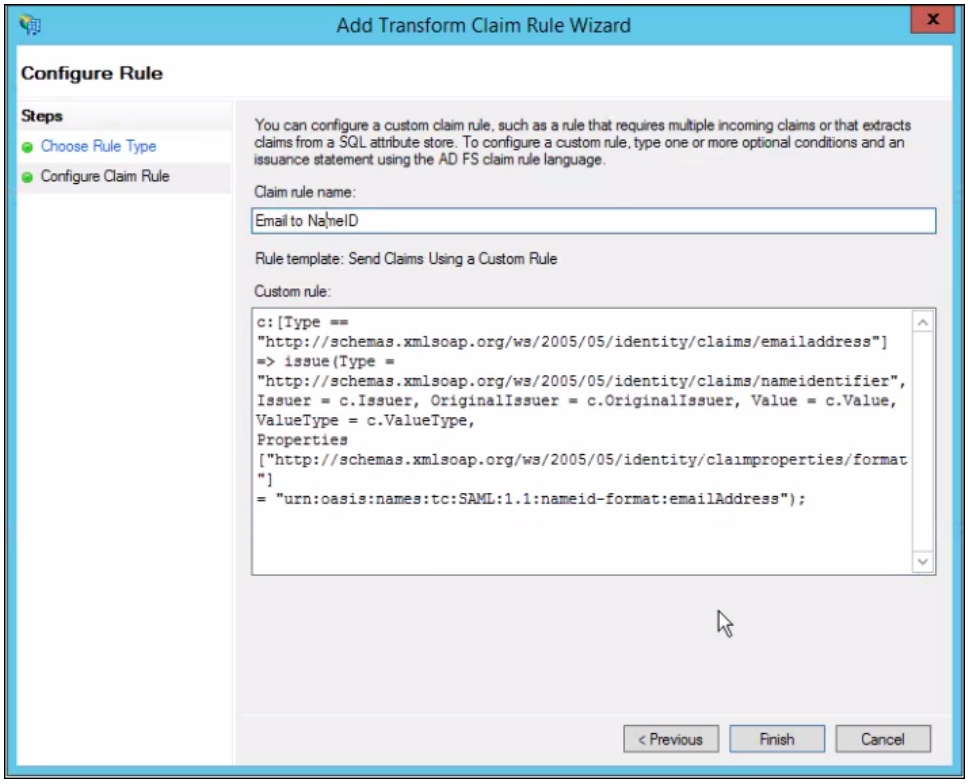
=> issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"), query
 = ";userPrincipalName;{0}", param = c.Value);
```



10. Repeat step 7 with the following configuration.

```
c:\[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"\]

=> issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
 = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
Properties\["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"\]
 = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```



11. Download the AD FS metadata XML file and save the file on your local system.

Test the Identity Provider Integration

Describes testing the identity provider integration. To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

View the SAML Certificates in Secure Access

Describes viewing the saml certificates in secure access. Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Configure Duo Security for SAML

Describes configuring duo security for saml. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the Duo Security SAML IdP with Secure Access by uploading the Duo Security XML metadata file to Secure Access, or alternatively add the Duo Security metadata in Secure Access manually.

Procedure for Configure Duo Security for SAML

Describes procedure for configure duo security for saml. Step 1 – Choose an Authentication Method Step 2 – Add an Identity Provider

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Prerequisites

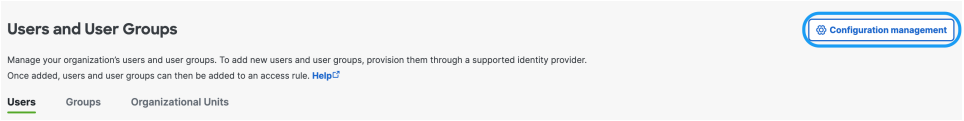
- Full Admin user role. For more information, see Manage Accounts.
- Send **id.secureaccessfed.cisco.com** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Domains.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Domains.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access Security profile. For more information, see Manage Security Profiles.
- Download your IdP's metadata file in XML format.
- The IdP SAML XML metadata file must have a signing key.
- Enable cookies on the browsers on user devices. For more information, see your browser's documentation.

Step 1 – Choose an Authentication Method

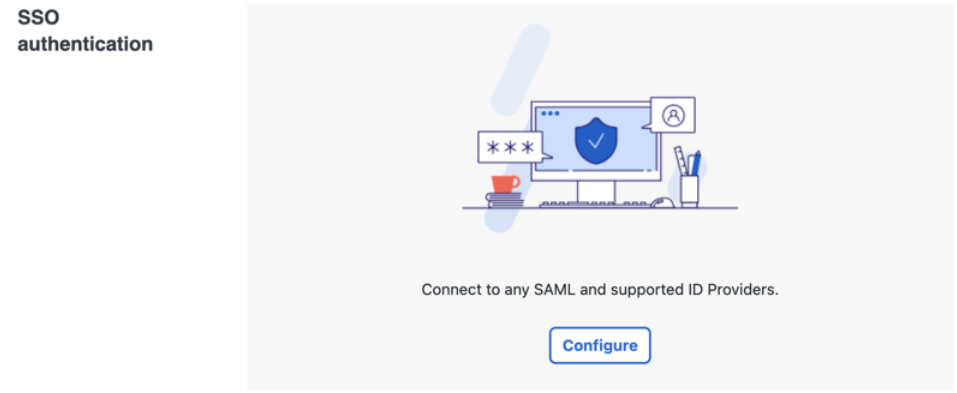
Provides instructions for step 1 – choose an authentication method. Navigate to Connect Users, Groups, and Endpoint Devices and click Configuration Management.

Procedure

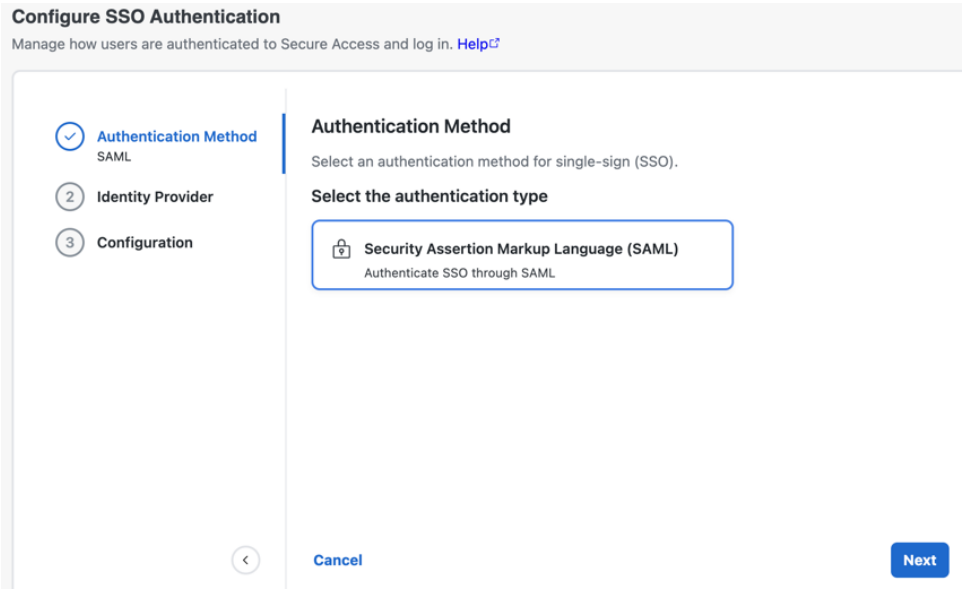
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.

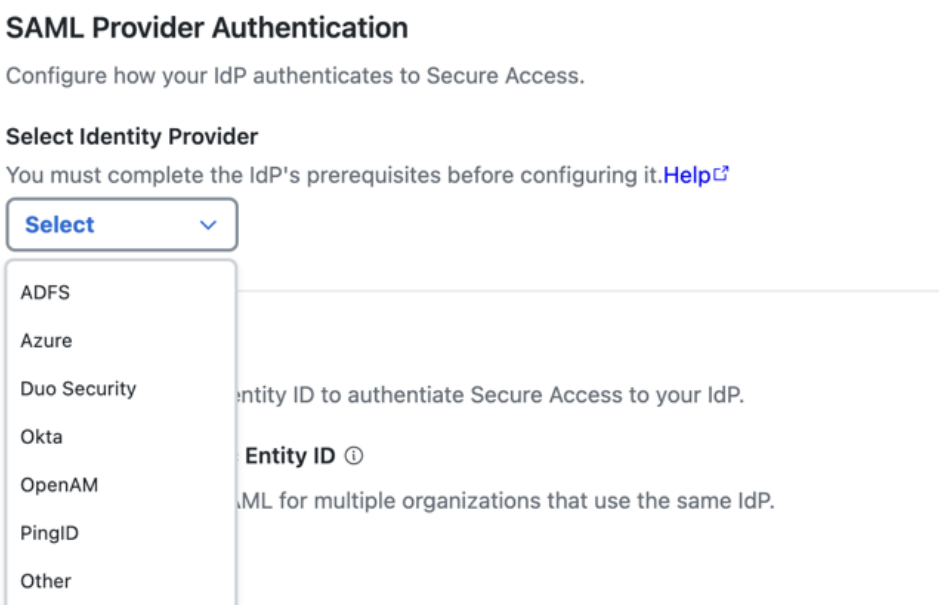


Step 2 – Add an Identity Provider

Provides instructions for step 2 – add an identity provider. For Identity Provider, choose Duo Security. Secure Access supports various IdPs.

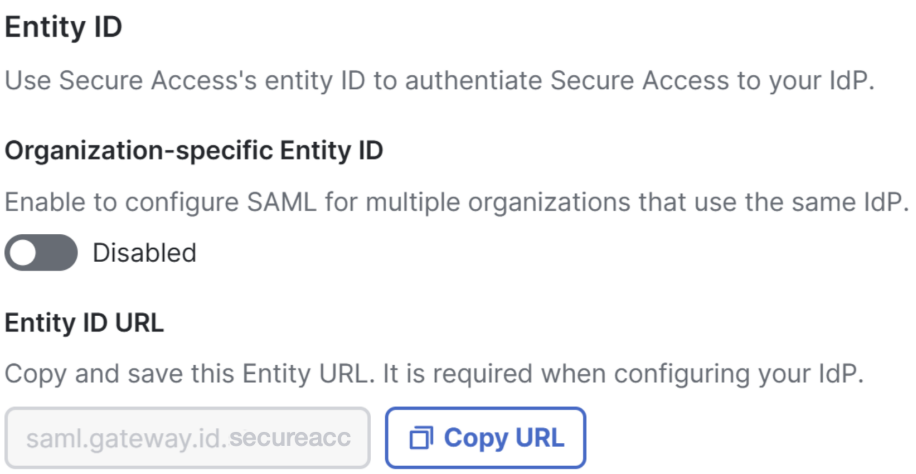
Procedure

1. For **Identity Provider**, choose **Duo Security**. Secure Access supports various IdPs.



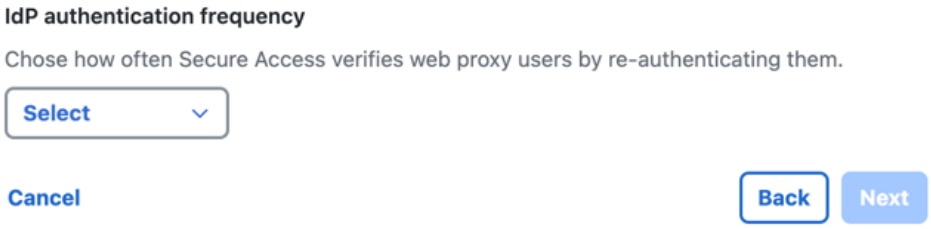
2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security and Zero Trust (ZT) for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**. Secure Access allows you to override the default Secure Access SAML EntityID on a per-Org basis.

3. For **Entity ID URL**, click **Copy URL** to make a local copy of the Secure Access Entity ID URL. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**.



4. Choose a time interval when a user must authenticate with Secure Access.

   The time intervals are:
   - **Daily**
   - **Weekly**
   - **Monthly**



5. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes step 3 – add the identity provider's saml metadata to secure access. Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Duo Security. The Secure Access Metadata XML file includes the Secure Access root certificate.

Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Duo Security. The Secure Access Metadata XML file includes the Secure Access root certificate.

Then, either upload the Duo Security SAML metadata XML file to Secure Access or add the SAML metadata directly in Secure Access.

- Step 3a – Upload the Identity Provider's SAML Metadata XML File
- Step 3b – Add the Identity Provider's SAML Metadata

Step 3a – Upload the Identity Provider's SAML Metadata XML File

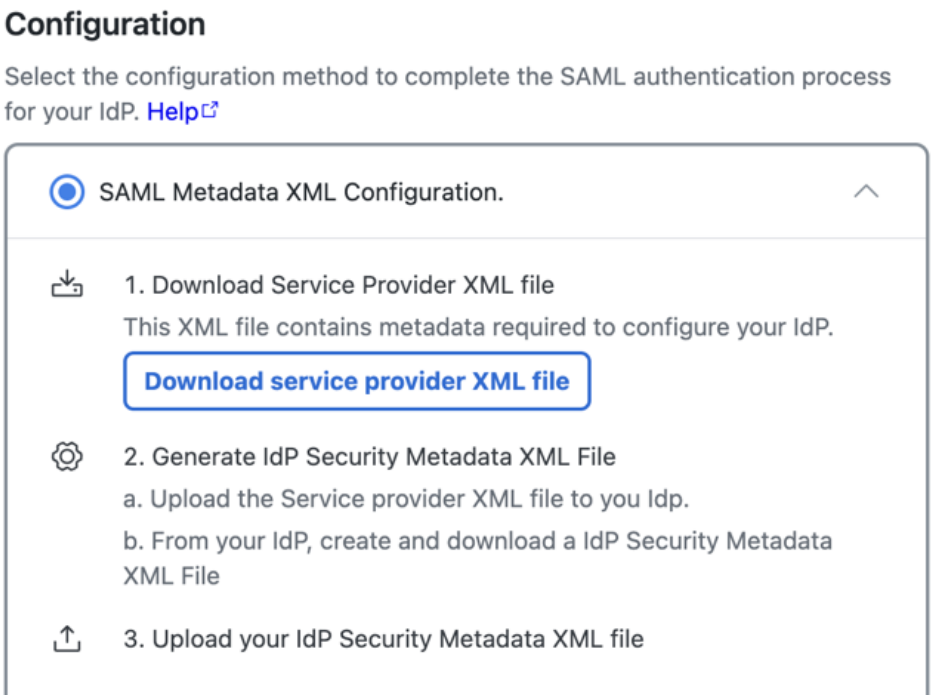
Provides instructions for step 3a – upload the identity provider's saml metadata xml file. Download the Secure Access Metadata XML file, configure the SAML IdP, and then upload the IdP's metadata XML file to Secure Access.

Download the Secure Access Metadata XML file, configure the SAML IdP, and then upload the IdP's metadata XML file to Secure Access.

Procedure

---

1. Check **SAML Metadata XML Configuration**.



2. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

3. Configure Duo Security for SAML.

   Extract the **EntityID** and **AssertionConsumerService** URLs from the Secure Access metadata file and add these to the applicable fields in Duo Security. For more information, see Configure the Duo Security Single Sign-On Application.

4. Upload the configured IdP Metadata XML file to Secure Access, and then click **Done**.

   The IdP's Metadata XML file contains the IdP's root certificate, which is required to integrate the IdP with Secure Access.



Step 3b – Add the Identity Provider's SAML Metadata

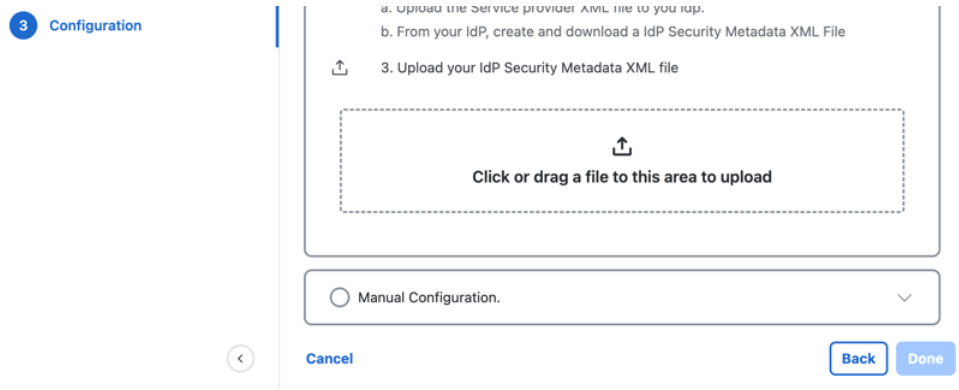
Provides instructions for step 3b - add the identity provider's saml metadata. If you uploaded your IdP's SAML Metadata XML file to Secure Access, you do not have to complete the following steps.

> **Note**
>
> If you uploaded your IdP's SAML Metadata XML file to Secure Access, you do not have to complete the following steps.

Download the Secure Access Metadata XML file, configure the SAML IdP, and then add the IdP's metadata in Secure Access.

Procedure

1. Check **Manual Configuration**.



2. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

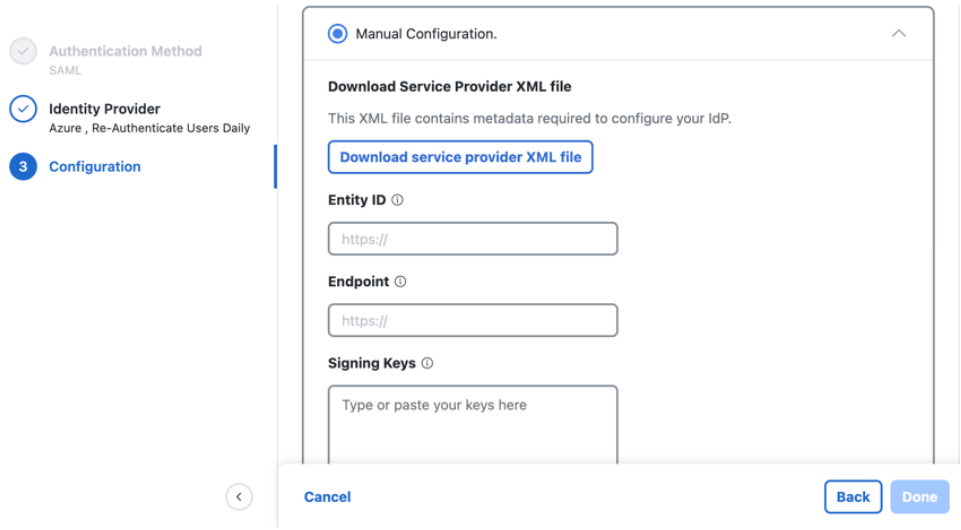
   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP signing certificate, refer to your vendor's documentation.

3. Configure Duo Security for SAML.

   Extract the **EntityID** and **AssertionConsumerService** URLs from the Secure Access metadata file and add these to the applicable fields in Duo Security. For more information, see Configure the Duo Security Single Sign-On Application.

4. Enter the identity provider's metadata, and then click **Done**.
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
   - **Signed Authentication Request (optional)**–Choose whether you can sign the authentication request for the IdP.

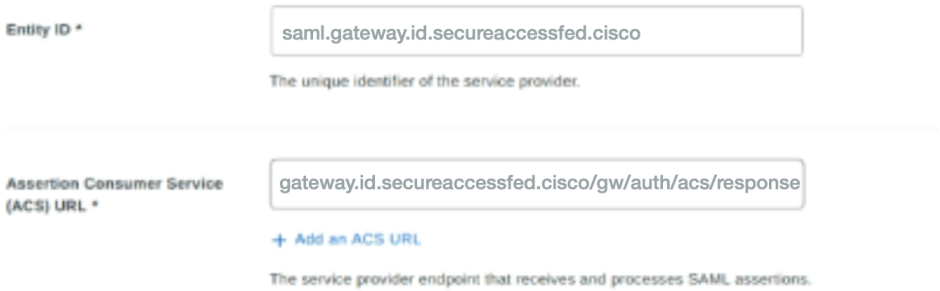


Configure the Duo Security Single Sign-On Application

Provides instructions for configuring the duo security single sign-on application. Sign in to the Duo admin portal and navigate to Applications Protect an Application.

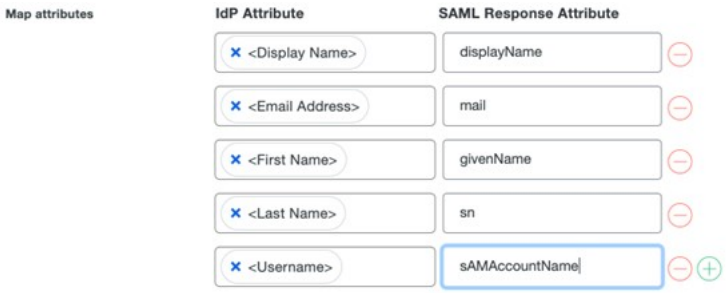
Procedure

1. Sign in to the Duo admin portal and navigate to **Applications** > **Protect an Application**.
2. Search for **Generic Service Provider** and select **2FA with SSO hosted by Duo**.
3. For **Entity ID**, enter **saml.gateway.id.secureaccessfed.cisco** and for **Assertion Consumer Service (ACS) URL**, enter **gateway.id.secureaccessfed.cisco/gw/auth/acs/response**.

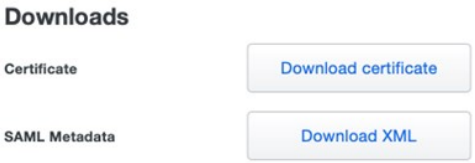


4. Enter an email address in the **NameID attribute** field.

5. Configure the **Map attributes** with the following data.
   - **Display name**–Enter the name you want to display.
   - **Email Address**–Enter an email address.
   - **First Name**–Enter the first name.
   - **Last Name**–Enter the last name.
   - **Username**–Enter the user name.



6. Click **Save**.
7. Click **Download certificate** to download the certificate, and then click **Download XML** to download the SAML Metadata file.



Test the Identity Provider Integration

Describes testing the identity provider integration. To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

View the SAML Certificates in Secure Access

Describes viewing the saml certificates in secure access. Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Configure Ping Identity for SAML

Describes configuring ping identity for saml. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity Provider (IdP) in Secure Access.

Configure the Ping Identity SAML IdP with Secure Access by uploading the Ping Identity XML metadata file to Secure Access, or alternatively add the Ping Identity metadata in Secure Access manually.

Procedure for Configure Ping Identity for SAML

Describes procedure for configure ping identity for saml. Step 1 – Choose an Authentication Method Step 2 – Add an Identity Provider

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Prerequisites

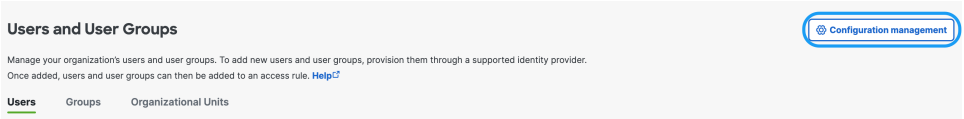
- Full Admin user role. For more information, see Manage Accounts.
- Send **id.secureaccessfed.cisco.com** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Domains.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Domains.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access Security profile. For more information, see Manage Security Profiles.
- Download your IdP's metadata file in XML format.
- The IdP SAML XML metadata file must have a signing key.
- Enable cookies on the browsers on user devices. For more information, see your browser's documentation.
- Enable HTTPS Inspection in the Secure Access Security profile. Secure Access must inspect the Cookie HTTP header to read the SAML cookie. The SAML cookie acts as the authentication token or surrogate. For more information, see Manage Security Profiles.
- You must install the Cisco Secure Access root certificate on all client machines egressing from networks or network tunnels where SAML is enabled. For more information, see Manage Certificates.

Step 1 – Choose an Authentication Method

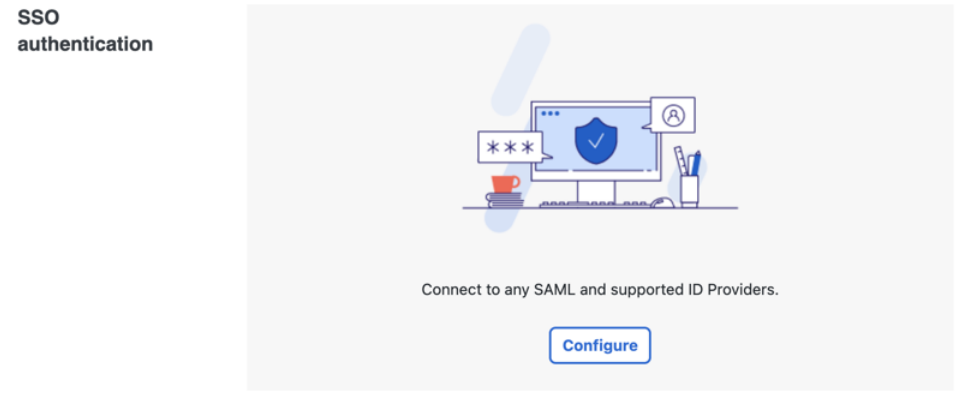
Provides instructions for step 1 – choose an authentication method. Navigate to Connect Users, Groups, and Endpoint Devices and click Configuration Management.

Procedure

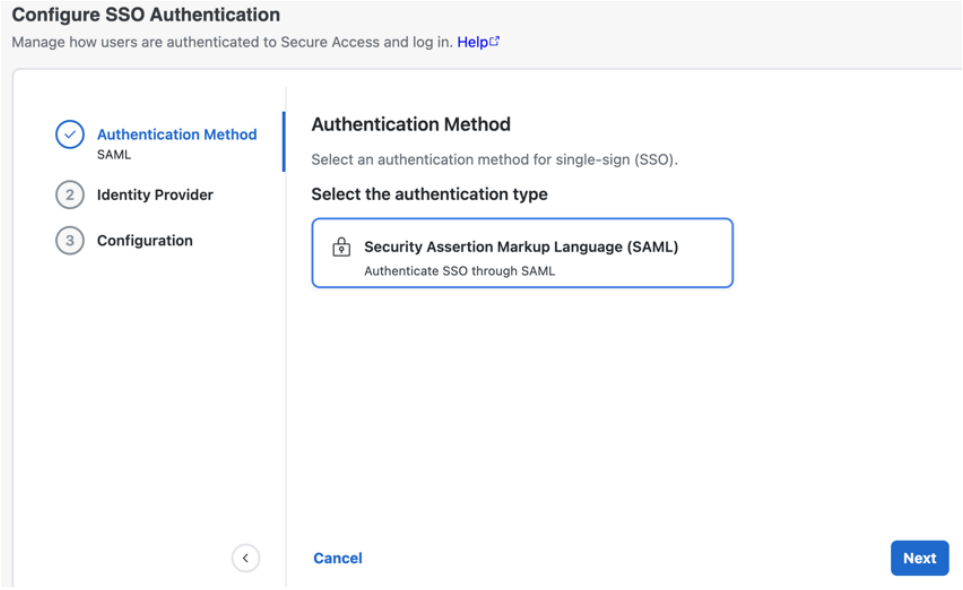
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.

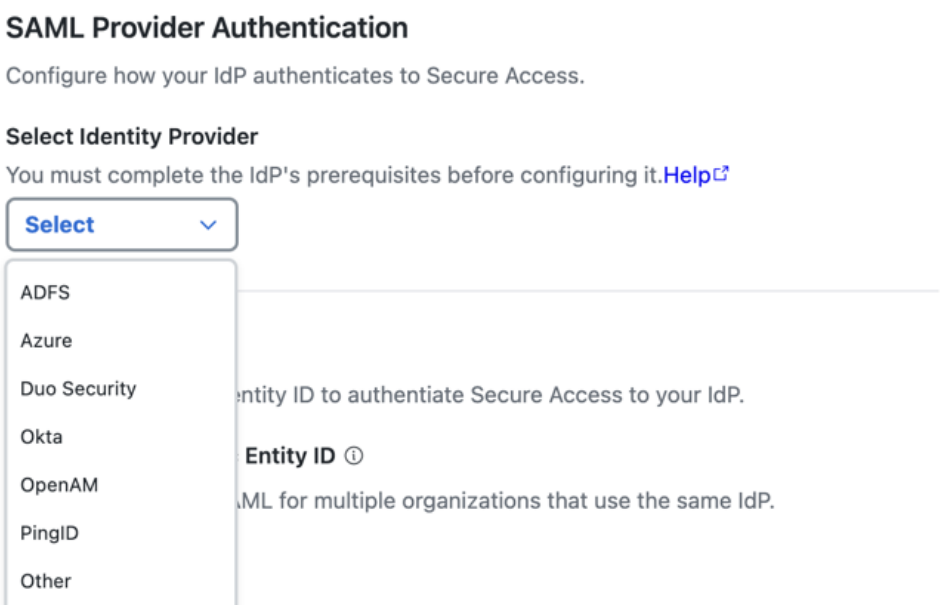


Step 2 – Add an Identity Provider

Provides instructions for step 2 – add an identity provider. For Identity Provider, choose PingID. Secure Access supports various IdPs.

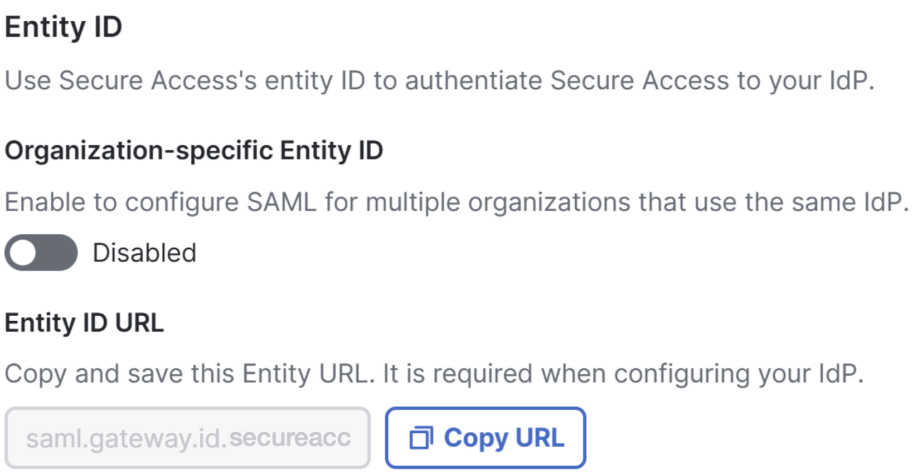
Procedure

1. For **Identity Provider**, choose **PingID**. Secure Access supports various IdPs.



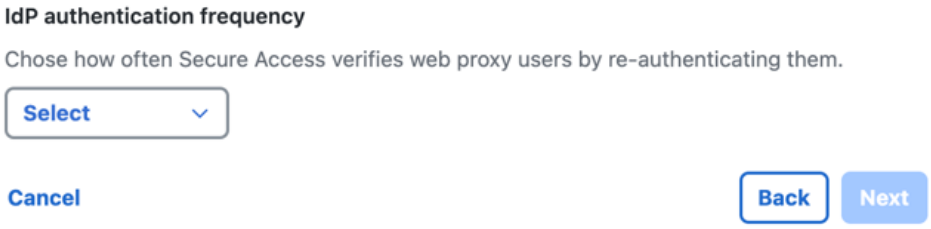
2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security and Zero Trust (ZT) for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**. Secure Access allows you to override the default Secure Access SAML EntityID on a per-Org basis.

3. For **Entity ID URL**, click **Copy URL** to make a local copy of the Secure Access Entity ID URL. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**.



4. Choose a time interval when a user must authenticate with Secure Access.

   The time intervals are:
   - **Daily**
   - **Weekly**
   - **Monthly**



5. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes step 3 – add the identity provider's saml metadata to secure access. Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Ping Identity. The Secure Access Metadata XML file includes the Secure Access root certificate.

Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Ping Identity. The Secure Access Metadata XML file includes the Secure Access root certificate.

Then, either upload the Ping Identity SAML metadata XML file to Secure Access or add the SAML metadata directly in Secure Access.

- Step 3a – Upload the Identity Provider's SAML Metadata XML File
- Step 3b – Add the Identity Provider's SAML Metadata

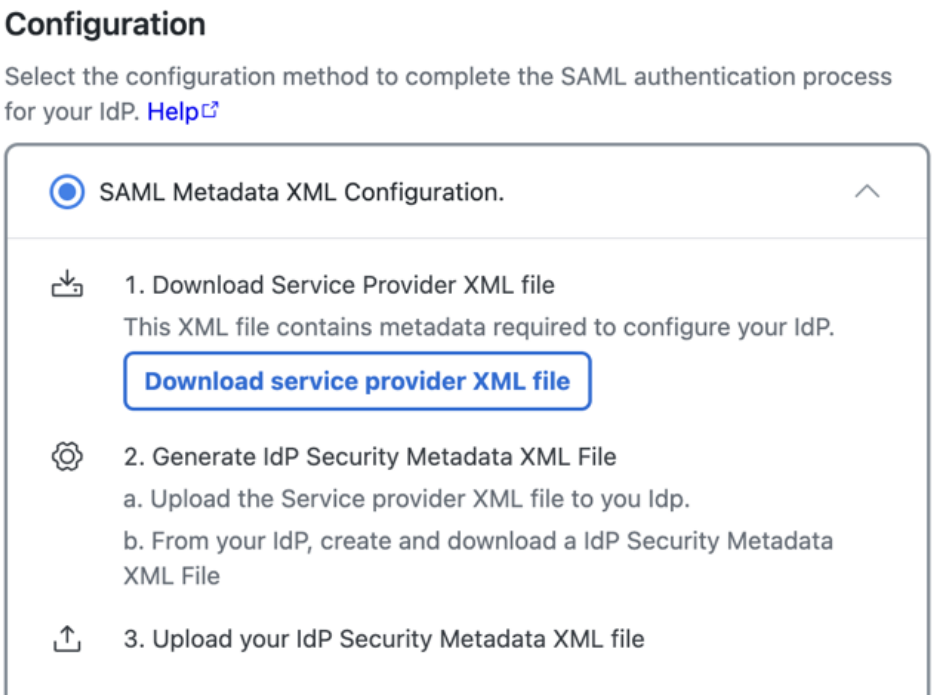
Step 3a - Upload the Identity Provider's SAML Metadata XML File

Provides instructions for step 3a – upload the identity provider's saml metadata xml file. Download the Secure Access Metadata XML file, configure the SAML IdP, and then upload the IdP's metadata XML file to Secure Access.

Download the Secure Access Metadata XML file, configure the SAML IdP, and then upload the IdP's metadata XML file to Secure Access.

Procedure

Check **SAML Metadata XML Configuration**.



What to do next

1. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

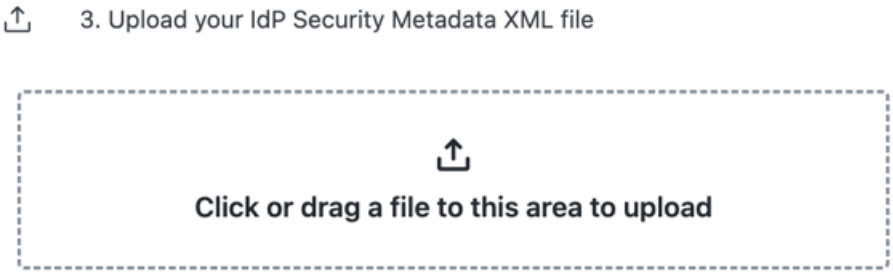
   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

2. Configure Ping Identity for SAML.

   You must configure Secure Access as a generic SAML 2.0 application within Ping Identity. Ping Identity does not provide a method to upload Secure Access metadata for automatic configuration. Extract the **EntityID** and **AssertionConsumerService** URLs from the Secure Access metadata and add these to the applicable fields in Ping Identity. Contact Ping Identity for assistance.

3. Upload the configured IdP Metadata XML file to Secure Access, and then click **Done**.

   The IdP's Metadata XML file contains the IdP's root certificate, which is required to integrate the IdP with Secure Access.



Step 3b – Add the Identity Provider's SAML Metadata

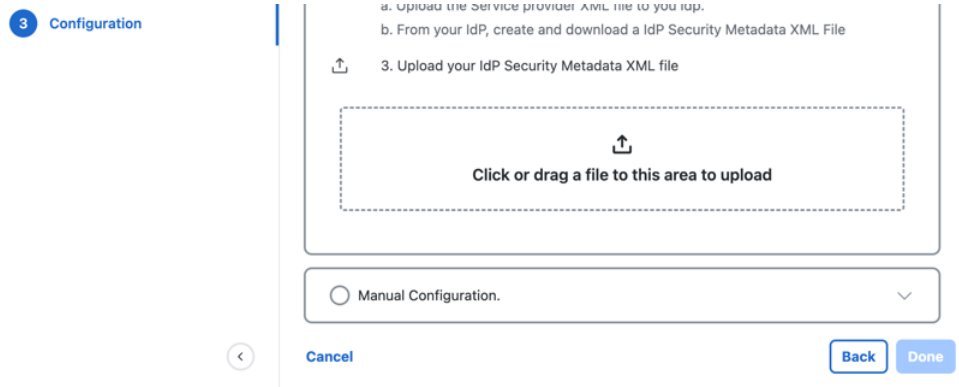
Provides instructions for step 3b - add the identity provider's saml metadata. If you uploaded your IdP's SAML Metadata XML file to Secure Access, you do not have to complete the following steps.

> **Note**
>
> If you uploaded your IdP's SAML Metadata XML file to Secure Access, you do not have to complete the following steps.

Download the Secure Access Metadata XML file, configure the SAML IdP, and then add the IdP's metadata in Secure Access.

Procedure

1. Check **Manual Configuration**.



2. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

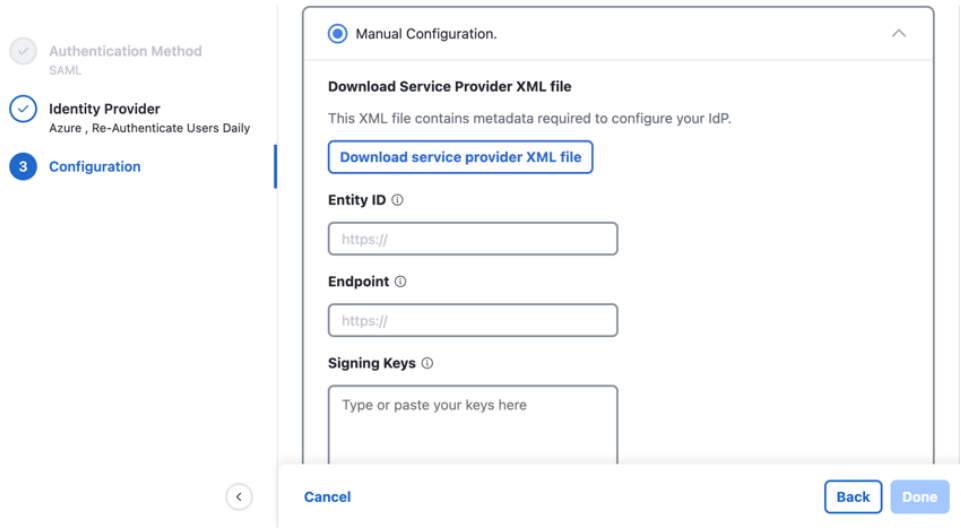
   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP signing certificate, refer to your vendor's documentation.

3. Configure Ping Identity for SAML.

   You must configure Secure Access as a generic SAML 2.0 application within Ping Identity. Ping Identity does not provide a method to upload Secure Access metadata for automatic configuration. Extract the **EntityID** and **AssertionConsumerService** URLs from the Secure Access metadata and add these to the applicable fields in Ping Identity. Contact Ping Identity for assistance.

4. Enter the identity provider's metadata, and then click **Done**.
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
   - **Signed Authentication Request (optional)**–Choose whether you can sign the authentication request for the IdP.



Test the Identity Provider Integration

Describes testing the identity provider integration. To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

View the SAML Certificates in Secure Access

Describes viewing the saml certificates in secure access. Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Configure OpenAM for SAML

Describes configuring openam for saml. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the OpenAM SAML IdP with Secure Access by uploading the OpenAM XML metadata file to Secure Access, or alternatively add the OpenAM metadata in Secure Access manually.

Procedure for Configure OpenAM for SAML

Describes procedure for configure openam for saml. Step 1 - Choose an Authentication Method Step 2 - Add an Identity Provider Step 3 - Add the Identity Provider's SAML Metadata to Secure Access

- Step 1 - Choose an Authentication Method

- Step 2 – Add an Identity Provider
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Prerequisites

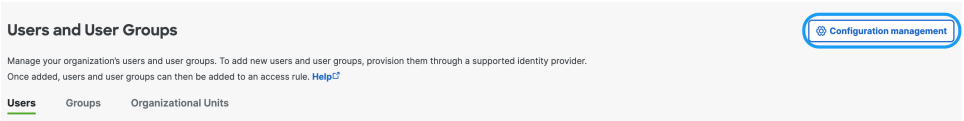
- Full Admin user role. For more information, see Manage Accounts.
- Send **id.secureaccessfed.cisco.com** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Domains.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Domains.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access Security profile. For more information, see Manage Security Profiles.
- Download your IdP's metadata file in XML format.
- The IdP SAML XML metadata file must have a signing key.
- Enable cookies on the browsers on user devices. For more information, see your browser's documentation.
- Enable HTTPS Inspection in the Secure Access Security profile. Secure Access must inspect the Cookie HTTP header to read the SAML cookie. The SAML cookie acts as the authentication token or surrogate. For more information, see Manage Security Profiles.

Step 1 – Choose an Authentication Method

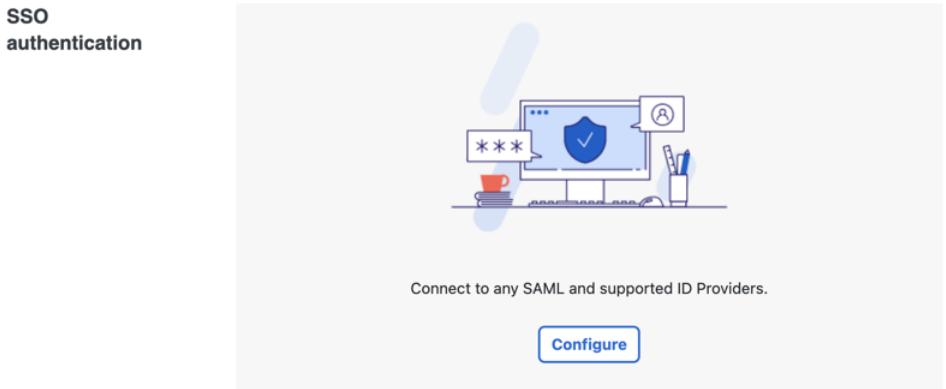
Provides instructions for step 1 – choose an authentication method. Navigate to Connect Users, Groups, and Endpoint Devices and click Configuration Management.

Procedure

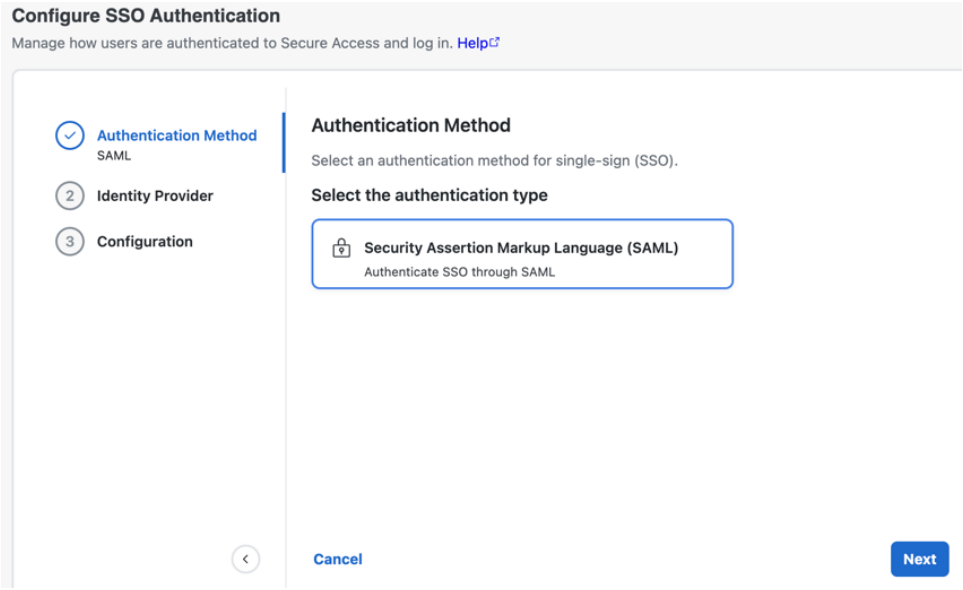
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.

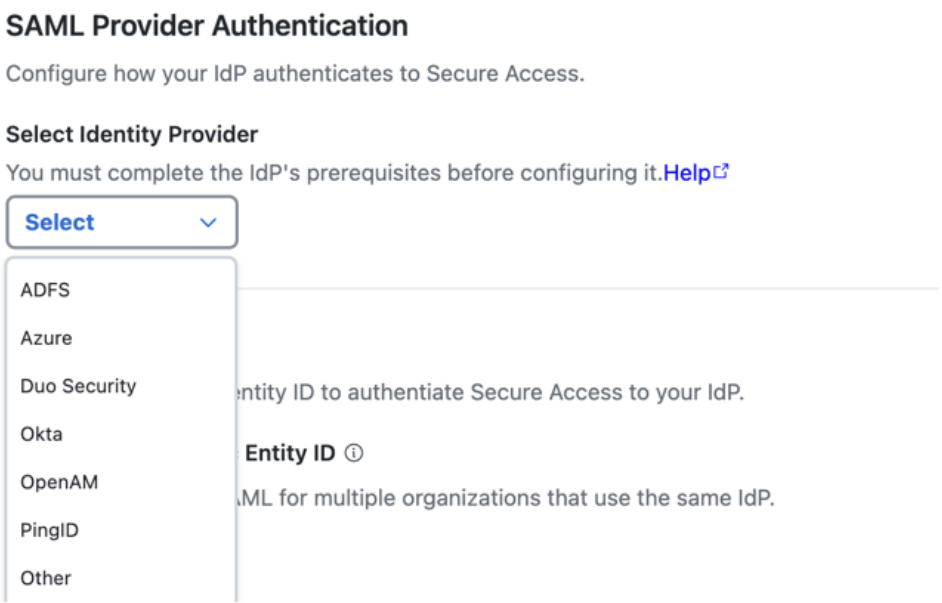


Step 2 – Add an Identity Provider

Provides instructions for step 2 – add an identity provider. For Identity Provider, choose OpenAM. Secure Access supports various IdPs.

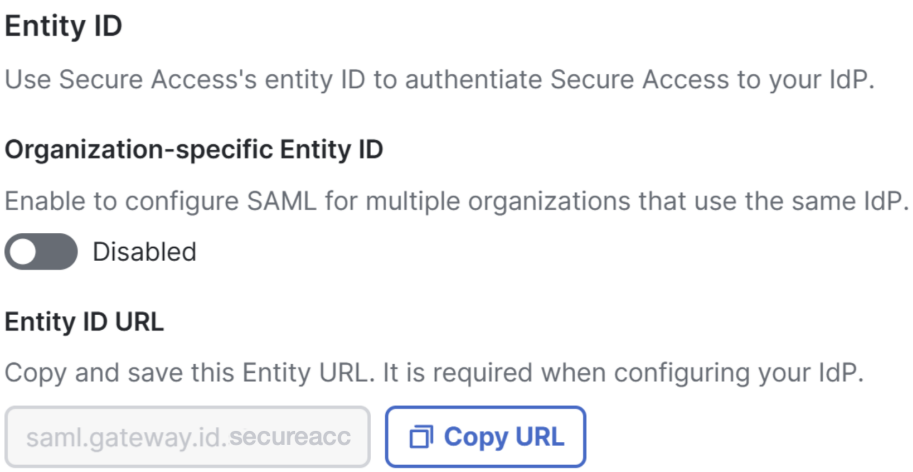
Procedure

1. For **Identity Provider**, choose **OpenAM**. Secure Access supports various IdPs.



2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security and Zero Trust (ZT) for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**. Secure Access allows you to override the default Secure Access SAML EntityID on a per-Org basis.

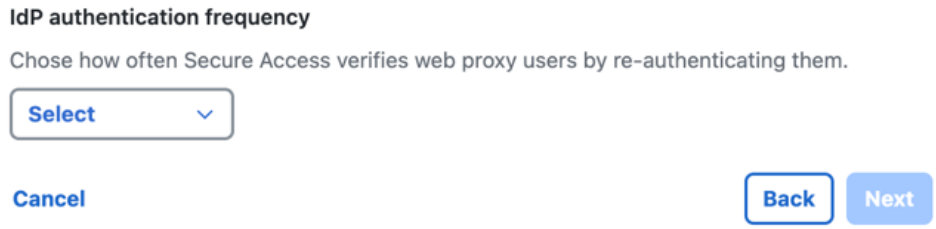
3. For **Entity ID URL**, click **Copy URL** to make a local copy of the Secure Access Entity ID URL. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**.



4. Choose a time interval when a user must authenticate with Secure Access.

   The time intervals are:

   - **Daily**
   - **Weekly**
   - **Monthly**



5. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes step 3 – add the identity provider's saml metadata to secure access. Download the Secure Access Metadata XML file (service provider file) to configure your instance of OpenAM. The Secure Access Metadata XML file includes the Secure Access root certificate.

Download the Secure Access Metadata XML file (service provider file) to configure your instance of OpenAM. The Secure Access Metadata XML file includes the Secure Access root certificate.

Then, either upload the OpenAM SAML metadata XML file to Secure Access or add the SAML metadata directly in Secure Access.

- Step 3a – Upload the Identity Provider's SAML Metadata XML File
- Step 3b – Add the Identity Provider's SAML Metadata

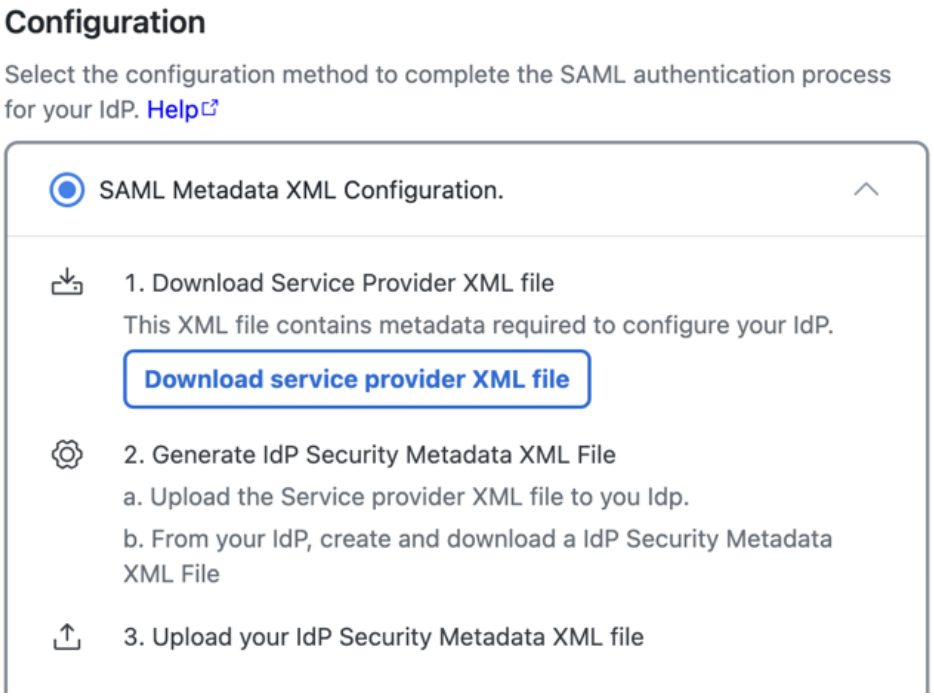
Step 3a – Upload the Identity Provider's SAML Metadata XML File

Provides instructions for step 3a - upload the identity provider's saml metadata xml file. Download the Secure Access Metadata XML file, configure the SAML IdP, and then upload the IdP's metadata XML file to Secure Access.

Download the Secure Access Metadata XML file, configure the SAML IdP, and then upload the IdP's metadata XML file to Secure Access.

Procedure

1. Check **SAML Metadata XML Configuration**.



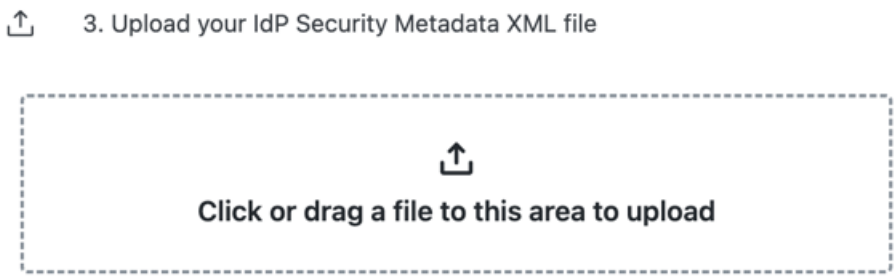
2. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

3. Configure your OpenAM instance with the Secure Access SAML metadata.
4. Upload the configured IdP Metadata XML file to Secure Access, and then click **Done**.

   The IdP's Metadata XML file contains the IdP's root certificate, which is required to integrate the IdP with Secure Access.



Step 3b – Add the Identity Provider's SAML Metadata

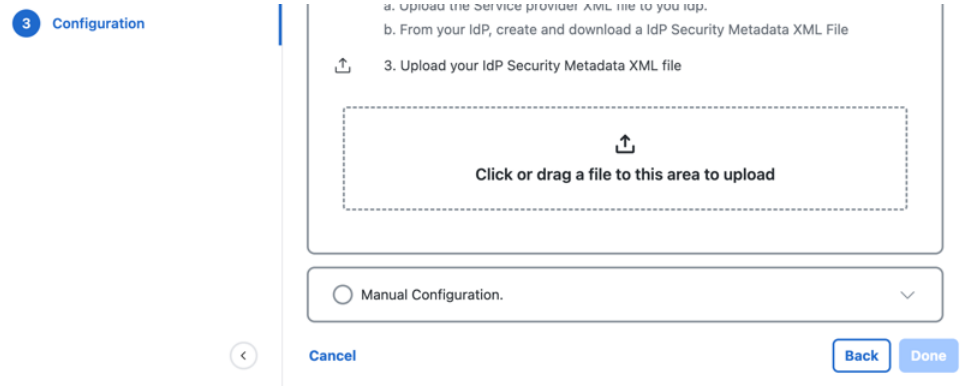
Provides instructions for step 3b – add the identity provider's saml metadata. Download the Secure Access Metadata XML file, configure the SAML IdP, and then add the IdP's metadata in Secure Access.

> **Note**
>
> If you uploaded your IdP's SAML Metadata XML file to Secure Access, you do not have to complete the following steps.

Download the Secure Access Metadata XML file, configure the SAML IdP, and then add the IdP's metadata in Secure Access.

Procedure

1. Check **Manual Configuration**.



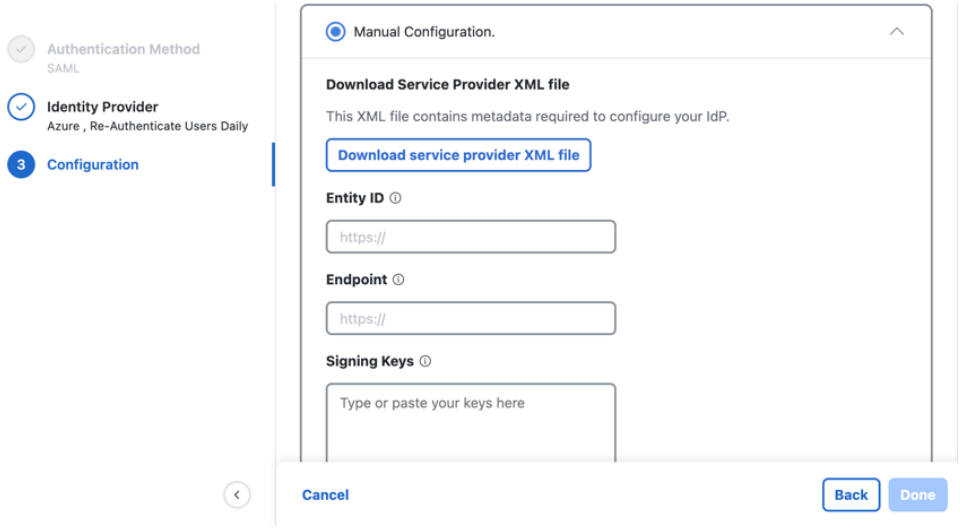
2. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP signing certificate, refer to your vendor's documentation.

3. Enter the identity provider's metadata, and then click **Done**.
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.

- **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
- **Signed Authentication Request (optional)**–Choose whether you can sign the authentication request for the IdP.



Test the Identity Provider Integration

Describes testing the identity provider integration. To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

View the SAML Certificates in Secure Access

Describes viewing the saml certificates in secure access. Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Configure Microsoft Entra ID for SAML

Describes configuring microsoft entra id for saml. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust (ZT) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the Microsoft Entra ID SAML IdP with Secure Access by uploading the Microsoft Entra ID XML metadata file to Secure Access, or alternatively add the Microsoft Entra ID metadata in Secure Access manually.

For information about provisioning an organization's users from Microsoft Entra ID in Secure Access, see Provision Users and Groups from Azure.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Provision users and groups from your organization in Secure Access. The users and groups must match the identities obtained from SAML. For more information, see Manage Users and Groups.
- Send **id.secureaccessfed.cisco.com** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Domains.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Domains.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access Security profile. For more information, see Manage Security Profiles.
- Download your IdP's metadata file in XML format.
- The IdP SAML XML metadata file must have a signing key.
- Enable cookies on the browsers on user devices. For more information, see your browser's documentation.
- Enable HTTPS Inspection in the Secure Access Security profile. Secure Access must inspect the Cookie HTTP header to read the SAML cookie. The SAML cookie acts as the authentication token or surrogate. For more information, see Manage Security Profiles.
- You must install the Cisco Secure Access root certificate on all client machines egressing from networks or network tunnels where SAML is enabled. For more information, see Manage Certificates.

Bypass Domains from SSL Decryption

Describes bypass domains from ssl decryption. We recommend that you bypass certain domains on the secure web gateway. For more information, see Manage Domains.

We recommend that you bypass certain domains on the secure web gateway. For more information, see Manage Domains.

To exclude a domain from Secure Access SSL Decryption, add the following domain names to the list of bypassed domains:

- **login.live.com**
- **login.microsoftonline.com**
- **msauth.net**
- **msftauth.net**

Procedure for Configure Microsoft Entra ID for SAML

Describes procedure for configure microsoft entra id for saml. Step 1 – Choose an Authentication Method Step 2 – Add an Identity Provider

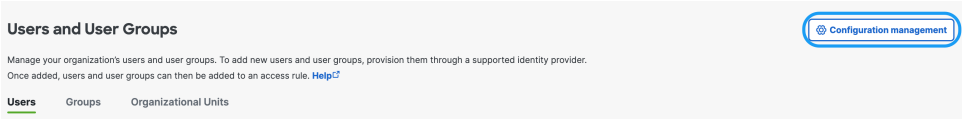
- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Configure the Identity Provider's SAML Metadata

Step 1 – Choose an Authentication Method

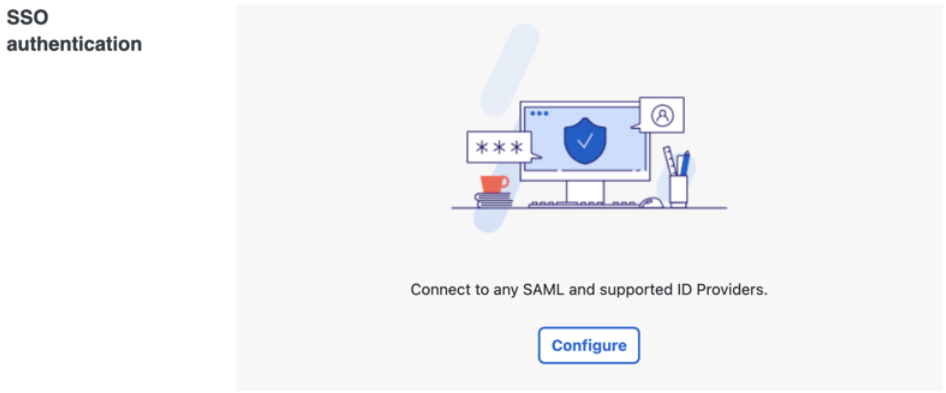
Provides instructions for step 1 – choose an authentication method. Navigate to Connect Users, Groups, and Endpoint Devices and click Configuration Management.

Procedure

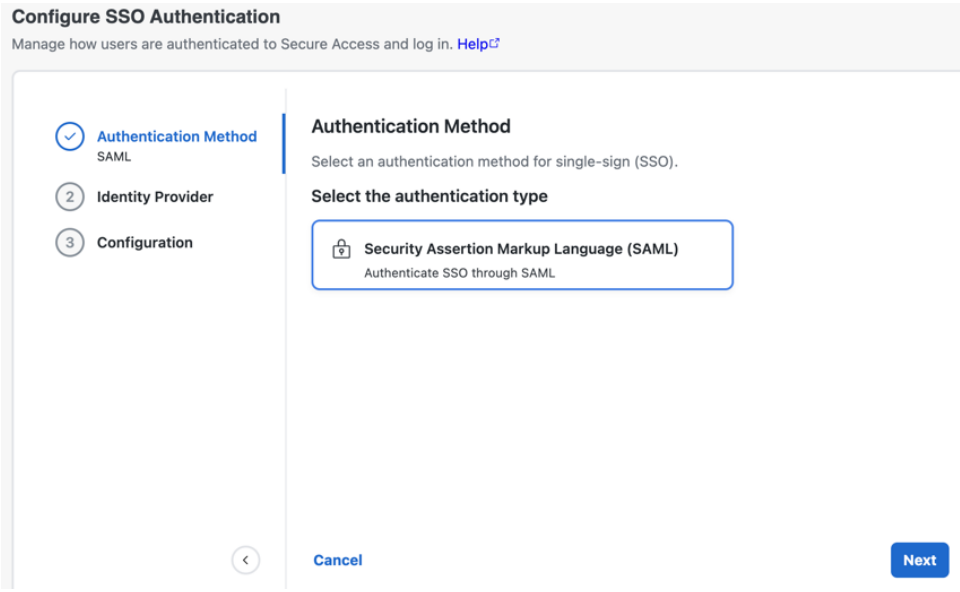
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.

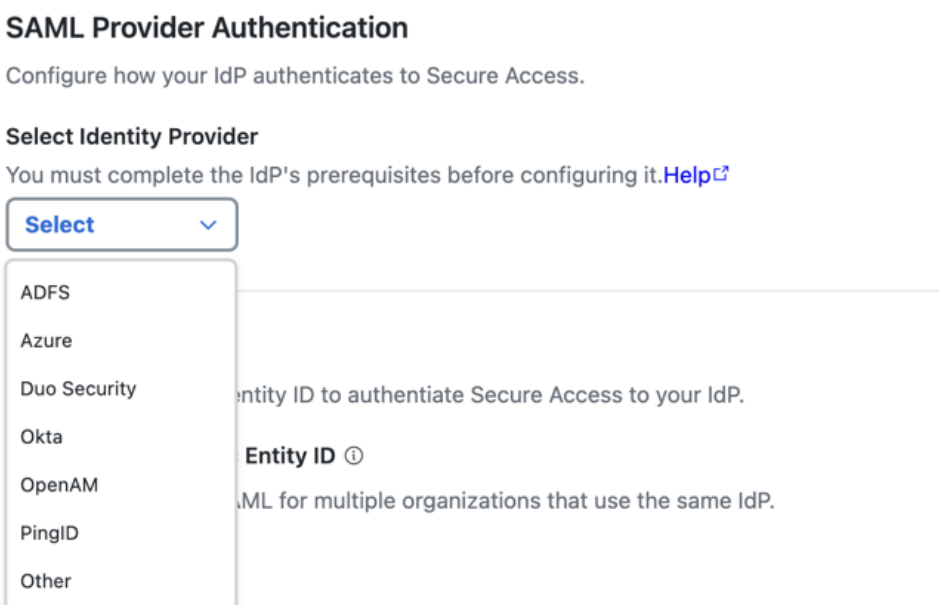


Step 2 – Add an Identity Provider

Provides instructions for step 2 – add an identity provider. For Identity Provider, choose Azure. Secure Access supports various IdPs.

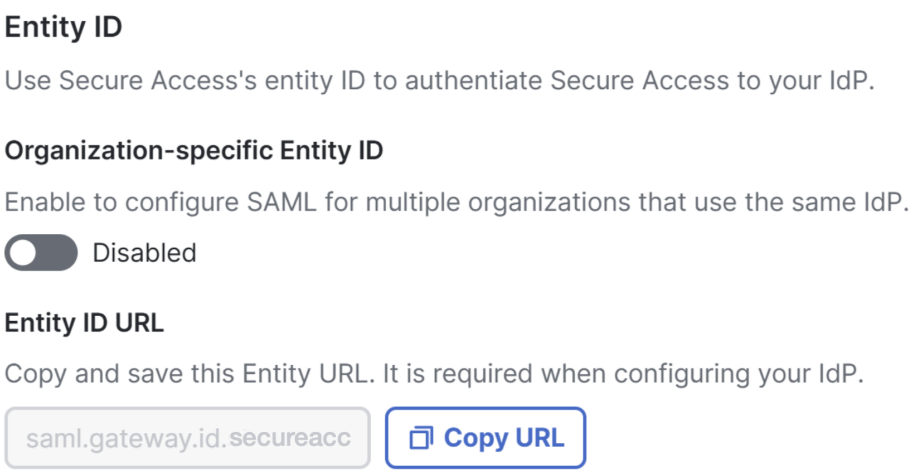
Procedure

1. For **Identity Provider**, choose **Azure**. Secure Access supports various IdPs.



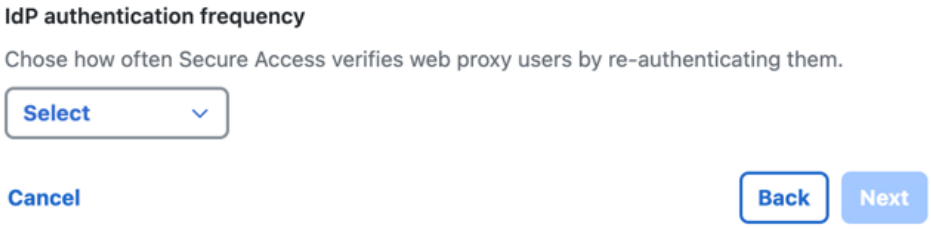
2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security and Zero Trust (ZT) for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**. Secure Access allows you to override the default Secure Access SAML EntityID on a per-Org basis.

3. For **Entity ID URL**, click **Copy URL** to make a local copy of the Secure Access Entity ID URL. The Secure Access SAML default common `EntityID` is **saml.gateway.id.secureaccessfed.cisco**.



4. Choose a time interval when a user must authenticate with Secure Access.

   The time intervals are:
   - **Daily**
   - **Weekly**
   - **Monthly**



5. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes step 3 – add the identity provider's saml metadata to secure access. Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Microsoft Entra ID. The Secure Access Metadata XML file includes the Secure Access root certificate.

Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Microsoft Entra ID. The Secure Access Metadata XML file includes the Secure Access root certificate.

> **Note**
>
> Microsoft Entra ID does not provide the option to directly upload the Secure Access metadata XML file. You must manually enter the Secure Access service provider metadata. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

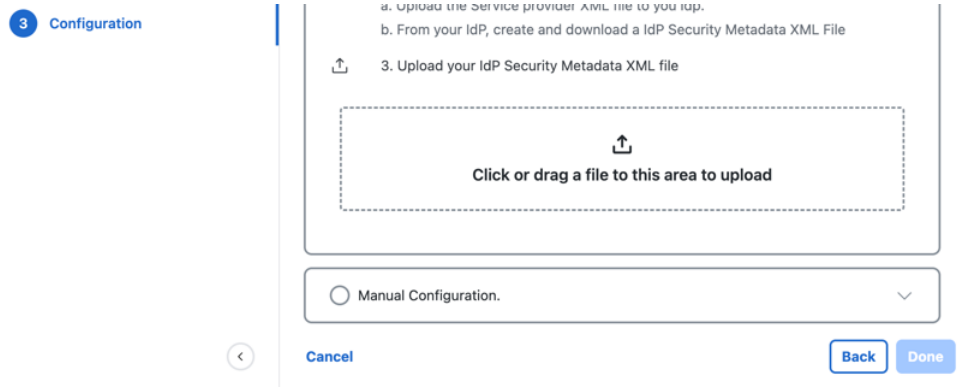
Step 3a – Download the Secure Access Service Provider XML File

Provides instructions for step 3a – download the secure access service provider xml file. Check Manual Configuration, and then click Download service provider XML file to save the Cisco_FedSSE_SP_Metadata XML file to your local device.

Procedure

---

1. Check **Manual Configuration**, and then click **Download service provider XML file** to save the **Cisco_FedSSE_SP_Metadata** XML file to your local device.



2. Open the **Cisco_FedSSE_SP_Metadata** XML file.

3. Copy the certificates from the **Cisco_FedSSE_SP_Metadata** XML file to a new file and save. Use the certificate file in the next step when you create the app integration in Azure.

Step 3b – Add Secure Access Service Provider Metadata to Microsoft Entra ID

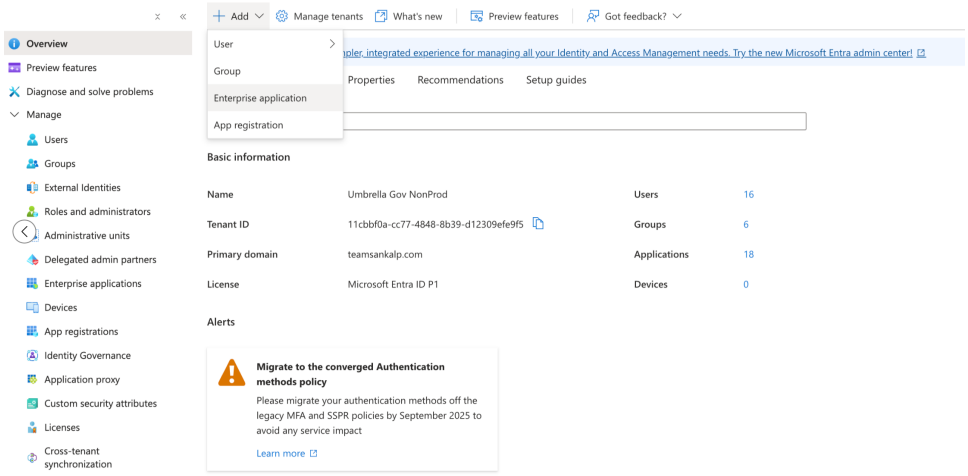
Provides instructions for step 3b – add secure access service provider metadata to microsoft entra id. Add the Secure Access service provider metadata to your instance of Microsoft Entra ID.

Add the Secure Access service provider metadata to your instance of Microsoft Entra ID.

You must configure Secure Access as a generic SAML 2.0 application within Azure. Azure does not provide a method to upload Secure Access metadata for automatic configuration. Extract the **EntityID** and **AssertionConsumerService** values from the Secure Access metadata file and add these to the applicable fields in Azure. Contact Microsoft for assistance.

Procedure

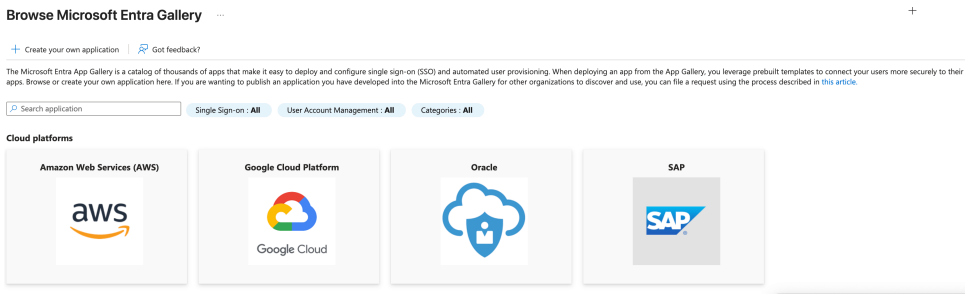
1. Sign in to Azure and click **Microsoft Entra ID**. Choose **Enterprise Applications** from the **+Add** drop-down menu.



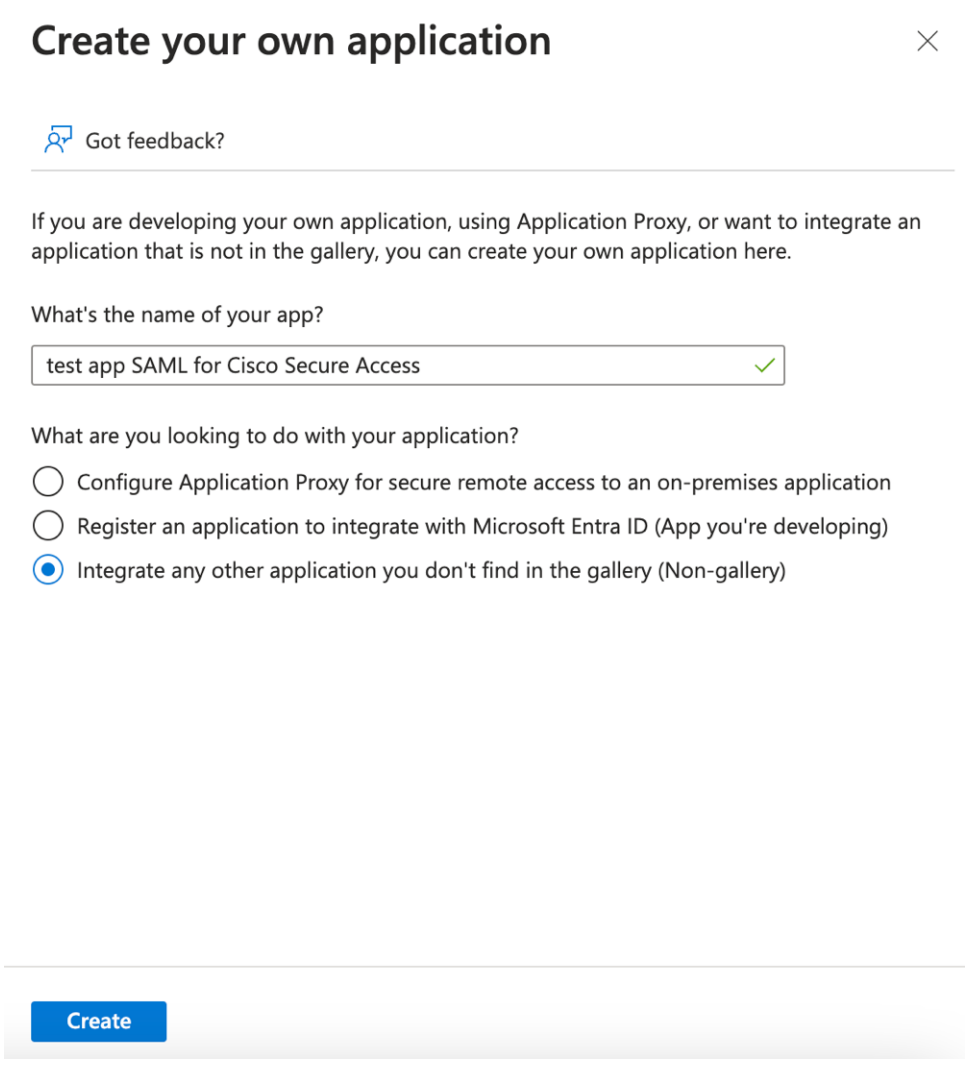
2. Select **New Application**.



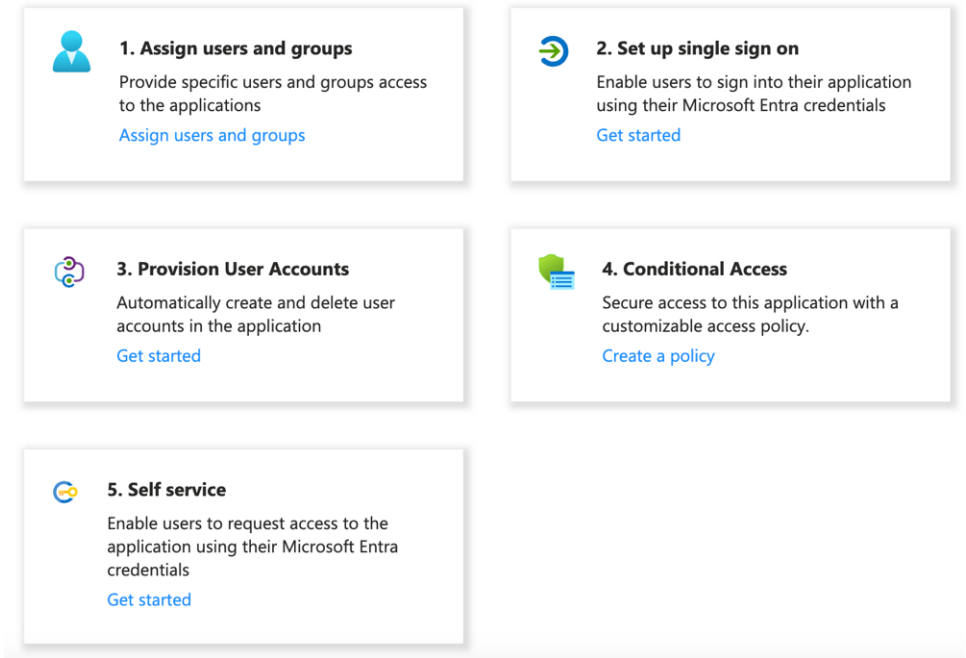
3. Select **Create your own Application**.



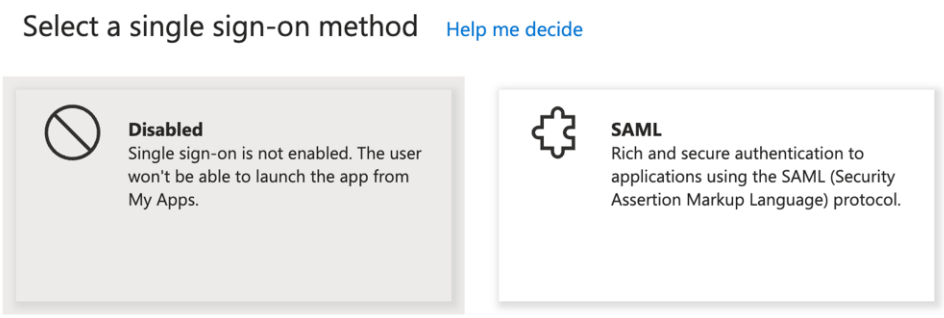
4. Give the new application a meaningful name, select **Integrate any other application you don't find in the gallery (Non-gallery)**, and then click **Create**.



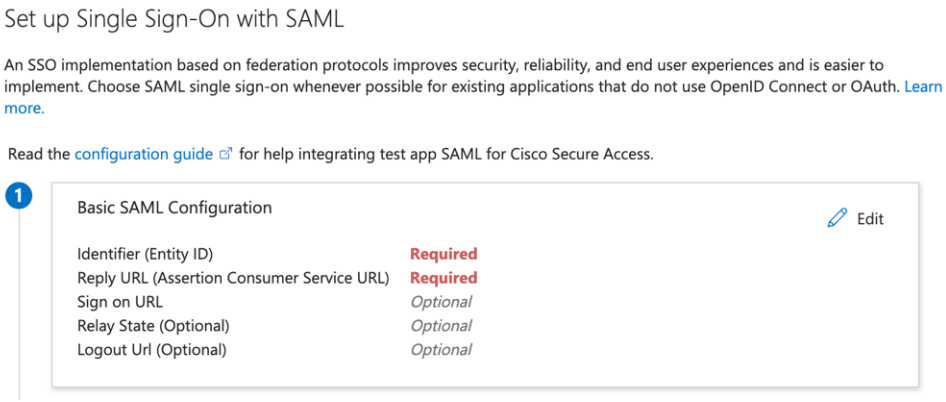
5. Navigate to **Getting Started**, and then click **Set up single sign on**.



6. Click **SAML** to select the sign-on method.

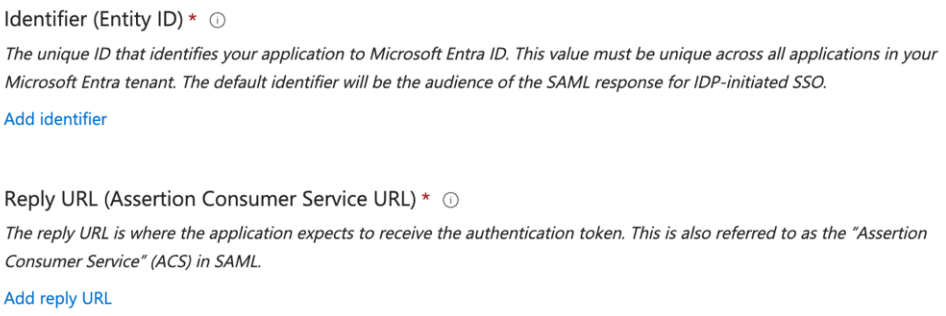


7. For **Basic SAML Configuration**, click **Edit**.



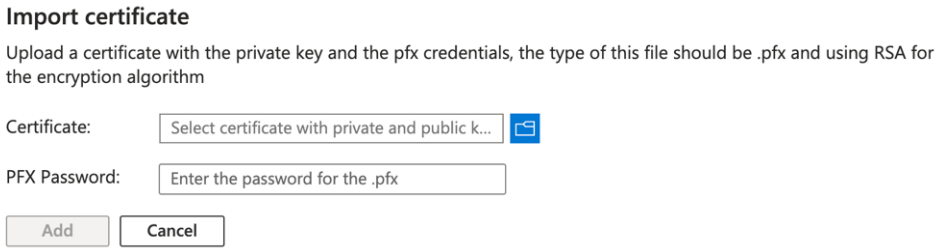
   a. For **Identifier (Entity ID)** (Microsoft Entra ID), click **Add identifier** and enter **saml.gateway.id.secureaccessfed.cisco** in the text area.

8. For **Reply URL (Assertion Consumer Service URL)**, click **Add reply URL** and enter **https://gateway.id.secureaccessfed.cisco/gw/auth/acs/response**.



9. **For SAML Certificates**, click **Edit**.

   a. Click **Import Certificate** to upload the root certificate that you downloaded from the **Cisco_SSE_SP_Metadata** XML file.



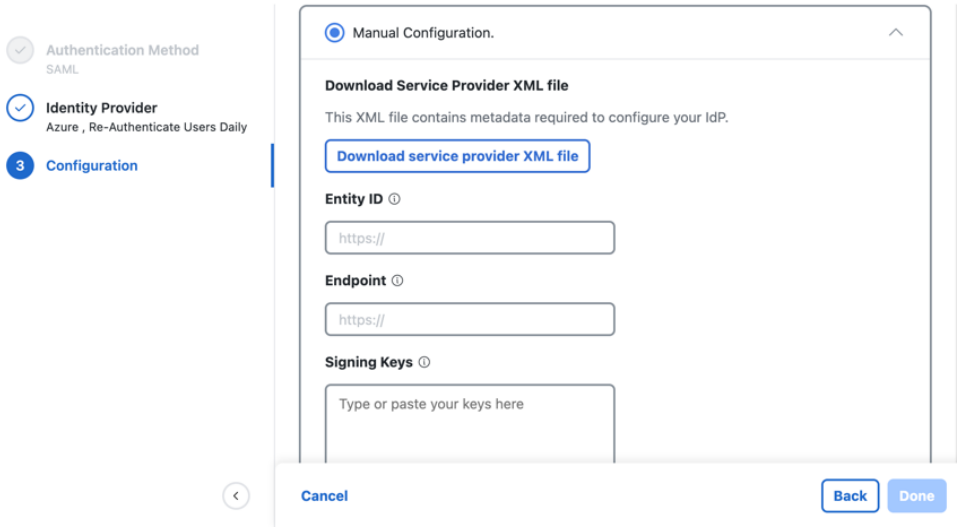
10. Download the **Federation Metadata XML** file. Use the file to upload the configured Azure SAML attributes to Secure Access.

Step 3c – Add the Azure SAML Metadata to Secure Access

Describes step 3c - add the azure saml metadata to secure access. Complete the manual configuration of Azure in Secure Access. Enter your Azure SAML metadata for the following Secure Access settings:

Complete the manual configuration of Azure in Secure Access. Enter your Azure SAML metadata for the following Secure Access settings:

- **Entity ID**–A globally unique name for an identity provider.
- **Endpoint**–The URL used to communicate with your identity provider.
- **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
- **Signed Authentication Request (optional)**–Choose whether to sign the authentication request for the IdP.



1. On Azure, copy the value of **Microsoft Entra Identifier**. Navigate to Secure Access and and enter the value in **Entity ID** .
2. On Azure, copy the value of **Login URL**. Navigate to Secure Access and enter the value in **Endpoint**.
3. On Azure, Copy the value of **Signing Certificate**. Navigate to Secure Access and enter the value in **Signing Keys**.
4. (Optional) Navigate to Secure Access and choose whether to sign the authentication request.
5. On Secure Access, click **Done**.

Test the Identity Provider Integration

Describes testing the identity provider integration. To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

To complete the integration of the SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

View the SAML Certificates in Secure Access

Describes viewing the saml certificates in secure access. Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access (service provider) and the SAML IdP. For more information, see Manage Certificates.

SAML Certificate Renewal Options

Describes saml certificate renewal options. A SAML identity provider (IdP) may require the verification of a service provider's request signing certificate. When you integrate a SAML IdP with Secure Access, you may have to import the Secure Access certificate information in to your IdP platform.

A SAML identity provider (IdP) may require the verification of a service provider's request signing certificate. When you integrate a SAML IdP with Secure Access, you may have to import the Secure Access certificate information in to your IdP platform.

> **Note**
>
> Many IdPs do not validate SAML request signatures and therefore these steps are not required. We recommend that you contact your IdP for confirmation.

There are two options for importing the certificate information into your IdP: Automatic Configuration and Manual Import.

Known Limitations

Describes known limitations. If you have multiple Secure Access organizations and use the Secure Access multiple-Org SAML EntityID, then you must not use the URL-based metadata update mechanism. The Multiple-Org SAML Entity ID only applies if you have multiple Secure Access organizations linked to the same IdP.

If you have multiple Secure Access organizations and use the Secure Access multiple-Org SAML EntityID, then you must not use the URL-based metadata update mechanism. The Multiple-Org SAML Entity ID only applies if you have multiple Secure Access organizations linked to the same IdP. In this scenario you should manually add the Secure Access request signing certificate to each IdP configuration.

Automatic Configuration Through the Fixed Metadata URL

Describes automatic configuration through the fixed metadata url. This option is the preferred configuration method for IdPs that support automatic updates of metadata through an URL. This includes popular IdPs such as AD FS and Ping Identity.

This option is the preferred configuration method for IdPs that support automatic updates of metadata through an URL. This includes popular IdPs such as AD FS and Ping Identity. The benefit is that the IdP automatically imports a new Secure Access certificate each year without manual intervention.

Prerequisites

- An IdP that supports automatic updates of a service provider's metadata from a URL, for example: AD FS and Ping Identity.
- Your IdP platform can read the Secure Access metadata URL:
  - `https://devices.api.secureaccessfed.cisco/admin/v2/samlsp/certificates/Cisco_SSE_SP_Metadata.xml`

- Your IdP platform can read the associated Certificate Authority URLs:
  - `http://r3.o.lencr.org`
  - `http://r3.i.lencr.org`
- Your IdP platform must support TLS 1.2 in order to connect to the Secure Access metadata URL securely. If the IdP application utilizes .NET framework 4.6.1 or earlier this may require some further configuration. See Microsoft's documentation.

Manual Import of the Secure Access Signing Certificate

Describes manual import of the secure access signing certificate. This option is for IdPs that do not support automatic updates of the SAML metadata. You must import the new Secure Access signing certificate each year in to your identity provider.

This option is for IdPs that do not support automatic updates of the SAML metadata. You must import the new Secure Access signing certificate each year in to your identity provider.

Test SAML Identity Provider Integration

Describes testing saml identity provider integration. After you integrate an SAML identity provider (IdP) with Cisco Secure Access, you can test whether a user in Secure Access can authenticate with the configured IdP.

After you integrate an SAML identity provider (IdP) with Cisco Secure Access, you can test whether a user in Secure Access can authenticate with the configured IdP.

Procedure for Test SAML Identity Provider Integration

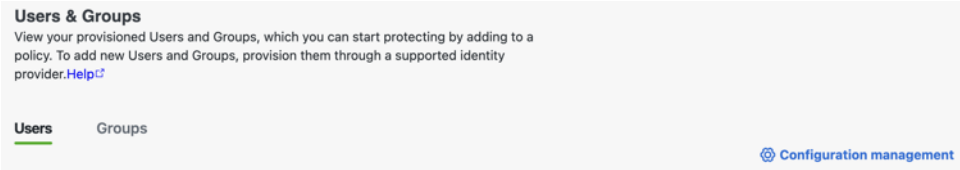
Provides instructions for testing saml identity provider integration.

Before you begin

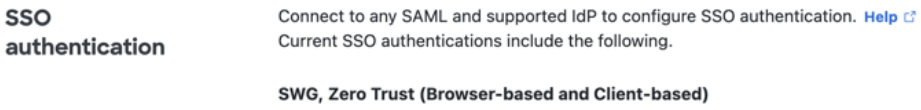
- Full Admin user role. For more information, see Manage Accounts.

Procedure

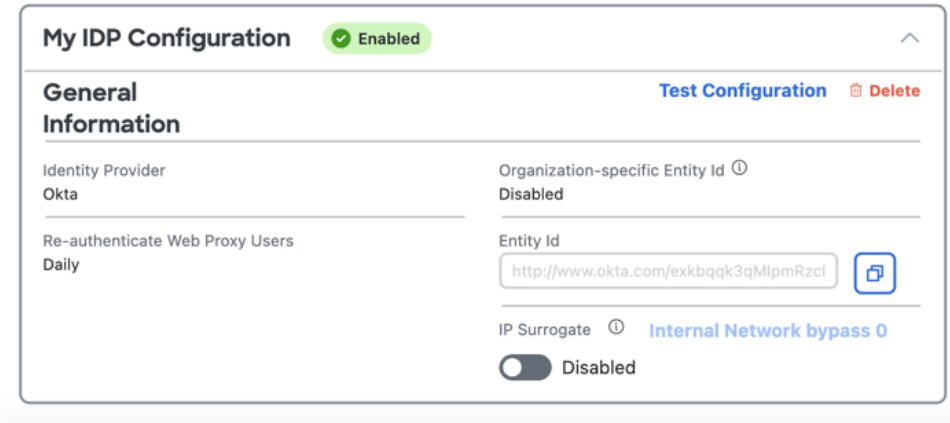
1. Navigate to **Connect** > **Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication**.



3. Click **Test Configuration** to confirm that a user in Secure Access can authenticate with the integrated IdP. Secure Access redirects you to sign in to your identity provider.



Delete SAML Identity Provider Integration

Describes deleting saml identity provider integration. After you integrate an SAML identity provider (IdP) with Cisco Secure Access, you can delete the IdP integration.

After you integrate an SAML identity provider (IdP) with Cisco Secure Access, you can delete the IdP integration.

Procedure for Delete SAML Identity Provider Integration

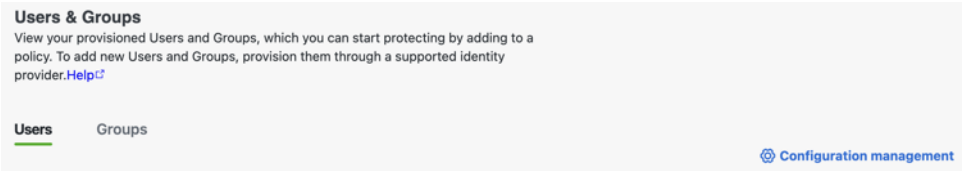
Provides instructions for procedure for delete saml identity provider integration.

Before you begin

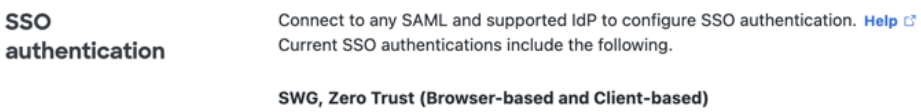
- Full Admin user role. For more information, see Manage Accounts.

Procedure

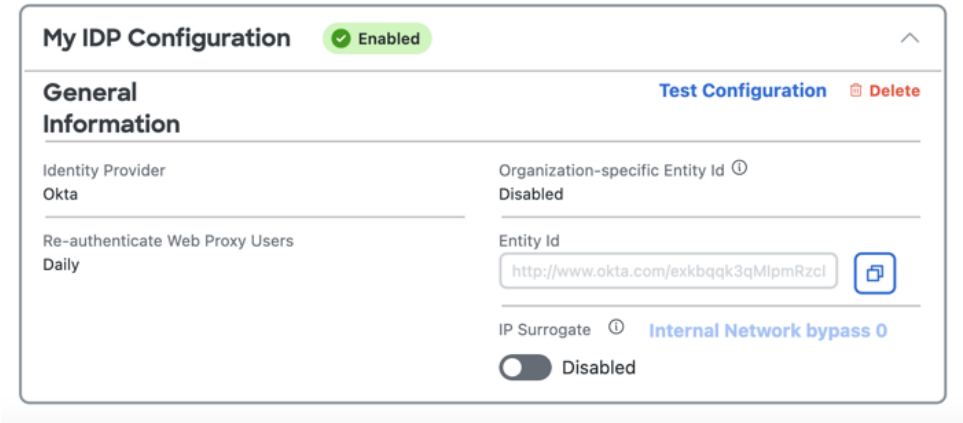
1. Navigate to **Connect** > **Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication**.



3. Click **Delete** to remove the integration between the IdP and Secure Access.


My IDP Configuration
Enabled
General Information
Test Configuration
Delete
Identity Provider
Okta
Organization-specific Entity Id
Disabled
Re-authenticate Web Proxy Users
Daily
Entity Id
http://www.okta.com/exkbqqk3qMlpmRzcl
IP Surrogate
Internal Network bypass 0
Disabled

15 Manage Virtual Private Networks

Topics:

- Add an IP Pool
- Manage VPN Profiles
- Add VPN Profiles
- Add a RADIUS Group
- Manage IP Pools

Introduces managing virtual private networks. A remote access virtual private network (VPN) allows individual users to connect to a network from a remote location using a computer or other supported devices connected to the Internet.

A remote access virtual private network (VPN) allows individual users to connect to a network from a remote location using a computer or other supported devices connected to the Internet. This allows mobile workers to connect from their home networks or a public Wi-Fi network, for example.

Manage the settings and profiles of your virtual private networks (VPNs) registered with Cisco Secure Access. See the following topics for more information related to Virtual Private Networks:

- Manage IP Pools
- Add an IP Pool
- Manage VPN Profiles
- Add VPN Profiles
- Add a RADIUS Group
- Traffic Steering for Client-Based Connections

Add an IP Pool

Describes adding an ip pool. VPN profiles require IP addressing pools in order to be fully-functional. In addition, control plane traffic such as RADIUS is sourced from the Secure Access IP address pools.

VPN profiles require IP addressing pools in order to be fully-functional. In addition, control plane traffic such as RADIUS is sourced from the Secure Access IP address pools.

Add an IP pool that is used to manage a set of IP addresses for your VPN profile. Optionally, add a RADIUS group for VPN profiles.

Prerequisites

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

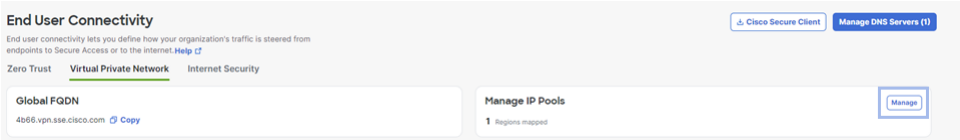
Add an IP Pool

Provides instructions for adding an ip pool. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

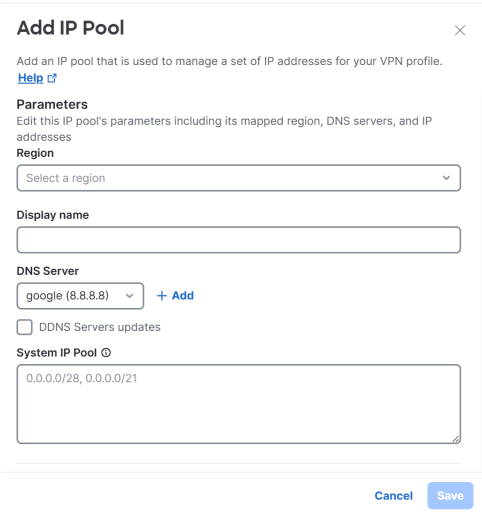
To configure the VPN IP Pool, complete the following steps:

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **Regions and IP Pools**, click **Manage**.



3. Click **Add IP Pool** to add an IP pool that can be used to manage a set of IP addresses for your VPN profiles.
4. Configure the **Parameters** the IP pool:
   - Map the IP pool to a **Region**.
   - Add a meaningful **Display name**.
   - Choose a pair of **DNS Servers** from the drop-down, or click **Add** to add a new DNS pair.
   - Add **System IP Pool** for use with remote access VPN endpoints. You can add multiple comma-separated ranges.



5. Click **Save** when you are done.

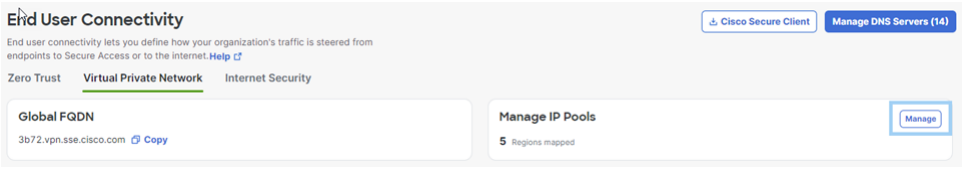
Add a RADIUS Group (optional)

Provides instructions for adding a radius group (optional). It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

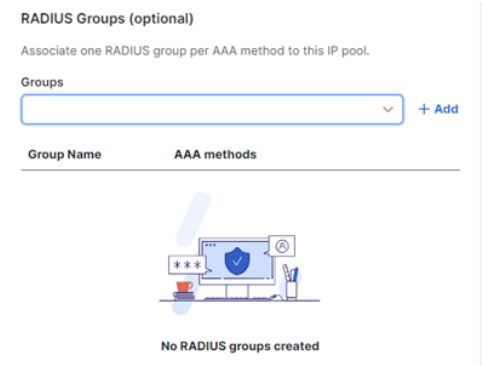
This section describes how to configure a RADIUS group and add servers to the group. This RADIUS group can be applied to the Management IP pool being configured and mapped to other IP pools.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **Manage IP Pools**, click **Manage**.



3. Click **Add IP Pool** and scroll down to **RADIUS Groups (optional)**.



4. Click **ADD RADIUS Group** to configure the RADIUS group and enter a meaningful **Group Name**.



5. Choose the AAA methods to apply to this RADIUS Group. Choose at least one method.

> **Note**
>
> If both the **Authentication** and **Authorization** methods are selected, the same port number must be used.

   a. **Authentication** - Enter the RADIUS authentication **Port** number. The valid range is from 1 to 65535.

      The default is 1812.

      Check **Microsoft CHAPv2** to use Microsoft Challenge Handshake Authentication Protocol Version 2 as the authentication method.

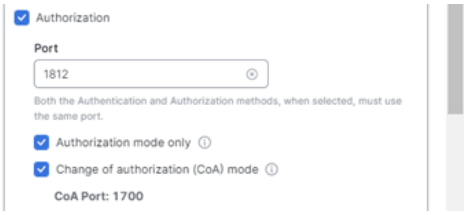


   b. **Authorization**- Enter the RADIUS authorization **Port** number. The valid range is from 1 to 65535.

      The default is 1812.

      When you check **Authorization mode only**, no common password is required.

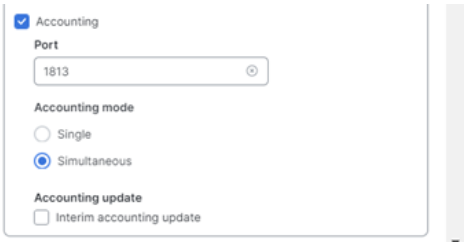
      When you check **Change of authorization (CoA) mode**, the RADIUS server group will be registered for CoA notification. If you enable CoA, the listening port for RADIUS CoA requests uses the default of 1700. Select this option when using this server group for ISE Policy Enforcement in remote access VPNs.



   c. **Accounting**- Enter the RADIUS accounting Port number. The valid range is from 1 to 65535. The default is 1813.

      Select the Accounting mode, either Single or Simultaneous. In single mode, accounting data is sent to only one server. In simultaneous mode, accounting data to all servers in the group.

      For Accounting update, select Interim accounting update to enable the periodic generation of RADIUS interim-accounting-update messages.



6. Configure the method **(Reactivation mode**) by which failed servers in a group are reactivated:

   a. Set the **Max failed attempts** to specify the maximum number of failed AAA transactions with a RADIUS server in the group before trying the next server. The range is from 1 and 5. The default is 3.

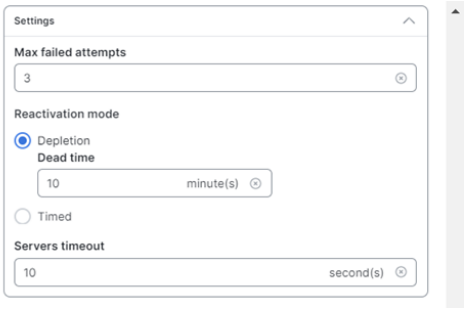
   b. Choose **Depletion, Dead time** to reactivate failed servers only after all of the servers in the group are inactive.

      This is the default reactivation mode. Specify the amount of time, between 0 and 1440 minutes, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers.

      Deadtime applies only if you configure fallback to the local database; authentication is attempted locally until the deadtime elapses. The default is 10 minutes.

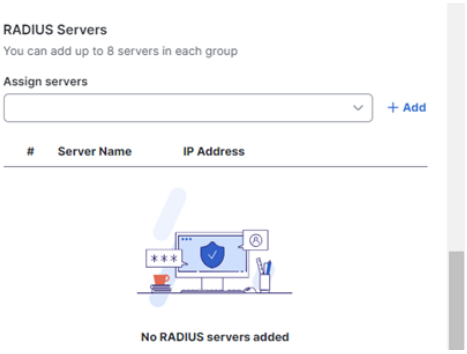
   c. Choose **Timed** to reactivate failed servers after 30 seconds of down time.

   d. Set the **Servers timeout** setting. Enter the number of seconds to wait for a response from a RADIUS server (in seconds). The default is 10 seconds.

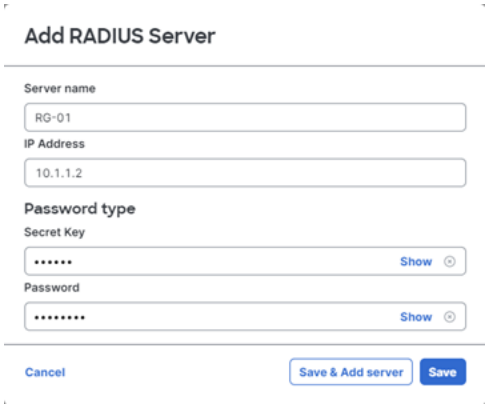


7. Scroll down to **RADIUS Servers** and click **Add**.

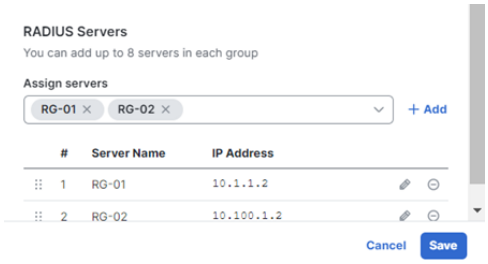
   You can add up to eight servers to each RADIUS group.



8. Enter a meaningful **Server name**, an **IP Address**, and a **Secret Key/Password** combination and click **Save & Add server**.



9. Click **Save** when you are done adding servers to complete the RADIUS Group.



Manage VPN Profiles

Describes managing vpn profiles. A remote access virtual private network (VPN) allows individual users to connect to a network from a remote location using a computer or other supported devices connected to the Internet.

A remote access virtual private network (VPN) allows individual users to connect to a network from a remote location using a computer or other supported devices connected to the Internet. This allows mobile workers to connect from their home networks or a public Wi-Fi network, for example.

See the following topics for more information related to VPN profiles:

- Add VPN Profiles
- Add a RADIUS Group

Add VPN Profiles

Describes adding vpn profiles. A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet. This section describes how to create VPN profiles to allow for configuration of remote user connections through a VPN.

A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet. This section describes how to create VPN profiles to allow for configuration of remote user connections through a VPN.

The following topics explain how to configure remote access VPN profiles.

Prerequisites

- Full Admin role in Secure Access. See Manage Accounts.

Procedure

- Step1 – General Settings
- Step 2 – Authentication, Authorization, and Accounting
- Step 3 – Traffic Steering (Split Tunnel)
- Step 4 – Cisco Secure Client Configuration

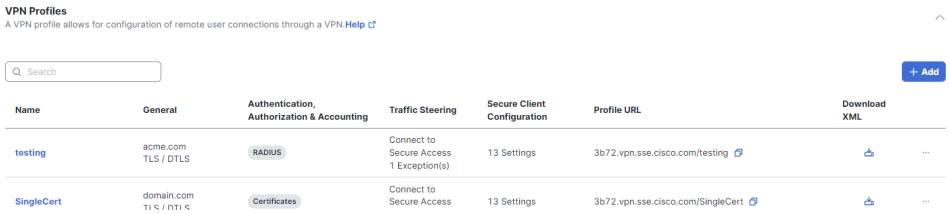
Step 1 – General Settings

Provides instructions for step 1 – general settings. Enter a name and configure the general settings that this VPN profile will use.

Enter a name and configure the general settings that this VPN profile will use.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **VPN Profiles**, click **VPN Profile**.



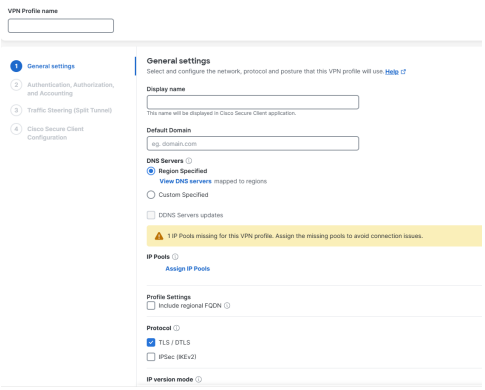
3. Enter a meaningful **VPN Profile name** for this profile.
4. Configure the **General settings** for this VPN profile:
5. Enter the **Display name** for this VPN profile:
6. Enter the **Default Domain**.
7. Choose the required **DNS Servers**.
   - Click the **Region Specified** radio button. Click **View DNS dervers** to view a list of DNS Servers mapped to the region.
   - Click the **Custom Specified** radio button. Click **Map DNS servers** to map a DNS server to a region for this VPN profile.

   > **Note**
   >
   > You can select one DNS server for all the regions.

   Click **DNS Server** to add a new DNS Server.

   The DNS server mapped through the **Manage IP Pool** page is set as the default server. Selecting another DNS server overwrites this default server.
8. Under **IP Pools**, click **Assign IP Pools** to select an IP pool that you want to map to a region for this VPN profile.
9. Under **Profile Settings**, check **Include regional FQDN** check box to add the required regional FQDN.
10. Select the protocol that this VPN profile will use:
    - TLS/DTLS
    - IKEv2

      At least one protocol must be selected. If both **TLS/DTLS** and **IKEv2** are selected, choose the primary protocol from the **Primary** drop-down.
11. Under **IP version mode,** check **IPv6** check box.
12. Optionally, choose a **Connect time posture** from the drop-down.



13. Click **Next**.

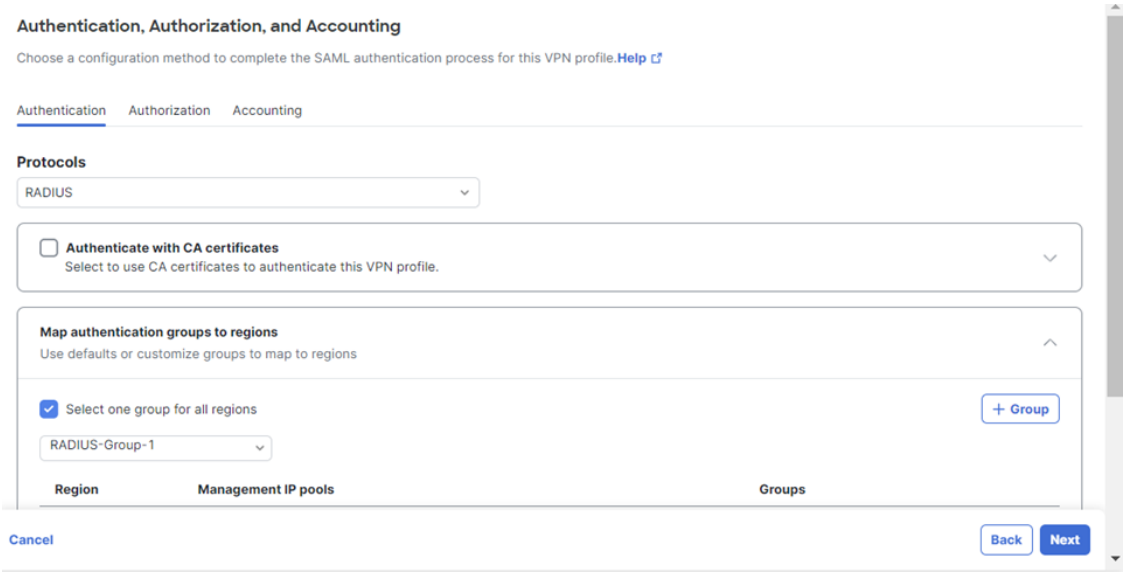
Step 2 – Authentication, Authorization, and Accounting

Describes step 2 - authentication, authorization, and accounting. Choose a configuration method from the Protocols drop-down to complete the authentication process for this VPN profile. Authentication is the process of identifying a user before granting access to the network and its resources.

Choose a configuration method from the **Protocols** drop-down to complete the authentication process for this VPN profile. Authentication is the process of identifying a user before granting access to the network and its resources. Authentication requires valid user credentials, a certificate, or both. You can use authentication alone, or combine it with authorization and accounting.

You can choose from the following authentication methods:

- SAML
- RADIUS
- Certificate



SAML

Describes saml. Use this option to authenticate users with SAML. When you choose SAML, each user is authenticated using the SAML single sign-on server. For more information about Secure Access and SAML, see Configure Integrations with SAML Identity Providers.

Use this option to authenticate users with SAML.

When you choose **SAML**, each user is authenticated using the SAML single sign-on server. For more information about Secure Access and SAML, see Configure Integrations with SAML Identity Providers. SAML authentication for remote access VPNs supports **SAML**, **SAML + Single CA certificate**, and **SAML + Multiple CA Certificates**.

The following procedures describe how to perform:

- SAML Metadata XML Configuration
- Manual Configuration

SAML Metadata XML Configuration

Provides instructions for saml metadata xml configuration. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

To complete your Identity Provider (IdP) setup for Single Sign-On (SSO), you must upload your IdP metadata XML file to Secure Access. To ensure secure Single Sign-On (SSO) and address recent security vulnerabilities (CVE-2025-54982), your Identity Provider (IdP) metadata must include a signing certificate. This certificate is required for verifying the authenticity and integrity of SAML assertions exchanged during the SSO process.

Before you begin

Make sure your IdP metadata XML file contains a `<md:KeyDescriptor use="signing">` element, which includes a valid `<ds:X509Certificate>`.

Example snippet from the IdP metadata XML:

```
<md:KeyDescriptor use="signing">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#  ">
        ds:X509Data
            ds:X509Certificate
                MIID.........
            </ds:X509Certificate>
        </ds:X509Data>
    </ds:KeyInfo>
</md:KeyDescriptor>
```

Procedure

1. Click the **SAML Metadata XML Configuration** option, provide your Service Provider XML file and follow the guidelines to complete your Identity Provider (IdP) setup.
2. Upload your IdP Security Metadata XML file to Secure Access. You can drag-and-drop the file or click the upload icon to browse and select the file.

> **Note**
>
> Failure to include a valid signing certificate in your IdP metadata will prevent the successful configuration of SSO on the dashboard. If the uploaded IdP metadata file does not include a valid signing certifiate, you will encounter the following error message: `Failure to save SSO configuration.`

Manual Configuration

Provides instructions for manual configuration. Click the Manual Configuration option complete the form with information obtained from your Service Provider (SP) and Identity Provider (IdP).

Procedure

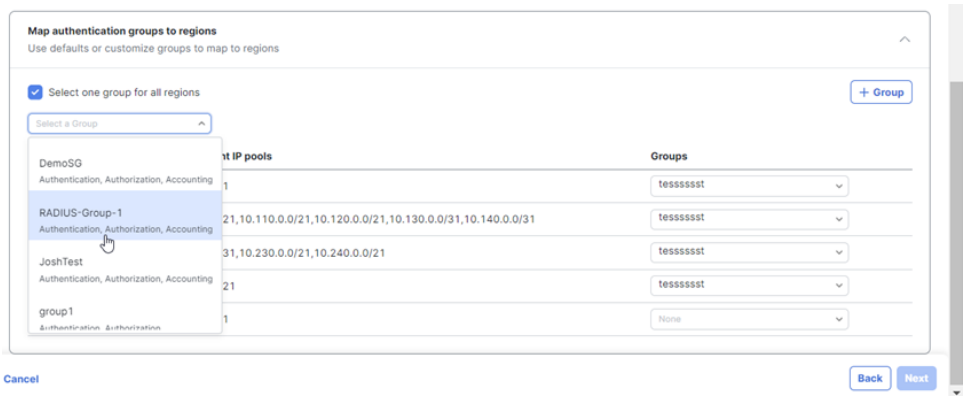
1. Click the **Manual Configuration** option complete the form with information obtained from your Service Provider (SP) and Identity Provider (IdP).
2. Download the SP Certificate.
3. Obtain the following from the SAML IdP:
   a. Identity Provider Entity ID URL.
   b. Sign-in URL.
   c. Sign-out URL.
   d. IdP Certificate.
   e. Request Signature.

RADIUS

Describes radius. Use this option to authenticate users on a RADIUS server. When you choose RADIUS, each user is authenticated using RADIUS group servers. RADIUS authentication for remote access VPNs supports RADIUS, RADIUS+ Single CA certificate, and RADIUS+ Multiple CA Certificates.

Use this option to authenticate users on a RADIUS server.

When you choose **RADIUS**, each user is authenticated using RADIUS group servers. RADIUS authentication for remote access VPNs supports **RADIUS**, **RADIUS+ Single CA certificate**, and **RADIUS+ Multiple CA Certificates**.



Certificate

Describes certificate. Use this option to authenticate users with trusted certificate authorities (CAs). When you choose Certificate, each user is authenticated with a client certificate. The client certificate must be configured on VPN client endpoints.

Use this option to authenticate users with trusted certificate authorities (CAs).

When you choose **Certificate**, each user is authenticated with a client certificate. The client certificate must be configured on VPN client endpoints. By default, the user name is derived from the client certificate fields CN and OU. If the user name is specified in other fields in the client certificate, use the **Primary field to authenticate** and **Secondary field to authenticate** field to map appropriate fields.

Select **Multiple Certificates** authentication to authenticate the VPN client using the machine and user certificates.

If have enabled **Multiple Certificates** authentication, you can select one of the following certificates to map the username and authenticate the VPN user:

- **First Cert**–Select this option to map the username from the machine certificate sent from the VPN client.
- **Second Cert**–Select this option to map the username from the user certificate sent from the client.

> **Note**
>
> If you do not enable multiple certificate authentication, the user certificate (second certificate) is used for authentication by default.

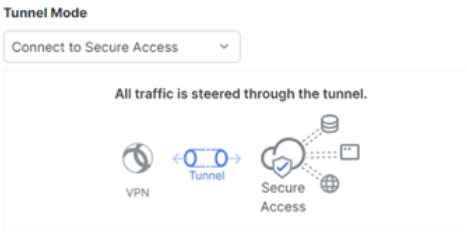
Step 3 – Traffic Steering (Split Tunnel)

Provides instructions for step 3 – traffic steering (split tunnel). Its purpose, requirements, and key details for Cisco Secure Access administrators.

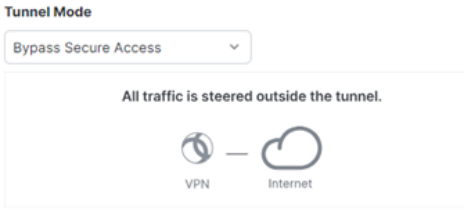
For **Traffic Steering (Split Tunnel)**, you can configure a VPN profile to maintain a full tunnel connection to Secure Access, or configure the profile to use a split tunnel connection to direct traffic through the VPN only if necessary.

Procedure

1. For **Tunnel Mode**, choose either:
   - **Connect to Secure Access** to direct all traffic through the tunnel; or,



   - **Bypass Secure Access** to direct all traffic outside the tunnel.



2. Depending on your selection, you can **Add Exceptions** to steer traffic inside or outside the tunnel. You can enter comma-separated IPs, domains, and network spaces.
3. For **DNS Mode**, you can accept the default mode or, depending on your selection, choose to **Tunnel all DNS** traffic or **Split DNS** traffic.

   When **Split DNS** is chosen, DNS names matching the configured **DNS Names** will be routed over the encrypted Secure Client connection for resolution. Any that do not match the configured **DNS Names** are routed via the local physical interface for the resolution.
4. Click **Next** to configure the Cisco Secure Client.

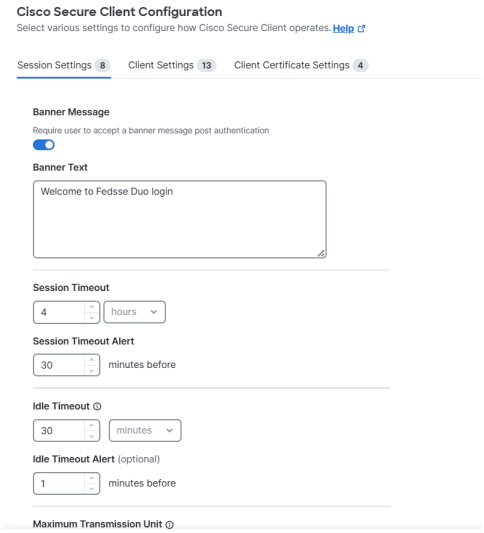
Step 4 – Cisco Secure Client Configuration

Provides instructions for step 4 – cisco secure client configuration. Its purpose, requirements, and key details for Cisco Secure Access administrators.

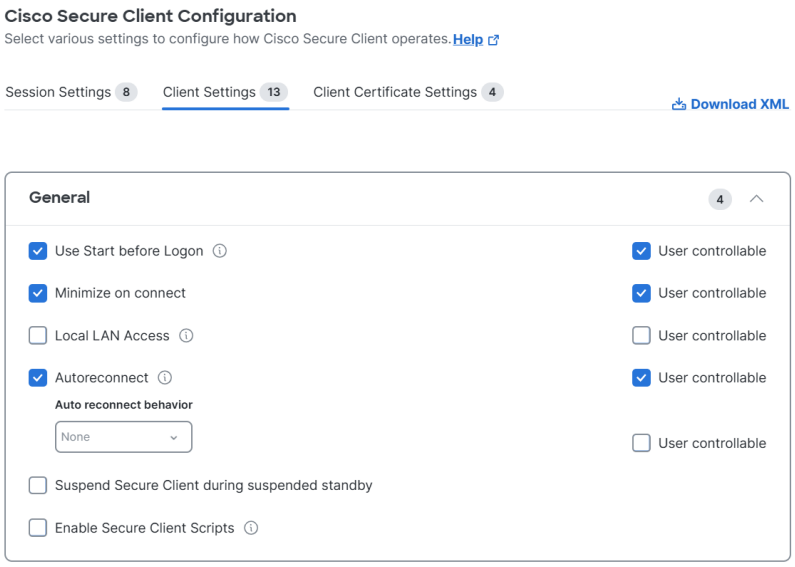
You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN profile.

Procedure

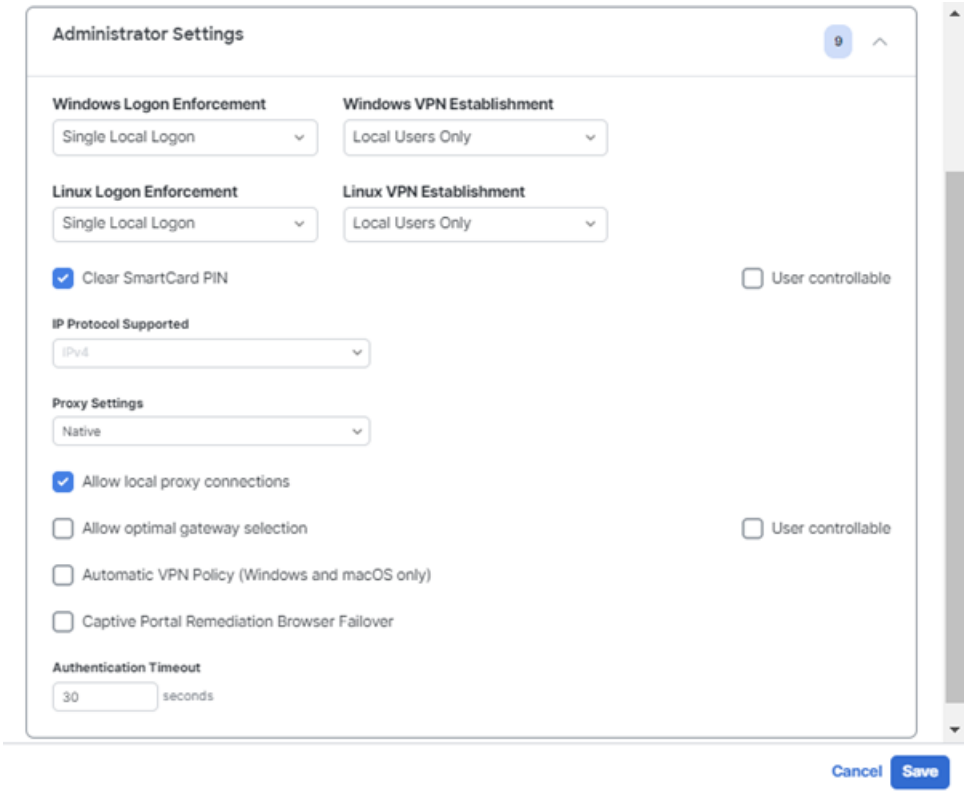
1. Click the **Session Settings** tab to modify session-specific settings, such as the **Banner Message**, **Session Timeout** and **Session Timeout Alert**, **Idle Timeout**, **Idle Timeout Alert**, **Maximum Transmission Unit**, and the **Smart card removal**.



2. Click the **Client Settings** tab then click **Edit** to modify client-specific sessions. See The Cisco Secure Client Profile Editor for complete information about Cisco Secure Client settings.
   a. Modify **General** client settings as needed.

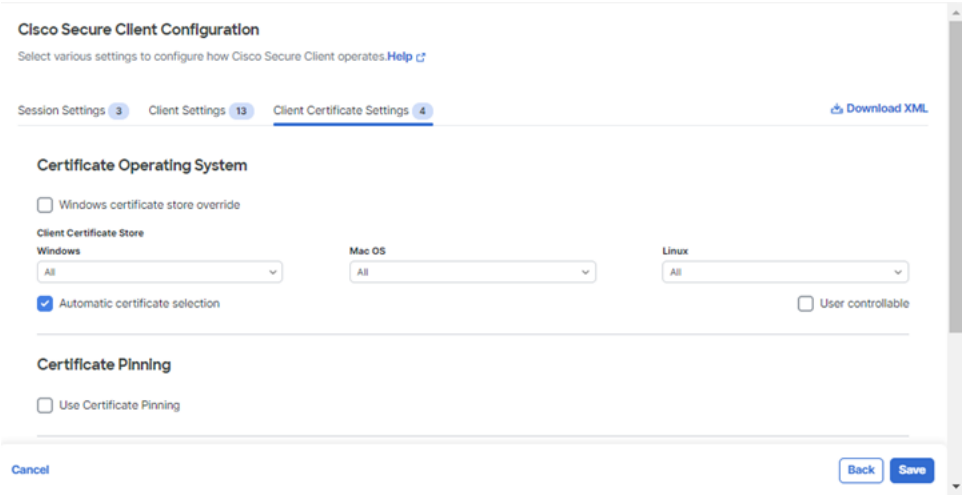


b. Modify **Administrative Settings** as needed.



c. Click **Save**.

3. Modify any **Client Certificate Settings** as needed.



4. Click **Save** to complete the VPN Profile.

Add a RADIUS Group

Provides instructions for adding a radius group. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

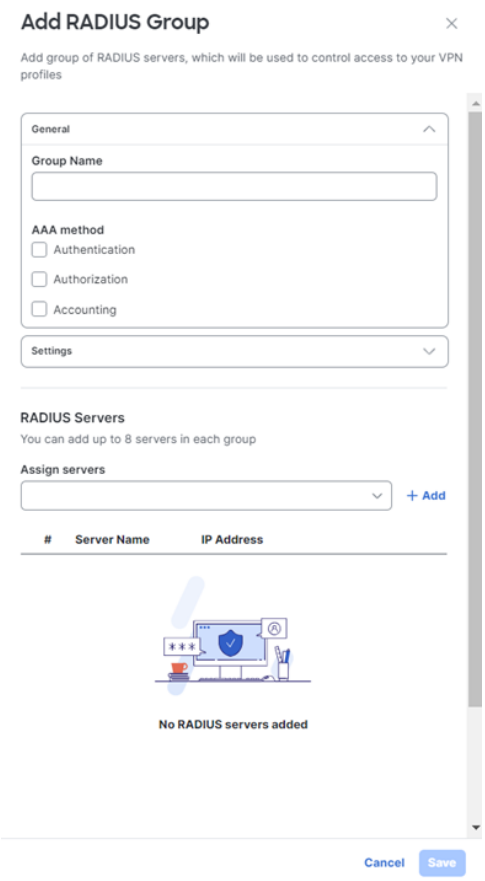
This section describes how to configure a RADIUS group and add servers to the group. This RADIUS group can be applied to the Authentication, Authorization, and Accounting (AAA) methods of a VPN profile configuration and mapped to other VPN profiles.

Before you begin

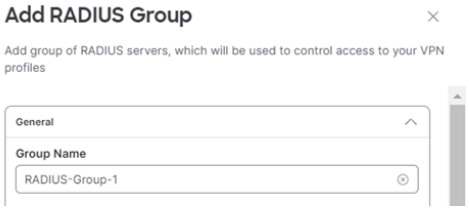
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **VPN Profiles**, click **Add**.
3. Complete **General settings** of the VPN Profile and click **Next**.
4. On the **Authentication, Authorization, and Accounting** page, expand the **Map authentication groups to regions** pane and click **+ Group**.



5. To configure the RADIUS group, enter a meaningful **Group Name**.



6. Choose the AAA methods to apply to this RADIUS Group. Choose at least one method.

> **Note**
>
> If both the **Authentication** and **Authorization** methods are selected, the same port number must be used.

   a. **Authentication**-Enter the RADIUS authentication **Port** number. The valid range is from 1 to 65535.

      The default is 1812.

      Check **Microsoft CHAPv2** to use Microsoft Challenge Handshake Authentication Protocol Version 2 as the authentication method.

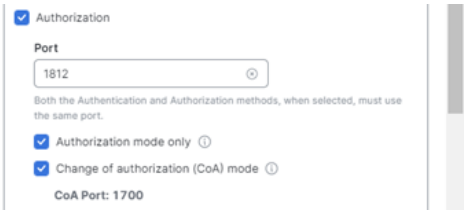


b. **Authorization**-Enter the RADIUS authorization **Port** number. The valid range is from 1 to 65535.

   The default is 1812.

   When you check **Authorization mode only**, no common password is required.

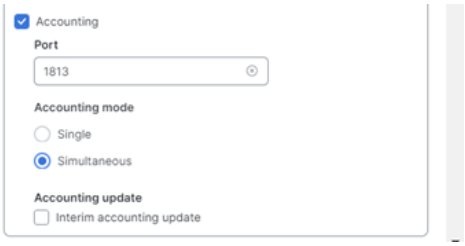
   When you check **Change of authorization (CoA) mode**, the RADIUS server group will be registered for CoA notification. If you enable CoA, the listening port for RADIUS CoA requests uses the default of 1700. Select this option when using this server group for ISE Policy Enforcement in remote access VPNs.



c. **Accounting**-Enter the RADIUS accounting **Port** number. The valid range is from 1 to 65535. The default is 1813.

   Select the **Accounting mode**, either **Single** or **Simultaneous**. In single mode, accounting data is sent to only one server. In simultaneous mode, accounting data to all servers in the group.

   For **Accounting update**, select **Interim accounting update** to enable the periodic generation of RADIUS interim-accounting-update messages.



7. Configure the method (**Reactivation mode**) by which failed servers in a group are reactivated:

   a. Set the **Max failed attempts** to specify the maximum number of failed AAA transactions with a RADIUS server in the group before trying the next server. The range is from 1 and 5. The default is 3.

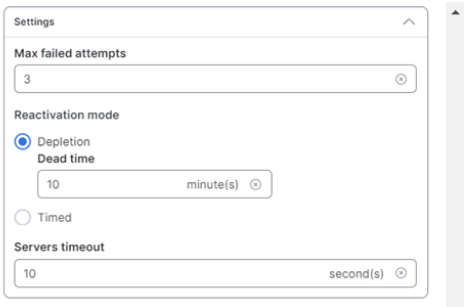
   b. Choose **Depletion, Dead time** to reactivate failed servers only after all of the servers in the group are inactive.

      This is the default reactivation mode. Specify the amount of time, between 0 and 1440 minutes, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers.

      Deadtime applies only if you configure fallback to the local database; authentication is attempted locally until the deadtime elapses. The default is 10 minutes.

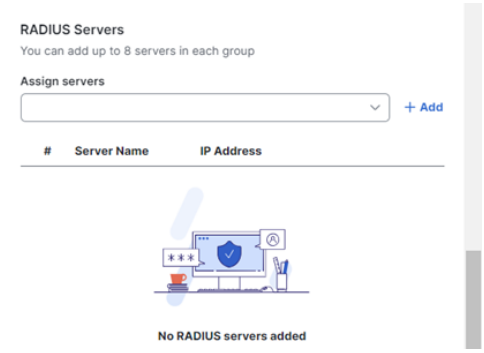
   c. Choose **Timed** to reactivate failed servers after 30 seconds of down time.

   d. Set the **Servers timeout** setting. Enter the number of seconds to wait for a response from a RADIUS server (in seconds). The default is 10 seconds.

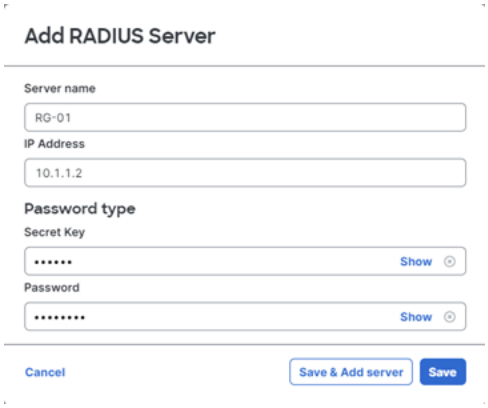


8. Scroll down to **RADIUS Servers** and click **Add**.

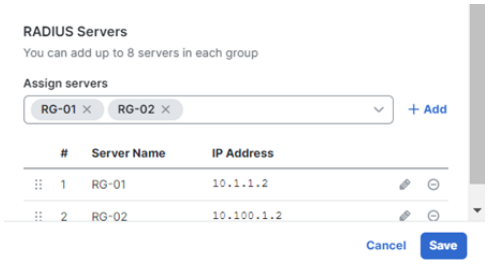
   You can add up to eight servers to each RADIUS group.



9. Enter a meaningful **Server name**, an **IP Address**, and a **Secret Key/Password** combination and click **Save & Add server**.



10. Click **Save** when you are done adding servers to complete the RADIUS Group.



Manage IP Pools

Describes managing ip pools. Manage your organization's sets of IP address pools that are used to secure the request and response traffic of your remote access VPN profiles. An IP address pool is a sequential range of IP addresses within a certain network. You can have multiple pool configurations.

Manage your organization's sets of IP address pools that are used to secure the request and response traffic of your remote access VPN profiles. An IP address pool is a sequential range of IP addresses within a certain network. You can have multiple pool configurations.

VPN profiles require IP addressing pools in order to be fully-functional. In addition, control plane traffic such as RADIUS is sourced from the Secure Access IP address pools.

See the following topics for more information related to IP pools:

- Add an IP Pool
- Add a RADIUS Group (optional)

16 Traffic Steering for Zero Trust Access Client-Based Connections

Topics:

- Traffic Steering for Zero Trust Access Client-Based Connections

Describes the purpose and procedures for traffic steering for zero trust access client-based connections and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Traffic Steering for Zero Trust Access Client-Based Connections

Describes traffic steering for zero trust access client-based connections. Traffic steering entries on the End User Connectivity > Zero Trust page apply only to client-based zero-trust access connections to internal destinations that are configured as private resources.

Traffic steering entries on the End User Connectivity > Zero Trust page apply only to client-based zero-trust access connections to internal destinations that are configured as private resources.

When you configure a Private Resource, Secure Access automatically adds an entry for each configured resource address for client-based zero-trust access to the Traffic Steering page, in order to direct end-user traffic to the resource.

You can view traffic steering rules, but in most cases you should not edit rules on this page. See Best Practices, below.

Important

Note about editing traffic steering entries

If you edit entries that were automatically added to this page when you configured a Private Resource, the traffic steering rules for the resource are NOT updated when you make future edits to the Private Resource configuration page.

Best Practices

Describes best practices. You should not add destinations directly to the zero-trust traffic steering page. Instead, add a Private Resource. See Add a Private Resource.

- You should not add destinations directly to the zero-trust traffic steering page. Instead, add a Private Resource. See Add a Private Resource.
- You should not edit entries on the zero-trust traffic steering page, except for the following purpose:

  Edit entries on the zero trust traffic steering page if you have configured the access address for a Private Resource as a wildcard FQDN of the format **.example.com* and you want to exclude specified subdomains from client-based zero-trust access.

  For instructions, see Using Wildcards to Configure Traffic Steering for Private Destinations.
- The number of destinations on the traffic steering page is limited. See Limitations and Range Limits.

Using Wildcards to Configure Traffic Steering for Private Destinations

Provides instructions for using wildcards to configure traffic steering for private destinations. When you configure a Private Resource, Secure Access automatically adds an entry for each configured resource address for client-based zero-trust access to the Traffic Steering page, in order to direct end-user traffic to the resource.

For more granular control over zero trust access to private resources, and to reduce the number of individual private destinations on the Zero Trust Traffic Steering page, consider using wildcards to configure these destinations.**Important**

Note about editing traffic steering entries

When you configure a Private Resource, Secure Access automatically adds an entry for each configured resource address for client-based zero-trust access to the Traffic Steering page, in order to direct end-user traffic to the resource.

If you edit entries that were automatically added to the Zero Trust Traffic Steering page when you configured a Private Resource, the traffic steering rules for the resource are NOT updated when you make future edits to the Private Resource configuration page.

- Full Admin user role. For more information, see Manage Accounts.
- Before using this procedure, see important caveats at Traffic Steering for Zero Trust Client-Based Connections.
- The private resource address to edit must be configured as a wildcard FQDN.

To exclude traffic from a configured Private Resource address:

Before you begin

Procedure

1. Navigate to **Connect** > **End User Connectivity**.
2. Click the **Zero Trust** tab.
3. For the resource to modify, click the ellipsis button at the end of the table row and choose **Edit**.
4. Provide subdomains to exclude from traffic steering for Zero Trust connections. For example, if your domain is **.example.com*, and you want to exclude traffic to *hr.example.com* and *boo.finance.example.com*, enter **hr** as an exclusion, then click **Add** and enter **boo.finance**.
5. Click **Save**.

17 Manage Internet Security

Topics:

- Manage Internet Security

Describes the purpose and procedures for manage internet security and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Internet Security

Describes managing internet security. You can configure DNS and web security in Cisco Secure Access for end users. User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file.

You can configure DNS and web security in Cisco Secure Access for end users. User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file.

Prerequisites

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

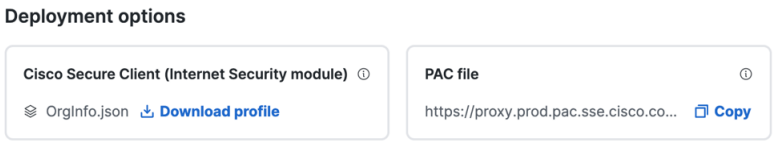
Before you begin, navigate to **Connect** > **End User Connectivity** > **Internet Security**.

Visibility of User Identities in Policy Rules

- Deploy the Secure Access Active Directory (AD) Connector. For more information, see Connect Active Directory to Secure Access.
- Provision users and groups in Secure Access. For more information, see Provision Users and Groups from Active Directory.

Copy the PAC file URL

1. Copy the Secure Access PAC File URL. For more information about PAC files, see Manage PAC Files.



Download the OrgInfo.json File

1. Download the Secure Access OrgInfo.json file to the user devices where you have deployed the Cisco Secure Client. For more information, see Download the OrgInfo.json File.

Manage Internet Security Bypass

Describes managing internet security bypass. You can configure Internet Security Bypass for web requests to destinations from end users in your organization. In Secure Access, add IP addresses, CIDR blocks, or domains for Internet Security Bypass.

You can configure Internet Security Bypass for web requests to destinations from end users in your organization. In Secure Access, add IP addresses, CIDR blocks, or domains for Internet Security Bypass.

Secure Access supports Internet Security Bypass for user devices with the Cisco Secure Client (formerly known as AnyConnect) and Umbrella Roaming Security module, or user devices with browsers that are configured with the Secure Access PAC file or a custom PAC file.

About Internet Security Bypass

Add destinations for Internet Security Bypass in Secure Access to either bypass the Secure Access DNS resolvers and Secure Web Gateway, or bypass the Secure Web Gateway only.

To bypass the Secure Access DNS resolvers and Secure Web Gateway, add the domains that are local to your organization or domains that should route to your organization's DNS resolvers only and not route to the Secure Access DNS servers.

Your local DNS servers will resolve the DNS requests that are sent from end users in the organization. DNS requests for the destinations do not route to the Secure Access DNS servers and Secure Web Gateway.

To bypass the Secure Access Secure Web Gateway only, add destinations for trusted applications, applications that are not reachable through web proxies, or applications that end users can access only from specific public IP addresses. If you bypass the Secure Web Gateway only, the DNS requests from end users will be resolved by the Secure Access DNS servers.

Steer Traffic to Secure Access or Bypass Domains

Provides instructions for steer traffic to secure access or bypass domains. Add domains to your list of bypass domains. The domain names in the bypass domain list should not route to the Cisco Secure Access DNS resolvers, but instead route to your internal DNS servers.

Procedure

Add domains to your list of bypass domains. The domain names in the bypass domain list should not route to the Cisco Secure Access DNS resolvers, but instead route to your internal DNS servers. For more information, see Manage Domains.



Manage Cisco Secure Client Settings

Describes managing cisco secure client settings. You can configure settings for devices that have the Cisco Secure Client deployed with the Umbrella Roaming Security module.

You can configure settings for devices that have the Cisco Secure Client deployed with the Umbrella Roaming Security module.

- Configure DNS and Web Security

Configure DNS and Web Security

Provides instructions for configuring dns and web security. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

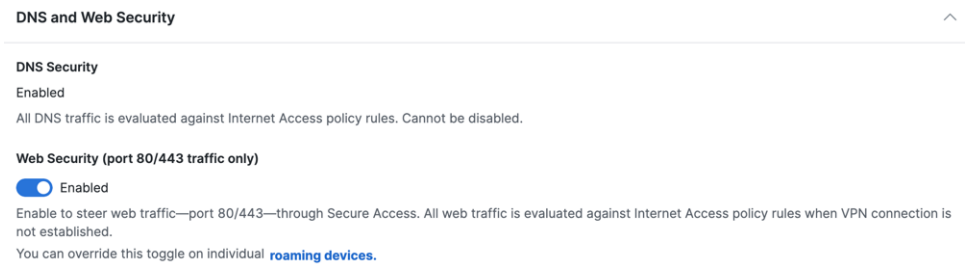
Configure DNS and Web security settings for the Cisco Secure Client.

Procedure

For **Cisco Secure Client Settings**, enable the **Web Security (port 80/443 traffic only)** toggle button.

What to do next

> **Note**
>
> The Secure Access DNS-layer security is always enabled on the Cisco Secure Client.



18 Manage PAC Files

Topics:

- Manage PAC Files

Describes the purpose and procedures for manage pac files and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage PAC Files

Describes managing pac files. When configuring Cisco Secure Access Internet Security, you have several choices as to how you can send web traffic to Secure Access. One of those choices is to integrate a proxy auto-config (PAC) file URL for the browsers that you use to reach web resources.

When configuring Cisco Secure Access Internet Security, you have several choices as to how you can send web traffic to Secure Access. One of those choices is to integrate a proxy auto-config (PAC) file URL for the browsers that you use to reach web resources.

After you integrate a PAC file on a device, all traffic through the browser is redirected to the Secure Access secure web gateway (SWG). For a PAC file deployment on a device, Secure Access DNS-layer security is not enforced on traffic generated on the browser. Secure Access DNS-layer security applies only to browser traffic to non-web resources, which bypasses the PAC file.

What is a PAC file?

Describes what is a pac file?. A proxy auto-config (PAC) file is used by browsers to select the correct proxy server that can fetch a requested URL.

A proxy auto-config (PAC) file is used by browsers to select the correct proxy server that can fetch a requested URL.

Known Limitations

As an administrator, you can download and deploy the Secure Access PAC file only if you are on a network that has been added as a Registered Network to Secure Access. PAC files are not supported for other connection mechanisms.

Recommendations

For the most part, integrating the Secure Access PAC file into your system so that all browser-based traffic is proxied is straightforward. However, you may have to customize the PAC file before integrating it into your system.

> **Note**
>
> Microsoft has deprecated PAC file support for the file:// and ftp:// protocols in Windows 10 on Edge. Hosting the PAC file on the local machine will not work on this browser. For more information, see Windows 10 does not read a PAC file referenced by a file protocol.

- ocsp.int-x3.letsencrypt.org
- isrg.trustid.ocsp.identrust.com
- *.cisco.com
- *.opendns.com
- *.secureaccessfed.cisco
- *.umbrellagov.com
- *.okta.com
- *.oktacdn.com
- *.pingidentity.com
- secure.aadcdn.microsoftonline-p.com

Deploy the Secure Access PAC File for Windows

Describes deploying the secure access pac file for windows. The Cisco Secure Access secure web gateway (SWG) requires that you deploy a proxy auto-config (PAC) file URL on a browser to successfully reach web resources.

The Cisco Secure Access secure web gateway (SWG) requires that you deploy a proxy auto-config (PAC) file URL on a browser to successfully reach web resources. If you're behind a firewall, you may also need to deploy the Secure Access's PAC file on the browser so that it points to the correct proxy server. A PAC file is only used with Secure Access Internet Security.

After an organization's administrator adds internal domains in Secure Access, the Secure Access PAC file contains the list of configured internal domains. Web traffic to internal domains is not sent to the SWG. For more information about internal domains, see Manage Domains.

Procedure for Deploy the Secure Access PAC File for Windows

Describes procedure for deploy the secure access pac file for windows. Full Admin user role. For more information, see Manage Accounts.

> **Note**
>
> We have attempted to provide you with the latest information about how to configure your operating system (OS) and browsers to use Secure Access's PAC file. However, as OS and browser functionality can change at any time, we cannot guarantee that these third-party procedures will remain accurate. For more information on deploying a PAC file URL to your browser, see your OS and browser's Help.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- To download and use the Secure Access PAC file, add your network's egress IP to Secure Access as a Registered Network. Secure Access only allows the PAC file to download from a trusted network. PAC files are not supported for other connection mechanisms. For more information, see Manage Registered Networks.

Copy the Secure Access PAC File URL

Provides instructions for copy the secure access pac file url. Navigate to Connect End User Connectivity Internet Security . Copy the Secure Access PAC file URL and save to your system.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. Copy the Secure Access PAC file URL and save to your system.

Deploy the Secure Access PAC File URL for Chrome and Edge Browsers

Provides instructions for deploying the Secure Access PAC file url for Chrome and Edge browsers.

Procedure

1. In Windows, navigate to **Start** > **Settings** > **Network & internet** > **Proxy**.
2. For **Automatic proxy setup**, click **Set up**.
3. Set **Use setup script** to **On**.

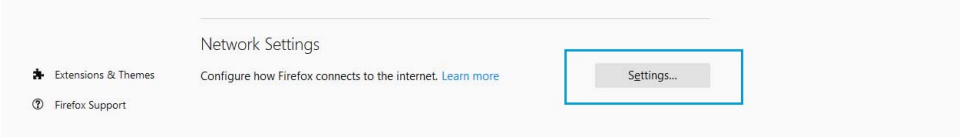
4. For **Script Address**, paste the Secure Access PAC file URL.
5. Click **Save**.

Deploy the Secure Access PAC File URL for Firefox

Provides instructions for deploying the secure access pac file url for firefox. In Firefox, navigate to Settings, scroll to Network Settings, and then click Settings.

Procedure

1. In Firefox, navigate to **Settings**, scroll to **Network Settings**, and then click **Settings**.



2. Select **Automatic Proxy Configuration URL** and paste the Secure Access PAC file URL.
3. Click **OK**.

Deploy the Secure Access PAC File for macOS

Describes deploying the secure access pac file for macos. The Cisco Secure Access secure web gateway (SWG) requires that you deploy a proxy auto-config (PAC) file URL on a browser to successfully reach web resources.

The Cisco Secure Access secure web gateway (SWG) requires that you deploy a proxy auto-config (PAC) file URL on a browser to successfully reach web resources. If you're behind a firewall, you may also need to deploy the Secure Access's PAC file on the browser so that it points to the correct proxy server. A PAC file is only used with Secure Access Internet Security.

After an organization's administrator adds internal domains in Secure Access, the Secure Access PAC file contains the list of configured internal domains. Web traffic to internal domains is not sent to the SWG. For more information about internal domains, see Manage Domains.

Procedure for Deploy the Secure Access PAC File for macOS

Describes procedure for deploy the secure access pac file for macos. Full Admin user role. For more information, see Manage Accounts.

> **Note**
>
> We have attempted to provide you with the latest information about how to configure your operating system (OS) and browsers to use Secure Access's PAC file. However, as OS and browser functionality can change at any time, we cannot guarantee that these third-party procedures will remain accurate. For more information on deploying a PAC file URL to your browser, see your OS and browser's Help.

- Full Admin user role. For more information, see Manage Accounts.
- To download and use the Secure Access PAC file, add your network's egress IP to Secure Access as a Registered Network. Secure Access only allows the PAC file to download from a trusted network. PAC files are not supported for other connection mechanisms. For more information, see Manage Registered Networks.

Copy the Secure Access PAC File URL

Provides instructions for copy the secure access pac file url. Navigate to Connect End User Connectivity Internet Security . Copy the Secure Access PAC file URL and save to your system.

Procedure

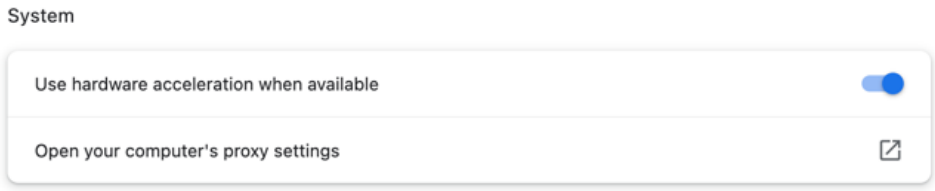
1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. Copy the Secure Access PAC file URL and save to your system.

Deploy the Secure Access PAC File URL to Chrome

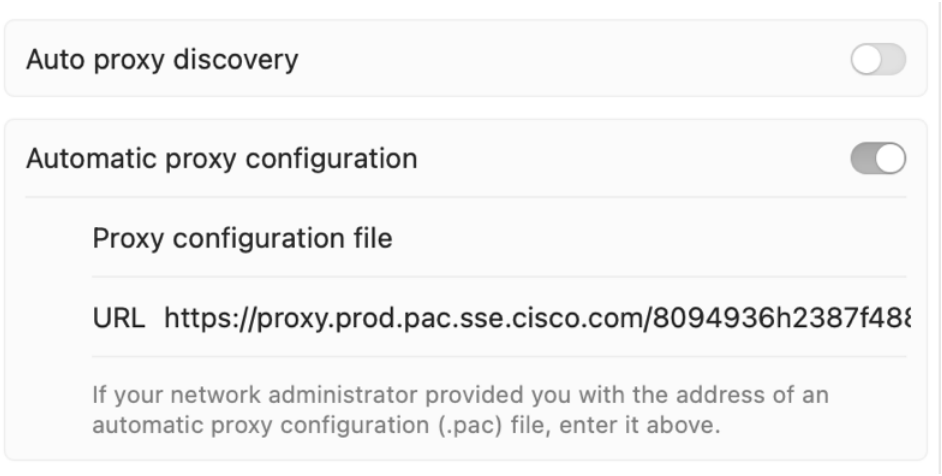
Provides instructions for deploying the secure access pac file url to chrome. In your Chrome browser, navigate to chrome://settings/system and click Open your computer's proxy settings.

Procedure

1. In your Chrome browser, navigate to **chrome://settings/system** and click **Open your computer's proxy settings**.



2. Enable **Automatic proxy configuration** and paste the Secure Access PAC file URL.



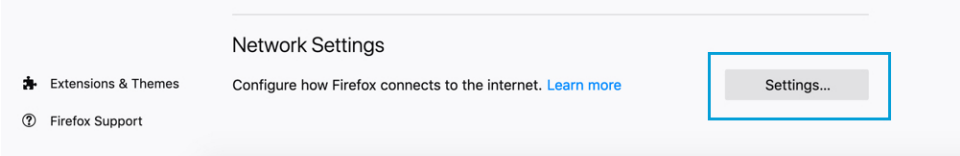
3. Click **OK** and then **Apply**.

Deploy the Secure Access PAC File URL to Firefox

Provides instructions for deploying the secure access pac file url to firefox. Open your Firefox browser, navigate to Firefox Preferences , scroll to Network Settings, and click Settings.

Procedure

1. Open your Firefox browser, navigate to **Firefox** > **Preferences**, scroll to **Network Settings**, and click **Settings**.



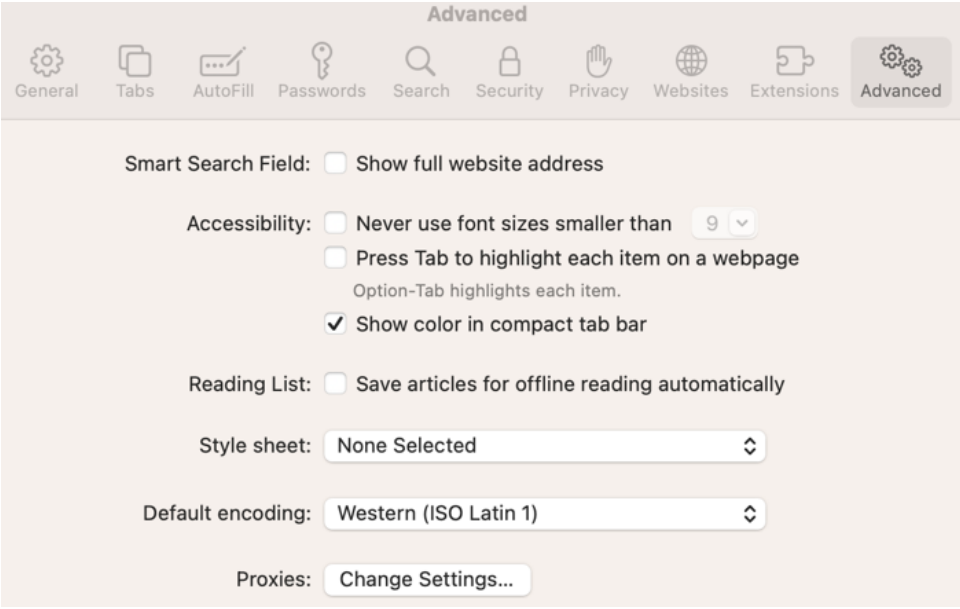
2. Check **Automatic Proxy Configuration URL** and paste the Secure Access PAC file URL.
3. Click **OK**.

Deploy the Secure Access PAC File URL to Safari

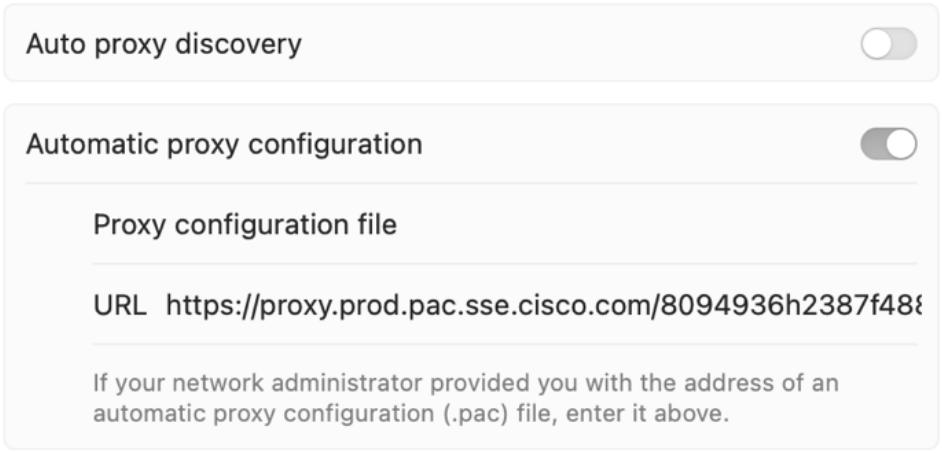
Provides instructions for deploying the secure access pac file url to safari. Open your Safari browser, navigate to Safari Settings Advanced , and then click Change Settings.

Procedure

1. Open your Safari browser, navigate to **Safari** > **Settings** > **Advanced**, and then click **Change Settings**.



2. Enable **Automatic proxy configuration** and paste the Secure Access PAC file URL.



3. Click **OK** and then **Apply**.

Customize the Secure Access PAC File

Describes customize the secure access pac file. After an organization's administrator adds internal domains in Cisco Secure Access, the Secure Access PAC file contains the list of configured internal domains. Web traffic to internal domains is not sent to the secure web gateway (SWG).

After an organization's administrator adds internal domains in Cisco Secure Access, the Secure Access PAC file contains the list of configured internal domains. Web traffic to internal domains is not sent to the secure web gateway (SWG). For more information about internal domains, see Manage Domains.

To bypass additional internal domains on the SWG, you can customize the Secure Access PAC file. Using the Secure Access PAC File URL, download and edit the PAC File, and then add any other internal domains to the PAC File.

If you require any manual editing of the PAC file, you must host the PAC file on a web server in your own environment. For more information about hosting a PAC file, see your web server's documentation.

Secure Access supports IP-based domains. However, you must enter the IP in the browser's address bar as the domain portion of the URL. For example, `https://1.2.3.4/URLpath/`. The PAC file does not resolve a domain to IP before matching an IP-based domain for bypass.

Procedure for Customize the Secure Access PAC File

Describes procedure for customize the secure access pac file. Copy the Secure Access PAC File URL, and then download and edit the PAC File.

Copy the Secure Access PAC File URL, and then download and edit the PAC File.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- To download the Secure Access PAC file, add your network's egress IP to Secure Access as a Registered Network. Secure Access only allows the PAC file to download from a trusted network. For more information, see Manage Registered Networks.

Copy the Secure Access PAC File

Provides instructions for copy the secure access pac file. Navigate to Connect End User Connectivity Internet Security . Copy the Secure Access PAC file URL.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. Copy the Secure Access PAC file URL.

Download the Secure Access PAC File

Provides instructions for downloading the secure access pac file. Paste the copied PAC URL into a browser's address bar and then press Enter or Return to download the PAC file.

Procedure

Paste the copied PAC URL into a browser's address bar and then press **Enter** or **Return** to download the PAC file.

What to do next

Edit the PAC File

Provides instructions for editing the pac file. Open the downloaded PAC file with a text editor. Add the internal domains that should should be bypassed, and then save the PAC file.

Procedure

1. Open the downloaded PAC file with a text editor.
2. Add the internal domains that should should be bypassed, and then save the PAC file.

> **Note**
>
> Provide a comma-delimited list of domain name and surround each domain name in the list with quotation marks. The wildcard character asterisk ***** is supported and treated as any value of any length. Use extreme caution when using this wildcard as well as periods. For example, ***.example.com** bypasses www.example.com, **mail.example.com**, and **c.23.example.com**. ***example.com** bypasses www.example.com as well as **phishingexample.com**.

What to do next

```
//-----------------------Customer Section-----------------------
    //Add your internal domains within quotations marks like "wwwin.acme.com"

    //after the right parenthesis below. Please remove the two examples
    //below and add your own internal domains.

    var dont_proxy_customer_list = new Array(
        "wwwin.example.org",
        "*.example.org"
    );

    //Warning to Administrators: Touching any section after this point might
    //affect your users browsing experience and lead to considerable number
    //of issues and loading your customer support.
    //---------------------End Customer Section----------------------
```

19 Manage Registered Networks

Topics:

- Add Network Resources
- Point Your DNS to Cisco Secure Access
- Clear Your DNS Cache
- Update a Network Resource
- Delete a Network Resource

Introduces managing registered networks. A resource is an internet capable entity that is managed by your organization. After you add a resource to Cisco Secure Access, your resource is protected against threats and attacks through security configurations defined in policy rules.

A resource is an internet capable entity that is managed by your organization. After you add a resource to Cisco Secure Access, your resource is protected against threats and attacks through security configurations defined in policy rules. Secure Access can support high-level entities within your organization–for example, registered or internal networks –or very granular entities–for example, a single user logged into Microsoft o365. For more information about policy rules, see Manage the Access Policy.

A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access supports both static and dynamic IPv4 addresses. In Secure Access, all traffic originating from the public IP space is identified as coming from that network. The public IP space or IP range defines the scope of the network resource.

To start protecting the networks in your organization, see Add Network Resources.

Add Network Resources

Describes adding network resources. A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access supports both static and dynamic IPv4 addresses.

A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access supports both static and dynamic IPv4 addresses. In Secure Access, all traffic originating from the public IP space is identified as coming from that network. The public IP space or IP range defines the scope of the network resource.

To start protecting your public networks managed by your organization, add network resources to Secure Access. Once you've configured and added a network resource, build policy rules to extend Secure Access's protection to any device that connects to the internet from behind that network. For more information about Secure Access policy rules, see Manage the Access Policy.

> **Note**
>
> The Secure Access policy supports the use of PAC files with a public static network. For more information about PAC files, see Manage PAC Files.

Prerequisites for Add Network Resource

Describes prerequisites for add network resource. Full Admin user role. For more information, see Manage Accounts. Your network's IP address is unique within Secure Access.

- Full Admin user role. For more information, see Manage Accounts.
- Your network's IP address is unique within Secure Access.
- Determine if you have a dynamic IP address. For more information, see Dynamic IP Address–IPv4 Only.

Dynamic IP Address—IPv4 Only

Secure Access supports dynamic IP addresses only over IPv4. Most home, small school, and small business networks are provisioned typically by Internet Service Providers (ISPs) with a dynamic IP address (IPv4) when defining each unique internet network.

If you have a dynamic IP address, the public IP of your network changes over time when the lease for that IP address changes. An internet service provider (ISP) provides a dynamic IP address to your device temporarily. Your IP may stay the same for some time period, but the lease eventually expires and is given to another customer of your ISP. When your IP address registered with Secure Access changes, Secure Access's security settings no longer apply. These settings no longer match your account information and you must update the network resource's IP.

To automatically maintain the IPv4 dynamic IP address of your network resource, install the Cisco Dynamic IP Updater on at least one computer within the network. Once installed, the device registers the network information with the Cisco Dynamic IP Updater. The Cisco Dynamic IP Updater automates the discovery and registration of a network's IP address to your Secure Access account whenever the dynamic IP address changes. If you do not register your IPv4 dynamic IP address through the Cisco Dynamic IP Updater, you must manually reenter your IP address each time it changes.

> **Note**
>
> Most Dynamic DNS (DDNS) clients work toward keeping your network updated. Secure Access does not support third-party DDNS clients.

Download the Cisco Dynamic IP Updater

Download the Cisco Dynamic IP Updater for your system.

- Windows Dynamic IP Updater
- Mac Dynamic IP Updater

Install the Cisco Dynamic IP Updater

Install the Cisco Dynamic IP Updater on one of the devices on your dynamic IP network.

- Ensure that the device where you install the Cisco Dynamic IP Updater is stationary to the network and not a laptop (only used in the network on which you are configuring Secure Access).
- Ensure that the device is always powered on or turned on before any other devices sign on to the network.

Procedure for Add Network Resource

Describes procedure for add network resource. Add a network resource where the network has a public static IP address or IP address range, or a dynamic IP address.

Add a network resource where the network has a public static IP address or IP address range, or a dynamic IP address.

> **Note**
>
> We recommend that you register all of your organization's networks with Secure Access at the same time. Pre-registering networks ensures that all IP spaces that belong to your organization are added to Secure Access. If you have more than one public egress IP in your organization, configure a network resource for each IP address. You must point your network's DNS to the Secure Access DNS global resolvers. Until your DNS traffic is connected to the Secure Access DNS resolvers, your networks are not protected and traffic is not logged in the Activity Search report.

- Step 1 – Select the Network
- Step 2 – Configure the Network Resource
- Step 3 – Change the DNS Settings on Your Relevant Network Device
- Step 4 – Apply a Policy Rule to the Network Resource
- Step 5 – Test Your Network

Step 1 – Select the Network

Provides instructions for step 1 – select the network. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

First, determine the IP address of your network.

Procedure

1. Go to http://www.whatismyip.com.
   Your IPv4 addresses and location are displayed.
2. In Secure Access, navigate to **Resources** > **Registered Networks**.
   The public IP address of your network is listed at the top of the page.

What to do next

Note

Depending on your package, if you attempt to add a network other than the one currently being used to access Secure Access, Secure Access may prompt you to contact Support for manual verification. If this occurs, you'll also need manual verification from Support for IPv4 ranges larger than a /29 network.

Verification cases are created automatically and you'll receive an update as soon as it's reviewed. For more information about your current package, see Determine Your Current Package.

Step 2 – Configure the Network Resource

Provides instructions for step 2 – configure the network resource. Its purpose, requirements, and key details for Cisco Secure Access administrators.

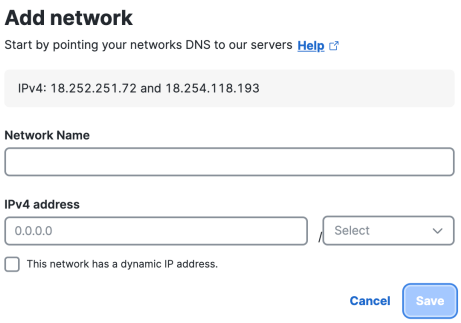
Before you begin, determine if you have an IPv4 dynamic IP address. Secure Access only supports dynamic IP addresses for IPv4. Most home, small school, and small business networks are provisioned typically by Internet Service Providers (ISPs) with a dynamic IP address (IPv4) when defining each unique internet network.

Note

If possible, add the network resource from the IP address used to sign into Secure Access. Otherwise, Secure Access sends an email to the user account and requires that you visit a link from the IP address of the network that you are registering.

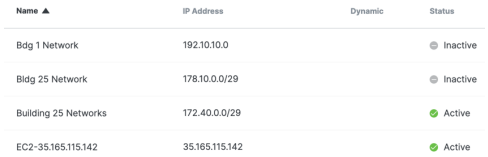
Procedure

1. Navigate to **Resources** > **Registered Networks** and click **Add Network**.
2. Give your network resource a descriptive **Network Name**.



3. Choose an internet protocol: **IPv4**.
4. Add the network's IP address and choose a subnet mask.
5. For IPv4 only, if you have a dynamic IP address, check **This network has a dynamic IP address**.
6. Click **Save**.

   Once Secure Access validates your IP address, the network resource is listed at **Resources** > **Registered Networks**. Initially, Secure Access lists the status of your network as **Inactive**. When Secure Access receives DNS traffic from the network, the network resource's status changes to **Active**.



Name ▲	IP Address	Dynamic	Status
Bdg 1 Network	192.10.10.0		Inactive
Bldg 25 Network	178.10.0.0/29		Inactive
Building 25 Networks	172.40.0.0/29		Active
EC2-35.165.115.142	35.165.115.142		Active

Step 3 – Change the DNS Settings on Your Relevant Network Device

Describes step 3 – change the dns settings on your relevant network device. You only need to change the DNS settings on your edge DNS equipment, typically a DNS or DHCP server, or a router–a DSL router or cable modem if that's the only router in your network.

You only need to change the DNS settings on your edge DNS equipment, typically a DNS or DHCP server, or a router–a DSL router or cable modem if that's the only router in your network. For information about how to configure devices including laptops or routers, see Point Your DNS to Cisco Secure Access.

> **Note**
>
> The device where you test the network must have retrieved a new set of DNS servers from the DNS/DHCP server or router, or you must change the device's DNS settings manually before verifying the configuration of the network resource.

Step 4 – Apply a Policy Rule to the Network Resource

Describes step 4 – apply a policy rule to the network resource. Add the network resource to an existing Secure Access policy rule or create a new policy rule and apply the rule to the network resource.

Add the network resource to an existing Secure Access policy rule or create a new policy rule and apply the rule to the network resource. If you do not add the network resource to a policy rule, Secure Access applies the Default policy rule to protect the network resource.

Step 5 – Test Your Network

Describes step 5 – test your network. Verify that your network's DNS connections are routed through Cisco Secure Access's global network.You may need to restart your client's network interface or your device.

Verify that your network's DNS connections are routed through Cisco Secure Access's global network.

> **Note**
>
> You may need to restart your client's network interface or your device.

Point Your DNS to Cisco Secure Access

Describes point your dns to cisco secure access. Configure your DNS to direct traffic from your network to the Cisco Secure Access DNS resolvers in the AWS GovCloud region.

Configure your DNS to direct traffic from your network to the Cisco Secure Access DNS resolvers in the AWS GovCloud region. When a request to resolve a hostname on the internet is made from a network pointed at our DNS addresses, Secure Access applies the security settings configured in your policy rules.

To have Secure Access protect your networks, you need to explicitly change the DNS settings in your operating system or hardware firewall or router to Secure Access's name server IP addresses and turn off the automatic DNS servers provided by your ISP.

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

Cisco Secure Access DNS Resolvers – IP addresses

Describes cisco secure access dns resolvers – ip addresses. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

IPv4	Description
18.252.251.72	Primary
18.254.118.193	Secondary

Procedure for Point Your DNS to Cisco Secure Access

Describes procedure for point your dns to cisco secure access. Change the DNS server addresses to Cisco Secure Access DNS server addresses.

Change the DNS server addresses to Cisco Secure Access DNS server addresses.

- Step 1 – Identify Where Your Public DNS Server Addresses Are Configured
- Step 2 – Log Into the Server or Router Where DNS is Configured
- Step 3 – Change Your DNS Server Addresses
- Step 4 – Test Your New DNS Settings

Prerequisites

- Administrative privileges on the device or server where the DNS is configured.

Note

We recommend that only users who have administrative access to the router, DNS server, or their own computer attempt to use these instructions as you need this level of access to complete these steps.

Step 1 – Identify Where Your Public DNS Server Addresses are Configured

Describes step 1 – identify where your public dns server addresses are configured. Determine which device or server on your network maintains the addresses of your public DNS servers–most often a router or DNS server.

Determine which device or server on your network maintains the addresses of your public DNS servers–most often a router or DNS server. Typically, the device that provides an internal non-routable IP address (DHCP) or the device that serves as your default gateway is also where you configure public DNS servers.

Step 2 – Log Into the Server or Router Where DNS is Configured

Provides instructions for step 2 – log into the server or router where dns is configured. Log into the server or router where the DNS settings are configured.

Procedure

1. Log into the server or router where the DNS settings are configured.
2. Locate the DNS settings for this device. If you are unsure of where these settings are and require guidance on configuring a server or router, see Step 3 – Change Your DNS Server Addresses.

Step 3 – Change Your DNS Server Addresses

Provides instructions for step 3 – change your dns server addresses. Some ISPs hard-code their DNS servers into the equipment they provide. If you are using such a device, you can not configure it to use Secure Access.

Before you change your DNS settings to use Secure Access, record the current DNS server addresses or settings (for example, write them down on a piece of paper). Retain a copy of these DNS settings in case you need to revert to them at a later date.

Some ISPs hard-code their DNS servers into the equipment they provide. If you are using such a device, you can not configure it to use Secure Access. Instead, you can configure each of your computers by installing the Cisco Secure Client or configuring the DNS server addresses on each computer. For more information about configuring a Windows, macOS, or Linux computer, see Computer Configuration.

The process for changing your DNS settings varies according to the operating system and version (Windows, Mac, or Linux) or the device (DNS server, router, or mobile device). This procedure might not apply to your OS, router, or device. For authoritative information, see the vendor documentation.

To change your settings on a typical router:

Procedure

1. In your browser, enter the IP address to access the router's user interface and enter your password.
2. Find the area of configuration in which DNS server settings are specified and replace those addresses with the Cisco Secure Access IP addresses.

IPv4
18.252.251.72

IPv4
18.254.118.193

3. Save your changes and exit your router's user interface.
4. Flush your DNS cache.
5. Confirm that your DNS is set as static.
6. Test that your setup is working correctly. See Step 4 – Test Your New DNS Settings.

What to do next

Tip

When you make changes to DNS, you may have cached results that affect service. Flush your DNS cache to ensure that you're receiving only the latest DNS results. For information on how to flush your DNS cache, see Clear Your DNS Cache.

Note

Email servers have unique DNS configurations. We don't recommend that you configure your email servers to point to Secure Access DNS.

Step 4 – Test Your New DNS Settings

Describes step 4 – test your new dns settings. If you have trouble getting web pages to load, contact Cisco Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

If you have trouble getting web pages to load, contact Cisco Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Clear Your DNS Cache

Describes clear your dns cache. After you configure your DNS to direct traffic from your network to the Cisco Secure Access global DNS resolvers, you may need to clear the DNS cache on your computers, servers, and browsers in your organization.

After you configure your DNS to direct traffic from your network to the Cisco Secure Access global DNS resolvers, you may need to clear the DNS cache on your computers, servers, and browsers in your organization.

Prerequisites

- Administrative privileges on the device or server where the DNS is configured and user devices in the organization running browsers.

Clear Your DNS Cache on Computers and Servers

Describes clear your dns cache on computers and servers. Choose the operating system version of the devices in your organization and follow the steps to clear the DNS cache on the devices.

Choose the operating system version of the devices in your organization and follow the steps to clear the DNS cache on the devices.

Windows 7 and Earlier

Provides instructions for windows 7 and earlier. Click the Start Menu. Navigate to All Programs. Choose Accessories and right-click Command Prompt.

Procedure

1. Click the Start Menu.
2. Navigate to **All Programs**.
3. Choose **Accessories** and right-click **Command Prompt**.
4. Choose **Run as Administrator**.
5. Run the following command in the command line and press enter.

```
ipconfig /flushdns
```

Windows 8 and Newer

Provides instructions for windows 8 and newer. Press the Windows Key or hover over the bottom left corner, and then click the Windows icon.

Procedure

1. Press the Windows Key or hover over the bottom left corner, and then click the Windows icon.
2. Begin typing Command Prompt.
3. Right-click the application and select **Run as Administrator**.
4. Run the following command in the command line and press enter.

```
ipconfig /flushdns
```

OS X 10.4 TIGER

Provides instructions for os x 10.4 tiger. Click the Terminal icon in the dock or in Finder under Application/Utilities/Terminal.

Procedure

1. Click the **Terminal** icon in the dock or in Finder under `Application/Utilities/Terminal`.
2. Run the following command in the command line and hit enter.

```
lookupd -flushcache
```

OS X 10.5 and 10.6 LEOPARD

Provides instructions for os x 10.5 and 10.6 leopard. Click the Terminal icon in the dock or in Finder under Application/Utilities/Terminal.

Procedure

1. Click the **Terminal** icon in the dock or in Finder under `Application/Utilities/Terminal`.
2. Run the following command in the command line and press enter.

```
dscacheutil -flushcache
```

OS X 10.7 and 10.8 Lion

Provides instructions for os x 10.7 and 10.8 lion. Click the Terminal icon in the dock or in Finder under Application/Utilities/Terminal.

Procedure

1. Click the **Terminal** icon in the dock or in Finder under `Application/Utilities/Terminal`.
2. Run the following command in the command line and press enter.

```
sudo killall -HUP mDNSResponder
```

OS X 10.9 and 10.10

Provides instructions for os x 10.9 and 10.10. Click the Terminal icon in the dock or in Finder under Application/Utilities/Terminal.

Procedure

1. Click the Terminal icon in the dock or in Finder under `Application/Utilities/Terminal`.
2. Run the following command in the command line and press enter.

```
dscacheutil -flushcache;sudo killall -HUP mDNSResponder
```

Linux

Provides instructions for linux. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Procedure

1. Open a terminal window.
2. Run the following command in the command line and press enter.

```
sudo /etc/init.d/nscd restart
```

Ubuntu Linux

Provides instructions for ubuntu linux. Open a terminal window. Run the following command on the command line and press enter.

Procedure

1. Open a terminal window.
2. Run the following command on the command line and press enter.

```
sudo service network-manager restart
```

Clear Your DNS Cache on Browsers

Describes clear your dns cache on browsers. Choose the browser and operating system version of the devices in your organization and follow the steps to clear the DNS cache on the browsers.

Choose the browser and operating system version of the devices in your organization and follow the steps to clear the DNS cache on the browsers.

Internet Explorer 8 and Newer – Windows

Provides instructions for internet explorer 8 and newer – windows. Navigate to the History menu. Select Delete Browsing History. Check all boxes except passwords and then click Delete.

Procedure

1. Navigate to the **History** menu.
2. Select **Delete Browsing History**.
3. Check all boxes except passwords and then click **Delete**.

Mozilla Firefox – Windows

Provides instructions for mozilla firefox – windows. Click Firefox at the top left of your browser. Navigate to the History menu.

Procedure

1. Click Firefox at the top left of your browser.
2. Navigate to the **History** menu.
3. Select **Clear Recent History** and check all boxes.
4. Under **Time range to clear**, select all options except passwords, and then click **Clear Now**.

Apple Safari – macOS

Provides instructions for apple safari – macos. Expand the cog icon in the upper right corner. Select Reset Safari. Check all boxes and then click Reset.

Procedure

1. Expand the cog icon in the upper right corner.
2. Select **Reset Safari**.
3. Check all boxes and then click **Reset**.

Apple Safari – macOS

Provides instructions for apple safari – macos. Go to the Safari menu. Select Reset Safari. Check all boxes and then click Reset.

Procedure

1. Go to the Safari menu.
2. Select **Reset Safari**.
3. Check all boxes and then click **Reset**.

Google Chrome – Windows

Provides instructions for google chrome – windows. Expand the wrench icon in the upper right corner. Select History and check all boxes.

Procedure

1. Expand the wrench icon in the upper right corner.
2. Select **History** and check all boxes.
3. Select **Clear data for this time period**, and then choose all options except passwords.
4. Click **Clear Data**.

Google Chrome – macOS

Provides instructions for google chrome – macos. Navigate to the Chrome menu, and then select More Tools. Select Clear Browsing Data, and then choose all options except passwords.

Procedure

1. Navigate to the Chrome menu, and then select **More Tools**.
2. Select **Clear Browsing Data**, and then choose all options except passwords.
3. Click **Clear Data**.

Update a Network Resource

Provides instructions for updating a network resource. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

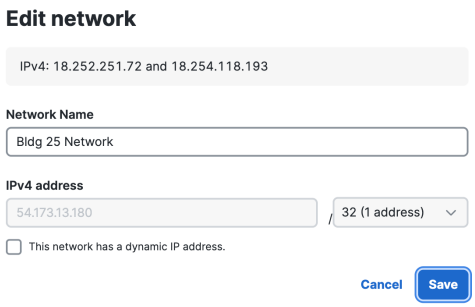
Once you add a Registered Network resource–a public static or dynamic IP network–to Cisco Secure Access, you can update the resource.

Before you begin

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

Procedure

1. Navigate to **Resources** > **Registered Networks**.
2. Click the ellipses (**...**) available in the same row as the network name you want to edit, and select **Edit**.



3. Edit the **Network Name** as needed.
4. If you have a dynamic IP address, check **This network has a dynamic IP address**.
5. Click **Save**.

Delete a Network Resource

Provides instructions for deleting a network resource. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Once you add a Registered Network resource–a public static or dynamic IP network–to Cisco Secure Access, you can remove the Network resource from Secure Access. After you delete a Network resource, you can no longer apply a policy rule to the resource and the network is not protected by Secure Access.

Before you begin

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

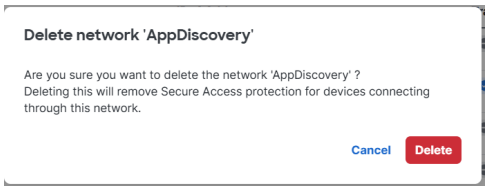
Procedure

1. Navigate to **Resources** > **Registered Networks**.
2. Hover over a network resource and click the three dots icon and then click **Delete**.



3. Click **Delete** to confirm.

The Network resource is deleted from Secure Access and is removed from any policy rules.



20 Manage Internal Networks

Topics:

- Add Internal Network Resources
- Update an Internal Network Resource
- Delete an Internal Network Resource

Introduces managing internal networks. A resource is an internet capable entity that is managed by your organization. After you add a resource to Cisco Secure Access, your resource is protected against threats and attacks through security configurations defined in policy rules.

A resource is an internet capable entity that is managed by your organization. After you add a resource to Cisco Secure Access, your resource is protected against threats and attacks through security configurations defined in policy rules. Secure Access can support high-level entities within your organization–for example, registered or internal networks –or very granular entities–for example, a single user logged into Microsoft o365. For more information about policy rules, see Manage the Access Policy.

An Internal Network resource represents a private address space of IP addresses. Internal networks are managed by your organization and are non-routable. Some examples of internal networks are: local area networks (LANs) found in branch or residential offices. Internal Network resources use networks or network tunnels to forward DNS traffic from your organization's internal network to Secure Access.

To start protecting the internal networks in your organization, see Add Internal Network Resources.

Add Internal Network Resources

Provides instructions for adding internal network resources. To start protecting an internal network, add an Internal Network resource to Cisco Secure Access. Once added, you can apply an existing policy rule to the internal network resource or add a new policy rule to protect the resource.

An Internal Network resource represents a private address space of IP addresses. Internal networks are managed by your organization and are non-routable or RFC1918 compliant. You must configure an Internal Network resource with either a Network or Network Tunnel resource. The associated network or network tunnel forwards DNS traffic from devices on your organization's internal network to Secure Access.

To start protecting an internal network, add an Internal Network resource to Cisco Secure Access. Once added, you can apply an existing policy rule to the internal network resource or add a new policy rule to protect the resource. Build policy rules to extend Secure Access's protection to any device that connects to the internet from behind the internal network. For more information about Secure Access policy rules, see Manage the Access Policy.

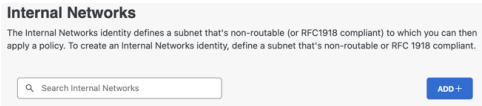
In Secure Access, all traffic originating from that IP space is identified as coming from that internal network. The private IP space or IP range defines the scope of the resource. The traffic sent from user devices on your organization's internal network is visible in the Secure Access Activity Search report.

Before you begin

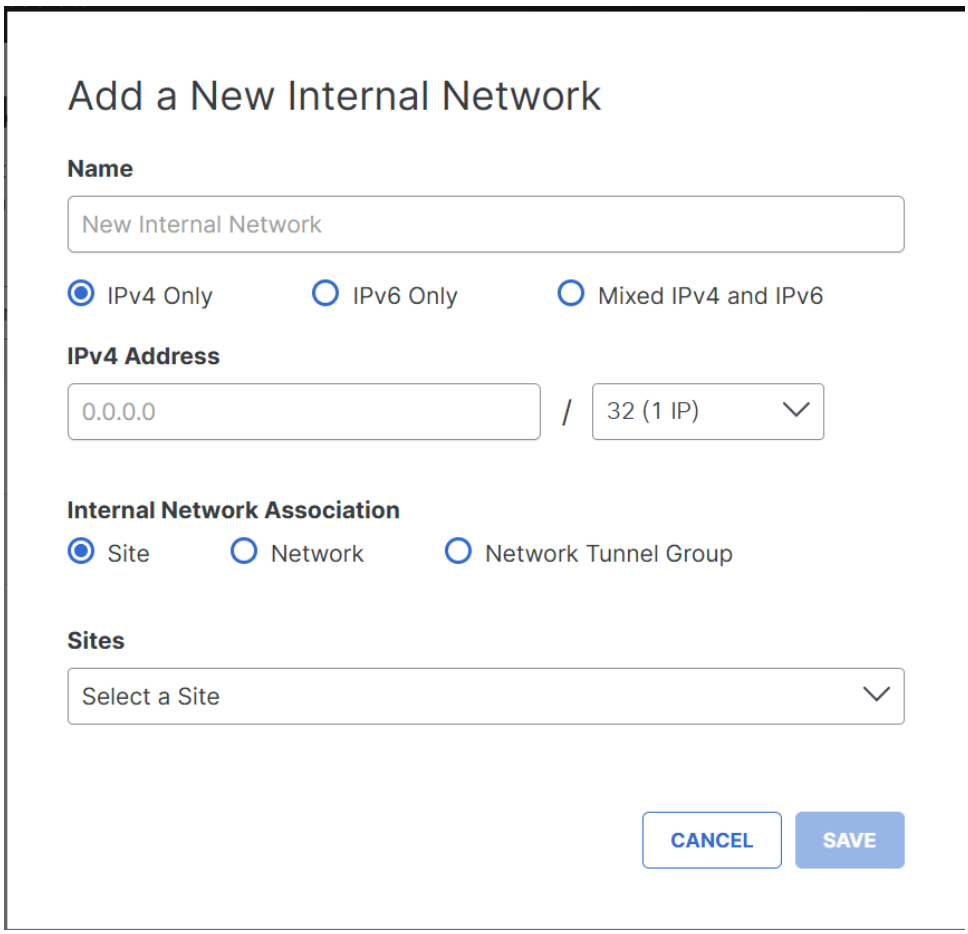
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internal Networks** and click **Add**.

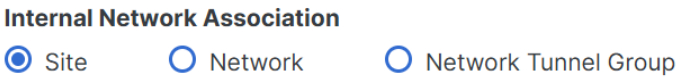


2. Give a descriptive internal network name for **Name**.

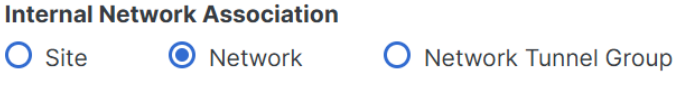


3. Enter an IPv4 address and choose a range.
4. Choose **Site** or **Network** or **Network Tunnel Group**.

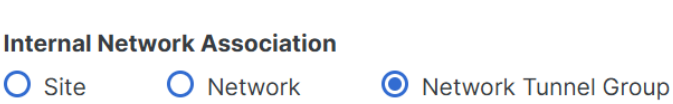
   For **Site**, select the Site to associate with the Internal Network resource.

   For **Networks**, select the Network to associate with the Internal Network resource.

   For **Network Tunnel Group**, select the Network Tunnel Group to associate with the Internal Network resource.

5. Click **Save**.

Update an Internal Network Resource

Provides instructions for updating an internal network resource. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

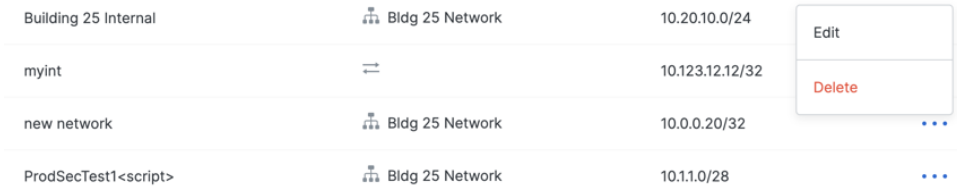
Once you add Internal Network resources to Cisco Secure Access, you can you can update the resource.

Before you begin

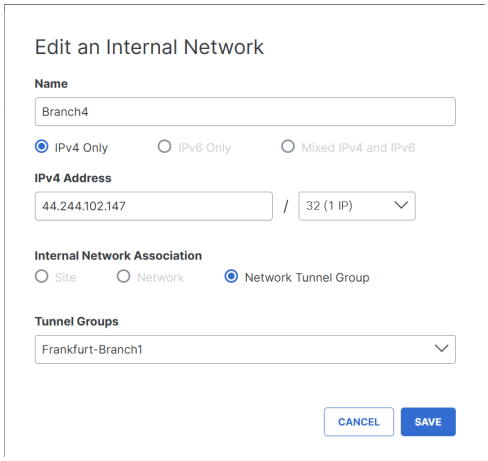
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internal Networks**.
2. For an Internal Network resource, click the ellipsis (**...**) and choose **Edit** to open the Internal Network resource.



3. Follow the steps in Add Internal Network Resources to update the Internal Network resource.



4. Click **Save**.

Delete an Internal Network Resource

Provides instructions for deleting an internal network resource. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

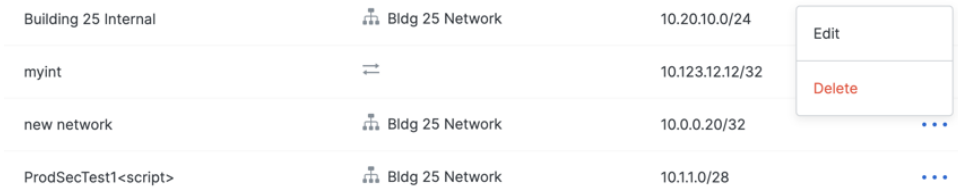
Once you add Internal Network resources to Cisco Secure Access, you can remove an Internal Network resource from Secure Access. After you delete an Internal Network resource, you can no longer apply a policy rule to the resource and the internal network is not protected by Secure Access.

Before you begin

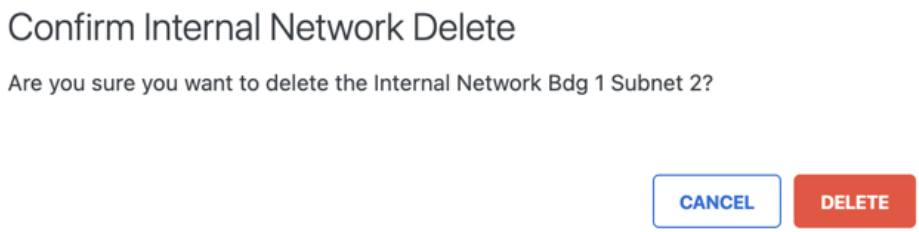
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internal Networks**.
2. For an Internal Network resource, click the ellipsis (**...**) and choose **Delete**.



3. Click **Delete** to remove the internal network resource from Secure Access.



21 Manage Destination Lists

Topics:

- Add a Destination List
- Upload Destinations From a File
- Edit a Destination List
- Download Destinations to a CSV File
- Control Access to Custom URLs
- Wildcards in Destination Lists
- Add Punycode Domain Name to Destination List

Introduces managing destination lists. A destination list is a collection of domains, URLs, IP addresses (IPv4 and IPv6), and CIDR blocks. Use destination lists in internet access rules to block, allow, or isolate traffic, or in DLP rules to monitor or block sensitive data uploaded to the web.

A destination list is a collection of domains, URLs, IP addresses (IPv4 and IPv6), and CIDR blocks. Use destination lists in internet access rules to block, allow, or isolate traffic, or in DLP rules to monitor or block sensitive data uploaded to the web.

You can allow or block destination lists based on the policies that are applied to the identities in your organization.

Important

Large destination lists can impact Secure Access performance. We recommend that you set a limit of no more than 100 destinations per list.

Note

Internet access rules specify how traffic to internet destinations should be handled. The rules apply to traffic from managed devices to public internet sites and applications, including public cloud applications of which your company is a tenant.

You can add a destination list to Secure Access at any time. However, the destination list has no effect until you have added it to an internet access rule.

Guidelines and Best Practices

- Domains in destination lists must comply with the format described in RFC-1035.
- Each fully qualified domain name that you add in a destination list must contain less than 253 characters.
- Secure Access assumes implied left asterisk wildcards in domains. You may not include wildcards in domains.
- In URLs, Secure Access assumes right-side wildcards by URL path segment. (i.e., https://www.example.com matches https://www.example.com/abc/def but not https://www.sub.example.com/abc/def.) You must use URLs that follow standard syntax rules. (See RFC-3986). Secure access normalizes the format. (See Control Access to Custom URLs.)

Note

Destination lists accept domain names that are encoded in Punycode. For more information, see Add Punycode Domain Name to Destination List.

Destination List Examples

Valid destination list entries:

- example.com (Domain)
- sub.domian.com (Domain)
- http://www.example.com/path.file.txt (URL)
- us (Country code top-level domain)
- com (Top-level domain)
- 198.51.100.0 (IPv4 address)
- 2001:DB8::/32 (IPv6 CIDR)
- 102.9.2.0/24 (CIDR block)

Invalid destination list entries:

- example.* (Uses asterisk)
- 2001:DB8:/128 (Malformed address)
- 2001:DB8:/32 (Malformed CIDR)
- http://www.example.com/path/file?.txt (URL with ? wildcard)

Add a Destination List

Provides instructions for adding a destination list. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

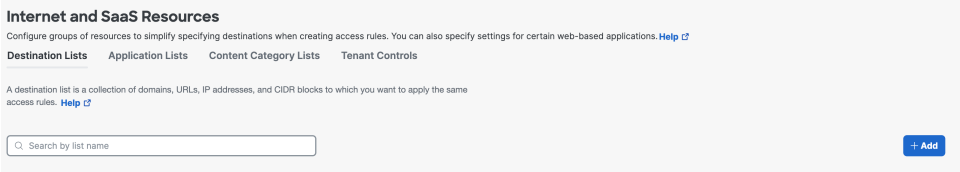
Cisco Secure Access enables administrators to manage destinations grouped by destination lists. Destination lists either allow or block access to destinations: domains, URLs, CIDRs, and IPs. Add a destination list with destinations and then apply the destination list to various policy rules.

Before you begin

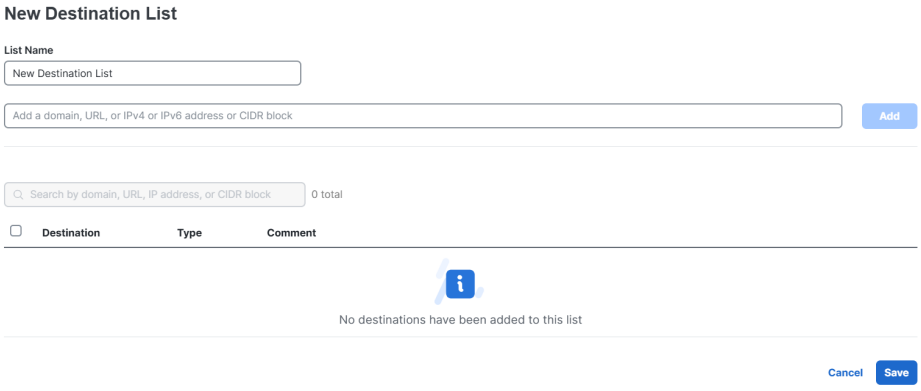
- Full Admin role in Secure Access. See Manage Accounts.
- For supported destination types and guidelines, see Manage Destination Lists.
- If you want to upload a list of destinations from a file, see Upload Destinations from a File.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**
2. Click **Add**.



3. In the **List Name** field, enter a descriptive name.



4. In the next field, enter a domain, URL, IPv4 or IPv6 address, or CIDR.
5. Click **Add**.

> **Tip**
>
> You can upload destinations in bulk from a text file, but you must first save and edit the destination list. For more information, see Upload Destinations from a File.

6. Click **Save**.

The destination list is now available as a destination when you add an internet access rule.

Upload Destinations From a File

Provides instructions for uploading destinations from a file. Files must be text files and must include only one destination per line. Before uploading, review your list for extra-space characters, commas, and so on. Exceptions to the format of a single destination per line can result in errors.

You can import destinations in bulk from a text file into an existing destination list.

Note

Supported files for upload

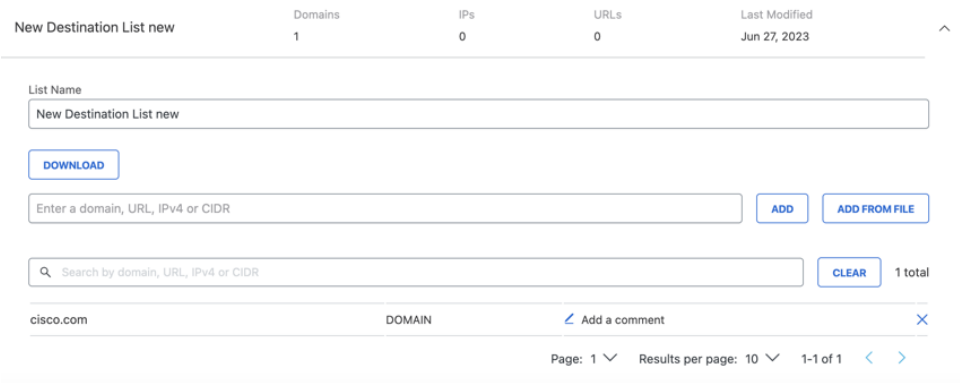
Files must be text files and must include only one destination per line. Before uploading, review your list for extra-space characters, commas, and so on. Exceptions to the format of a single destination per line can result in errors.

Before you begin

- Full Admin role in Secure Access. See Manage Accounts.
- For supported destination types and guidelines, see Manage Destination Lists.

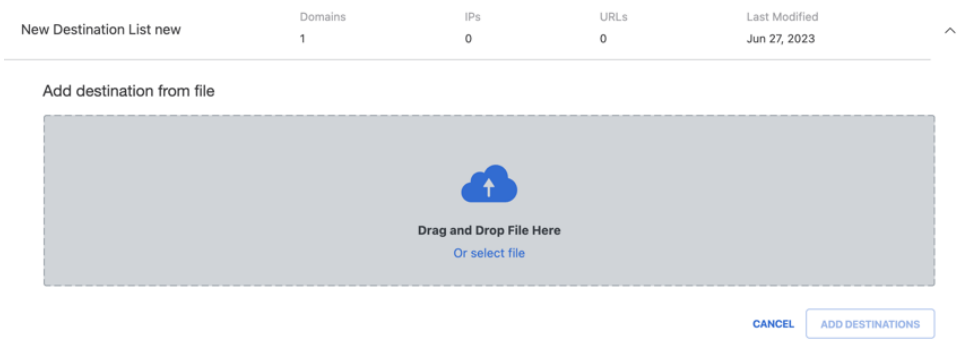
Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.
2. If you are uploading destinations to an existing list, navigate to the list and click the caret to expand the list.
3. If the list you want to upload the file to does not yet exist:
   a. Add a destination list. You don't need to add any destinations.
   b. Save the new list.
   c. Click the caret in the table row to expand the new list.



4. Click **Add From File**.

   The current uploader supports text files in the format of one destination per line. Excel files are not supported.



5. Select or drag and drop a .txt file that contains your destinations.

   If you want to remove the file and choose a different file, click **Replace**.

6. Click **Add destinations**.

   Supported destinations in the file are added to your destination list.

   If your bulk upload includes unsupported destinations, the upload does not fail, but only supported destinations are added.

7. Immediately after uploading the destinations, look for a pop-up at the bottom of your browser. If the file contained unsupported destinations, this pop-up is displayed.



8. To download a spreadsheet that you can use to determine which destinations failed and why, click the link in the pop-up.
9. Click **Save**.

Edit a Destination List

Provides instructions for editing a destination list. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

A destination list can be edited at any time. If a destination list is part of an enabled internet access rule, changes are effective immediately.

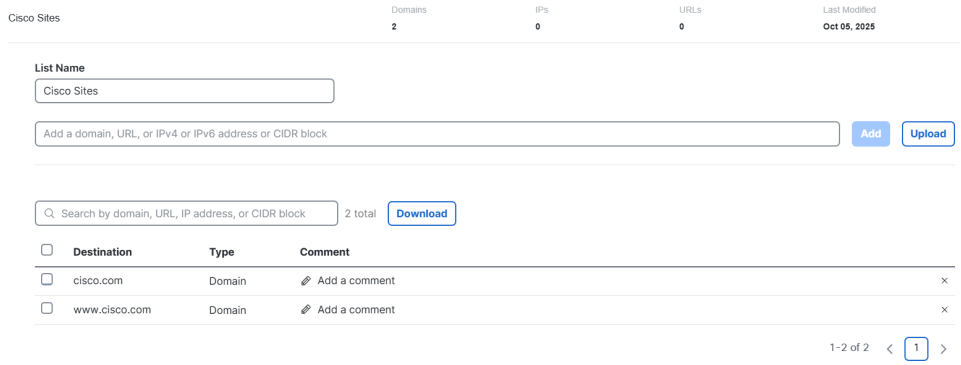
Before you begin

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

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.
2. Expand a destination list.
3. Make your changes.

> **Tip**
>
> You can upload destinations in bulk from a text file. For more information, see Upload Destinations from a File.



4. Click **Save**.

Download Destinations to a CSV File

Provides instructions for downloading destinations to a csv file. After you've added a destination list to Secure Access, you can download a CSV-formatted list of destinations.

After you've added a destination list to Secure Access, you can download a CSV-formatted list of destinations. Downloading a CSV file of the destinations is useful for when you need to update the destinations or share the destinations with teams that do not have permission to view the destination list in Secure Access. The CSV file includes the information about the destinations in the destination list, including whether destinations are allowed and blocked.

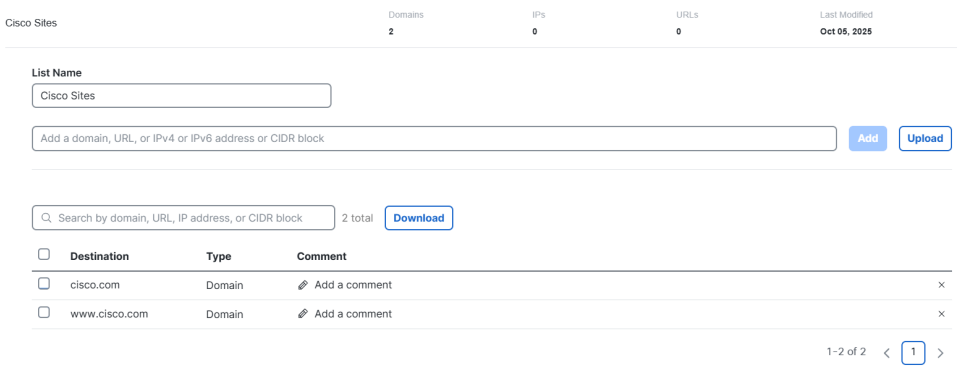
You can remove or add entries in the CSV file, and then upload a file of destinations to a destination list. For more information, see Upload Destinations from a File.

Before you begin

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

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.
2. Expand a destination list and click **Download**.
   The information for the destinations in the destination list are saved in a CSV file on your system.



Control Access to Custom URLs

Describes control access to custom urls. Adding custom URLs to a destination list allows Secure Access to extend a domain in a destination list to encompass full URLs.

Adding custom URLs to a destination list allows Secure Access to extend a domain in a destination list to encompass full URLs. This allows you to control access to a web site's pages based on the full URL of that portion of the web site pages.

Prerequisites

- Install a root certificate to support SSL decryption of URLs.
- The custom URL destination list is protocol-agnostic. This means that Secure Access does not expect that it's possible to know which protocol a web site will use in advance. Therefore, adding a protocol in front of a URL is not required when defining a destination list. Instead, with SSL decryption enabled, Secure Access can block a URL whether it's HTTP or HTTPS and thus minimize the difficulty of creating a destination list. For more information, see Manage Certificates.

Block a URL

Provides instructions for block a url. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

To block a URL, you can add it to a blocked destination list or create a new blocked destination list for URLs.

To add a URL to an existing blocked destination list:

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Expand a destination list
3. Add a URL.
4. Click **Save**.

> **Note**
>
> It is important to specify the URL correctly so that what's in your policy rule matches what the user is trying to access and is controlled correctly by access settings (block, allow, or warn—depending on the policy type).

URL Normalization

Describes url normalization. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

URLs normalize automatically using the following criteria:

URL Normalization	
Protocol Schema (the protocol should be stripped)	hxxp://xyz.com/test → xyz.com/test
Username: Password (should be stripped)	user:pass@xyz.com → xyz.com
Ports (should be stripped)	xyz.com:8080/abc → xyz.com/abc
Trailing slashes (stripped from the end of the URL)	xyz.com/abc/ → xyz.com/abc

URL Normalization for Destination Lists

Describes url normalization for destination lists. URL filtering conforms to URL normalization standards. Certain guidelines must be followed to ensure that the URL you are entering is what you want to block or allow.

URL filtering conforms to URL normalization standards. Certain guidelines must be followed to ensure that the URL you are entering is what you want to block or allow. These can sometimes mean that the way a URL is displayed in the browser's address bar is not how it should be specified in a destination list. This is not done automatically. You must format the URL using the guidelines listed here for it to be blocked or allowed as intended. For guidelines, see URL Normalization.

Troubleshooting Unblocked URLs

Describes troubleshooting unblocked urls. If the Secure Access block page does not display when navigating to a URL you expect to be blocked, ensure that the policy rule with the destination list enabled is higher in order than other rules that the enrolled resources may be part of.

If the Secure Access block page does not display when navigating to a URL you expect to be blocked, ensure that the policy rule with the destination list enabled is higher in order than other rules that the enrolled resources may be part of.

Wait up to five minutes before testing again after any changes are made to ensure that enough time has passed for the changes to be replicated throughout Secure Access.

If problems persist, clear the local browser cache on your machine. Alternatively, clear your machine's DNS cache—a reboot will accomplish this.

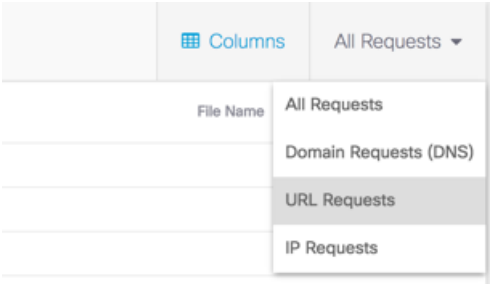
Also, check to see if you have a local—on-premise—proxy that is interfering.

Additionally, confirm that you have installed certificates. For more information, see Manage Certificates.

Reporting for Blocked URLs

Describes reporting for blocked urls. The Secure Access Activity Search report supports the use of URLs as a search filter.

The Secure Access Activity Search report supports the use of URLs as a search filter.



After you've filtered for URLs, add another filter to show the custom block URLs that belong to your destination lists.

Examples

Describes examples. The following examples show a single URL and what you can and cannot enter to have a block of that URL enforced.

The following examples show a single URL and what you can and cannot enter to have a block of that URL enforced. The list of URLs is built out from a single example, modifying a single parameter to show whether the URL "//a.co/cx/15195/100/setup_1848x19m.exe?z=z&super=bad&test=yes" would be blocked based on a URL.

In these examples, the protocol is stripped as it would be by the interface.

If you wanted to block this URL *a.co/cx/15195/100/setup_1848x19m.exe?z=z&super=bad&test=yes* the following logic would apply.

URL	Blocked?	Reason
a.co/cx/15195/100/setup_1848x19m.exe?z=z&super=bad&test=yes	Yes	The full URL is entered.
a.co/cx/15195/100/setup_1848x19m.exe?super=bad&test=yes&z=z	Yes	"&" is a delimiter; therefore, it's added as another level to the URL after the word "yes".
a.co/cx/15195/100/setup_1848x19m.exe?super=bad&test=yes	No	"?" is a delimiter so the URL still would begin at the "yes" and any enforcement would happen after that.
a.co/cx/15195/100/setup_1848x19m.exe?	No	Given the "?", it still means only characters after "yes" will be enforced; therefore, a direct download of this file would be allowed.
a.co/cx/15195/100/setup_1848x19m.exe	No	We will still only block any paths after "yes"; therefore, a direct download of this file would be allowed.

If you want to block this URL *g.com/a/d*, the following logic applies.

> **Note**
>
> These are only examples of destination list entries that would and would not block the URL `g.com/a/d`.

URL	Blocked?	Reason
g.com/a/d	Yes	The full URL is entered.

URL	Blocked?	Reason
g.com/a/d?g	Yes	Delimits the path with the query "g" but still just a delimiter thus this will be enforced.
g.com/a/d?	Yes	URL + the "?" delimiter.
g.com/a/	No	The URL ends with "/d" so anything before "/d" would not be enforced.
g.com/a/?a	No	The URL ends with "/d" so anything before "/d" would not be enforced.

If you want to block this URL *d.co/cx/15195/100*, the following applies.

Note

These are only examples of which destination list entries would block the URL "d.co/cx/15195/100" and which would not.

URL	Enforced	Reason
d.co/cx/15195/100	Yes	The full URL is entered.
d.co/cx/15195/100/?	Yes	Everything after the delimited "/" after 100 would be blocked.
d.co/cx/15195/100/	Yes	Everything after the delimited "/" after 100 would be blocked.
d.co/cx/15195/100	Yes	Everything after the delimiting "/" after 100 would be blocked.
d.co/cx/15195/10	No	The delimiter is only for paths after the "/" so any changes to the final path of /100/ would be ignored.
d.co/cx/15195/1000	No	The delimiter is only for paths after the "/" so any changes to the final path of /100/ would be ignored.
d.co/cx/15195/	No	The delimiter is only for paths after the "/" so any changes to the final path of /100/ would be ignored.
d.co/cx/15195	No	The delimiter is only for paths after the "/" so any changes to the final path of /100/ would be ignored.

> **Note**
>
> There are normalization rules that most administrators never encounter. If you find that a URL is not being properly filtered and you've confirmed that all criteria are met, see the URL Normalization RFC.

Troubleshooting

Describes troubleshooting. If you encounter issues with the custom URL feature, contact Support and include the output of the following commands:

If you encounter issues with the custom URL feature, contact Support and include the output of the following commands:

macOS

```
dig proxy.opendnstest.com
```

```
dig debug.umbrellagov.com txt
```

Windows

```
nslookup proxy.opendnstest.com
```

```
nslookup -type=txt debug.umbrellagov.com
```

Wildcards in Destination Lists

Describes wildcards in destination lists. Wildcards support top-level domains (TLDs) to allow broad allows or blocks for destination lists. Every domain in a block or allow destination list has an implied left-side and right-side wildcard. Asterisks (*) are not supported.

Wildcards support top-level domains (TLDs) to allow broad allows or blocks for destination lists.

Every domain in a block or allow destination list has an implied left-side and right-side wildcard.

> **Note**
>
> Asterisks (*) are not supported.

Destination List Entry	Implied Wildcard
domain.com	*.domain.com/*
com	*.com/*
www.domain.com	*.www.domain.com/*

It is not possible to use an asterisk in a wildcard to navigate to a different part of the domain. For example, the following wildcards will *not* work:

- *.domain.com
- subdomain.*.com

- sub*.com
- domain.*

Adding domain.com to a destination list results in requests to domain.com or its subdomains, such as www.domain.com or www.domain.com/path.

Use caution as adding a TLD to an allow list may open your network to malware threats, and adding a TLD to a block list may block more than expected due to CNAMEs and CDNs.

Note

Regular expressions in URL paths are not supported.

Add Punycode Domain Name to Destination List

Describes adding punycode domain name to destination list. To block suspicious destinations and prevent phishing attacks, you can add a domain name that is encoded in Punycode to destination lists.

To block suspicious destinations and prevent phishing attacks, you can add a domain name that is encoded in Punycode to destination lists.

What is Punycode?

Punycode is a way to represent domain names that use characters outside of the standard ASCII set. The domain name system (DNS) accepts a subset of ASCII characters for domain name labels. Because Punycode uses characters that look similar, Punycode can be used to mislead unsuspecting users to malicious content.

In phishing attacks, a malicious actor may replace certain ASCII characters in a domain name with Unicode characters. A browser or mobile client displays the altered domain name (as Unicode) which closely resembles an authentic domain name. For example, bücher.com and bucher.com look similar but are different domains.

To prevent phishing attacks and block malicious domain names, encode a domain name that contains Unicode characters in Punycode. Once encoded, add the Punycode string to a destination list. For more information about Punycode, see RFC 3429.

Note

You must add Punycode-encoded domain names to a destination list one at a time.

Examples of Unicode and Punycode Encoded Strings

Unicode	Punycode	Description
a	a-	Only one ASCII character.
🤩	xn--n28h	Only one emoji character.
α	mxa	Only one Greek character.
starƅucks.com	xn--starucks-hpd.com	Domain name with a Unicode character.
adıdas.de	http://xn--addas-o4a.de/	Domain name with a Unicode character.

22 Manage Application Lists

Topics:

- Add an Application List
- Application Categories
- Delete an Application List

Introduces managing application lists. Secure Access organizes application-based resources into categories based on the type of processes or services provided, for example: shopping, education, or human resources. You can add applications or entire application categories to an application list.

Secure Access organizes application-based resources into categories based on the type of processes or services provided, for example: shopping, education, or human resources. You can add applications or entire application categories to an application list. Once saved, application lists are available to choose as destinations in all of your access rules.

Use application lists to simplify destination management and apply access rules consistently. However, you can also choose individual applications and entire application categories directly in internet access rules.

For certain applications, you can allow access to the application but restrict uploads, downloads, and posting to the application. See Advanced Application Controls. You will configure these controls directly in the internet access rule when the destination includes an application that offers those controls.

When a new application is added to a category, Secure Access automatically adds that application to all configuration settings that include that entire category. For each application list, the new application will use the same default action as that applies to the Application category as a whole.

Note

It is not possible to search for an application with fewer than three letters in its name—for example, "QQ" or "YY". These applications must be manually picked from the tree under their respective categories or wildcarded in search—for example, "QQ*". This behavior is by design.

Add an Application List

Provides instructions for adding an application list. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

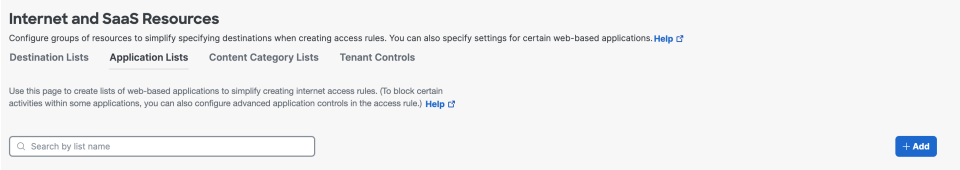
Cisco Secure Access application lists organize application-based destinations into categories based on the type of processes or services provided, for example: shopping, education, or human resources. To control traffic to applications, add application categories to an Application list and then select the list in a policy rule. You can reuse application lists in multiple policy rules.

Before you begin

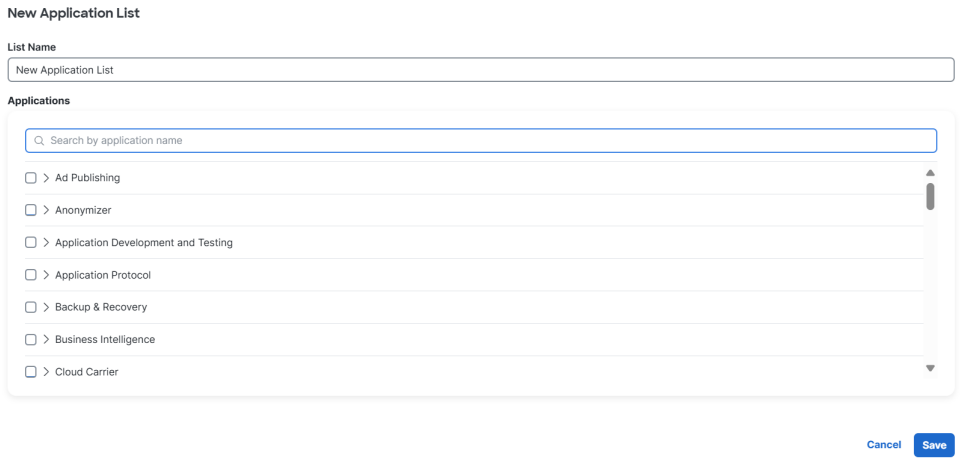
- Full Admin user role. For more information, see Manage Accounts.

Procedure

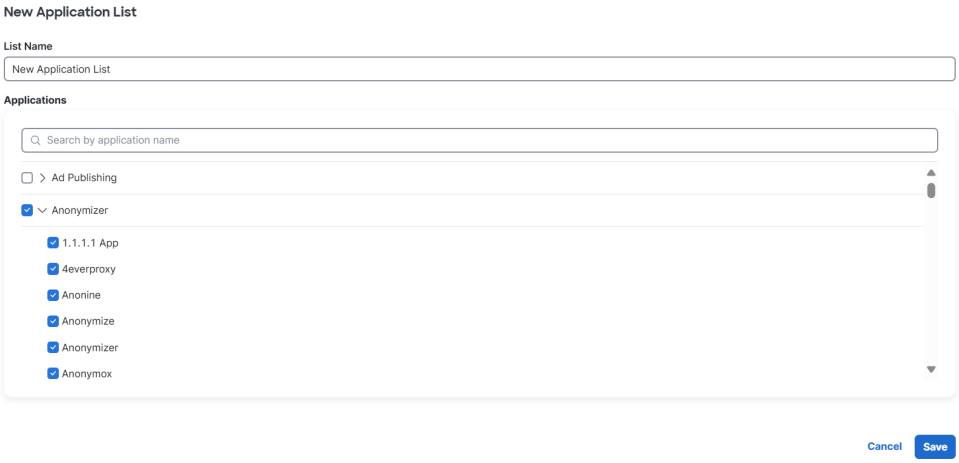
1. Navigate to **Resources** > **Internet and SaaS Resources** > **Application Lists** and click **Add**.



2. Give your application list a descriptive **List Name**.



3. Search for applications and then select applications, or expand each application category and choose individual applications within the category. When you select only a few apps within a category, the category is marked with a dash. When you select an entire category, it is marked with a check.



- For information about the available categories, see Application Categories.

> **Note**
>
> About New Applications Added to a Category
>
> When a new application is added to a category, Secure Access automatically adds that application to all configuration settings that include that entire category. For each application list, the new application will use the same default action as that applies to the Application category as a whole.

4. Click **Save**.

Application Categories

Describes application categories. The system is capable of discovering thousands of apps; these are divided into categories for ease of reference. Categorization of discoverable apps is conducted by a team of researchers, and based on similarities among apps as well as a number of other quantitative application feature sets.

The system is capable of discovering thousands of apps; these are divided into categories for ease of reference. Categorization of discoverable apps is conducted by a team of researchers, and based on similarities among apps as well as a number of other quantitative application feature sets.

Category Descriptions

Discovered apps are assigned to the following categories:

- **Ad Publishing**–Applications that enable publishers and ad networks to manage ad serving and trafficking.
- **Anonymizer**–Services that provide an anonymous proxy tool that attempts to make activity on the Internet untraceable.
- **Application Development and Testing**–Applications suited for application development and testing cycles, or for building integration applications in the cloud and within the enterprise.
- **Application Protocols** –Application layer protocols that govern how data is transmitted and received over a network, enabling different services such as web browsing, email, file transfer, and online transactions as well as

allowing software applications to communicate with each other. These include SSH, FTP, SMTP and other such applications.

- **Backup and Recovery**–Applications for backup and recovery of file systems and raw data stores on servers and desktop systems.
- **Business Intelligence**–Applications for analytics such as dashboards, reporting systems, scenario modeling, and data analysis.
- **Cloud Broker**–Applications that manage the use, performance, and delivery of cloud services and negotiate relationships between cloud providers and cloud consumers.
- **Cloud Carrier**–Intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers through a network, telecommunication, and other access devices.
- **Cloud Service Provider**–Based on NIST definition of a cloud service, which we believe is being (slowly) adopted as the industry standard. The NIST definition includes the following criteria: on-demand self-service, rapid elasticity, and measured service. CASI additionally adds vendor intent to provide computing-related services (Compute, Network, Storage and/or Software Application). If in doubt whether web or cloud, we will be conservative and assume cloud until we can prove otherwise.
- **Cloud Storage**–Applications that offer massively scalable storage capacity that can be used for applications, and file storage.
- **Collaboration**–Applications that enhance communication and collaboration in workgroups, within enterprises, and across enterprises.
- **Compute**–Fundamental computing resources for running cloud-based systems that can be dynamically provisioned and configured as needed.
- **Content Delivery Network (CDN)**–Applications that store content and files to improve the performance and cost of delivering content for web-based systems by offering a large distributed system of servers deployed in multiple data centers across the Internet.
- **Content Management**–Applications for managing the production of and access to content, enforcing document production workflows, and providing workspaces for groups or enterprises to find and access documents.
- **Customer Relationship Management (CRM)**–Applications that manage interactions with current and future customers, including organization and automation across sales, marketing, and customer service functions.
- **Database Management**–Applications offering scalable data management solutions for structured or unstructured data, relational database solutions or scalable non-SQL datastores.
- **E-Commerce**–Applications that facilitate the buying and selling of products or services.
- **Education**–Applications that provide educational or training courses, general learning opportunities or specific employee training independent of their location.
- **Enterprise Resource Planning (ERP)**–Applications that manage operations or management of a business; which can include internal and external resources, including tangible assets, financial resources, materials, and human resources.
- **Financial Services**–Applications for managing financial processes and information.
- **Games**–Online and mobile games.
- **Healthcare**–Applications that provide access to health, medical, and personal fitness systems.
- **Hosting Services**–Applications that enable corporate or individual websites or other content to be accessible over the internet.
- **Human Resources**–Applications for managing human resources and HR functions.

- **IT Service Management**–Applications that support specific IT functions to plan, deliver, operate and control IT services.
- **Legal**–Applications that provide access to legal documents and public records and support legal content.
- **Marketing & Sales**–Applications that are specifically designed for marketing and sales functions.
- **Media**–Applications that host or stream media as a service.
- **Office Productivity**–Applications for producing information and other standard office-oriented tasks such as documentation, presentations, project management, and so on.
- **Others**–Used for those services where no existing categorization would fit.
- **P2P**–Peer to Peer torrents like apps and protocols.
- **Search**–Web or app-based search.
- **Security**–Applications that support security activities to ensure adherence to regulatory compliance rules and protect information, data applications, and infrastructure.
- **Service Management**–Applications that support general operational activities outside of the IT function.
- **Shopping**–Web or app-based basic online shopping.
- **Social Networking**–Applications that establish and maintain a connection among users that are tied in one or more specific types of interdependency.
- **Software Repository**–Software repositories.
- **Support**–Applications that provide access to customer support services.
- **Travel**–Applications that provide travel management services.
- **Web Content**–Mostly app-based services that provide content. It can be through a login or paid portal.

For some applications, you can allow access to the application but block activities such as uploads, downloads, or posting. For more information and a list of applications that support these blocks, see Advanced Application Controls.

Delete an Application List

Provides instructions for deleting an application list. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

After you create an application list, you can delete the list from Secure Access.

Before you begin

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

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Application Lists**.
2. Expand an application list, and then click **Delete**.
3. If the list is used in any rules, you will see a list of those rules. You cannot delete the list if it is used in rules. Delete the list from the rules or delete the rules, then try again.

23 Manage Content Category Lists

Topics:

- Available Content Categories
- Add a Content Category List
- Request a Category for an Uncategorized Destination
- Dispute a Content Category
- View Content Categories in Reports

Introduces managing content category lists. Secure Access classifies internet destinations using content-based categories. Examples of content categories are: gambling, social networking, and alcohol.

Secure Access classifies internet destinations using content-based categories. Examples of content categories are: gambling, social networking, and alcohol.

To speed rule creation and to apply rules consistently to groups of categories, you can create content category lists. For example, you can create a list of categories that you want to block, and another list that you will use in rules with the Warn action.

Then, when you select a destination in an internet access rule, you can select one or more content category lists. You can also select individual categories.

Available Content Categories

Describes available content categories. You can use the following content categories as destinations in internet access rules. Web sites that Cisco Talos classifies as belonging to a category destination are handled by the rule.

You can use the following content categories as destinations in internet access rules. Web sites that Cisco Talos classifies as belonging to a category destination are handled by the rule.

- **Adult**—Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers), general information about sex, non-pornographic in nature, genital piercing, adult products or greeting cards, information about sex not in the context of health or disease.
- **Advertisements**—Banner and pop-up advertisements that often accompany a web page, other advertising websites that provide advertisement content. Advertising services and sales are classified as Business and Industry.
- **Alcohol**—Alcohol as a pleasurable activity, beer and wine making, cocktail recipes, liquor sellers, wineries, vineyards, breweries, alcohol distributors. Alcohol addiction is classified as Health and Medicine. Bars and restaurants are classified as Dining and Drinking.
- **Animals and Pets**—Information about domestic animals, livestock, service animals, pets and their care. Veterinary services, medicines, and animal health. Pet and animal training, aquariums, zoos, and animal shows. Includes animal shelters, humane societies, animal centric charities, and sanctuaries, bee keeping, training, and animal husbandry; dinosaurs and extinct animals.
- **Arts**—Galleries and exhibitions, artists and art, photography, literature and books, performing arts and theater, musicals, ballet, design, architecture. Cinema and television are classified as Entertainment.
- **Astrology**—Astrology, horoscope, fortune telling, numerology, psychic advice, tarot.
- **Auctions**—Online and offline auctions, auction houses, and classified advertisements.
- **Business and Industry**—Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital, office supplies, industrial equipment (process equipment), machines and mechanical systems, heating equipment, cooling equipment, materials handling equipment, packaging equipment, manufacturing: solids handling, metal fabrication, construction and building, passenger transportation, commerce, industrial design, construction, building materials, shipping and freight (freight services, trucking, freight forwarders, truckload carriers, freight and transportation brokers, expedited services, load and freight matching, track and trace, rail shipping, ocean shipping, road feeder services, moving and storage).
- **Cannabis**—Websites that focus on the recreational and medicinal consumption of cannabis. Sites may include marketing, discussions about legal and regulatory issues, growth and production, paraphernalia, research, and investment in the cannabis industry. Dispensaries, cannabinoid (CBD oil, THC, etc.) based products are also included.
- **Chat and Instant Messaging**—Web-based instant messaging and chat rooms.
- **Cheating and Plagiarism**—Promoting cheating and selling written work, such as term papers, for plagiarism.
- **Child Abuse Content**—Worldwide illegal child sexual abuse content. Secure Access blocks all web requests that match the Child Abuse Content category. Traffic is enforced globally by the secure web gateway (SWG) and default Security profile.
- **Cloud and Data Centers**—Platforms used to serve cloud infrastructure or data center hosting to support an organization's applications, services, or data processing. Due to the de-centralized nature of these domains and IP addresses, a more specific category cannot be applied based on content or ownership.
- **Computer Security**—Offering security products and services for corporate and home users.
- **Computers and Internet**—Information about computers and software, such as hardware, software, software support, information for software engineers, programming and networking, website design, the web and Internet in general, computer science, and computer graphics. Freeware and Shareware is a separate category.

- **Conventions, Conferences, and Trade Shows**–Seminars, trade shows, conventions and conferences themed around a particular industry, market, or common interest. May include information about acquiring tickets, registration, abstract or presentation proposal guidelines, workshops, sponsorship details, vendor or exhibitor information, and other marketing or promotional material. This category includes academic, professional, as well as pop-culture events, all of which tend to be a short-lived or annual event.
- **Cryptocurrency**–Online brokerages and websites that enable users to trade cryptocurrencies; information regarding cryptocurrencies including analysis, commentary, advice, performance indexes, and price charts. General information about cryptomining and mining businesses are included in this category but domains and IP addresses directly involved in mining activities are categorized as Cryptomining.
- **Dating**–Dating, online personals, matrimonial agencies.
- **Digital Postcards**–Enabling sending of digital postcards and e-cards.
- **Dining and Drinking**–Eating and drinking establishments, restaurants, bars, taverns, and pubs, restaurant guides and reviews.
- **DIY Projects**–Guidance and information to create, improve, modify, decorate and repair something without the aid of experts or professionals.
- **DNS over HTTPS (DoH) and DNS over TLS (Transport Layer Security)**–Encrypted DNS requests using either the DNS over HTTPS (DoH) protocol or the DNS over TLS protocol. These protocols are typically used as a layer of security and privacy by end-users, but the encryption hides the destination of the request and passes it through a third-party.
- **Dynamic and Residential**–IP addresses of broadband links that usually indicates users attempting to access their home network, for example for a remote session to a home computer.
- **Education**–Education-related, such as schools, colleges, universities, teaching materials, and teachers' resources, technical and vocational training, online training, education issues and policies, financial aid, school funding, standards and testing.
- **Entertainment**–Details or discussion of films, music and bands, television, celebrities and fan websites, entertainment news, celebrity gossip, entertainment venues. Compare the Arts category.
- **Extreme**–Material of a sexually violent or criminal nature, violence and violent behavior, tasteless, often gory photographs, such as autopsy photos, photos of crime scenes, crime and accident victims, excessive obscene material, shock websites.
- **Fashion**–Clothing and fashion, hair salons, cosmetics, accessories, jewelry, perfume, pictures and text relating to body modification, tattoos and piercing, modeling agencies. Dermatological products are classified as Health and Medicine.
- **File Transfer Services**–File transfer services with the primary purpose of providing download services and hosted file sharing.
- **Filter Avoidance**–Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services.
- **Finance**–Primarily financial in nature, such as accounting practices and accountants, taxation, taxes, banking, insurance, investing, the national economy, personal finance involving insurance of all types, credit cards, retirement and estate planning, loans, mortgages. Stock and shares are classified as Online Trading.
- **Freeware and Shareware**–Providing downloads of free and shareware software.
- **Gambling**–Casinos and online gambling, bookmakers and odds, gambling advice, competitive racing in a gambling context, sports booking, sports gambling, services for spread betting on stocks and shares. Websites dealing with gambling addiction are classified as Health and Medicine. Government-run lotteries are classified as Lotteries.
- **Games**–Various card games, board games, word games, and video games, combat games, sports games, downloadable games, game reviews, cheat sheets, computer games and Internet games, such as role-playing games.

- **Government and Law**–Government websites, foreign relations, news and information relating to government and elections, information relating to the field of law, such as attorneys, law firms, law publications, legal reference material, courts, dockets, and legal associations, legislation and court decisions, civil rights issues, immigration, patents and copyrights, information relating to law enforcement and correctional systems, crime reporting, law enforcement, and crime statistics.
- **Hacking**–Discussing ways to bypass the security of websites, software, and computers.
- **Hate Speech**–Websites promoting hatred, intolerance, or discrimination on the basis of social group, color, religion, sexual orientation, disability, class, ethnicity, nationality, age, gender, gender identity, sites promoting racism, sexism, racist theology, hate music, neo-Nazi organizations, supremacism, Holocaust denial.
- **Health and Medicine**–Health care; diseases and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in the context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in the context of health (disease and health care).
- **Humor**–Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as Adult.
- **Hunting**–Professional or sport hunting, gun clubs and other hunting related sites.
- **Illegal Activities**–Promoting crime, such as stealing, fraud, illegally accessing telephone networks, computer viruses, bombs, and anarchy, websites depicting murder and suicide as well as explaining ways to commit them.
- **Illegal Downloads**–Providing the ability to download software or other materials, serial numbers, key generators, and tools for bypassing software protection in violation of copyright agreements. Torrents are classified as Peer File Transfer.
- **Illegal Drugs**–Information about recreational drugs, drug paraphernalia, drug purchase and manufacture.
- **Infrastructure and Content Delivery Networks**–Content delivery infrastructure and dynamically generated content, websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.
- **Internet of Things**–Domains used to monitor the general health, activity, or aid in the configuration of Internet of Things (IoT) and other network-aware electronics. Additionally these sites may provide software or firmware updates or allow remote access to administer the device. IoT exists in both consumer and professional segments, in products such as printers, televisions, thermostats, system monitoring, automation, and smart appliances.
- **Internet Telephony**–Telephonic services using the internet.
- **Job Search**–Career advice, resume writing and interviewing skills, job placement services, job databanks, permanent and temporary employment agencies, employer websites.
- **Lingerie and Swimsuits**–Intimate apparel and swimwear, especially when modeled.
- **Lotteries**–Sweepstakes, contests, and state-sponsored lotteries.
- **Military**–Military, such as the armed forces, military bases, military organizations, anti-terrorism.
- **Mobile Phones**–Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the Business and Industry category.
- **Museums**–Museums and exhibits, both online and physical, dedicated to preserving information regarding subjects that could be of general interest or highly specialized. Subjects could range from art, history, science, or be of cultural importance.
- **Nature and Conservation**–Sites related to natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation, forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry).

- **News**–News, headlines, newspapers, television stations, magazines, weather, ski conditions.
- **Non-governmental Organizations**–Non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.
- **Non-sexual Nudity**–Nudism and nudity, naturism, nudist camps, artistic nudes.
- **Not Actionable**–Sites that have been inspected but are unreachable or do not have enough content to be assigned a category.
- **Online Communities**–Affinity groups, special interest groups, web newsgroups, message boards. Excludes websites classified as Professional Networking or Social Networking.
- **Online Document Sharing and Collaboration**–Cloud-based software used to create, convert, or edit documents. Collaboration and sharing features may be available with access permissions typically configured by the author. Documents may be stored online or available to download.
- **Online Meetings**–Online meetings, desktop sharing, remote access and other tools that facilitate multi-location collaboration.
- **Online Storage and Backup**–Offsite and peer-to-peer storage for backup, sharing, and hosting.
- **Online Trading**–Online brokerages, websites that enable the user to trade stocks online, information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock splits. Services for spread betting on stocks and shares are classified as Gambling. Other financial services are classified as Finance.
- **Organizational Email**–Websites used to access business email (often via Outlook Web Access).
- **Paranormal**–UFOs, ghosts, cryptid, telekenesis, urban legends and myths.
- **Parked Domains**–Websites that monetize traffic from the domain using paid listings from an ad network, or are owned by 'squatters' hoping to sell the domain name for a profit. These also include fake search websites which return paid ad links.
- **Peer File Transfer**–Peer-to-peer file request websites. This does not track the file transfers themselves.
- **Personal Sites**–Websites about and from private individuals, personal homepage servers, websites with personal contents, personal blogs with no particular theme.
- **Personal VPN**–Virtual private network (VPN) sites or tools that are typically for personal use,and, may or may not be approved for corporate usage.
- **Photo Search and Images**–Facilitating the storing and searching for, images, photographs, and clip-art.
- **Politics**–Websites of politicians, political parties, news and information on politics, elections, democracy, and voting.
- **Pornography**–Sexually explicit text or depictions. Includes explicit anime and cartoons, general explicit depictions, other fetish material, explicit chat rooms, sex simulators, strip poker, adult movies, lewd art, web-based explicit email.
- **Private IP Addresses as Host**–Private IP addresses which are used as the host part of a URL. Private IP addresses are meant for internal use behind border routers only, so they are not publicly routable.
- **Professional Networking**–Social networking for the purpose of career or professional development. See also Social Networking.
- **Real Estate**–Information that would support the search for real estate, office and commercial space, real estate listings, such as rentals, apartments, and homes, house building.
- **Recipes and Food**–Sites dedicated to sharing or discussing information about cooking, recipes, and food or non-alcoholic beverages; cultural aspects of cuisine and food; diet descriptions and adherence tips, general nutrition

information about foods. Use and instruction on cooking appliances and utensils. Food celebrity, lifestyle, and enthusiast blogs.

- **Reference**–City and state guides, maps, time, reference sources, dictionaries, libraries.
- **Regional Restricted Law (Germany)**–URLs that are restricted in Germany due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Law (Great Britain)**–URLs that are restricted in Great Britain due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Law (Italy)**–URLs that are restricted in Italy due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Law (Poland)**–URLs that are restricted in Poland due to content which may be unlawful as determined by the regional government.
- **Religion**–Religious content, information about religions, religious communities.
- **SaaS and B2B**–Web portals for online business services.
- **Safe for Kids**–Directed at, and specifically approved for, young children.
- **Science and Technology**–Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar subjects, space exploration, meteorology, geography, energy (fossil, nuclear, renewable), communications (telephones, telecommunications).
- **Search Engines and Portals**–Search engines and other initial points of access to information on the Internet.
- **Sex Education**–Factual websites dealing with sex, sexual health, contraception, pregnancy.
- **Shopping**–Bartering, online purchasing, coupons and free offers, general office supplies, online catalogs, online malls.
- **Social Networking**–Social networking. See also Professional Networking.
- **Social Science**–Sciences and history related to society, archaeology, anthropology, cultural studies, history, linguistics, geography, philosophy, psychology, women's studies.
- **Society and Culture**–Family and relationships, ethnicity, social organizations, genealogy, seniors, child-care.
- **Software Updates**–Websites that host updates for software packages.
- **Sports and Recreation**–All sports, professional and amateur, recreational activities, fishing, fantasy sports, public parks, amusement parks, water parks, theme parks, spas.
- **Streaming Audio**–Real-time streaming audio content including Internet radio and audio feeds.
- **Streaming Video**–Real-time streaming video including Internet television, web casts, and video sharing.
- **Terrorism and Violent Extremism**–Terrorist or extremist websites that promote death or violence as part of their ideology. Sites may contain graphic or disturbing images, videos, and text. Some sites may not advocate terrorism but share first-hand material of a violent nature.
- **Tobacco**–Pro-tobacco websites, tobacco manufacturers, pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as Health and Medicine.
- **Transportation**–Personal transportation, information about cars and motorcycles, shopping for new and used cars and motorcycles, car clubs, boats, airplanes, recreational vehicles (RVs), and other similar items. Note, car and motorcycle racing is classified as Sports and Recreation.
- **Travel**–Business and personal travel, travel information, travel resources, travel agents, vacation packages, cruises, lodging and accommodation, travel transportation, flight booking, airfares, car rental, vacation homes.

- **Uncategorized**–Any site (domain, URL, or IP address) that has not been categorized–that does not match a security or content category–is blocked. Note that Cisco Talos does not categorize IP addresses as content, only domains, and URLs. IP addresses found to be malicious are placed into a relevant security category. If a URL does not resolve to a content category, Secure Access looks for the URL's domain for a category. If the domain is not categorized then Secure Access treats the URL as uncategorized.

  Note

  Use caution when enabling this category as it will match any domain or URL that has not been categorized by Cisco Talos. This may have unintended results, blocking access to sites not meant to be blocked. Before enabling this setting, we recommend that you first monitor your "Uncategorized" traffic through the Activity Search report. This will help you determine what type of impact that enabling the Uncategorized content category will have on your organization. For more information about monitoring uncategorised traffic, see Activity Search Report.

- **URL Shortener**–Domains used to shorten long URLs, brand URLs, or may obscure the final destination of a hyperlink.
- **Weapons**–Information relating to the purchase or use of conventional weapons such as gun sellers, gun auctions, gun classified ads, gun accessories, gun shows, and gun training, general information about guns, other weapons may be included. Government military websites are classified as Military.
- **Web Cache and Archives**–Cached or archived web content often stored for preservation or to decrease load times.
- **Web Hosting**–Website hosting, bandwidth services.
- **Web Page Translation**–Translation of web pages between languages.
- **Web-based Email**–Public web-based email services. Websites enabling individuals to access their company or organizations email service are classified as Organizational Email.

To make a request to categorize an uncategorized destination:

1. Log into talosintellgence.com with your cisco.com credentials.
2. Click **My Account**.
3. Submit a request to recategorize the domain.

Add a Content Category List

Provides instructions for adding a content category list. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

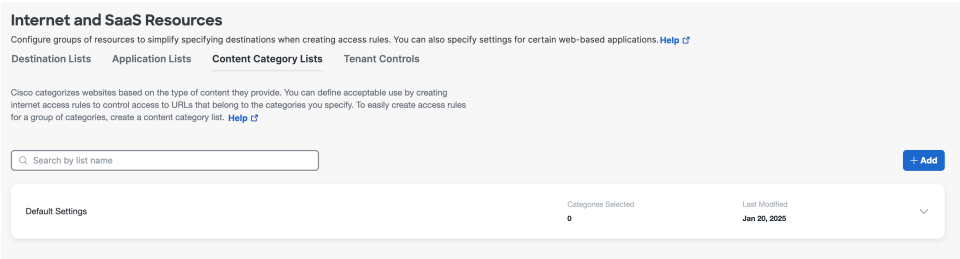
Content category lists allow you to speed rule creation and apply rules consistently to groups of categories.

Before you begin

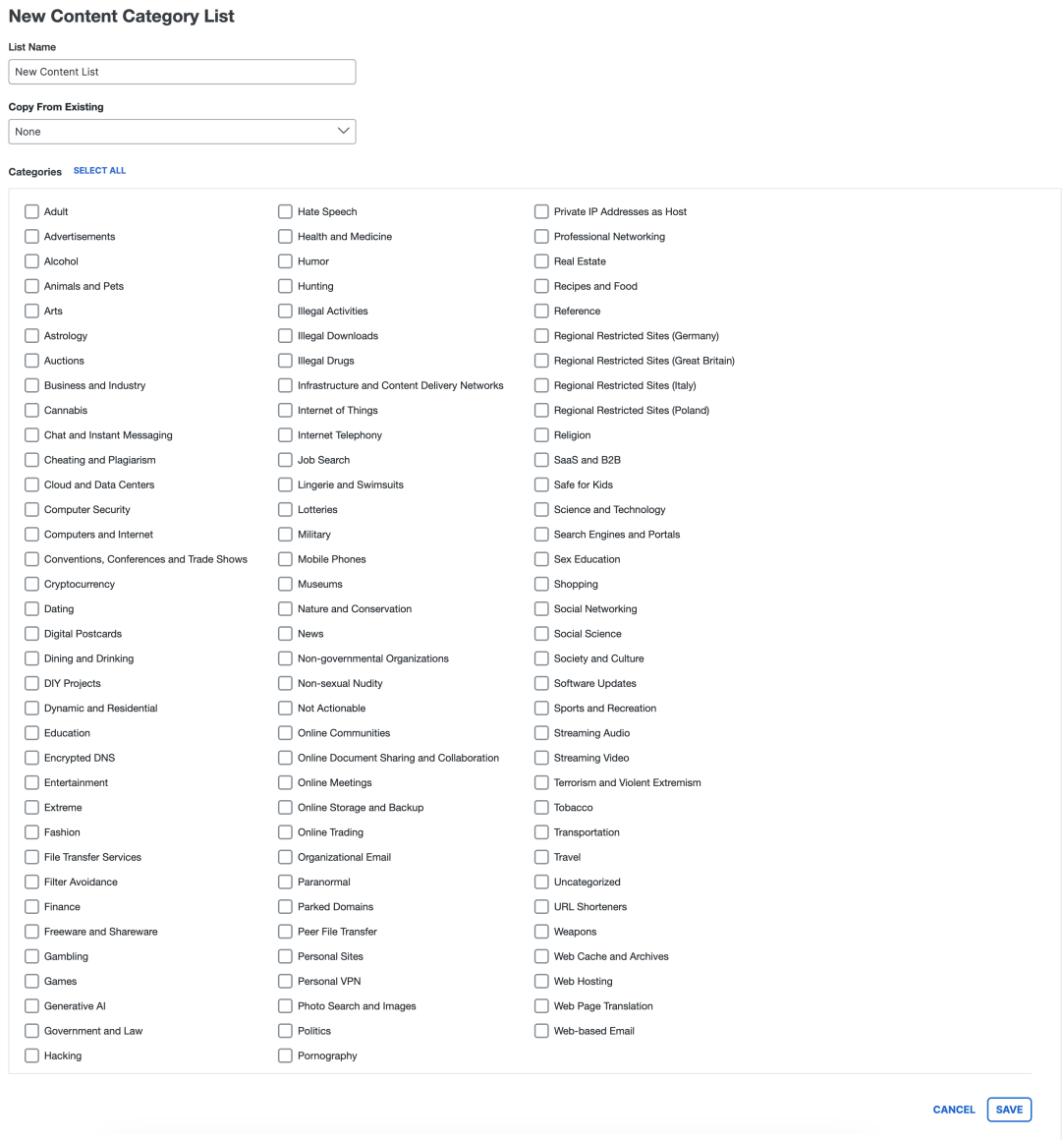
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Content Category Lists**.



2. Click **Add**.
3. Give your configuration a descriptive **List Name**.



4. Select the content categories you want to add to the list.
5. Click **Save**. The new Content Category list is now available as a destination in internet access rules.

Request a Category for an Uncategorized Destination

Provides instructions for request a category for an uncategorized destination. Its purpose, requirements, and key details for Cisco Secure Access administrators.

You can ask Cisco to categorize an uncategorized destination.

Before you begin

- You must have credentials for your Cisco account.

Procedure

1. Navigate to talosintelligence.com.
2. Click **Support**.
3. Click **Content Categorization**.
4. Click **Cisco Login**.
5. Sign in with your cisco.com credentials.
6. Follow the onscreen instructions to submit a request to recategorize the domain.

Dispute a Content Category

Provides instructions for dispute a content category. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Secure Access uses the content categories that are maintained by Cisco Talos. If you disagree with a destination's content-category classification, you can dispute it.

Before you begin

- You must have credentials for your Cisco account.

Procedure

1. Navigate to talosintelligence.com.
2. Click **Support**.
3. Click **Content Categorization**.
4. Click **Cisco Login**.
5. Sign in with your cisco.com credentials.
6. Follow the onscreen instructions.

Procedure

Provides instructions for procedure. Navigate to talosintelligence.com. Click Support. Click Content Categorization. Click Cisco Login. Sign in with your cisco.com credentials.

Procedure

1. Navigate to talosintelligence.com.
2. Click **Support**.
3. Click **Content Categorization**.
4. Click **Cisco Login**.
5. Sign in with your cisco.com credentials.
6. Follow the onscreen instructions.

View Content Categories in Reports

Describes viewing content categories in reports. You can view information about content categories, such as requests that Secure Access blocked because of content categories.

You can view information about content categories, such as requests that Secure Access blocked because of content categories.

Prerequisites

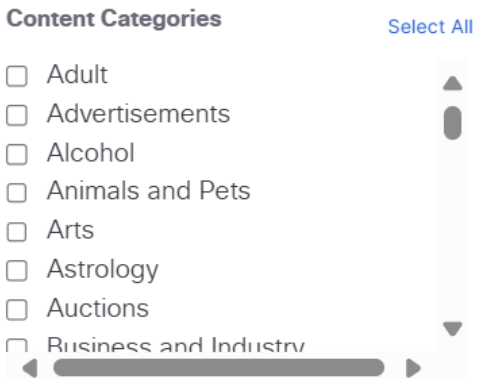
- A minimum user role of Read-only. For more information, see Manage Accounts.

View Content Categories in Activity Search Report

Provides instructions for viewing content categories in activity search report. Navigate to Monitor Activity Search . Scroll down to Content Categories and select your desired filters.

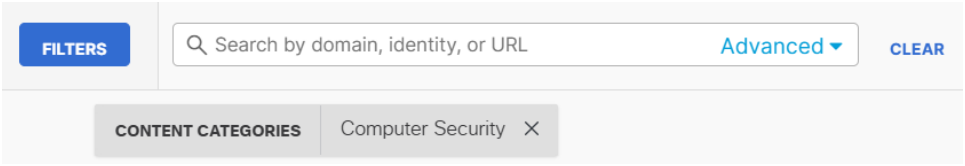
Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. Scroll down to Content Categories and select your desired filters.

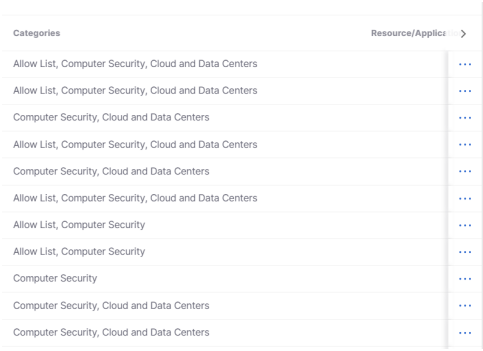


What to do next

Your filtered categories appear at the top of the report.



The Categories column of the report displays both legacy and new Talos content categories.

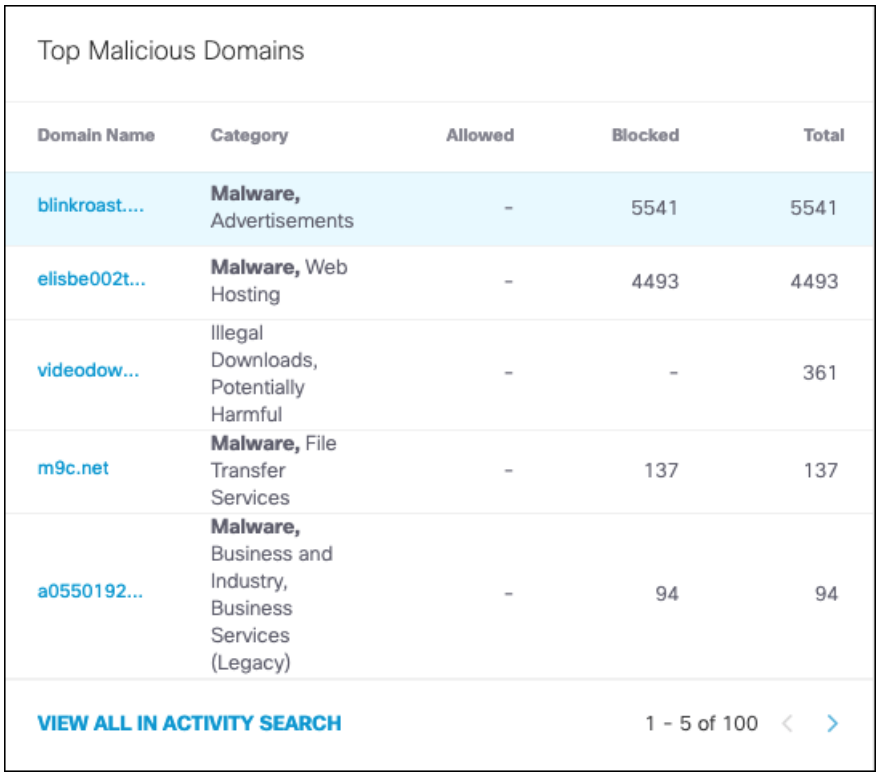


View Content Categories in Top Threats Report

Provides instructions for viewing content categories in top threats report. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Procedure

Navigate to **Monitor** > **Top Threats** > **Top Malicious Domains**.

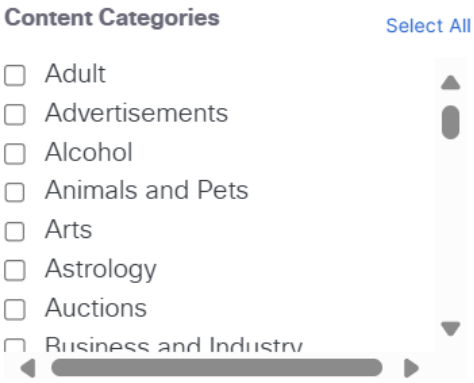


View Content Categories in Total Requests Report

Provides instructions for viewing content categories in total requests report. Navigate to Monitor Total Requests . Filter by content categories. Click Apply.

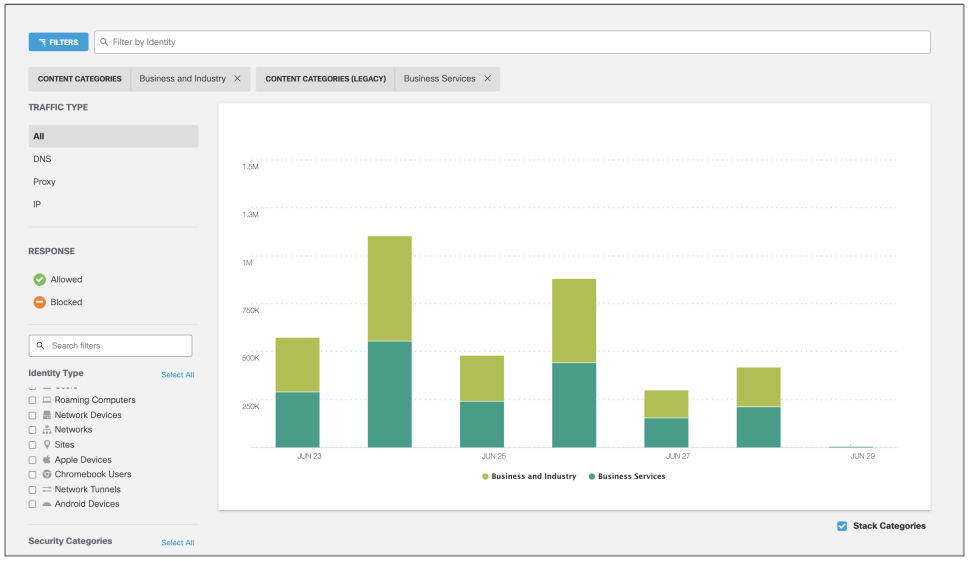
Procedure

1. Navigate to **Monitor** > **Total Requests**.
2. Filter by content categories. Click **Apply**.



What to do next

The graph displays data for the selected Talos content categories.



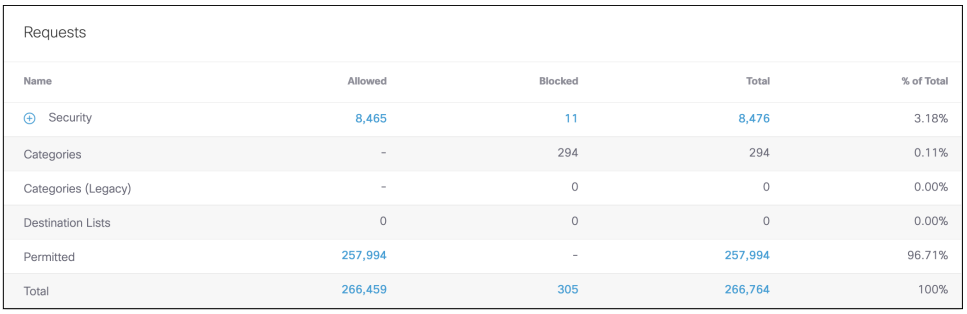
View Content Categories in Activity Volume Report

Provides instructions for viewing content categories in activity volume report. Navigate to Monitor Activity Volume . The table displays data for both the Talos content categories.

Procedure

Navigate to **Monitor** > **Activity Volume**.

The table displays data for both the Talos content categories.



Requests

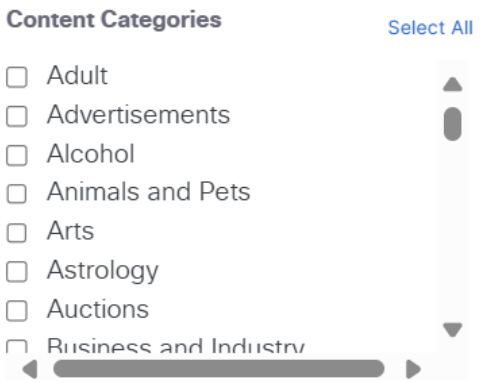
Name	Allowed	Blocked	Total	% of Total
Security	8,465	11	8,476	3.18%
Categories	-	294	294	0.11%
Categories (Legacy)	-	0	0	0.00%
Destination Lists	0	0	0	0.00%
Permitted	257,994	-	257,994	96.71%
Total	266,459	305	266,764	100%

View Content Categories in Top Destinations Report

Provides instructions for viewing content categories in top destinations report. Navigate to Monitor Top Destinations . Filter by content categories. The category column of the report displays the Talos content categories.

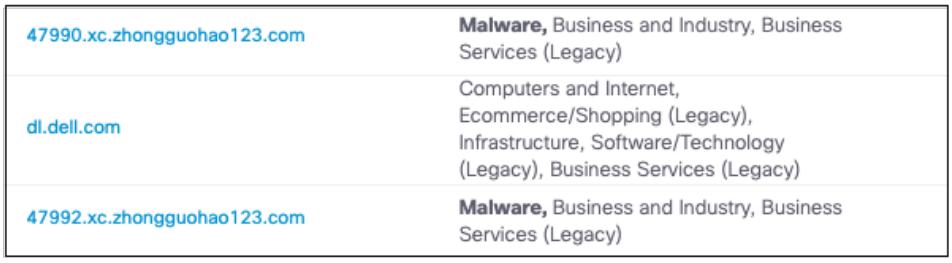
Procedure

1. Navigate to **Monitor** > **Top Destinations**.
2. Filter by content categories.



What to do next

The category column of the report displays the Talos content categories.



47990.xc.zhongguohao123.com	**Malware,** Business and Industry, Business Services (Legacy)
dl.dell.com	Computers and Internet, Ecommerce/Shopping (Legacy), Infrastructure, Software/Technology (Legacy), Business Services (Legacy)
47992.xc.zhongguohao123.com	**Malware,** Business and Industry, Business Services (Legacy)

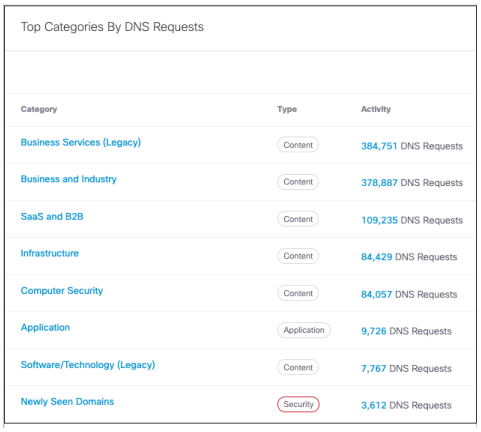
View Content Categories in Top Categories Report

Provides instructions for viewing content categories in top categories report. Navigate to Monitor Top Categories . The category column of the report displays the Talos content categories.

Procedure

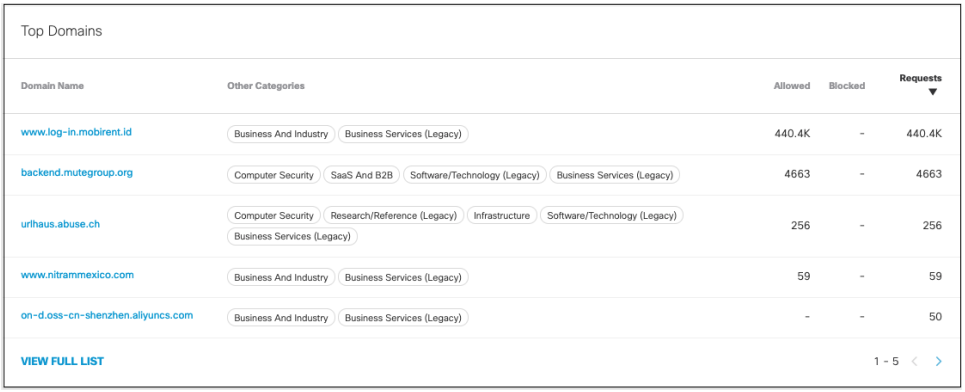
1. Navigate to **Monitor** > **Top Categories**.

   The category column of the report displays the Talos content categories.



2. Click a category to see its details.

   - If you scroll down to **Top Domains,** in the Other Categories column, you can see the Talos content categories among the categories.



24 Manage Tenant Control Profiles

Topics:

- Add a Tenant Controls Profile
- Control Cloud Access to Microsoft 365
- Control Cloud Access to Google G Suite
- Control Cloud Access to Slack
- Control Cloud Access to Dropbox
- Use Tenant Controls in Access Rules
- Review Tenant Controls Through Reports

Introduces managing tenant control profiles. Secure Access tenant controls allow you to provision connectivity for users to certain SaaS applications in the cloud. When configured, access is limited to only those resources that are approved for your organization.

Secure Access tenant controls allow you to provision connectivity for users to certain SaaS applications in the cloud. When configured, access is limited to only those resources that are approved for your organization. The result is that your organization is protected and secure when users and devices reach resources in the cloud that are running on shared domain names.

Secure Access supports tenant controls for the following platforms:

- Microsoft 365
- Google G Suite
- Slack
- Dropbox

You create tenant control profiles for one or more applications.

To use a tenant control profile in an access rule, see Use Tenant Controls in Access Rules.

Add a Tenant Controls Profile

Provides instructions for adding a tenant controls profile. Secure Access tenant controls allow you to provision connectivity for users to the following SaaS applications and suites in the cloud:

Secure Access tenant controls allow you to provision connectivity for users to the following SaaS applications and suites in the cloud:

- Dropbox
- Microsoft 365
- Google G Suite
- Slack

You configure tenant controls as profiles that you can use in one or more internet-access rules. Each tenant-controls profile can include more than one type of application or suite. For example, you can create a single profile that includes configurations for both Microsoft Office 365 and Slack.

Before you begin

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

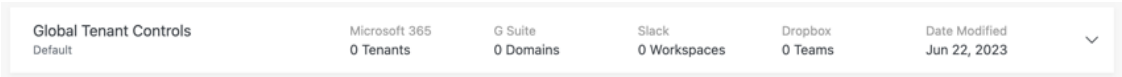
The following data is required to configure tenant controls and allow access to cloud-based applications and suites:

- **Microsoft 365**–**Tenant Domain** and **Tenant Directory ID**. See Azure Active Directory documentation.
- **Google Workspace**–**Domains**. See **Use a web proxy server to block accounts** in Google Workspace Admin Help.
- **Slack**–**Workspace ID**. See Approve Slack workspaces for your network.
- **Dropbox**–Team Name and Team ID. For information about the Team ID and how to find it using Dropbox developer tools, see Dropbox for HTTP developers. Choose the Team Name to provide a mnemonic identifier for the team.

For more information, see the application's documentation or contact the application's Support.

Procedure

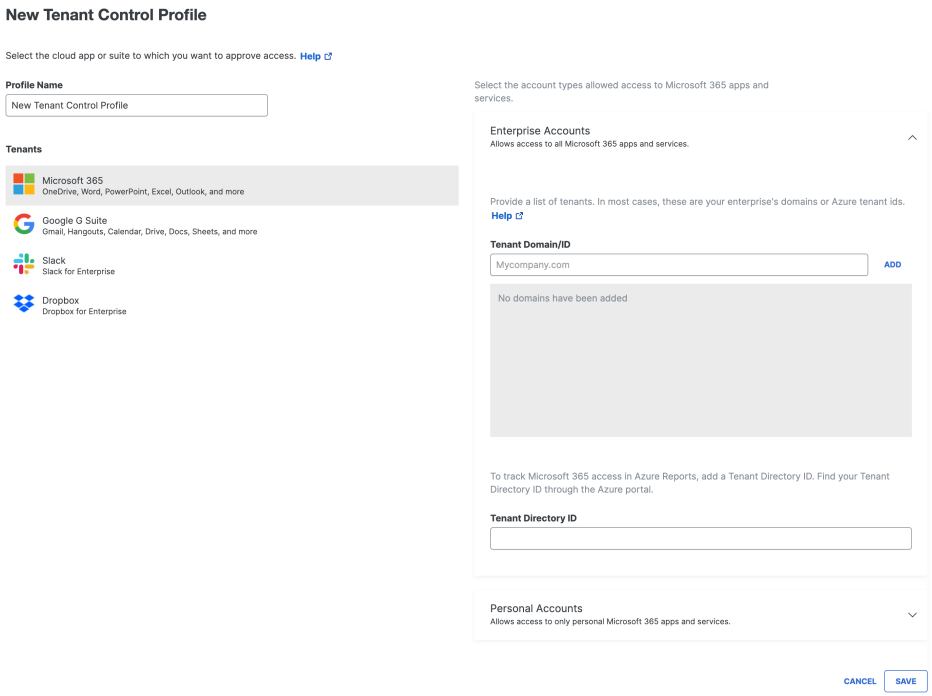
1. Navigate to **Resources** > **Internet and SaaS Resources.**
2. Click **Tenant Controls.**.
3. Click the default **Global Tenant Controls** profile.
   a. Alternatively, click **Add**



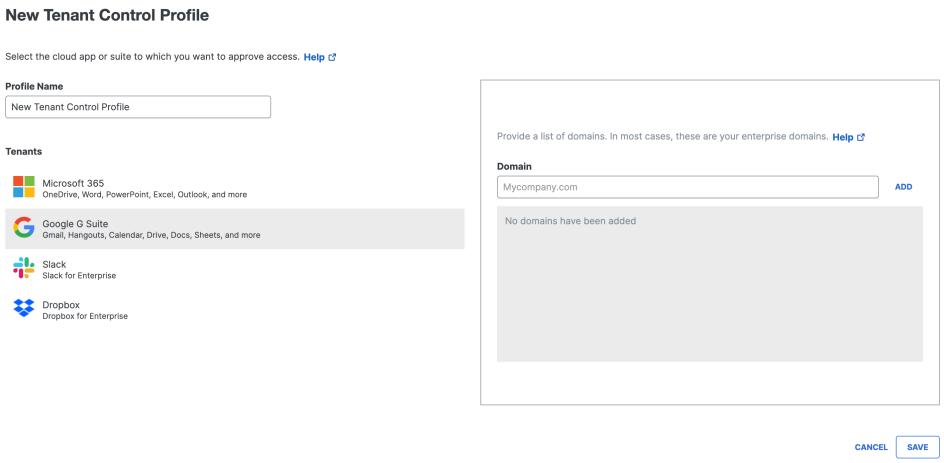
4. Give your configuration a descriptive **Profile Name**.
5. Select a tenant.
6. In the right pane, add specific data and domain information to grant access to those tenants from within your organization.

   If you aren't sure what information to enter for a tenant, see the application's documentation or contact the application's support.

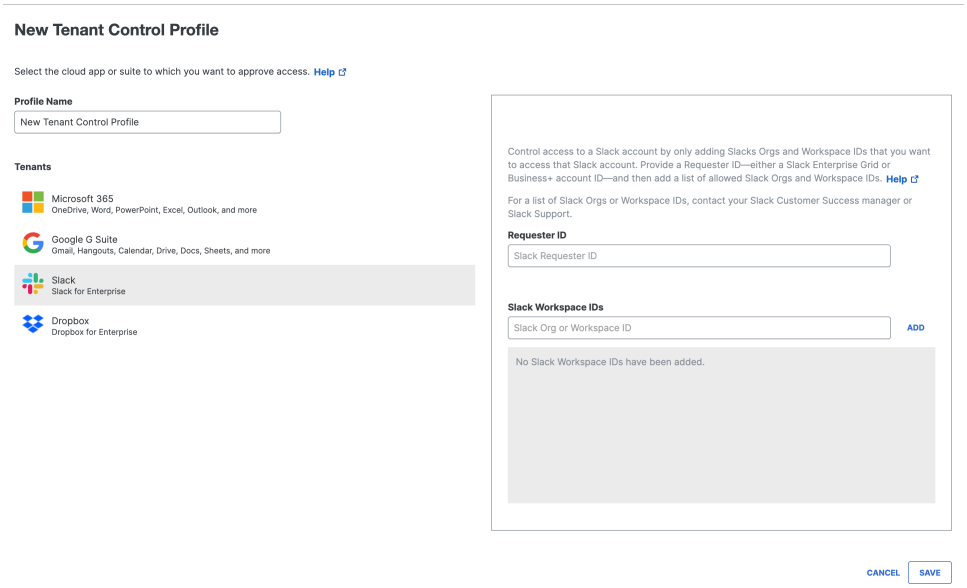
- **Microsoft 365–Tenant Domain** and, optionally, **Tenant Directory ID**. See also, Azure Active Directory documentation.



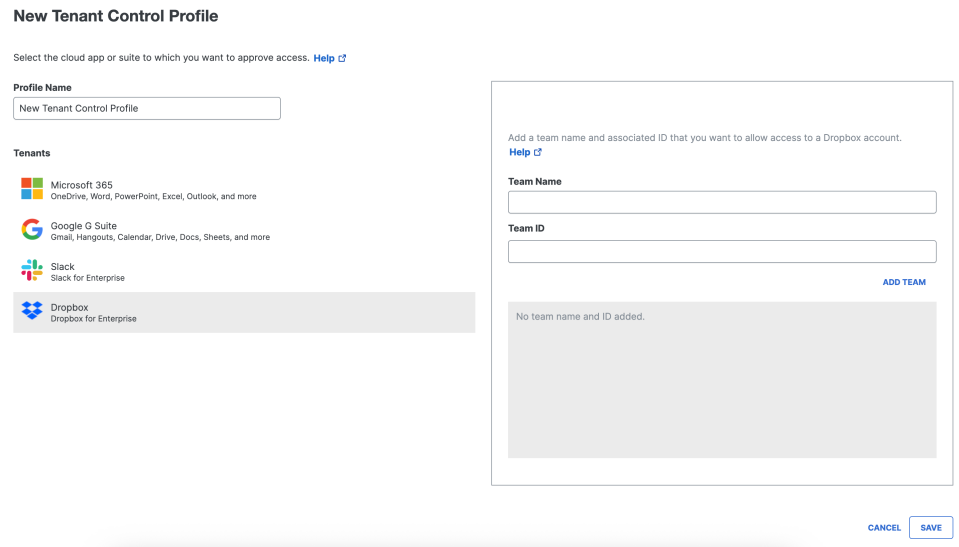
- **Google G Suite–Domain**. Scroll to "Use a web proxy server to block accounts" in G Suite Admin Help.



- **Slack–Workspace ID**. See also, Approve Slack workspaces for your network.



- **Dropbox – Team Name** and **Team ID**, see Dropbox documentation for network control.



7. After you've configured access to applications, click **Save**.

What to do next

Result: The new tenant-control profile is now available for selection in the Security Controls section when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to Microsoft 365

Provides instructions for control cloud access to microsoft 365. Its purpose, requirements, and key details for Cisco Secure Access administrators.

Use a tenant-control profile to manage access to the cloud-based application Microsoft 365. Once added, you can select the profile in an internet-access rule.

Before you begin

Microsoft 365 requires the following data to configure tenant controls for access to the cloud-based application:

- **Tenant Domain**
- **Tenant Directory ID**

For more information about this data and how to acquire it, see Azure Active Directory documentation.

The Microsoft 365 Compatibility feature exempts Microsoft 365 traffic from inspection and policy enforcement, allowing it to pass through Secure Access unaltered. When you configure tenant controls for Microsoft 365, Secure Access decrypts these Microsoft login domains (**login.microsoftonline.com**, **login.microsoft.com**, and **login.windows.net**) for the purpose of tenant enforcement.

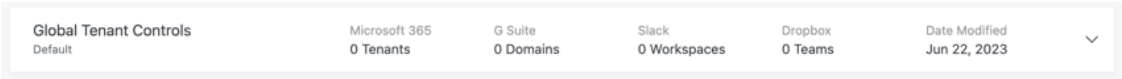
For more information, see the official Microsoft documentation and Microsoft 365 Compatibility.

> **Note**
>
> Microsoft 365 tenant restrictions do not block personal or consumer accounts, such as Hotmail or Outlook.

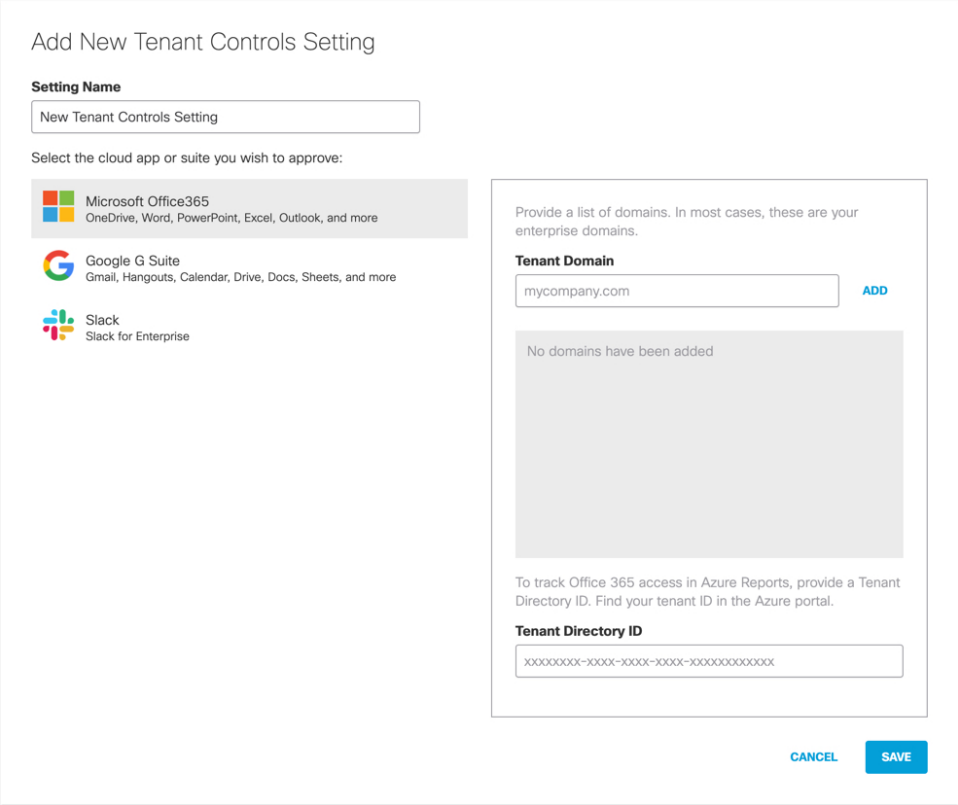
Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources.**
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

> **Note**
>
> Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.



4. Give your configuration a descriptive **Profile Name** and select **Microsoft 365**.



5. To grant access to Microsoft 365 from within your organization:

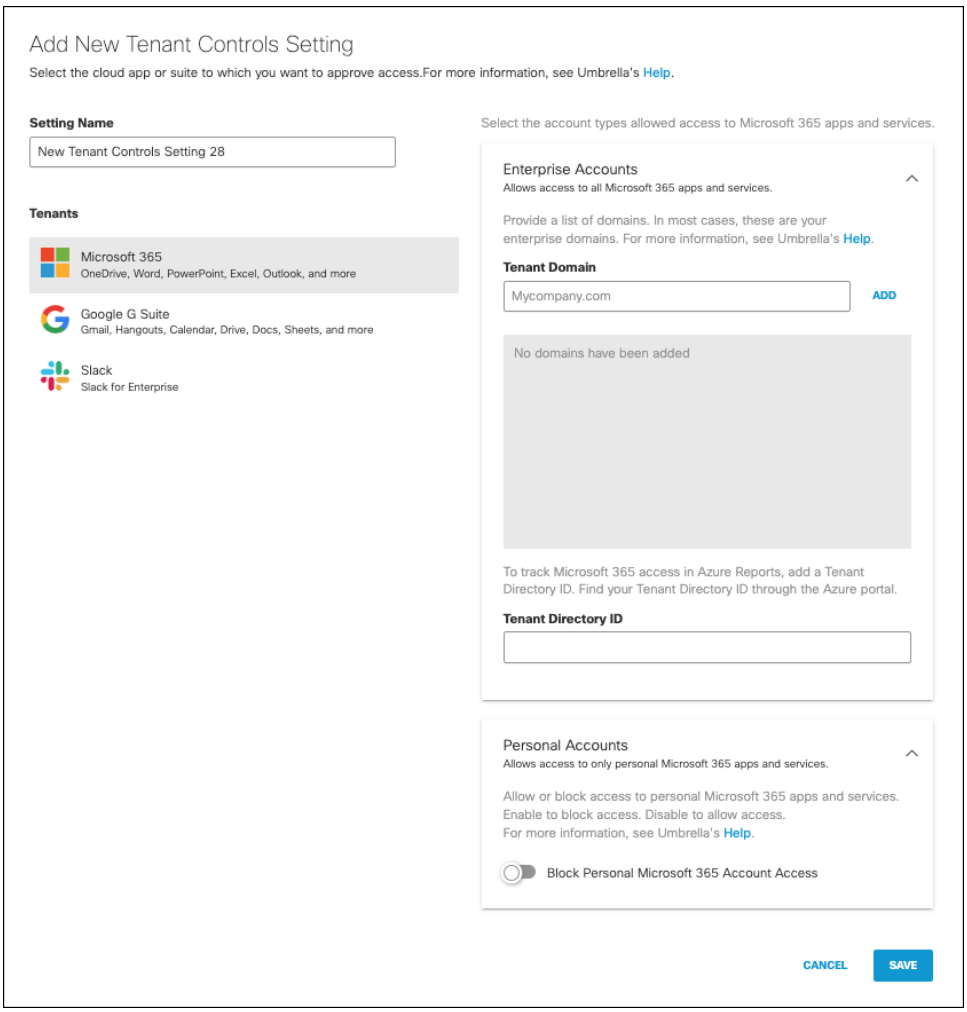
   a. Add your organization's Microsoft 365 **Tenant Domain** and click **Add**.

   > **Note**
   >
   > You can add multiple Tenant Domains.

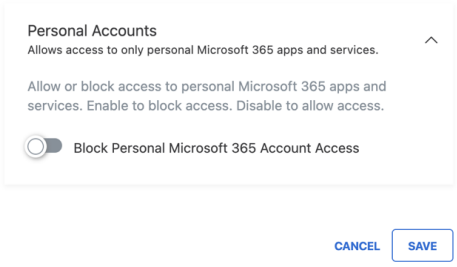
   b. Optionally, add your organization's **Tenant Directory ID** for Microsoft 365.

      This ID is used to track Office 365 access in Azure Reports.

      For more information about how to acquire the Tenant Directory ID, see Microsoft's documentation or contact Microsoft Support.



6. Optionally, click the toggle to Block Personal Microsoft 365 accounts.



7. Click **Save**.

> **Note**
>
> The new Tenant Controls profile is now available for selection when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to Google G Suite

Provides instructions for control cloud access to google g suite. Its purpose, requirements, and key details for Cisco Secure Access administrators.

The Secure Access tenant controls profile manages access to the cloud-based application Google G Suite. Once added, you can select this profile in an internet access rule.

Before you begin

The following Google G Suite specific data is required to configure Tenant Controls settings and allow access to to the cloud-based suite Google G Suite:

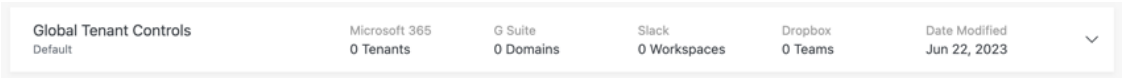
- **Domains**

  For more information about this data and how to acquire it, scroll to "Use a web proxy server to block accounts" in G Suite Admin Help.

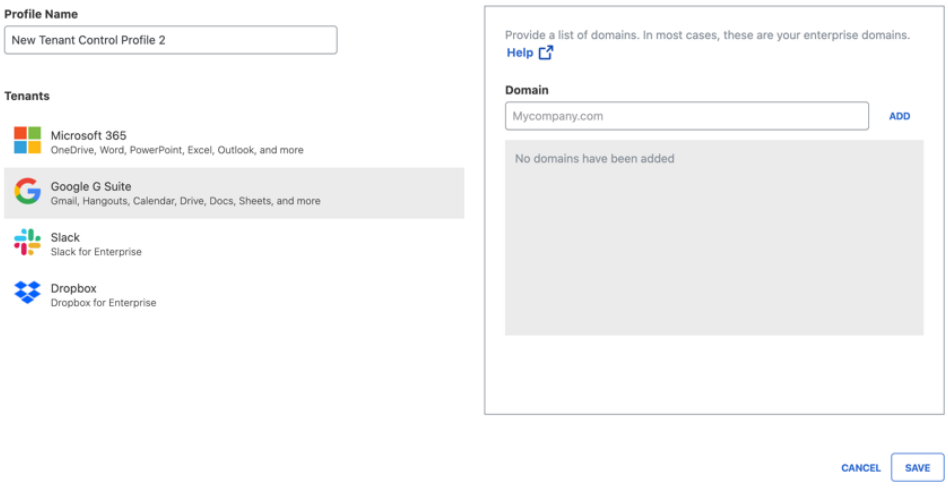
Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources**.
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

> **Note**
>
> Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.



4. Give your configuration a good descriptive **Profile Name** and select **Google G Suite**.



5. To grant access to Google G Suite from within your organization:
   a. Add an enterprise domain and click **Add**.

> **Note**
>
> You can add multiple domains.

6. Click **Save**.
   This new Tenant Controls setting is now available for selection when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to Slack

Provides instructions for control cloud access to slack. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

The Secure Access tenant controls profile manages access to the cloud-based application Slack.

Before you begin

Slack requires the following data to configure tenant controls for access to the cloud-based application:

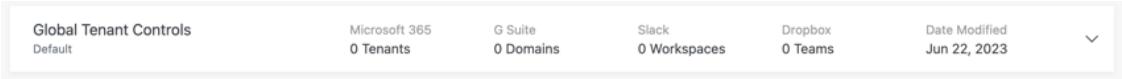
- **Workspace ID**
- **Requester ID** (for Business+ or Enterprise Slack Workspace ID)

For more information about this data, see Approve Slack workspaces for your network.

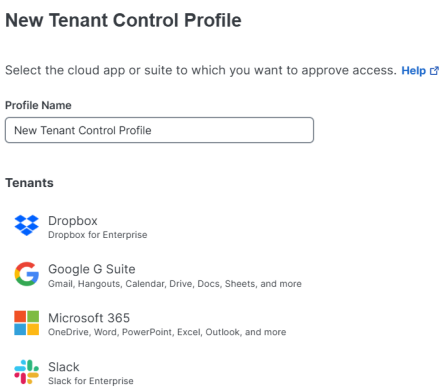
Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources.**
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

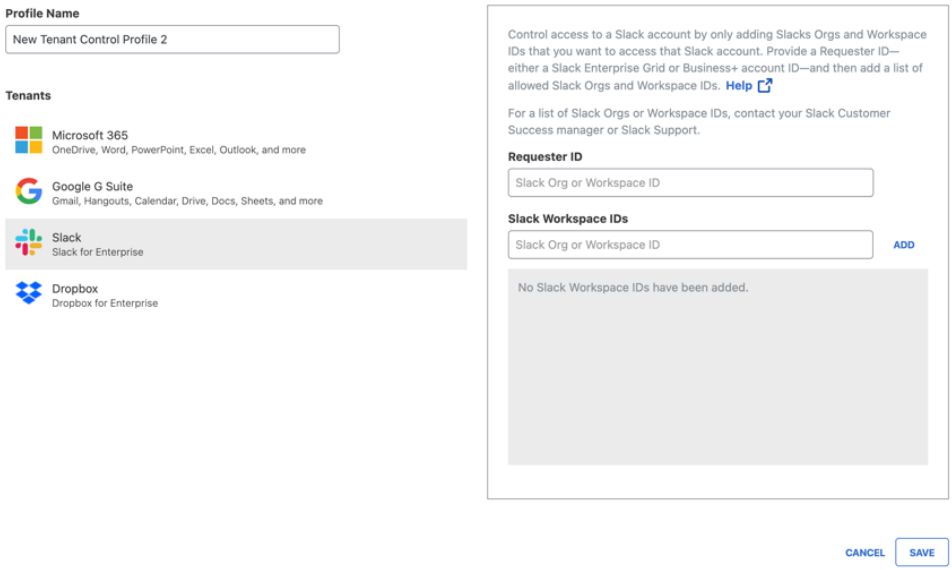
> **Note**
>
> Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.



4. Give your configuration a descriptive **Profile Name** and select **Slack**.



5. To grant access to Slack from within your organization:
   a. Enter a **Requester ID** and a **Workspace ID**. You can add multiple workspace IDs.



6. Click **Save**.

   The new tenant controls profile is now available when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

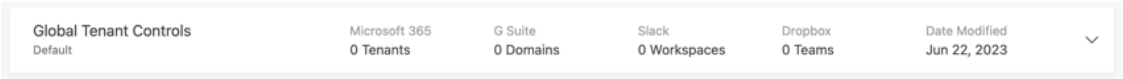
Procedure for Control Cloud Access to Slack

Provides instructions for procedure for control cloud access to slack.

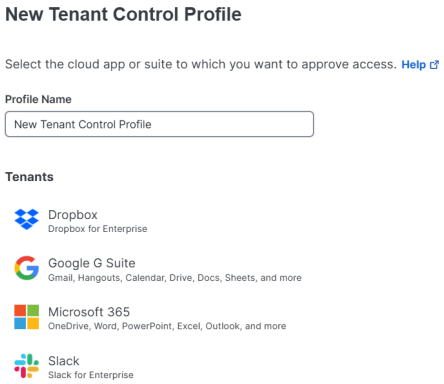
Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources.**
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

> **Note**
>
> Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.

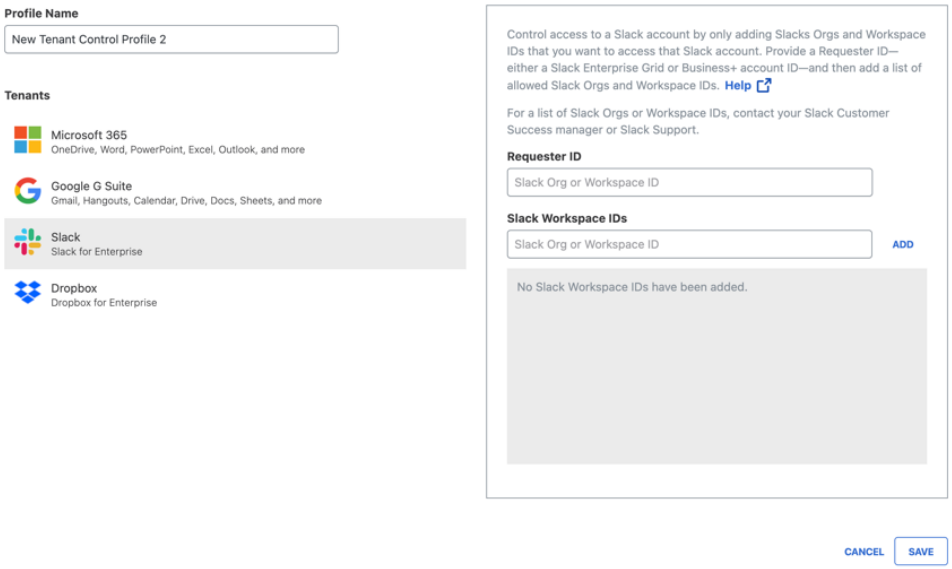


4. Give your configuration a descriptive **Profile Name** and select **Slack**.



5. To grant access to Slack from within your organization:

   a. Enter a **Requester ID** and a **Workspace ID**. You can add multiple workspace IDs.



6. Click **Save**.

   The new tenant controls profile is now available when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to Dropbox

Provides instructions for control cloud access to dropbox. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

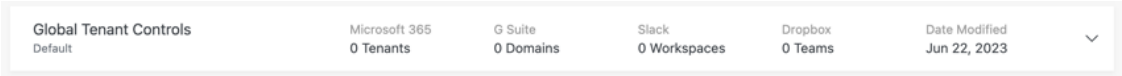
The Secure Access tenant controls profile manages access to the cloud-based application Slack.

Before you begin
Dropbox requires the following data to configure tenant controls for access to the cloud-based application.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources.**
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

> **Note**
>
> Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.



4. Give your configuration a good descriptive **Profile Name** and select **Dropbox**.
5. To grant access to Dropbox from within your organization:
   a. Enter a **Requester ID** and a **Workspace ID**. You can add multiple workspace IDs.
6. Click **Save**.

   The new Tenant Controls profile is now available when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Use Tenant Controls in Access Rules

Describes using tenant controls in access rules. To use tenant controls in internet-access rules: Add tenant control profiles for the applications that require such controls.

To use tenant controls in internet-access rules:

- Add tenant control profiles for the applications that require such controls.
- Decryption must be enabled for the rule. Make sure it is enabled in the security profile selected in the rule.
- The option to select a tenant control profile appears in the Security Controls section of the rule (after you choose destinations and then click Next.)

Review Tenant Controls Through Reports

Provides instructions for reviewing tenant controls through reports. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

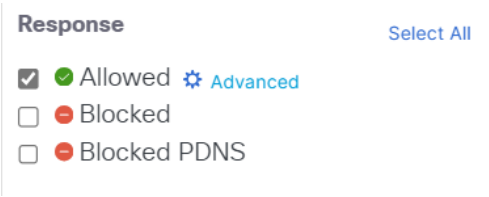
Use the Activity Search report to view identity activity when you're tracking attempts to access cloud-based applications that are controlled by the tenant-controls profile.

Before you begin

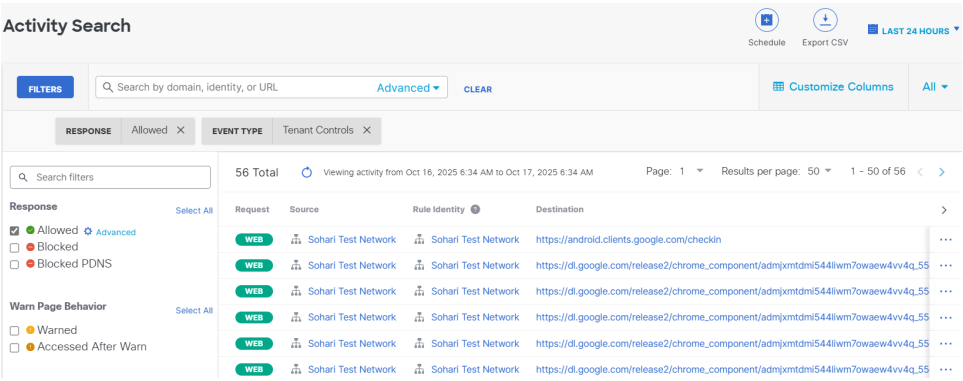
- A minimum role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. In the **Response** filter, select **Allowed** or **Blocked** or **Blocked PDNS**.



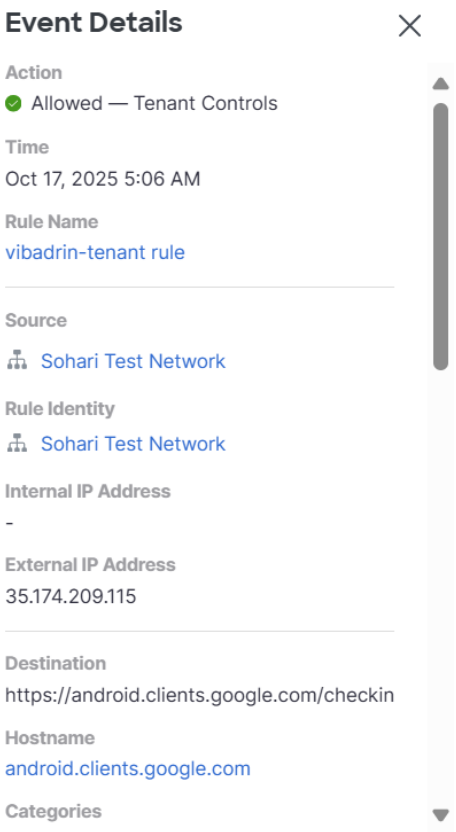
3. Under **Event Type**, select **Tenant Controls**.



Note

Since the blocking of tenants occurs at the vendor level, Secure Access displays tenant controls as Allowed in Activity Search.

4. To access detailed information about a tenant-control event, from the Action menu, choose **View Full Details**.


Event Details
Action
Allowed — Tenant Controls
Time
Oct 17, 2025 5:06 AM
Rule Name
vibadrin-tenant rule
Source
Sohari Test Network
Rule Identity
Sohari Test Network
Internal IP Address
-
External IP Address
35.174.209.115
Destination
https://android.clients.google.com/checkin
Hostname
android.clients.google.com
Categories

25 Manage Roaming Devices

Topics:

- View Internet Security Settings for Roaming Devices
- Edit Internet Security Settings for Roaming Devices
- Delete a Roaming Device

Introduces managing roaming devices. Cisco Secure Access Roaming Devices represent user devices that have deployed the Cisco Secure Client with the Umbrella Roaming Security module. The Cisco Secure Client syncs with Secure Access to manage the DNS and Web security on the device.

Cisco Secure Access Roaming Devices represent user devices that have deployed the Cisco Secure Client with the Umbrella Roaming Security module. The Cisco Secure Client syncs with Secure Access to manage the DNS and Web security on the device. As part of the sync, a Roaming Device resource is added to Secure Access. An administrator of the organization can apply policy rules to the Roaming Device resource. For more information about the Cisco Secure Client with the Umbrella Roaming Security module, see Manage Internet Security on Cisco Secure Client.

In Secure Access, you can view the Roaming Devices in the organization, edit the Internet Security settings for certain devices or all devices, override the Internet Security settings for the devices, and delete a Roaming Device.

- View Internet Security Settings for Roaming Devices
- Edit Internet Security Settings for Roaming Devices
- Delete a Roaming Device

View Internet Security Settings for Roaming Devices

Describes viewing internet security settings for roaming devices. A Roaming Device resource represents a user device that has deployed the Cisco Secure Client with the Umbrella Roaming Security module.

A Roaming Device resource represents a user device that has deployed the Cisco Secure Client with the Umbrella Roaming Security module.

The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices. The Umbrella Roaming Security module includes:

- DNS-layer security
- Web security

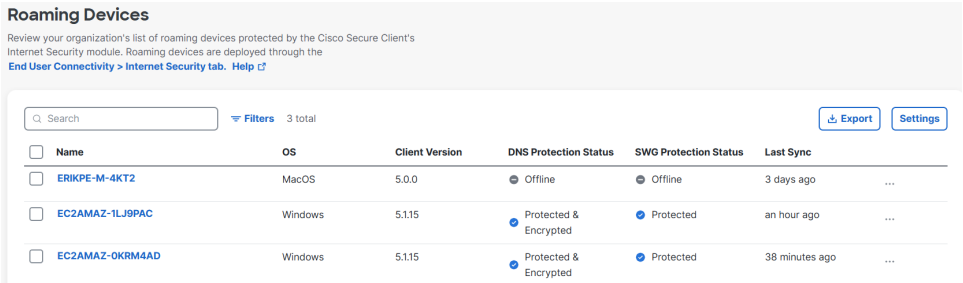
Once deployed, the Cisco Secure Client registers the user device with Secure Access. Cisco Secure Access adds the device to the list of Roaming Device resources managed by the organization. Cisco Secure Client syncs with Secure Access periodically and the device's DNS and web traffic is protected by the organization's policy rules. As an administrator, you can override, enable, or disable the internet security settings for the roaming devices in the organization.

Procedure for View Internet Security Settings for Roaming Devices

Provides instructions for procedure for view internet security settings for roaming devices. Navigate to Resources Roaming Devices . Click a device name to open the Roaming Device resource.

Procedure

1. Navigate to **Resources** > **Roaming Devices**.
2. Click a device name to open the Roaming Device resource.



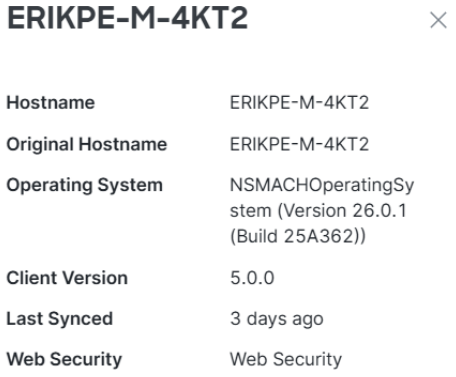
3. The Roaming Device resource displays the device's internet security details.

Host Information

Describes host information. Name–name of the device Hostname–hostname of the device Original Hostname–original hostname of the device

- **Name**–name of the device
- **Hostname**–hostname of the device
- **Original Hostname**–original hostname of the device
- **Operating System**–operating system and version
- **Client Version**–Version of Cisco Secure Client
- **Last Synced**–last date when Cisco Secure Client received a sync from Secure Access

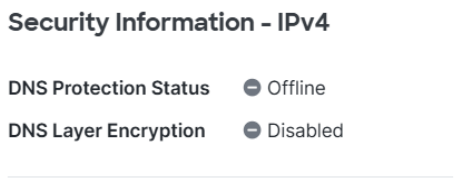
- **Web Security**–specifies whether Cisco Secure Client has internet security deployed



Security Information – IPv4

Describes security information - ipv4. DNS Protection Status–specifies the status of the DNS protection traffic on the roaming device. DNS-layer Encryption–specifies whether DNS-layer security with encryption is deployed.

- **DNS Protection Status**–specifies the status of the DNS protection traffic on the roaming device.
- **DNS-layer Encryption**–specifies whether DNS-layer security with encryption is deployed.



Edit Internet Security Settings for Roaming Devices

Describes editing internet security settings for roaming devices. The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices. The Umbrella Roaming Security module includes:

The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices. The Umbrella Roaming Security module includes:

- DNS-layer security
- Web security

The Cisco Secure Client default deployment enables DNS-layer security. You must activate the Secure Web Gateway (SWG) internet security settings in your instance of Secure Access.

Secure Access has various options to configure the Internet Security settings on Roaming Devices:

- Always enable the Secure Web Gateway settings for all Roaming Devices
- Always Override the Secure Web Gateway settings for all Roaming Devices
- Use the Secure Web Gateway settings in the default policy rule

Procedure for Edit Internet Security Settings for Roaming Devices

Describes procedure for edit internet security settings for roaming devices. You can override the internet security settings globally or disable the Cisco Secure Client Umbrella Roaming Security module on individual Roaming Devices.

You can override the internet security settings globally or disable the Cisco Secure Client Umbrella Roaming Security module on individual Roaming Devices. Unless configured, all devices follow the global settings for internet security in the Cisco Secure Client Umbrella Roaming Security module settings.

For example, in a scenario where there are 100 Roaming Devices and internet security is enabled globally, you have the option to override any of those 100 devices to disable internet security. However, if Secure Access internet security is disabled globally, the devices that are enabled through the override remain enabled.

Prerequisites

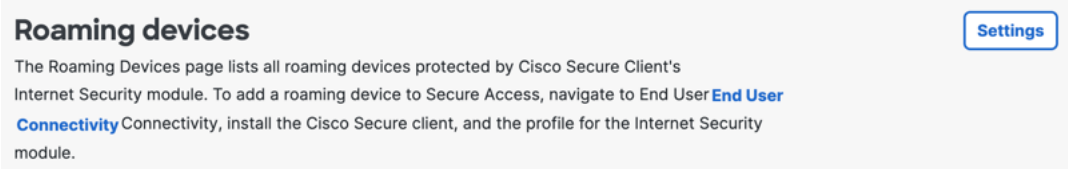
- Full Admin role in Secure Access. For more information, see Manage Accounts.

Edit the Auto-Delete Interval for Roaming Devices

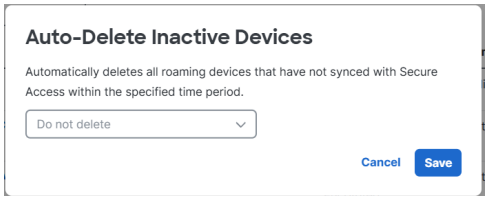
Provides instructions for editing the auto-delete interval for roaming devices. Navigate to Resources Roaming Devices . Click Settings to set the auto-delete interval setting.

Procedure

1. Navigate to **Resources** > **Roaming Devices**.
2. Click **Settings** to set the auto-delete interval setting.



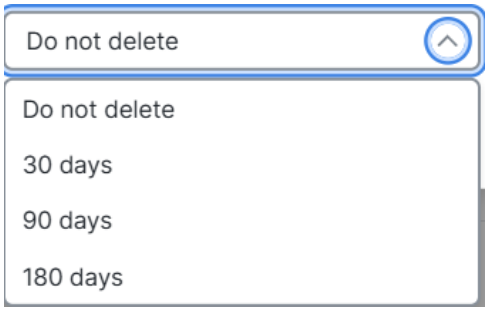
3. From the dropdown, choose **Do not delete** or the time period that the roaming devices must sync with Secure Access before the devices are deleted from the organization, and then click **Save**.



What to do next

The time intervals to sync roaming devices with Secure Access are:

- **Do not delete**–do not delete the Roaming Devices in the organization.
- **30 days**–delete the Roaming Devices in the organization if the devices have not synced with Secure Access in 30 days.
- **90 days90 days**–delete the Roaming Devices in the organization if the devices have not synced with Secure Access in 90 days.
- **180 days**–delete the Roaming Devices in the organization if the devices have not synced with Secure Access in 180 days.



Disable the Internet Security Settings

Provides instructions for disabling the internet security settings. Navigate to Resources Roaming Devices . Select the devices to disable the SWG setting.

Procedure

1. Navigate to **Resources** > **Roaming Devices**.
2. Select the devices to disable the SWG setting.
3. From the **Action** menu, select **Web Security**>**Always Disable (override)**.

What to do next

The SWG Agent displays as **Disabled** in the Roaming Computer's details. The SWG Agent only appears in the details when the override is used.

Enable the Internet Security Settings

Provides instructions for enabling the internet security settings. Navigate to Resources Roaming Computers . Select the devices for which you want to enable the SWG module. You can select up to 100 devices at a time on the page.

Procedure

1. Navigate to **Resources** > **Roaming Computers**.
2. Select the devices for which you want to enable the SWG module. You can select up to 100 devices at a time on the page.
3. From the **Action** menu, select **Web Security** > **Always enable (override)**.

> **Note**
>
> The Action menu does not appear until you select a device.

What to do next

The SWG Agent displays as **Enabled** in the Roaming Computer's details. The SWG Agent only appears in the details when the override is used.

Remove the Internet Security Override on Roaming Devices

Provides instructions for removing the internet security override on roaming devices. Its purpose, requirements, and key details for Cisco Secure Access administrators.

It is also possible to remove the SWG override and revert to the global setting. For example, in a scenario where 100 Roaming devices have SWG enabled globally, but 50 have been disabled through the override, those devices can have the override removed to revert back to the global setting.

Procedure

1. Navigate to **Resources** > **Roaming Computers**.
2. Select the devices for which you want to remove the SWG override. You can select up to 100 devices at a time on the page.

   > **Note**
   >
   > Select the checkbox at the top of the column to select all devices on the page.

3. From the **Action** menu, select **Web Security** > **Follow settings in End User Connectivity**. You can select up to 100 devices at a time on the page.

Delete a Roaming Device

Provides instructions for deleting a roaming device. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

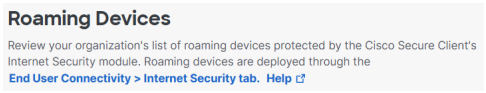
An administrator can delete a Roaming Device resource in Secure Access. Once deleted, the Roaming Device is removed from any Secure Access policy rules and is no longer protected by Secure Access.

Before you begin

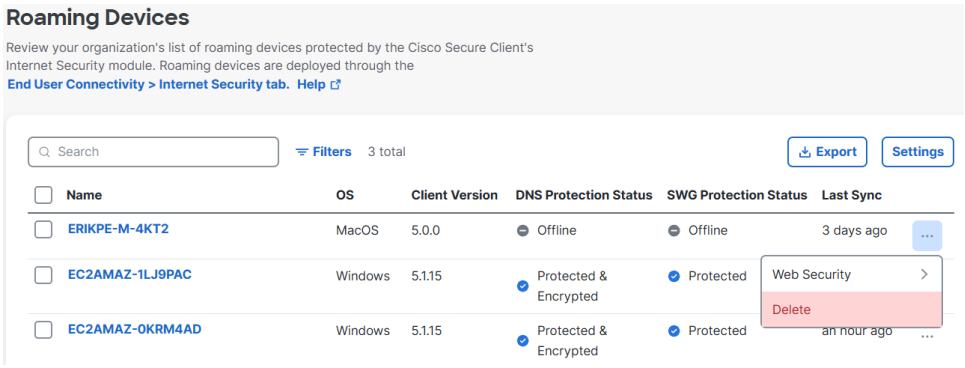
- Full Admin user role. For more information, see Manage Accounts.

Procedure

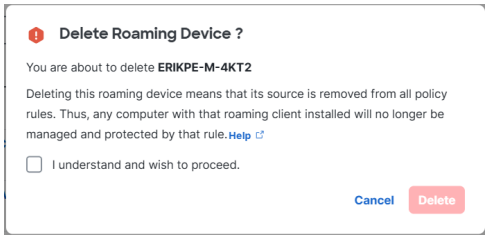
1. Navigate to **Resources** > **Roaming Devices**.

2. Click the ellipsis (**...**) to open the action menu, and then click **Delete**.



3. Check **I understand and wish to proceed**, and then click **Save**.



26 Manage Private Resources

Topics:

- Manage Private Resources

Describes the purpose and procedures for manage private resources and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Private Resources

Describes managing private resources. You can configure and add private resources to your organization. Private resources are applications, networks, or subnets that your organization controls. These resources are not publicly accessible from outside your network, such as:

You can configure and add private resources to your organization. Private resources are applications, networks, or subnets that your organization controls. These resources are not publicly accessible from outside your network, such as:

- Applications and services that run on-premises in your data center
- Resources running on private clouds hosted from your data center

Step 1 – Configure Private Resources

Provides instructions for step 1 – configure private resources. Configure end user connections to a private resource, and then add a private resource to a private resource group.

Configure end user connections to a private resource, and then add a private resource to a private resource group.

Procedure

1. **Understand your connection options** Specify connection requirements for private resources where you want to allow access.
   - For more information, see Comparison of Zero Trust Access and VPN.
   - For more information, see Manage Branch Connections.
2. **Add Private Resources**
   - Work with resource owners to gather the information needed to configure each resource. For more information, see Add Private Resources.

Optional Configuration for Private Resources

Provides instructions for optional configuration for private resources. (Optional) Block zero-trust access to specified subdomains (Optional) Add Private Resource Groups

Procedure

1. **(Optional) Block zero-trust access to specified subdomains**
   If you configure a Private Resource with an IP address having a leading wildcard (for example: ***.example.com**), you can block zero-trust connections to subdomains that you specify.

   Note

   User devices must have the Cisco Secure Client deployed. For more information, see Using Wildcards to Configure Traffic Steering for Private Destinations.
2. **(Optional) Add Private Resource Groups**

To speed creation and management of access rules, and ensure consistent handling of related private resources, create groups of private resources that you want to manage as a unit. For more information, see Add Private Resource Groups.

Step 2 — Set Up Network Connections, VPN Profiles, and Certificates

Provides instructions for step 2 – set up network connections, vpn profiles, and certificates. Configure network connectivity for zero-trust connections Add Network Tunnel Groups.

Procedure

1. **Configure network connectivity for zero-trust connections** Add Network Tunnel Groups.

   To allow Secure Access to communicate with and direct traffic to your private resources. For more information, see Manage Network Connections.
2. **Add VPN profiles** To allow VPN connections to private resources, add VPN profiles to your organization. VPN configurations such as VPN traffic steering rules must exist for the applicable network address spaces. For more information, see Manage Virtual Private Networks.
3. **Add and manage certificates for private resources** Secure Access requires certificates in order to connect user traffic with your private resources and decrypt that traffic for inspection by the Intrusion Prevention System (IPS). You can upload the certificate for a resource when you configure the resource, or manage certificates from the certificate list. For more information, see Certificates for Private Resource Decryption.

Step 3 — Add Private Resources in Private Access Rules

Provides instructions for step 3 – add private resources in private access rules. Add private access rules After you add private resources to your organization, these resources are available for you to use as destinations in your private access rules.

Procedure

Add private access rules After you add private resources to your organization, these resources are available for you to use as destinations in your private access rules. Add private access rules that define which users and devices can access the private resource in the organization. For more information, see Add a Private Access Rule.

Step 4 — Set Up the Cisco Secure Client and Distribute URLs

Provides instructions for step 4 – set up the cisco secure client and distribute urls. Ensure that user devices are set up for client-based Zero Trust Access To configure resources for client-based zero-trust access, ensure that user devices meet the requirements for Zero Trust.

Procedure

1. **Ensure that user devices are set up for client-based Zero Trust Access** To configure resources for client-based zero-trust access, ensure that user devices meet the requirements for Zero Trust. You must have the Cisco Secure Client Zero Trust Access module deployed on the devices in your organization. For more information, see Requirements for Cisco Secure Access with Zero Trust.

2. **Distribute URLs for browser-based Zero Trust Access** Establish a system for making users aware of the special URLs needed for browser-based Zero Trust Access.

Add a Private Resource

Provides instructions for adding a private resource. Configure a private resource to specify connection information for the resource, then configure access rules to determine which users and devices can access the resource using the connection methods you have enabled.

Private resources are the applications, networks or subnets that are internal resources hosted in your data center, including resources hosted on a private cloud in your data center, that have a login page that cannot be accessed from outside the network.

Configure a private resource to specify connection information for the resource, then configure access rules to determine which users and devices can access the resource using the connection methods you have enabled.

Configure a resource controlled by your organization.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Gather IP or CIDR addresses for your private resources.
- If you will specify resource addresses using domain names (FQDNs), you must add at least one internal DNS server that can route traffic to your resource. For more information, see Add DNS Servers.
- For each resource, you must choose connection options. For descriptions of the options, see the topics under Manage Connections to Private Destinations.
- To allow client-based Zero Trust Access and inspect traffic using the Intrusion Prevention (IPS) feature, you must provide the resource's certificate to Secure Access so that Secure Access can display it to end-user devices.

  Note

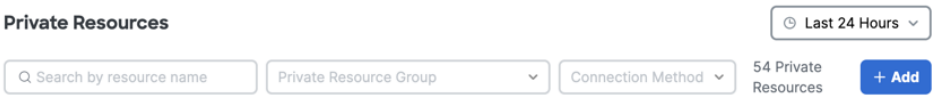
  For browser-based connections, the certificate must be signed by a publicly recognized certificate authority (CA).

- Plan your private resource configurations to avoid configuration conflicts such as duplicate or overlapping addresses.

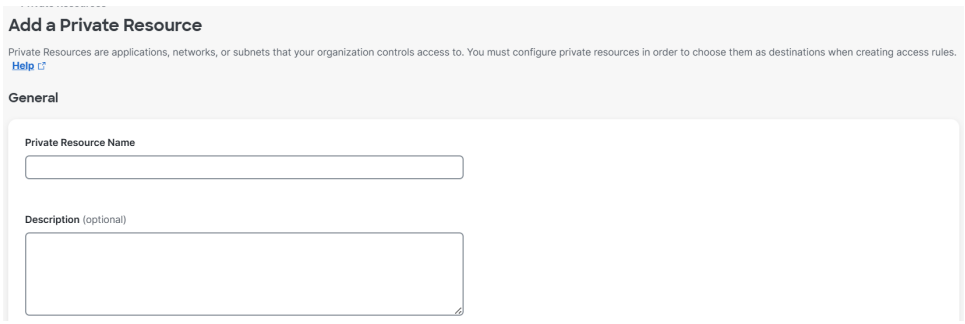
  For example, if a resource can be reached using multiple addresses, decide in advance whether you will create a single resource with multiple addresses or multiple resources.

Procedure

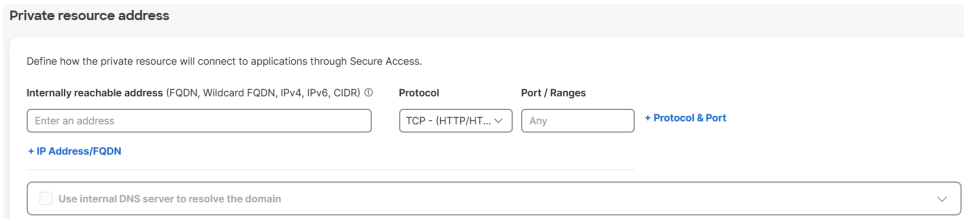
1. Navigate to **Resources** > **Private Resources**, choose **Private Resources**, and then click **+Add**.



2. For **Private Resource Name**, enter a meaningful name for the resource. For **Description**, we recommend that you provide information such as the purpose of the resource or the name of the resource owner.



3. Provide information for **Private resource address**.



For **Internally reachable address**, enter an IP address, FQDN, wildcard FQDN (in the format *.example.com), protocol, and port or port ranges.

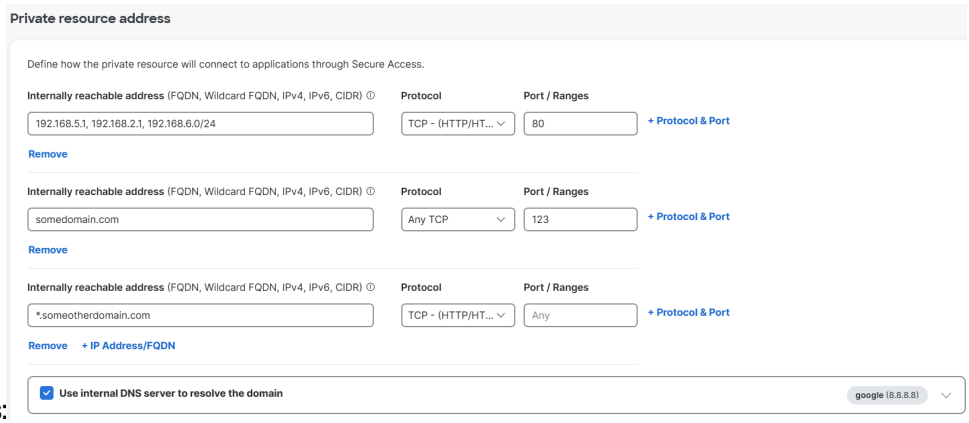
The address you provide does _not _ need to be publicly accessible from outside the network.

If you will allow browser-based access to this resource by users who do not have the Cisco Secure Client installed on their devices, the protocol you select must include HTTP/HTTPS.

Ensure that each address you add does not duplicate or overlap with addresses in other configured private resources.

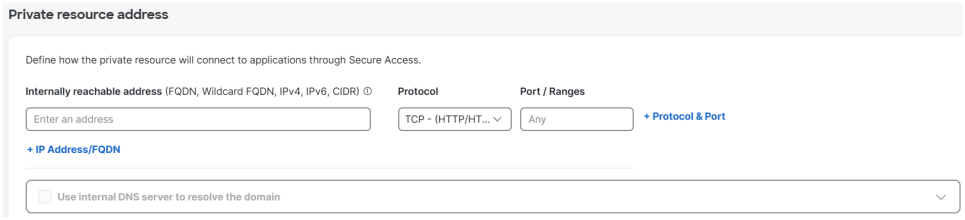
If you will decrypt traffic to this resource:

- In each address line, you can specify a single IP address (no address ranges) or CIDR block, or a comma-separated list of addresses or CIDR blocks, or an FQDN with or without wildcard. Add addresses and FQDNs as separate lines.
- If the address includes a wildcard FQDN, the wildcard must be the first character in the address string (*.example.com).
- Specify a single port or "Any" port; no comma-separated port numbers, no port ranges.
- If you need to decrypt traffic to multiple ports for the same address, click **+ IP Address/FQDN** and add a separate address line for each port.
- Select a protocol that includes TCP and does not include UDP.
- Exampleconfigurations:



If you have entered a domain and Secure Access will route traffic to this resource using a network tunnel:

- Select an internal DNS server that can route traffic to the specified resource address.
- To configure an internal DNS server, see Add DNS Servers.

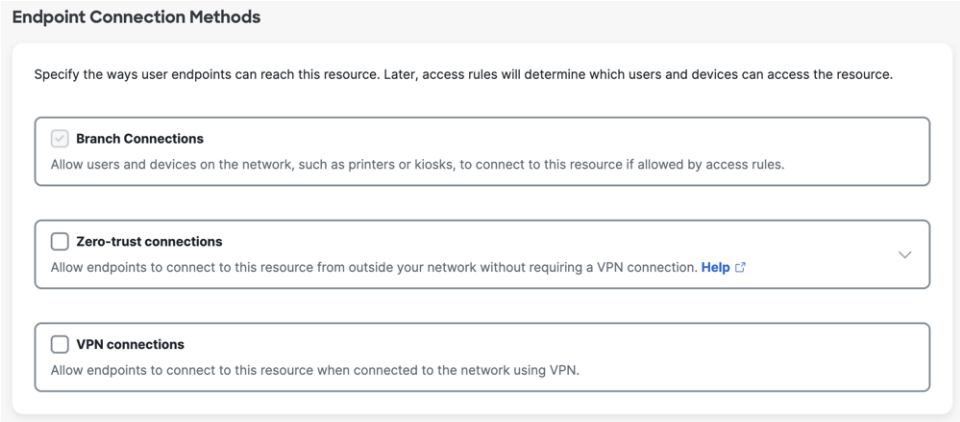


4. Choose which **Endpoint Connection Methods** to allow. Branch connections are configured for all private resources. For more information, see Manage Branch Connections.

   You can allow any or all of these options:

   - Zero-trust connections
     - for devices with the Cisco Secure Client installed.
     - for devices without the Secure Client (using a browser)
   - VPN connections

   For details, see Comparison of Zero Trust Access and VPN.



5. If you allow Zero Trust Access connections, choose whether to allow connections from devices with and without the Secure Client installed. You can allow either or both of these options.

   If you want mobile devices or devices that your organization does not manage (such as contractor, vendor, or Bring-Your-Own devices) to be able to connect to this resource, you must enable browser-based access.

   Browser-based (clientless) access offers fewer controls on device security than client-based access does.

6. If you allow Client-based Zero Trust Access connections:

   Enter the address you want users to use in order to connect to this resource.

   For best security (to keep the internal IP address of this resource private), you should provide a domain rather than an IP address. Your internal DNS server must be able to route traffic to this address. For example, you can enter *mail.example.com*.

   This address can be the same as the address you entered above for Secure Access to connect to the resource.

7. If you allow Browser-based Zero Trust Access:

   - The protocol selected above for the connection to Secure Access must include HTTP/HTTPS in order to enable this option.

- Enter the publicly accessible address that you will give to users in order to access this resource.

  Specifically, you will enter a URL prefix that uniquely identifies this resource. Secure Access will join the prefix to *<your organization's tenant ID>-ztna.sse.cisco.io* to form the public URL address. You will give the entire URL to end users, and Secure Access will route traffic using this address to the resource.

  If you don't provide a URL prefix, Secure Access adds one for you, based on the resource name.

- This address will be reachable from outside your network, but the actual resource address is not exposed, offering safety if this address falls into unauthorized hands.
- You must provide this dummy address to end users.
- The certificate that the resource presents to end-user devices must be signed by a publicly recognized certificate authority (CA.)
- If you enable decryption in the next step, the option to **Validate application certificate** will be disabled. This is expected.

8. If you allow VPN connections:

   If you enable both Zero Trust connections and VPN connections, users will connect to the resource using zero trust.

9. For **Decryption**, enable **Decrypt Traffic**.

   Decryption is required in order to inspect traffic for threats using the intrusion prevention (IPS) feature. For security reasons, you should enable this option. You can enable this option depending on the resource address. For details, see information about the **Internally reachable address** field on this page.

   Because traffic is routed through Secure Access, Secure Access must be able to display the resource's certificate to end-user devices. If you have already uploaded the applicable certificate, select the certificate. Otherwise, upload or paste the device's certificate (public and private keys) here. Include all intermediate certificates in the certificate chain.

   If you enable decryption, the option to **Validate application certificate** for browser-based traffic will be disabled, even if you have previously enabled it. This is expected.

   > **Note**
   >
   > Only PEM encoding is supported.

Add a Private Resource Group

Provides instructions for adding a private resource group. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

You can create private resource groups with private resources and use these components as destinations in private access rules. Private resource groups enable you to apply access rules consistently to all resources in the group.

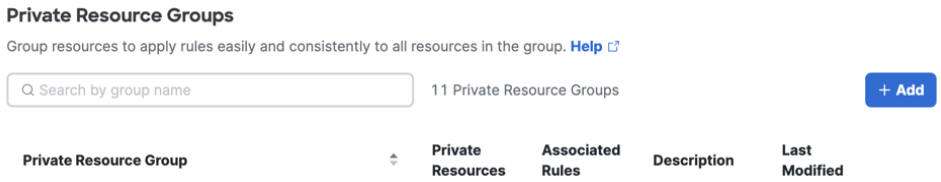
Configure a resource group with the private resources in your organization.

Before you begin

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

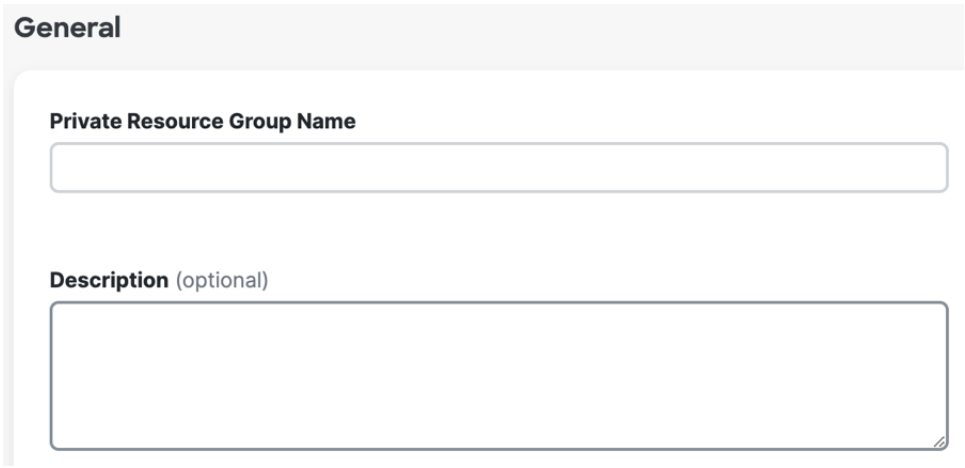
Procedure

1. Navigate to **Resources** > **Private Resources**, choose **Private Resource Groups**, and then click **+Add**.

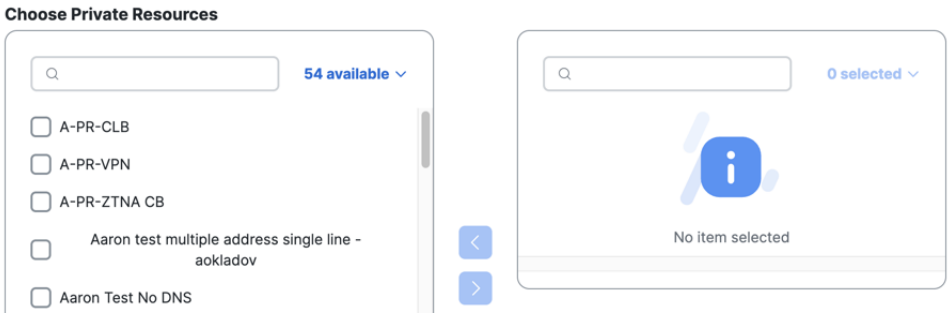


2. For **Private Resource Group Name**, enter a meaningful name for the resource group. For **Description**, we recommend that you provide information such as the purpose of the resource group.

> **Note**
>
> The description is optional.



3. For **Choose Private Resources**, add private resources to the group:
   a. For **Copy from existing private resource group**, choose a resource group name to add the resources in that group to your new resource group.
   b. For **Choose Private Resources**, check the resources and click the **arrow** (greater than sign) to add the selected resources to the group.



4. Click **Save**.

27 Manage Connections to Private Destinations

Topics:

- Comparison of Zero Trust Access and VPN
- Comparison of Client-Based and Browser-Based Zero Trust Access Connections
- Network Authentication for Zero Trust Access
- Manage Branch Connections

Introduces managing connections to private destinations. Secure Access supports several types of connections to private resources: Zero Trust Access—Sometimes called Zero Trust Network Access (ZTNA)Client-basedBrowser-based or clientless

Secure Access supports several types of connections to private resources:

- **Zero Trust Access**—Sometimes called Zero Trust Network Access (ZTNA)
  - **Client-based**
  - **Browser-based** or clientless
- **VPN**—Remote Access Virtual Private Network

For details, see:

- Comparison of Zero Trust Access and VPN and
- Comparison of Client-Based and Browser-Based Zero Trust Connections.

You will enable connection options for each private resource when you configure the resource. You can enable any or all of these options for each private resource.

If you enable both zero-trust and VPN connections for a resource, users will connect to the resource using zero trust.

Comparison of Zero Trust Access and VPN

Describes comparison of zero trust access and vpn. Zero Trust Access is Cisco's alternative to VPN for secure remote access connections to configured private resources.

Zero Trust Access is Cisco's alternative to VPN for secure remote access connections to configured private resources.

You can allow either or both connection methods for each private resource.

Zero Trust Access security benefits

- Remote users connect to specific private resources rather than to an entire network, minimizing risk surface area.
- You can allow authorized users of unmanaged devices to connect to specific resources without granting them access to your network. You will distribute a dummy URL to those users, so the real address is not exposed. This solution lets you securely provide browser-based access to end users such as:
  - contractors, vendors, trainers, outside legal counsel, etc.
  - employees on leave
- End-users' endpoint/device posture can be assessed each time they access a resource, rather than just once when they join the network.
- An attacker who breaches a device or zero-trust connection cannot glean information about your internal network
- Endpoint posture is evaluated continuously to verify that the end-user device meets requirements.
- Access to each resource is blocked unless access is granted.
- Simpler setup than VPN.

Zero Trust Access end user benefits

- Remote users can connect to internal resources in situations where they cannot use VPN. For example, an employee who is visiting a customer or vendor site can connect.
- Users do not need to log in separately to the network before they can access resources configured for zero trust access.
- After an end user with a managed device has completed initial setup of Cisco Secure Client, the user has the same experience accessing a resource whether in the office or working remotely.
- Faster performance than VPN

When to enable VPN

- To allow end users to connect to all resources on the network that are not configured to disallow VPN access.
- To enable connections to private destinations that are not configured as private resources.
- To enforce some endpoint requirements that are not currently available in client-based zero-trust posture profiles.
- While transitioning your organization to Zero Trust Access.
- For traffic that cannot be connected using Zero Trust Access, including traffic to the following types of applications:
  - Client-to-client traffic, for example peer-to-peer Voice Over IP (VOIP)
  - Server-to-client traffic, for example remote assistance
  - Applications that require a unique client IP address, for example those that use the SMBv1 protocol

- Applications that require SRV DNS records, for example Active Directory, Kerberos, or the Microsoft Configuration Manager
- Applications that perform an ICMP connectivity check before connecting using TCP or UDP

Comparison of Client-Based and Browser-Based Zero Trust Access Connections

Describes comparison of client-based and browser-based zero trust access connections. You can configure up to two ways for users to connect to private resources using Zero Trust Access:

You can configure up to two ways for users to connect to private resources using Zero Trust Access:

Client-based connections:

- The Cisco Secure Client is installed on the end-user device.
- Users can access using any protocol.
- Users access using the internal resource address you specify in the Private Resource.
- The client-based posture profile offers more options for controlling endpoint (device) requirements than the browser-based posture profile offers.
- You can block access to specified subdomains when the resource address for client-based connections is configured as a wildcard FQDN.
- If traffic is blocked, the user sees a Block page if all requirements are met.

  See Block pages for Private Resources.

Browser-based connections:

- Access does not require a client installed on the user endpoint device.
- Use this option to allow access from devices with an operating system that the client does not support.
- You can enable this option for private resources to allow connections from users who do not have managed devices, such as contractors, vendors, and others with bring-your-own (BYOD) and mobile devices. You do not need to install anything on such devices.
- Access is solely via browser.
- Users access private resources using a dummy URL that does not expose your actual resource address. Secure Access redirects browser-based traffic to the actual resource if access rules allow the traffic.
- You can specify endpoint (device) requirements for these connections, but fewer than in the client-based posture profile.
- If traffic is blocked, the user sees only a standard browser error. This prevents bad actors from obtaining information about your resources.

Network Authentication for Zero Trust Access

Describes network authentication for zero trust access. In addition to any other authentication requirements you configure, you can require end users to re-authenticate themselves at an interval that you choose before they can connect to private resources using Zero Trust Access.

In addition to any other authentication requirements you configure, you can require end users to re-authenticate themselves at an interval that you choose before they can connect to private resources using Zero Trust Access.

End users need to sign in only once during the interval you specify; after signing in, users can connect to any private resources that are enabled for Zero Trust Access, when rules allow access. When the interval ends, users must sign in again to regain Zero Trust Access to allowed private resources for the specified period of time.

You will want to balance security needs with end-user convenience. For example, for most applications, you may want to require that users re-authenticate about once per day, while for sensitive applications, you may want to require re-authentication as often as hourly.

The interval specified on the Rule Defaults page is used by default for all new private access rules. To set or change the default interval, see Important Information About Changing Rule Defaults and Edit Rule Defaults and Global Settings.

For each private access rule that includes at least one private resource as a destination, you can choose to use the default interval or specify a different interval. See Add a Private Access Rule.

These authentication options are in addition to any sign-in requirements required by mechanisms outside of Secure Access, such as those required to access individual resources.

If you disable this authentication option, users are never prompted to sign in again after they have authenticated once.

To require re-authentication for every session, enable the option and set the interval to 0 days, 0 hours, 0 minutes.

Manage Branch Connections

Describes managing branch connections. Secure Access protects users and devices that are connected on an organization's branch and internal networks. An enterprise may have multiple branch offices distributed across various geographical locations.

Secure Access protects users and devices that are connected on an organization's branch and internal networks. An enterprise may have multiple branch offices distributed across various geographical locations. Each branch office may allow connections only to certain applications and services managed by the organization and block connections to other private resources.

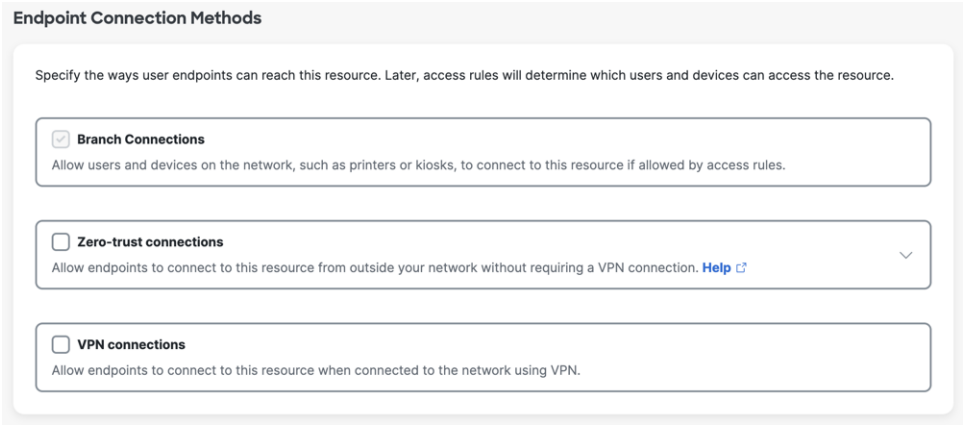
When on a branch network protected by Secure Access, users and devices can connect seamlessly to the internet and private applications and services. You can control how users and devices connect to private resources by adding private access policy rules for network sources and destinations. For example, you can define policy rules that block or allow access to private resources from IOT devices, kiosks, or printers.

Endpoint Connection Methods

Describes endpoint connection methods. Secure Access supports various types of network connections to private resources: Branch connections Zero-trust connections VPN connections

Secure Access supports various types of network connections to private resources:

- **Branch connections**
- **Zero-trust connections**
- **VPN connections**



When you add a private resource to Secure Access, Secure Access automatically enables **Branch Connections** to the private destination. For information about Zero Trust and VPN connections, see Manage Connections to Private Destinations.

A Branch network may represent an IP or CIDR address of a router or device in your enterprise. You can configure Branch networks to connect through a Network Tunnel Group to a private resource. For more information about Network Tunnel Groups, see Manage Network Tunnel Groups.

Branch Networks in Private Access Rules

Describes branch networks in private access rules. Once you add a private resource to Secure Access for your organization, you can configure private access rules that protect the branch connections to your private resources. A private access rule may include branch networks in both source and destination components.

Once you add a private resource to Secure Access for your organization, you can configure private access rules that protect the branch connections to your private resources. A private access rule may include branch networks in both source and destination components. For more information, see Add a Private Access Rule.



Users and Groups Connections to Private Resources

Describes users and groups connections to private resources. Users, groups, and devices on your corporate networks, including branch offices, can always connect to a private resource if allowed by private access rules.

Users, groups, and devices on your corporate networks, including branch offices, can always connect to a private resource if allowed by private access rules. When users, groups, and user devices connect to private resources from a branch network, Secure Access does not evaluate the device's endpoint posture.

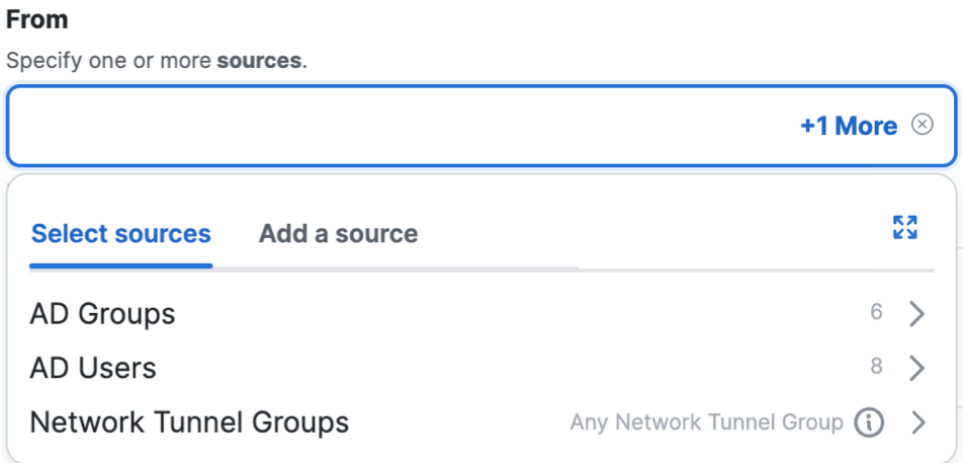
Sources for Branch Network Connections

Describes sources for branch network connections. In your private access rules, select the sources that you configured for your organization, or add individual branch or internal network IP or CIDR addresses. For more information, see Add a Private Access Rule: Sources.

In your private access rules, select the sources that you configured for your organization, or add individual branch or internal network IP or CIDR addresses. For more information, see Add a Private Access Rule: Sources.

- **Users**–Users appear in private access rules after you add them to your organization.
- **Groups**–Groups appear in private access rules after you add them to your organization.

- **Network Tunnel Groups**–Network Tunnel Groups appear in private access rules after you add them to your organization. The source is identified by the Network Tunnel Group ID.
- **IP** or **CIDR**–A branch or internal network's IP or CIDR address that you add to the access rule. The source is only available in the access rule.

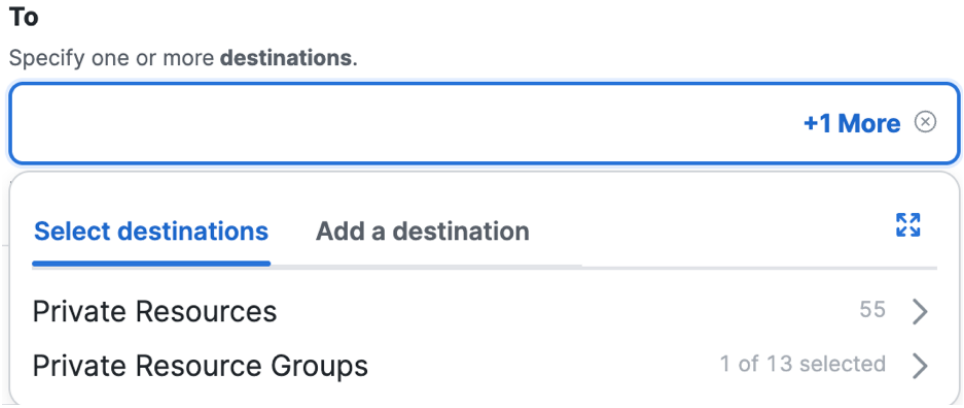


Destinations for Branch Network Connections

Describes destinations for branch network connections. In your private access rules, select the destinations that you configured for your organization, or add individual branch or internal network IP or CIDR addresses. For more information, see Add a Private Access Rule: Destinations.

In your private access rules, select the destinations that you configured for your organization, or add individual branch or internal network IP or CIDR addresses. For more information, see Add a Private Access Rule: Destinations.

- **Private Resources**–Private Resources appear in private access rules after you add them to your organization. The destination component is an IP, CIDR, fully-qualified domain name (FQDN), port, and protocol.
- **Private Resource Groups**–Private Resource Groups appear in private access rules after you add them to your organization. The destination component is an IP, CIDR, fully-qualified domain name (FQDN), port, and protocol.
- **IP** or **CIDR**, **Port**, **Protocol**–A branch or internal network's IP or CIDR address, port, and protocol that you add to the access rule. The destination is only available in the access rule.



Source Connections to Destinations

Describes source connections to destinations. Secure Access supports connections from Branch network source components to various destination components. Private Resource Group

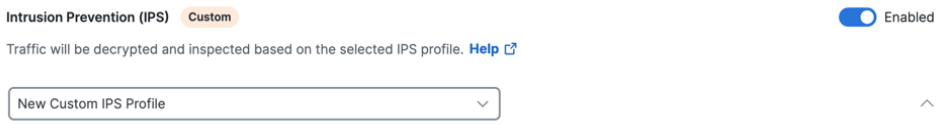
Secure Access supports connections from Branch network source components to various destination components.

Source	Private Destination
Network Tunnel Group	• Private Resource Group • Private Resource
IP or CIDR (Branch network) defined on the private access rule.	• Private Resource Group • Private Resource • IP or CIDR (Branch network) defined on the private access rule.
IP or CIDR (Internal network) defined on the private access rule.	IP or CIDR (Internal network) defined on the private access rule.

Add an IPS Profile on Private Access Rules

Describes adding an ips profile on private access rules. When you add a private access rule that includes branch connections to private resources, configure the security controls on the rule by adding an IPS profile. For more information, see Add a Private Access Rule: Configure Security Control Options.

When you add a private access rule that includes branch connections to private resources, configure the security controls on the rule by adding an IPS profile. For more information, see Add a Private Access Rule: Configure Security Control Options.



Secure Access protects branch connections to private resources, internal networks, and other branch networks through the Intrusion Prevention System (IPS) profile. For more information, see Manage IPS Profiles.

Log Connections From Branch Networks to Private Resources

Describes log connections from branch networks to private resources. Secure Access logs every connection and event from a branch network to a private application, service, internal network, or branch network. The events are recorded in the Admin Audit log.

Secure Access logs every connection and event from a branch network to a private application, service, internal network, or branch network. The events are recorded in the Admin Audit log. Secure Access enforces access to private applications and follows industry compliance and security standards. For more information, see Manage Logging.

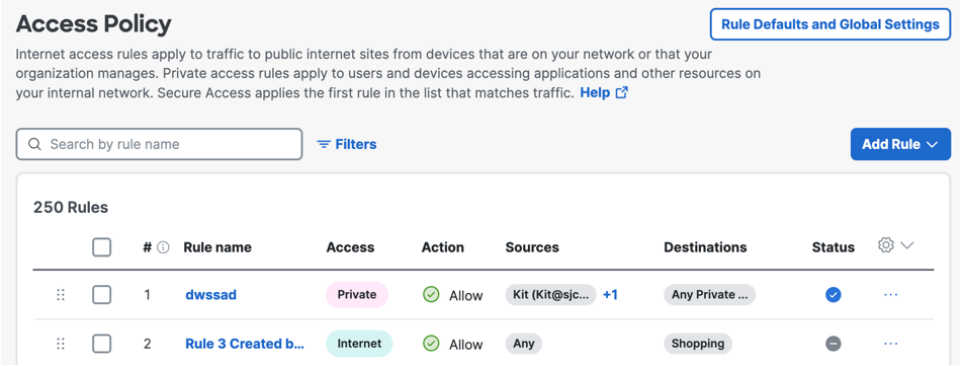
28 Manage the Access Policy

Topics:

- About the Access Policy
- Show Additional Data on Your Access Rules
- Edit the Order of the Rules in Your Access Policy
- Rule Defaults: Default Settings for Access Rules
- Global Settings for Access Rules
- Edit Rule Defaults and Global Settings
- Edit the Default Access Rules

Introduces managing the access policy. Secure Access has a single unified policy, which consists of policy rules and settings. Your private access and internet policy rules and the default policy rules control the access and security of your resources and protect the traffic in your organization.

Secure Access has a single unified policy, which consists of policy rules and settings. Your private access and internet policy rules and the default policy rules control the access and security of your resources and protect the traffic in your organization. Before you start adding rules to your policy, we recommend that you read through the topics in this section in full.



Private and Internet Access Rules in Your Policy

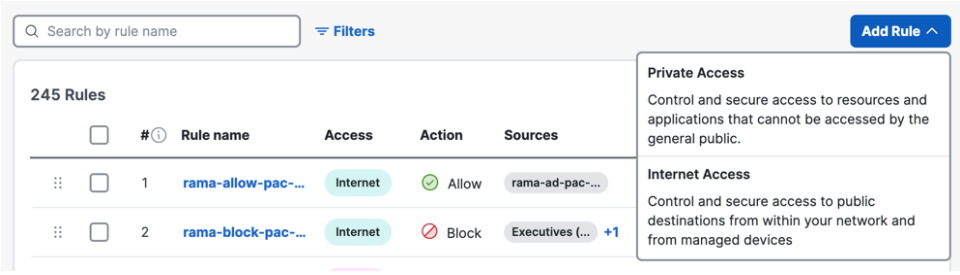
There are two types of access rules:

- **Private access rules**–Controls access to applications hosted from your data center and private clouds.

  To create and work with these rules, see Get Started with Private Access Rules.

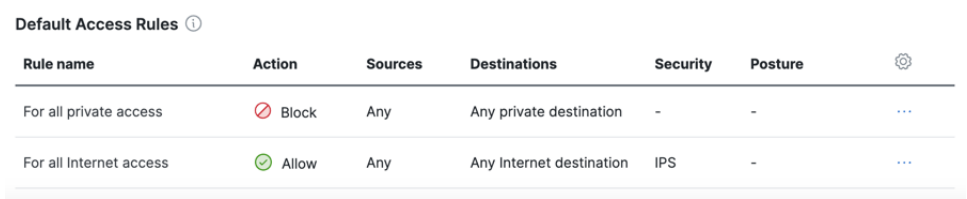
- **Internet access rules**–Controls access to resources on the internet from managed devices.

  To create and work with these rules, see Get Started with Internet Access Rules.



Default Access Rules in Your Policy

If your traffic does not match any of the rules in your policy, Secure Access applies the settings on the Default Access rules. For more information, see Edit the Default Access Rules.


Default Access Rules

Rule name	Action	Sources	Destinations	Security	Posture
For all private access	Block	Any	Any private destination	-	-
For all Internet access	Allow	Any	Any Internet destination	IPS	-

Rule Defaults and Global Settings

- For more information, see Global Settings for Access Rules.
- For more information, see Rule Defaults: Default Settings for Access Rules.

About the Access Policy

Describes about the access policy. The Cisco Secure Access policy is the collection of your internet and private access rules, rule defaults, and global settings. The policy displays your configured rule data and allows you to choose how to prioritize the rules in your policy.

The Cisco Secure Access policy is the collection of your internet and private access rules, rule defaults, and global settings. The policy displays your configured rule data and allows you to choose how to prioritize the rules in your policy. Once you add a rule, you can edit various components on the rule. You decide how to view and manage your rules that best meets your organization's access controls to resources.

Best Practices

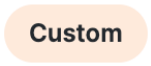
Describes best practices. When working with access rules, keep the following in mind: You can change the rule defaults and global settings. For more information, see Rule Defaults: Default Settings for Access Rules and Edit Rule Defaults and Global Settings.

When working with access rules, keep the following in mind:

- You can change the rule defaults and global settings. For more information, see Rule Defaults: Default Settings for Access Rules and Edit Rule Defaults and Global Settings.
- At the top of each rule is a summary section. After you add your rule, the summary displays the configured rule components.
- If you edit an access rule after saving it, you cannot change the action. Instead, create a new rule.
- In each rule, features where you can configure a default option show one of the following indicators:
  - **Rule Defaults**–If you see this icon beside a control, it means the selected option or value is the selection configured on the rule default page.

  - **Custom**–If you see this icon beside a control, it means the selected option or value is different from the selection configured on the rule default page.

Default Rule Data

Describes default rule data. The Secure Access policy displays various columns of data on your configured internet and private access rules. For information about choosing additional data on your rules, see Show Additional Data on Your Access Rules.

The Secure Access policy displays various columns of data on your configured internet and private access rules. For information about choosing additional data on your rules, see Show Additional Data on Your Access Rules.



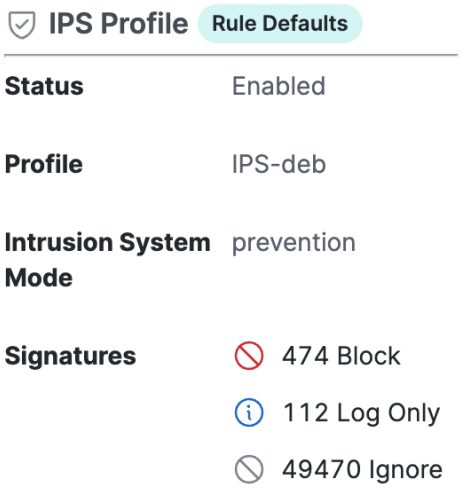
- **#**–The pound sign (hash symbol) indicates the priority of the rule.
- **Rule name**–The name that you assigned to the rule.
- **Access**–The type of access rule either **Internet** or **Private**.

- **Action**–The type of action on the rule.
  - For internet access rules: **Allow**, **Block**, **Isolate**, or **Warn**.
  - For private access rules: **Allow** or **Block**.
- **Sources**–The sources that can connect to the destinations.
- **Destinations**–The resources that are available on the organization and from the internet.
- **Security**–The security controls applied to the rule.

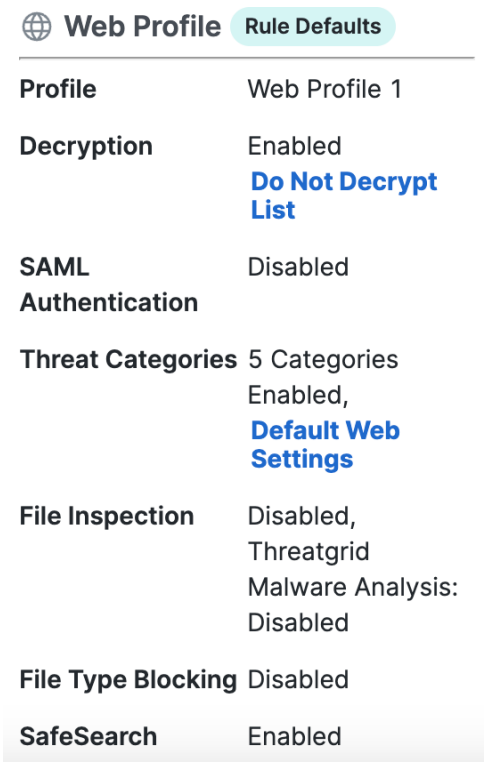


Security controls are the globally-configured profiles that are enabled on the rule: Intrusion Prevention (IPS), Web, and Tenant profiles. Hover over the security icon to display the profile information for the rule.

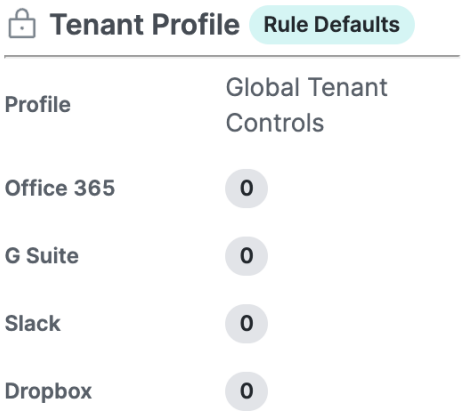
- **IPS Profile**. For more information, see Manage IPS Profiles.



- **Security Profile**. For more information, see Manage Security Profiles.



- **Tenant Profile**. For more information, see Manage Tenant Control Profiles.



- **Hits**–The number of times Secure Access applied the rule to the traffic defined by the sources and destinations. For more information, see Edit the Order of the Rules in Your Access Policy.
- **Status**–The state of the rule. Indicates whether the rule is enabled or disabled.
  - **Enabled Rule**

    
  - **Disabled Rule**

Show Additional Data on Your Access Rules

Provides instructions for show additional data on your access rules. To customize the policy table, you can change the height of the table rows, add more columns of rule data, and remove the Security and Hits columns.

The Cisco Secure Access policy table lists the configured properties, security controls, logging, and status information for your internet and private access rules. The table shows a default set of columns on the table. You can customize your view of the policy table. For more information about the default rule data, see Access Policy Rule Data.

To customize the policy table, you can change the height of the table rows, add more columns of rule data, and remove the **Security** and **Hits** columns.

Customize the row height on the policy table, select additional data to display about your access rules, and remove data columns on your policy table view.



Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Your policy has at least one configured access rule.

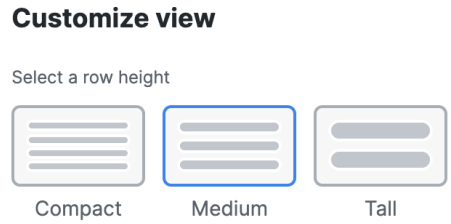
Procedure

1. Navigate to **Secure** > **Access Policy**, and then click **Customize view**.

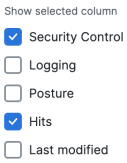
   

2. (Optional) For **Select a row height**, choose the height of the rows in the policy table.

   Select either **Compact**, **Medium**, or **Tall**. The default table row height is **Medium**.

3. For **Show selected columns**, add the names of the data columns to display on your policy table and remove the **Security Control** or **Hits** columns.

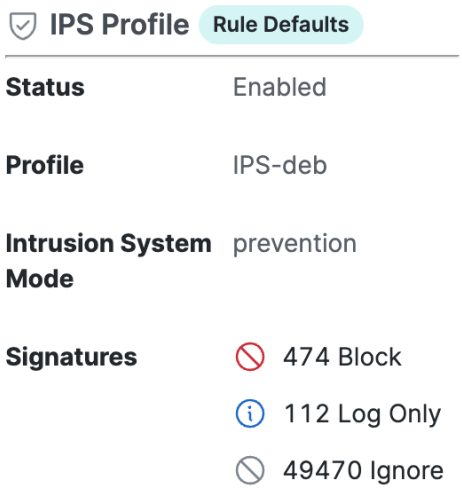
   

   - **Security**–The security controls applied to the rule.

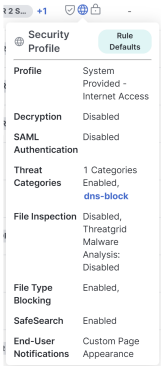


Security controls are the globally-configured profiles that are enabled on the rule: Intrusion Prevention (IPS), Web, and Tenant profiles. Hover over the security icon to display the profile information for the rule.

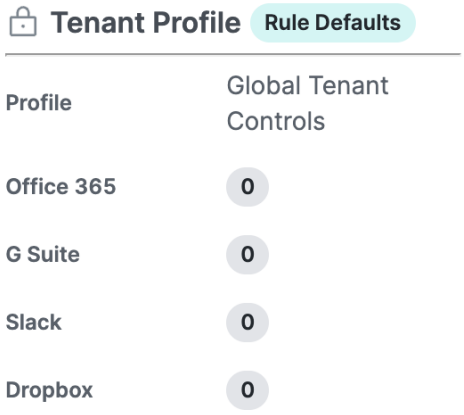
- **IPS Profile**. For more information, see Manage IPS Profiles.

- **Security Profile**. For more information, see Manage Security Profiles.

- **Tenant Profile**. For more information, see Manage Tenant Control Profiles.

- **Logging**–Indicates whether logging is enabled for the organization.
- **Posture**–The name of the endpoint posture profile that is defined on the rule.

- **Hits**–The number of times Secure Access applied the rule to the traffic defined by the sources and destinations. For more information, see Edit the Order of the Rules in Your Access Policy.
- **Last Modified**–The date of the modification of the access rule by the user account.

> **Note**
>
> Hover over the date to display the ID of the user account that last modified the rule.



4. Click **Reset to default** to show the policy table with the default rule data view or click anywhere on the page outside of the **Customize View** component to enable your selections and close the window.



Edit the Order of the Rules in Your Access Policy

Describes editing the order of the rules in your access policy. The order of the rules listed on the Policy page is critical to traffic handling.

The order of the rules listed on the Policy page is critical to traffic handling.

Traffic is handled by the first rule in the list that matches the traffic. Rules lower in the list have no effect on traffic that matches a rule higher in the list.

Order your rules so that more specific rules are above more general rules that might also apply to the traffic.

Put essential rules at the top, such as rules blocking access for all users to sites that you absolutely do not want any users to visit.

If no rule in the list matches the traffic, Secure Access applies the applicable default access rule for the type of traffic (internet access or private access.) Default access rules (one for each type) appear at the bottom of the Policy page.

An error in configuration may result in unintended results: Resources may be unprotected from threats or users may access destinations you want blocked. Plan and design your rules before you build them.

Ways to reorder rules:

- On the Access Policy page, right-click a rule and choose one of the following options:
  - **Move to top** of the list
  - **Move to bottom** of the list
  - **Move to** and then choose an order
- While editing a rule, click the Rule Order field and click the rule you want to be immediately before the rule you are moving.

Rule Defaults: Default Settings for Access Rules

Describes rule defaults: default settings for access rules. When you create a new access rule, the rule is configured with the default rule settings unless you select other options in the rule.

When you create a new access rule, the rule is configured with the default rule settings unless you select other options in the rule. The rule defaults are a collection controls for endpoint security posture and security profiles, and the zero trust authentication interval property. To change the default rule settings, see Edit Rule Defaults and Global Settings.

Important

Important Information About Changing Rule Defaults

If you change a rule default, all existing rules that are configured to use a particular rule default will change to use the new default.

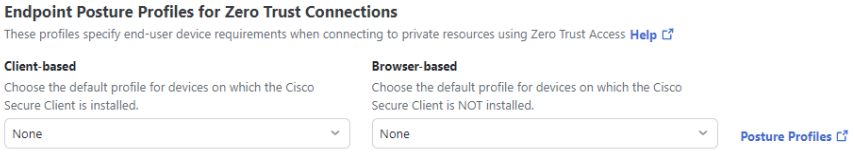
For example, if you change the default IPS Profile from **Balanced Security and Connectivity** to **Maximum Security**, the IPS profile in all existing rules that are configured to use the default IPS Profile will now use the **Maximum Security** settings for IPS.

Existing rules that are configured to use custom settings are not affected by changing the rule default. To determine whether a rule uses default or custom settings, see About the Access Policy on page 390.

Zero Trust Access: Endpoint Posture Profiles

Describes zero trust access: endpoint posture profiles. These profiles specify end-user device requirements when connecting to private resources using Zero Trust Access.

These profiles specify end-user device requirements when connecting to private resources using Zero Trust Access.



There are two types of profiles to choose from:

- **Client-based**–Choose this as the default profile for devices on which the Cisco Secure Client is installed.
- **Browser-based**–Choose this as the default profile for devices on which the Cisco Secure Client **is not** installed.

For more information about Zero Trust posture profiles, see Manage Zero Trust Access Posture Profiles.

Zero Trust Access: User Authentication Interval

Describes zero trust access: user authentication interval. This feature is sometimes called "step-up authentication." Specify the default frequency with which end users must verify their identity, in order to connect to any private resource using client-based zero trust access.

This feature is sometimes called "step-up authentication."

Specify the default frequency with which end users must verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network.

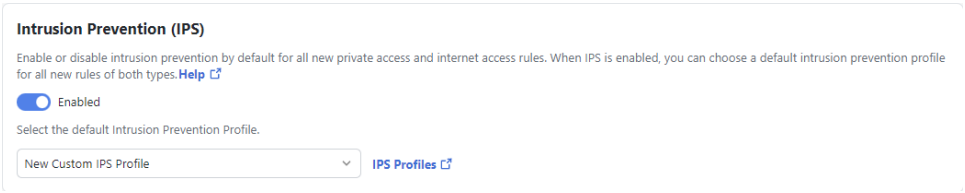
> **Note**
>
> The default interval is three days.

For more information, see Network Authentication for Zero Trust Access.

Intrusion Prevention (IPS)

Describes intrusion prevention (ips). Enable or disable intrusion prevention by default for all new private access and internet access rules. When IPS is enabled, you can choose a default intrusion prevention profile for all new rules of both types.

Enable or disable intrusion prevention by default for all new private access and internet access rules. When IPS is enabled, you can choose a default intrusion prevention profile for all new rules of both types.

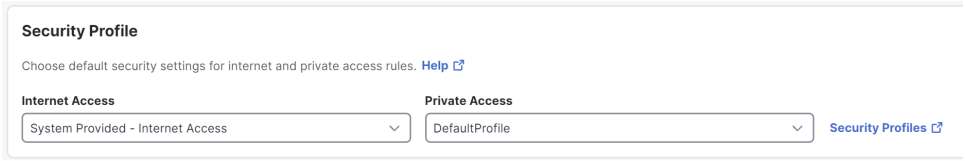


For more information about Zero Trust posture profiles, see Manage IPS Profiles.

Security Profile

Describes security profile. A security profile lets you configure settings that you can use in a rule as a set. Choose a profile to apply to all new access rules of each type (internet and private access). For more information about Security profiles, see Manage Security Profiles.

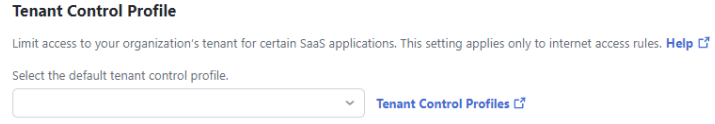
A security profile lets you configure settings that you can use in a rule as a set. Choose a profile to apply to all new access rules of each type (internet and private access). For more information about Security profiles, see Manage Security Profiles.



Tenant Control Profile

Describes tenant control profile. Limit access to your organization's tenant for certain SaaS applications. This setting applies only to internet access rules.

Limit access to your organization's tenant for certain SaaS applications. This setting applies only to internet access rules.



For more information about Zero Trust posture profiles, see Manage Tenant Controls.

Global Settings for Access Rules

Describes global settings for access rules. In Cisco Secure Access, the Access policy has a Global Settings configuration that affects all rules of the applicable type: internet access rules or private access rules.

In Cisco Secure Access, the Access policy has a Global Settings configuration that affects all rules of the applicable type: internet access rules or private access rules.

Some global settings are intended only for troubleshooting purposes. Change these settings only if you have good reason to do so. For more information, see Edit Rule Defaults and Global Settings.

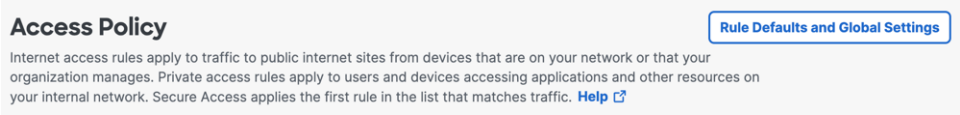
Global Settings for Access Rules

Provides instructions for global settings for access rules. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Change the global settings on the Access policy for the organization.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Click **Rule Defaults and Global Settings**.



3. Click **Global Settings**.
4. Manage the global settings on the Access policy.
   - Microsoft 365 Compatibility
   - Decryption
   - Decryption Logging
   - Certificate Pinning
5. Scroll to the bottom of the page, and then click **Save**.

Microsoft 365 Compatibility

Describes microsoft 365 compatibility. This setting applies only to web security features, not to IPS. If you use tenant controls for Microsoft 365, see additional information at Use Tenant Controls in Access Rules.

This setting applies only to web security features, not to IPS.

The Microsoft 365 Compatibility feature exempts Microsoft 365-related domains, marked as **Optimize** and **Allow** in Microsoft's endpoint categories, to bypass inspection and policy enforcement by web security features, allowing traffic to those domains to pass through unaltered. The domains are excluded from HTTPS decryption and content filtering. The Microsoft 365 traffic appears in the Secure Access reports, however, since HTTPS inspection is disabled, traffic is logged only at the host/domain level and does not show the full URL.

Tenant Controls

If you use tenant controls for Microsoft 365, see additional information at Use Tenant Controls in Access Rules.

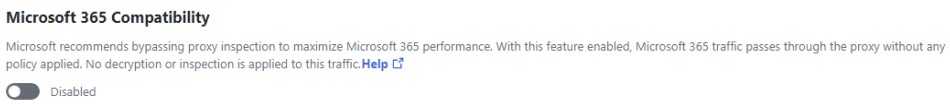
Limitations

Describes limitations. Microsoft 365 traffic is still sent to Secure Access's web proxy service in all deployment methods (Tunnel, AnyConnect, PAC). To stop this traffic from hitting Secure Access entirely, add manual 'External Domain' entries or route the traffic direct to the internet from your connecting devices.

- Microsoft 365 traffic is still sent to Secure Access's web proxy service in all deployment methods (Tunnel, AnyConnect, PAC). To stop this traffic from hitting Secure Access entirely, add manual 'External Domain' entries or route the traffic direct to the internet from your connecting devices.
- File Inspection will no longer apply to this traffic.
- This will not prevent the Microsoft 365 traffic egressing from a Secure Access IP address
- This does not apply to all Microsoft/Microsoft 365 domains. Only those categorized as important for performance by Microsoft.
- This setting allows a number of important Microsoft 365 domains so web security and filtering do not apply to them, and prevents these domains from triggering Secure Access SAML authentication.

> **Note**
>
> MS Intune sync requires "manage.microsoft.com" to be added to the Do Not Decrypt List(s) used in the relevant rules even when Microsoft365 Compatibility is enabled.

For more information, see the official Microsoft documentation.



Decryption

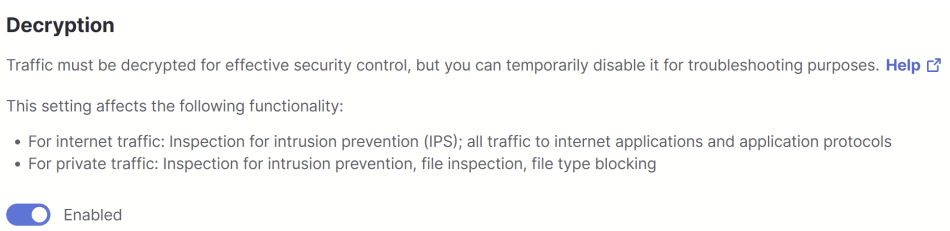
Describes decryption. Traffic must be decrypted for effective security control, but you can temporarily disable decryption for troubleshooting purposes. This setting applies to the following functionality:

Traffic must be decrypted for effective security control, but you can temporarily disable decryption for troubleshooting purposes.

This setting applies to the following functionality:

- **For internet destinations**: Intrusion prevention (IPS) and all traffic to internet application and application protocol destinations.
- **For private resources**: Intrusion prevention (IPS), file inspection, and file type blocking

Disabling decryption does not disable affected features, but decreases their effectiveness for encrypted traffic. Traffic that is not encrypted is not affected.



For information about other decryption settings, see Manage Traffic Decryption.

Decryption Logging

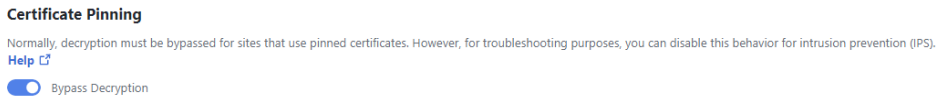
Describes decryption logging. You can enable or disable decryption logging globally in Global Settings, for traffic to private resources or internet destinations or both.

You can enable or disable decryption logging globally in Global Settings, for traffic to private resources or internet destinations or both.

Certificate Pinning

Describes certificate pinning. Certificate pinning is an Internet security mechanism which allows applications to resist impersonation against HTTPS servers using mis-issued or otherwise fraudulent digital certificates.

Certificate pinning is an Internet security mechanism which allows applications to resist impersonation against HTTPS servers using mis-issued or otherwise fraudulent digital certificates. However, if this security feature causes problems when users attempt to access destinations that are both essential and trusted, you may bypass this security feature for destinations that use certificate pinning.



Edit Rule Defaults and Global Settings

Provides instructions for editing rule defaults and global settings. Secure Access is pre-configured with default and global settings for access rules. We recommend that you change the default policy rule settings. You may need to change the global settings.

Important

Before you change the default rule settings on the Cisco Secure Access policy, see Important Information About Changing Rule Defaults.

Secure Access is pre-configured with default and global settings for access rules. We recommend that you change the default policy rule settings. You may need to change the global settings.

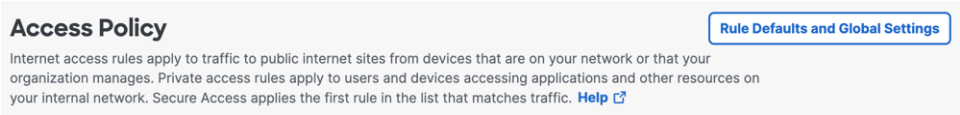
To change rule defaults or global settings:

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- If you are changing the rule defaults, understand the ramifications of doing so. For more information, see Important Information About Changing Rule Defaults.
- Review the settings available on each policy rule:
  - Rule Defaults
  - Global Settings

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Click **Rule Defaults and Global Settings**.



3. Click the tab to edit **Rule Defaults** or **Global Settings**.

   For details about each setting, see:

   - Rule Defaults
   - Global Settings

4. Scroll to the bottom of the page, and then click **Save**.

Edit the Default Access Rules

Describes editing the default access rules. There are two default access rules: Default internet access rule Default private access rule

There are two default access rules:

- Default internet access rule
- Default private access rule

These rules apply to traffic that does not match any other rule.

Default access rules appear at the bottom of the Access Policy listing page.

Default Internet Access Rule

- Secure Access applies this rule to traffic to internet destinations that does not match any other internet access rule in the policy.
- The default internet access rule **allows** traffic that hits it. You cannot change the rule action.
- You can edit logging settings.
- You can edit security control settings.
- Posture is not applicable for internet access rules.

Default Private Access Rule

- Secure Access applies this rule to traffic to private destinations that does not match any other private access rule in the policy.
- The default private access rule **blocks** traffic that hits it. You cannot change the rule action.
- You can edit logging settings.
- Because the action for this rule is Block, security control settings are not needed or offered.

- Posture is not applicable for the default access rule, because the traffic will be blocked whether or not posture requirements are met.

To View or Edit Default Access Rules

Provides instructions for to view or edit default access rules. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

To view or edit a default access rule:

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Scroll to the bottom of the page.
3. In the **Default Access Rules** section, click the ellipsis at the far right side of a rule and choose **View** or **Edit**.
4. Make and save your changes.

29 Get Started With Internet Access Rules

Topics:

- Components for Internet Access Rules
- Default Settings for Internet Access Rules
- Add an Internet Access Rule
- About Configuring Destinations in Internet Access Rules
- Advanced Application Controls
- About Configuring Sources in Internet Access Rules
- Global Settings for Internet Access Rules
- About Isolated Destinations
- Troubleshoot Internet Access Rules

Introduces get started with internet access rules. Internet access rules specify how traffic to internet destinations should be handled. Traffic to internet destinations is allowed by default.

Internet access rules specify how traffic to internet destinations should be handled.

Traffic to internet destinations is allowed by default. You must create rules to block access to internet destinations, either for acceptable use or security reasons; to warn users before you allow access; or to isolate specified internet traffic.

1. **Plan your internet access rule set**

   Plan your rule set so you get the results you expect. Read the documentation and familiarize yourself with the various components that make up rules.

2. **Create rule components**

   You will assemble rules largely from components, for example source, destination, and security control components. For more information, see Components for Internet Access Rules.

3. **Specify rule defaults**

   New rules will use the default security controls and other settings that you specify on the Rule Defaults page. For more information, see Default Settings for Internet Access Rules.

4. **Edit the default internet access rule**

   Traffic to internet destinations that does not match any other internet access rule in the policy will be handled by the default internet access rule. Traffic that matches this rule is **allowed** unless it violates security controls. For more information, see Edit the Default Access Rules.

5. **Add internet access rules**

   For more information, see Add an Internet Access Rule.

6. **Review the global settings**

   Normally you will not change these settings for internet access rules, but you should be familiar with their impact. For more information, see Global Settings for Internet Access Rules.

7. **Review the rule order**

   Make sure the order of the rules on the Policy page will have the results you expect. For more information, see Edit the Order of the Rules on the Policy Page.

8. **Test your internet access rules**

Components for Internet Access Rules

Describes components for internet access rules. You will create access rules by assembling components that you or others have previously created.

You will create access rules by assembling components that you or others have previously created.

Components described in this topic are reusable; you can use the same component (such as a source) in multiple rules, speeding and simplifying policy creation.

For example, you can define a set of users as a source, then use the same source in an internet access rule and in a private access rule for the same set of users.

Some components are "profiles", or sets of settings bundled together that you choose as a unit when configuring a rule.

> **Note**
>
> Most components for internet access rules are different from components needed for private access rules.

Sources

Describes sources. You will configure access policies for specific source-destination pairs. Sources are the users, groups of users, or other entities that comprise the "From" end of traffic that an access policy applies to.

You will configure access policies for specific source-destination pairs. Sources are the users, groups of users, or other entities that comprise the "From" end of traffic that an access policy applies to.

The following reusable sources (source objects) can be used in internet access rules:

- Users
- User Groups
- Network Tunnel Groups

  You can apply rules to traffic originating from IP addresses in network segments defined by Network Tunnel Groups.
- Registered Networks

  You can apply rules to traffic originating from IP addresses in network segments defined by Registered Networks.
- Internal Networks

  You can apply rules to traffic originating from IP addresses in network segments defined by Internal Networks.
- Roaming Devices

  You can apply rules to traffic originating from managed devices that have the Cisco Secure Client installed, but that may not currently be on the corporate network.

In a rule, you can also specify sources by typing in IP addresses and subnets, but these are NOT reusable source components. If you do this, you can type in port and protocol in the rule's destination.

See also About Configuring Sources in Internet Access Rules.

Destinations

Describes destinations. You will configure access policies for specific source-destination pairs. Destinations are the web applications, web sites in particular categories, or other internet destinations that comprise the "To" end of traffic that an internet access policy applies to.

You will configure access policies for specific source-destination pairs. Destinations are the web applications, web sites in particular categories, or other internet destinations that comprise the "To" end of traffic that an internet access policy applies to.

Reusable destinations (destination objects) in internet access rules:

- Destination Lists

  List groups of domains, URLs, IP addresses, and CIDR blocks to which you want to apply the same policy.

  You can create custom lists of destinations based on any criteria you choose.

- Content Category Lists

  Create lists of web sites based on the content or type of the site, so you can control access to a variety of sites as a group. For example, you might create a content category list that includes all sites belonging to the Adult, Child abuse, and Pornography categories.

- Application Lists

  Create lists of web-based applications to which you want to apply the same policy. For example, if you want to apply a single policy to all social media applications, you can create an application list that includes all applications in the Social Networking category.

  For some web-based applications, you can allow access to the application, but block uploads, downloads, and posting or sharing information. You will see these options in each rule when you configure applicable destinations in the rule. For details, see Advanced Application Controls.

When configuring rules, you can also:

- Specify web sites by content category, or specify web applications or categories of web application, without creating content category lists or application lists.
- Type destination IP addresses, ports, and protocols directly into the rule.

However, best practice is generally to create reusable destination objects when possible, so that you can apply rules consistently.

See also About Configuring Destinations in Internet Access Rules.

Security Controls

Describes security controls. Security controls make use of profiles and other pre-configured sets of settings. The following types of security controls apply to internet traffic:

Security controls make use of profiles and other pre-configured sets of settings.

The following types of security controls apply to internet traffic:

- Intrusion Prevention (IPS)
- Web Security
- Tenant Controls

Intrusion Prevention (IPS)

Describes intrusion prevention (ips). Intrusion Prevention protects your network and assets by inspecting traffic for specified threat characteristics. You will specify a single intrusion prevention profile in each access rule.

Intrusion Prevention protects your network and assets by inspecting traffic for specified threat characteristics.

You will specify a single intrusion prevention profile in each access rule.

- Set Up Certificates for Decrypting Internet Traffic

- Configure Intrusion Prevention (IPS) Profiles
- Configure the Do Not Decrypt List for IPS

Set Up Certificates for Decrypting Internet Traffic

Describes setting up certificates for decrypting internet traffic. Internet traffic must be decrypted in order to allow it to be inspected by the intrusion prevention and for web security features. In order to decrypt this traffic, certificates are required.

Internet traffic must be decrypted in order to allow it to be inspected by the intrusion prevention and for web security features. In order to decrypt this traffic, certificates are required. You may have already set up these certificates to decrypt traffic for web security features.

See Certificates for Internet Decryption.

Configure Intrusion Prevention (IPS) Profiles

Describes configuring intrusion prevention (ips) profiles. Intrusion Prevention (IPS) detects a large number of known threats. Sets of settings are grouped together in profiles, which you can specify in access rules.

Intrusion Prevention (IPS) detects a large number of known threats. Sets of settings are grouped together in profiles, which you can specify in access rules. Secure Access provides several pre-configured profiles that address common needs, such as Balanced Security and Connectivity or Maximum Security. Or you can create a custom profile using Snort signatures. You can also choose to block or just monitor traffic that matches a profile.

You can choose a different IPS profile for each access rule based on the balance of convenience vs. risk appropriate for the particular traffic.

For details, see Manage IPS Profiles.

Configure the Do Not Decrypt List for IPS

Describes configuring the do not decrypt list for ips. Secure Access must decrypt traffic in order to allow the Intrusion Prevention feature to inspect the traffic for threats.

Secure Access must decrypt traffic in order to allow the Intrusion Prevention feature to inspect the traffic for threats.

However, decrypting traffic to certain sites, such as health-related or financial sites, may be restricted by privacy laws in some geographic regions.

Use the default Do Not Decrypt List to specify destinations that should not be decrypted by intrusion prevention processes (IPS.)

The Web Security feature also requires decryption in order to be effective; you can use this list for Web Security decryption, or you can create and use a different list or lists for Web Security.

For details, see Important Information About Do Not Decrypt Lists.

Web Security

Describes web security. You will specify a single Web Security Profile in each internet access rule, but web security profiles include multiple components that you should pre-configure.

You will specify a single Web Security Profile in each internet access rule, but web security profiles include multiple components that you should pre-configure.

- Configure Threat Category Settings
- Configure SAML Authentication
- Set Up Certificates for Decrypting Internet Traffic
- Configure Do Not Decrypt Lists for Web Security

- (Optional) Configure Custom End-User Block and Warn Notifications
- Configure Security Profiles

Configure Threat Category Settings

Describes configuring threat category settings. Choose the types of web-borne threats to block. Blocking some threat categories may affect legitimate traffic.

Choose the types of web-borne threats to block. Blocking some threat categories may affect legitimate traffic.

See Threat Categories.

Configure SAML Authentication

Describes configuring saml authentication. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

SAML authentication is required for some web security features.

See Manage Security Profiles

Set Up Certificates for Decrypting Internet Traffic

Describes setting up certificates for decrypting internet traffic. If you have already set up certificates for this purpose for the intrusion prevention feature, you may not need to do anything more.

If you have already set up certificates for this purpose for the intrusion prevention feature, you may not need to do anything more.

Internet traffic must be decrypted in order to allow it to be inspected by the intrusion prevention and web security features, to apply acceptable use controls, for rules in which the rule action is Isolate or Warn, and to display end-user notifications when destinations are blocked.

In order to decrypt this traffic, certificates are required.

See Certificates for Internet Decryption.

Configure Do Not Decrypt Lists for Web Security

Describes configuring do not decrypt lists for web security. Secure Access must decrypt internet traffic in order to allow Web Security features to protect your network effectively.

Secure Access must decrypt internet traffic in order to allow Web Security features to protect your network effectively.

However, decrypting traffic to certain sites, such as health-related or financial sites, may be restricted by confidentiality law in certain geographic regions.

Use a Do Not Decrypt List to specify destinations that should not be decrypted by web security processes. You can create different Do Not Decrypt Lists for different regions or purposes.

You can use the same Do Not Decrypt List that you use for IPS, or create one or more Do Not Decrypt lists to use only for security features included in the security profile.

For details, see Important Information About Do Not Decrypt Lists.

(Optional) Configure Custom End-User Block and Warn Notifications

Describes (optional) configure custom end-user block and warn notifications. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

If you do not want to use the default Secure Access-branded notifications, configure the notifications that are presented to end users who attempt to access internet destinations that are blocked, and notifications to present when users attempt to access destinations that match a rule configured with the Warn action.

End-user notifications require decryption.

See Manage Notification Pages.

Configure Security Profiles

Describes configuring security profiles. Sets of web security settings grouped into profiles control the following aspects of security for internet traffic:

Sets of web security settings grouped into profiles control the following aspects of security for internet traffic:

- **Decryption** (including Do Not Decrypt lists)

  See information above.

- **SAML Authentication**

  See information above.

- **Threat categories**

  See information above.

- **File inspection**

  File inspection detects threats using Cisco Advanced Malware Protection and Cisco Secure Malware Analytics.

  See Manage File Inspection and File Analysis.

- **File type blocking**

  Block files based on their type. For example, you can prevent users from downloading executable files from the web.

  See Manage File Type Control.

- **SafeSearch**

  SafeSearch filters out offensive, explicit, unsafe, and harmful results from searches in Google, YouTube, Yahoo, and Bing.

  See SafeSearch

- **End-user notifications**

  Web pages shown to users who attempt to access blocked destinations or destinations allowed with a warning.

  See information above.

You will enable these options in a security profile that you will choose in a rule. See Manage Security Profiles.

Tenant Controls

Describes tenant controls. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

If your company uses Microsoft 365, Slack, Google G-Suite, or Dropbox, see Manage Tenant Control Profiles.

Default Settings for Internet Access Rules

Describes default settings for internet access rules. You can choose default settings that will automatically populate newly created access rules by default.

You can choose default settings that will automatically populate newly created access rules by default.

Configure these settings on the Rule Defaults page: Navigate to **Secure** > **Access Policy**, click **Global Settings and Rule Defaults**, then click the **Rule Defaults** tab.

The following settings apply to internet access rules:

- **Intrusion Prevention (IPS) Profile**

  Specify the traffic-inspection behavior to use by default in new access rules.

  This setting applies to both private access rules and internet access rules.

  For more information about IPS profiles, see Manage IPS Profiles.

- **Security Profile**

  Specify a default set of settings that control security and other interactions for end users accessing the internet.

  For more information about security profiles, see Manage Security Profiles.

- **Tenant Controls**

  If your company uses Microsoft 365, Google G-Suite, Slack, or Dropbox, you must configure tenant controls.

  For more information about tenant controls, see Manage Tenant Control Profiles.

For details, see Rule Defaults and Edit Rule Defaults and Global Settings.

Important

Choose rule defaults carefully; changing these settings later may impact existing rules. See Important Information About Changing Rule Defaults.

Add an Internet Access Rule

Provides instructions for adding an internet access rule. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Internet access rules specify how traffic to internet destinations should be handled.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- At a minimum, you should configure the following before creating internet access rules:
  - Components for Internet Access Rules
  - Default Settings for Internet Access Rules
- For other factors involved in creating and enforcing internet access rules, see Manage Internet Access Rules.

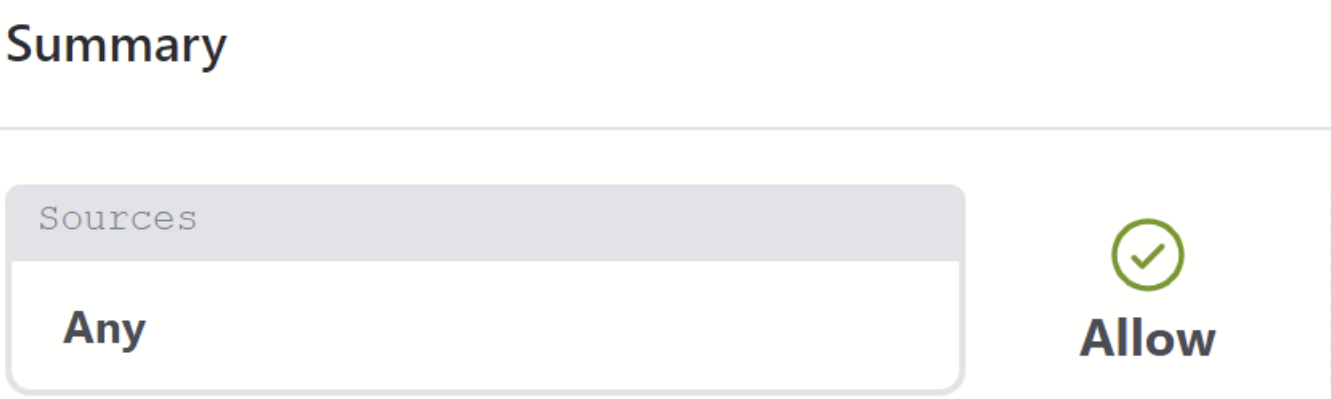
Note

Prerequisites for internet access rules are similar to but different from prerequisites for private access rules.

Procedure

1. Navigate to **Secure** > **Access Rules**.
2. Click **Add Rule** > **Internet Access**.

At the top of the rule is a summary section. Controls you configure in this rule will be summarized here:



3. Configure access criteria:

   See Access Options

4. Click **Next**.

   The Next button is not available until you give the rule a name and then click out of the Rule name field.

5. Configure security controls:

   See Security Control Options

6. Click **Save**.
7. (Optional) Enable or disable the rule using the toggle at the top of the page.

Prerequisites

Describes prerequisites. Full Admin user role. For more information, see Manage Accounts. At a minimum, you should configure the following before creating internet access rules:Components for Internet Access RulesDefault Settings for Internet Access Rules

- Full Admin user role. For more information, see Manage Accounts.
- At a minimum, you should configure the following before creating internet access rules:
  - Components for Internet Access Rules
  - Default Settings for Internet Access Rules
- For other factors involved in creating and enforcing internet access rules, see Manage Internet Access Rules.

> **Note**
>
> Prerequisites for internet access rules are similar to but different from prerequisites for private access rules.

Procedure

Describes procedure. Navigate to Secure Access Rules . Click Add Rule Internet Access .At the top of the rule is a summary section. Controls you configure in this rule will be summarized here:At the top of the rule is a summary section.

1. Navigate to **Secure** > **Access Rules**.
2. Click **Add Rule** > **Internet Access**.

   At the top of the rule is a summary section. Controls you configure in this rule will be summarized here:



3. Configure access criteria:

   See Access Options

4. Click **Next**.

   The Next button is not available until you give the rule a name and then click out of the Rule name field.

5. Configure security controls: See Security Control Options
6. Click **Save**.
7. (Optional) Enable or disable the rule using the toggle at the top of the page.

Access Options

Describes accessing options. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- Disable or enable the rule
- Logging settings
- Summary
- Rule name
- Rule order
- Rule action
- Sources
- Destinations
- Advanced Application Controls

Disable or Enable the rule

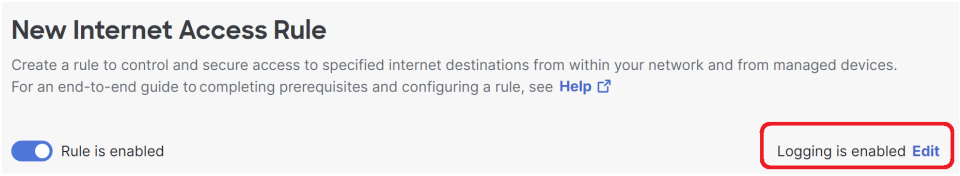
Describes disabling or enable the rule. After you configure the rule and click Save, the rule will take effect only if this toggle shows as Enabled.

After you configure the rule and click Save, the rule will take effect only if this toggle shows as Enabled.

Logging settings

Describes logging settings. Logging options are at the top right corner of the page: To choose options, click Edit. For details, see Manage Logging.

Logging options are at the top right corner of the page:



To choose options, click **Edit**.

For details, see Manage Logging.

Summary

Describes summary. After you configure the rule, view a summary of the rule's action here. If you see an Upgrade button, this means your company has an opportunity to upgrade to a licensing package that offers additional functionality. For details, contact your Cisco sales representative.

After you configure the rule, view a summary of the rule's action here.

If you see an **Upgrade** button, this means your company has an opportunity to upgrade to a licensing package that offers additional functionality. For details, contact your Cisco sales representative.

Rule name

Describes rule name. You must give your rule a name before you can click Next at the bottom of the page (to specify security controls.)

You must give your rule a name before you can click Next at the bottom of the page (to specify security controls.)

Rule order

Describes rule order. Specify where you want this rule in the overall rule order. Secure Access applies the first rule in the list on the Policy page that matches the traffic.

Specify where you want this rule in the overall rule order.

Secure Access applies the first rule in the list on the Policy page that matches the traffic.

Order your rules so that more specific rules are above more general rules that might also apply to the traffic.

For important guidelines, see Edit the Order of Rules on the Access Policy Page.

Rule action

Describes rule action. By default, access to internet destinations is allowed unless an access rule blocks or modifies access using the Warn or Isolate options.

By default, access to internet destinations is allowed unless an access rule blocks or modifies access using the Warn or Isolate options.

The action you choose determines which other options are available in the rule.

Specify the rule action before you specify other settings including source and destination, or those configurations will be reset when you change the action.

- **Allow** - When the action is Allow, traffic can still be blocked if it does not pass the security controls specified in the rule.
- **Block** - If you want to display a notification page to end users who attempt to access a blocked destination, see Manage Notification Pages.
- **Warn** - When the action is Warn:
  - End users must click a link in a warning notification to access the destination.

- The destination can include only content categories and content category lists.
- You can configure a custom warning notification that Secure Access will present to users who attempt to access a warned destination. You can also preview the notification page. See Manage Notification Pages.
- Decryption must be enabled in order to present the notification.
- For required certificates for displaying notifications, see Certificates for Internet Decryption.

- **Isolate** - If your license includes the Remote Browser Isolation feature, Secure Access creates a virtual browser that hosts applicable destination access requests. This action is available only for certain destinations.

  For information about the Isolate action, see Understand Isolated Destinations.

  If you see an **Upgrade** button, click it for information about enhanced functionality for this feature.

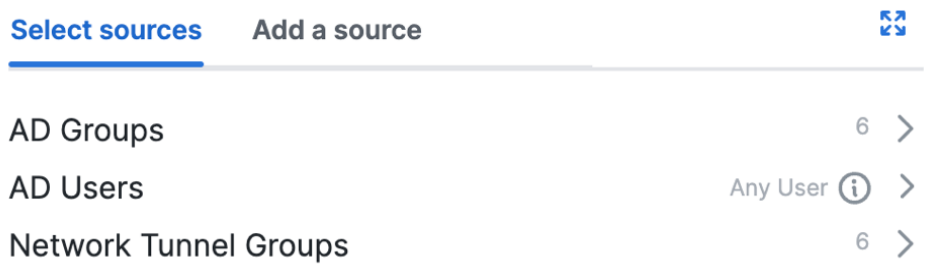
Sources

Describes sources. We recommend that you create reusable components rather than adding source IP addresses directly to a rule. See Components for Internet Access Rules. For detailed tips and guidelines when configuring sources, see About Configuring Sources for Internet Access Rules.

We recommend that you create reusable components rather than adding source IP addresses directly to a rule. See Components for Internet Access Rules. For detailed tips and guidelines when configuring sources, see About Configuring Sources for Internet Access Rules.

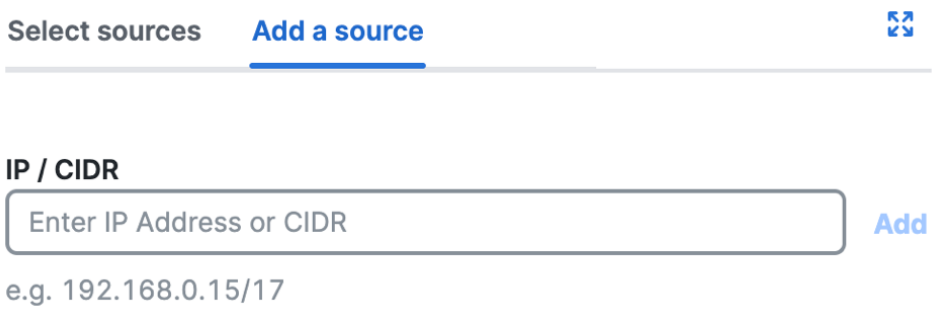
- For **Select sources**, click in the white space beside the default value ("Any") and choose the configured source components in your organization. When you finish choosing your sources, click **Done**.

  For descriptions of the different types of sources, including links to how to create reusable sources, see Components for Internet Access Rules.



- For **Add a source**, enter an IP or CIDR address as network connection source in the access rule, and then click **Add**. When you finish adding your sources, click **Done**.

  This option is useful if you need to quickly address a specific issue that arises, for example to immediately block a particular user's access to an internet destination. For more information, see About Configuring Source in Private Access Rules.



> **Note**
>
> The arrows out icon opens a window to configure the sources in your rule.

Destinations

Describes destinations. We recommend that you create reusable components rather than adding destinations directly in a rule. For more information, see Components for Internet Access Rules. For detailed tips and guidelines when configuring destinations, see About Configuring Destinations for Internet Access Rules.

We recommend that you create reusable components rather than adding destinations directly in a rule. For more information, see Components for Internet Access Rules. For detailed tips and guidelines when configuring destinations, see About Configuring Destinations for Internet Access Rules.

Click in the white space beside the default value ("Any") and specify destinations:

- **Select destinations**

  The destination options available depend on the rule action you choose.

  Usually you will select destinations that you or others have previously configured.

  For more information, see Components for Internet Access Rules.

- For **Add a destination**, select **Port**, **IP/CIDR Address**, and **Protocol**. Choose from one of the supported protocols: **Any**, **TCP**, **UDP**, or **ICMP**. After each selection, click **Add**. When you finish adding the attributes of the private destination, click **Done**.

Advanced Application Controls

Describes advanced application controls. If configured destinations include Application Lists, Application Categories, or individual applications selected from Application Categories that support the ability to control uploads, downloads, posting, or sharing without entirely blocking access to the application, you will see the Advanced Application Controls section.

If configured destinations include Application Lists, Application Categories, or individual applications selected from Application Categories that support the ability to control uploads, downloads, posting, or sharing without entirely blocking access to the application, you will see the Advanced Application Controls section.

See Advanced Application Controls.

Security Control Options

Describes security control options. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- Intrusion Prevention (IPS)
- Security Profile
- Tenant Control Profile
- Advanced Security Controls

Intrusion Prevention (IPS)

Describes intrusion prevention (ips). Choose the IPS profile that includes the threat detection settings that you want applied to traffic that matches this rule. You can also disable intrusion prevention for this rule.

Choose the IPS profile that includes the threat detection settings that you want applied to traffic that matches this rule. You can also disable intrusion prevention for this rule.

See Manage IPS Profiles.

Security Profile

Describes security profile. Choose the security profile that includes the web-related settings that you want applied to traffic that matches this rule.

- Choose the security profile that includes the web-related settings that you want applied to traffic that matches this rule.
- For all rules, including Block, Warn, and Isolate rules, unless you have good reason not to, choose a security profile that is configured to decrypt the traffic that will hit the rule. Decryption is required to accurately process traffic to most internet destinations.
  - Best practice: If decryption is disabled in a security profile, or if decryption is enabled only to show notifications, use that profile only in rules that include only trusted destinations.
  - For important information about decryption, see Security Profiles for Internet Access and Manage Traffic Decryption.
- If the rule will block traffic or warn users, you can choose a security profile that specifies the notifications to display to end users.

For more information, see Security Profiles for Internet Access.

Tenant Control Profile

Describes tenant control profile. Tenant controls affect access to Microsoft 365, Google G Suite, Slack, and Dropbox. For more information, see Manage Tenant Control Profiles.

Tenant controls affect access to Microsoft 365, Google G Suite, Slack, and Dropbox.

For more information, see Manage Tenant Control Profiles.

For additional requirements, see Use Tenant Controls in Access Rules.

Advanced Security Controls

Describes advanced security controls. This section includes options to skip enforcement of certain security features, which you may want to do permanently for trusted destinations or temporarily to troubleshoot an issue.

This section includes options to skip enforcement of certain security features, which you may want to do permanently for trusted destinations or temporarily to troubleshoot an issue.

This section includes the ability to access files without decrypting them (sometimes known as "protected file bypass") and the ability to not enforce certain web security features for this rule.

In general, you should allow access to encrypted files only for trusted destinations, because encrypted files cannot be effectively assessed for threats. By default, access to encrypted files is not enabled.

Disable security features only when you have a specific reason to do so.

Next Steps

Describes next steps. Return to Manage Internet Access Rules and review additional steps you should take after configuring a rule.

Return to Manage Internet Access Rules and review additional steps you should take after configuring a rule.

About Configuring Destinations in Internet Access Rules

Describes about configuring destinations in internet access rules. Secure Access internet rules enable you to configure DNS and Web security for your organization's web traffic. You can add pre-configured destination components or combinations of IP addresses, ports, and transport protocols for destinations on an internet rule.

Secure Access internet rules enable you to configure DNS and Web security for your organization's web traffic. You can add pre-configured destination components or combinations of IP addresses, ports, and transport protocols for destinations on an internet rule. When you add multiple network address components on the destinations, Secure Access combines the entries as a set using the boolean OR operator.

Destination Components for Internet Access Rules

Describes destination components for internet access rules. You should pre-configure destinations that you can select in internet access rules. For descriptions and links to configuration instructions for each component type, see Components for Internet Access Rules.

- You should pre-configure destinations that you can select in internet access rules. For descriptions and links to configuration instructions for each component type, see Components for Internet Access Rules.
- You can also specify web sites by their content category, or specify individual web applications or categories of web application without creating content category lists or application lists, by choosing **Content Categories** or **Application Categories**.
- Depending on the destinations you select (for example certain applications, application lists, or application categories) other options may appear in the rule.
- If you see an option to "Select All", this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in future
- When you select a list or group, entities that are added to the list or group in the future are automatically included. For example, if you select a Destination List, any destinations that you add to that destination list later are automatically included.
- If this rule involves tenant controls, you must include the relevant application as a destination in the rule, as well as configuring the applicable tenant control profile and specifying that profile in the Security Controls section of the rule. For more information, see Manage Tenant Control Profiles.
- When specifying applications, it is not possible to search for an application with fewer than three letters in its name—for example, "QQ" or "YY". You must pick the applications manually from the tree under their respective categories or use a wildcard in search—for example, "QQ*". This behavior is by design.

Destinations Created Directly in an Internet Access Rule

Describes destinations created directly in an internet access rule. Destinations in internet rules accept various combinations of IP addresses, ports 80 and 443, and the TCP, UDP, and ICMP transport protocols.

Destinations in internet rules accept various combinations of IP addresses, ports 80 and 443, and the TCP, UDP, and ICMP transport protocols. When you add multiple network address components for destinations, Secure Access combines the entries into a set using the boolean OR operator.

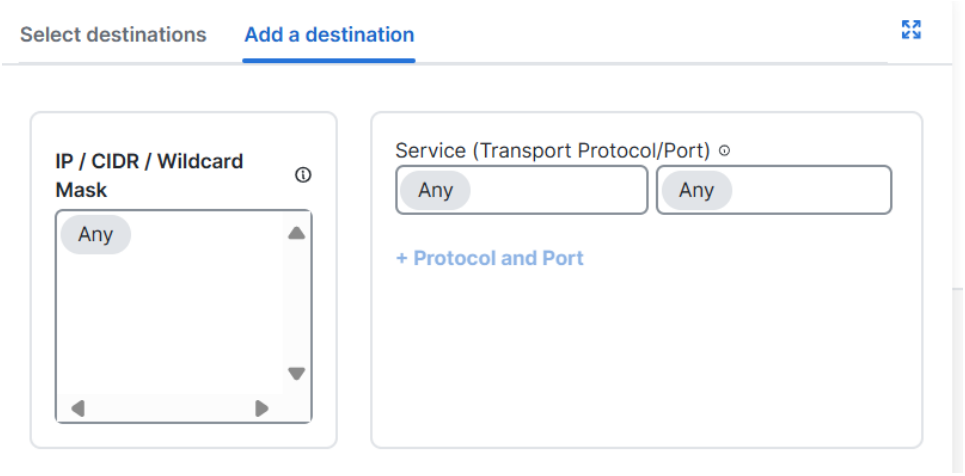
You can add destinations directly in a rule rather than choosing destination components. However, this is generally not recommended. Destinations that you add to a rule are not reusable components, are not dynamically updated, and cannot be used in any other rule.

This option is useful if you need to quickly address a specific issue that arises, for example to immediately allow access to a necessary destination that is being blocked by another rule, or to immediately block access to a problem destination.

IP Addresses and CIDR Blocks

Describes ip addresses and cidr blocks. Destinations accept IP addresses and CIDR blocks.Secure Access does not accept private non-routable addresses for destinations, only public IP addresses.Secure Access does not require that your destination IP address is the IP of a Registered Network in Secure Access.

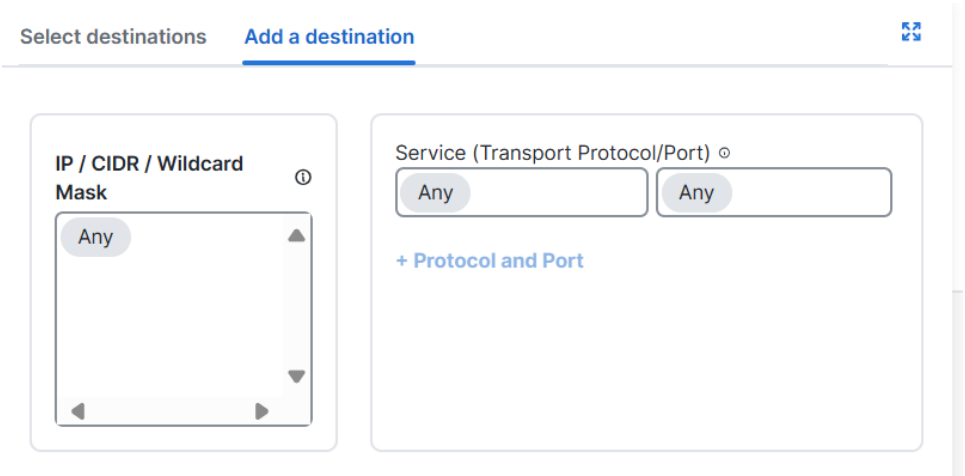
- Destinations accept IP addresses and CIDR blocks.
  - Secure Access does not accept private non-routable addresses for destinations, only public IP addresses.
  - Secure Access does not require that your destination IP address is the IP of a Registered Network in Secure Access.



Ports

Describes ports. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- Destinations accept ports 80 and 443 directly on an internet access rule.

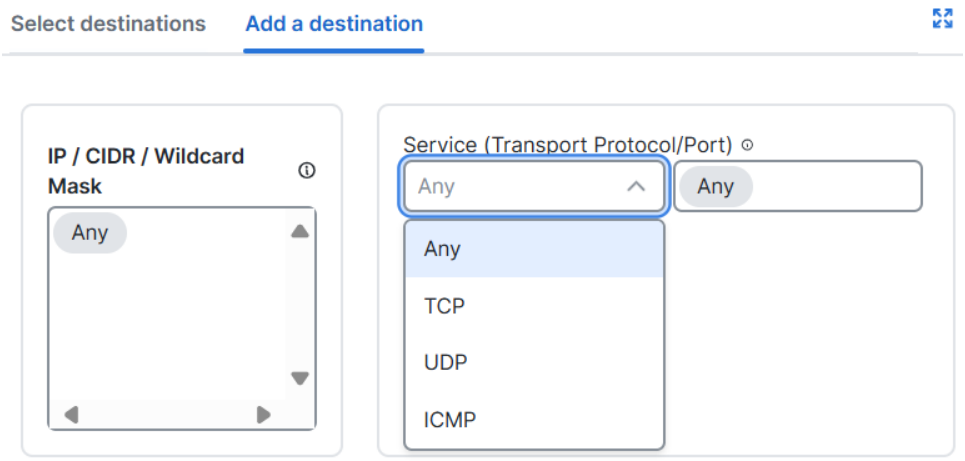


Protocols

Describes protocols. Destinations accept the TCP, UDP, and ICMP transport protocols. If you add the TCP protocol for a destination on a rule, the rule applies only for web traffic that is protected by the secure web gateway.

- Destinations accept the TCP, UDP, and ICMP transport protocols.

- If you add the TCP protocol for a destination on a rule, the rule applies only for web traffic that is protected by the secure web gateway.
- Destinations only accept UDP or ICMP protocols that describe non-web traffic. Connections on UDP or ICMP are protected by your IPS profile settings.
- You can choose **Any** protocol for the destination. If you select **Any**, web traffic is managed by the secure web gateway.



Combining Multiple Destinations in a Rule (Boolean Logic)

Describes combining multiple destinations in a rule (boolean logic). If an internet access rule includes multiple destinations, the following boolean logic applies:

If an internet access rule includes multiple destinations, the following boolean logic applies:

- All types of destinations, and all destinations within a type, are treated as using the boolean OR operator: Traffic to each destination you specify in a rule matches the rule.

  For example, if you specify a content category and an application list as destinations in a single rule, traffic to any destination that is a member of either group will match the rule.

- If you type in values of different types (IP address, port, protocol), traffic matches if any of the specified values match the rule.

  For example, if you specify an IP address and a port, traffic to any IP address on the specified port matches the rule, as does traffic to the specified address on any port.

  If you specify **Any** protocol, then all traffic will match the rule, regardless of any other destinations you specify.

Number of Destinations in a Rule

Describes number of destinations in a rule. You can include up to 5000 destinations in an internet access rule. However, for optimal performance, include no more than 100 destinations in a rule.

You can include up to 5000 destinations in an internet access rule. However, for optimal performance, include no more than 100 destinations in a rule.

Advanced Application Controls

Describes advanced application controls. Some web-based applications offer the option to allow users to access the site but not to perform activities such as uploading, downloading, posting, or sharing content on those sites.

Some web-based applications offer the option to allow users to access the site but not to perform activities such as uploading, downloading, posting, or sharing content on those sites.

Depending on the destinations you select in an internet access rule, you will see an Advanced Application Controls section.

This section appears only if destinations added to the rule include one or more applications that allow granular controls on activities. These applications must be included in application lists or application categories selected as destinations, or be individual applications selected from application categories.

Use these advanced controls if you want to allow access to the site but block certain actions. If you don't want to allow access to the site at all, select the application, Application List, or Application Category in the destination list for the rule.

Applications with Advanced Controls

Describes applications with advanced controls. If apps have advanced app controls, you can block all content for the app, block the app from uploading content including posts and shares, block the app from downloading content, or block the app from deleting content.

If apps have advanced app controls, you can block all content for the app, block the app from uploading content including posts and shares, block the app from downloading content, or block the app from deleting content.

- Cloud Storage
- Collaboration
- Content Management
- Media
- Office Productivity
- P2P
- Social Networking

Cloud Storage

Describes cloud storage. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Applications	Category	Upload	Download	Post/Share	Delete
Box Cloud Storage	Cloud Storage	Yes	Yes	Yes	Yes
Dropbox	Cloud Storage	Yes	Yes	Yes	Yes
Flickr	Cloud Storage	Yes			
File Dropper	Cloud Storage	Yes			
GrosFichiers	Cloud Storage	Yes	Yes		
Google Drive	Cloud Storage	Yes			
Leap File	Cloud Storage	Yes			Yes
MediaFire	Cloud Storage		Yes		Yes
Microsoft OneDrive	Cloud Storage				Yes
OpenDrive	Cloud Storage	Yes			
Onehub	Cloud Storage	Yes			
PicDrop	Cloud Storage	Yes			Yes
SendThisFile	Cloud Storage	Yes			Yes

Applications	Category	Upload	Download	Post/Share	Delete
SmugMug	Cloud Storage	Yes	Yes		Yes
SlideShare	Cloud Storage	Yes	Yes		Yes
4shared	Cloud Storage	Yes			Yes

Collaboration

Describes collaboration. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Applications	Category	Upload	Download	Post/Share	Notes
Cisco Webex Teams	Collaboration			Yes	
Microsoft Teams	Collaboration	Yes		Yes	
Gyazo Teams	Collaboration	Yes			
Slack	Collaboration	Yes	Yes	Yes	
WhatsApp	Collaboration	Yes			If you upload a Whatsapp file that has already been previously uploaded, Secure Access does block the upload of the file. As a workaround, manually delete the existing version of the file from the Whatsapp servers.

Content Management

Describes content management. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Applications	Category	Upload	Download	Post/Share
Egnyte Connect	Content Management	Yes		
Lucidchart	Content Management	Yes		
Pastebin	Content Management	Yes		

Media

Describes media. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Applications	Category	Upload	Download	Post/Share
Dailymotion	Media	Yes		
Giphy	Media	Yes		
Veoh	Media	Yes		
Vimeo	Media	Yes		
YouTube	Media	Yes		

Office Productivity

Describes office productivity. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Applications	Category	Upload	Download	Post/Share
Basecamp	Office Productivity			Yes
DocHub	Office Productivity	Yes		
AOL Mail	Office Productivity		Yes	
Evernote	Office Productivity			Yes
Gmail	Office Productivity	Yes Only for Gmail attachment uploads.		
Mail.ru	Office Productivity	Yes Only for Mail.ru attachment uploads.		
Smartsheet	Office Productivity	Yes		
Trello	Office Productivity	Yes		
Yandex Mail	Office Productivity	Yes		
Yahoo Mail	Office Productivity		Yes	

P2P

Describes p2p. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Applications	Category	Upload	Download	Post/Share
Citrix ShareFile	P2P	Yes		
Filesend	P2P	Yes		
GigaFile	P2P		Yes	
Hightail	P2P	Yes		
WeTransfer	P2P	Yes	Yes	
Wikisend	P2P	Yes		

Social Networking

Describes social networking. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Applications	Category	Upload	Download	Post/Share
Facebook	Social Networking	Yes		
Facebook Messenger	Social Networking	Yes		
Instagram	Social Networking	Yes		Yes
LinkedIn	Social Networking	Yes	Yes	Yes
Pinterest	Social Networking	Yes		Yes
Tik Tok	Social Networking	Yes		Yes
Twitter	Social Networking	Yes		Yes

Procedure

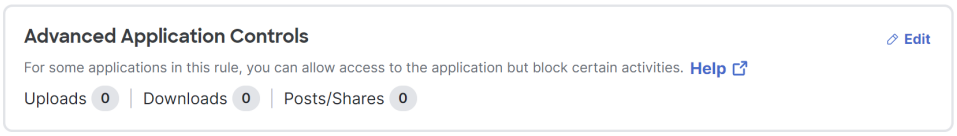
Provides instructions for procedure. Full Admin user rule. For more information, see Manage Accounts. In an internet access rule, add as destinations any application categories or applications from the table above, or a configured application list that includes any of the above applications or categories.

Before you begin

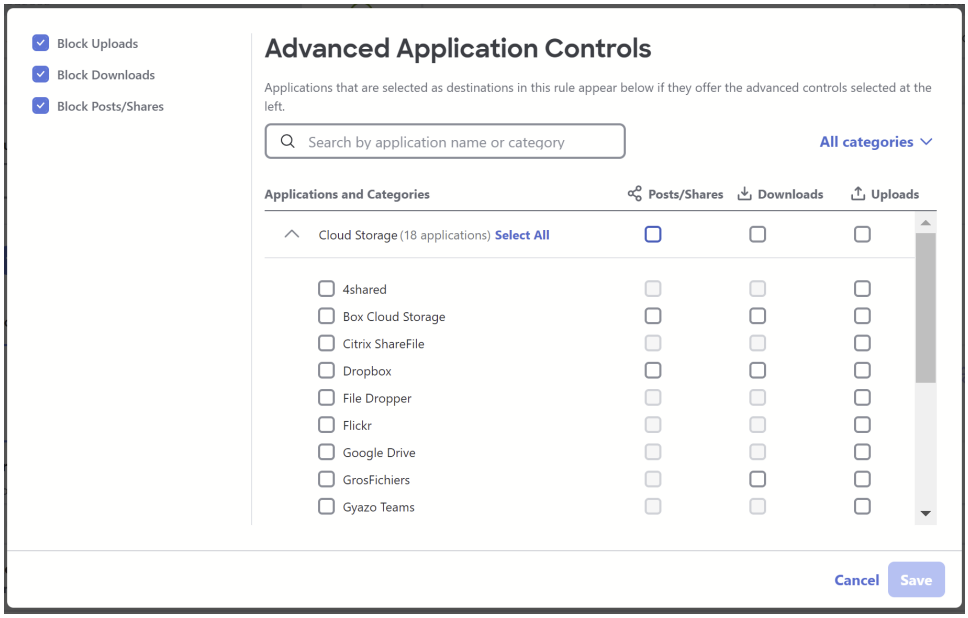
- Full Admin user rule. For more information, see Manage Accounts.

Procedure

1. In an internet access rule, add as destinations any application categories or applications from the table above, or a configured application list that includes any of the above applications or categories.
2. The Advanced Application Controls option will appear:



3. Click **Edit**.
4. In the pane on the left, select the types of activities to block:



5. (Optional) Filter the list in the main pane by clicking **All categories** and choosing a category.
6. In the main pane, select the activities to block for each application in the list
7. (Optional) If you filtered the list, choose a different category, then select the activities to block for that category.

   Repeat as needed for each category in the **All categories** list.
8. Click **Save**.

Troubleshooting

Describes troubleshooting. If advanced application control is not working as expected, check the following: Decryption must be enabled in the security profile selected in the rule.

If advanced application control is not working as expected, check the following:

- Decryption must be enabled in the security profile selected in the rule.
- The site must not be on the **Do Not Decrypt** list selected in the security profile.
- The domain–for example, dropbox.com–is not configured for **Bypass Web Proxy** on the **Connect** > **End User Connectivity** > **Internet Security** page. Any domains or IPs on this list will bypass Secure Access and be routed by your local DNS server. This list applies to PAC file and AnyConnect deployments.
- When an application is blocked, a web notification page will not be displayed. Instead, an error message will be displayed in the application.

About Configuring Sources in Internet Access Rules

Describes about configuring sources in internet access rules. Secure Access internet rules enable you to configure DNS and Web security for your organization's web traffic. You can add pre-configured source components or IP addresses and CIDR blocks on a source in an internet rule.

Secure Access internet rules enable you to configure DNS and Web security for your organization's web traffic. You can add pre-configured source components or IP addresses and CIDR blocks on a source in an internet rule. When you add

multiple network address components on the sources, Secure Access combines the components as a set using the boolean OR operator.

Source Components for Internet Access Rules

Describes source components for internet access rules. You should pre-configure sources for internet access rules. See Source Components for Internet Access Rules.

You should pre-configure sources for internet access rules. See Source Components for Internet Access Rules.

If you see an option to "Select All", this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in future.

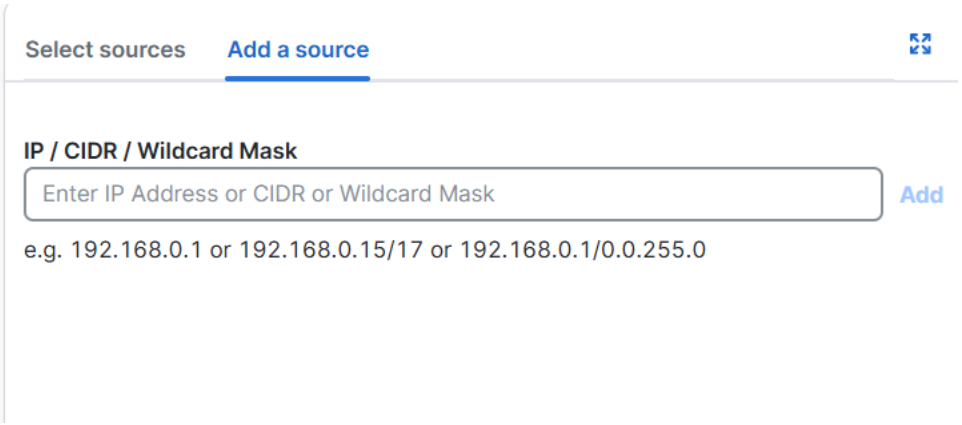
If you select Network Tunnel Groups, Secure Access secures and controls access from traffic from IPsec tunnels established by your supported network devices. If you need to know what tunnels are included in a group, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and look at the group configuration.

If you select a network tunnel group, the destination also includes IP addresses configured in the network tunnel group for routing, in addition to all associated Internal Networks. IP addresses include routes advertised using Border Gateway Protocol, if that option is selected in the network tunnel group configuration.

Sources Added Directly in an Internet Access Rule

Describes sources added directly in an internet access rule. You can enter IP addresses and CIDR blocks directly in an internet rule. If you want to specify a port or protocol, specify those in the destination of the rule.

You can enter IP addresses and CIDR blocks directly in an internet rule. If you want to specify a port or protocol, specify those in the destination of the rule.



IP Addresses and CIDR Blocks

- Sources accept private non-routable IPs (RFC-1918 compliant) or IPs for Registered Networks in Secure Access.
- Sources do not require a deployed IPsec tunnel for the source IP address.
- Sources only accept valid IP addresses.

Combining Multiple Sources in a Rule (Boolean logic)

Describes combining multiple sources in a rule (boolean logic). If an internet access rule includes multiple sources, the following boolean logic applies:

If an internet access rule includes multiple sources, the following boolean logic applies:

- All types of sources, and all sources within a type, are treated as using the boolean OR operator: Traffic to each source you specify in a rule matches the rule.

For example, if you specify a user group and a network tunnel group as sources, traffic from any member of either group will match the rule.

Global Settings for Internet Access Rules

Describes global settings for internet access rules. Global settings generally apply to all rules. However, some settings apply only to private access rules, not to internet access rules.

Global settings generally apply to all rules. However, some settings apply only to private access rules, not to internet access rules.

Do not change global settings unless you have a specific reason to do so.

If your company uses either of the following, verify that the applicable global settings are correct for your company:

- Microsoft 365 applications
- Applications that use pinned certificates

Decryption-related settings:

- **Decryption**

  Intrusion prevention requires decryption in order to be effective.

  In general, you should not disable this feature.

  For troubleshooting purposes, you can temporarily disable decryption for intrusion prevention for all access rules.

  This setting applies to both private access rules and internet access rules.

- **Decryption Logging**

  Choose whether to enable or disable logging of decryption events for internet access rules.

For more information about these settings, see Global Settings for Access Rules.

To change default rule settings, see Edit Rule Defaults and Global Settings.

About Isolated Destinations

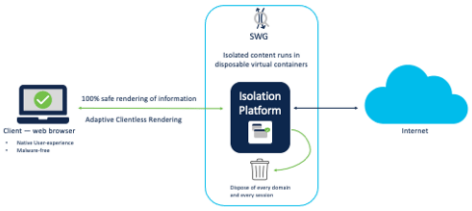
Describes about isolated destinations. Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Your Current Package.

> **Note**
>
> Secure Access Packages and Feature Availability

Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Your Current Package. If you encounter a feature here that you do not have access to, contact your sales representative for more information about your current package. See also, Cisco Secure Access Packages

Remote browser isolation (RBI) protects identities from potential malware and other threats by redirecting browsing to a cloud-based host. Destinations and threat categories supported by RBI can be isolated when added to an Internet access rule in a Secure Access policy. When you add a rule and specify an Isolate rule action, the selected destination or threat

category in the rule will create a remote browser when users attempt to access the content. Instead of blocking identities from the endpoints, a cloud-based browser hosts the browsing session for that destination or threat category.



Prerequisites

Describes prerequisites. There are prerequisites that must be met before you can successfully isolate destinations. Decryption must be enabled for the rule. Make sure it is enabled in the security profile selected in the rule.

There are prerequisites that must be met before you can successfully isolate destinations.

Secure Access Prerequisites

- **Decryption** must be enabled for the rule. Make sure it is enabled in the security profile selected in the rule.
- If a **Do Not Decrypt** list is specified in the security profile, the list cannot include destinations (within destination lists, content categories, or application settings) that are required for isolation to ensure those domains and URLs can be decrypted.
- Destinations required or intended for isolation should not be included your bypass lists. For more information see Manage Domains and Manage Internet Security.

Browser Prerequisites

- Access to third-party cookies enabled.

> **Note**
>
> By default, most browsers (for example, Google Chrome) have third-party cookies blocked in incognito mode. You must update this setting to allow access to third-party cookies for isolation to work.

- Minimum supported browser versions:
  - Apple Safari 9
  - Google Chrome 34
  - Microsoft Edge 12
  - Mozilla Firefox 17
  - Samsung Internet 11
- The Cisco Secure Access root certificate or customer CA-signed certificate must be installed. For more information, see Manage Certificates .

> **Note**
>
> Browser extensions and plugins are not supported and browser-specific features are not guaranteed to work. Regardless of the browser the user initiates the browsing session with, the cloud-based browser for isolation will always be Google Chrome.

Secure Access Package Support for RBI and Isolation Rules

Describes secure access package support for rbi and isolation rules. Secure Access remote browser isolation (RBI) provides an added layer of protection against browser-based security threats for high-risk users. RBI moves the most dangerous part of browsing the internet away from the end user's device and into the cloud.

Secure Access remote browser isolation (RBI) provides an added layer of protection against browser-based security threats for high-risk users. RBI moves the most dangerous part of browsing the internet away from the end user's device and into the cloud. This makes it possible for users to visit risky web destinations safely, enabling users to be productive and access the web destinations they need without negative impacts.

Secure Access provides two levels of RBI support:

Isolate Any

Supported destinations include:

- All content categories
- All destination lists
- All applications
- All threat categories

Isolate Risky

Supported destinations include:

- Uncategorized content categories
- All threat categories

When chosen as the rule action, the availability of destinations and threat categories is based on your Secure Access package's RBI support.

- Isolate Any is bundled with the Secure Access Advantage.
- Isolate Risky is bundled with Secure Access Essentials.
- If you have the Secure Access Essentials package and want the **Isolate Any** capability, you need to upgrade to the Secure Access Advantage package.
- You cannot upgrade your RBI capability independent of the Secure Access Advantage package upgrade.

Limitations of Isolation

Describes limitations of isolation. Policy rule configuration: You can isolate either destinations or threat categories in a Secure Access policy Internet access rule. You cannot specify both in the same rule. You can create a separate rule for each type.

- **Policy rule configuration:** You can isolate either **destinations** or **threat categories** in a Secure Access policy Internet access rule. You cannot specify both in the same rule. You can create a separate rule for each type.
- **Page requests:** Only top-level page requests can be isolated and pages can either be entirely isolated (top-level request and resource requests) or not.
- **Application actions:** Isolation only functions for an entire application, not for specific actions such as uploads or posts. When an application is isolated, it can no longer be blocked, allowed, or warned, even at the action level. For example, if one rule in a ruleset is configured to block Box Cloud Storage uploads, but another rule is configured to isolate Box Cloud Storage for the same identities, uploads for Box Cloud Storage will **not** be blocked.
- **Package status:** If your Secure Access package expires or downgrades, any rule with **Isolate** will no longer work as expected. You should review and update the **Action** setting for these rules as needed.

Troubleshoot Internet Access Rules

Describes troubleshooting internet access rules. To troubleshoot internet access rules: Problems while creating the rule Problems after creating a rule

To troubleshoot internet access rules:

- Problems while creating the rule
- Problems after creating a rule

General troubleshooting tips

- Navigate to the Overview page for possible status notifications
- Use Activity Search to look for logged events

Problems while creating the rule

Describes problems while creating the rule. The Next button is unavailable The Next button is not available until you give the rule a name and then click out of the Rule name field.

The Next button is unavailable

The Next button is not available until you give the rule a name and then click out of the **Rule name** field.

Problems after creating a rule

Describes problems after creating a rule. Internet traffic is unexpectedly blocked Internet traffic is unexpectedly allowed Internet Access rule is not matching traffic as expected

- Internet traffic is unexpectedly blocked
- Internet traffic is unexpectedly allowed
- Internet Access rule is not matching traffic as expected

Internet traffic is unexpectedly blocked

Describes internet traffic is unexpectedly blocked. A few things to try, either to temporarily suspend problematic blocks to allow end users to access a needed resource, or to narrow down the cause of the problem:

A few things to try, either to temporarily suspend problematic blocks to allow end users to access a needed resource, or to narrow down the cause of the problem:

- Because traffic to internet destinations is allowed by default, there may be one or more existing rules that explicitly block this traffic.
- You can temporarily disable a rule that blocks desired traffic.
- To allow immediate access to a necessary destination that is being blocked by another rule, create a new access rule (using the "Enter manually" option for source and/or destination if necessary) and put this rule at or near the top of the rule list on the Policy page so it hits before more general rules that would otherwise apply to the traffic.
- Try disabling enforcement of certain web security features for a rule, in the Advanced settings at the bottom of the Security Controls section of the rule.
- Try disabling intrusion prevention (IPS) for a rule.
- Try disabling intrusion prevention (IPS) on the Rule Defaults page, which disables it for all rules that are configured to use the default setting for IPS.
- Try disabling decryption for intrusion prevention (IPS) for all rules in Global Settings, which effectively disables intrusion prevention.
- If the issue involves Microsoft 365 applications or sites that use certificate pinning, check Global Settings.

Internet traffic is unexpectedly allowed

Describes internet traffic is unexpectedly allowed. A few things to try, either to block problematic traffic, or to narrow down the cause:

A few things to try, either to block problematic traffic, or to narrow down the cause:

- Verify that any existing rule blocking the traffic is enabled (toggle at the top of the rule page)
- To immediately block access to a problem destination that is unexpectedly being allowed, you can create a new access rule (using the "Enter manually" option for source and/or destination if necessary).
- Make sure decryption is not disabled in the Security Profile, including in the security profile selected in Rule Defaults.
- Make sure IPS is not disabled in the rule default or in the rule
- Make sure IPS Decryption and Certificate Pinning are not disabled in Global Settings.
- Make sure the destination is not on a Do Not Decrypt list used by the IPS feature or specified in the rule's security profile.
- Make sure web features are being enforced for the rule (Advanced settings at bottom of Security Controls section in the rule)
- Check the configured sources and destinations of the rule you expect to block the traffic to be sure they include the problematic source and destination.
- Check each rule component of the rule you expect to block the traffic (rule action and each security control) to be sure each specifies the behavior you expect.
- Check the rule order; traffic may be hitting a different rule than the one you expect.

Internet Access rule is not matching traffic as expected

Describes internet access rule is not matching traffic as expected. Some things to try: Make sure the rule is enabled (toggle at top of rule page)

Some things to try:

- Make sure the rule is enabled (toggle at top of rule page)

- Make sure web features are being enforced for the rule (Advanced settings at bottom of Security Controls section in the rule)
- Check the configured sources and destinations of the rule you expect to match the traffic to be sure they include the problematic source and destination.
- Check the rule order; traffic may be hitting a different rule than the one you expect.

30 Get Started With Private Access Rules

Topics:

- Components for Private Access Rules
- Default Settings for Private Access Rules
- Add a Private Access Rule
- About Configuring Sources in Private Access Rules
- About Configuring Destinations in Private Access Rules
- About Endpoint Requirements in Access Rules
- Allowing Traffic from Users and Devices on the Network
- Global Settings for Private Access Rules
- Troubleshoot Private Access Rules

Introduces get started with private access rules. Private access rules control and secure access to internal resources and applications that are private and should not be accessed by the general public.

Private access rules control and secure access to internal resources and applications that are private and should not be accessed by the general public.

Traffic to private destinations is blocked by default. You must create rules to allow traffic to private destinations.

1. **Plan your private access rule**

   Plan your rule so that you get the results you expect. For example, factors such as rule order impact traffic handling.

2. **Create rule components.**

   You will assemble rules largely from components, including but not limited to source, destination, endpoint posture, and security control components. For more information, see Components for Private Access Rules.

3. **Specify rule defaults.**

   New rules will use the default security controls and other settings that you specify on the Rule Defaults page. For more information, see Default Settings for Private Access Rules.

4. **Add private access rules**

   Generally, you will create rules to allow access to private resources. For more information, see Add a Private Access Rule.

5. **Configure logging for the default private access rule**

   Traffic to private destinations that does not match any other private access rule in the policy will be handled by the default private access rule. Traffic that matches this rule is **blocked**. For more information, see Edit the Default Access Rules.

6. **Edit the global settings**

   For more information, see Global Settings for Private Access Rules.

7. **Review the rule order**

   Make sure the order of the rules on the Policy page will have the results you expect. For more information, see Edit the Order of the Rules on the Policy Page.

8. **Distribute dummy access URLs to end users**

   For rules allowing access to private resources using browser-based connections, distribute the remotely accessible dummy URL to the users who will use it to connect to the resource. You configure a URL for each resource when configuring the resource. For more information, see Add a Private Resource.

Note

Users who are not allowed access may see a Block page

Users that attempt to access a configured private resource will see a Block page if all of the following are true:

- The user's access is blocked by a Block rule, including by the default private access rule.
- The user's device has the Cisco Secure Client installed.
- Decryption is enabled on the private resource configuration page.
- VPN connections are not enabled on the private resource configuration page.
- Zero Trust connections are enabled for the resource.

You cannot customize this block page, and this block page is NOT the same block page that users see when they attempt to access a blocked internet destination.

Components for Private Access Rules

Describes components for private access rules. You can create access rules by adding rule components that you or others have configured to a rule. Components described in this topic are reusable. You can use the same component (such as a source) in multiple rules, speeding and simplifying rule creation.

You can create access rules by adding rule components that you or others have configured to a rule. Components described in this topic are reusable. You can use the same component (such as a source) in multiple rules, speeding and simplifying rule creation. For example, you can define a set of users as a source, then use the same source in an internet access rule and in a private access rule for the same set of users. Some components are profiles, or groups of settings bundled together that you choose as a unit when configuring a rule.

Sources

Describes sources. Users User Groups Network Tunnel Groups You can apply rules to traffic originating from IP addresses in network segments defined by Network Tunnel Groups.

- Users
- User Groups
- Network Tunnel Groups

  You can apply rules to traffic originating from IP addresses in network segments defined by Network Tunnel Groups.
- Internal Networks

  You can apply rules to traffic originating from IP addresses in network segments defined by Internal Networks.

(In a rule, you can also specify sources by entering IP addresses, subnets, and ports, but these are NOT reusable source components.)

See also About Configuring Sources in Private Access Rules.

Destinations

Describes destinations. In a rule, you can also specify destinations by entering IP addresses, subnets, ports, and protocols, but these are not reusable destination components and have serious limitations.

In a rule, you can also specify destinations by entering IP addresses, subnets, ports, and protocols, but these are not reusable destination components and have serious limitations.

- Private Resources
- Private Resource Groups

See also About Configuring Destinations in Private Access Rules.

Private Resources

Describes private resources. Secure Workload routes traffic securely to applications and other resources on your network, based on Private Resource configurations.

Secure Workload routes traffic securely to applications and other resources on your network, based on Private Resource configurations.

Define connection requirements for applications in your data center, including resources on private clouds. You will also specify the types of connections permitted for each resource, including Zero Trust Network Access with and without installed client, and VPN.

See Manage Private Resources.

Private Resource Groups

Describes private resource groups. (Optional) After you add private resources, you can create groups of them for convenience and consistency, to easily apply an access rule to a collection of resources.

(Optional) After you add private resources, you can create groups of them for convenience and consistency, to easily apply an access rule to a collection of resources.

See Add a Private Resource Group.

Endpoint Posture Profiles (for Endpoint Requirements)

Describes endpoint posture profiles (for endpoint requirements). You can require endpoints to meet requirements such as operating system version, firewall, and disk encryption before connecting to a network or resource. _These requirements are rule-matching criteria that determine whether a rule matches the traffic.

You can require endpoints to meet requirements such as operating system version, firewall, and disk encryption before connecting to a network or resource. _These requirements are rule-matching criteria that determine whether a rule matches the traffic.

Endpoint requirements are defined in posture profiles. There are several types of posture profile, depending on the type of connection and characteristics of the end-user device:

- **Client-based zero-trust posture profiles**: For end-user devices on which the Cisco Secure Client is installed
- **Browser-based zero-trust posture profiles**: For end-user devices on which the Cisco Secure Client is NOT installed
- **VPN posture profiles**: For end-user devices that are connected to the network using remote access VPN.

When you configure a private resource, you will specify which of the above types of connections are allowed for that resource.

When you create a private access rule, you will specify a posture profile with device requirements for each type of connection allowed by the private resources specified as destinations in the rule.

You can create different posture profiles, each with a different set of requirements, then choose appropriate profiles for each rule.

You can specify default posture profiles for zero-trust access connections (client-based and browser-based.) Create a profile with the desired default endpoint requirements for each connection type, then specify the default profiles on the Rule Defaults page. See Rule Defaults and Edit Rule Defaults and Global Settings.

Posture profile options apply only to User and User Group sources.

VPN posture is evaluated when the user connects to the network, which occurs before access rules evaluate the traffic.

Endpoint posture is not evaluated for branch connections.

See Manage Endpoint Security.

Security Controls

Describes security controls. Private access rules have (and need) less varied security controls than internet access rules. Intrusion Prevention protects your network and assets by inspecting traffic for specified threat characteristics. Threat signatures are collected into collections called IPS Profiles.

Private access rules have (and need) less varied security controls than internet access rules.

Intrusion Prevention (IPS)

Intrusion Prevention protects your network and assets by inspecting traffic for specified threat characteristics. Threat signatures are collected into collections called IPS Profiles.

When you configure an access rule, you can choose a predefined IPS profile such as Balanced Security and Connectivity or Maximum Security, or create a custom profile using Snort signatures that you choose. You can also choose whether to block or just monitor traffic that matches an IPS profile.

You can specify a default IPS profile on the Rule Defaults page that is automatically selected in each new rule. Default settings apply to both private access rules and internet access rules. See Rule Defaults and See Edit Rule Defaults and Global Settings.

See Manage IPS Profiles.

Default Settings for Private Access Rules

Describes default settings for private access rules. You can choose default settings that will automatically populate newly created access rules by default.

You can choose default settings that will automatically populate newly created access rules by default.

Configure these settings on the Rule Defaults page: Navigate to **Secure** > **Access Policy**, click **Global Settings and Rule Defaults**, then click the **Rule Defaults** tab.

The following settings apply to private access rules:

- **Zero Trust Connection Endpoint Posture Profiles**

  Posture profiles specify end-user device requirements when connecting to private resources using zero-trust access. Specify default requirements for connections from devices on which the Cisco Secure Client is installed and from devices on which the client is not installed.

  When choosing default posture profiles, keep in mind that if endpoints do not meet the requirements specified in the profile selected in a rule, the rule will not match the traffic.

  For more information about these posture profiles, see Manage Zero Trust Access Posture Profiles.

- **Zero Trust Access: User Authentication Interval**

  Specify the frequency with which end user must sign in to the network, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network.

  For details, see Network Authentication for Zero Trust Access.

- **Intrusion Prevention (IPS) Profile**

  Specify the traffic-inspection behavior to use by default in new access rules.

  Important

  This setting applies to both private access rules and internet access rules.

  For more information about IPS Profiles, see Manage IPS Profiles.

The other settings on the Rule Defaults page apply only to internet access rules.

To edit default settings, see See Edit Rule Defaults and Global Settings.

Important

Choose rule defaults carefully; changing these settings later may impact existing rules. See Important Information About Changing Rule Defaults.

Add a Private Access Rule

Describes adding a private access rule. Cisco Secure Access connects users, devices, both public and branch networks, and network tunnels to private resources in your enterprise. Private resources are applications and services that you deploy on your enterprise's infrastructure or private cloud.

Cisco Secure Access connects users, devices, both public and branch networks, and network tunnels to private resources in your enterprise. Private resources are applications and services that you deploy on your enterprise's infrastructure or private cloud. When you add a private resource to your organization, Secure Access enables Branch network connections to the resource.

Once you add your sources and private resources to Secure Access, you can create private access rules with these source and destination components. For more information, see Components for Private Access Rules.

In a private access rule, add the source or destination components that you configured for your organization. You can also enter sources and destinations directly into your rules. These single-use source and destination components are only available on an access rule, not shared by your policy.

The access rule defines the **Action**, **Source**, **Security Controls**, and **Destinations** for the rule. In your private access rule's **Security Controls**, Secure Access provides a default Intrusion Prevention System (IPS) profile. You can configure and apply other IPS profiles for your Branch networks to Private Resources rules. For more information, see Manage Private Access Rules.

Prerequisites

Describes prerequisites. Full Admin user role. For more information, see Manage Accounts. Add sources to your organization. For more information, see Components for Private Access Rules.

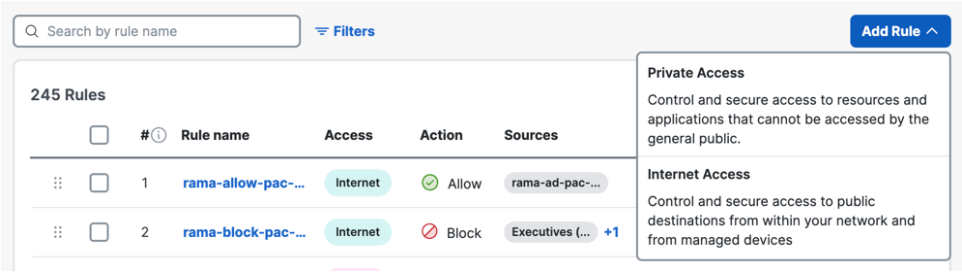
- Full Admin user role. For more information, see Manage Accounts.
- Add sources to your organization. For more information, see Components for Private Access Rules.
- Add Private Resources to your organization. For more information, see Add a Private Resource.
- Edit Default Settings for Private Access Rules.

Set Up the Private Access Rule

Provides instructions for setting up the private access rule. Navigate to Secure Access Policy . Click Add Rule, and then choose Private Access.

Procedure

1. Navigate to **Secure** > **Access Policy**.



2. Click **Add Rule**, and then choose **Private Access**.

   At the top of the rule is a summary that describes the configured components of your rule.



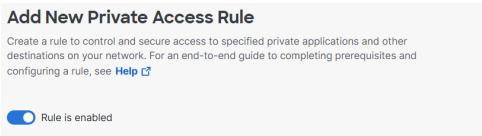
Enable the Rule and Edit Your Logging Settings

Provides instructions for enabling the rule and edit your logging settings. Toggle the rule to enable it. After you configure and save the rule to your policy, the rule is enabled.

Procedure

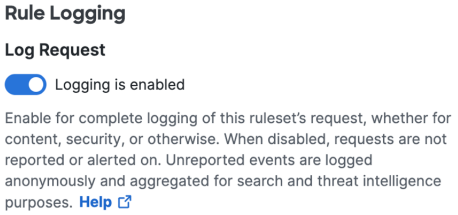
1. Toggle the rule to enable it. After you configure and save the rule to your policy, the rule is enabled.

   You can toggle off the rule at any time to disable it.

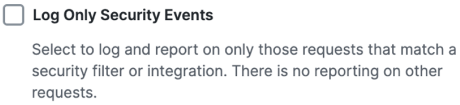
   

2. Click **Edit** to manage your logging settings on the access rule.

   a. For **Log Request**, toggle off or on to choose whether Secure Access logs the events for the traffic managed by the access rule.

   b. For **Log Only Security Events**, select whether Secure Access logs the events that match the security filters. For more information, see Manage Logging.

Add a Rule Name

Provides instructions for adding a rule name. For Rule name, add a meaningful name for your access rule. The Rule name is required. You must give your rule a name before you can continue to configure the Security Controls on the access rule.

Procedure

For **Rule name**, add a meaningful name for your access rule.

The **Rule name** is required. You must give your rule a name before you can continue to configure the **Security Controls** on the access rule.

> **Note**
>
> The **Next** button on the access rule is not available until you enter a name for the rule.



Choose a Rule Order

Provides instructions for choosing a rule order. For Rule order, choose a new priority for the rule, or keep the rule order assigned to the rule by Secure Access.

Procedure

For **Rule order**, choose a new priority for the rule, or keep the rule order assigned to the rule by Secure Access.

When you add a new rule, Secure Access assigns the next lowest priority to the rule. Secure Access applies the first rule in the list on the Policy page that matches the traffic. Order your rules so that more specific rules that might apply to the traffic are above more general rules. For more information, see Edit the Order of Rules on the Access Policy Page.

What to do next



Step 1 — Specify Access Options

Describes step 1 – specify access options. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- Rule Action
- Sources
- Destinations
- Endpoint Requirements
- User Authentication Requirements

Rule Action

Provides instructions for rule action. Choose Allow or Block to assign how Secure Access applies the configured components in the access rule.

Procedure

Choose **Allow** or **Block** to assign how Secure Access applies the configured components in the access rule.

Note

Secure Access blocks the traffic in your organization to private destinations unless an access rule allows the connections.

What to do next

Note

When the action is **Allow** and the traffic does not pass the security controls defined in the rule, Secure Access blocks the traffic.

Sources

Provides instructions for sources. We recommend that you use your organization's reusable source components in your access rules. For more information, see Components for Private Access Rules: Sources.

We recommend that you use your organization's reusable source components in your access rules. For more information, see Components for Private Access Rules: Sources.

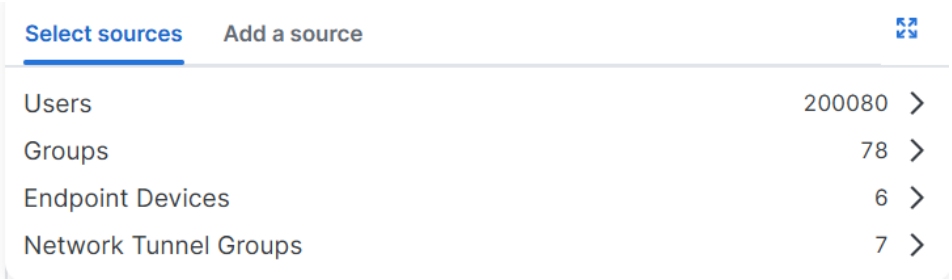
Note

The connection methods for a destination depend on the type of sources that you choose.

If you select Users or User Groups, you can choose destinations enabled for virtual private networks (VPNs) and Zero Trust Access connections, not Branch connections.

Procedure

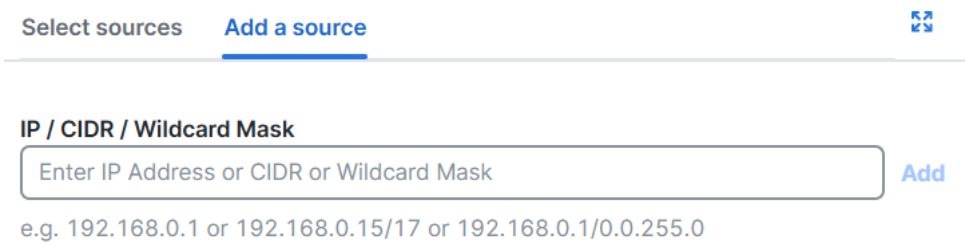
1. For **Select sources**, click in the white space beside the default value ("Any") and choose the configured source components in your organization. When you finish choosing your sources, click **Done**.



2. For **Add a source**, enter an IP or CIDR address as network connection source in the access rule, and then click **Add**. When you finish adding your sources, click **Done**.

What to do next

For more information, see About Configuring Source in Private Access Rules.



> **Note**
>
> The arrows out icon opens a window to configure the sources in your rule.

Destinations

Provides instructions for destinations. We recommend that you use your organization's configured destination components in your access rules. For more information, see Components for Private Access Rules: Destinations.

We recommend that you use your organization's configured destination components in your access rules. For more information, see Components for Private Access Rules: Destinations.

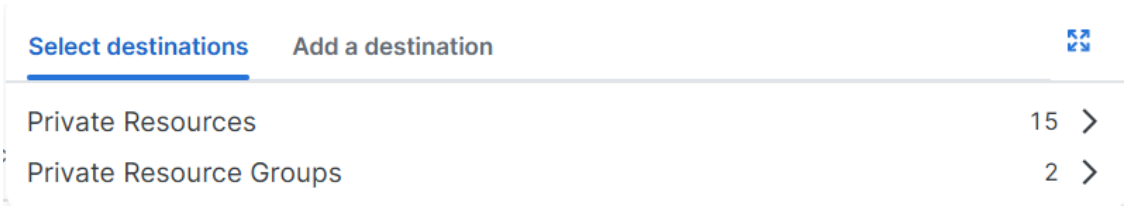
Procedure

1. For **Select destinations**, click in the white space beside the default value ("Any") and choose the configured **Private Resource Groups** and **Private Resources** in your organization. When you finish choosing your private resources, click **Done**.

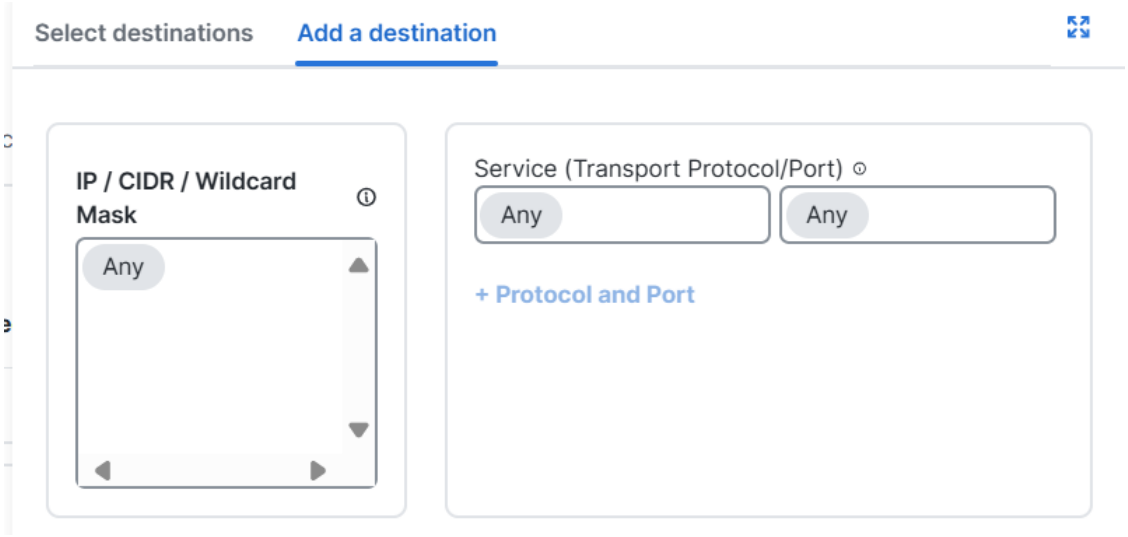
   > **Note**
   >
   > The arrows out icon opens a window to configure the destinations in your rule.

   a. For each **Private Resource**, hover over the network connections icons.

   Secure Access describes the type of network connections supported by the private destination.

2. For **Add a destination**, select **Port**, **IP/CIDR Address**, and **Protocol**. Choose from one of the supported protocols: **Any**, **TCP**, **UDP**, or **ICMP**. After each selection, click **Add**. When you finish adding the attributes of the private destination, click **Done**.



What to do next

To allow VPN access to a private resource, specify its IP or CIDR address, subnet, port, or protocol with the **Add a destination** option.

> **Note**
>
> You might use this option to allow users from one branch to access private applications in another branch.
>
> Destinations that you enter manually are not reusable in another access rule.

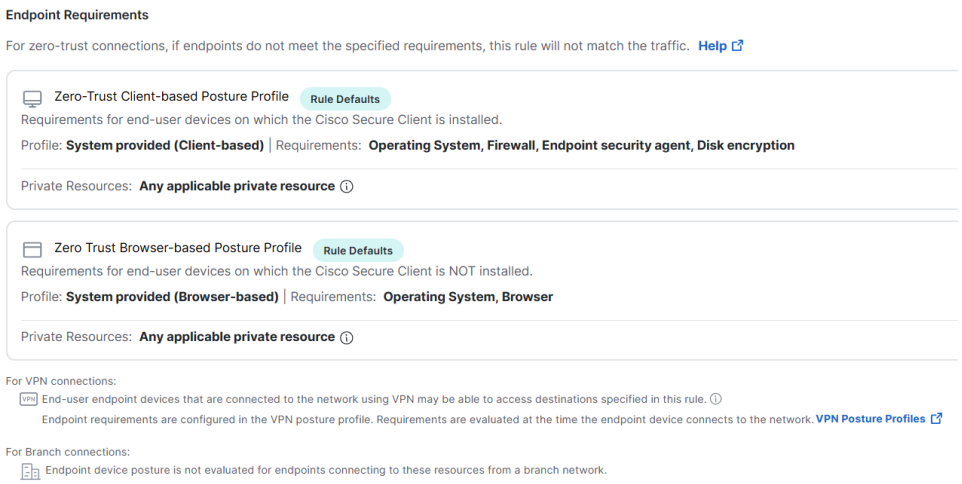
For more information, see About Configuring Destinations in Private Access Rules.

Endpoint Requirements

Describes endpoint requirements. Branch connections to private destinations do not require additional configuration. For important information about endpoint requirements and traffic handling, see About Endpoint Requirements in Access Rules.

Branch connections to private destinations do not require additional configuration. For important information about endpoint requirements and traffic handling, see About Endpoint Requirements in Access Rules.

For general information about posture profiles, see Manage Endpoint Security.

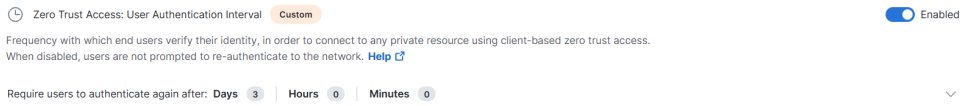


User Authentication Requirements

Describes user authentication requirements. For Zero Trust Access: User Authentication Interval, toggle on or off whether Secure Access prompts users to authenticate before connecting to private destinations.

For **Zero Trust Access: User Authentication Interval**, toggle on or off whether Secure Access prompts users to authenticate before connecting to private destinations.

When **Zero Trust Access: User Authentication Interval** is enabled, you can set the interval when Secure Access requests that you authenticate.



This setting determines how often users must sign in to the network in order to make a Zero Trust connection to a private resource specified as a destination in this rule. Users are prompted to sign in only once per interval if they try to connect to a resource during that time, regardless of the private resources they access.

This option appears only if destinations include at least one private resource.

You can use the default interval as configured on the Rule Defaults page or specify a different interval.

For more information, see Network Authentication for Zero Trust Access.

Step 2 — Configure Security Control Options

Provides instructions for step 2 – configure security control options. Its purpose, requirements, and key details for Cisco Secure Access administrators.

Intrusion Prevention (IPS) is the only security control option needed for private access rules.

Procedure

1. Use the default IPS profile as specified on the Rule Defaults page, or choose a different IPS profile that includes the threat detection settings that you want applied to traffic that matches this rule.
2. Click **Save**.

> **Note**
>
> We recommend that you do not disable your IPS Profiles. For more information, see Manage IPS Profiles.

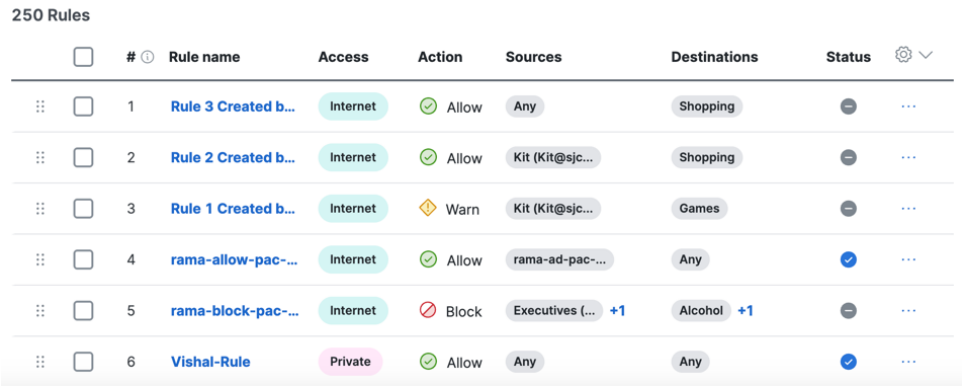
Summary

Provides instructions for summary. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

After you add a rule to your policy, you can edit the rule and then view the rule summary.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Navigate to a rule, and then click on the horizontal elipsis (**...**) to expand the rule menu.



3. Click **Edit** to open the rule and view the rule summary.



What to do next

The summary contains the components that you configured on the access rule:

- **Sources**
- **Action**
- **Security Controls**
- **Destinations**

If you see an **Upgrade** button, this means that your organization has an opportunity to upgrade to a subscription that offers additional functionality. For more information, see Contact Cisco Secure Access Support.

About Configuring Sources in Private Access Rules

Describes about configuring sources in private access rules. Let the following information guide you when you add sources to a private access rule. Source Components Sources created directly in Private Access Rules If there are multiple sources in a rule (Boolean logic)

Let the following information guide you when you add sources to a private access rule.

- Source Components
- Sources created directly in Private Access Rules
- If there are multiple sources in a rule (Boolean logic)

Source components

Describes source components. If you see an option to "Select All", this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in future

- If you see an option to "Select All", this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in future
- When you select Network Tunnel Groups, Secure Access secures and controls access from traffic from IPsec tunnels established by your supported network devices. If you need to know what tunnels are included in a group, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and look at the group configuration.

Sources created directly in a private access rule

Describes sources created directly in a private access rule. If you want to specify port or protocol, specify those in the destination of the rule.

If you want to specify port or protocol, specify those in the destination of the rule.

If you will allow access from a branch network, and you specify users or user groups, you must also configure SAML authentication for those users.

If there are multiple sources in a rule (Boolean logic)

Describes if there are multiple sources in a rule (boolean logic). If a rule includes multiple sources, the following boolean logic applies:

If a rule includes multiple sources, the following boolean logic applies:

All types of sources, and all sources within a type, are treated as using the boolean OR operator: Traffic to each source you specify in a rule matches the rule.

For example, if you specify a user group and then type in a CIDR block, traffic that either belongs to the user group or originates from an IP address within the CIDR block will match the rule.

About Configuring Destinations in Private Access Rules

Describes about configuring destinations in private access rules. Let the following information guide you when you add destinations to a private access rule. Destination components for private access rules Destinations created directly in a private access rule If there are multiple destinations in a rule (Boolean logic)

Let the following information guide you when you add destinations to a private access rule.

- Destination components for private access rules
- Destinations created directly in a private access rule
- If there are multiple destinations in a rule (Boolean logic)

Destination components for private access rules

Describes destination components for private access rules. When you select a Private Resource Group, resources that are added to the group in the future are automatically included.

- When you select a Private Resource Group, resources that are added to the group in the future are automatically included.
- If you see an option to "Select All", this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in future
- All configured private resources allow connections from authenticated users on the network, including branch networks.
- Other connection methods (zero trust client-based and browser-based, VPN) for each resource are determined by the private resource configuration.

Destinations created directly in a private access rule

Describes destinations created directly in a private access rule. You can specify IP addresses, CIDR blocks, ports, and protocols directly in an access rule, without creating a private resource first.

You can specify IP addresses, CIDR blocks, ports, and protocols directly in an access rule, without creating a private resource first.

All destinations allow connections from authenticated users on the network, including branch networks.

Zero-trust connections are not available for destinations that are not configured as private resources.

> **Note**
>
> Security controls do not apply to traffic to destinations added directly into a rule:

The following controls are not applied to traffic to destinations that you specify by typing IP addresses, CIDR blocks, ports, or protocols directly into the rule:

- Endpoint posture requirements
- Intrusion prevention (IPS)

If destinations include both configured private resources or groups and destinations typed directly into a rule, security controls are applied only to the configured private resources or groups.

If there are multiple destinations in a rule (Boolean logic)

Describes if there are multiple destinations in a rule (boolean logic). If a private access rule rule includes multiple destinations, the following boolean logic applies:

If a private access rule rule includes multiple destinations, the following boolean logic applies:

- All types of destinations, and all destinations within a type, are treated as using the boolean OR operator: Traffic to each destination you specify in a rule matches the rule.

For example, if you specify a private resource group and a set of IP addresses as destinations in a single rule, traffic to any destination belonging to either group or set will match the rule.

- If you type in values of different types (IP address, port, protocol), traffic matches if any of the specified values match the rule.

  For example, if you specify an IP address and a port, traffic to any IP address on the specified port matches the rule, as does traffic to the specified address on any port.

  If you specify ANY protocol, then all traffic will match the rule, regardless of any other destinations you specify.

About Endpoint Requirements in Access Rules

Describes about endpoint requirements in access rules. If endpoints do not meet the requirements specified in posture profiles, traffic is handled differently for zero trust connections and VPN connections:

> **Note**
>
> Important note about traffic handling

If endpoints do not meet the requirements specified in posture profiles, traffic is handled differently for zero trust connections and VPN connections:

- **For zero trust connections**, if endpoints do not meet the requirements in the posture profile specified in a private access rule, the rule will not match the traffic.

  If no other rule matches the traffic, Secure Access applies the default private access rule, which will block the traffic. The default private access rule appears at the bottom of the list of rules on the Access Policy listing page.

- **For VPN connections**, posture is evaluated at the time the device connects to the network. If endpoints do not meet the requirements specified in the VPN posture profile, the device cannot connect to the network.

For more information about posture profiles, see Manage Endpoint Security.

Allowing Traffic from Users and Devices on the Network

Describes allowing traffic from users and devices on the network. In addition to creating access rules for remote users accessing private resources, you must create rules to allow traffic from users and devices on the network, including those in branch offices.

In addition to creating access rules for remote users accessing private resources, you must create rules to allow traffic from users and devices on the network, including those in branch offices.

Devices that might require such a rule include kiosks, Internet of Things (IOT) devices, and printers.

When you create the rule, you can create one or more private resources to use as sources and destinations, or you can add sources and destinations directly in the rule. For more information, see Manage Branch Connections.

Global Settings for Private Access Rules

Describes global settings for private access rules. Global settings generally apply to all rules. However, some settings apply only to internet access rules, not to private access rules.

Global settings generally apply to all rules. However, some settings apply only to internet access rules, not to private access rules.

The following global settings apply to private access rules:

- **Decryption**

  Intrusion prevention requires decryption in order to be effective.

  For troubleshooting purposes, you can temporarily disable decryption for intrusion prevention for all access rules.

  This setting applies to both private access rules and internet access rules.

- **Decryption Logging**

  Determine whether to enable or disable logging of decryption events for private access rules.

For more information about these settings, see Global Settings for Access Rules.

To change default rule settings, see Edit Rule Defaults and Global Settings.

Troubleshoot Private Access Rules

Describes troubleshooting private access rules. To troubleshoot private access rules: Problems while creating the rule Problems after creating a rule

To troubleshoot private access rules:

- Problems while creating the rule
- Problems after creating a rule

General Troubleshooting Tips

Describes general troubleshooting tips. Navigate to the Overview page for possible status notifications Use Activity Search to look for logged events

- Navigate to the Overview page for possible status notifications
- Use Activity Search to look for logged events

Problems While Creating a Rule

Describes problems while creating a rule. The Next button is not available until you give the rule a name and then click out of the Rule name field.

Next button is not available

The Next button is not available until you give the rule a name and then click out of the Rule name field.

Problems After Creating a Rule

Describes problems after creating a rule. Traffic is unexpectedly blocked Traffic is unexpectedly allowed Rule is not matching traffic as expected

- Traffic is unexpectedly blocked
- Traffic is unexpectedly allowed
- Rule is not matching traffic as expected

Traffic is unexpectedly blocked

Describes traffic is unexpectedly blocked. A few things to try, either to temporarily suspend problematic blocks, or to narrow down the cause:

A few things to try, either to temporarily suspend problematic blocks, or to narrow down the cause:

- Verify that any existing rule allowing the traffic is enabled.
- To allow immediate access to a necessary destination that is being blocked, you can create a new access rule allowing the traffic (using the "Enter manually" option for source and/or destination if necessary).
- You can disable intrusion prevention (IPS) for a rule.
- You can disable intrusion prevention (IPS) on the Rule Defaults page, which disables it for all rules that are configured to use the default setting for IPS.
- You can disable decryption for intrusion prevention (IPS) for all rules in Global Settings, which effectively disables intrusion prevention.
- If a Zero Trust connection is unsuccessful:
  - Make sure that zero trust connections are enabled for the resource.
  - Check the Traffic Steering page (Connect > End User Connectivity > Zero Trust) for absence of, exceptions to, or conflicts with the applicable Private Resource configuration.
  - Endpoint requirements as specified in zero trust posture profiles are rule-matching criteria, not security criteria. Try specifying posture profile(s) that have no requirements and see if the traffic matches.
- If a VPN connection is unsuccessful, ensure that:
  - There is a VPN traffic steering rule for the applicable network address space
  - There is an access rule allowing the traffic (either for a configured private resource or for the applicable network address space)
  - If a Private Resource is configured for the resource, it must permit VPN connections.
- Assess whether the following situation applies: App A is dependent on App B, but App B is not included in the private resource or access rule configurations.

Traffic is unexpectedly allowed

Describes traffic is unexpectedly allowed. A few things to try, either to block problematic traffic, or to narrow down the cause:

A few things to try, either to block problematic traffic, or to narrow down the cause:

- Because traffic to private destinations is blocked by default, this means there is one or more existing rules that explicitly allows this traffic. You will need to find any such rules.
- Make sure the applicable rule is enabled (toggle at top of rule page)
- Make sure IPS is not disabled in the rule default or in the rule. Any rule tagged to use the default setting continues to use the default setting even if the default setting has changed.
- Make sure IPS Decryption is not disabled in Global Settings.
- Check each rule component (rule action and each posture and security control) to be sure each specifies the behavior you expect.
- Check to see that an expected exception to connect to the private resource appears as expected on the Traffic Steering page (Connect > End User Connectivity > Zero Trust.)

- To immediately block access to a problem destination that is unexpectedly being allowed, you can create a new access rule (using the "Enter manually" option for source and/or destination if necessary) and put this rule at or near the top of the rule list on the Policy page so it hits before more general rules that would otherwise apply to the traffic.

Rule does not match traffic as expected

Describes rule does not match traffic as expected. Some things to try: Check the private resource configuration. Check the sources and destinations configured in the rule to be sure they include the problematic source and destination.

Some things to try:

- Check the private resource configuration.
- Check the sources and destinations configured in the rule to be sure they include the problematic source and destination.
- Endpoint requirements as specified in posture profiles are matching criteria, not security criteria. Try specifying posture profile(s) that have no requirements and see if the traffic matches.
- Check other rules in the rule order; traffic may be hitting a different rule than the one you expect.
- If you have configured a Private Resource, then modified the automatically created entry on the Traffic Steering page (for example, to exclude subdomains from zero-trust access), then modified addresses on the Private Resource configuration page, the resource addresses are not updated for traffic steering purposes. You must manually update the address(es) on the Traffic Steering page.

31 Manage Endpoint Security

Topics:

- Manage Endpoint Security

Describes the purpose and procedures for manage endpoint security and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Endpoint Security

Describes managing endpoint security. Secure Access is a converged cloud security solution that enables fast, reliable, and secure private network connections to your applications. End users are assured of a secure, transparent user experience, anywhere they work – office, home, or on the road.

Secure Access is a converged cloud security solution that enables fast, reliable, and secure private network connections to your applications. End users are assured of a secure, transparent user experience, anywhere they work – office, home, or on the road. User devices can read, write, and update private resources by setting up virtual private networks (VPNs) or zero trust network access (ZTNA) connections to Secure Access through IPsec network tunnels.

About Endpoint Posture

Describes about endpoint posture. Posture is a service in Secure Access that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies.

Posture is a service in Secure Access that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control user access to protected areas of a network.

About Posture Profiles

Describes about posture profiles. Posture profiles define requirements for end-user devices when accessing the network and private resources. There are two types of profiles, depending on your connection type:

Posture profiles define requirements for end-user devices when accessing the network and private resources. There are two types of profiles, depending on your connection type:

- **VPN** - Define posture requirements for end-user devices connecting to the network using VPN. The VPN client must be installed on the end-user device. Requirements are checked when the device connects to the network. See Manage VPN Connection Posture Profiles.
- **Zero Trust Access** - Define posture profiles for user devices that connect to resources on the network without using VPN. See Manage Zero Trust Access Posture Profiles.

Endpoint Posture Assessment

Describes endpoint posture assessment. Endpoint posture assessment involves orchestrating and performing data collection and evaluating the posture of a given endpoint.

Endpoint posture assessment involves orchestrating and performing data collection and evaluating the posture of a given endpoint.

Typically, endpoint posture information is gathered and then published to appropriate data repositories to make collected information available for further analysis supporting organizational security processes.

Endpoint posture assessment typically includes:

- Collecting the attributes of a given endpoint;
- Making the attributes available for evaluation and action; and
- Verifying that the endpoint's posture is in compliance with enterprise standards and policy.

Endpoint Attributes

Describes endpoint attributes. The following sections describe the endpoint attributes that are evaluated. This option checks for the existence of any required operating systems that are needed on the endpoint device.

The following sections describe the endpoint attributes that are evaluated.

Supported Operating Systems

This option checks for the existence of any required operating systems that are needed on the endpoint device.

The operating system hosts and manages your data, applications, and connected devices. Inadequate protections for the operating system could also affect the performance of all of these components and ultimately affect productivity of your users and the organization.

The following sections describe the supported operating systems and package dependencies for Secure Access posture profiles.

- Windows
- Mac OS
- Linux

Inadequate protections for the operating system could also affect the performance of all of these components and ultimately affect productivity of your users and the organization.

Firewall Conditions

This option checks for the existence of a firewall on the endpoint device.

- Windows–Require the platform-native firewall to be running on the endpoint device.
- Mac OS X–Require the platform-native firewall to be running on the endpoint device.

Endpoint Security Agents

This option checks for the existence of an endpoint security agent required to be running on the endpoint device.

System Password Enforcement

This option checks whether a system password is required on the endpoint device.

Disk Encryption

This option checks for the existence of disk encryption running on the endpoint device.

Disk encryption ensures that files are always stored on disk in an encrypted form. The files become available to the operating system and applications in readable form while the system is running and unlocked by a trusted user. An unauthorized user inspecting the contents of the disk directly finds garbled random-looking data instead of the actual files.

With user data encryption enabled, the /home directory in the file system is encrypted and user data is available when the system is running. The user /home partition is mounted on a separate disk partition and block level encryption is enabled for that disk.

Supported Browsers

This option checks for the existence of a required web browser on the endpoint device.

Windows Registry Conditions

This option checks for the existence of a registry key or the value of the registry key on the endpoint device.

File Conditions

This option checks for the existence of a file, the date of a file, and the versions of a file on the endpoint device.

Process Conditions

This option checks if an application or process is running or not running on the endpoint device.

Certificate Conditions

This option checks if any required server certificates are present and valid on the endpoint device.

32 Manage Zero Trust Access Posture Profiles

Topics:

- Manage Zero Trust Access Posture Profiles

Describes the purpose and procedures for manage zero trust access posture profiles and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Zero Trust Access Posture Profiles

Describes managing zero trust access posture profiles. These profiles specify end-user device requirements when connecting to private resources using Zero Trust Access.

These profiles specify end-user device requirements when connecting to private resources using Zero Trust Access.

There are two types of profiles to choose from:

- **Client-based** - Choose this as the default profile for devices on which the Cisco Secure Client is installed. See Add a Client-Based Zero Trust Access Posture Profile
- **Browser-based** - Choose this as the default profile for devices on which the Cisco Secure Client **is not** installed. See Add a Browser-Based Zero Trust Access Posture Profile

Client-based access permits more posture requirements than clientless access, so you should tailor profiles to the type of access.

Zero Trust Access Posture Attributes

Describes zero trust access posture attributes. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- Supported operating systems
- Firewall
- Endpoint security agents
- System password
- Disk encryption
- Browser

Add a Client-Based Zero Trust Access Posture Profile

Provides instructions for adding a client-based zero trust access posture profile. Its purpose, requirements, and key details for Cisco Secure Access administrators.

Configure a client-based Zero Trust Access posture profile to define posture requirements for endpoint devices that connect to private resources. Cisco Secure Client must be installed on the endpoint device, and Secure Access checks the requirements when the device connects to the network.

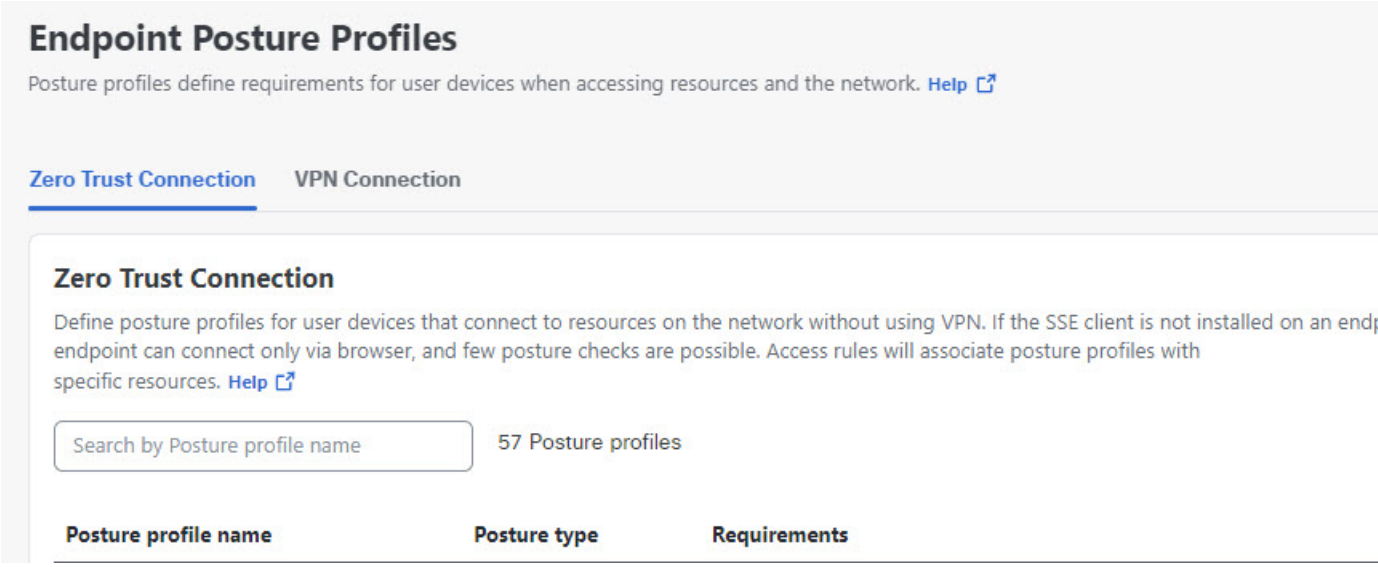
> **Note**
>
> Each requirement is optional, and requirements can be configured in any order. However, endpoints must meet all conditions of any configured requirement.

Before you begin

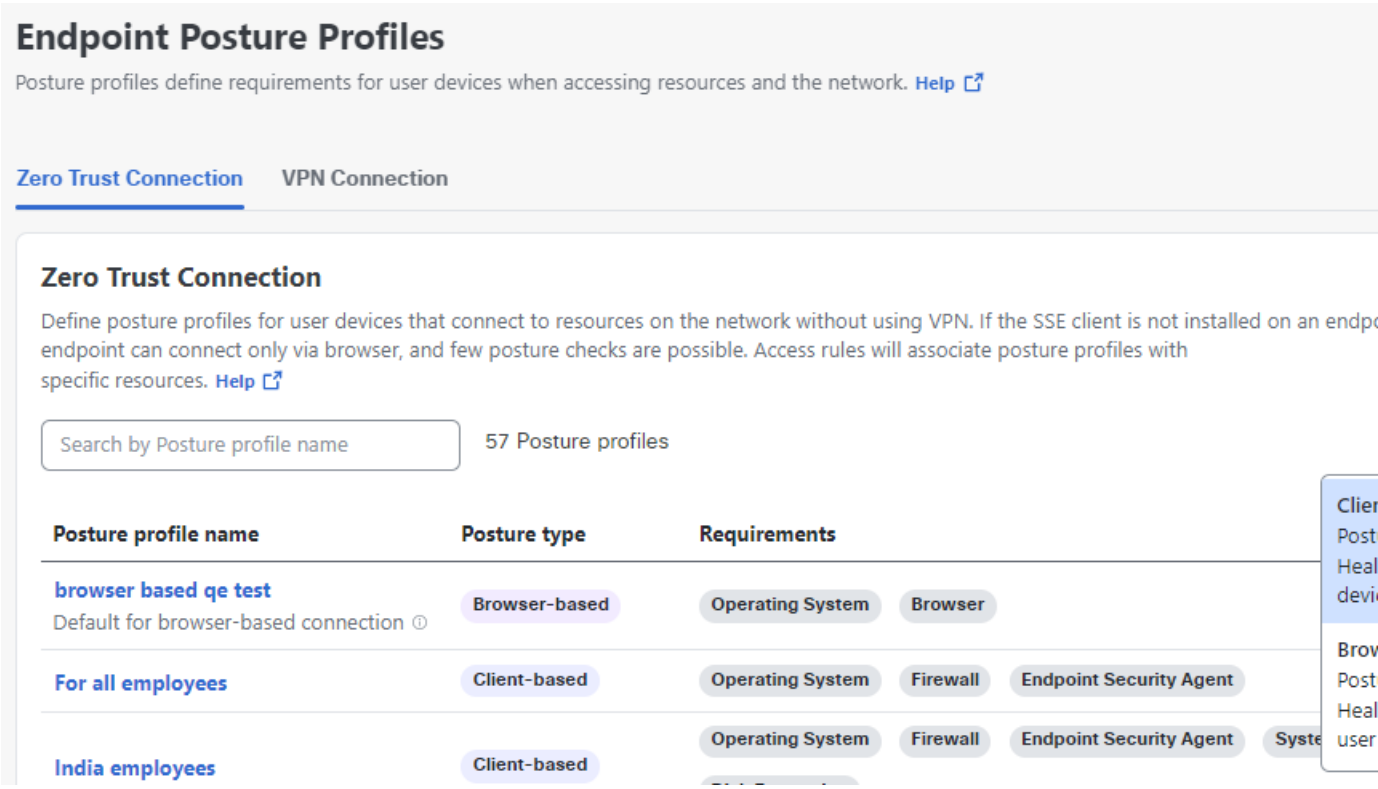
- Full Admin user role. For more information, see Manage Accounts.

Procedure

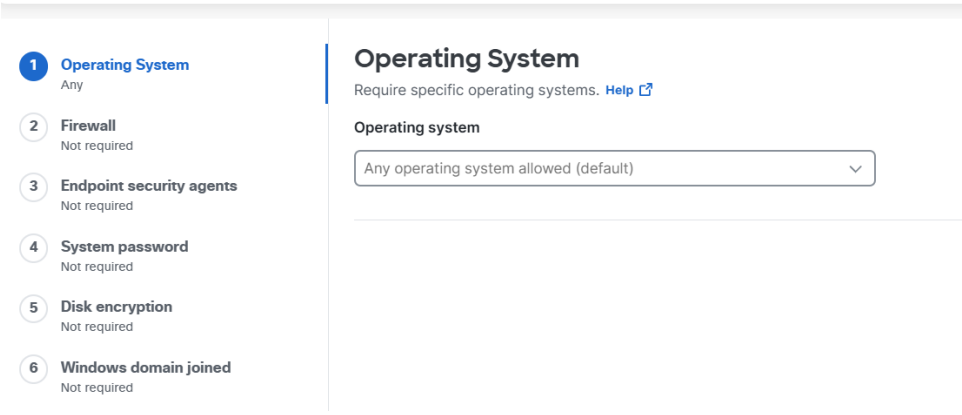
1. Navigate to **Secure** > **Profiles** > **Endpoint Posture Profiles**.



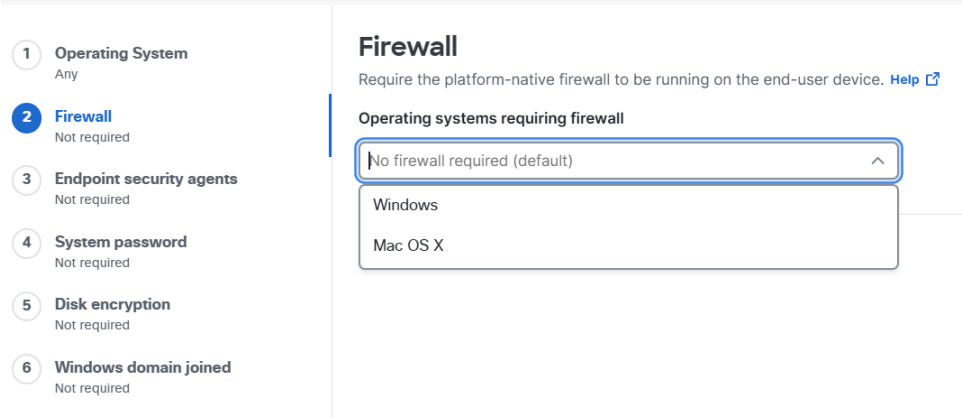
2. For **Zero Trust Connection**, click **Add Posture Profile** and choose **Client-based**.



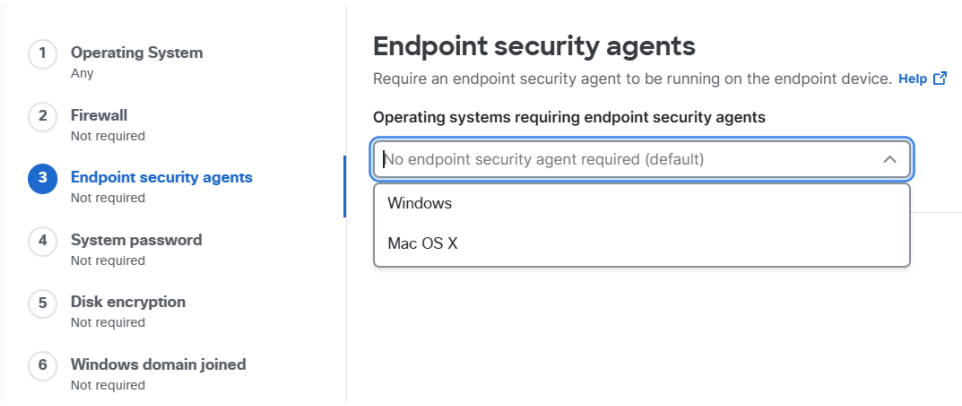
3. Give your posture profile a good descriptive **Name**.
4. For the **Operating System** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select endpoint security agents. See Supported Operating Systems.



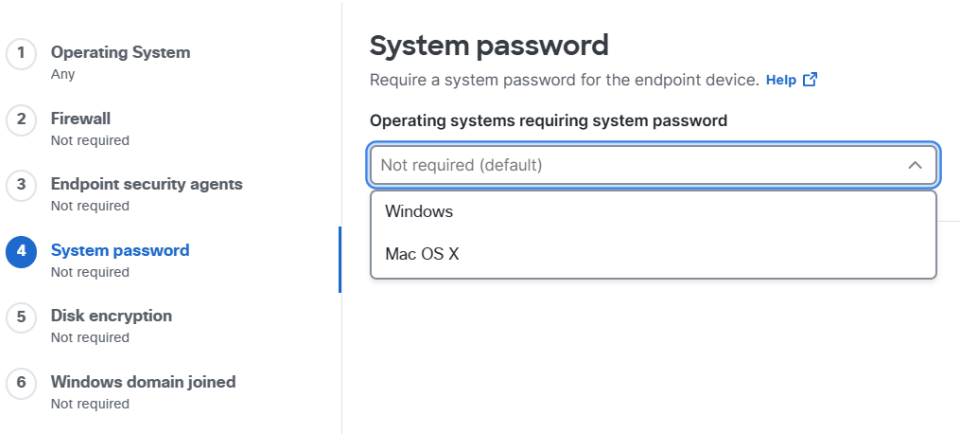
5. For the **Firewall** option, choose the firewall for your profile. Click **Save and Exit** or **Next** to select endpoint security agents. See Firewall Requirements.



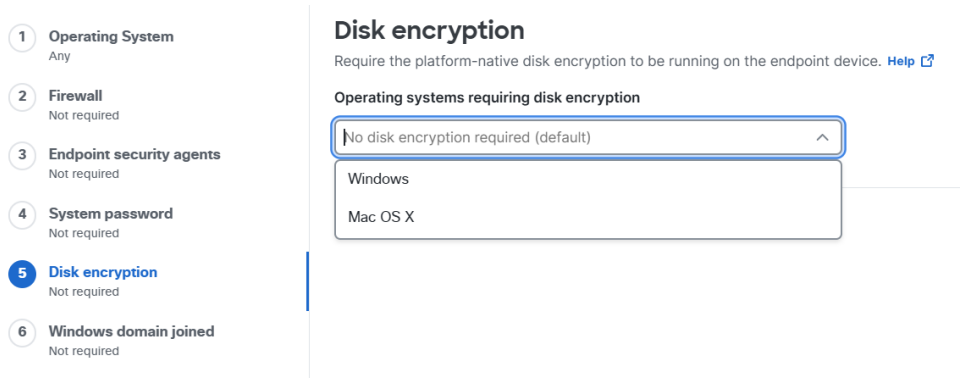
6. For the **Endpoint security agent** option, choose an endpoint security agent for your profile. Click **Save and Exit** or **Next** to select Windows registry entries. See Endpoint Security Agents.



7. For the **System password** option, choose whether to enforce a system password for the endpoint. Click **Save and Exit** or **Next** to select disk encryption. See Endpoint Security Agents.



8. For the **Disk encryption** option, choose the disk encryption package(s) for your profile. Click **Save and Exit** or **Next** to return to the OS requirements. See Disk Encryption.



9. Review and finalize the profile.

Add a Browser-Based Zero Trust Access Posture Profile

Provides instructions for adding a browser-based zero trust access posture profile. Its purpose, requirements, and key details for Cisco Secure Access administrators.

Configure a browser-based Zero Trust Access posture profile to define posture requirements for endpoint devices that connect to private resources. Note that the Cisco Secure Client is not installed on these endpoint devices, and Secure Access checks the requirements when a device connects to the network.

> **Note**
>
> Each requirement is optional; and requirements can be configured in any order. However, endpoints must meet all conditions of any configured requirement.

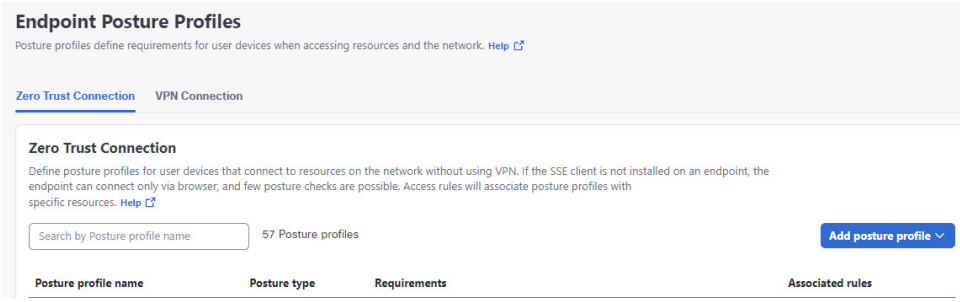
Before you begin

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

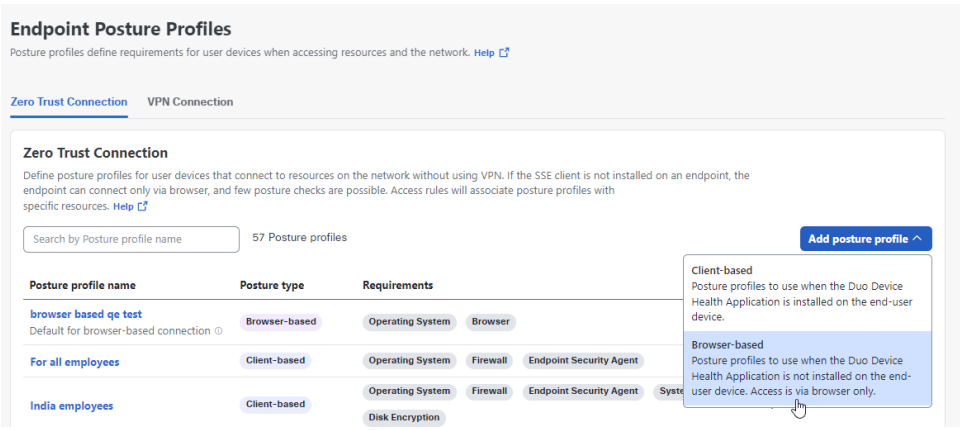
Procedure

---

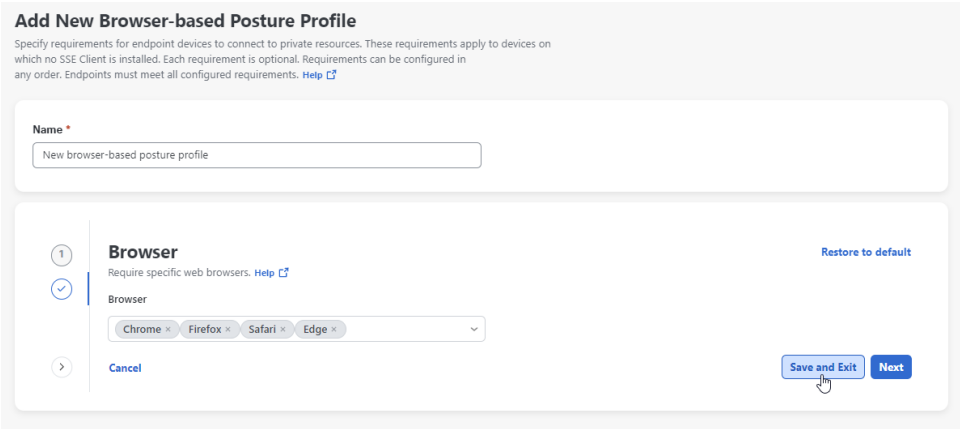
1. Navigate to **Secure** > **Profiles** > **Endpoint Posture Profiles**.



2. For **Zero Trust Connection**, click **Add Posture Profile** and choose **Browser-based**.
3. Give your posture profile a good descriptive **Name**.
4. Add the required operating systems from the drop-down list. Click **Save and Exit** or **Next** to select supported browsers.



5. Add the required browsers from the drop-down list.



6. Click **Save and Exit** to complete the posture profile. Optionally, click **Next** to modify the selected operating systems.

33 Manage VPN Connection Posture Profiles

Topics:

- Manage VPN Connection Posture Profiles

Describes the purpose and procedures for manage vpn connection posture profiles and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage VPN Connection Posture Profiles

Describes managing vpn connection posture profiles. Posture profiles define requirements for user devices when accessing resources and the network. Profiles in this list apply when users access specific resources using VPN. The VPN client must be installed on the end-user device.

Posture profiles define requirements for user devices when accessing resources and the network.

Profiles in this list apply when users access specific resources using VPN. The VPN client must be installed on the end-user device. Requirements are checked when the device connects to the network.

VPN Posture Attributes

Describes vpn posture attributes. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- Operating System
- Endpoint security agent
- Windows registry entries
- Firewall
- Disk encryption
- Files
- Processes
- Certificates

Add a VPN Connection Posture Profile

Provides instructions for adding a vpn connection posture profile. Configure a VPN connection posture profile to define posture requirements for end-user devices connecting to the network using VPN.

Configure a VPN connection posture profile to define posture requirements for end-user devices connecting to the network using VPN. The VPN client must be installed on the end-user device, and Secure Access checks the requirements when the device connects to the network.

> **Note**
>
> Each requirement is optional; and requirements can be configured in any order. However, endpoints must meet all conditions of any configured requirement.

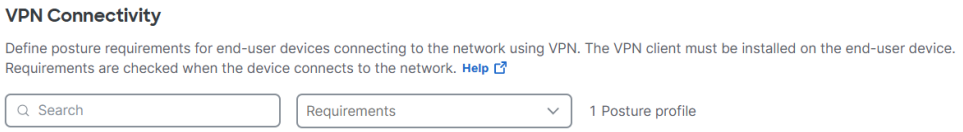
Before you begin

- Valid credentials for the Secure Access dashboard.
- Full Admin role in Secure Access. For more information, see Manage Accounts.

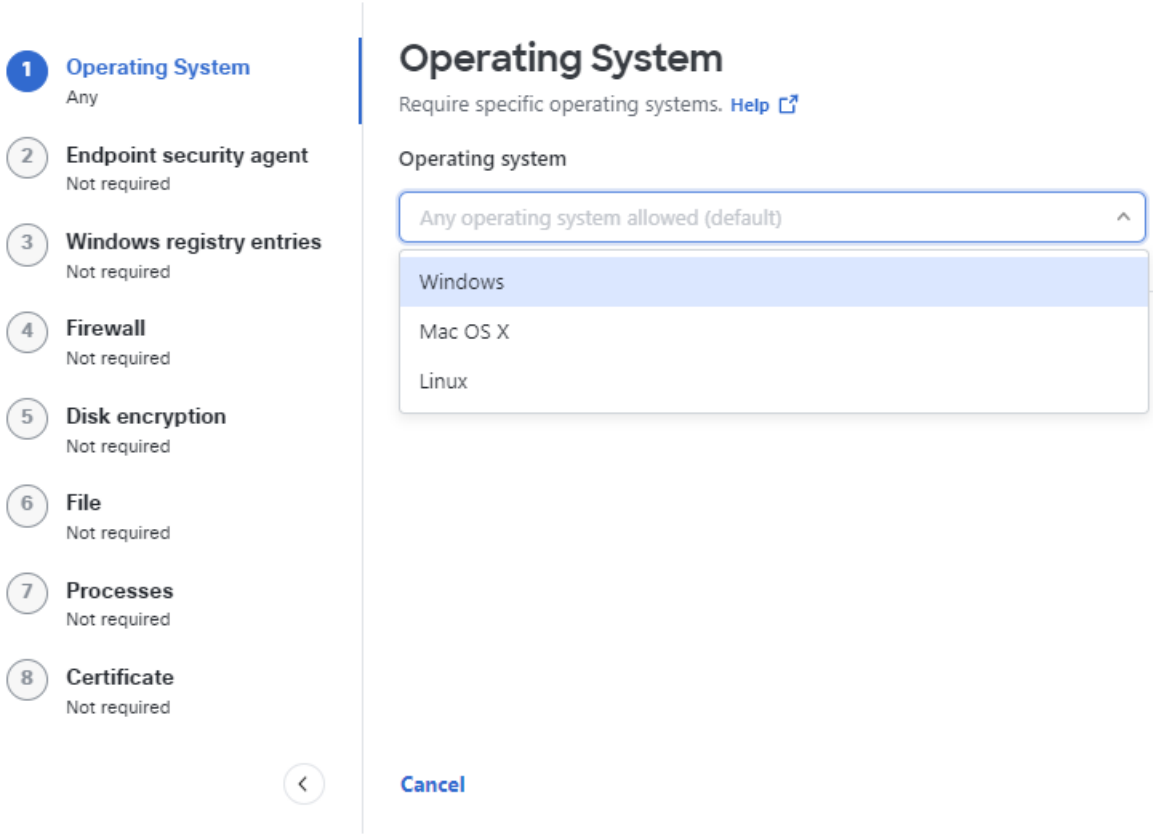
Procedure

1. Navigate to **Secure** > **Profiles** > **Endpoint Posture Profiles**.

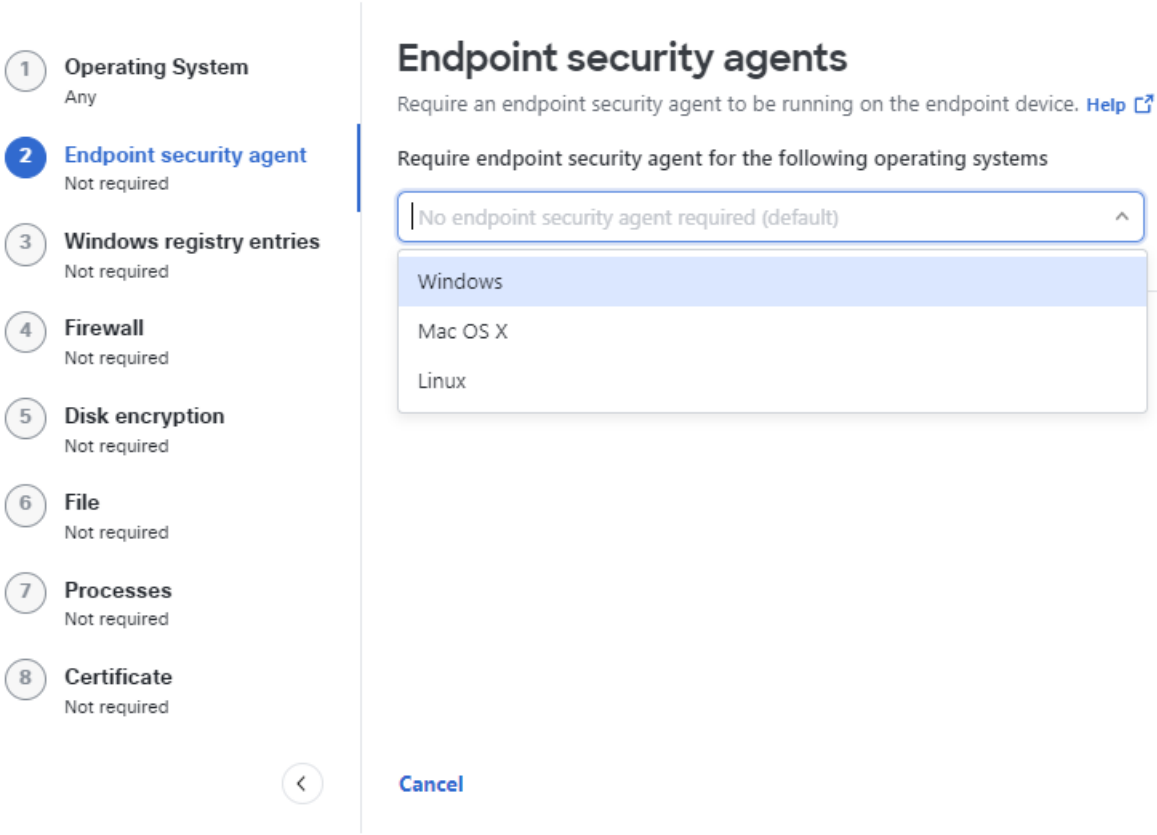
2. For **VPN Connection**, click **Add Posture Profile** .



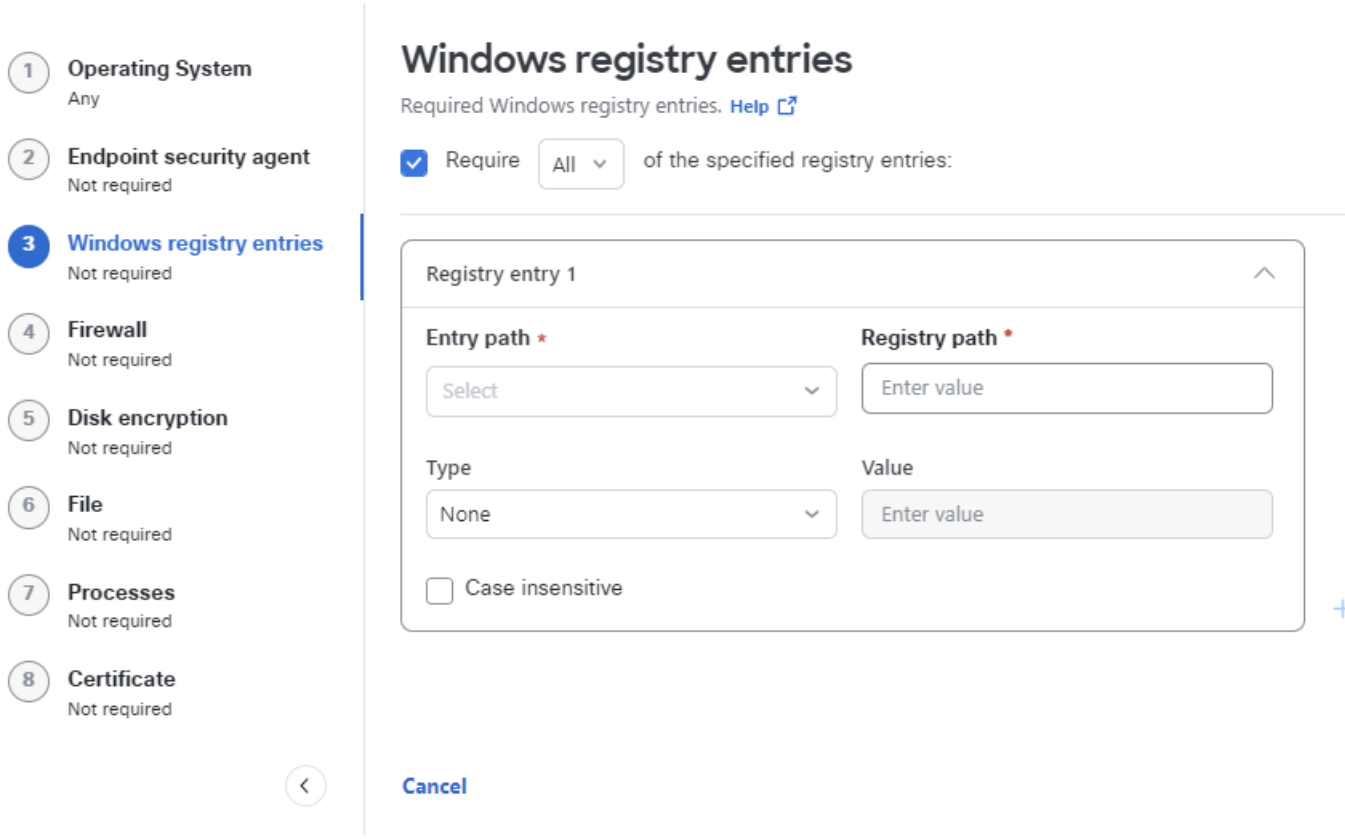
3. Give your posture profile a good descriptive **Name**.
4. For the **Operating System** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select endpoint security agents. See Supported Operating Systems.



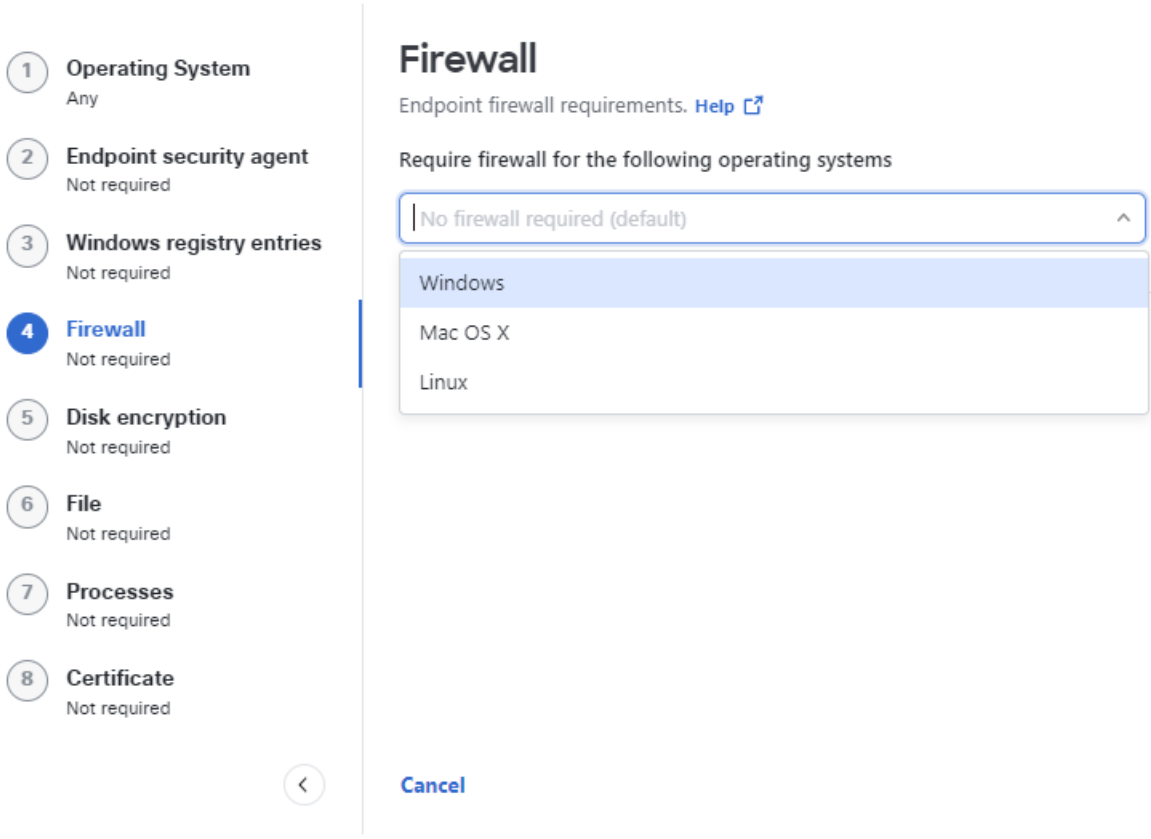
5. For the **Endpoint security agent** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select Windows registry entries. See Endpoint Security Agents.



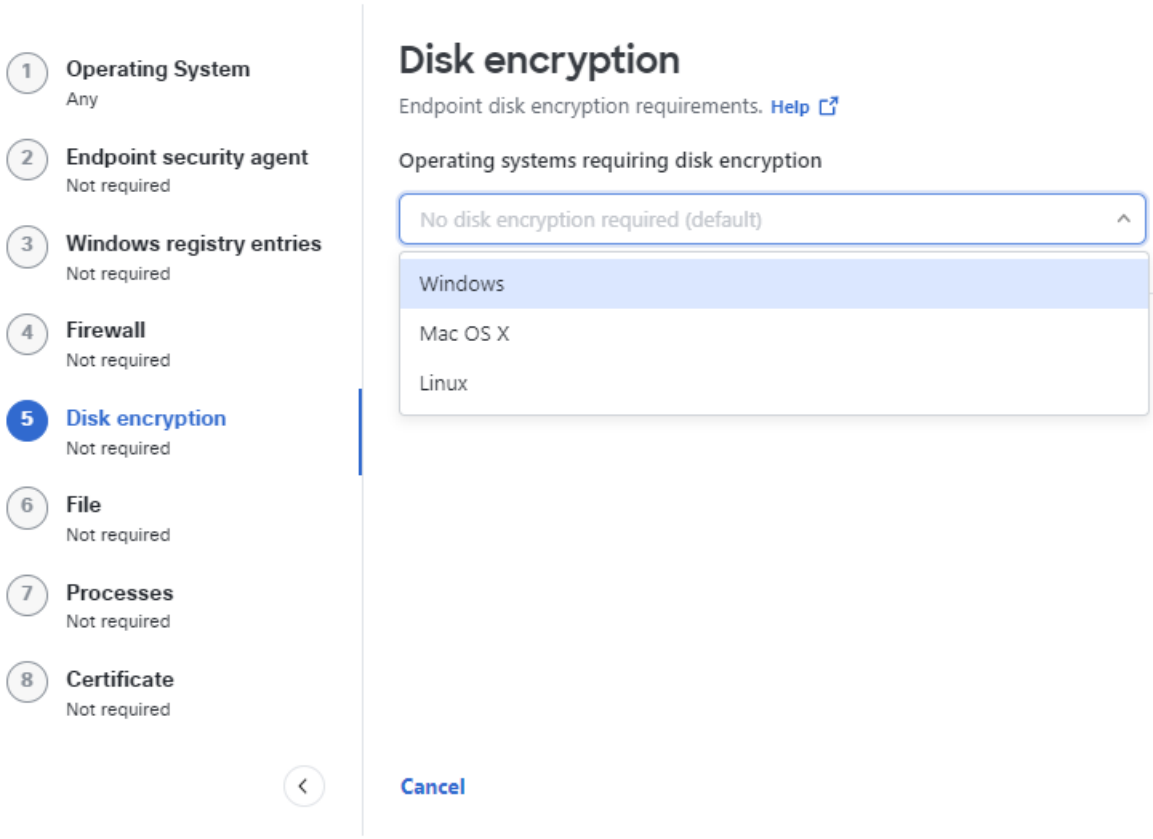
6. For the **Windows registry entries** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select endpoint firewalls. See Windows Registry Entries.



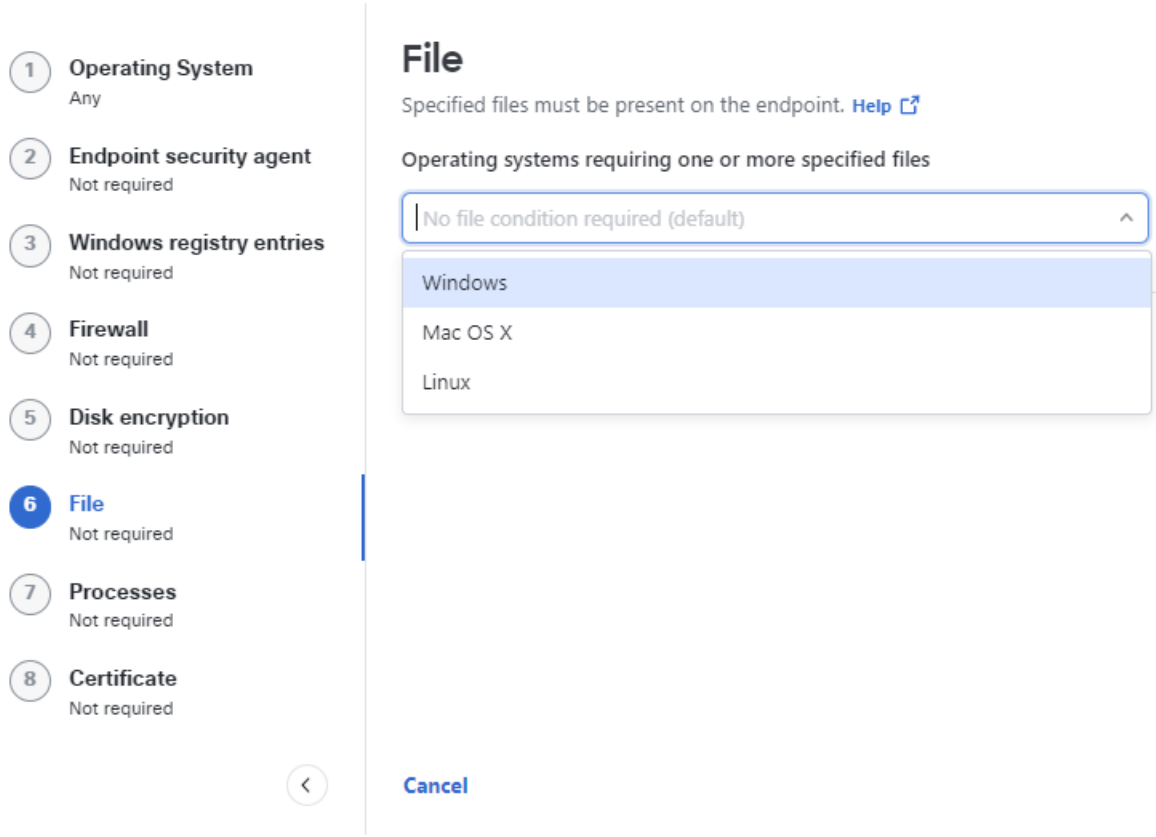
7. For the **Firewall** option, choose the firewall for your profile. Click **Save and Exit** or **Next** to select disk encryption. See Firewall Requirements.



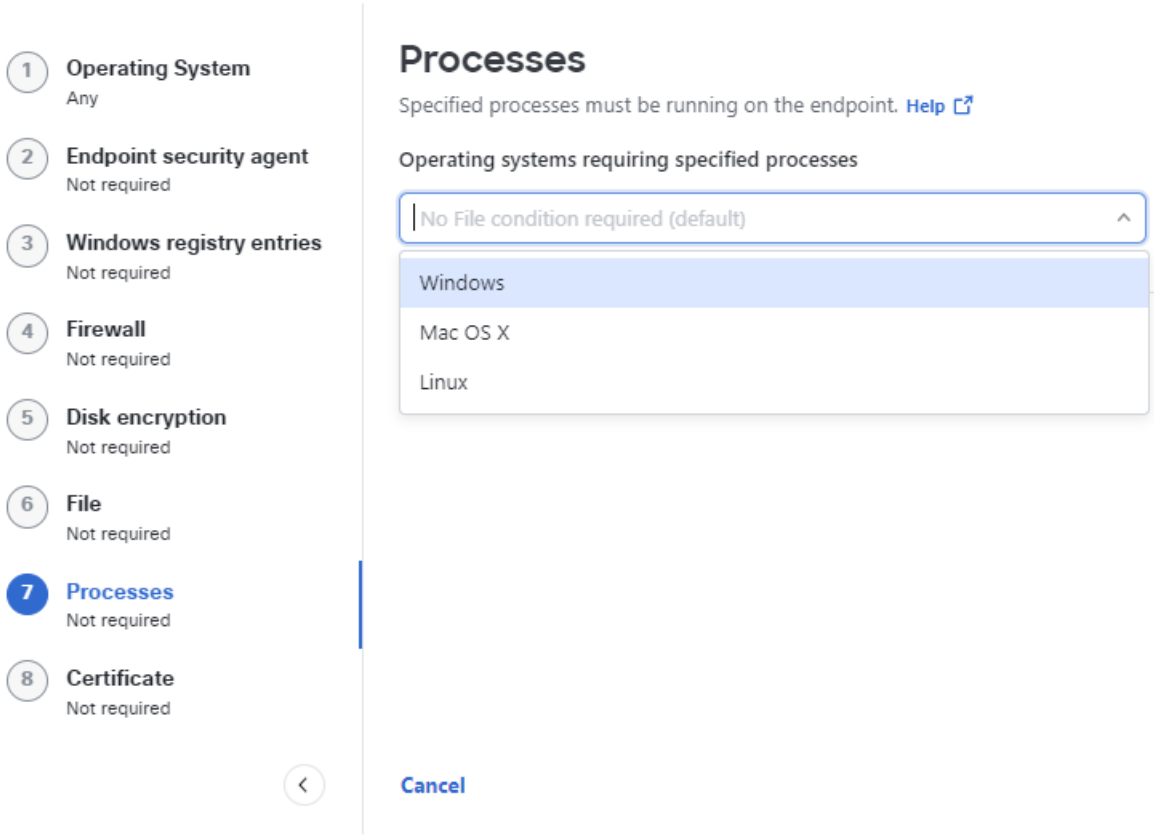
8. For the **Disk encryption** option, choose the disk encryption package(s) for your profile. Click **Save and Exit** or **Next** to configure any OS file requirements. See Disk Encryption.



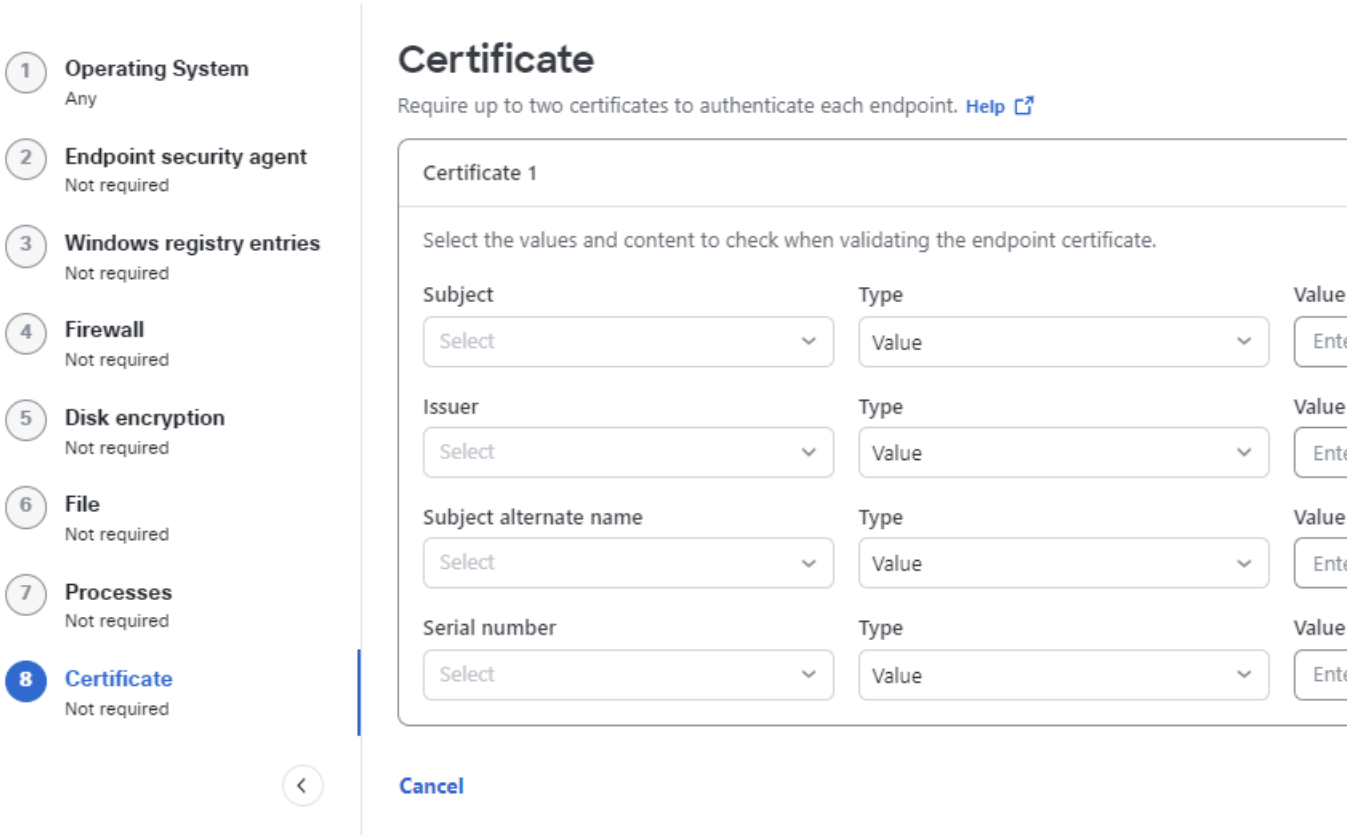
9. For the **File** option, specify any files that are required for the operating system. Click **Save and Exit** or **Next** to configure any OS process requirements. See File Requirements.



10. For the **Processes** option, specify any process that are required for the operating system. Click **Save and Exit** or **Next** to configure any endpoint certificates. See Process Requirements.



11. For the **Certificate** option, specify up to two certificates to authenticate each endpoint. Click **Save and Exit** or **Next** to return to the OS requirements. See Certificate Requirements.



12. Review and finalize the profile.

34 Manage IPS Profiles

Topics:

- Manage IPS Profiles

Describes the purpose and procedures for manage ips profiles and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage IPS Profiles

Describes managing ips profiles. Secure Access's Intrusion Prevention System (IPS) protects your network and assets from known threats. You define IPS profiles with signature lists that group these threats and allow you to specify how each threat should be handled.

Secure Access's Intrusion Prevention System (IPS) protects your network and assets from known threats. You define IPS profiles with signature lists that group these threats and allow you to specify how each threat should be handled. You then specify an IPS profile in each access rule.

How IPS Works

Describes how ips works. Secure Access IPS uses signature-based detection and provides an added layer of protection against threats such as malware, botnets, phishing, and command and control call backs. When IPS is enabled, it's enabled for your entire environment, including all of your network tunnels.

Secure Access IPS uses signature-based detection and provides an added layer of protection against threats such as malware, botnets, phishing, and command and control call backs. When IPS is enabled, it's enabled for your entire environment, including all of your network tunnels.

IPS Signature Lists contain signatures filtered by three actions:

- **Block**–Signatures are screened for threats on your network and recorded in Activity Search.
- **Log Only**–Signatures are recorded in Activity Search, but not screened for threats.
- **Ignore**–Signatures are completely ignored and not recorded in Activity Search.

Hit Counts

Hit counts represent the amount of times signatures were detected on your network for a certain period. By default, hit count durations for all lists are set to the last 24 hours. Each list's hit count duration can be changed to the last five minutes, last hour, yesterday, or the last 30 days. Hit counts may also be reset at any time.

Cisco-Provided IPS Signature Lists

The IPS signature lists provided by Cisco are constructed based on the balance between network connectivity and network security. The more a list is focused on security the more signatures are set to Blocked in that list rather than Log Only or Ignored.

- **Connectivity Over Security**–This signature list places an emphasis on network connectivity and throughput at the possible expense of security. Traffic is inspected less deeply, and fewer rules are evaluated.
- **Balanced Security and Connectivity**–This signature list attempts to balance network connectivity and security to keep users secure while being less obtrusive toward normal traffic. Less strict than Connectivity Over Security.
- **Security Over Connectivity**–This signature list emphasizes security over network connectivity. Traffic is inspected more deeply and more rules are evaluated. The result is an increase in false positives and network latency.
- **Maximum Detection**–This signature list places all emphasis on security, such that network connectivity and throughput are compromised. Only select this setting when total protection is required as alerts must be monitored and validated manually.

Decryption is Required for Effective Intrusion Prevention

Describes decryption is required for effective intrusion prevention. IPS requires decryption in order to effectively evaluate threats in traffic. Decrypting traffic requires certificates that you must provide and manage:

IPS requires decryption in order to effectively evaluate threats in traffic. Decrypting traffic requires certificates that you must provide and manage:

- Certificates required for decrypting traffic to internet destinations. For more information, see Certificates for Internet Decryption.
- Certificates required for decrypting traffic to private destinations. For more information, see Certificates for Private Resource Decryption.

Exceptions for Traffic That Should Not be Decrypted

Describes exceptions for traffic that should not be decrypted. If regulation or policy requires traffic to certain types of internet destinations to remain confidential, you can use the default Do Not Decrypt List for this purpose. Navigate to Secure Settings Do Not Decrypt Lists and configure the default list.

If regulation or policy requires traffic to certain types of internet destinations to remain confidential, you can use the default Do Not Decrypt List for this purpose. Navigate to **Secure** > **Settings** > **Do Not Decrypt Lists** and configure the default list. (Additional lists that you create on this page do not apply to IPS.) For more informatin, see Important Information About Do Not Decrypt Lists.

IPS is Used in Both Types of Access Rules

Describes ips is used in both types of access rules. IPS profiles are used in both internet access rules and private access rules.

IPS profiles are used in both internet access rules and private access rules.

Settings such as the default IPS profile and the decryption setting global settings apply to both types of access rules.

Add a Custom IPS Signature List

Describes adding a custom ips signature list. You can use the system-provided signature lists in custom IPS profiles to build your own custom IPS signature lists that fit your organization's specific needs.

You can use the system-provided signature lists in custom IPS profiles to build your own custom IPS signature lists that fit your organization's specific needs.

Prerequisites

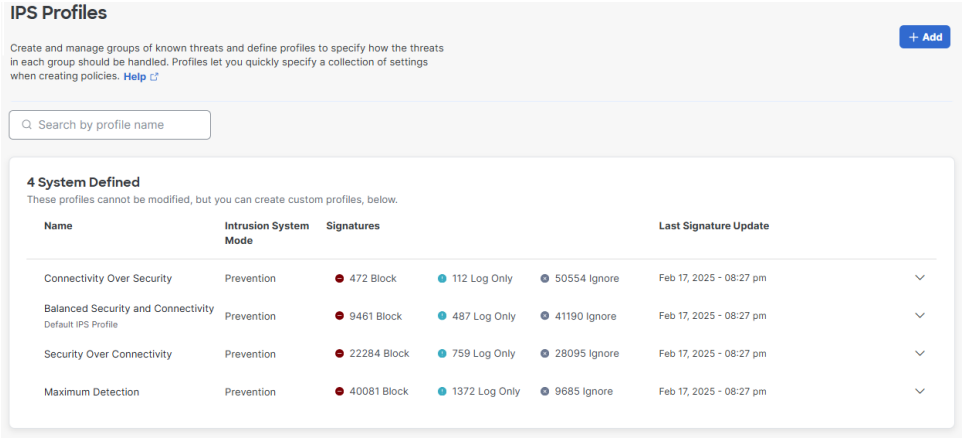
- Full admin access to the Secure Access dashboard. For more information, see Manage Accounts.

Procedure

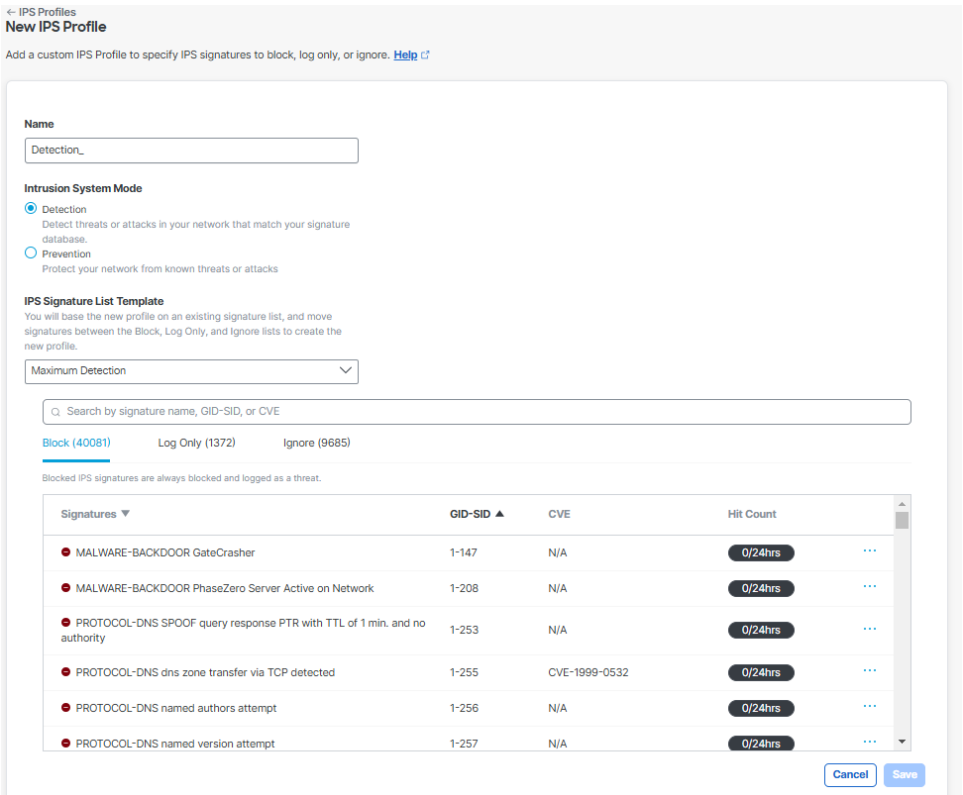
Provides instructions for procedure. Navigate to Secure Profiles IPS Profiles . Click Add and enter a name for your custom signature list and choose either Detection or Prevention for Intrusion System Mode.

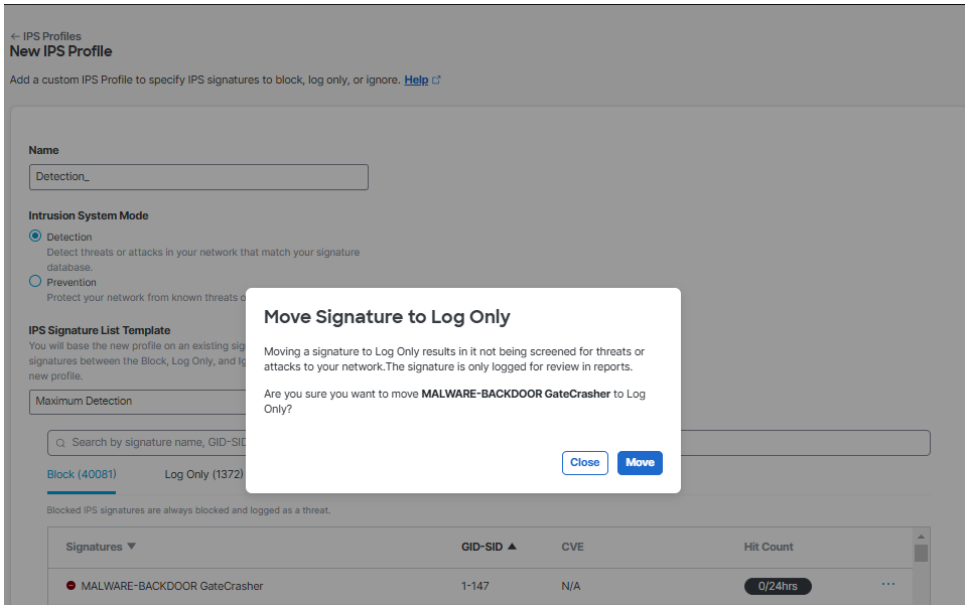
Procedure

1. Navigate to **Secure** > **Profiles** > **IPS Profiles**.

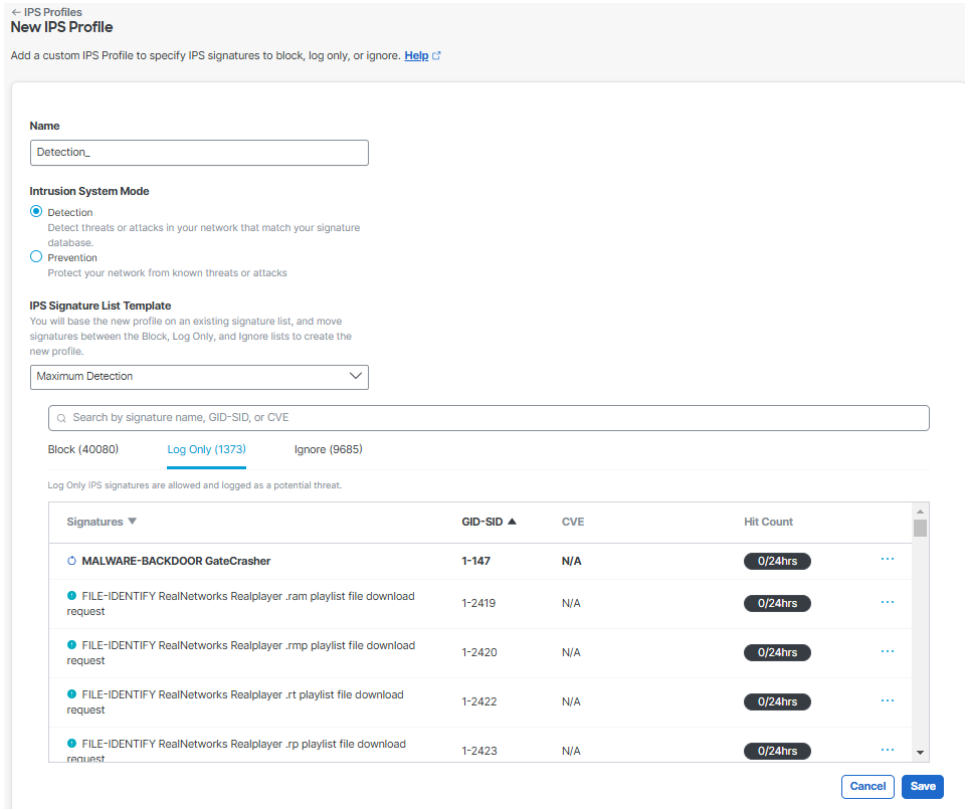


2. Click **Add** and enter a name for your custom signature list and choose either **Detection** or **Prevention** for **Intrusion System Mode**.
   - **Detection**–Detect threats or attacks in your network that match your signature database. When Detection Only mode is used, your IPS settings can be tested on your network without affecting traffic. Signatures that would be blocked in Protection mode will be logged in Activity Search as "Allowed (Would Block)" under IPS Signatures.
   - **Prevention**–Protect your network from known threats or attacks.
3. Under **IPS Signature List Template**, choose the signature list to apply these settings to.
4. Change which signatures are blocked, logged only, or ignored. Click the menu next to the signature you want to move and click **Move to Block**, **Move to Log Only**, or **Move to Ignore**. A prompt appears asking you to confirm your choice.





5. Click **Move**. The signature you moved is now within the section you chose.



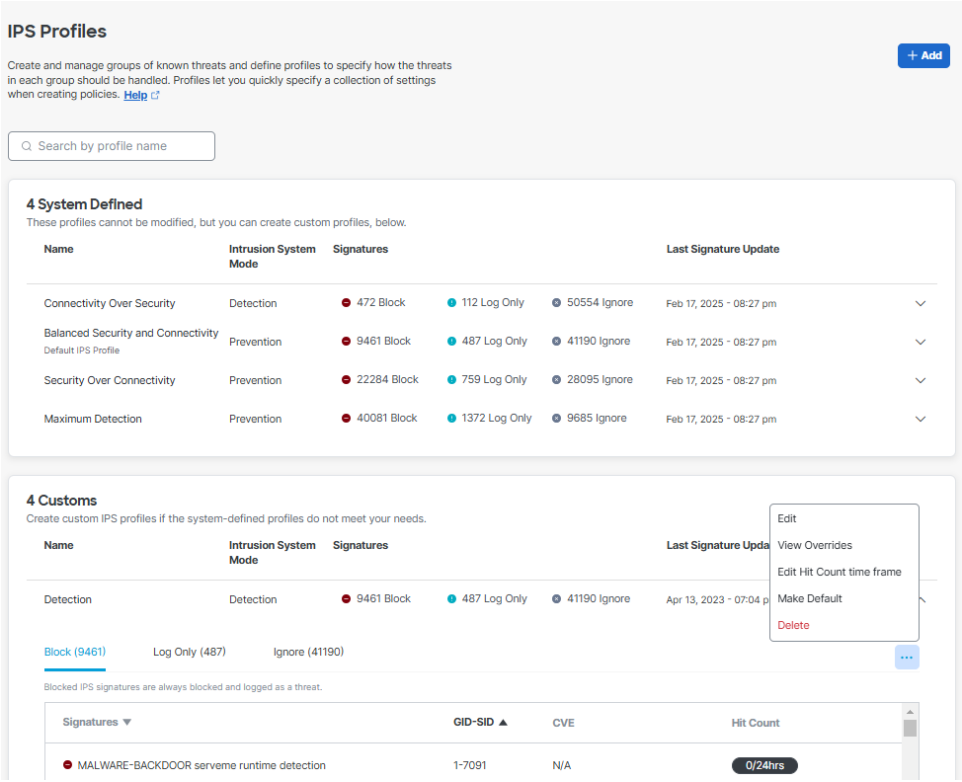
6. Click **Save** to finish creating your custom signature list.

Reset a Signature's Action

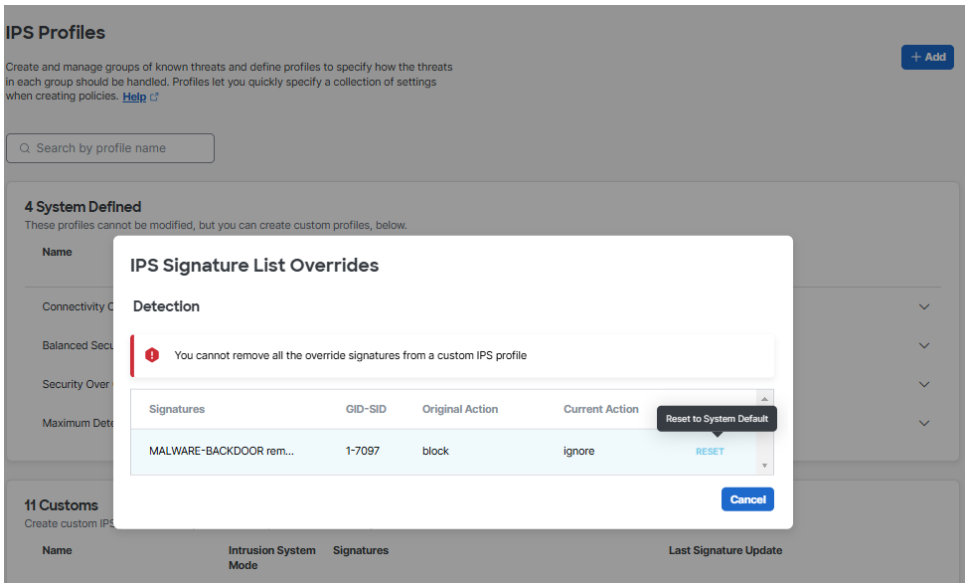
Provides instructions for resetting a signature's action. Navigate to Secure Profiles IPS Profiles . Under Custom IPS Signature Lists, click the list you want to edit. The list expands.

Procedure

1. Navigate to **Secure** > **Profiles** > **IPS Profiles**.
2. Under Custom IPS Signature Lists, click the list you want to edit. The list expands.
3. Click the More Actions menu and click **View Overrides** to view the list of signatures that have been moved.



4. Locate the signature you want to reset and click **Reset to System Default** for that signature. A prompt appears asking you to confirm your choice.



5. The signature you reset is now set back to its original action from the default list your custom list is based on.
6. Click **Save** to finish editing your custom signature list.

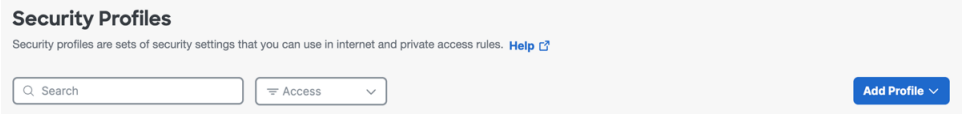
35 Manage Security Profiles

Topics:

- Security Profiles for Internet Access
- Add a Security Profile for Internet Access
- Enable SafeSearch
- Security Profiles for Private Access
- Add a Security Profile for Private Access

Introduces managing security profiles. A Cisco Secure Access Security profile is a reusable component that you can use in the rules on the Access policy.

A Cisco Secure Access Security profile is a reusable component that you can use in the rules on the Access policy.



There are two types of Security profiles:

- **Security Profiles for internet access rules**–For more information, see Security Profiles for Internet Access.
- **Security Profiles for private access rules**–For more information, see Security Profiles for Private Access.

Note

You can configure up to 100 Security profiles in Secure Access, which includes security profiles for both internet and private access rules.

Security Profiles for Internet Access

Describes security profiles for internet access. A Security profile for internet access includes security controls and other settings such as acceptable use controls that you configure as a set.

A Security profile for internet access includes security controls and other settings such as acceptable use controls that you configure as a set. Once you add the security profile in Secure Access, you can use this profile on one or more internet access rules in the Access policy. For example, you can use different security profiles for different sets of users, or for different types of destinations.

Note

Secure Access comes with a partially configured security profile for internet access; you must either configure that profile to suit your needs or create a different security profile and designate that profile as the default security profile for internet access rules.

To configure security profiles for internet access, see detailed information in Add a Security Profile for Internet Access.

Functionality Included in a Security Profile for Internet Access

Describes functionality included in a security profile for internet access. You can configure various settings and security controls on a security profile for internet access.

You can configure various settings and security controls on a security profile for internet access.

- Decryption
- SSO Authentication
- Security and Acceptable Use Controls
- End-User Notifications

Decryption

Describes decryption. Decryption is necessary for proper functioning of all features enabled in the security profile, and for processing traffic to most internet destinations in general. When enabled, all internet traffic will be decrypted except as specified in the selected Do Not Decrypt list.

Decryption is necessary for proper functioning of all features enabled in the security profile, and for processing traffic to most internet destinations in general. When enabled, all internet traffic will be decrypted except as specified in the selected Do Not Decrypt list. For more information about decryption, see Manage Traffic Decryption.

Generally, you should disable decryption only if the security profile will be used in rules that:

- Have only destinations to which traffic should never be decrypted, for example for privacy or confidentiality reasons, such as medical or financial sites, for locations that regulate this traffic.
- Have sources that only include devices on which you cannot install certificates required to decrypt and inspect traffic, such as devices that are not managed by your organization, for example vendors' or contractors' devices.
- Have only sources that cannot respond to certificates required for decryption, such as IoT devices, printers, or kiosks
- Allow access to applications that will not work properly if decryption is enabled, including Microsoft 365 and applications that use certificate pinning.

- Include only known safe destinations.

  For example, use this profile for rules that control access to the sites that IoT devices access in order to update their software.

If you enable decryption, you can opt not to decrypt traffic to specific destinations. For more information, see Important Information About Do Not Decrypt Lists.

SSO Authentication

Describes sso authentication. If your organization uses SSO authentication, you should generally enable this option on the networks and tunnels configured for the rules that use this profile.

If your organization uses SSO authentication, you should generally enable this option on the networks and tunnels configured for the rules that use this profile.

Requirements for Enabling OIDC Authentication

- Configure Open ID Connect (OIDC) authentication to authorize connections to the Secure Web Gateway (SWG) from user devices on networks and network tunnels, and connections using Zero Trust Access (ZTA).

Requirements for Enabling SAML Authentication

- Configure SAML authentication to authorize connections to the SWG from user devices on networks and network tunnels, and connections using Zero Trust Access (ZTA). For more information, see Configure Integrations with SAML Identity Providers.
- Decryption must also be enabled for network SAML enforcement.

Requirements for Disabling SAML Authentication

- Decryption is disabled in the security profile, or is enabled only for notifications.
- The security profile will be used in rules that include sources that:
  - Are not configured for SAML authentication.
  - Cannot be authenticated using SAML.

    For example, if the rule source includes:

    - Devices that are not managed by your organization, when certificates are required for authentication but cannot be installed on the device. Such devices might be used by contractors or vendors on your guest network.
    - Devices such as IoT devices, printers, or kiosks that cannot respond to authentication requests or present certificates required for authentication.

  - Should not be authenticated using SAML.

    For example, if users should not be identified for privacy or confidentiality reasons, such as by regulation or policy.

Security and Acceptable Use Controls

Describes security and acceptable use controls. Configure security and control the use of the threat categories, file inspection, file type blocking, and SafeSearch settings.

Configure security and control the use of the threat categories, file inspection, file type blocking, and SafeSearch settings.

Option	Description	More Information
Threat Categories	Block traffic to sites that have been categorized as risky or threatening.	Manage Threat Categories
File inspection	Block download of files known to carry threats, and analyze files for suspicious behaviors.	Manage File Inspection
File type blocking	Block files based on filename extension, such as executable files.	Manage File Type Controls
SafeSearch	Return only family-friendly search results in popular search engines.	Enable SafeSearch

Note

For acceptable use controls on access to web sites based on categories that are not known security threats, see Manage Content Category Lists. You will specify these categories or lists in access rules.

End-User Notifications

Describes end-user notifications. You configure two types of end-user notifications in security profiles for internet access: Block notifications that end users see instead of a browser error when they attempt to access a destination that is blocked by an access rule.

You configure two types of end-user notifications in security profiles for internet access:

- Block notifications that end users see instead of a browser error when they attempt to access a destination that is blocked by an access rule.
- Warning notifications that end users must click through in order to access destinations in rules configured with the Warn action.

For information about configuring Block and Warn pages, see Manage Notification Pages.

Get Started: Security Profiles for Internet Access

Describes get started: security profiles for internet access. Add a Security Profile. For more information, see Add a Security Profile for Internet Access.

- Add a Security Profile. For more information, see Add a Security Profile for Internet Access.
- Modify or delete a Security Profile. For more information, see Edit a Security Profile and Delete a Security Profile.
- Enable SafeSearch for the organization. For more information, see Enable SafeSearch.

Add a Security Profile for Internet Access

Describes adding a security profile for internet access. A Cisco Secure Access Security profile is a set of security controls and other settings that you can use in access rules.

A Cisco Secure Access Security profile is a set of security controls and other settings that you can use in access rules.

For information about each of the components or controls that you can configure in a Security profile for internet access, see Security Profiles for Internet Access.

Prerequisites

- Full Admin user role is required. For more information, see Manage Accounts.
- In Secure Access, configure the components that you will select in a security profile for internet access.
  - Add a **Do Not Decrypt** list. For more information, see Add a Do Not Decrypt List for Security Profiles.
  - Create the list of threat categories. For more information, see Manage Threat Categories.
  - Carefully review the information about enabling file analysis with Cisco Secure Malware Analytics. For more information, see Enable File Analysis by Cisco Secure Malware Analytics.
  - (Optional) Create custom notification pages that Secure Access will display when rules that use this security profile match traffic that blocks access or displays a warning. Customizations can include the logo, message, and contact information of your choice. For more information, see Notification Pages.

Procedure

Note

You can add up to 100 security profiles in Secure Access for the organization.

Configure the settings on a Security profile and add the profile to the organization. After you add the Security profile, configure any related security settings and use the Security profile in an access rule. For more information, see Configure Additional Security Options.

The following steps outline how to configure and apply security settings to your organization:

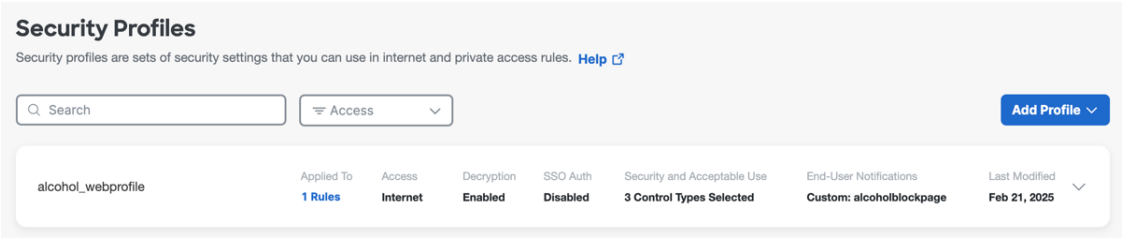
- Add a Security Profile
- Enable or Disable Decryption
- SSO Authentication
- Security and Acceptable Use Controls
- Configure End-User Notifications

Add a Security Profile

Provides instructions for adding a security profile. Navigate to Secure Security Profiles . Click Add Profile, and then select Internet Access.

Procedure

1. Navigate to **Secure** > **Security Profiles**.



2. Click **Add Profile**, and then select **Internet Access**.

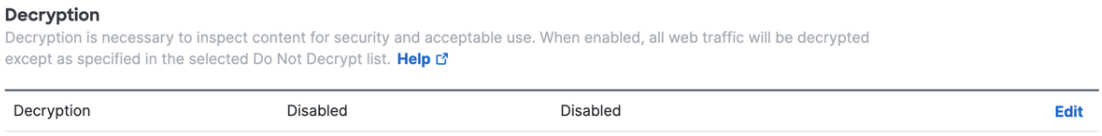
3. Follow the below procedures to configure the settings on the security profile.
   - Enable or Disable Decryption
   - SSO Authentication
   - Security and Acceptable Use Controls
   - Configure End-User Notifications

Enable or Disable Decryption

Provides instructions for enabling or disable decryption. Navigate to Decryption, and then click Edit. Choose a decryption option. Decryption is required for most security features to work properly. For more information about decryption, see Manage Traffic Decryption.

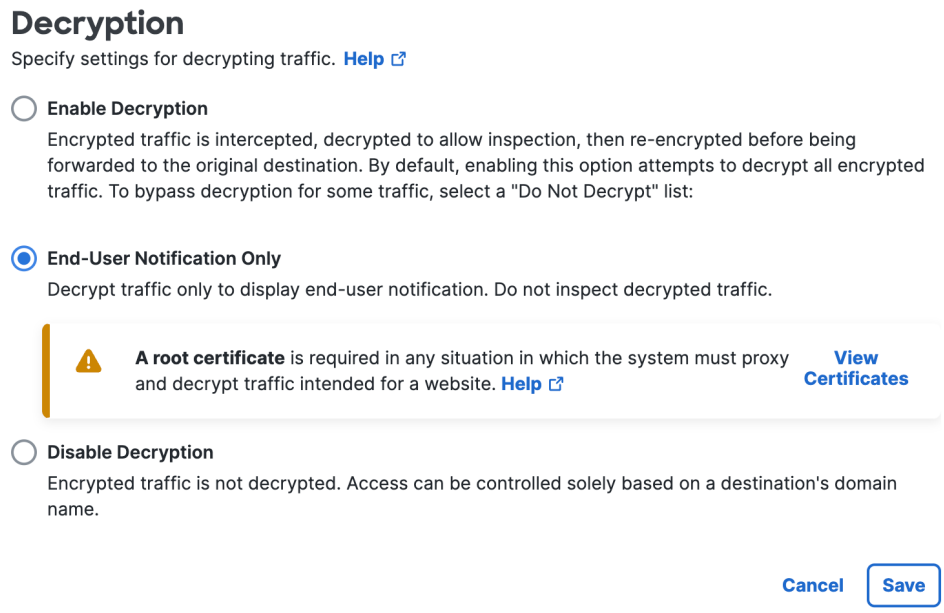
Procedure

1. Navigate to **Decryption**, and then click **Edit**.



2. Choose a decryption option.

> **Note**
>
> Decryption is required for most security features to work properly. For more information about decryption, see Manage Traffic Decryption.



a. Click **Enable Decryption**.

Encrypted traffic is intercepted, decrypted to allow inspection, then re-encrypted before being forwarded to the original destination. By default, enabling this option attempts to decrypt all encrypted traffic. To bypass decryption for some traffic, select a **Do Not Decrypt** list.

b. Click **End-User Notification Only**.

Decrypt traffic only to display end-user notification. Do not decrypt traffic for inspection.

> **Note**
>
> A root certificate is required in any situation in which the system must proxy and decrypt traffic intended for a website.

c. Click **Disable Decryption**.

Encrypted traffic is not decrypted. Access can be controlled solely based on a destination's domain name.

3. Click **Save**.

> **Note**
>
> If you enabled decryption, choose a **Do Not Decrypt** list. For more information, see Add a Do Not Decrypt List for Security Profiles.

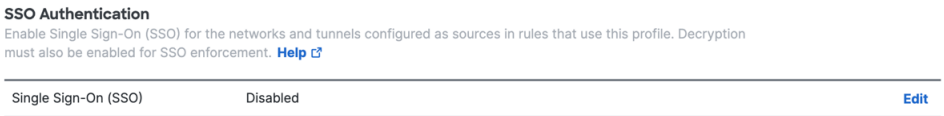
SSO Authentication

Provides instructions for enabling or disabling SSO Authentication.

Enable or disable SSO Authentication. For information about the SSO authentication setting on the profile, see Security Profiles for Internet Access.

Procedure

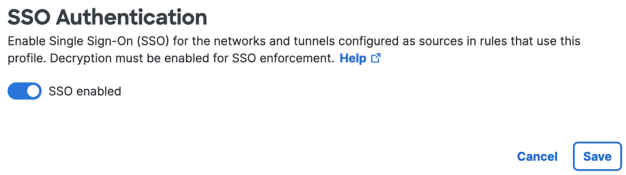
1. Navigate to **SSO Authentication**, navigate to Single Sign-On (SSO), and then click **Edit**.



2. Click **SSO enabled** to toggle the setting on.

Note

If you enable this option, ensure that decryption is enabled in the same security profile and in any rule in the Access policy that uses this profile.



3. Click **Save**.

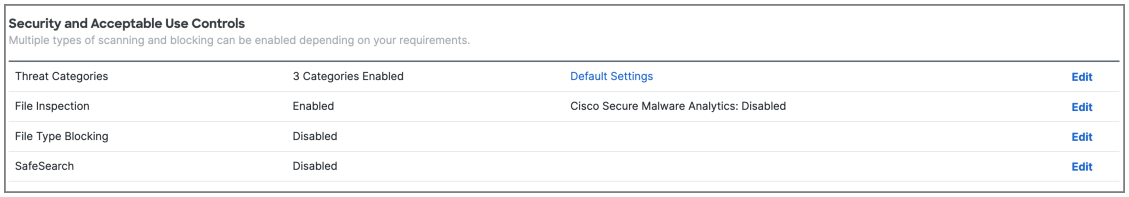
Note

(Optional) Click **SSO disabled** to toggle the setting off.

Security and Acceptable Use Controls

Describes security and acceptable use controls. Configure security and acceptable use controls in the Security Profile. Depending on your requirements, you can enable multiple kinds of scanning and blocking. For information about these settings, see Security Profiles for Internet Access.

Configure security and acceptable use controls in the Security Profile. Depending on your requirements, you can enable multiple kinds of scanning and blocking. For information about these settings, see Security Profiles for Internet Access.

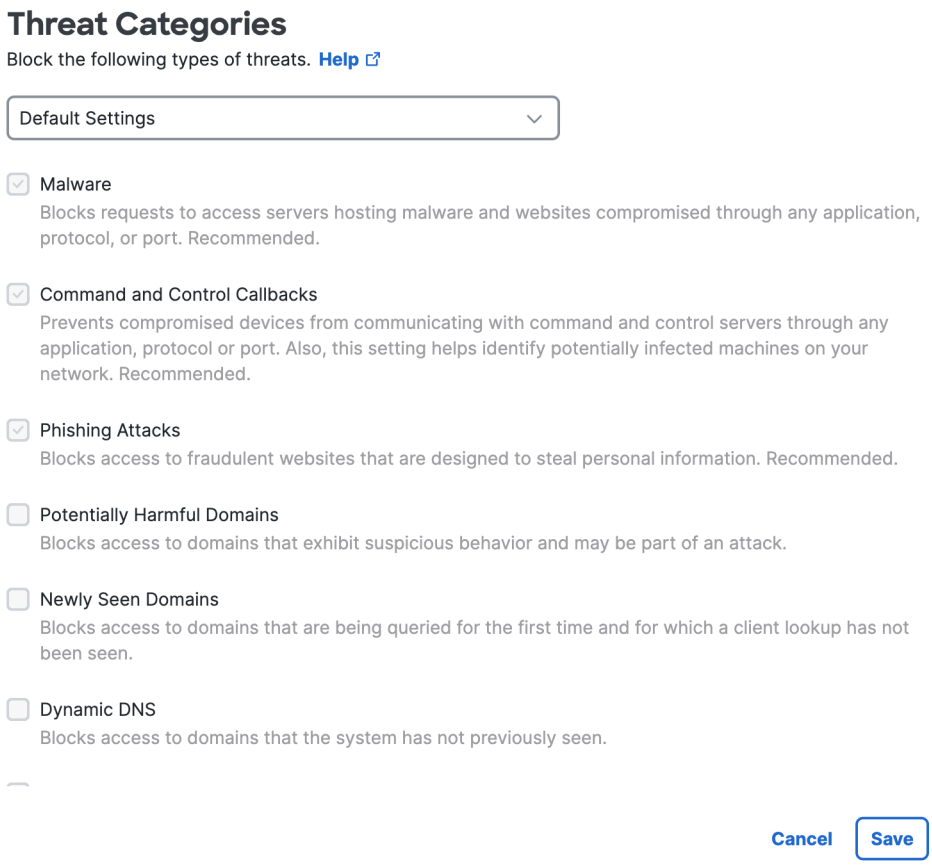


Threat Categories

Provides instructions for threat categories. For Threat Categories, click Edit. To block access to known malicious sites and potentially risky sites based on threat category, choose from the existing lists of threat categories.

Procedure

1. For **Threat Categories**, click **Edit**.



2. To block access to known malicious sites and potentially risky sites based on threat category, choose from the existing lists of threat categories.
3. Click **Save**.

File Inspection

Provides instructions for file inspection. For File inspection, click Edit. Choose the file inspection and analysis tools to use to protect traffic that matches rules that use this security profile.

Procedure

---

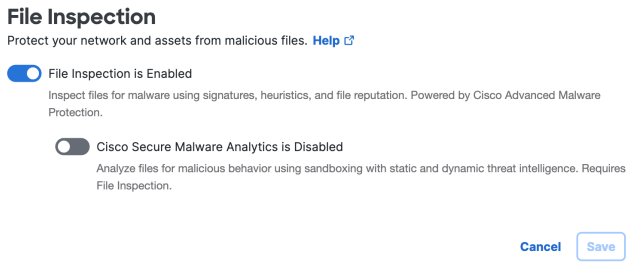
1. For **File inspection**, click **Edit**.
2. Choose the file inspection and analysis tools to use to protect traffic that matches rules that use this security profile.

   Important

   If this is the first time you enable Cisco Secure Malware Analytics, Secure Access displays the option to select a sandbox region. Before you enable Cisco Secure Malware Analytics, we recommend that you review the instructions about this option. For more information, see Enable File Analysis by Cisco Secure Malware Analytics.

   a. Click **File Inspection is Enabled**.

   b. (Optional) Click **Cisco Secure Malware Analytics is Enabled**.



3. Click **Save**.

File Type Blocking

Describes file type blocking. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

For more information, see Enable File Type Controls.

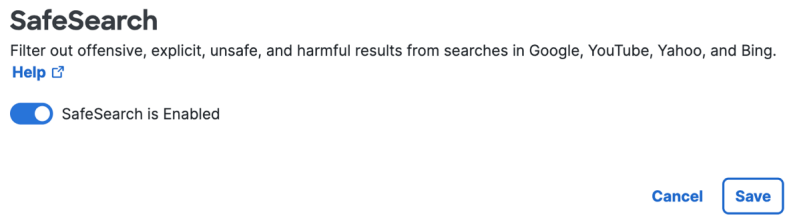
SafeSearch

Provides instructions for safesearch. For SafeSearch, click Edit. Enable this option to filter out offensive, explicit, unsafe, and harmful search results in Google, YouTube, Yahoo, and Bing.

Procedure

---

1. For **SafeSearch**, click **Edit**.



2. Enable this option to filter out offensive, explicit, unsafe, and harmful search results in Google, YouTube, Yahoo, and Bing.
3. Click **Save**.

Configure End-User Notifications

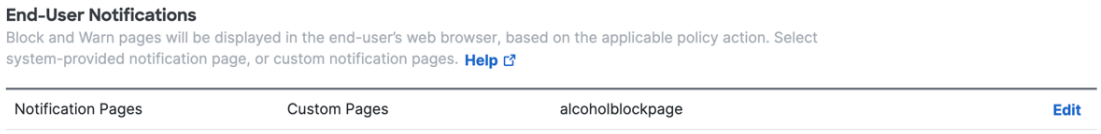
Provides instructions for configuring end-user notifications. Configure end-user notifications for the organization. Secure Access displays Block and Warn pages in the end-user's web browser. The display of the Block or Warn page is based on the action that you configure in each rule where the security profile is used.

Configure end-user notifications for the organization. Secure Access displays Block and Warn pages in the end-user's web browser. The display of the Block or Warn page is based on the action that you configure in each rule where the security profile is used. For more information, see Manage Notification Pages.

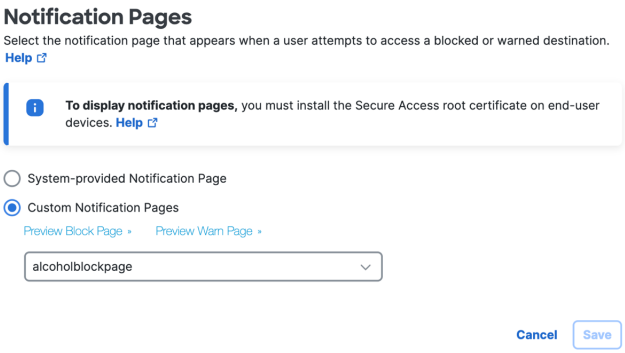
Procedure

---

1. In the **Security Profile for Internet Access** page, navigate to **End-User Notifications**.



2. Navigate to **Notification Pages**, and then click **Edit**.



3. Choose one of the options.

   Each option includes a Block notification and a Warn notification.

   a. Click **System-provided Notification Pages**.

   b. Click **Custom Notification Pages**.

> **Note**
>
> For custom pages, choose the pages that you want to display.

4. (Optional) To preview the pages that you have selected, click the **Preview** links.
5. Click **Save**.

View Security Profiles

Provides instructions for viewing security profiles. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

View the configured security profiles in Secure Access.

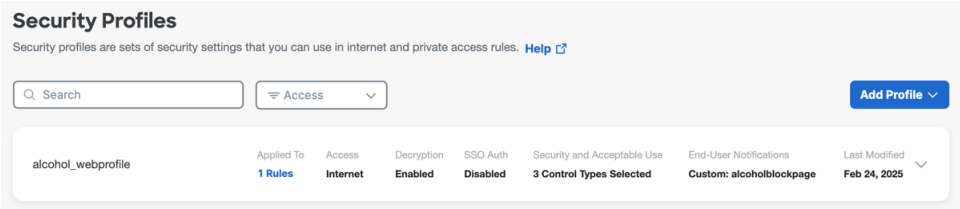
Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Navigate to a security profile and expand the profile.

   A configured security profile includes these details:

   - Name of the security profile.
   - **Applied To**–The number access rules where the security profile is included.
   - **Access**–The type of the security profile.

- **Decryption**–Specifies whether decryption is enabled on the profile.
- **SSO Auth**–Specifies whether SSO authentication has been enabled on the profile.
- **Security and Acceptable Use**–Lists the number of security controls that are enabled on the profile.
- **End-User Notifications**–Lists the type of notifications that are configured on the profile.
- **Last Modified**–The date when the security profile was last updated.



Configure Additional Security Options

Describes configuring additional security options. Configure additional functionality that is required for your selected features. For example, configure: Traffic decryption Decryption requires certificates. For more information, see Certificates for Internet Decryption.

Configure additional functionality that is required for your selected features. For example, configure:

- **Traffic decryption**

  Decryption requires certificates. For more information, see Certificates for Internet Decryption.

- **SSO authentication**:

  If you enable this option in a security profile, ensure that you configure SSO authentication.

  - For **SAML**, enable SAML for the Cisco Secure Client roaming security module.

    For more information, see Configure Integrations with SAML Identity Providers.

  - **Open ID Connect (OIDC)**

- **Notification pages**

  To display notification pages, you must install a Secure Access root CA certificate on all end-user devices. This may not be the same certificate you use for decrypting internet traffic. For more information, see Certificates for Internet Decryption.

Add a Security Profile on Internet Access Rules

Describes adding a security profile on internet access rules. Add the security profile to one or more internet access rules. For more information, see Add an Internet Access Rule and Default Settings for Internet Access Rules.

Add the security profile to one or more internet access rules. For more information, see Add an Internet Access Rule and Default Settings for Internet Access Rules.

Edit a Security Profile

Provides instructions for editing a security profile. After you add a security profile in Secure Access, you can modify it.

After you add a security profile in Secure Access, you can modify it.

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Expand a security profile, and then click **Edit**.
3. Choose any of the security controls and settings to modify.

   For more information, see:

   - Enable or Disable Decryption
   - SSO Authentication
   - Security and Acceptable Use Controls
   - Configure End-User Notifications

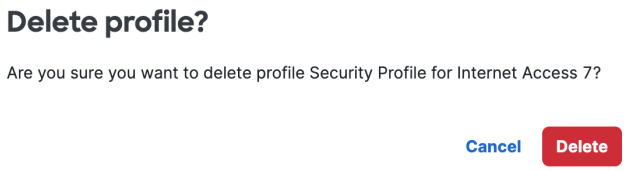
Delete a Security Profile

Provides instructions for deleting a security profile. After you add a security profile in Secure Access, you can remove it.

After you add a security profile in Secure Access, you can remove it.

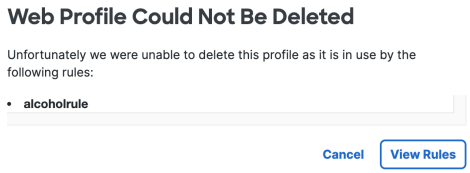
Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Expand a security profile, and then click **Delete**.
3. Confirm the removal of the security profile.
   a. Click **Delete** to confirm the removal of the security profile.



   b. If the security profile is in use on an access rule, you can not remove the profile.

   First remove the security profile from the access rules where it is included, and the try to remove the security profile again.



Enable SafeSearch

Describes enabling safesearch. SafeSearch is a search engine filter for internet-bound traffic that blocks search results for explicit content such as pornography, violence, gore, and other offensive adult content.

SafeSearch is a search engine filter for internet-bound traffic that blocks search results for explicit content such as pornography, violence, gore, and other offensive adult content. When enabled, if an end user enters a potentially inappropriate or suggestive phrase into a search engine, the search engine only returns safe "family-friendly" results.

SafeSearch applies to Google, YouTube, Yahoo, and Bing. SafeSearch can not be disabled on an end-user device for any applicable search engine or site.

When you enable SafeSearch in a security profile, you must also enable decryption in the same security profile. For more information, see Manage Traffic Decryption.

To enable SafeSearch and decryption, see Add a Security Profile for Internet Access.

Confirm That SafeSearch is Working

Describes confirm that safesearch is working. The most reliable way to confirm that SafeSearch is enabled is to visit a search engine or site where SafeSearch settings are enforced. You can also perform a search using a term that might be deemed inappropriate and review search results.

The most reliable way to confirm that SafeSearch is enabled is to visit a search engine or site where SafeSearch settings are enforced. You can also perform a search using a term that might be deemed inappropriate and review search results. Only "family friendly" results should be returned.

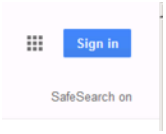
Tests must be done through a source that is included in an access rule that is configured to use a security profile in which SafeSearch is enabled.

The following topics provide guidance on how to verify SafeSearch enforcement for popular search engines such as Google, YouTube, Yahoo, and Bing.

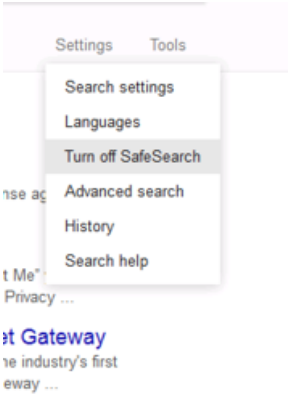
Google

Describes google. After attempting a search in Google, a SafeSearch on indicator should be displayed. In the browser, under Settings, if you select Turn off SafeSearch, it has no effect and explicit sites are not listed in searches.

After attempting a search in Google, a **SafeSearch on** indicator should be displayed.



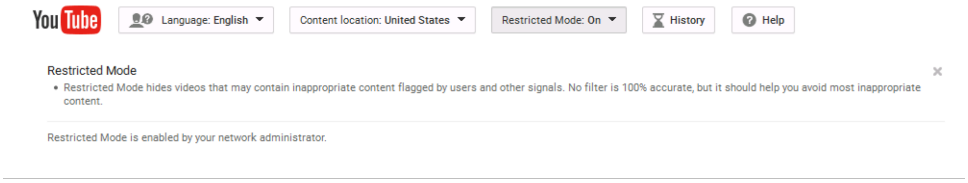
In the browser, under **Settings**, if you select **Turn off SafeSearch**, it has no effect and explicit sites are not listed in searches.



YouTube

Describes youtube. Results when searching YouTube displays that “Restricted Mode” is "On". Expanding this result indicates that "Restricted Mode is enabled by your network administrator".

Results when searching YouTube displays that “Restricted Mode” is "On". Expanding this result indicates that "Restricted Mode is enabled by your network administrator".

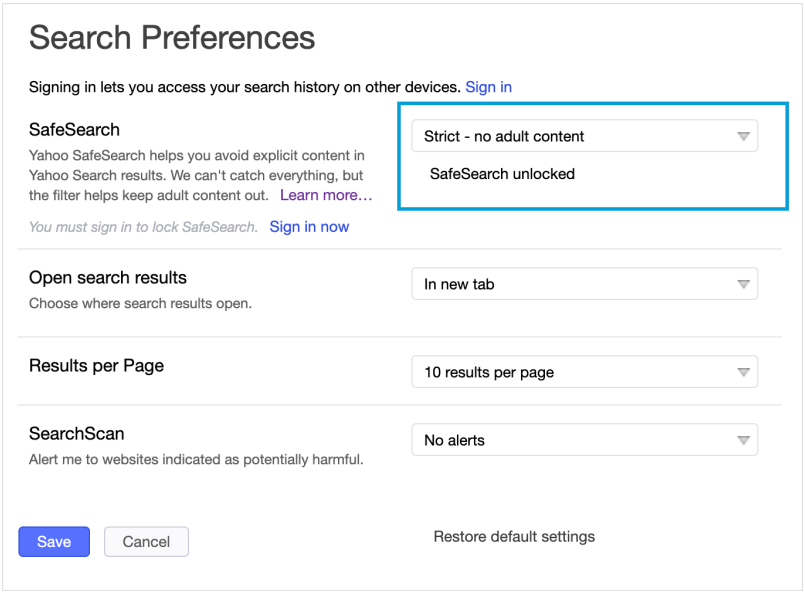


Yahoo

Describes yahoo. From the Yahoo search page, click Settings and then Preferences. SafeSearch should be set to Strict - no adult content. You cannot change the setting.

From the Yahoo search page, click **Settings** and then **Preferences**.

SafeSearch should be set to **Strict - no adult content**. You cannot change the setting.

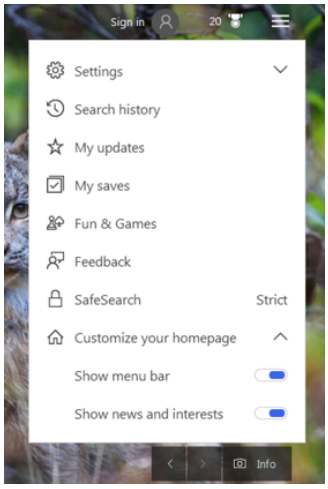


Bing

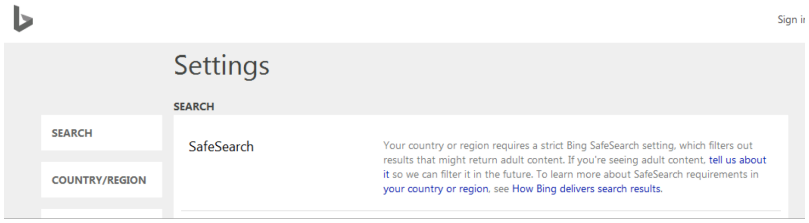
Describes bing. From the menu icon, Bing displays that SafeSearch is set to “Strict”. Clicking SafeSearch takes you to a page describing SafeSearch, but there is no disable option.

From the menu icon, Bing displays that SafeSearch is set to “Strict”.

Figure 1: safesearch_bing.png



Clicking **SafeSearch** takes you to a page describing SafeSearch, but there is no disable option.



Security Profiles for Private Access

Describes security profiles for private access. A security profile for private access rules lets you configure the following options to protect resources on your network from malicious files:

A security profile for private access rules lets you configure the following options to protect resources on your network from malicious files:

- File Inspection and File Type Blocking
- File Type Controls

To configure security profiles for private access, see Add a Security Profile for Private Access.

Security profile for private access blocks both downloading and uploading of file types selected in file type controls.

Add a Security Profile for Private Access

Provides instructions for adding a security profile for private access. A security profile for private access rules lets you configure options to protect resources on your network from malicious files.

A security profile for private access rules lets you configure options to protect resources on your network from malicious files.

A security profile is a set of security controls and other settings that you can use in access rules. To add a security profile, navigate to **Secure** > **Security Profiles**.

Before you begin

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

- **Caution:** Certain initial settings affect all file analysis operations in your organization, for both private and internet traffic, and cannot be changed once configured. Be sure you understand these settings before you proceed. See Manage File Inspection and File Analysis.
- Understand the file-related options in the profile:
  - File Inspection and File Type Blocking
  - File Type Controls

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Click **Add Profile** > **Private Access**.
3. Configure file-related options.

What to do next

- Add the security profile to one or more private access rules.

36 Threat Categories

Topics:

- Manage Threat Categories

Introduces threat categories. Secure Access groups harmful destinations into categories based on the type of threat they present, and allows you to control access to those destinations.

Manage Threat Categories

Introduces managing threat categories. Secure Access groups harmful destinations into categories based on the type of threat they present, and allows you to control access to those destinations.

Secure Access groups harmful destinations into categories based on the type of threat they present, and allows you to control access to those destinations. You create lists of threat categories to block access to, then specify a threat category list in each security profile, then specify a security profile in each internet access rule.

For a list of all threat categories and a description of each, see Threat Categories.

Default Threat Category List

A default threat category list ships with Secure Access. This default list is included in the default security profile and by default in all security profiles that you create.

You can change the enabled threat categories in the default list, and you can create different threat category lists to use in different security profiles.

The following threat categories are enabled in the threat categories list that is included by default in security profiles: Malware, Command Control Callbacks, and Phishing.

Reporting on Threat Category Access Attempts

When traffic is blocked based on one of these categories, Secure Access generates a reporting event.

If a domain matches a threat category but is not set to be blocked by a web security setting in the security profile selected for your rule, it is still reported as an allowed visit to a destination that matches one of the threat categories.

Threat Category Descriptions

Describes threat category descriptions. Malware—Blocks requests to access servers hosting malware and websites compromised through any application, protocol, or port. Recommended.

- **Malware**—Blocks requests to access servers hosting malware and websites compromised through any application, protocol, or port. Recommended.
- **Command Control Callbacks**—Prevents compromised devices from communicating with command and control servers through any application, protocol or port. Also, this setting helps identify potentially infected machines on your network. Recommended.
- **Phishing Attacks**—Blocks access to fraudulent websites that are designed to steal personal information. Recommended.
- **Potentially Harmful Domains**—Blocks access to domains that exhibit suspicious behavior and may be part of an attack.
- **Newly Seen Domains**—Blocks access to domains that are being queried through Secure Access for the first time and for which Secure Access has not yet seen a client lookup. Not all new domains are necessarily harmful; blocking access to this category may block access to legitimate sites.
- **Dynamic DNS**—Blocks access to sites that host dynamic DNS content. Not all sites in this category are necessarily harmful; blocking access to this category may block access to legitimate sites.
- **DNS Tunneling VPN**—Blocks VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These services can be used to bypass corporate policies regarding access and data transfers.
- **Cryptomining**—Blocks access to crypto mining pools where "miners" group together and share resources—processing power—to better gather and share cryptocurrencies. Also blocks known web crypto mining source code repositories.

Add a Threat Category List

Provides instructions for adding a threat category list. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

You can create different threat category lists to use in different security profiles, which you can then use in different internet access rules.

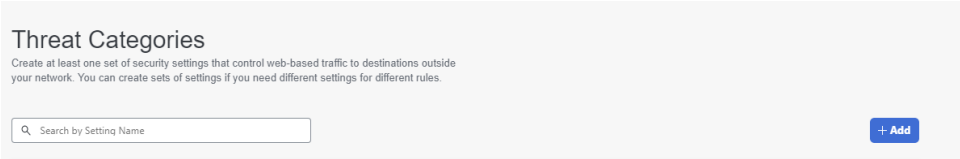
For example, you may want to block access to potentially risky sites for some users, even if this means potentially blocking access to legitimate sites, while for other users you may want to avoid blocking access to any legitimate sites even if it may expose them to risky sites.

Before you begin

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

Procedure

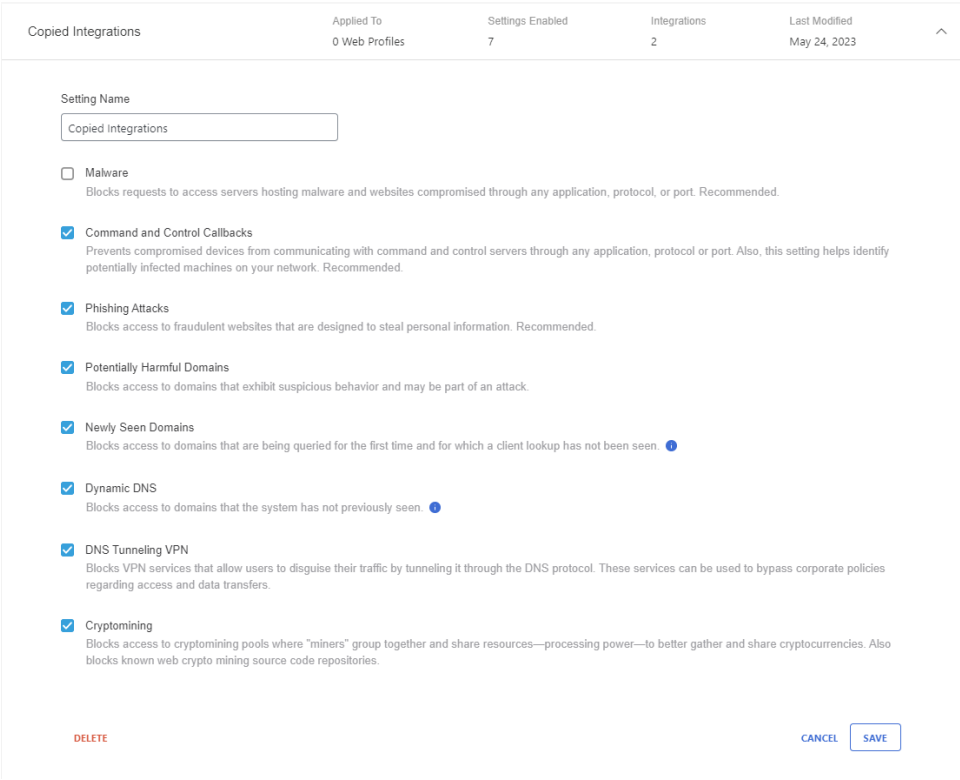
1. Navigate to **Secure** > **Settings** > **Threat Categories** and click **Add**.



2. Give your setting a good descriptive **Setting Name**.

   Select security categories.

   For more information about the categories, see Manage Threat Categories.



3. Click **Save**.

This new threat category list is now available for selection when you add a security profile.

Dispute a Threat Categorization

Provides instructions for dispute a threat categorization. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

When a destination is classified in a category which you disagree with, you can dispute the categorization. Secure Access and Cisco Talos share a unified set of threat categories. You can submit a category dispute request through Cisco Talos

.

Before you begin

- You must have credentials for your Cisco account.

Procedure

1. Navigate to talosintelligence.com.
2. Click **Support**.
3. Click **Content Categorization**.
4. Click **Cisco Login**.
5. Sign in with your cisco.com credentials.
6. Follow instructions on the screen.

37 Manage File Inspection and File Analysis

Topics:

- Manage File Inspection and File Analysis

Describes the purpose and procedures for manage file inspection and file analysis and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage File Inspection and File Analysis

Describes managing file inspection and file analysis. Protect your network from malicious files using file inspection and file analysis. Malicious files can be encountered through an explicit download, such as when a user clicks a link in an email, or through a behind-the-scenes 'drive-by' download scenario.

Protect your network from malicious files using file inspection and file analysis.

Malicious files can be encountered through an explicit download, such as when a user clicks a link in an email, or through a behind-the-scenes 'drive-by' download scenario.

Secure Access offers two options for evaluating files for malicious content:

- File Inspection

Once inspected and analyzed, Secure Access allows "good" files through and blocks the downloading of malicious files. When a malicious file is deleted, Secure Access shows the end user a block page.

Overview of Configuring File Inspection and Analysis

Describes overview of configuring file inspection and analysis. To maximize protection, enable both options. If File Inspection does not detect that a file is malicious, and Secure Malware Analytics is not enabled, the file can be downloaded when requested.

To maximize protection, enable both options. If File Inspection does not detect that a file is malicious, and Secure Malware Analytics is not enabled, the file can be downloaded when requested.

To configure these features:

- Enable file inspection and analysis in a security profile and configure the features
- Ensure that decryption is enabled in the security profile
- Configure block notification pages and choose the applicable page in the security profile
- Associate the security profile with an internet access rule. See Manage Security Profiles

File Inspection Details

Describes file inspection details. When File Inspection is enabled, Secure Access scans files using two features: Cisco Advanced Malware Protection (AMP) and

When File Inspection is enabled, Secure Access scans files using two features:

- Cisco Advanced Malware Protection (AMP) and
- a proprietary antivirus scanner

Cisco Advanced Malware Protection (AMP)

AMP is built on an extensive collection of real-time threat intelligence and dynamic malware analytics supplied by the Talos Security Intelligence and Research Group, and Secure Malware Analytics intelligence feeds. The Cisco AMP engine does not do real-time sandboxing, instead, the Cisco AMP integration blocks files with a known bad reputation based on the checksum or hash of the file. The AMP checksum database is comprised of lookup and data from all AMP customers and is a dynamic global community resource shared between customers utilizing the technology. For more information about AMP, see Advanced Malware Protection (AMP).

Antivirus Scanner

Archives (such as .zip or .rar files) are decompressed and scanned to a maximum of 16 levels of recursion. Files compressed above 16 levels of recursion are blocked. A password-protected archive is not scanned as it cannot be decompressed without a password. However, a password-protected archive can be blocked under the antivirus' Protected Archive category. Secure Access blocks downloads if there is a scanning error or the file is found to be corrupt. Once virus scanning is complete, the file is either delivered or the connection is terminated.

Enable File Inspection

Provides instructions for enabling file inspection. File Inspection uses multiple features to evaluate for malicious files. For details, see Manage File Inspection and Analysis.

To inspect files for threats, enable the file inspection features in security profiles for internet and private access, then assign the security profiles to internet and private access rules.

File Inspection uses multiple features to evaluate for malicious files. For details, see Manage File Inspection and Analysis.

Once inspections are complete, a file is either delivered to the end user or the connection is terminated and the user is shown a block page.

Once you have enabled File Inspection, to monitor and review Umbrella's inspection activities, use the Security Activity and Activity Search reports.

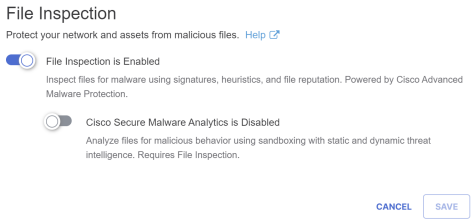
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Determine which options you want to enable. For details, see Manage File Inspection.

  If you will enable file analysis: Before you enable that feature, see important caveats in Enable File Analysis by Secure Malware Analytics. By default, File Inspection is enabled and file analysis is not. You must first enable File Inspection before you can enable file analysis.
- Decryption must be enabled. See Manage Traffic Decryption.
- Certificates are required to decrypt traffic and detect files, and to display block notifications for files blocked in internet traffic.
  - For internet traffic, see Certificates for Internet Decryption.
  - For traffic to private resources, configure certificates in each private resource or see Manage Certificates for Private Resource Decryption.

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Click **+Add Profile** or expand an existing profile.
3. In the **Security and Acceptable Use Controls** section, for **File Inspection**, click **Edit**.
4. Enable **File Inspection** if it is not already enabled:



5. Click **Save**.
6. If you will enable file analysis using Cisco Secure Malware Analytics, see important information and follow the procedure in Enable File Analysis by Cisco Secure Malware Analytics.
7. For security profiles for internet access: In the same profile, ensure that Decryption is enabled.
8. For security profiles for private access: Ensure that destinations configured in the rule are configured as Private Resources with decryption enabled.
9. Choose a security profile that has file inspection enabled when you configure access rules.

Enable File Analysis by Cisco Secure Malware Analytics

Provides instructions for enabling file analysis by cisco secure malware analytics. For file processing details, see Manage File Inspection and Analysis.

For maximum protection, files that are unknown to the File Inspection service (AMP) that are not blocked by the anti-virus feature can be sent to Secure Malware Analytics for further analysis.

For file processing details, see Manage File Inspection and Analysis.

When you enable this option, you will create a Secure Malware Analytics account.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Determine which options you want to enable. For details, see Manage File Inspection.

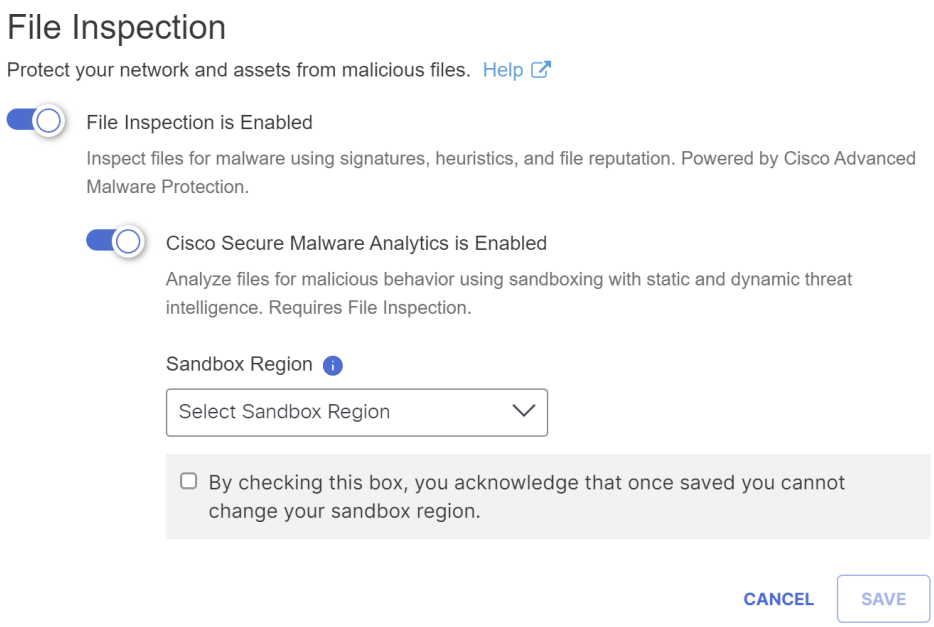
  If you will enable file analysis: Before you enable that feature, see important caveats in Enable File Analysis by Secure Malware Analytics. By default, File Inspection is enabled and file analysis is not. You must first enable File Inspection before you can enable file analysis.
- Decryption must be enabled. See Manage Traffic Decryption.
- Certificates are required to decrypt traffic and detect files, and to display block notifications for files blocked in internet traffic.
  - For internet traffic, see Certificates for Internet Decryption.
  - For traffic to private resources, configure certificates in each private resource or see Manage Certificates for Private Resource Decryption.

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Expand an existing profile or click **+Add Profile** to add a new profile (for either internet or private access.)
3. In the **Security and Acceptable Use Controls** section, for **File Inspection**, click **Edit**.
4. Enable **File Inspection** if it is not already enabled.

   You cannot enable file analysis unless File Inspection is enabled.
5. Enable **Cisco Secure Malware Analytics**:

   If this is the first time you are enabling this option, you will see this:



6. If you are enabling Secure Malware Analytics for the first time:

   Important

   Read the rest of this procedure before completing the procedure.

   a. There is a time limit for performing additional tasks after saving this configuration.

   b. Select a **Sandbox Region** (**North America** or **Europe**) based on your data sovereignty preferences, then acknowledge that you understand that this location cannot be changed. The sandbox holds files captured from both internet and private traffic.

   c. As soon as you click Save in the next step in this procedure, your organization's sandbox region is set and cannot be changed.

   d. Be prepared to access and take action on the email message you will receive after you click Save in the next step. The email will be sent to the address associated with your Secure Access administrator account.

7. Click **Save**.
8. Log into Secure Malware Analytics:

   Important

   You must log into Secure Malware Analytics within 36 hours of setting your sandbox region.

   a. Take action using the email message you will receive from Secure Malware Analytics.

      You will sign into Secure Malware Analytics using the unique link provided in the email message.

      If you chose the Europe sandbox, the link goes to panacea.threatgrid.eu.

      If you chose the North America sandbox, it goes to panacea.threatgrid.com.

      You will accept the End User License Agreement and set up your password. Your Secure Malware Analytics username will be the same email address as your Secure Access account.

b. Store your Secure Malware Analytics password securely so that you can use it later; you will need to sign in to Secure Malware Analytics to review information about files sent for analysis.

Test File Inspection

Describes testing file inspection. After setting up file inspection, we recommend that you check your configured security profile and internet access rules. You can evaluate File Inspection by pointing your browser to one of our test files.

After setting up file inspection, we recommend that you check your configured security profile and internet access rules. You can evaluate File Inspection by pointing your browser to one of our test files.

Prerequisites

- A source device that is known to have access controlled by Secure Access.
- An internet access rule near the top of the rule order that has a security profile with File Inspection enabled.

  To ensure that the traffic is not blocked by other security features, test the security profile in a rule that has all other security and acceptable use features disabled. Ensure that no other rule in the access policy hits the traffic first.

Procedure

Provides instructions for procedure. Browse to one of Cisco's EICAR test files. After loading a File Inspection test file, you should see a block page. Diagnostic information includes details about which server the file went through. If you do not see a block page, see Troubleshoot File Inspection.

Procedure

1. Browse to one of Cisco's EICAR test files.

Test File	Description
http://proxy.opendnstest.com/download/eicar.com	Clear text test file.
https://ssl-proxy.opendnstest.com/download/eicar.com	Encrypted test file.
http://proxy.opendnstest.com/download/AMP_TEST_FILE.txt	Cisco AMP clear text test file.
https://ssl-proxy.opendnstest.com/download/AMP_TEST_FILE.txt	Cisco AMP encrypted test file.

2. After loading a File Inspection test file, you should see a block page. Diagnostic information includes details about which server the file went through. If you do not see a block page, see Troubleshoot File Inspection.

Block Page Diagnostic Information

Provides instructions for block page diagnostic information. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Block page diagnostic information identifies the hostname of the reputation authority. When proxying a domain or URL, Secure Access evaluates the destination in two phases.

Procedure

1. Secure Access receives a request and checks the reputation of the domain or URL. If the destination is known to be malicious, Secure Access blocks the request and displays a block page. The block page diagnostic information lists the `Server` as `nginx`.
2. Next, Secure Access checks if a destination matches a security category or is blocked by an internet access rule. If a destination is not blocked, then Secure Access retrieves any requested content from the URL, then scans the requested files by file inspection (antivirus and AMP). If a file is malware, Secure Access returns a block page. The block page diagnostic information lists the `Server` as `mps`.

Monitor File Inspection and Analysis Activity

Describes monitoring file inspection and analysis activity. There are several places to monitor file inspection and Secure Malware Analytics activity.

There are several places to monitor file inspection and Secure Malware Analytics activity.

Monitor and Review File Inspection and Analytics

To review inspection activity at any time, use the Security Activity and Activity Search reports.

Monitor and Review Secure Malware Analytics

Your Secure Access licensing package includes access to a version of the dashboard in Secure Malware Analytics.

To review submitted files and Secure Malware Analytics activity, sign into Secure Malware Analytics.

The URL that you sign into depends on the sandbox region you chose the first time you enabled the Secure Malware Analytics feature in Secure access:

- If you chose Europe, use https://panacea.threatgrid.eu/login.
- If you chose North America, use https://panacea.threatgrid.com/login.

The first time you enable Secure Malware Analytics in a security profile, you set up credentials to access Secure Malware Analytics. You cannot use your Secure Access credentials to sign into Secure Malware Analytics.

For information about how to use Secure Malware Analytics, see the online help in Secure Malware Analytics.

Depending on your licensing package, you may not have access to all features in the Secure Malware Analytics dashboard. If you are a Secure Malware Analytics Cloud customer and have access to the full functionality of Secure Malware Analytics, you can link your Secure Access account to your Secure Malware Analytics Cloud portal. For more information, contact your account manager or Secure Malware Analytics support.

Monitor file Submission Limits

If your licensing package limits the number of files that Secure Access can submit to Secure Malware Analytics, you should monitor file submission rates to ensure that potentially harmful files are analyzed.

To do this, sign into Secure Malware Analytics using the credentials you set up the first time you enabled Secure Malware Analytics in Secure Access.

The file limit applies to each rolling 24 hour period. At the end of the rolling 24 hour time period, the file quota is cleared and submissions start again–if the file limit is reached; otherwise, submissions continue unabated. To remove the limit, contact your account manager.

To determine your current licensing package, navigate to Admin > Licensing. For more information, see Determine Your Current Package. See also Cisco Secure Access Packages.

For more information about how to use Secure Malware Analytics, see the online Help in the Secure Malware Analytics dashboard.

Troubleshoot and Monitor File Inspection and Analysis

Describes troubleshooting and monitor file inspection and analysis. When File Inspection is enabled, and Secure Access does not present a block page when expected:

General Troubleshooting

When File Inspection is enabled, and Secure Access does not present a block page when expected:

- Check to be sure that the rule that matched the traffic has the security profile that has file inspection and analysis enabled.
- Ensure that the rule that needs to match the traffic is above other rules in the policy that the traffic might also match.
- Confirm that a required certificate is installed. For more information, see Certificates for Internet Decryption.

Wait at least five minutes before testing again after any policy changes to ensure enough time has passed for the changes to be replicated throughout the Secure Access infrastructure. If problems persist, try clearing the local browser cache on your machine, or even your machine's DNS cache (a reboot will accomplish this).

38 Manage File Type Controls

Topics:

- Enable File Type Controls
- File Types to Block
- Review File Type Controls Through Reports

Introduces managing file type controls. Cisco Secure Access provides security use controls in the Security profile. One of the security controls–File Type Blocking–controls access to certain types of files.

Cisco Secure Access provides security use controls in the Security profile. One of the security controls–File Type Blocking–controls access to certain types of files. When enabled, a source that attempts to download a selected file type is presented with a Block page and the requested file cannot be downloaded.

Secure Access checks a file based on the file's file extension and also evaluates each file to determine its type. For example, if a .gif file extension is changed to .xyz, Secure Access is still able to detect that the file is a .gif file. Thus, if you set your policy rule to block .gif files but allow .xyz files, Secure Access blocks any .gif file that has had its extension changed to .xyz.

Enable File Type Controls

Describes enabling file type controls. In Cisco Secure Access, you can manage the file type controls for either internet or private access in the Security profile. The file type control settings determine whether an end user can access certain types of files on internet or private destinations.

In Cisco Secure Access, you can manage the file type controls for either internet or private access in the Security profile. The file type control settings determine whether an end user can access certain types of files on internet or private destinations.

Important

For internet destinations and internet access rules in the Access policy, Secure Access supports the option to manage the upload, download, or upload and download of file types selected in the Security profile. Secure Access is releasing this option beginning on June 1, 2025 and completing the rollout of the feature on July 31, 2025.

About File Type Controls for Internet Access

Describes about file type controls for internet access. In a Security profile, configure the file type controls for files on internet destinations. You can choose whether to control the upload, download, or upload and download of certain types of files.

In a Security profile, configure the file type controls for files on internet destinations. You can choose whether to control the **upload**, **download**, or **upload and download** of certain types of files. Then, add the Security Profile for internet access to the internet access rules in the Access policy.

If **File Type Blocking** is enabled and a user device attempts to download or upload a selected file type from an internet destination, Secure Access presents a Block page instead of the requested resource.

Note

Blocking some file types may cause a website not to display correctly.

About File Type Controls for Private Access

Describes about file type controls for private access. In a Security profile, configure the file type controls for files on private destinations. You can choose whether to download certain types of files. Then, add the Security Profile for private access to the private access rules in the Access policy.

In a Security profile, configure the file type controls for files on private destinations. You can choose whether to **download** certain types of files. Then, add the Security Profile for private access to the private access rules in the Access policy.

Procedure

Describes procedure. Enable File Type Blocking for Internet Access Enable File Type Blocking for Private Access Full Admin user role. For more information, see Manage Accounts.

- Enable File Type Blocking for Internet Access
- Enable File Type Blocking for Private Access

Prerequisites

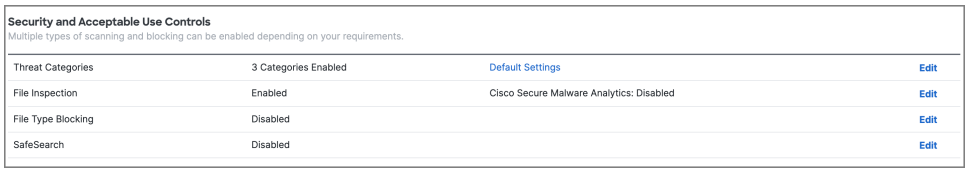
- Full Admin user role. For more information, see Manage Accounts.
- Enable decryption in the same Security profile for internet access where you configure the file type controls.
- In private access rules, configure decryption for private resources as rule destinations.

Enable File Type Blocking for Internet Access

Provides instructions for enabling file type blocking for internet access. Navigate to Secure Security Profiles , Click Add Profile and then choose Internet Access, or expand an existing Security profile.

Procedure

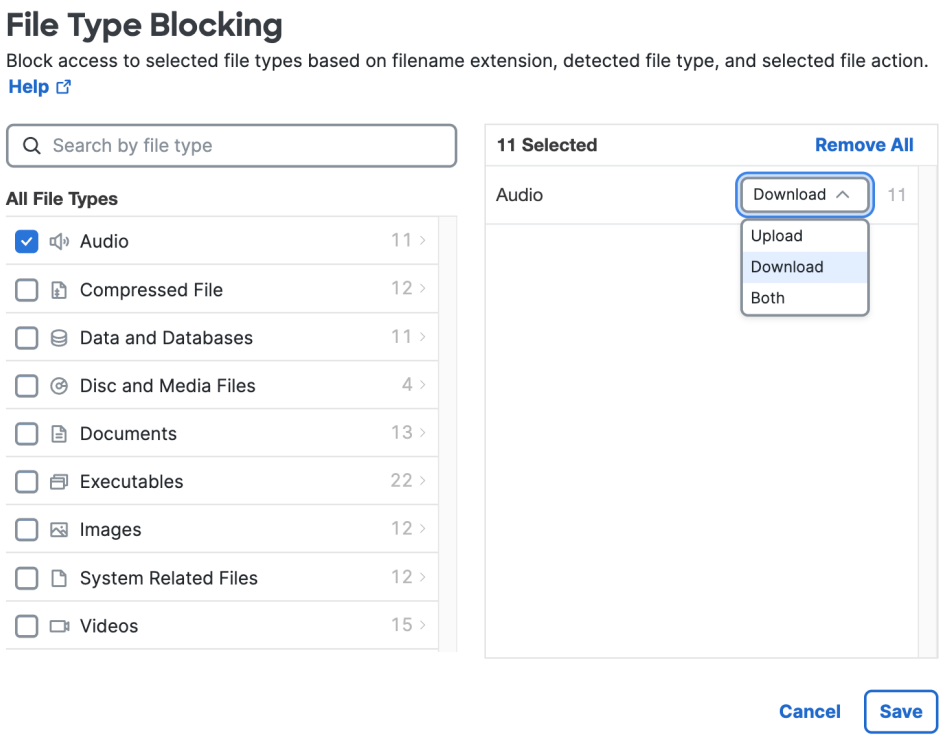
1. Navigate to **Secure** > **Security Profiles**,
2. Click **Add Profile** and then choose **Internet Access**, or expand an existing Security profile.
3. Navigate to **Security and Acceptable Use Controls**, navigate to **File Type Blocking**, and then click **Edit**.



4. For **File Type Blocking**, search for specific file types or choose the file types to block.
   a. Check the categories of the file types to choose all file types in the group, or expand a file type category to choose specific file types. For more information about available file types, see File Types to Block.

   > **Note**
   >
   > When an entire file type group is selected, all future file types added to that group are also blocked.

   b. Choose either **Upload**, **Download**, or **Both**.



5. Click **Save**.

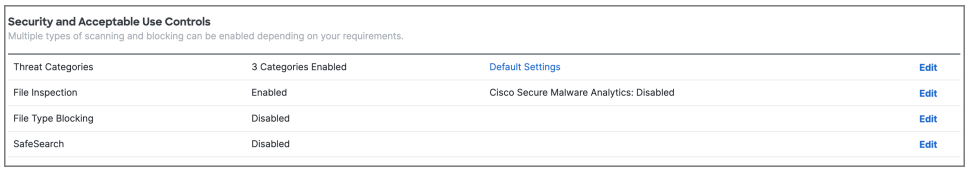
   Use the Security profile in an internet access rule to apply the file type blocking security controls to the configured destinations.

Enable File Type Blocking for Private Access

Provides instructions for enabling file type blocking for private access. Navigate to Secure Security Profiles , Click Add Profile and then choose Private Access, or expand an existing Security profile.

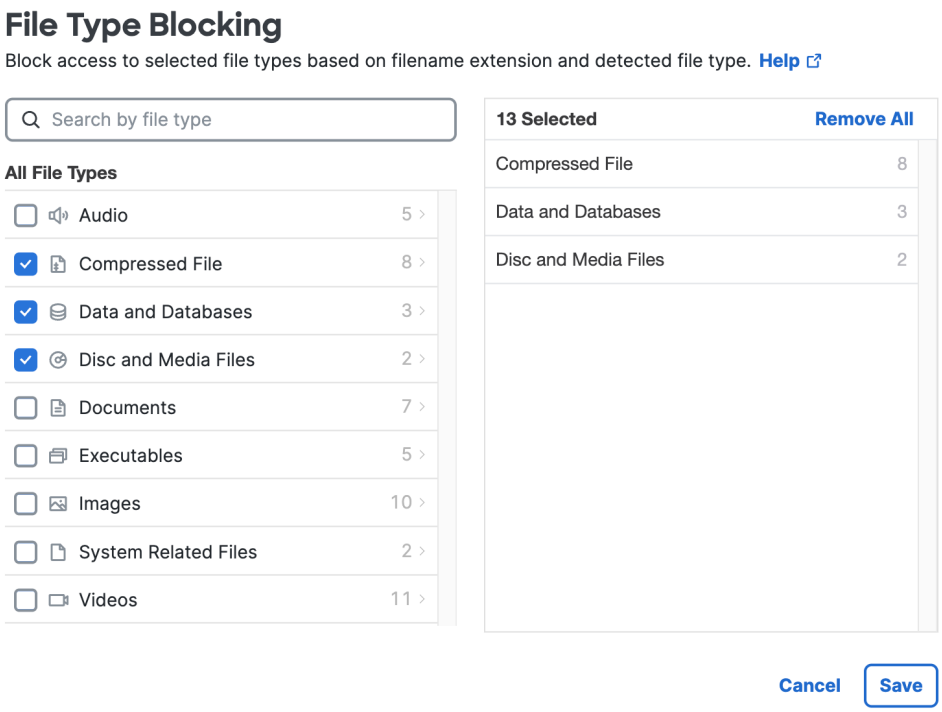
Procedure

1. Navigate to **Secure** > **Security Profiles**,
2. Click **Add Profile** and then choose **Private Access**, or expand an existing Security profile.
3. Navigate to **Security and Acceptable Use Controls**, navigate to **File Type Blocking**, and then click **Edit**.



4. For **File Type Blocking**, search for specific file types or choose the file types to block.
   - Check the categories of the file types to choose all file types in the group, or expand a file type category to choose specific file types. For more information about available file types, see File Types to Block.

> **Note**
>
> When an entire file type group is selected, all future file types added to that group are also blocked.



5. Click **Save**.

   Use the Security profile in a private access rule to apply the file type blocking security controls to the configured destinations.

File Types to Block

Describes file types to block. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

You can block the following file types in a Security profile.

Audio	Compressed	Data and Database	Disc and Media	Documents	Executable	Image	System-related	Video
aif cda m4a mid mp3 mpa ram snd wav wma wpl	7z arj deb gz pak pkg rar rar rpm tar.gz tbz z zip	csv dat db log mdb nzb sav sql tar torrent	dmg iso toast vcd	doc docm docx dotm pdf pop potm pptx rtf tex xls xlsm xlsx	apk bat bin cgi com dll exe hta jar js moo msi pif pl prg py sh swf vb vbs vm wsf	ai bmp gif ico jpeg jpg png ps psd rm svg tif tiff	bak cab cpl cur drv emu icns ini ps1 scr sys tmp	avi flv gat h264 m4v mkv mov mp4 mpeg qtm rm rv ssm vob wmv

Review File Type Controls Through Reports

Provides instructions for reviewing file type controls through reports. Its purpose, requirements, and key details for Cisco Secure Access administrators.

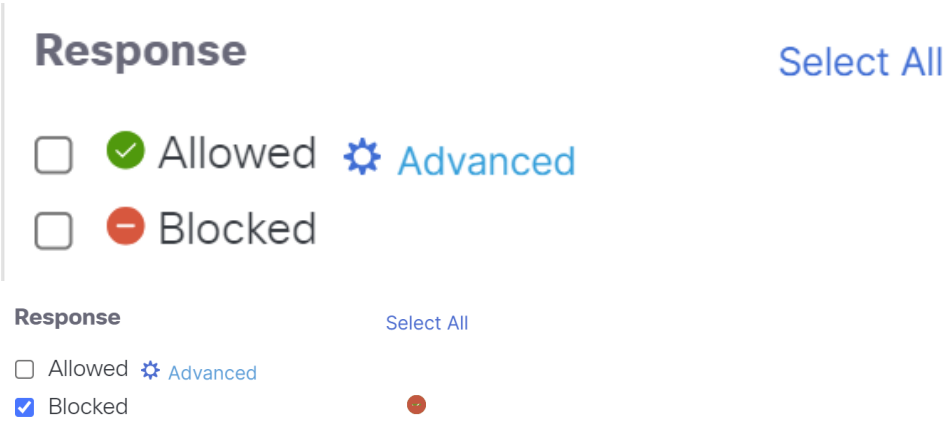
File types enabled through security profiles are listed in the Activity Search Report.

Before you begin

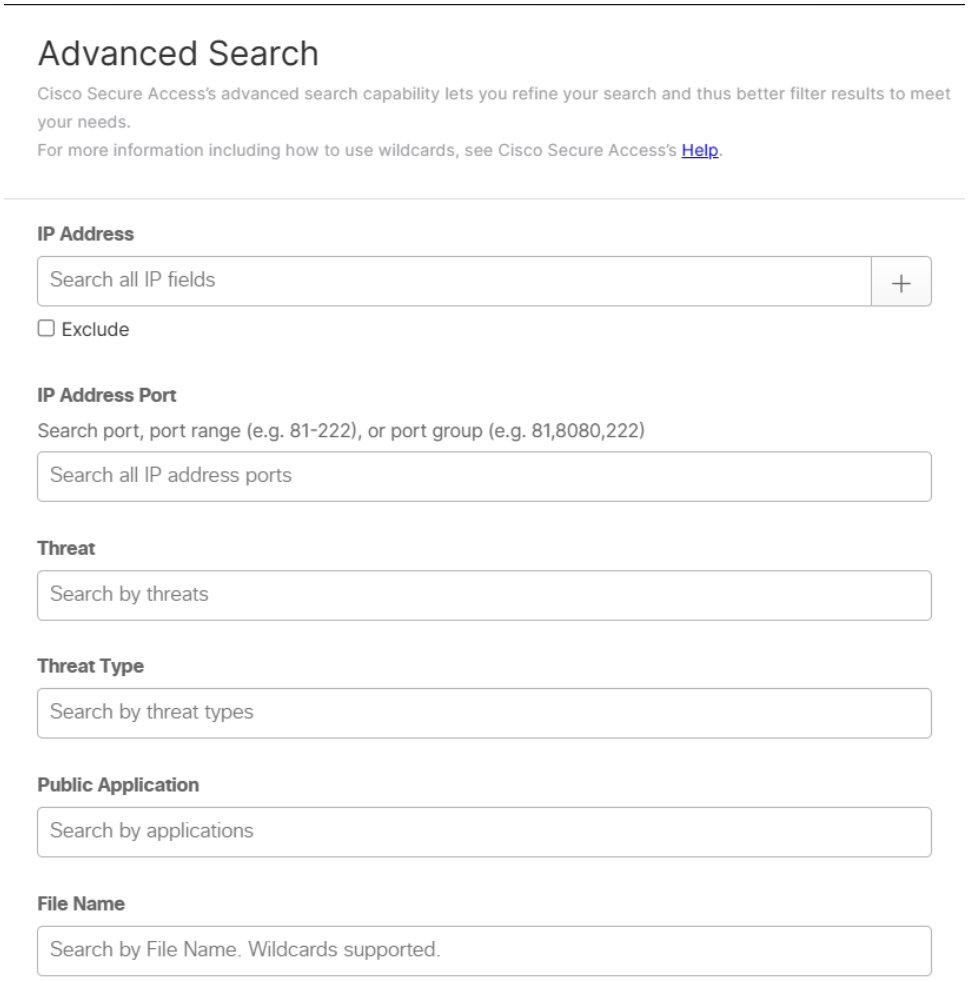
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. Under the **Response** filter, choose **Blocked**.

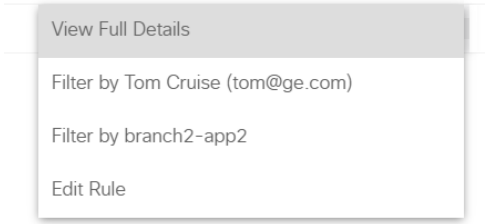


3. Click **Advanced** in the search bar to bring up the Advanced search. Under **File Name**, enter the asterisk wildcard symbol and a file type to search by. Click **Apply**.

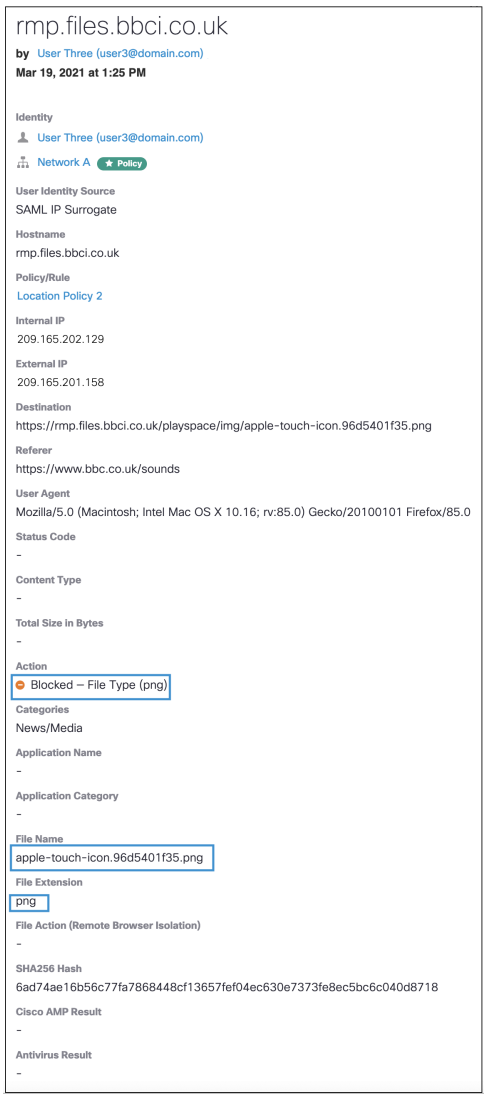


The results will filter by events where files of that type were blocked.

4. Click the action menu and select **View Full Details.**



5. View further details of the blocked file, such as the action taken, the name of the file, and the file extension.


rmp.files.bbci.co.uk
by User Three (user3@domain.com)
Mar 19, 2021 at 1:25 PM
Identity
User Three (user3@domain.com)
Network A
Policy
User Identity Source
SAML IP Surrogate
Hostname
rmp.files.bbci.co.uk
Policy/Rule
Location Policy 2
Internal IP
209.165.202.129
External IP
209.165.201.158
Destination
https://rmp.files.bbci.co.uk/playspace/img/apple-touch-icon.96d5401f35.png
Referer
https://www.bbc.co.uk/sounds
User Agent
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:85.0) Gecko/20100101 Firefox/85.0
Status Code
-
Content Type
-
Total Size in Bytes
-
Action
Blocked – File Type (png)
Categories
News/Media
Application Name
-
Application Category
-
File Name
apple-touch-icon.96d5401f35.png
File Extension
png
File Action (Remote Browser Isolation)
-
SHA256 Hash
6ad74ae16b56c77fa7868448cf13657fef04ec630e7373fe8ec5bc6c040d8718
Cisco AMP Result
-
Antivirus Result
-

39 Manage Notification Pages

Topics:

- Manage Notification Pages

Describes the purpose and procedures for manage notification pages and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Notification Pages

Describes managing notification pages. Secure Access displays notification pages to end users when users try to: Access a destination that is blocked by security profile configurations in an internet access rule. In this case, they see a Block page.

Secure Access displays notification pages to end users when users try to:

- Access a destination that is blocked by security profile configurations in an internet access rule. In this case, they see a Block page.
- Access an internet destination that matches a rule that is configured with the Warn action. In this case, they see a Warn page.

You can display the default Secure Access notification or create one or more custom notifications to display in different situations.

Each security profile is associated with a single notification page configuration that includes both Block and Warn pages.

View Notification Pages Displayed to End Users

In Secure Access you can view the default notification page and any custom notification pages. For more information, see Preview Notification Pages.

Display Custom Notification Pages to End Users

- Create custom notification pages for blocked destinations and destinations in rules configured with the Warn action. See Create Custom Block and Warn Pages.
- Configure one or more security profiles to use custom notification pages. See Add a Security Profile.
- In the default security profile, choose the block and warn pages to display when traffic matches internet access rules that use the default security profile. To choose a default security profile, see Edit Rule Defaults and Global Settings.
- Configure internet access rules to use the security profiles which you have configured to display your custom notification pages. If you want to display a Warn page, choose the Warn action in the rule.
- Deploy required certificate(s). For more information, see Certificates for Internet Decryption.If user devices do not have the necessary certificate, users will see standard browser error when they try to access a blocked destination.

About Warn Pages for Internet Access Traffic

When end users try to access a destination in an access rule configured with the Warn action, they must click a link in a warning message in order to access the destination.

A Warn page, once clicked through, allows content access for one hour. After one hour, the Warn page reappears and the user must click through again to access the requested destination.

About Block Pages for Private Access Traffic

The notification pages described in this section do not apply to private access rules. See Manage Private Access Rules.

Preview Notification Pages

Provides instructions for preview notification pages. In Cisco Secure Access, you can preview the default notification page and any custom notification pages. Secure Access displays a preview of the notification pages from a Security profile for internet access and on the Secure Settings Notification Pages page.

In Cisco Secure Access, you can preview the default notification page and any custom notification pages. Secure Access displays a preview of the notification pages from a Security profile for internet access and on the **Secure** > **Settings** > **Notification Pages** page.

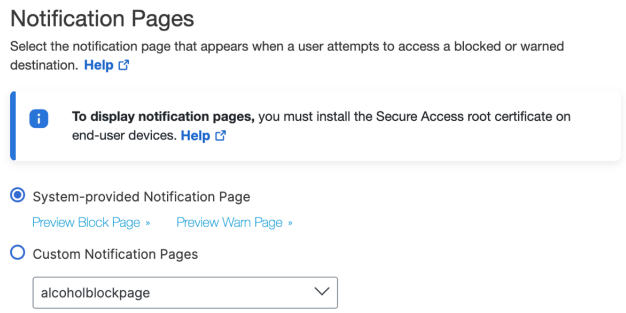
This guide describes the steps to preview default and custom notification pages from a Security profile for internet access.

Before you begin

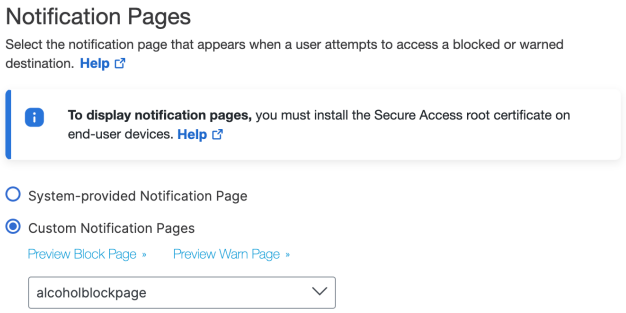
- Full Admin user role. For more information, see Manage Accounts.
- The organization's DNS must resolve to the Secure Access's DNS servers.

Procedure

1. Navigate to **Secure** > **Profiles** > **Security Profiles**.
2. Edit an existing profile, or click **Add Profile** > **Internet Access**.
3. Scroll down to **End-User Notifications** and click **Edit**.
4. Preview the default notification pages.
   a. Select **System-provided Notification Pages**.
   b. Click the blue Preview links (one each for Block and Warn pages).



5. Preview a custom notification page.
   a. Select **Custom Notification Pages**.
   b. Click **Choose an existing appearance** and choose the notification page design you want to preview.
   c. Click the blue Preview links (one each for Block and Warn pages).



6. Click **Save**

Create Custom Block and Warn Pages

Provides instructions for creating custom block and warn pages. Instead of showing end users the default block or warn message with the Secure Access logo, you can display your own logo, custom Block and Warn messages, and an option to contact an administrator.

Instead of showing end users the default block or warn message with the Secure Access logo, you can display your own logo, custom Block and Warn messages, and an option to contact an administrator. You can also display different pages depending on the reason for the block.

You can create a custom Block page and a custom Warn page as a set, and then choose them in security profiles for internet access.

Before you begin

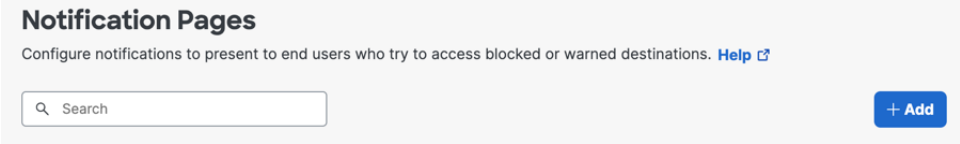
- Full Admin user role. For more information, see Manage Accounts.
- Gather your logo, help desk email address, and any other information you want to provide.
- If you use a custom logo, Secure Access notification pages support PNG and JPEG.

  Images larger than 125x70 pixels will be cropped and resized.

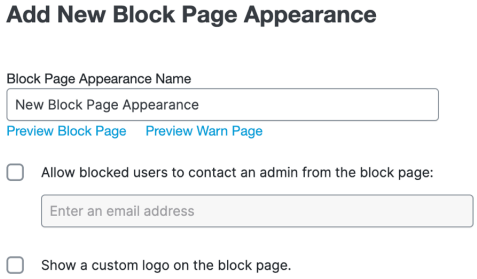
Procedure

1. Navigate to **Secure** > **Settings** > **Notification Pages**.
2. Click **+Add**, or expand the setting you want to edit.

   The settings on the page are optional.

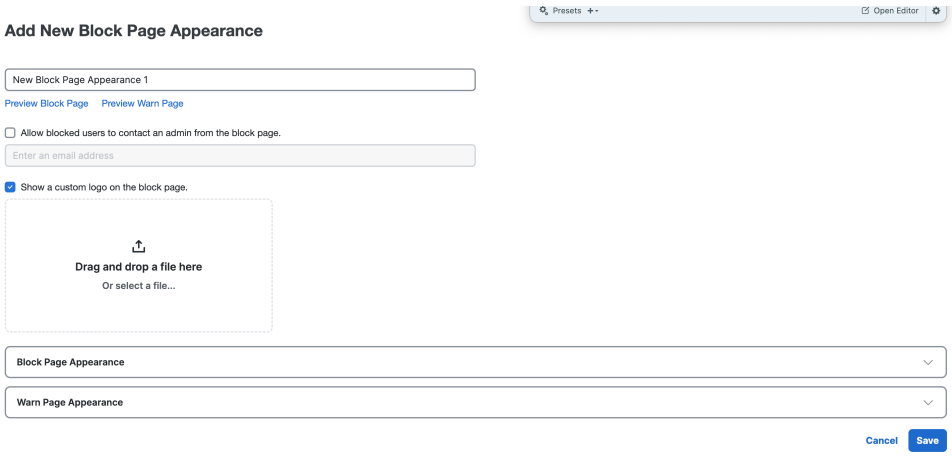


3. If this is a new configuration, name this set of notification pages.



4. Click **Allow blocked users to contact an admin from the block page**. If you want to allow end users to contact an administrator from a block message, provide the email address that will be used to forward user messages. For more information, see Allow Users to Contact an Administrator.
5. Click **Show a custom logo on the block page**.

   Secure Access notification pages support PNG and JPEG. Images larger than 125x70 pixels will be cropped and resized.



6. Expand **Block Page Appearance**.
   a. If you want to display a unique message based on the reason for the block, click **Differently** and click a Block reason. If you want to display the same message for all block reasons, select **The Same** so that users see a consistent notification regardless of the reason for the block.
   b. Click **Show a block page with the default message** to display the default message.
   c. Click **Show a block page with a custom message** to specify your custom message.

      You can adjust the size of text, as well as bold, italicize, underline, or strikethrough it. You can also add hyperlinks, numbered lists, and bulleted lists.

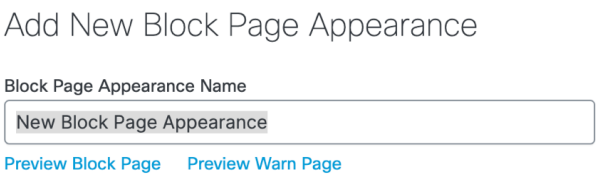
      You can also use the following variables within your message.

      - **[domain]**–Substitutes the domain name that the end-user tried to browse to.
      - **[client_ip]**–Substitutes the external IP address of the client that is hitting the block page.

   d. Click **Redirect Users to this URL** and enter the URL to which users should be redirected.

7. Expand **Warn Page Appearance**.
   a. Click **Show a warn page with the default message** to display the default message.
   b. Click **Show a warn page with a custom message** to specify your custom message, using the same guidelines as for a custom block message.

8. Preview your notification pages:
   a. Scroll to the top of your configuration.
   b. Click the **Preview Block Page** or **Preview Warn Page** links.



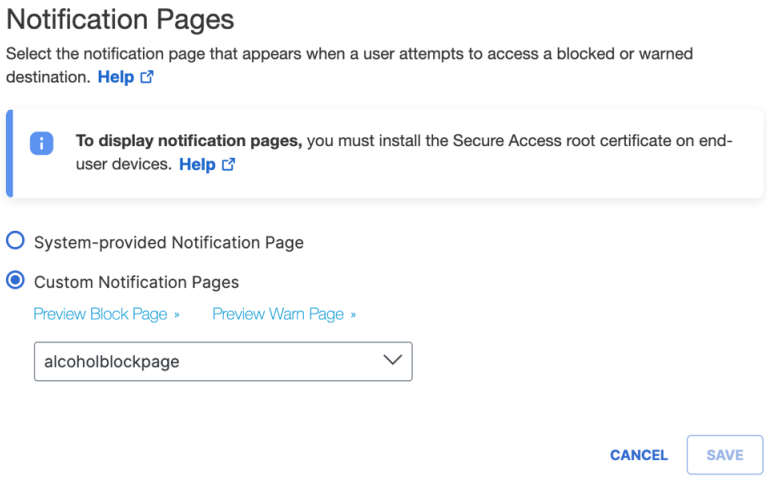
9. Click **Save**.

Link a Custom Notification Page Appearance to a Security Profile

Provides instructions for link a custom notification page appearance to a security profile. Navigate to Secure Security Profiles and expand the profile you'd like to link.

Procedure

1. Navigate to **Secure** > **Security Profiles** and expand the profile you'd like to link.
2. Under **End-User Notifications** click **Edit** for **Notification Pages**.



3. Choose **Custom Notification Pages**, and then choose the notification page appearance to get the set of block and warn pages.
4. Click **Save**.

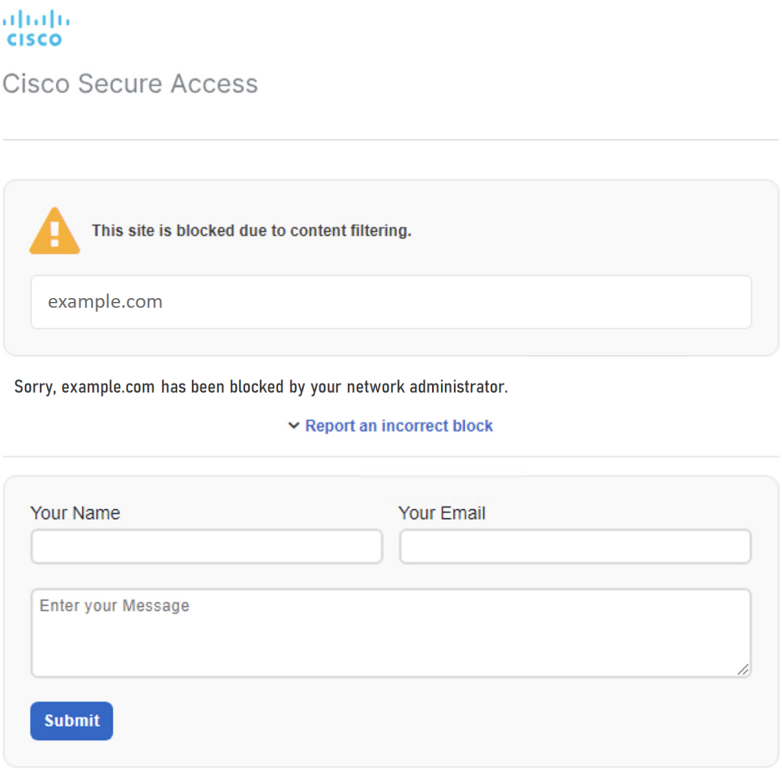
What to do next

Complete the remaining requirements described in Manage Notification Pages.

Allow Users to Contact an Administrator

Provides instructions for allow users to contact an administrator. If you configure Secure Access to allow end users to contact an administrator from the block page, users can notify you if they feel a website should not be blocked.

If you configure Secure Access to allow end users to contact an administrator from the block page, users can notify you if they feel a website should not be blocked. When end users attempt to access blocked sites, Secure Access includes a contact form at the bottom of block notifications:



After the end user submits the form, Secure Access sends an email message to the administrator address you provided, including the user's message and diagnostic information that helps you determine whether to allow access to the site.

Note

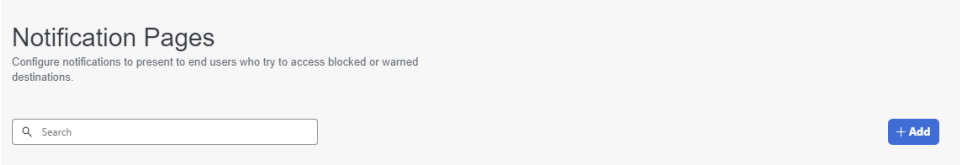
Assistance With Allowing Websites: If you are unsure if a website should be allowed or have questions about a domain classification, contact Support.

Before you begin

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

Procedure

1. Navigate to **Secure** > **Settings** > **Notification Pages** and click the setting you want to edit.

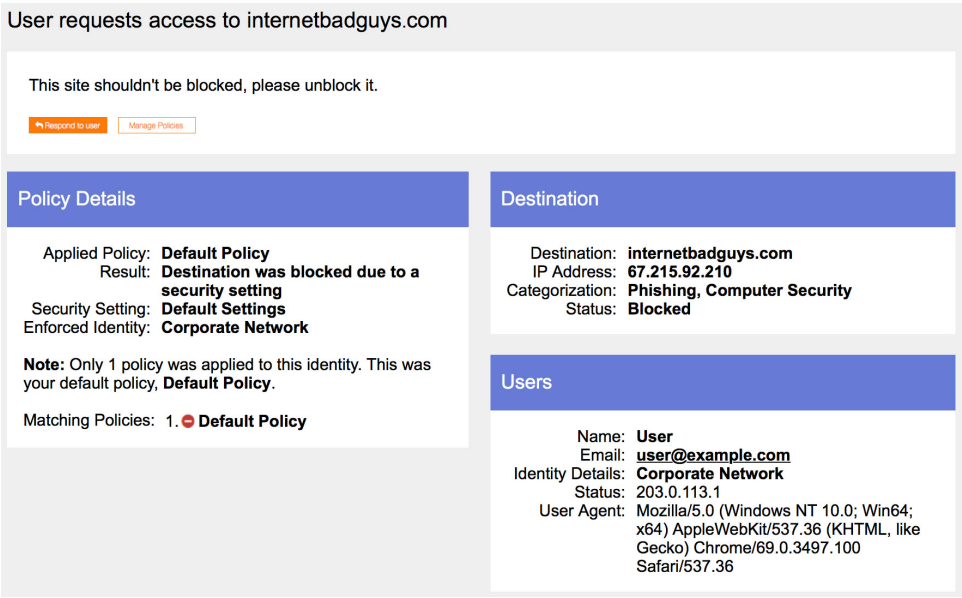


2. Select **Allow blocked users to contact an admin from the block page** and enter an email address of the administrator, to allow end-users to contact an administrator from your organization. You can only add one email.



3. Click **Save**.

The following is an example of an email sent to an administrator when a user sent a message from a block page:



Block Page IP Addresses

Describes block page ip addresses. When Secure Access blocks a domain or URL, the Secure Access DNS servers display a block page instead of the requested page. Secure Access provides different types of block pages depending on the security event.

When Secure Access blocks a domain or URL, the Secure Access DNS servers display a block page instead of the requested page. Secure Access provides different types of block pages depending on the security event.

IP Addresses for Secure Access Block Pages

The following table describes the types of block pages, DNS record types, and Anycast IP addresses for the Secure Access servers.

Block Page Type	Record Type	IPv6 Addresses
Domain List	A	18.253.87.126, 18.253.94.118, 18.253.45.107
Domain List	AAAA	2600:1f15:3a9:7900:88ea:d972:3b3a:7a46, 2600:1f15:3a9:7901:3db6:77bf:525b:8e96, 2600:1f15:3a9:7902:b9d7:218b:91ea:a727
Command and Control Callback	A	18.252.236.99, 18.253.205.239, 16.64.88.211
Command and Control Callback	AAAA	2600:1f15:3a9:7900:c93b:96cc:9c8a:1cfa, 2600:1f15:3a9:7901:3ce8:3056:eaa5:f8db, 2600:1f15:3a9:7902:7f5b:ffa9:e18a:eedf
Content Category or Application	A	182.30.49.246, 18.254.225.10, 16.64.34.204
Content Category or Application	AAAA	2600:1f15:3a9:7900:dbe3:4913:94a2:28e7, 2600:1f15:3a9:7901:c751:a90b:a7d0:783a, 2600:1f15:3a9:7902:3897:34e9:ed25:b88c

Block Page Type	Record Type	IPv6 Addresses
Malware	A	18.254.71.48, 16.64.77.81, 16.64.3.101
Malware	AAAA	2600:1f15:3a9:7900:3d59:9958:fcf7:4d4b, 2600:1f15:3a9:7901:baed:f166:bb99:b852, 2600:1f15:3a9:7902:542d:b93c:62c1:da4d
Phishing	A	16.64.58.196, 182.30.95.86, 16.64.44.65
Phishing	AAAA	2600:1f15:3a9:7900:90c4:c14:60f4:78ec, 2600:1f15:3a9:7901:9037:4de:9df1:b3ef, 2600:1f15:3a9:7902:36d9:ec53:c1d:384
Security Integrations, Newly Seen Domains, DNS Tunneling VPN, Potentially Harmful, and Dynamic DNS	A	16.64.101.72, 18.252.86.49, 18.252.224.185, 16.64.116.188, 16.64.19.231, 18.254.233.234
Security Integrations, Newly Seen Domains, DNS Tunneling VPN, Potentially Harmful, and Dynamic DNS	AAAA	2600:1f15:3a9:7900:e608:e9d7:8148:b66e, 2600:1f15:3a9:7901:2a94:3c22:9765:b43b, 2600:1f15:3a9:7902:a7c0:1479:a270:1699

Domains for Secure Access Block Pages

Secure Access displays block pages on these domains:

- **block.secureaccessfed.cisco**
- **phishing.block.secureaccessfed.cisco**
- **malware.block.secureaccessfed.cisco**

40 Manage Traffic Decryption

Topics:

- Manage Traffic Decryption

Describes the purpose and procedures for manage traffic decryption and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Traffic Decryption

Describes managing traffic decryption. Decryption is used for various purposes in Secure Access. You will configure decryption when you configure those features.

Decryption is used for various purposes in Secure Access. You will configure decryption when you configure those features.

- Internet Access Features Requiring Decryption
- Internet Traffic That Should Not Be Decrypted
- Decryption in Private Access Rules
- Decryption Settings
- Decryption requires certificates
- Decryption Logging
- Troubleshooting Decryption
- Important Information About Do Not Decrypt Lists
- Add a Do Not Decrypt List for Security Profiles

Internet Access Features Requiring Decryption

Describes internet access features requiring decryption. The following features require decryption or do not work effectively on encrypted traffic: Intrusion prevention (IPS) for traffic to internet destinations.Traffic must be decrypted in order to inspect HTTPS traffic for known threats and behaviors.

The following features require decryption or do not work effectively on encrypted traffic:

- Intrusion prevention (IPS) for traffic to internet destinations.

  Traffic must be decrypted in order to inspect HTTPS traffic for known threats and behaviors.

- Web security (configured in security profiles).

  Decryption is required for inspection by the security and acceptable use features.

- File inspection and analysis and enforcement of file type controls. For more information, see Manage File Inspection and File Analysis and Manage File Type Control.
- Destinations that are derived from SAML configurations.
- Remote browser isolation (RBI)—If you choose Isolate as the rule action in an internet access rule, affected traffic must be decrypted. Enable decryption in the security profile that you choose for that rule.
- Displaying block and warning notifications to end users. When a destination triggers a warning page, users can only access that destination by clicking the link in the warning notification. For more information, see
  - Manage Notification Pages
  - Tenant Controls
  - Advanced Application Controls.
  - Data Loss Prevention.

Sites that use HTTP rather than HTTPS do not require decryption to benefit from the functionality listed above. However, most sites use HTTPS. Enforcement based on threat categories never requires decryption.

Internet Traffic That Should Not Be Decrypted

Describes internet traffic that should not be decrypted. Certain traffic should not be decrypted for various reasons: N/A See Advanced settings in the Security Controls section of each internet access rule.

Certain traffic should not be decrypted for various reasons:

Traffic that should not be decrypted	How to Configure, and More Information
Traffic to confidential internet destinations, based on laws, regulations, or policy	See Important Information About Do Not Decrypt Lists.
Sites with pinned certificates (for IPS)	See Global Settings for Access Rules.
Sites with pinned certificates (for web security features)	N/A
Microsoft 365 applications	See Global Settings for Access Rules.
Trusted files	See **Advanced** settings in the Security Controls section of each internet access rule. This feature is sometimes called "Protected file bypass."

Decryption in Private Access Rules

Describes decryption in private access rules. Decryption is required for Intrusion prevention (IPS) for traffic to private destinations. Traffic must be decrypted in order to inspect it for known threats and behaviors.

Decryption is required for Intrusion prevention (IPS) for traffic to private destinations. Traffic must be decrypted in order to inspect it for known threats and behaviors.

Traffic to private resources will be decrypted for inspection by the IPS feature only if decryption is enabled for that resource and the required certificate is present.

Traffic to private destinations that are not configured as private resources (that is, traffic to destinations that you type directly into an access rule) is not decrypted.

You will configure decryption for private resources when you configure the private resource.

See Add a Private Resource.

Decryption Settings

Describes decryption settings. Decryption-specific settings appear in the following components: Security profile Do Not Decrypt Lists for Security Profiles Private Resource

Decryption-specific settings appear in the following components:

- Security profile
- Do Not Decrypt Lists for Security Profiles
- Private Resource
- Global Settings

  This settings affect decryption, for private or internet traffic or both.
- Internet access rules, Advanced settings section at the bottom of each rule

Decryption Requires Certificates

Describes decryption requires certificates. In most cases, decryption requires uploading or installing certificates. For details, see Certificates for Internet Decryption.

In most cases, decryption requires uploading or installing certificates. For details, see Certificates for Internet Decryption.

Decryption Logging

Describes decryption logging. Enable or disable decryption logging in Global Settings. See Edit Rule Defaults and Global Settings. To view decryption logs, see Reports.

Enable or disable decryption logging in Global Settings. See Edit Rule Defaults and Global Settings.

To view decryption logs, see Reports.

Troubleshooting Decryption

Describes troubleshooting decryption. If you suspect decryption is causing issues, try the following: Check decryption logs. Temporarily disable decryption globally for IPS, on the Global Settings page. See Edit Rule Defaults and Global Settings.

If you suspect decryption is causing issues, try the following:

- Check decryption logs.
- Temporarily disable decryption globally for IPS, on the Global Settings page. See Edit Rule Defaults and Global Settings.
- Look at the options for traffic that should not be decrypted in the table above.
- See other troubleshooting topics in this guide. The issue may not be specifically related to decryption. For example, see Troubleshoot Private Access Rules and Troubleshoot Internet Access Rules.

Important Information About Do Not Decrypt Lists

Describes important information about do not decrypt lists. Traffic that is not decrypted cannot be effectively inspected for threats. However, in order to comply with confidentiality regulations in some locations, certain traffic should not be decrypted. You can use Do Not Decrypt lists to specify these destinations.

Traffic that is not decrypted cannot be effectively inspected for threats.

However, in order to comply with confidentiality regulations in some locations, certain traffic should not be decrypted. You can use Do Not Decrypt lists to specify these destinations.

Do Not Decrypt lists apply only to destinations in internet access rules, and they are used for both web security and intrusion prevention (IPS) features.

Currently, IPS profiles and security profiles support Do Not Decrypt lists differently:

- All IPS profiles use a single Do Not Decrypt list.
- Each security profile can use any Do Not Decrypt list.
- The types of destinations that you can specify for IPS and web features are different. See the applicable sections below.

Do Not Decrypt List for IPS

Describes do not decrypt list for ips. Destinations on the system-provided Do Not Decrypt list are not decrypted for inspection by the intrusion prevention (IPS) feature.

Destinations on the system-provided Do Not Decrypt list are not decrypted for inspection by the intrusion prevention (IPS) feature.

All IPS profiles use the system-provided Do Not Decrypt list that ships with Secure Access. You can add destinations to this list.

To configure this list, navigate to **Secure** > **Settings** > **Do Not Decrypt Lists**.

Note

About decryption in private access rules

Do not use the system-provided Do Not Decrypt list for private destinations. Instead, you can configure a private resource and not enable decryption for that resource. See Add Private Resources.

Do Not Decrypt Lists for Web

Describes do not decrypt lists for web. When a Do Not Decrypt list is associated with a security profile, destinations on the list will not be decrypted by the security and acceptable use features enabled in that profile.

When a Do Not Decrypt list is associated with a security profile, destinations on the list will not be decrypted by the security and acceptable use features enabled in that profile.

Initially, the default Do Not Decrypt List for security profiles is the same system-provided Do Not Decrypt List that is used for IPS. You can either use this single list for both IPS and security security features, or you can create additional do-not-decrypt lists for use in security profiles. If you want to specify applications as destinations for web security features, create a custom Do Not Decrypt list and specify that list in the security profile. See Add a Do Not Decrypt List for Security Profiles.

Differences Between IPS and Web Destination Types

Describes differences between ips and web destination types. The types of destinations that you can choose not to decrypt is different for IPS and web security features:

The types of destinations that you can choose not to decrypt is different for IPS and web security features:

	Applications	Sites that belong to specified Content Categories	Domains
IPS	No	Yes	Yes
Web	Yes	Yes	Yes

The System-Provided Do Not Decrypt List

Describes the system-provided do not decrypt list. The system-provided Do Not Decrypt list is the only list used by the IPS feature. The same list is the default list used by the web security features.

The system-provided Do Not Decrypt list is the only list used by the IPS feature. The same list is the default list used by the web security features. The system-provided Do Not Decrypt list does not include the ability to specify applications; this option is available only in custom lists.

Initially, this list is empty. Add the destinations that are important to your organization.

Limitation: Do Not Decrypt Based on Content Category

Describes limitation: do not decrypt based on content category. While web site categorization is updated continuously, it is not possible to categorize all web sites on the internet, and some sites may be categorized incorrectly.

While web site categorization is updated continuously, it is not possible to categorize all web sites on the internet, and some sites may be categorized incorrectly. Therefore, if you choose not to decrypt traffic based on content category, it is possible that traffic to sites that should not be decrypted may be decrypted, and traffic that should be decrypted may not be decrypted.

This limitation is not unique to Cisco.

Add a Do Not Decrypt List for Security Profiles

Provides instructions for adding a do not decrypt list for security profiles. Decrypting traffic to certain destinations may be prohibited by regional privacy regulations.

Decrypting traffic to certain destinations may be prohibited by regional privacy regulations.

Create a custom Do Not Decrypt list to specify destinations that will not be decrypted by the security and acceptable use features in a security profile. HTTPS traffic to these destinations cannot be properly inspected for threats when traffic is not decrypted.

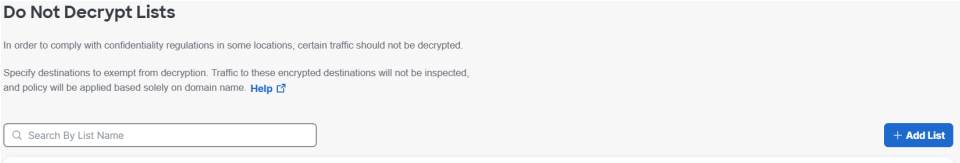
If you need to specify a Do Not Decrypt address for IPS profiles, edit the system-provided Do Not Decrypt List.

Before you begin

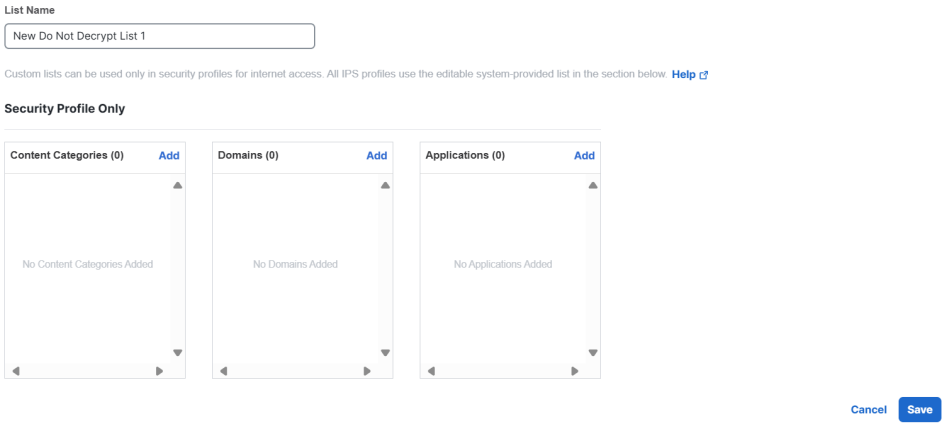
- Full Admin user role. For more information, see Manage Accounts.

Procedure

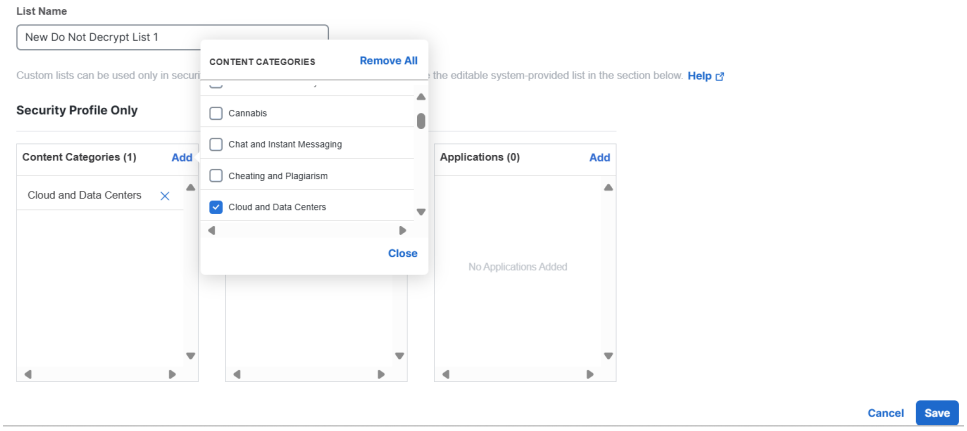
1. Navigate to **Secure** > **Settings** > **Do Not Decrypt Lists** and click **Add**.



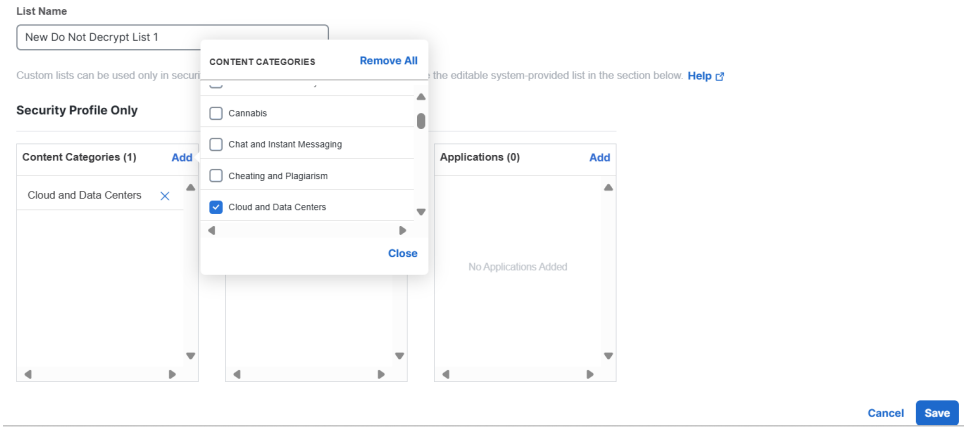
2. Give your list a good descriptive **List Name**.



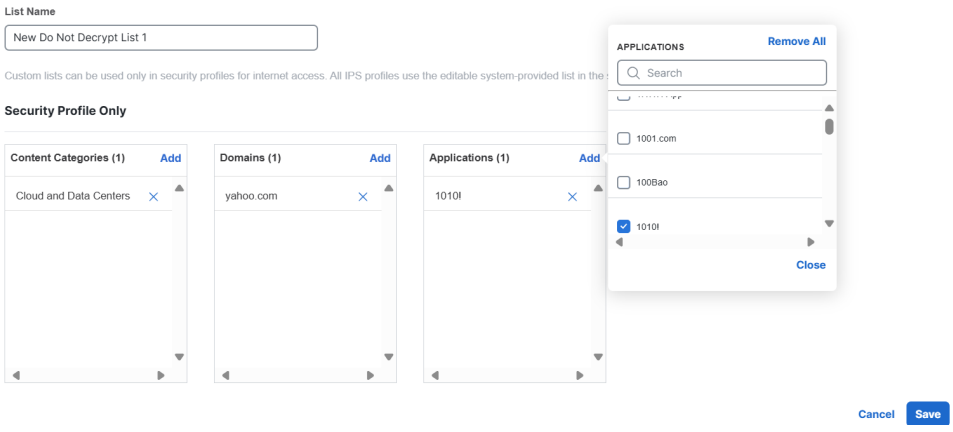
3. Add content categories, applications, and domains that will be exempt from decryption:
   a. Click **Add**, select **Categories** to be exempt from HTTPS inspection and then click **Close**.



b. Click **Add**, select **Categories** to be exempt from HTTPS inspection and then click **Close**.



c. Click **Add**, select **Applications** to be exempt from decryption and then click **Close**.



4. Click **Save**.

Your new Do Not Decrypt List is saved to Secure Access and available for selection when adding Security profiles to the Access policy.

41 Manage Certificates

Topics:

- Certificates for Internet Decryption
- Install the Cisco Secure Access Root Certificate
- Add Custom CA Signed Root Certificate
- Manage Certificates for Private Resource Decryption
- View the Cisco Trusted Root Store
- Manage SAML Certificates for Identity Providers
- Certificates for Private Resource Decryption
- Certificates for SAML Authentication
- Manage SAML Certificates for Service Providers
- VPN Certificates for User and Device Authentication
- Manage CA Certificates for VPN Connections

Introduces managing certificates. Certificates are used for various purposes in Secure Access, including: Decryption required for threat detection in traffic to private resources

Certificates are used for various purposes in Secure Access, including:

- Decryption required for threat detection in traffic to private resources
- Decryption required for threat detection in traffic to internet resources
- Presenting notification pages for blocked and warned internet destinations
- Establishing trust between Secure Access and your identity providers for SAML authentication. For more information, see Certificates for SAML Authentication.
- Authenticating users and devices in VPN connections. For more information, see VPN Certificates for User and Device Authentication.

Certificate Installation Methods

Certificate installation can be done on a per-browser or per-machine basis. For larger deployments, you can perform an automatic installation through Group Policy Objects (GPO). Note that the automatic installation through GPO is only supported for the Edge or Chrome browsers on Windows systems. As such, for Firefox or Safari browsers, and for users on non-Windows operating systems, you must perform the manual installation procedure.

You can also install a certificate automatically–through Active Directory Group Policy Objects–for a group of users in Microsoft Windows Active Directory. This automatic installation of a certificate is only supported for Edge or Chrome browsers on Windows systems. For all other browsers and systems, you must perform the manual installation procedure.

For more information, see Install the Cisco Secure Access Root Certificate.

Certificates for Internet Decryption

Describes certificates for internet decryption. Certificates are required for secure internet access. Specifically, certificates are required to decrypt traffic in order to inspect it for threats, and to present notifications to end users when access is blocked or triggers a warning.

Certificates are required for secure internet access. Specifically, certificates are required to decrypt traffic in order to inspect it for threats, and to present notifications to end users when access is blocked or triggers a warning. Web security features and the intrusion prevention (IPS) feature all require decryption in order to be effective.

End-user devices that connect to resources through Secure Access must trust the connection with Secure Access. You must set up certificates to establish this trust.

For internet traffic, depending on the features you need, there are two ways for end-user devices to validate the certificate that Secure Access presents to end-user devices that connect to internet resources through Secure Access:

1. You can install the self-signed Secure Access certificate into the browser trust stores of all end-user endpoint devices, or
2. You can sign the Secure Access certificate using your corporate certificate authority (CA) so that it can be validated by an existing certificate in the trust store of end-user devices. This method also allows you to easily revoke the certificate if needed, without having to update all end-user devices.

Certificates for Displaying Notifications

You can use only this method:

- Option 1: Distribute Self-Signed Certificates to End-User Devices

Certificates for Decrypting Internet Traffic

You can use either of these methods:

- Option 1: Distribute Self-Signed Certificates to End-User Devices
- Option 2: Use a Signed Certificate

Option 1: Distribute Self-Signed Certificates to End-User Devices

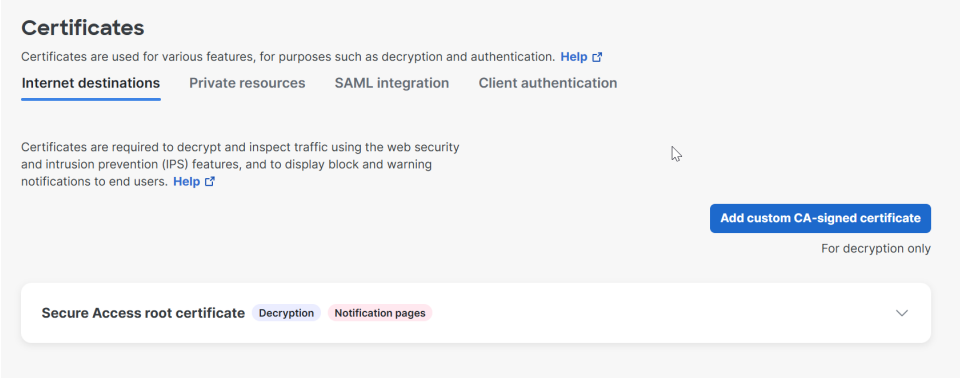
Provides instructions for option 1: distribute self-signed certificates to end-user devices. It also identifies related requirements, procedures, and operational considerations.

Before you begin

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

Procedure

1. Navigate to **Secure** > **Settings** > **Certificates** and click the **Internet destinations** tab.
2. Expand **Secure Access root certificate**.



3. Download the Secure Access certificate.
4. Install the downloaded certificate in the trust store of all devices in your organization.

   For more information, see Certificate Installation Methods.

   Identify the certificate

   The SHA1 hash of the file uniquely identifies the certificate file; you can use it to determine whether a file is this file, and whether the file has been modified from the original.

Option 2: Use a Signed Certificate for Decrypting Internet Traffic

Describes option 2: use a signed certificate for decrypting internet traffic. It also identifies related requirements, procedures, and operational considerations.

If your organization's managed devices already have the root certificate required to validate certificates signed by your corporate certificate authority (CA), you can sign the Secure Access certificate with your corporate CA, instead of installing the Secure Access self-signed certificate on every end-user device. This certificate cannot be used to display notifications. For more information, see Add Customer CA Signed Root Certificate.

Install the Cisco Secure Access Root Certificate

Describes installing the cisco secure access root certificate. A root certificate or your own Certificate Authority (CA) signed root certificate is required where Cisco Secure Access must proxy and decrypt HTTPS traffic that requests a web resource.

A root certificate or your own Certificate Authority (CA) signed root certificate is required where Cisco Secure Access must proxy and decrypt HTTPS traffic that requests a web resource.

The procedures on this page describe how to download and install the Cisco Secure Access root certificate. You can also use these procedures to install your own CA signed root certificate.

Download the Cisco Secure Access Root Certificate

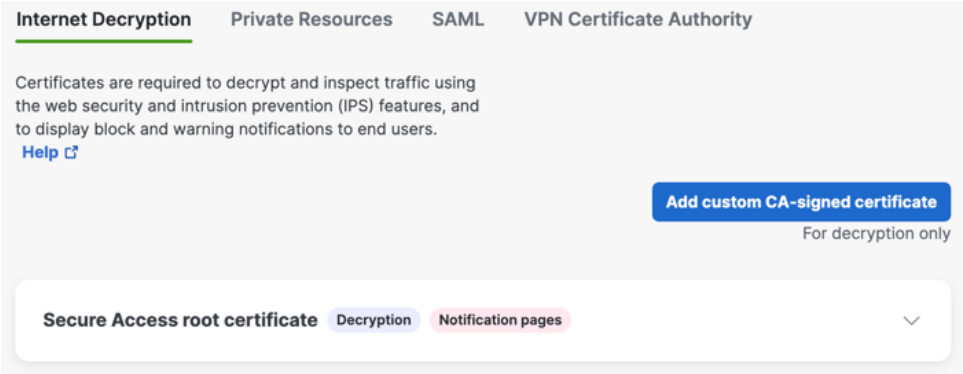
Provides instructions for downloading the cisco secure access root certificate. You must have administrative privileges on the devices in the organization or network administrative permissions over the network.

Before you begin

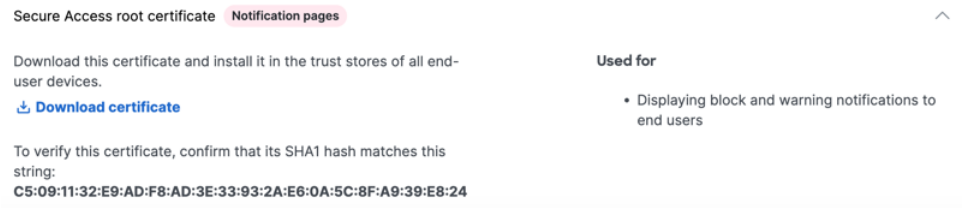
- You must have administrative privileges on the devices in the organization or network administrative permissions over the network.
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Certificates** > **Decryption**, and then expand **Secure Access root certificate**.



2. Click **Download certificate** to download the **Cisco_Secure_Access_Root_CA.cer** file.



Automatically Install the Cisco Secure Access Root Certificate (For an Active Directory Network)

Describes automatically install the cisco secure access root certificate (for an active directory network). Install the Cisco Secure Access Root Certificate with Group Policy Using the Microsoft Management Console (MMC)

As a network administrator of an Active Directory network environment, you can automatically install the Cisco Secure Access root certificate in all of your users' browsers by creating a Group Policy Object (GPO) on your Active Directory server. Create a GPO using either the Microsoft Management Console (MMC) or the Group Policy Management Console (GPMC).

- Install the Cisco Secure Access Root Certificate with Group Policy Using the Microsoft Management Console (MMC)
- Install the Cisco Secure Access Root Certificate with Group Policy Using the Group Policy Management Console (GPMC)

Install the Cisco Secure Access Root Certificate with Group Policy Using the Microsoft Management Console (MMC)

Provides instructions for installing the cisco secure access root certificate with group policy using the microsoft management console (mmc). Before you begin, download the Cisco Secure Access root certificate. See Prerequisites.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

1. Log into your Active Directory server using a domain administrator account.
2. Select **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**. The Microsoft Management Console (MMC) is displayed.

3. To create a domain-wide policy, right-click your domain root Organizational Unit (OU), which is displayed as your domain name, and select **Properties** from the context menu.
4. In the <*OU_Name*> Properties dialog box, click the **Group Policy** tab.
5. Click **New**, name the policy Secure Access Certificate Installer, and press **Return / Enter**.
6. Select the new Group Policy Object and click **Edit**. The Group Policy Object Editor is displayed.
7. In the configuration options sidebar, expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies**, right-click **Trusted Root Certification Authorities**, and select **Import**.
8. In the Certificate Import wizard, click **Next**, and in the File to Import page, click **Browse**. Navigate to where you downloaded the certificate authority on your local system, and double-click the **Cisco_Secure_Access_Root_CA.cer** file.
9. With the full path to the certificate displayed in the **File name** field, click **Next**.
10. Accept the default option, place all certificates in the following store (Trusted Root Certification Authorities), click **Next**, and then click **Finish** and **OK**.

What to do next

You have now created the Group Policy Object to install the Cisco Secure Access root certificate on all of the computers in your domain. The new policy may not take effect immediately on all client machines. By default, the background synchronization processing happens every 90 to 120 minutes at randomized times. Rebooting client machines forces the synchronization.

You can check that the Group Policy has propagated to all computers in the domain by opening your browser on a workstation, opening **Tools** > **Internet Options** > **Content** > **Certificates** > **Trusted Root Certification Authorities**, and ensuring that the Cisco Secure Access root certificate is present.

Install the Cisco Secure Access Root Certificate with Group Policy Using the Group Policy Management Console (GPMC)

Provides instructions for installing the cisco secure access root certificate with group policy using the group policy management console (gpmc).

The Microsoft Group Policy Management Console (GPMC) with Service Pack 1 (SP1) unifies the management of Group Policy across the enterprise. The GPMC consists of an MMC snap-in and a set of programmable interfaces for managing Group Policy.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

---

1. Log into your Active Directory server using a domain administrator account.
2. Select **Start** > **All Programs** > **Administrative Tools** > **Group Policy Management**. The Group Policy Management Console (GPMC) appears.
3. To create a domain-wide policy, right-click your domain root **Organizational Unit (OU)**, which is displayed as your domain name, and select **Create and Link a GPO Here** from the context menu.

   The New GPO dialog box appears.
4. In the **Name** field of the New GPO dialog box, enter a meaningful name for the policy object.
5. Right-click the new **Group Policy Object**, **Secure Access Certificate Installer**, on the right side of the window, and select **Edit** from the context menu. The Group Policy Object Editor appears.
6. In the left configuration options sidebar, expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**, right-click **Trusted Root Certification Authorities**, and select **Import** from the context menu.

7. In the Certificate Import wizard click **Next**, and in the File to Import page, click **Browse** and navigate to where you downloaded the certificate authority on your local system, and double-click the **Cisco_Secure_Access_Root_CA.cer** file.
8. With the full path to the certificate displayed in the **Filename** field, click **Next**.
9. Accept the default option, Place all certificates in the following store (Trusted Root Certification Authorities), click **Next**, then click **Finish** and **OK**.

What to do next

You have now created the Group Policy Object to install the Cisco Secure Access root certificate on all of the computers in your domain. The new policy may not take effect immediately on all client machines. By default, the background synchronization processing “only” happens every 90 to 120 minutes (at randomized times). Rebooting client machines forces the synchronization.

You can check that the Group Policy has propagated to all computers in the domain by opening your browser on a workstation, opening **Tools** > **Internet Options** > **Content** > **Certificates** > **Trusted Root Certification Authorities**, and ensuring that the Cisco Secure Access root certificate is present.

Install the Cisco Secure Access Root Certificate in Firefox Using Group Policy

Describes installing the cisco secure access root certificate in firefox using group policy. By default, Group Policy cannot configure Firefox. In general, deploying the Cisco Secure Access root certificate can be difficult in Firefox because there is no built-in way to centrally manage Firefox.

By default, Group Policy cannot configure Firefox. In general, deploying the Cisco Secure Access root certificate can be difficult in Firefox because there is no built-in way to centrally manage Firefox.

Install the Cisco Secure Access Root Certificate on Chromebooks Using the Google Admin Console

Describes installing the cisco secure access root certificate on chromebooks using the google admin console. Before you begin, download the Cisco Secure Access root certificate. See Prerequisites.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Using the Google Admin console, you can deploy certificates to your Chromebooks. For more information, see Google Support-Set Up Certificates.

Manually Install the Cisco Secure Access Root Certificate (Single Computer)

Describes manually install the cisco secure access root certificate (single computer). Install the Cisco Secure Access Root Certificate in Edge or Chrome on Windows

- Install the Cisco Secure Access Root Certificate in Edge or Chrome on Windows
- Install the Cisco Secure Access Root Certificate in Firefox on Windows
- Install the Cisco Secure Access Root Certificate in All Browsers on Mac OS X
- Install the Cisco Secure Access Root Certificate on Mac OS X Through the Command Line
- Install the Cisco Secure Access Root Certificate in Chromium or Chrome on Linux

Install the Cisco Secure Access Root Certificate in Edge or Chrome on Windows

Provides instructions for installing the cisco secure access root certificate in edge or chrome on windows. Before you begin, download the Cisco Secure Access root certificate. See Prerequisites.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

1. Click **Install Certificate**.
2. In the Certificate Import wizard, click **Next**.
3. In the Certificate Store window, select **Place all certificates in the following store** and then click **Browse**.
4. In the Select Certificate Store window, select **Trusted Root Certification Authorities** and click **OK**.

   In the Certificate Store window, the Certificate store shows **Trusted Root Certification Authorities**.
5. Click **Next** and then click **Finish**.
6. In the Security Warning windows, click **Yes** to install the certificate.

   If the certificate installed successfully, the Certificate Import wizard displays "The import was successful."
7. Click **OK**.
8. Restart the browser.

Install the Cisco Secure Access Root Certificate in Firefox on Windows

Provides instructions for installing the cisco secure access root certificate in firefox on windows. Before you begin, download the Cisco Secure Access root certificate. See Prerequisites.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

1. Click the **Open Menu** icon near the top right-hand corner of the browser window.
2. Click **Options** > **Advanced** > **Certificates** > **View Certificates** > **Authorities** > **Import**.
3. Browse for and select the Cisco Root Cert, downloaded in the first step.
4. Select **Trust this Certificate to identify websites**, then click **OK** and **OK** again.
5. Restart Firefox.

   To interact with the Firefox certificate store from the command line, use the **certutil** tool from the NSS Tools package. For more information, see Using the Certificate Database Tool.

Install the Cisco Secure Access Root Certificate in All Browsers on Mac OS X

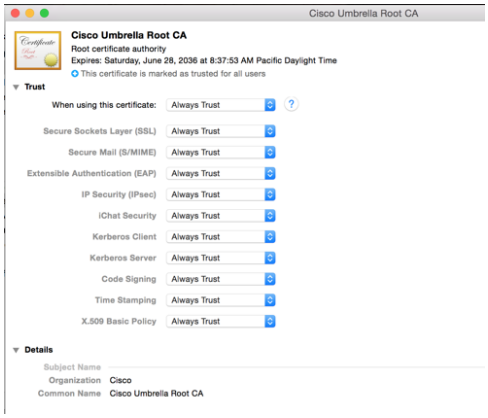
Provides instructions for installing the cisco secure access root certificate in all browsers on mac os x.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

1. Double-click the file or drag and drop it on top of the Keychain Access icon in the `Applications | Utilities` folder. The Add Certificate window appears.
2. Click **Always Trust**.

3. Double-click the Cisco Secure Access root certificate to open its properties window. From the **When using this certificate** drop-down menu, choose **Always Trust**.



Install the Cisco Secure Access Root Certificate on Mac OS X Through the Command Line

Provides instructions for installing the cisco secure access root certificate on mac os x through the command line. Before you begin, download the Cisco Secure Access root certificate. See Prerequisites.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

Run the following command:

```
sudo /usr/bin/security add-trusted-cert -d -r trustRoot -p ssl -p basic -k
/Library/Keychains/System.keychain /path/to/Cisco_Secure_Access_Root_CA.cer
```

Install the Cisco Secure Access Root Certificate in Chromium or Chrome on Linux

Provides instructions for installing the cisco secure access root certificate in chromium or chrome on linux. Before you begin, download the Cisco Secure Access root certificate. See Prerequisites.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

---

1. Open Chromium Settings.
2. Scroll down to **HTTPS/SSL**.
3. Click **Manage certificates**.
4. Click **Authorities**.
5. Click **Import**.
6. Select the **Cisco_Secure_Access_Root_CA.cer** file and click **Open**.
7. Select **Trust this CA to identify Websites**.
8. Click **OK**.

Add Custom CA Signed Root Certificate

Describes adding custom ca signed root certificate. You can use a certificate signed by your Certificate Authority (CA) to enable secure connections between user devices in your organization and Cisco Secure Access.

You can use a certificate signed by your Certificate Authority (CA) to enable secure connections between user devices in your organization and Cisco Secure Access.

A root certificate is required for Block Pages and Internet Decryption.

- For Block Pages, if you visit a blocked domain through HTTPS, a certificate must be installed so that Secure Access presents a block page rather than a browser error. For more information, see Manage Notification Pages.
- For HTTPS decryption and inspection, if a domain is proxied, install a certificate so that Secure Access can decrypt HTTPS traffic without the browser presenting an error. For more information, see Manage Traffic Decryption.

You can use either the Cisco Secure Access root certificate or your own CA-signed certificate. To use your own CA-signed certificate, upload a certificate signed by your CA to Secure Access.

Certificate Requirements

Describes certificate requirements. When you issue a certificate signed by your own CA, you must meet the following requirements: The encoding must use UTF8String.

When you issue a certificate signed by your own CA, you must meet the following requirements:

- The encoding must use UTF8String.
- You must use the same character encoding for all certificates in your certificate chain.
- The “Subject Name” in the CSR file downloaded from Secure Access must be honored.
  - The certificate must be valid for no more than three years.
  - The certificate must be an X509v3 certificate with an RSA public key not less than 2048 and no more than 4096.
- Use one of the following signature algorithms:
  - SHA256withRSA
  - SHA384withRSA
  - SHA512withRSA
- Include the following X509v3 extensions:
  - X509v3 Basic Constraints marked as critical: **CA:TRUE**
  - X509v3 Key Usage, marked as critical: **Certificate Sign**, **CRL Sign**

Install Root Certificate in Browsers

Provides instructions for installing root certificate in browsers. For information about how to install certificates in browsers, see Install the Cisco Secure Access Root Certificate.

Prerequisites

- A Certificate Signing Request (CSR) file downloaded from Secure Access.
- Microsoft Certificate Services, Active Directory Certificate Services, or OpenSSL to sign the CSR with your CA.

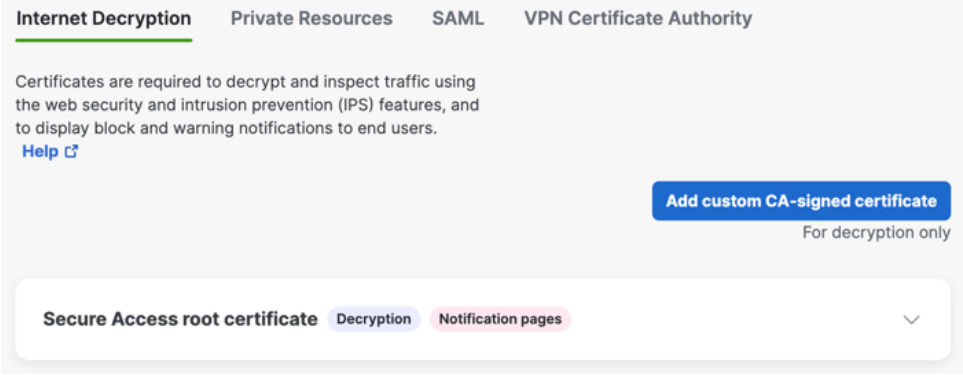
For information about how to install certificates in browsers, see Install the Cisco Secure Access Root Certificate.

Procedure

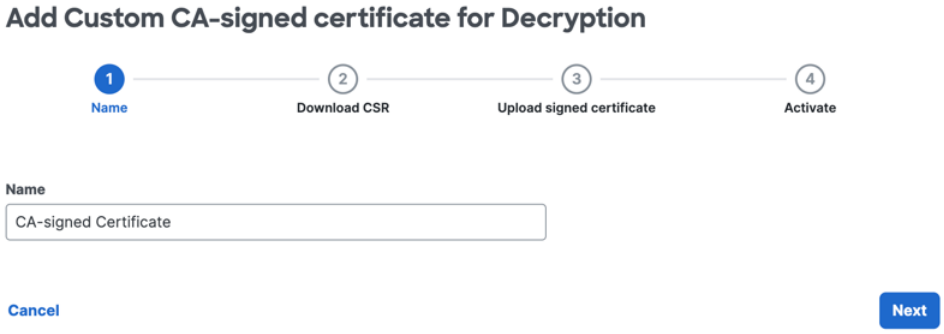
Provides instructions for adding a custom CA-signed certificate.

Procedure

1. Navigate to **Secure** > **Certificates** > **Internet Decryption**, and click **Add custom CA-signed certificate**.



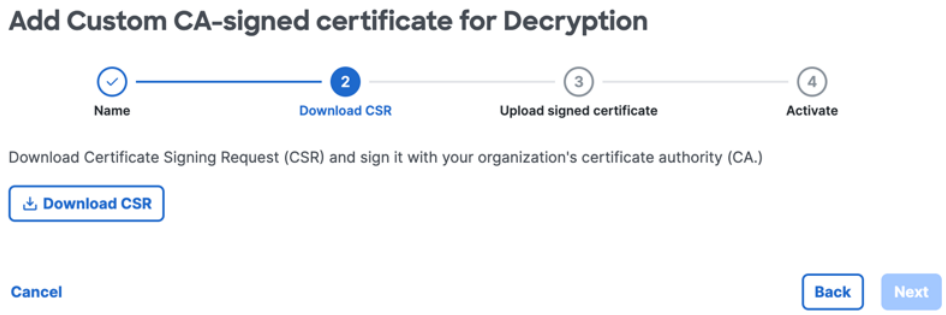
2. Enter a descriptive name for your certificate, and then click **Next**.



3. Click **Download CSR** to save the Secure Access Certificate Signing Request (.csr) file to the local system, and then click **Next**.

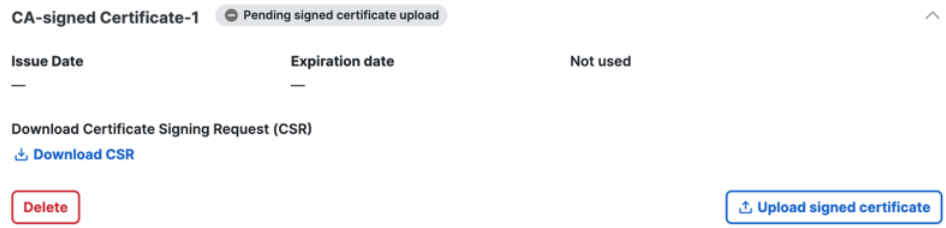
   Use a tool such as Microsoft Certificate Services or OpenSSL to sign the CSR with your corporate certificate signing authority (CA).

> **Note**
>
> You must download the Secure Access CSR file to complete the step.



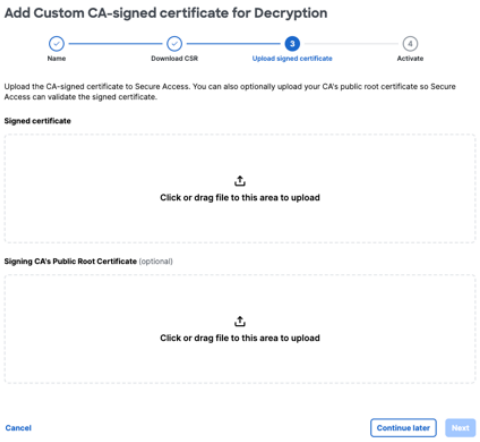
4. Sign the downloaded CSR file with your corporate certificate authority (CA).
5. Once you have signed the downloaded .csr file, click **Upload signed certificate**.

   Certificate status is `Pending signed certificate upload` until you upload your own CA signed root certificate.



6. Browse to the certificate that you have generated with the Secure Access CSR or drag the signed certificate file onto Secure Access, and then click **Next**.

   You can optionally also upload your signing certificate authority's public root certificate to Secure Access. This allows Secure Access to validate the signed certificate that you uploaded.



7. Confirm that end-user devices have the root certificate required to validate server certificates that are signed by your organization's CA. Managed devices typically already have the required certificate.
8. For **Activate**, click **Use for decryption** to activate the CA signed certificate in Secure Access, and then click **Start using for decryption**.

Manage Certificates for Private Resource Decryption

Describes managing certificates for private resource decryption. Secure Access's Intrusion Prevention System (IPS) can protect your private resources. Private resources are applications, networks, or subnets that are not publicly accessible from outside your network.

Secure Access's Intrusion Prevention System (IPS) can protect your private resources. Private resources are applications, networks, or subnets that are not publicly accessible from outside your network. Secure Access requires certificates in order to connect user traffic with your private resources and decrypt that traffic for inspection by the IPS. You can upload the hosting server's certificate for a resource when you configure the resource, or manage certificates from the certificate list. Endpoint devices must be able to validate the certificates that you upload.

Install a Certificate Authority Certificate on a Private Resource

Provides instructions for installing a certificate authority certificate on a private resource. Install your corporate Certificate Authority (CA) root certificate on the private resource in your organization. For information about installing certificates, see Install the Cisco Secure Access Root Certificate.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- A private resource added to Secure Access with decryption enabled to inspect traffic using the intrusion prevention (IPS) feature. For more information about private resources, see Manage Private Resources. For more information about IPS, see Manage IPS Profiles.

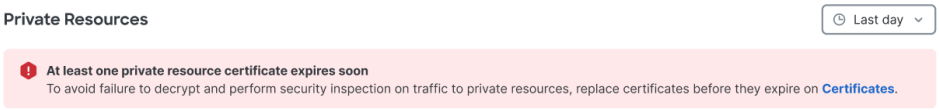
Procedure

Install your corporate Certificate Authority (CA) root certificate on the private resource in your organization. For information about installing certificates, see Install the Cisco Secure Access Root Certificate.

View Notifications About Expired Private Resource Certificates

Describes viewing notifications about expired private resource certificates. When a certificate for Private Resource Decryption has expired or will expire within 90 days, the Resources Private Resources page will display an expiry banner.

When a certificate for Private Resource Decryption has expired or will expire within 90 days, the **Resources** > **Private Resources** page will display an expiry banner:



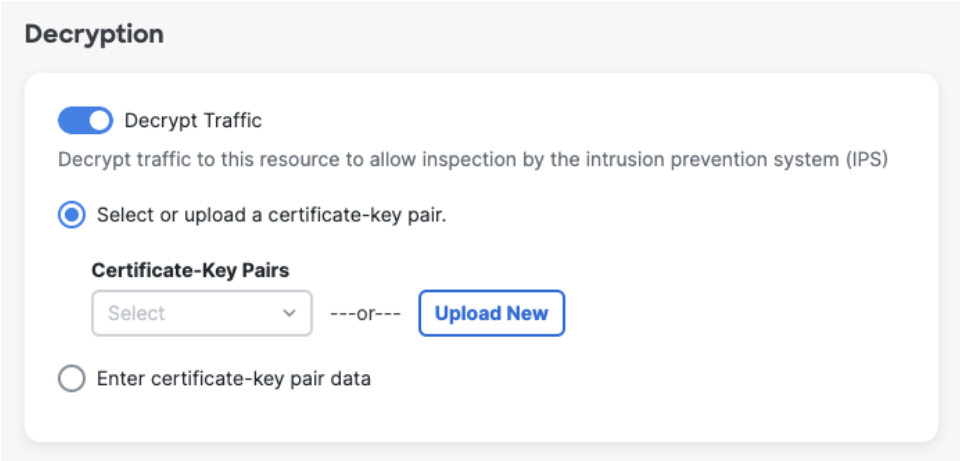
Users with the **Full Admin** or **Security Administrator** role can follow the **Certificates** link to update the certificate, or close the banner. If the certificate is not updated, a closed banner will reappear the next time the user opens the **Private Resources** page.

Option 1: Upload or enter a certificate-key pair directly to the private resource

Provides instructions for uploading or entering a certificate-key pair directly to a private resource, then saving the certificate settings in Cisco Secure Access.

Procedure

1. Navigate to **Resources** > **Private Resources**.
2. Click an existing private resource or add a new private resource.
3. Scroll down to **Decrypt**.
4. Once enabled, **Decrypt Traffic** displays certificate-key configuration options:



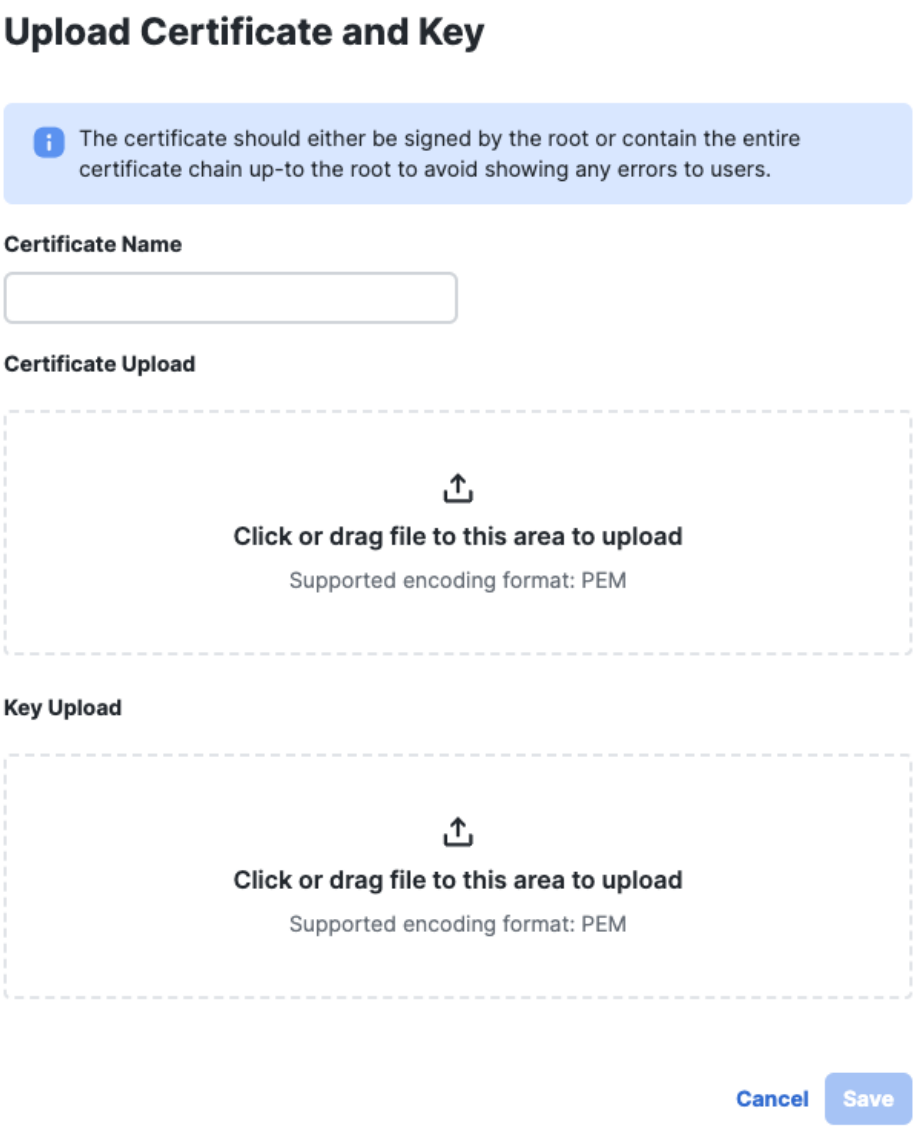
5. Select an existing certificate, upload a new certificate, or paste certificate values.
6. Click **Save**.

Option 2: Upload a certificate and key to the Certificates page

Provides instructions for option 2: upload a certificate and key to the certificates page. Navigate to Secure Certificates Private Resources.

Procedure

1. Navigate to **Secure** > **Certificates** > **Private Resources**.
2. Click **Upload Certificate and Key**.



3. Customize the certificate name, upload the hosting server's certificate and any intermediate certificates required to complete the chain, then click **Save**.
4. As in **Option 1** above, navigate to **Resources** > **Private Resources** to configure the private resource to use this certificate-key pair.

View the Cisco Trusted Root Store

Provides instructions for viewing the cisco trusted root store. A root certificate is required when Secure Access proxies and decrypts HTTPS traffic intended for a website. Cisco provides trusted root store bundles, which contain information about certificates used by Cisco products.

A root certificate is required when Secure Access proxies and decrypts HTTPS traffic intended for a website. Cisco provides trusted root store bundles, which contain information about certificates used by Cisco products. Within a bundle, you can view the list of trusted Cisco Certification Authorities (CA), type of root certificate, and certificate fingerprint (SHA-1).

The Secure Access trusted root certificate information is stored in the Cisco Trusted Union Root bundle. The Cisco Trusted Union Root bundle is a PKCS#7 bundle file (.p7b). The Cisco Trusted Union Root bundle is signed with a digital signing certificate, which you use to verify the bundle.

Download the Cisco Trusted Union Root Bundle

Provides instructions for downloading the cisco trusted union root bundle. You must have administrative privileges on the devices in the organization or network administrative permissions over the network. Use a version of OpenSSL v1.0 or greater to extract the root bundle.

Before you begin

- You must have administrative privileges on the devices in the organization or network administrative permissions over the network.
- Use a version of OpenSSL v1.0 or greater to extract the root bundle.

Procedure

1. Navigate to the Cisco Cryptographic Services site at Cisco PKI: Policies, Certificates, and Documents.
2. Under **Trusted Root Stores**, download the Cisco Trusted Union Root Bundle: https://www.cisco.com/security/pki/trs/ios_union.p7b.

Extract the Certificates

Describes extract the certificates. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Step 1: Extract the Signing Certificate

Provides instructions for step 1: extract the signing certificate. Extract the signing certificate from the Trusted Union Root bundle (ios_union.p7b) and save the signing certificate in a file named RootBundleSigningCertificate.cer.

Procedure

Extract the signing certificate from the Trusted Union Root bundle (**ios_union.p7b**) and save the signing certificate in a file named **RootBundleSigningCertificate.cer**.

```
openssl pkcs7 -in ios_union.p7b -inform DER -print_certs >
RootBundleSigningCertificate.cer
```

Step 2: Extract Certificate Bundle as Message

Describes step 2: extract certificate bundle as message. Use the extracted signing certificate (RootBundleSigningCertificate.cer) to verify the Trusted Union Root bundle (ios_union.p7b).

Use the extracted signing certificate (**RootBundleSigningCertificate.cer**) to verify the Trusted Union Root bundle (**ios_union.p7b**).

```
# This command extracts the certificate bundle as a message into the
#   file iosBundleBodyVerified.p7b if the signature verifies
openssl cms -verify -nointern -noverify -inform DER -in ios_union.p7b -outform
```

```
 DER \
  -out iosBundleBodyVerified.p7b -certfile RootBundleSigningCertificate.cer
```

The output is similar to:

```
Verification successful
```

Step 3: Extract PEM-Formatted Certificates From Bundle

Describes step 3: extract pem-formatted certificates from bundle. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

```
# This command extracts the certificates from the bundle into a separate
#   file, iosCerts.PEM, containing only the PEM-formatted certificates from
the bundle.
openssl pkcs7 -inform DER -print_certs -outform PEM < iosBundleBodyVerified.p7b
 \
  |grep -v 'subject=' |grep -v 'issuer=' |sed '/^$/d' > iosCerts.PEM
```

Step 4: Generate Individual Certificate Files

Describes step 4: generate individual certificate files. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Linux

```
# If you are on Linux, use this command to split the PEM bundle into individual
 certificate files
# (Does not work on a Mac due to GNU awk)
awk 'BEGIN {c=0;} /BEGIN CERT/{c++} {print > c ".pem"}' < ../iosCerts.PEM
```

macOS

```
# If you are on a Mac, use this command to split the PEM bundle into individual
 certificate files
# (Does not work on Linux due to split not supporting the -p flag)
split -p "-----BEGIN CERTIFICATE-----" iosCerts.PEM individual-
```

View an Individual Certificate File

Describes viewing an individual certificate file. Use openssl x509 to view the contents of an individual certificate file as plain text. Provide the name of the individual file as an argument to the openssl command.

Use `openssl x509` to view the contents of an individual certificate file as plain text. Provide the name of the individual file as an argument to the `openssl` command.

```
openssl x509 -in <individual-file> -text
```

Manage SAML Certificates for Identity Providers

Describes managing saml certificates for identity providers. To establish a trust relationship between Cisco Secure Access (service provider) and an integrated SAML identity provider (IdP), certificates are exchanged between Secure Access and the SAML IdP.

To establish a trust relationship between Cisco Secure Access (service provider) and an integrated SAML identity provider (IdP), certificates are exchanged between Secure Access and the SAML IdP. An administrator uploads the service provider's certificates from the Secure Access XML Metadata to the IdP platform's trust store. Then, an administrator imports the SAML IdP's XML Metadata that contains the IdP's certificates in to Secure Access.

After you integrate an SAML identity provider (IdP) in Secure Access, you can manage the identity provider's certificates. Secure Access displays notifications about certificates that may expire. When the IdP certificates expire, an administrator must import new IdP certificates (XML Metadata) in Secure Access to prevent connection disruptions.

Secure Access manages the expiration of IdP certificates for various connection methods and SAML IdP integrations. IdP certificates are used to establish the trust relationship between the service provider and the IdP. The IdP authenticates users that connect to Secure Access with:

- Zero Trust (ZT)
- Networks and network tunnels protected by Internet Security
- Virtual Private Networks (VPNs) with a configured VPN profile

Procedure

Provides instructions for procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- An integration of an SAML IdP with Secure Access. For more information, see Configure Integrations with SAML Identity Providers and Manage Virtual Private Networks.

Procedure

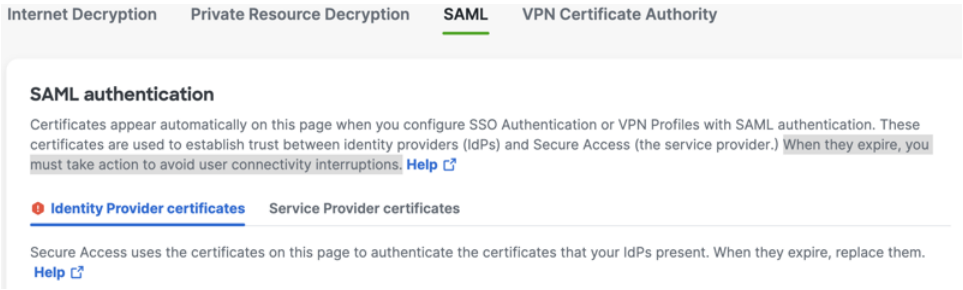
1. Manage IdP certificates integrated with Secure Access.
2. View notifications about the expiration of Secure Access certificates that are deployed in SAML IdP integrations and VPN Profiles.

View Notifications About Expired Identity Provider Certificates

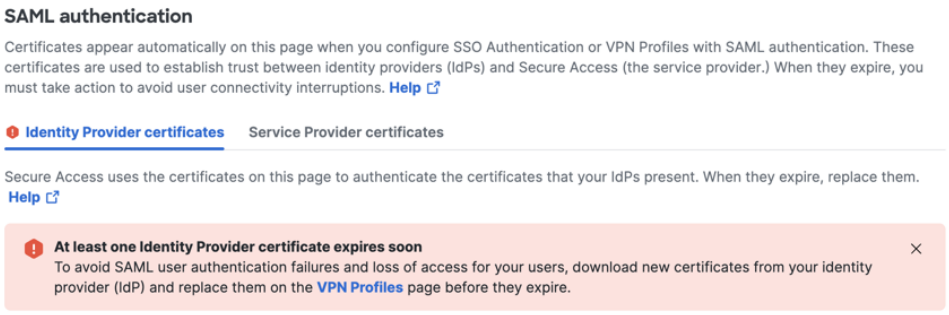
Provides instructions for viewing notifications about expired identity provider certificates.

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Integration** > **Identity Provider Certificates**.



2. Secure Access displays any notifications about expiring certificates.

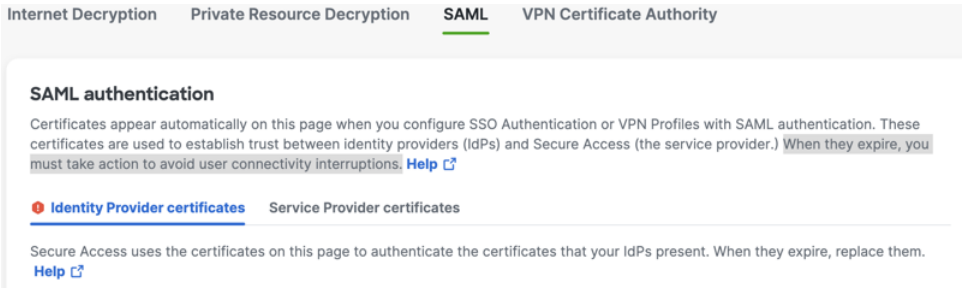


Manage Web Security and Zero Trust Identity Provider Certificates

Provides instructions for managing web security and zero trust identity provider certificates.

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Integration** > **Identity Provider Certificates**.



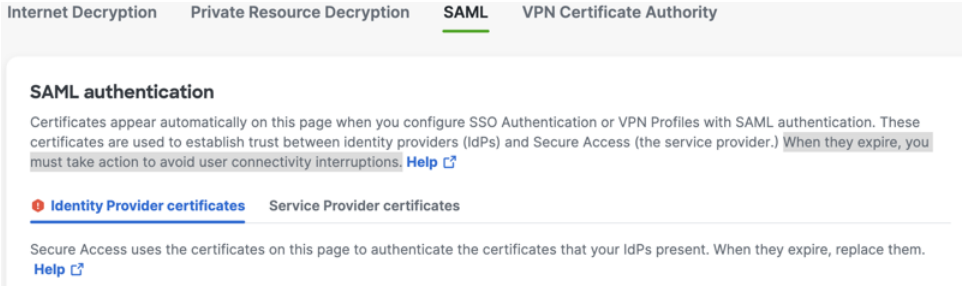
2. For **Web Security and Zero Trust SAML**, view the SAML IdP certificates integrated in Secure Access.
   - **Issuer**–The Certificate Authority that issued the certificate. Includes the common name (CN), organization unit (OU), and country of origin (C).
   - **Serial number**–The serial number of the certificate.
   - **Expiration date**–The date when the certificate is no longer valid.

Manage Virtual Private Network Identity Provider Certificates

Provides instructions for managing virtual private network identity provider certificates. Navigate to Secure Certificates SAML Integration Identity Provider Certificates .The SSE Cert View interface.

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Integration** > **Identity Provider Certificates**.



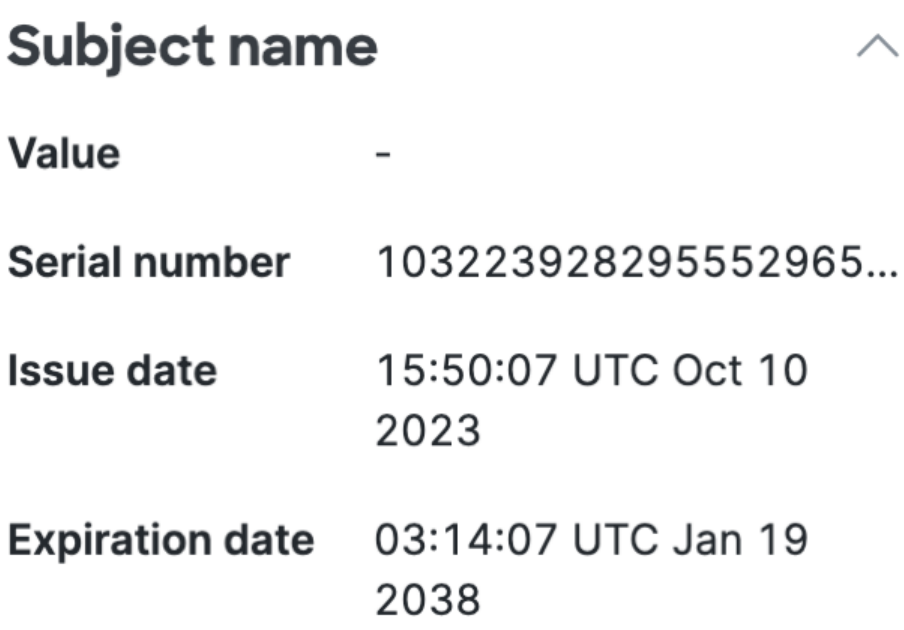
2. For **VPN SAML**, click on a certificate in the list to open the certificate details.

   The certificate is found in the VPN Profile.

   - **VPN Profile**–The name of the VPN profile.
   - **Issuer**–The Certificate Authority that issued the certificate. Includes the common name (CN), organization unit (OU), and country of origin (C).
   - **Serial number**–The serial number of the certificate.
   - **Expiration date**–The date when the certificate is no longer valid.

3. For **Subject name**, get the following certificate details:

   - **Value**
   - **Serial number**–The certificate's serial number.
   - **Issued date**–The date when the certificate was released.
   - **Expiration date**–The date when the certificate is no longer valid.

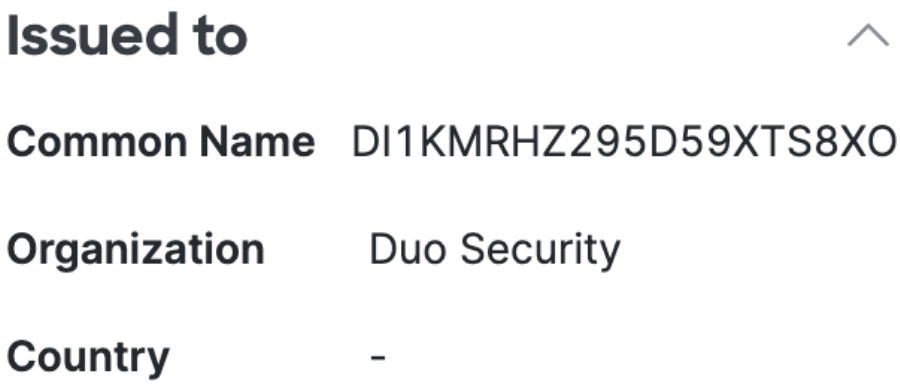


4. **Issued to** is the entity that uses the certificate to build a trust relationship with Secure Access.

   For **Issued to**, get the following certificate details:

   - **Common Name**–The fully-qualified domain name that is secured by the certificate.

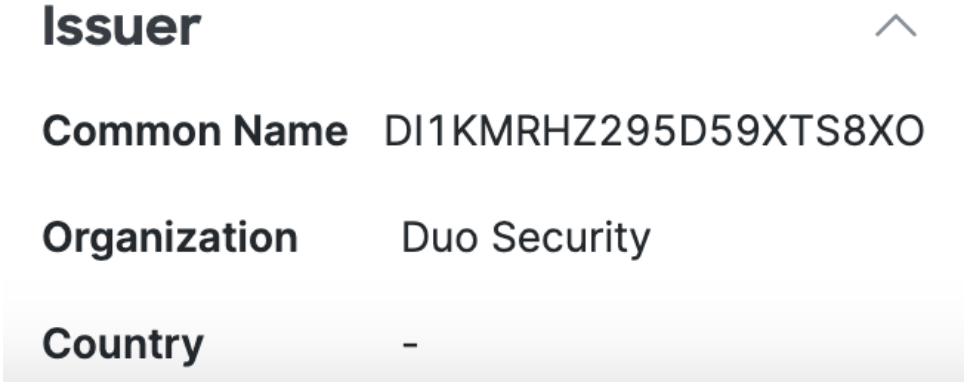
- **Organization**–The organization that is issued the certificate.
- **Country**–The country where the certificate was issued specified in the two-character country code.



5. **Issuer** is the entity (trusted authority) that issues the certificate.

   For **Issuer**, get the following certificate details:

   - **Common Name**–The fully-qualified domain name that is secured by the certificate.
   - **Organization**–The organization that issued the certificate.
   - **Country**–The country where the certificate was issued specified in the two-character country code.



Certificates for Private Resource Decryption

Describes certificates for private resource decryption. Certificates are required to decrypt traffic to private resources in order to inspect that traffic for threats.

Certificates are required to decrypt traffic to private resources in order to inspect that traffic for threats.

When you configure a private resource and enable decryption, you must upload the hosting server's certificate to Secure Access. Include any intermediate certificates required to complete the chain.

If multiple resources are hosted from a single server, you can use a single certificate for all of those resources.

Endpoint devices must be able to validate the certificates that you upload.

For more information about certificates for private resource decryption, see Manage Certificates for Private Resource Decryption.

Certificates for SAML Authentication

Describes certificates for saml authentication. Cisco Secure Access integrates with various Security Assertion Markup Language (SAML) identity providers (IdPs) that authenticate users.

Cisco Secure Access integrates with various Security Assertion Markup Language (SAML) identity providers (IdPs) that authenticate users. When a user requests a resource, Secure Access verifies the identity of the user through a trusted exchange with the integrated IdP and authorizes the user to get the resource. Users on devices must authenticate with Secure Access before connecting to private or web resources. The Secure Access services–Zero Trust (ZT), secure web gateway (SWG), and virtual private networks (VPNs)–must trust the connections from users and devices.

To set up a trust relationship between Secure Access (service provider) and an SAML IdP, an administrator imports the SAML IdP XML Metadata in to Secure Access, and then uploads the Secure Access XML Metadata to the SAML IdP's platform. The administrator adds the service provider's certificates to the IdP platform's trust store.

After you integrate an SAML IdP with Secure Access, you can manage the certificates in Secure Access for both the service provider (Secure Access) and your organization's IdPs. Secure Access lists a certificate's subject name, serial number, and expiration date and displays notifications about certificates that may expire.

- Manage SAML Certificates for Service Providers
- Manage SAML Certificates for Identity Providers

Manage SAML Certificates for Service Providers

Describes managing saml certificates for service providers. To establish a trust relationship between Cisco Secure Access (service provider) and an integrated SAML identity provider (IdP), certificates are exchanged between Secure Access and the SAML IdP.

To establish a trust relationship between Cisco Secure Access (service provider) and an integrated SAML identity provider (IdP), certificates are exchanged between Secure Access and the SAML IdP. An administrator uploads the service provider's certificates from the Secure Access XML Metadata to the IdP platform's trust store. Then, an administrator imports the SAML IdP's XML Metadata that contains the IdP's certificates in to Secure Access.

After you integrate an SAML identity provider (IdP) in Secure Access, you can manage the service provider's certificates. Secure Access displays notifications about certificates that may expire. When the service provider certificates expire, an administrator must upload new certificates from the Secure Access XML Metadata to the integrated SAML IdP platform's trust store to prevent connection disruptions.

Secure Access manages the expiration of service provider certificates for various connection methods and SAML IdP integrations. Service provider certificates are used to establish the trust relationship between the service provider and the IdP. The IdP authenticates users that connect to Secure Access with:

- Zero Trust (ZT)
- Networks and network tunnels protected by Internet Security
- Virtual Private Networks (VPNs) with a configured VPN profile

Procedure

Provides instructions for procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- An integration of an SAML IdP with Secure Access. For more information, see Configure Integrations with SAML Identity Providers and Manage Virtual Private Networks.

Procedure

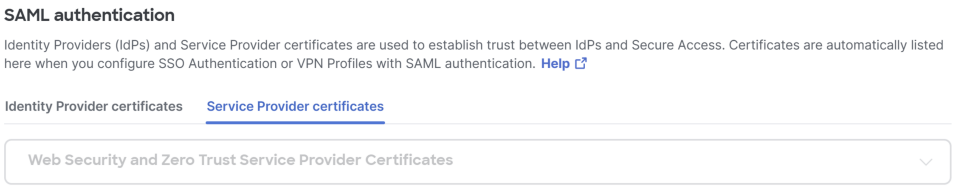
1. Download service provider certificates.
2. View notifications about the expiration of Secure Access certificates that are deployed in SAML IdP integrations and VPN Profiles.

View Notifications About Expired Service Provider Certificates

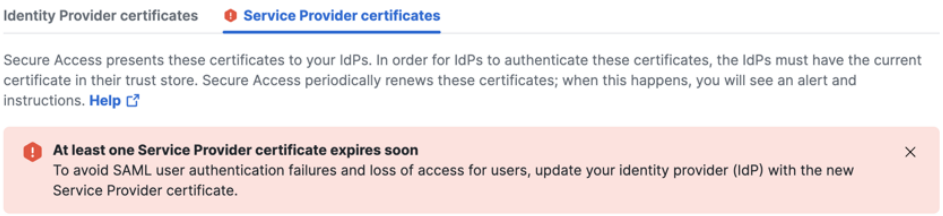
Provides instructions for viewing notifications about expired service provider certificates.

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Integration** > **Service Provider Certificates**.



2. Secure Access displays any notifications about certificates that may expire.

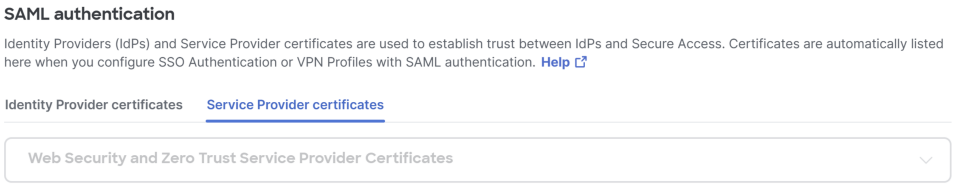


Download Web Security and Zero Trust Service Provider Certificates

Provides instructions for downloading web security and zero trust service provider certificates. Navigate to Secure Certificates SAML Integration Service Provider Certificates .The SAML Authentication interface.

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Integration** > **Service Provider Certificates**.



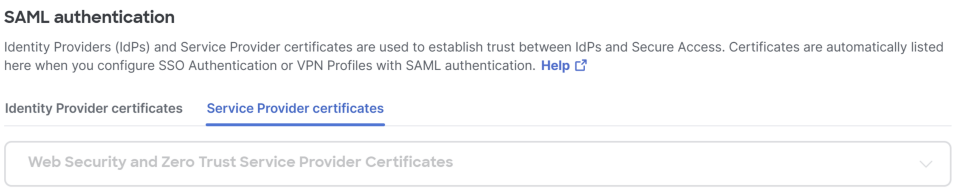
2. Upload a new Secure Access service provider certificate to the SAML IdP.
   a. For **Automatic Configuration**, copy the **Automatic Certificate Updates URL** and upload the Secure Access XML Metadata file to your SAML IdP.
   b. For **Manual Configuration**, in the list of certificates, click **download** on a certificate to save the certificate to your local system. Then, upload the certificate to the SAML IdP.
      - **Subject name**–The certificate's common name, which defines the entity that manages the certificate.
      - **Serial number**–The serial number of the certificate.
      - **Expiration date**–The date when the certificate is no longer valid.

Download Virtual Private Network Service Provider Certificates

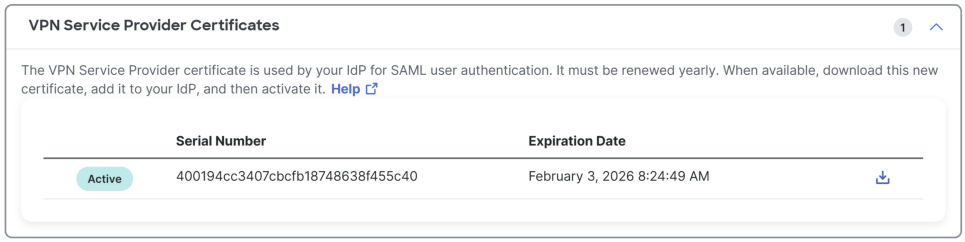
Provides instructions for downloading virtual private network service provider certificates. Navigate to Secure Certificates SAML Integration Service Provider Certificates.

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Integration** > **Service Provider Certificates**.



2. For **VPN Service Provider**, click **download** on a certificate in the list to save the certificate to your local system. Then, upload the certificate to the SAML IdP.
   - **Serial number**–The serial number of the certificate.
   - **Expiration date**–The date when the certificate is no longer valid.



VPN Certificates for User and Device Authentication

Describes vpn certificates for user and device authentication. Users that connect over virtual private networks (VPNs) to private resources are protected by Cisco Secure Access. The user devices must trust their network communications with Secure Access.

Users that connect over virtual private networks (VPNs) to private resources are protected by Cisco Secure Access. The user devices must trust their network communications with Secure Access.

To set up the trust between Secure Access and the user devices in the organization that connect over a VPN, install a certificate signed by your organization's Certificate Authority (CA) on all devices and upload your organization's signed CA root certificate to Secure Access. CA root certificates enable Secure Access to authenticate users and devices that connect over VPNs.

Once you upload signed CA certificates for VPN connections to Secure Access, you can view the details about the certificates, revoke a certificate, and delete a certificate. For more information about VPN Certificate Authority certificates, see Manage CA Certificates for VPN Connections.

Manage CA Certificates for VPN Connections

Describes managing ca certificates for vpn connections. Secure Access authenticates users and devices using the organization's Certificate Authority (CA) certificate.

Secure Access authenticates users and devices using the organization's Certificate Authority (CA) certificate.

Certificates described in this section are used when devices connect to networks using virtual private networks (VPNs).

- .

Install an Identity Certificate on User Devices

Provides instructions for installing an identity certificate on user devices. Full Admin user role. For more information, see Manage Accounts. Install on the user devices in your organization an identity certificate signed by your corporate Certificate Authority (CA) and validated by the certificate you will upload.

Before you begin

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

Procedure

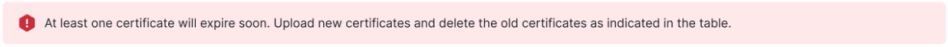
Install on the user devices in your organization an identity certificate signed by your corporate Certificate Authority (CA) and validated by the certificate you will upload.

View Notifications About Expired CA Certificates for Client Authentication

Provides instructions for viewing notifications about expired ca certificates for client authentication.

Procedure

1. Navigate to **Secure** > **Certificates** > **Client authentication**.
2. Secure Access displays a banner if a certificate has expired or will expire within 90 days:

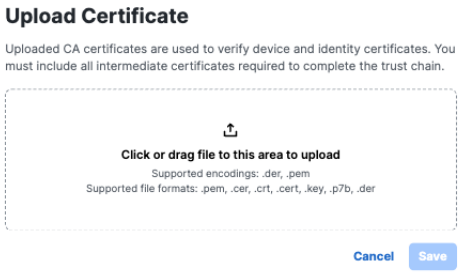


Upload Certificate Authority (CA) Certificates for client authentication

Provides instructions for uploading certificate authority (ca) certificates for client authentication. Navigate to Secure Certificates Client authentication . Click Upload certificate.

Procedure

1. Navigate to **Secure** > **Certificates** > **Client authentication**.
2. Click **Upload certificate**.



3. Upload your signed CA root certificate.
4. Select **VPN Authentication** as the purpose for the certificate.
5. (Optional) Configure certificate revocation settings.

   For details, see Manage Certificate Revocation Settings.

6. Click **Save**.

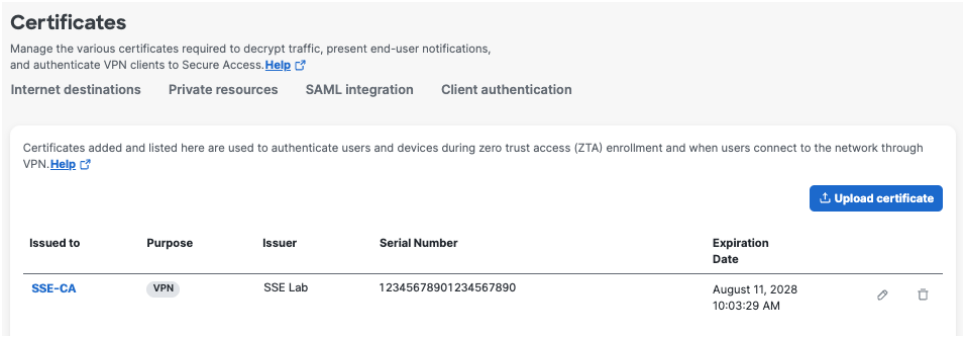
View Uploaded CA Certificates

Provides instructions for viewing uploaded ca certificates. Navigate to Secure Certificates Client authentication . Secure Access lists the certificates uploaded by your organization.

Procedure

Navigate to **Secure** > **Certificates** > **Client authentication**.

Secure Access lists the certificates uploaded by your organization.



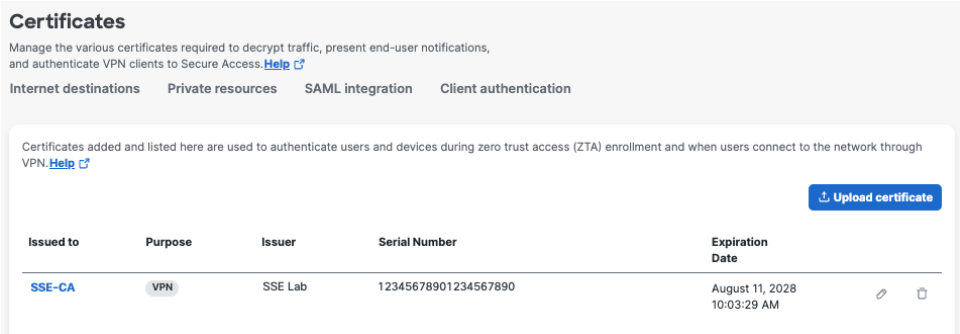
- **Issued to**–The name issued to the CA certificate.
- **Purpose**–Whether the certificate is used for VPN authentication or Zero Trust Access enrollment or both.
- **Issuer**–The CA that issued the certificate.
- **Serial Number**–The serial number of the certificate.
- **Expiration Date**–The date when the certificate is no longer valid.

Manage Certificate Revocation Settings

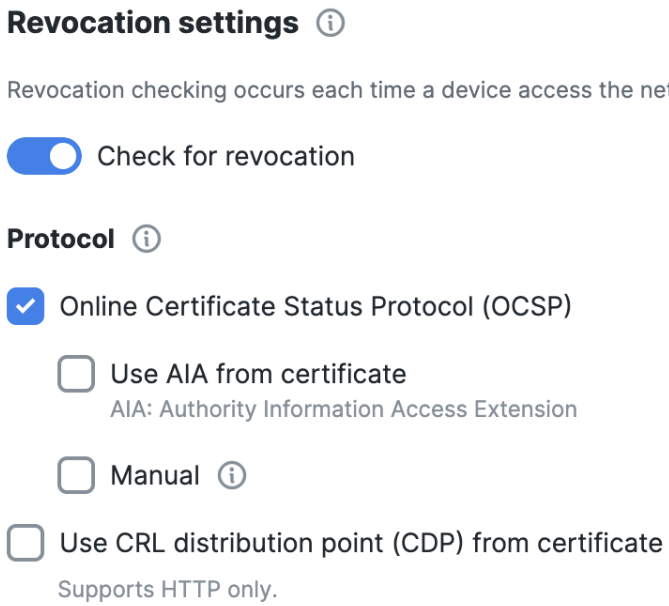
Provides instructions for managing certificate revocation settings.

Procedure

1. Navigate to **Secure** > **Certificates** > **Client authentication**.
2. Click the CA certificate name under the **Issued to** column to view the certificate details..



3. Under **Revocation settings**, enable **Check for revocation**. This is a crucial step to ensure the certificate is not revoked.
4. Choose the Protocol:
   a. Check the **Online Certificate Status Protocol (OCSP)** check box to use online certificate as the primary method for checking revocation status.
   b. **Use AIA from certificate**
   c. **Manual**
   d. Check the **Use CRL distribution point (CDP) from certificate** check box to check the Certificate Revocation List (CRL) distribution point in the certificate's CRL Distribution Points (CDP) extension to see if the certificate has been revoked.



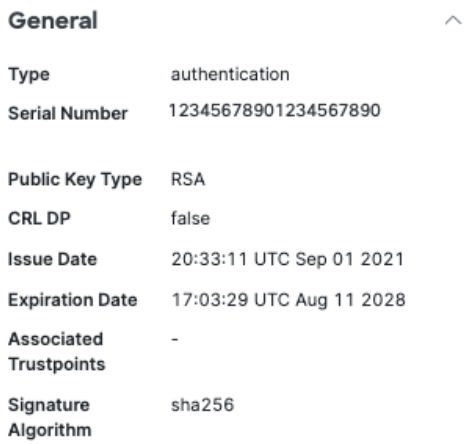
5. Click **Save**.

View CA Certificate Details

Provides instructions for viewing ca certificate details. Click a certificate name to view details. General certificate details: Type–The type of the certificate.

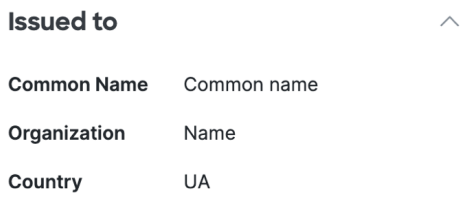
Procedure

1. Click a certificate name to view details.
2. **General** certificate details:
   - **Type**–The type of the certificate.
   - **Serial Number**–The serial number of the certificate
   - **Purpose** –Whether the certificate is used for VPN authentication or Zero Trust Access enrollment or both.
   - **Public Key Type**–The type of the public key.
   - **CRL DP**–Certificate Revocation List (CRL) Distribution Point. The location where you can check the revocation of the certifcate.
   - **Issue Date**–The date from which the certificate is valid.
   - **Expiration Date**–The date when the certificate is not valid.
   - **Associated Trustpoints**
   - **Signature Algorithm**–The cryptographic hash algorithm (Secure Hashing Algorithm 256).



3. **Issued to** certificate details.

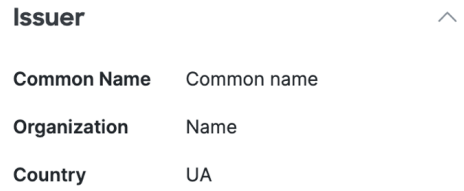
   The entity that uses the certificate to build a trust relationship with Secure Access.
   - **Common Name**–The fully-qualified domain name that is secured by the certificate.
   - **Organization**–The organization that is issued the certificate.
   - **Country**–The country where the certificate was issued specified in the two-character country code.



4. **Issuer** certificate details.

   The issuer is the entity (trusted authority) that issues the certificate.

   - **Common Name**–The fully-qualified domain name that is secured by the certificate.
   - **Organization**–The organization that issued the certificate.
   - **Country**–The country where the certificate was issued specified in the two-character country code.



Delete a Client Authentication CA Certificate

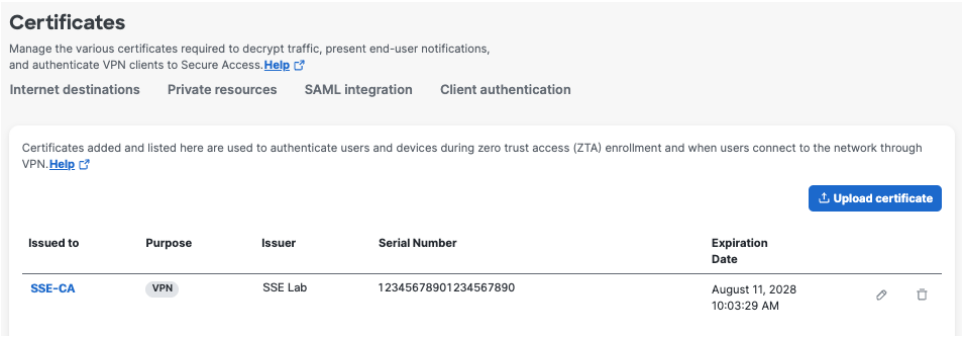
Provides instructions for deleting a client authentication ca certificate. Deleting a CA certificate has different effects depending on the configured purpose of the certificate:

Deleting a CA certificate has different effects depending on the configured purpose of the certificate:

- Deleting a CA certificate used for VPN authentication immediately prevents access.
- Deleting a CA certificate used for Zero Trust Access enrollment prevents new enrollments and enrollment renewals authenticated by that certificate, but does not terminate existing connections or immediately prevent further access. See Unenroll a Device from Zero Trust Access.

Procedure

1. Navigate to **Secure** > **Certificates** > **Client authentication**.



2. To remove a certificate, follow the steps in one of the options:

   a. Click on a certificate **Issued to** link to open the certificate details, and then click **Delete**. Click **Delete** again to confirm the removal of the certificate.

b. Click on the delete icon to **Delete**. Click **Delete** again to confirm the removal of the certificate.

Expired Certificates

Describes expired certificates. For certificates used for Zero Trust Access enrollment: If a CA certificate expires and you replace it, you must re-generate the configuration file and distribute it to all user devices that use Zero Trust Access.

For certificates used for Zero Trust Access enrollment: If a CA certificate expires and you replace it, you must re-generate the configuration file and distribute it to all user devices that use Zero Trust Access.

42 Manage the Data Loss Prevention Policy

Topics:

- Add a Real Time Rule to the Data Loss Prevention Policy
- Understand Exclusions in a Real Time Rule
- Supported Applications
- Add a SaaS API Rule to the Data Loss Prevention Policy
- Discovery Scan
- Edit a Data Loss Prevention Rule
- Delete a Data Loss Prevention Rule
- Enable or Disable a Data Loss Prevention Rule
- Supported File and Form Types
- Best Practices for the Data Loss Protection Policy

Introduces managing the data loss prevention policy. Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Current Package.

> **Note**
>
> Secure Access Packages and Feature Availability
>
> Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Current Package. If you encounter a feature here that you do not have access to, contact your sales representative for more information about your current package. For more information, click Cisco Secure Access Packages.

The Data Loss Prevention (DLP) policy helps to protect sensitive data uploaded to the web. It discovers and protects sensitive data stored and shared in your cloud-sanctioned applications.

The DLP policy can be configured with multiple DLP rules; **Real Time** DLP rules inspect the web traffic traversing the proxy and **SaaS API-based** rules ensure data protection of data in the cloud. Furthermore, DLP Administrators can initiate on-demand Discovery Scans to learn about all the files in the applicable cloud applications that contain matches with the selected Data Classifications.

1. Real Time Rules: are added to the policy to define what web proxy traffic to monitor (identities and destinations), the content or document properties to search for, and whether content should be monitored or blocked. For example, an office may want to monitor its network for file uploads that include credit card numbers, as the uploads are a breach of the company's privacy and security policies. A Real Time DLP rule designed to monitor the network and uploads to domains can block these files.
2. SaaS API Rules: operate by leveraging the APIs of the applicable cloud tenants to scan and look for data violations in the cloud-stored files. As files in the selected tenant change in content or context (with whom we share), Secure Access near-time assesses the changed file against this rule's criteria. If a match is made, this rule's action is immediately enforced.

Data violations detected through the Real Time and SaaS API rules are logged as part of the unified Events view of the Data Loss Prevention Report.

Discovery Scans operate similarly to the SaaS API rules; they exercise the necessary cloud APIs to determine the files in the applicable cloud tenant that contain data matching any of the configured Data Classifications at the time the scan runs. Files containing matching data are considered to be in violation of the Discovery Scan.

The Discovery tab in the Data Loss Prevention Report lists the files in violation of the most recently initiated Discovery Scan. Additionally, DLP Administrators can

quickly retrieve the reported offending files from any of the last 10 generated Discovery Scans.

Realtime DLP rules support scanning traffic isolated by the RBI (Remote Browser Isolation) in the outbound direction, in addition to scanning non-isolated HTTPs traffic. When the system detects a DLP violation in RBI traffic, a pop-up dialog will appear in the user's browser to warn of a potential data security violation.

Real Time rules, SaaS API rules, and Discovery Scans all support scanning embedded files.

Limitations

1. The rate limit is dependent on vendor SLA, which is usually up to 10 RPS for Microsoft 365 and up to 20 RPS for Google Drive.
    - The Discovery Scan can scan up to 36,000 files per hour and 864,000 files per day with an average file size of 1MB.
    - The incremental scan and Discovery Scan share the same rate limits, therefore, file changes (i.e. incremental) during the Discovery Scan are counted and have an effect on the Discovery Scan throughput.
    - An org that triggers more than 864k events per day will be at risk of not having all their events scanned.
2. Triggering a Discovery Scan should take place around 24 hours after the tenant authorization, as the system needs time to evaluate and enumerate the users in the organization. Any triggering beforehand might not include all users and hence, the system is unable to scan all files.
3. The DLP scans the plain text of files up to 50 MB.
4. DLP scans archives as well as files containing embedded files. For these, DLP can extract and scan content for up to 100 files nested up to 10 levels deep.
5. Revoke share for internal or external works only for organizations with one domain in Google Drive due to Google API limitation.

Add a Real Time Rule to the Data Loss Prevention Policy

Provides instructions for adding a real time rule to the data loss prevention policy. There is only one data loss prevention policy.

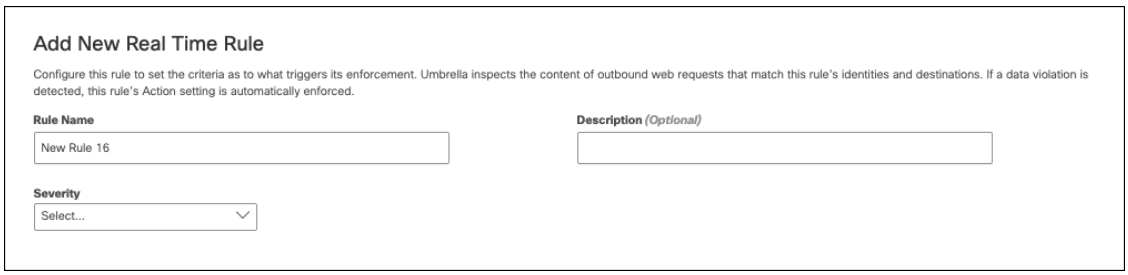
There is only one data loss prevention policy. Rules are added to the policy to define what traffic to monitor (resources and destinations), the data classifications that require monitoring, and whether content should be blocked or only monitored.

Before you begin

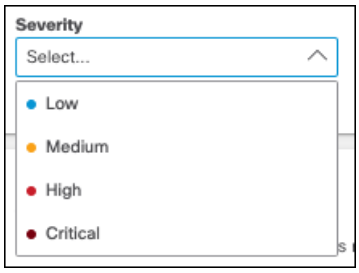
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**, click **Add Rule**, and choose **Real Time Rule**.
2. Under **Add New Real Time Rule**, give your rule a meaningful name and description.



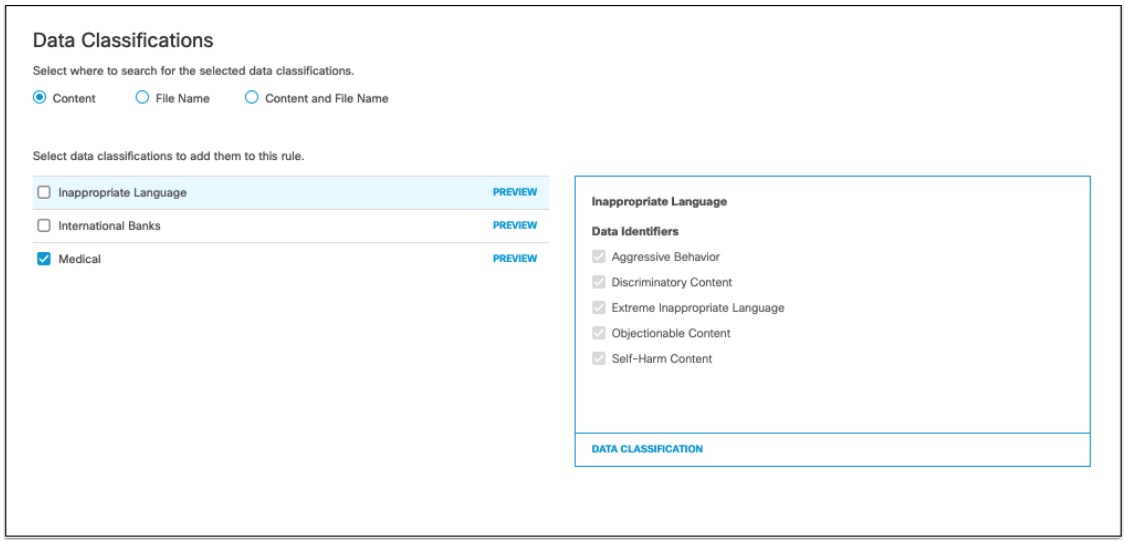
3. Choose a severity for your rule based on the risk involved or importance within the ruleset.



4. Choose where you would like this rule to search for these data classifications.
   - **Content**–(Default) Searches only the content of files for the selected data classifications.
   - **File Name**–Searches only file names for the selected data classifications.
   - **Content and File Name**–Searches content and file names for the selected data classifications. Both content and file name do not need to match for the rule to apply, only one or the other.

> **Note**
>
> Choosing **Content**, **File Name**, or **Content and File Name** refers to scanning file uploads for the selected data classifications and configured file labels.

5. Select classifications to apply this rule. For more information, see manage data classifications.



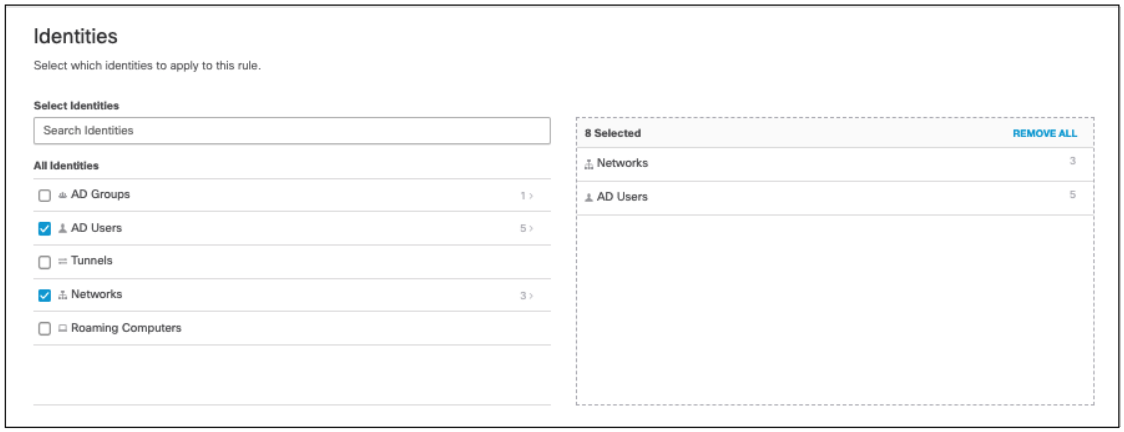
6. Add up to 10 case-sensitive file label names to apply to this rule. The rule will search for any of the configured file label names in the value of the files' document properties. This includes Microsoft Office Document Properties, Microsoft Office Sensitivity Labels, and Adobe PDF Document Properties. File uploads to Confluence and Jira are not scanned for file labels.

> **Note**
>
> A DLP rule can be configured with either data classifications or file labels or both. When a DLP rule is configured with both, then a DLP event is raised when any of the selected data classifications and when any of the configured file labels are detected in the inspected file.



> **Note**
>
> Microsoft Sensitivity Labels
>
> Secure Access currently supports detection of Microsoft sensitivity labels in the file properties' values of the inspected file for Microsoft Word, Excel, PowerPoint, and .pdf files. Ensure you configure the rule with the name of the sensitivity labels, not the Display Names.

7. Select identities to apply to this rule.

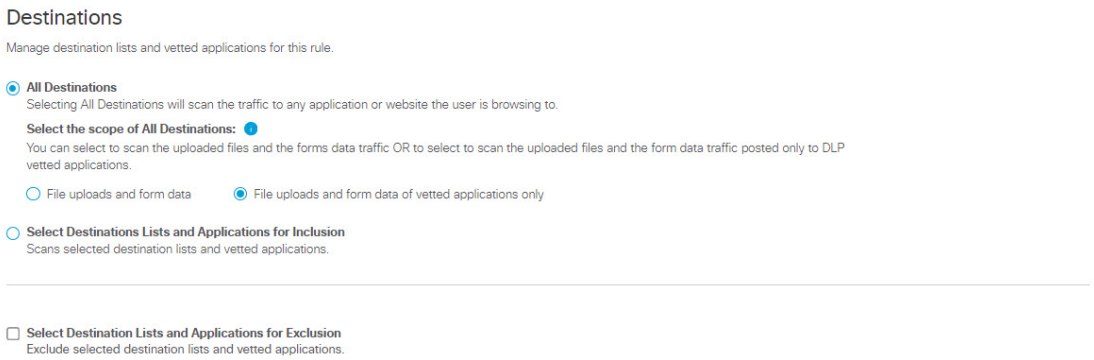


8. Under **Destinations**, select **All Destinations** or **Select Destination Lists and Applications for Inclusion**.
   - **All Destinations**–Monitors all outbound web requests or blocks all file uploads that originate from the selected identities for this rule.

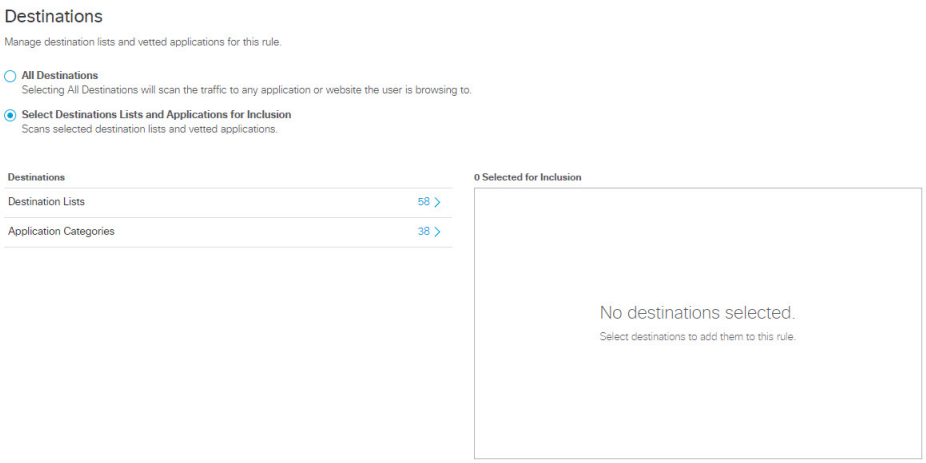
     When **All Destinations** is selected, you can select the type of data Secure Access monitors:
     - Choose **File uploads and form data** to monitor all uploaded files and forms data for all web destinations users visit.

       > **Note**
       >
       > Use care when choosing **All Destinations File uploads and form data** because it significantly widens the scope of the data the rule scans and can result in excessive false positives, blocking users' access to many sites inappropriately. We recommend that rules applied to all destinations not include built-in identifiers with lenient tolerances or custom identifiers with regexes that define a broad scope. Design regexes to narrowly identify the data you seek, and include threshold and proximity criteria.

     - Choose **File uploads and form data of vetted applications only** to monitor all uploaded files and forms data associated only with DLP Supported Applications.

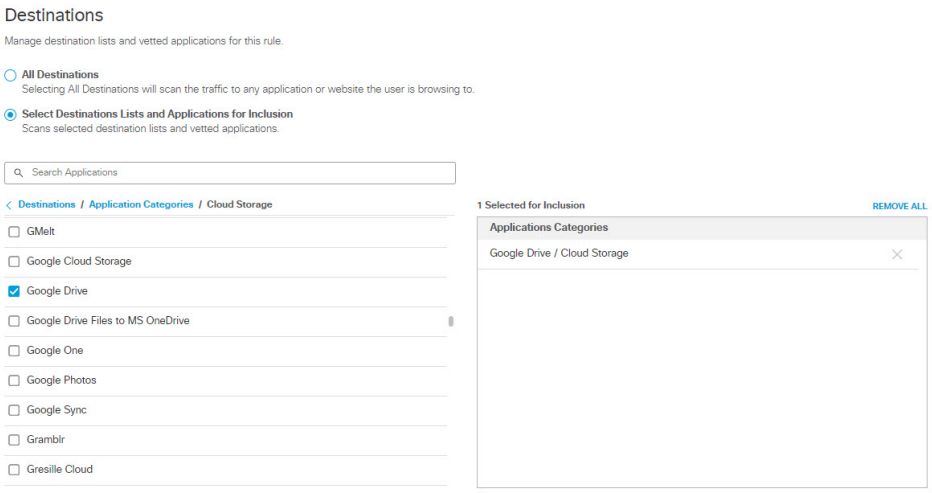


- **Select Destination Lists and Applications for Inclusion**–Monitors all web requests and blocks all file uploads matching the identities selected on the rule, the selected destination lists, and supported applications.

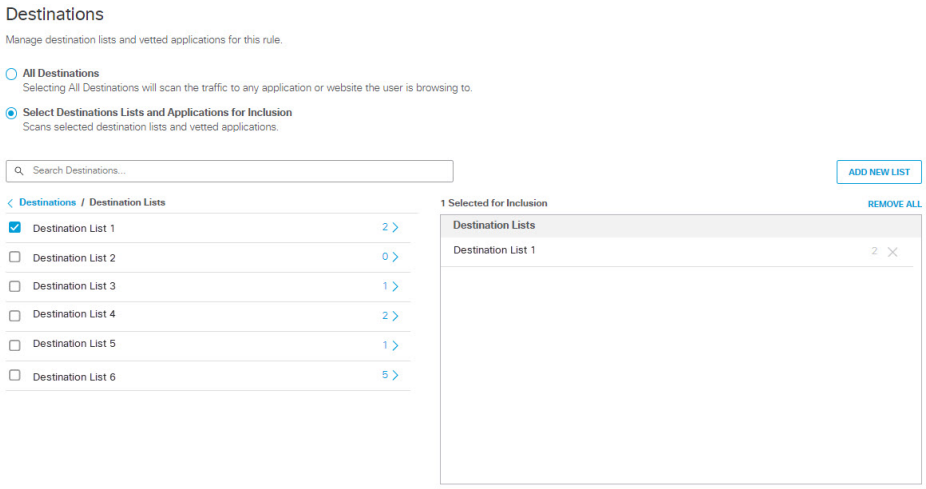


  - To add applications for inclusion, under **Destinations** expand **Application Categories**. (See Application Categories) for a list of available categories.) Expand categories and check the boxes for the applications you want to add to the rule. You can search for an application by entering at least three consecutive letters from the application name in the search box.

> **Note**
>
> It is not possible to search for an application with fewer than three letters in its name–for example, "QQ" or "YY." These applications must be manually selected from the hierarchy under their respective categories, or wildcarded in search–for example, "QQ*". This behavior is by design.

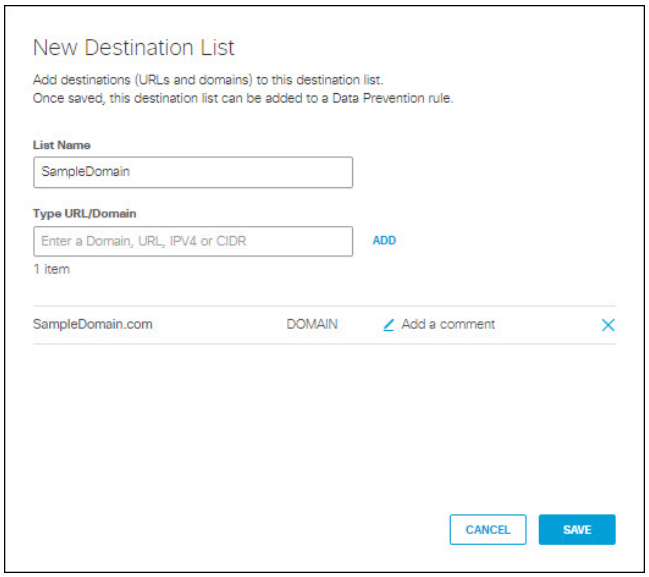


- To add destination lists for inclusion, under **Destinations** expand **Destination Lists** and check the boxes for the destination lists you want to add to the rule.

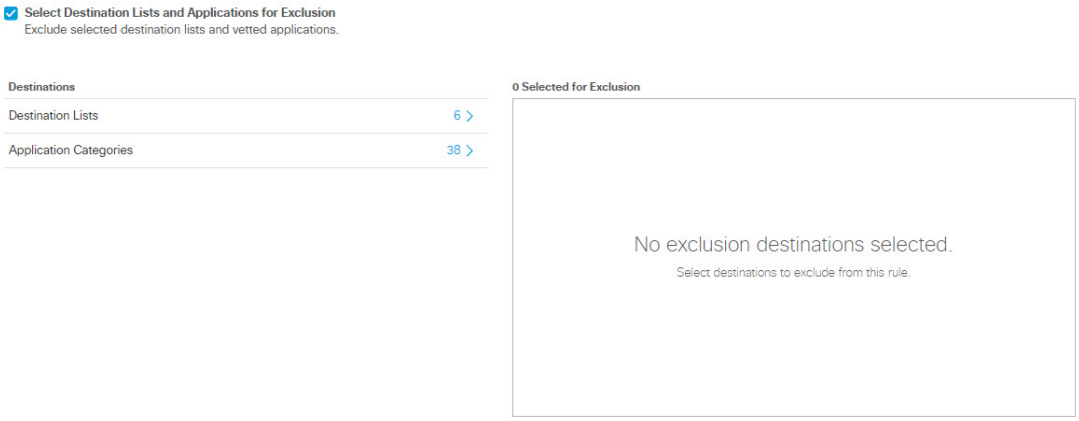


- To create a new destination list and add it for inclusion, under **Destinations** expand **Destination Lists** and click **ADD NEW LIST.** Under **List Name** enter a unique name for the list. For each URL/Domain to be in the list, enter a domain name, URL, IPV4 address or CIDR, and click **Add**. Click **Save** when done.

> **Note**
>
> Adding a new destination list to the rule here automatically adds it for inclusion.

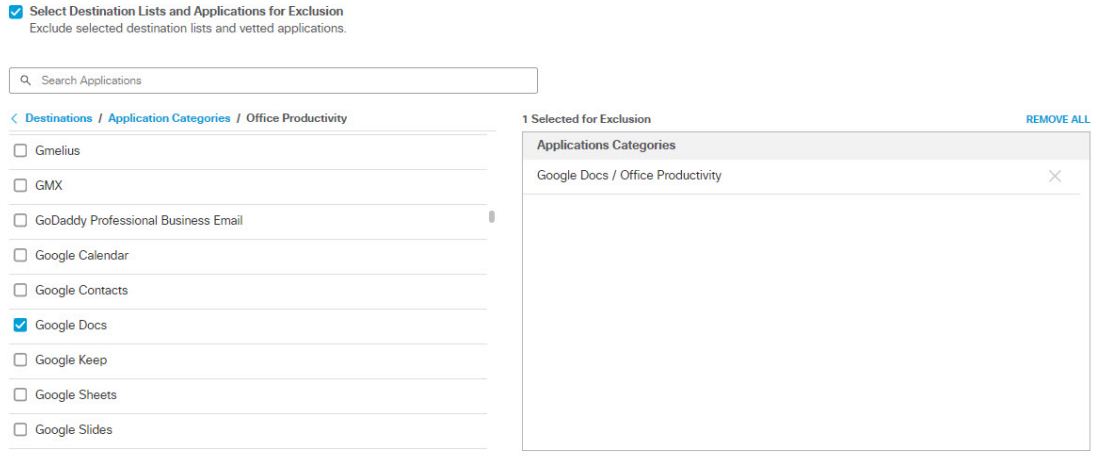


9. Check the checkbox **Select Destination Lists and Applications for Exclusion** to select destinations and applications to exclude from this rule.

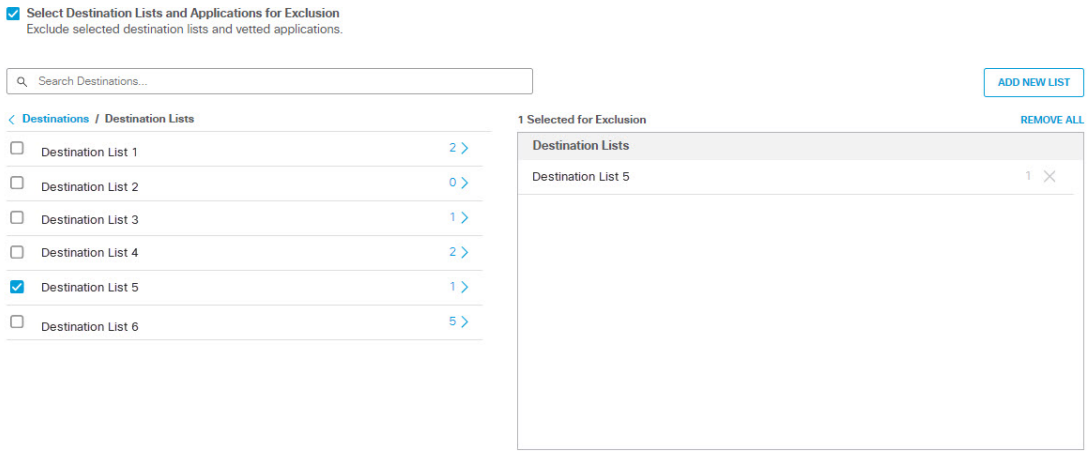


- To exclude applications, under **Destinations** expand **Application Categories**. (See Application Categories) for a list of available categories.) Expand categories and check the boxes for the applications you want to exclude from the rule. You can search for an application by entering at least three consecutive letters from the application name in the search box.

> **Note**
>
> It is not possible to search for an application with fewer than three letters in its name–for example, "QQ" or "YY." These applications must be manually selected from the hierarchy under their respective categories, or wildcarded in search–for example, "QQ*". This behavior is by design.

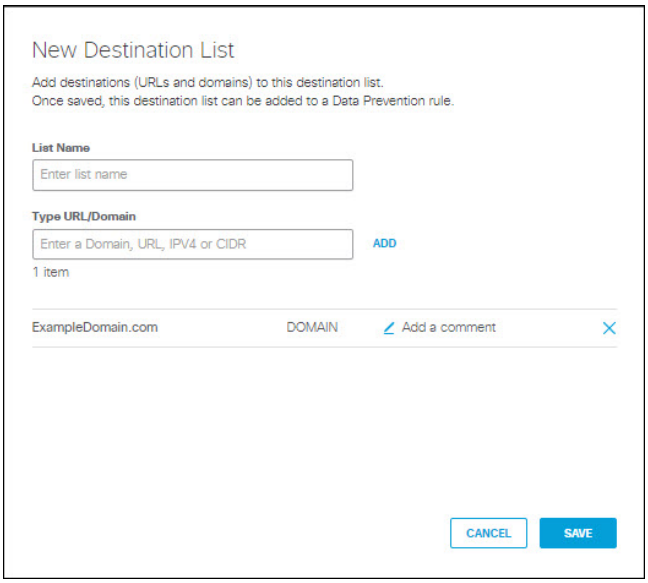


- To exclude destination lists, under **Destinations** expand **Destination Lists** and check the boxes for the destination lists you want to exclude from the rule.

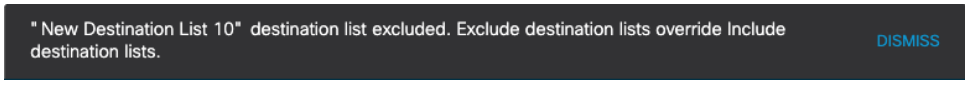


- To create a new destination list and exclude it, under **Destinations** expand **Destination Lists** and click **ADD NEW LIST.** Under **List Name** enter a unique name for the list. For each URL/Domain to be in the list, enter a domain name, URL, IPV4 address or CIDR, and click **Add**. Click **Save** when done.

> **Note**
>
> Adding a new destination list to the rule here automatically adds it for exclusion.



> **Note**
>
> When a destination list is selected for both inclusion and exclusion in a rule, it will automatically be excluded. Exclusion destination lists always override inclusion destination lists. Similarly, if a domain is included on an inclusion destination list and an exclusion destination list, the domain will be excluded.



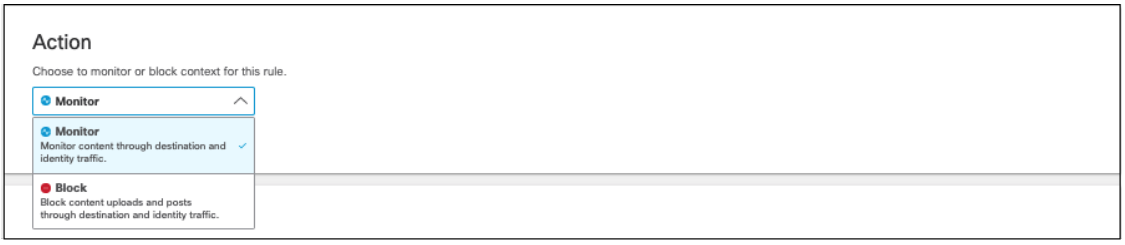
10. Under **Action**, from the drop-down list, choose **Monitor** or **Block**.

- **Monitor**–Monitor file uploads and data submitted in web forms.

  The rule will search for content that matches supported workflows (See Supported Applications) and policy-configured destinations and identities.

- **Block**–Block file uploads.

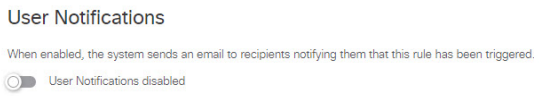
  The rule will search for content that matches supported workflows (See Supported Applications) and the policy-configured destinations and identities. When content matches these workflows, the rule blocks the content.



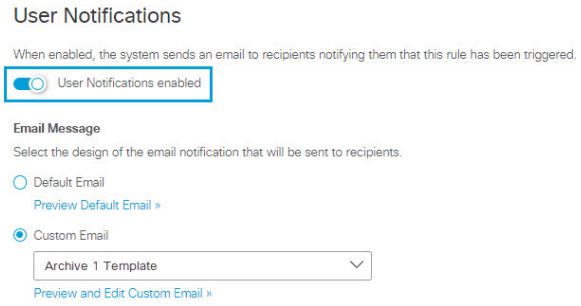
> **Note**
>
> Limited Availability
>
> Secure Access can optionally block all password-protected files directed to destinations configured in the DLP rules. If enabled, this feature impacts all file types and all users and cannot be configured for finer granularity. This feature is not generally available; contact Secure Access Support to have it enabled in your account.

11. Under **User Notifications** you can enable and configure an email notification to be sent to a user who performs an action that triggers a violation of the rule. You can use a default email template provided by the system, or create your own custom template.

> **Note**
>
> The system gets the "send to" address for the email from UPN field in the authenticated active directory. Some identity configurations may not be able to provide the end user's email address, in which case the system will be unable to send the email. These cases include:
>
> - The user uses network or tunnel identities, in which case the user's IP address will be available to the system, but not the email address.
> - The user did not authenticate through active directory, so the system has no information about the user.
> - The user's email address is not stored in the UPN field in the authenticated active directory.



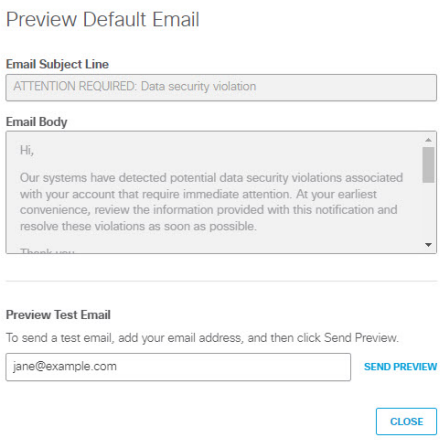
a. Enable user notifications.



b. Choose the email template:

To Use the Default Email Template:

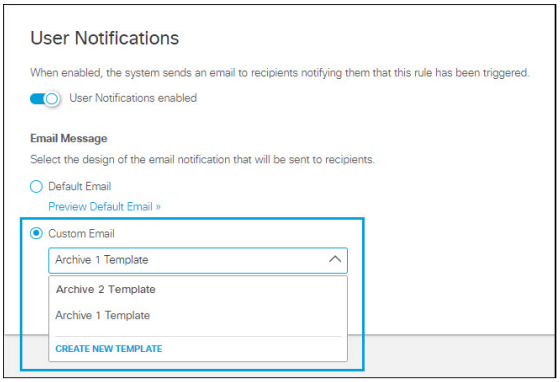
1. Click **Default Email**.
2. To preview the content of the email that will be send to users, click on **Preview Default Email**. You can review the email subject line and text, but you cannot change it.

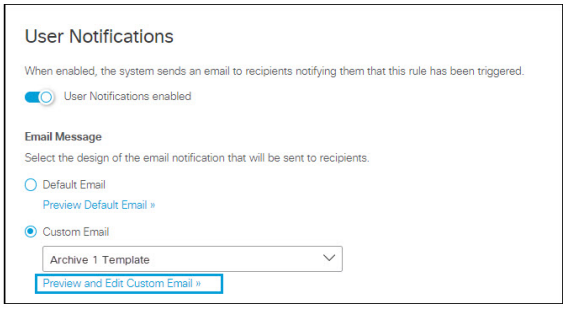


3. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)
4. Click **CLOSE** to return to the Data Loss Prevention Policy page.

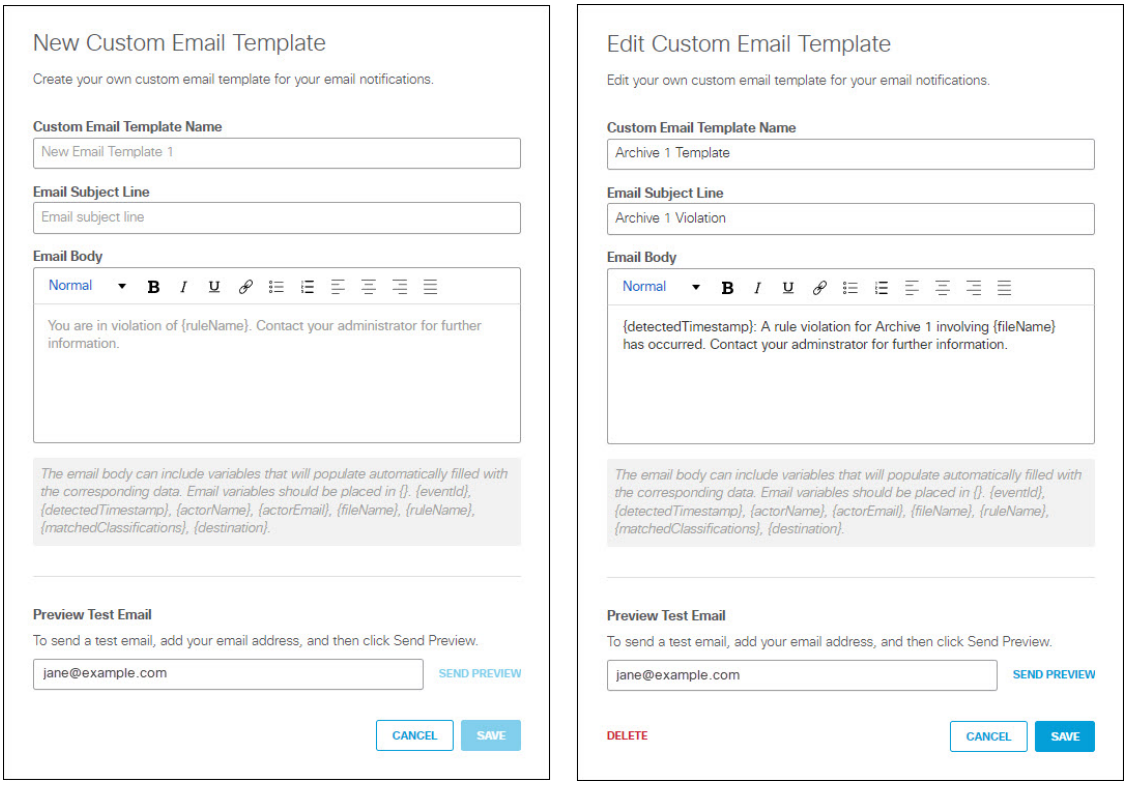
To Use a Custom Email Template:

1. Click **Custom Email**.
2. From the drop down menu, select an existing custom template, or choose **CREATE CUSTOM TEMPLATE**. If you select an existing custom template, you can click **Preview and Edit Custom Email** to review and change the template.





3. When you choose to create or edit a custom template for email notifications of policy violations you will see one of these two dialogs, which are almost identical:



The **Edit Custom Email Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You may not delete a template that is in use by any rule.

To create a new template or change an existing template:

a. Enter a unique **Custom Email Template Name**.

b. Enter an **Email Subject Line**.

c. Enter the text of the email in the **Email Body** text box.

The email text can include the following variables, which you must enclose in braces (**{}**):

- **{eventId}** - The unique identifier the system generates for the policy violation event.
- **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
- **{actorName}** - Name of the user whose action triggered the violation. (Secure Access gets this information from the authenticated Active Directory.)
- **{actorEmail}** - Email address of the user whose action triggered the violation. (Secure Access gets this information from the authenticated Active Directory.)
- **{fileName}** - Name of the data file that triggered the violation.
- **{ruleName}** - Name of the rule that was triggered.
- **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)
- **{destination}** - URL or IP address of the intended destination for the monitored request.

> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

d. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)

e. Click **SAVE** to return to return to the Data Loss Prevention Policy page.

12 Click **Save**.

> **Note**
>
> All fields must have options selected to save.

Understand Exclusions in a Real Time Rule

Describes understand exclusions in a real time rule. The Data Loss Prevention policy evaluates all active Real Time rules against the web requests in your environment.

The Data Loss Prevention policy evaluates all active Real Time rules against the web requests in your environment. Upon determining that a web request matches the identity and destination criteria of a Real Time rule, Secure Access then inspects the web request for matches with the rule's configured data classifications and file labels. Exclusions enable you to narrow your data criteria monitoring to specific applications and destinations. For example, if you have the rule to monitor data classifications for an application, but want to exclude some domains or URLs from being scanned, you can exclude a destination list with those domains. Traffic through that application will be scanned with the exception of the destination list excluded.

Within the context of a Real Time rule, exclusions will always override inclusions. For example, if a rule states that a domain on one list is excluded but the same domain is included on another destination list, the domain will automatically be excluded from the rule.

Supported Applications

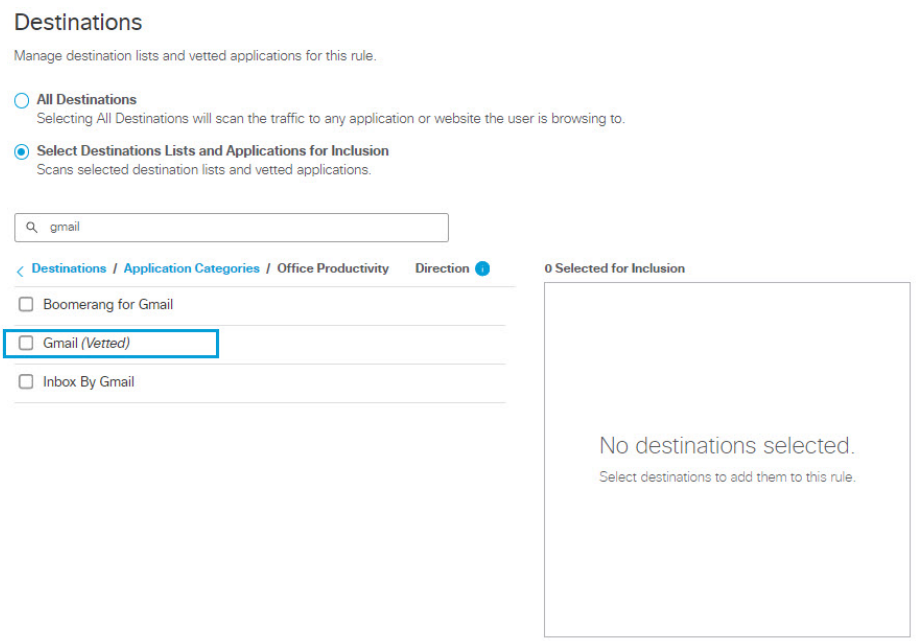
Describes supported applications. The Real Time DLP rules inspect the content of all Secure Access proxied web requests matching the resources and destinations selected in the Real Time rules of the Data Loss Prevention (DLP) policy.

The Real Time DLP rules inspect the content of all Secure Access proxied web requests matching the resources and destinations selected in the Real Time rules of the Data Loss Prevention (DLP) policy. When a Real Time DLP rule is configured with **Select Destination Lists and Applications for Inclusion**, Secure Access scans for data violations every web request matching the rule's applicable resources and targeting a destination matching the rule-configured destinations. A web request can be a web form or a file upload. File uploads can be scanned for matches with the selected data classifications in the file content, file name, or either. Moreover, a file upload can be scanned for the presence of

document properties matching the rule's File Labels settings. For more information, see Add a Real Time Rule to the Data Loss Prevention Policy.

Verified applications also support other workflows besides file uploads. For example, if the rule is configured to **Select Destination Lists and Applications for Inclusion** and Yahoo Mail is chosen as an application to scan for content, the policy can scan for file uploads, emails sent, and draft emails saved. Violations within these workflows are then blocked or monitored, depending on the action selected in the rule. However, some applications have limitations when scanning for file names of file uploads. For example, the DLP policy can scan Dropbox for file uploads, but the file name can not be scanned.

The DLP Real Time rules support thousands of applications, this link was 404 in readme, so I converted it to plain text divided into categoriesdivided into categories for ease of reference. Before January of 2024, DLP supported a more limited set of applications; the table below lists those applications and the limitations on their support. These applications appear in the GUI with the notation *(Vetted)*, as shown in the example below:



The list of apps marked *Vetted* in the GUI, and their workflow limitations, is listed below:

Application	Supported Workflows	File Name Limitations
Box Cloud Storage	File upload	
Concur Invoice	Receipt upload	
Confluence	File upload; edit a file **Note** To scan file uploads, you must select Atlassian and Confluence as destinations for the DLP rule.	
DLPTest.com	Submit test message; File upload	

Application	Supported Workflows	File Name Limitations
Dropbox	File upload; File upload add comment; File upload update comment **Note** Dropbox Paper is not supported using Real Time DLP, but may be supported using SaaS API DLP.	File names of file uploads are not scanned.
Facebook Messenger	Upload a file to chat	
Gmail	Send email; attach a file; save a draft; send an email (classic); save a draft (classic)	
Jira	Create a ticket (epic/story/task/subtask/bug/customer issue/customer request) description; upload an attachment to a newly created ticket (Atlassian must also be selected); add a comment to a ticket; edit a comment in a ticket; edit description **Note** To scan file uploads, you must select Atlassian and Jira as destinations for the DLP rule.	
LinkedIn SlideShare	File upload; publish content after a file upload; edit a published slide; edit privacy settings of a post; report content as inappropriate; upload thoughts and ideas on a slideshare; like a thought or slide; upload files from a Cloud app (Dropbox, GDrive, Box, Gmail, OneDrive); share content using linkedIn, Facebook, or Twitter	
Monday	Create workspace; create board; add item-update with file upload; add an item-update reply with file upload; add a message to Text column; add text to Long Text column; add an update with a file upload to a sub-item; reply to a sub-item update with a file upload; add a local file to File column; add an email address or text to Email column; upload a file to a shared form; add text to the dashboard text widget;	

Application	Supported Workflows	File Name Limitations
PasteBin	Post a message	
SalesForce	File upload; upload file via chatter; write a post in chatter; write a note;	
ServiceNow	Service management post incident; service automation post incident	
ShareFile	Create note; create request list; upload a file to a task; create a task; add task comment; send an invite to a new user; share a file; file upload; submit a form; remote upload a form; create a file drop; share a file via email; send an email	File names of files uploaded to ShareFile storage are not scanned.
Slack	File upload; post a message in a channel	
SmartSheet	File upload; upload attachment to a form; add comment to a form	
WeTransfer	File upload; upload a file to a message	File names of files uploaded to WeTransfer are not scanned.
WorkDay HCM	Add an address; edit an address; add text to a field; upload a file	
Yahoo Mail	Upload file; send an email; save a draft	

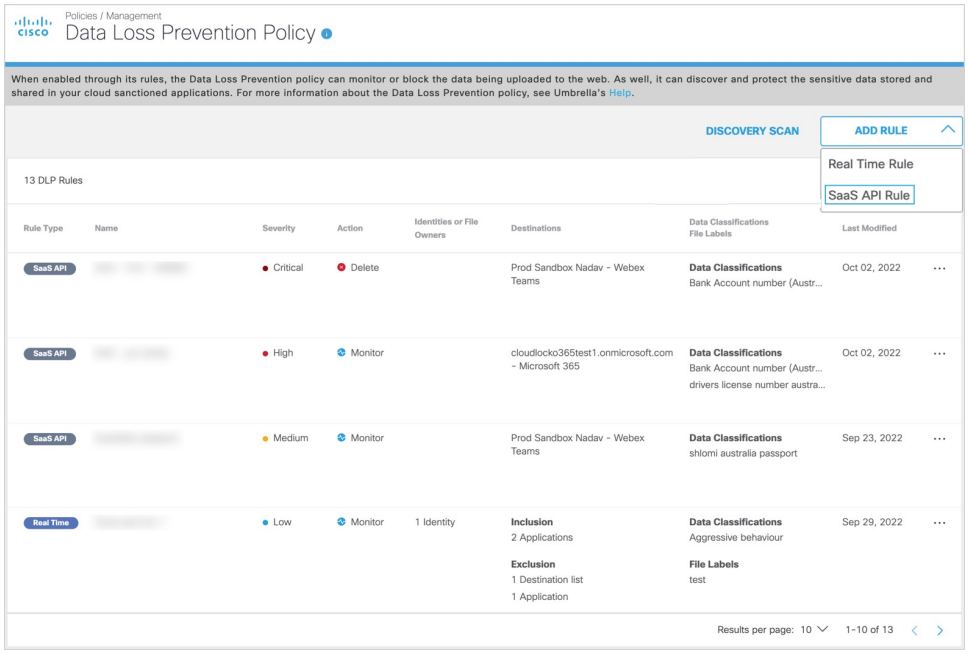
Add a SaaS API Rule to the Data Loss Prevention Policy

Provides instructions for adding a saas api rule to the data loss prevention policy. Configure a SaaS API Rule to set the criteria as to what triggers the scanning.

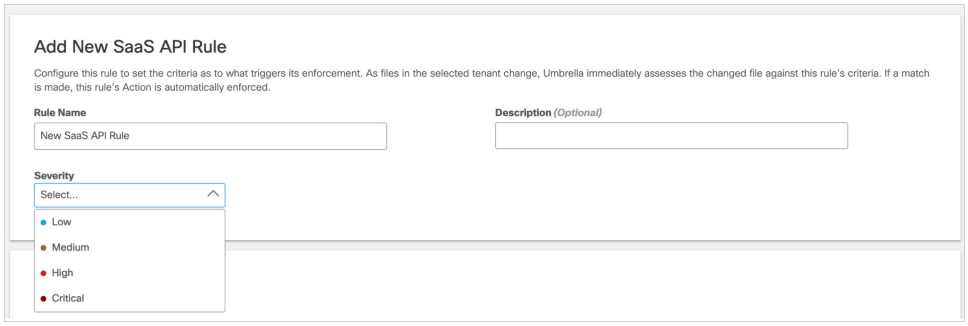
Configure a SaaS API Rule to set the criteria as to what triggers the scanning. As files in the selected tenant are scanned upon content change and context (sharing) change, Secure Access assesses the file against this rule's criteria. If a match is made, this rule's action is immediately enforced. If Secure Access detects a violation, the offending file is listed in the Data Loss Prevention Report.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**. The page displays a list of all Real Time and SaaS API Rules created.
2. From the **Add Rule** drop-down, select **SaaS API Rule**.



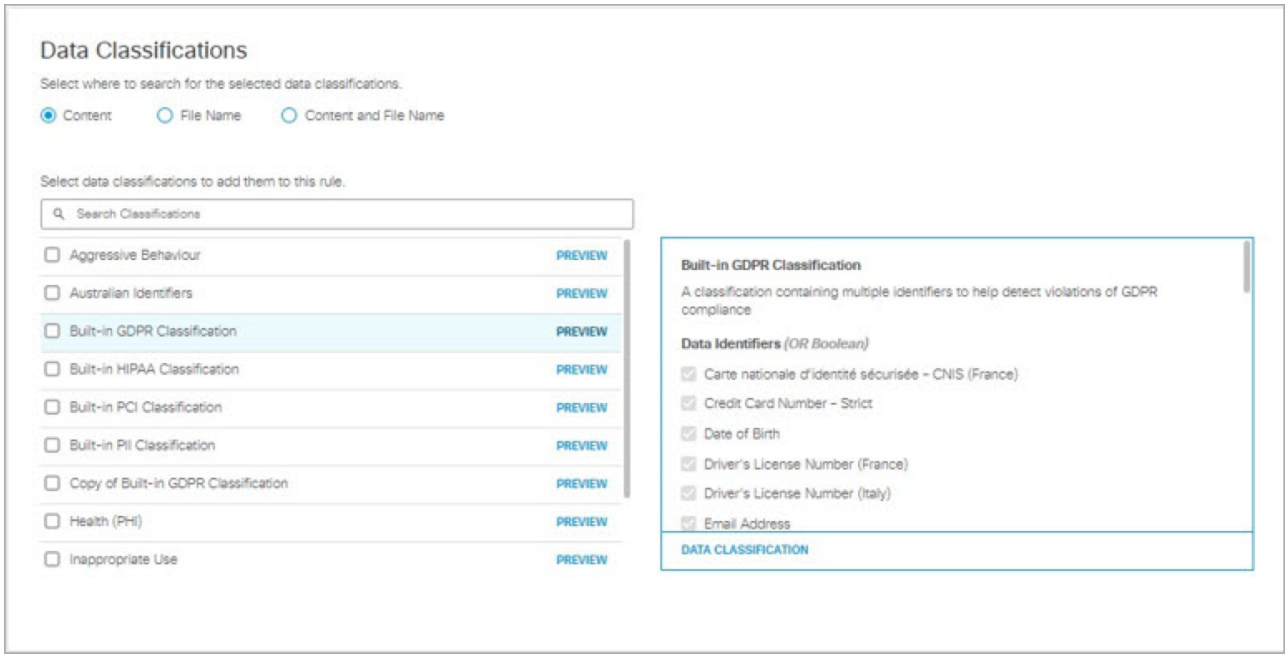
3. In the **Add New SaaS API Rule** page, enter a meaningful **Rule Name** and **Description**. Select a **Severity** value from the drop-down based on the risk involved or importance within the ruleset. (Assigning severity values can help later on when you need to filter events in the Data Loss Prevention report.)



4. Select where in scanned files you would like this rule to search for the data classifications that you choose:
   - **Content**–(Default) Scans only the content of files for the selected data classifications.
   - **File Name**–Scans only file names for the selected data classifications.
   - **Content and File Name**–Scans content and file names for the selected data classifications. Both content and file name do not need to match for the rule to apply, only one or the other.

> **Note**
>
> Choosing **Content**, **File Name**, or **Content and File Name** refers to scanning file uploads for the selected data classifications and configured file labels.

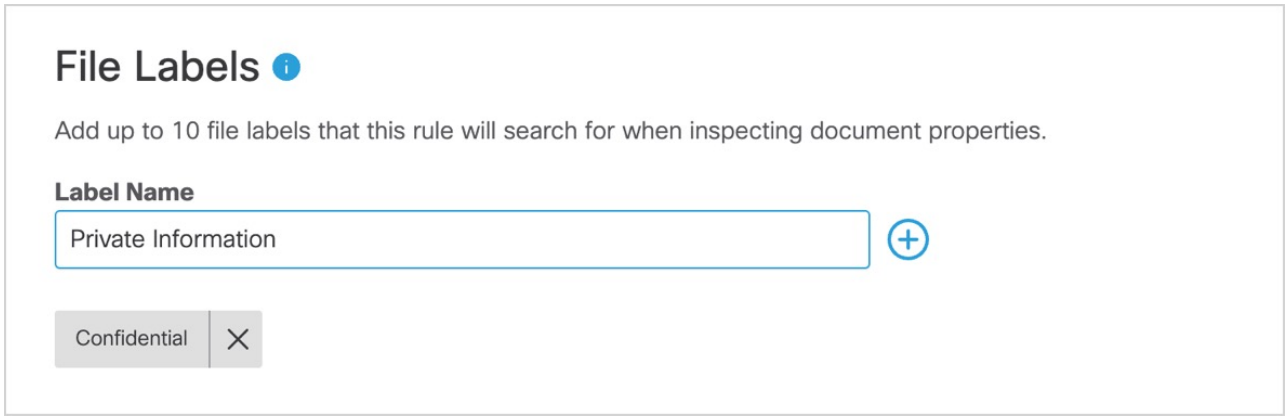
5. Select Data Classifications to apply this rule; you can choose a data classification of your own making or a built-in data classification provided by Umbrella. (See Manage Data Classifications and Built-In Data Classification Templates.) Hover over **PREVIEW** to view data identifiers associated with each data classification.



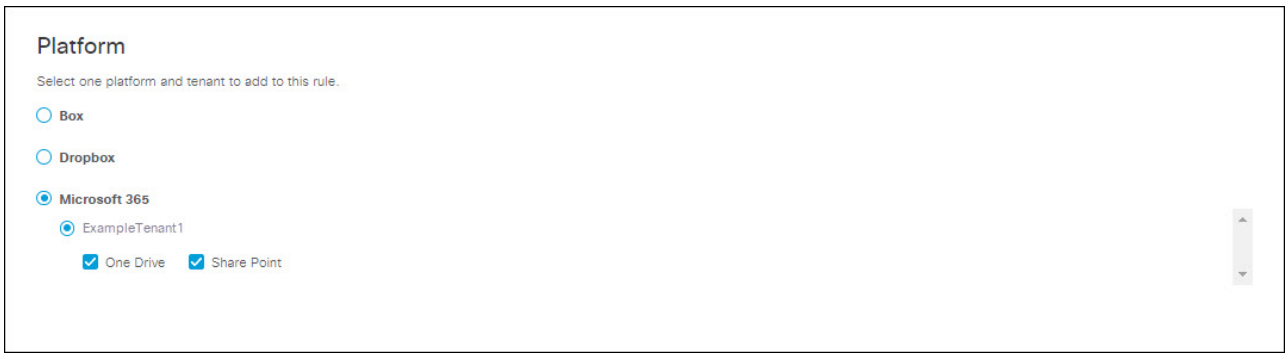
6. Add up to 10 case-sensitive file label names to apply to this rule. The rule will search for any of the configured file label names in the value of the files' document properties. This includes:
   - Microsoft Office Document Properties
   - Microsoft Office Sensitivity Labels
   - Adobe PDF Document Properties

   File uploads to Confluence and Jira are not scanned for file labels.

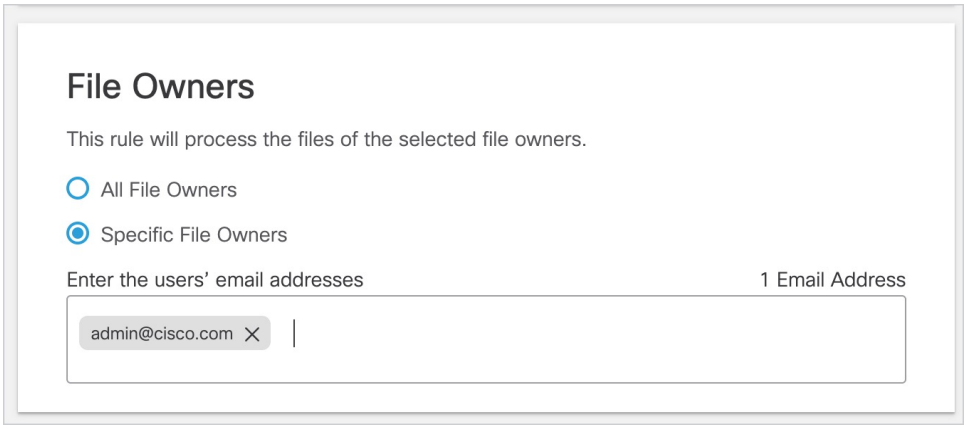
> **Note**
>
> Microsoft Sensitive Labels
>
> Secure Access currently supports the detection of Microsoft sensitivity labels in the file properties' values of the inspected file for Microsoft Word, Excel, PowerPoint, and .pdf files. Ensure you configure the rule with the name of the sensitivity labels, not the Display Names.



7. Under **Platform**, select one platform and tenant for this rule.



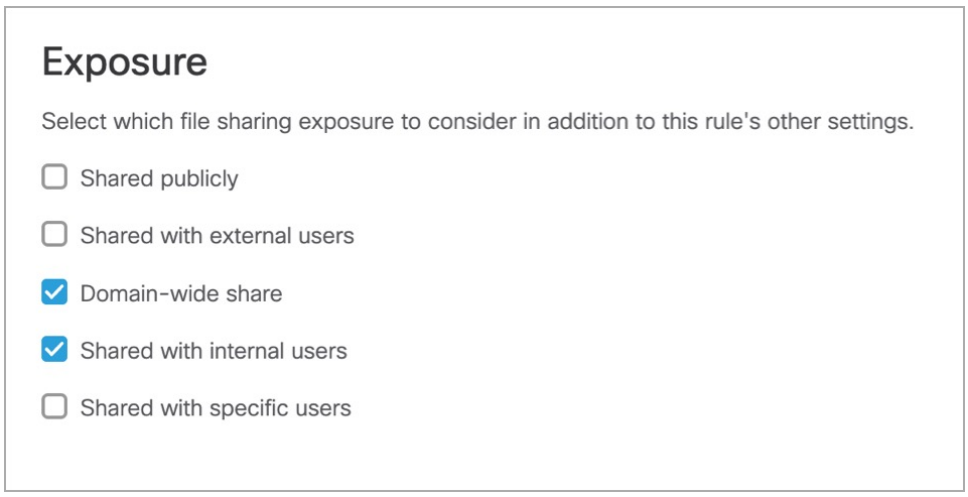
8. Select an option under **File Owners** to define the scope of the processed files.
   - Select **All File Owners** to process the files of all owners.
   - Select **Specific File Owners** to process the files of specified owners. Enter the owners' email addresses.



9. Optionally select the file sharing permissions to consider when processing files to search for data violations.
   - Shared Publicly- Accessible to all users with the link to the file.
   - Shared with External Users- Shared with users who do not belong to the authorized domains.
   - Domain-wide Share- Shared with all users in a domain.
   - Shared with Internal Users- Shared with users who belong to the authorized domains.
   - Shared with Specific Users- Shared with specific users by their email addresses.

   The table below indicates which Exposure settings are available for each platform:

	Shared Publicly	Shared with external users	Domain-wide share	Shared with internal users	Shared with specific users
Microsoft Office 365	✓	✓	✓	✓	✓
Dropbox	✓	✓	–	–	✓
Box	✓	✓	–	–	✓
Google	✓	✓	✓	✓	✓
Webex Teams	–	✓	–	✓	✓



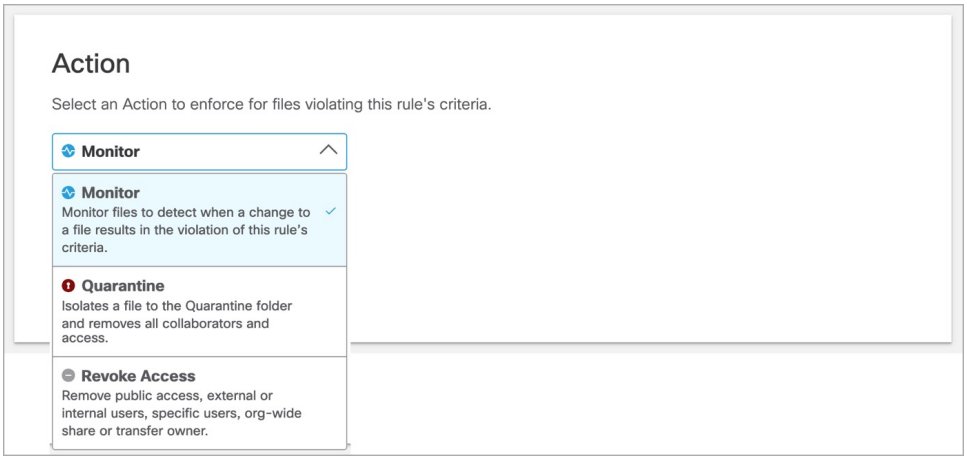
Note

- A DLP rule can be configured with either Data Classifications, File Labels or both. Exposure is an optional criterion.
- When a DLP rule is configured with all 3 criteria, then a DLP event is raised when any of the selected Data Classifications and when any of the configured file labels are detected in the inspected file and when the file's permissions match any of the selected exposure settings.

10. From the **Action** drop-down list, choose **Monitor**, **Quarantine**, **Delete** or **Revoke Access**.
    - **Monitor**- Detects and logs a DLP event for every modified file violating this rule's criteria
    - **Quarantine**- Isolates a file that violates the rule criteria to the quarantine folder
    - **Delete**- Permanently deletes when a change is detected that violates the rule criteria
    - **Revoke Access**- Removes public link, all external or internal users, and any share permission within the entire organization. This action also removes the file owner and transfers the ownership to the selected user.

    The table below indicates which Actions settings are available for each platform:

	Monitor	Quarantine	Delete	Revoke Access
Microsoft Office 365	✓	✓	–	✓
Dropbox	✓	✓	–	✓
Box	✓	✓	–	✓
Google	✓	✓	–	✓
Webex Teams	✓	–	✓	–



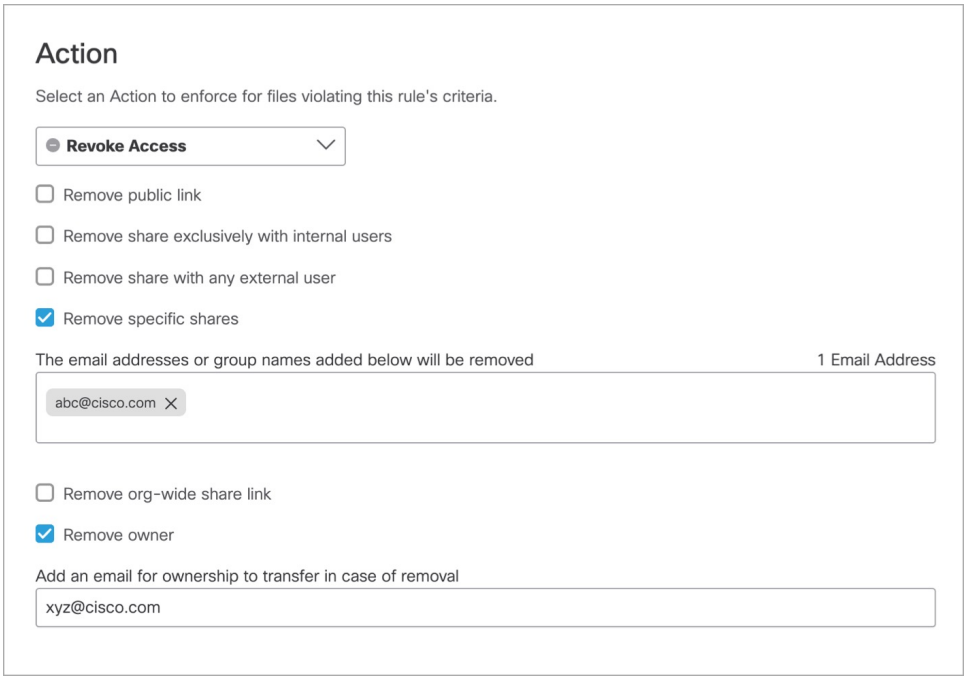
Note

If you choose **Quarantine**:

- The file identified as exposing sensitive data is moved to the Cisco_Quarantine/DLP folder Umbrella created in the root path of the Global Admin who authorized the tenant.
- In lieu of the quarantined file, a text file is left in the original location with the name ***filename*.ppt_*Unique-Event-ID*_Cisco_Quarantined.txt** explaining to the original File Owner that the file is identified as exposing sensitive data and for more information to contact their organization administrator.
- The user who authorizes access to Umbrella will have access to the quarantine folder. All other accesses and collaborators are removed.
- Thus, we recommend that the admin add the relevant DLP Admins as additional collaborators to the folder.

11. If you chose **Revoke Access**:

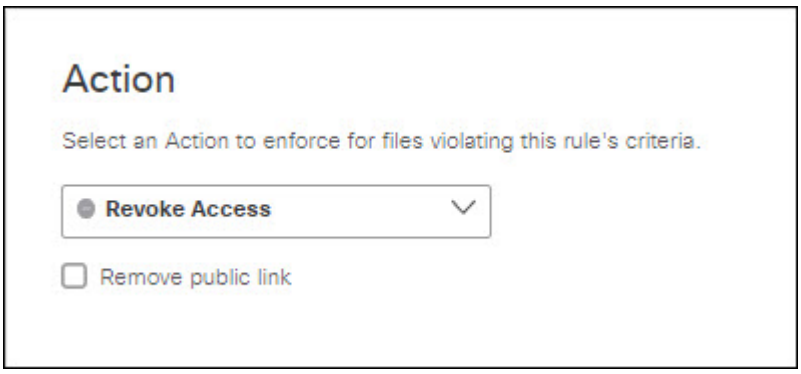
- If you chose **Google Drive** for the Platform, choose from the following options:
  - **Remove public link**: Removes any file link that has public exposure.
  - **Remove share exclusively with internal users**: Removes all internal users of files that were shared with few specific internal users.
  - **Remove share with any external user**: Removes all external users. (External users are not part of the organization domain)
  - **Remove specific shares**: Entered email addresses or group email addresses are removed.
  - **Remove org-wide share link**: Removes any share permission with the entire organization.
  - **Remove owner**: Removes the file owner and transfers ownership to a new email address.



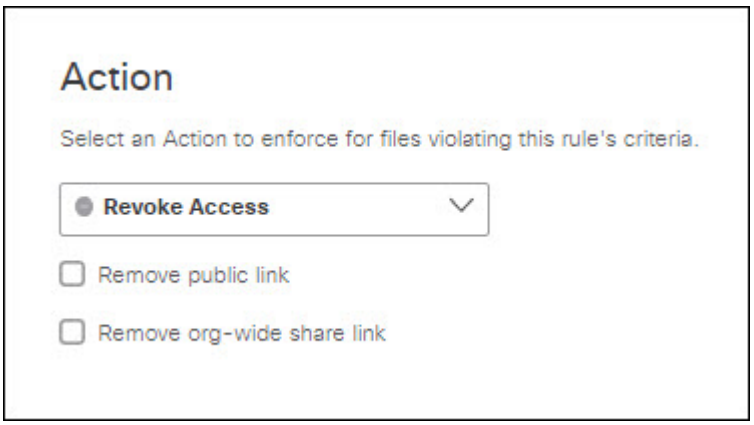
- If you chose **Microsoft 365** for the platform, choose from the following options:
  - **Remove public link**: Removes any file link that has public exposure.
  - **Remove org-wide share link**: Removes any share permission with the entire organization.



- If you chose **Box** for the platform, you may choose the following option:
  - **Remove public link**: Removes any file link that has public exposure.

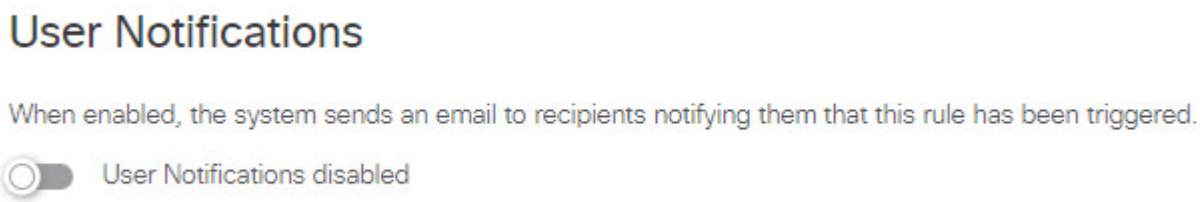


- If you chose **Dropbox** for the platform, you may choose from the following options:
  - **Remove public link**: Removes any file link that has public exposure.
  - **Remove org-wide share link**: Removes any share permission with the entire organization.

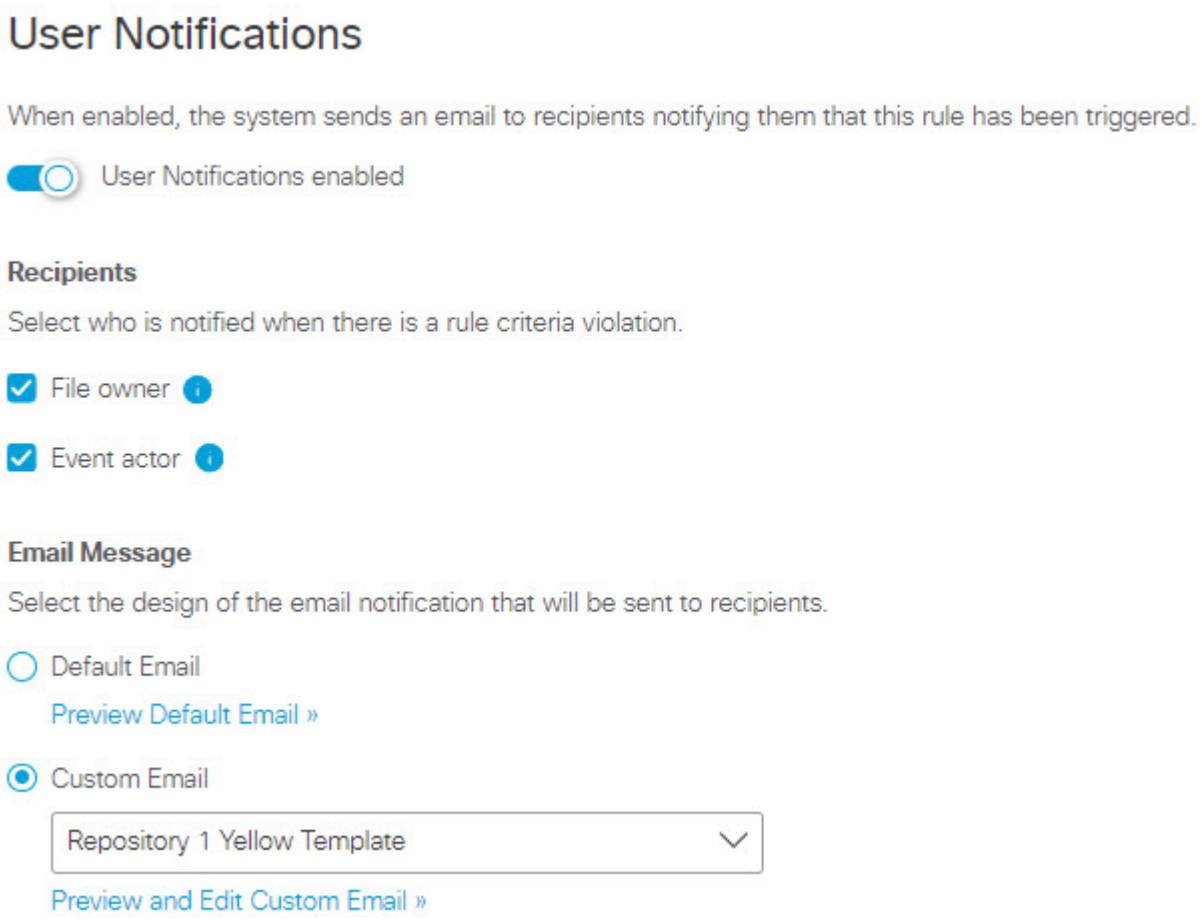


12. Under **User Notifications** you can enable and configure an email notification to be sent to one or both of the following users:
    - The owner of the file associated with a rule violation
    - The user who performs an action that triggers a rule violation

    You can use a default email template provided by the system, or create your own custom template.



    a. Enable user notifications.



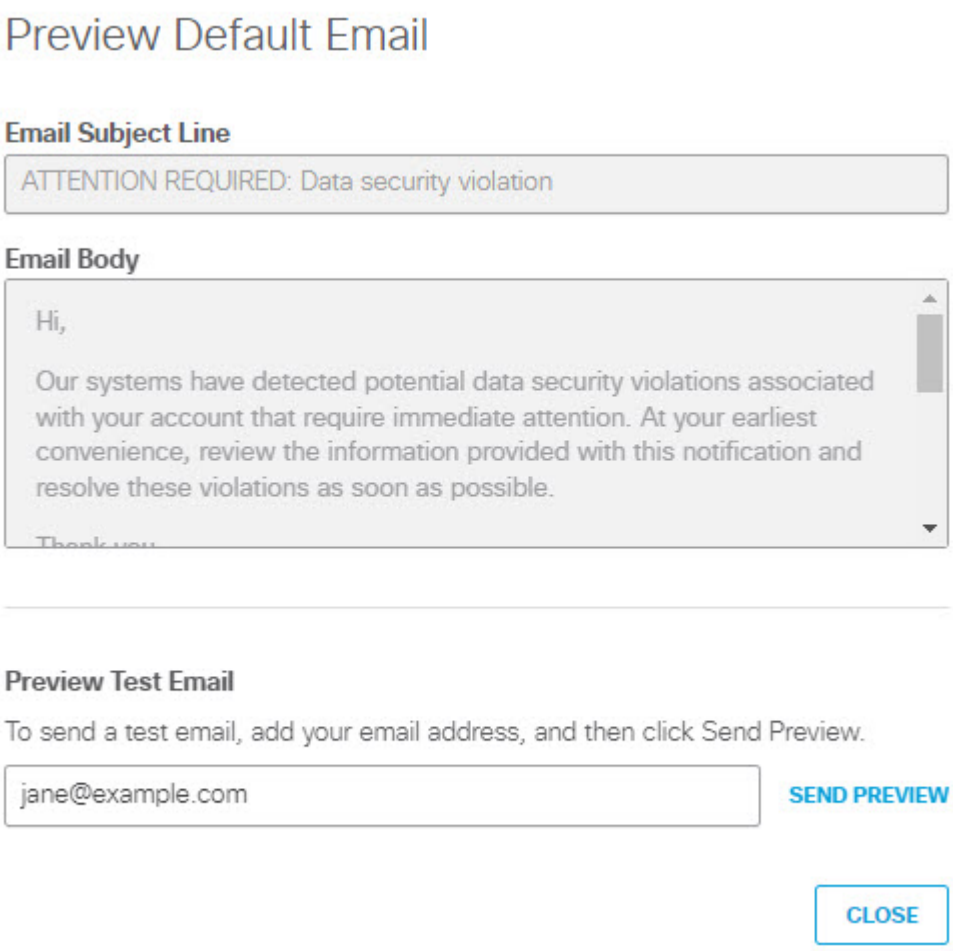
b. Select one or both of the following email recipients:

- **File owner** - The owner of the file associated with the rule violation
- **Event actor** - The user who performs an action that triggers the rule violation

c. Choose the email template:

To Use the Default Email Template:

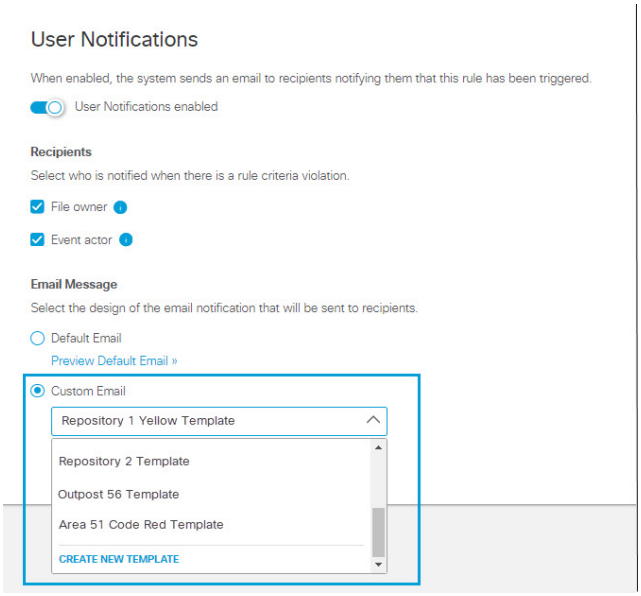
1. Click **Default Email**.
2. To preview the content of the email that will be send to users, click on **Preview Default Email**. You can review the email subject line and text, but you cannot change it.

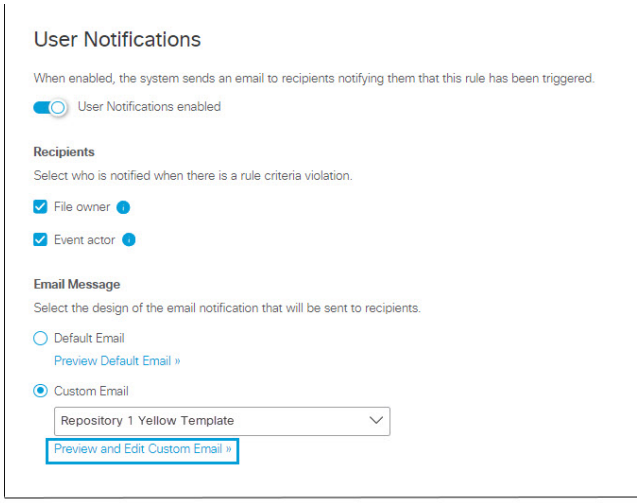


3. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)
4. Click **CLOSE** to return to the Data Loss Prevention Policy page.

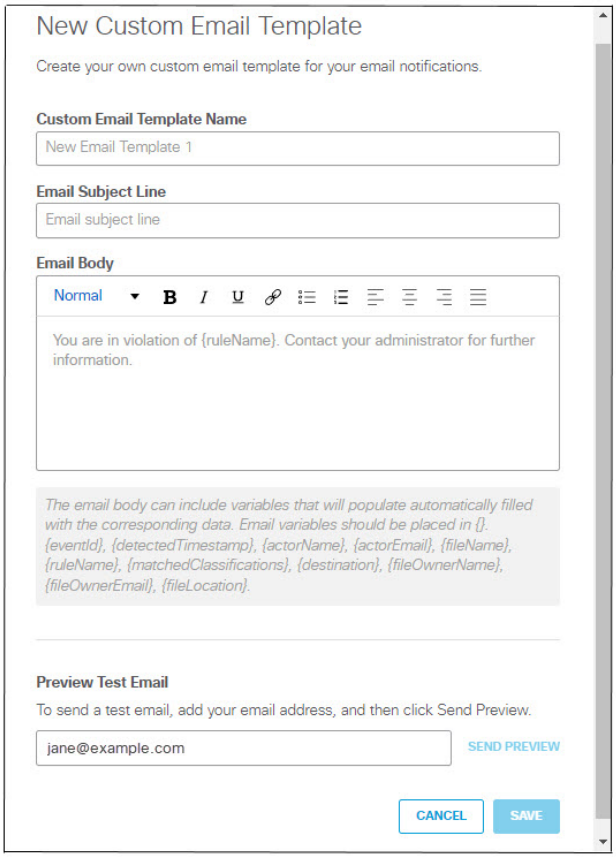
To Use a Custom Email Template:

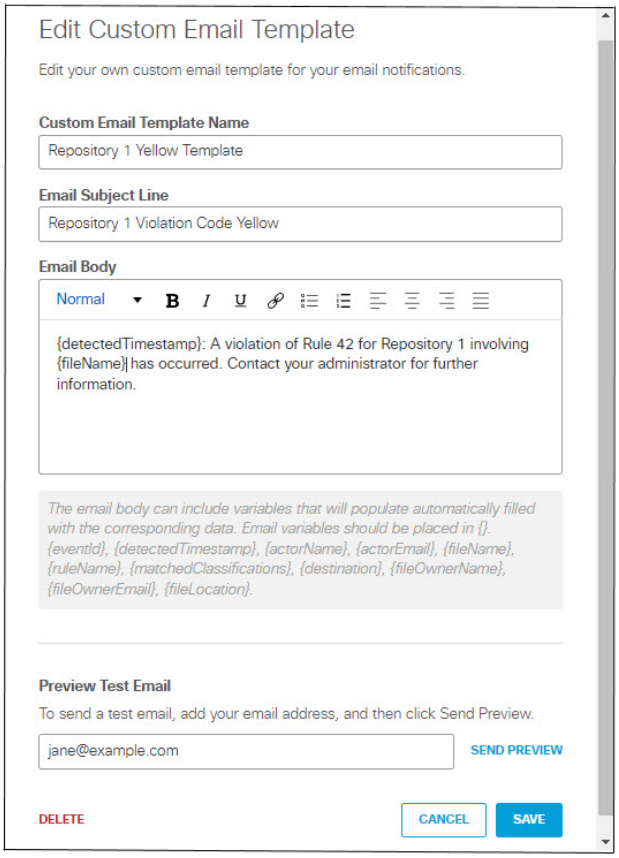
1. Click **Custom Email**.
2. From the drop down menu, select an existing custom template, or choose **CREATE CUSTOM TEMPLATE**. If you select an existing custom template, you can click **Preview and Edit Custom Email** to review and change the template.





3. When you choose to create or edit a custom template for email notifications of policy violations you will see one of these two dialogs, which are almost identical:





The **Edit Custom Email Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You may not delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Email Template Name**.
2. Enter an **Email Subject Line**.

3. Enter the text of the email in the **Email Body** text box.

   The email text can include the following variables, which you must enclose in braces (**{}**):

   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)
   - **{destination}** - The application or platform type of the tenant associated with the violation. (E.g., Google Drive or One Drive; see Manage Tenant Controls.)
   - **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileLocation}** - The file URL.

   > **Note**
   >
   > The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

4. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)
5. Click **SAVE** to return to return to the Data Loss Prevention Policy page.

13. Click **Save**. All fields must have options selected to save.

Discovery Scan

Describes discovery scan. Discovery Scan inspects the content of all files in the tenant that are modified over the selected date range. As files in the selected tenant are scanned upon content change and context (sharing) change, Secure Access assesses the file.

Discovery Scan inspects the content of all files in the tenant that are modified over the selected date range. As files in the selected tenant are scanned upon content change and context (sharing) change, Secure Access assesses the file. If Secure Access detects a violation, the offending file is listed in the Data Loss Prevention Report.

This topic walks you through how to initiate a scan and how to cancel an ongoing scan.

Note

A discovery scan must be triggered around 24 hours after tenant authorization as the system evaluates and enumerates the users in the organization. Any triggering beforehand might not include all users. Secure Access performs discovery scans on file of up to 50 MB. For each file, the scan extracts up to the first 5 MB of plain text from the file, and scans that data for violations.

Prerequisites

- You must authenticate a tenant for at least one of the platforms Secure Access supports for SaaS API Data Loss Prevention: Google Drive, Microsoft 365, Dropbox, and Box. For more information, see Manage SaaS API Data Loss Prevention.

Prerequisites

Describes prerequisites. You must authenticate a tenant for at least one of the platforms Secure Access supports for SaaS API Data Loss Prevention: Google Drive, Microsoft 365, Dropbox, and Box. For more information, see Manage SaaS API Data Loss Prevention.

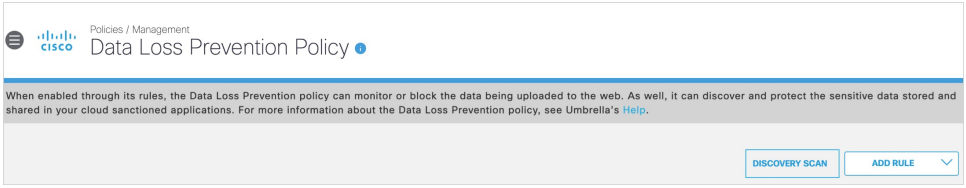
- You must authenticate a tenant for at least one of the platforms Secure Access supports for SaaS API Data Loss Prevention: Google Drive, Microsoft 365, Dropbox, and Box. For more information, see Manage SaaS API Data Loss Prevention.

Initiate a Discovery Scan

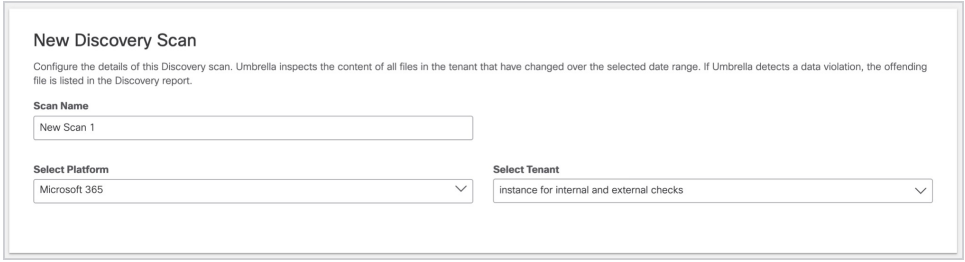
Provides instructions for initiate a discovery scan.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Protection Policy**.
2. Click **Discovery Scan**.



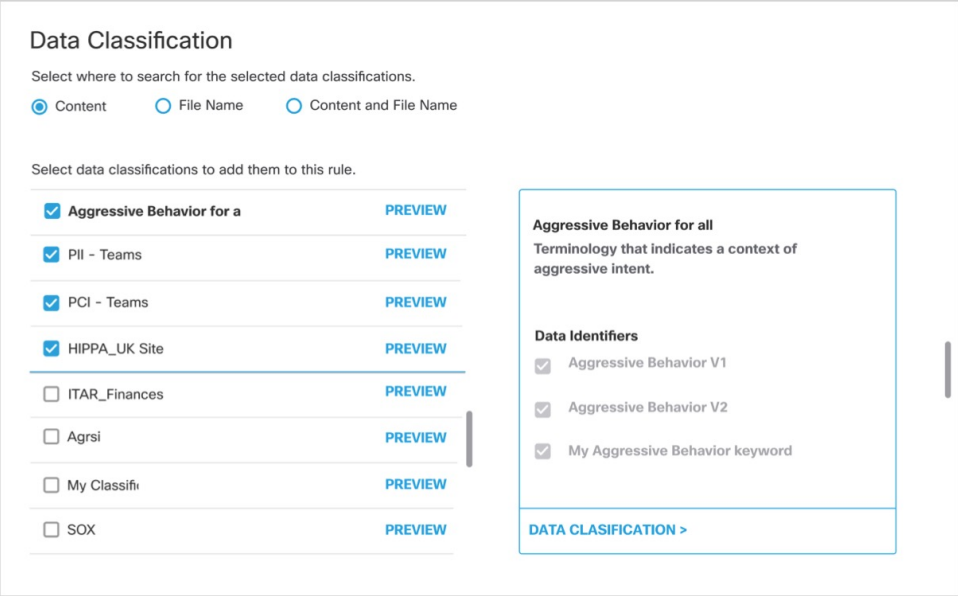
3. Enter the **Scan Details**. Choose a platform and tenant of the platform from the drop-down lists.



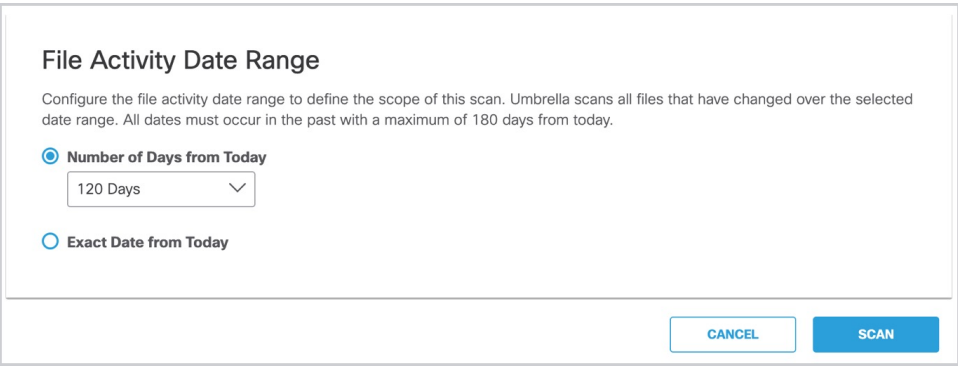
4. Select where in uploaded files you would like the scan to search for the data classifications that you choose.
   - **Content**–(Default) Searches only the content of files for the selected data classifications.
   - **File Name**–Searches only file names for the selected data classifications.
   - **Content and File Name**–Searches content and file names for the selected data classifications. Both content and file name do not need to match for the scan to apply, only one or the other.

> **Note**
>
> Choosing Content, File Name, or Content and File Name refers to scanning file uploads for the selected data classifications and configured file labels.

5. Select the required **Data Classification** of your choice. You can select multiple tenants.

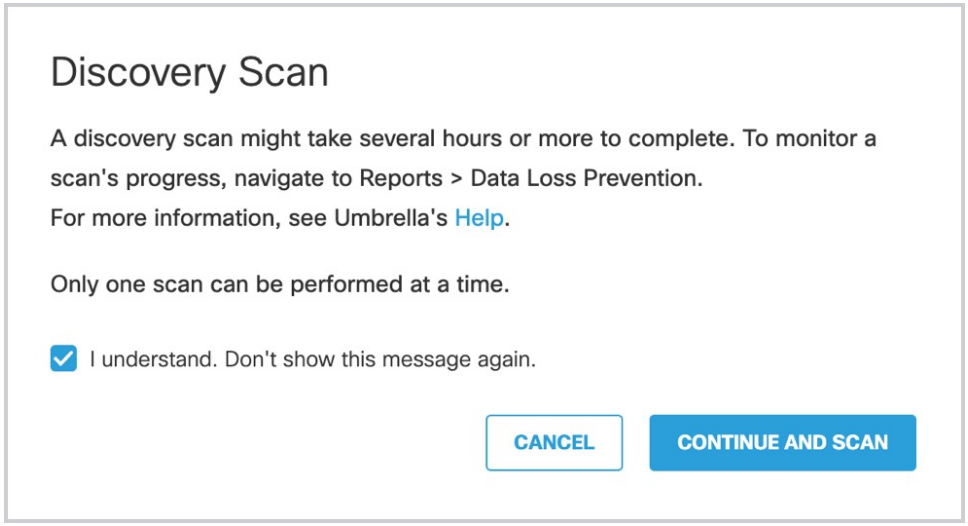


6. Enter the Date Range to define the scanning scope. Note that only files modified in the selected date range are scanned.



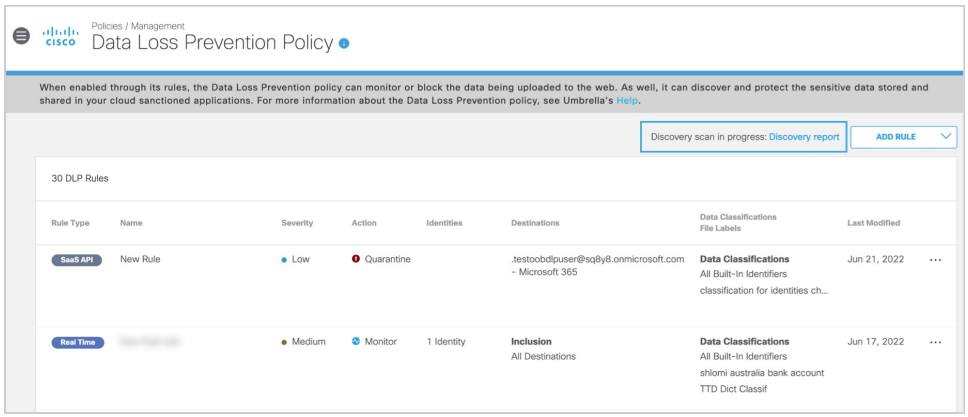
7. Click **Scan** to initiate.
8. Click **Continue and Scan**.

> **Note**
>
> Only one scan executes at a time. The scan might take a while. Once completed, you can initiate another scan.



9. Click **Discovery Report** to view the progress of the scan results.

   For more information on DLP reports, refer to DLP Report.

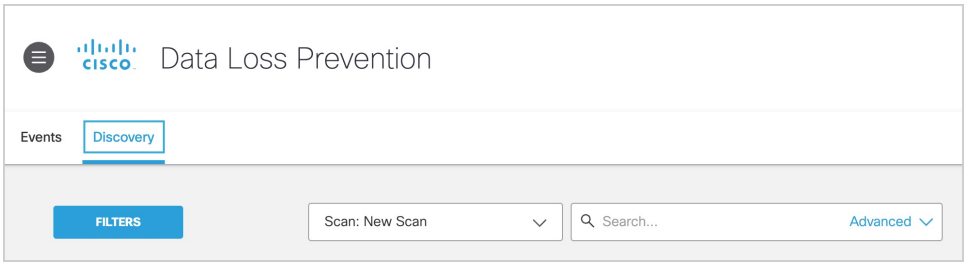


Cancel a Discovery Scan

Provides instructions for cancelling a discovery scan.

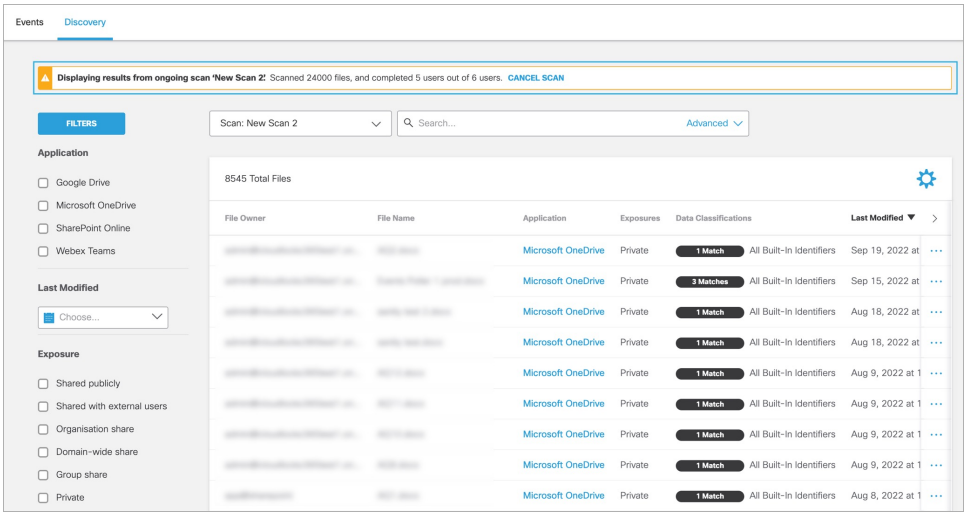
Procedure

1. Navigate to **Reporting** > **Additional Reports** > **Data Loss Prevention**.
2. Switch to the **Discovery** tab.

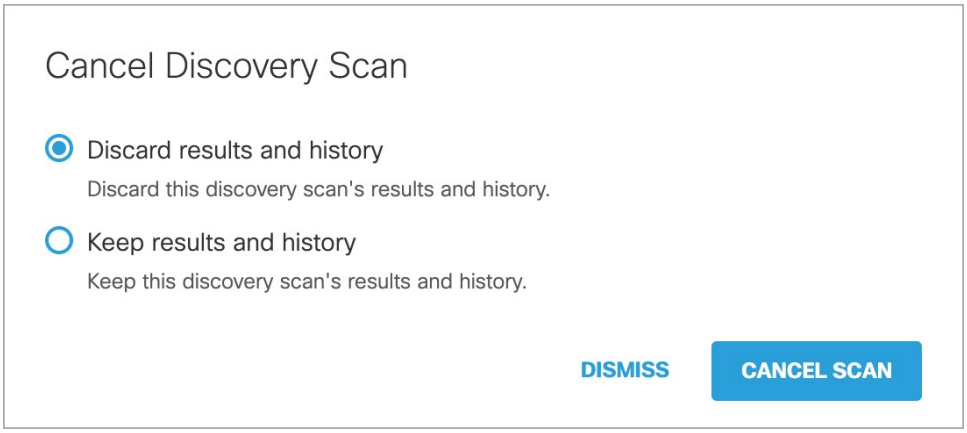


3. Click **Cancel Scan**. Results of the ongoing scan are displayed in the ribbon.

> **Note**
>
> Note that the cancelation of a scan might take a few minutes.



4. You can choose to either discard or keep the scan results and history. Click **Cancel Scan**.



Edit a Data Loss Prevention Rule

Describes editing a data loss prevention rule. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

After adding a Real Time or SaaS API rule, you can edit it to change what traffic it monitors (identities and destinations) or what cloud tenant is applicable to, the data classifications and file labels that represent the data violation criteria, and the action to be enforced upon detecting data violations in the scanned content.

> **Note**
>
> Editing a rule does not impact any running Discovery Scan, it only impacts incoming events for the scan.

Procedure

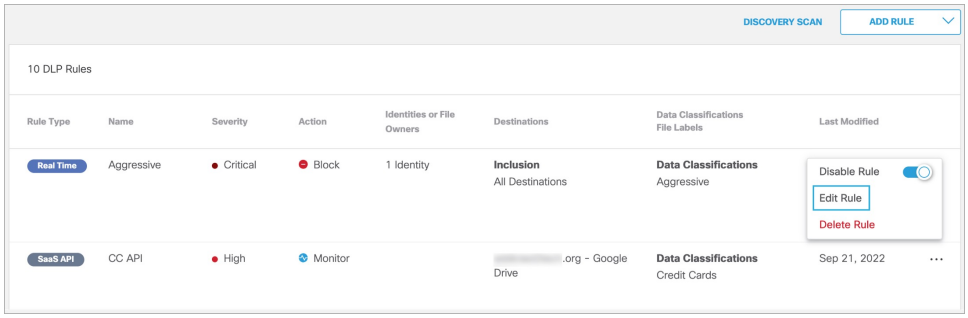
Provides instructions for editing a data loss prevention policy rule.

Before you begin

- Full admin access to the Secure Access dashboard. See Manage User Roles.
- For Real Time DLP rules, HTTPS Inspection must be enabled either on the Web Default Policy, or at least one web policy ruleset where the same identity is configured in a DLP rule. For example, if the identity "Network A" is configured for a DLP rule, it must also be configured for a web policy ruleset where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**.
2. Click the **More Actions** menu, and select **Edit Rule**.



3. Make the changes and click **Save**.

Delete a Data Loss Prevention Rule

Describes deleting a data loss prevention rule. You can delete a Data Loss Prevention rule at any time. To edit a rule, see Edit a Data Loss Prevention Rule.

You can delete a Data Loss Prevention rule at any time. To edit a rule, see Edit a Data Loss Prevention Rule.

Deleting a rule does not impact a running Discovery Scan, it only impacts incoming events for the scan.

Procedure

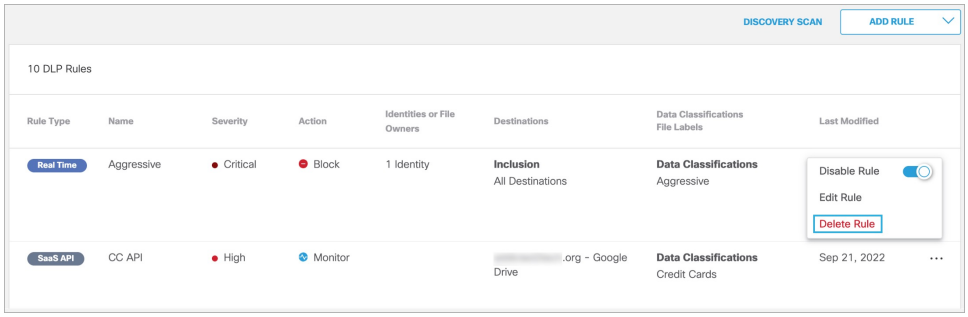
Provides instructions for deleting a Data Loss Prevention Policy rule.

Before you begin

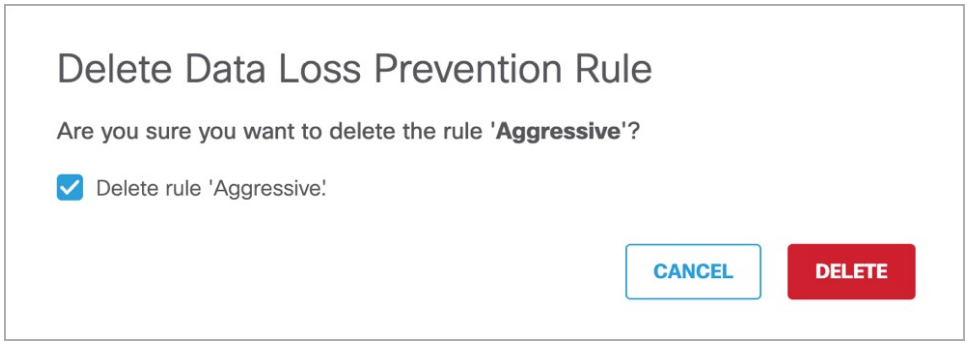
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**.
2. Click the **More Actions** menu, and click **Delete Rule**.



3. Confirm deleting the rule and then click **Delete**.



Enable or Disable a Data Loss Prevention Rule

Describes enabling or disable a data loss prevention rule. Newly added rules are automatically enabled for the Data Loss Prevention policy. When you navigate to Secure Policy Data Loss Prevention Policy , disabled rules appear faded.

Newly added rules are automatically enabled for the Data Loss Prevention policy. When you navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**, disabled rules appear faded. Note that enabling or disabling a rule does not impact any running Discovery Scan, it only impacts incoming events for the scan.

Disable a Rule

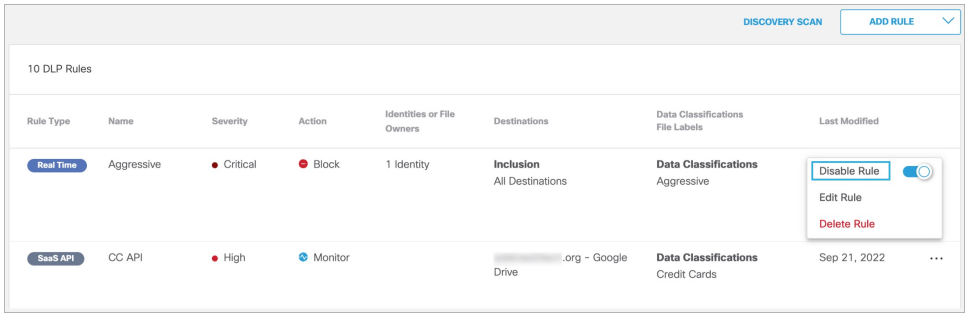
Provides instructions for disabling a rule.

Before you begin

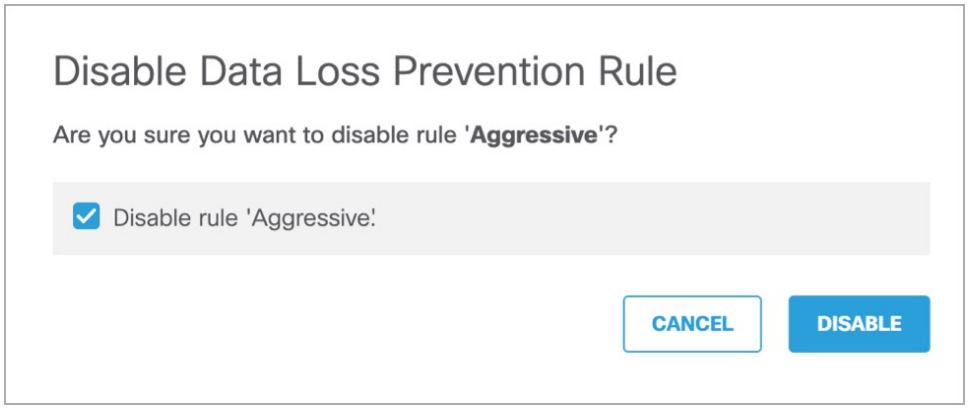
- Full Admin user role. For more information, see Manage Accounts.
- For Real Time DLP rules, HTTPS Inspection must be enabled either on the Web Default Policy, or at least one web policy ruleset where the same identity is configured in a DLP rule. For example, if the identity "Network A" is configured for a DLP rule, it must also be configured for a web policy ruleset where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**.
2. Click the **More Actions** menu, and click **Disable Rule**.



3. Confirm disabling the rule and then click **Disable**.



Enable a Rule

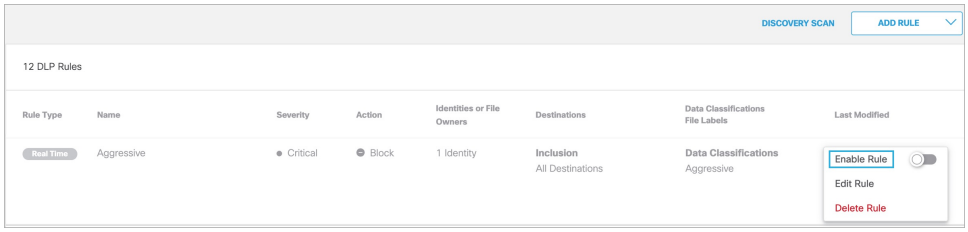
Provides instructions for enabling a rule.

Before you begin

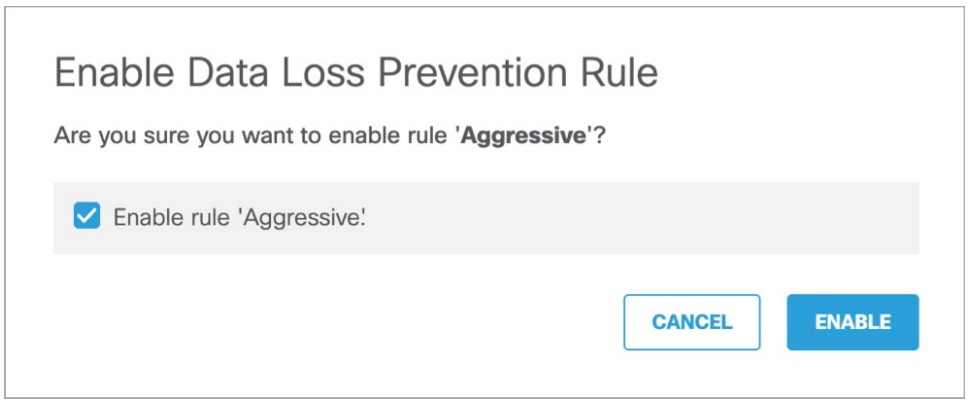
- Full Admin user role. For more information, see Manage Accounts.
- For Real Time DLP rules, HTTPS Inspection must be enabled either on the Web Default Policy, or at least one web policy ruleset where the same identity is configured in a DLP rule. For example, if the identity "Network A" is configured for a DLP rule, it must also be configured for a web policy ruleset where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Protection Policy**.
2. Click the **More Actions** menu, and click **Enable Rule**.



3. Confirm enabling the rule and then click **Enable**.



Supported File and Form Types

Describes supported file and form types. The Data Loss Prevention policy can monitor or block the data being uploaded to the web. The policy discovers and protects the sensitive data contained in your cloud-sanctioned applications. The DLP scans the plain text of files up to 50 MB.

The Data Loss Prevention policy can monitor or block the data being uploaded to the web. The policy discovers and protects the sensitive data contained in your cloud-sanctioned applications. The DLP scans the plain text of files up to 50 MB. DLP scans archives as well as files containing embedded files; for these, DLP can extract and scan content for up to 100 files nested up to 10 levels deep. Secure Access scans all files uploaded through the Secure Access SWG proxy that match the Real Time rules' criteria, as well as the files stored in the Secure Access authorized cloud tenants and performs a deeper analysis for the following mime types:

Mime Type	File Type
application/msword	Word .doc, .docx
application/pdf	PDF
application/rtf	RTF
application/vnd.ms-excel	Excel .xlsx
application/vnd.ms-powerpoint	PowerPoint .ppt
application/vnd.oasis.opendocument.presentation	OpenDocument Presentation .odp
application/vnd.oasis.opendocument.spreadsheet	OpenDocument Sheet .ods
application/vnd.oasis.opendocument.text	OpenDocument Word .oth
application/vnd.openxmlformats-officedocument.presentationml.presentation	PowerPoint .pptx
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Excel .xlsx
message/rfc822	E-mail

Mime Type	File Type
text/csv	CSV
text/html	HTML/XML
text/plain	Plain text .txt
text/rtf	RTF
text/tab-separated-values	TSV
text/url	URL

The Real Time DLP rules can scan the content of all applicable web requests of the following form types:

- JSON
- XML
- URL encoded
- Multipart form

Best Practices for the Data Loss Protection Policy

Describes best practices for the data loss protection policy. Some of the Data Loss Prevention policy's built-in identifiers have the potential to produce false positives if not customized to narrow the scope of the inspection. The following are recommended to reduce the number of false positives in these classifications.

Some of the Data Loss Prevention policy's built-in identifiers have the potential to produce false positives if not customized to narrow the scope of the inspection. The following are recommended to reduce the number of false positives in these classifications. For more information on customizing an identifier, see Copy and Customize a Data Identifier.

Threshold

The default threshold for built-in identifiers without tolerance is 1. This means that the policy will search for content where the identifier is met only once within a file. Increasing the threshold will scan content for instances where the identifier is met more than once, creating fewer false positives for each individual instance of the identifier. A threshold of 10, for example, only monitors or blocks a file if 10 instances of the identifier are found in the file.

Proximity Terms

Proximity keywords reduce false positives by requiring identifiers to match within 10 terms of specified words.

For example, a Canadian bank account identifier will search for a pattern matching Canadian bank account numbers and transit numbers. A document containing several random numbers matching that pattern could produce false positives, however, if proximity terms such as "Canada" and "bank" are added to the customized identifier, the scope of the inspection is reduced.

43 Manage Data Classifications

Topics:

- Create a Data Classification
- Copy and Customize a Data Identifier
- Delete or Edit a Classification
- Create an Exact Data Match Identifier
- Index Data for an EDM
- Create an Indexed Document Match Identifier
- Built-In Data Classifications
- Exact Data Match Field Types

Introduces managing data classifications. The Data Loss Prevention (DLP) policy monitors or blocks content based on the rules configured for the policy. The rules use data identifiers and data classifications, which describe the type of data to be monitored or blocked.

The Data Loss Prevention (DLP) policy monitors or blocks content based on the rules configured for the policy. The rules use *data identifiers* and *data classifications*, which describe the type of data to be monitored or blocked. The file and form types supported by the DLP policy are listed here.

Data identifiers describe the content the Data Loss Prevention Policy monitors or blocks. Data identifiers can describe Personal Information Identifiers (PII) that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers. Data identifiers can also describe certain content an organization may wish to monitor or block within its network traffic, such as discriminatory or aggressive content. Umbrella provides a collection of built-in data identifiers (see Built-in Data Identifiers and Individual Data Identifiers), and you can create custom identifiers based on the built-in data identifiers (see Copy and Customize a Data Identifier).

Data classifications are groups of data identifiers combined for the purpose of monitoring or blocking closely related content. For example, you can create a data classification that encompasses medically related content by including the built-in identifiers for ICD codes, drug names, prescription names, health conditions, and national drug code names. The classification, when applied to a rule in the Data Loss Prevention Policy, will monitor or block content matching those identifiers.

There are three ways to establish a data classification to apply to a data loss prevention rule:

- You can create a custom data classification entirely of your own design. See Create a Data Classification on page 603.
- You can create a custom data classification based on a built-in data classification provided by Secure Access. See Copy and Customize a Data Identifier on page 609
- You can apply a built-in data classification provided by the system.

Secure Access provides four different built-in data classifications. You can apply these directly to your DLP rules or copy them and customize the copies to create your own data classifications. Each of the built-in data classifications has a different set of built-in data identifiers associated with it. The four pre-defined data classifications are described in Built-In Data Classifications.

Create a Data Classification

Describes creating a data classification. You can create a data classification to help you monitor content with specific characteristics. Custom data classifications can be used in real time rules, SaaS API rules and discovery scans.

You can create a data classification to help you monitor content with specific characteristics. Custom data classifications can be used in real time rules, SaaS API rules and discovery scans.

The building blocks for data classifications are data identifiers. The data identifiers that you choose for a data classification determine the type of data for which rules using that data classification will scan.

Using the inclusion and exclusion options on the Data Classification page, you can fine-tune your classification to be more precise and reduce false positives. You can exclude specific terms and regular expression (regex) patterns by creating a custom identifier in the exclusion area, or by excluding a pre-existing built-in identifier.

The exclusion applies only to the content that's been matched, not to every document that meets the exclusion criteria.

For example, consider a data classification that targets the built-in identifier Health Condition and Person Name (US). You want to block instances of "John Smith cancer" while allowing instances of "John Smith cancer fundraising." To achieve this, you can craft a custom data identifier for "cancer fundraising" and set up an exclusion for this identifier within your data classification. As a result, matches for the Health Condition and Person Name (US) identifier will be flagged, except when the phrase "cancer fundraising" is present.

The system compares data identifiers selected for exclusion against both the keywords and the proximity terms of included data identifiers. If the Data Loss Prevention Report reveals that a particular rule or identifier is generating false positives, consider using terms and identifiers exclusion to remedy the situation.

> **Note**
>
> If you select a data identifier for both inclusion and exclusion, exclusion will take precedence.

The system offers built-in data identifiers that you can choose from.

Built-In Identifiers

These identify data using pattern matching and dictionary lookups. The descriptions shown in the GUI provide details about the type of data they match. For more information, see Built-In Data Identifiers.

The system offers three types of data identifiers you can create yourself applying different methods of data analysis:

Custom Identifiers

You can create custom identifiers to match specific terms and pattern expressions of your choosing. See Create a Custom Identifier.

Exact Data Match Identifiers

Exact Data Match Identifiers use fingerprinting to identify data in structured documents that match criteria you define. (See Create an Exact Data Match Identifier for more information.)

Indexed Document Match Identifiers

Indexed Document Match Identifiers use fingerprinting to identify data in unstructured documents that match criteria you define. See Create an Indexed Document Match Identifier for more information.

To delete or edit a data classification, see Delete or Edit a Classification.

Procedure

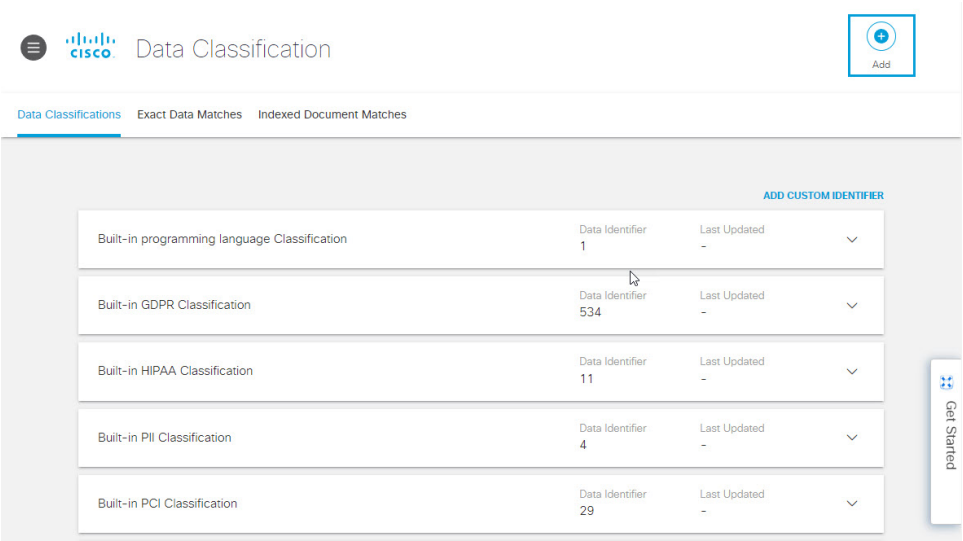
Provides instructions for procedure.

Before you begin

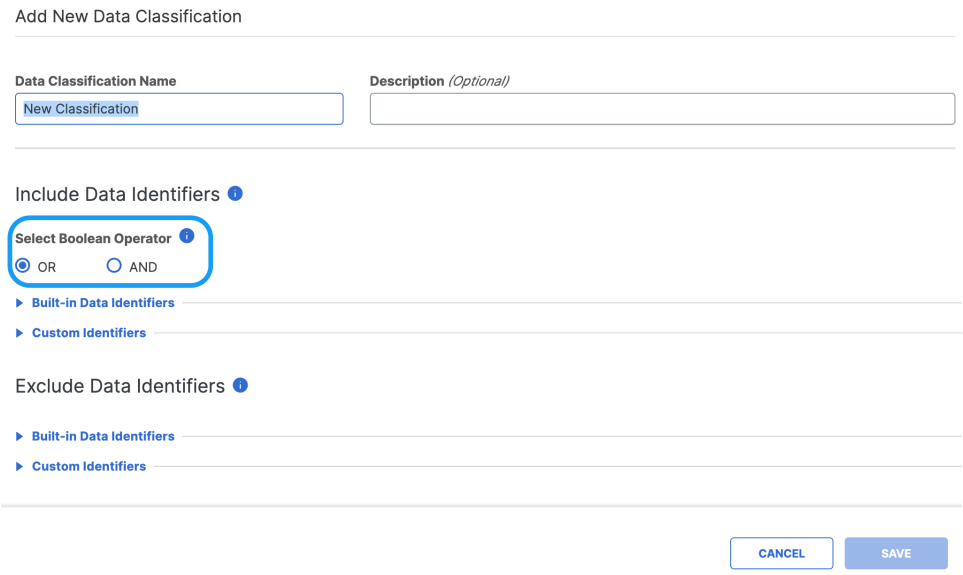
- Full Admin user role. For more information, see Manage Accounts.

Procedure

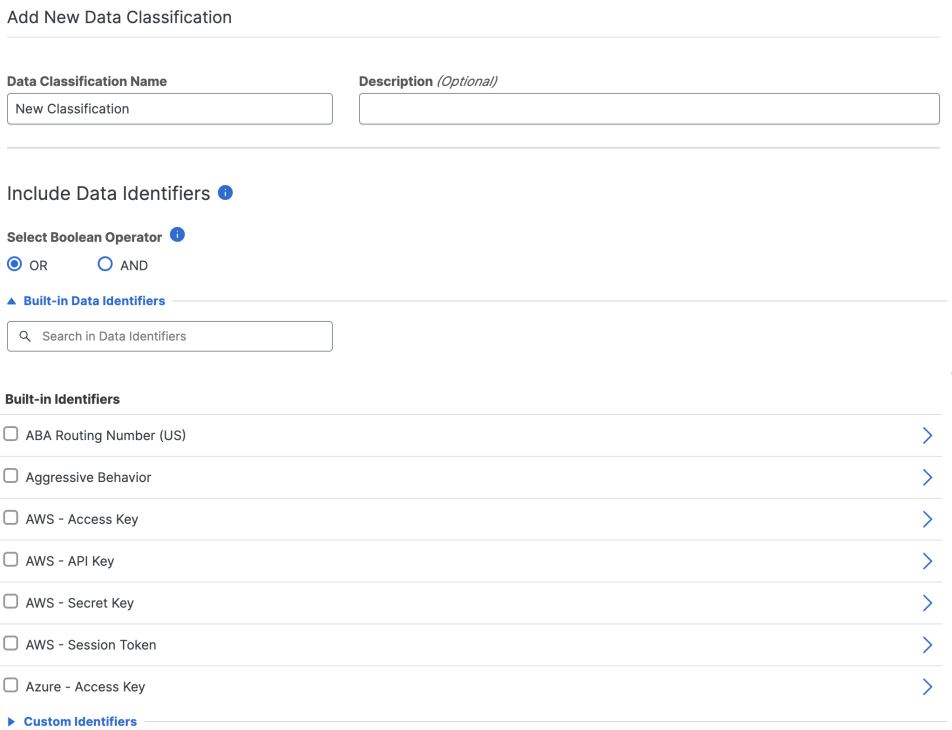
1. Navigate to **Secure** > **Settings** > **Data Classification** and click **Add**.



2. Give your classification a meaningful name and description.
3. Under **Include Data Identifiers**, select a Boolean operator to separate the identifiers included in the classification.
   - **OR**–At least one of the data identifiers included must match during rule evaluation.
   - **AND**–All of the data identifiers included must match during rule evaluation.



4. Under **Include Data Identifiers**, expand **Built-in Data Identifiers** and select data identifiers to include in the data classification.



5. Under **Include Data Identifiers**, expand **Custom Identifiers** and select custom identifiers to include in the data classification.

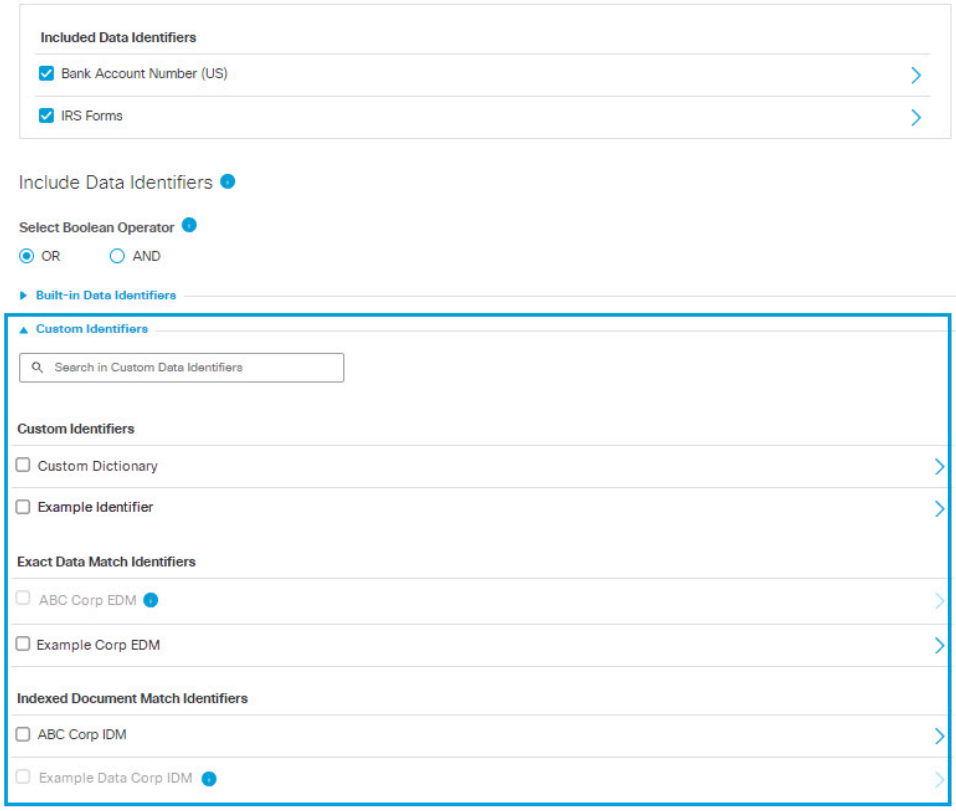
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

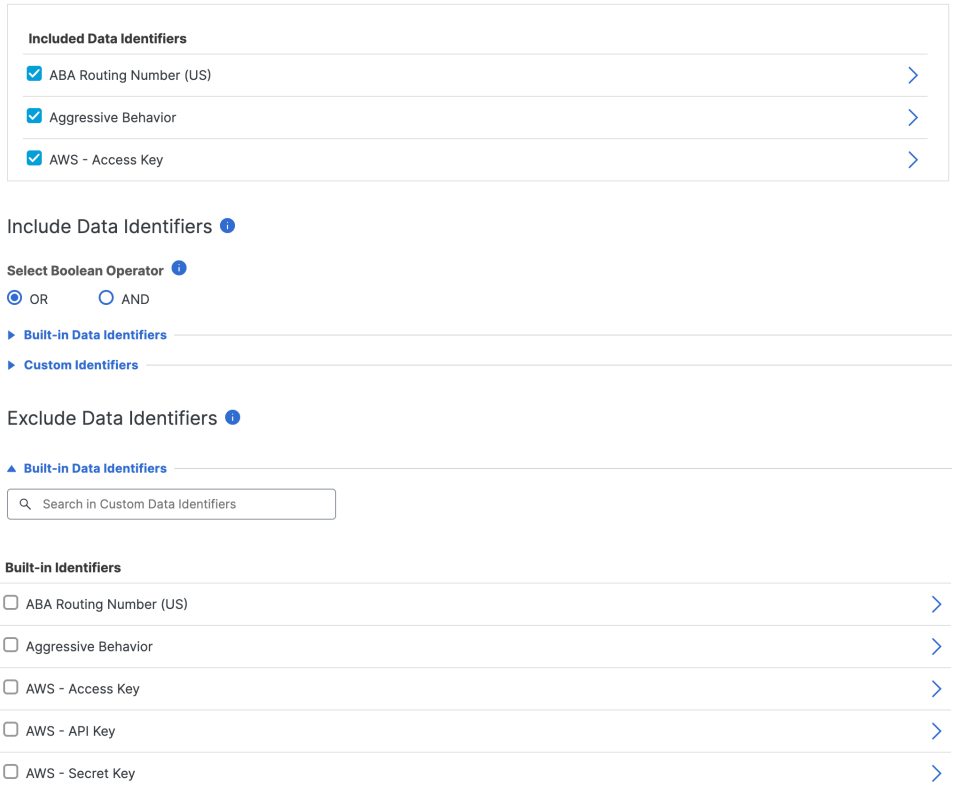
     > **Note**
     >
     > Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

   - Indexed Document Match Identifiers

> **Note**
>
> Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)



6. Under **Exclude Data Identifiers**, expand **Built-in Data Identifiers** and choose data identifiers to exclude from the data classification.



7. Under **Exclude Data Identifiers**, expand **Custom Identifiers** and choose custom data identifiers to exclude from the data classification.

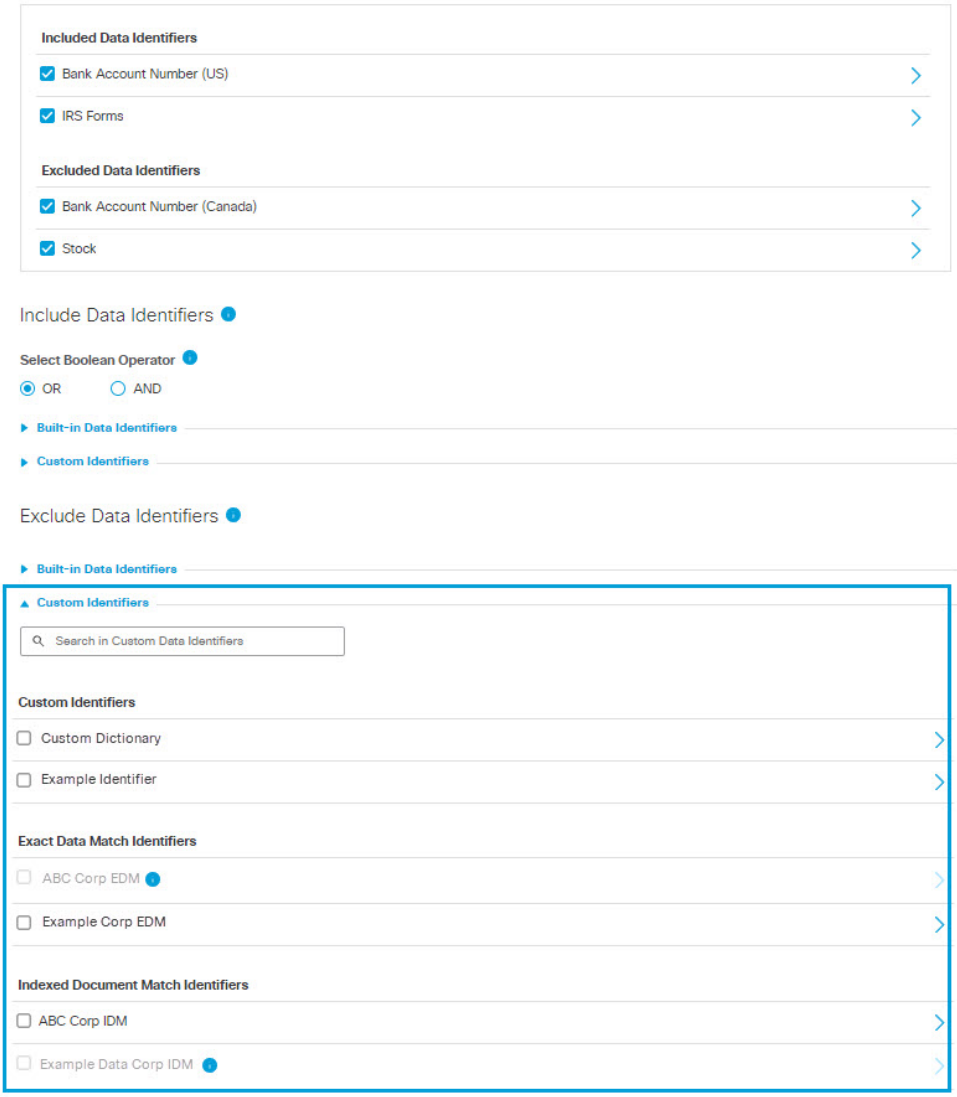
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

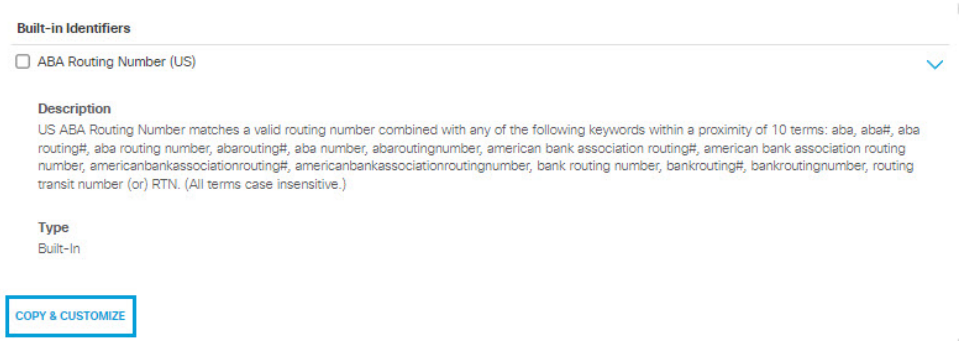
     > **Note**
     >
     > Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

   - Indexed Document Match Identifiers

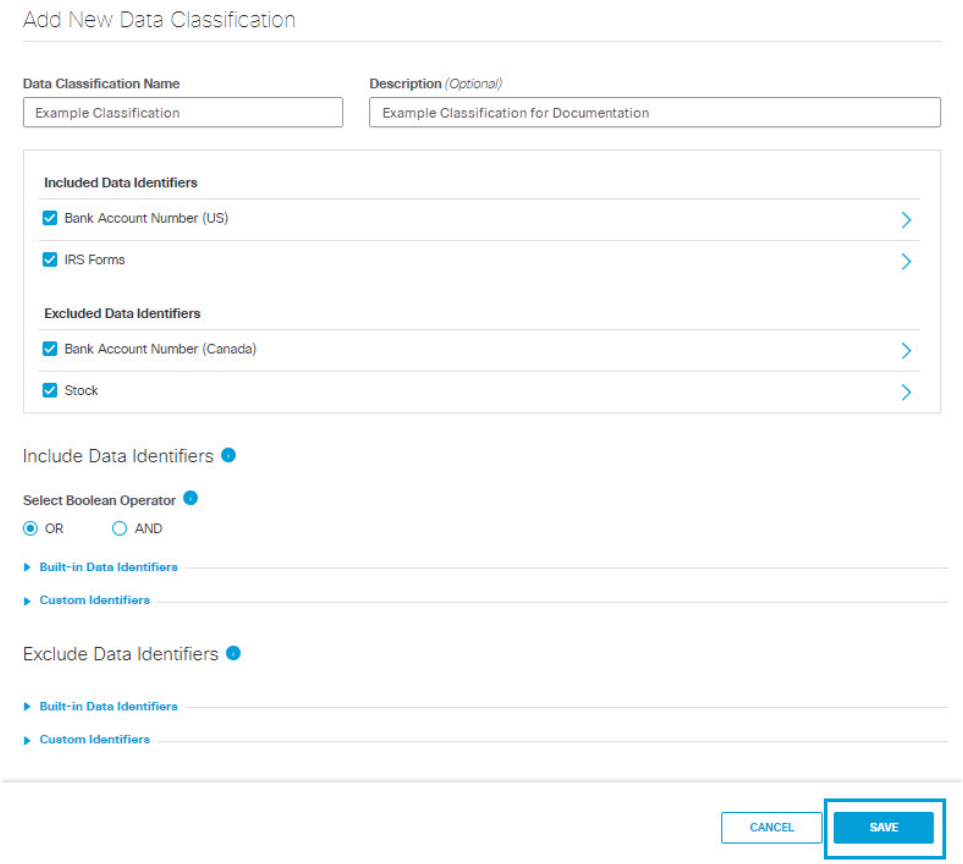
> **Note**
>
> Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)



8. You may expand any built-in data identifier and click **COPY & CUSTOMIZE** to create a new customized data identifier. See Copy and Customize a Data Identifier.



9. Click **Save**.



What to do next

Your new classification is listed on the Data Classification page, and will be available to you when you Add a Real Time Rule to the Data Loss Prevention Policy, Add a SaaS API Rule to the Data Loss Prevention Policy, or initiate a new Discovery Scan.

Copy and Customize a Data Identifier

Describes copy and customize a data identifier. The system provides four different built-in data classifications you can use in real time rules, SaaS API rules, and discovery scans. These are:

The system provides four different built-in data classifications you can use in real time rules, SaaS API rules, and discovery scans. These are:

PII Data Classification

Personal Information Identifiers; data that includes any personal information that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers.

PCI Data Classification

Data related to the Payment Card Industry.

GDPR Data Classification

Common personal data associated with the European Union's General Data Protection Regulation. Customers can use these identifiers to support GDPR compliance within their organizations.

HIPAA Data Classification

Personal medical and healthcare data associated with the United States' Health Insurance Portability and Accountability Act. Customers can use these identifiers to support HIPAA compliance within their organizations.

For more details on each of these built-in data classifications, see Built-In Data Classifications. You can create custom data classifications based on any of these built-in data classifications. Simply copy the desired built-in classification, make changes to the copy, and save it as a custom data classification.

The building blocks for data classifications are data identifiers. The data identifiers selected for a data classification determine the type of data for which rules using that data classification will scan. Built-in data classifications have data identifiers already selected for them; you can produce your own customized versions of these classifications by removing selected identifiers or adding other identifiers.

Using the inclusion and exclusion options on the Data Classification page, you can fine-tune your classification to be more precise and reduce false positives. You can exclude specific terms and regular expression (regex) patterns by creating a custom identifier in the exclusion area, or by excluding a pre-existing built-in identifier.

The exclusion applies only to the content that's been matched, not to every document that meets the exclusion criteria.

For example, consider a data classification that targets the built-in identifier Health Condition and Person Name (US). You want to block instances of "John Smith cancer" while allowing instances of "John Smith cancer fundraising." To achieve this, you can craft a custom data identifier for "cancer fundraising" and set up an exclusion for this identifier within your data classification. As a result, matches for the Health Condition and Person Name (US) identifier will be flagged, except when the phrase "cancer fundraising" is present.

The system compares data identifiers selected for exclusion against both the keywords and the proximity terms of included data identifiers. If the Data Loss Prevention Report reveals that a particular rule or identifier is generating false positives, consider using terms and identifiers exclusion to remedy the situation.

> **Note**
>
> If you select a data identifier for both inclusion and exclusion, exclusion will take precedence.

The system offers two types of built-in data identifiers you can choose to remove from or add to your customized version of a built-in data classification:

- Built-In Identifiers

  These identify data using pattern matching and dictionary lookups. The descriptions shown in the GUI provide details about the type of data they match. For more information, see Built-In Data Identifiers.

The system offers three types of data identifiers you can create yourself applying different methods of data analysis. You can add these to your customized version of a built-in data classification:

- Custom Identifiers

  You can create custom identifiers to match specific terms and pattern expressions of your choosing. See Create a Custom Identifier .

- Exact Data Match Identifiers

  Exact Data Match Identifiers use fingerprinting to identify data in structured documents that match criteria you define. (See Create an Exact Data Match Identifier for more information.)

- Indexed Document Match Identifiers

  Indexed Document Match Identifiers use fingerprinting to identify data in unstructured documents that match criteria you define. See Create an Indexed Document Match Identifier for more information.

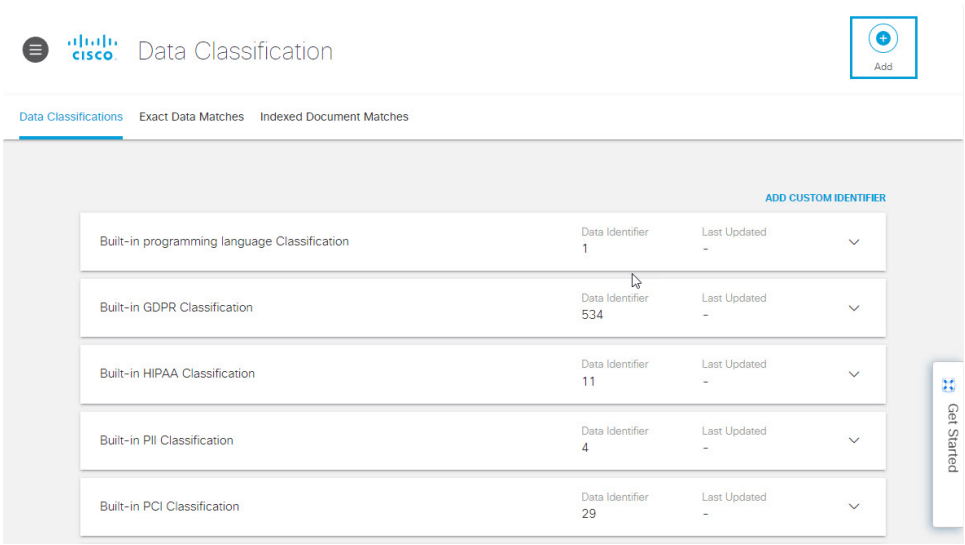
To delete or edit a data classification, see Delete or Edit a Classification.

Procedure

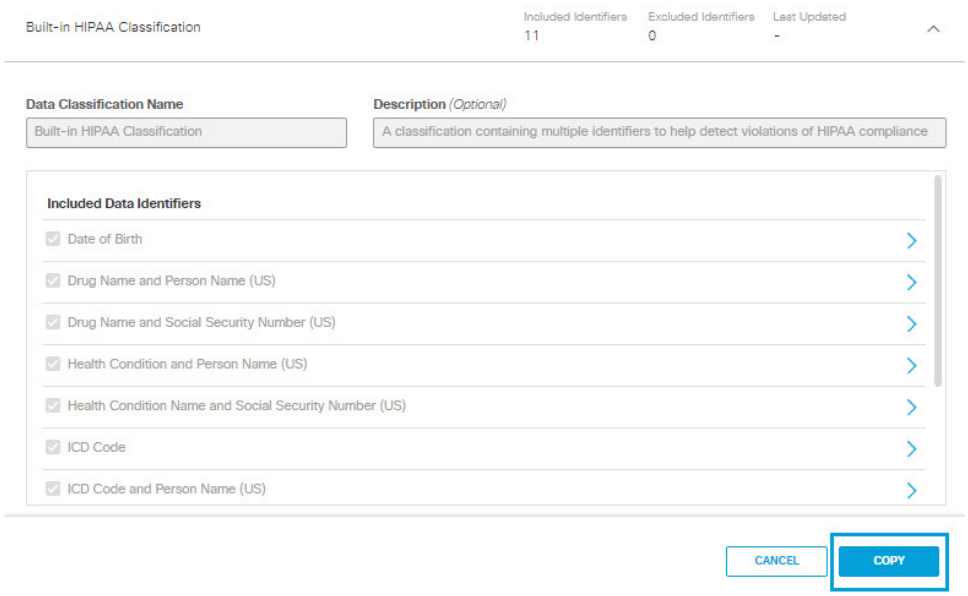
Provides instructions for procedure.

Procedure

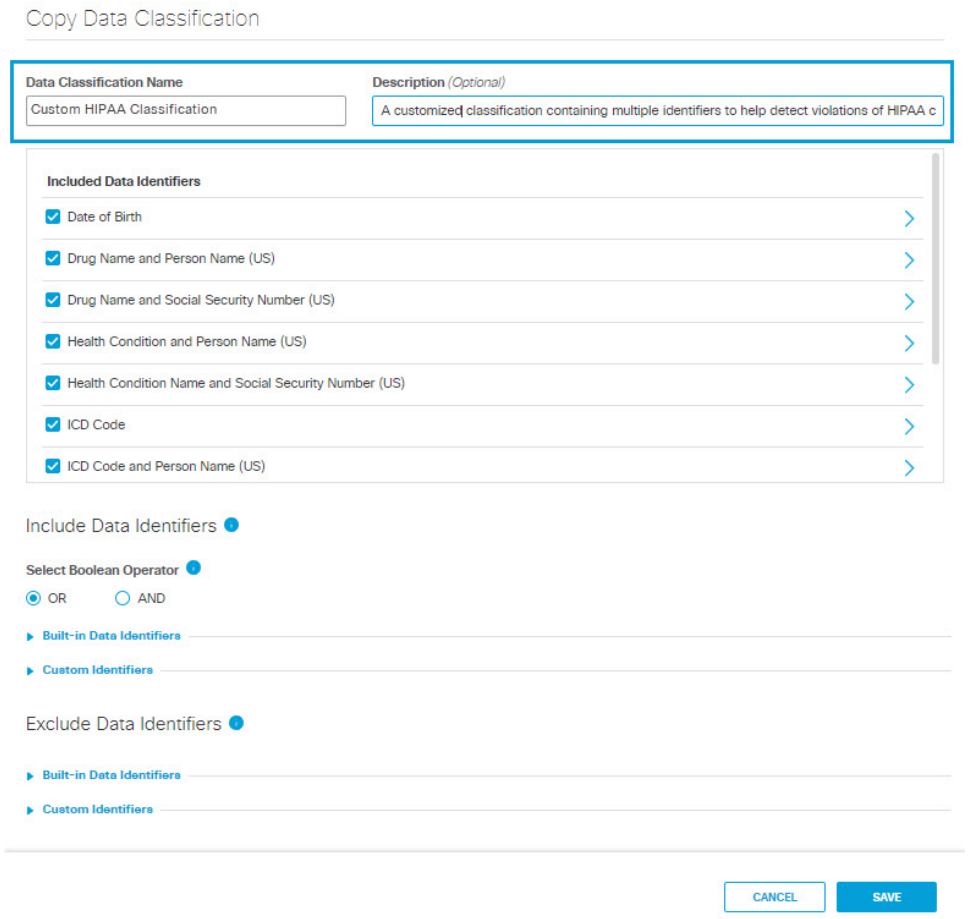
1. Navigate to **Secure** > **Settings** > **Data Classification**.



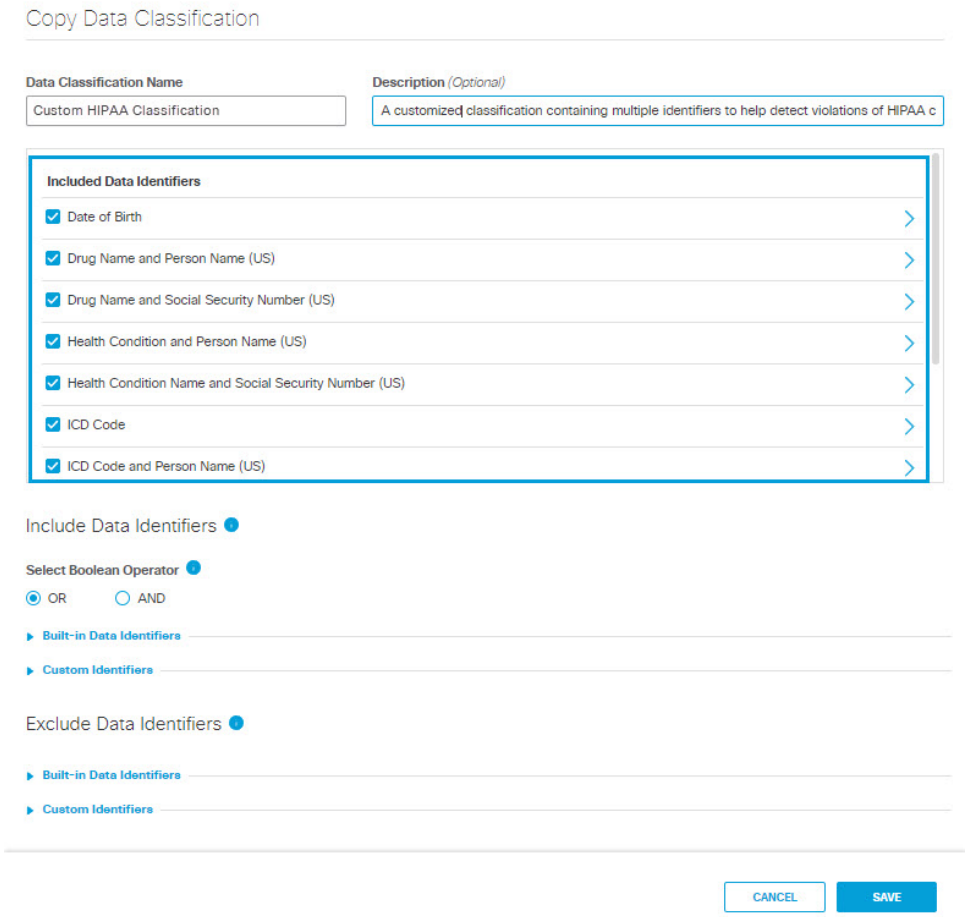
2. Expand one of the built-in data classifications and click **Copy**.



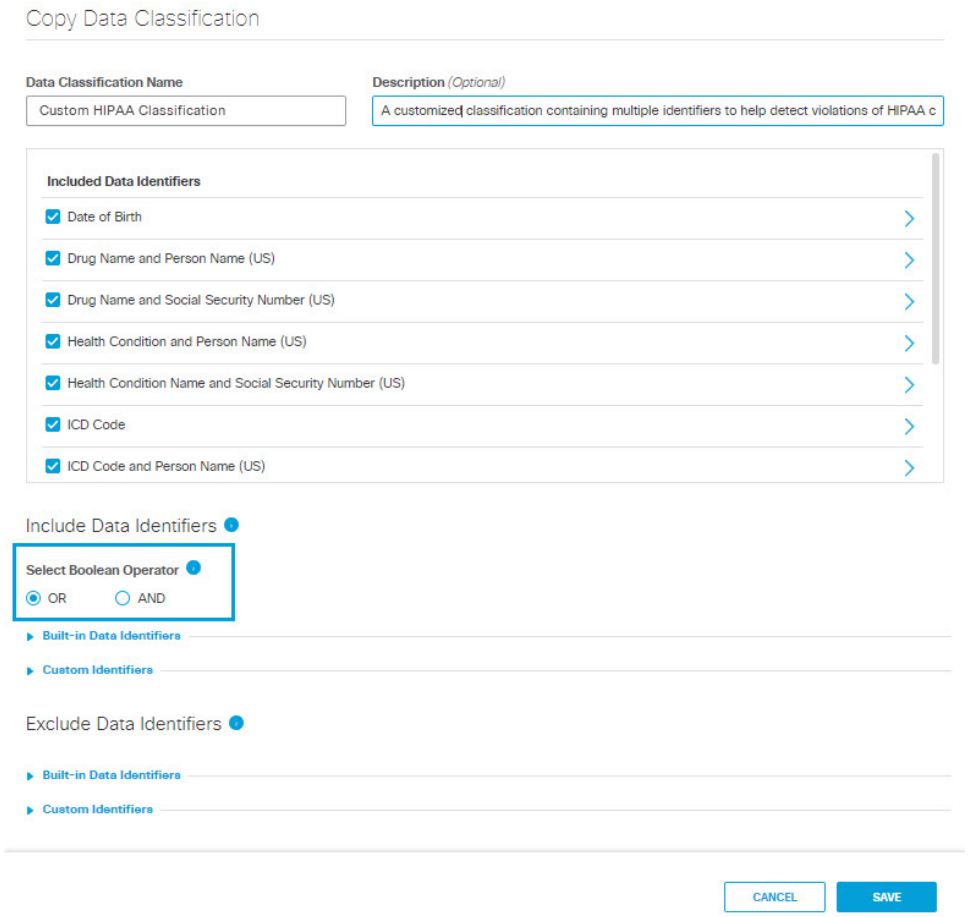
3. Give the new data classification a meaningful name and description.



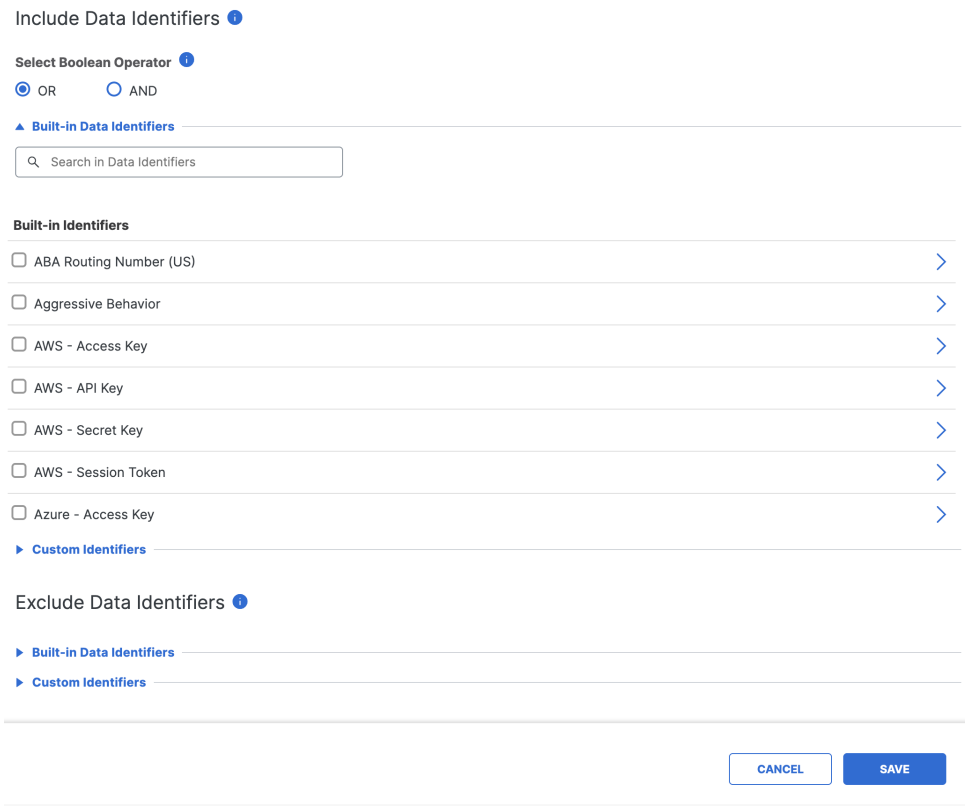
4. Under **Included Data Identifiers** deselect pre-selected data identifiers as needed.



5. Under **Include Data Identifiers**, you may change the Boolean operator to separate the identifiers included in the classification:
   - **OR**–At least one of the data identifiers selected must match during rule evaluation.
   - **AND**–All of the data identifiers selected must match during rule evaluation.



6. Under **Include Data Identifiers** expand **Built-in Data Identifiers** and select additional data identifiers to include in the data classification.



7. Under **Include Data Identifiers** expand **Custom Identifiers** and select custom data identifiers to include in the data classification.

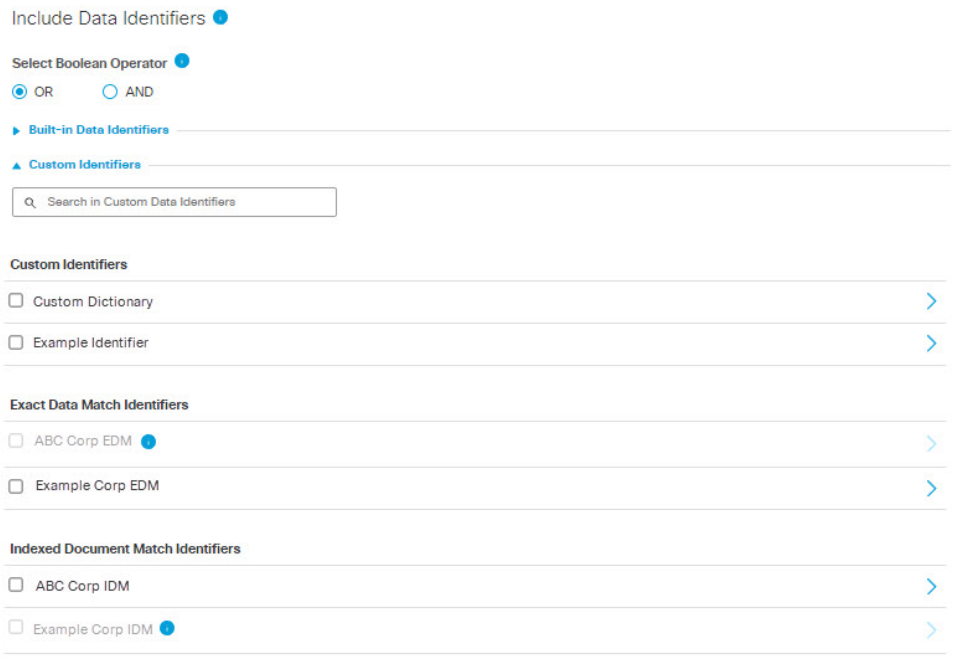
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

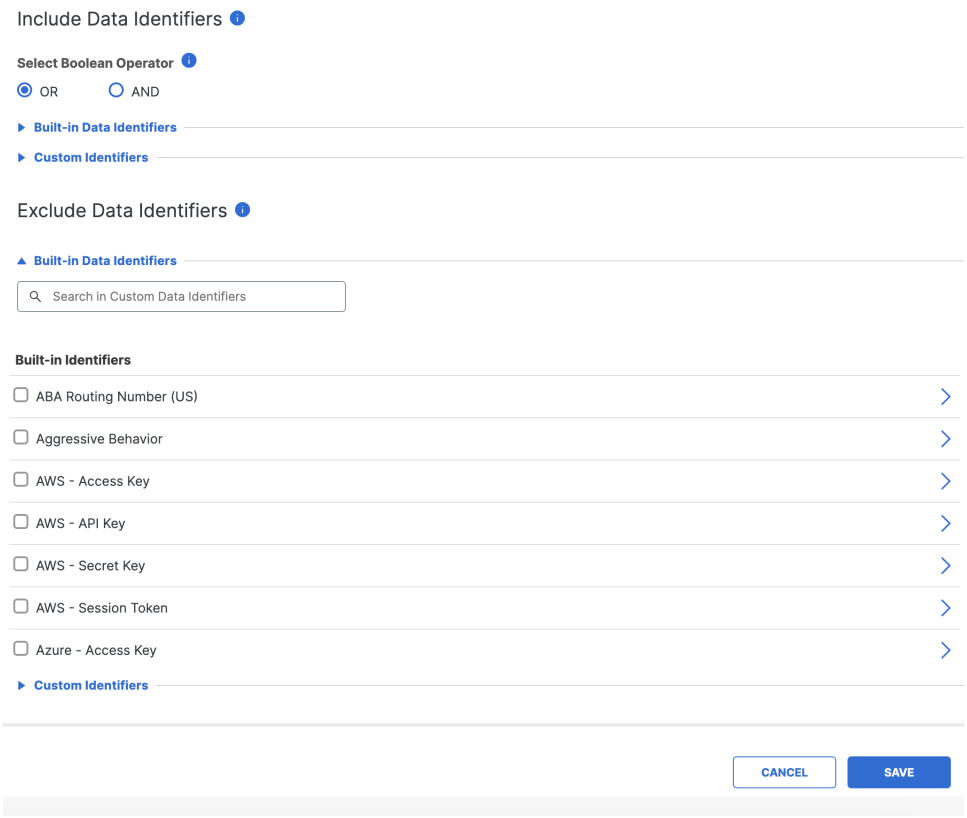
     > **Note**
     >
     > Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

   - Indexed Document Match Identifiers

> **Note**
>
> Index Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)



8. Under **Exclude Data Identifiers**, expand **Built-in Data Identifiers** and choose data identifiers to exclude from the data classification.



9. Under **Exclude Data Identifiers**, expand **Custom Identifiers** and choose custom data identifiers to exclude from the data classification.

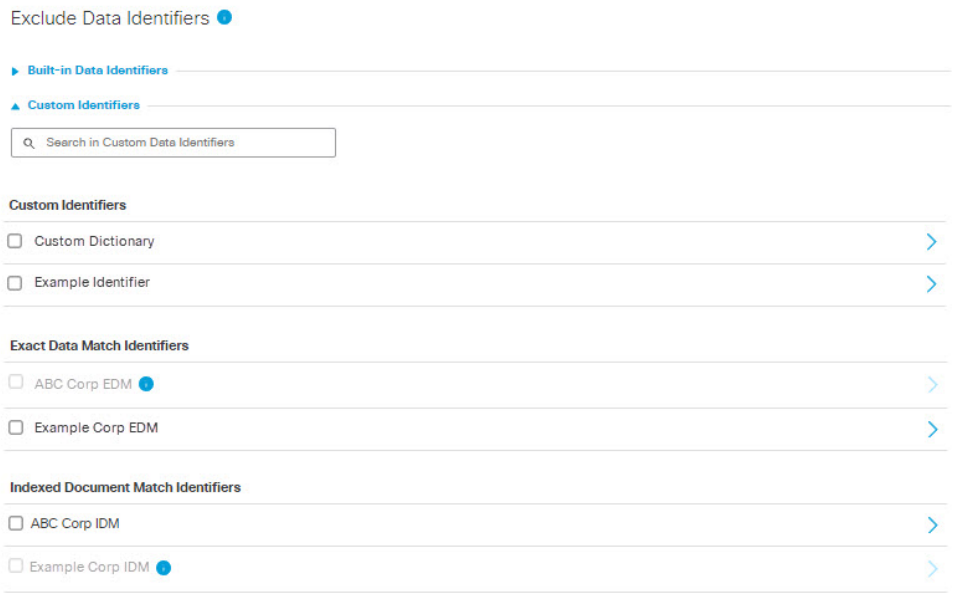
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

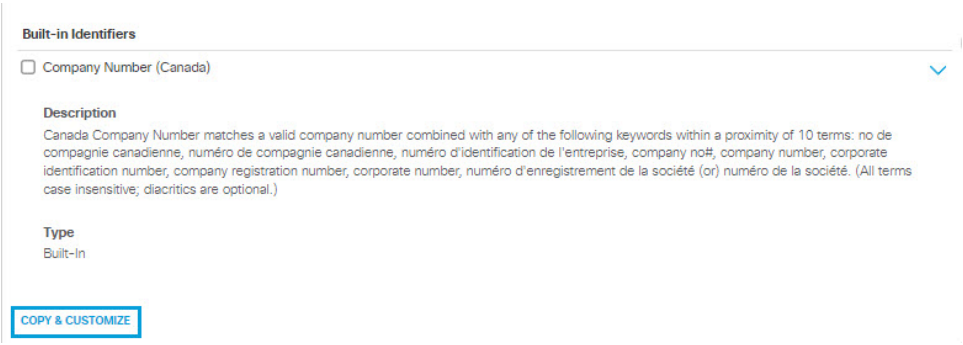
     > **Note**
     >
     > Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

   - Indexed Document Match Identifiers

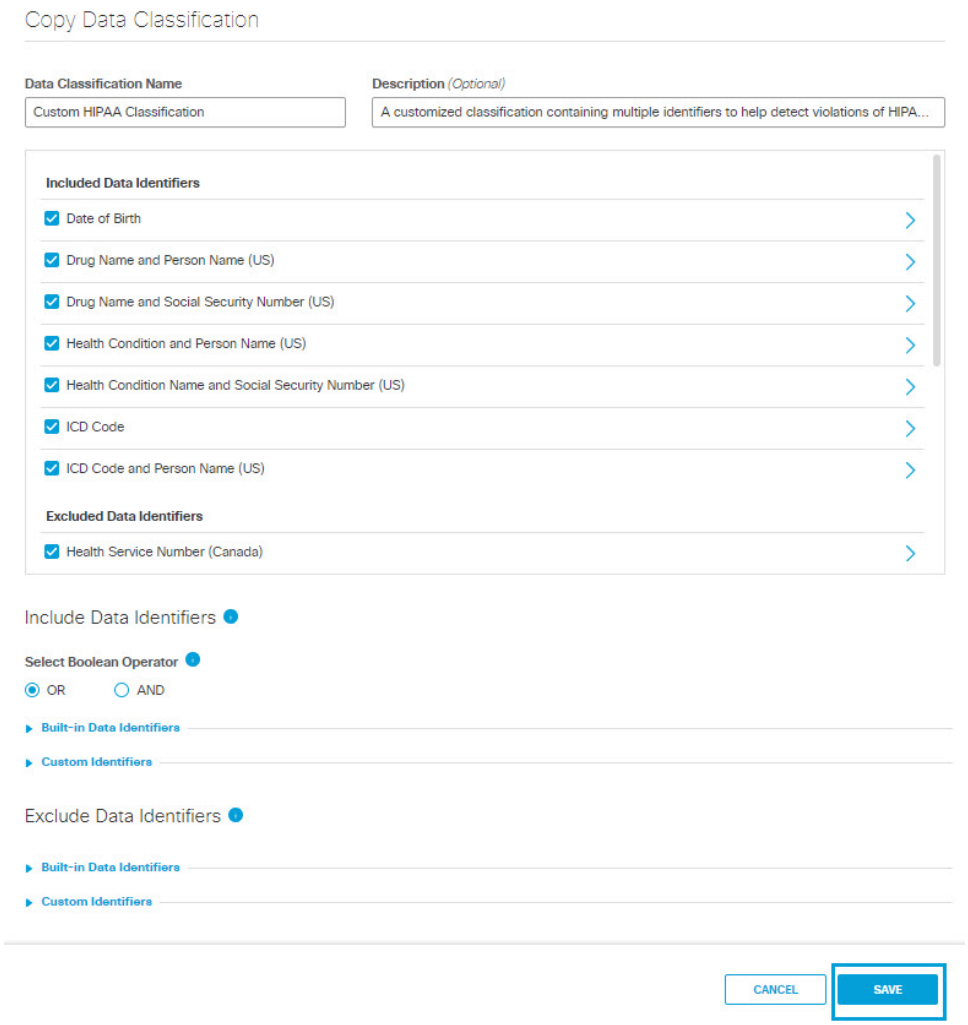
> **Note**
>
> Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)



10. You may expand any built-in data identifier and click **COPY & CUSTOMIZE** to create a new customized data identifier. See Copy and Customize a Data Identifier.



11. Click **Save**.



What to do next

Your new classification is listed on the Data Classification page, and will be available to you when you Add a Real Time Rule to the Data Loss Prevention Policy, Add a SaaS API Rule to the Data Loss Prevention Policy, or initiate a new Discovery Scan.

Delete or Edit a Classification

Describes deleting or edit a classification. After adding a data classification, you can delete or edit it at any time. To add a data classification, see Add a Data Classification or Copy and Customize a Built-In Data Classification.

After adding a data classification, you can delete or edit it at any time. To add a data classification, see Add a Data Classification or Copy and Customize a Built-In Data Classification.

> **Note**
>
> You cannot edit or delete a built-in data classification.

- Edit a Classification
- Delete a Classification

Delete a Classification

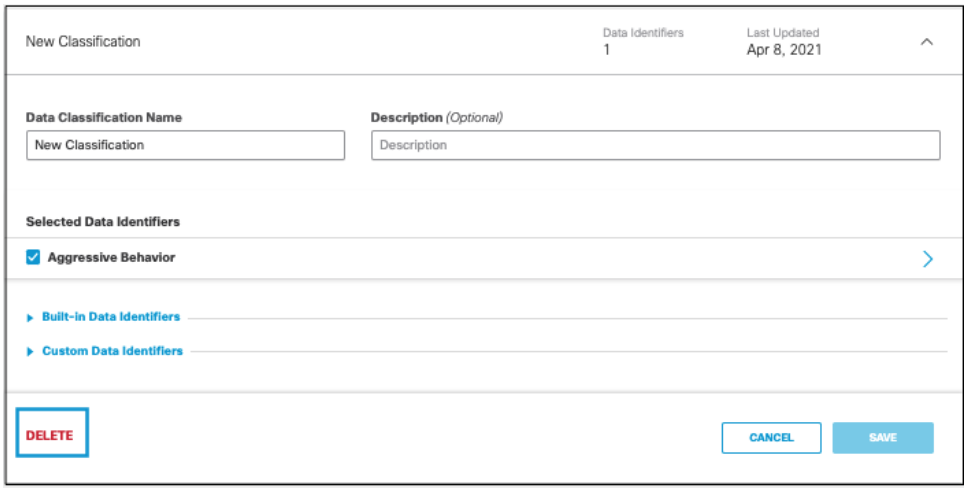
Provides instructions for deleting a classification.

Before you begin

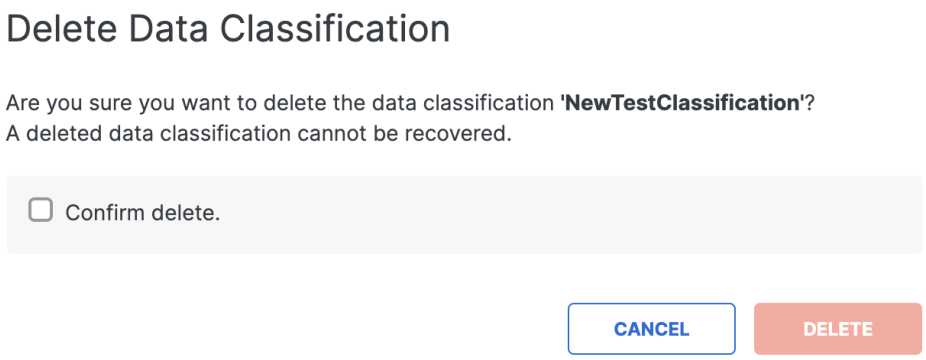
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Settings** > **Data Classification**.
2. Expand a data classification and click **Delete**.



3. Confirm deleting the classification and then click **Delete**.



Edit a Classification

Provides instructions for editing a classification. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

> **Note**
>
> You may not edit a built-in data classification.

Procedure

1. Navigate to **Secure** > **Settings** > **Data Classification**.
2. Expand a data classification.
3. Edit the data classification as needed and click **Save**.

Create an Exact Data Match Identifier

Describes creating an exact data match identifier. Exact Data Matching (EDM) is a data classification and matching technique that effectively detects data loss incidents involving sensitive records maintained and stored in a structured data format.

Exact Data Matching (EDM) is a data classification and matching technique that effectively detects data loss incidents involving sensitive records maintained and stored in a structured data format. EDM is designed to help protect sensitive data by fingerprinting data instead of leveraging pattern matching techniques.

Umbrella performs Exact Data Matching using an EDM template, which you create by uploading a plain text CSV file that describes the fields to be matched, and choosing an EDM type for each field described in the CSV file. You must also specify which fields are required for a match, and their priority. Once the EDM template is created, you will obtain an ID for it from the Umbrella UI.

You must then download the DLP indexer and run the indexer against your data records using the EDM template. The DLP indexer validates records against the template and generates hash fingerprints for those records, creating an EDM.

Once you have run the indexer, you will have an Exact Data Match Identifier associated with the documents. You will then be able to:

1. Create a Data Classification that uses the EDM as a custom data identifier (as described in Create a Data Classification or Copy and Customize a Built-In Data Classification).
2. Create a DLP rule that uses the Data Classification including that EDM Identifier. (For more information on DLP rules, see Manage the Data Loss Prevention Policy.)

With these configurations in place, Secure Access will be able to monitor and/or block transmission of structured files containing records that match your indexed data. Matching records meet the criteria you establish when you create the EDM template.

Procedure

Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. JVM version 17+ The template CSV you upload must meet the following requirements: The file can not be larger than 10 KB.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- JVM version 17+
- The template CSV you upload must meet the following requirements:
  - The file can not be larger than 10 KB.
  - The second and ensuing rows may contain sample data; be aware, however, that this data will not be indexed unless it also appears in the source data CSV file.
- The DLP indexer supports data files with up to 55 million records. The exact records limit is determined by the total number of columns and the number of those are of Alphanumeric type. The indexer displays the exact limit when attempting to load a file that exceeds it. If your dataset is larger than the limit, you need to split the records into multiple files.
- Both the template and source data CSV files must meet the following requirements:
  - The file name must not include space characters.
  - A multi-term (multi-word) field can contain a maximum of 6 space-separated words.
  - The data file must contain only 1 byte or 2 byte UTF-8 encoded characters.
  - The first row of data must have between 1 and 50 fields and each row must have the same number of fields.
  - The first row of data must specify the name of each field, and each value must be unique.
  - Data in the second and ensuing rows must comply with the EDM field types and supported formats (see Exact Data Match Field Types).
  - The field names in the sample data template must match the field names in the actual data source file. The field names must appear in the same order in both files.

Caution

Do *not* create, edit, or view the template or source data CSV file using Microsoft Excel, as this may corrupt the file. Use a text editor.

Note

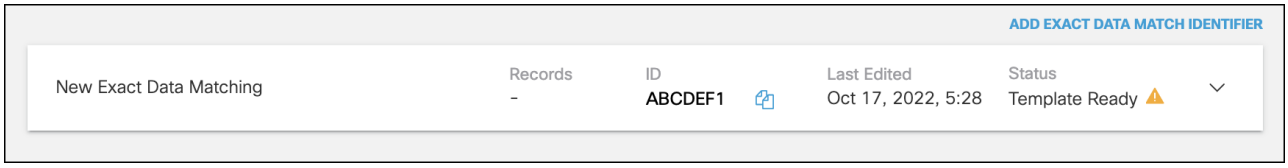
If any of the values provided in the source file to the DLP indexer fail to be validated as per the supported format, then the DLP indexer will skip that record and proceed with indexing the remaining records. The indexer also behaves in this manner for any records that may exceed the template-defined fields, and for empty rows or records with empty primary values. The position of the skipped records in the file will be provided as part of the output of the DLP indexer.

The following procedure uses the following example CSV file for both the template and indexed source data:

```
Email,SSN,Passport number - US,Credit card number
r_t@gmail.com, 113011111,123456789USA1234567U1234567, 5205105105105109
r_ppp@gmail.com, 248257990,123456789USA1234567U1234567, 4532237384050172
r_opop@gmail.com, 363265019,123456789USA1234567U1234567, 4532549977031249
ppo_t@gmail.com, 417279936,123456789USA1234567U1234567, 4539157470627290
```

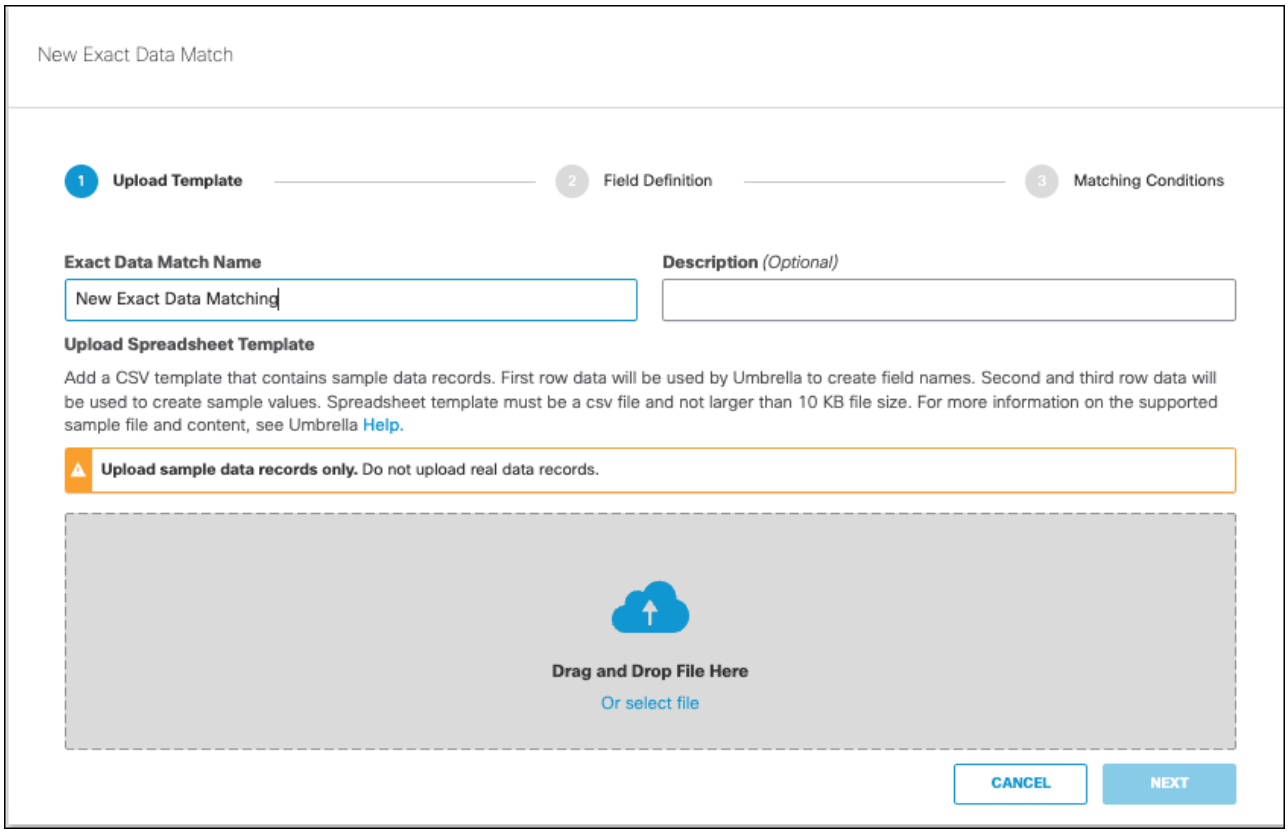
Procedure

1. Navigate to **Secure** > **Settings** > **Data Classification** > **Exact Data Matches** and click **Add Exact Data Match Identifier**.



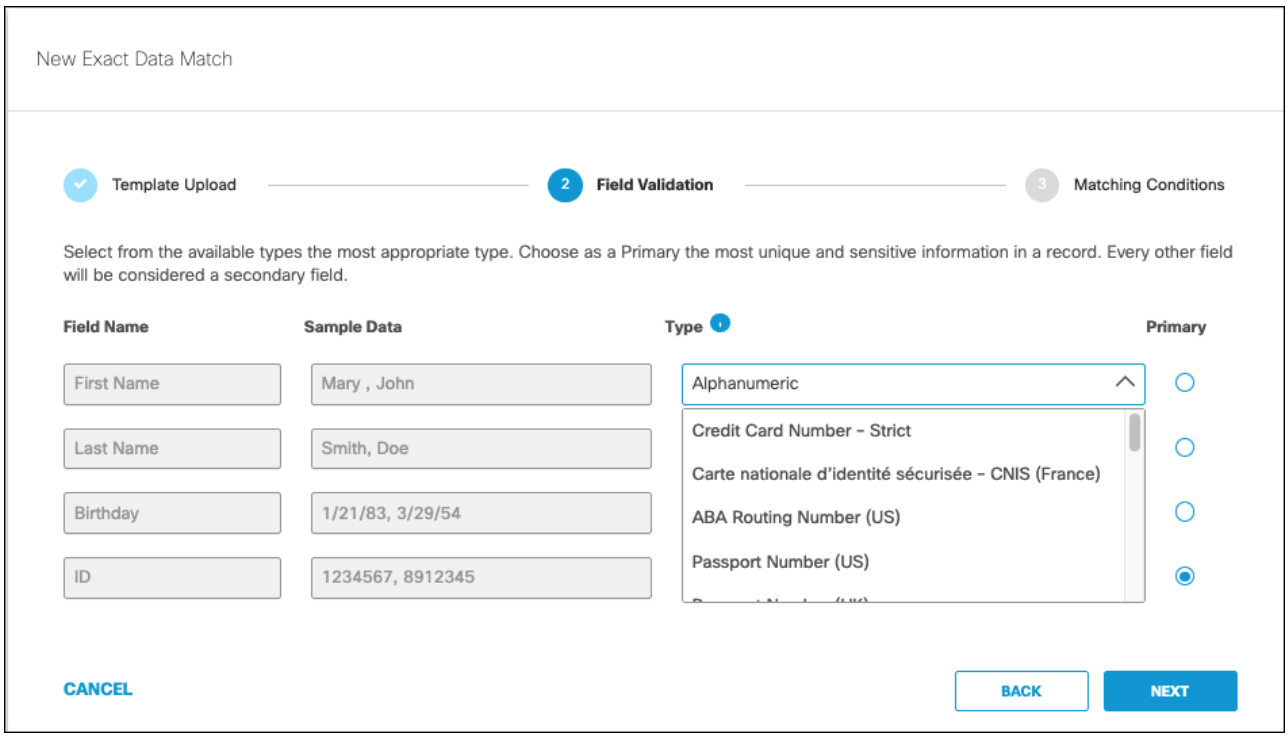
2. Provide a name and description for the exact data match, then upload sample data and click **Next**.

> **Note**
>
> Do not upload any real data in the CSV. Use only sample data.



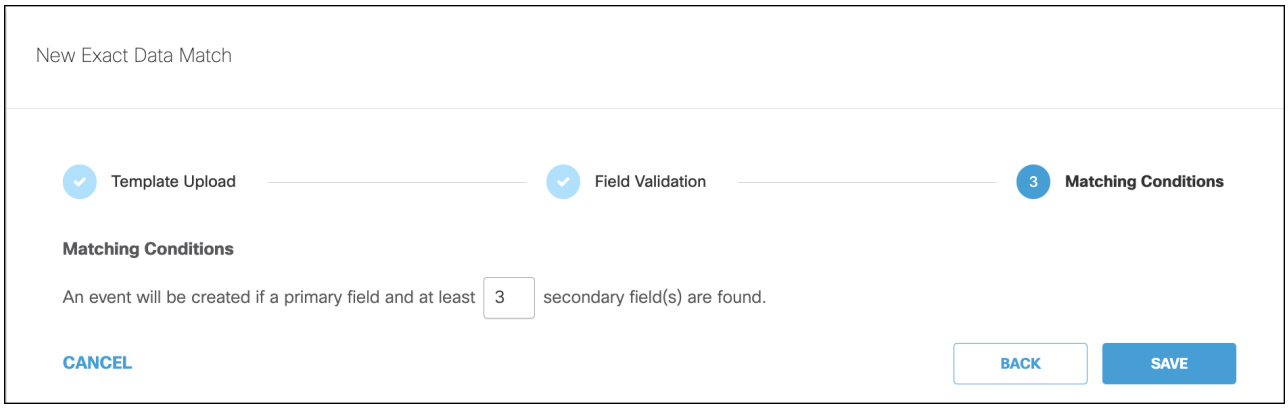
3. From the drop-down menu, choose the type of data of each field.

   The available field types are described in Exact Data Matcher Types:



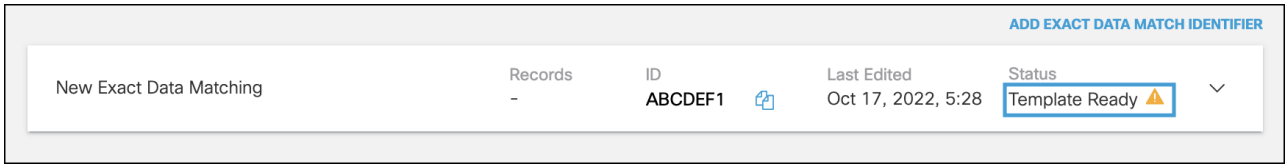
4. Select the Primary field that must be found with other data fields for the identifier to match and click **Next**. The primary field should be the field in the record to always match. The secondary fields are the number of fields in the record that should be present with the primary field to match.
5. Enter the minimum number of secondary fields required to be found within 10 terms of the primary field for a match. You can have no secondary field, or up to as many fields in the record that are not the primary field. For example, if at least 3 secondary fields are required, then the identifier will only trigger an event when 3 or more additional fields are found with the primary field. If the .csv file has only 1 column, then the secondary option is greyed-out and automatically set to 0. Click **Save**.

> **Note**
>
> The secondary fields must each be a different identifier.

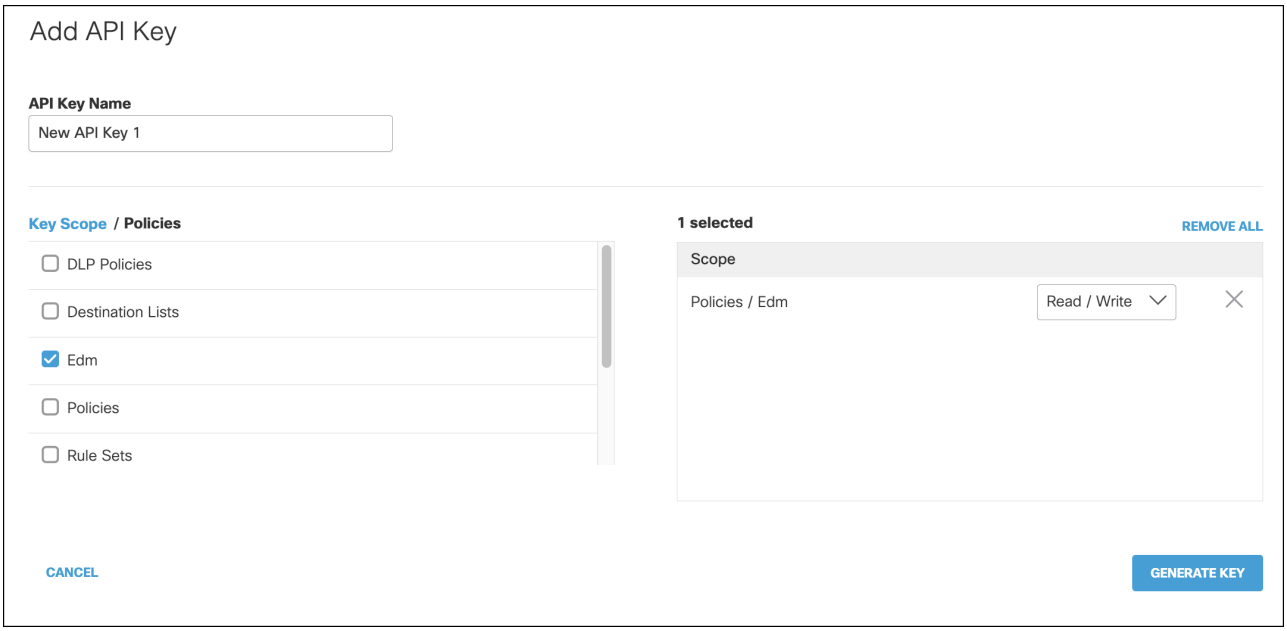


The exact data matcher now has a status of **Template Ready**.

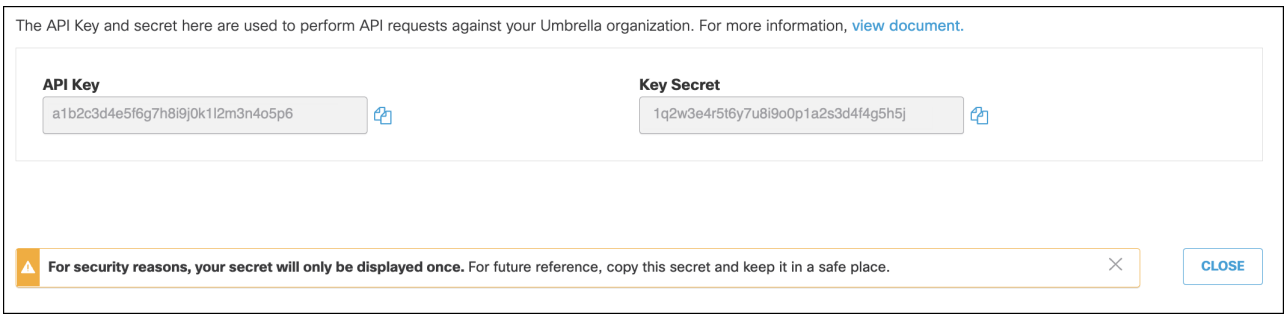
> **Note**
>
> **Note**: When the EDM is **Template Ready**, you can edit the field types, the primary field selection, and the matching conditions. It can not be added to a data classification.



6. Create an API key and secret for the EDM data indexer.
   a. Navigate to **Admin** > **API Keys** and click **Open API Keys**.
   b. Click **Add** and provide a name for the API Key.
   c. Select **Policies** > **Exact Data Matching** for the scope and choose **Read/Write** for the permissions. Then click **Generate Key**.



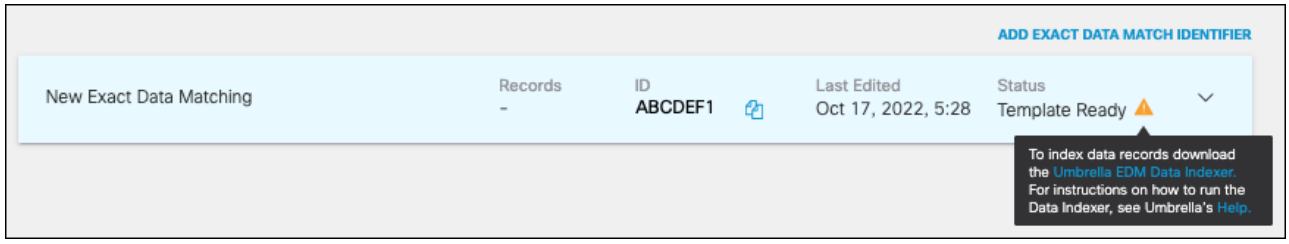
   d. Copy and save the API Key and Secret somewhere safe, as you will need it in the EDM Indexer.



7. Use the Secure Access EDM Indexer to index your data records. For more information on the indexer, see Index Data for an EDM on page 627.

a. Navigate to **Policy** > **Policy Components** > **Data Classification** > **Exact Data Matching**, hover on the **Template Ready** icon, and click **Umbrella EDM Data Indexer** to download the indexer.

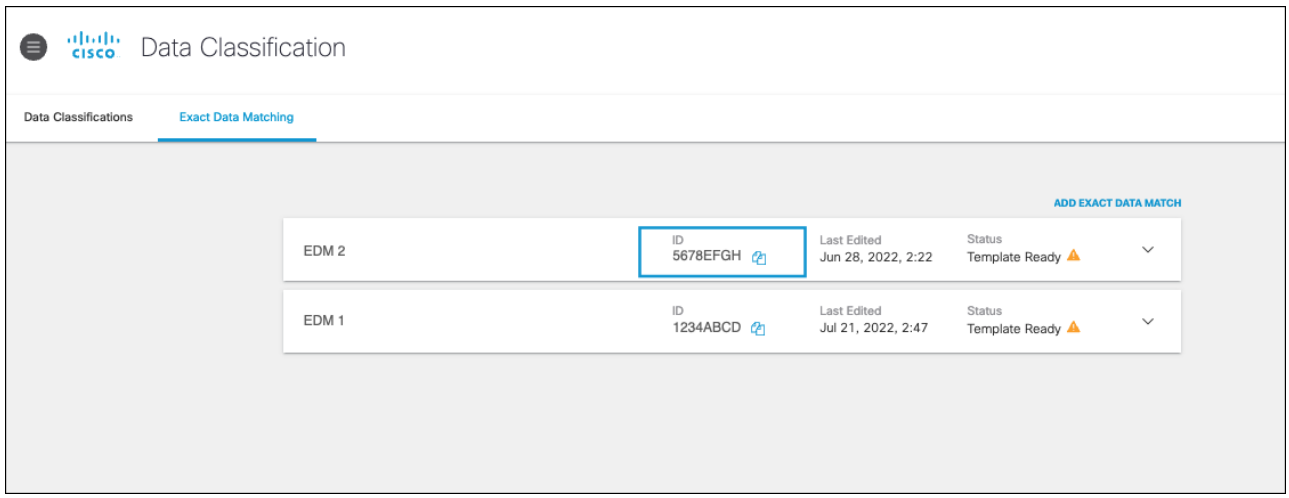
> **Note**
>
> The indexer should be downloaded locally to the root folder of the device where the data records are stored. The indexer and data records should be located under the same directory.



b. Run the indexer in a terminal window (on the same device where the indexer is saved) with the following command: `java -jar edm-lander.jar -i <source_file.csv> -e <edm_template_id> -k <authKey> -s <authSecret>` where:

- **<source_file.csv>**–the relative path to the csv spreadsheet with the actual data records
- **<edm_template_id>**–the ID of the EDM identifier retrievable from Umbrella UI.
- **<authkey>**–the API Key generated at Step 6d.
- **<authsecret>**–the API Secret generated at Step 6d.

> **Note**
>
> If the source file size is smaller than 500KB, the memory allocated to Java will default to 1GB and this switch is not needed.



The EDM Identifier now has a status of **Data Indexed**.

> **Note**
>
> When the EDM has a status of **Data Indexed**, you can add the EDM to a data classification but you can not edit the field types, primary field selection, or matching condition.

If you update your source file with new or changed records, you need to run the DLP indexer again on that file using the same EDM Identifier ID, API Key, and API Secret. This ensures that policies configured to use the EDM Identifier are updated to reflect the new data fingerprints. For more information, see Update the Indexed Data Set Periodically on page 630.

Index Data for an EDM

Describes index data for an edm. The DLP indexer creates irreversible fingerprints of critical data structured in records with a consistent format and uploads them to Secure Access to establish a custom Exact Data Matching (EDM) Identifier.

The DLP indexer creates irreversible fingerprints of critical data structured in records with a consistent format and uploads them to Secure Access to establish a custom Exact Data Matching (EDM) Identifier. EDM Identifiers enable Secure Access to protect sensitive data by using data fingerprinting techniques as opposed to pattern matching techniques.

EDM Identifiers can be added to a Data Classification (see Manage Data Classifications) as custom identifiers; DLP rules that use these identifiers can monitor and/or block files that match the data you have indexed.

You need to run the DLP indexer in two different circumstances:

- When you initially create an EDM Identifier, you run the indexer on the data set you want to detect. This topic provides basic information for running the indexer, but for a description of the process to use the indexer within the context of creating an EDM Identifier, see Create an Exact Data Match Identifier. You cannot use the indexer to create an EDM Identifier without also performing the steps described in that topic.
- When the data set to be detected changes, you run the indexer to produce an updated version of the EDM Identifier. This process is described in Update the Indexed Data Set Periodically.

> **Note**
>
> To see a summary of the indexer options available, invoke the indexer with the **-h** option. (**java -jar <*directory-path*>\dlp-indexer.jar -h**.)

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- JVM version 17+
- You must download the indexer using the Secure Access GUI. See Step 6 in Create an Exact Data Match Identifier.
- Before running the DLP indexer you must generate an API Key and Secret using the Secure Access GUI. See Step 8 in Create an Exact Data Match Identifier.

> **Note**
>
> If you already have a key and secret generated for use with a previous run of the DLP indexer, you may use those.

- The indexer supports indexing source files with up to 55 million records. The exact records limit is determined by the total number of columns and how many of those are of alphanumeric type. The indexer will report the exact limit when attempting to load a file that exceeds it. If your dataset is larger than the limit, you need to split the records into multiple files. For errors received when indexing a large file, see Memory Tuning for DLP Exact Data Matching Indexer.
- The source data CSV file you index must meet the following requirements:
  - A multi-term (multi-word) field can contain a maximum of 6 space-separated words.
  - The data file must contain only 1 byte or 2 byte UTF-8 encoded characters.
  - The first row of data must have between 1 and 50 fields and each row must have the same number of fields.
  - The first row of data must specify the name of each field, and each value must be unique.
  - Data in the second and ensuing rows must comply with the EDM field types and supported formats (See Exact Data Match Field Types.)
  - The field names in the sample data template must match the field names in the actual data source file. The field names must appear in the same order in both files.

> **Caution**
>
> Do not create, edit, or view the source data CSV file using Microsoft Excel, as this may corrupt the file. Use a text editor.

> **Note**
>
> If any of the values provided in the source file to the DLP indexer fail to be validated as per the supported format, then the DLP indexer will skip that record and proceed with indexing the remaining records. The indexer also behaves in this manner for any records that may exceed the template-defined fields, and for empty rows or records with empty primary values. The DLP indexer generates messages reporting the position of any skipped records in the file.

Run the DLP Indexer to Create an EDM Identifier

Provides instructions for running the dlp indexer to create an edm identifier. When you create a new EDM Identifier, you need to run the DLP indexer on the data set to upload the first set of data records.

When you create a new EDM Identifier, you need to run the DLP indexer on the data set to upload the first set of data records. For the full procedure to create an EDM identifier, see Create an Exact Data Match Identifier.

Procedure

1. Review the Prerequisites, especially:

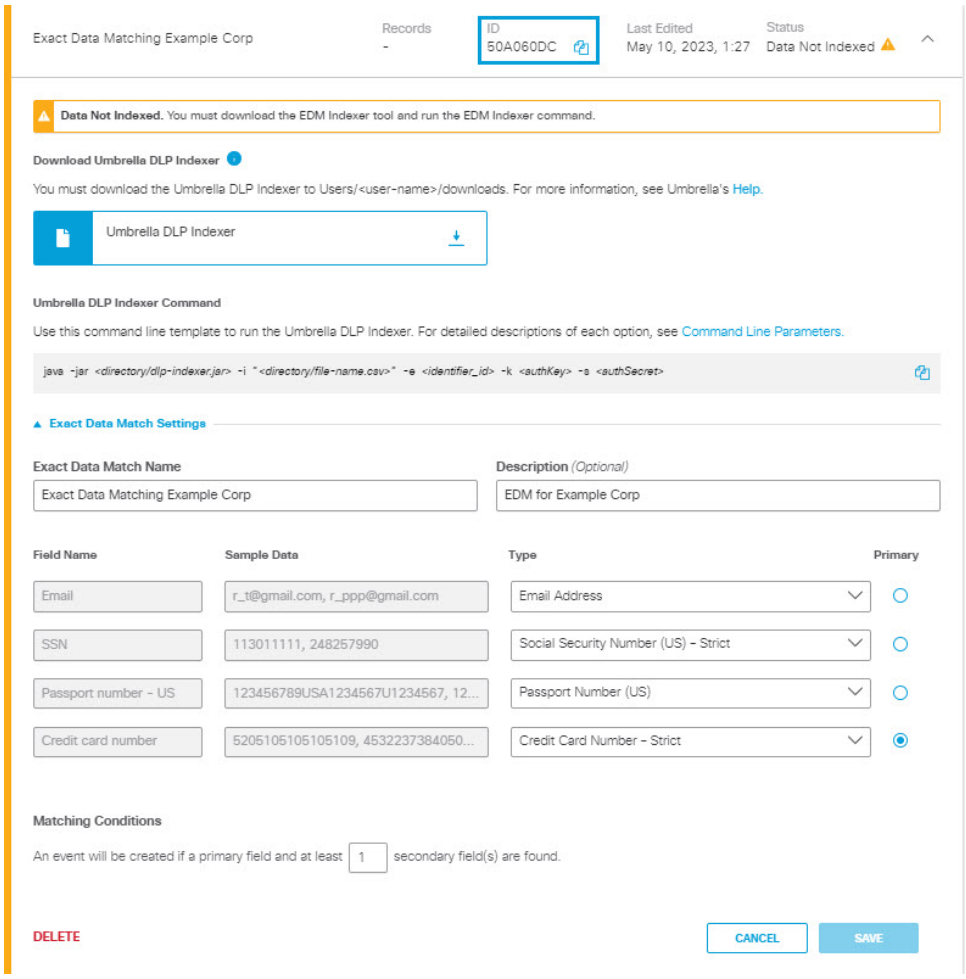
- Be sure you have the API key and secret. (See Step 8 in Create an Exact Data Match Identifier.)
- Be sure you have the EDM Identifier ID. (See Step 7 in Create an Exact Data Match Identifier.)

2. Run the indexer in a terminal window with the following command:

   java -jar <*directory_path*>\dlp-indexer.jar -i " <*directory_path*>\<*source-file*>.csv" -e <*edm-template-id*> -k <*authKey*> -s <*authSecret*>

   Where:

   - **<*directory_path*>\dlp-indexer.jar** –the relative path to the location of the DLP indexer
   - **" <*directory_path*>\<*source-file*>.csv"** –the relative path to the csv spreadsheet with the actual data records
   - **<*edm-template-id*>** –the ID of the EDM Identifier retrievable from the Secure Access UI using the copy icon shown in the following screenshot. (See also Step 7 in Create an Exact Data Match Identifier.)



- **<*authKey*>** –the API Key previously saved at Step 8d of Create an Exact Data Match Identifier.
- **<*authSecret*>** –the API Secret previously saved at Step 8d of Create an Exact Data Match Identifier.

If the indexer runs successfully, the exact data matcher will have a status of **Data Indexed**.

Note

When the EDM has a status of Data Indexed, you can add the EDM to a data classification but you can not edit the field types, primary field selection, or matching condition.

Update the Indexed Data Set Periodically

Provides instructions for updating the indexed data set periodically. When your source data changes, the existing EDM Identifier on your configured policy must be updated to reflect the new data fingerprints.

When your source data changes, the existing EDM Identifier on your configured policy must be updated to reflect the new data fingerprints. Using a script allows you to automatically rerun the DLP indexer periodically to update your source data to Secure Access without manually performing the initial procedure over again. After you rerun the DLP indexer with the updated version of the source file against the ID of your EDM Identifier, the DLP Policies configured with that EDM Identifier account for the most recent updates to your critical records.

Procedure

1. In a terminal window, set the the API Key and Secret previously used to index the identifier (saved in Step 8d of Create an Exact Data Match Identifier) to the environment variables **DLP_AUTH_KEY** and **DLP_AUTH_SECRET**.
2. Run the command to re-index the identifier as part of a periodically executed script or manually as needed:

   java -jar <*directory_path*>\dlp-indexer.jar -i " <*directory_path*>\<*source-file*>.csv"

   -e <*edm_template-id*> -k DLP_AUTH_KEY -s DLP_AUTH_SECRET

   Where:

   - **\<*directory_path*>\dlp-indexer.jar** –the relative path to the location of the DLP indexer
   - **"\<*directory_path*>\<*source-file*>"** .csv –the relative path to the csv spreadsheet with the actual data record.
   - **<*edm-template-id*>** –the ID used to index the EDM Identifier originally.

Troubleshooting

Provides instructions for troubleshooting. If the indexer reports a failure, examine the output error messages to determine the problem. If the indexer returns an error message that reads, "Error: A JNI error has occurred, please check your installation and try again," check the following:

If the indexer reports a failure, examine the output error messages to determine the problem.

If the indexer returns an error message that reads, "Error: A JNI error has occurred, please check your installation and try again," check the following:

Procedure

1. Confirm you have the latest version of the Java Development Kit installed.

2. Confirm that you have your PATH system variable set correctly:
   a. Check the location where you have Java installed.
      - For Windows this is normally **C:\Program Files\Java\jdk-<version-number>\bin**
      - For Linux this is normally **/usr/java/jdk-<version-number>/bin**
   b. Use the instructions here to set the PATH system variable appropriately for your operating system.

What to do next

> **Note**
>
> If the data indexer fails to process the input file and returns a **base64** encoded error code, provide that code to the Secure Access Support to assist you with troubleshooting.

Create an Indexed Document Match Identifier

Provides instructions for creating an indexed document match identifier. Indexed Document Matching (IDM) is a data matching technique that detects data loss incidents involving sensitive information maintained in unstructured formats for all DLP-supported file types.

Indexed Document Matching (IDM) is a data matching technique that detects data loss incidents involving sensitive information maintained in unstructured formats for all DLP-supported file types. IDMs enable Umbrella to scan documents used in a wide range of disciplines such as tax forms, merger and acquisition forms, medical records, bank statements, stock agreements, medical power of attorney forms, US patent files, non-disclosure agreements, resumes, source code, and more.

Umbrella performs Indexed Document Matching by creating hash fingerprints of text extracted from your sensitive documents, as opposed to leveraging pattern matching techniques. To create the fingerprints, you must download the DLP indexer and then run it against your documents from a command line prompt. The indexer extracts the document text, performs fingerprinting and indexing operations on it, then hashes the indexed text and uploads it to the Umbrella DLP. (Generally document text represents a low percentage of total document size, so indexing only text reduces the space required to store IDMs.)

Once you have run the indexer, you will have an Indexed Document Match Identifier associated with the documents. You will then be able to:

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- JVM version 17+
- The source file(s) you index must be in one of the formats supported by the DLP policy.

Procedure

1. Create a Data Classification that uses the IDM as a custom data identifier (as described in Create a Data Classification Using a Template or Create a Data Classification Without a Template).

2. Create a DLP rule that uses the Data Classification including that IDM Identifier. (For more information on DLP rules, see Manage the Data Loss Prevention Policy.)

What to do next

With these configurations in place, Umbrella will be able to monitor and/or block transmission of unstructured files that match at least a user-configurable percentage of the data text indexed for the IDM.

> **Note**
>
> To see a summary of the indexer options available, invoke the indexer with the **-h** option. (**java -jar <*directory-path*>\dlp-indexer.jar -h**.)

Limitations

Describes limitations. The total amount of indexed text for all the IDMs in your organization must not exceed 1 GB. You can increase this limit at no cost; contact customer support. The DLP indexer displays an error message if you exceed your allotted quota.

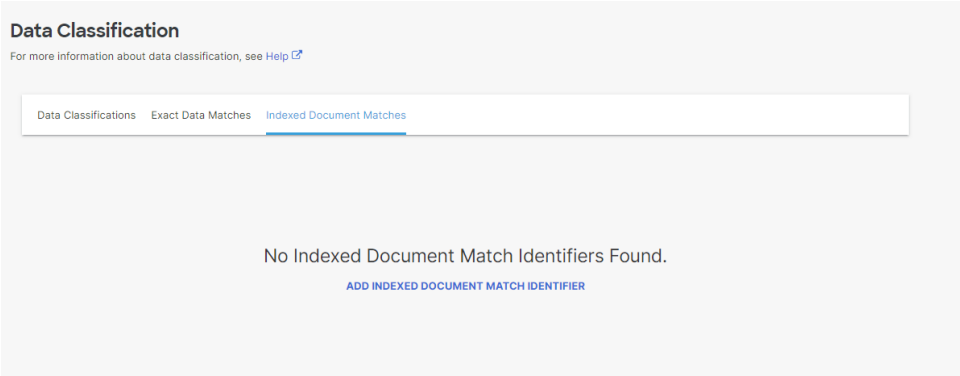
- The total amount of indexed text for all the IDMs in your organization must not exceed 1 GB. You can increase this limit at no cost; contact customer support. The DLP indexer displays an error message if you exceed your allotted quota.
- The data files must contain only 1 byte or 2 byte UTF-8 encoded characters, or Unicode characters.
- After you create an IDM Identifier, when you re-run the indexer using the same IDM Identifier, the indexer completely overwrites the previous index associated with that identifier. To add new data to an existing IDM, when you run the indexer again, include both the original data path and the new data path in the command to run the indexer.

Create an Indexed Document Match Identifier

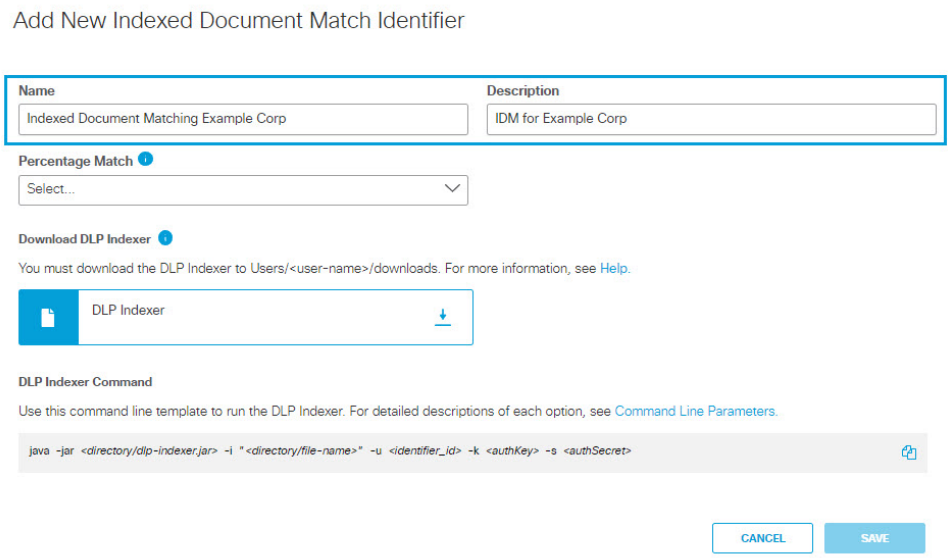
Provides instructions for creating an indexed document match identifier.

Procedure

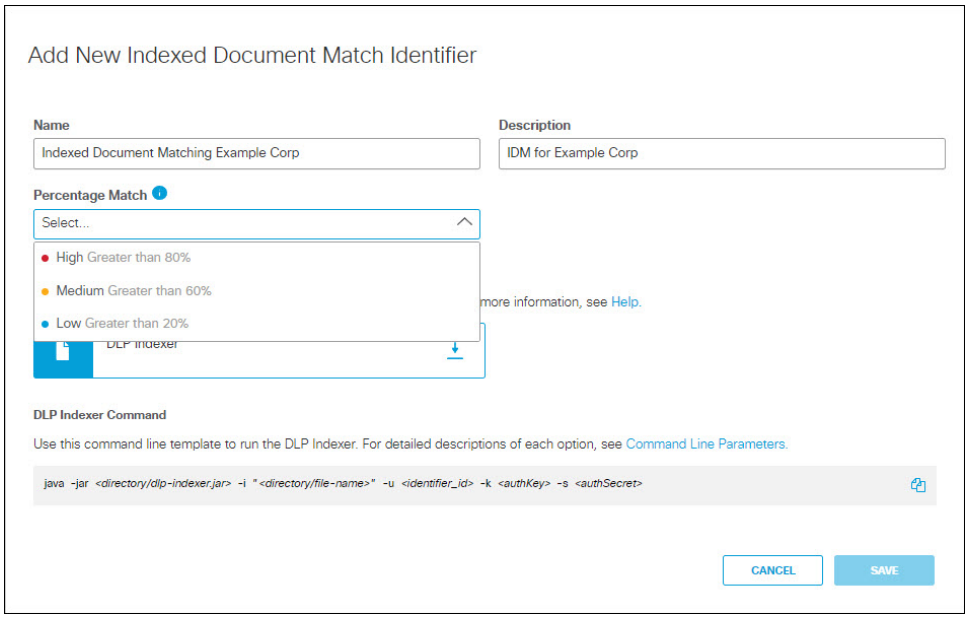
1. Navigate to **Secure** > **Settings** > **Data Classification** > **Indexed Document Matches** and click **ADD INDEXED DOCUMENT MATCH IDENTIFIER**.



2. Provide a name and description for the Indexed Document Match Identifier.

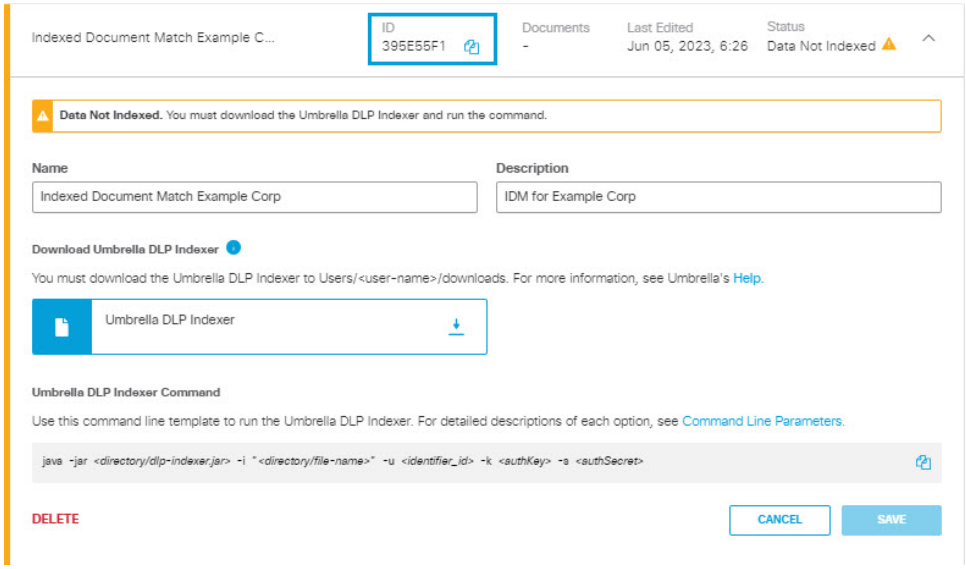


3. Select the level of percentage match required for a scanned document to be considered a match against a document included in the IDM:
   - High: 80% or more of the scanned document must match a document indexed for the IDM.
   - Medium: 60% or more of the scanned document must match a document indexed for the IDM.
   - Low: 20% or more of the scanned document must match a document indexed for the IDM.

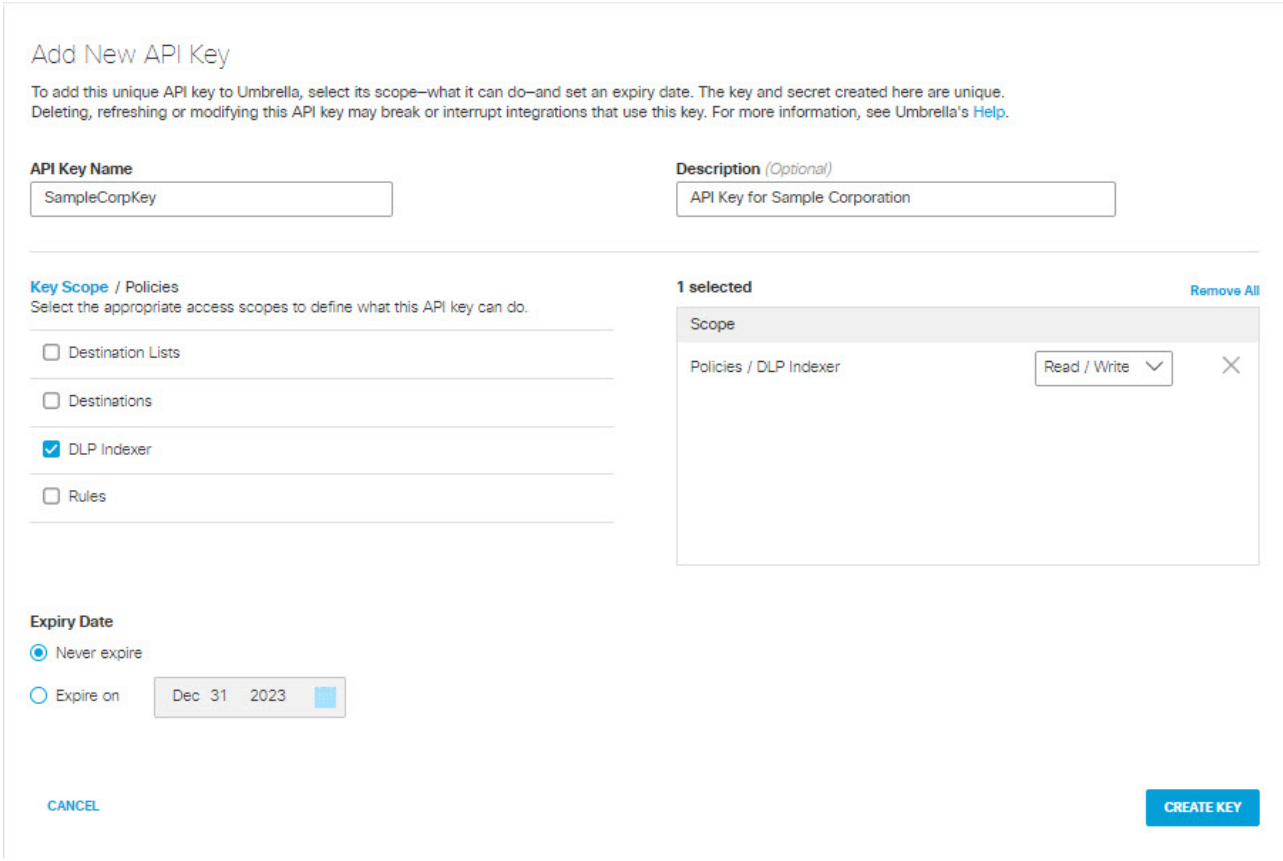


4. If you have not already downloaded the Umbrella DLP indexer, click the download icon to do so.
5. Click **Save.**
6. The Indexed Document Match Identifier now has a status of **Data Not Indexed.** You can expand the listing to view the details about the IDM Identifier. After you have indexed the IDM Identifier, you will be able to add it to a Data Classification as a custom identifier. Make note of the ID for the Indexed Document Match Identifier; you will need it to run the DLP indexer.

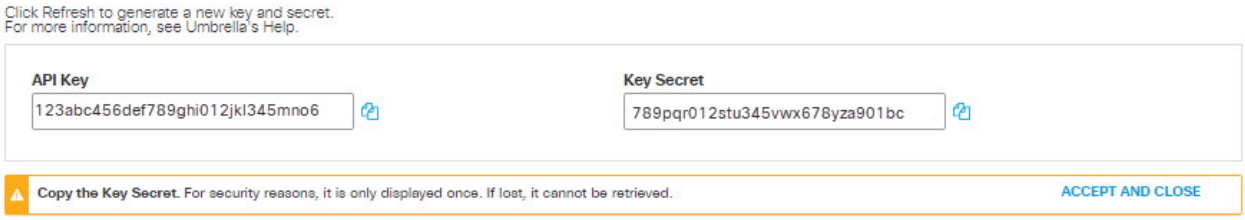
> **Note**
>
> The display page does not display the full IDM Identifier ID; use the **Copy** icon to copy the ID.



7. Create an API key and secret for the DLP indexer.
   a. Navigate to **Admin** > **API Keys** and click **Add**.
   b. Provide an **API Key Name** and **Description** for the API Key.
   c. Select **Policies** > **DLP Indexer** for the scope and choose **Read/Write** for the permissions. Then click **Create Key**.



d. Copy and save the API Key and Secret somewhere safe, as you will need them to run the DLP indexer.

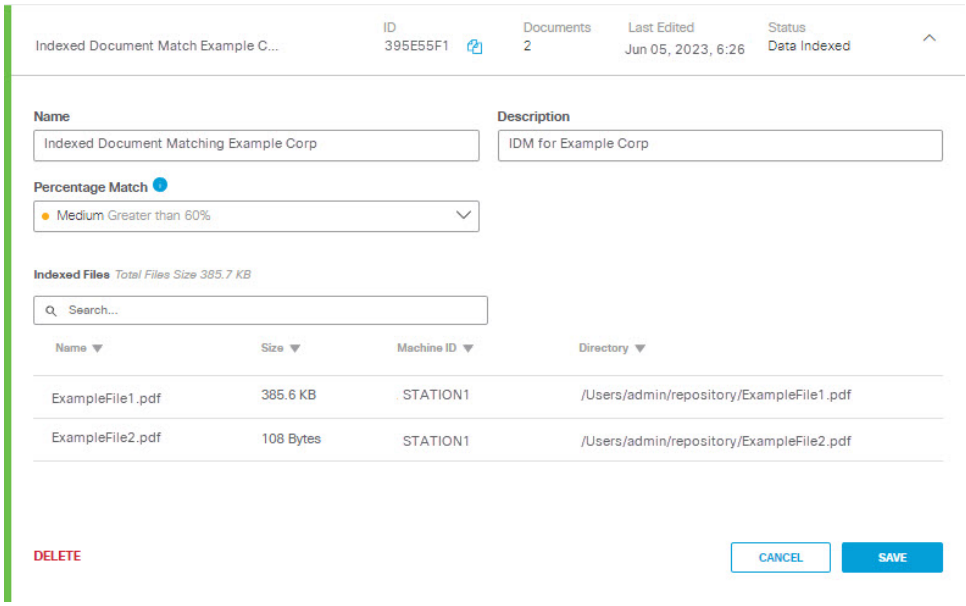


8. Use the Umbrella DLP indexer to fingerprint your example files.

Run the indexer in a terminal window with the following command: **java -jar <*directory-path*>\dlp-indexer.jar -i "<*directory_paths or file-names separated by commas*>" -u <*IDM-id*> -k <_authKey _> -s <*authSecret*>**

where:

- **<*directory-path*>\dlp-indexer.jar**–the relative path to the location of the DLP indexer.
- **<*directory_paths or file-names separated by commas*>**–the relative path to the directory containing your data, or a comma-separated list of files or directories.
- **<*IDM_id*>**–the ID of the IDM Identifier retrievable from Umbrella UI. (See Step 6.)
- **<*authKey*>**–the API Key previously saved at Step 7d.
- **<*authSecret*>**–the API Secret previously saved at Step 7d.



What to do next

The Indexed Document Match Identifier now has a status of **Data Indexed**; expand the listing to see details about the indexed files. You can now add the IDM to a Data Classification.

If you change your source file or directories you need to run the indexer on that file or directory again using the same IDM Identifier ID, API Key, and API Secret. This ensures that policies configured to use the IDM are updated to reflect the new data fingerprints. For more information, see Monitor the Indexed Data Set and Re-Index as Needed.

Monitor the Indexed Data Set and Re-Index as Needed

Describes monitoring the indexed data set and re-index as needed. As your source data changes, you need to re-index it using the same IDM Identifier to capture those changes so Umbrella will use them when scanning documents.

As your source data changes, you need to re-index it using the same IDM Identifier to capture those changes so Umbrella will use them when scanning documents. You can automate the re-indexing process to trigger a re-index when the source data has changed. Using the indexer monitor option causes the indexer to perform an initial index, then monitor your source data for updates and re-index as necessary. This is a useful option in a dynamic environment. In monitor mode, after performing an initial index the indexer checks the source data for changes every ten minutes, and if a change is detected, re-indexes the data.

You can run the indexer in monitor mode as a background process to automatically rerun the DLP indexer periodically to update your source data to Umbrella.

Use the following command to start the indexer in monitor mode:

java -jar <*directory-path*>\dlp-indexer.jar -i " <*directory_paths or file-names separated by commas*>" -u <*IDM-id*> -k <_authKey _> -s <*authSecret*> -y -m

Where:

- **<*directory-path*>\dlp-indexer.jar** – the relative path to the location of the DLP indexer.
- **<*directory_paths or file-names separated by commas*>**–the relative path to the directory containing your data, or a comma-separated list of files or directories.
- **<*IDM_id*>**–the ID of the IDM Identifier retrievable from Umbrella UI. (See Step 6.)
- **<*authKey*>**– the API Key previously saved at Step 7d of Create an Indexed Document Match Identifier.

- **<*authSecret*>**– the API Secret previously saved at Step 7d of Create an Indexed Document Match Identifier.
- The **-y** argument causes the indexer to automatically overwrite an existing index.

  When you run the indexer to re-index an existing IDM, it prompts for a yes/no confirmation before overwriting that IDM. Using the **-y** argument allows you to run the indexer without manually responding to the prompt.
- The **-m** argument causes the indexer to operate in monitor mode.

Troubleshooting

Provides instructions for troubleshooting. If the indexer reports a failure, examine the output error messages to determine the problem. If the indexer returns an error message that reads, "Error: A JNI error has occurred, please check your installation and try again," check the following:

If the indexer reports a failure, examine the output error messages to determine the problem.

If the indexer returns an error message that reads, "Error: A JNI error has occurred, please check your installation and try again," check the following:

Procedure

1. Confirm you have the latest version of the Java Development Kit installed.
2. Confirm that you have your PATH system variable set correctly:
   a. Check the location where you have Java installed.
      - For Windows this is normally **C:\Program Files\Java\jdk-<version-number>\bin**
      - For Linux this is normally **/usr/java/jdk-<version-number>/bin**
   b. Use the instructions here to set the PATH system variable appropriately for your operating system.

> **Note**
>
> If the data indexer fails to process the input file and returns a **base64** encoded error code, provide that code to the Umbrella Support to assist you with troubleshooting.

Built-In Data Classifications

Describes built-in data classifications. Secure Access provides four different pre-defined data classifications. You can use the pre-defined data classifications in one of two ways:

Secure Access provides four different pre-defined data classifications. You can use the pre-defined data classifications in one of two ways:

- You can create a custom data classification by copying a pre-defined data classification template provided by Secure Access, and customizing the copy. See Copy and Customize a Built-In Data Classification.
- You can apply a pre-defined data classification template provided by Secure Access to a DLP rule. (See Add a Real Time Rule to the Data Loss Prevention Policy and Add a SaaS API Rule to the Data Loss Prevention Policy).

Each of the built-in data classifications has a different set of built-in data identifiers associated with it. The built-in data classifications are:

- PII Data Classification

  Personal Information Identifiers; data that includes any personal information that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers. The data identifiers associated with the PII Data Classification are:

  - Multiple Personal Identifiers – PII (Australia) - Strict
  - Multiple Personal Identifiers – PII (European Union)
  - Multiple Personal Identifiers – PII (UK) - Strict
  - Multiple Personal Identifiers – PII (US) - Strict

- PCI Data Classification

  Data related to the Payment Card Industry. The data identifiers associated with the PCI Data Classification are:

  - Credit Card Number - Strict
  - Expiry Date (Austria)
  - Expiry Date (Belgium)
  - Expiry Date (Croatia)
  - Expiry Date (Cyprus)
  - Expiry Date (Czech)
  - Expiry Date (Denmark)
  - Expiry Date (Estonia)
  - Expiry Date (Finland)
  - Expiry Date (France)
  - Expiry Date (Germany)
  - Expiry Date (Greece)
  - Expiry Date (Hungary)
  - Expiry Date (Ireland)
  - Expiry Date (Italy)
  - Expiry Date (Latvia)
  - Expiry Date (Lithuania)
  - Expiry Date (Luxembourg)
  - Expiry Date (Malta)
  - Expiry Date (Netherlands)
  - Expiry Date (Poland)
  - Expiry Date (Portugal)
  - Expiry Date (Romania)
  - Expiry Date (Slovakia)

- Expiry Date (Slovenia)
- Expiry Date (Spain)
- Expiry Date (Sweden)
- Expiry Date (UK/US)
- Security Code (Austria)
- Security Code (Belgium)
- Security Code (Croatia)
- Security Code (Cyprus)
- Security Code (Czech)
- Security Code (Denmark)
- Security Code (Estonia)
- Security Code (Finland)
- Security Code (France)
- Security Code (Germany)
- Security Code (Greece)
- Security Code (Hungary)
- Security Code (Ireland)
- Security Code (Italy)
- Security Code (Latvia)
- Security Code (Lithuania)
- Security Code (Luxembourg)
- Security Code (Malta)
- Security Code (Netherlands)
- Security Code (Poland)
- Security Code (Portugal)
- Security Code (Romania)
- Security Code (Slovakia)
- Security Code (Slovenia)
- Security Code (Spain)
- Security Code (Sweden)
- Security Code (UK/US/EU except Bulgaria)

- GDPR Data Classification

  Common personal data associated with the European Union's General Data Protection Regulation. Customers can use these identifiers to support GDPR compliance within their organizations. The data identifiers associated with the GDPR Data Classification are:

- Carte national d'identité sécurisée – CNIS (France)
- Credit Card Number – Strict
- Criminal Record (Austria)
- Criminal Record (Belgium)
- Criminal Record (Croatia)
- Criminal Record (Cyprus)
- Criminal Record (Czech)
- Criminal Record (Denmark)
- Criminal Record (Estonia)
- Criminal Record (Finland)
- Criminal Record (France)
- Criminal Record (Germany)
- Criminal Record (Greece)
- Criminal Record (Hungary)
- Criminal Record (Ireland)
- Criminal Record (Italy)
- Criminal Record (Latvia)
- Criminal Record (Lithuania)
- Criminal Record (Luxembourg)
- Criminal Record (Malta)
- Criminal Record (Netherlands)
- Criminal Record (Poland)
- Criminal Record (Portugal)
- Criminal Record (Romania)
- Criminal Record (Slovakia)
- Criminal Record (Slovenia)
- Criminal Record (Spain)
- Criminal Record (Sweden)
- Criminal Record (UK)
- Date of Birth
- Driver's License Number (Austria)
- Driver's License Number (Belgium)
- Driver's License Number (Croatia)
- Driver's License Number (Cyprus)
- Driver's License Number (Czech Republic)

- Driver's License Number (Denmark)
- Driver's License Number (Estonia)
- Driver's License Number (Finland)
- Driver's License Number (France)
- Driver's License Number (Germany)
- Driver's License Number (Greece)
- Driver's License Number (Hungary)
- Driver's License Number (Ireland)
- Driver's License Number (Italy)
- Driver's License Number (Latvia)
- Driver's License Number (Lithuania)
- Driver's License Number (Luxembourg)
- Driver's License Number (Malta)
- Driver's License Number (Netherlands)
- Driver's License Number (Poland)
- Driver's License Number (Portugal)
- Driver's License Number (Romania)
- Driver's License Number (Slovakia)
- Driver's License Number (Slovenia)
- Driver's License Number (Spain)
- Driver's License Number (Sweden)
- Driver's License Number (UK)
- Email Address
- Ethnicity (Austria)
- Ethnicity (Belgium)
- Ethnicity (Croatia)
- Ethnicity (Cyprus)
- Ethnicity (Czech)
- Ethnicity (Denmark)
- Ethnicity (Estonia)
- Ethnicity (Finland)
- Ethnicity (France)
- Ethnicity (Germany)
- Ethnicity (Greece)
- Ethnicity (Hungary)

- Ethnicity (Ireland)
- Ethnicity (Italy)
- Ethnicity (Latvia)
- Ethnicity (Lithuania)
- Ethnicity (Luxembourg)
- Ethnicity (Malta)
- Ethnicity (Netherlands)
- Ethnicity (Poland)
- Ethnicity (Portugal)
- Ethnicity (Romania)
- Ethnicity (Slovakia)
- Ethnicity (Slovenia)
- Ethnicity (Spain)
- Ethnicity (Sweden)
- Ethnicity (UK)
- Eye Color (Austria)
- Eye Color (Belgium)
- Eye Color (Croatia)
- Eye Color (Cyprus)
- Eye Color (Czech)
- Eye Color (Denmark)
- Eye Color (Estonia)
- Eye Color (Finland)
- Eye Color (France)
- Eye Color (Germany)
- Eye Color (Greece)
- Eye Color (Hungary)
- Eye Color (Ireland)
- Eye Color (Italy)
- Eye Color (Latvia)
- Eye Color (Lithuania)
- Eye Color (Luxembourg)
- Eye Color (Malta)
- Eye Color (Netherlands)
- Eye Color (Poland)

- Eye Color (Portugal)
- Eye Color (Romania)
- Eye Color (Slovakia)
- Eye Color (Slovenia)
- Eye Color (Spain)
- Eye Color (Sweden)
- Eye Colour (UK)
- Gender (Austria)
- Gender (Belgium)
- Gender (Croatia)
- Gender (Cyprus)
- Gender (Czech)
- Gender (Denmark)
- Gender (Estonia)
- Gender (Finland)
- Gender (France)
- Gender (Germany)
- Gender (Greece)
- Gender (Hungary)
- Gender (Ireland)
- Gender (Italy)
- Gender (Latvia)
- Gender (Lithuania)
- Gender (Luxembourg)
- Gender (Malta)
- Gender (Netherlands)
- Gender (Poland)
- Gender (Portugal)
- Gender (Romania)
- Gender (Slovakia)
- Gender (Slovenia)
- Gender (Spain)
- Gender (Sweden)
- Gender (UK)
- Hair Color (Austria)

- Hair Color (Belgium)
- Hair Color (Croatia)
- Hair Color (Cyprus)
- Hair Color (Czech)
- Hair Color (Denmark)
- Hair Color (Estonia)
- Hair Color (Finland)
- Hair Color (France)
- Hair Color (Germany)
- Hair Color (Greece)
- Hair Color (Hungary)
- Hair Color (Ireland)
- Hair Color (Italy)
- Hair Color (Latvia)
- Hair Color (Lithuania)
- Hair Color (Luxembourg)
- Hair Color (Malta)
- Hair Color (Netherlands)
- Hair Color (Poland)
- Hair Color (Portugal)
- Hair Color (Romania)
- Hair Color (Slovakia)
- Hair Color (Slovenia)
- Hair Color (Spain)
- Hair Color (Sweden)
- Hair Colour (UK)
- Height (Austria)
- Height (Belgium)
- Height (Croatia)
- Height (Cyprus)
- Height (Czech)
- Height (Denmark)
- Height (Estonia)
- Height (Finland)
- Height (France)

- Height (Germany)
- Height (Greece)
- Height (Hungary)
- Height (Ireland)
- Height (Italy)
- Height (Latvia)
- Height (Lithuania)
- Height (Luxembourg)
- Height (Malta)
- Height (Netherlands)
- Height (Poland)
- Height (Portugal)
- Height (Romania)
- Height (Slovakia)
- Height (Slovenia)
- Height (Spain)
- Height (Sweden)
- Height (UK)
- International Bank Account Number – IBAN (Austria)
- International Bank Account Number – IBAN (Belgium)
- International Bank Account Number – IBAN (Croatia)
- International Bank Account Number – IBAN (Cyprus)
- International Bank Account Number – IBAN (Czech Republic)
- International Bank Account Number – IBAN (Denmark)
- International Bank Account Number – IBAN (Estonia)
- International Bank Account Number – IBAN (Finland)
- International Bank Account Number – IBAN (France)
- International Bank Account Number – IBAN (Germany)
- International Bank Account Number – IBAN (Greece)
- International Bank Account Number – IBAN (Hungary)
- International Bank Account Number – IBAN (Ireland)
- International Bank Account Number – IBAN (Italy)
- International Bank Account Number – IBAN (Latvia)
- International Bank Account Number – IBAN (Lithuania)
- International Bank Account Number – IBAN (Luxembourg)

- International Bank Account Number – IBAN (Malta)
- International Bank Account Number – IBAN (Netherlands)
- International Bank Account Number – IBAN (Poland)
- International Bank Account Number – IBAN (Portugal)
- International Bank Account Number – IBAN (Romania)
- International Bank Account Number – IBAN (Slovakia)
- International Bank Account Number – IBAN (Slovenia)
- International Bank Account Number – IBAN (Spain)
- International Bank Account Number – IBAN (Sweden)
- International Bank Account Number – IBAN (UK)
- IP Address
- National Identity Number (Greece)
- National Identity Number – OIB (Croatia)
- National Insurance Number – NINO (UK)
- Passport Number (Austria)
- Passport Number (Belgium)
- Passport Number (Croatia)
- Passport Number (Cyprus)
- Passport Number (Czech Republic)
- Passport Number (Denmark)
- Passport Number (Estonia)
- Passport Number (Finland)
- Passport Number (France)
- Passport Number (Germany)
- Passport Number (Greece)
- Passport Number (Hungary)
- Passport Number (Ireland)
- Passport Number (Italy)
- Passport Number (Latvia)
- Passport Number (Lithuania)
- Passport Number (Luxembourg)
- Passport Number (Malta)
- Passport Number (Netherlands)
- Passport Number (Poland)
- Passport Number (Portugal)

- Passport Number (Romania)
- Passport Number (Slovakia)
- Passport Number (Slovenia)
- Passport Number (Spain)
- Passport Number (Sweden)
- Passport Number (UK)
- Phone Number (Austria)
- Phone Number (Belgium)
- Phone Number (Croatia)
- Phone Number (Cyprus)
- Phone Number (Czech Republic)
- Phone Number (Denmark)
- Phone Number (Estonia)
- Phone Number (Finland)
- Phone Number (France)
- Phone Number (Germany)
- Phone Number (Greece)
- Phone Number (Hungary)
- Phone Number (Ireland)
- Phone Number (Italy)
- Phone Number (Latvia)
- Phone Number (Lithuania)
- Phone Number (Luxembourg)
- Phone Number (Malta)
- Phone Number (Netherlands)
- Phone Number (Poland)
- Phone Number (Portugal)
- Phone Number (Romania)
- Phone Number (Slovakia)
- Phone Number (Slovenia)
- Phone Number (Spain)
- Phone Number (Sweden)
- Phone Number (UK)
- Postcode (Austria)
- Postcode (Belgium)

- Postcode (Croatia)
- Postcode (Cyprus)
- Postcode (Czech)
- Postcode (Denmark)
- Postcode (Estonia)
- Postcode (Finland)
- Postcode (France)
- Postcode (Germany)
- Postcode (Greece)
- Postcode (Hungary)
- Postcode (Ireland)
- Postcode (Italy)
- Postcode (Latvia)
- Postcode (Lithuania)
- Postcode (Luxembourg)
- Postcode (Malta)
- Postcode (Netherlands)
- Postcode (Poland)
- Postcode (Portugal)
- Postcode (Romania)
- Postcode (Slovakia)
- Postcode (Slovenia)
- Postcode (Spain)
- Postcode (Sweden)
- Postcode (UK)
- Race (Austria)
- Race (Belgium)
- Race (Croatia)
- Race (Cyprus)
- Race (Czech)
- Race (Denmark)
- Race (Estonia)
- Race (Finland)
- Race (France)
- Race (Germany)

- Race (Greece)
- Race (Hungary)
- Race (Ireland)
- Race (Italy)
- Race (Latvia)
- Race (Lithuania)
- Race (Luxembourg)
- Race (Malta)
- Race (Netherlands)
- Race (Poland)
- Race (Portugal)
- Race (Romania)
- Race (Slovakia)
- Race (Slovenia)
- Race (Spain)
- Race (Sweden)
- Race (UK)
- Region (Austria)
- Region (Belgium)
- Region (Croatia)
- Region (Cyprus)
- Region (Czech)
- Region (Denmark)
- Region (Estonia)
- Region (Finland)
- Region (France)
- Region (Germany)
- Region (Greece)
- Region (Hungary)
- Region (Ireland)
- Region (Italy)
- Region (Latvia)
- Region (Lithuania)
- Region (Luxembourg)
- Region (Malta)

- Region (Netherlands)
- Region (Poland)
- Region (Portugal)
- Region (Romania)
- Region (Slovakia)
- Region (Slovenia)
- Region (Spain)
- Region (Sweden)
- Region (UK)
- Religion (Austria)
- Religion (Belgium)
- Religion (Croatia)
- Religion (Cyprus)
- Religion (Czech)
- Religion (Denmark)
- Religion (Estonia)
- Religion (Finland)
- Religion (France)
- Religion (Germany)
- Religion (Greece)
- Religion (Hungary)
- Religion (Ireland)
- Religion (Italy)
- Religion (Latvia)
- Religion (Lithuania)
- Religion (Luxembourg)
- Religion (Malta)
- Religion (Netherlands)
- Religion (Poland)
- Religion (Portugal)
- Religion (Romania)
- Religion (Slovakia)
- Religion (Slovenia)
- Religion (Spain)
- Religion (Sweden)

- Religion (UK)
- Social Security Number – INSEE (France)
- VAT ID Number (Austria)
- VAT ID Number (Belgium)
- VAT ID Number (Croatia)
- VAT ID Number (Cyprus)
- VAT ID Number (Czech Republic)
- VAT ID Number (Denmark)
- VAT ID Number (Estonia)
- VAT ID Number (Finland)
- VAT ID Number (France)
- VAT ID Number (Germany)
- VAT ID NumberT (Greece)
- VAT ID Number (Hungary)
- VAT ID Number (Ireland)
- VAT ID Number (Italy)
- VAT ID Number (Latvia)
- VAT ID Number (Lithuania)
- VAT ID Number (Luxembourg)
- VAT ID Number (Malta)
- VAT ID Number (Netherlands)
- VAT ID Number (Poland)
- VAT ID Number (Portugal)
- VAT ID Number (Romania)
- VAT ID Number (Slovakia)
- VAT ID Number (Slovenia)
- VAT ID Number (Spain)
- VAT ID Number (Sweden)
- VAT ID Number (UK)
- Weight (Austria)
- Weight (Belgium)
- Weight (Croatia)
- Weight (Cyprus)
- Weight (Czech)
- Weight (Denmark)

- Weight (Estonia)
- Weight (Finland)
- Weight (France)
- Weight (Germany)
- Weight (Greece)
- Weight (Hungary)
- Weight (Ireland)
- Weight (Italy)
- Weight (Latvia)
- Weight (Lithuania)
- Weight (Luxembourg)
- Weight (Malta)
- Weight (Netherlands)
- Weight (Poland)
- Weight (Portugal)
- Weight (Romania)
- Weight (Slovakia)
- Weight (Slovenia)
- Weight (Spain)
- Weight (Sweden)
- Weight (UK)

- HIPAA Data Classification

  Personal medical and healthcare data associated with the United States' Health Insurance Portability and Accountability Act. Customers can use these identifiers to support HIPAA compliance within their organizations. The data identifiers associated with the HIPAA Data Classification template are:

  - Date of Birth
  - Drug Name and Person Name (US)
  - Drug Name and Social Security Number (US)
  - Health Condition and Person Name (US)
  - Health Condition and Social Security Number (US)
  - ICD Code
  - ICD Code and Person Name (US)
  - ICD Code and Social Security Number (US)
  - Medical Prescriptions
  - National Drug Code Number - NDC

- Social Security Number (US) - Strict

Exact Data Match Field Types

Describes exact data match field types. When creating an Exact Data Match (EDM) template, you must choose an EDM type for each field provided. The EDM types are similar to the Built-in Data Identifiers in that specific patterns must be found to match the identifier.

When creating an Exact Data Match (EDM) template, you must choose an EDM type for each field provided. The EDM types are similar to the Built-in Data Identifiers in that specific patterns must be found to match the identifier. Unlike Built-In Identifiers, EDM types do not use keywords to find data matches.

Supported EDM Types

Describes supported edm types. ABA Routing Number (US)– A 9-digit number used by banks to identify specific financial institutions in the United States.

- **ABA Routing Number (US)**– A 9-digit number used by banks to identify specific financial institutions in the United States.
- **Alphanumeric**–Up to 6 words composed of 1 and 2-byte UTF-8 encoded characters, delimited by spaces.
- **Bank Account Number (US)**–A 5-digit number denoting a bank account number issued in the United States.
- **Carte nationale d'identité sécurisée – CNIS (France)**–A 12-digit number denoting the French national identity card number.
- **Credit Card Number**–A valid 15 or 16-digit credit card number that passes the Luhn validation and includes any of the following delimiters: space, no space, ~, or -.
- **Date**–A date value matching one of the following formats where the `<delimiter>` is no space, /, or -. :
  - the European format of `<dd><delimiter><mm><delimiter><yyyy>` or
  - the American format of `<mm><delimiter><dd><delimiter><yyyy>`
- **Email Address**–A valid email address using ASCII characters.
- **Fiscal Identification Number – Número de identificación fiscal – NIF (Spain)**– A number issued to Spanish nationals for identification purposes. The pattern matches`<dddddddd><a>` where:
  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
- **ICD Code**–A number matching the pattern of one of the typical International Classification of Diseases (ICD) codes.
- **Individual Taxpayer Identification Number – ITIN (US)**–A United States tax processing number issued by the Internal Revenue Service (IRS). The pattern must match the format of `<ddd><delimiter><dd><delimiter><dddd>` where:
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, or -
- **International Bank Account Number – IBAN (UK)**–An international bank account number for the UK. The pattern matches a format of `<aadd><delimiter><aaaadddd><delimiter><dddd><delimiter><dddd><delimiter><dd>` where:

  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, or -

- **IP Address**–A valid IPv4 address.
- **National Drug Code Number (NDC)**–Segments of the National Drug Code (NDC) used in the united States to identify drugs for human use. The pattern matches a format of `<ddddd><delimiter><ddd><delimiter><dd>` where:
  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is ~ or -
- **National Insurance Number – NINO (UK)**–An identification number issued to individuals by the United Kingdom Department for Work and Pensions. The pattern matches with a format of `<aa><delimiter><dd><delimiter><dd><delimiter><dda>` where:
  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, -, or .
- **Passport Number (US)**–An identification number issued to citizen and non-citizen nationals of the United states. The pattern must match a format of `<ddddddddd>USA<ddddddd>U<ddddddd>` where `d` is any ASCII digit from 0 to 9.
- **Passport Number (UK)**–An identification number that serves as proof of nationality or immigration status in the United Kingdom. The pattern must match one of the following formats:
  - a 9-digit number
  - `<ddddddddd>GBR<ddddddd>U<ddddddd>` where `d` is any ASCII digit from 0 to 9
- **Postcode (UK)**– A number matching the typical UK postal code patterns, where the number can include a space between the inward and outward segments.
- **Social Security Number - INSEE (France)**National identification numbers for The National Institute of Statistics and Economic Studies issued at birth to French nationals. The number can be 12 or 15 digits. The pattern matches a format of `<ddddddddddddd><delimiter><dd>` where:
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~
- **Social Security Number (US) – Strict**–An identification number issued in the United States to citizens, permanent residents, and temporary working residents. The pattern matches`<aaa><delimiter><dd><delimiter><dddd>` where:
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, -, or .

44 Built-in Data Identifiers

Topics:

- Built-in Data Identifiers

Describes the purpose and procedures for built-in data identifiers and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Built-in Data Identifiers

Describes built-in data identifiers. Secure Access provides a wide selection of built-in data identifiers you can choose to incorporate into DLP policy to classify a wide range of sensitive data, both structured and unstructured.

Secure Access provides a wide selection of built-in data identifiers you can choose to incorporate into DLP policy to classify a wide range of sensitive data, both structured and unstructured.

The built-in identifier can classify specific data values based on pattern matching, bloom filters, and dictionaries incorporating proximity terms.

Built-in identifiers are not directly incorporated into DLP rules; you must first select and incorporate them into Data Classifications which you then apply to DLP rules. (See Manage Data Classifications).

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

Tolerances

Describes tolerances. Some built-in data identifiers have three versions, each with a different tolerance level associated with it. Tolerance levels determine how many instances of an identifier must appear within a document for that document to be considered a match. There are three tolerance levels:

Some built-in data identifiers have three versions, each with a different tolerance level associated with it. Tolerance levels determine how many instances of an identifier must appear within a document for that document to be considered a match. There are three tolerance levels:

- Lenient tolerance requires only a single instance of an identifier to appear within a document for that document to be considered a match.
- Moderate tolerance requires more occurrences of an identifier than Lenient tolerance, but fewer than Strict tolerance. (The exact number varies depending upon the identifier.)
- Strict tolerance requires the most occurrences of an identifier to appear within a document for that document to be considered a match. (The exact number varies depending upon the identifier.)

For identifiers that support tolerance levels, you can choose the tolerance level that best matches your level of concern for catching every occurrence of those identifiers.

Copy and Customize a Built-In Data Classification

Describes copy and customize a built-in data classification. The system provides four different built-in data classifications you can use in real time rules, SaaS API rules, and discovery scans. These are:

The system provides four different built-in data classifications you can use in real time rules, SaaS API rules, and discovery scans. These are:

PII Data Classification

Personal Information Identifiers; data that includes any personal information that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers.

PCI Data Classification

Data related to the Payment Card Industry.

GDPR Data Classification

Common personal data associated with the European Union's General Data Protection Regulation. Customers can use these identifiers to support GDPR compliance within their organizations.

HIPAA Data Classification

Personal medical and healthcare data associated with the United States' Health Insurance Portability and Accountability Act. Customers can use these identifiers to support HIPAA compliance within their organizations.

For more details on each of these built-in data classifications, see Built-In Data Classifications. You can create custom data classifications based on any of these built-in data classifications. Simply copy the desired built-in classification, make changes to the copy, and save it as a custom data classification.

The building blocks for data classifications are data identifiers. The data identifiers selected for a data classification determine the type of data for which rules using that data classification will scan. Built-in data classifications have data identifiers already selected for them; you can produce your own customized versions of these classifications by removing selected identifiers or adding other identifiers.

The system allows you to choose from the available built-in data identifiers to remove from or add to your customized version of a built-in data classification.

- Built-In Identifiers

  These identify data using pattern matching and dictionary lookups. The descriptions shown in the GUI provide details about the type of data they match. For more information, see Built-In Data Identifiers.

The system offers three types of data identifiers you can create yourself applying different methods of data analysis. You can add these to your customized version of a built-in data classification:

- Custom Identifiers

  You can create custom identifiers to match specific terms and pattern expressions of your choosing. See Create a Custom Identifier.

- Exact Data Match Identifiers

  Exact Data Match Identifiers use fingerprinting to identify data in structured documents that match criteria you define. (See Create an Exact Data Match Identifier for more information.)

- Indexed Document Match Identifiers

  Indexed Document Match Identifiers use fingerprinting to identify data in unstructured documents that match criteria you define. See Create an Indexed Document Match Identifier for more information.

To delete or edit a data classification, see Delete or Edit a Classification.

Procedure

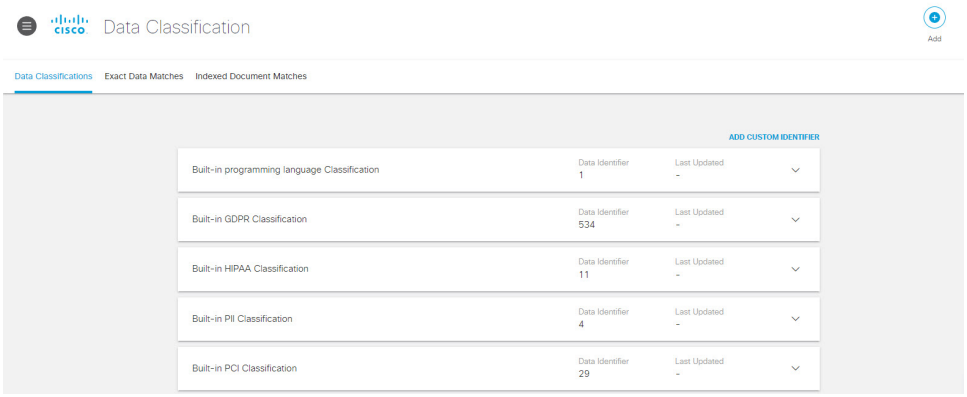
Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. Navigate to Secure Settings Data Classification .

Before you begin

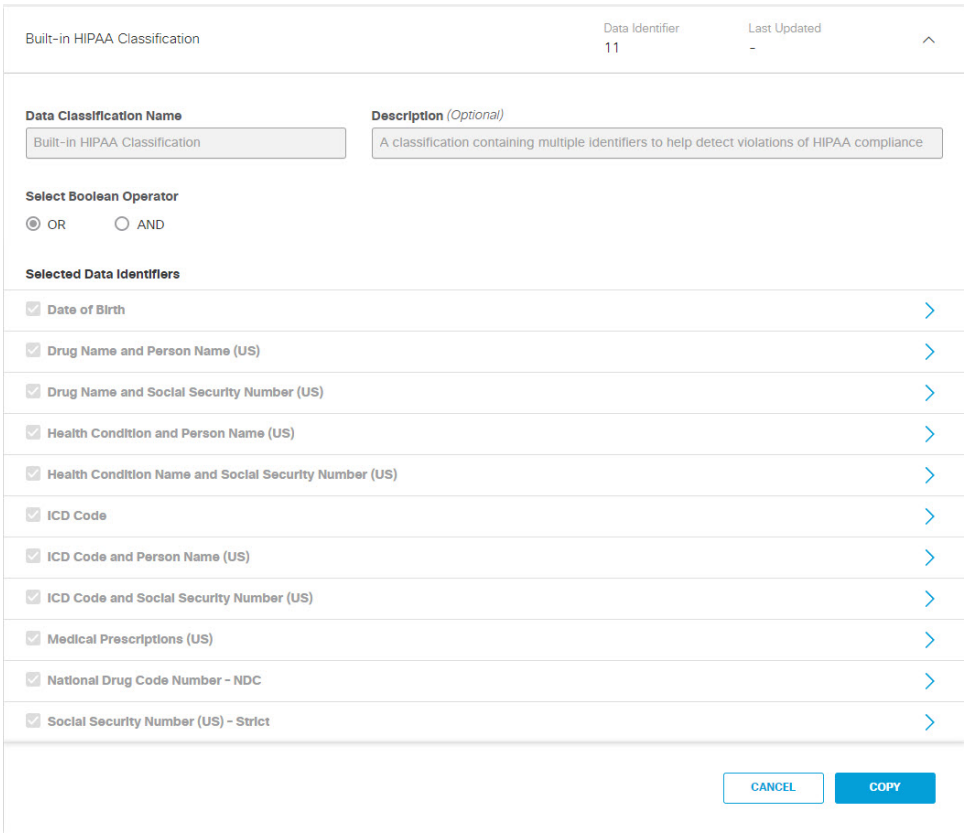
- Full Admin user role. For more information, see Manage Accounts.

Procedure

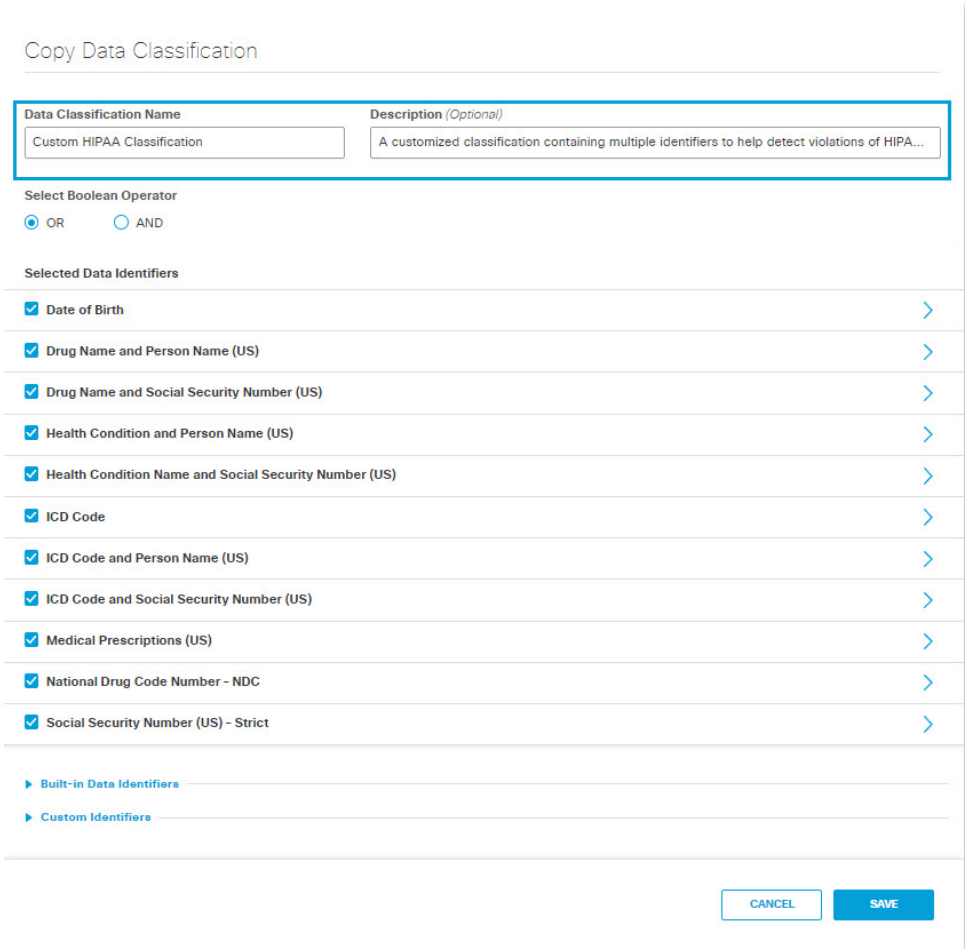
1. Navigate to **Secure** > **Settings** > **Data Classification**.



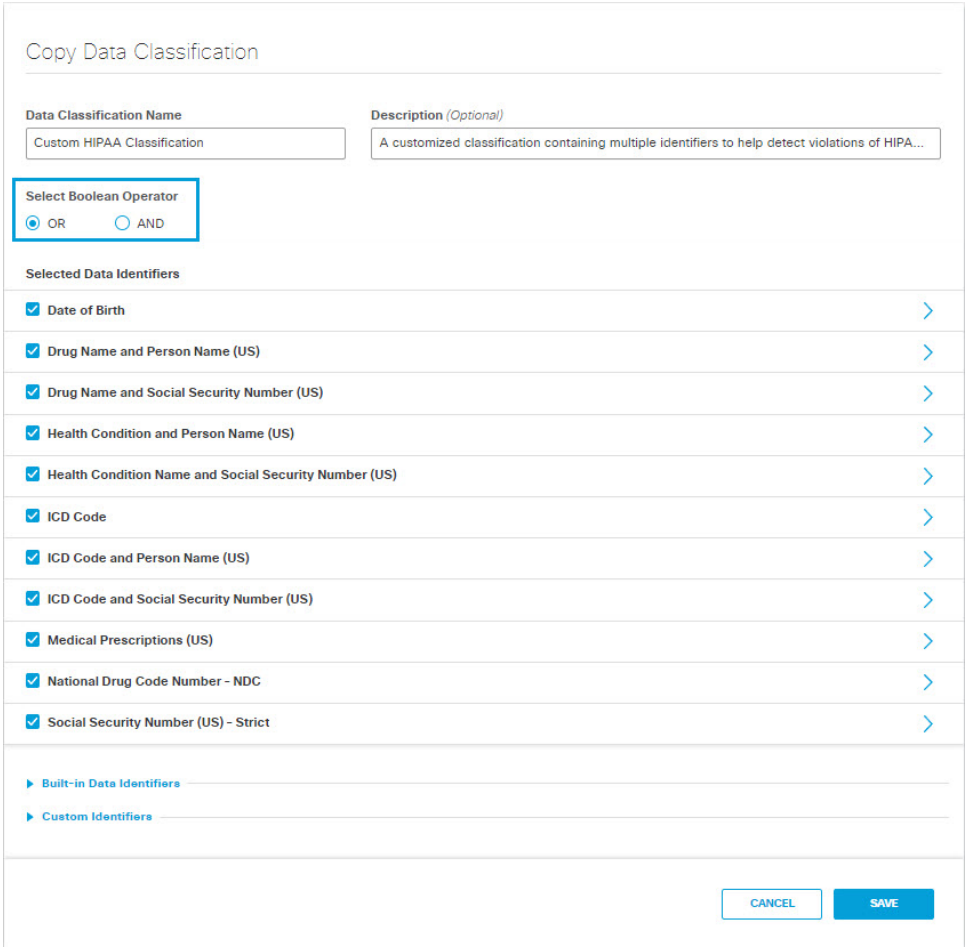
2. Expand one of the built-in data classifications and click **Copy**.



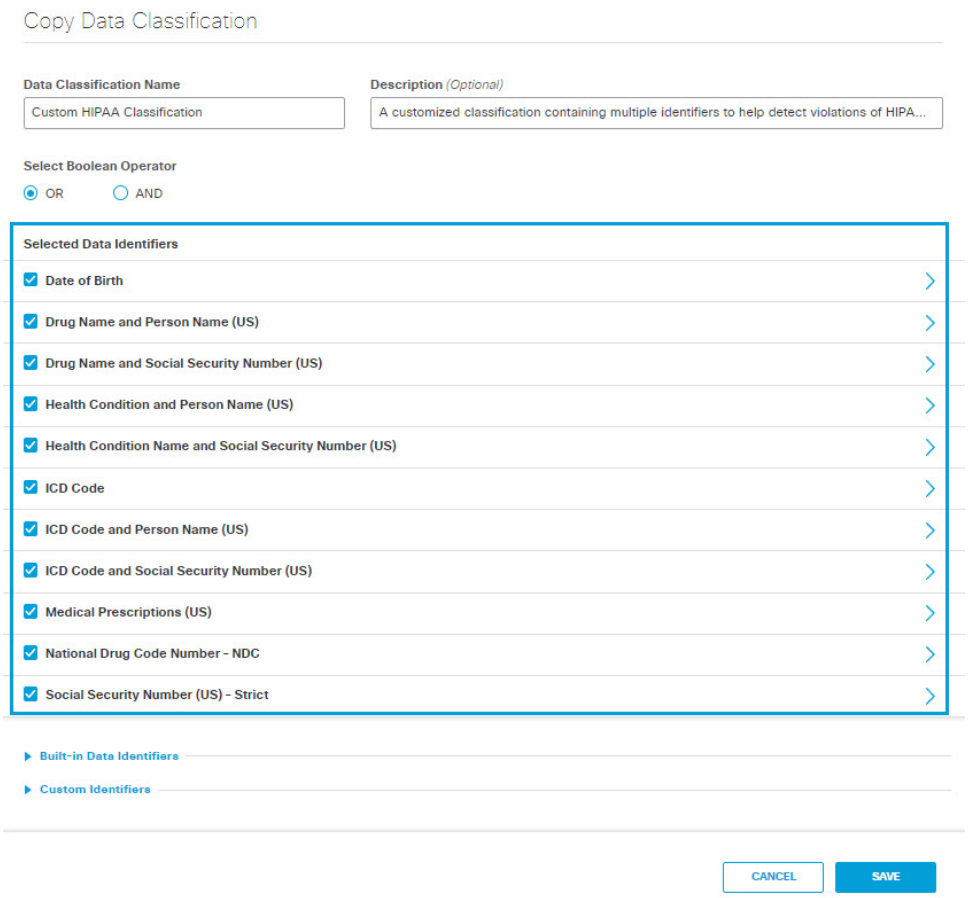
3. Give the new data classification a meaningful name and description.



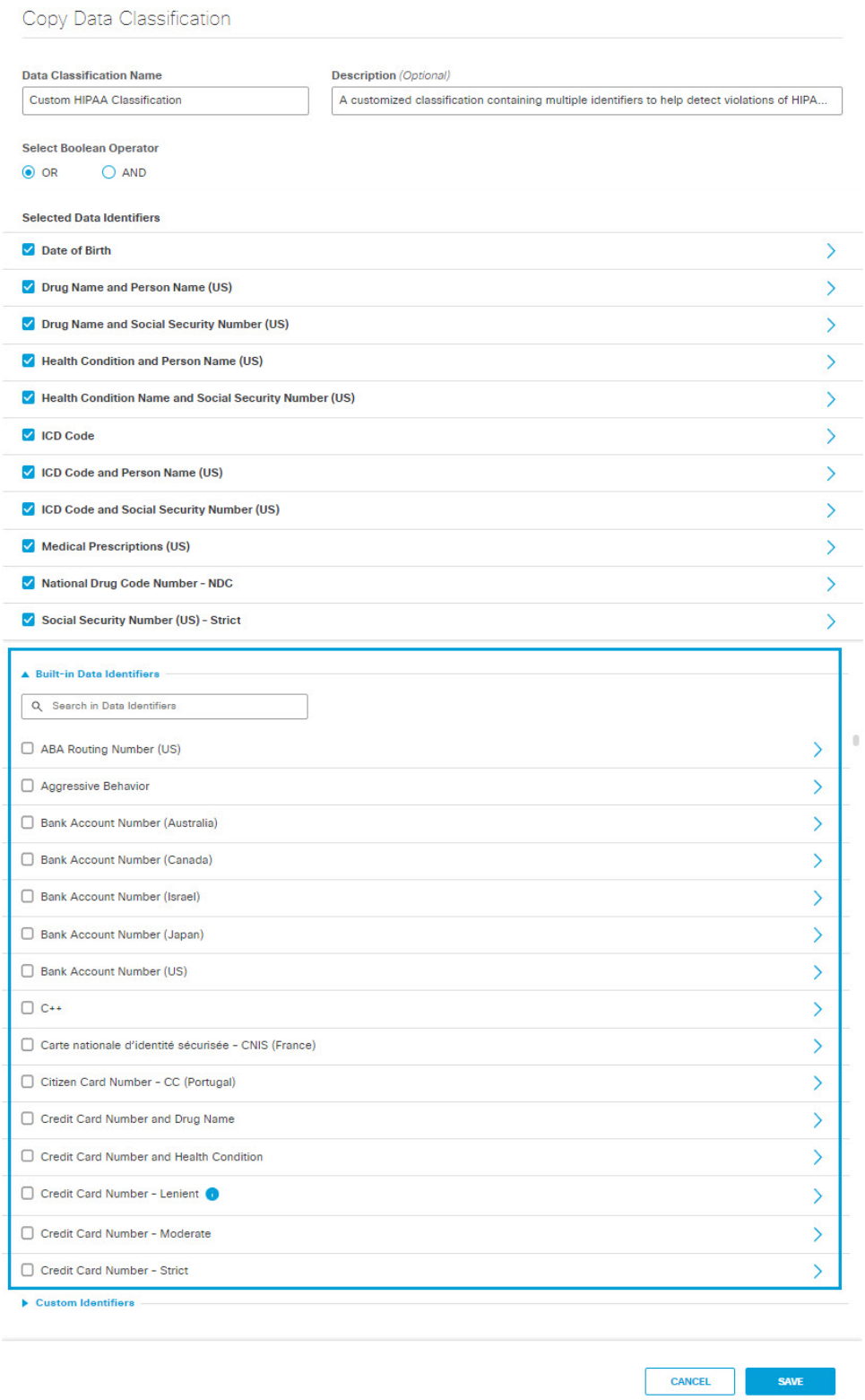
4. Make the desired changes to the new data classification. Choose from the following:
   - Change the Boolean operator
     - **OR**–At least one of the data identifiers selected must match during rule evaluation.
     - **AND**–All of the data identifiers selected must match during rule evaluation.



- Deselect pre-selected data identifiers.

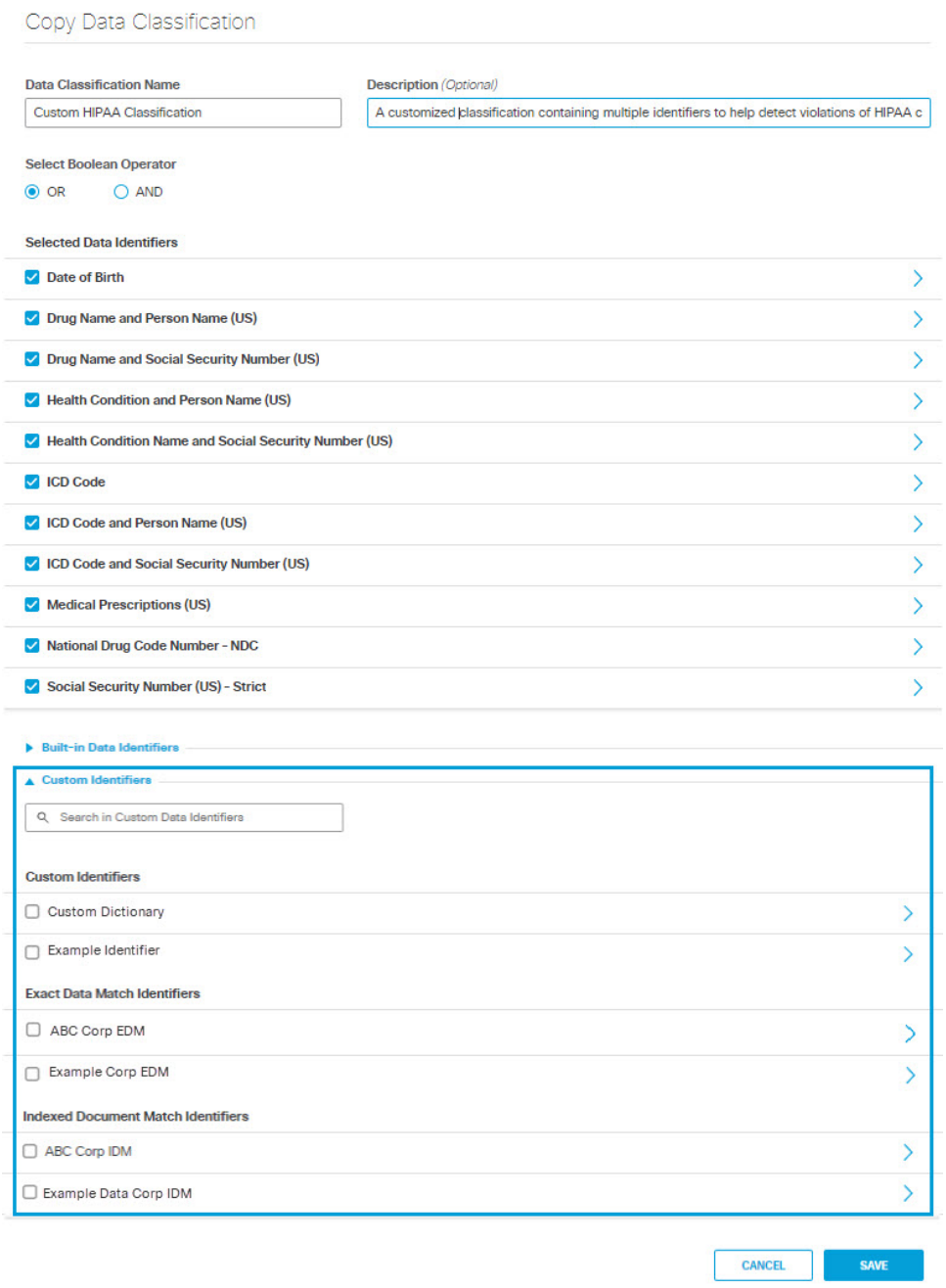


- Expand **Built-in Data Identifiers** and select additional data identifiers.

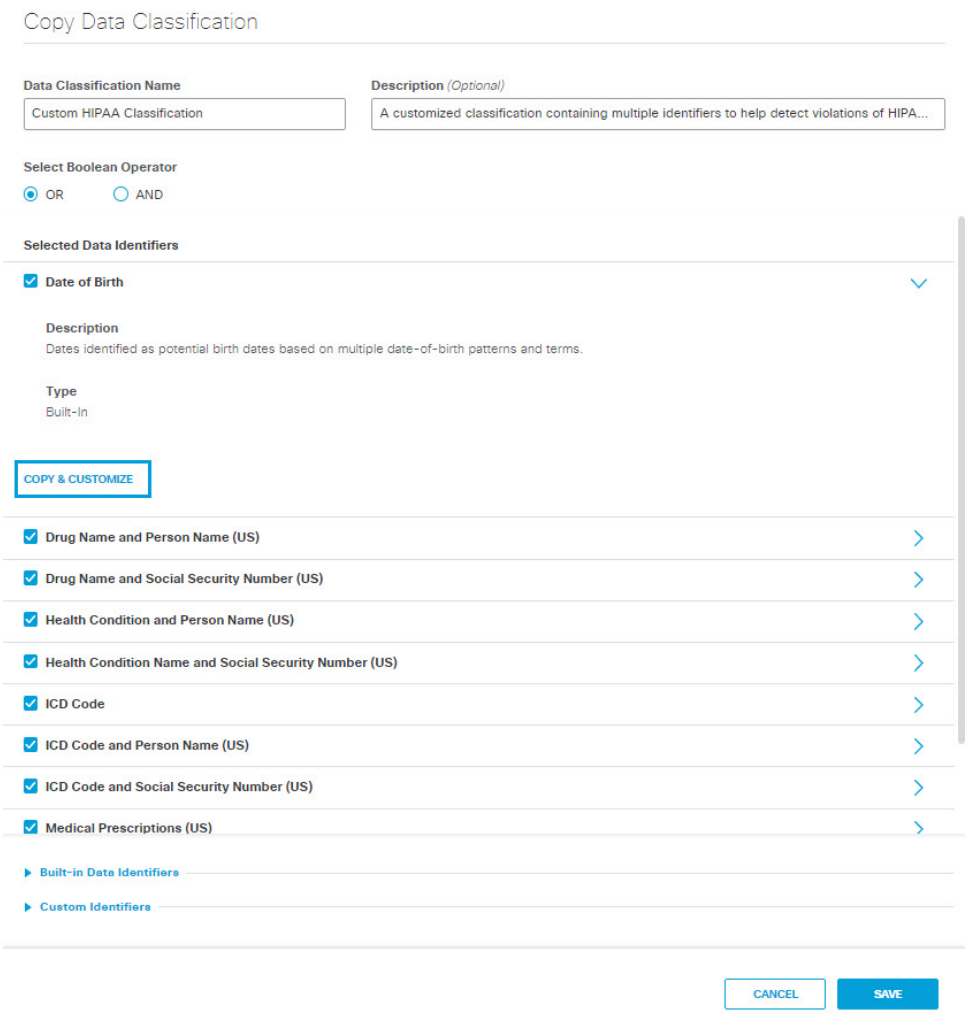


- Expand **Custom Identifiers** and select additional data identifiers (**Custom Identifiers**, **Exact Data Match Identifiers**, and **Indexed Document Match Identifiers**).

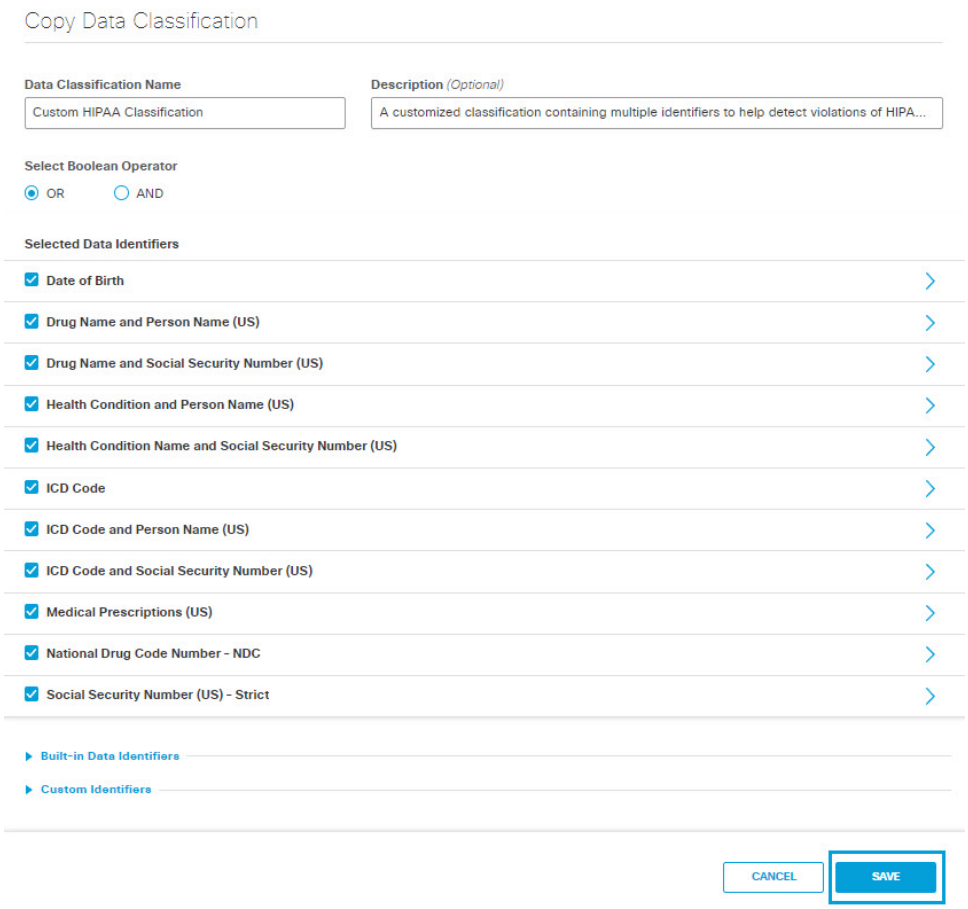
> **Note**
>
> Exact Data Match Identifiers and Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier or Create an Indexed Document Match Identifier for more information.)



- You may expand any built-in data identifier and click **COPY & CUSTOMIZE** to create a new customized data identifier. See Copy and Customize a Data Identifier.

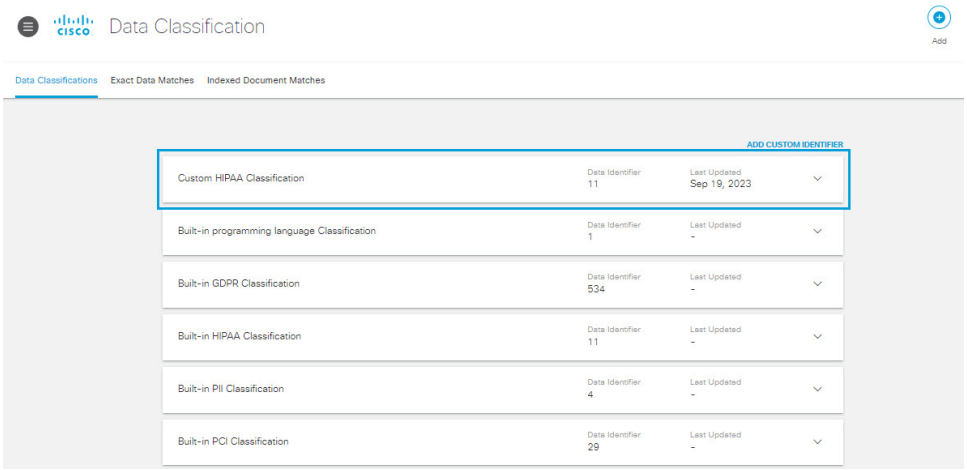

Copy Data Classification
Data Classification Name
Custom HIPAA Classification
Description (Optional)
A customized classification containing multiple identifiers to help detect violations of HIPA...
Select Boolean Operator
OR
AND
Selected Data Identifiers
Date of Birth
Description
Dates identified as potential birth dates based on multiple date-of-birth patterns and terms.
Type
Built-In
COPY & CUSTOMIZE
Drug Name and Person Name (US)
Drug Name and Social Security Number (US)
Health Condition and Person Name (US)
Health Condition Name and Social Security Number (US)
ICD Code
ICD Code and Person Name (US)
ICD Code and Social Security Number (US)
Medical Prescriptions (US)
Built-in Data Identifiers
Custom Identifiers
CANCEL
SAVE

5. Click **Save**.



What to do next

Your new classification is listed on the Data Classification page, and it will be available to you when you Add a Real Time Rule to the Data Loss Prevention Policy, Add a SaaS API Rule to the Data Loss Prevention Policy, or initiate a new Discovery Scan.



Create a Custom Identifier

Describes creating a custom identifier. A custom identifier can be used as part of a data classification to define terms and pattern expressions a DLP rule must match to generate an incident. You can optionally further restrict matching criteria using additional qualifiers:

A custom identifier can be used as part of a data classification to define terms and pattern expressions a DLP rule must match to generate an incident. You can optionally further restrict matching criteria using additional qualifiers:

- Specify a threshold, to indicate the minimum number of occurrences of a term or pattern that must appear within a document to qualify as a match.
- Specify proximity keywords, at least one of which must appear within 20 terms of a term or pattern to qualify as a match.

If you specify both a threshold and proximity keywords, a document is considered a match only if it contains a custom identifier term or pattern that appears at least the number of times indicated by threshold, and at least one of those occurrences appears within 20 terms of at least one of the proximity keywords.

> **Note**
>
> Secure Access blocks documents containing a custom identifier only if the identifier is surrounded by a word boundary. A document containing a custom identifier with an alphanumeric character (a-z, A-Z, 0-9) adjacent to it will not be blocked. For example, for the custom identifier **c.t** matches **cat** and **cot**, but not **housecat** or **citation**.

Once you create a custom identifier, you can add it to a data classification. To create a data classification, see Create a Data Classification or Copy and Customize a Built-In Data Classification.

Procedure

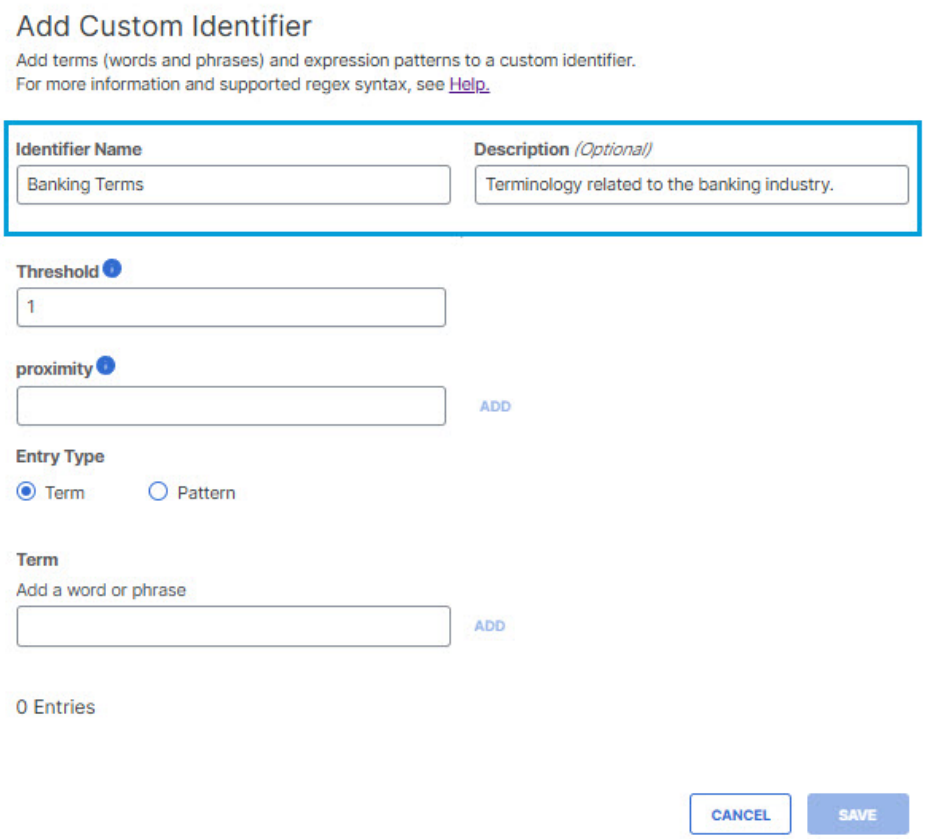
Provides instructions for adding a custom identifier.

Before you begin

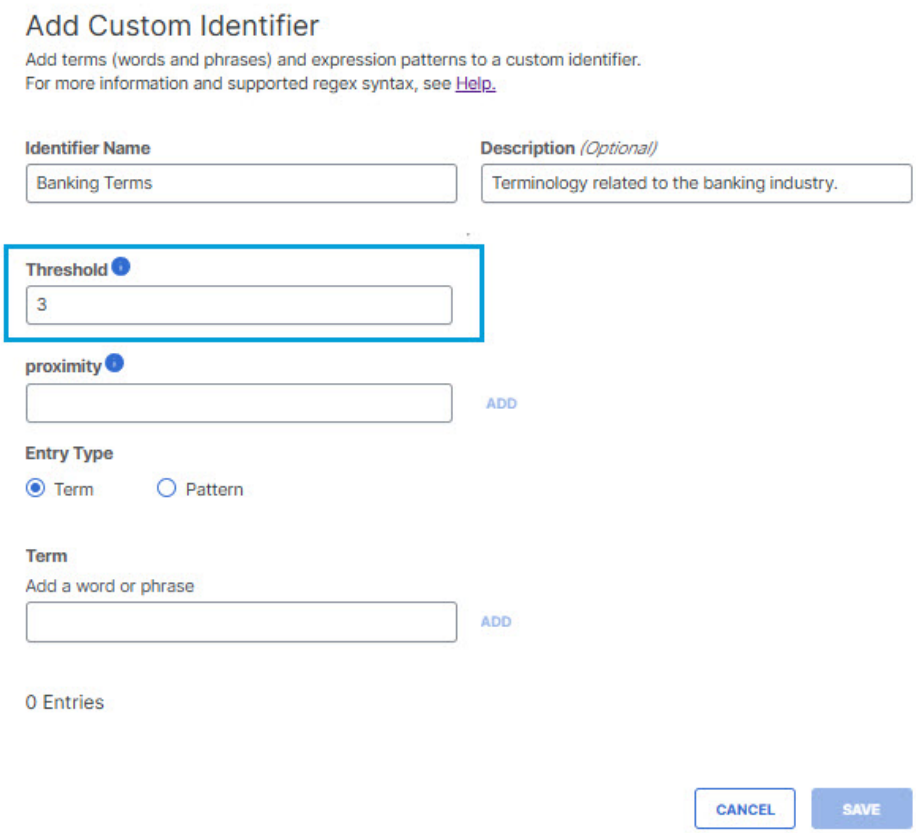
- Full Admin user role. For more information, see Manage Accounts.

Procedure

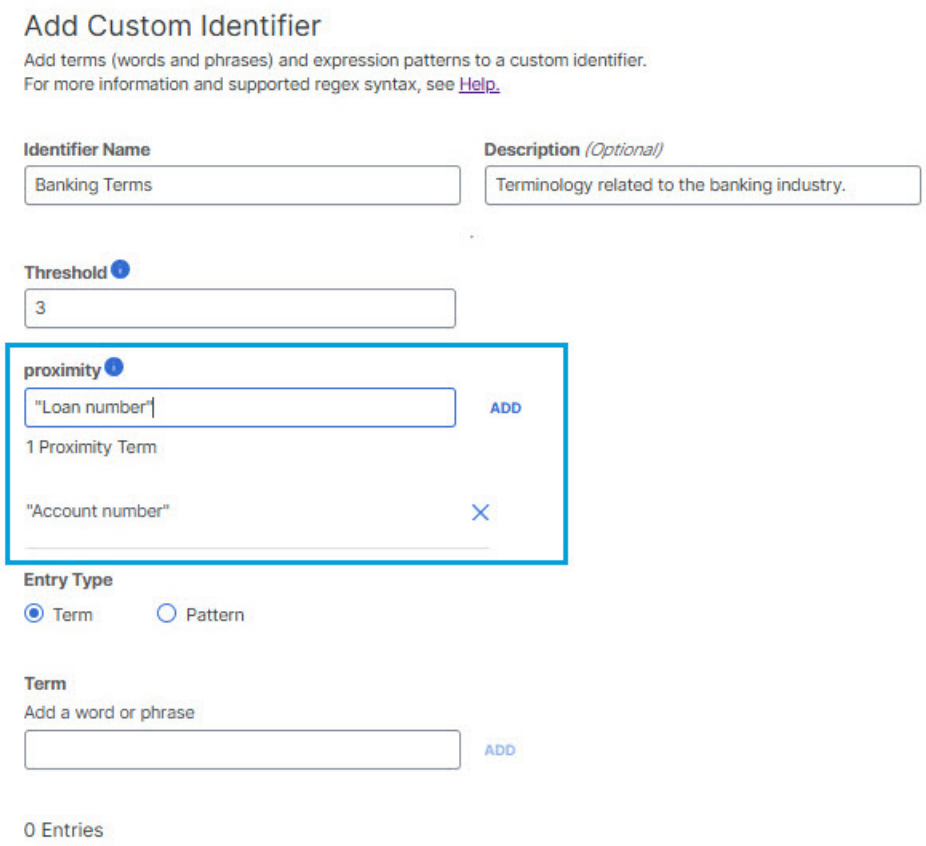
1. Navigate to **Secure** > **Settings** > **Data Classification**.
2. Click **Add Custom Identifier**.
3. Give the custom identifier a meaningful name and description.



4. (Optional) Specify the threshold for your identifier. (Legal range: 1 - 300.) This represents the number of occurrences of this identifier that must be detected in a document for Umbrella to generate an incident. A threshold of 3, for example, only generates an incident if 3 instances of the identifier are found in the file. The default threshold is 1.



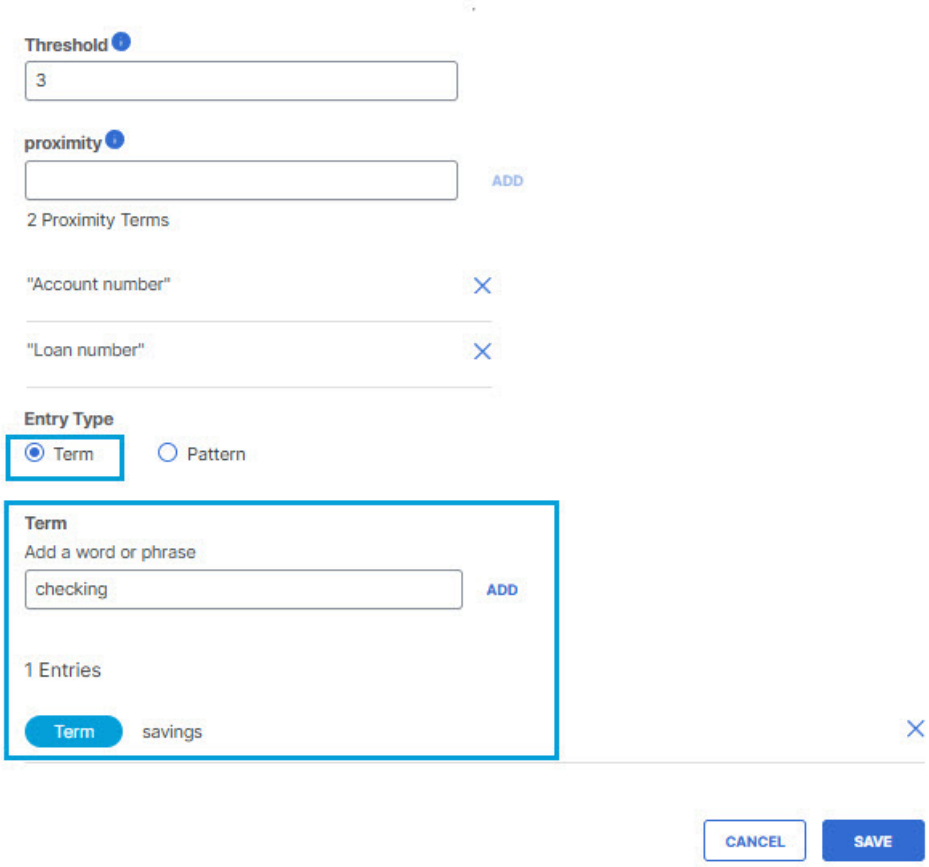
5. (Optional) Specify a proximity keyword and then click **ADD**. You can repeat this step to add up to 10 proximity keywords for your custom identifier. If you specify proximity keywords, Secure Access will not generate an incident unless at least one of the occurrences of a matching term or pattern appears within 20 terms of a proximity keyword.



6. Add terms and patterns to your custom identifier.

> **Note**
>
> You cannot upload or enter terms and patterns as a CSV. You must enter each item individually.

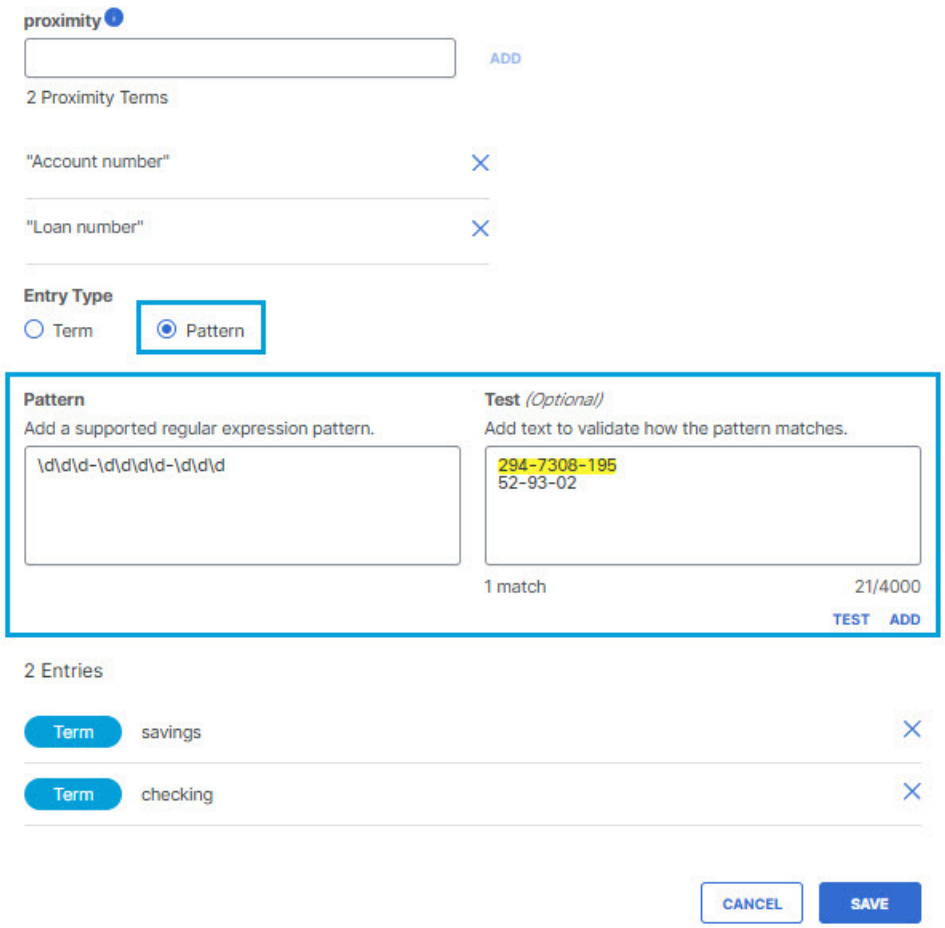
   a. For **Terms**, add up to 100 terms and click **ADD** for each term.



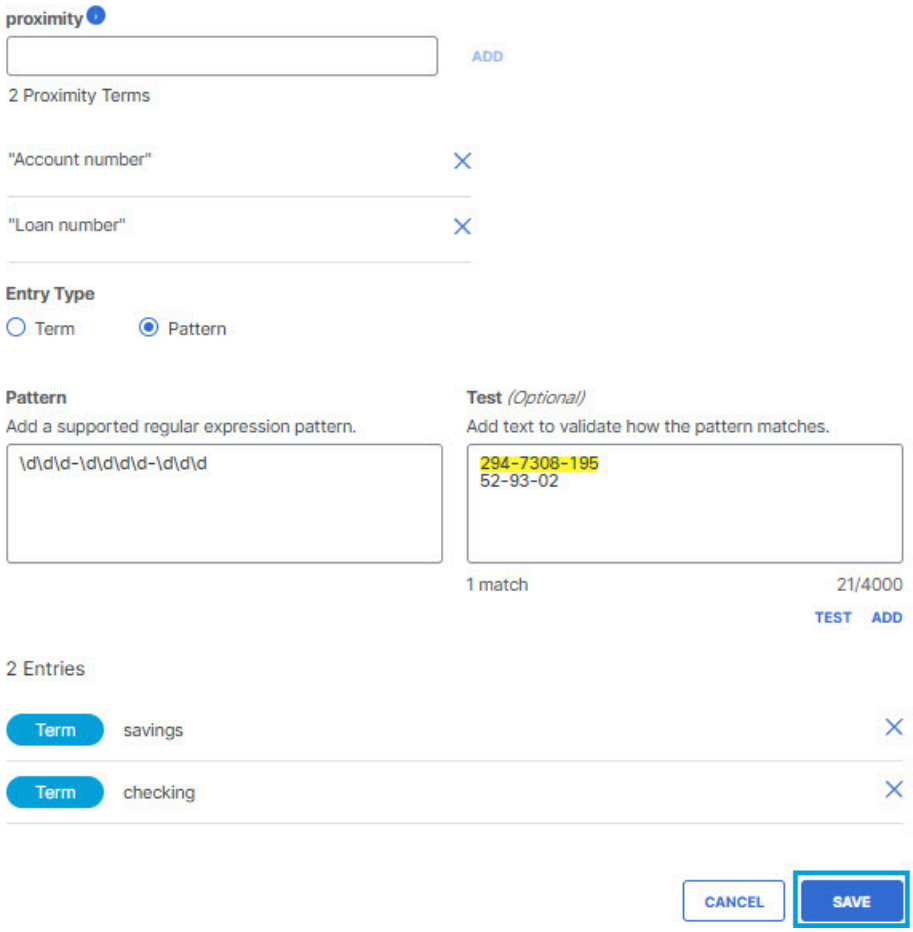
7. For **Pattern**, enter a regular expression 3-1,000 characters long. You can add up to 10 patterns to a custom identifier. For more information, see Custom Regular Expression Patterns.

   After adding a regular expression, you can enter sample text in the **Test** box, and click **TEST** to verify the pattern matches.

   Click **ADD** when you are satisfied that you have the pattern you want.

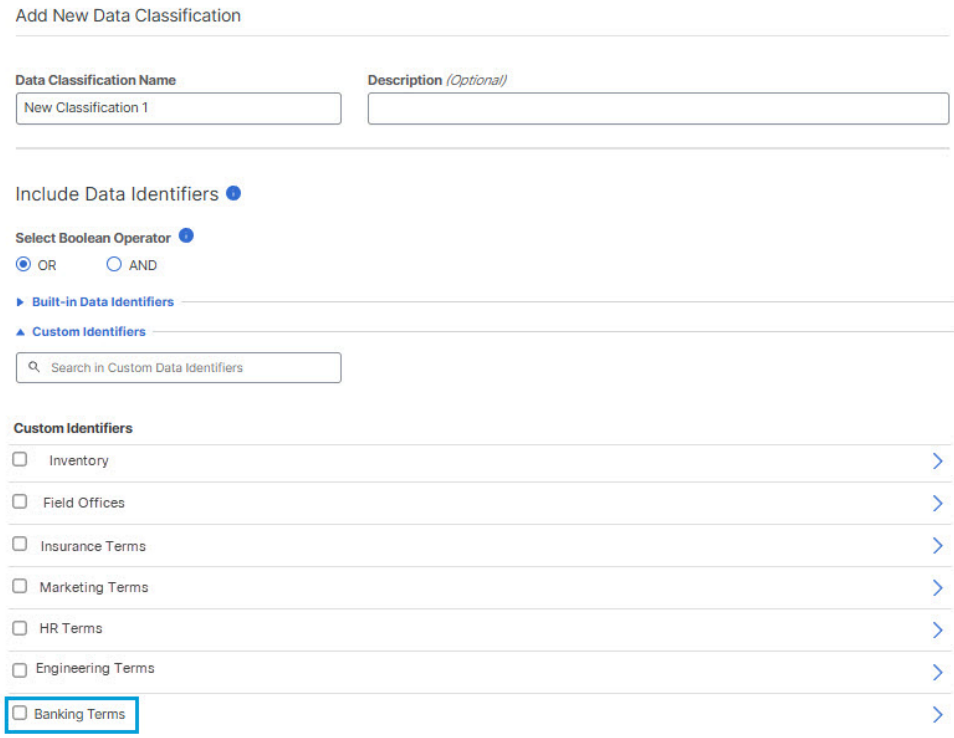

proximity
ADD
2 Proximity Terms
"Account number"
"Loan number"
Entry Type
Term
Pattern
Pattern
Add a supported regular expression pattern.
\d\d\d-\d\d\d\d-\d\d\d
Test (Optional)
Add text to validate how the pattern matches.
294-7308-195
52-93-02
1 match
21/4000
TEST
ADD
2 Entries
Term
savings
Term
checking
CANCEL
SAVE

8. Click **SAVE**.



What to do next

Your custom dictionary appears under Custom Identifiers when editing or creating a classification. (See Create a Data Classification or Copy and Customize a Built-In Data Classification.)



Custom Regular Expression Patterns

Describes custom regular expression patterns. Custom regular expression patterns for DLP data classifications support basic Java syntax with some limitations.

> **Note**
>
> You must create your own regex. The creation of custom regex is outside the scope of Secure Access Support.

Custom regular expression patterns for DLP data classifications support basic Java syntax with some limitations.

Limitations

Describes limitations. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

General

Describes general. A regex can have a maximum of 150 characters. A custom dictionary can have a maximum of 10 regex.

- A regex can have a maximum of 150 characters.
- A custom dictionary can have a maximum of 10 regex.
- A custom dictionary can have a maximum of 100 entries.
- The minimum length of a regex pattern is 3.
- The maximum number of matches for a regex is 1000.

Regex Syntax

Describes regex syntax. Anchor Flags^ can not be used as an input start position.$ can not be used as an input end position.

- Anchor Flags
  - `^` can not be used as an input start position.
  - `$` can not be used as an input end position.
- Back References
  - `\n` cannot be used to reference a previous capture group n.

The following must be used for these character definitions:

- Whitespace–`'\u0020'`
- Dash–`'\u002D'`
- Single quote–`(char)0x0027`
- Double quote–`'\u0022'`

Regex Breadth

Describes regex breadth. Wildcards.* and .+ are not accepted.()* and ()+ are not accepted. .* and .+ are not accepted. ()* and ()+ are not accepted.

- Wildcards
  - `.*` and `.+` are not accepted.
  - `()*` and `()+` are not accepted.
- `|` alternations have a maximum of 20 per pattern.

Word Boundary

Describes word boundary. The regular expression is wrapped in a word boundary to ensure it matches the entire word. Words are comprised of alphanumeric character (a-z, A-Z, 0-9) and the boundary cannot contain a word character on each side of the boundary.

The regular expression is wrapped in a word boundary to ensure it matches the entire word. Words are comprised of alphanumeric character (a-z, A-Z, 0-9) and the boundary cannot contain a word character on each side of the boundary.

Example:When the regular expression is `cat`, the sentence "The cat chased the mouse" will match, but "The catchased the mouse" will not match.

Individual Data Identifiers

Describes individual data identifiers. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

These identifiers only appear in combination with other identifiers.

Drug Name

Describes drug name. Drug Name is a content identifier that identifies unique drug names as referenced in the "Orange Book" (Approved Drug Products with Therapeutic Equivalence Evaluations) published by the US Food and Drug Administration (FDA). It is available from the FDA.

Drug Name is a content identifier that identifies unique drug names as referenced in the "Orange Book" (*Approved Drug Products with Therapeutic Equivalence Evaluations*) published by the US Food and Drug Administration (FDA). It is available from the FDA.

Health Condition

Describes health condition. Health Condition is a content identifier that detects health conditions based on a comprehensive dictionary. The dictionary of health conditions is compiled from https://www.cdc.gov/nndss/index.html.

Health Condition is a content identifier that detects health conditions based on a comprehensive dictionary. The dictionary of health conditions is compiled from https://www.cdc.gov/nndss/index.html.

ICD-10 Code

Describes icd-10 code. The International Statistical Classification of Diseases and Related Health Problems (ICD) is a classification list compiled by the World Health Organization (WHO) for the purpose of coding diseases, signs and symptoms, abnormal findings, complaints, social circumstances, and external causes of injury or diseases.

The International Statistical Classification of Diseases and Related Health Problems (ICD) is a classification list compiled by the World Health Organization (WHO) for the purpose of coding diseases, signs and symptoms, abnormal findings, complaints, social circumstances, and external causes of injury or diseases. This policy identifies content in the 11th revision of ICD.

US Person Name

Describes us person name. Person name is a content identifier used in numerous policies. It is backed by US Census information.

Person name is a content identifier used in numerous policies. It is backed by US Census information.

45 Manage SaaS API Data Loss Prevention

Topics:

- Enable SaaS API Data Loss Protection for Box Tenants
- Enable SaaS API Data Loss Protection for Dropbox Tenants
- Enable SaaS API Data Loss Protection for Google Drive Tenants
- Enable SaaS API Data Loss Protection for Microsoft 365 Tenants
- Enable SaaS API Data Loss Protection for Webex Teams

Introduces managing saas api data loss prevention. The Data Loss Prevention (DLP) policy helps to protect sensitive data uploaded to the web. It can discover and protect sensitive data stored and shared in your cloud-sanctioned applications.

The Data Loss Prevention (DLP) policy helps to protect sensitive data uploaded to the web. It can discover and protect sensitive data stored and shared in your cloud-sanctioned applications. Granting Secure Access permissions to the APIs of customers' cloud tenants allows for discovering malicious files and files with data violations. You can enable more than one tenant of a supported platform. For example, a school administrator, with an instance of Box for faculty and another instance for students, can enable both tenants. This results in complete malware protection and data loss prevention for Box.

Note

Secure Access does not save the tenant credentials. For revocation and re-authorization, insert the credentials again.

You can authorize the following platforms, all of which have support for both Cloud Malware and DLP.

- Box - Cloud Malware and Data Loss Prevention
- Dropbox - Cloud Malware and Data Loss Prevention
- Google Drive - Cloud Malware and Data Loss Prevention
- Microsoft 365 (Sharepoint and OneDrive) - Cloud Malware and Data Loss Prevention
- Webex Teams - Cloud Malware and Data Loss Prevention

Enable SaaS API Data Loss Protection for Box Tenants

Describes enabling saas api data loss protection for box tenants. To apply DLP SaaS API rules to files in a Box tenant, you must authorize the tenant using the procedure described below.

To apply DLP SaaS API rules to files in a Box tenant, you must authorize the tenant using the procedure described below. Once the tenant is authorized, for each file residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

Authorize a Tenant

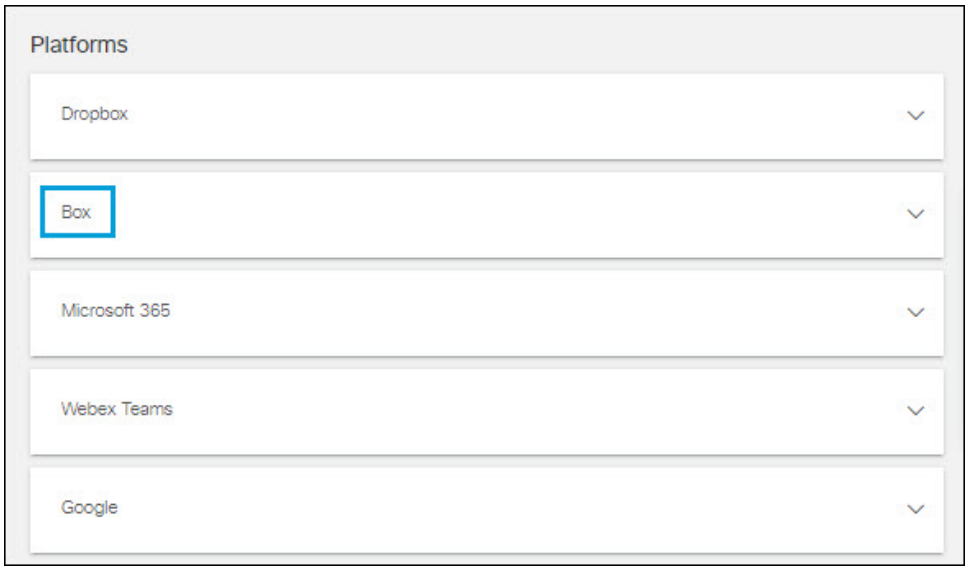
Provides instructions for authorizing a Box tenant.

Before you begin

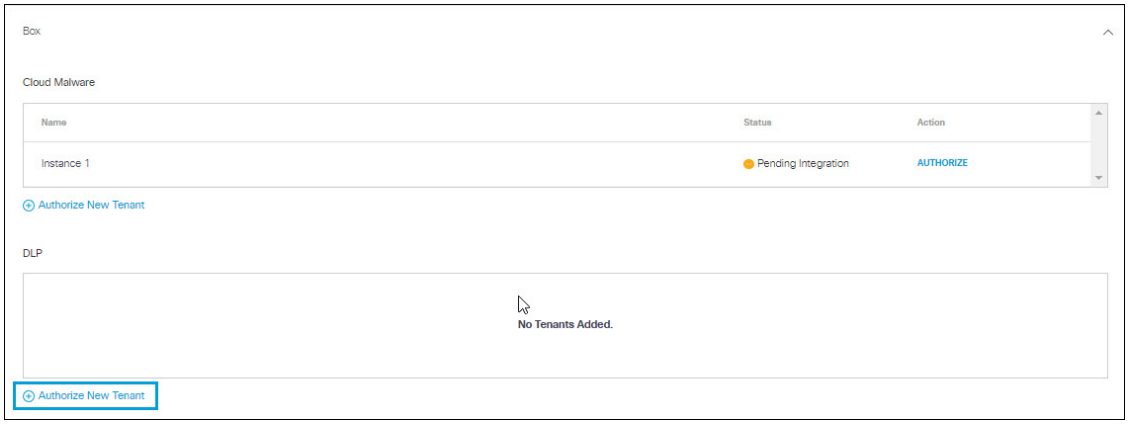
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization).
- The user performing the installation *must* use a Box account with Box admin privileges. (Co-admin privileges are insufficient.)

Procedure

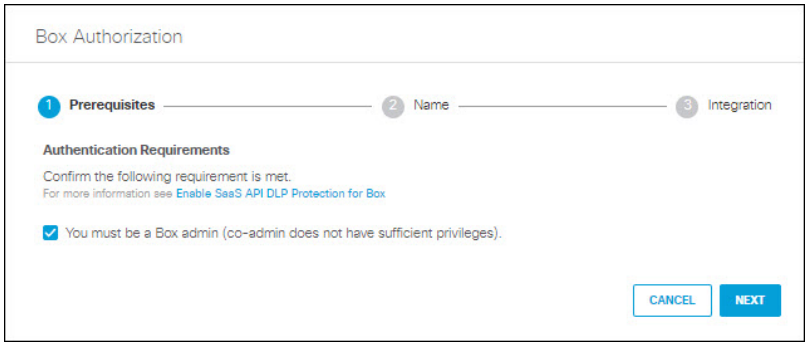
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Box**.



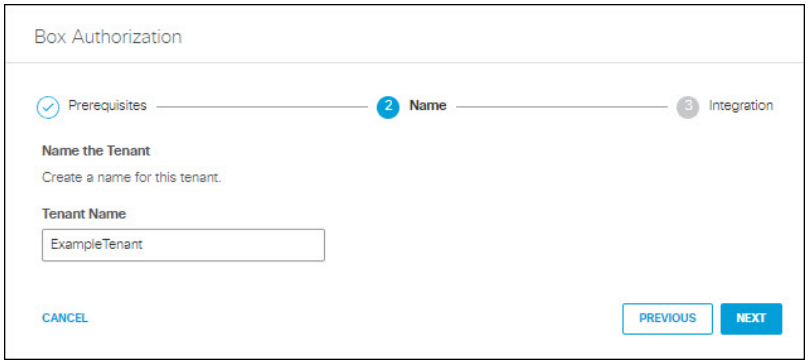
3. In the DLP subsection, click **Authorize New Tenant** to add a Box tenant to your Secure Access environment.



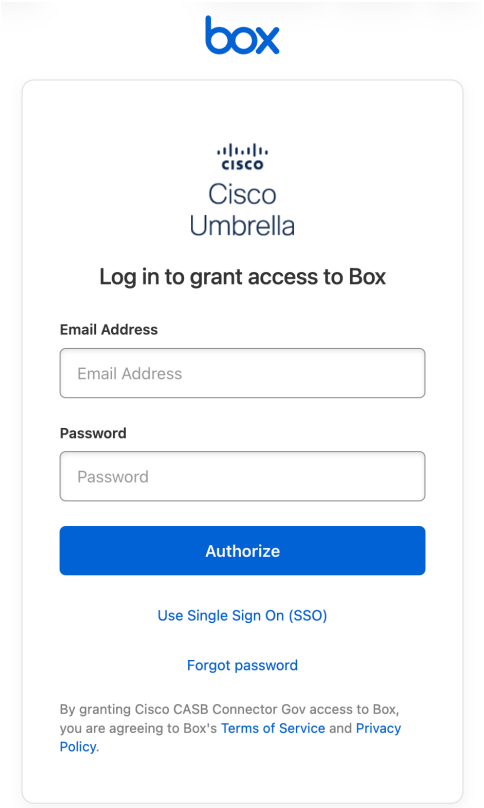
4. In the **Box Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



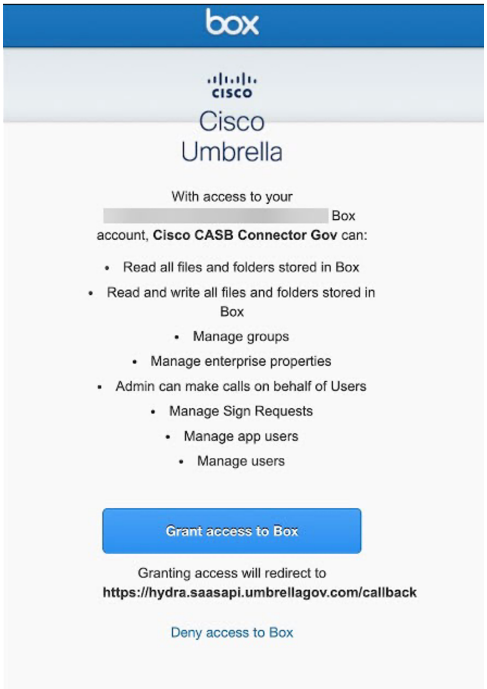
5. Enter the name of your tenant, then click **Next**.



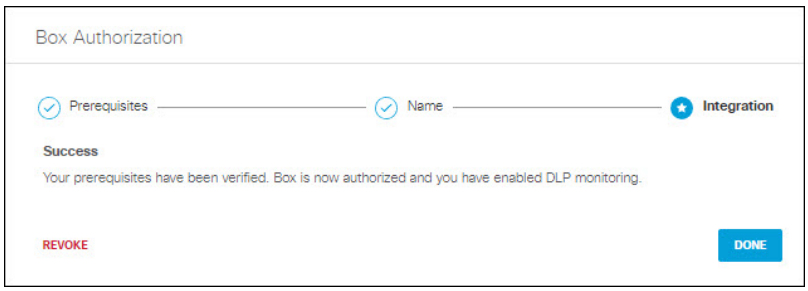
6. Click **Next** to be redirected to the Box login page.
7. Log in to Box with admin privileges to grant access.



8. Click **Grant access to Box** to complete the authorization.



9. You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.

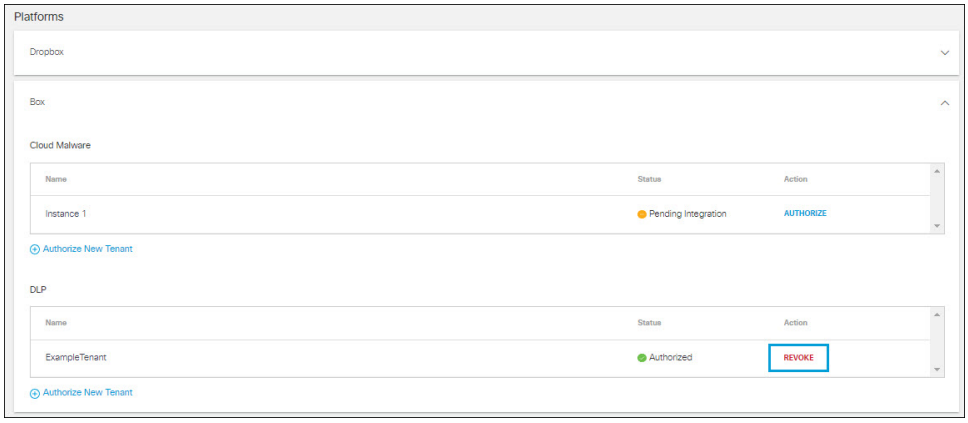


Revoke Authorization

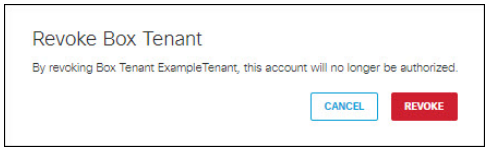
Provides instructions for revoking authorization.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



Enable SaaS API Data Loss Protection for Dropbox Tenants

Describes enabling saas api data loss protection for dropbox tenants. Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- It is recommended to use a service account for the installation.

Limitation

Describes limitation. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

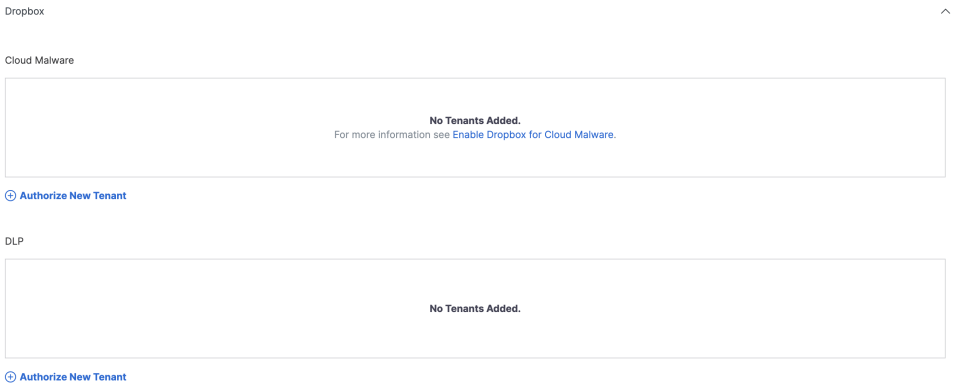
- Secure Access supports SaaS API Data Loss Prevention only for Dropbox Enterprise accounts.

Authorize a Tenant

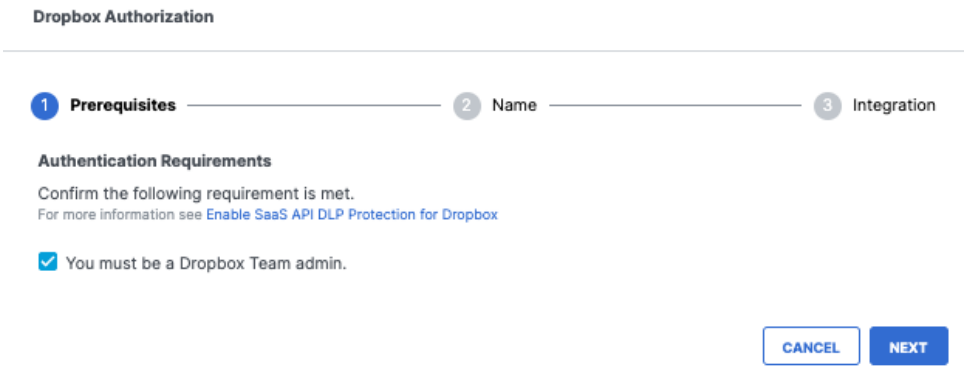
Provides instructions for authorizing a Dropbox tenant.

Procedure

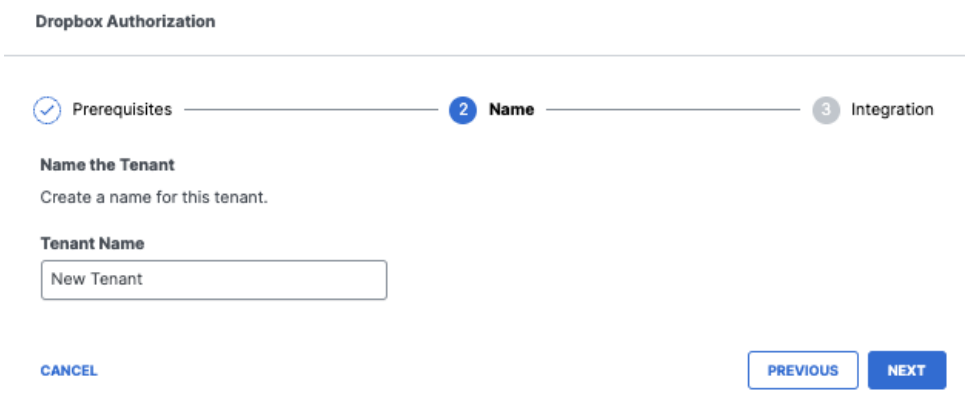
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Dropbox**.
3. Under **DLP**, click **Authorize New Tenant** to add a Dropbox tenant to your Secure Access environment.



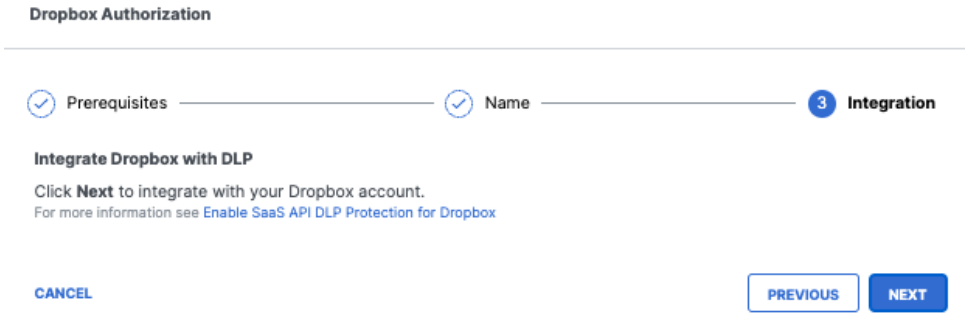
4. In the **Dropbox Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



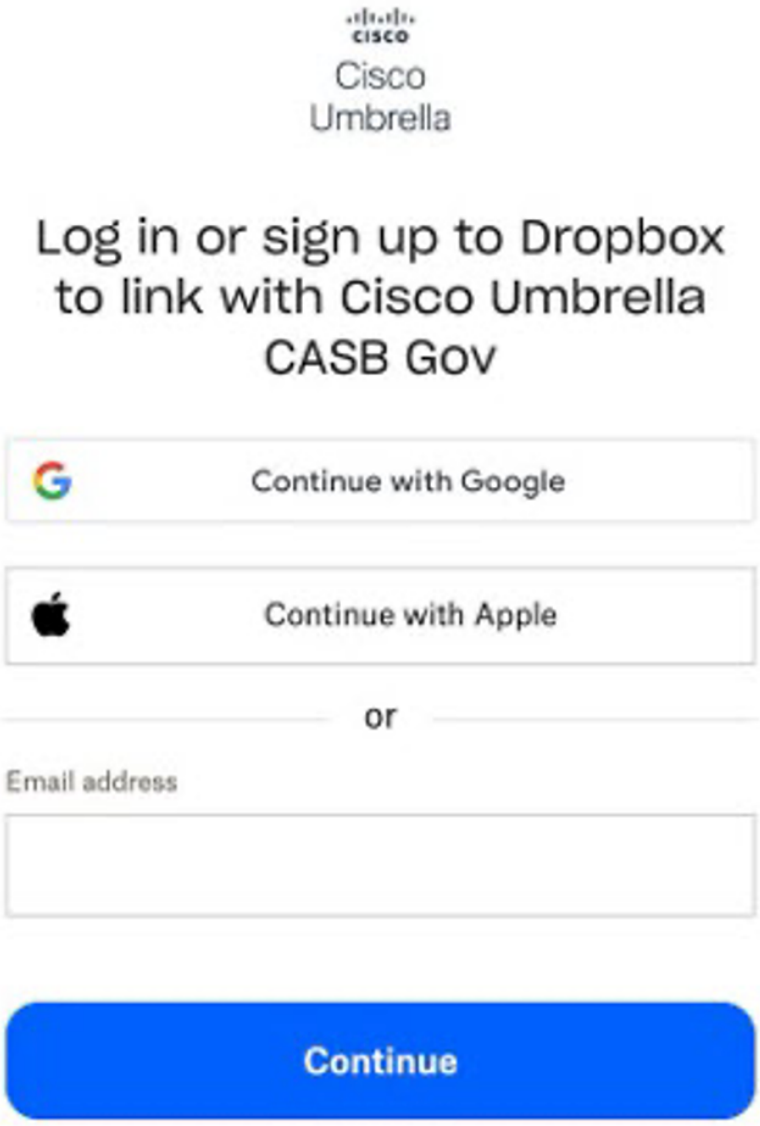
5. Enter the tenant name, then click **Next**.



6. Click **Next** to be redirected to the Dropbox login page.



7. Log in to Dropbox with Dropbox Team admin credentials to grant access.



8. You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may take up to eight hours for the integration to be confirmed and appear as **Authorized**.
9. Click **Done** to complete.

Revoke Authorization

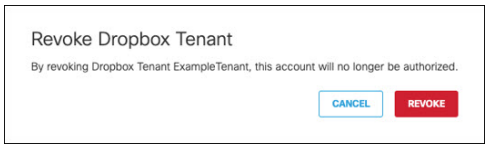
Provides instructions for revoking authorization.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



Enable SaaS API Data Loss Protection for Google Drive Tenants

Describes enabling saas api data loss protection for google drive tenants. Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Cisco CASB Gov must be installed in the tenant by a Google Admin User.
- It is recommended to use a service account for the installation.

Validation

Provides instructions for validation. Log in to https://admin.google.com with admin credentials. Navigate to Apps Google Workspace Marketplace Apps App List .

Procedure

1. Log in to https://admin.google.com with admin credentials.
2. Navigate to **Apps** > **Google Workspace Marketplace Apps** > **App List**.
3. Ensure that the **Cisco CASB Gov** application is present and enabled for your admin or for the group you are a part of.
4. Navigate to **Apps** > **Google Workspace** > **Drive And Docs** and ensure that the drive service is enabled for your admin or for a group you are part of.

What to do next

The Secure Access DLP Connector needs access to your Google account. This allows Secure Access DLP Connector to:

View, Edit, Create, and Delete all of your Google Drive files

View domains related to your customers

View groups on your domain

View organization units on your domain

View and manage the provisioning of users on your domain

View Information about users on your domain

View audit reports for your G suite domain

View usage reports for your G suite domain

View, Edit, Configure, and Delete your Google Cloud data and view the email address for your Google Account

View your primary Google Account email address

View your personal information that is made publicly available

Manage your sites

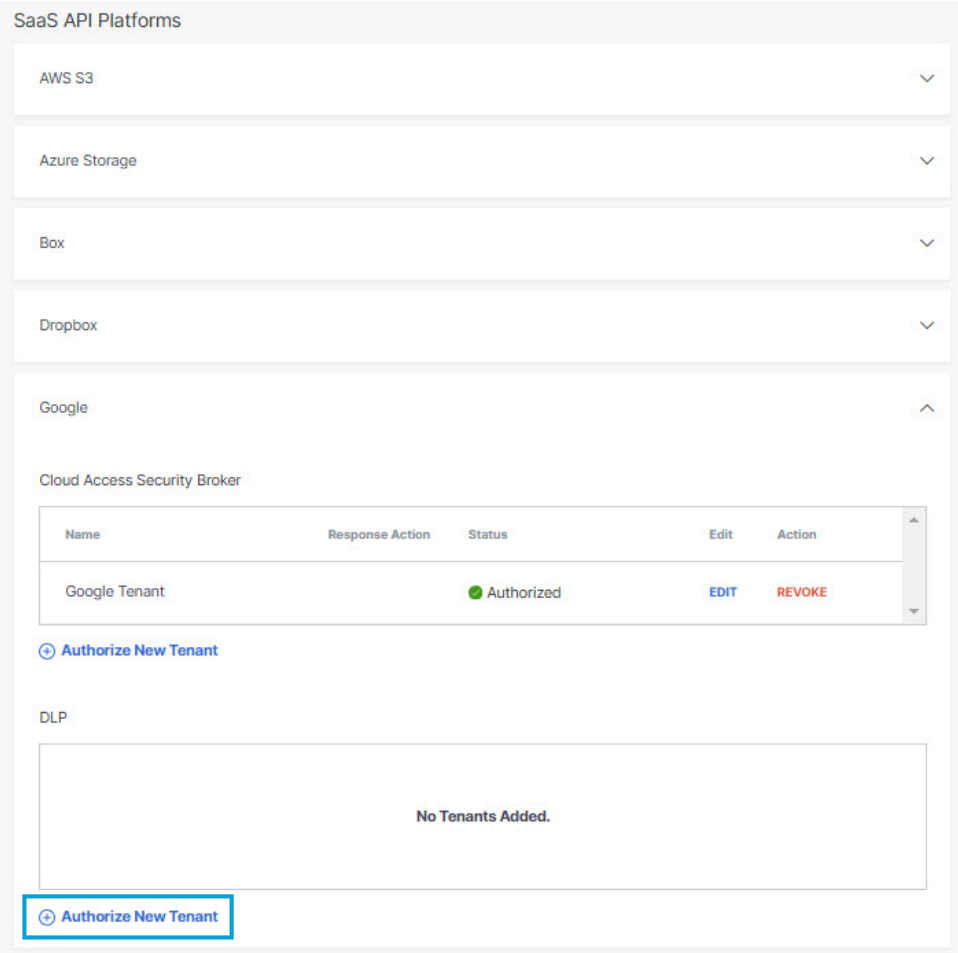
View the activity history of your Google apps

Authorize a Tenant

Provides instructions for authorizing a Google Drive tenant.

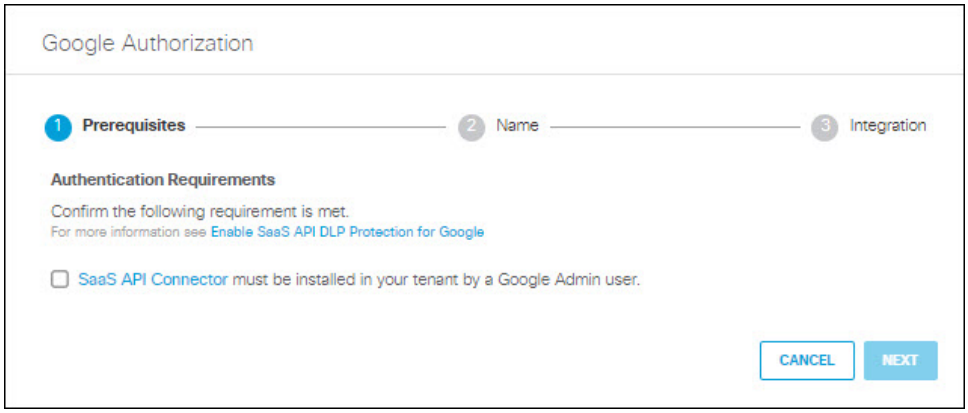
Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **SaaS API Platforms**, click **Google**.
3. Click **Authorize New Tenant** to add a Google Drive tenant to your Secure Access environment.

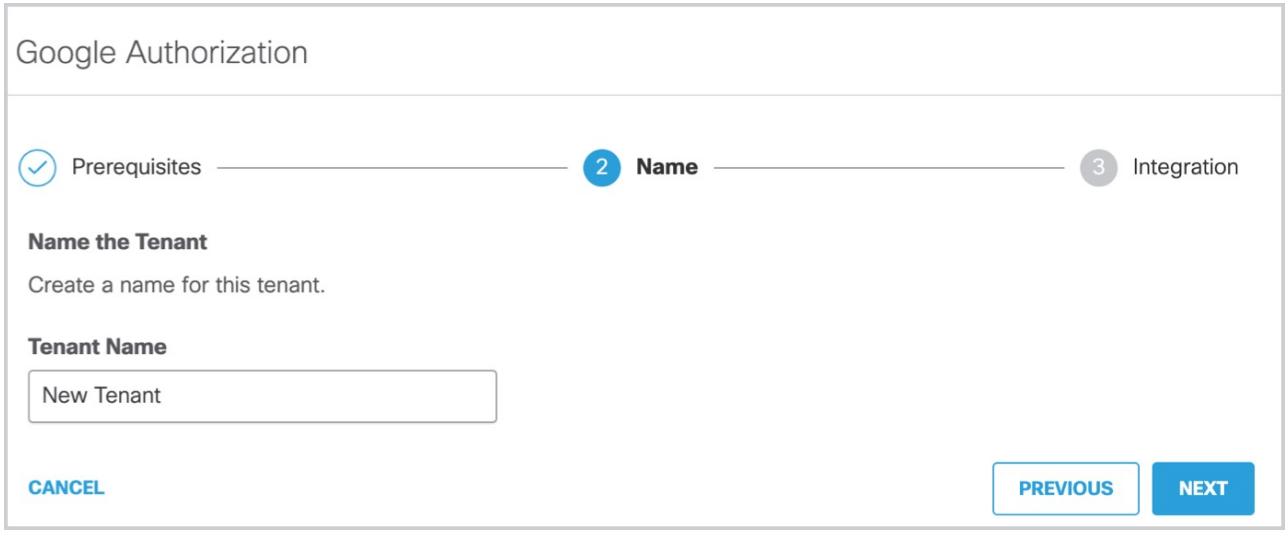


4. In the **Google Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.

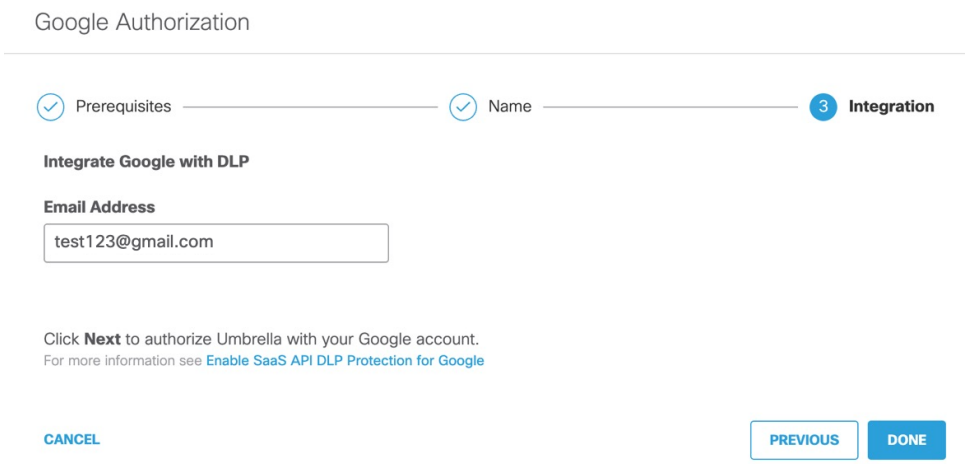
> **Note**
>
> The link to the SaaS API Connector brings you to the Umbrella DLP Connector site in the Google Workspace Marketplace. This is correct, despite the nomenclature difference.



5. Enter the tenant name, then click **Next**.



6. Enter the **Email Address**, then click **Next**.



You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may be up to 8 hours for the integration to be confirmed and appear as **Authorized**.

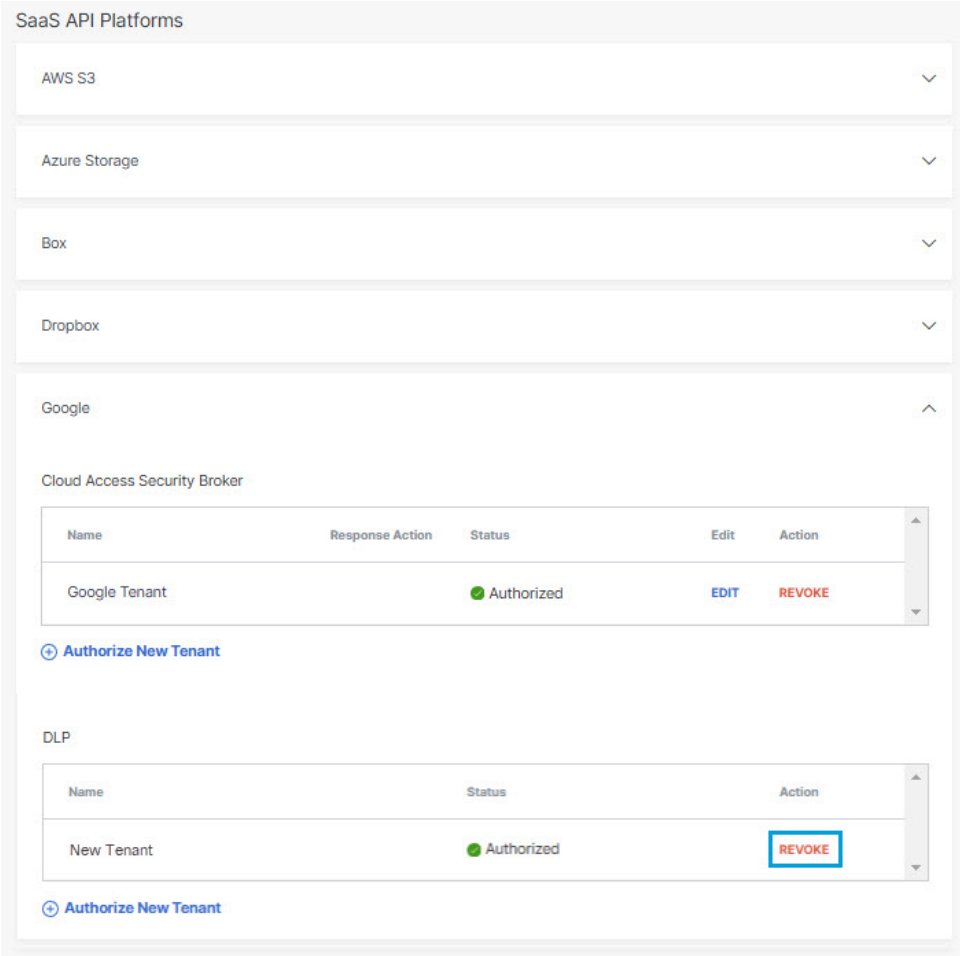
7. Click **Done** to complete.

Revoke Authorization

Provides instructions for revoking authorization.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.

Enable SaaS API Data Loss Protection for Microsoft 365 Tenants

Describes enabling saas api data loss protection for microsoft 365 tenants. You can enable SaaS API Data Loss prevention for authorized tenants that use the following Microsoft 365 applications:

You can enable SaaS API Data Loss prevention for authorized tenants that use the following Microsoft 365 applications:

- Sharepoint Online
- OneDrive

> **Note**
>
> You cannot add an application to an existing tenant. If you have an existing Microsoft 365 tenant that uses one or two of these applications and you wish to add another application to that tenant, you must first revoke authorization for the existing tenant, then create a new tenant using all the desired applications.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- The user performing the installation *must* use a service account with a Microsoft 365 Global Admin and active license
- SharePoint Online and OneDrive must be enabled
- Audit log must be enabled for Microsoft 365. For more information, refer to Microsoft technical documentation and search for **Turn auditing on or off.**
- The following IP address must be allowed if there are Firewall rules that prevent third-party applications:

  18.253.223.180
- Users must have the following API permissions for Microsoft:

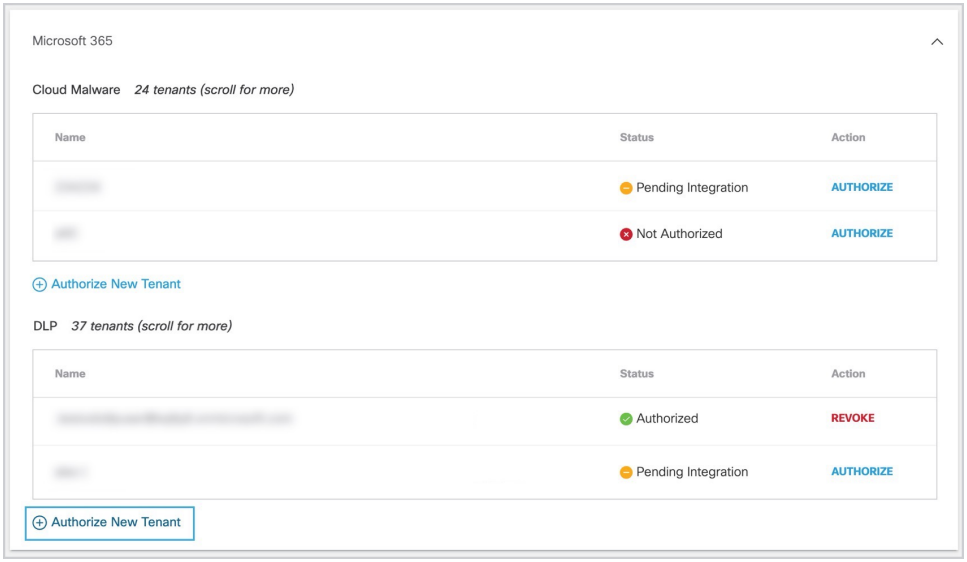
API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
Directory.Read.All	Application	Read directory data	Yes
Files.Read.All	Delegated	Read all files that user can access	No
Files.Read.All	Application	Read files in all site collections	Yes
Sites.Read.All	Delegated	Read items in all site collections	No
User.Read	Delegated	Sign in and read user profile	No
User.Read.All	Application	Read all users' full profiles	Yes
Microsoft 365 Management APIs			
ActivityFeed.Read	Application	Read activity data for the Organization	Yes
SharePoint			
Site.FullControl.All	Application	Full control of all site collections	Yes
User.Read.All	Application	Read user profiles	Yes

Authorize a Tenant

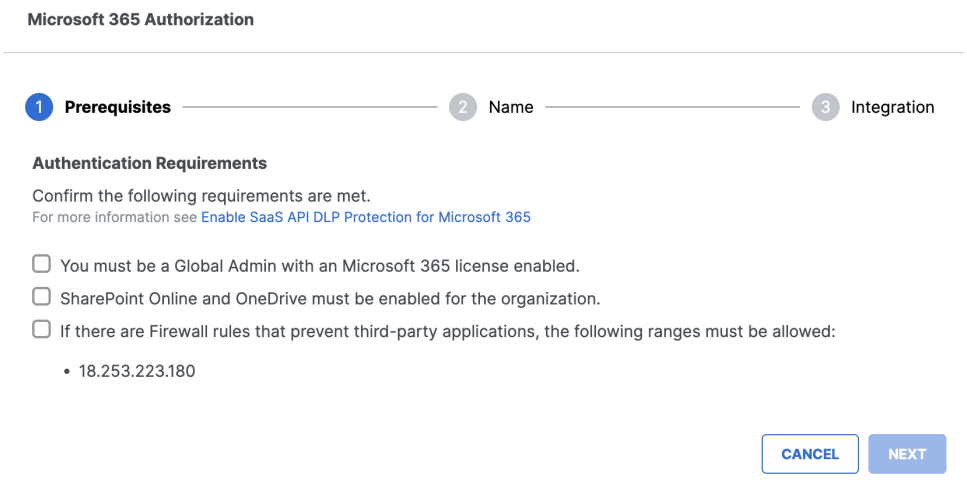
Provides instructions for authorizing a Microsoft 365 tenant.

Procedure

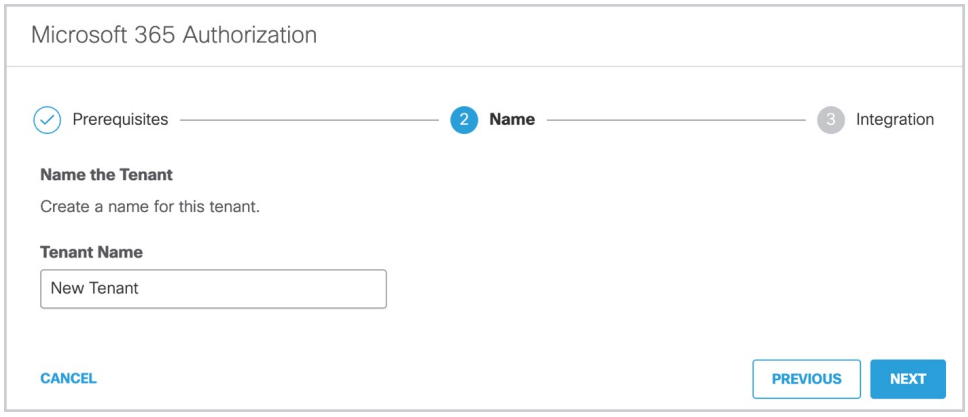
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Microsoft 365**.



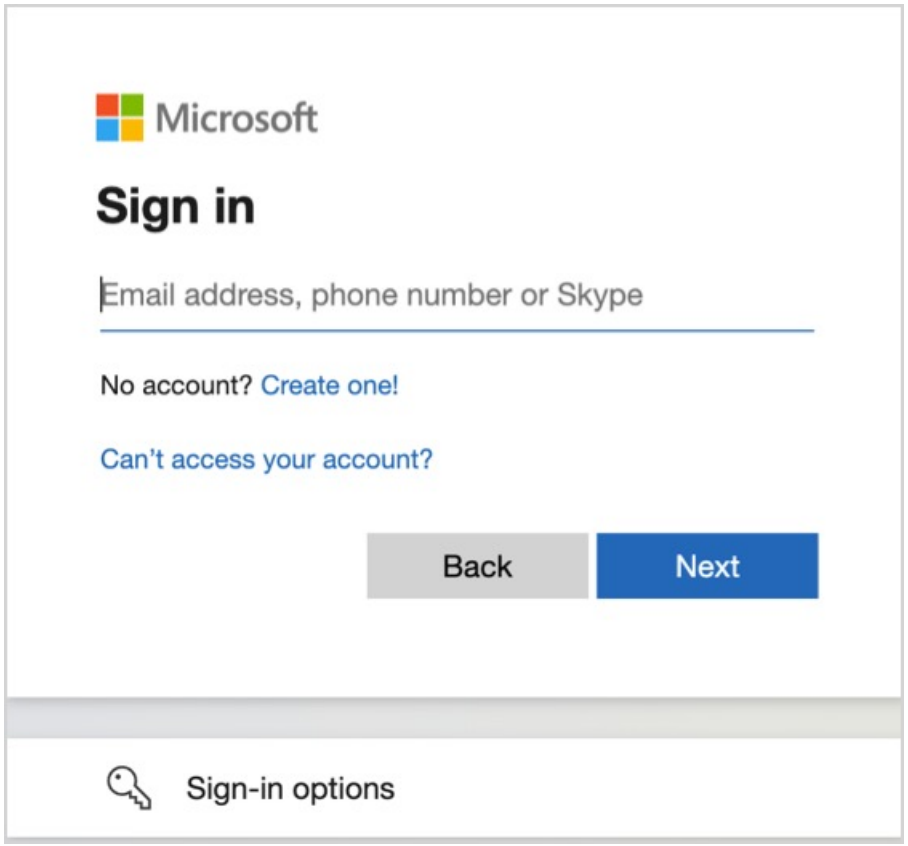
3. Click **Authorize New Tenant** in the **DLP** subsection to add a Microsoft 365 tenant to your Secure Access environment.
4. In the **Microsoft 365 Authorization** dialog, check the checkboxes to verify you meet the prerequisites, then click **Next**.



5. Provide a name for your tenant, then click **Next**.



6. Click **Next** to be redirected to the Microsoft 365 login page.
7. Log in to Microsoft 365 with admin credentials to grant access.



You are redirected to Secure Access and a message appears showing the integration was successful.

8. Click **Done** to complete.

Revoke Authorization

Provides instructions for revoking authorization for a Microsoft 365 tenant.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is not authorized.



Enable SaaS API Data Loss Protection for Webex Teams

Describes enabling saas api data loss protection for webex teams. Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)

Prerequisites

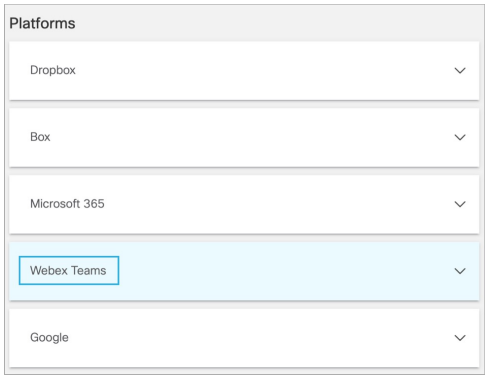
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Full Administrator Privileges in Webex Teams and the Compliance Officer role
- The `EventsAPI` in your Webex Teams instance must be enabled. Contact your Webex Teams support team to ensure that the `EventsAPI` is turned on.

Authorize a Tenant

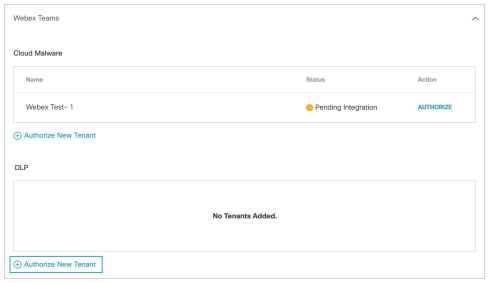
Provides instructions for authorizing a Webex Teams tenant.

Procedure

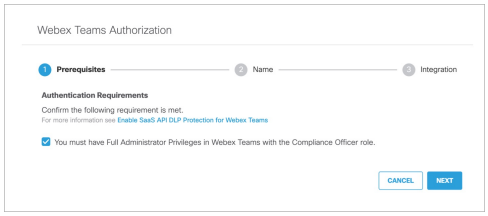
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Webex Teams**.



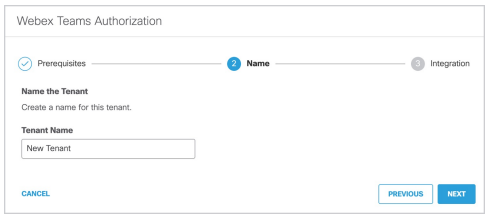
3. In the DLP subsection, click **Authorize New Tenant** to add a Webex Teams tenant to your Secure Access environment.



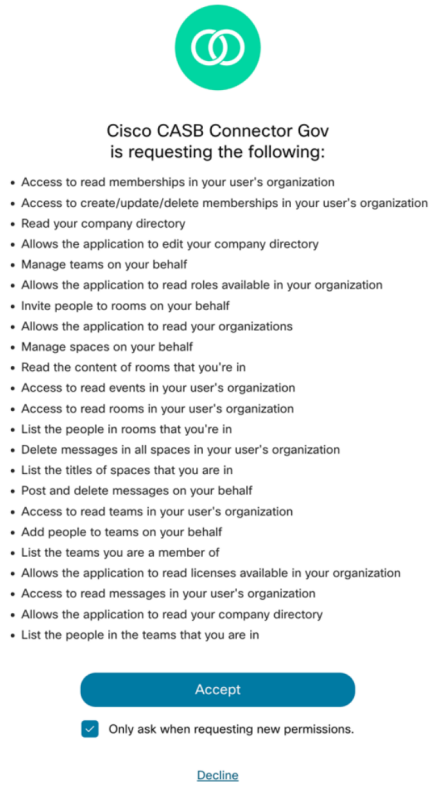
4. In the **Webex Teams Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



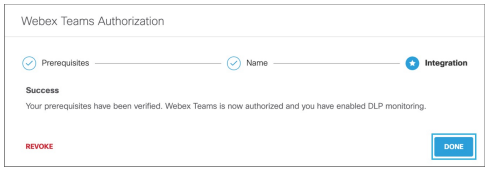
5. Enter the name of your tenant, then click **Next**.



6. Click **Next** to complete the integration.
7. Click **Accept** to complete the authorization.



8. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.

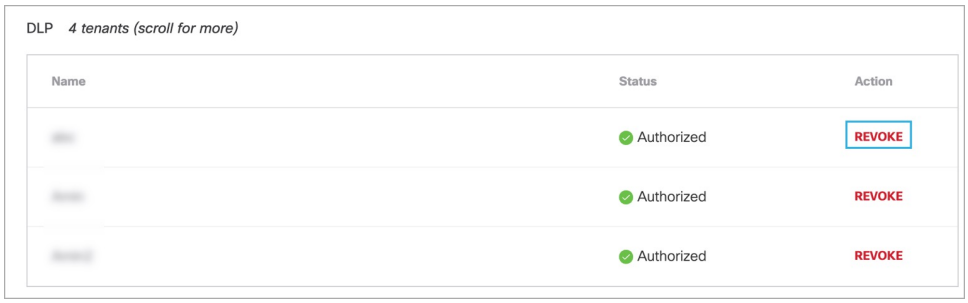


Revoke Authorization

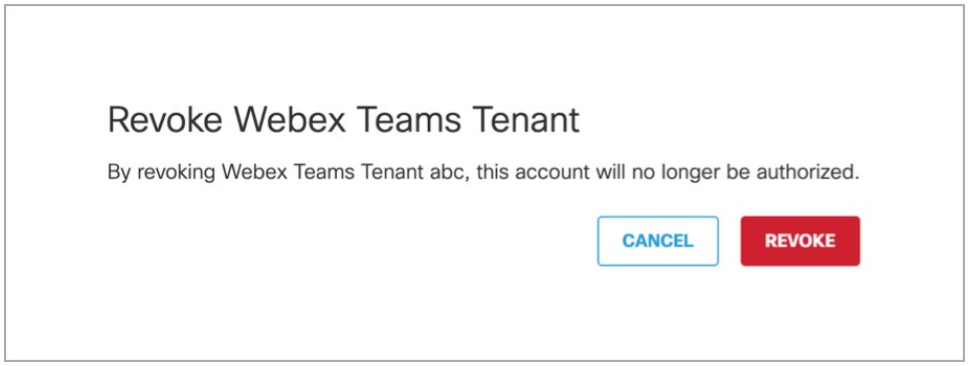
Provides instructions for revoking authorization for a Webex Teams tenant.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is not authorized.


Revoke Webex Teams Tenant
By revoking Webex Teams Tenant abc, this account will no longer be authorized.
CANCEL
REVOKE

46 Manage Cloud Malware Protection

Topics:

- Enable Cloud Malware Protection
- Revoke Authorization for a Platform
- Enable Cloud Malware Protection for Box Tenants
- Enable Cloud Malware Protection for Dropbox Tenants
- Enable Cloud Malware Protection for Google Drive
- Enable Cloud Malware Protection for Microsoft 365 Tenants
- Enable Cloud Malware Protection for Webex Teams

Introduces managing cloud malware protection. Cloud Malware Protection scans your environment's cloud platforms for malicious files and any other risks. You can enable more than one instance of a platform.

Cloud Malware Protection scans your environment's cloud platforms for malicious files and any other risks. You can enable more than one instance of a platform. For example, a school administration with an instance of Box for teachers and faculty and another for students can enable both instances, the result being complete malware protection for Box.

When you authenticate a tenant for Cloud Malware protection, the scan begins immediately and inspects new and updated files as changes occur. Additionally, one week after the tenant is authenticated Cloud Malware also initiates a retroactive scan of all existing files for the tenant going back in time as far as recorded. The time it takes to complete the retroactive scan depends on the number of files in the tenants and their size and on the API rate limit of the platform vendor.

When Cloud Malware Protection finds malicious files, the information is presented in the Cloud Malware Report. You can remediate potential risk by configuring a response action that Umbrella will automatically apply for malicious files detected within the tenant:

- For Webex Teams you can delete the file.
- For Dropbox, Box, Microsoft 365, and Google you can quarantine the file.
  - The quarantined file is moved into a folder named `Cisco_Quarantine_Malware` in the root path of the admin who authorized the tenant, removes all collaborators, and changes the file owner to the platform admin.
  - A text file is left in the original location of the quarantined file with the name `<filename>.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware or exposing sensitive data, and for more information to contact their organization administrator.

Enable Cloud Malware Protection

Provides instructions for enabling cloud malware protection. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

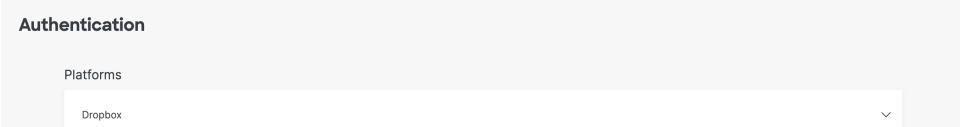
Enable Cloud Malware Protection so that Secure Access scans your environment's cloud platforms for malicious files and any other risks. When Cloud Malware Protection finds malicious files, the information is presented in the Cloud Malware Report. You can configure your Cloud Malware tenant to automatically apply a response action to malicious files when they are detected, or you can manually trigger a response action from the Cloud Malware report.

Before you begin

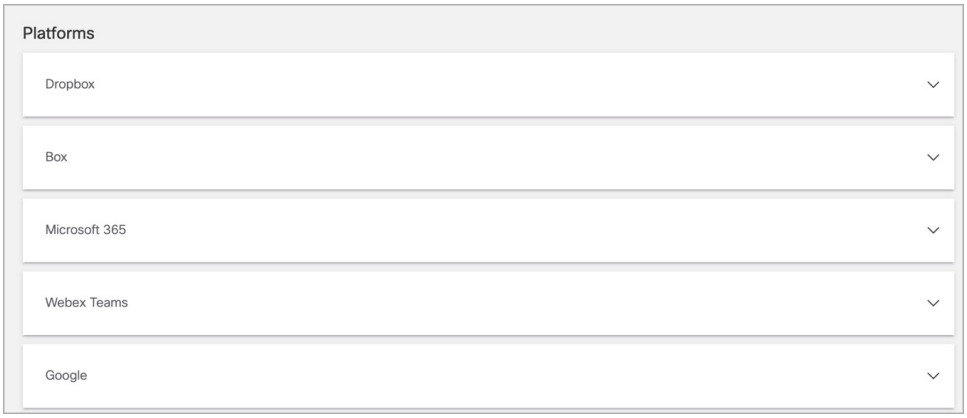
- Full Admin user role. For more information, see Manage Accounts.

Procedure

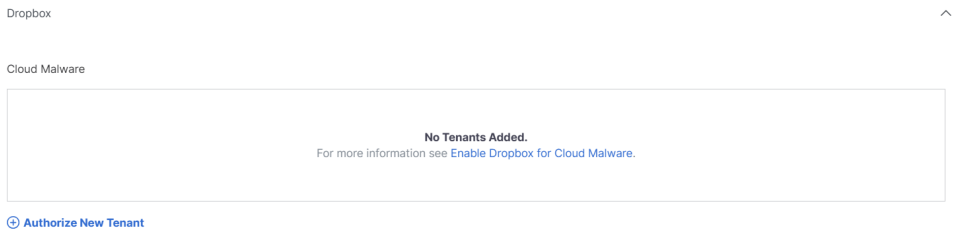
1. Navigate to **Admin** > **Authentication**.



2. In the **Platforms** section, expand a platform.



3. Click **Authorize New Tenant** to add an tenant of this platform to your Secure Access environment. You can authorize more than one tenant of the same platform.



Revoke Authorization for a Platform

Provides instructions for revoke authorization for a platform. It also identifies related requirements, procedures, and operational considerations.

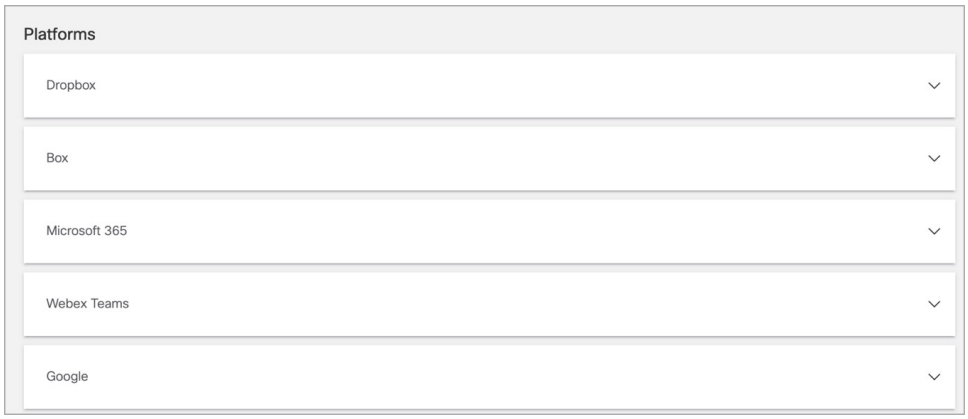
After authorizing a platform in your Secure Access environment, you can revoke authorization at any time.

Before you begin

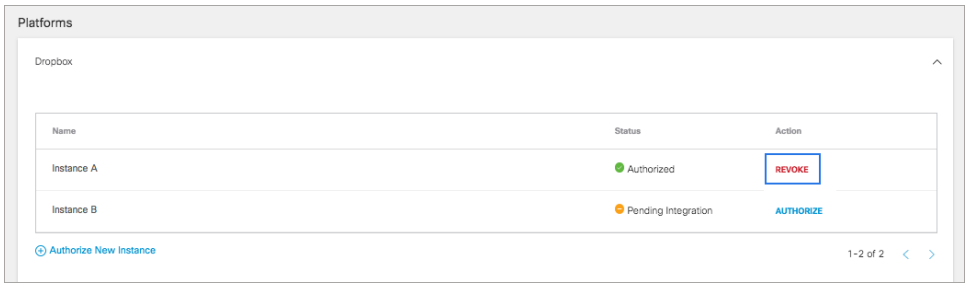
- Full Admin user role. For more information, see Manage Accounts.

Procedure

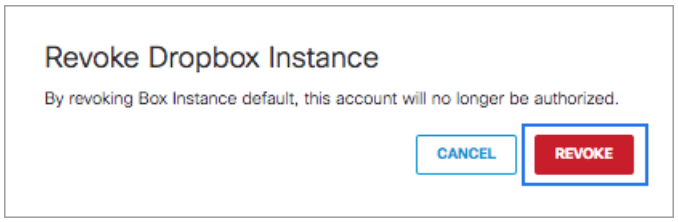
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click the platform that you wish to revoke.



3. Choose the instance to revoke and click **Revoke**.



4. Click **Revoke** again to complete the process.



Enable Cloud Malware Protection for Box Tenants

Describes enabling cloud malware protection for box tenants. Secure Access supports Cloud Malware protection for all files within your Box deployment.

Secure Access supports Cloud Malware protection for all files within your Box deployment.

Prerequisites

- The person performing the installation must be a Box Admin (not Co-Admin)
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Published and unpublished applications must be enabled in the Box Admin Console (see Verify Box Application Settings.

Limitation

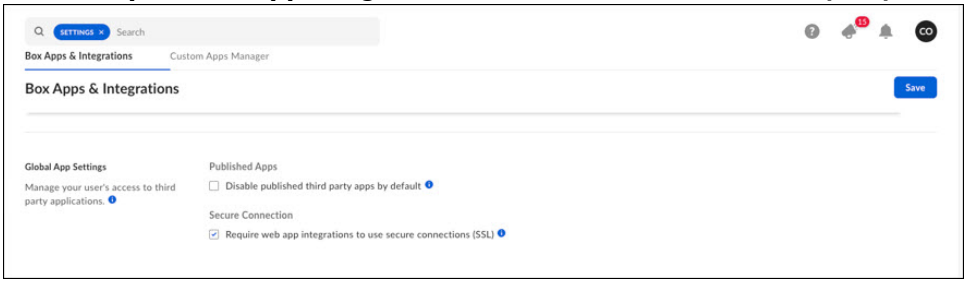
- A tenant that fails to authenticate cannot be deleted.

Verify Box Application Settings

Provides instructions for verifying box application settings. Log into the Box Admin Console. Navigate to Settings (the Gear icon) Enterprise Settings Apps .

Procedure

1. Log into the Box Admin Console.
2. Navigate to **Settings (the Gear icon)** > **Enterprise Settings** > **Apps**.
3. In the **Global App Settings** section:
   - Do *not* check: **Disable published third party apps by default**.
   - Check: **Require web app integrations to use secure connections (SSL)**.



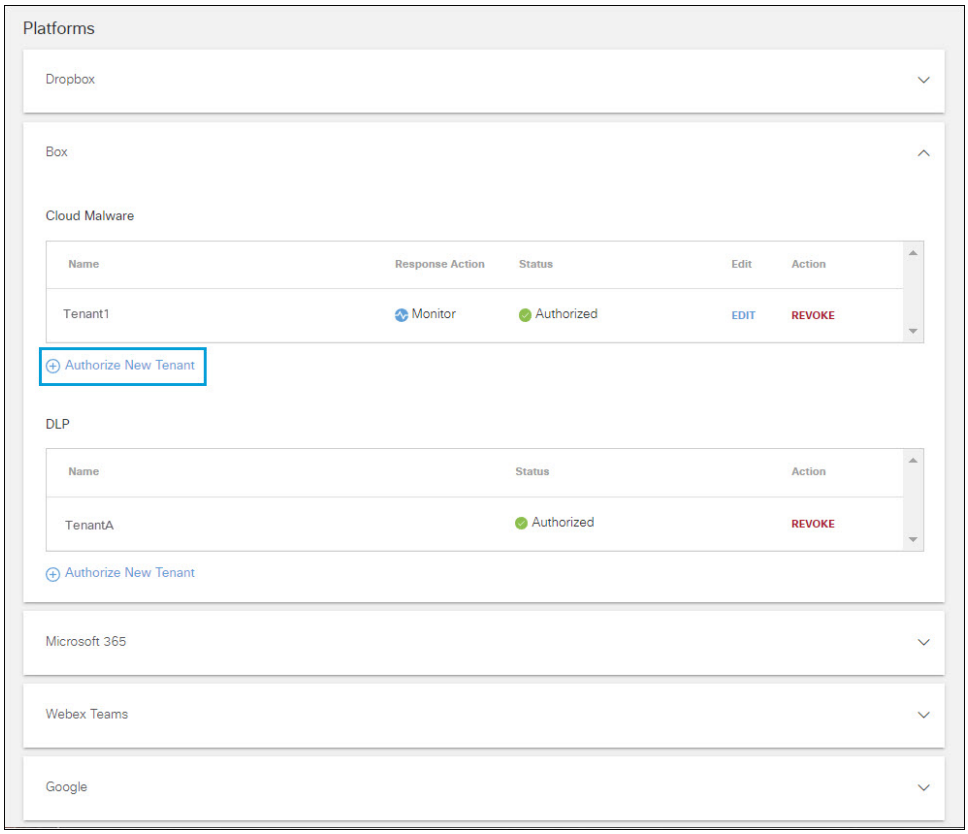
   - Click **Save**.

Authorize a Tenant

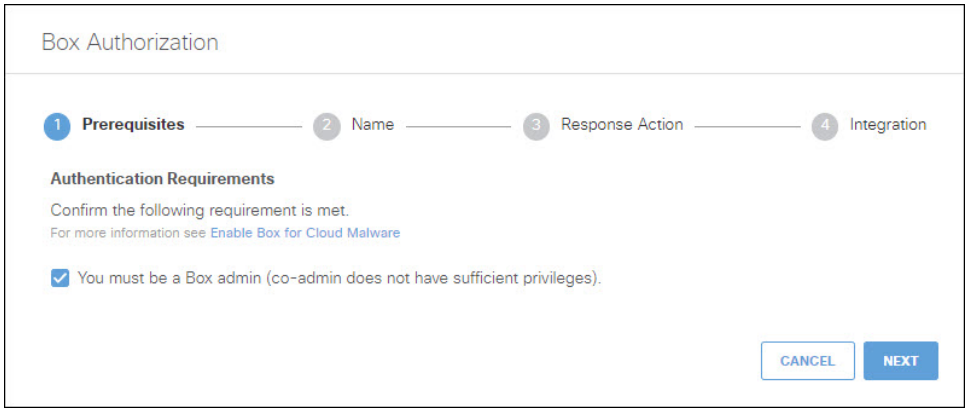
Provides instructions for authorize a tenant. Navigate to Admin Authentication . Under Platforms, click to expand Box. Under Cloud Malware, click Authorize New Tenant to add a Box tenant to your Secure Access environment.

Procedure

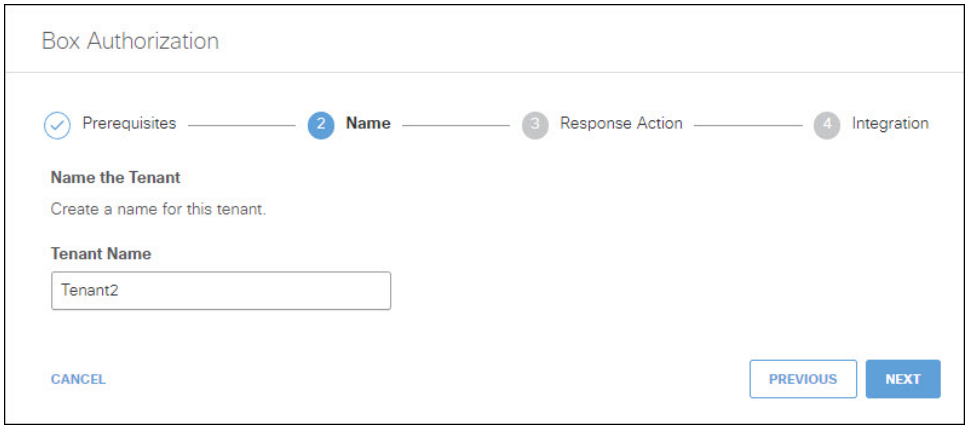
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click to expand **Box**.



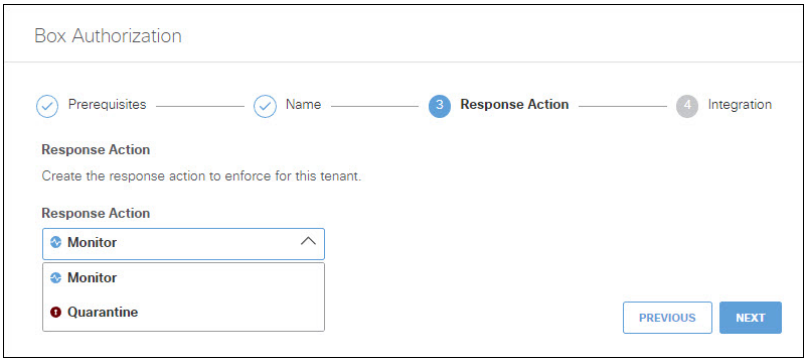
3. Under **Cloud Malware**, click **Authorize New Tenant** to add a Box tenant to your Secure Access environment.
4. In the **Box Authorization** dialog box, check the checkbox to verify you meet the prerequisites, then click **Next**.



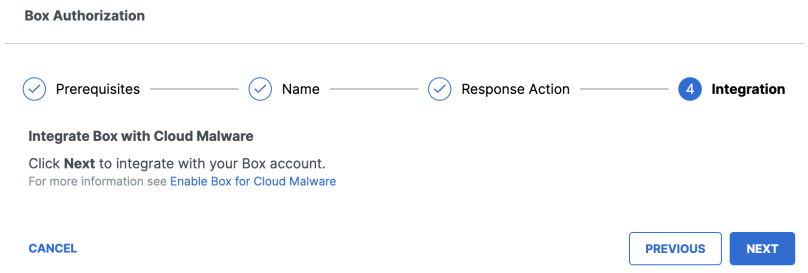
5. Enter the tenant name, then click **Next**.



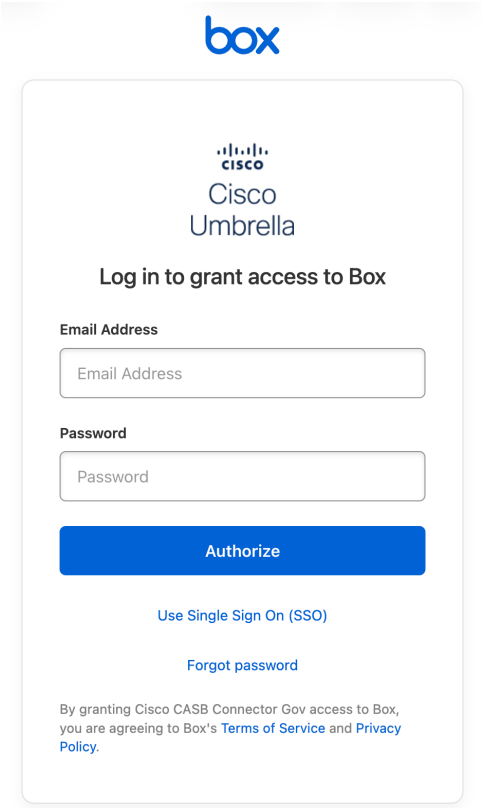
6. Select a **Response Action** for Secure Access to apply to Box files found with malware, then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine** > **Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Box admin.
     - Replace the file in its original location with a text file named `<filename>.ppt_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



7. Click **Next** to be redirected to the Box login page.

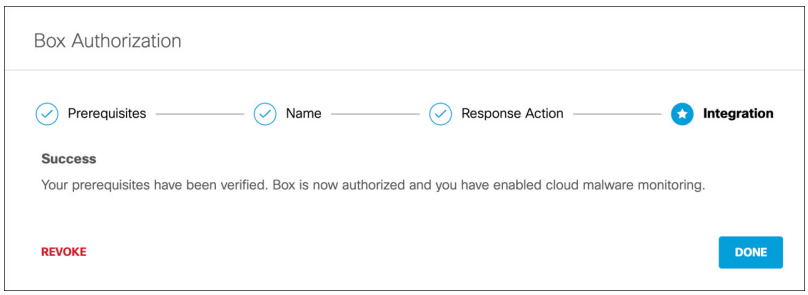


8. Log in to Box with admin credentials to grant access.



You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized.

9. Click **Done** to complete.



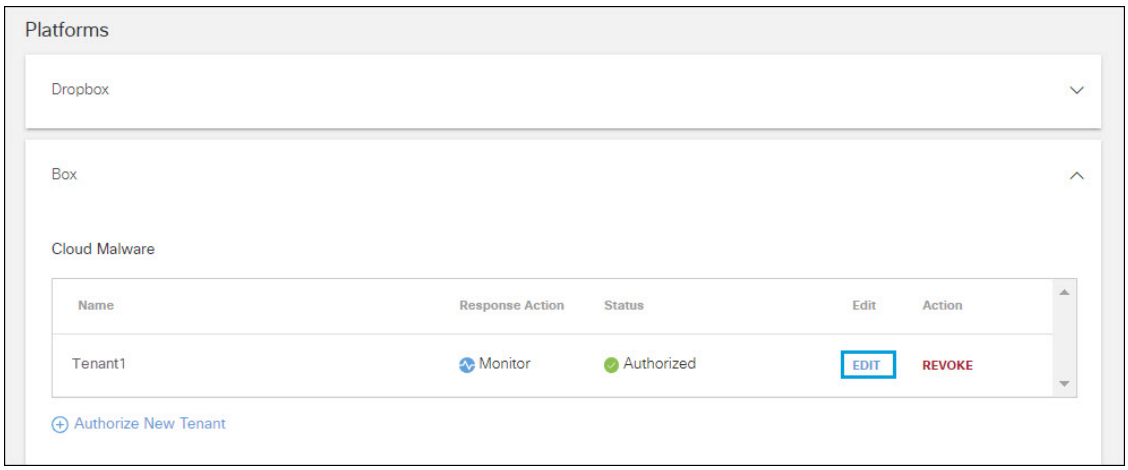
Edit a Tenant

Provides instructions for editing a tenant. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

You can change the Response Action you have selected for a tenant.

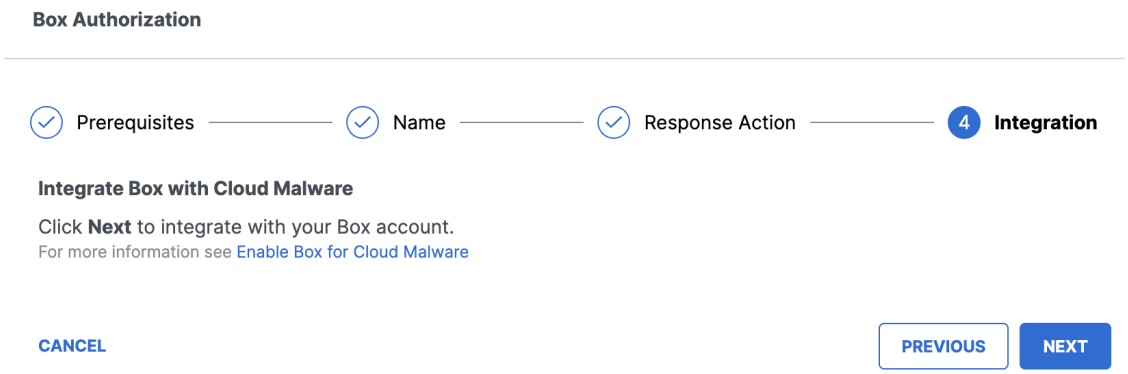
Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Box**.
3. In the **Cloud Malware** section , under **Action**, click **Edit**. You can edit any tenant.

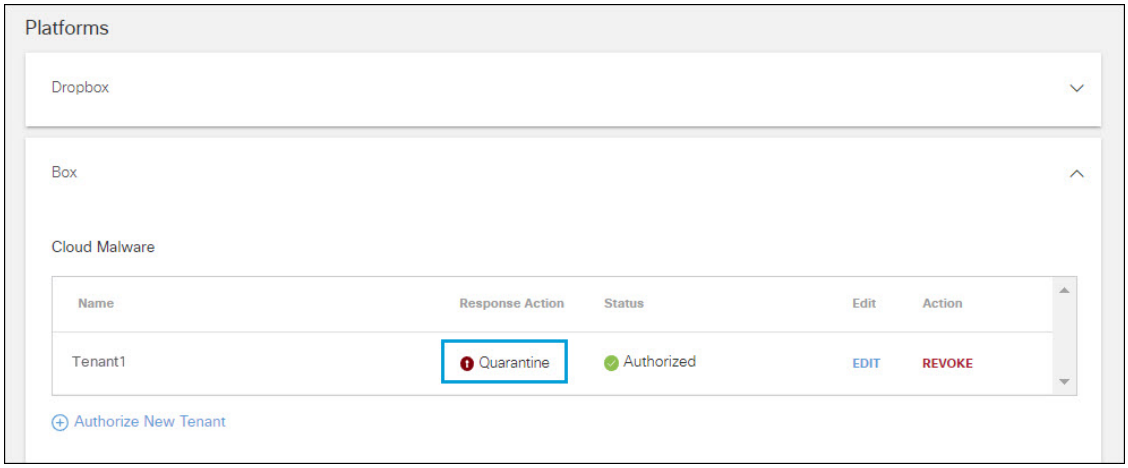


4. Select a **Response Action** for Secure Access to apply to Box files found with malware, then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Authentication** > **Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Box admin.
     - Replace the file in its original location with a text file named `<filename>.ppt_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

5. Click **Next** to complete.



The new **Response Action** is displayed.

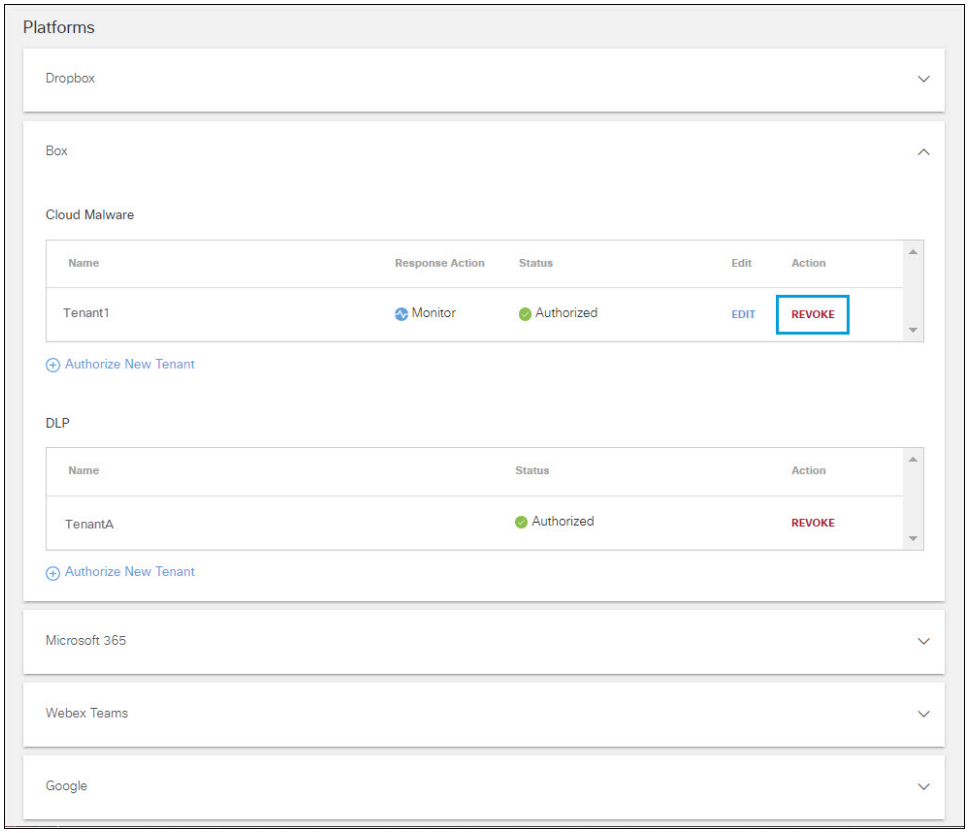


Revoke Authorization

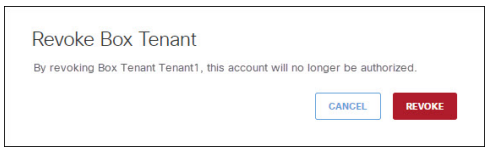
Provides instructions for revoking authorization for Box tenants.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



Enable Cloud Malware Protection for Dropbox Tenants

Describes enabling cloud malware protection for dropbox tenants. Secure Access supports Cloud Malware protection for all files within your Dropbox deployment, including those in Dropbox teams folders.

Secure Access supports Cloud Malware protection for all files within your Dropbox deployment, including those in Dropbox teams folders.

Prerequisites

- You must have an active Dropbox tenant and the person doing the installation must be a Dropbox Team Admin
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)

Limitation

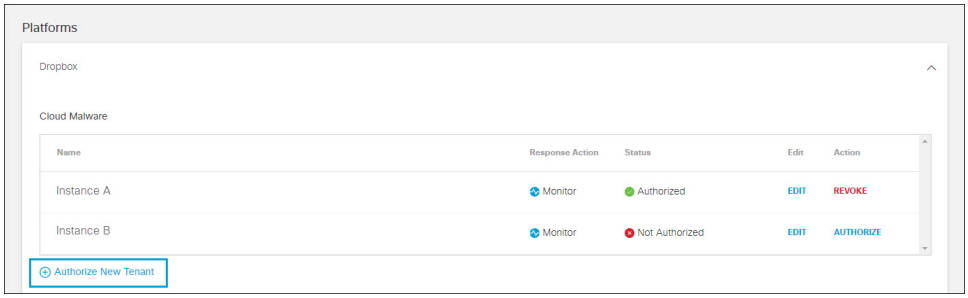
- A tenant that fails to authenticate cannot be deleted.

Authorize a Tenant

Provides instructions for authorize a tenant. Navigate to Admin Authentication . Click Authorize New Tenant to add a Dropbox tenant to your Secure Access environment.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Dropbox**.
3. Click **Authorize New Tenant** to add a Dropbox tenant to your Secure Access environment.

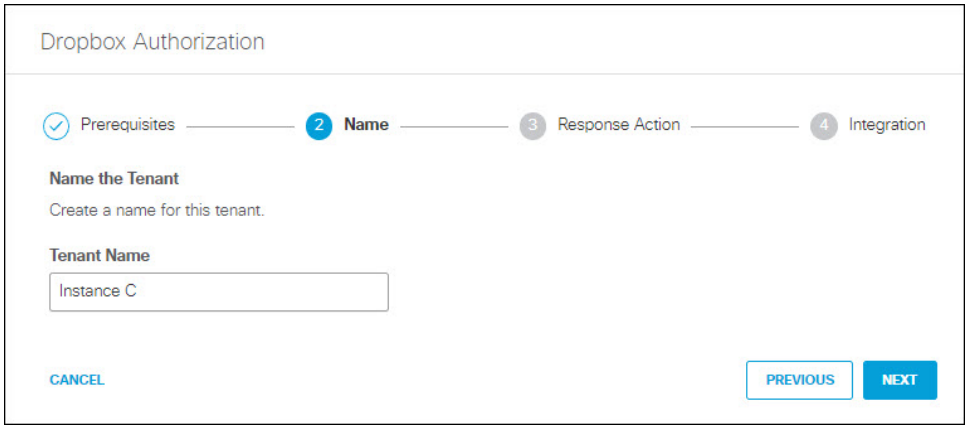


4. In the **Dropbox Authorization** dialog box, check the checkbox to verify you meet the prerequisite, then click **Next**.

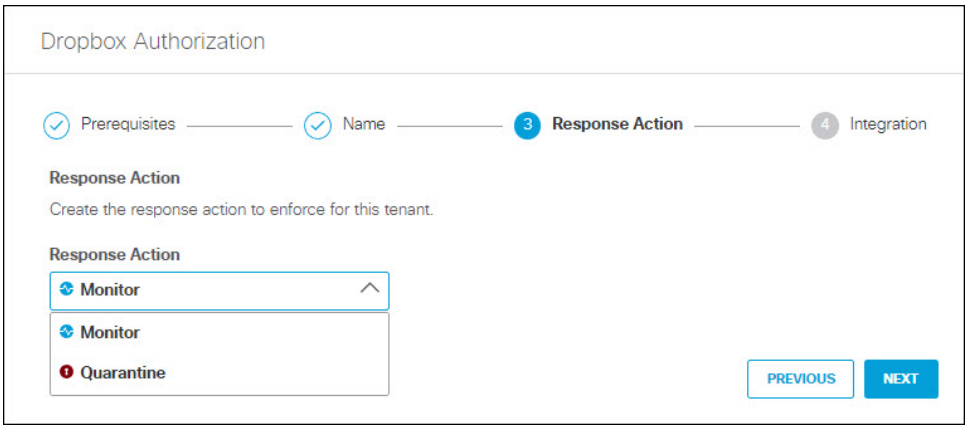
In the **Dropbox Authorization** dialog box, check the checkbox to verify you meet the prerequisite, then click **Next**.



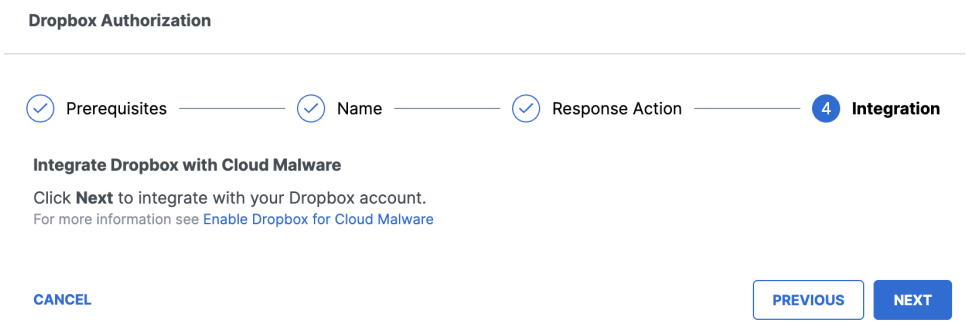
5. Enter the tenant name, then click **Next**.



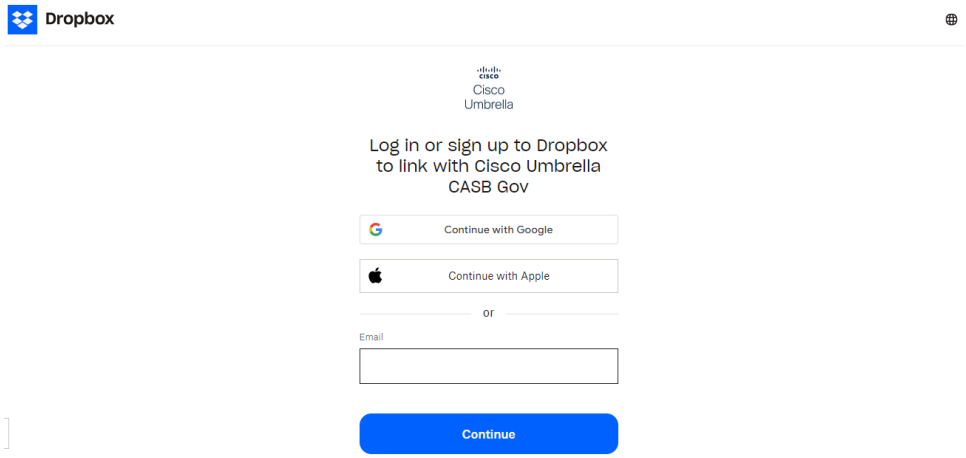
6. Select a **Response Action** for Secure Access to automatically apply to Dropbox files found with malware, then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine** > **Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Dropbox admin.
     - Replace the file in its original location with a text file named *filename*`.ppt_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



7. Click **Next** to be redirected to the Dropbox's login page.



8. Log in to Dropbox with admin credentials to grant access.



You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as **Authorized**.

9. Click **Done** to complete.

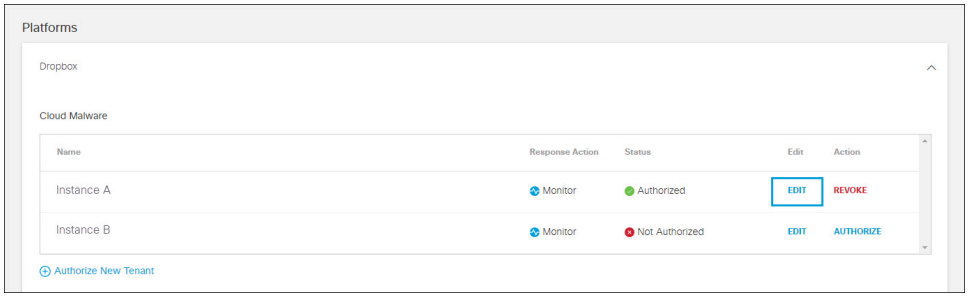
Edit a Tenant

Provides instructions for editing a tenant. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

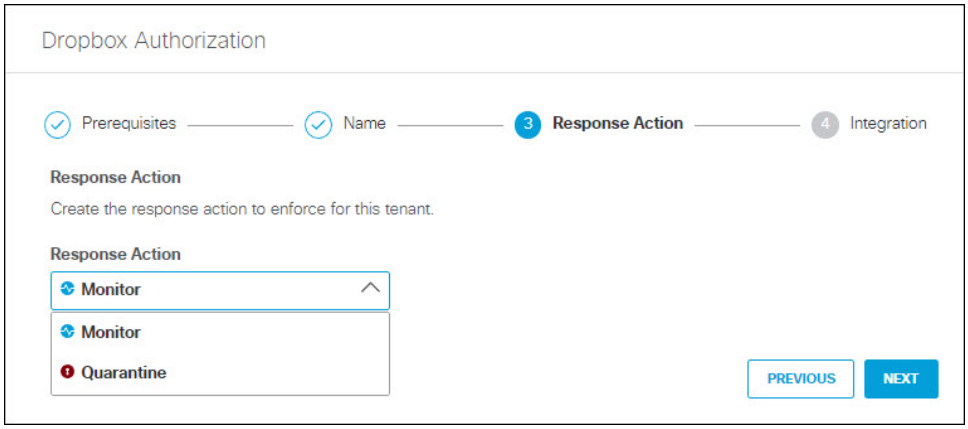
You can change the Response Action you have selected for a tenant.

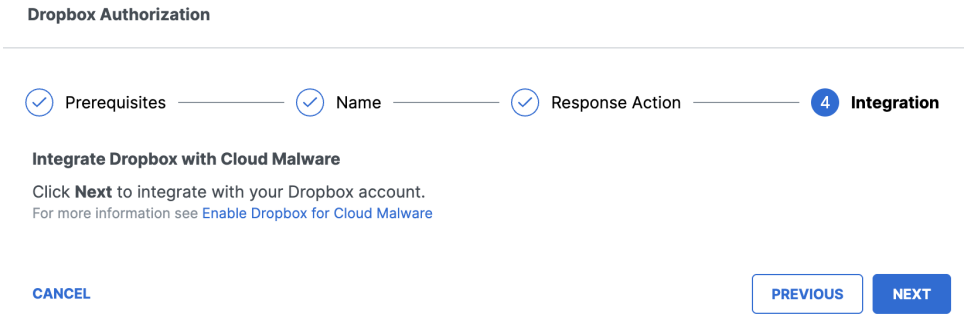
Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **Dropbox**.
3. In the **Cloud Malware** section , from the **Edit** column, click **Edit**. You can edit any tenant.



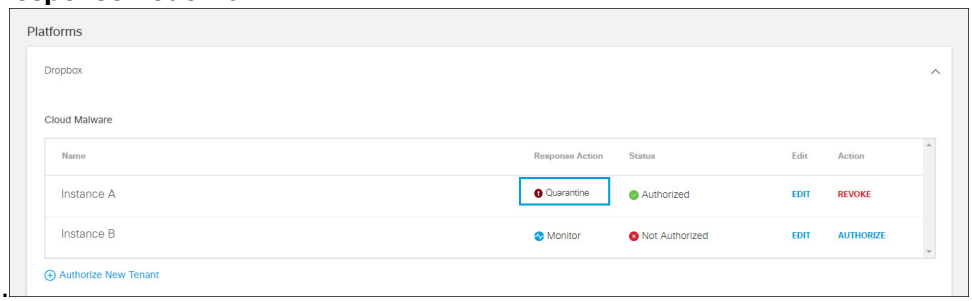
4. Select a **Response Action** for Secure Access to automatically apply to Dropbox files found with malware, then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine**> **Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Dropbox admin.
     - Replace the file in its original location with a text file named ***filename*.ppt_Quarantined.txt** explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.





5. Click **Next** to complete.

6. The new **Response Action** is displayed.

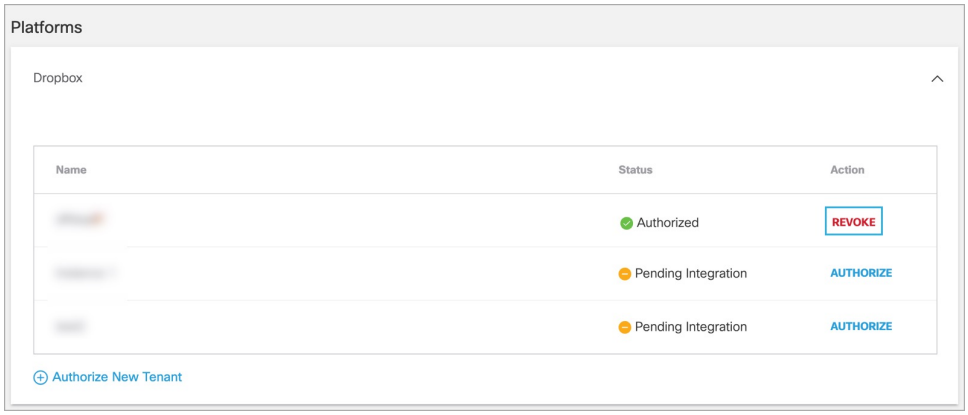


Revoke Authorization

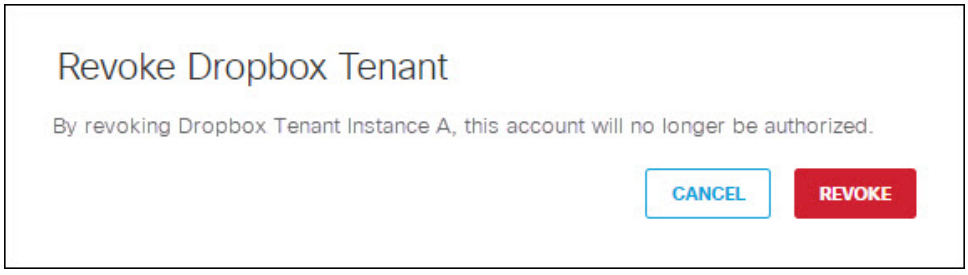
Provides instructions for revoke authorization. Navigate to Admin Authentication . Under Platforms, click Dropbox. Under Action, click Revoke. You can revoke any authorized tenant.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Dropbox**.
3. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



4. Click **Revoke**. The selected account is no longer authorized.



Enable Cloud Malware Protection for Google Drive

Describes enabling cloud malware protection for google drive. The person performing the authentication must be a Google Super Admin and have an active Google user license.

Prerequisites

- The person performing the authentication *must* be a Google Super Admin and have an active Google user license.
- Chrome or Firefox is recommended with pop-up blockers/ad blockers disabled (only for the duration of authorization).
- Cisco Cloud Access Security Broker (CASB) Gov (also known as the SaaS API Connector) must be installed in the tenant by a Google Admin User. We recommend using a service account for the installation.

Limitation

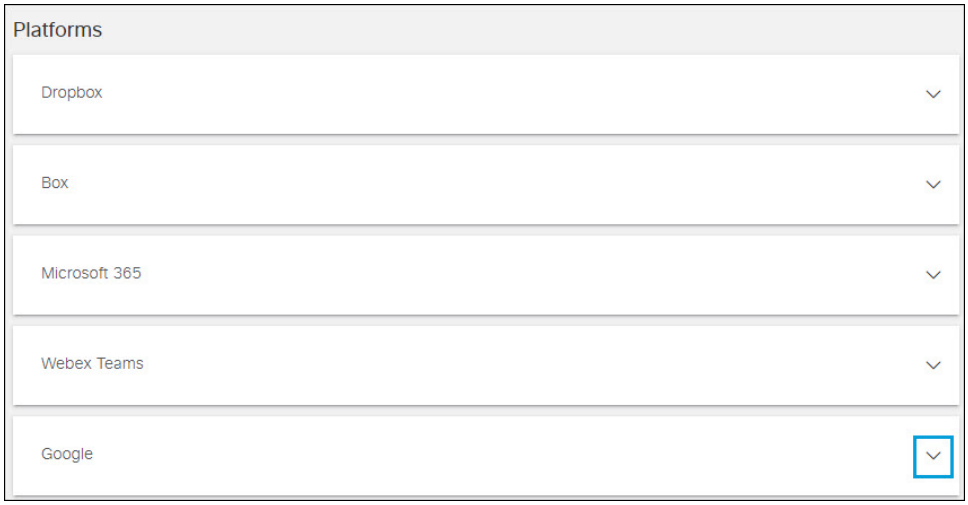
- A tenant that fails to authenticate cannot be deleted.

Authorize a Tenant

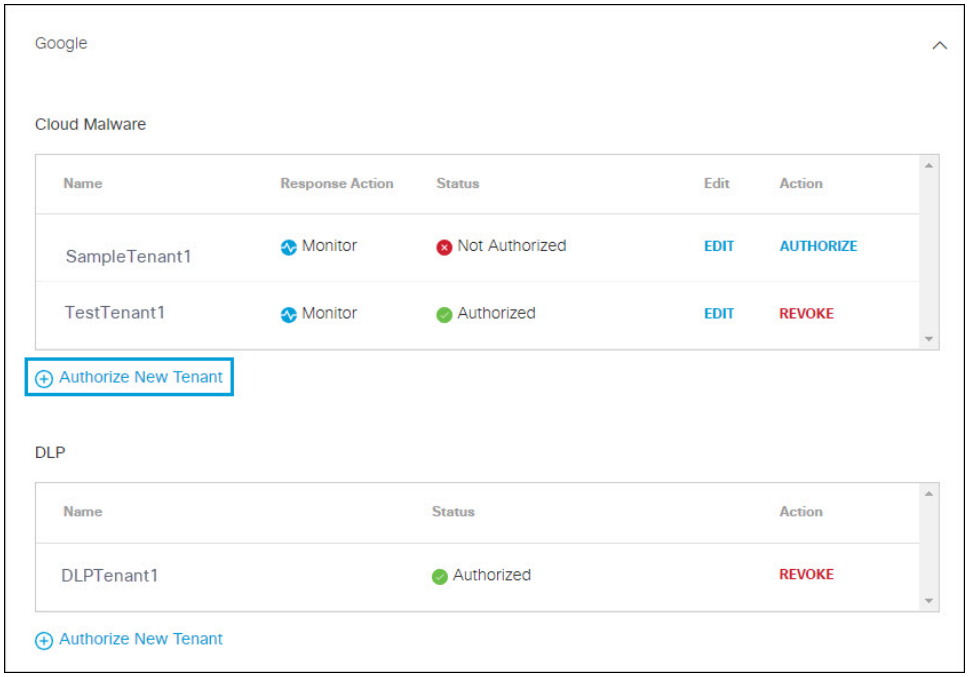
Provides instructions for authorize a tenant. In the Secure Access dashboard, navigate to Admin Authentication . In the Platforms section, click to expand Google.

Procedure

1. In the Secure Access dashboard, navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click to expand **Google**.

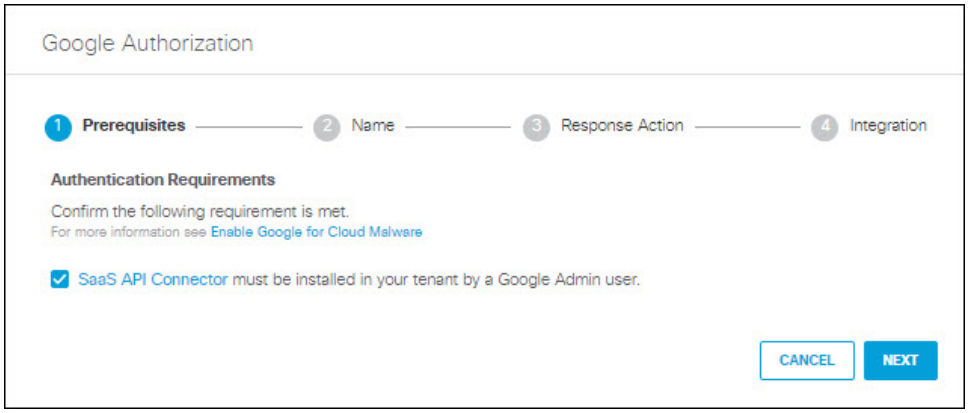


3. In the **Cloud Malware** section, click **Authorize New Tenant** to add a Google tenant to your Secure Access environment.

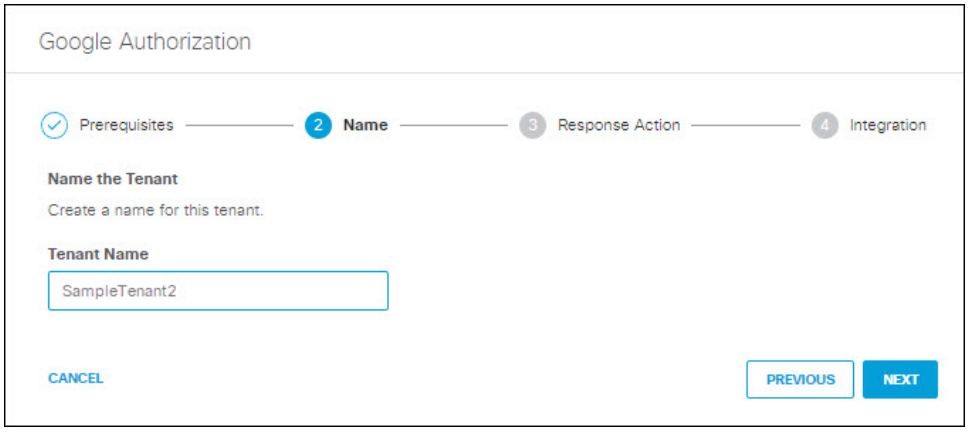


4. In the **Google Authorization** dialog box, check the checkbox to verify you meet the prerequisite, then click **Next**.

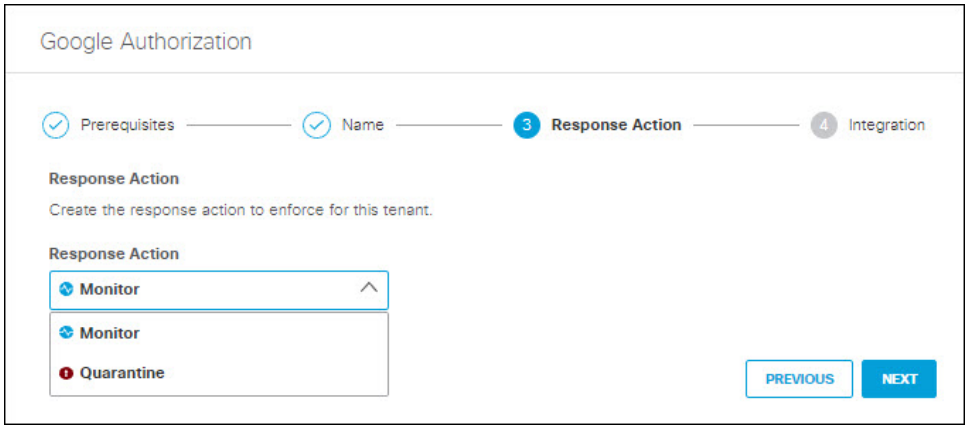
> **Note**
>
> The link to the SaaS API Connector brings you to the Secure Access DLP Connector site in the Google Workspace Marketplace. This is correct, despite the nomenclature difference.



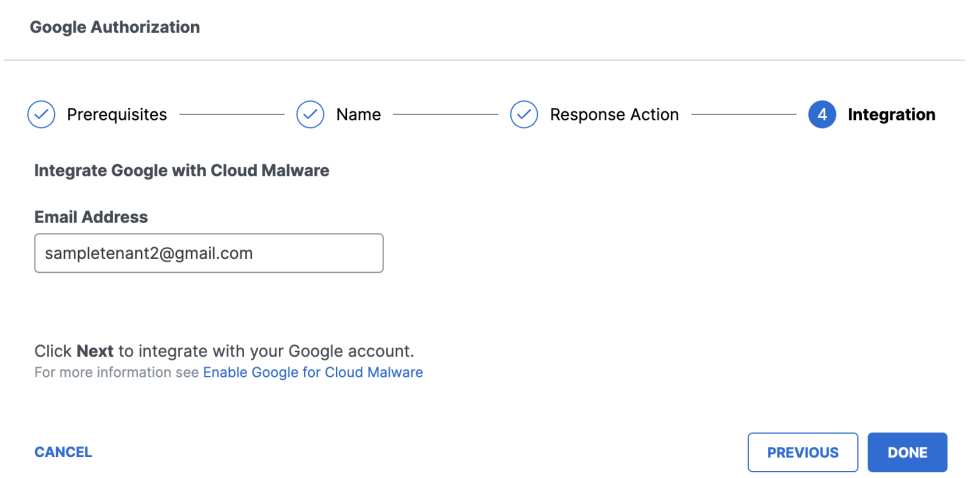
5. Add a **Tenant Name** and then click **Next**.



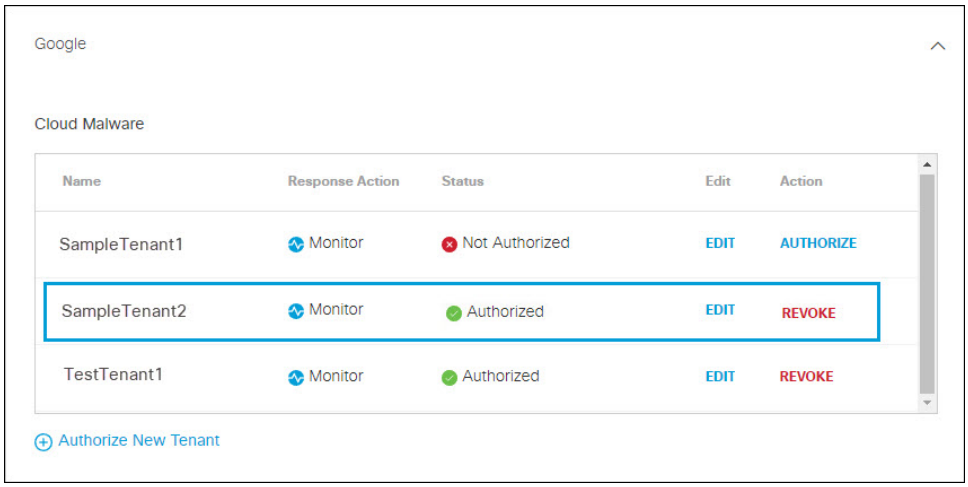
6. Select a **Response Action** for Secure Access to apply to Google files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Google admin.
     - Replace the file in its original location with a text file named ***filename*.ppt_Cisco_Quarantined.txt** explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



7. Add a gmail **Email Address** and then click **Done**.



The new tenant appears in the **Cloud Malware** section.



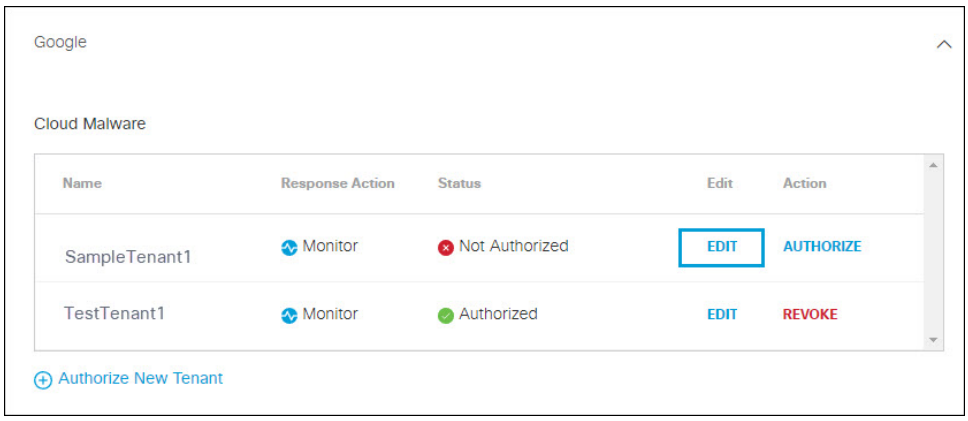
Edit a Tenant

Provides instructions for editing a tenant. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

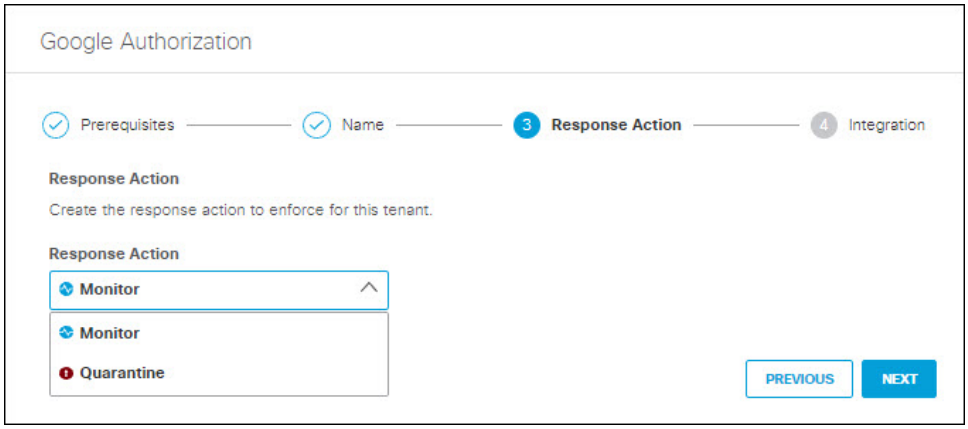
You can change the Response Action you have selected for a tenant.

Procedure

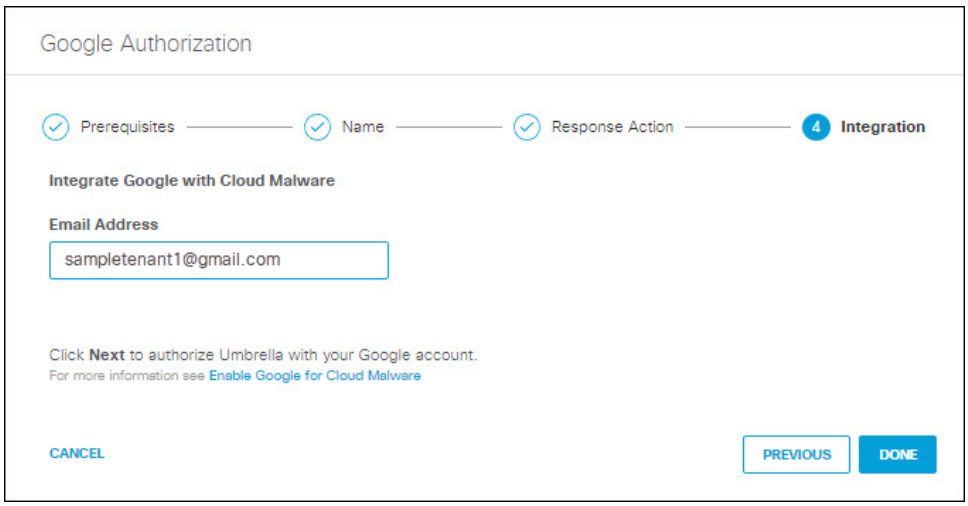
1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **Google**.
3. In the **Cloud Malware** section, from the **Edit** column click **Edit**



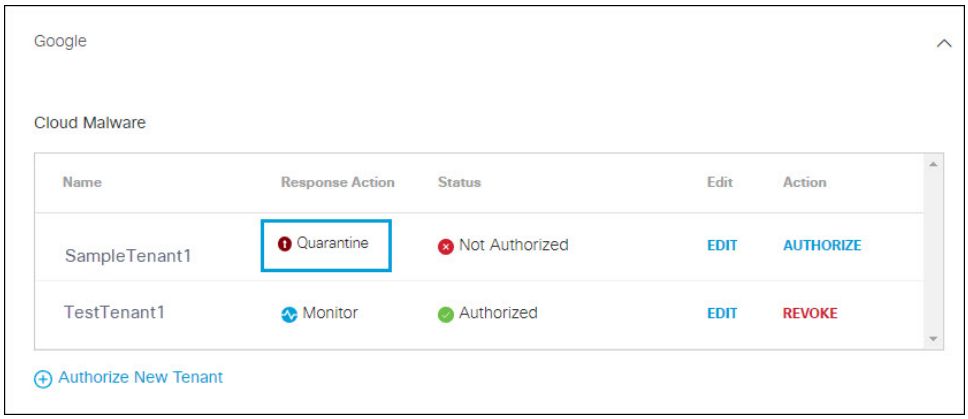
4. Select a **Response Action** for Secure Access to apply to Google files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Google admin.
     - Replace the file in its original location with a text file named ***filename*.ppt_Cisco_Quarantined.txt** explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



5. Click **Done**.



The new **Response Action** is displayed.



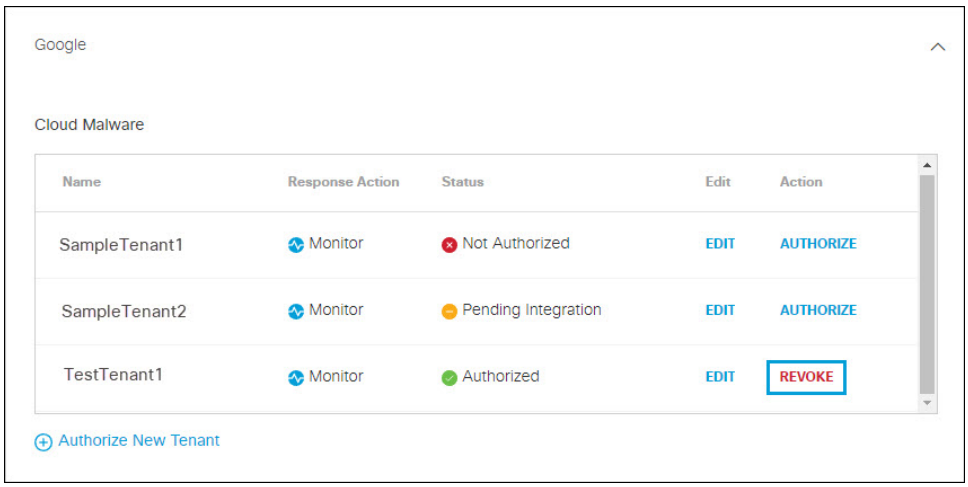
Revoke Authorization

Provides instructions for revoke authorization. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

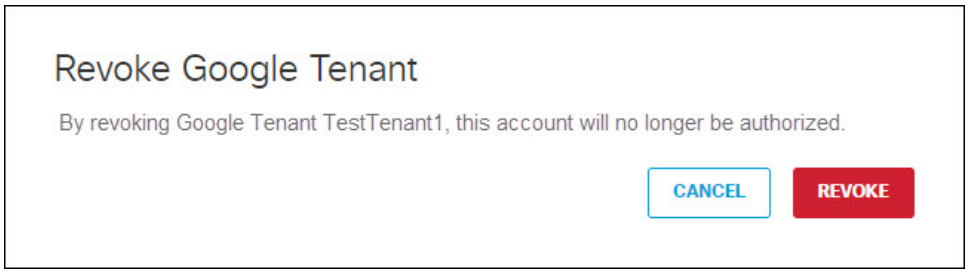
You can revoke any authorized tenant.

Procedure

1. From the **Action** column, click **Revoke**.



2. Click **Revoke**. The selected tenant is no longer authorized.



Enable Cloud Malware Protection for Microsoft 365 Tenants

Describes enabling cloud malware protection for microsoft 365 tenants. Secure Access supports Cloud Malware protection for both OneDrive and SharePoint sites within your Microsoft 365 deployment.

Secure Access supports Cloud Malware protection for both OneDrive and SharePoint sites within your Microsoft 365 deployment.

Note

Running both MS365 and Cloud Malware:

MS365 and Cloud Malware both protect users against malware. However, their functionalities are not redundant. MS365 might discover malware that Cloud Malware does not find. Cloud Malware also finds malware that MS365 overlooks. There is value to running MS365 and Cloud Malware simultaneously.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- The user performing the installation *must* use a service account with a Microsoft 365 Global Admin and active license
- Audit log must be enabled for Microsoft 365. For more information, refer to Microsoft Technical documentation and search for **Turn auditing on or off.**
- SharePoint Online and OneDrive must be enabled

- The following IP address must be allowed if there are Firewall rules that prevent third-party applications:

  18.253.223.180

- If you use Conditional Access Policy (CAP) to restrict access to your Microsoft 365 tenant, you must grant the above Secure Access IP address access in the CAP. You must also grant your current egress IP access in the CAP. These IP addresses are cached by Microsoft and used as part of the conditional access checks.
- Users must have the following API permissions for Microsoft:

API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
Directory.Read.All	Application	Read directory data	Yes
Files.Read.All	Delegated	Read all files that user can access	No
Files.Read.All	Application	Read files in all site collections	Yes
Sites.Read.All	Delegated	Read items in all site collections	No
User.Read	Delegated	Sign in and read user profile	No
User.Read.All	Application	Read all users' full profiles	Yes
Microsoft 365 Management APIs			
AcitivityFeed.Read	Application	Read activity data for the Organization	Yes
SharePoint			
Site.FullControl.All	Application	Full control of all site collections	Yes
User.Read.All	Application	Read user profiles	Yes

Limitation

- A tenant that fails to authenticate cannot be deleted.

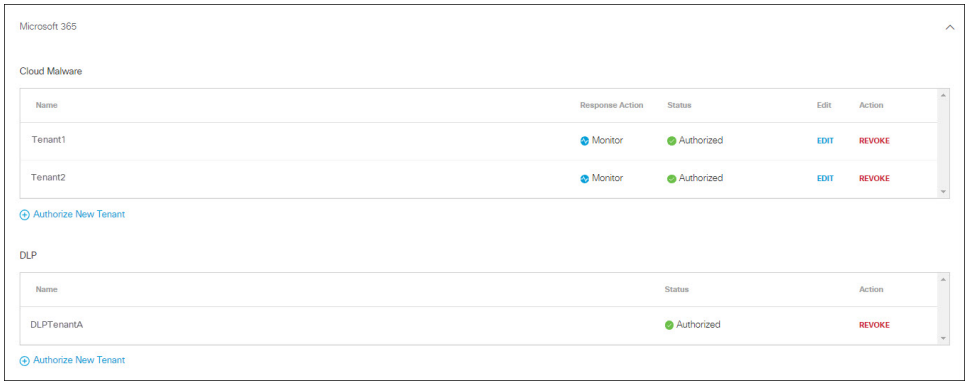
Authorize a Tenant

Provides instructions for authorize a tenant. Navigate to Admin Authentication . Under Platforms, click Microsoft 365. Click Authorize New Tenant in the Cloud Malware subsection to add a Microsoft 365 tenant to your Secure Access environment.

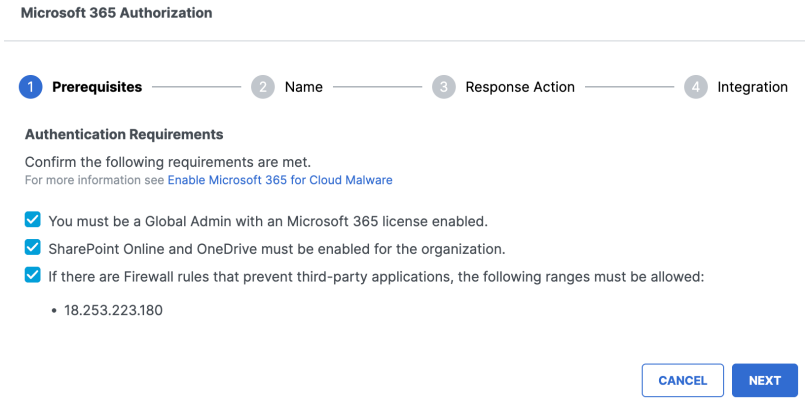
Procedure

1. Navigate to **Admin** > **Authentication**.

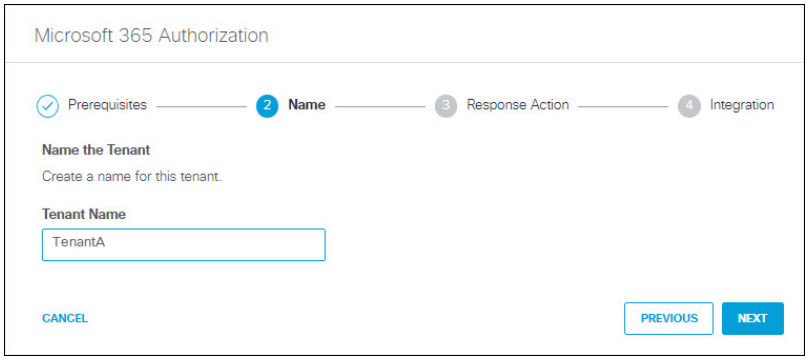
2. Under **Platforms**, click **Microsoft 365**.



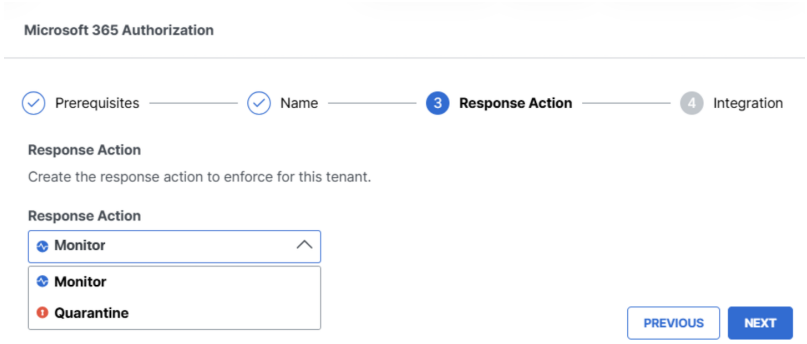
3. Click **Authorize New Tenant** in the **Cloud Malware** subsection to add a Microsoft 365 tenant to your Secure Access environment.
4. In the **Microsoft 365 Authorization** dialog, check the checkboxes to verify you meet the prerequisites, then click **Next**.



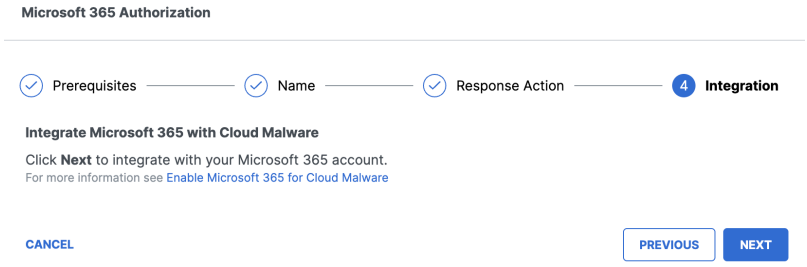
5. Provide a name for your tenant, then click **Next**.



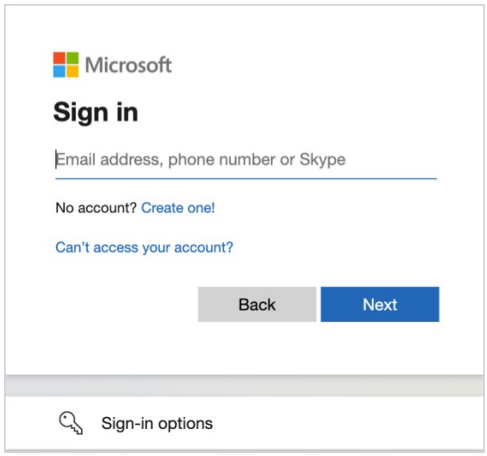
6. Select a **Response Action** for Secure Access to apply to Microsoft 365 files found with malware, then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named `Cisco_Quarantine > Malware` in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Microsoft 365 admin.
     - Replace the file in its original location with a text file named `<filename>.ppt_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



7. Click **Next** to be redirected to the Microsoft 365 login page.

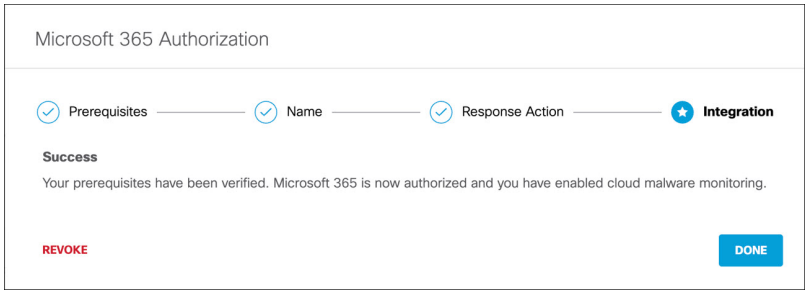


8. Log in to Microsoft 365 with admin credentials to grant access.



You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized.

9. Click **Done** to complete.



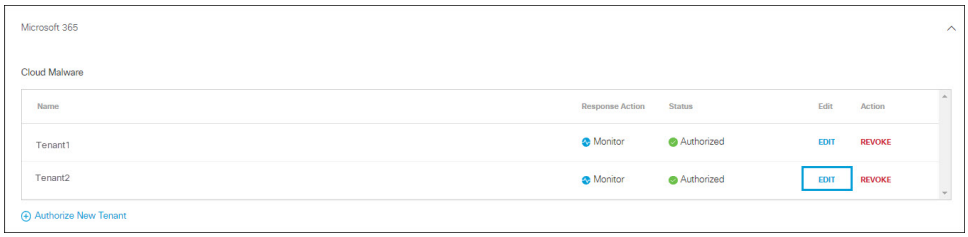
Edit a Tenant

Provides instructions for editing a tenant. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

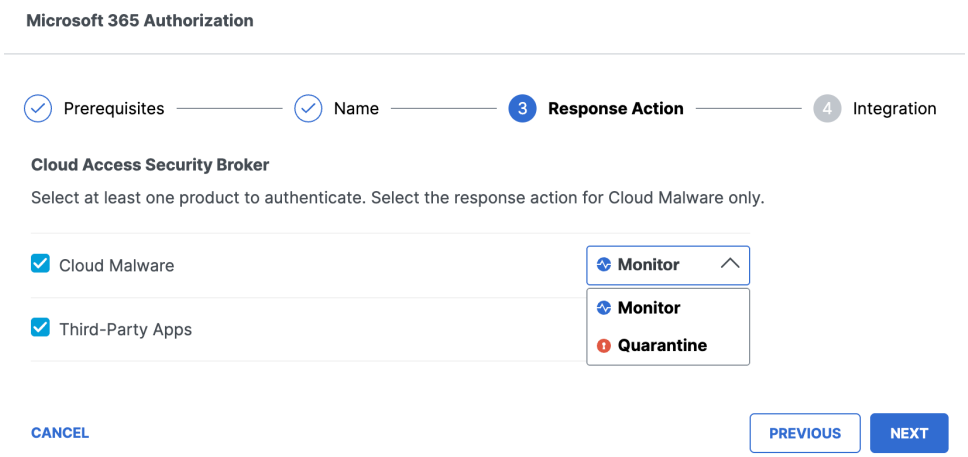
You can change the Response Action you have selected for a tenant.

Procedure

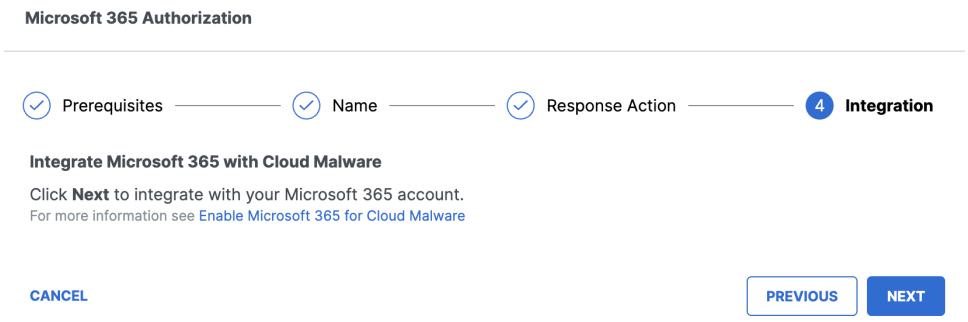
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Microsoft 365**.
3. In the **Cloud Malware** section , under **Action**, click **Edit**. You can edit any tenant.



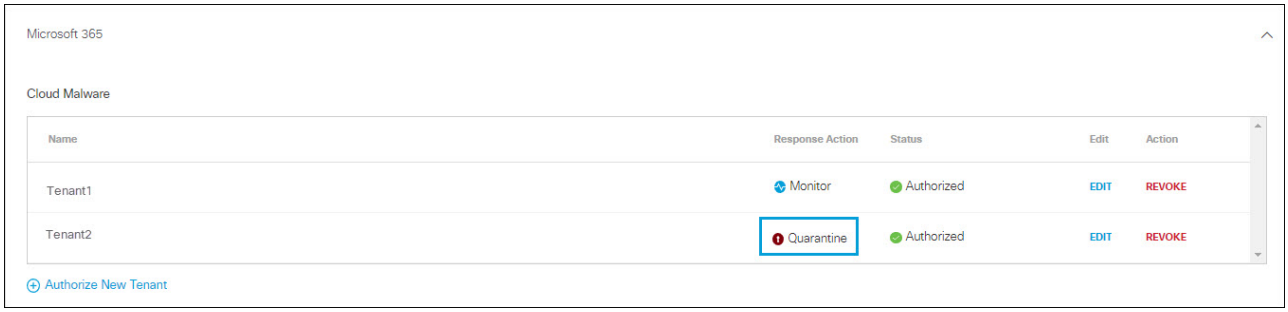
4. Select a **Response Action** for Secure Access to apply to Microsoft 365 files found with malware, then click **Next**.
   - Choose **Cloud Malware**, **Third-Party Apps**, or both for authentication.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine** > **Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Microsoft 365 admin.
     - Replace the file in its original location with a text file named ***filename*.ppt_Quarantined.txt** explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



5. Click **Next** to complete.



6. The new Response Action is displayed.

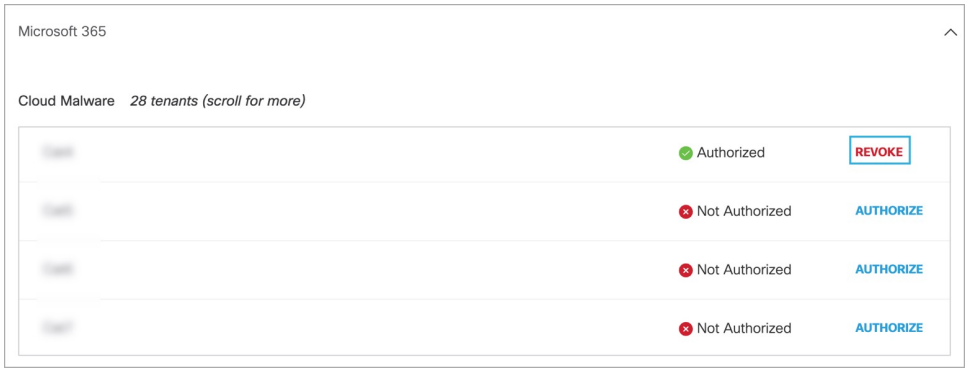


Revoke Authorization

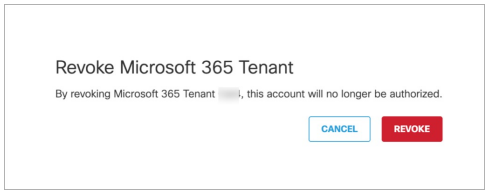
Provides instructions for revoke authorization. Under Action, click Revoke. You can revoke any authorized tenant. Confirm to proceed. The selected account is not authorized.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is not authorized.



Enable Cloud Malware Protection for Webex Teams

Describes enabling cloud malware protection for webex teams. Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Full Administrator Privileges in Webex Teams and the Compliance Officer role
- The `EventsAPI` in your Webex Teams instance must be enabled. Contact your Webex Teams support team to ensure that the `EventsAPI` is turned on.

Limitation

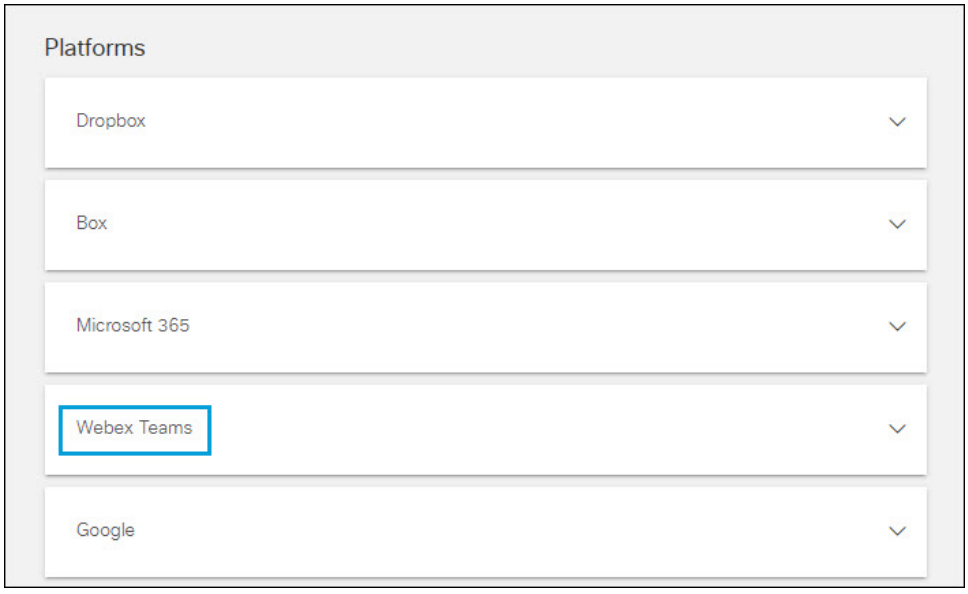
- A tenant that fails to authenticate cannot be deleted.

Authorize a Tenant

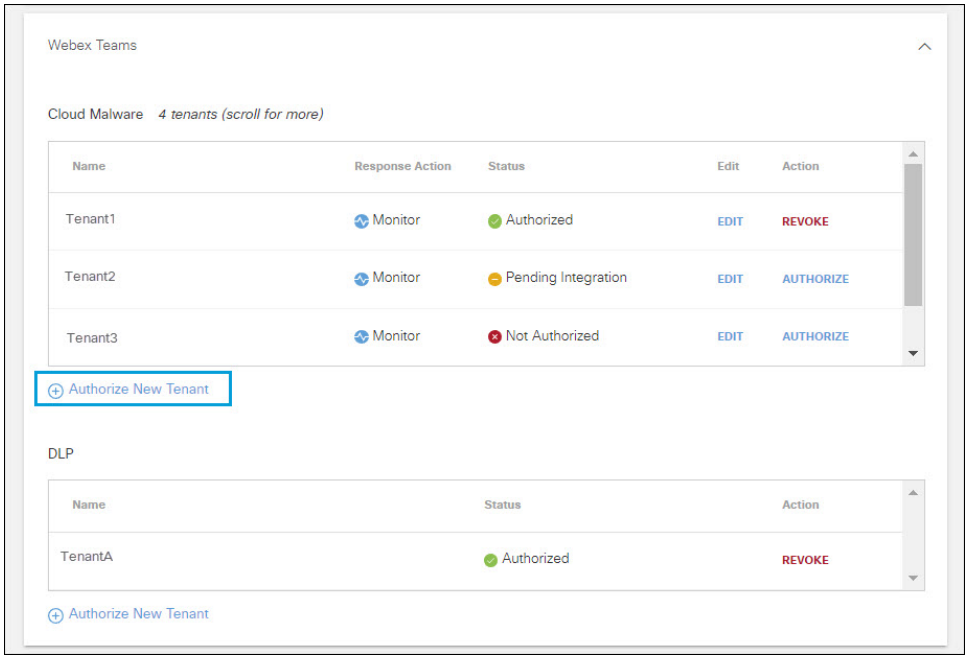
Provides instructions for authorize a tenant. Navigate to Admin Authentication . Under Platforms, click Webex Teams. In the Cloud Malware subsection, click Authorize New Tenant to add a Webex Teams tenant to your Secure Access environment.

Procedure

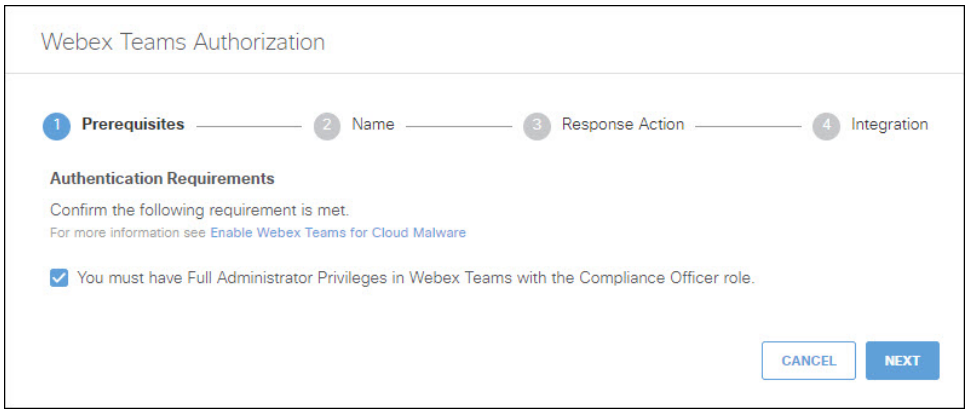
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Webex Teams**.



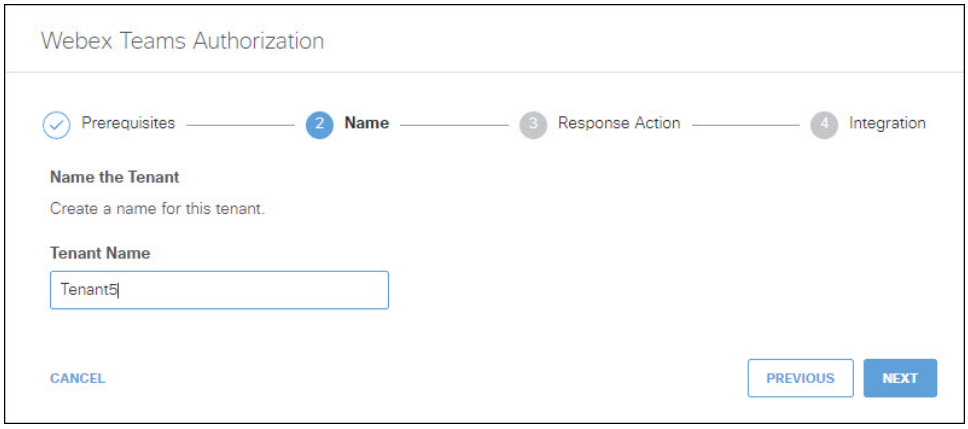
3. In the Cloud Malware subsection, click **Authorize New Tenant** to add a Webex Teams tenant to your Secure Access environment.



4. In the **Webex Teams Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.

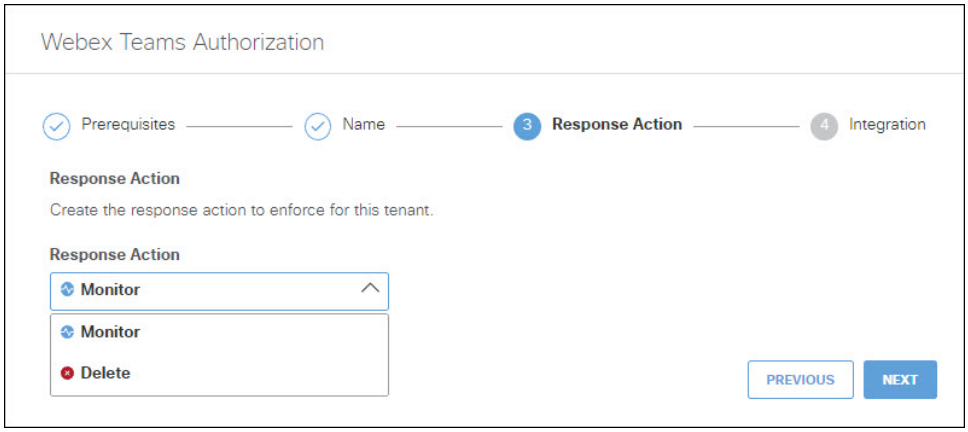


5. Enter the name of your tenant, then click **Next**.

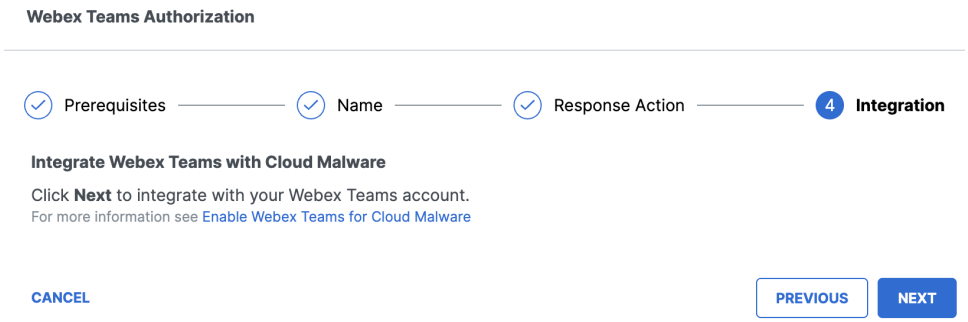


6. Select a **Response Action** for Secure Access to apply to Webex Teams files found with malware, then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually delete these files from the Cloud Malware report.

- Choose **Delete** to delete the file.



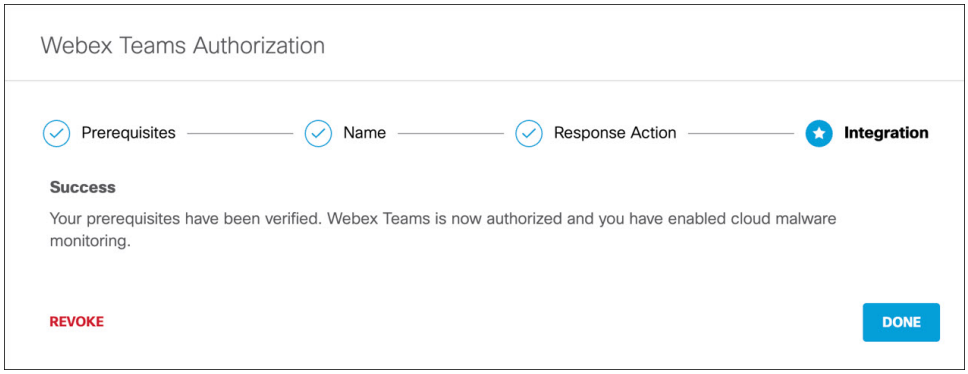
7. Click **Next** to complete the integration.



8. Enter your credentials and click **Sign in**.



9. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done**.



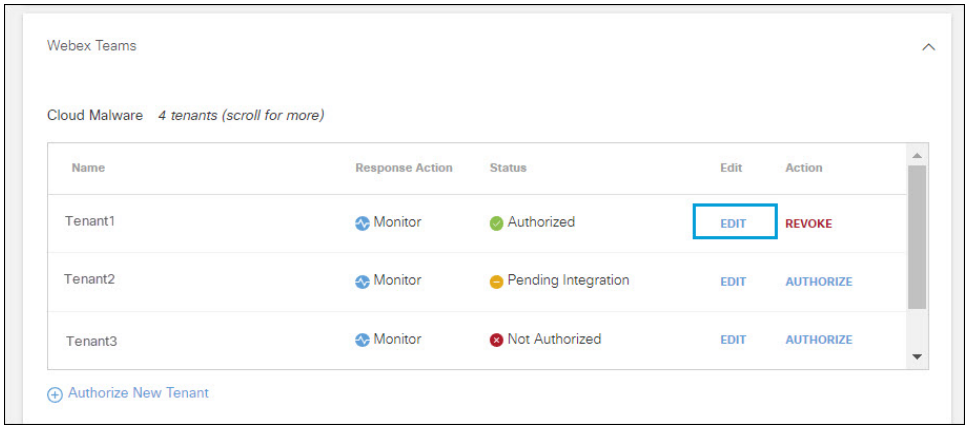
Edit a Tenant

Provides instructions for editing a tenant. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

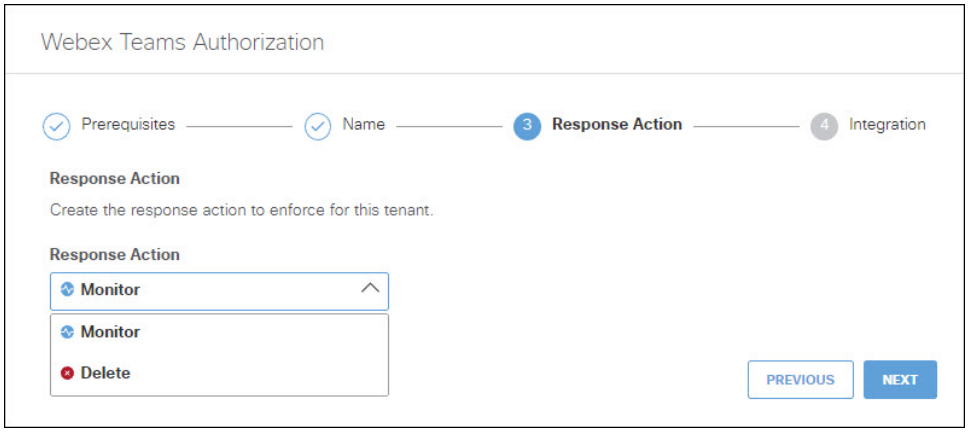
You can change the Response Action you have selected for a tenant.

Procedure

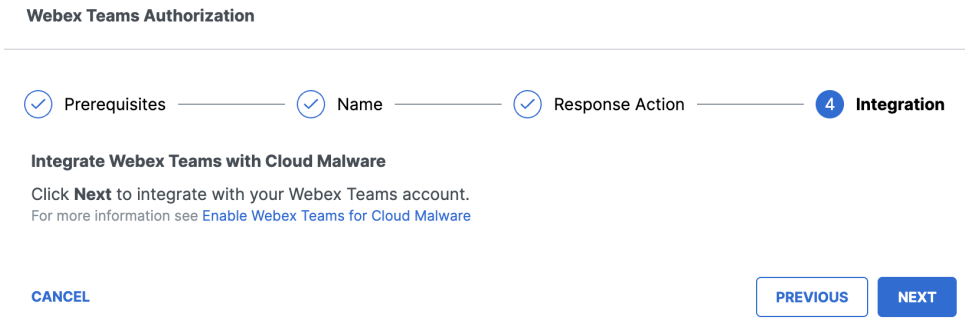
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Webex Teams**.
3. In the **Cloud Malware** section , under **Action**, click **Edit**. You can edit any tenant.



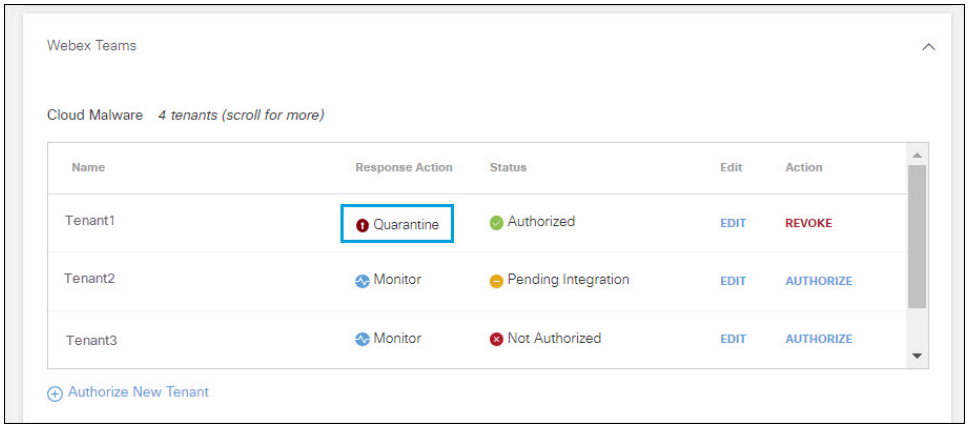
4. Select a **Response Action** for Secure Access to apply to Webex Teams files found with malware, then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually delete these files from the Cloud Malware report.
   - Choose **Delete** to delete the file.



5. Click **Next** to continue.



6. The new **Response Action** is displayed.

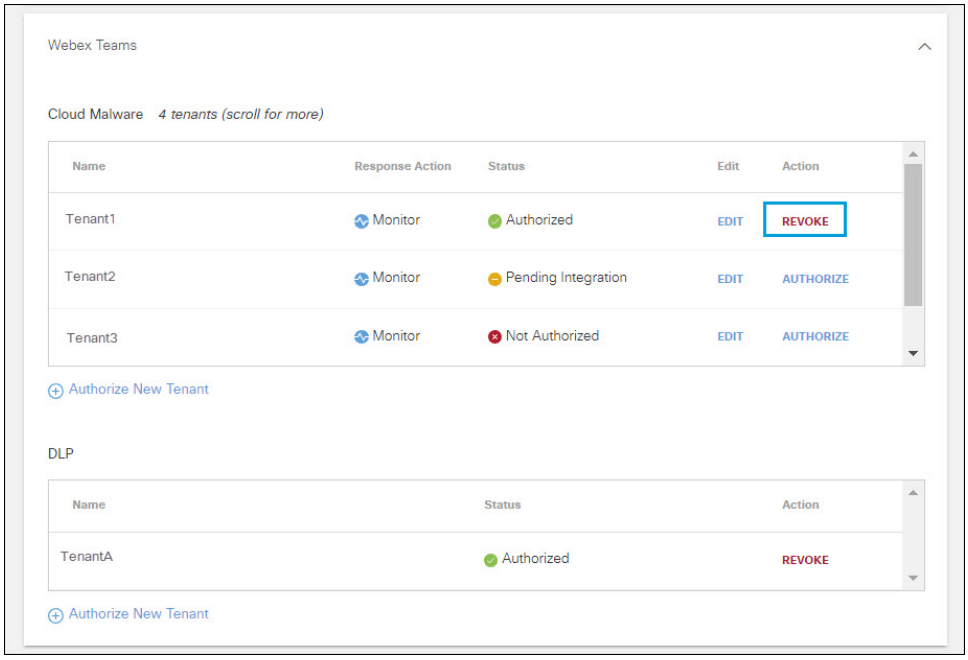


Revoke Authorization

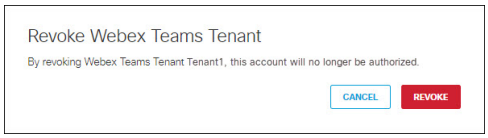
Provides instructions for revoking authorization for Webex Teams tenants.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



47 Manage Logging

Topics:

- Manage Logging

Describes the purpose and procedures for manage logging and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Logging

Describes managing logging. Secure Access allows for the logging of events and traffic, and these logs can be saved to your own S3 bucket.

Secure Access allows for the logging of events and traffic, and these logs can be saved to your own S3 bucket.

Secure Access logs are CSV-formatted, compressed (gzip), and saved every 10 minutes. For more information, see Log Formats and Versioning.

Enable Logging

Provides instructions for enabling logging. Secure Access allows for the logging of events and traffic through a policy's rule. By default, logging is disabled. Logging can be enabled or disabled at any time for any rule.

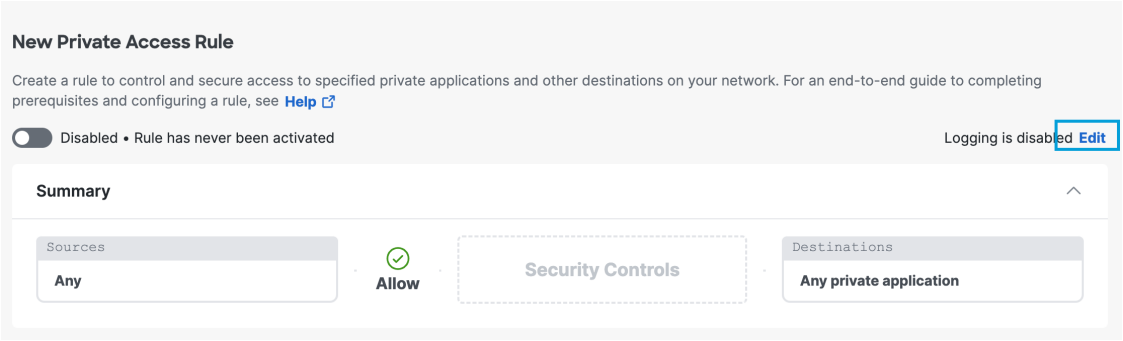
Secure Access allows for the logging of events and traffic through a policy's rule. By default, logging is disabled. Logging can be enabled or disabled at any time for any rule.

Before you begin

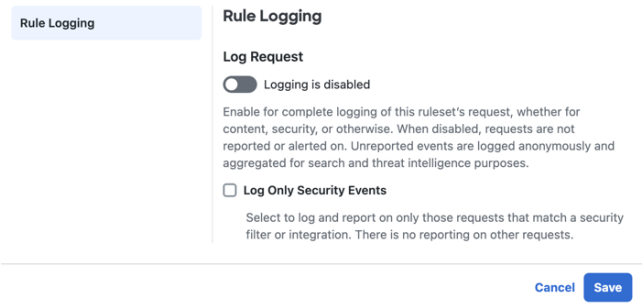
- Full Admin user role is required. For more information, see Manage Accounts.

Procedure

1. For each rule, click **Edit** and make changes as needed.



2. Make changes as needed and click **Save**.



Settings are:

- **Log Request**– Enable the logging of this ruleset's request to log all request activity for a rule including content, security, or otherwise.

- **Log Only Security Events**–Only logs security events and not all requests. This provides better user privacy.

Enable Logging to Your Own S3 Bucket

Describes enabling logging to your own s3 bucket. You can configure Secure Access to log events to an Amazon S3 bucket that you manage. To enable logging to a self-managed Amazon S3 bucket, follow the prerequisite steps to set up an AWS account and create an Amazon S3 bucket.

You can configure Secure Access to log events to an Amazon S3 bucket that you manage. To enable logging to a self-managed Amazon S3 bucket, follow the prerequisite steps to set up an AWS account and create an Amazon S3 bucket. Once you have created an S3 bucket in Amazon, configure Secure Access to use it for the storage of logs.

Prerequisites

Describes prerequisites. Full Admin user role is required. For more information, see Manage Accounts. A login to Amazon AWS service (http://aws.amazon.com/console/). If you don't have an account, Amazon provides free sign-up for S3.

- Full Admin user role is required. For more information, see Manage Accounts.
- A login to Amazon AWS service (http://aws.amazon.com/console/). If you don't have an account, Amazon provides free sign-up for S3.

> **Note**
>
> Amazon requires a credit card in case your usage exceeds free plan usage.

- A bucket configured in Amazon S3 to be used for storing logs. The S3 bucket must be provisioned in the AWS GovCloud (US-East) (us-gov-east-1) region.For more information, see Amazon's S3 documentation.

> **Note**
>
> Periods in S3 bucket names are not supported.

JSON Bucket Policy

Describes json bucket policy. When you set up your Amazon S3 bucket in AWS GovCloud (US-East), you must add a bucket policy that accepts uploads from Secure Access. Copy the following preconfigured JSON and substitute your S3 bucket name for bucketname.

When you set up your Amazon S3 bucket in AWS GovCloud (US-East), you must add a bucket policy that accepts uploads from Secure Access. Copy the following preconfigured JSON and substitute your S3 bucket name for `bucketname`. Then, paste the Secure Access S3 bucket policy into your Amazon S3 bucket policy.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "bucket-name-sid1",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS":
"arn:aws-us-gov:iam::362951712785:role/s3-log-exporter-role-reporting-prod-01"

            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws-us-gov:s3:::your-bucket-name/*"
        },
        {
            "Sid": "bucket-name-sid2",
            "Effect": "Deny",
            "Principal": {
                "AWS":
"arn:aws-us-gov:iam::362951712785:role/s3-log-exporter-role-reporting-prod-01"

            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws-us-gov:s3:::your-bucket-name/*"
        },
        {
            "Sid": "bucket-name-sid3",
            "Effect": "Allow",
            "Principal": {
                "AWS":
"arn:aws-us-gov:iam::362951712785:role/s3-log-exporter-role-reporting-prod-01"

            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws-us-gov:s3:::your-bucket-name"
        },
        {
            "Sid": "bucket-name-sid4",
            "Effect": "Allow",
            "Principal": {
                "AWS":
"arn:aws-us-gov:iam::362951712785:role/s3-log-exporter-role-reporting-prod-01"

            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws-us-gov:s3:::your-bucket-name"
        }
    ]
}
```

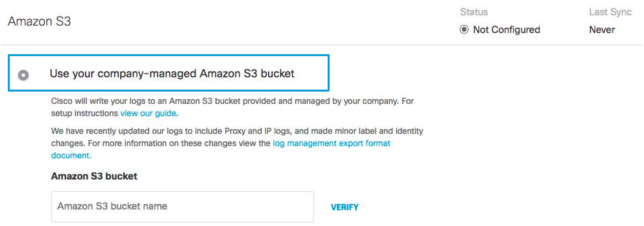
Procedure

Provides instructions for procedure. You must first configure a bucket in Amazon S3 to be used for storing logs. The S3 bucket must be provisioned in the AWS GovCloud (US-East) (us-gov-east-1) region. For more information, see Amazon's S3 documentation.

> **Note**
>
> You must first configure a bucket in Amazon S3 to be used for storing logs. The S3 bucket must be provisioned in the AWS GovCloud (US-East) (us-gov-east-1) region. For more information, see Amazon's S3 documentation.

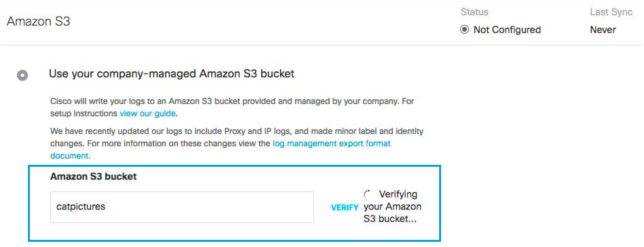
Procedure

1. Navigate to **Admin** > **Log Management** and in the **Amazon S3** area select **Use your company-managed Amazon S3 bucket**.

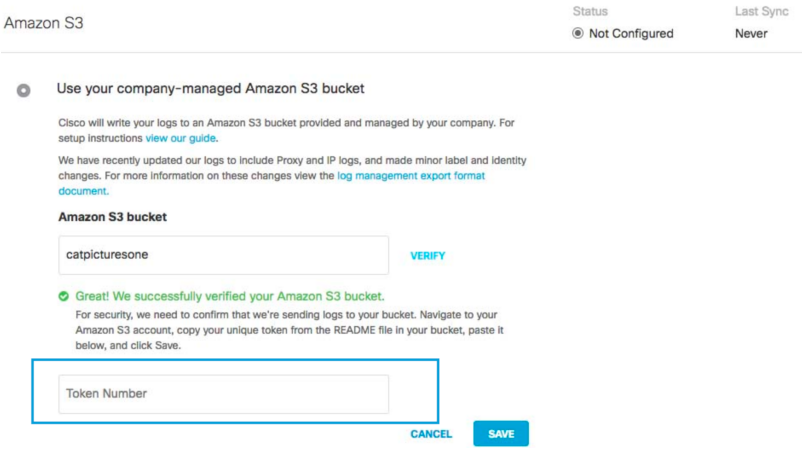


2. In the **Amazon S3 Bucket** field, type or paste the exact bucket name you created in Amazon S3 and click **Verify**.

   Secure Access verifies your bucket, connects to it, and saves a README_FROM_UMBRELLA.txt file to your bucket.



3. Open the `README_FROM_UMBRELLA.txt` file Secure Access saved to your bucket, copy and paste the token listed in it into **Token Number**, and click **Save**.



S3 Bucket Data Path

Describes s3 bucket data path. You can integrate your self-managed AWS S3 bucket with the Cisco Cloud Security App for Splunk. Use the data path to your AWS S3 bucket to set up the integration. The S3 bucket data path contains the following path fields:

You can integrate your self-managed AWS S3 bucket with the Cisco Cloud Security App for Splunk. Use the data path to your AWS S3 bucket to set up the integration. The S3 bucket data path contains the following path fields:

```
<AWS S3 bucket name>-<AWS region>/<AWS S3 bucket directory prefix>
```

1. **AWS S3 bucket name and AWS region**–the name of your AWS S3 bucket, a dash (–), and the **AWS region**.
2. **AWS S3 bucket directory prefix**–the directory prefix (customer folder name) to the AWS S3 bucket.

Sample S3 Bucket Data Path:

```
my_company_name-us-gov-east-1/dnslogs
```

Use the data path to your self-managed S3 bucket to:

- Download log files with the AWS CLI.
- Set up your AWS S3 bucket with the Cisco Cloud Security App for Splunk. The Cisco Cloud Security App for Splunk enables you to analyze your Secure Access logs found in your AWS S3 bucket. For more information, see Cisco Cloud Security App for Splunk.

Download Files From the S3 Bucket Locally

Describes downloading files from the s3 bucket locally. You can use the Amazon command-line interface (CLI) to download files from a self-managed S3 bucket to your local directory.

You can use the Amazon command-line interface (CLI) to download files from a self-managed S3 bucket to your local directory.

Prerequisites

- Install the AWS CLI to your system.

Run the AWS CLI to download your files from an S3 bucket to your local directory. To run the AWS CLI command in test mode (without syncing files), use the `--dryrun` flag.

AWS CLI command syntax:

```
aws s3 sync s3://DATAPATH /path/to/local/directory/
```

Detailed sample command:

```
aws s3 sync s3://mycompany-us-gov-east-1/dnslogs
/opt/splunk/etc/apps/TA-cisco_umbrella/data/
```

Stop Logging

Provides instructions for stopping logging. You can stop logging at any time. When logging is stopped, Secure Access immediately stops sending logs to your S3 storage.

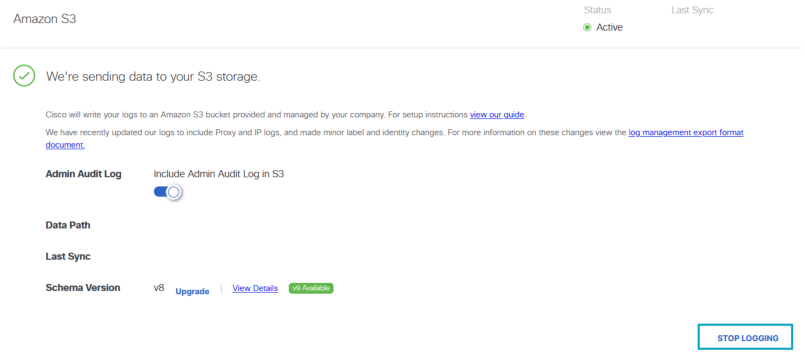
You can stop logging at any time. When logging is stopped, Secure Access immediately stops sending logs to your S3 storage.

Before you begin

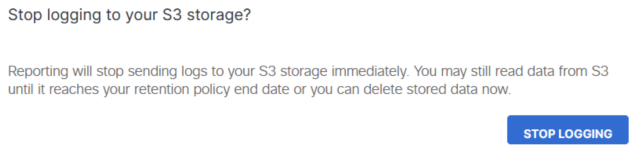
- Full Admin user role is required. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Log Management**.
2. In the **Amazon S3** area, click **Stop Logging**.



3. Click **Stop Logging** to confirm your request.



Log Formats and Versioning

Describes log formats and versioning. Cisco Secure Access stores zipped comma-separated values (CSV) log files in your own AWS S3 bucket. Each log file displays multiple columns of information extracted from your Secure Access logs.

Cisco Secure Access stores zipped comma-separated values (CSV) log files in your own AWS S3 bucket. Each log file displays multiple columns of information extracted from your Secure Access logs. A log file may have additional fields that are not shown on the Secure Access reports.

The latest version of the Secure Access log format is version 9 (v9).

> **Note**
>
> Logs are not always chronological and are not always in the specific time bucket based on the timestamp of the log event.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Configure logging to an Amazon S3 bucket. See Enable Logging to Your Own S3 Bucket.

Log File Name Formats

Describes log file name formats. Logs are uploaded in ten-minute intervals from the Secure Access log queue to the AWS S3 bucket. Within the first two hours after a completed configuration, you should receive your first log upload to your AWS S3 bucket.

Logs are uploaded in ten-minute intervals from the Secure Access log queue to the AWS S3 bucket. Within the first two hours after a completed configuration, you should receive your first log upload to your AWS S3 bucket.

Note

To check if everything is working, the **Last Sync** time in Secure Access should update and logs should begin to appear in your AWS S3 bucket. The logs appear in a GZIP format with the following file name format. The files will also be sorted into date-stamped folders.

- **DNS traffic**

  `dnslogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

- **Web traffic**

  `proxylogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

- **Firewall traffic**

  `firewalllogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

- **Admin Audit logs**

  `auditlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

- **IPS traffic**

  `intrusionlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

- **DLP traffic**

  `dlplogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

- **Remote Access VPN traffic**

  `vpnlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

- **Zero Trust Network Access traffic**

  `ztnalogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

Subfolders

Describes subfolders. Logs are uploaded to AWS S3 buckets in the appropriate subfolder.

Logs are uploaded to AWS S3 buckets in the appropriate subfolder with the following naming format.

```
<subfolder>/<YYYY>-<MM>-<DD>/<YYYY>-<MM>-<DD>-<hh>-<mm>-<xxxx>.csv.gz
```

Secure Access names a log subfolder (`<subfolder>`) with one of the following folder names:

- `dnslogs`
- `proxylogs`

- `firewalllogs`
- `iplogs`
- `auditlogs`
- `dlplogs`
- `vpnlogs`
- `ztnalogs`

The **<xxxx>** segment of the log GZIP file name is a random string of four alphanumeric characters, which prevents duplicate file names from being overwritten.

Example: `dnslogs/2019-01-01/2019-01-01-00-00-e4e1.csv.gz`

Find Your Log Schema Version

Describes find your log schema version. Depending on the Secure Access subscription that you have, and depending on the type of AWS S3 bucket you configure, there are different versions of the log schemas available.

Depending on the Secure Access subscription that you have, and depending on the type of AWS S3 bucket you configure, there are different versions of the log schemas available. Once your system is configured to log to an AWS S3 bucket you can view the log schema version in use.

Log Schema Versions

Describes log schema versions. V1–For customers who have configured their own S3 bucket before November 2017. To upgrade from v1 to a higher version of the Secure Access log format, you must remove your existing S3 bucket, disable the integration, and then recreate a new bucket.

- **v1**–For customers who have configured their own S3 bucket *before* November 2017.

  > **Note**
  >
  > To upgrade from **v1** to a higher version of the Secure Access log format, you must remove your existing S3 bucket, disable the integration, and then recreate a new bucket. For all other versions, you can upgrade from the Log Management screen of the Secure Access dashboard by clicking **Upgrade**.

- **v2**–For customers who have configured their own S3 bucket *after* November 2017, or are using a Cisco-managed bucket. This version is inclusive of everything in version 1.
- **v3**– The same as version 2, but adds two new fields: Most Granular Identity Type and Identity Types for DNS logs.
- **v4**–The same as version 3, but adds the Blocked Categories field for DNS and Proxy logs.
- **v5**–The same as version 4, but adds three new fields: all Identities, all Identity Types, and Request Method for Proxy logs.
- **v6**–The same as version 5, but adds the following fields to Proxy logs: Certificate Errors, Destination Lists IDs, DLP Status, File Name, Rule ID, and Ruleset ID.
- **v7**–The same as version 6, but adds the DLP file label field.
- **v8**–The same as version 7, but adds fields to the Proxy, DLP, and Firewall logs.
  - Proxy logs–Adds the Isolate Action, File Action, and Warn Status fields.
  - DLP logs–Changes the Event Type field. The event type is either `Real Time` or `SaaS API`.

  - Firewall logs–Adds the FQDNs and Destination List IDs fields.

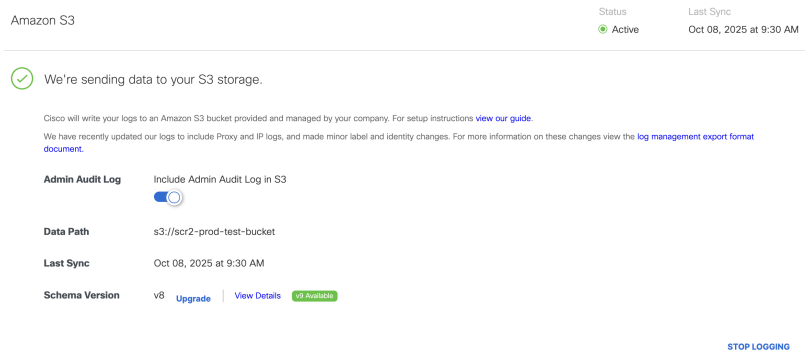
- **v9**–The same fields as version 8, but the v9 log format adds fields to the IPS and Web logs.
  - Adds new fields to the **Intrusion Prevention System (IPS)** logs: **operation mode**, **policy resource ID**, **direction**, **firewall rule ID**, **IPS config type**, **AWS region**.
  - Adds new fields to the **Web** logs: **forwarding method** and **producer**.
  - Adds **Remote Access Virtual Private Network** logs.
  - Adds **Zero Trust Network Access** logs.

View Your Log Schema Version and Last Sync Time

Provides instructions for viewing your log schema version and last sync time. It also identifies related requirements, procedures, and operational considerations.

Procedure

1. Navigate to **Admin** > **Log Management**.
2. In the **Amazon S3** area, Secure Access displays the log **Schema Version** in use and **Last Sync** time.**Last Sync** is the date and time of the last sync of your logs to Amazon S3.



Log File Fields

Describes log file fields. Each type of Secure Access log contains various log fields. Not all field values are available in every log record. When a field does not have a value, Secure Access sets the field to the empty string ("").

Each type of Secure Access log contains various log fields. Not all field values are available in every log record. When a field does not have a value, Secure Access sets the field to the empty string (""). For information about the formats of the Secure Access reports, see Reports and CSV Formats.

- Admin Audit Log Formats
- Cloud Firewall Log Formats
- DLP Log Formats
- DNS Log Formats
- IPS Log Formats
- Remote Access VPN Log Formats
- Web Log Formats

- Zero Trust Network Access Log Formats

Estimate the Size of a Log

Describes estimate the size of a log. The size of your S3 logs depends on the number of events that occur and the volume of the traffic in your organization.

The size of your S3 logs depends on the number of events that occur and the volume of the traffic in your organization.

1. Download one of your Secure Access log files. The Secure Access log file is a comma-separated values (CSV) file.
2. Count the number of rows in the CSV file minus one for the header row.

   The number of rows is equivalent to the number of events in the twenty-four hour period.
3. Multiply the number of rows of data by the number of bytes of data listed in a single row in the file.

   The result is the estimate of the size of the event log recorded for one day.

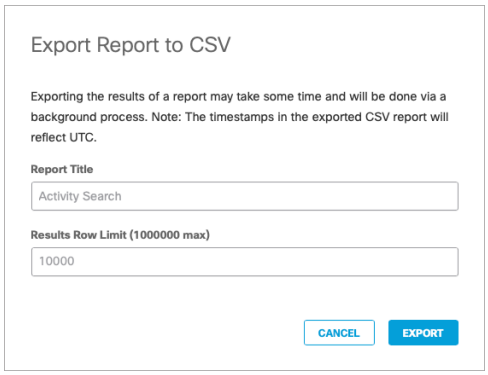
Estimate the Size of an Exported Report

Provides instructions for estimate the size of an exported report. The size of an exported report depends on the number of events that occur, which is dependent on the volume of your traffic.

The size of an exported report depends on the number of events that occur, which is dependent on the volume of your traffic. The size of each log line varies based on a number of items–for example, the length of the domain name or the number of categories. Assuming each log line is 220 bytes, a million requests would be 220 MB.

Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. For Filters, run a report for the last 24 hours and then click the **Export CSV** icon.



3. Open the downloaded CSV file. The number of rows (minus one for the header) is the number of queries per day. Multiply the number of rows by the number of bytes in one row to get the estimate for one day.

Reports and CSV Formats

Describes the content and purpose of reports and csv formats. Cisco Secure Access has various reports that you can download from Secure Access in the comma-separated values (CSV) format. For information about the size of a report, see .

Cisco Secure Access has various reports that you can download from Secure Access in the comma-separated values (CSV) format. For information about the size of a report, see Estimate the Size of an Exported Report on page 740.

The following sections describe the log fields for each type of Secure Access report:

- Activity Search Report on page 741
- Top Categories Report on page 743
- Top Destinations Report on page 743
- Top Resources Report on page 744

Activity Search Report

Describes the content and purpose of activity search report. You can export the results of the Activity Search Report to a CSV format. For more information, see and .

You can export the results of the Activity Search Report to a CSV format. For more information, see Export Report Data to CSV on page 981 and View the Activity Search Report on page 997.

Fields in the Activity Search Report:

- **Type**–The type of request made, such as DNS.
- **Date**–The date the request was made.
- **Time**–The time the request was made, in UTC.
- **Action**–Whether the request was Allowed or Blocked.
- **Errors**–Any certificate or protocol errors in the request.
- **Ruleset ID**–The ID number assigned to the ruleset.
- **Ruleset Name**–The ruleset that was applied.
- **Rule ID**–The ID number assigned to the rule.
- **Rule Name**–The rule that was applied.
- **Destination List IDs**–The ID number assigned to a destination list.
- **Destination Lists**
- **Signature List ID**–The unique ID assigned to a Default or Custom Signature List.
- **IPS Signature**–The threat detected in our IPS/IDS protection.
- **IPS Signature Severity**–The severity of the IPS Signature.
- **IPS Signature CVE**–Common vulnerabilities and exposures related to the IPS Signature.
- **Identities**–All tunnel identities associated with this request.
- **Identity Types**–The types of identity that were associated with the request. For example, Roaming Computers or Networks.
- **Policy or Ruleset Identity**–The identity that made the request.
- **Policy or Ruleset Identity Type**–The type of the identity that made the request.
- **Forwarding Method**–The method used to forward the identity of the client to the proxy.
- **Internal IP**–The internal IP address that made the request.
- **External IP**–The external IP address that made the request.
- **Source IP**–The IP of the computer making the request.
- **Destination IP**–The destination IP requested.
- **Source Port**–The port the request was made on.

- **Destination Port**–The destination port the request was made on.
- **Destination**–The domain of the request.
- **Hostname**–The name of the host.
- **Categories**–The content categories, if any, that matched against the destination IP address or port requested.
- **Integrations**–Integration categories you set.
- **Blocked Categories**–The category that resulted in the destination being blocked.
- **Application**–The application associated with the request.
- **Application Category**–The categories for any applications associated with the request.
- **Query Type**–The type of DNS request that was made.
- **Content Type**–The type of web content; typically text or html.
- **Protocol**–The actual protocol of the traffic. For example, TCP, UDP, or ICMP.
- **Filename**–The name of the file.
- **File Action (Remote Browser Isolation)**–The action taken on a file during a Remote Browser Isolation session.
- **Total Size in Bytes**–The total size in bytes.
- **Request Size**–Request size in bytes.
- **Response Size**–Response size in bytes.
- **Packet Size**–Packet size in bytes.
- **Referrer**–The referring domain or URL.
- **User Agent**–The browser agent that made the request.
- **Status Code**–The HTTP status code.
- **Direction**–The direction of the packet. It is directed either towards the internet or to the customer's network.
- **Threats**–Any threats associated with the request.
- **Threat Types**–The types of threats associated with the request.
- **SHA256 Hash**–The hex digest of the response content.
- **Cisco AMP Result**–The malware detected by AMP.
- **Cisco AMP Disposition**–What action was taken on the file download.
- **Cisco AMP Score**–The risk score associated with the downloaded file. This field returns blank unless the verdict is Unknown, in which the value will be 0.
- **Antivirus Result**–Threats detected by the antivirus.
- **Potentially Unwanted Applications**–A list of all potentially unwanted application (PUA) results for the proxied file as returned by the antivirus scanner.
- **Detected Response File Type**–The file type of the response, as detected by the file type control that blocked the request based on factors such as URL or content type header.
- **Isolated State**–Whether the Remote Browser Isolation state was isolated or not.
- **Data Loss Prevention State**–Whether the DLP status was allowed or blocked.
- **Tenant Controls**–Whether the request is Tenant Application Access Control protected.

Zero Trust Access Activity Search Fields

Describes the fields in the Zero Trust Access event details of the Activity Search report.

The Activity Search report displays the Zero Trust Access event details.

Field Name	Reports Section	Description
Ingress Region	Event Details	The geographic region of the data center where Secure Access received the incoming traffic.
Tunnel Type	Event Details	The type of traffic supported by the network tunnel, which the endpoint established with the proxy. The transport protocol on the tunnel is either **HTTP** or **HTTP3**.
Transaction ID	Event Details	The unique ID associated with the Zero Trust request. Use the transaction ID to correlate and troubleshoot connection issues.
Block Reason	Block Details	Secure Access provides an explanation for blocking access to the private resource.
Associated Rule	Block Details	When access was blocked for not meeting access or posture requirements, Secure Access reports the closest matched policy rule that would have allowed access.
Associated Posture	Block Details	The posture profile that is configured for the associated rule.
Endpoint Application	Endpoint Details	The name of the endpoint application, which initiated the connection.
Application Signature	Endpoint Details	The SHA256 signature of the endpoint application process.
Endpoint Username	Endpoint Details	The username that is associated with the endpoint application process.

Top Categories Report

Describes the content and purpose of top categories report. You can export the results of the Top Categories Report to a CSV format. For more information, see and .

You can export the results of the Top Categories Report to a CSV format. For more information, see Export Report Data to CSV on page 981 and Top Categories Report on page 1073.

Fields in the Top Categories Report:

- **Category**–A content category in which a request was made. See Manage Content Category Lists on page 336.
- **Count**–The number of requests made for the category.

Top Destinations Report

Describes the content and purpose of top destinations report. You can export the results of the Top Destinations Report to a CSV format. For more information, see and .

You can export the results of the Top Destinations Report to a CSV format. For more information, see Export Report Data to CSV on page 981 and Top Destinations Report on page 1063.

Fields in the Top Destinations Report:

- **Domain**–The domain that was requested.
- **Query Count**–The number of requests for the domain.
- **Categories**–The content categories that matched against the destination requested. See Manage Content Category Lists on page 336.

Top Resources Report

Describes the content and purpose of top resources report. You can export the results of the Top Resources Report to a CSV format. For more information, see .

You can export the results of the Top Resources Report to a CSV format. For more information, see Export Report Data to CSV on page 981.

Fields in the Top Resources Report:

- **Identity**–The identity making requests.
- **Query Count**–The number of requests made by the identity.

Admin Audit Log Formats

Describes the content and purpose of admin audit log formats. The Cisco Secure Access Admin Audit logs show the administrative changes to your organization's Secure Access settings.

The Cisco Secure Access Admin Audit logs show the administrative changes to your organization's Secure Access settings. For information about the size of a log file, see Estimate the Size of a Log on page 740.

Example

This is an example of a v4 through v9 Admin Audit log event:

```
id,timestamp,email,user,type,action,logged in from,before,after
"123","2024-07-22
10:46:45","[user@domain.com](mailto:user@domain.com)","","logexportconfigurations","update","209.165.200.227","version:
 4","version: 5"
```

Order of Fields in Admin Audit Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

V9 Log Format

The CSV fields in the header row of the Admin Audit log.

```
id,timestamp,email,user,type,action,logged in from,before,after
```

> **Note**
>
> The last two fields, "Before" and "After," may contain line breaks if the previous or updated value spans multiple lines.

The description of each field and the log version in which each field was released, from **Version 4** up to **Version 9**. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
id	A unique identifier of the audit event.	v4
timestamp	The date and time of the administrative change event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v4
email	The email of the user that triggered the event.	v4
user	The account name of the user who created the change.	v4
type	Where the change was made, such as settings or a policy.	v4
action	The type of change made, such as Create, update, or Delete.	v4
logged in from	The user's IP source.	v4
before	The policy or setting before the change was made.	v4
after	The policy or setting after the change was made.	v4

Cloud Firewall Log Formats

Describes the content and purpose of cloud firewall log formats. Cloud firewall logs show traffic that has been handled by Secure Access cloud-delivered firewall.

Cloud firewall logs show traffic that has been handled by Secure Access cloud-delivered firewall. For information about the size of a log file, see Estimate the Size of a Log on page 740.

Example

This is an example of a v9 Cloud Firewall log:

```
timestamp,origin IDs,identities,identity type,direction,protocol,packet
size,source IP,source port,destination IP,destination port,data center,rule
ID,action,fqdns,destination list IDs,first packet timestamp,last packet
timestamp,packets sent,packets received,bytes sent,bytes received,fw event id
"2024-06-14 18:59:57","\[211039844\]","Passive Monitor", "CDFW Tunnel
Device","UNKNOWN","1","84","172.17.3.4","605","146.112.25.129","443","tls_ed","12","ALLOW","google.com,apple.com","4,6","178957","178957","3","3","108","55","342"
```

Order of Fields in the Cloud Firewall Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

V9 Log Format

The CSV fields in the header row of the Cloud Firewall logs.

```
timestamp,origin ids,identities,identity type,direction,protocol,packet
size,source ip,source port,destination ip,destination port,data center,rule
id,action,fqdns,destination list ids,first packet timestamp,last packet
timestamp,packets sent,packets received,bytes sent,bytes received,fw event id
```

The description of each field and the log version in which each field was released, up to **Version 9**. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the cloud-delivered firewall traffic event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v1
origin ids	The unique identity of the network tunnel.	v1
identities	The names of the network tunnel.	v5
identity type	The type of identity that made the request. Should always be `CDFW Tunnel Device`.	v5

Field name	Description	Release version
direction	The direction of the packet. It is destined either towards the internet or to the customer's network.	v1
protocol	The actual protocol of the traffic. Valid values are: `TCP`, `UDP`, or `ICMP`.	v1
packet size	The size in bytes of the packet sent to the CDFW.	v1
source ip	The internal IP address of the user-generated traffic towards the CDFW. If the traffic goes through NAT before it comes to CDFW, it will be the NAT IP address.	v1
source port	The internal port number of the user-generated traffic towards the CDFW.	v1
destination ip	The destination IP address of the user-generated traffic towards the CDFW.	v1
destination port	The destination port number of the user-generated traffic towards the CDFW.	v1
data center	The name of the data center that processed the user-generated traffic.	v1
rule id	The ID of the rule that processed the user traffic.	v1
action	The final verdict whether to allow or block the traffic based on the rule.	v1
fqdns	The fully qualified domain names (FQDNs) that match the request.	v8
destination list ids	The destination list IDs that Secure Access applied in the rule.	v8
first packet timestamp	The timestamp when the first packet of the session was received in UTC in seconds. Populated only for traffic handled by Cisco Secure Firewall.	v9
last packet timestamp	The timestamp when the last packet of the session was received in UTC in seconds. Populated only for traffic handled by Cisco Secure Firewall.	v9
packets sent	The number of packets sent during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
packets received	The number of packets received during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9

Field name	Description	Release version
bytes sent	The number of bytes sent during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
bytes received	The number of bytes received during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
fw event id	The ID of the firewall event. Populated only for traffic handled by Cisco Secure Firewall.	v9

Data Loss Prevention (DLP) Log Formats

Describes the content and purpose of data loss prevention (dlp) log formats. The Cisco Secure Access DLP logs show information about DLP events where data identifiers were triggered and a violation occurred. DLP logs are available in all log format versions.

The Cisco Secure Access DLP logs show information about DLP events where data identifiers were triggered and a violation occurred. DLP logs are available in all log format versions. For information about the size of a log file, see Estimate the Size of a Log on page 740.

Note

A single DLP event can present in multiple rows of the logs when different data identifiers and file labels are triggered for the same content. Rows related to the same content or event have the same Unique Event ID.

Example

This is an example of a v9 DLP log event:

```
timestamp,event type,unique event
id,severity,identity,owner,name,application,destination,action,rule,data
classification,data identifier,content type,file size,sha 256 hash,file label
"2022-02-15 12:05:45","Real
[illegible]
 PCI Classification","Credit Card Number -
Strict","text/html","48","abbd2352c3cfea8846871928bf99ca24dc3a6f162170926649381a6d968869ab",
 "Confidential"
```

Order of Fields in the DLP Log

Note

Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

V9 Log Formats

The CSV fields in the header row of the DLP logs.

```
timestamp,event type,unique event
id,severity,identity,owner,name,application,destination,action,rule,data
classification,data identifier,content type,file size,sha 256 hash,file label
```

The description of each field and the log version in which each field was released, up to **Version 9**. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the DLP event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v6
event type	The type of event that matched a data identifier. `Real Time` denotes a proxy-based DLP event triggered by a Real Time rule and `SaaS API` denotes a DLP event triggered by any of the SaaS API rules.	v8
unique event id	The unique identifier for the event. There can be multiple violation matches in one event.	v6
severity	The severity of the rule: `Low/Info`, `Medium/Warn`, `High/Alert`, or `Critical`.	v6
identity	The source that triggered the violation.	v6
owner	The owner of the file.	v6
name	The name of the file.	v6
application	The application of the request.	v6
destination	The domain of the request.	v6
action	If the violation was `Blocked` or `Monitored`.	v6
rule	The DLP rule name.	v6
data classification	The data classification whose data identifier matched on the violation.	v6
data identifier	The data identifier that matched on the request.	v6
content type	The mime type of the file that matches the data identifier.	v6

Field name	Description	Release version
file size	The size of the file in bytes.	v6
sha 256 hash	The hex digest of the response content.	v6
file label	The file name label that matched on the file properties.	v7

DNS Log Formats

Describes the content and purpose of dns log formats. The Cisco Secure Access DNS logs show your organization's traffic through the Secure Access DNS resolvers. For information about the size of a log file, see .

The Cisco Secure Access DNS logs show your organization's traffic through the Secure Access DNS resolvers. For information about the size of a log file, see Estimate the Size of a Log on page 740.

Examples

This is an example of a v9 DNS Log of an Allowed Action event:

```
timestamp,most granular identity,identities,internal ip,external ip,action,query
 type,response code,domain,categories,most granular identity type,identity
types,blocked categories
"2024-09-11 18:46:00","Active Directory User (adusername@example.net)","Active
 Directory User
(adusername@example.net),WIN11-SNG01-Example","10.10.1.100","24.123.132.133","Allowed","1
 (A)","NOERROR","domain-visited.com.","Software/Technology,Business
Services,Allow List,Infrastructure and Content Delivery Networks,SaaS and
B2B,Application","AD Users","AD Users,Anyconnect Roaming Client",""
```

An example of a v9 DNS Log of a Blocked Action event with Blocked Categories.

```
timestamp,most granular identity,identities,internal ip,external ip,action,query
 type,response code,domain,categories,most granular identity type,identity
types,blocked categories
"2024-09-11 18:46:00","Active Directory User (adusername@example.net)","Active
 Directory User
(adusername@example.net),WIN11-SNG01-Example","10.10.1.100","24.123.132.133","Blocked","1
 (A)","NOERROR","domain-visited.com.","Chat,Social Networking","AD Users","AD
 Users,Anyconnect Roaming Client","Social Networking"
```

Order of Fields in the DNS Log

Note

Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

V9 Log Formats

The CSV fields in the header row of the DNS logs.

```
timestamp,most granular identity,identities,internal ip,external ip,action,query
 type,response code,domain,categories,most granular identity type,identity
types,blocked categories
```

The description of each field and the log version in which each field was released, up to **Version 9**. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the DNS event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v8
most granular identity	The first identity matched with this request in order of granularity.	v8
identities	All identities associated with this request.	v5
internal ip	The internal IP address that made the request.	v8
external ip	The external IP address that made the request.	v8
action	Whether the request was allowed or blocked.	v8
query type	The type of DNS request that was made.	v8
response code	The DNS return code for this request.	v8
domain	The domain that was requested.	v8
categories	The security or content categories that the destination matches. For category definitions, see Manage Threat Categories and Manage Content Category Lists.	v8
most granular identity type	The first identity type matched with this request in order of granularity.	v3
identity types	The type of identity that made the request, for example: Roaming Computer, Network.	v3
blocked categories	The categories that resulted in the destination being blocked.	v4

IPS Log Formats

Describes the content and purpose of ips log formats. The Cisco Secure Access IPS logs show the traffic, events, and possible threats detected by the Secure Access Intrusion Prevention System.

The Cisco Secure Access IPS logs show the traffic, events, and possible threats detected by the Secure Access Intrusion Prevention System. For information about the size of a log file, see Estimate the Size of a Log on page 740.

Example

This is an example of a v9 IPS log:

```
timestamp,identities,identity types,generator id,signature id,signature
message,signature list id,severity,attack classification,cves,ip
protocol,session id,source ip,source port,destination ip,destination
port,action,operation mode,policy resource id,direction,firewall rule id,ips
config type,aws region
"2024-09-11 23:17:13","Firewall Tunnel Name","Network
Tunnels","1","16606","SERVER-ORACLE BEA WebLogic Server Plug-ins Certificate
overflow attempt","50516","HIGH","Attempted User Privilege
Gain","cve-2009-1016","TCP","12345","123.123.123.123","80","1.1.1.1","40762","Would
 Block","IDS","50516","S2C","21171","PROFILE","eu-central-2b"
```

Order of Fields in the IPS Log

Note

Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

V9 Log Format

The CSV fields in the header row of the IPS log.

```
timestamp,identities,identity types,generator id,signature id,signature
message,signature list id,severity,attack classification,cves,ip
protocol,session id,source ip,source port,destination ip,destination
port,action,operation mode,policy resource id,direction,firewall rule id,ips
config type,aws region
```

The description of each field and the log version in which each field was released, up to **Version 9**. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the IPS detection event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v8
identities	All tunnel identities that are associated with this request.	v8
identity types	The type of identity that is associated with this request.	v8
generator id	Unique ID assigned to the part of the IPS that generated the event.	v8
signature id	Used to uniquely identify signatures.	v8
signature message	A brief description of the signature.	v8
signature list id	Unique ID assigned to a Default or Custom Signature List.	v8
severity	The severity level of the rule. Valid values are: `High`, `Medium`, `Low`, and `Very Low`.	v8
attack classification	The category of attack detected by a rule that is part of a more general type of attack class. Valid values are: `trojan-activity`, `attempted-user`, and `unknown`.	v8
cves	A list of information about security vulnerabilities and exposures.	v8
ip protocol	The actual protocol of the traffic, such as `TCP`, `UDP`, `ICMP`.	v8
session id	The unique identifier of a session, which is used to group the correlated events between various services.	v8
source ip	The IP of the computer making the request.	v8
source port	The port number of the request.	v8
destination ip	The port number of the request.	v8
destination port	The destination port number of the request.	v8

Field name	Description	Release version
action	The action performed when criteria meets a rule, for example: `block`, `warn`, and `would_block`.	v8
operation mode	The mode of operation of the IPS, either detection or prevention. Valid values are: `IDS`, `IPS`, and `UNKNOWN`.	v9
policy resource id	The ID of the IPS policy resource. An example of a policy resource is: signature list.	v9
direction	The direction of the packet that matches the signature. Valid values are: `S2C`, `C2S`, and `UNKNOWN`.	v9
firewall rule id	The ID of the rule that matches the firewall session.	v9
ips config type	The type of the IPS configuration. Valid values are: `CONFIG`, `PROFILE`, and `UNKNOWN`.	v9
aws region	The AWS region where Secure Access stores your logs.	v9

Remote Access VPN Log Formats

Describes the content and purpose of remote access vpn log formats. The Cisco Secure Access remote access virtual private network (VPN) logs show the VPN session connection events, which are managed by the Secure Access VPN services. Some relevant fields to aid debugging and trouble-shooting VPN sessions include:

The Cisco Secure Access remote access virtual private network (VPN) logs show the VPN session connection events, which are managed by the Secure Access VPN services. Some relevant fields to aid debugging and trouble-shooting VPN sessions include:

- Display Username for Failed Events – Significantly improves how quickly issues can be tracked and addressed.
- ASA Syslog Message ID Extraction Support – Offers detailed insights by identifying the specific sys-log messages used in the remote access logs.
- Device ID – Includes the device ID with every event, providing critical help to network administrators in numerous ways.
- Failed Events for Posture – Provides vital information for effective triage during failed connection attempts.

For information about the size of a log file, see Estimate the Size of a Log on page 740.

Examples

This is an example v9 Secure Access VPN log of a **CONNECTED** event:

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version
"2024-09-11
```

```
2:40:51","hostname","user-1","CONNECTED","[295358]","7","sample-uuid","2368","35","us","","148","IKEv2","CiscoSecureAccessVPN","24.123.123.123","10.10.1.10","","","Mac
 OS X 14.6.1","5.1.2.42"
```

This is an example of v9 Secure Access VPN log of a **DISCONNECTED** event:

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version
"2024-09-11
2:28:52","hostname","user-1","DISCONNECTED","[295358]","7","sample-uuid","2368","35","us","","148","IKEv2","CiscoSecureAccessVPN","24.123.123.123","10.10.1.10","2024-09-11T19:54:02Z","User
 Requested","Mac OS X 14.6.1","5.0.05040"
```

This is an example of v9 Secure Access VPN log of a failed **AUTHORIZATION-CHECK** event:

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version
"2024-09-11
2:40:51","hostname","user-1","FAILED","[295358]","7","sample-uuid","2368","35","us","","148","IKEv2","CiscoSecureAccessVPN","24.123.123.123","10.10.1.10","","","Mac
 OS X 14.6.1","5.1.2.42"
```

This is an example of v9 Secure Access VPN log of a failed **CERT-AUTH-CHECK** event:

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version
"2024-09-11
2:40:51","hostname","user-1","FAILED","[295358]","7","sample-uuid","2368","35","us","","148","IKEv2","CiscoSecureAccessVPN","24.123.123.123","10.10.1.10","","","Mac
 OS X 14.6.1","5.1.2.42"
```

Order of Fields in the RAVPN Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

V9 Log Format

The CSV fields in the header row of the RAVPN logs.

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version
```

The description of each field and the log version in which each field was released, up to **Version 9**. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the RAVPN event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.'	v9
hostname	The name of the node on the Cisco headend side where user VPN connections are established and events are generated.	v9
aws region	The AWS region that stores your VPN logs.	v9
event type	The label that describes the type of event. Valid values are: `CONNECTED`, `DISCONNECTED`, `FAILED`, or `UNKNOWN`.	v9
origin ids	The internal IP address of the device that connected to the Secure Access remote VPN services.	v9
origin type	The type of device connected to the Secure Access VPN services.	v9
user id	The ID of the VPN user. The ID is the email address associated with the user account.	v9
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID on page 6 .	v9
retention days	The number of days that AWS S3 stores your Secure Access VPN log.	v9
storage location	The two-character label that identifies the location of your Cisco-managed VPN logs. Configure the storage location on Secure Access for your organization. The storage location options are: eu or us.	v9
msp organization id	The Secure Access managed organization ID.	v9
session id	The unique ID of the VPN session.	v9
session type	The protocol used by the device with the VPN session, for example: `TLS`.	v9

Field name	Description	Release version
vpn profile	The name of the VPN connection profile that establishes a VPN session.	v9
public ip	The public IP address of the device with the Cisco Secure Client and VPN module.	v9
assigned ip	The IP address assigned to the device with the Cisco Secure Client and VPN module.	v9
connected at	The date and time of the start of the initial `CONNECTED` VPN event for a `DISCONNECTED` event expressed in milliseconds as a UTC-formatted string.	v9
disconnection reason	The description of the VPN disconnected event. The value is `null` for other event types.	v9
os version	The type and version of the user device's operating system.	v9
anyconnect version	The version of the Cisco Secure Client with the VPN module.	v9

Web Log Formats

Describes the content and purpose of web log formats. The Cisco Secure Access Web logs show your organization's traffic through the Secure Access proxy.

The Cisco Secure Access Web logs show your organization's traffic through the Secure Access proxy. For information about the size of a log file, see Estimate the size of a log.

Example

This is an example of a v9 Web log event:

```
timestamp,policy identity label,internal client ip,external client
ip,destination ip,content type,action,url,referer,user agent,status code,request
 size,response size,response body size,sha—sha256,categories,av
detections,puas,amp disposition,AMP malware name,amp score,policy identity
type,blocked categories,identities,identity types,request method,dlp
status,certificate errors,file name,ruleset id,rule ID,destination list
ids,isolate action,file action,warn status,forwarding method,producer
"2025-01-06
13:39:24","SIG2-Denver","10.XXX","10.XXX","10.XXX","","ALLOWED","https://example.com/","","","200","157","641","","","Software/Technology,Allow
 List,Computers and Internet","","","","","","Network
Tunnels","","SIG2-EX,RTO-XXXX-SIG","Network Tunnels,Internal
Networks","CONNECT","","","","13368132","610352","9999583","not_isolated","","","",""
```

Order of Fields in the Web Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

```
n","File Action","Warn Status","Forwarding Method","Producer"
```

V9 Log Format

The CSV fields in the header row of the Web log.

```
timestamp,policy identity label,internal client ip,external client
ip,destination ip,content type,action,url,referer,user agent,status code,request
 size,response size,response body size,sha—sha256,categories,av
detections,puas,amp disposition,AMP malware name,amp score,policy identity
type,blocked categories,identities,identity types,request method,dlp
status,certificate errors,file name,ruleset id,rule ID,destination list
ids,isolate action,file action,warn status,forwarding method,producer
```

The description of each field and the log version in which each field was released, up to **Version 9**. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the Web traffic event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v1
policy identity label	The identity that made the request.	v1
internal client ip	The internal IP address of the computer making the request.	v1
external client ip	The egress IP address of the network where the request originated.	v1
destination ip	The destination IP address of the request.	v1
content type	The type of web content, typically `text/html`.	v1
action	Whether the request was allowed or blocked.	v1

Field name	Description	Release version
url	The URL requested.	v1
referer	The referring domain or URL.	v1
user agent	The browser agent that made the request.	v1
status code	The HTTP status code; should always be `200` or `201`.	v1
request size	Request size in bytes.	v1
response size	Response size in bytes.	v1
response body size	Response body size in bytes.	v1
sha–sha256	The hex digest of the response content.	v1
categories	The security categories for this request, such as `Malware`.	v1
av detections	The detection name according to the antivirus engine used in file inspection.	v1
puas	A list of all potentially unwanted application (PUA) results for the proxied file as returned by the antivirus scanner.	v1
amp disposition	The status of the files proxied and scanned by Cisco Advanced Malware Protection (AMP) as part of the File Inspection feature; can be `Clean`, `Malicious` or `Unknown`.	v1
amp malware name	If Malicious, the name of the malware according to AMP.	v1
amp score	The score of the malware from AMP. This field returns blank (`""`) unless the verdict is Unknown, in which the value will be `0`.	v1
policy identity type	The first identity type that made the request. Examples: `Roaming Computer`, `Network`.	v1
blocked categories	The category that resulted in the destination being blocked.	v4
identities	All identities associated with this request.	v5
identity types	The type of identities that were associated with the request. Examples: `Roaming Computer`, `Network`.	v5
request method	The HTTP request method. Examples: `GET`, `POST`, `HEAD`, `PUT`, `DELETE`.	v5
dlp status	If the request was Blocked for DLP.	v6
certificate errors	Any certificate or protocol errors in the request.	v6

Field name	Description	Release version
file name	The name of the file.	v6
ruleset id	The ID number assigned to the ruleset.	v6
rule id	The ID number assigned to the rule.	v6
destination list ids	The ID number assigned to a destination list.	v6
isolate action	The remote browser isolation state associated with the request.	v8
file action	The action taken on a file in a remote browser isolation session. Valid values are: `UNKNOWN`, `DETECT`, `BLOCK`, `MALWARE_CLOUD_LOOKUP`, `MALWARE_WHITELIST`, `CLOUD_LOOKUP_TIMEOUT`, `CUSTOM_DETECTION`, `CUSTOM_DETECTION_BLOCK`, `ARCHIVE_BLOCK_DEPTH_EXCEEDED`, `ARCHIVE_BLOCK_ENCRYPTED`, `ARCHIVE_BLOCK_FAILED_TO_INSPECT`, `TID_BLOCK`	v8
warn status	The Warn page's state associated with the request.	v8
forwarding method	The method used to forward the proxy events. Example: `Secure Web Appliance`.	v9
producer	The producer of the proxy events.	v9

Zero Trust Access Log Formats

Describes the content and purpose of zero trust access log formats. The Cisco Secure Access Zero Trust Access logs show your organization's traffic through the Secure Access Zero Trust Access services.

The Cisco Secure Access Zero Trust Access logs show your organization's traffic through the Secure Access Zero Trust Access services. ZTA logs include traffic events that take place at the time of ZTA session authentication for both client-based and browser-based ZTA sessions.

For information about the size of a log file, see Estimate the Size of a Log on page 740.

Example

This is an example of a v9 Zero Trust Access log event:

```
timestamp,identity email,identity labels,identity type
labels,hostname,verdict,client os,client browser,client geo location,client
ip,ruleset id,rule id,private app group id,private app id,private resource
id,private resource group id,step up auth type,step up auth result,step up
auth token life,posture id,requested id fqdn,resolved ip,app connector group
id,headend type,duo device id,duo device id string,system password,client
firewall,disk encryption,anti malware agents
"2017-10-02 23:52:53","network@example.com","Network. AD
Computer","Networks","ts-auto.com","ALLOW","Mac OS 10.9.5","Chrome
```

```
99,"aaa",1000,1,3,12,25,19,20,76,"ALS","SDS",60,26,"probe.cr",111,5,"A",,"2a4365a8e8e40","aaa[10]","S","THRAY","\cisco
 1.20.0.877, windows-defender 1.20.0.877\]",
```

Order of Fields in Zero Trust Access Logs

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

```
ssword","Client Firewall","Disk Encryption","Anti Malware Agents"
```

V9 Log Format

The CSV fields in the header row of the Zero Trust Access log.

```
timestamp,identity email,identity labels,identity type
labels,hostname,verdict,client os,client browser,client geo location,client
ip,ruleset id,rule id,private app group id,private app id,private resource
id,private resource group id,step up auth type,step up auth result,step up
auth token life,posture id,requested id fqdn,resolved ip,app connector group
id,headend type,duo device id,duo device id string,system password,client
firewall,disk encryption,anti malware agents
```

The description of each field and the log version in which each field was released, up to **Version 9**. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the ZTA event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v9
identity email	The email address of the Active Directory user.	v9
identity labels	The list of labels for the identity.	v9
identity type labels	The label of the identity type.	v9
hostname	The hostname of the user device.	v9
verdict	Whether the user has access to a resource.	v9
client os	The operating system of the user device.	v9

Field name	Description	Release version
client browser	The name of the browser on the user device.	v9
client geo location	The regional location of the user device.	v9
client ip	The IP address of the user device.	v9
ruleset id	The ID of the ruleset.	v9
rule id	The ID of the access rule.	v9
private app group id	The ID of the private application group.	v9
private app id	The ID of the private application.	v9
private resource id	The ID that Secure Access assigns to the customer-defined private application.	v9
private resource group id	The ID if the rule matched is based on the private application group.	v9
step up auth type	The type of authentication. Valid values are: `SAML_SSO`, `MFA`, or `NONE`.	v9
step up auth result	The result of the authentication. Valid values are: `SUCCESS` or `FAILURE`.	v9
step up auth token life	The time in seconds between when you generated the token and used the token.	v9
posture id	ID of the matching posture profile.	v9
requested id fqdn	The IP or FQDN of the requested application.	v9
resolved ip	The IP of the application returned by the proxy.	v9
app connector group id	The group ID of the App Connector.	v9
headend type	The type of the headend. Valid values are: `CLAP` or `BAP`.	v9
duo device id	The ID of the Duo App on the device.	v9
duo device id string	The ID label of the Duo App on the device.	v9
system password	Whether the system password is enabled with its timeout in seconds.	v9
client firewall	The client system firewall. Valid values are `SYS` or `NONE`.	v9
disk encryption	The client Disk Encryption Type. Valid values are: `SYS`, `NONE` or `THIRD PARTY`.	v9
anti malware agents	The clients' anti malware agents.	v9

48 Manage API Keys

Topics:

- Add Secure Access API Keys
- Add KeyAdmin API Keys

Introduces managing api keys. The Secure Access API keys and Key Admin API keys enable you to interact programmatically with your instance of the Secure Access platform.

The Secure Access API keys and Key Admin API keys enable you to interact programmatically with your instance of the Secure Access platform. You can create an API key and secret for each type of key and manage all of your organization's API keys in Secure Access.

- **API Key**–An intent-based Secure Access API key with a configurable key name, description, expiration date, and key access scopes. The API key description is optional.
- **KeyAdmin API key**–An API key that you can use in a program or script to create and manage your organization's Secure Access API keys. The KeyAdmin API key has a configurable key name, description, and expiration date, and key access scopes. The key access scopes are limited to the management of Secure Access API keys. The API key description is optional.

Your API key and API secret are credentials that enable you to authenticate to Secure Access and create short-lived API access tokens.

Note

API keys, passwords, secrets, and tokens allow access to your private data. You should never share your credentials with another user or organization.

Add Secure Access API Keys

Describes adding secure access api keys. The Secure Access API enables you to create, manage, and protect the users, user devices, network connections, and private resources in your organization.

The Secure Access API enables you to create, manage, and protect the users, user devices, network connections, and private resources in your organization. In a script or client program, use your Secure Access API key credentials to authenticate with Secure Access and generate a short-lived API access token. Then, with your generated access token, you can interact with the Secure Access platform. You must include your access token in an API request for every operation. For more information, see Secure Accesss API Authentication.

You can create any number of granular, multi-scoped Secure Access API keys. When you create an API key, choose a unique key name, description, key expiration date, and API key scopes and permissions. The API key description and expiration date are optional. If you do not set an expiration date when you add the key, Secure Access sets your API key to never expire. For each key scope and API resource, choose either **Read-Only** or **Read/Write** API key permissions.

Once you add an API key to Secure Access, you can refresh your key's credentials, update the key's name, description, expiration date, and key scopes, and delete the API key.

Add API Key

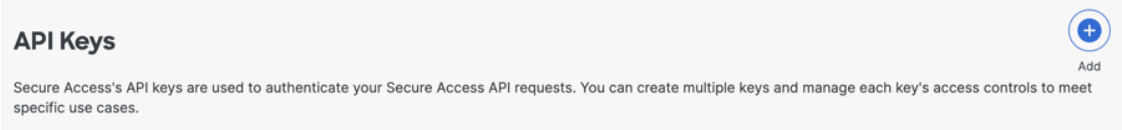
Provides instructions for adding api key. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin API Keys .

Before you begin

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

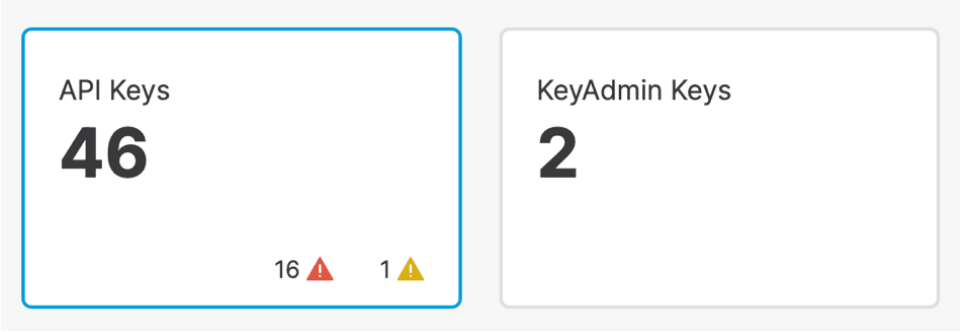
Procedure

1. Navigate to **Admin** > **API Keys**.

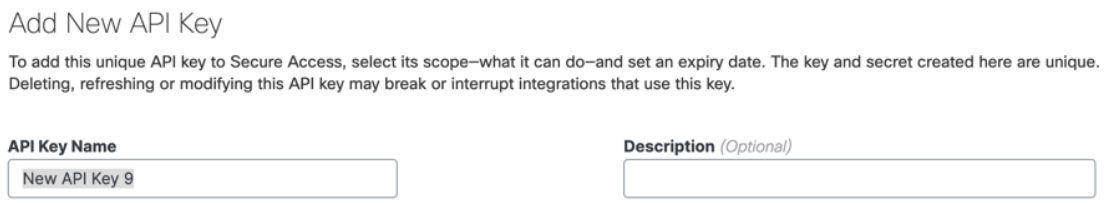


2. Click **API Keys** and then click **Add**.

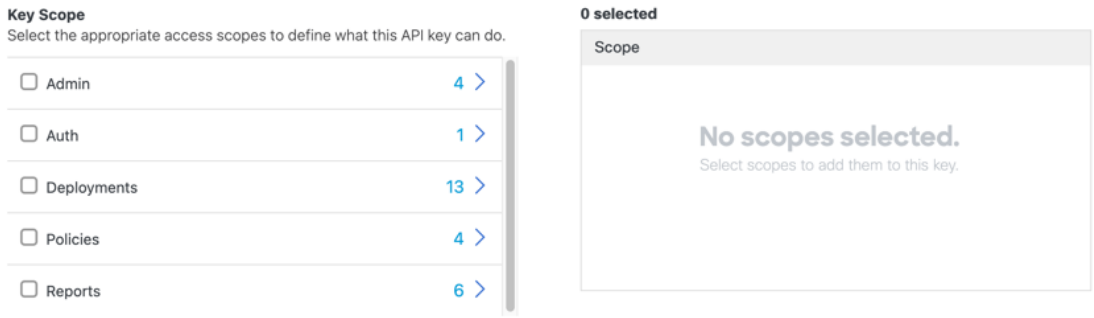
   The number of expired API keys appears next to the red triangle. The number of API keys that expire within 30 days appears next to the yellow triangle.



3. Enter a name and description for the key. A name must contain less than 256 characters. The key description is optional.



4. Select the key scopes and expand a key scope to view the resources. Check each resource in a key scope to enable access to the resource.

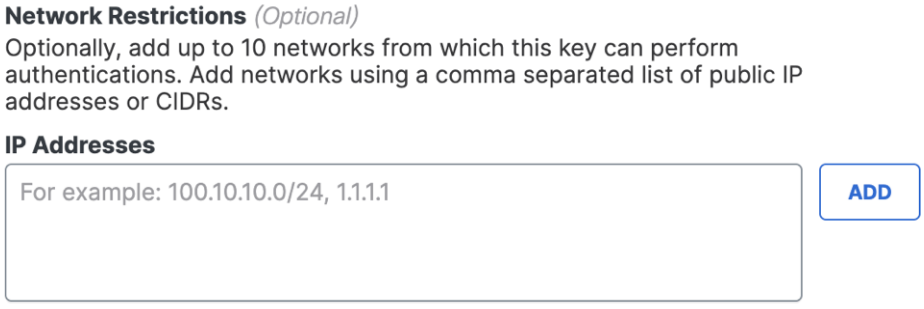


5. Choose **Read-Only** or **Read / Write** for the selected scope and resource.
6. For **Expiry Date**, choose an expiration date or choose **Never expire**.



7. (Optional) For **Network Restrictions**, enter a comma-separated list of public IP addresses or CIDRs, then click **Add**.

> **Note**
>
> You can add up to ten networks to your API key. You can only use your API key to authenticate requests for clients on the selected networks.



8. Click **Create Key**.
9. Copy and save your **API Key** and **Key Secret**.
10. Click **Accept and Close**.



Refresh API Key

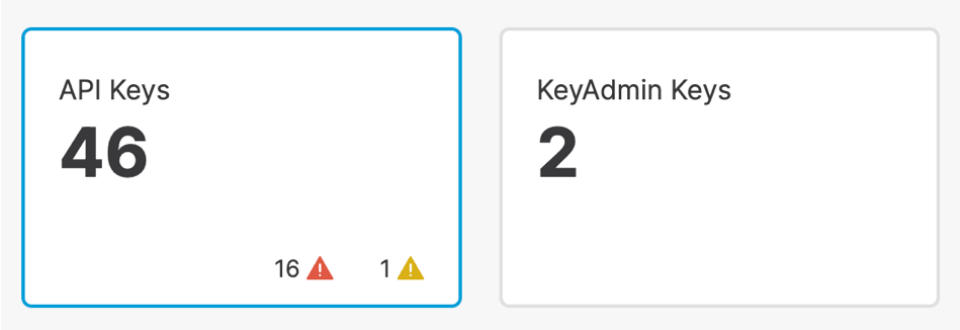
Provides instructions for refresh api key. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin API Keys .

Before you begin

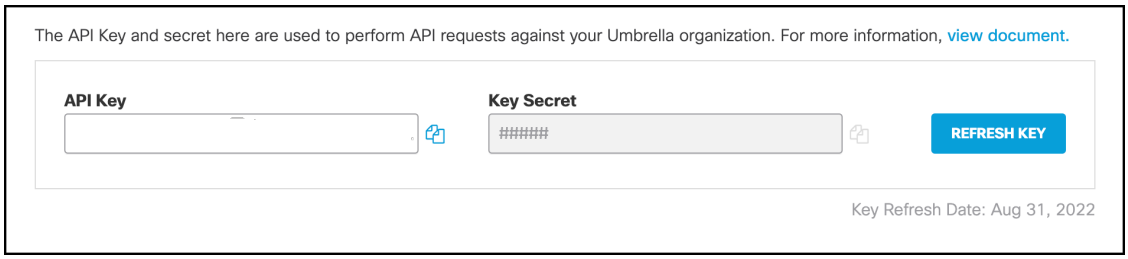
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **API Keys**.
2. Click **API Keys**, and then expand an API key.



3. Click **Refresh Key**.



4. Copy and save your **API Key** and **Key Secret**.
5. Click **Accept and Close**.



Update API Key

Provides instructions for updating api key. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

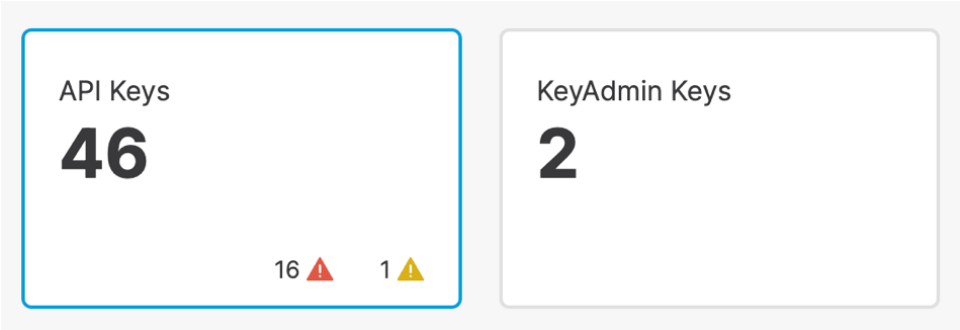
You can modify one or multiple settings on your API key.

Before you begin

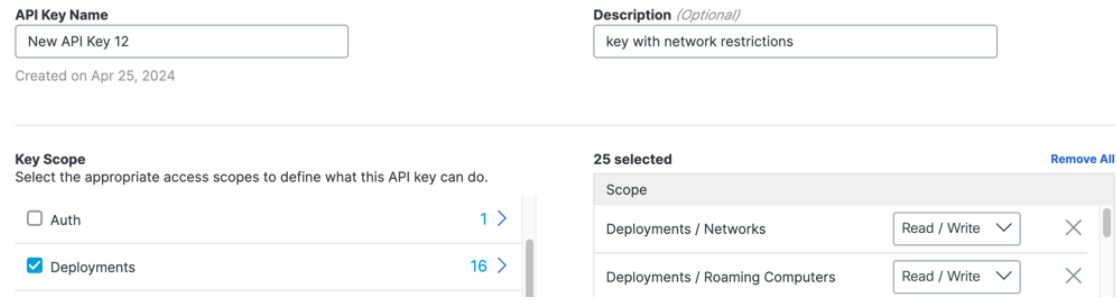
Full Admin user role. For more information, see Manage Accounts.

Procedure

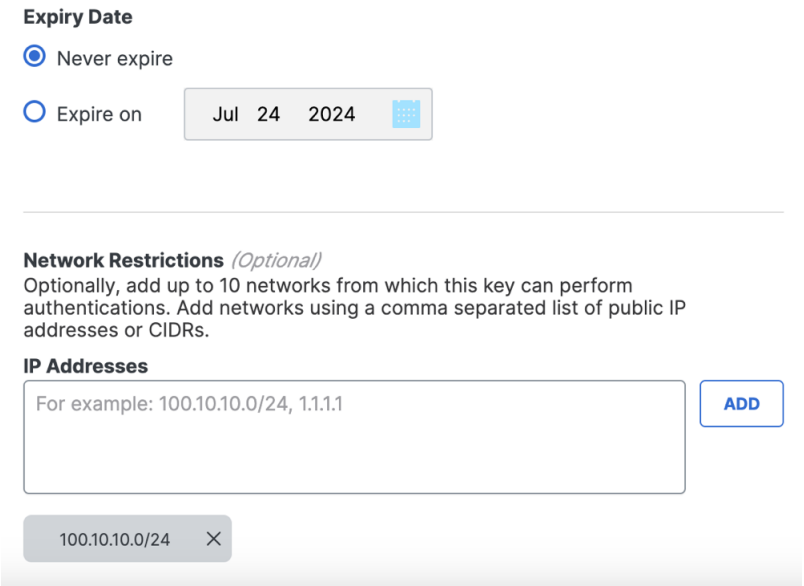
1. Navigate to **Admin** > **API Keys**.
2. Click **API Keys**, and then expand an API key.



3. Modify the **API Key Name**, **Description**, and selected scopes and permissions in **Key Scope**.



4. Modify the **Expiry Date**.
5. For **Network Restrictions**, update the list of IP addresses or CIDRs. Click on the **X** to remove a network address.



6. Click **Save**.

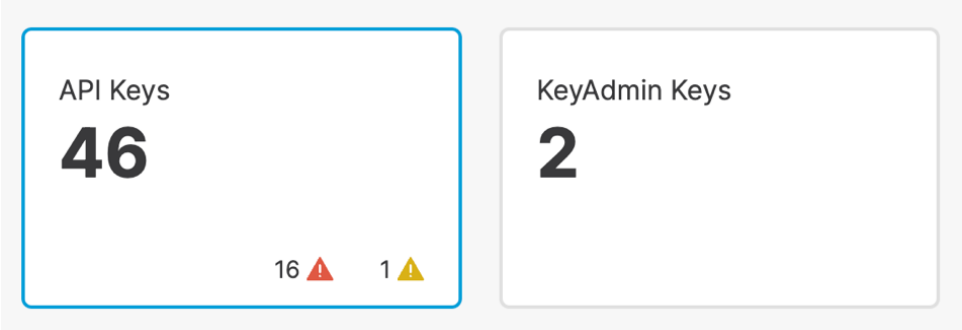
Delete API Key

Provides instructions for deleting api key. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin API Keys .

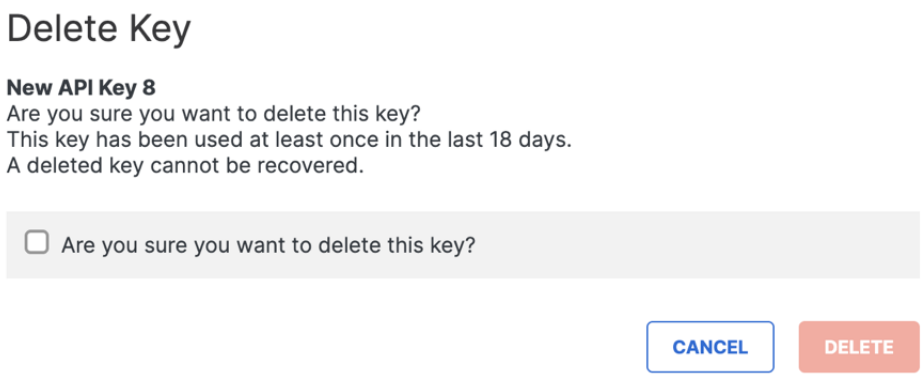
Before you begin
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **API Keys**.
2. Click **API Keys**, and then expand an API key.



3. Click **Delete**. In the dialog window, click **Delete** to remove the API key from your organization.



Add KeyAdmin API Keys

Describes adding keyadmin api keys. The Secure Access Key Admin API enables you to create and manage Secure Access API keys. In a script or client program, use your KeyAdmin API key credentials to authenticate with Secure Access and generate a short-lived API access token.

The Secure Access Key Admin API enables you to create and manage Secure Access API keys. In a script or client program, use your KeyAdmin API key credentials to authenticate with Secure Access and generate a short-lived API access token. Then, make API requests with your access token to the Key Admin API to create Secure Access API keys for your organization. You must include your access token in an API request for every operation. For more information, see Secure Access API Authentication.

You can create any number of Key Admin API keys for your organization. When you create a KeyAdmin API key, choose a unique key name, description, key expiration date, and the KeyAdmin API key scopes. The key description and expiration

date are optional. If you do not set an expiration date when you add the key, Secure Access sets your KeyAdmin API key to never expire.

Once you add a KeyAdmin API key to Secure Access, you can refresh your key's credentials, update the key's name, description, expiration date, and key scopes, and delete the API key.

Use Cases

Describes using cases. Programmatically create Secure Access API keys. Programmatically manage the Secure Access API keys in your organization–refresh API key credentials, update API key properties, or delete API keys.

- Programmatically create Secure Access API keys.
- Programmatically manage the Secure Access API keys in your organization–refresh API key credentials, update API key properties, or delete API keys.
- Write scripts or client programs that use KeyAdmin API keys to create and manage Secure Access API keys, and with your generated API keys, make requests to the Secure Access API. Integrate the client programs into your continuous integration or continuous delivery pipelines.

Add KeyAdmin API Key

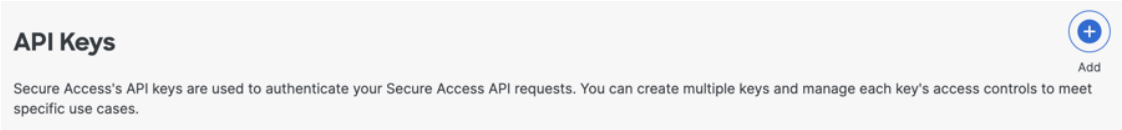
Provides instructions for adding keyadmin api key. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin API Keys .

Before you begin

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

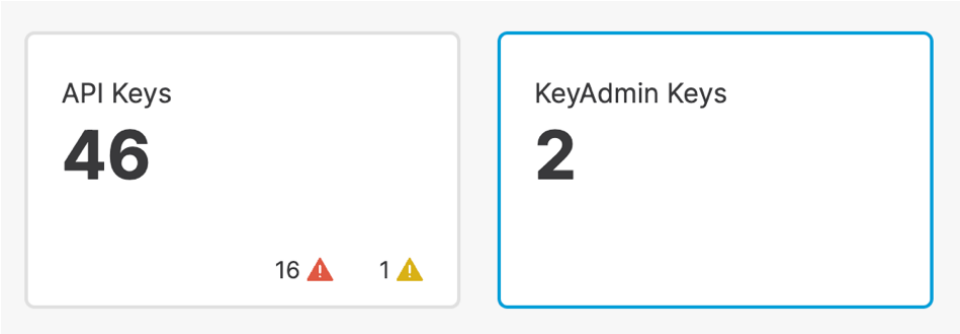
Procedure

1. Navigate to **Admin** > **API Keys**.



2. Click **KeyAdmin Keys** and then click **Add**.

   The number of expired API keys appears next to the red triangle. The number of API keys that expire within 30 days appears next to the yellow triangle.

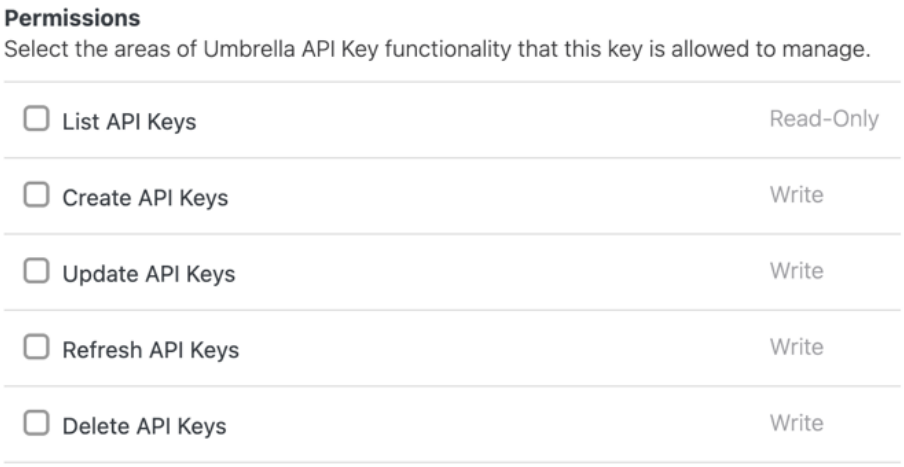


3. Enter a name and description for the key. A name must contain less than 256 characters.

   The key description is optional.



4. Select the permissions for the key.

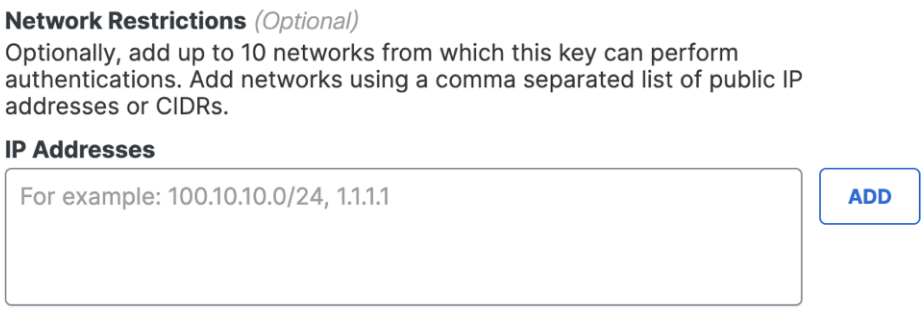


5. For **Expiry Date**, choose the expiration date for the key, or choose **Never expire**.



6. (Optional) For **Network Restrictions**, enter a comma-separated list of public IP addresses or CIDRs, then click **Add**.

> **Note**
>
> You can add up to ten networks to your API key. You can only use your API key to authenticate requests for clients on the selected networks.



7. Click **Create Key**.
8. Copy and save your **KeyAdmin Key** and **Key Secret**.
9. Click **Accept and Close**.



Refresh KeyAdmin API Key

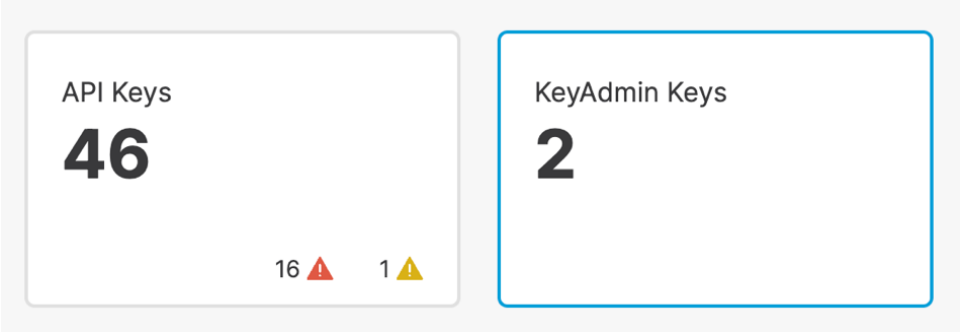
Provides instructions for refresh keyadmin api key. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin API Keys .

Before you begin

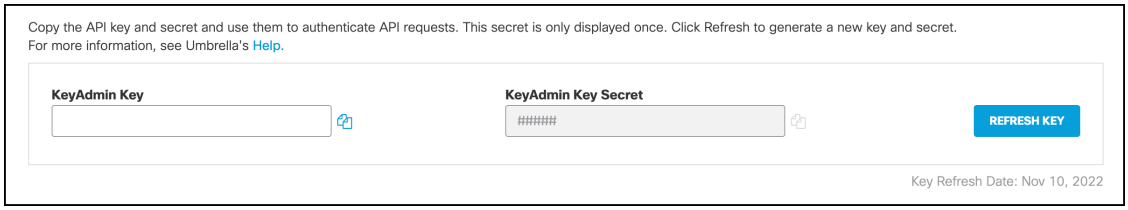
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **API Keys**.
2. Click **KeyAdmin Keys**, and then expand an API key.



3. Click **Refresh Key**.



4. Copy and save your **KeyAdmin Key** and **Key Secret**.
5. Click **Accept and Close**.



Update KeyAdmin API Key

Provides instructions for updating keyadmin api key. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

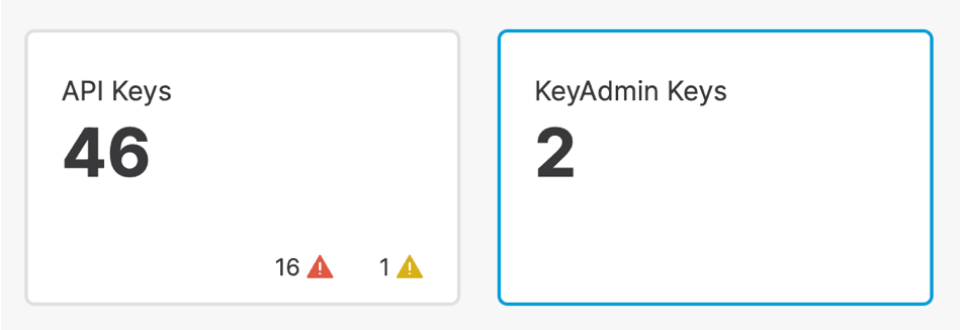
You can modify one or multiple settings on your API key.

Before you begin

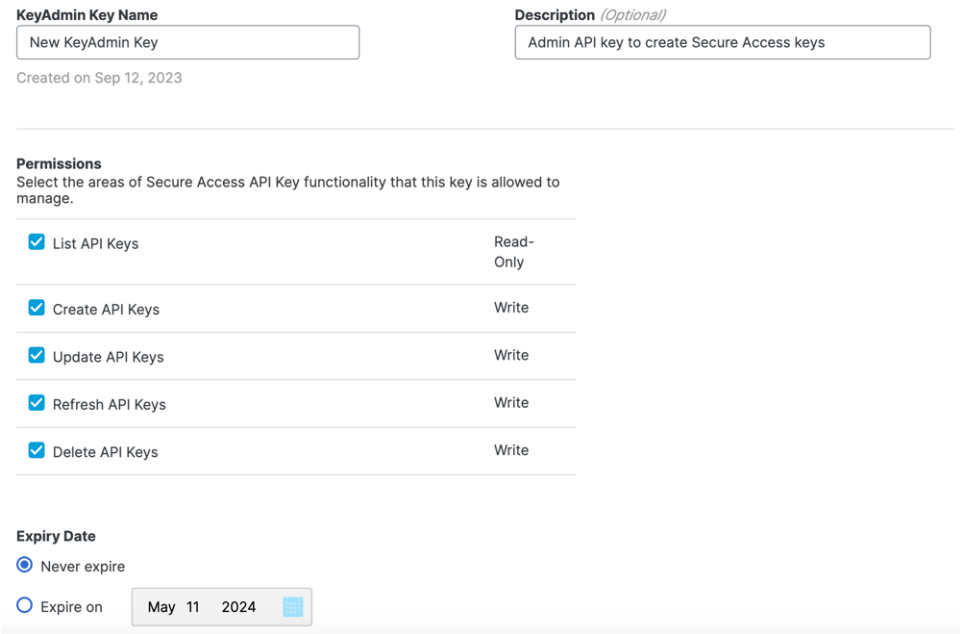
Full Admin user role. For more information, see Manage Accounts.

Procedure

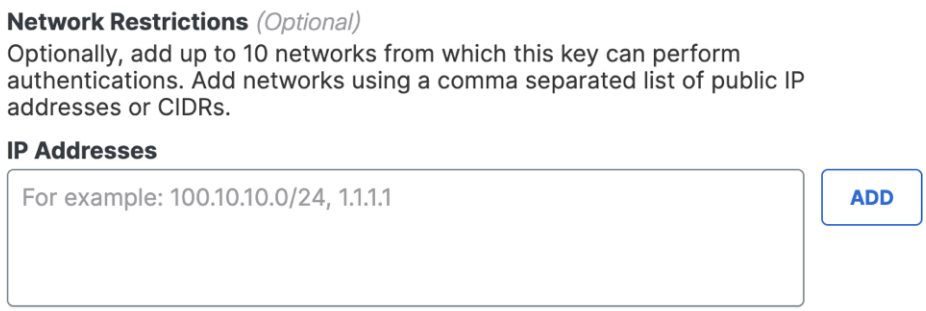
1. Navigate to **Admin** > **API Keys**.
2. Click **KeyAdmin Keys**, and then expand an API key.



3. Modify the **KeyAdmin Key Name**, **Description**, **Permissions**, and **Expiry Date**.



4. For **Network Restrictions**, update the list of IP addresses or CIDRs. Click on the **X** to remove a network address.



5. Click **Save**.

Delete KeyAdmin API Key

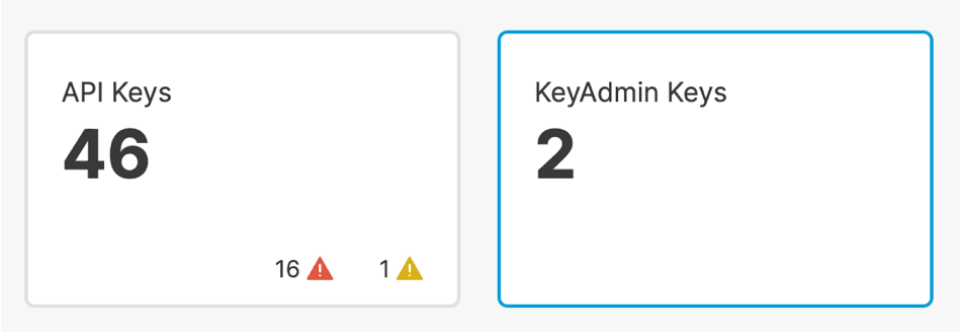
Provides instructions for deleting keyadmin api key. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin API Keys .

Before you begin

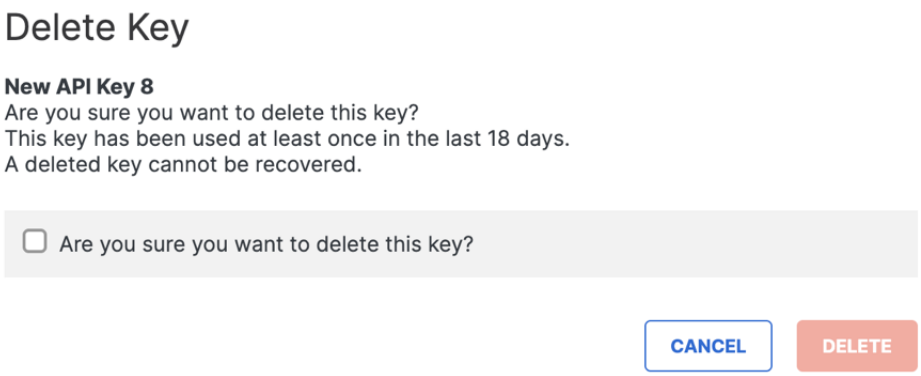
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **API Keys**.
2. Click **KeyAdmin Keys**, and then expand an API key.



3. Click **Delete**. In the dialog window, click **Delete** to remove the API key from your organization.



49 Manage Accounts

Topics:

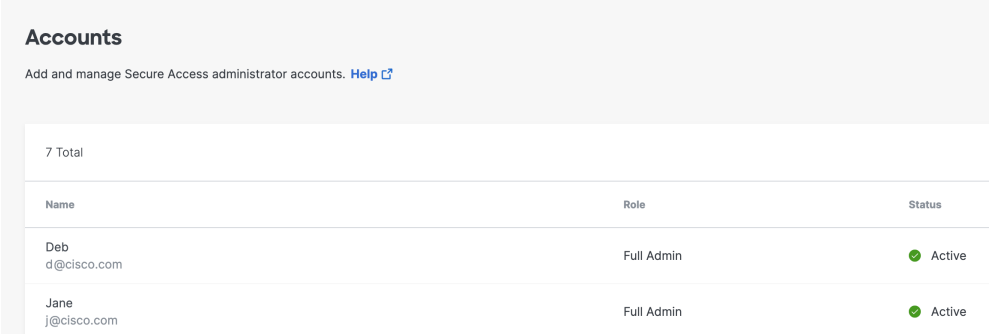
- Add a New Account
- Edit Account Settings
- Delete an Account
- Hide Sources with De-identification

Introduces managing accounts. You can share access to Cisco Secure Access with other people in your organization by inviting them to create an account.

You can share access to Cisco Secure Access with other people in your organization by inviting them to create an account.

You can manage accounts by navigating to **Admin** > **Accounts** . At a glance, you can see all of the accounts that have access to Secure Access. This includes their name, assigned role, whether they have two-factor authentication enabled, and their account status.

When you create an account for another administrator, you assign a role that defines what type of access they have to Secure Access. You can allow multiple users to view Secure Access while restricting the ability to make changes to a select few administrators.



Add a New Account

Describes adding a new account. You can add users to your instance of Cisco Secure Access by adding a new account. Each account is assigned a role that sets that account's permissions to view, write, change, and delete Secure Access configurations.

You can add users to your instance of Cisco Secure Access by adding a new account. Each account is assigned a role that sets that account's permissions to view, write, change, and delete Secure Access configurations.

Procedure

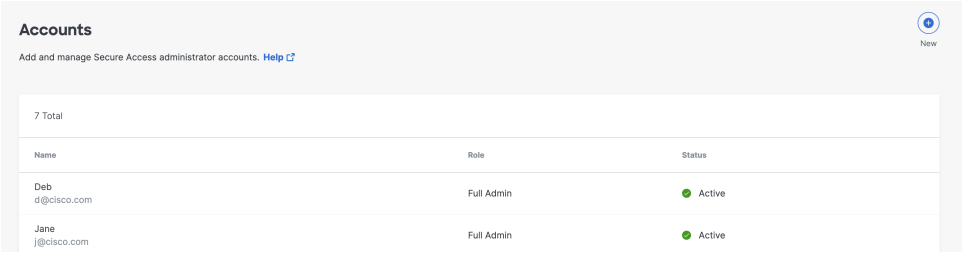
Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin Accounts and click New.

Before you begin

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

Procedure

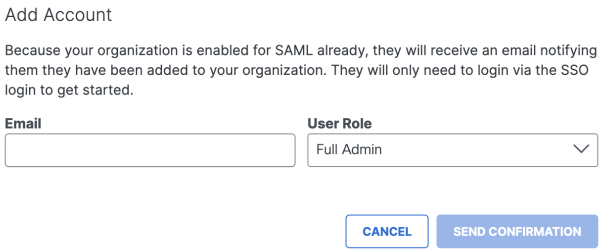
1. Navigate to **Admin** > **Accounts** and click **New**.



2. Enter the user's email address, choose a **User Role**, and then click **Send Confirmation**.

   User roles are:

   - **Full Admin**–Grants full access to Secure Access. This includes the ability to add users and assign roles.
   - **Read-Only**–Grants limited access to Secure Access. A Read-Only administrator can only view pages and reports. Functionality, including buttons, may not be displayed or available.
   - **Security Administrator**–Grants the same access as the **Full Admin** role, but does not have access to Data Loss Prevention (DLP) classifications, DLP policies, or the DLP Report.



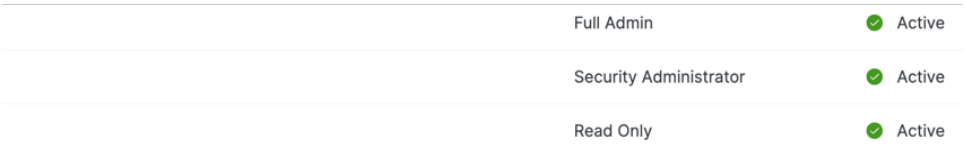
3. A message is sent to the new user's email address with instructions for setting a password.

> **Note**
>
> When the new user clicks **Confirm Invite**, Secure Access redirects them to the Secure Access login page.

What to do next

After a user creates a password and signs in, the user has access to your instance of Secure Access. The user's role controls their level of access.

Once the account is added, its status is **Active** and you can edit the account. For more information, see Edit Account Settings.



Edit Account Settings

Describes editing account settings. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

With administrator rights, you can change an account's settings at any time.

Procedure

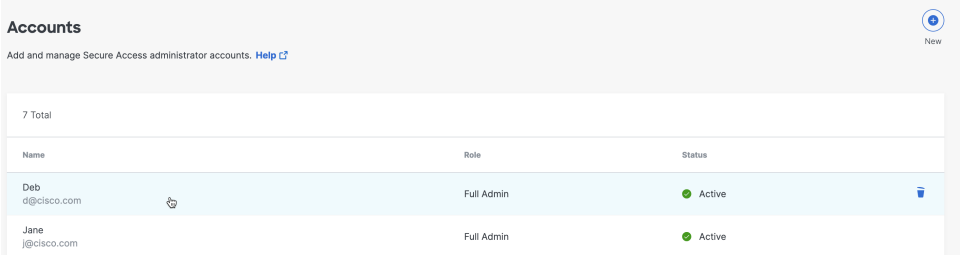
Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin Accounts and click a listed account entry.

Before you begin

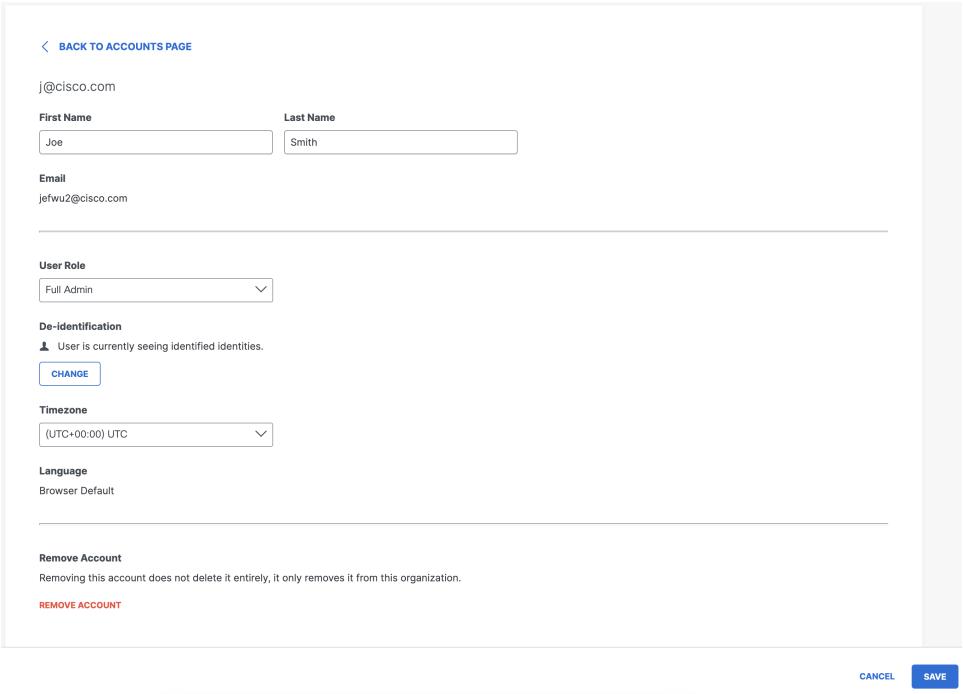
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Accounts** and click a listed account entry.



2. Update account settings as needed.



What to do next

The following account settings can be changed:

- **First Name** and **Last Name**
- **User Role**–The user role of the account. Only accounts with the user role of Full Admins can change user roles.
- **Timezone**–The timezone used in activity and reporting data shown within the dashboard. The timezone selection is unique to each account.
- **Remove Account**–Delete the account from Secure Access.

Delete an Account

Describes deleting an account. After adding a user to your instance of Secure Access, you can delete their account at any time. For information on how to add an account, see Add a New Account.

After adding a user to your instance of Secure Access, you can delete their account at any time. For information on how to add an account, see Add a New Account.

Procedure

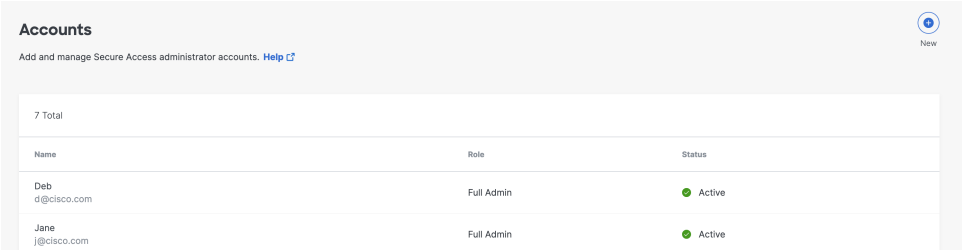
Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin Accounts . Hover over the account that you want to delete and then click the delete icon next to the account.

Before you begin

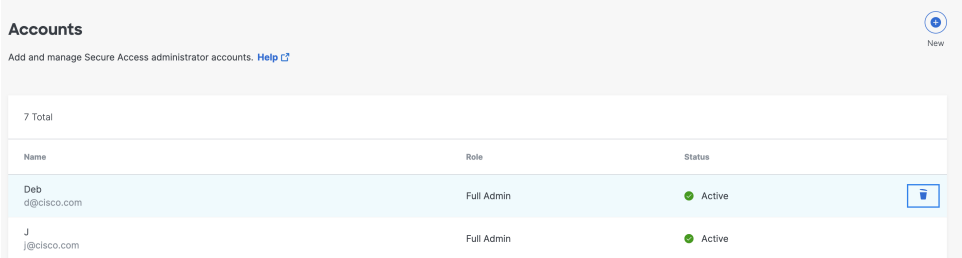
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Accounts**.



2. Hover over the account that you want to delete and then click the delete icon next to the account.



Hide Sources with De-identification

Describes hide sources with de-identification. Some regions or organizations require restrictions to hide the sources of users making internet requests. To comply with these restrictions, you can hide source names when generating a report by enabling de-identification for a user.

Some regions or organizations require restrictions to hide the sources of users making internet requests. To comply with these restrictions, you can hide source names when generating a report by enabling de-identification for a user. When enabled, a hash unique to that source replaces the source (identity) name.

Identity	Internal IP
fd90b6d53d205d60051946cca54995b6354a7a67	
465dae55fdc826ae81b8a3c1cb4d4bc7a80dc9d7	
b2d1f9c5524d5ad9c7125d9e1a1071d8e7fee6b2	3ac1e140a26b912baab0bc2fe5190d2de0229cc5
c76acef928dbf1c74b8705ac95ff899c4dae04a0	eea0b58f1ceec612d3f6e2b3973a0e48cd3f44e6
c76acef928dbf1c74b8705ac95ff899c4dae04a0	eea0b58f1ceec612d3f6e2b3973a0e48cd3f44e6
465dae55fdc826ae81b8a3c1cb4d4bc7a80dc9d7	

> **Note**
>
> You cannot enable or disable de-identification on your own account. At least two administrators are required to use this feature and any administrator can turn it on or off for another account.

Source Types

Describes source types. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

The following source types are de-identified:

- AD usernames
- computer/hostnames
- internal IP addresses
- Chromebook identities
- mobile identities
- GSuite users and groups
- SAML-obtained users and groups
- internal IP addresses

Enable De-identification

Provides instructions for enabling de-identification. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin Accounts and click an account name.

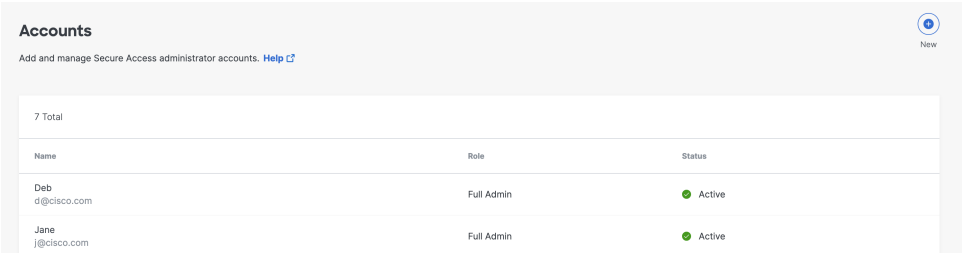
Before you begin

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

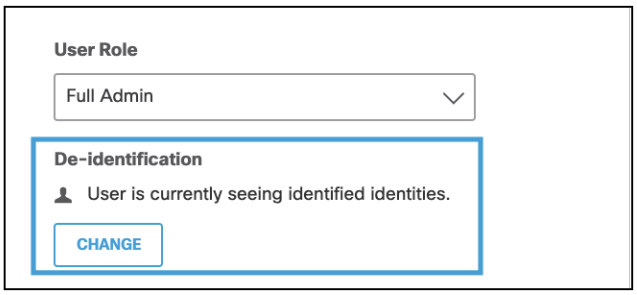
Procedure

1. Navigate to **Admin** > **Accounts** and click an account name.

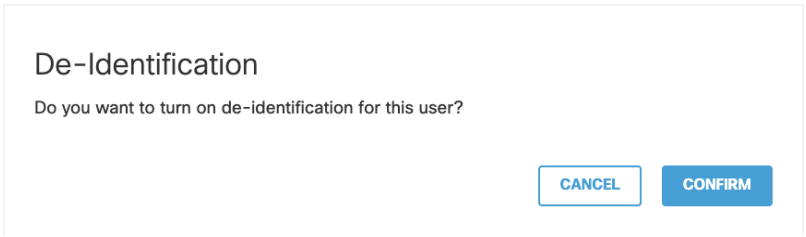
> **Note**
>
> You cannot enable de-identification for your own account.



2. Under **De-identification** click **Change**.



3. Click **Confirm**.



What to do next

De-identification is enabled and source (identity) names are replaced with a hash.

Disable De-identification

Provides instructions for disabling de-identification. Full Admin user role. For more information, see Manage Accounts. Navigate to Admin Accounts and click an account name.

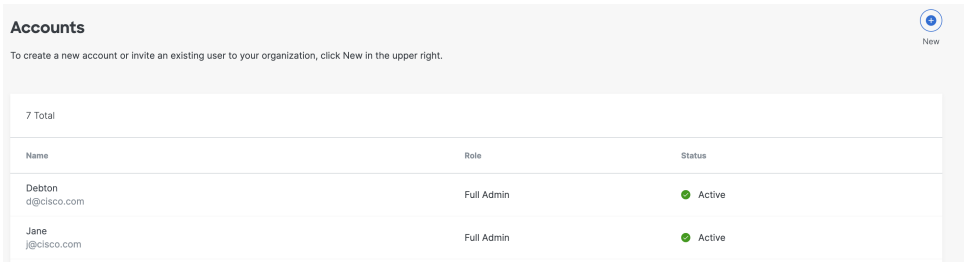
Before you begin

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

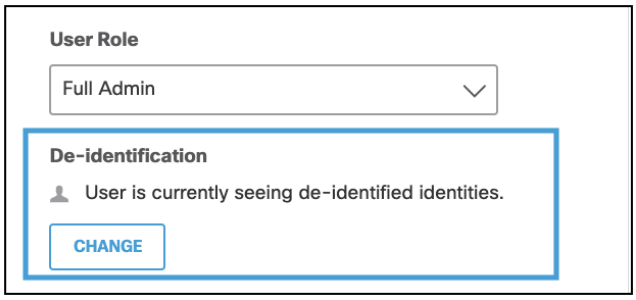
Procedure

1. Navigate to **Admin** > **Accounts** and click an account name.

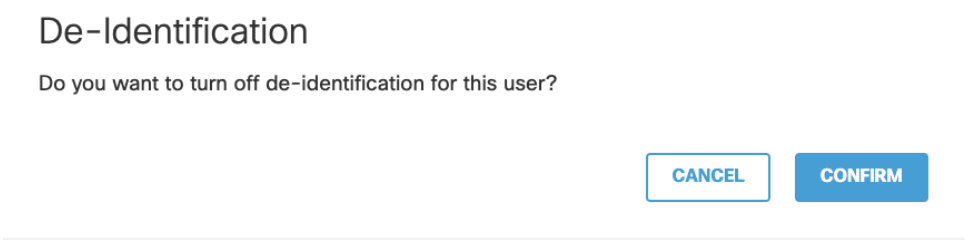
> **Note**
>
> You cannot enable de-identification for your own account.



2. Under **De-identification** click **Change**.



3. Click **Confirm**.



What to do next

De-identification is disabled and the account can view identity names.

Limitations

Describes limitations. Because the purpose of de-identification is to remove the visibility of the identity names for the user, de-identification includes the following limitations:

Because the purpose of de-identification is to remove the visibility of the identity names for the user, de-identification includes the following limitations:

- The scheduling and exporting of reports is unavailable.
- The Application Discovery report is unavailable.
- You cannot search by an active directory username, roaming computer name, or internal IP name.

  However, you can click the hash name to view the source's (identity) details.
- There is no access to API key management and creation.
- There is no access to S3 Log Management (self-managed or Cisco-managed).
- Full administrators with De-identification enabled will see encoded information in all reports except for the Data Loss Prevention Report.

50 Manage Domains

Topics:

- Add Internal Domains

Describes managing domains. Cisco Secure Access provides domain management—the list of domains and IP addresses where the traffic to these resources bypass the Secure Access DNS resolvers.

Cisco Secure Access provides domain management—the list of domains and IP addresses where the traffic to these resources bypass the Secure Access DNS resolvers.

You can add destinations to your domains list to route them to your local resolver. DNS queries for destinations found in the domains list bypass the Secure Access DNS resolvers and instead query the local network's DNS servers.

Add Internal Domains

Describes adding internal domains. You can add destinations to your domains list to route them to your local resolver. DNS queries for destinations found in the domains list bypass the Secure Access DNS resolvers and instead query the local network's DNS servers.

You can add destinations to your domains list to route them to your local resolver. DNS queries for destinations found in the domains list bypass the Secure Access DNS resolvers and instead query the local network's DNS servers.

Secure Access populates the domains list with any domains used by your organization to access local resources while on the organization's network (at the physical location or connected through VPN). Internal Domains is pre-populated with the **.local TLD** and all **RFC-1918 (private network)** reverse DNS address space.

> **Note**
>
> A Secure Access domains list cannot exceed 5000 entries.

Procedure

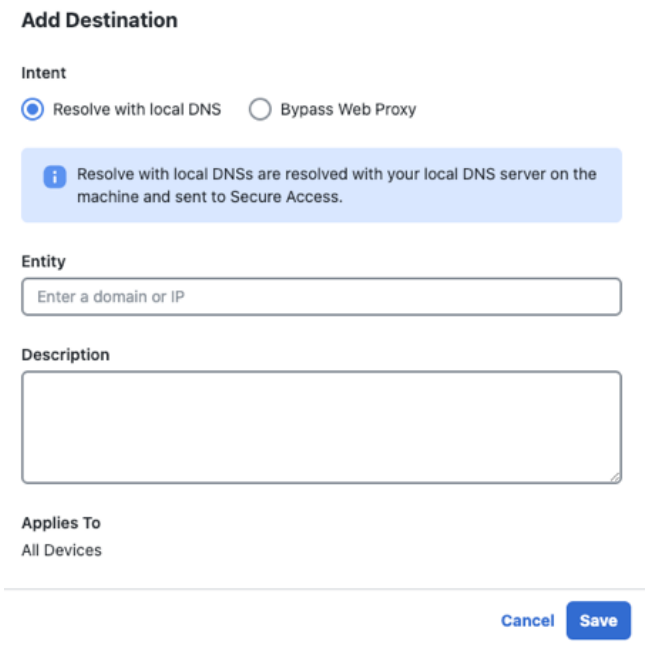
Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. Navigate to End User Connectivity Internet Security .

Before you begin

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

Procedure

1. Navigate to **End User Connectivity** > **Internet Security**.
2. For **Internet Security bypass**, click **Add Destination**.
3. Check **Resolve with local DNS** or **Bypass Web Proxy**.



4. For **Entity**, enter a domain or IP address.
5. For **Description**, enter a meaningful description of the destination.
6. Click the **Applies To** drop-down list to add sites and devices for this domain. By default, all sites and all devices are selected, but individual sites and devices can be selected but can be deselected. In addition to sites and devices, internal domains apply to the AnyConnect Roaming Security module and the PAC file. "Devices" refers specifically to roaming clients and mobile devices; other types of devices may have other means of rerouting DNS traffic, such as exclusion lists.



7. Click **Save** to add the domain to the domains list.

51 Manage Resources

Topics:

- Manage Resources

Describes the purpose and procedures for manage resources and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage Resources

Describes managing resources. Items under the Resources menu are reusable components (sometimes known as "objects") that can be used as sources or destinations when configuring access rules.

Items under the Resources menu are reusable components (sometimes known as "objects") that can be used as sources or destinations when configuring access rules.

Resource menu items that can be used as sources in access rules:

Describes resource menu items that can be used as sources in access rules:. It also identifies related requirements, procedures, and operational considerations.

- Registered Networks
- Internal Networks
- Roaming Devices

Resource menu items that can be used as destinations in internet access rules:

Describes resource menu items that can be used as destinations in internet access rules:. Internet and SaaS resources include: Destination Lists

Internet and SaaS resources include:

- Destination Lists
- Application Lists
- Content Category Lists
- Tenant Control Profiles

Resource menu items that can be used as destinations in private access rules:

Describes resource menu items that can be used as destinations in private access rules:. It also identifies related requirements, procedures, and operational considerations.

- Private Resources

Additional resources

Describes additional resources. Not all source and destination components are configured under the Resources menu. For example, Users and Groups can also be used as sources but are configured elsewhere.

Not all source and destination components are configured under the Resources menu. For example, Users and Groups can also be used as sources but are configured elsewhere.

52 Manage DNS Servers

Topics:

- Manage DNS Servers

Describes the purpose and procedures for manage dns servers and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Manage DNS Servers

Describes managing dns servers. Cisco Secure Access protects the DNS traffic in your organization. Add DNS servers to resolve DNS requests to internet resources.

Cisco Secure Access protects the DNS traffic in your organization. Add DNS servers to resolve DNS requests to internet resources.

Procedure

Provides instructions for procedure. Add an IP address or address range for a DNS server. Your DNS traffic routes through the DNS servers managed by Secure Access.

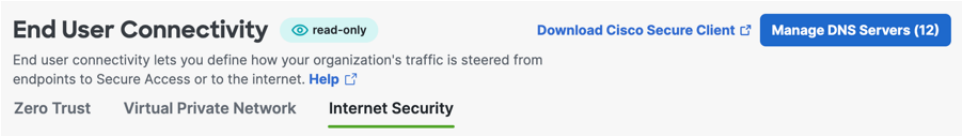
Add an IP address or address range for a DNS server. Your DNS traffic routes through the DNS servers managed by Secure Access.

Before you begin

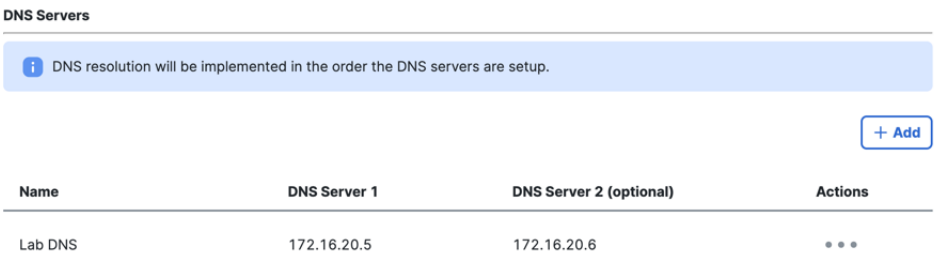
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Remote User Connectivity** and click **Manage DNS Servers**.



2. Click **Add**.
3. Enter a label for DNS server in **Name** and for **DNS Server 1** provide the IP address of the primary DNS server. If you have a secondary DNS server, add an IP address for **DNS Server 2**.
4. Click **Save** and then click **Close**.



Part II

DNS Forwarders

Topics:

- Get Started with Virtual Appliances
- Manage VAs in Secure Access
- Deploy Virtual Appliances
- Configure Virtual Appliances
- Local DNS Forwarding
- Test Virtual Appliance Deployments
- SNMP Monitoring for Virtual Appliances
- Troubleshoot Virtual Appliances
- PIV-CAC Support

53 Get Started with Virtual Appliances

Topics:

- Get Started with Virtual Appliances

Describes the purpose and procedures for get started with virtual appliances and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Get Started with Virtual Appliances

Describes get started with virtual appliances. Cisco Secure Access Virtual Appliances (VAs) are lightweight virtual machines. Virtual Appliances function as conditional DNS forwarders on your network. VAs record the internal IP address information of DNS requests for usage in reports, security enforcement, and category filtering.

Cisco Secure Access Virtual Appliances (VAs) are lightweight virtual machines. Virtual Appliances function as conditional DNS forwarders on your network. VAs record the internal IP address information of DNS requests for usage in reports, security enforcement, and category filtering. VAs encrypt and authenticate DNS data for enhanced security.

Supported Deployments

You can deploy Secure Access VAs with these hypervisors and cloud environments:

- VMWare ESX/ESXi
- Windows Hyper-V

For more information, see Deploy Virtual Appliances.

How Secure Access Virtual Appliances Work

Describes how secure access virtual appliances work. Virtual Appliances act as conditional DNS forwarders in your network. VAs intelligently forward public DNS queries to the Cisco Secure Access global network and local DNS queries to your existing local DNS servers and forwarders.

Virtual Appliances act as conditional DNS forwarders in your network. VAs intelligently forward public DNS queries to the Cisco Secure Access global network and local DNS queries to your existing local DNS servers and forwarders. Every public DNS query sent to Secure Access is encrypted, authenticated, and includes the client's internal IP address.

VAs do not cache DNS records. Caching occurs on the Secure Access DNS resolvers. When a VA responds with records to an endpoint's DNS query, any Time-to-Live (TTL) values in the response are equal to the TTLs as set by the authoritative DNS nameserver minus any time a record set has been in the Secure Access resolver cache.

Virtual Appliances and Granular Identity Information

Describes virtual appliances and granular identity information. If you already forward DNS requests to Secure Access, all the DNS traffic visible in your Secure Access reports come from Registered Networks.

If you already forward DNS requests to Secure Access, all the DNS traffic visible in your Secure Access reports come from Registered Networks. The VAs provide internal IP visibility, allowing you to track down malicious or inappropriate traffic within your network to a specific IP address.

Without Virtual Appliances

You can not research security and DNS traffic for an individual computer or IP address.

app.yesware.com	Allowed		Office NAT 1	67.215.[redacted]	N/A
app.yesware.com	Allowed		Office NAT 1	67.215.[redacted]	N/A

With Virtual Appliances

Virtual Appliances record the internal IP address of every DNS request. You can associate DNS traffic to a specific internal IP address.

search.cpan.org	Allowed	Software/Technology	Vancouver	67.215.	10.10.10.183
.cisco.com	Allowed	Software/Technology,...	forwarder04....	67.215.	10.111.0.208
data.flurry.com	Allowed	Software/Technology	Townsend	67.215.	10.112.0.62
ads.flurry.com	Allowed	Software/Technology,...	Townsend	67.215.	10.112.0.62

Active Directory Integration

Describes active directory integration. You can enable the integration of Active Directory (AD) with Secure Access VAs. AD provides user, group, or computer identity information in both reports and access rules. For more information, see the AD Integration with Virtual Appliances.

You can enable the integration of Active Directory (AD) with Secure Access VAs. AD provides user, group, or computer identity information in both reports and access rules. For more information, see the AD Integration with Virtual Appliances.

Configure Granular Rules

Describes configuring granular rules. Set various access rules in your policy for example, bring your own device (BYOD) corporate networks, guest Wi-Fi, server-only networks, by specifying the internal IP or IP range. Granular rules make it easy to filter unwanted content and malicious traffic on a per-network basis.

Set various access rules in your policy for example, bring your own device (BYOD) corporate networks, guest Wi-Fi, server-only networks, by specifying the internal IP or IP range. Granular rules make it easy to filter unwanted content and malicious traffic on a per-network basis.

Prerequisites for Virtual Appliances

Describes prerequisites for virtual appliances. The Cisco Secure Access Virtual Appliance is a lightweight virtual machine that acts as a non-caching, conditional DNS forwarder. Before you deploy the Secure Access Virtual Appliances in your environments, we recommend that you review the requirements and prerequisites.

The Cisco Secure Access Virtual Appliance is a lightweight virtual machine that acts as a non-caching, conditional DNS forwarder. Before you deploy the Secure Access Virtual Appliances in your environments, we recommend that you review the requirements and prerequisites.

Note: Secure Access Virtual Appliance images are configured with Ubuntu v22.04.

Endpoint Software

Describes endpoint software. You are not required to install client-side software for Virtual Appliance deployments. You do not have to reconfigure image operating systems.

- You are not required to install client-side software for Virtual Appliance deployments.
- You do not have to reconfigure image operating systems.

Virtual Appliance Requirements

Describes virtual appliance requirements. For information about license and package requirements, see Determine Your Current Package. At a minimum, to process millions of DNS queries per day, allocate these resources for each VA: Two virtual CPU cores 2GB RAM 7GB of disk space

- For information about license and package requirements, see Determine Your Current Package.
- **At a minimum, to process millions of DNS queries per day, allocate these resources for each VA:**
  - Two virtual CPU cores

    - 2GB RAM
    - 7GB of disk space

- Deploy two Virtual Appliances in a Site. VAs must be deployed in pairs to ensure redundancy at the DNS level and to allow for updates without downtime.
- Download a fresh image from Secure Access for each deployment.
- Ensure your hypervisor host has the correct date and time. The incorrect date or time can cause update or sync issues with the VAs. The VA syncs time independently and is always set to UTC by default. For more information, see, Network Time Protocol Servers.
- Each VA can process millions of DNS requests in a single day. If your network could exceed this number, see Virtual Appliance Sizing Guide.

Microsoft Hyper-V Requirements

Your Microsoft Hyper-V appliance must have one of the following Windows Server operating systems:

- Windows Server 2012, SP1, or R2 (Standard or Data center), 2016 or 2019 with Hyper-V role
- Hyper-V Server 2012, 2012 R2, 2016 or 2019

> **Note**
>
> Deploying the virtual appliance through System Center Virtual Machine Manager (SCVMM) has not been qualified and is not officially supported.

Networking Requirements

Describes networking requirements. Once VAs are deployed, endpoint clients must exclusively resolve DNS through the VAs and not your local DNS forwarders. This is usually accomplished through the network's DHCP configuration. For more information, see Local DNS Forwarding.

Once VAs are deployed, endpoint clients must exclusively resolve DNS through the VAs and not your local DNS forwarders. This is usually accomplished through the network's DHCP configuration. For more information, see Local DNS Forwarding.

Allow Connections to Various Domains and Services

Describes allow connections to various domains and services. You must allow connections to certain domains and URLs for the Virtual Appliances to communicate with the Secure Access cloud services and local DNS servers. These requirements apply to each platform where the VA is deployed.

You must allow connections to certain domains and URLs for the Virtual Appliances to communicate with the Secure Access cloud services and local DNS servers. These requirements apply to each platform where the VA is deployed.

- For DNS traffic to Secure Access, see Secure Access DNS Resolvers.
    - Standard and encrypted DNS queries to the Secure Access DNS resolvers.
        - Port 443 is used as failover if your firewall does not allow DNSCrypt on port 53.
        - Port 5353 is used as failover if DNSCrypt is not allowed on port 53 and port 443.
- For DNS traffic on internal domains, allow connections on the Virtual Appliance to local DNS servers on UDP and TCP port 53.
- For more information, see Secure Access DNS and Web – Client Certificate Revocation Services.

- For more information, see Secure Access DNS and Web – Client Configuration Services.
- For more information, see Secure Access Cisco Secure Client and External DNS Resolution.

Network Time Protocol Servers

Describes network time protocol servers. Allow connections from your Virtual Appliances to NTP servers on UDP port 123. 185.125.190.57 /32 (IPv4)

Allow connections from your Virtual Appliances to NTP servers on UDP port 123.

- **ntp.ubuntu.com**
  - 185.125.190.57 /32 (IPv4)
  - 185.125.190.56/32 (IPv4)
  - 91.189.91.157/32 (IPv4)
  - 185.125.190.58/32 (IPv4)
  - 2620:2d:4000:1::41 (IPv6)
  - 2620:2d:4000:1::40 (IPv6)
  - 2620:2d:4000:1::3f (IPv6)

> **Note**
>
> If you have configured custom NTP servers on the VA, use the custom NTP server IPs instead.

Intrusion Protection Systems (IPS) and Deep Packet Inspection (DPI)

Describes intrusion protection systems (ips) and deep packet inspection (dpi). If you have deployed an IPS or DPI, ensure that traffic on port 53 TCP/UDP to and from the VAs is excluded from packet inspection. The Secure Access DNS encryption methods might be flagged and dropped.

If you have deployed an IPS or DPI, ensure that traffic on port **53 TCP/UDP** to and from the VAs is excluded from packet inspection. The Secure Access DNS encryption methods might be flagged and dropped. If the VAs can not successfully send and receive encrypted DNS packets, Secure Access displays a warning.

Network Address Translation (NAT)

Describes network address translation (nat). If a routing device running a separate NAT is placed between the endpoints and VAs in your organization, than Secure Access displays the NAT device's IP address for the endpoint's IP address.

If a routing device running a separate NAT is placed between the endpoints and VAs in your organization, than Secure Access displays the NAT device's IP address for the endpoint's IP address. The endpoints must reach the VAs without being subjected to a separate NAT. If you are unable to remove a routing device with a separate NAT, you may have to run a separate set of VAs within that NAT. If you have any questions regarding this matter, contact Support.

Encrypting Traffic with DNSCrypt

Describes encrypting traffic with dnscrypt. Virtual Appliances support DNSCrypt between the virtual machine and the Secure Access public DNS resolvers. This means that any information contained in the EDNS packets forwarded from the VA are encrypted by DNSCrypt and cannot be intercepted.

Virtual Appliances support DNSCrypt between the virtual machine and the Secure Access public DNS resolvers. This means that any information contained in the EDNS packets forwarded from the VA are encrypted by DNSCrypt and cannot be intercepted. For optimum protection, this feature is enabled by default.

Unencrypted traffic is considered a problem that should be resolved. When encryption can not be established between your VA and the Secure Access DNS servers, Secure Access displays a warning. Encryption is established with a probe sent on port 53 (UDP/TCP) to the following addresses:

- IPv4: 18.252.251.72 and 18.254.118.193

If you have a firewall or IPS/IDS doing deep packet inspection and expecting to see only DNS traffic, the probe may fail.

If the probe fails, it is retried on 443 (UDP/TCP) and then on 5353 (UDP). Thus, the encrypted packets may not match the expected traffic on that port. Review your firewall configuration if that is the case and open a case with Support if you believe that you are allowing this traffic.

Virtual Appliance Deployment Guidelines

Describes virtual appliance deployment guidelines. Cisco Secure Access supports various deployments and configurations of Secure Access Virtual Appliances (VAs). Note: You must configure the Internal Domains for your organization. The endpoints must use the Secure Access Virtual Appliances as the primary DNS server.

Cisco Secure Access supports various deployments and configurations of Secure Access Virtual Appliances (VAs).

Note: You must configure the Internal Domains for your organization. The endpoints must use the Secure Access Virtual Appliances as the primary DNS server.

Deploy Virtual Appliances in Pairs

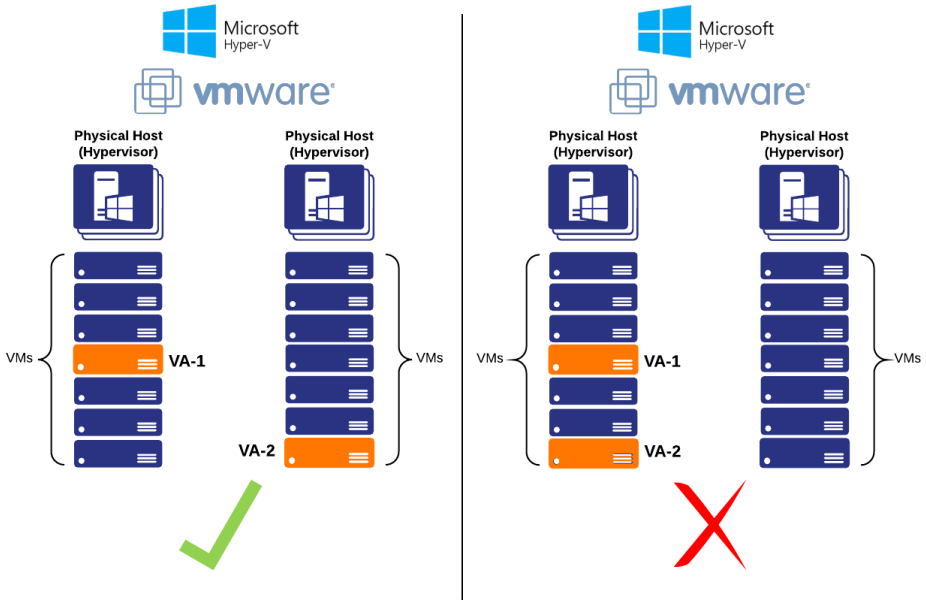
Describes deploying virtual appliances in pairs. VAs must always be deployed in pairs. Running two or more VAs offers high availability in case of system updates.

VAs must always be deployed in pairs. Running two or more VAs offers high availability in case of system updates. This ensures that there is no interruption in Internet service during an update, and allows you to configure updates for scheduled maintenance windows or off-hours.

- **No downtime associated with upgrades** When an upgrade takes place, individual virtual appliances will restart, causing up to 20 minutes of downtime. During this time, any DNS queries routed to the virtual appliance will time out and you will lose internet connectivity. Running two VAs ensures that there is no interruption in Internet service.
- **Ability to schedule updates** Running two VAs allows for scheduling updates. You can schedule updates for off-hours or during scheduled maintenance windows.
- **High availability** If issues arise in one of your VAs, or if you would like to rebuild or move a VA to another host, you can take action without interruptions.

To set up a second virtual appliance, repeat the procedure for setting up the first one. For more information, see Deploy Virtual Appliances.

Whenever possible, deploy VAs on separate physical hypervisor hosts. If a hypervisor hosting a VA becomes unavailable, the second VA will continue serving DNS requests without



interruption.

Multiple DNS Egresses

Describes multiple dns egresses. In most cases where multiple offices or points of presence exist, each office sends and receives its DNS traffic. An office independently sends DNS queries directly to Secure Access. In this case, each office requires its own pair of VAs.

In most cases where multiple offices or points of presence exist, each office sends and receives its DNS traffic. An office independently sends DNS queries directly to Secure Access. In this case, each office requires its own pair of VAs. When using Secure Access, DNS queries always route to the closest Secure Access data center.

Single DNS Egress

Describes single dns egress. In some cases, especially if the networks are geographically close to one another, a single egress may handle all DNS traffic originating from multiple networks.

In some cases, especially if the networks are geographically close to one another, a single egress may handle all DNS traffic originating from multiple networks. This topology is typically used to route traffic through security appliances, Active Directory Domain Controllers, or other network and security devices at a central location to avoid deploying and managing them at every location. This is usually accomplished with a Site-2-Site VPN or an MPLS circuit.

In this case, only the office which sends and receives public DNS queries requires VAs.

Double NAT

Describes double nat. Endpoints and Virtual Appliances that are not behind the same Network Address Translation (NAT) address result in the VAs seeing the IP address of the NAT device instead of the endpoint's IP address.

Endpoints and Virtual Appliances that are not behind the same Network Address Translation (NAT) address result in the VAs seeing the IP address of the NAT device instead of the endpoint's IP address.

With Secure Access Virtual Appliance deployments, we do not recommend a double NAT environment. A double NAT environment can limit both the ability to create granular rules and endpoint-level reporting in Secure Access. However, you can still create a separate rule for the NAT IP address, which would be useful for Guest Wi-FI situations, where knowing the endpoint IP address may not necessarily be helpful, but having a separate rule for that group of endpoints is important.

Virtual Appliance Sizing Guide

Describes virtual appliance sizing guide. The following information is a guide to help you deploy the Cisco Secure Access Virtual Appliances (VAs) in your organization's environment.

The following information is a guide to help you deploy the Cisco Secure Access Virtual Appliances (VAs) in your organization's environment. The key factors are ensuring that the hardware prerequisites are met, and understanding the network latencies between hops and the overall number of Secure Access Sites and users for each VA.

Prerequisites and Network Requirements

- For more information, see Prerequisites for Virtual Appliances.

High-Traffic Sites and Virtual Appliances

Describes high-traffic sites and virtual appliances. For sizing guidance, increasing the number of CPU cores on a VA will improve its performance, but the amount of RAM allocated to the machine must scale along with the number of CPU cores present.

For sizing guidance, increasing the number of CPU cores on a VA will improve its performance, but the amount of RAM allocated to the machine must scale along with the number of CPU cores present.

Secure Access requires that you allocate at least 1 GB of RAM for each CPU core on the VA. For example, a VA deployed with two CPU cores should have a minimum of 2GB of RAM allocated to it.

VA Specifications	Maximum Queries per Second at Maximum 80% CPU Utilization
1 CPU, 1GB RAM	1300
2 CPU, 2 GB RAM	3500
4 CPU, 4 GB RAM	8000
8 CPU, 8 GB RAM	16000
16 CPU, 16 GB RAM	28000

AD Connector Sizing Guidelines

Describes ad connector sizing guidelines. For Active Directory integration with Virtual Appliances, we recommend that you size the AD Connector deployment for the number of VAs and domain controllers configured to communicate with this connector.

For Active Directory integration with Virtual Appliances, we recommend that you size the AD Connector deployment for the number of VAs and domain controllers configured to communicate with this connector.

Number of Virtual Appliances	Number of Domain Controllers	Minimum Connector Specifications
1-2	1-5	2 CPU, 1 GB RAM
4-15	6-20	4 CPU, 8 GB RAM
16-20	21-64	4 CPU, 16 GB RAM
>20	>64	8 CPU, 32 GB RAM

Each domain controller is assumed to process a maximum of 400 AD events a second. If any of your domain controllers are processing more events, make sure to increment the number of domain controllers accordingly. For example, if you

have a domain controller that processes around 1000 AD events a second at peak load, count that as three domain controllers in the sizing table above.

If a connector is run on a system with lower CPU and memory specifications, the connector will continue to function. Some optimizations, such as parallel synchronization of login events to virtual appliances, will not be turned on.

Deployment Considerations

Describes deployment considerations. The number and location of VAs deployed in your environment depends on: Overall latency:Latency between VA and the Secure Access Anycast DNS resolversLatency between users and the VAs

The number and location of VAs deployed in your environment depends on:

- Overall latency:
  - Latency between VA and the Secure Access Anycast DNS resolvers
  - Latency between users and the VAs
- Number of Sites
- Number of users served by the VAs

Overall Latency

Describes overall latency. In general, clients on the network have the best web browsing experience when the total time to retrieve web resources is under 300ms.

In general, clients on the network have the best web browsing experience when the total time to retrieve web resources is under 300ms. This total time to obtain web resources (such as documents, images, and stylesheets) includes both the time to retrieve a DNS response and the time needed to establish a connection with the server indicated in the DNS response. Secure Access aims to minimize the distance that a DNS packet must travel from a client device to our DNS resolvers. However, we do not control the responsiveness of those web servers or how traffic from various locations on the Internet is routed.

TOTAL TIME = *Time to retrieve DNS response + Time to retrieve a web resource*

There are two factors to consider when optimizing DNS response time: the distance between the VA and the Secure Access Anycast DNS resolvers, and the distance between the client and the VA.

The VA, when deployed, will forward all externally-bound DNS requests to the Secure Access DNS resolvers, 18.252.251.72 and 18.254.118.193. Therefore, when determining the latency between the VA and the closest Secure Access data center, we recommend an average DNS response time under 150ms for the best user experience.

When determining where to deploy VAs in your environment, you will want to take into account the distance between the clients that will utilize the VAs and the VAs themselves. For optimal performance, an average ping time between a client and the VM host on which the VA lives should not exceed 50ms.

Number of Secure Access Sites

Describes number of secure access sites. Secure Access Sites allow you to divide up your Secure Access deployments. Each Secure Access Site is an isolated deployment in which the components will only communicate with other components in the same Secure Access Site.

Secure Access Sites allow you to divide up your Secure Access deployments. Each Secure Access Site is an isolated deployment in which the components will only communicate with other components in the same Secure Access Site. This is primarily useful in environments containing locations with high-latency connections or in environments with locations whose internal IP space overlaps.

Secure Access requires that you deploy at least two Virtual Appliances for a Site. This ensures high availability of the Virtual Appliances and the option to receive updates without downtime.

Number of Users for a VA

Describes number of users for a va. A typical VA deployed with minimum hardware requirements has a tested throughput of at least 2000 queries per second.

A typical VA deployed with minimum hardware requirements has a tested throughput of at least 2000 queries per second.

Taking into account these metrics, a single VA can handle DNS requests from at least 57,000 concurrent users. Secure Access defines a single user as a client that generates an average of 1000 DNS requests in a typical eight-hour workday. Therefore, Secure Access defines concurrent users as the number of users or devices sending DNS requests to a VA at the same time.

If the VA specifications are increased to two virtual CPUs and 1GB RAM, a single VA will be able to handle DNS requests from at least 115,000 concurrent users. The number of users on the network likely will NOT be the limiting factor when determining the number of VAs to deploy.

54 Manage VAs in Secure Access

Topics:

- Configure Authentication for Virtual Appliances
- Manage DNS Forwarders
- Manage Site for Virtual Appliance
- Configure Updates for Virtual Appliances

Introduces managing vas in secure access. Cisco Secure Access Virtual Appliances (VAs) are lightweight virtual machines that function as conditional DNS forwarders on your network. Secure Access VAs support DNS-layer security only.

Cisco Secure Access Virtual Appliances (VAs) are lightweight virtual machines that function as conditional DNS forwarders on your network. Secure Access VAs support DNS-layer security only.

In Secure Access, you can manage the configuration and deployment of the VAs for your organization.

First, download the images for the VAs and configure authentication for the VAs. Then deploy the VAs in your environment.

- Configure the authentication for secure communications between Secure Access and your VAs. For more information, see Configure Authentication for Virtual Appliances.
- Download the software images to deploy the Secure Access VAs in your environment. For more information, see Deploy Virtual Appliances.

Manage the Secure Access Site.

- Manage the Site associated with the VA. For more information, see Manage Site for Virtual Appliance.

Manage the settings and updates for the VAs.

- Manage the settings for the DNS forwarders. For more information, see Manage DNS Forwarders.
- Configure automatic updates on the VAs in the organization or make a manual update to a VA. For more information, see Configure Updates to Virtual Appliances.

Configure Authentication for Virtual Appliances

Describes configuring authentication for virtual appliances. Cisco Secure Access communicates with the Secure Access Virtual Appliances (VAs) that are deployed in your organization. Secure Access makes software syncs and health checks to your VAs and requires that API requests from the VAs use authentication.

Cisco Secure Access communicates with the Secure Access Virtual Appliances (VAs) that are deployed in your organization. Secure Access makes software syncs and health checks to your VAs and requires that API requests from the VAs use authentication.

To manage the authentication of the communications from the VAs to Secure Access, we recommend that you configure API key credentials for your VA deployments.

Your API key credentials apply to all AD Connectors and Virtual Appliances deployed in your environment.

> **Note**
>
> The API key authentication is available for Secure Access Virtual Appliance version 3.7.0 and newer and the Cisco AD Connector version 1.14.4 or newer.

For more information about configuring authentication for AD Connectors and Virtual Appliances, see Configure Authentication for AD Connectors and VAs.

How to Set Up Your API Credentials

Provides instructions for how to set up your api credentials. First, create the Secure Access Key Admin API key and secret.

Procedure

1. First, create the Secure Access Key Admin API key and secret.
2. Then, use your Secure Access Key Admin API key credentials to generate your Secure Access client API key and secret.

What to do next

Your Secure Access client API key credentials are stored in the Virtual Appliances deployed in the organization.

Important

Secure Access client API key credentials are valid for 90 days.

Virtual Appliances use your Secure Access client API key credentials to generate an OAuth 2.0 access token. The access token is included in every API request from the Virtual Appliance to Secure Access.

Authentication for VAs is available in Secure Access Virtual Appliance version 3.7.0 and newer.

Procedure

Provides instructions for procedure. Create a Secure Access Key Admin API key and secret. Use the Secure Access Key Admin API credentials to generate your Secure Access client API key credentials.

Create a Secure Access Key Admin API key and secret. Use the Secure Access Key Admin API credentials to generate your Secure Access client API key credentials.

The Secure Access client API key and secret are stored in the VAs that you deploy in your environments. The generated API credentials (key and secret) apply to all VAs in the organization.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Secure Access Virtual Appliance version 3.7.0 and newer.

Procedure

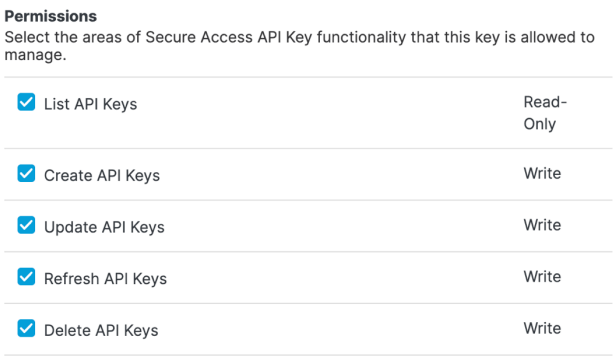
1. Step 1 - Create the Key Admin API Key Credentials
2. Step 2 - Add the Key Admin API Key Credentials

Step 1 – Create the Key Admin API Key Credentials

Provides instructions for step 1 – create the key admin api key credentials. Create a Secure Access Key Admin API key. For more information, see Add Key Admin API Keys.

Procedure

Create a Secure Access Key Admin API key. For more information, see Add Key Admin API Keys. Select each type of permission for the key.



Note

Save your Key Admin API key and secret and use these credentials to configure the authentication for the VAs in the organization.

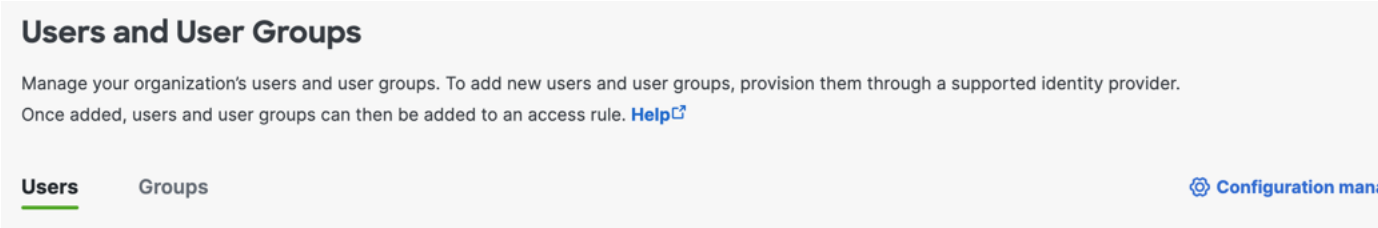
Step 2 – Add the Key Admin API Key Credentials

Provides instructions for step 2 – add the key admin api key credentials. Add the Secure Access Key Admin API key and secret to the VA configuration in Users and Groups. Then, generate a Secure Access client API key and secret.

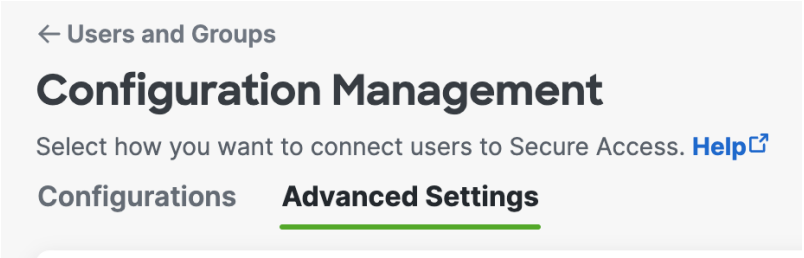
Add the Secure Access Key Admin API key and secret to the VA configuration in **Users and Groups**. Then, generate a Secure Access client API key and secret.

Procedure

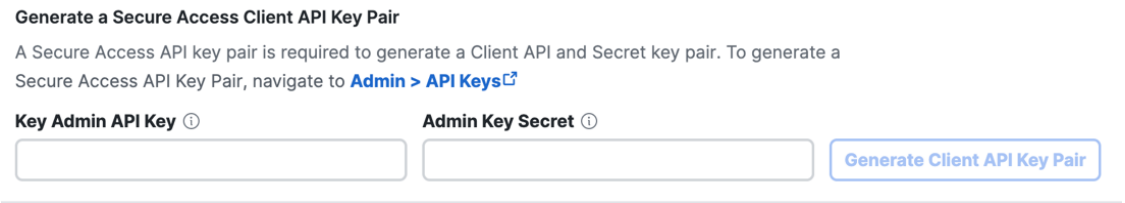
1. Navigate to **Connect** > **Users and User Groups** > **Configuration Management**.



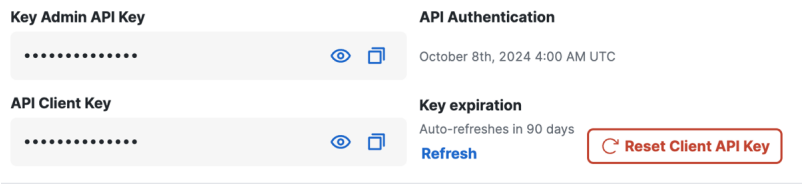
2. Click **Advanced Settings**.



3. For **Key Admin API Key**, add the Key Admin API key, and for **Key Admin Key Secret**, add the Key Admin API key secret. For information about creating the Key Admin API key, see Step 1 - Create the Key Admin API Key Credentials.



4. After you add the Key Admin API key and secret, click **Generate Client API Key Pair**.
5. Save the Secure Access client API key and secret. Secure Access updates the client API key and secret automatically every 90 days.



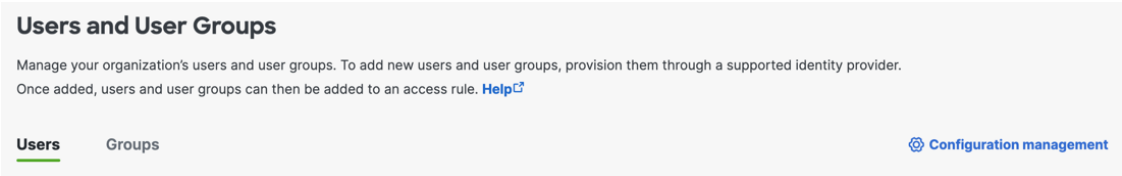
Refresh Client API Key and Secret

Provides instructions for refresh client api key and secret. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Refresh your Secure Access client API key and secret.

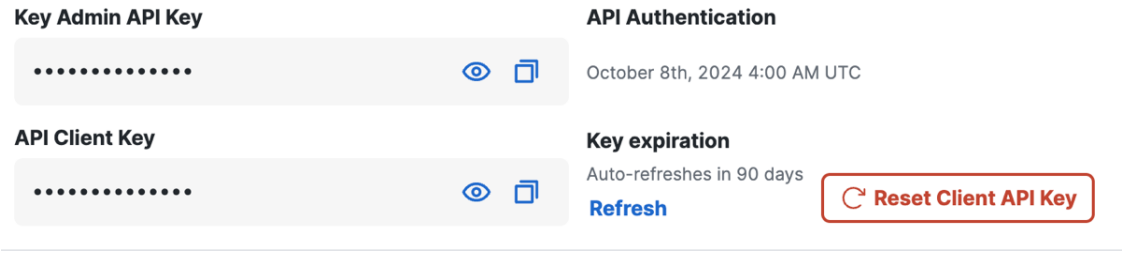
Procedure

1. Navigate to **Connect** > **Users and User Groups** > **Configuration Management**.

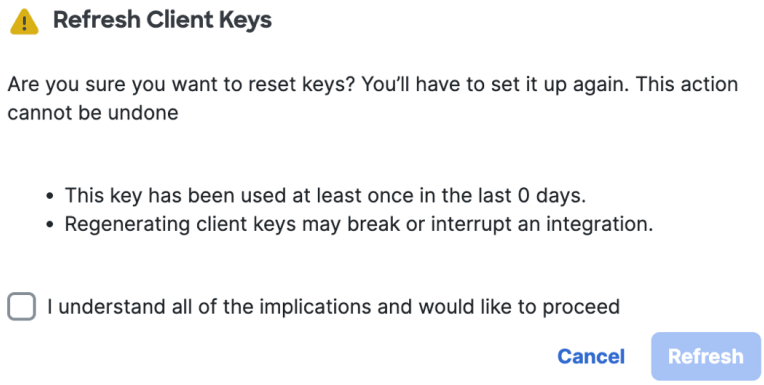


2. Click **Advanced Settings**.
3. Click **Refresh**.

   Secure Access refreshes the client API key and secret.



4. For **Refresh Client Keys**, check the box to confirm the deletion of the client API key and secret.



5. Click **Refresh**.

Reset Client API Key

Provides instructions for resetting client api key. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

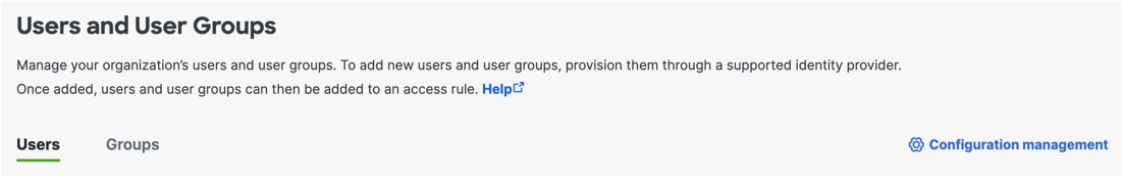
Delete your Secure Access Key Admin API key and Secure Access client API key.

Important

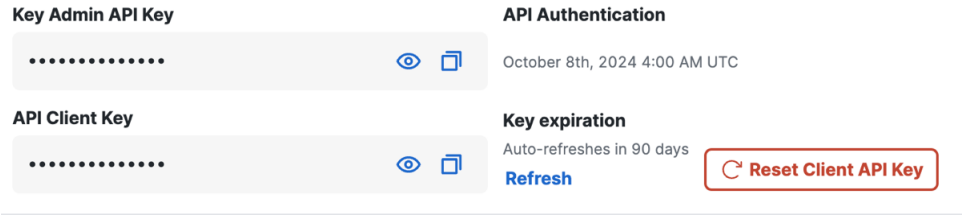
After you delete the Key Admin API key and client API key, existing VA deployments may continue to use the stored Secure Access client API key and secret for up to 90 days.

Procedure

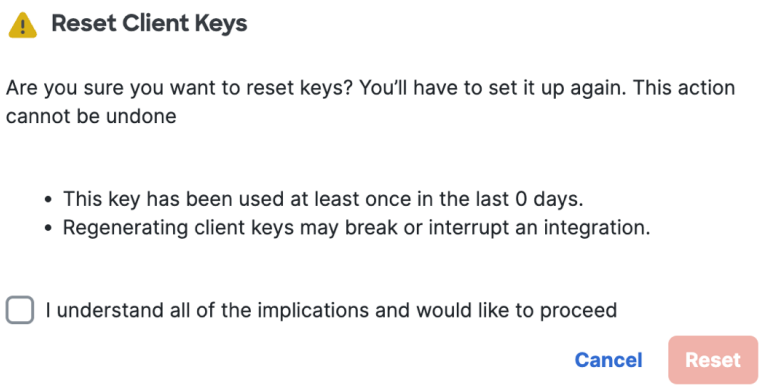
1. Navigate to **Connect** > **Users and User Groups** > **Configuration Management**.



2. Click **Advanced Settings**.
3. Click **Reset Client API Key**.



4. For **Reset Client API Keys**, check the box to confirm the deletion of both the Key Admin API key and client API key for the VAs in the organization.



5. Click **Reset**.

Manage DNS Forwarders

Describes managing dns forwarders. Once deployed in your environment, you can view your Cisco Secure Access Virtual Appliances (VAs) in Cisco Secure Access. Navigate to DNS Forwarders in Secure Access and manage the settings for the VAs.

Once deployed in your environment, you can view your Cisco Secure Access Virtual Appliances (VAs) in Cisco Secure Access. Navigate to **DNS Forwarders** in Secure Access and manage the settings for the VAs. On each VA, you can manage the Secure Access Site for the VA, reset the VA's password, and upgrade and delete a VA.

Procedure

Describes procedure. View the properties of each deployed Virtual Appliance, sync configuration settings to the deployed VAs, and manage the Virtual Appliances.

View the properties of each deployed Virtual Appliance, sync configuration settings to the deployed VAs, and manage the Virtual Appliances.

- View the DNS Forwarders

- Sync the Configuration Settings to Deployed VAs
- Edit a Site
- Upgrade a Virtual Appliance
- Reset Password for Virtual Appliance
- Delete a Virtual Appliance

Prerequisites

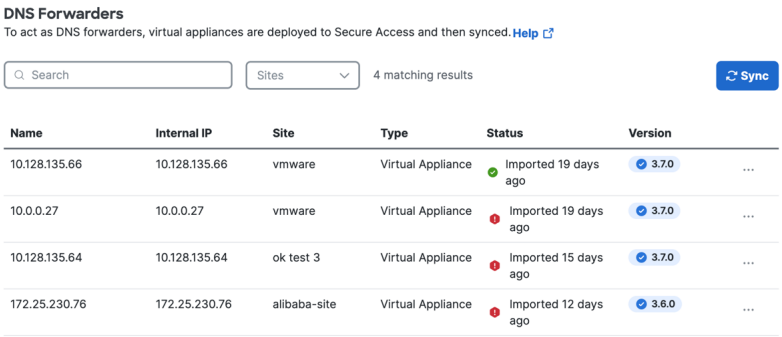
- Full Admin user role. For more information, see Manage Accounts.

View the DNS Forwarders

Provides instructions for viewing the dns forwarders. Navigate to Connect DNS Forwarders . On DNS Forwarders, view the deployed Virtual Appliances. The VAs have several properties:

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. On **DNS Forwarders**, view the deployed Virtual Appliances. The VAs have several properties:
   - **Name**–The descriptive name of the VA.
   - **Internal IP**–The internal IP address of the VA.
   - **Site**–The name of the Site associated with the VA.
   - **Type**–The type of the DNS Forwarder, for example: Virtual Appliance.
   - **Status**–The status of the VA.
   - **Version**–The version of the deployed software image on the VA.



Sync the Configuration Settings to Deployed VAs

Provides instructions for sync the configuration settings to deployed vas. Secure Access refreshes the latest configuration settings for the deployed Virtual Appliances.

Secure Access refreshes the latest configuration settings for the deployed Virtual Appliances.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. On **DNS Forwarders**, click **Sync**.

Edit a Site

Describes editing a site. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- For more information, see Manage Site for Virtual Appliance.

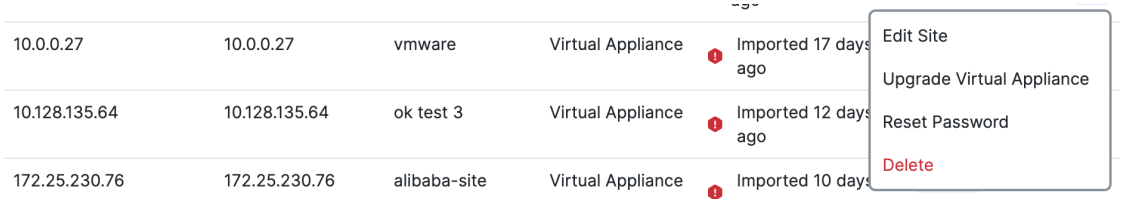
Upgrade a Virtual Appliance

Provides instructions for upgrade a virtual appliance. The update of a VA results in the loss of DNS service for the duration of the update.

The update of a VA results in the loss of DNS service for the duration of the update. We highly recommend that you perform updates during non-business hours, or preferably, deploy a second VA for this site to automate the process of updates without introducing VA downtime.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Navigate to a Virtual Appliance and click the ellipsis (**...**), and then click **Upgrade Virtual Appliance**.



3. For **Upgrade Virtual Appliance**, click **Upgrade**.

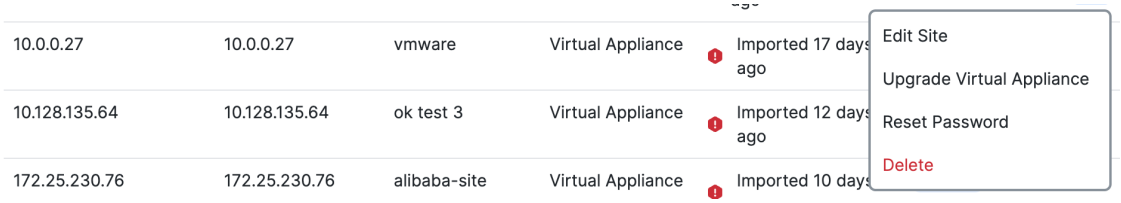
Reset Password

Provides instructions for resetting password. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

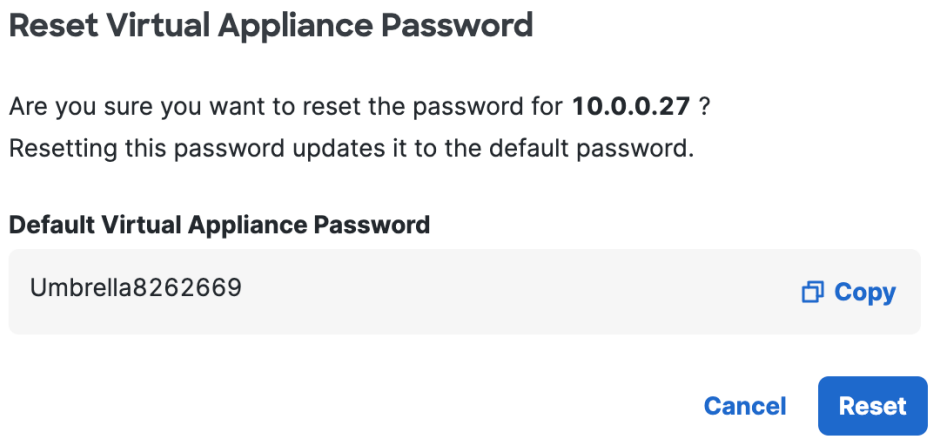
Reset a Virtual Appliance's password. The Virtual Appliance username is **vmadmin**.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance and click the ellipsis (**...**), and then seelect **Reset Password**.



3. For **Reset Virtual Appliance Password**, click. **Reset**, to generate a new password for the Virtual Appliance.



> **Note**
>
> It can take up to 15 minutes for the password to reset and sync with the deployed VAs.

Delete a Virtual Appliance

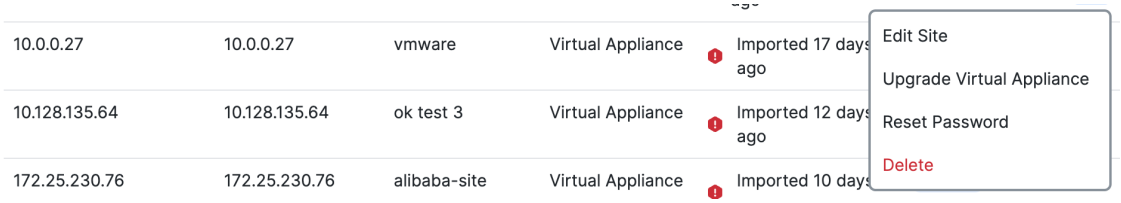
Provides instructions for deleting a virtual appliance. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Remove the Virtual Appliance from the organization.

Procedure

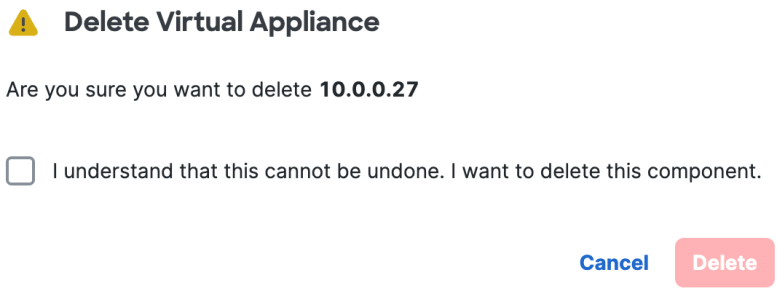
---

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance and click the ellipsis (**...**), and then select **Delete**.



3. Check the box to confirm the deletion of the VA, and then click **Delete**.

What to do next



Manage Site for Virtual Appliance

Describes managing site for virtual appliance. A Cisco Secure Access Virtual Appliance (VA) is associated with a Secure Access Site. You can add a new Site, select and rename a Site, or delete the Site for the VA.

A Cisco Secure Access Virtual Appliance (VA) is associated with a Secure Access Site. You can add a new Site, select and rename a Site, or delete the Site for the VA. If you do not select a Site for the VA, Secure Access uses the default Site.

For information about Internal Networks, see Manage Internal Networks.

Procedure

Provides instructions for procedure. Add a new site, select a site, rename a site, or delete a site for the VA.

Add a new site, select a site, rename a site, or delete a site for the VA.

Before you begin

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

Procedure

1. Add a Site
2. Select a Site
3. Rename a Site
4. Delete a Site

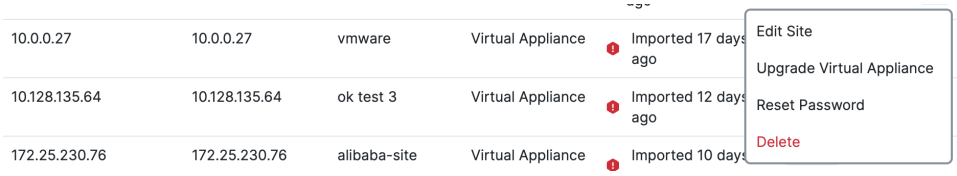
Add a Site

Provides instructions for adding a site. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Add a Site for the VA.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance, click the ellipsis (**...**), and then select **Edit Site**.



3. Click **+Add**, enter a descriptive name for the Site, and then click **Save**. After you add a Site, associate the Site with an Internal Network. For more information, see Manage Internal Networks.



Select a Site

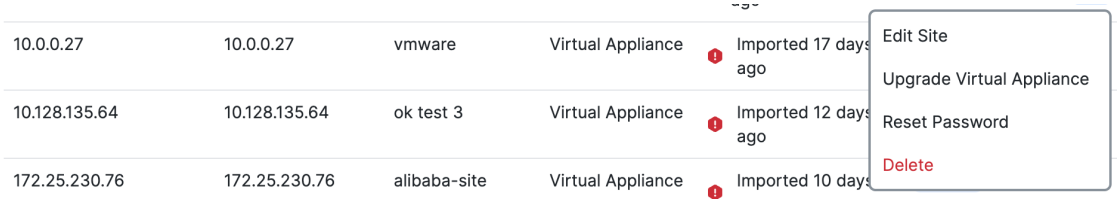
Provides instructions for selecting a site. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Select a Site for the VA.

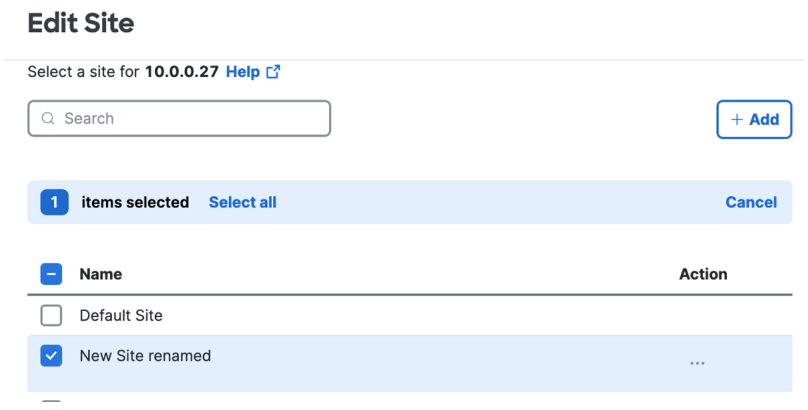
Procedure

---

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance, click the ellipsis (**...**), and then select **Edit Site**.



3. Locate and select a Site for the VA, and then click **Save**.



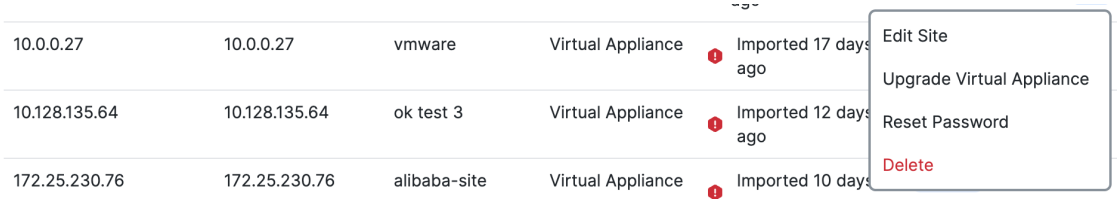
Rename a Site

Provides instructions for rename a site. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

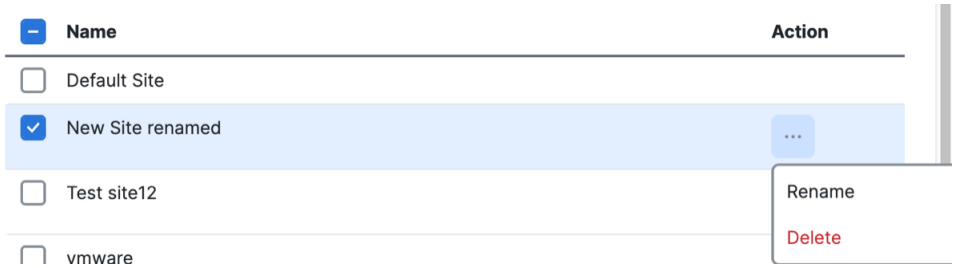
Edit the name of a Site.

Procedure

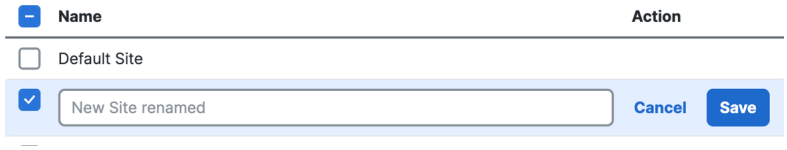
1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance, click the ellipsis (**...**), and then select **Edit Site**.



3. Locate the name of a Site, and then for **Action** click the ellipsis (**...**).



4. Click **Rename**, enter a descriptive name in the text area, and then click **Save**.



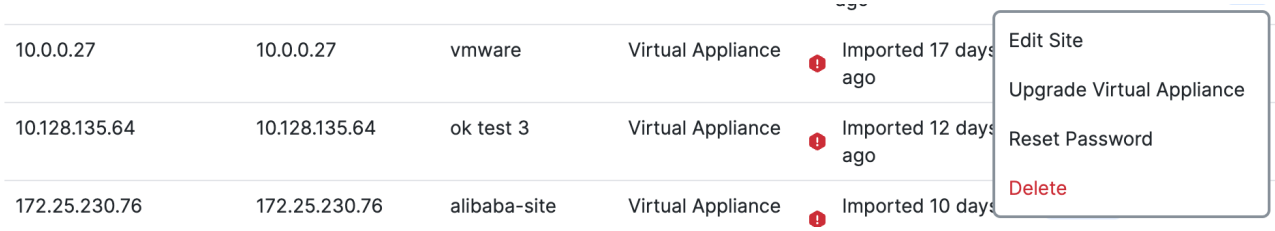
Delete a Site

Provides instructions for deleting a site. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

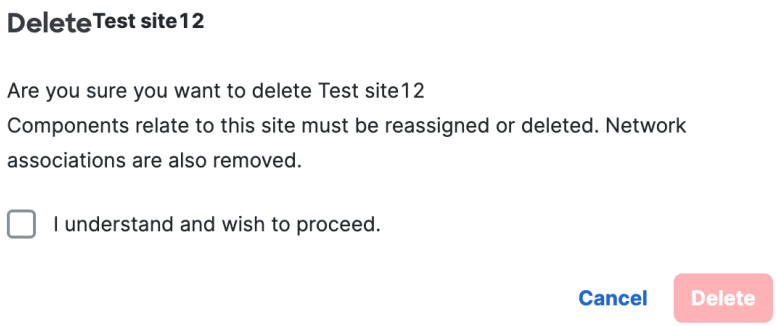
Delete a Site.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance, click the ellipsis (**...**), and then select **Edit Site**.



3. Locate the name of a Site, and then for **Action** click the ellipsis (**...**).
4. Click **Delete**, check **I understand and wish to proceed**, and then click **Delete** to remove the Site.



Configure Updates for Virtual Appliances

Describes configuring updates for virtual appliances. Cisco Secure Access Virtual Appliances (VAs) can receive automatic software updates. New software versions for the Virtual Appliances become available and are usually applied without any intervention required.

Cisco Secure Access Virtual Appliances (VAs) can receive automatic software updates. New software versions for the Virtual Appliances become available and are usually applied without any intervention required.

How Secure Access Updates Your Virtual Appliance

Describes how secure access updates your virtual appliance. You can configure updates for the VAs in your organization. Secure Access makes API requests from each VA and pushes out software updates. If you wish to update a specific VA first, do this manually.

You can configure updates for the VAs in your organization. Secure Access makes API requests from each VA and pushes out software updates. If you wish to update a specific VA first, do this manually. For more information, see Manually Configure Update of a Virtual Appliance.

Logic is built-in to our API to prevent two VAs at a single site from updating at once or updating when one of the VAs is in an error state. The following checks are performed:

1. The API checks if there is only a single VA for the site. If there is only one VA, the API does not offer a command to auto-update.
2. If there is a secondary VA for the site but it is in an error state, then the first VA will not auto-update.
3. The API checks to see if a second VA for that site is already updating and if it is in a mid-update state it will not auto-update during that window of time. If we have ordered a VA to update and have not heard back that it has completed, this qualifies as a mid-update state.
4. If all the prerequisite checks have been met, the VA is updated.

Prerequisites and Network Requirements

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

Procedure

Describes procedure. Configure Automatic Updates of Virtual Appliances Manually Configure Update of a Virtual Appliance Postpone Updates to Virtual Appliances

- Configure Automatic Updates of Virtual Appliances
- Manually Configure Update of a Virtual Appliance
- Postpone Updates to Virtual Appliances

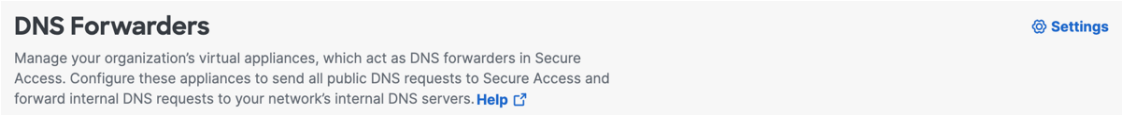
Configure Automatic Updates of Virtual Appliances

Provides instructions for configuring automatic updates of virtual appliances. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

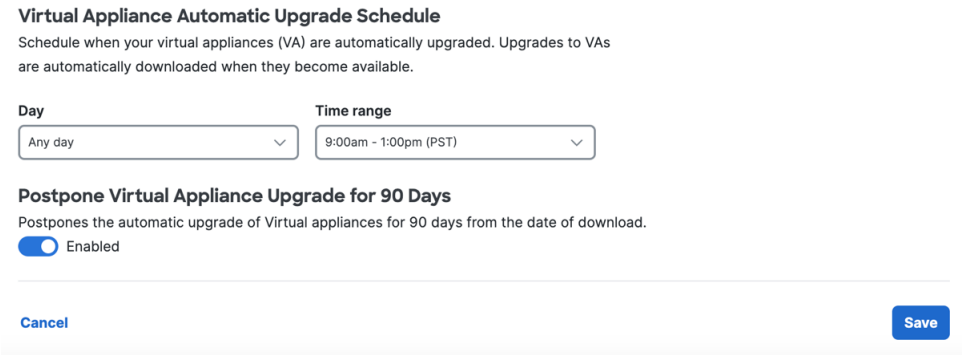
Set up automatic updates to your deployed Virtual Appliances.

Procedure

1. Navigate to **Connect** > **DNS Forwarders** > **Settings**.

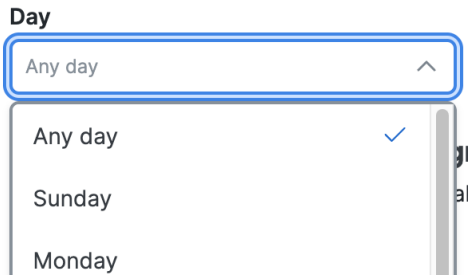


2. For **Virtual Appliance Automatic Upgrade Schedule**, choose the **Day** and **Time range** for the automatic software updates.

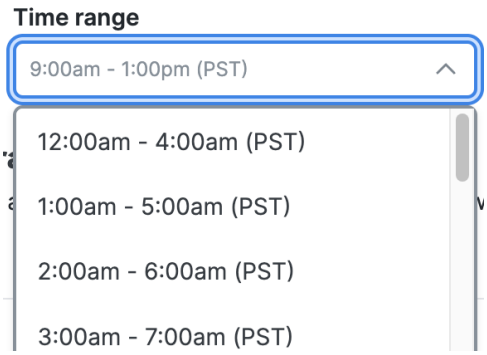


What to do next

1. For **Day**, select **Any day** or a day of the week.



2. For **Time range**, select one of the available times.



3. Click **Save**.

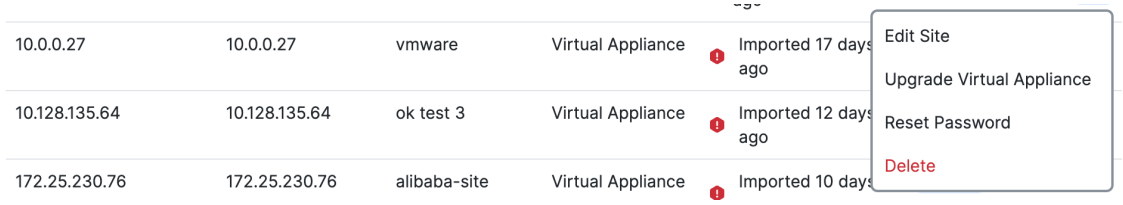
Manually Configure Update of a Virtual Appliance

Provides instructions for manually configure update of a virtual appliance. The update of a VA results in the loss of DNS service for the duration of the update.

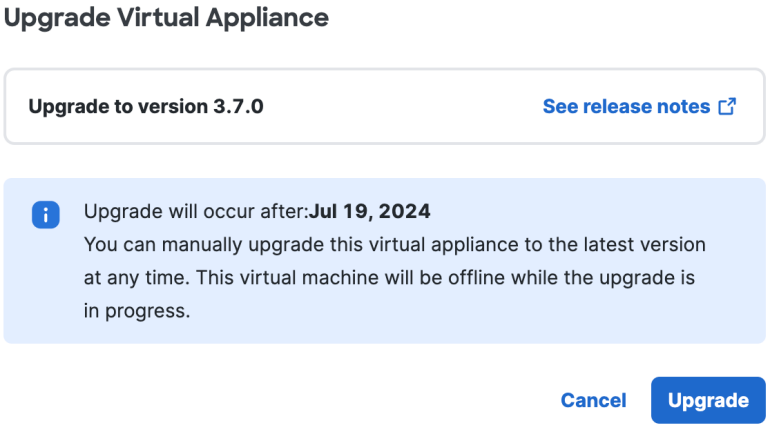
The update of a VA results in the loss of DNS service for the duration of the update. We highly recommend that you perform updates during non-business hours, or preferably, deploy a second VA for this site to automate the process of updates without introducing VA downtime.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Navigate to a Virtual Appliance and click the ellipsis (**...**), and then click **Upgrade Virtual Appliance**.



3. For **Upgrade Virtual Appliance**, click **Upgrade**.



Postpone Updates to Virtual Appliances

Provides instructions for postpone updates to virtual appliances. You can postpone the upgrade of the software on the Secure Access Virtual Appliances in your environment. Configure the delay of the upgrade for 90 days since the latest software update was made available.

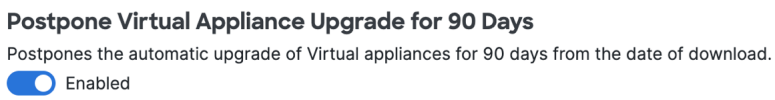
You can postpone the upgrade of the software on the Secure Access Virtual Appliances in your environment. Configure the delay of the upgrade for 90 days since the latest software update was made available.

After 90 days, Secure Access upgrades the software on your Virtual Appliances according to the schedule that you configured.

> **Note**
>
> The software update delay applies to major releases only, and not for patch releases.

Procedure

1. Navigate to **Connect** > **DNS Forwarders** > **Settings**.
2. For **Postpone Virtual Appliance Automatic Upgrade for 90 Days**, select **Enabled**.



55 Deploy Virtual Appliances

Topics:

- Deploy Virtual Appliances

Describes the purpose and procedures for deploy virtual appliances and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Deploy Virtual Appliances

Describes deploying virtual appliances. Secure Access requires that you deploy two Virtual Appliances (VAs) for a given site. It is critical that these VAs are not cloned or copied in any way.

Secure Access requires that you deploy two Virtual Appliances (VAs) for a given site. It is critical that these VAs are not cloned or copied in any way.

Guidelines

Describes guidelines. Set up and configure your virtual appliances manually. Do not copy or clone your virtual appliances. Cloning your virtual appliances may disrupt syncs with Secure Access if you have to restore the VAs.

- Set up and configure your virtual appliances manually. Do not copy or clone your virtual appliances. Cloning your virtual appliances may disrupt syncs with Secure Access if you have to restore the VAs.
- VAs do not cache any data that would require backing up. Deploy two VAs on a site in order to avoid downtime if one of the VAs is not available.
- You should understand how to deploy a virtual machine in your environments.

Deploy the Secure Access Virtual Appliances

Describes deploying the secure access virtual appliances. Choose a deployment procedure based on your OS and software: Deploy VAs in Hyper-V for Windows 2012 or Higher

Choose a deployment procedure based on your OS and software:

- Deploy VAs in Hyper-V for Windows 2012 or Higher
- Deploy VAs in VMware

Deploy VAs in Hyper-V for Windows 2012 or Higher

Describes deploying vas in hyper-v for windows 2012 or higher. Deploy Cisco Secure Access Virtual Appliances in Microsoft Hyper-V for Windows Server 2012 or higher.

Deploy Cisco Secure Access Virtual Appliances in Microsoft Hyper-V for Windows Server 2012 or higher.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Configure Authentication for the Virtual Appliances

Describes configuring authentication for the virtual appliances. Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** button only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- One of the following Windows Server operating systems:
  - Windows Server 2012, SP1, or R2 (Standard or Datacenter), 2016 or 2019 with Hyper-V role.
  - Hyper-V Server 2012, 2012 R2, 2016 or 2019.
- Basic knowledge of Hyper-V.

> **Note**
>
> Secure Access does not support Virtual Appliances that are deployed using System Center Virtual Machine Manager (SCVMM).

Procedure

Describes procedure. Step 1 – Download and Extract the Hyper-V Installer Step 2 – Import the Virtual Appliance Step 3 – Copy and Rename Image Files

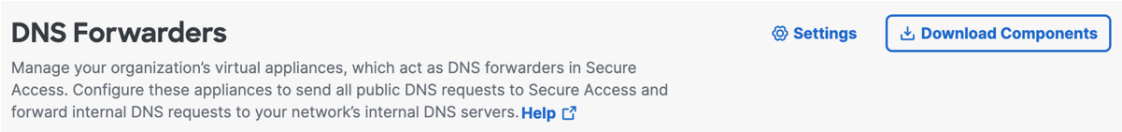
- Step 1 – Download and Extract the Hyper-V Installer
- Step 2 – Import the Virtual Appliance
- Step 3 – Copy and Rename Image Files
- Step 4 – Select Network Adapter
- Step 5 – Select Hard Drive
- Step 6 – Power on the Virtual Machine
- Step 7 – Repeat for the Second Virtual Appliance

Step 1 - Download and Extract the Hyper-V Installer

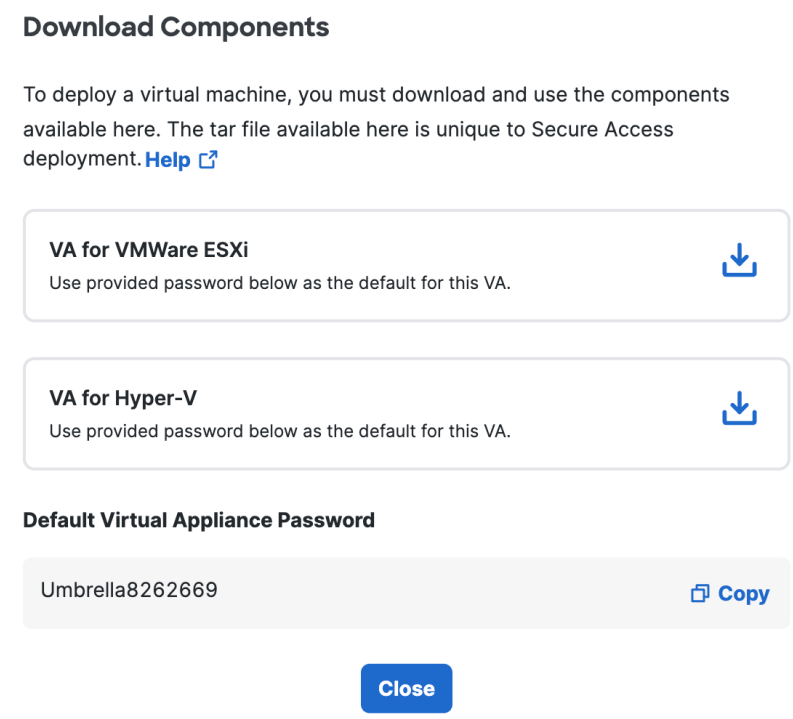
Provides instructions for step 1 – download and extract the hyper-v installer. Navigate to Connectors DNS Forwarders and click Download Components.The Secure Access Forwards Main interface.

Procedure

1. Navigate to **Connectors** > **DNS Forwarders** and click **Download Components**.



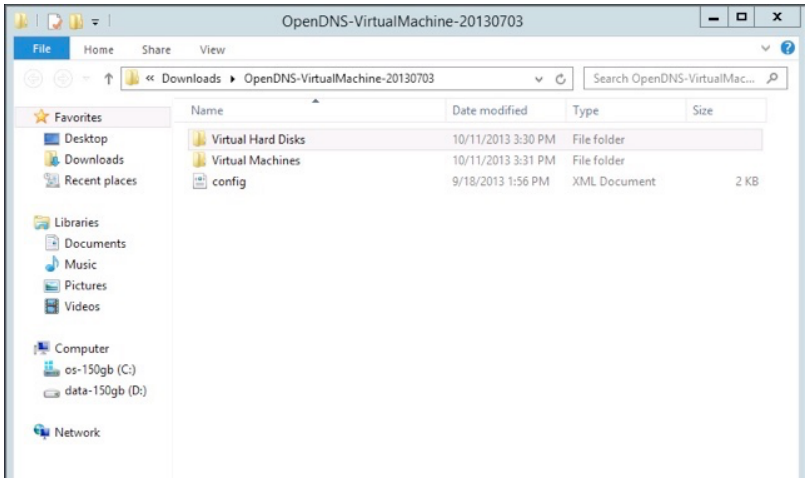
2. Click **Download** for **VA for Hyper-V**.



Secure Access generates and downloads a tar file unique to your deployment. This tar file includes:

- a zip file containing the virtual hard disks that need to be deployed on Hyper-V
- a signature file
- a Cisco public certificate to validate the signature
- a readme file

3. Extract the contents of the tar file using the command `tar -xvf <tar filename> -C <Destination folder>`. To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. When successful, you will see a message saying “Verified OK."
4. Extract the .zip file. You'll find two folders–**Virtual Hard Disks** and **Virtual Machines**–and a **config** file.



Step 2 – Import the Virtual Appliance

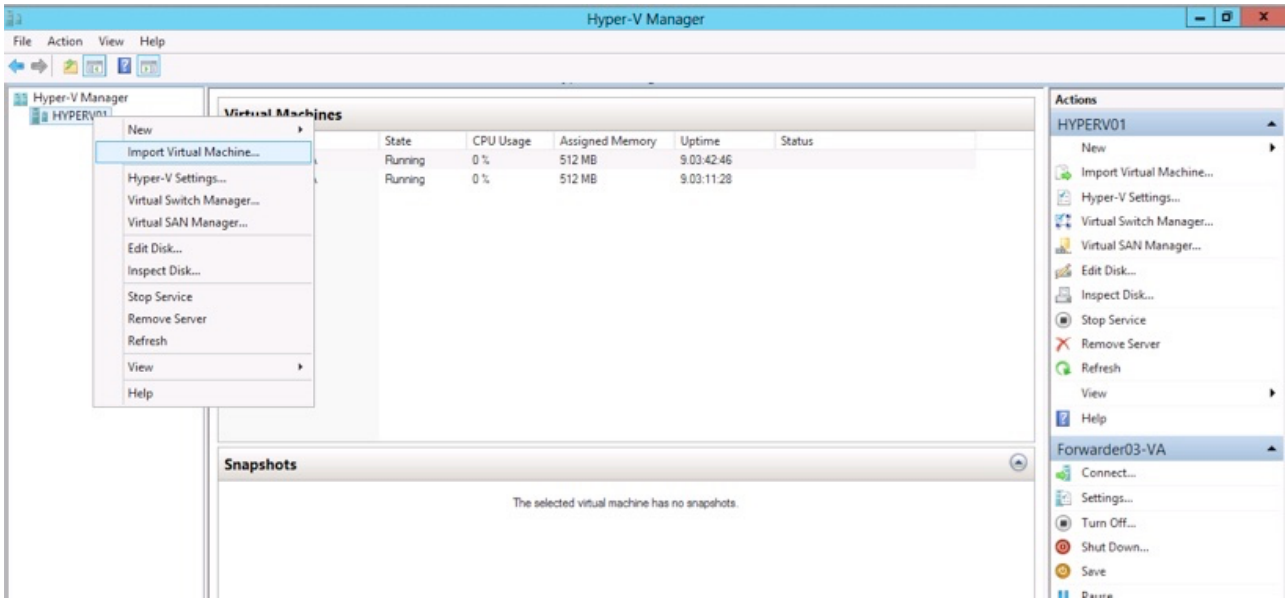
Provides instructions for step 2 – import the virtual appliance. Microsoft has introduced a "Generation 2" style of VM profile on Hyper-V for Windows 2012 R2 and higher versions.

> **Note**
>
> Using Windows 2012 R2 or Higher Versions
>
> Microsoft has introduced a "Generation 2" style of VM profile on Hyper-V for Windows 2012 R2 and higher versions. As a result, the import steps below will fail with the error: "*Hyper-V did not find virtual machines to import from location [path]*"
>
> You will need to create a new virtual machine as "Generation 1", then skip to 3. Copy and Rename Image Files.
>
> For more information about Generation 1 vs. Generation 2, see Generation 2 Virtual Machine Overview.

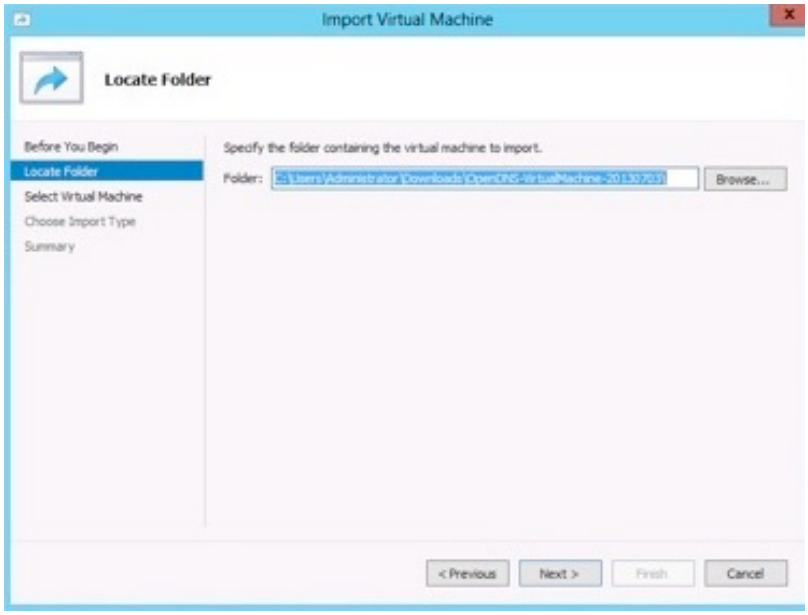
> **Note**
>
> Step 2 in this procedure applies to Windows 2012 only, and not **Windows 2012 *R2*** .

Procedure

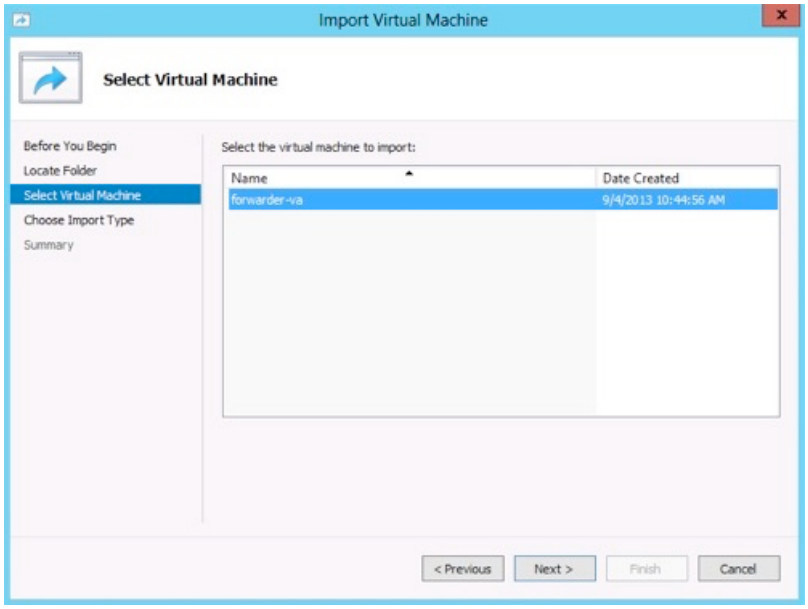
1. Select your Hyper-V server, right-click its name and select **Import Virtual Machine** from the menu.



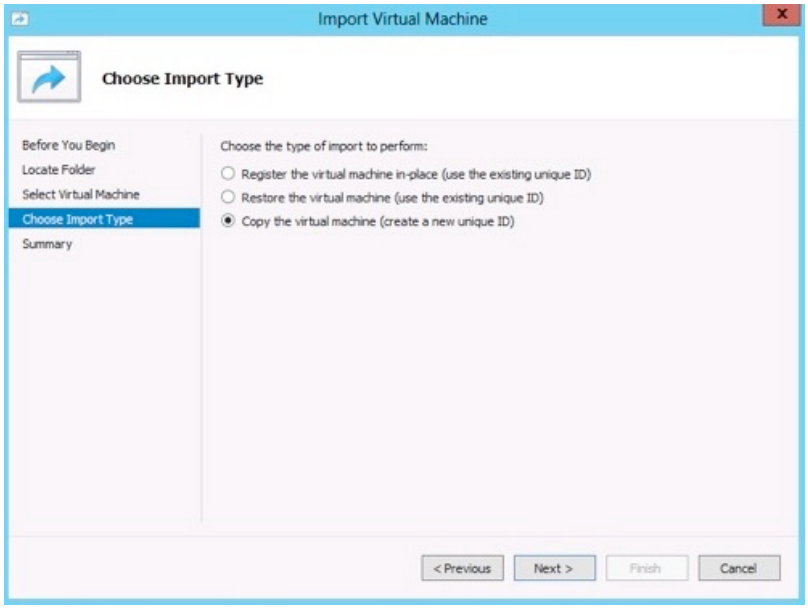
2. Navigate to the extraction folder from your download, select that folder to import, and then click **Next**.



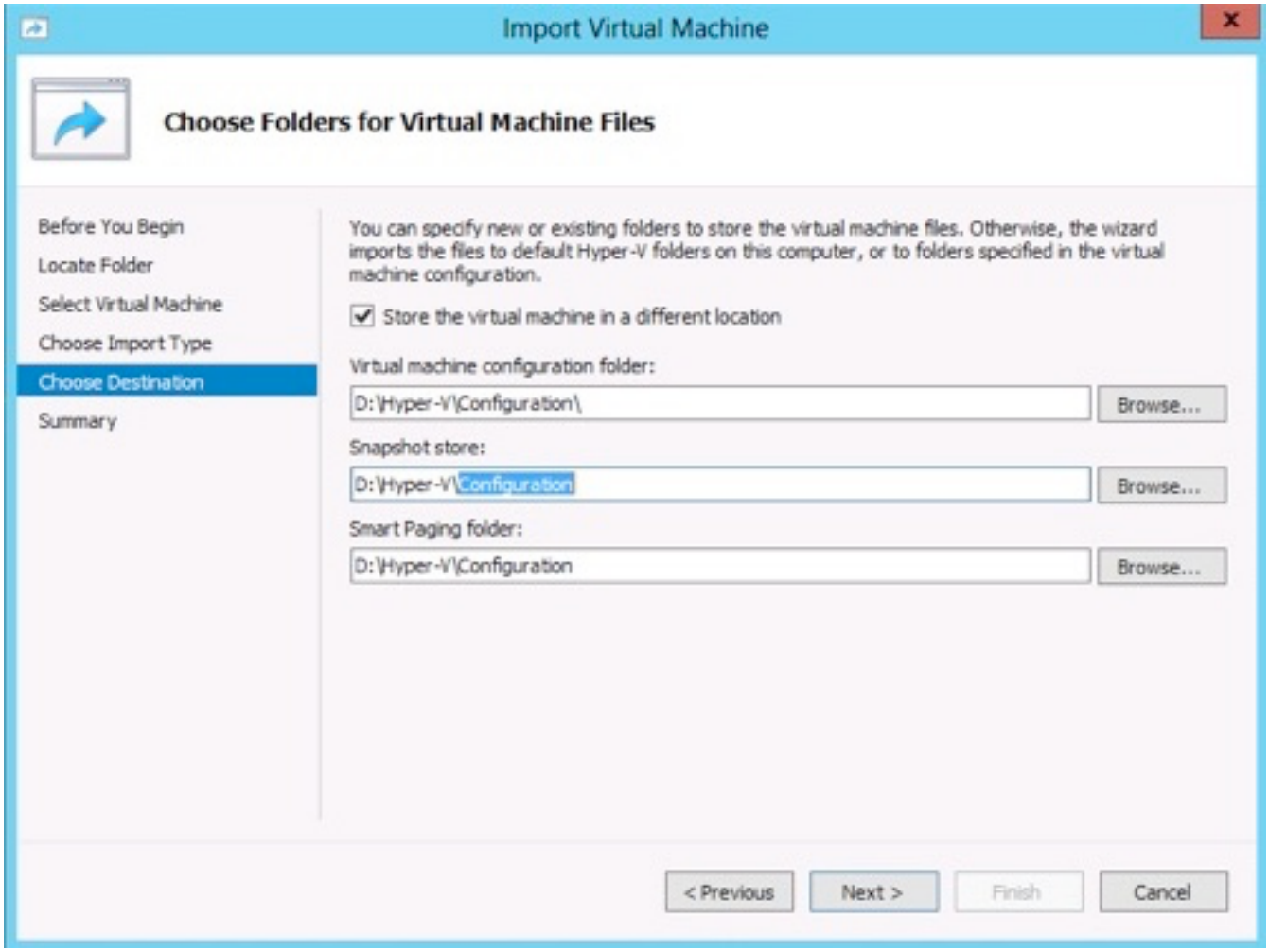
3. Select **forwarder-va** as the virtual machine to import and click **Next**.



4. Select **Copy the virtual machine (create a new unique ID)** and click **Next**.



5. Choose destination folders to install to. By default, these are the **Hyper-V Configuration** folders, but you can choose another folder.



> **Note**
>
> If selecting a different folder, pick a drive with sufficient space and create a folder with a specific name for the virtual machine, such as \opendnsforwarder-1. This can be helpful to ensure you're able to distinguish between the two virtual appliances in your file structure.

6. Click **Finish**.

Step 3 – Copy and Rename Image Files

Provides instructions for step 3 - copy and rename image files. In Windows Explorer, navigate to the \Virtual Hard Disks subfolder within the extracted download folder created in Step 1.

Procedure

1. In Windows Explorer, navigate to the **\Virtual Hard Disks** subfolder within the extracted download folder created in **Step 1**.
2. Copy the two files from that location to the Virtual Machine Configuration Folder you specified in the previous step.
3. The two files, **dynamic** and **forwarder-va**. must be renamed per the VA that is being installed. For example, rename:

   dynamic to **Dynamic-VA-1**

   and

   forwarder-va to **Forwarder-VA-1**

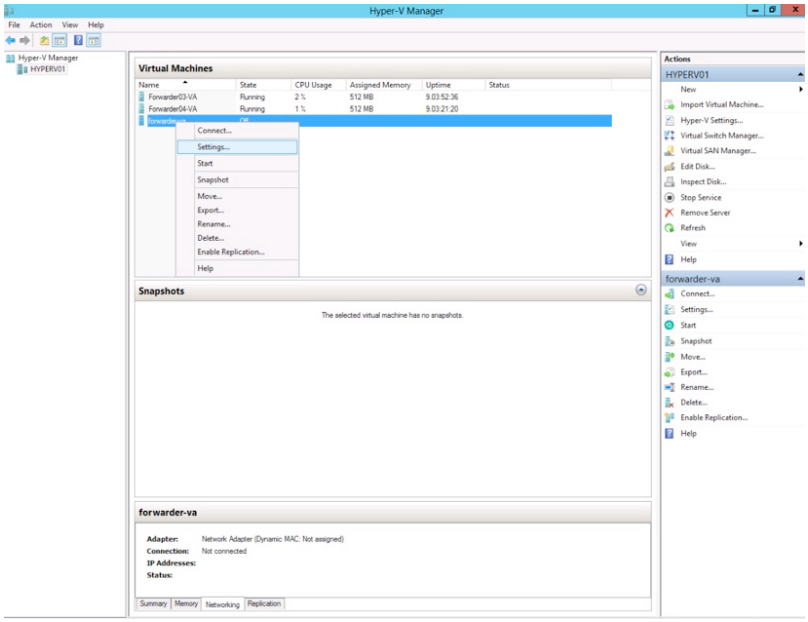
   If configuring your second VA, change the number accordingly. This can help ease the management of multiple virtual appliances and avoids conflicts between filenames when configuring your second VA.

Step 4 – Select Network Adapter

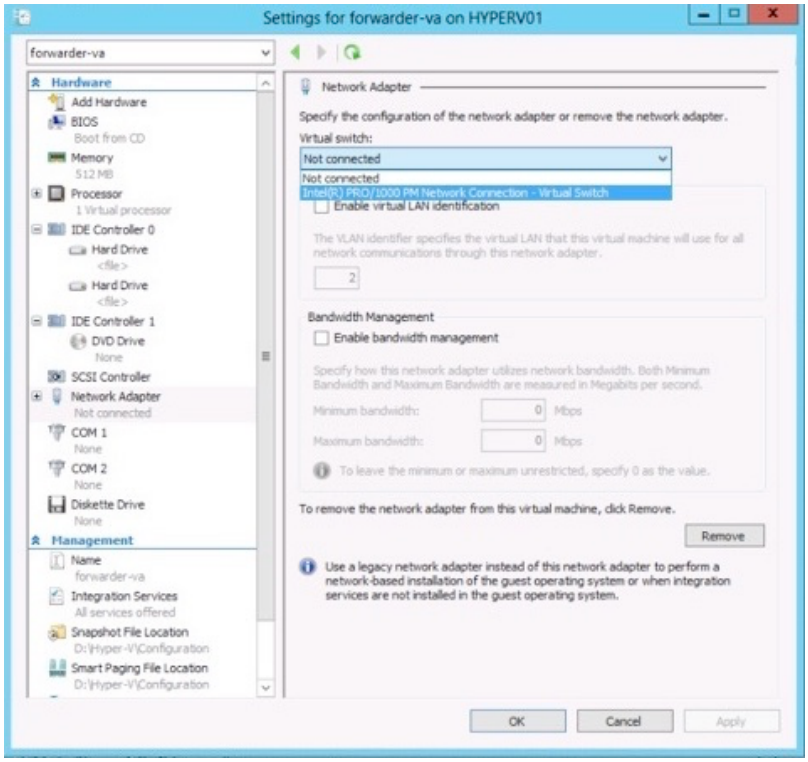
Provides instructions for step 4 - select network adapter. In the Hyper-V Manager, select the virtual machine you've created, right-click and choose Settings.The T Dts Rvt Atoe7orsb Ubc Q Va Settings interface.

Procedure

1. In the Hyper-V Manager, select the virtual machine you've created, right-click and choose **Settings**.



2. Under **Hardware**, select **Network Adapter**, and then assign a virtual switch that has internet access.

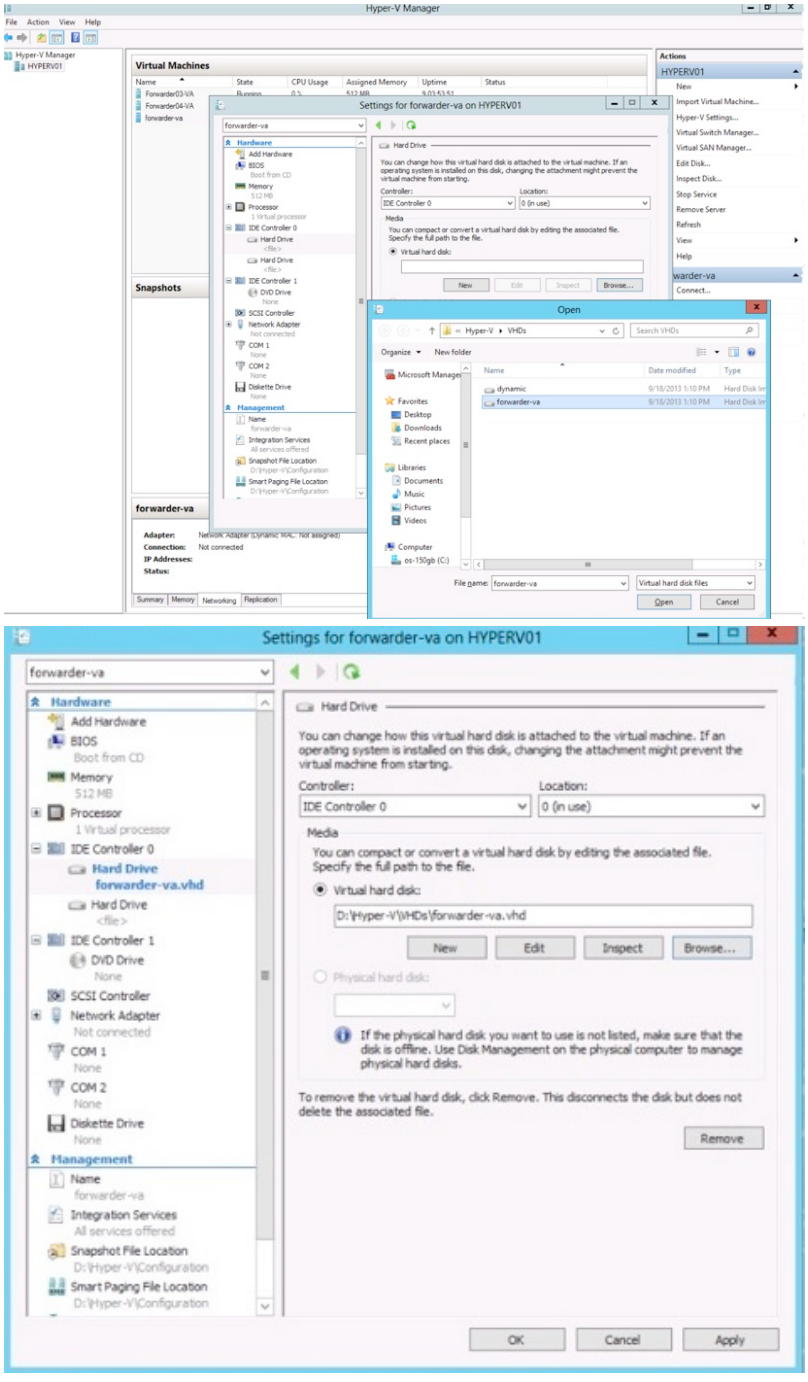


Step 5 – Select Hard Drive

Provides instructions for step 5 – select hard drive. In Settings for Hardware, select the hard drives. Ideally, they should be under the same IDE controller.

Procedure

1. In **Settings for Hardware**, select the hard drives. Ideally, they should be under the same IDE controller. For hard drive settings, browse to the Virtual Machine Configuration Folder and the first hard drive should be set to the forwarder file (Forwarder-va) and the second hard drive should be set to the dynamic (Dynamic) file.

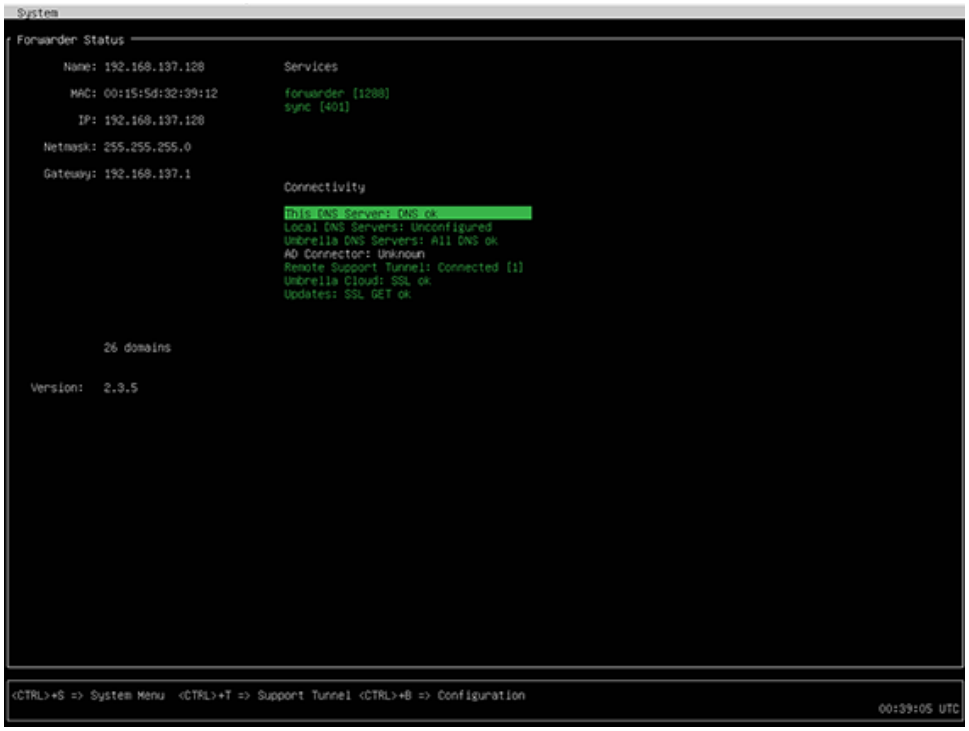


2. Click **Apply**.

Step 6 – Power on the Virtual Machine

Describes step 6 – power on the virtual machine. If all is well, you'll see the Virtual Appliance console screen. For information about configuring VAs, see Configure Virtual Appliances.

If all is well, you'll see the Virtual Appliance console screen. For information about configuring VAs, see Configure Virtual Appliances.



Step 7 – Repeat for the Second Virtual Appliance

Describes step 7 – repeat for the second virtual appliance. Two VAs are required per Umbrella site. It is critical that these VAs are not cloned or copied in any way. Each VA must be set up and configured manually.

Two VAs are required per Umbrella site. It is critical that these VAs are **not** cloned or copied in any way. Each VA must be set up and configured manually.

To build your second VA, repeat procedures starting at 2. Import Virtual Appliance.

Deploy VAs in VMware

Describes deploying vas in vmware. Deploy Cisco Secure Access Virtual Appliances (VAs) in VMware. You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Deploy Cisco Secure Access Virtual Appliances (VAs) in VMware.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Configure Authentication for the Virtual Appliances

Describes configuring authentication for the virtual appliances. Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization.

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** button only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Basic knowledge of VMware ESXi. For more information, see the VMware documentation.

Procedure

Describes procedure. Step 1 – Download OVF Template Step 2 – Deploy OVF Template Step 3 – Deploy a Second Virtual Appliance Step 4 – Power on the Virtual Machines

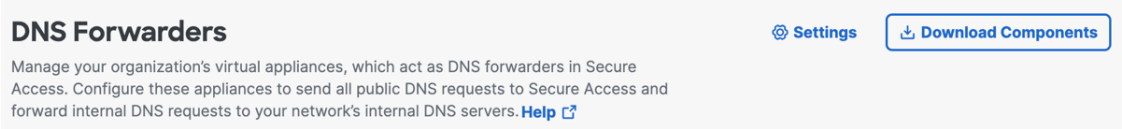
- Step 1 – Download OVF Template
- Step 2 – Deploy OVF Template
- Step 3 – Deploy a Second Virtual Appliance
- Step 4 – Power on the Virtual Machines

Step 1 - Download OVF Template

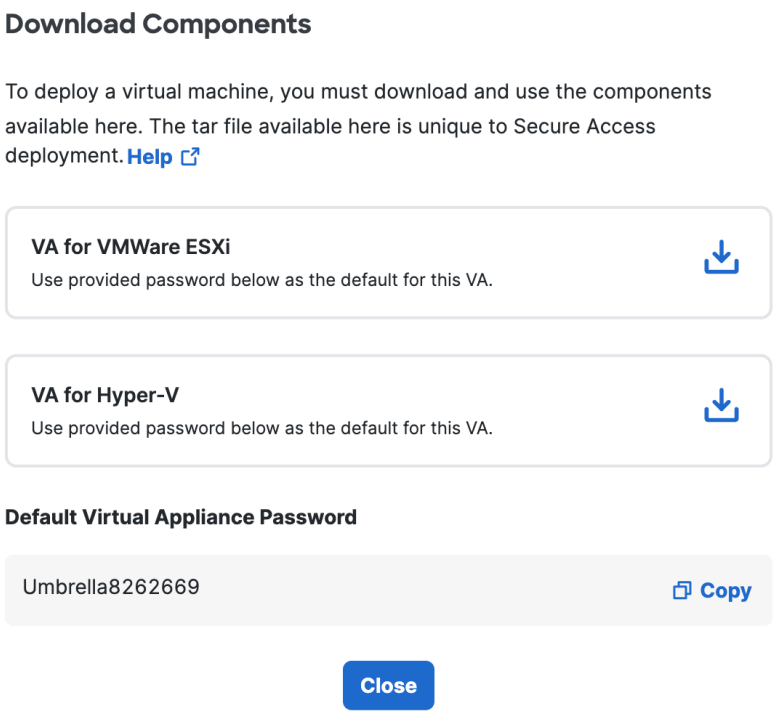
Provides instructions for step 1 – download ovf template. Navigate to Connect DNS Forwarders and click Download Components. Click Download for VA VMWare ESXi.The Secure Access Download Va Images interface.

Procedure

1. Navigate to **Connect** > **DNS Forwarders** and click **Download Components**.



2. Click **Download** for **VA VMWare ESXi**.



Umbrella generates and downloads a .tar file unique to your deployment. This tar file includes:

- an .ovf template containing the virtual hard disks that need to be deployed on VMware
- a signature file
- a Cisco public certificate to validate the signature
- a readme file

3. Extract the contents of the tar file using the command `tar -xvf <tar filename> -C <Destination folder>`.

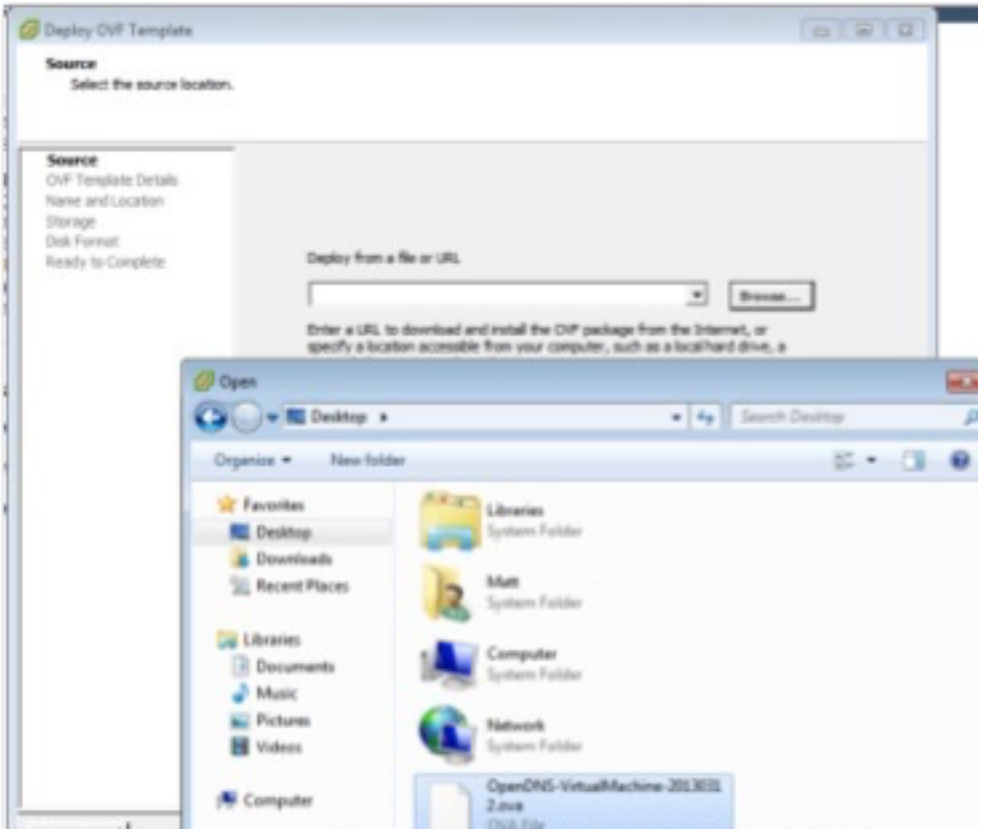
   To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. On successful signature validation, you should see a message saying “Verified OK."

Step 2 – Deploy OVF Template

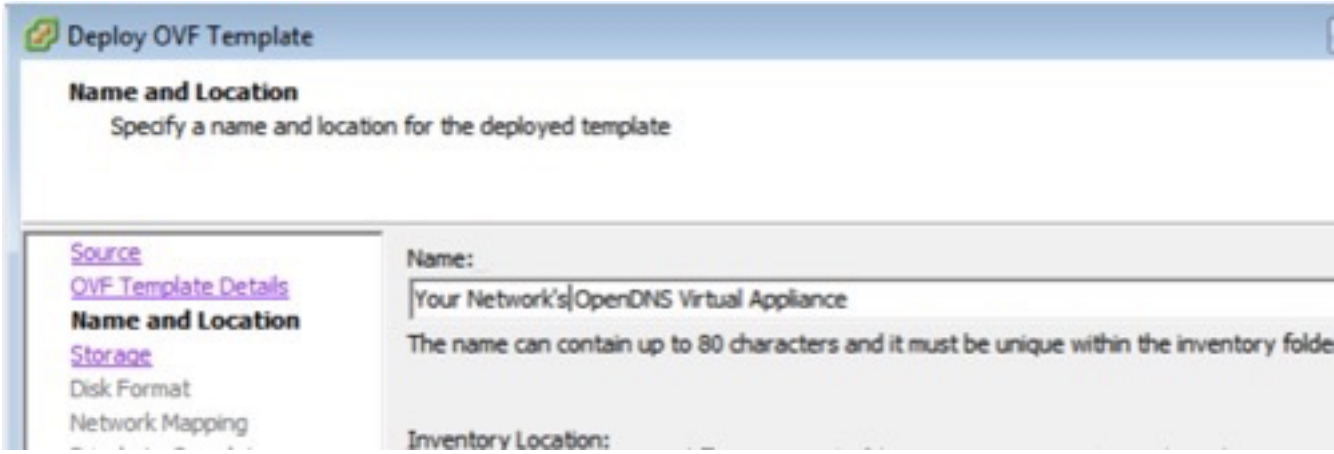
Provides instructions for step 2 - deploy ovf template.

Procedure

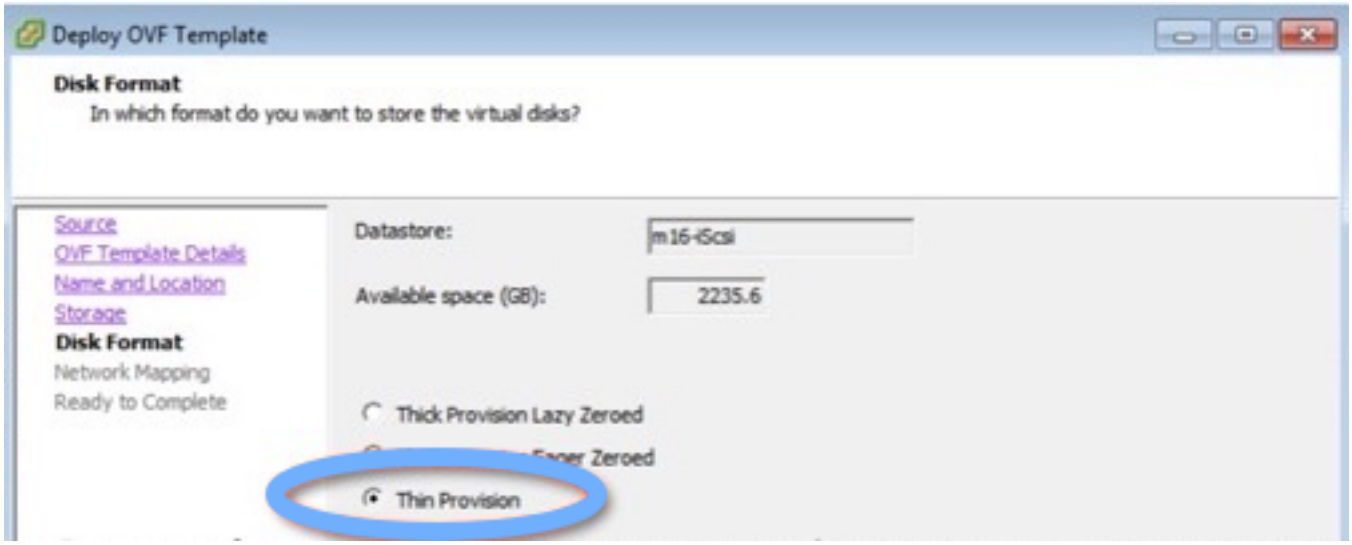
1. Log into your VMware vSphere client and select the **File** tab.
2. Click **Deploy OVF Template**, choosing the downloaded .ova template.



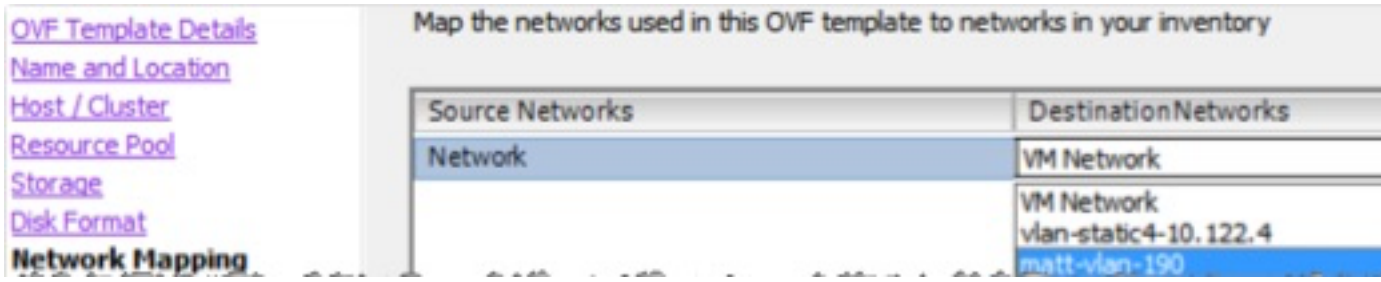
3. Follow the deployment wizard prompts, but be sure to follow these steps:
   - For the source, browse to the .ova file you just downloaded.
   - Specify a unique name and location for your VA.



4. Select the disks appropriate to your environment. It is recommended to select **Thin Provision** for the disk format, but it is not mandatory.



5. Select or map a network.



6. Click **Finish**.The system begins to deploy the VA. During the deployment, subsequent prompts update you about the status of the deployment.

Step 3 – Deploy a Second Virtual Appliance

Provides instructions for step 3 – deploy a second virtual appliance. While the first VA is deploying, repeat the previous two steps to configure your second VA. Two VAs are required per Umbrella site. It is critical that these VAs are not cloned or copied in any way.

Procedure

While the first VA is deploying, repeat the previous two steps to configure your second VA.

Note

Two VAs are required per Umbrella site. It is **critical** that these VAs are **not** cloned or copied in any way. Each VA must be set up and configured manually.

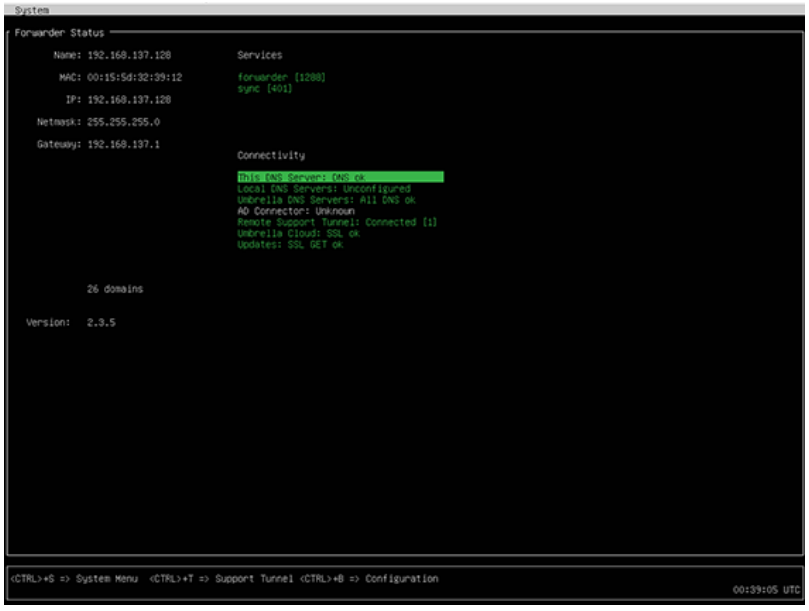


Step 4 – Power on the Virtual Machines

Provides instructions for step 4 – power on the virtual machines. If the deployment succeeded, you'll see the VA console screen. For information about configuring VAs, see Configure Virtual Appliances.

Procedure

If the deployment succeeded, you'll see the VA console screen. For information about configuring VAs, see Configure Virtual Appliances.



56 Configure Virtual Appliances

Topics:

- Configure Virtual Appliances

Describes the purpose and procedures for configure virtual appliances and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Configure Virtual Appliances

Describes configuring virtual appliances. Configure your Cisco Secure Access Virtual Appliances (VAs) deployed in VMWare and Hyper-V. Deploy Virtual Appliances in your environments. For more information, see Deploy Virtual Appliances.

Configure your Cisco Secure Access Virtual Appliances (VAs) deployed in VMWare and Hyper-V.

Prerequisites

- Deploy Virtual Appliances in your environments. For more information, see Deploy Virtual Appliances.

Enter Configuration Mode on a VA Deployed on VMware and Hyper-V

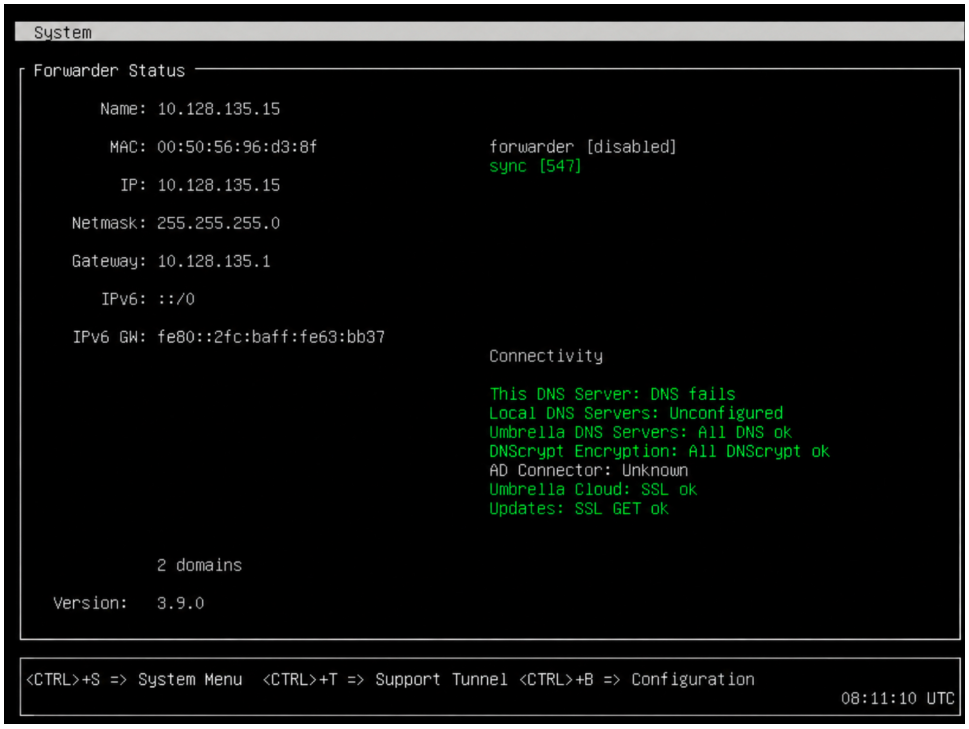
Provides instructions for entering configuration mode on a va deployed on vmware and hyper-v. When you open the VA in your preferred hypervisor's console, and you'll see a configuration menu. As seen in the lower right corner, the system time is set to UTC by default.

When you open the VA in your preferred hypervisor's console, and you'll see a configuration menu. As seen in the lower right corner, the system time is set to UTC by default. This will not affect your DNS, network, or hypervisor.

> **Note**
>
> To access the VA console efficiently, use a native application (such as VMware vSphere Client, VMware Remote Console, or RDP).

If you have deployed the VA in a network that supports DHCP, the VA is automatically assigned a DHCP IP address and registers to Secure Access using this IP. This IP address appears on the configuration and in Secure Access.

This screenshot shows the VA start menu in an IPv4 only deployment with IPv4 addressing details..



Procedure

1. Press **Ctrl+B**. When prompted, provide a password for configuration changes.

   Tip

   Using the numeric lock or the number pad on your keyboard may return incorrect characters. You must change the password when you enter Configuration Mode. Your password must be at least eight characters long, include at least one lowercase character, one uppercase character, one digit, and one special character. Your password cannot be the same as your last password.

   Note

   `Umbrella<OrgID>` should be set as the default password for the VA. Your Org ID can be retrieved from the dashboard URL in your address bar. For example, if your Org ID is `2406960`, the default password for the VA would be `Umbrella2406960`. For more information about the Secure Access Org ID, see Find Your Organization ID.

2. Optionally, enable remote configuration of this VA over SSH, enter:

   ```
   config va ssh enable
   ```

3. If you have enabled SSH, you can now remotely connect to the VA over SSH and enter Configuration Mode after authentication. Enter:

   ```
   ssh vmadmin@<VA's IP address>
   ```

   Note

   Configuration mode does not support concurrent access by more than two users.

Configure the VA Through Configuration Mode

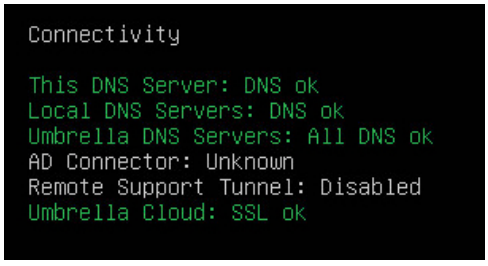
Describes configuring the va through configuration mode. Configuring the VA involves configuring the name, IP details, and local DNS servers. It is mandatory to configure the name and IP, netmask, and gateway (unless already configured).

Configuring the VA involves configuring the name, IP details, and local DNS servers. It is mandatory to configure the name and IP, netmask, and gateway (unless already configured). Failing to do this results in the VA not being able to register to Secure Access.

> **Note**
>
> Active Directory integration is currently not supported for IPv6 endpoints.

Field	Description
Name*	The name associated with the VA in Secure Access. This is a descriptive name, similar to a hostname for a computer or server. If you have multiple hypervisor hosts, appending or prepending numbers or letters to indicate the local hypervisor host is advised. 1. To configure the name, enter `config va name <name>`
IP, Netmask, and Gateway*	Give the VA a local, static IP address on the same network as your endpoints which will utilize the VAs for DNS resolution. **Note** Configuring an IPv4 address is mandatory. 1. To configure the IP, Netmask, and Gateway for the VA, enter: `config va interface<ipaddress><netmask> <gateway>`
Local DNS 1-6	Configure your local DNS servers that will receive DNS queries for internal domains. These are usually your Windows Servers with the DNS server role installed. You can enter IPv4 address here. For more information and commands to configure local DNS servers, see Local DNS Forwarding.

*Mandatory parameters for the VA.



If you have entered the Configuration Mode over SSH, to validate status, enter:

If tests complete without error, the next step is to verify that the VA syncs with Secure Access.

```
config va status
```

Configure a Second VA

Describes configuring a second va. Repeat the previous steps to configure a second VA. A second VA is required for continuous operation, high availability, and automatic upgrades.

Repeat the previous steps to configure a second VA. A second VA is required for continuous operation, high availability, and automatic upgrades.

- Do not clone the first VA. Secure Access does not recognize a cloned VA.
- Ensure that your second VA is set up manually.

> **Note**
>
> Azure AD Domain Services is currently not supported. For identity integration with the VA, the AD Connector and Domain Controllers should be deployed as VMs in Azure. Alternately, these components can be deployed on-premise provided there is an ExpressRoute or MPLS connection over which the AD Connector can communicate with the VA in Azure.

Configure Settings on VAs

Describes configuring settings on vas. Configure other settings on your Cisco Secure Access Virtual Appliances (VAs). For more information, see Prerequisites for Virtual Appliances.

Configure other settings on your Cisco Secure Access Virtual Appliances (VAs).

Prerequisites

- For more information, see Prerequisites for Virtual Appliances.

Configure Rate Limiting

Describes configuring rate limiting. You can set rate limits of DNS queries on a VA for a single IP address. Use rate limits to prevent any single endpoint from attempting to flood the VA with DNS queries and causing a Denial-of-Service on the VA.

You can set rate limits of DNS queries on a VA for a single IP address. Use rate limits to prevent any single endpoint from attempting to flood the VA with DNS queries and causing a Denial-of-Service on the VA.

Enable Rate Limits on a VA

Enable rate limits on the Virtual Appliance. Rate-limiting is off by default.

- **pps**–The number of packets accepted for each second from an individual IP. Supported values are 10 to 100,000.
- **burst**–The packet burst rate.

```
config va per-ip-rate-limit enable <pps> <burst>
```

Disable Rate Limiting

Disable rate limits on the Virtual Appliance.

```
config va per-ip-rate-limit disable
```

Check Status and Packet Drops

Check status and packet drops on the Virtual Appliance.

```
config va show
```

Configure NTP Servers

Describes configuring ntp servers. By default, VAs use Ubuntu NTP servers (ntp.ubuntu.com) as their time servers. You can configure your VAs to use other NTP servers.

By default, VAs use Ubuntu NTP servers (**ntp.ubuntu.com**) as their time servers. You can configure your VAs to use other NTP servers.

Add NTP Servers to the VA

```
config ntp add <serverIP1> <serverIP2>
```

Remove NTP Servers

```
config ntp remove <serverIP1> <serverIP2>
```

View the VA's Current NTP Servers

```
config ntp show
```

Configure DNSSEC Support

Describes configuring dnssec support. Secure Access supports DNSSEC by performing validation on queries sent from Secure Access DNS resolvers to upstream authorities.

Secure Access supports DNSSEC by performing validation on queries sent from Secure Access DNS resolvers to upstream authorities.

If your endpoints are making DNS queries with the **DNSSEC OK (DO)** bit to the VA, the default behavior of the VA is to turn off this bit before forwarding the query to Secure Access or the local DNS server.

Configure VA to Preserve the DO Bit

Describes configuring va to preserve the do bit. Configure the VA to preserve the DO bit when forwarding the DNS query to Secure Access or the local DNS server.

Configure the VA to preserve the DO bit when forwarding the DNS query to Secure Access or the local DNS server.

> **Note**
>
> The VA preserves any DNSSEC Security Resource Records in the DNS response to the endpoint.

```
config va dnssec enable
```

Turn Off the DO Bit

Describes turning off the do bit. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

```
config va dnssec disable
```

Command	Description	Notes
config va dnssec enable	Configure the VA to preserve the DO bit when forwarding the DNS query to Secure Access and/or the local DNS server.	Preserves any DNSSEC Security Resource Records in the DNS response to the endpoint.
config va dnssec disable	Disable the above configuration.	

Configure Logging to Remote Syslog Server

Describes configuring logging to remote syslog server. Virtual Appliances can forward logs to a remote syslog server. If configured, Secure Access forwards logs related to internal DNS queries, logs on upgrades and reboots of the VA, and admin audit.

Virtual Appliances can forward logs to a remote syslog server. If configured, Secure Access forwards logs related to internal DNS queries, logs on upgrades and reboots of the VA, and admin audit.

Configure the Destination of the Remote Syslog Server

Describes configuring the destination of the remote syslog server.

```
config logexport destination <server-ip-address:port> <protocol>
```

Supported Values for `<protocol>`:

- TCP, UDP, or TLS.
- If no value is specified, TCP is the default.
- If the protocol value is TCP or UDP and a port is not specified, 514 is assigned as the default port.
- If the protocol value is TLS and a port is not specified, 6514 is taken as the default port.

To forward the logs over a TLS-encrypted session, first create the certificates for the client (VA) and server (remote syslog server). The certificates can be self-signed or signed by a Root certificate authority (CA).

Add the key and certificate to the VA using the following commands:

```
config logexport key <copy the contents from keyForClientCert.pem file>
config logexport cert <copy the contents from ClientCert.pem file>
config logexport ca \<copy the contents from selfsignedCA.pem|chainCertCA.pem
 file>
```

> **Note**
>
> The CA configured in the last command should be the CA used to sign the server certificate.

Configure Log Export Internal DNS

Describes configuring log export internal dns. All internal DNS queries sent to the internal DNS server are logged at the syslog server. Logs include the date and time, the internal domain being queried and the private IP, hostname and username of the source endpoint that made the query.

All internal DNS queries sent to the internal DNS server are logged at the syslog server. Logs include the date and time, the internal domain being queried and the private IP, hostname and username of the source endpoint that made the query.

> **Note**
>
> If AD integration is not configured for the VA, the hostname and username of the source endpoint are not available.

```
config logexport enable internaldns
```

Format for internal DNS queries:

- Date
- Time
- Hostname (forwarder)
- VA Label:
  - InternalDNS
- Internal IP of source
- User AD identity of source (if a user identity is mapped to this IP else "NULL")
- Host AD identity of source (if a host identity is mapped to this IP else "NULL")
- Internal Domain being queried

Configure Log Export Enable Health

Describes configuring log export enable health. Reboots and upgrades of the VA are logged at the syslog server. Format for VA boot:

Reboots and upgrades of the VA are logged at the syslog server.

```
config logexport enable health
```

Format for VA boot:

- Date
- Time
- Hostname ("forwarder")
- VA Label:

- Health
- VA started

Format for VA upgrade:

- Date
- Time
- Hostname (forwarder)
- VA Label: Health
- VA downloaded version <x.y.z> or VA upgraded to version <x.y.z>

Configure Log Export Enable Admin

Describes configuring log export enable admin. Admin audit log (logins by admin users and config commands run on the VA) are logged at the syslog server.

Admin audit log (logins by admin users and config commands run on the VA) are logged at the syslog server.

```
config logexport enable admin
```

Format for User Login to VA:

- Date
- Time
- Hostname (forwarder)
- VA Label: Audit-Auth
  - SSH login from as <vmadmin/vmuser> succeeded/failed or "Console login as <vmadmin/vmuser> succeeded/failed

Format for Configuration change:

- Date
- Time
- Hostname (forwarder)
- VA Label: `AuditLog-Config command executed`

Configure Log Export Enable All

Describes configuring log export enable all. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Enables logging of internal DNS, health, and admin logs at the syslog server.

```
config logexport enable all
```

Configure Log Export Status

Describes configuring log export status. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Run this command to check the status of the log forwarding:

```
config logexport status
```

Turn Off Logging

Describes turning off logging. Run this command to turn off logging: You can set the feature option to internaldns, health, audit or all.

Run this command to turn off logging:

```
config logexport disable <feature>
```

Note

You can set the `feature` option to `internaldns`, `health`, `audit` or `all`.

Example:

```
config logexport disable all
```

Configure Dual-NIC Support on the VA

Describes configuring dual-nic support on the va. NIC Terminology–Throughout this section, the terms NIC, network interface, and network adapter are used interchangeably.Virtual Appliances support a dual-NIC configuration. This dual-NIC configuration is intended to enable the DMZ deployment of a VA for traffic segregation with one network interface.

Important

NIC Terminology–Throughout this section, the terms NIC, network interface, and network adapter are used interchangeably.

Virtual Appliances support a dual-NIC configuration. This dual-NIC configuration is intended to enable the DMZ deployment of a VA for traffic segregation with one network interface. The network interface is used for outbound communication and the other network interface is used for internal communication.

Dual-NIC support has only been qualified on VAs running on Hyper-V and VMware. There is no change to existing behavior if the VA is deployed with a single NIC. Configuring more than two NICs on the VA is not supported.

Configure an Existing VA to Support Dual-NIC

Provides instructions for configuring an existing va to support dual-nic. Open your existing VA in your preferred hypervisor's console or SSH to the VA.

Procedure

1. Open your existing VA in your preferred hypervisor's console or SSH to the VA.
2. Run the command to show the configuration of the VA. Ensure that the IP configured here is the IP that will be used for internal communication. This is the IP that your endpoints will use for DNS resolution.

> **Note**
>
> Before adding a secondary network adapter, save the MAC address of the existing network adapter before adding a secondary network adapter.
>
> ```
> config va show
> ```

3. Shut down the VA and add a second network adapter using your hypervisor console. This is the network adapter you will be using for your outbound communication. This should be of the same driver type as your primary network adapter.

> **Note**
>
> Some platforms may not permit the addition of a second network adapter after the VA has been created.

4. Turn the VA on, enter the Configuration mode from the console or through SSH, and run the command `config va show`. This command returns the name of the second adapter.

> **Note**
>
> Adding a second adapter when the VA is powered on may result in the adapter not being detected or the corruption of the existing configuration. The VA needs to be compulsorily shut down before adding the second adapter.

5. For the secondary adapter, assign the IP, netmask, and gateway parameters to be used for outbound (Internet) communication. Enter: `config va interface <*interface name*> <*ip address*> <*netmask*> <*gateway*>`. Verify against the MAC address of the respective adapters to ensure that the IP addresses are not misconfigured.

> **Note**
>
> You cannot direct DNS requests to the IP configured on the secondary adapter because incoming DNS traffic will be blocked on this IP.

6. Once you have saved changes, enable traffic segregation. Static routes are configured for the IP on the secondary adapter to all Secure Access destinations required for the proper functioning of the VA. Configuring additional static routes is currently not supported. Enter:

```
config va dmz enable
```

Deploy a New VA to Support Dual-NIC DMZ Mode

Provides instructions for deploying a new va to support dual-nic dmz mode. You can deploy a new VA with dual-NIC support. The configuration steps are similar to configuring an upgraded VA. You can add the secondary adapter to the VM using the hypervisor console, before powering on the VM.

You can deploy a new VA with dual-NIC support. The configuration steps are similar to configuring an upgraded VA. You can add the secondary adapter to the VM using the hypervisor console, before powering on the VM. Both adapters should be of the same driver type.

Procedure

1. Enter configuration mode on the VA and retrieve the name of both adapters. Run:

```
config va show
```

2. Configure the primary adapter and then the secondary adapter. Ensure that the primary adapter is configured with the IP that you wish to use for internal communication and that the secondary adapter is configured with the IP to be used for internet-bound communication. Run:

```
config va interface <interface name> <ip address> <netmask> <gateway>
```

3. Once both adapters are configured, enable traffic segregation. Run:

```
config va dmz enable
```

Configure Load Balancing

Describes configuring load balancing. You can configure your Virtual Appliances behind a load balancer that meets the following requirements: The DNS response from the Virtual Appliance routes through the load balancer. Thus, the response to the client comes from the address of the load balancer.

You can configure your Virtual Appliances behind a load balancer that meets the following requirements:

- The load balancer is able to inject the source IP address of the client making the query in the EDNS Client Subnet (ECS) field of the DNS request sent to the VA.
- The DNS response from the Virtual Appliance routes through the load balancer. Thus, the response to the client comes from the address of the load balancer.

This feature has specifically been qualified with the F5 BIGIP-LTM 16.1.1 version, where the F5 can inject the endpoint source IP in DNS requests that it forwards to VAs in the load balancing pool. Refer to F5 documentation on ECS injection in DNS requests when forwarding these requests to a DNS server pool.

By default, the VA does not accept DNS requests with the ECS option from any endpoint. To allow the VA to accept DNS requests with the ECS option from load balancers, the load balancer IP has to be added to the VA configuration using the following commands:

Add a Load Balancer

Describes adding a load balancer. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

```
config loadbalancer add <server-ip/prefix>
```

Remove a Load Balancer

Describes removing a load balancer. You can add a maximum of 8 load balancers to a VA. Also, add or remove a single load balancer at a time.

```
config loadbalancer remove <server-ip/prefix>
```

> **Note**
>
> You can add a maximum of 8 load balancers to a VA. Also, add or remove a single load balancer at a time.

Configure Identity Association Timeouts

Describes configuring identity association timeouts. Use the config admap command to configure association timeouts for a given IP address. You can also view or clear the AD mapping. You can only clear the mappings of an individual IP address.

Use the `config admap` command to configure association timeouts for a given IP address. You can also view or clear the AD mapping. You can only clear the mappings of an individual IP address.

Example commands:

```
config admap view <ip address>
```

```
config admap clear <ip address>
```

```
config admap set-user-timeout 28800
# This command sets the host timeout for 8 hours
```

```
config admap set-host-timeout 28800
# This command sets the host timeout for 8 hours
```

```
config admap show-timeout
```

Configure API Key Credentials for Authentication

Describes configuring api key credentials for authentication. Once you delete the Secure Access API key credentials that you created for authentication of your Virtual Appliances, the VAs have 90 days to use the existing API client key and secret.

Once you delete the Secure Access API key credentials that you created for authentication of your Virtual Appliances, the VAs have 90 days to use the existing API client key and secret. After 90 days, your VAs can not sync with Secure Access.

> **Note**
>
> Unless you have unusual circumstances, we do not recommend that you delete your Secure Access API key credentials.

Configure the Client ID and Client Secret

Describes configuring the client id and client secret. Create a new set of API client credentials in Secure Access. For more information, see Configure Authentication for Virtual Appliances.

1. Create a new set of API client credentials in Secure Access. For more information, see Configure Authentication for Virtual Appliances.

2. With your generated Secure Access API client key and secret, run the `config authcred set` command:

```
config authcred set "<client_id>:<client_secret>"
```

57 Local DNS Forwarding

Topics:

- Local DNS Forwarding

Describes the purpose and procedures for local dns forwarding and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Local DNS Forwarding

Describes local dns forwarding. Cisco Secure Access Virtual Appliances (VAs) are conditional DNS forwarders in your network, forwarding public DNS queries to Secure Access, and local DNS queries to your existing local DNS servers and forwarders, respectively.

Cisco Secure Access Virtual Appliances (VAs) are conditional DNS forwarders in your network, forwarding public DNS queries to Secure Access, and local DNS queries to your existing local DNS servers and forwarders, respectively.

When the VAs receive queries which match domains or subdomains of a local DNS zone (local domain), the VA forwards those queries to your local DNS server for resolution instead of the Secure Access public DNS resolvers. This is accomplished by defining your local domain names in Secure Access.

Important

Do not set your local DNS forwarders to point to the VAs. It is possible to create loops in DNS in this configuration and it's not recommended or supported.

Manage Domains in the VA

Describes managing domains in the va. Any DNS queries received by the VAs which match a domain on the Internal Domains list, will be forwarded to the local DNS server as described in Configure Virtual Appliances.

Any DNS queries received by the VAs which match a domain on the Internal Domains list, will be forwarded to the local DNS server as described in Configure Virtual Appliances.

The following domains/zones are **pre-populated** and do *not* need to be added:

- ***RFC1918*** –non-publicly routable address spaces used only for reverse DNS on internal networks. All local IP address space for reverse lookups (PTR records) is covered with this entry. Adding **in-addr.arpa** reverse lookup zones are not needed.
- ***.local*** –Any domain name with a TLD of .local.

You have a choice of what type of identities are set to respect these internal domains:

- All Sites–Covers all requests that are made through a VA.
- Sites listed under All Sites–Covers requests only made through VAs deployed in the selected sites.
- All Devices–Covers all requests that are made through a roaming device.

Which domains should be added?

Provides instructions for which domains should be added?. Any domain name which has a forward lookup zone on your local DNS servers must be added, along with any domains that are configured with conditional forwarders.

Any domain name which has a **forward lookup zone** on your local DNS servers must be added, along with any domains that are configured with conditional forwarders. If you already know which domains to add, skip the Add A and PTR Records for the VAs section.

On Windows Server, this information is located in the DNS Manager tool.

Procedure

1. Open the DNS Manager (**Start** > **Run** and type "dnsmgmt.msc").

2. Expand the **Server name** and **Forward Lookup Zones** sections. Any domains listed here are treated as local by your local DNS forwarders. Add these domains to your internal domains list in Secure Access. This is a critical part of the setup process.
3. If any public IPs are in use as local IPs, also add the **Reverse Lookup Zone** of any public IPs which have local DNS records attached. RFC-1918 reverse lookup zones are included by default. These are entered in the in-addr.arpa format.

> **Note**
>
> Be aware that it can take up to 10 minutes for the virtual appliance to synchronize with changes you make to the Internal Domains list.

(Optional) Add A and PTR Records for the VAs

Describes (optional) add a and ptr records for the vas. Adding A and PTR records for the VAs makes them easy to identify within your network topology, including firewall and security appliance logs.

Adding A and PTR records for the VAs makes them easy to identify within your network topology, including firewall and security appliance logs.

If you're unfamiliar with adding A and PTR records, see the Microsoft articles:

- Add a PTR record
- Add a host (A) record

After adding A and/or PTR records, verify the records:

Verify PTR record

From a command prompt, enter:

```
nslookup <VA IP ADDRESS>
```

You should see the record in the last line of the result.

```
nslookup 192.168.1.10

    Server:192.168.1.1
    Address:192.168.1.1#53
    Non-authoritative answer:
    9.168.192.in-addr.arpaname = \[va01.corp.domain.com\]
```

Verify A record From a command prompt, enter:

```
nslookup <VA HOSTNAME>
```

You should see the record in the last line of the result.

```
nslookup va01.corp.domain.com

   Server: 192.168.1.1
    Address: 192.168.1.1#53
    Non-authoritative answer:
    Name: va01.corp.domain.com
    Address: 192.168.1.9
```

Configure Local DNS Servers on the VA

Describes configuring local dns servers on the va. You can configure the VA to send queries for local domains to any local DNS server. You can also selectively forward DNS queries for specific local domains to specific local DNS servers.

You can configure the VA to send queries for local domains to any local DNS server. You can also selectively forward DNS queries for specific local domains to specific local DNS servers.

Use the following commands to configure the VA to send queries for local domains to local DNS servers:

Task	Command	Note
Configure up to 6 local DNS servers	**config localdns add <ip>**	The command must be entered individually for each local DNS server. The command does not take multiple IP inputs.
Remove a configured local DNS server	**config localdns remove <ip>**	
Add a local DNS server and assign specific internal domains to this server	**config localdns add <ip of local DNS server><domain1><domain2_domainN>**	Add Internal domains to Secure Access. Requests for other internal domains will not be forwarded to these local DNS servers.
Show the list of internal DNS servers and any domain mappings against these servers	**config localdns show**	

> **Note**
>
> If you are assigning specific domains to specific local DNS servers, be sure to add at least one local DNS server with no domain assignment so that it can support queries for all other internal domains.

Examples

Describes examples. You can also combine the above features to have some local domains redirected to specific local DNS servers and other domains redirected to the remaining local DNS servers.

You can also combine the above features to have some local domains redirected to specific local DNS servers and other domains redirected to the remaining local DNS servers.

Command	Outcome
config localdns add 209.165.200.229 internaldomain1.com	DNS queries for internaldomain1.com will now be forwarded to 209.165.200.229 and 209.165.200.229.
config localdns add 209.165.200.229 internaldomain1.com internaldomain2.com	DNS queries for internaldomain2.com will now be forwarded to 209.165.200.229
config localdns add 209.165.200.229	DNS queries for all other internal domains will be forwarded to 209.165.200.229

58 Test Virtual Appliance Deployments

Topics:

- Test Virtual Appliance Deployments

Describes the purpose and procedures for test virtual appliance deployments and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Test Virtual Appliance Deployments

Describes testing virtual appliance deployments. After you deploy the Cisco Secure Access Virtual Appliances (VAs) in your environment and set up internal domains in Secure Access, we recommend that you test your Virtual Appliances.

After you deploy the Cisco Secure Access Virtual Appliances (VAs) in your environment and set up internal domains in Secure Access, we recommend that you test your Virtual Appliances.

To begin enforcing your DNS-layer security settings, DNS traffic from the endpoints on your network must exclusively use the VAs as a DNS forwarder.

Prerequisites

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

Resolve Public and Local DNS Queries

Describes resolve public and local dns queries. Before configuring endpoints to utilize the VAs for DNS traffic, ensure that the VAs are capable of resolving public and local DNS queries. The simplest test is to open a command prompt from a local endpoint and run the nslookup command:

Before configuring endpoints to utilize the VAs for DNS traffic, ensure that the VAs are capable of resolving public and local DNS queries. The simplest test is to open a command prompt from a local endpoint and run the **nslookup** command:

nslookup opendns.com <VA IP Address>

```
nslookup opendns.com. 192.168.10.1

    Server:   192.168.10.1
    Address: 192.168.10.1#53

    Non-authoritative answer:
    Name: opendns.com
    Address: 67.215.92.218
```

- If the lookup times out, confirm that you have met firewall requirements. For more information, see Prerequisites for Virtual Appliances.
- If the test succeeds, perform the same test again, but this time with a local resource, such as a domain controller or mail server.

nslookup dc01.localdomain.corp. <VA IP Address>

```
nslookup dc01.localdomain.corp.

    Server:  192.168.10.1
    Address: 192.168.10.1#53

    Non-authoritative answer:
    Name: dc01.localdomain.corp
    Address: 192.168.10.47
```

If the result is something other than expected, ensure the domain was added as an internal domain in Secure Access.

When deploying the VA, we recommend the following for DNS configuration on any internal DNS servers:

- On the DNS server adapter settings, use the loopback address (127.0.0.1) so that the server will use itself for DNS resolution. The second entry should be another internal DNS server.

- On the forwarder settings of the DNS server, we recommend using the Secure Access Anycast IPs (18.252.251.72/18.254.118.193) rather than the virtual appliance IPs. This limits the ability to see the source IP when viewing reports but avoids any problems with DNS loops if there is a misconfiguration on either the VA or internal DNS server.
- If the server also acts as a mail server, the best option is to point to your ISP's DNS servers or other recursive resolvers such as those provided by your ISP.

Test with Endpoints

Describes testing with endpoints. Before sending most or all of your network's DNS traffic to the VAs, testing with several endpoints is highly recommended. First, change an endpoint's DNS settings to the IPs of the VAs, and then verify the following:

Before sending most or all of your network's DNS traffic to the VAs, testing with several endpoints is highly recommended. First, change an endpoint's DNS settings to the IPs of the VAs, and then verify the following:

- **Local and Remote DNS is functioning**–Ensure that local resources, internet resources, and applications are working as expected; this includes cloud-based applications, local websites, and commonly-used resources on the internet in general.
- **Verify in the Secure Access Reports**–Within a few minutes of changing DNS on an endpoint, you should start seeing traffic containing the Internal IP address in the Secure Access reports.

Example.com	Allowed	Software/Technology	Vancouver	192.0.2.1	192.0.2.254
Example.org	Allowed	Software/Technology,...	forwarder04....	198.51.100.1	198.51.100.254
Example.net	Allowed	Software/Technology	Townsend	198.51.100.1	198.51.100.254
Example2.net	Allowed	Software/Technology,...	Townsend	198.51.100.1	198.51.100.254

Secure Access recommends testing for between two and five days with several computers, preferably from different areas of your organization, before switching all production traffic to the VAs.

If DNS fails to resolve after modifying your DNS settings, confirm that you have met the network requirements. For more information, see Prerequisites for Virtual Appliances.

Transition Production Traffic

Provides instructions for transition production traffic. After successful testing, begin utilizing the VAs for production DNS traffic.The Secure Access VAs must be the only servers listed as DNS servers. Using a mixture of the VAs and other types of DNS servers is not supported.

After successful testing, begin utilizing the VAs for production DNS traffic.

Important

The Secure Access VAs must be the **only** servers listed as DNS servers. Using a mixture of the VAs and other types of DNS servers is not supported.

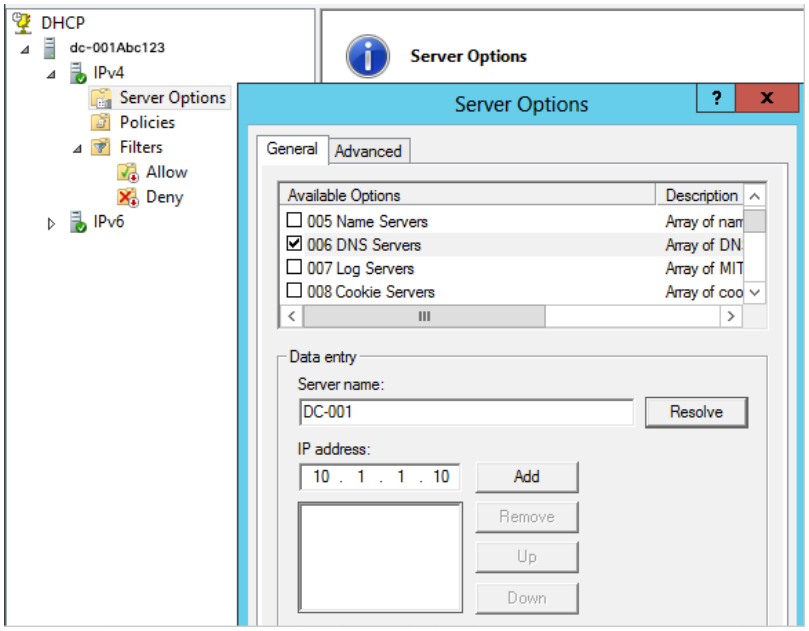
In most network environments using Windows Server, local IP addressing is handled through the **DHCP Manager**. To update your endpoints' DNS settings to point to the VAs, change the DNS Servers in your DHCP scope options.

Procedure

1. Open **DHCP Manager** and navigate to **Start** > **Administrative Tools** > **DHCP**.
2. Select IPv4 or specific scope, if applicable.
3. Right-click Server Options or Scope Options.

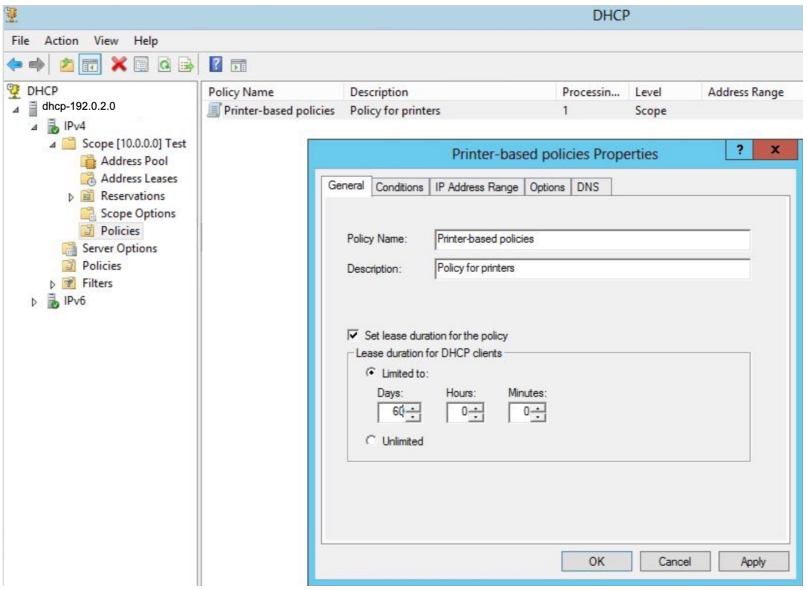
4. Select **006 DNS Servers**, *remove***ALL** the existing local DNS servers, and *add* the IP addresses of the VAs.

What to do next



The VAs must be the **only** DNS servers in this list. It is not possible to use a mixture of VAs and other DNS servers.

After updating the DNS Servers in the DHCP options, wait for the DHCP leases on the endpoints to expire and see the new changes. In most cases, DHCP lease durations are seven days or less, but sometimes may be set to higher values. We recommend verifying the DHCP lease duration in the **DHCP Manager**.



Unfortunately, there is no easy way to force an immediate DHCP lease renewal. One method is to use a **Group Policy Object** to deploy and execute a *batch* file with the `ipconfig /renew` command in it; this would cause the endpoints to recognize the VAs as their DNS servers.

59 SNMP Monitoring for Virtual Appliances

Topics:

- SNMP Monitoring for Virtual Appliances

Describes the purpose and procedures for snmp monitoring for virtual appliances and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

SNMP Monitoring for Virtual Appliances

Describes snmp monitoring for virtual appliances. The Cisco Secure Access Virtual appliances (VAs) support the Simple Network Management Protocol (SNMP), including versions SNMPv2c and SNMPv3. You can configure and enable SNMP in a VA to monitor the health of the VA and provide connectivity statistics.

The Cisco Secure Access Virtual appliances (VAs) support the Simple Network Management Protocol (SNMP), including versions SNMPv2c and SNMPv3. You can configure and enable SNMP in a VA to monitor the health of the VA and provide connectivity statistics. SNMP monitoring on a VA is disabled by default.

Enable SNMP Monitoring

Describes enabling snmp monitoring. In the Secure Access VA, the SNMP configuration supports the SHA-1, DES-128, and AES-128 algorithms. Configure SNMPv2 with the config snmp command, for example:

In the Secure Access VA, the SNMP configuration supports the SHA-1, DES-128, and AES-128 algorithms.

SNMPv2.x

Configure SNMPv2 with the `config snmp` command, for example:

```
config snmp configure -v2 <options> <args>
```

If your VA uses SNMP version 2.3 or earlier, configure SNMP with the `support snmp` command, for example:

```
support snmp <options> <args>
```

SNMPv3

When you configure SNMPv3 in your VA, provide a `username` and `password`. All other parameters are optional.

Configure SNMPv3 with the `config snmp` command, for example:

```
config snmp configure -v3 <options> <args>
```

Privacy Password

The SNMP privacy password is a string that can include 8-255 alphanumeric characters.

> **Note**
>
> The SNMP privacy password can not include special characters.

Configure SNMP in Secure Access Virtual Appliance

Provides instructions for configuring snmp in secure access virtual appliance. Enter the Configuration Mode on the VA. Use the configure option with the SNMP command. See the SNMP Command Syntax for the list of command-line arguments.

Procedure

1. Enter the Configuration Mode on the VA. Use the `configure` option with the SNMP command. See the SNMP Command Syntax for the list of command-line arguments.
2. Enable SNMP monitoring.`config snmp enable`

3. Enter **exit** to return to the VA console.

SNMP Command Syntax

Describes snmp command syntax. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

```
 Usage: config snmp <options> <args>

        The options parameter must be one of the following: configure | enable
 | disable | status

         configure      -v2 \[ -c '<community string>' \]
                            Enables SNMP v2.
                            * c - Community string; The default Community
string is 'public'.
                        -v3 -u '<username>' -p '<password>' \[-a [MD5|SHA\]
-x \[AES|DES\] -X \[password\]]
                            Enables SNMP v3 with username and password.
                           * u - Username can include at most 32 alphanumeric
 characters.
                            * p - Password can include 8-12 alphanumeric
characters.
                            * a - Optional password hash algorithm; Default
SHA.
                            * x - Optional encryption algorithm; Default AES.
                            * X - Privacy password is used with the AES
algorithm.
                                  The privacy password can include 8-255
alphanumeric characters.
                                  Special characters are not supported.

         enable         Enable SNMP.
         disable        Disable SNMP.
         status         Show the SNMP service status and Version information.
         -h, --help     Display this usage information.
```

About SNMP Monitoring

Describes about snmp monitoring. The Secure Access VA listens on port 161 for SNMP queries. The VA supports SNMP monitoring of:

The Secure Access VA listens on port 161 for SNMP queries. The VA supports SNMP monitoring of:

- Health statistics–CPU, load, memory, disk space, and status.
- Connectivity statistics–Connectivity to Secure Access resolvers, connectivity to the local DNS servers, connectivity to the Active Directory (AD) connector, and connectivity to the Secure Access API.

Standard OIDs Supported by the Virtual Appliance

Describes standard oids supported by the virtual appliance. AWS does not support monitoring the VA's disk usage with OIDs. Virtual Appliances support querying of the system OIDs 1.3.6.1.2.1.1.1 to 1.3.6.1.2.1.1.7.

> **Note**
>
> AWS does not support monitoring the VA's disk usage with OIDs.

Information	OID	Notes
Load	UCD-SNMP-MIB::laTable Load-1 (1 minute load): .1.3.6.1.4.1.2021.10.1.3.1 Load-5 (5 minute load): .1.3.6.1.4.1.2021.10.1.3.2 Load-15 (15 minutes load): .1.3.6.1.4.1.2021.10.1.3.3	If the five minute load is consistently greater than .75 of the number of processor cores, the VA is running short of processing power.
CPU	UCD-SNMP-MIB:systemStats Percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0 Percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0 Percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0	
Memory Utilization	UCD-SNMP-MIB::memory Available swap: .1.3.6.1.4.1.2021.4.4.0 Total swap: .1.3.6.1.4.1.2021.4.3.0	If the ratio of Available swap to Total swap is consistently lower than 0.5, the VA is running low on memory.
Disk Usage	Percentage of space used on data portion of disk: .1.3.6.1.4.1.8072.1.3.2.4.1.2.9.100.105.115.107.117.49.53.97.103.101.1	If this value is consistently greater than 0.8, the VA may be running out of disk space.

> **Note**
>
> Virtual Appliances support querying of the system OIDs **1.3.6.1.2.1.1.1** to **1.3.6.1.2.1.1.7**.

Extended OIDs Supported by the Virtual Appliance

Describes extended oids supported by the virtual appliance. The asterisk (*) denotes an OID which returns the throughput of the VA–the number of queries handled per second.

Information	OID
VA status (dns)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.7.116.104.105.115.100.110.115.1
Connectivity to Secure Access resolvers (dns)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.3.100.110.115.1
Connectivity to local DNS servers (localdns)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.8.108.111.99.97.108.100.110.115.1
Connectivity to Secure Access (cloud)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.5.99.108.111.117.100.1
Connectivity to AD connectors (ad)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.2.97.100.1
Queries per second over last 5 minutes*	.1.3.6.1.4.1.8072.1.3.2.4.1.2.4.113.112.115.53
Queries per second over last 15 minutes*	.1.3.6.1.4.1.8072.1.3.2.4.1.2.5.113.112.115.49.53

The asterisk (*) denotes an OID which returns the throughput of the VA—the number of queries handled per second.

For the first 5 OIDs in the table above, search for the following sub-strings in the output:

- **green**—Indicates a status of Okay.
- **red**—Indicates a status of Not Okay.
- **yellow**—indicates a status of Partially Okay.
- **white**—indicates a status of Not Configured.

> **Note**
>
> If an SNMP probe against any of these OIDs results in a timeout, we recommend that you increase the timeout value when issuing the probe.

60 Troubleshoot Virtual Appliances

Topics:

- Troubleshoot Virtual Appliances

Describes the purpose and procedures for troubleshoot virtual appliances and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Troubleshoot Virtual Appliances

Describes troubleshooting virtual appliances. Log in to your Cisco Secure Access Virtual Appliance (VA) to diagnose error conditions on the Virtual Appliance.

Log in to your Cisco Secure Access Virtual Appliance (VA) to diagnose error conditions on the Virtual Appliance.

Prerequisites

A username and password to sign in to your Virtual Appliance.

Reset a Virtual Appliance's Password

Describes resetting a virtual appliance's password. You can reset the password for a Virtual Appliance in Secure Access. For more information, see Manage DNS Forwarders: Reset Password.

You can reset the password for a Virtual Appliance in Secure Access. For more information, see Manage DNS Forwarders: Reset Password.

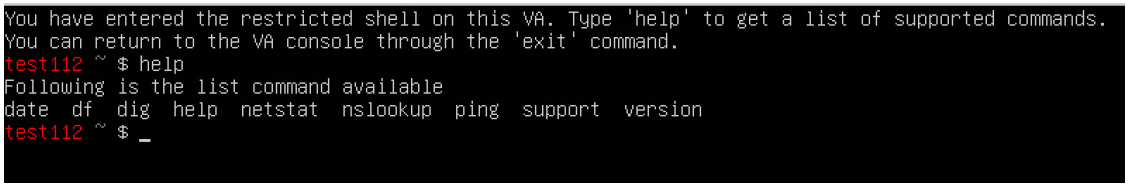
Use Configuration Mode to Troubleshoot

Provides instructions for using configuration mode to troubleshoot. The VA allows basic troubleshooting commands to be executed using the Configuration Mode.

The VA allows basic troubleshooting commands to be executed using the Configuration Mode.

Procedure

1. To enter the Configuration Mode, on the VA console, press **Ctrl+B**. You can also enter the Configuration Mode by initiating an SSH connection to the VA.



2. To view a list of supported commands in the restricted shell, enter **help**.
3. To return to the VA console, type **exit**.

What to do next

If the VA console crashes, the VA automatically enters the restricted shell.

Troubleshoot Intermittent DNS Resolution Failures on a VA Deployed on Azure

Describes troubleshooting intermittent dns resolution failures on a va deployed on azure. If you have deployed the VA on Azure as a stand-alone virtual machine (VM) without a public IP address, you might experience intermittent DNS resolution issues when heavy DNS traffic is directed at the VA.

If you have deployed the VA on Azure as a stand-alone virtual machine (VM) without a public IP address, you might experience intermittent DNS resolution issues when heavy DNS traffic is directed at the VA. This is due to SNAT port exhaustion on virtual machines deployed to Azure (such as the VA) because Azure only pre-allocates 1024 UDP ports

for standalone VMs without a public IP address. To address this issue, you may either need to assign a public IP to each VA or deploy VAs behind a public Standard Load Balancer in Azure.

Note: If you are assigning a public IP to a VA, make sure that there are no inbound port rules for this VA that allow inbound access from the internet.

Troubleshoot DNS Resolution in Configuration Mode

Describes troubleshooting dns resolution in configuration mode. The nslookup command can be used to test DNS queries on the VA. This test reflects how a users' DNS lookups will be answered and is subject to internal domains routing and other processing on the VA.

The **nslookup** command can be used to test DNS queries on the VA. This test reflects how a users' DNS lookups will be answered and is subject to internal domains routing and other processing on the VA.

You can specify a server IP address as a parameter for **nslookup**. This is useful for testing a Local DNS server or the Secure Access cloud directly. These tests bypass the VA software.

Troubleshoot DNS Resolution Failures Behind a Firewall

Describes troubleshooting dns resolution failures behind a firewall. The VA offers DNSCrypt functionality that protects the content of your DNS queries. This functionality may be blocked by your firewall.

The VA offers DNSCrypt functionality that protects the content of your DNS queries. This functionality may be blocked by your firewall.

If you are using the Cisco ASA firewall, you can see an indication of this in the ASA log. For example:

```
Dropped UDP DNS request from inside:192.168.1.1/53904 to
outside-fiber:18.254.118.193/53; label length 71 bytes exceeds protocol limit
 of 63 bytes
```

DNS resolution is not affected by this blocking, but your DNS queries are not fully protected.

To address this, ensure that your firewall allows outbound queries on port 443 and 5353 for both TCP and UDP to the Secure Access resolver IP addresses as mentioned in the Pre-requisites section.

61 PIV-CAC Support

Topics:

- PIV-CAC Support

Describes the purpose and procedures for piv-cac support and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

PIV-CAC Support

Provides instructions for piv-cac support. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

The purpose of this feature is to replace the common password-based SSH login with individual smart card-based public key authentication for each administrator and to allow multiple smart cards to be used on the SSH client, passing only the current card's authentication while rejecting others.

To enable PIV-CAC support:

Procedure

1. Enter Configuration Mode on a VA Deployed on VMware or Hyper-V.

   When you open the VA in your preferred hypervisor's console, you will see a configuration menu. The system time is set to UTC by default. This will not affect your DNS, network, or hypervisor. If you have deployed the VA in a network that supports DHCP, the VA is automatically assigned a DHCP IP address and registers to Umbrella using this IP. This IP address appears on the configuration as well as the Umbrella dashboard.

2. Press **Ctrl+B** and when prompted, provide a password for configuration changes.

   > **Note**
   >
   > Using the numbers lock or the number pad on your keyboard may return incorrect characters. You must change the password when you enter Configuration Mode. Your password must contain a minimum of eight characters and include a minimum of one lowercase character, one uppercase character, one digit, and one special character. Your new password cannot be the same as your last password.

   > **Note**
   >
   > Umbrella<*OrgID*> should be set as the default password for the VA. Your Org ID can be retrieved from the dashboard URL in your address bar. For example, if your Org ID is `2406960`, the default password for the VA would be `Umbrella2406960`. For more information about the Umbrella Org ID, see Find Your Organization ID.

3. Optionally, enable remote configuration of this VA over SSH by entering **config va ssh enable**.
4. If you have enabled SSH, you can now remotely connect to the VA over SSH and enter Configuration Mode after authentication. Enter **ssh vmadmin@<VA's IP address>**.

   > **Note**
   >
   > Configuration mode does not support concurrent access by more than two users.

5. Once SSH is enabled, only password based authentication is supported by default.
6. To use PIV-CAC in VA, enable Public-Key based authentication by entering config ssh publickey enable. Once enabled, you can add the public keys from PIV-CAC cards by entering **config ssh add <public-key>**.

7. You can now remotely connect to the VA over SSH using PIV-CAC smart cards and enter Configuration Mode after authentication. Enter **ssh vmadmin@<VA's IP address>**. (Assuming Client side configuration is done to use PIV-CAC for authenticating with Servers)
8. If needed, you can disable the password based authentication to VA by entering **config ssh password disable**. This will make sure only authorized PIV-CAC users can login into VA.

> **Note**
>
> Disabling both authentication modes cannot be done. Ensure that a minimum of one public key added in VA is a VALID key. If password based authentication is disabled, and if the keys added in VA are not valid, then User cannot access VA anymore and it cannot be recovered as vmadmin is the only user login supported in VA.

Part III

Cisco Secure Client

Topics:

- Get Started with Cisco Secure Client
- Manage Client-based Zero Trust Access from Mobile Devices
- Manage Zero Trust Access on Cisco Secure Client
- Manage Virtual Private Networks on Cisco Secure Client
- Manage Internet Security on Cisco Secure Client

62 Get Started with Cisco Secure Client

Topics:

- Download Cisco Secure Client
- Install the Root Certificate for All Browsers
- Install the Cisco Secure Client

Introduces get started with cisco secure client. Cisco Secure Client provides security to user devices on any network from any location. User devices can connect to private resources through Zero Trust Access or VPNs, or access internet resources protected by the Cisco Secure Access DNS-layer security and web security.

Cisco Secure Client provides security to user devices on any network from any location. User devices can connect to private resources through Zero Trust Access or VPNs, or access internet resources protected by the Cisco Secure Access DNS-layer security and web security.

Secure Client manages the endpoint security on user devices in your organization. Secure Client ensures that both Windows and macOS devices have a uniform, continuous security experience. For more information about Secure Client, see Cisco Secure Client At-a-Glance.

Important

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

Secure Client features:

- Endpoint compliance
- User identity verification and device communications managed by Zero Trust Access, VPNs, and internet security, including roaming protection
- Threat protection
- Network and identity visibility
- Inspection service

To get started, download the Secure Client pre-deployment package on the user devices in your organization.

- Download the Cisco Secure Client
- Install the Cisco Secure Client
- Manage Internet Security on Cisco Secure Client
- Manage Zero Trust Access on Cisco Secure Client
- Manage Virtual Private Networks on Cisco Secure Client

Download Cisco Secure Client

Describes downloading cisco secure client. Your options for downloading the Cisco Secure Client pre-deployment package in Secure Access. Option 1: Download any version of Secure Client using the link in Secure Access to Cisco Software Central.

This topic explains your options for downloading the Cisco Secure Client pre-deployment package in Secure Access.

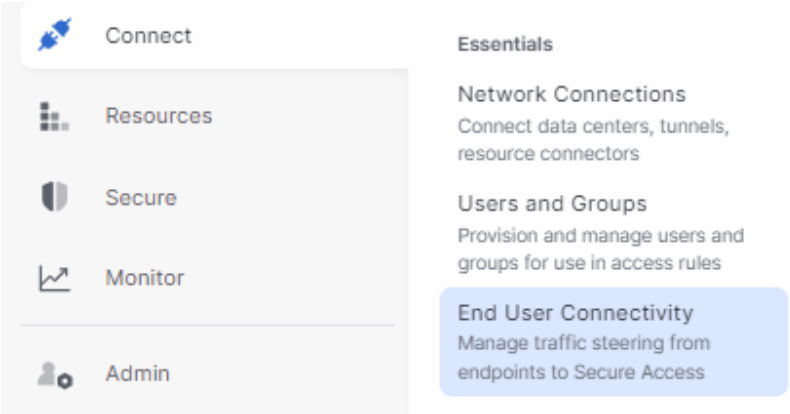
- **Option 1**: Download any version of Secure Client using the link in Secure Access to Cisco Software Central. You will need a valid service contract that is associated with your Cisco.com profile.
- **Option 2**: Download any version of Secure Client using the link in Secure Access to Cisco SecureX. Choose this option if you want to use cloud management.
- **Option 3**: Download the current version of Secure Client using the shortcut buttons in Secure Access.

Procedure

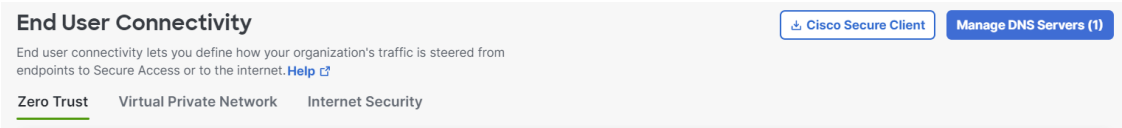
Provides instructions for procedure. In Secure Access, navigate to Connect End User Connectivity . On the End User Connectivity page, click Cisco Secure Client.

Procedure

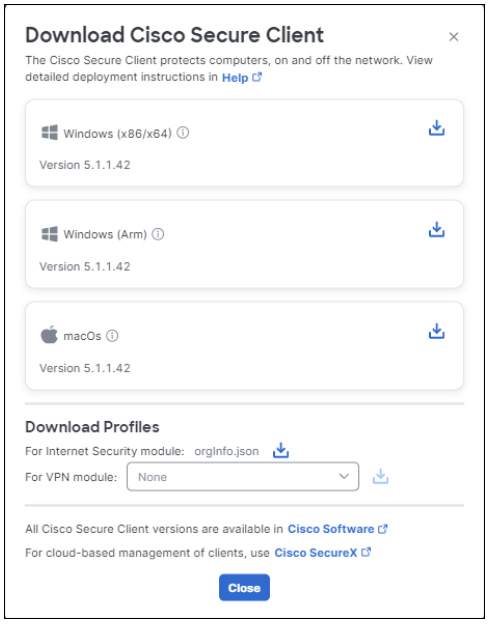
1. In Secure Access, navigate to **Connect** > **End User Connectivity**.



2. On the End User Connectivity page, click **Cisco Secure Client**.



3. In the Download Cisco Secure Client window, do one of the following:



- To download a previous version of Secure Client, click the **Cisco Software** link.
  a. In Cisco Secure Central, download the desired Secure Client pre-deployment package and the version for the OS on the end-user device.
     - Examples:
       - macOS–`cisco-secure-client-macos-5.1.0.136-predeploy-k9.pkg`
       - Windows–`cisco-secure-client-win-5.1.0.136-predeploy-k9.msi`
- To download a cloud-managed version of Secure Client, click the **Cisco SecureX** link.
  a. In SecureX, download the desired version of Secure Client.
- To download the current version of Secure Client, click the download buttons.

4. In the **Download Profiles** section:
   a. Download the orginfo.json file.
      - The json file is used with the Internet Security module (also known as the Umbrella roaming module). The file tells the module where to report and which policies to enforce.
   b. Choose all applicable VPN profiles.
      - The VPN profile tells Secure Access which VPN profiles to enforce. You created the VPN profiles in the End-User Connectivity module of Secure Access (**show menu path)**
5. Click **Close**.
6. Distribute Secure Client on all end-user devices.

Install the Root Certificate for All Browsers

Describes installing the root certificate for all browsers. Steps to perform the installation of certificates vary based on the operating system and browser type. For more information, see Install the Cisco Secure Access Root Certificate.

To inspect web traffic, perform SSL decryption, or render a block page correctly when a browser on a user device attempts to visit a blocked HTTPS web site, install the Cisco Secure Access root certificate for each browser on the organization's user devices. User devices must have the Cisco Secure Client deployed with the Umbrella module.

Steps to perform the installation of certificates vary based on the operating system and browser type. For more information, see Install the Cisco Secure Access Root Certificate.

Inspect and Decrypt HTTPS Traffic

Provides instructions for inspect and decrypt https traffic. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Inspect HTTPS traffic and perform SSL decryption.

Procedure

1. Install a Secure Access root certificate for each browser on a user device.
2. Enable **HTTPS inspection** in the Security profile for the Secure Access secure web gateway (SWG). If you do not enable HTTPS inspection, Secure Access is unable to perform file inspection, URL matching, advanced application controls, or provide URL level visibility for HTTPS communications.
3. Enable **Decryption** in the Security profile for the Secure Access secure web gateway (SWG).

   For more information, see Manage Security Profiles.

Render Block and Warn Pages

Describes render block and warn pages. Render Block and Warn pages correctly. When a browser on user device visits a blocked HTTPS website, even without HTTPS inspection or SSL decryption enabled, Secure Access does not downgrade the HTTPS protocol to HTTP when serving a block page.

Render Block and Warn pages correctly.

1. When a browser on user device visits a blocked HTTPS website, even without HTTPS inspection or SSL decryption enabled, Secure Access does not downgrade the HTTPS protocol to HTTP when serving a block page. Thus, if a root certificate is not installed, the web browser displays a certificate warning to the user. For more information, see Manage Notification Pages.

Install the Cisco Secure Client

Describes installing the cisco secure client. Cisco Secure Client provides security to user devices on any network, whether the device connects to private resources using Zero Trust Access, VPN, or is securely connected to the internet using DNS-layer security and the secure web gateway (SWG).

Cisco Secure Client provides security to user devices on any network, whether the device connects to private resources using Zero Trust Access, VPN, or is securely connected to the internet using DNS-layer security and the secure web gateway (SWG). As an administrator, you will deploy Secure Client on your organization's user devices that meet the client's minimum operating system requirements.

Procedure

Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. Administrative privileges on the user device.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Administrative privileges on the user device.

Procedure

Install the Cisco Secure Client on any user devices in your organization. You can customize the client modules that deploy with the package. For more information about the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

---

63 Manage Client-based Zero Trust Access from Mobile Devices

Topics:

- Set up the Zero Trust Access App for iOS Devices
- Set up the Zero Trust Access App for Android on Samsung Devices
- Monitor and Troubleshoot Zero Trust Access from Mobile Devices

Introduces managing client-based zero trust access from mobile devices. Cisco Secure Access offers client-based Zero Trust Access to private resources using a platform-native app on certain mobile devices.

Cisco Secure Access offers client-based Zero Trust Access to private resources using a platform-native app on certain mobile devices.

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

Set up the Zero Trust Access App for iOS Devices

Describes setting up the zero trust access app for ios devices. End users can access private resources from their Apple iOS mobile devices (iPhone or iPad) using the Zero Trust Access app. This Cisco Secure Client app uses Apple's platform-native zero trust network access technology.

End users can access private resources from their Apple iOS mobile devices (iPhone or iPad) using the Zero Trust Access app. This Cisco Secure Client app uses Apple's platform-native zero trust network access technology.

Zero Trust Access app for iOS:



System Requirements

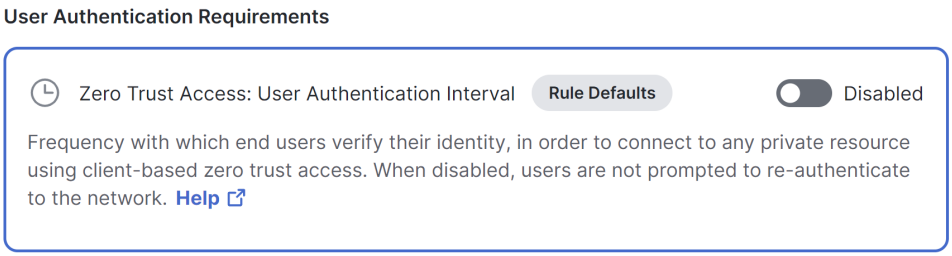
Describes system requirements. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Apple iPhone or iPad running iOS 17.2 or later

Guidelines and Limitations

Describes guidelines and limitations. IOS does not currently support step-up authentication, so users will not be able to use the Zero Trust Access app to access a private resource if step up authentication is enabled for that resource.

iOS does not currently support step-up authentication, so users will not be able to use the Zero Trust Access app to access a private resource if step up authentication is enabled for that resource. You can disable this functionality by default on the Rule Defaults page, or disable it in private access rules that include access for iOS devices:



For information, see Network Authentication for Zero Trust Access.

Configure Settings in Cisco Secure Access

Provides instructions for configuring settings in cisco secure access. Ensure that private resources can be accessed using Zero Trust Access from supported endpoint OS versions:

Ensure that private resources can be accessed using Zero Trust Access from supported endpoint OS versions:

Procedure

1. Configure a client-based posture profile that includes iOS devices and supported iOS versions: Navigate to **Secure** > **Endpoint Posture Profiles**. For information, see Add a Client-Based Zero Trust Access Posture Profile.
2. Ensure that each applicable private resource is configured to allow client-based Zero Trust Access connections. For information, see Add a Private Resource.
3. Ensure that a network tunnel group is configured to send ZTA traffic to this resource. Navigate to **Connect** > **End User Connectivity**. For information, see Manage Network Connections.
4. Configure a private access rule that allows traffic to the applicable private resources using the posture profile you configured in Step 1.
5. Ensure that the end user is configured for single sign-on authentication (SSO).

Install the App

Describes installing the app. There are two ways to distribute the app to IOS devices: You or end users can obtain the app from the App Store

There are two ways to distribute the app to IOS devices:

- You or end users can obtain the app from the App Store
- You can use your EMM/MDM vendor ecosystem

Have End Users Enroll in Zero Trust Access

Provides instructions for have end users enroll in zero trust access. The Zero Trust Access client app will walk end users through the enrollment process, which they should find reasonably straightforward.

The Zero Trust Access client app will walk end users through the enrollment process, which they should find reasonably straightforward.

You can give your end users the following instructions for (if applicable) installing the app and enrolling in Zero Trust Access:

Procedure

1. If your administrator has not yet installed the Zero Trust Access app on your device: Install the app from the App Store.
2. In order to enroll your device for Zero Trust Access, you will need your work email address and your single sign-on credentials.
3. Launch the app and follow the instructions.

   Important

   You must allow notifications.

   a. You will be prompted to sign in using Single sign-on credentials.
   b. When you see an **Approve** prompt, verify that the information on the screen is correct, then tap **Approve**.
   c. You may need to sign in again the first time you access an application on your network.
4. You may be required to sign in again periodically in order to access applications on your network. This is expected.

Notes for administrators

Describes notes for administrators. The enrollment process requires users to allow notifications. Notifications keep users up-to-date on Zero Trust Access and allows the Zero Trust Access application to communicate with the backend relay configuration.

- The enrollment process requires users to allow notifications. Notifications keep users up-to-date on Zero Trust Access and allows the Zero Trust Access application to communicate with the backend relay configuration.
- To monitor and troubleshoot client-based zero trust access connections from mobile devices, see Monitor and Troubleshoot Zero Trust Access from Mobile Devices.

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

Describes setting up the zero trust access app for android on samsung devices. End users can access private resources from their Samsung mobile devices running the Android operating system using the Zero Trust Access app. This Cisco Secure Client app uses platform-native zero trust network access technology.

End users can access private resources from their Samsung mobile devices running the Android operating system using the Zero Trust Access app. This Cisco Secure Client app uses platform-native zero trust network access technology.

Requirements and Prerequisites

- Samsung device running Android version 14+ and Samsung Knox 3.10 or higher. Example: Samsung S23.
- A Mobile Device Management (MDM) System where Samsung Knox Service Plugin (KSP) can be configured. Cisco has tested Ivanti Neurons, formerly known as MobileIron cloud version.
- A Google Play store account.

Configure Cisco Secure Access

Provides instructions for configuring cisco secure access. Configure a posture profile for client-based Zero Trust Connections that includes Android devices: Navigate to Secure Endpoint Posture Profiles .

Procedure

1. Configure a posture profile for client-based Zero Trust Connections that includes Android devices: Navigate to **Secure** > **Endpoint Posture Profiles**.
2. Configure a private resource that allows client-based ZTA connections: Navigate to **Resources** > **Private Resources**.
3. Ensure that a network tunnel is configured to send ZTA traffic to this resource. Navigate to **Connect** > **End User Connectivity**.
4. Configure a private access rule that allows the user ID associated with the Samsung Android device to access the private resource you configured above. Select a posture profile that includes Android devices.Navigate to **Secure** > **Access Rules**.

Install the App

Describes installing the app. There are two ways to distribute the app to Android Samsung devices: You or end users can obtain the app from the Google Play store: https://play.google.com/store/apps/details?id=com.cisco.secureclient.zta

There are two ways to distribute the app to Android Samsung devices:

- You or end users can obtain the app from the Google Play store: https://play.google.com/store/apps/details?id=com.cisco.secureclient.zta
- You can use your EMM/MDM vendor ecosystem

(Optional) Set up the Android device for Zero Trust Access using MDM

Describes (optional) set up the android device for zero trust access using mdm. If your organization uses a Mobile Device Management (MDM) solution, you can streamline and automate the deployment and configuration of the Zero Trust Access (ZTA) app on Android devices.

If your organization uses a Mobile Device Management (MDM) solution, you can streamline and automate the deployment and configuration of the Zero Trust Access (ZTA) app on Android devices. Using MDM allows you to enforce consistent security policies across all devices and makes the setup process easier for end users.

The following procedures describe how to:

1. Add the app to MDM on page 884
2. Set up the App on the Samsung Device on page 885

Add the app to MDM

Provides instructions for adding the app to mdm. Follow these steps to deploy the Knox Service Plugin (KSP) and configure the Cisco Secure Client (Zero Trust Access) app for Samsung devices using Ivanti.

Follow these steps to deploy the Knox Service Plugin (KSP) and configure the Cisco Secure Client (Zero Trust Access) app for Samsung devices using Ivanti.

Procedure

1. Sign in to your Ivanti dashboard with administrator credentials.
2. Add Knox Service Plugin to App Catalog.
   a) Navigate to **Apps** > **App** Catalog and click **+Add**.
   b) From the **Source** drop-down, choose **Google Play store**.
   c) In the **Search** field, enter **Knox Service Plugin**. The app should appear. If it does not, check your spelling, network, or permissions.
   d) Click **Knox Service Plugin** and then click **Approve** if prompted.
   e) Click **Select** and change the category for the app if needed. Then click **Next**.
3. Assign the App to Users or Devices.
   a) By default, **Delegate this app to all spaces** is selected. Click **Next**.
   b) Choose which people or devices will get the Knox Service Plugin (KSP) app. By default, **Everyone** is selected. Click **Next**.
4. Configure Managed Settings.
   a) If **Managed Configurations for Android** does not appear, add it and give it a name.
   b) Enable **Auto-launch on install**.
   c) In the **Managed Configurations** section, click **Expand All** to display all settings.
5. Enter Knox and ZTNA Details.
   a) If you need to obtain a free Knox License key for the next steps, see Manage Knox Licenses.
   b) In the **Profile name(version)** field, enter your Samsung Knox profile name and make sure the slider is set to **On**.
   c) In the **Knox License key(Knox Suite, DualDAR, etc)** field, enter your Samsung Knox license key and set the slider **On**.

d) Enable **Debug Mode**.

6. Select Device Enrollment Type.
   a) In the **Device-wide policies** section, choose the device enrollment type as:

   Fully Manage Device (DO)

   or

   Work Profile-on company owned devices (WP-C), also known as PO (Profile Owner)

   > **Note**
   >
   > PO enrollment is more common. These instructions assume PO enrollment.

   Important

   If you are doing a PO-type enrollment, ensure your device is not part of any other configuration, as it could conflict with the PO config.

7. Configure ZTNA Policy.
   a) Scroll down to the **ZTNA Policy** section.
   b) Enable the **Enable ZTNA controls** setting.
   a) In the **Package Name** field, enter `com.cisco.secureclient.zta` (if needed, click the **Refresh** button to the right of the field to allow typing).
   b) You can leave **Package Signature** blank.
8. Click **Next** to finish Managed App configuration.
9. Set Device Installation Requirements.
   a) For **Install on device**, add a config or edit the config if one is listed.
   b) Enable **Device Installation Configurations** and **Require installation on device**.
   c) Click **Update** or **Save** to retain your changes.
10. Assign and Distribute the Configuration.
   a) From the left menu, navigate to **Configurations**.
   b) Find the configuration called **Android enterprise: Work Profile (Android for Work)** or similar and click it.
   c) Click the pencil to edit the configuration.
   d) Click **Next** on the first screen.
   e) On the **Distribute** screen, make sure your user/device/group is selected.
   f) Click **Done**.

Set up the App on the Samsung Device

Provides instructions for setting up the app on the samsung device. Follow these steps to enroll your Samsung device and install the Cisco Zero Trust Access app using Ivanti MDM.

Follow these steps to enroll your Samsung device and install the Cisco Zero Trust Access app using Ivanti MDM.

Procedure

1. Enroll the Device in Ivanti MDM.
   a) On the Samsung device, sign into your Google Play store account.
   b) Install the **Ivanti Go** app from the Google Play store.
   c) Open the **Ivanti Go** app and enter your work email address to begin MDM enrollment.
   d) Enter your Ivanti password.
   e) Follow the remaining steps to complete MDM enrollment.
2. Verify Work Profile Creation.
   a) Once enrollment is complete, your device will have a Work profile managed by your MDM.
      This is a separate partition on the device for "work apps," which appear with a small briefcase icon to distinguish them from personal apps.
   b) To view your work apps:
      1. Swipe up from the bottom of the phone to show all installed apps.
      2. At the bottom, select **Work** to display apps installed in the work profile.
      3. **Personal** will show your regular apps.
3. Confirm App Installation in Ivanti.
   a) In the Ivanti dashboard, navigate to **Devices** > **Devices**.
   b) Locate your device by name or model number.
   c) Click on your device, then select the **Installed Apps** tab.
   d) Wait a few minutes for the **Knox Service Plugin (KSP)** app to appear in the list of installed apps.
      The KSP app and any other configured apps should be installed automatically.
4. Activate and Update KSP.
   a) On the device, open the **Knox Service Plugin** app from the Work profile.
   b) The work profile should display a configuration and indicate a successful setup.
   c) If the configuration is not successful, tap the **APPLY LATEST POLICIES** button to update it.
5. Add Google Play Account to Work Profile.
   a) On your Samsung device, add your Google Play store account to the Work profile. (Navigate to **Android Settings** > **Manage Accounts** > **Work** > **Add Account**.)
6. Install the Cisco Zero Trust Access app.
   a) In the work profile, open the **Play Store** app and ensure the correct Google Play account is selected.
   b) In the search field, enter **Cisco Zero Trust Access** or the app ID **com.cisco.secureclient.zta**.
   c) Tap and install the **Cisco Zero Trust Access** app or use this direct link.

Enroll the Device in Zero Trust Access

Provides instructions for enroll the device in zero trust access. If you do not use an EMM/MDM tool to install the app, either you or the end user can install the app from the Google Play store.

If you do not use an EMM/MDM tool to install the app, either you or the end user can install the app from the Google Play store. After the app is installed, either you or the user can enroll the app in Zero Trust Access.

If applicable, you can give these instructions to the end user:

Procedure

1. If your administrator has not yet installed the Zero Trust Access app on your device: Install the app from the Google Play store.
2. The first time you start the Zero Trust Access app, if your administrator has not yet enrolled your device, the app will prompt you to enroll in Zero Trust Access.
3. In order to enroll your device for Zero Trust Access, you will need your work email address and your single sign-on credentials.
4. Start the Zero Trust app.
5. Follow the instructions on the screens.

   Important

   You must allow notifications or the app will not work.

   a. You will be prompted to sign in using Single sign-on credentials.
   b. When you see an **Approve** prompt, verify that the information on the screen is correct, then tap **Approve**.
   c. You may need to sign in again the first time you access an application on your network.
6. You may be required to sign in again periodically in order to access applications on your network. This is expected.

Notes for administrators

Describes notes for administrators. To monitor and troubleshoot client-based zero trust access connections from mobile devices, see Monitor and Troubleshoot Zero Trust Access from Mobile Devices.

- To monitor and troubleshoot client-based zero trust access connections from mobile devices, see Monitor and Troubleshoot Zero Trust Access from Mobile Devices.

Monitor and Troubleshoot Zero Trust Access from Mobile Devices

Describes monitoring and troubleshoot zero trust access from mobile devices. This topic applies to client-based zero trust access connections from iOS devices and Samsung devices running Android operating systems.

This topic applies to client-based zero trust access connections from iOS devices and Samsung devices running Android operating systems.

Monitor Activity

Provides instructions for monitoring activity. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

After a mobile device begins to access private resources, you can monitor that activity:

Procedure

1. To view details about the enrolled device including, app version, client version and sync / enrollment dates: Navigate to **Connect** > **Users and Groups** page and click the user enrolled in the mobile app.

2. To view access logs: Navigate to **Monitor** > **Activity Search**. To filter the view, click on **ZTNA client-based** on the top right side of the table and select an appropriate time window.
   - iOS access logs will have ‘apple-ios' in the OS column.
   - Android access logs will have 'samsung-android' in the OS column.

General Troubleshooting

Describes general troubleshooting. Make sure the device is running a supported and permitted operating system, as configured in the endpoint posture profile configured in the applicable access rule.

Make sure the device is running a supported and permitted operating system, as configured in the endpoint posture profile configured in the applicable access rule.

Troubleshoot iOS Devices

Provides instructions for troubleshooting ios devices. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

To troubleshoot enrolled iOS devices:

Procedure

1. Confirm that the Zero Trust Access relay configuration was added:
   - On the device, go to **Settings** > **VPN & Relays**.
   - In the Per-App Relays section, **Zero Trust** displays.
   - To view information about the Zero Trust relay configuration, click the **(i)** icon.
2. Confirm that Zero Trust Access logs are available:
   - In the Zero Trust Access application, go to **Settings**.
   - Choose **Troubleshooting**.
3. Confirm that the sync configurations and user unenrollment page displays:
   - In the Zero Trust Access application, click the status frame.

Troubleshoot Samsung Devices Running Android OS

Provides instructions for troubleshooting samsung devices running android os. To send logs from the Android device: From the home screen, tap Settings Send Logs .

Procedure

1. **To send logs from the Android device**: From the home screen, tap **Settings** > **Send Logs**.
2. **To enable verbose logging**: From the home screen, tap Settings, enable verbose logging, and restart the device.
3. **To sync configurations**: From the home screen, tap**You're enrolled** > **Sync now**.
4. **To unenroll the user**: From the home screen, tap **You're enrolled** > **Unenroll**.

5. **To view ZTA statistics**: From the home screen, tap **You're enrolled** and scroll to the **General** section.
6. If a Cisco support representative requests certificate information: From the home screen, tap **You're enrolled** and scroll to **Certificate** section.

---

64 Manage Zero Trust Access on Cisco Secure Client

Topics:

- Requirements for Secure Client with Zero Trust Access
- Invite Users to Enroll in Zero Trust Access for Secure Client
- Troubleshoot Client-Based Zero Trust Access
- Unenroll a Device from Zero Trust Access

Introduces managing zero trust access on cisco secure client. Cisco Secure Client supports Zero Trust Access to private resources from user devices. To use the Secure Client with Zero Trust Access on a supported device, a user must enroll in Zero Trust Access on the Secure Client.

Cisco Secure Client supports Zero Trust Access to private resources from user devices. To use the Secure Client with Zero Trust Access on a supported device, a user must enroll in Zero Trust Access on the Secure Client.

Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, SaaS apps, and internet resources protected by Secure Access. Secure Client is configured with various software modules.

A Secure Client module may require the deployment of a certain profile to run module successfully. A system configuration manager or remote monitoring and management (RMM) system can download, install, and deploy the Secure Client on an organization's user devices. For more information about the Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

Enroll in Zero Trust Access

To deploy Secure Client with Zero Trust Access on user devices, an administrator from the Secure Access organization must invite end users in the organization to enroll in Zero Trust Access on the Secure Client on their device. For more information, see Invite Users to Enroll in Zero Trust for Cisco Secure Client.

Requirements for Secure Client with Zero Trust Access

Describes requirements for secure client with zero trust access. Cisco Secure Client with the Zero Trust Access module must meet these requirements:

Cisco Secure Client with the Zero Trust Access module must meet these requirements:

- Windows 10 and 11
- macOS versions 11, 12, 13
- Windows devices must support Trusted Platform Module (TPM) 2.0
- Mac devices must support Secure Enclave

Invite Users to Enroll in Zero Trust Access for Secure Client

Provides instructions for invite users to enroll in zero trust access for secure client. If your organization plans to deploy Cisco Secure Client with Zero Trust Access on end-user devices, the administrator must complete a few prerequisite tasks and then invite users to enroll in Zero Trust Access.

If your organization plans to deploy Cisco Secure Client with Zero Trust Access on end-user devices, the administrator must complete a few prerequisite tasks and then invite users to enroll in Zero Trust Access.

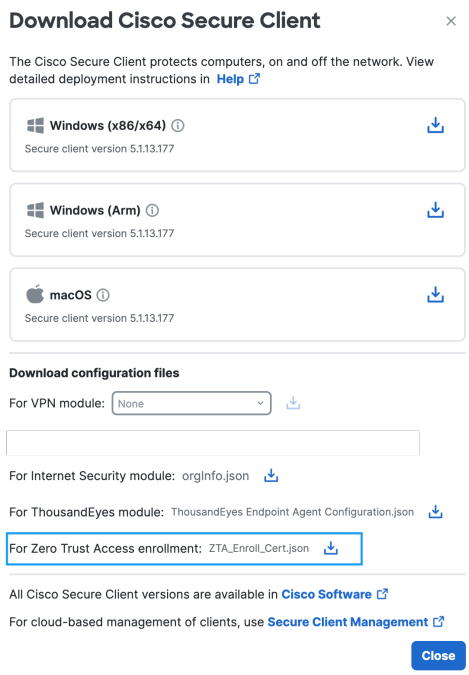
Recommended: Use MFA Authentication and Biometric Identity

For the highest security during end-user enrollment, we strongly advise that you take advantage of your established MFA-based authentication and the use of biometric identity for end-user authentication.

Before you begin

Before inviting users to enroll in Zero Trust Access, ensure the following requirements are met:

- Install Cisco Secure Client with the Zero Trust Access module on all user devices.
- Deploy the ZTA enrollment Certificate. The `ZTA_Enroll_Cert.json` file is required for device registration. Deploy this file to the target devices before prompting users to enroll.
  1. In the Secure Access dashboard, navigate to **Connect** > **End User Connectivity** > **Zero Trust Access** and click **Cisco Secure Client** .



2. Download the `ZTA_Enroll_Cert.json` file.
3. Deploy the `ZTA_Enroll_Cert.json` file to the following directory on the user devices:
   - macOS: /opt/cisco/secureclient/zta/enrollmentchoices
   - Windows: C:\\ProgramData\\Cisco\\Cisco Secure Client\\ZTA\\enrollment_choices

- Provision users and groups in your organization. For more information, see Manage Users and Groups.
- Ensure that users have SSO authentication configured through a SAML identity provider (IdP).
- Configure a Secure Access endpoint posture profile. For more information, see Manage Endpoint Security.

Procedure

1. Create an email distribution list of the users for whom you have provisioned the prerequisites.

   Zero Trust Access may not be familiar to your end users, so we recommend that you educate them on its benefits before prompting them to enroll. To help with that effort, following is some suggested language that you can use to speak about Zero Trust Access that includes instructions on how to enroll.
2. Customize the invitation using the following template. Ensure you replace the placeholder text (*insert apps for initial rollout*) with the specific applications available to your organization.

   ### Email Template for End Users

   Copy and customize the following text for your organization:

> **Note**
>
> Many of today's workers, like you, work remotely from time to time. That helps you to be productive, but it also increases risk from cyberthreats such as ransomware.
>
> That's why we're adopting a new approach, called Zero Trust Access, for you to securely access corporate resources. Zero Trust Access complements VPN access, making it simpler for you to access certain corporate apps while providing increased security. Please enroll in Zero Trust Access promptly to continue accessing these applications without interruption.
>
> The initial list of corporate applications that will be available using Zero Trust Access includes (*insert apps for initial rollout*). We will share further updates as more applications are made available through Zero Trust Access.
>
> **How to enroll** Zero Trust Access is a software component of Cisco Secure Client that is already installed on your company device. To enroll in Zero Trust Access, follow these steps:
>
> **a.** Open the Cisco Secure Client window. If you can't find the window, try searching for **Secure Client**.
>
> **b.** In the Zero Trust Access section, click **Enroll**.
>
> **c.** Enter your company email address.
>
> **d.** Sign in using your SSO credentials.
>
> **Result**: You are now enrolled in Zero Trust Access. Depending on IT security requirements, you may be asked to authenticate from time to time to continue accessing certain applications.
>
> Need enrollment help? Contact the IT help desk.

3. Send the customized email to your list of users.

Troubleshoot Client-Based Zero Trust Access

Describes troubleshooting client-based zero trust access. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

- Pre-Enrollment Errors
- Enrollment Errors
- Post-Enrollment Errors
- Requests to Reauthenticate

Pre-Enrollment Errors

Describes pre-enrollment errors. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Error	Description	Condition
Cannot begin enrollment	Cannot begin enrollment. Contact your IT help desk about these errors.	Occurs when there is a KDF, DHA, or TPM error or some combination.

Error	Description	Condition
Device registration error	An issue with the Device Desktop occurred. Contact your IT help desk.	Occurs when Duo desktop is not installed, is not running, or is non-responsive. The user is asked to ensure that the app is running or contact IT help desk for assistance.
Server certification error	Error initiating enrollment	Client is unable to verify the proxy server certificate.
Cannot connect to DHA		Occurs when the client is unable to communicate with the Device Health application because DHA is not installed.

Enrollment Errors

Describes enrollment errors. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Error	Description	Condition
Certification enrollment error		Occurs when the certificate does not install in the background during enrollment. The certificate is required for Zero Trust Access to work properly.
No network connection		Occurs when the user doesn't have an active or working internet connection (wired or wireless).
User auth error during enrollment	Error initiating enrollment. Contact your IT help desk.	Occurs when the user has provided an invalid email address or password (or both). The system is unable to verify the user's credentials.

Post-Enrollment Errors

Describes post-enrollment errors. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Error	Description	Condition
Network not allowed	Your organization requires you to be on an authorized network to log in.	Occurs when a private resource is not configured to allow Zero Trust access. Also occurs when the destination is not a configured private resource, but rather is an IP address that was typed directly into an access rule.
User IP address block	Your organization requires you to be on an authorized network to log in.	Occurs when the system is configured to allow access only from specific IP addresses, and the user is trying to access private resources from an unapproved IP address.

Error	Description	Condition
Application blocked for everyone	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user did not match any rule and was blocked by default or when a rule was not created to allow access to the application.
User blocked implicitly	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user did not match any rule and was blocked by default or when a rule was not created to allow the user access to the application either directly or via a group.
Time-based application block	You do not have permission to access this application at this time. Contact your IT help desk.	Occurs when the user does not match any rule and was blocked by default or the application does not allow access at this time.
User IP block	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user is using an unauthorized device to access; the user's credentials aren't associated with the IP or with that device.
User blocked explicitly	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user is blocked by a rule that denies access or when the user does not have permission to connect or access the resource.
Access protocol block	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	User does not have permission to connect to the resource using the current protocol.
User location block	Location is not allowed.	Occurs when the user did not match any rule and is blocked by default or when the user is not allowed access to the application from their current location.
Cannot connect to DHA		Occurs when there is no response when the client tried to communicate with DHA.

Requests to Reauthenticate

Describes requests to reauthenticate. If an end user is offline for an extended time, for example on vacation, Secure Access may prompt the user to reauthenticate in order to restore access to private resources. This is normal and expected.

If an end user is offline for an extended time, for example on vacation, Secure Access may prompt the user to reauthenticate in order to restore access to private resources. This is normal and expected.

Requirements for Secure Client with Zero Trust Access <**Troubleshoot Client-Based Zero Trust Access Errors** > Manage Virtual Private Networks on Cisco Secure Client

Unenroll a Device from Zero Trust Access

Describes unenroll a device from zero trust access. To unenroll a device from Zero Trust Access, see Unenroll Devices for Client-Based Zero Trust Access. Be sure to review the description of this functionality at the top of the page.

To unenroll a device from Zero Trust Access, see Unenroll Devices for Client-Based Zero Trust Access. Be sure to review the description of this functionality at the top of the page.

65 Manage Virtual Private Networks on Cisco Secure Client

Topics:

- Download the Virtual Private Network XML Profile
- CA Certificates for VPN Connections

Introduces managing virtual private networks on cisco secure client. Cisco Secure Client supports virtual private network (VPN) connections from user devices to private resources and Software as a Service (SaaS) resources in data centers and private and public clouds.

Cisco Secure Client supports virtual private network (VPN) connections from user devices to private resources and Software as a Service (SaaS) resources in data centers and private and public clouds. The Cisco Secure Client VPN module requires the Secure Access VPN XML file deployed on the user device.

Cisco Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, software as a service (SaaS) apps, and internet resources protected by Secure Access. The Cisco Secure Client is configured with various software modules. A Cisco Secure Client module may require the deployment of a certain profile to run the module successfully. A system configuration manager or remote monitoring and management (RMM) system can download, install, and deploy the Cisco Secure Client on an organization's user devices.

Prerequisites

- Administrative privileges on the user devices in the organization.
- Download the virtual private network (VPN) XML connection metadata from your Secure Access organization. For more information, see Download the Virtual Private Network XML Profile.

For more information about the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

Download the Virtual Private Network XML Profile

Provides instructions for downloading the virtual private network xml profile. The Cisco Secure Client supports the use of various profiles to configure the deployment of the client modules. A Cisco Secure Client module may require a certain profile present to install the module successfully.

The Cisco Secure Client supports the use of various profiles to configure the deployment of the client modules. A Cisco Secure Client module may require a certain profile present to install the module successfully.

The Cisco Secure Client virtual private network (VPN) module requires the VPN XML profile. Cisco Secure Client installs with the VPN module. You can download the Cisco Secure Client VPN profile from Secure Access.

The Cisco Secure Client VPN profile configures the VPN module on the user device and connects clients securely to resources protected by Secure Access.

The Cisco Secure Client VPN profile describes the connection and security metadata for the VPN module.

Before you begin

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

Procedure

1. **Download the Cisco Secure Client VPN Profile.**

   The Cisco Secure Client VPN profile describes the connection and security metadata for the VPN module.

   a) Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
   b) For a VPN profile, click **Download XML** to save the Cisco Secure Client VPN profile to the local system.

2. **Copy the VPN Profile to the Target Directory.**

   Copy the Cisco Secure Client VPN XML file to the Cisco Secure Client VPN profile directory on the user devices.

OS	Location	File	Description
Windows	**%ProgramData%\Cisco\Cisco Secure Client\VPN\Profile**	AnyConnect VPN Profile	
macOS	**/opt/cisco/secureclient/vpn/profile**	AnyConnect VPN Profile	

CA Certificates for VPN Connections

Describes ca certificates for vpn connections. To authenticate users and devices when connected over a virtual private network (VPN), Secure Access must have the root certificate authority (CA) certificate for the user devices.

To authenticate users and devices when connected over a virtual private network (VPN), Secure Access must have the root certificate authority (CA) certificate for the user devices.

Set up the trust between Secure Access and the user devices in the organization that connect over a VPN:

1. Install a certificate signed by your organization's Certificate Authority (CA) on all devices where you have deployed the Cisco Secure Client with the VPN module.

2. Upload your organization's signed CA root certificate to Secure Access. For more information, see VPN Certificates for User and Device Authentication.

66 Manage Internet Security on Cisco Secure Client

Topics:

- Umbrella Roaming Security Module Requirements
- Domain Management
- DNS Protection Status
- Interpret Internet Security Diagnostics
- Download the OrgInfo.json File
- Customize Windows Installation of Cisco Secure Client
- Customize macOS Installation of Cisco Secure Client

Introduces managing internet security on cisco secure client. Cisco Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, software as a service (SaaS) apps, and internet resources protected by Secure Access. The Cisco Secure Client is configured with various software modules.

Cisco Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, software as a service (SaaS) apps, and internet resources protected by Secure Access. The Cisco Secure Client is configured with various software modules. A Cisco Secure Client module may require the deployment of a certain profile to run the module successfully. A system configuration manager or remote monitoring and management (RMM) system can download and deploy the Cisco Secure Client on an organization's user devices.

A Roaming Device is a user device that has Cisco Security Client deployed on the device with the Umbrella (Roaming Security) module.

Cisco Secure Client deployed with the Umbrella module enables secure internet access on user devices. The Umbrella module includes:

- DNS-layer security
- Web security–Secure web gateway (SWG)

Once deployed, Cisco Secure Client registers the user device with Secure Access and the device is added to the list of Roaming Device resources. Cisco Secure Client syncs with Secure Access periodically and the user device's web traffic is protected by the Secure Access policy. An organization's administrators can manage Roaming Devices protected by internet security in Secure Access. For more information, see Manage Internet Security.

For more information about the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

Umbrella Roaming Security Module Requirements

Describes umbrella roaming security module requirements. To ensure that the Cisco Secure Client Umbrella Roaming Security module deploys and runs successfully, a user device must meet certain system and network requirements.

To ensure that the Cisco Secure Client Umbrella Roaming Security module deploys and runs successfully, a user device must meet certain system and network requirements.

System Requirements

Describes system requirements. The Cisco Secure Client supports all vendor-maintained, generally available releases of an operating system unless otherwise noted.

The Cisco Secure Client supports all vendor-maintained, generally available releases of an operating system unless otherwise noted.

Cisco Secure Client version 5.1.0 and higher is supported on:

- Windows 10 x86 and x64 devices
- Windows 11 x64 and ARM64 devices
  - ARM64 devices only support the Secure Client with the VPN module, DART, Secure Firewall posture, Network Visibility module, Umbrella module, and ISE posture.
- macOS 11.x or higher

For more information about the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

Network Requirements

Describes network requirements. For more information, see Network Requirements for Secure Access: DNS Block Pages For more information, see Network Requirements for Secure Access: SAML Identity Provider Domains. When using an SSL-VPN, add the IP address of the VPN head-end to the external domains settings.

Secure Access DNS Block Pages

For more information, see Network Requirements for Secure Access: DNS Block Pages

Secure Access and SAML Identity Provider Domains

- For more information, see Network Requirements for Secure Access: SAML Identity Provider Domains.

> **Note**
>
> When using an SSL-VPN, add the IP address of the VPN head-end to the external domains settings. For more information, see Manage Domains.

Network Access

Host Names

The Cisco Secure Client Umbrella Roaming Security module uses hostnames for registration. All machines must have a hostname that is unique within your organization.

Secure Access DNS Resolvers

For more information, see Network Requirements for Secure Access: DNS Resolvers.

Encrypted DNS

For more information, see Network Requirements for Secure Access: Encrypted DNS.

External DNS Resolution

For more information, see Network Requirements for Secure Access: External DNS Resolution.

HTTP and HTTPS

The Cisco Secure Client Umbrella Roaming Security module uses HTTP (80/TCP) and HTTPS (443/TCP) to communicate with Secure Access for the following uses:

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

Windows Only: If you utilize an HTTP proxy that is configured at the user-level (normally using GPO), make sure the `SYSTEM` user is also configured to use the proxy. Otherwise, add the following rules to your firewall to ensure the Cisco Secure Client Umbrella (Roaming Security) module can reach Secure Access.

Secure Access DNS – Client Configuration Services

For more information, see Network Requirements for Secure Access: Client Sync Services.

Secure Access DNS – Client Sync Services

For more information, see Network Requirements for Secure Access: Client Sync Services.

Secure Access DNS and Web – Client Certificate Revocation Services

For more information, see Network Requirements for Secure Access: Client Certificate Revocation Services.

Transport Layer Security Protocol

For more information, see Network Requirements for Secure Access: Transport Layer Security Protocol.

Roaming Security DNS Requirements

Describes roaming security dns requirements. The Cisco Secure Client Umbrella Roaming Security module is not compatible with other DNS serving software. You should not install the Cisco Secure Client Umbrella module on a device that serves DNS requests.

- The Cisco Secure Client Umbrella Roaming Security module is not compatible with other DNS serving software. You should not install the Cisco Secure Client Umbrella module on a device that serves DNS requests.
- Uninstall **DNSCrypt** before your install the Cisco Secure Client Umbrella (Roaming Security) module. The Cisco Secure Client Umbrella (Roaming Security) module installer automatically detects installations of DNSCrypt and prompts the administrator to uninstall before proceeding with the installation.
- Install the Cisco Secure Client Umbrella Roaming Security module on the **C:\ drive**. The Cisco Secure Client Umbrella module does not support secondary or remote drive installations.
- The Cisco Secure Client Umbrella Roaming Security module supports IPv4 connectivity for macOS and Windows.

Internal Domains

Describes internal domains. The Cisco Secure Client sends all of your DNS lookups directly from your computer to the Secure Access global network resolvers.

The Cisco Secure Client sends all of your DNS lookups directly from your computer to the Secure Access global network resolvers. Thus, to ensure that Cisco Secure Client directs internal DNS requests to your internal DNS servers for resolution, you must add your local domain names to the internal domains list in Secure Access. The Cisco Secure Client's Umbrella module syncs with Secure Access periodically to check for new internal domains. This is a **critical** part of the setup process. We recommend that you populate the list of internal domains before you deploy the Umbrella (Roaming Security) module. For more information, see Domain Management.

Domain Management

Describes domain management. Cisco Secure Access provides the option to manage domains when endpoints connect to internet resources with the Cisco Secure Client or a PAC file. Domain management allows DNS queries for certain domains to query the local network's DNS servers instead of the Secure Access DNS servers.

Cisco Secure Access provides the option to manage domains when endpoints connect to internet resources with the Cisco Secure Client or a PAC file. Domain management allows DNS queries for certain domains to query the local network's DNS servers instead of the Secure Access DNS servers.

If you do not specify a list of internal domains, all DNS queries are sent directly to Secure Access, and as a result, cannot reach your network's local resources (for example: computers, servers, printers) on internally-hosted domains that rely on local DNS servers.

When you add internal domains to your bypass list, these internal domain queries sent from an endpoint with a Secure Access PAC file or the Cisco Secure Client bypass the Secure Access DNS resolvers. However, in the case of a tunnel, this configuration is not passed down, so there is no way to bypass traffic to the proxy per-organization with a custom configuration for network tunnels.

To ensure uninterrupted access to these resources, administrators should add the appropriate domains to the organization's domain bypass list. The domain bypass list syncs to all Cisco Secure Clients in your organization.

Internal Domains List

Describes internal domains list. Populate the internal domains list with domains used by your organization to access local resources while on the organization's network (at the physical location or connected through VPN).

Populate the internal domains list with domains used by your organization to access local resources while on the organization's network (at the physical location or connected through VPN). The internal domains list is pre-populated with the **.local TLD** and all **RFC-1918 (private network)** reverse DNS address space. Secure Access syncs newly added domains to Cisco Secure Clients within about one hour. For more information, see Manage Domains.

DNS Suffixes

Describes dns suffixes. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

The domains contained in the DNS suffixes configuration on a computer's adapter and global network settings are imported automatically into a Cisco Secure Client's internal domains list each time the Cisco Secure Client starts or a new network adapter (such as a VPN or wireless connection) is initiated. This sync process helps Cisco Secure Clients adapt when on newly seen networks where they may want to access local resources without adding the domain through the Secure Access.

Operational Flow

Describes operational flow. The Cisco Secure Client can handle internal and external DNS queries gracefully. The Cisco Secure Client's internal domains list is populated by two sources:

The Cisco Secure Client can handle internal and external DNS queries gracefully.

Configure Internal Domains

The Cisco Secure Client's internal domains list is populated by two sources:

- Syncs from the Secure Access internal domains list.
- The DNS Suffixes list located in the local computer's networking configuration settings.

Cisco Secure Client and External Queries

External DNS queries that do not match a domain located on either of the internal domains lists are sent straight to Secure Access.

Cisco Secure Client and Internal Queries

DNS queries for domains contained in the domain bypass list (internal domains list) are sent through the local network's DNS servers.

- Internal domains that are hosted on the local network are resolved by the internal DNS server directly.
- Internal Domains that are not hosted on the local network are resolved by Secure Access or whichever public DNS servers are used for resolution.

Advanced Topics

Describes advanced topics. The following section focuses on more in-depth information and logic with internal domains and expected behavior. There are implications that should be considered with DNS Suffixes.

The following section focuses on more in-depth information and logic with internal domains and expected behavior.

Unencrypted

Although the Cisco Secure Client is able to send encrypted DNS queries to Secure Access **when in the encrypted state**, domains listed on the bypass domains list are sent unencrypted, because they are not sent to Secure Access.

DNS Suffixes (Continued)

There are implications that should be considered with DNS Suffixes.

- This could allow an organization to not add any domains to the internal domains list in Secure Access. If DHCP is configured to use your domains as DNS Suffixes, the Cisco Secure Client automatically considers the domain as local, even without adding the domain to the internal domains list in Secure Access.
- If you use DNS suffixes to rely on internal domain resolution instead of populating the internal domains list in Secure Access, the endpoint traffic has increased security. Since DNS queries sent to domains on the internal domains list are sent unencrypted, this implies that a machine performing DNS queries for domains on the Secure Access internal domains list always sends unencrypted traffic on *all* networks.

> **Note**
>
> During the deployment of the Cisco Secure Client on user devices, you can disable the feature that adds the domains contained in the DNS suffixes list.

DNS Protection Status

Provides instructions for dns protection status. After you deploy the Umbrella module in the installed Cisco Secure Client, DNS protection status changes appear in the Cisco Secure Client endpoint.

After you deploy the Umbrella module in the installed Cisco Secure Client, DNS protection status changes appear in the Cisco Secure Client endpoint. If you do not see DNS protection status, the Umbrella module is installed, but Internet Security (**OrgInfo.json**) is not deployed.

Procedure

View status information in the Cisco Secure Client Umbrella module on the user device.

Before you begin

Administrative privileges on the user device.

Procedure

1. Open the **Cisco Secure Client**.
2. Navigate to **Roaming Security** > **Statistics** to access the DNS and IP security information.

DNS and IP Layer State Descriptions

Describes DNS and IP layer state descriptions.

State	Description	Condition
Reserved	`Checking Connection Status.` No active network connections. The Umbrella module waits for an active network connection.	This operating state occurs during the following conditions: • When the module is first activated. • When a network interface change occurs. For example, as detection of a new network adapter, IP changes on an existing adapter, or a new VPN tunnel being established or torn down.

State	Description	Condition
Open	`You are not currently protected by Secure Access.` There is at least one active network connection; however, the Roaming Security agent can not connect to the Secure Access resolvers over port 53/UDP or 443/UDP on any active connection. The user is not protected by Secure Access and traffic events are not reported to Secure Access. The system's DNS settings revert to their original settings–DHCP or Static.	This operating state occurs during the following conditions: • No UDP port 443 or UDP port 53 connectivity to Secure Access resolvers (IPv4)). • The VPN tunnel may temporarily be in a state of tear down or establishment.
Protected	`You are protected by Secure Access.` A network connection is active, and the Umbrella module is able to connect to Secure Access resolvers over port 53/UDP, but not 443 UDP. The user is protected by Secure Access and traffic events are reported to Secure Access, but the connection is not encrypted.	This state may occur when the module is first activated or when there is a network interface change.

State	Description	Condition
Encrypted	`You are protected by Secure Access.` The Umbrella module has established a connection to Secure Access resolvers over port 443/UDP. The user is protected by Secure Access and traffic events are reported to Secure Access. The DNS queries are encrypted. Internal Domains are forwarded to DHCP-delegated or statically-set DNS servers and are therefore not encrypted.	This operating state occurs during the following conditions: • UDP port 443 connectivity to Secure Access resolvers (IPv4). • TCP port 443 and TCP port 53 connectivity to Secure Access resolvers (IPv4). **Note** TCP is only used when UDP responses are truncated.
Protected Network	`You are on a network protected by Secure Access.` The user device is behind a protected network—a network managed by Secure Access—and the organization has "Disable Behind Protected Networks" enabled in their dashboard. The Umbrella agent has reverted the DNS settings back to what was set through DHCP or statically set. The connection is not encrypted.	This operating state occurs during the following conditions: • The current endpoint network egress IP address is registered with the same Secure Access account as the endpoint. • Resolvers used are the Secure Access resolvers. Policy configured through the instance of Secure Access ("Disable Behind Protected Networks") dictates that the Umbrella module should be disabled when on a protected network. **Note** This state is not possible for all subscriptions because there is no network-level protection.
VPN Trusted Network State	`Disabled while you are on a trusted network.` The Umbrella module DNS protection is not active because the current endpoint network is configured as a Cisco Secure Client VPN trusted network.	

State	Description	Condition
		This operating state occurs during the following conditions: • AnyConnect VPN module is reporting the Trusted Network Detection state as trusted. • AnyConnect VPN tunnel is either not connected or established in full tunnel mode. The Secure Access policy rule indicates that the Umbrella module should be disabled when on an Cisco Secure Client VPN trusted network. **Note** This setting is true for all roaming package customers and cannot be changed by the administrator.
Disabled due to VPN State	`Disabled while your VPN is active.` The Umbrella module DNS protection is not active because the endpoint currently has an active Cisco Secure Client VPN tunnel established.	This operating state occurs during the following conditions: • Cisco Secure Client VPN module is reporting the Trusted Network Detection state as not trusted. • Cisco Secure Client VPN tunnel is established in full tunnel mode. Policy rule configured with Secure Access requires that the Umbrella module is disabled when a Cisco Secure Client VPN tunnel is established. **Note** This setting is true for all Umbrella module configurations. An administrator can not change the setting.
No OrgInfo.json State		This operating state occurs when the **OrgInfo.json** file is not deployed to the correct directory. For more information, see Download the OrgInfo.json File.

State	Description	Condition
	`You are not currently protected by Secure Access.` The Umbrella profile is not deployed. The Umbrella module DNS protection is not active because the endpoint currently has an active AnyConnect VPN tunnel established.	
Agent Unavailable State	`You are not currently protected by Secure Access.` Service unavailable. The Umbrella module DNS protection is not active because the Roaming Security agent is not running.	This operating state occurs when the Umbrella agent service is not currently running because of a crash or manual service stop.
Missing .NET Dependency State (Windows only)	`You are not currently protected by Secure Access.` Microsoft 4.0 NET framework is not installed. Roaming Security module DNS protection is not active because the Roaming Security agent is not running. The .NET runtime framework is missing.	This operating state occurs when the Umbrella agent service is not running due to a missing .NET 4.0 runtime.
Not Required	The client is not attempting coverage in this state, as it is not expected nor required. This state applies to IPv4 on Windows.	The client was not able to find a suitable local DNS resolver for the IP Protocol, and therefore is disabled awaiting the discovery of a suitable local DNS resolver.

Interpret Internet Security Diagnostics

Describes interpret internet security diagnostics. When deployed on a user device, the Cisco Secure Client with the Umbrella (Roaming Security) module can generate detailed diagnostic reports about the device's DNS and web traffic. The Cisco Secure Client's Diagnostic Tool (DART) module provides the diagnostic information about the device.

When deployed on a user device, the Cisco Secure Client with the Umbrella (Roaming Security) module can generate detailed diagnostic reports about the device's DNS and web traffic. The Cisco Secure Client's Diagnostic Tool (DART) module provides the diagnostic information about the device. As an administrator on the device, generate a diagnostic report from the Cisco Secure Client GUI or the Cisco Secure Client's DART command-line interface (CLI).

For information about the administration of the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.

Procedure

Describes procedure. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Generate the Cisco Secure Client diagnostic report on the user device.

Generate the Diagnostic Report from the Cisco Secure Client

Provides instructions for generating the diagnostic report from the cisco secure client. Administrative privileges on the user device. From the Cisco Secure Client menu, select Diagnostics and Reporting Tool, and then select Run.

Before you begin
Administrative privileges on the user device.

Procedure

1. From the Cisco Secure Client menu, select **Diagnostics and Reporting Tool**, and then select **Run**.
2. Send the generated **.zip** file to Cisco Support. For more information, see Contact Cisco Secure Access Support.

Generate the Diagnostic Report on the Command Line

Provides instructions for generating the diagnostic report on the command line. Administrative privileges on the user device. Find the Cisco Secure Client Umbrella module diagnostic tool on your system and run the Cisco Secure Client's DART executable.

Before you begin
Administrative privileges on the user device.

Procedure

1. Find the Cisco Secure Client Umbrella module diagnostic tool on your system and run the Cisco Secure Client's **DART** executable.

OS	Location
Windows	**%ProgramData%\Cisco\Cisco Secure Client\UmbrellaDiagnostic.exe**
macOS	**/opt/cisco/secureclient/bin/UmbrellaDiagnostic.app**

2. Send the generated **.zip** file to Cisco Support. For more information, see Contact Cisco Secure Access Support.

Download the OrgInfo.json File

Provides instructions for downloading the orginfo.json file. You can deploy various modules with the Cisco Secure Client. The Cisco Secure Client may require a certain profile present to install a module successfully.

You can deploy various modules with the Cisco Secure Client. The Cisco Secure Client may require a certain profile present to install a module successfully.

The Cisco Secure Client Umbrella Roaming Security module (DNS-layer and Web security) requires the Secure Access **OrgInfo.json** file. The Secure Access **OrgInfo.json** file associates a Cisco Secure Client deployment with the Umbrella Roaming Security module to a Secure Access user and organization. Once the module is deployed on the Cisco Secure Client, Secure Access applies the organization's configured policy rules to the device. The device's traffic events are visible in the Activity Search report.

If you use another **OrgInfo.json** file from a different organization in Secure Access to install the Cisco Secure Client Umbrella module, the roaming device is managed by that instance of Secure Access instead.

To deploy the Cisco Secure Client with the Umbrella Roaming Security module on a user device, download the **OrgInfo.json** file from Secure Access to the device.

Before you begin

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

Procedure

1. Download the OrgInfo.json File.
   a) Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
   b) For Cisco Secure Client, click **Download Profile** to save the **OrgInfo.json** file to the local system.
2. Copy the OrgInfo.json File to the Target Directory.
   a) Copy your **OrgInfo.json** file to either the location of the Cisco Secure Client install directory or the **Profiles\\umbrella** directory on the local system.

   When you deploy the **OrgInfo.json** file for the first time, the Cisco Secure Client copies the **OrgInfo.json** file to the data subdirectory (**/umbrella/data**), which also contains several registration files. If you need to deploy a new **OrgInfo.json** file, you must delete the data subdirectory. Alternatively, you can uninstall the Cisco Secure Client Umbrella Roaming Security module, which deletes the data subdirectory, and then reinstall the new **OrgInfo.json** file.

   Note

   If you deploy the **OrgInfo.json** file on the device after installing the Cisco Secure Client, the Cisco Secure Client Umbrella Roaming Security module directories already exist. If you deploy the **OrgInfo.json** file on the device before installing the Cisco Secure Client, you have to create the required directories for the Umbrella Roaming Security module on the device.

OS	Location	Description	File
Windows	**%ProgramData%\\Cisco\\Cisco Secure Client\\Umbrella**	You must copy the **OrgInfo.json** file that you downloaded from Secure Access to the target directory. Do not rename the file. Alternatively, before installing the Cisco Secure Client, copy the **OrgInfo.json** file to **\\Profiles\\umbrella**. The Umbrella module installer is located in **\\Profiles\\umbrella**	Umbrella module
macOS	**/opt/cisco/secureclient/umbrella/**		Umbrella module

Customize Windows Installation of Cisco Secure Client

Describes customize windows installation of cisco secure client. As an administrator of a user device, you can customize the installation of the Cisco Secure Client (formerly AnyConnect) with various modules and features on Windows.

As an administrator of a user device, you can customize the installation of the Cisco Secure Client (formerly AnyConnect) with various modules and features on Windows. The Cisco Secure Client deployment packages support several MSI properties that you can change during installation, including lockdown and disabling the display of the VPN module in the client's graphical user interface (GUI). Lockdown prevents the service from being disabled manually.

This guide describes how to deploy the Cisco Secure Client with the VPN, Umbrella (Roaming Security that includes both the DNS-layer security and Web security), and DART (diagnostics) modules. By default, the Cisco Secure Client deploys with the VPN module.

Requirements

Describes requirements. Windows 8.1 or newerThe Umbrella (Roaming Security) module requires the .NET framework 4.6.2 or newer

- Windows 8.1 or newer
  - The Umbrella (Roaming Security) module requires the .NET framework 4.6.2 or newer
- Windows 10 or 11 on ARM-64
- Cisco Secure Client 5.1 or newer
- Administrative privileges on the Windows device

Procedure

Describes procedure. You can deploy the Cisco Secure Client for Windows with several options including: Hide the VPN module in the Cisco Secure Client GUI.

You can deploy the Cisco Secure Client for Windows with several options including:

- Hide the VPN module in the Cisco Secure Client GUI.
- Hide the Cisco Secure Client installation from the Add/Remove Windows Programs list.
- Enable Lockdown.

Deploy the Cisco Secure Client VPN Module

Provides instructions for deploying the cisco secure client vpn module. Download the OrgInfo.json file from Secure Access. For more information, see Download the OrgInfo.json File. Download the Cisco Secure Client Pre-Deployment Package (Windows) from https://software.cisco.com/download/home.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Windows)** from https://software.cisco.com/download/home.

Procedure

Run the Windows installer to deploy the Cisco Secure Client VPN package with the `PRE_DEPLOY_DISABLE_VPN=1` option. The `PRE_DEPLOY_DISABLE_VPN` option hides the VPN module in the client's GUI. The VPN module is not disabled. Set the MSI property to `PRE_DEPLOY_DISABLE_VPN=1`.

What to do next

Note: If the VPN module is hidden in the client GUI, you can manage the VPN module through the Cisco Secure Client's CLI.

The following command disables the VPN functionality by copying the **VPNDisable_ServiceProfile.xml** file embedded in the MSI to the directory specified for profiles for VPN functionality.

For example:

```
msiexec /package cisco-secure-client-win-<version>-core-vpn-predeploy-k9.msi
/norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* c:\\output.log
```

Deploy the Cisco Secure Client Umbrella Roaming Security Module

Provides instructions for deploying the cisco secure client umbrella roaming security module. Download the OrgInfo.json file from Secure Access. For more information, see Download the OrgInfo.json File. Download the Cisco Secure Client Pre-Deployment Package (Windows) from https://software.cisco.com/download/home.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Windows)** from https://software.cisco.com/download/home.

Procedure

Run the Windows installer to deploy the Cisco Secure Client Umbrella Roaming Security module.

What to do next

```
msiexec /package cisco-secure-client-win-<version>-umbrella-predeploy-k9.msi
/norestart /passive /lvx* c:\\output.log
```

To enable lockdown, add `LOCKDOWN=1` in the command-line installer.

```
msiexec /package cisco-secure-client-win-<version>-umbrella-predeploy-k9.msi
/passive LOCKDOWN=1 /lvx* c:\\output.log
```

(Optional) Deploy the Cisco Secure Client DART Module

Provides instructions for (optional) deploy the cisco secure client dart module. Download the OrgInfo.json file from Secure Access. For more information, see Download the OrgInfo.json File. Download the Cisco Secure Client Pre-Deployment Package (Windows) from https://software.cisco.com/download/home.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Windows)** from https://software.cisco.com/download/home.

Procedure

Run the Windows installer to deploy the Cisco Secure Client DART (diagnostics and troubleshooting) package.

What to do next

```
msiexec /package cisco-secure-client-win-<version>-dart-predeploy-k9.msi
/norestart /passive /lvx* c:\\dart.log
```

Hide Cisco Secure Client from Add/Remove Programs List

Provides instructions for hide cisco secure client from add/remove programs list. You can hide the installed Cisco Secure Client modules from users that have permissions to view the Windows Add/Remove Programs list.

You can hide the installed Cisco Secure Client modules from users that have permissions to view the Windows Add/Remove Programs list.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Windows)** from https://software.cisco.com/download/home.

Procedure

Run the Windows installer for a Cisco Secure Client module package using `ARPSYSTEMCOMPONENT=1`. You can apply this option to all modules at the time of deployment.

What to do next

For example:

```
msiexec /package cisco-secure-client-win-<version>-umbrella-predeploy-k9.msi
/passive ARPSYSTEMCOMPONENT=1 /lvx* c:\\output.log
```

Optional OrgInfo.json Configurations

Describes optional orginfo.json configurations. After you deploy the Cisco Secure Client with the Umbrella Roaming Security module, you can update the OrgInfo.json file on the device. Only modify the internet security profile located at %ProgramData%\Cisco\Cisco Secure Client\Umbrella\data\OrgInfo.json.

> **Note**
>
> After you deploy the Cisco Secure Client with the Umbrella Roaming Security module, you can update the **OrgInfo.json** file on the device. Only modify the internet security profile located at **%ProgramData%\Cisco\Cisco Secure Client\Umbrella\data\OrgInfo.json**. The deployed Cisco Secure Client Umbrella Roaming Security module does not read the properties from the **%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json** file on the device. For more information, see Download the OrgInfo.json File.

When deploying the Umbrella (Roaming Security) module on the Cisco Secure Client, you can add and configure various parameters to the Umbrella **OrgInfo.json** file. These parameters, unlike `LOCKDOWN`, are applied to the **OrgInfo.json** profile directly rather than at the time of installation with an **msiexec** parameter. The following does not apply if run at install time.

Parameter	Values	Description
noAutoSuffix	`0` - Add the domains (default) `1` - Do not add domains	Does not add domains contained in the DNS Suffixes settings in network adapters and networking properties to your organization's Internal Domains list. This feature exists so that the Umbrella module is more aware of local resources and domains on foreign networks.
customUSResolvers	`\["18.252.251.72"", "18.254.118.193"\]` - Sets primary and secondary US-based Anycast addresses	Enables special DNS resolver Anycast addresses that limits DNS queries to only US-based Secure Access servers. Does not affect block pages or proxy.
noNXDOMAIN	`0` - Do re-query (default) `1` - Do not re-query	Automatically re-query public NXDOMAINS at the local resolvers. This feature allows roaming users to resolve internal domains on networks beyond their own without interruption or internal domains list management. **Note:** DNS search suffixes are sent to local resolvers, unless this functionality is disabled.

Customize macOS Installation of Cisco Secure Client

Describes customize macos installation of cisco secure client. Managed device manager (MDM) systems can customize the installation of the Cisco Secure Client (formerly AnyConnect) with various modules on macOS.

Managed device manager (MDM) systems can customize the installation of the Cisco Secure Client (formerly AnyConnect) with various modules on macOS. The Cisco Secure Client has the option to install with pre-configured Secure Access profiles and to hide the display of modules in the Cisco Secure Client's graphical user interface (GUI). Modify the Cisco Secure Client deployment disk image (DMG) file to select the modules to install with the client.

This guide describes how to deploy the Cisco Secure Client with the VPN, Umbrella (Roaming Security that includes both the DNS-layer security and Web security), and DART (diagnostics) modules. The default installation of the Cisco Secure Client deploys the virtual private network (VPN) module.

The Cisco Secure Client requires an XML configuration to deploy modules from the command-line interface (CLI) or MDM. You can use a transform (**ACTransforms.xml**) to deploy Cisco Secure Client without the VPN module.

Requirements

Describes requirements. MacOS version 10.14.6 or newer Cisco Secure Client 5.0 or newer Administrative privileges on the macOS device

- macOS version 10.14.6 or newer
- Cisco Secure Client 5.0 or newer
- Administrative privileges on the macOS device
- (Optional) macOS MDM permissions

Procedure

Describes procedure. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Choose the modules to install with the Cisco Secure Client on a macOS device.

Step 1 – Make the DMG Package Writeable

Provides instructions for step 1 - make the dmg package writeable. Use Disk Utility or hdiutil to change the permissions on the DMG package from Read Only to Read/Write.

Use Disk Utility or **hdiutil** to change the permissions on the DMG package from Read Only to Read/Write.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Mac OS)** from https://software.cisco.com/download/home.

Procedure

Open a **Terminal** and set the DMG file to Read/Write.

What to do next

```
hdiutil convert cisco-secure-client-macos-5.1.05040-predeploy-k9.dmg -format
UDRW -o csc-writeable.dmg
hdiutil attach csc-writeable.dmg
```

Step 2 – Generate the Module Installation Configuration File

Provides instructions for step 2 - generate the module installation configuration file. Generate the Cisco Secure Client module configuration file. The configuration file defines the modules to include with the installation of Cisco Secure Client.

Generate the Cisco Secure Client module configuration file. The configuration file defines the modules to include with the installation of Cisco Secure Client.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Mac OS)** from https://software.cisco.com/download/home.

Procedure

1. Open a **Terminal** and launch the DMG from **/Volumes**.

```
open /Volumes/Cisco\ Secure\ Client\ 5.1.05040
```

2. Run **installer** providing the `pkg` option with the name of the Cisco Secure Client package and the `showChoiceChangesXML` option. Redirect the output to **install_choices.xml** to generate the installation configuration file.

```
installer -pkg /volumes/Cisco\ Secure\ Client\ 5.1.05040/Cisco\ Secure\
Client.pkg -showChoiceChangesXML > ~/Downloads/install_choices.xml
```

Step 3 – Copy OrgInfo.json to Cisco Secure Client Installation Directory

Provides instructions for step 3 - copy orginfo.json to cisco secure client installation directory. Download the OrgInfo.json file from Secure Access. For more information, see Download the OrgInfo.json File. Download the Cisco Secure Client Pre-Deployment Package (Mac OS) from https://software.cisco.com/download/home.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Mac OS)** from https://software.cisco.com/download/home.

Procedure

1. Open a **Terminal** and launch the DMG from **/Volumes/Profiles**.

```
cd /Volumes/Cisco\ Secure\ Client\ <version>/Profiles/Umbrella/
```

2. Drag the **OrgInfo.json** file that you downloaded from Secure Access to **Volumes/Profiles**.

Step 4 – (Optional) Hide the VPN Module

Provides instructions for step 4 - (optional) hide the vpn module. To hide the display of the Cisco Secure Client VPN module in the client GUI, modify ACTransforms.xml.

To hide the display of the Cisco Secure Client VPN module in the client GUI, modify **ACTransforms.xml**.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.

- Download the **Cisco Secure Client Pre-Deployment Package (Mac OS)** from https://software.cisco.com/download/home.

Procedure

1. Open a **Terminal** and launch the **ACTransforms.xml** file from **/Volumes**.

```
open -e /Volumes/Cisco\ Secure\ Client\ 5.1.05040/Profiles/ACTransforms.xml
```

2. Remove the XML comments around the `Transforms` element, and then save **ACTransforms.xml**.

```
<Transforms>
<DisableVPN>true</DisableVPN>
<DisableCustomerExperienceFeedback>true</DisableCustomerExperienceFeedback>
</Transforms>
```

Step 5 - Customize the Cisco Secure Client Installation Modules

Provides instructions for step 5 - customize the cisco secure client installation modules. Edit install_choices.xml created in Step 2 - Generate the Module Installation Configuration File. Either skip or install the Cisco Secure Client modules defined in the configuration file.

Edit **install_choices.xml** created in Step 2 - Generate the Module Installation Configuration File. Either skip or install the Cisco Secure Client modules defined in the configuration file.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Mac OS)** from https://software.cisco.com/download/home.

Procedure

1. To skip a module, define the module with `0`.
2. To install a module, define the module with `1`.

What to do next

> **Note**
>
> Modifying `choice_vpn` does not supersede the changes that you made to **ACTransforms.xml**. The VPN module is required, even if the module is not displayed in the client GUI.

1. Open a **Terminal** and launch **install_choices.xml**.

2. Define an integer XML element for each module and assign to `0` or `1`, and then save **install_choices.xml**.

```
cd /Volumes
open -e ~/Downloads/install_choices.xml
```

Example – Customize Cisco Secure Client Modules

Describes example - customize cisco secure client modules. In the following example, the Core VPN, Umbrella, and DART modules are set to 1 and are included in the Cisco Secure Client installation.

In the following example, the Core VPN, Umbrella, and DART modules are set to `1` and are included in the Cisco Secure Client installation.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
 <dict>
  <key>attributeSetting</key>
  <true/>
  <key>choiceAttribute</key>
  <string>visible</string>
  <key>choiceIdentifier</key>
  <string>choice_anyconnect_vpn</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <false/>
  <key>choiceAttribute</key>
  <string>enabled</string>
  <key>choiceIdentifier</key>
  <string>choice_anyconnect_vpn</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <integer>1</integer>
  <key>choiceAttribute</key>
  <string>selected</string>
  <key>choiceIdentifier</key>
  <string>choice_anyconnect_vpn</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <true/>
  <key>choiceAttribute</key>
  <string>visible</string>
  <key>choiceIdentifier</key>
  <string>choice_fireamp</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <false/>
  <key>choiceAttribute</key>
  <string>enabled</string>
  <key>choiceIdentifier</key>
  <string>choice_fireamp</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <integer>0</integer>
```

```
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_fireamp</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_dart</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_dart</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>1</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_dart</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_firewall_posture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_firewall_posture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>0</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_firewall_posture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_iseposture</string>
</dict>
<dict>
```

```
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_iseposture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>0</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_iseposture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_nvm</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_nvm</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>0</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_nvm</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_umbrella</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_umbrella</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>1</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_umbrella</string>
```

```
 </dict>
 <dict>
  <key>attributeSetting</key>
  <true/>
  <key>choiceAttribute</key>
  <string>visible</string>
  <key>choiceIdentifier</key>
  <string>choice_thousandeyes</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <false/>
  <key>choiceAttribute</key>
  <string>enabled</string>
  <key>choiceIdentifier</key>
  <string>choice_thousandeyes</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <integer>0</integer>
  <key>choiceAttribute</key>
  <string>selected</string>
  <key>choiceIdentifier</key>
  <string>choice_thousandeyes</string>
 </dict>
</array>
</plist>
```

Step 6 – Set Up the Correct Extension Permission Settings

Provides instructions for step 6 - set up the correct extension permission settings. Download the OrgInfo.json file from Secure Access. For more information, see Download the OrgInfo.json File. Download the Cisco Secure Client Pre-Deployment Package (Mac OS) from https://software.cisco.com/download/home.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Mac OS)** from https://software.cisco.com/download/home.

Procedure

1. By default, macOS requires the user to accept the activation of a new System Extension. As a result, the user is presented with a popup. An MDM is required to approve the Cisco Secure Client system extension and disable the pop-up, using a management profile's SystemExtensions payload. For more information on System Extensions payloads, see System Extensions.
2. Follow the payload guidance in Cisco Secure Client Extension Approval using MDM to deploy the System Extension settings.

Step 7 – Install Cisco Secure Client with Selected Modules

Provides instructions for step 7 - install cisco secure client with selected modules. Install the Cisco Secure Client with the configured modules.

Install the Cisco Secure Client with the configured modules.

Before you begin

- Download the **OrgInfo.json** file from Secure Access. For more information, see Download the OrgInfo.json File.
- Download the **Cisco Secure Client Pre-Deployment Package (Mac OS)** from https://software.cisco.com/download/home.

Procedure

1. Open a **Terminal** and mount the DMG from **/Volumes**.

```
cd /Volumes
mount ~/Downloads/csc-writeable.dmg
hdiutil convert csc-writeable.dmg -format UDRO -o csc-readable.dmg
hdiutil detach /Volumes/Cisco\ Secure\ Client/<version>/
```

2. Run **installer** providing the `pkg` option with the name of the Cisco Secure Client package and the `applyChoiceChangesXML` option with **install_choices.xml**.

```
hdiutil attach ~/Downloads/csc-readable.dmg
sudo installer -pkg Cisco\ Secure\ Client\ 5.1.05040/Cisco\ Secure\ Client.pkg
 -applyChoiceChangesXML ~/Downloads/install_choices.xml -target /
```

Part IV

Managed Android

Topics:

- Secure Access Module for Cisco Secure Client (Android OS)
- Deploy the Android Client
- Manage Identities
- Export Device Data to CSV
- Troubleshooting

67 Secure Access Module for Cisco Secure Client (Android OS)

Topics:

- Secure Access Module for Cisco Secure Client (Android OS)

Describes the purpose and procedures for secure access module for cisco secure client (android os) and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Secure Access Module for Cisco Secure Client (Android OS)

Describes secure access module for cisco secure client (android os). DNS Policies Only Android Mobile Security is only supported in Secure Access for Access policies.

> **Note**
>
> **DNS Policies Only**
>
> Android Mobile Security is only supported in Secure Access for Access policies.

Mobile device threats are prevalent on any network. The Cisco Secure Access Module in Cisco Secure Client for Android OS is a roaming client for managed Android devices that offers protection from these threats at the DNS layer. This protection extends to both apps and browser-based traffic to the entire protected scope of the Android device.

A mobile device management system (MDM) is required to deploy this client to mobile devices and to push the Secure Access configuration to the mobile devices.

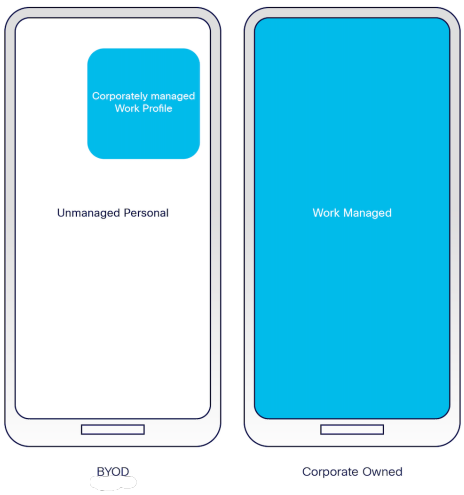
Device Security

Describes device security. There are two deployment modes for the Secure Access module for Cisco Secure Client: Personal "bring your own device" (BYOD)

There are two deployment modes for the Secure Access module for Cisco Secure Client:

- Personal "bring your own device" (BYOD)
- Organization-owned device

Secure Access coverage applies exclusively to the work profile of the Android device. For fully managed (organizational owned) devices, the entire device is covered. For employee-owned devices with a work profile, only the work profile is covered by Secure Access for Android. Please refer to the diagram below, where blue indicates Secure Access coverage:



Prerequisites

Describes prerequisites. An Android Enterprise compatible device deployment. The legacy Device Admin (DA) system is not supported at this time.

- An Android Enterprise compatible device deployment. The legacy Device Admin (DA) system is not supported at this time.
- Private DNS must be turned off for DNS interception to function properly.
- Android mobile devices running Android OS version 6.0.1 and above. Devices examples are Samsung, Google, and Motorola. FireOS devices and other Android forks are not supported.
- An MDM for deploying the software. You can use an MDM that meets your organizational security and compliance requirements.
- Access to a Secure Access subscription, including mobile device coverage
- A network meeting access requirements
  - For IPv4 networks, ensure that UDP ports 53, 5353, and 443 are accessible to the IP address 18.252.251.72.

Known Issues

Describes known issues. The app download may fail in the Google Play store after enabling the Secure Access module. This is a known limitation from Google on Android OS. To avoid this, download the apps before enabling the Secure Access module.

The app download may fail in the Google Play store after enabling the Secure Access module. This is a known limitation from Google on Android OS. To avoid this, download the apps *before* enabling the Secure Access module. Google has fixed this behavior in Android OS “Q”. For more information, see the Google issue tracker.

Some features may not work correctly on Huawei devices. For more information, see Troubleshooting.

68 Deploy the Android Client

Topics:

- Deploy the Android Client

Describes the purpose and procedures for deploy the android client and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Deploy the Android Client

Describes deploying the android client.

The process of deploying the Android client consists of three tasks:

- Download the Android Configuration
- Configure the mobile device manager (MDM) you use
- Push the Secure Access certificate

> **Note**
>
> Android Mobile Security is only supported in Secure Access for DNS policies.

Download Configuration

Android Configuration Download

MDM Configurations

> **Note**
>
> Use an MDM that meets your organizational security and compliance requirements.

Mobile device management (MDM) deployment is the responsibility of the customer. The Secure Access Android client supports standard Android Enterprise managed device deployment using any MDM that supports the required configuration profile delivery. Cisco does not integrate with or manage the customer MDM platform.

To deploy the client, download the configuration artifacts from the Secure Access dashboard and deploy them through your MDM of choice. The customer is responsible for selecting an MDM that meets their specific security and compliance requirements. Cisco does not validate or certify third party MDM platforms for compliance.

For more details, refer to Generic MDM Deployment Framework.

Secure Access Certificate

Push the Secure Access Certificate to Devices

Android Configuration Download

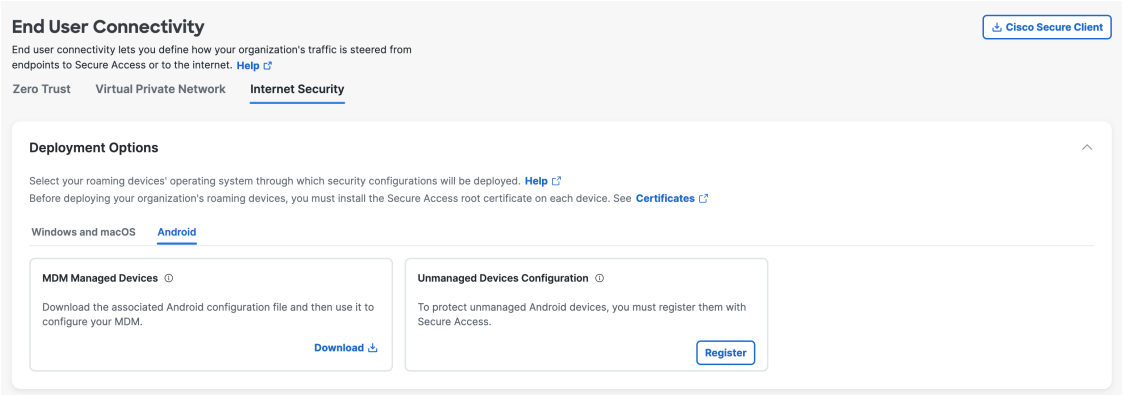
Provides instructions for android configuration download. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

By downloading an XML file from Secure Access and adding this file to your MDM system, your MDM system is able to push configuration information to both Cisco Security Connector (CSC) and Secure Access so that your Android device is registered with Secure Access. The result is that your Android device is protected by Secure Access.

For information about configuring your specific MDM system, see your MDM system's documentation.

Procedure

1. Navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **Android** tab.



2. Under the **MDM Managed Devices** section, click **Download**.

   The downloaded configuration file contains details that are required to enable Secure Access security on your Android device. For example, it includes the organization ID and unique registration token associated with your Secure Access organization.

```
{"organizationInfo":{"Value":{"organizationId":<orgid>,"productId":<product
id>"regToken":"<reg token>"}}}
```

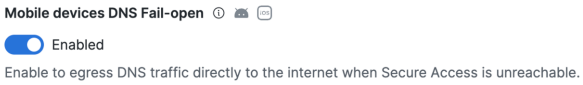
   Only one administrator is required to download the config file.

3. Save the file securely; you will use it in deploying your mobile device manager (MDM).

Fail Close/Open Scenario

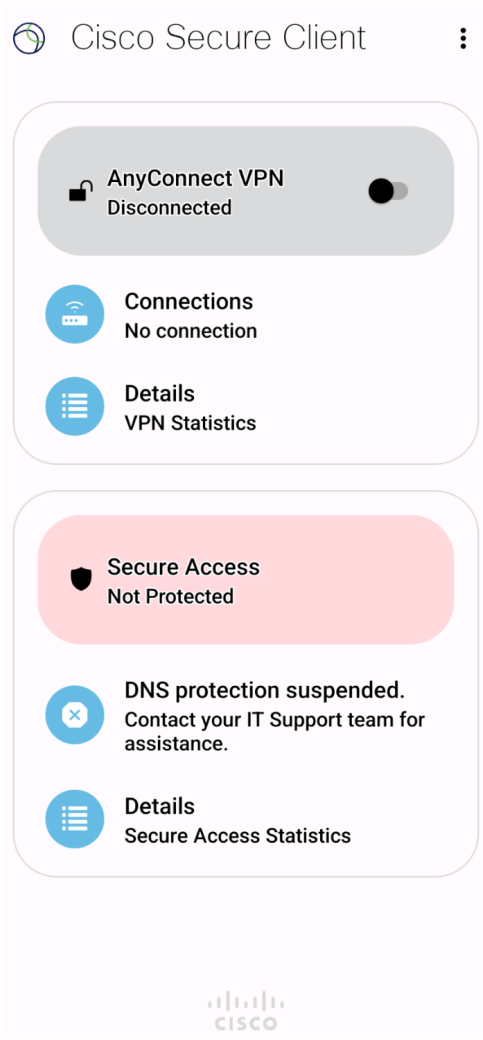
Describes fail close/open scenario. Navigate to Cisco Secure Client settings Advanced , and enable the Mobile devices DNS Fail-open field to egress DNS traffic directly to the internet when Secure Access is unreachable.

Navigate to **Cisco Secure Client settings** > **Advanced**, and enable the **Mobile devices DNS Fail-open** field to egress DNS traffic directly to the internet when Secure Access is unreachable.



> **Note**
>
> The Mobile Device Settings are the only settings applicable for Android devices under the Secure Access Security Settings.

In case of internal errors, such as the Secure Access Resolver is not reachable or the DNSCrypt Certificate is not available, the Secure Access UI displays the following:



Generic MDM Deployment Framework

Provides instructions for generic mdm deployment framework. MDM user interfaces are updated frequently by vendors. The following steps outline the standard deployment workflow for any MDM. For a detailed, step-by-step implementation example, refer to the VMware Workspace ONE section.

MDM user interfaces are updated frequently by vendors. The following steps outline the standard deployment workflow for any MDM. For a detailed, step-by-step implementation example, refer to the VMware Workspace ONE section.

Procedure

1. Locate the Cisco Secure Client - AnyConnect app in your MDM's managed app catalog (Managed Google Play). Approve the application and assign it to your target device groups.
2. Create a configuration profile for the application.

   Map the following keys from your downloaded configuration file:

   - Organization ID
   - Registration Token

> **Note**
>
> Ensure your environment is configured for single stack (note that dual stack is not currently supported).

3. Download the Secure Access root certificate from the Secure Access dashboard. Upload this to your MDM's certificate management section and push it to all managed devices to enable proper handling of block pages and Trusted Network Detection.
4. (Optional)If your organization requires a persistent connection, configure an **Always On VPN** profile within your MDM to prioritize Secure Access protection.

VMware Workspace ONE

Describes vmware workspace one. Deploy the Umbrella module on Android devices using zero-touch deployment. This method ensures seamless protection by enabling Always On VPN through the Mobile Device Manager (MDM) Workspace One, without manual intervention.

This section explains how to deploy the Umbrella module on Android devices using zero-touch deployment. This method ensures seamless protection by enabling Always On VPN through the Mobile Device Manager (MDM) Workspace One, without manual intervention.

The Umbrella module in Cisco Secure Client provides robust protection against threats by securing both applications and internet-based traffic at the DNS layer on Android devices.

> **Note**
>
> **Workspace ONE Details**
>
> For more information about using the Cisco Umbrella Anyconnect module with the Workspace ONE MDM, refer to the Workspace ONE documentation available online on VMWare's documentation website.

Important

Install the Cisco Secure Client only after you have published and installed the Always On VPN profile in Workspace One Intelligent Hub.

Prerequisites for Deployment

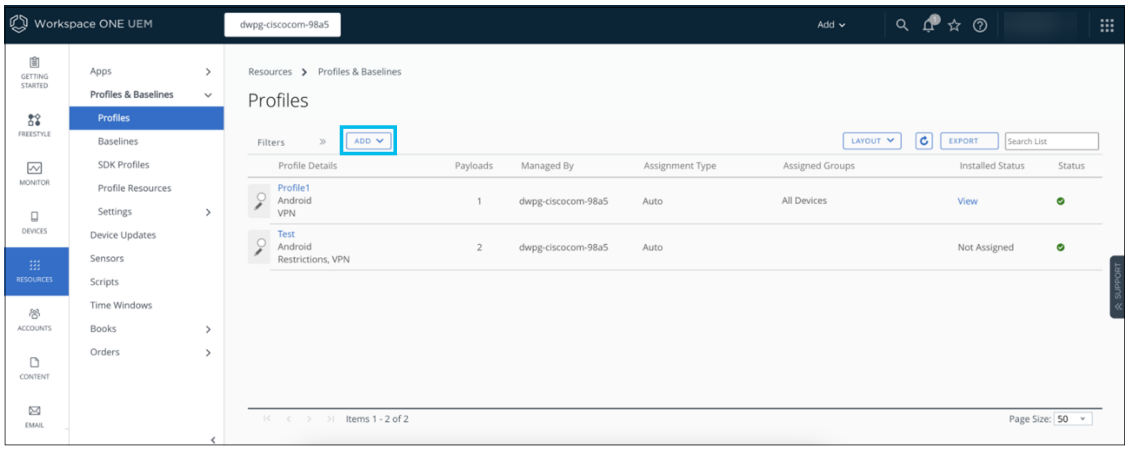
- Complete the Android EMM (Enterprise Mobility Management) registration, device enrollment, and a work profile creation.
- Ensure that the MDM app Hub is visible within the work profile.

Create Always On VPN Profile

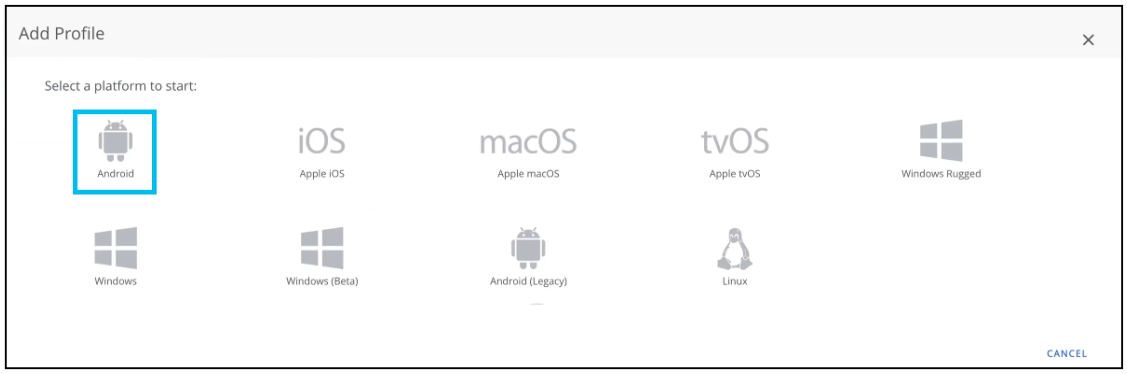
Provides instructions for creating always on vpn profile.

Procedure

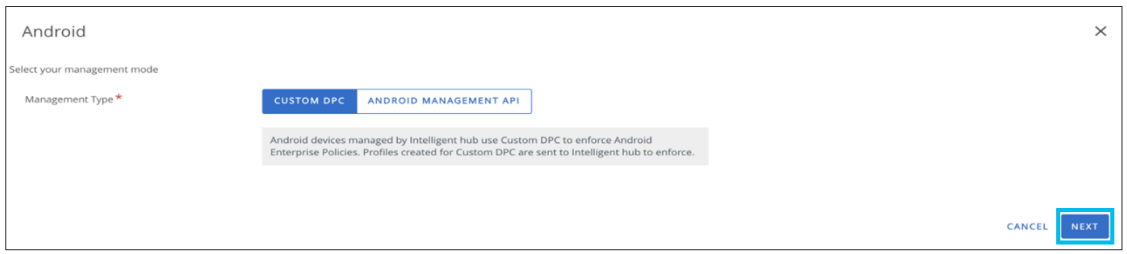
1. In the Workspace ONE UEM console, navigate to **Resources** > **Profiles & Baselines** > **Profiles**.
2. Click **Add** and choose **Add Profile** from the drop-down list.



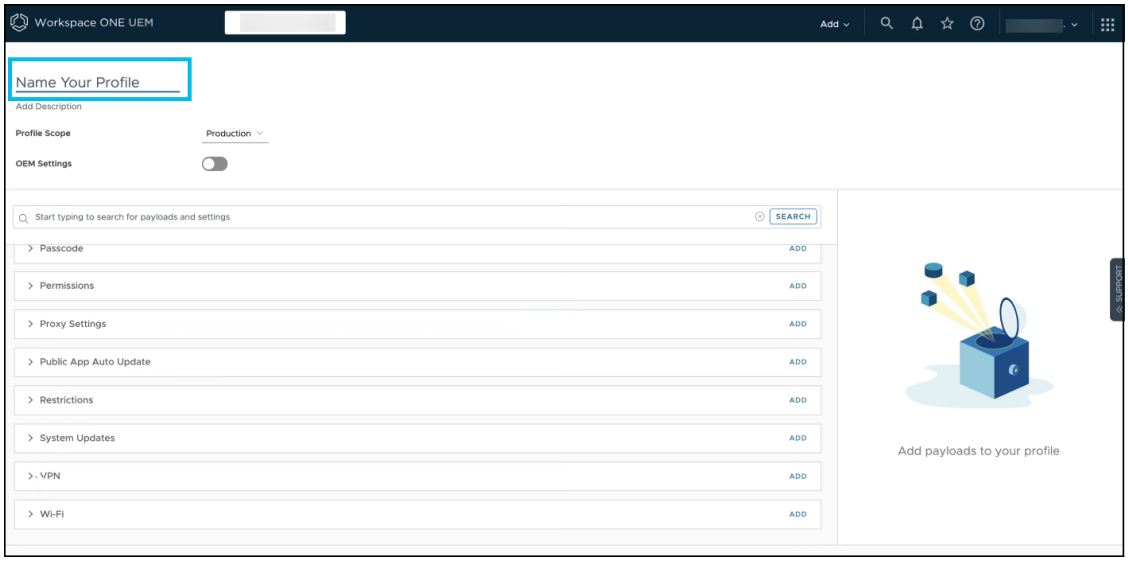
3. Select **Android** as the platform.



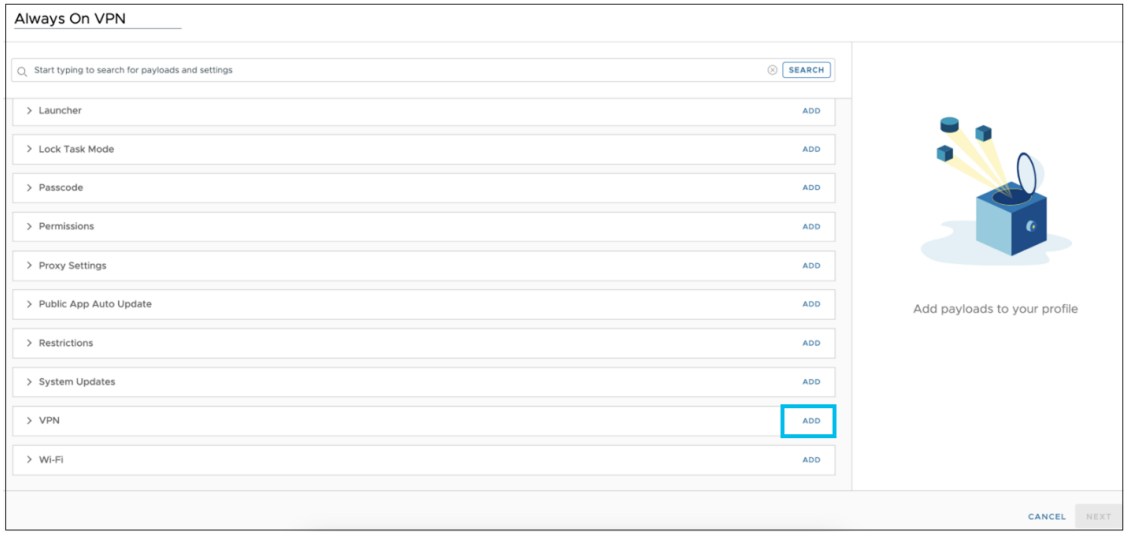
4. Choose **CUSTOM DPC** or **ANDROID MANAGEMENT API** as the **Management Type** and click **Next**.



5. Enter a name for your profile. For example, *Always On VPN*.

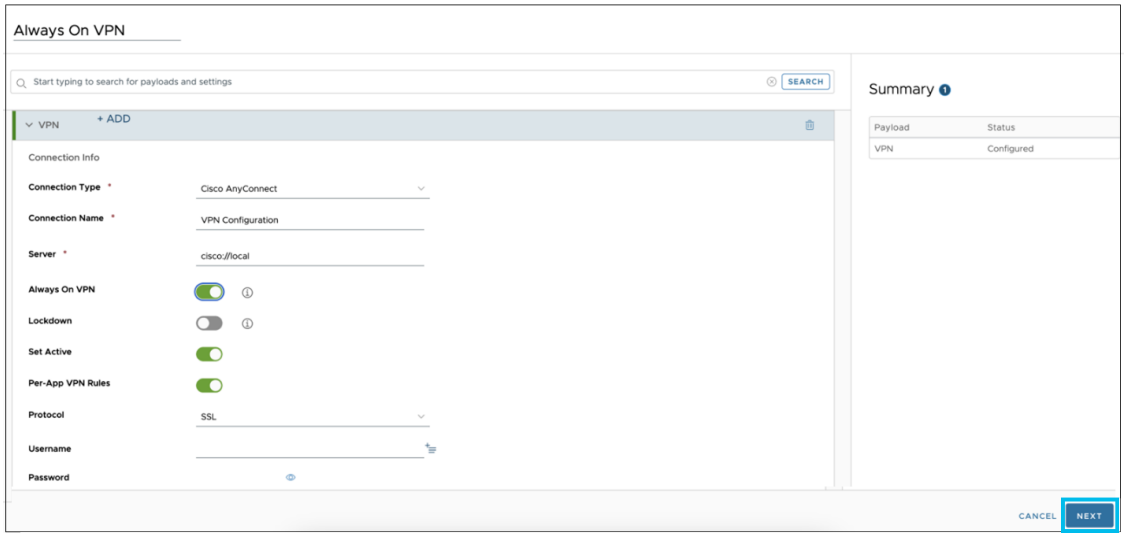


6. Navigate to the **VPN** section and click **Add**.

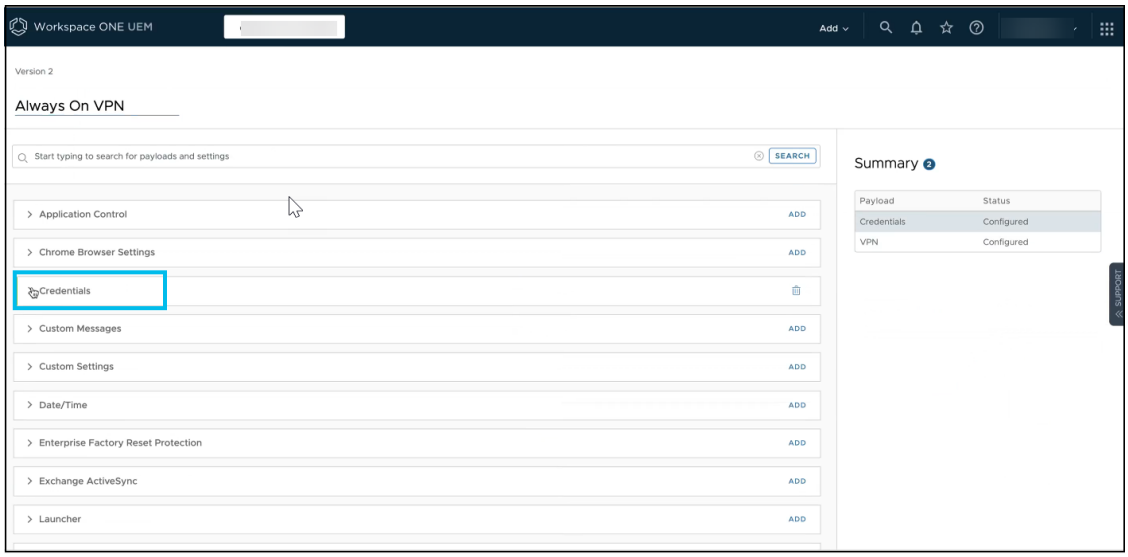


7. In the VPN setting configuration section, complete the fields, including the following:
   - From the **Connection Type** drop-down list, choose **Cisco AnyConnect**.
   - In the **Server** field, enter *cisco://local*.
   - In the **Connection Name**, enter the name.
   - Enable the **Always on VPN** button.
   - Enable the **Set Active** button.
   - Enable the **Per-App VPN Rules** button.

8. Click **Next**.



9. Search or navigate to the **Credentials** section, and click **Add**.

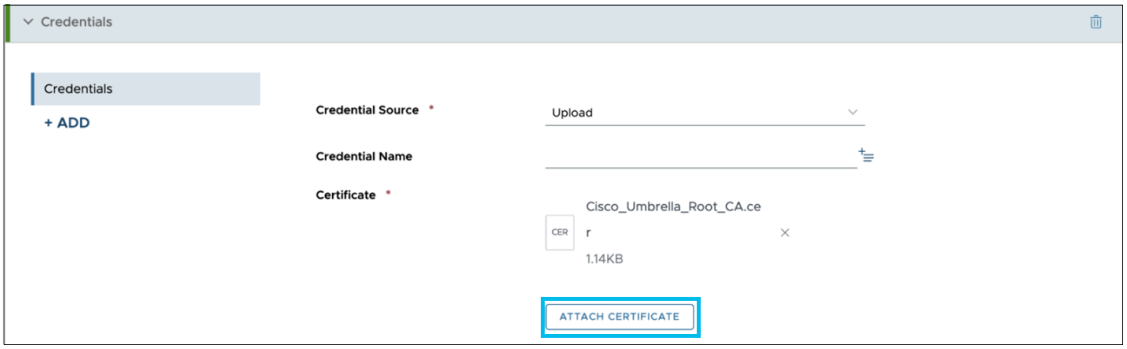


10. In the Credential section, do the following:

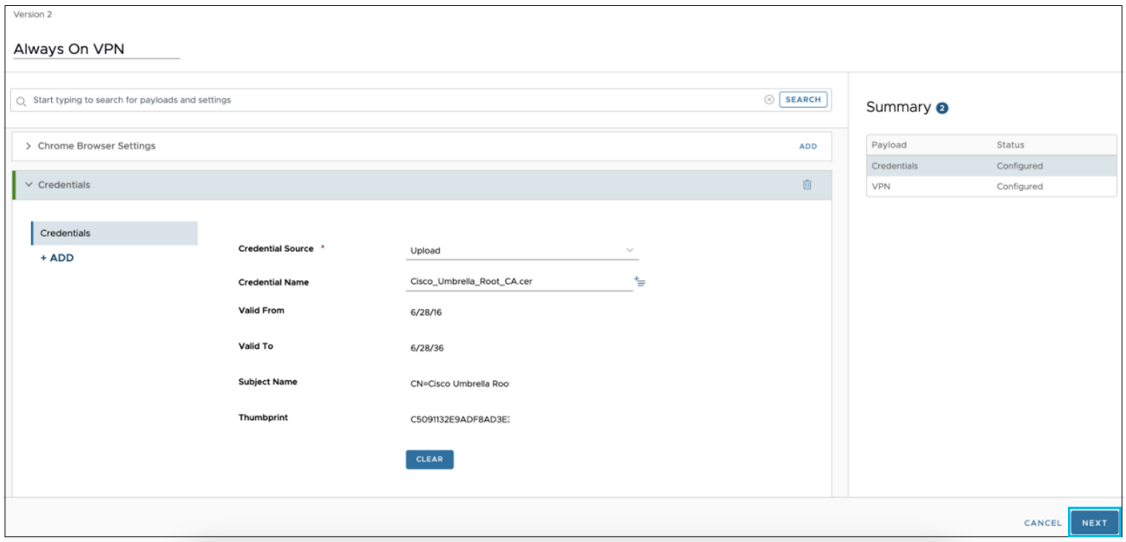
- From the **Credential Source** drop-down list, choose **Upload**.
- Click **Choose File** to browse and select the **Cisco_Umbrella_Root_CA Certificate** downloaded from Umbrella.

> **Note**
>
> In Umbrella, navigate to **Deployments** > **Configuration** > **Root Certificate**, expand **Cisco Root Certificate Authority**, and download the Cisco Umbrella root certificate, see Push the Umbrella Certificate to Managed Devices

- Click **ATTACH CERTIFICATE**.



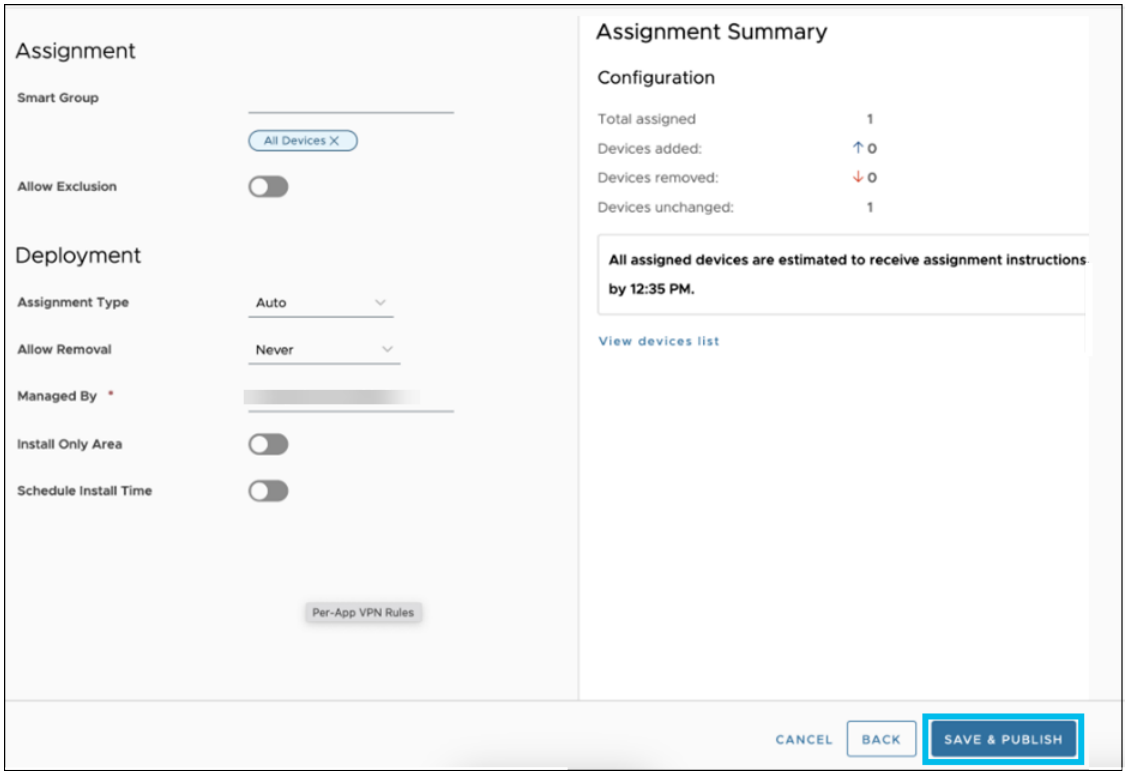
11. After successful upload of the certificate, the **Credential Name** would be added automatically and then click **Next**.



12. In the Assignment and Deployment profile settings screen, complete the fields, including the following:

- In the **Smart Group** field, choose the group of devices to which the Always On VPN profile is to be assigned.
- Select the appropriate deployment values. Choose **Auto** from the **Assignment Type** drop-down list, to deploy the profile to all device automatically.

13. Click **Save & Publish**.

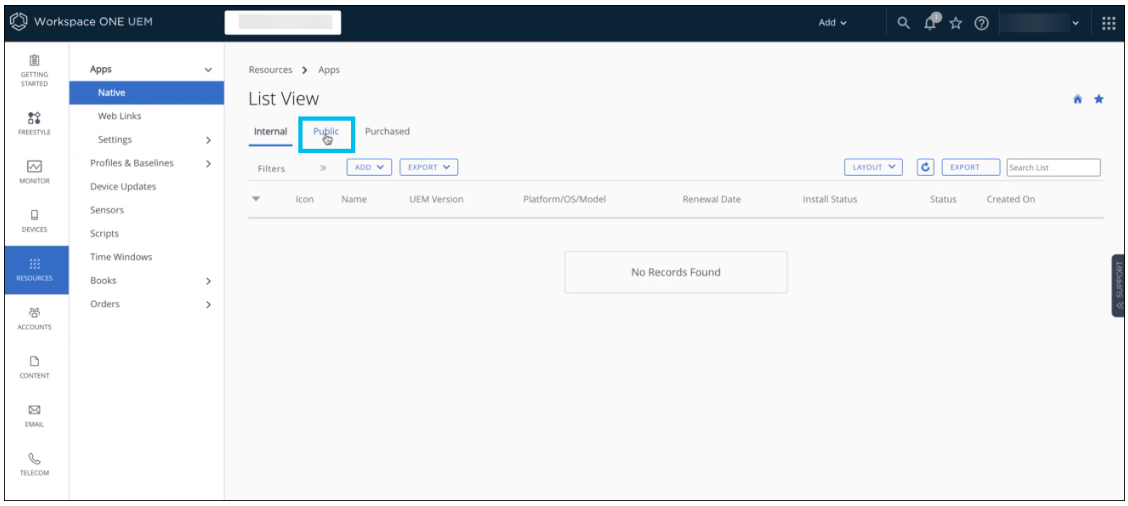


Add and Publish the Cisco Secure Client Application

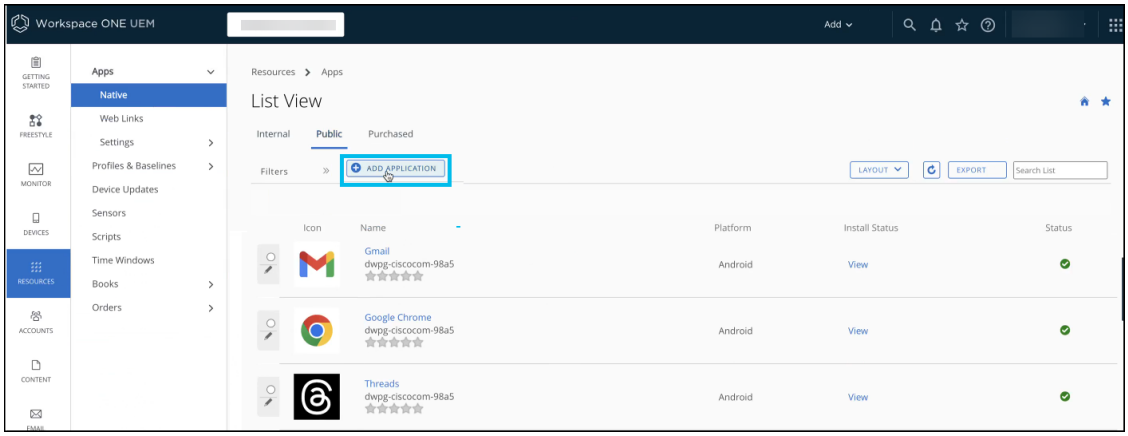
Provides instructions for adding and publish the cisco secure client application.

Procedure

1. In the **Workspace ONE UEM** console, navigate to **Resources** > **Native** > **Public**.

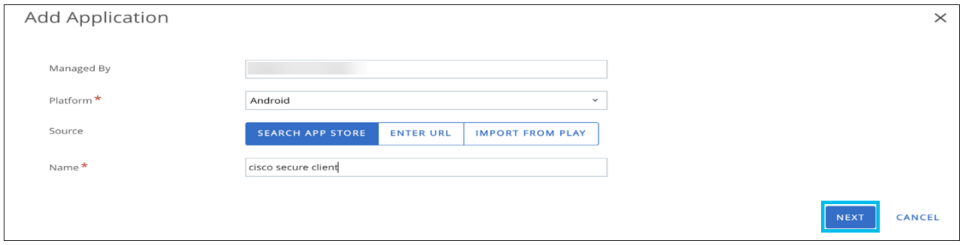


2. Click **Add Application**.

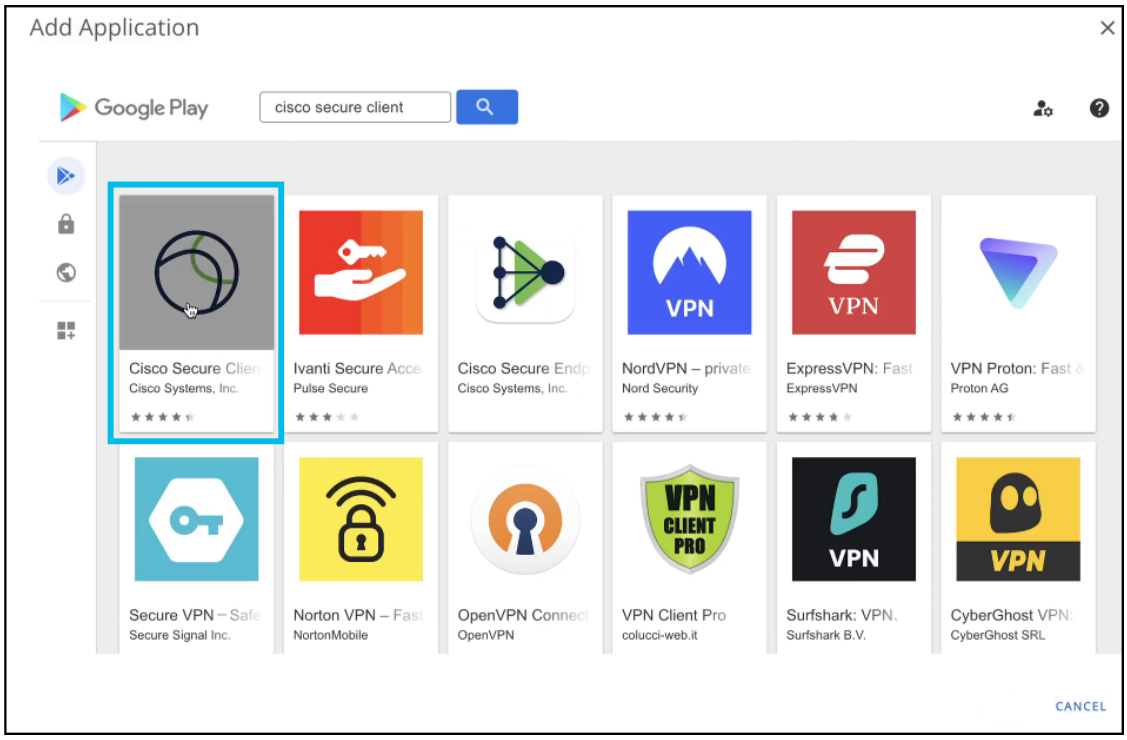


a. To add the **Cisco Secure Client** application, add the following details:

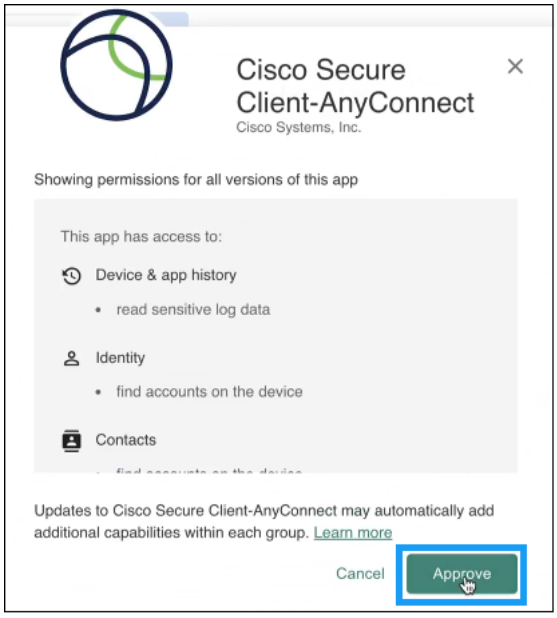
1. Enter **Managed By** field, choose the Organization Group that you set up to manage applications.
2. From the **Platform** drop-down list, choose **Android**.
3. In the **Source** field, select **SEARCH APP STORE** to search for the application in the app store.
4. In the **Name** field, enter *Cisco Secure Client* and click **Next**. Google Play launches within the console.



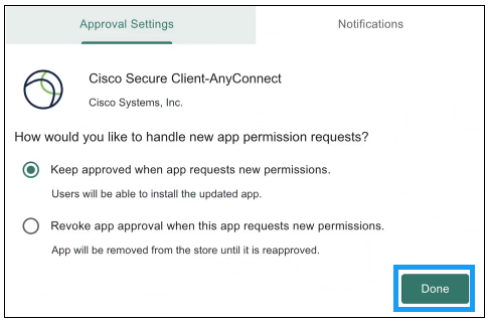
3. In the Google Play store, click the **Cisco Secure Client AnyConnect** application.



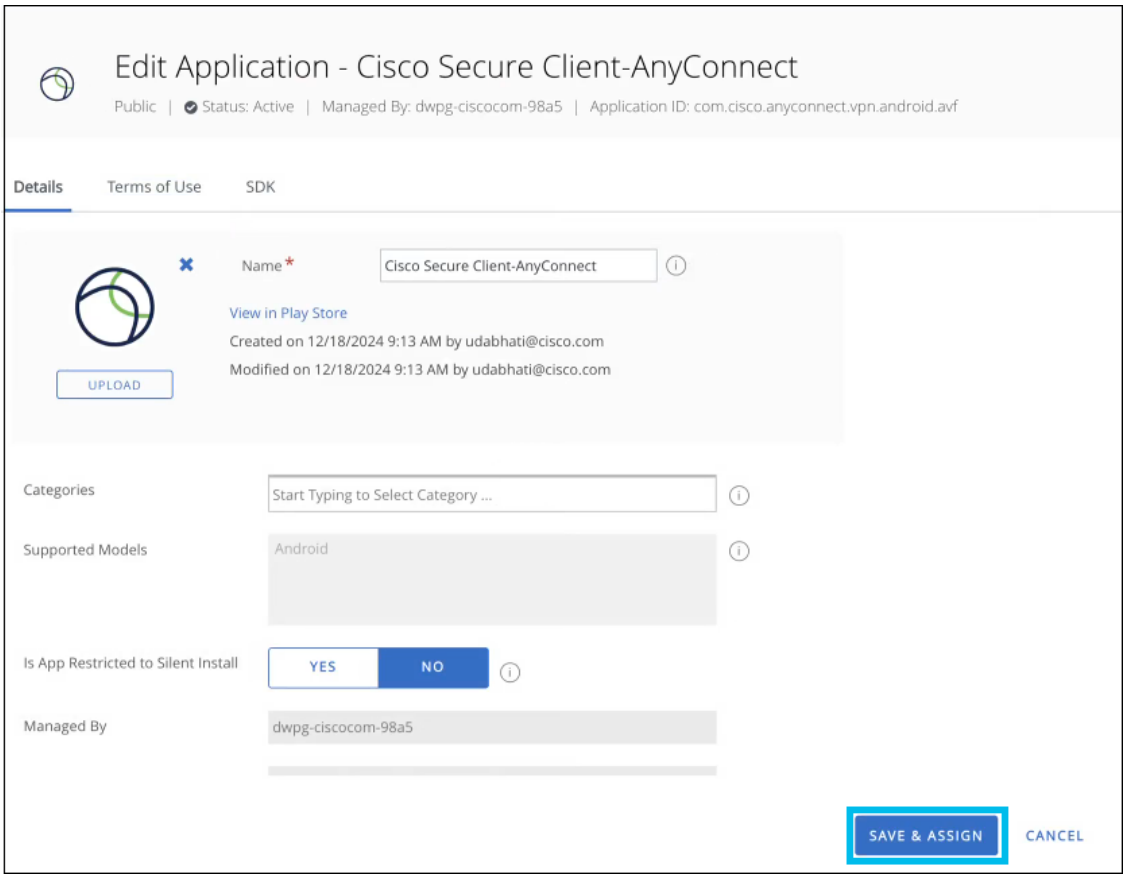
4. Click **Approve** to accept the permission for all versions of the application.



5. Click **Done** to handle the new app permission requests.

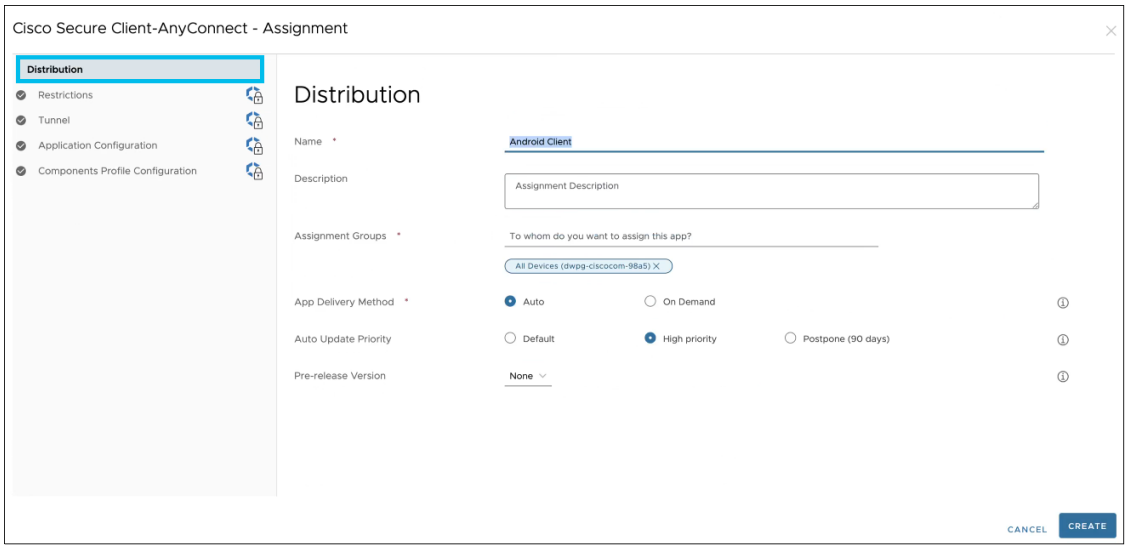


6. Now, click **Save & Assign**.

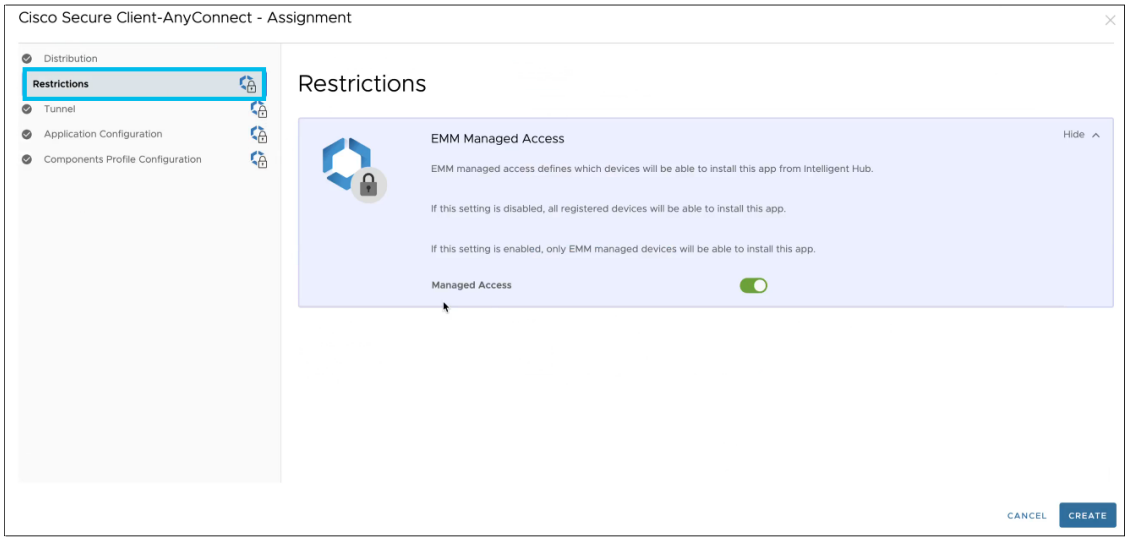


The Cisco Secure Client-AnyConnect Assignment Wizard appears:

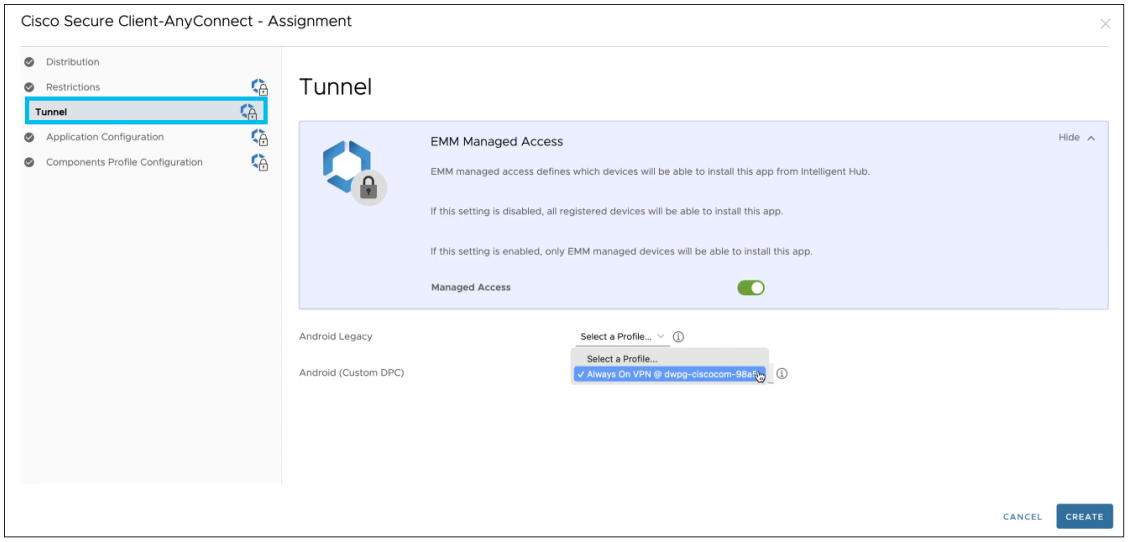
7. On the **Distribution** page, enter the necessary details to define how the application will be distributed. Click **Restrictions**.



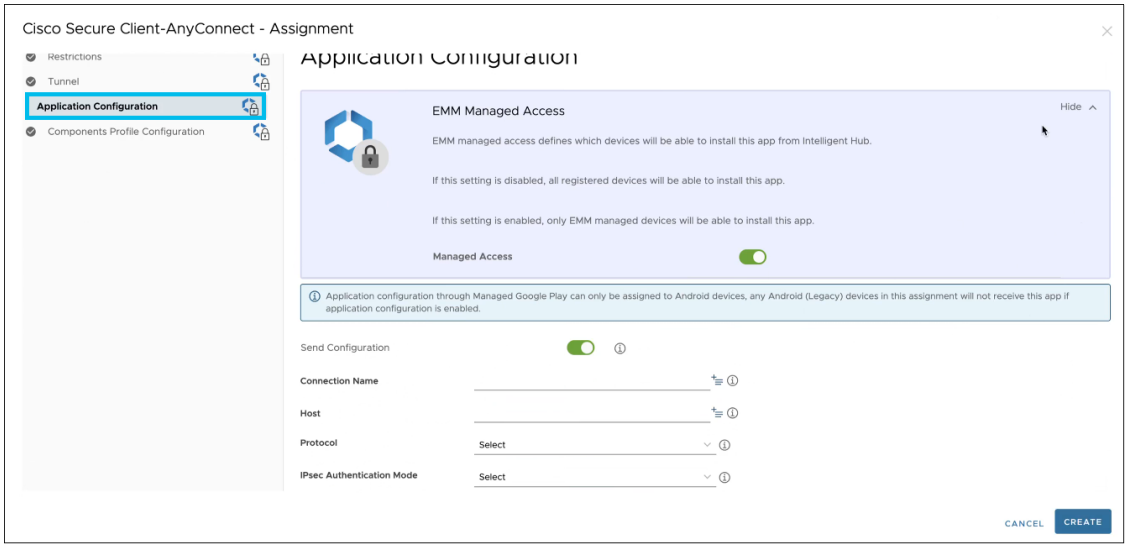
8. On the **Restrictions** page, enable the **Managed Access** button to allow only EMM managed devices to install the application. Click **Tunnel**.



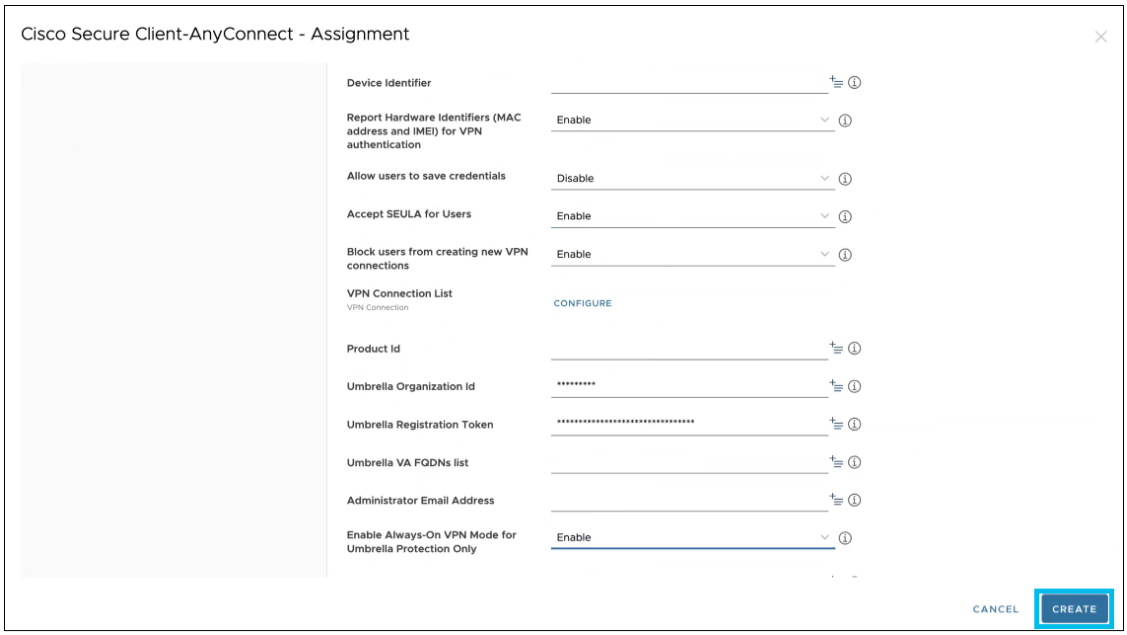
9. On the **Tunnel** page, from the **Android (Custom DPC)** drop-down list, choose the Always On VPN profile created in the Create Always On VPN Profile section. This enables the Always On VPN profile for the managed devices. Click **Application Configuration**.



The Application Configuration page appears.



10. On the **Application Configuration** page, complete the fields, including the following:
    - Leave the **Host** field empty, as the server details are taken from the profile.
    - From the **Accept SEULA For Users** drop-down list, choose **Enable** to prevent users from manually accepting the SEULA banner.
    - From the **Enable Always On VPN Mode for Secure Access Protection Only** drop-down list, choose **Enable** to allow the Cisco Secure Client application to automatically manage protection and seamlessly accept VPN connection requests when Secure Access protection is activated.
    - From the **Block users from creating new VPN connections** drop-down list, choose **Enable**.
    - Enter the application configuration details, such as, Secure Access Organization Id and Registration Token, by referring the **Android Config File** downloaded from the dashboard. For more information on how to download Android Config File, see Android Configuration Download.

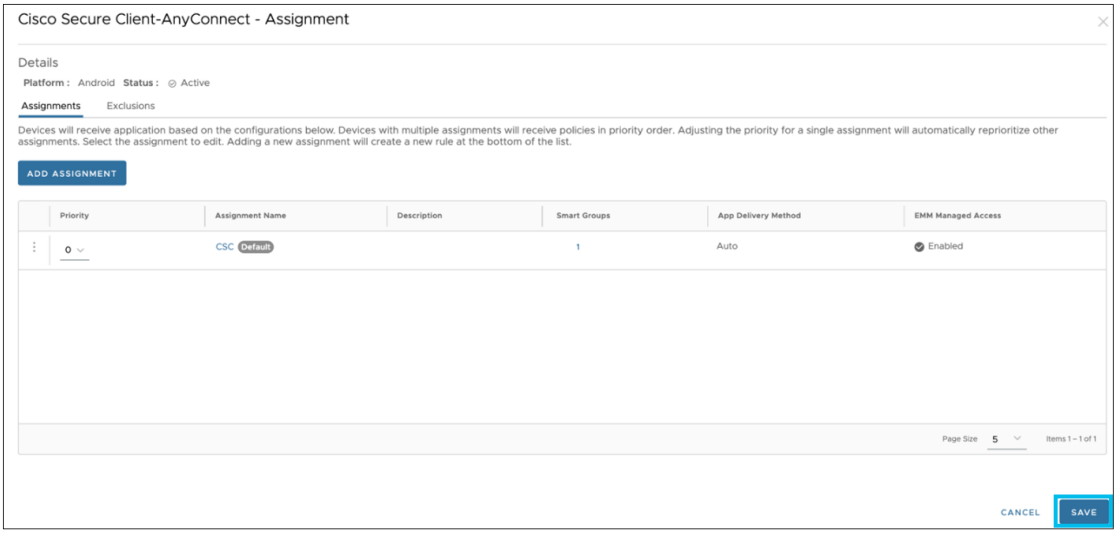


11. Click **Components Profile Configuration**.
12. Click **Create**.

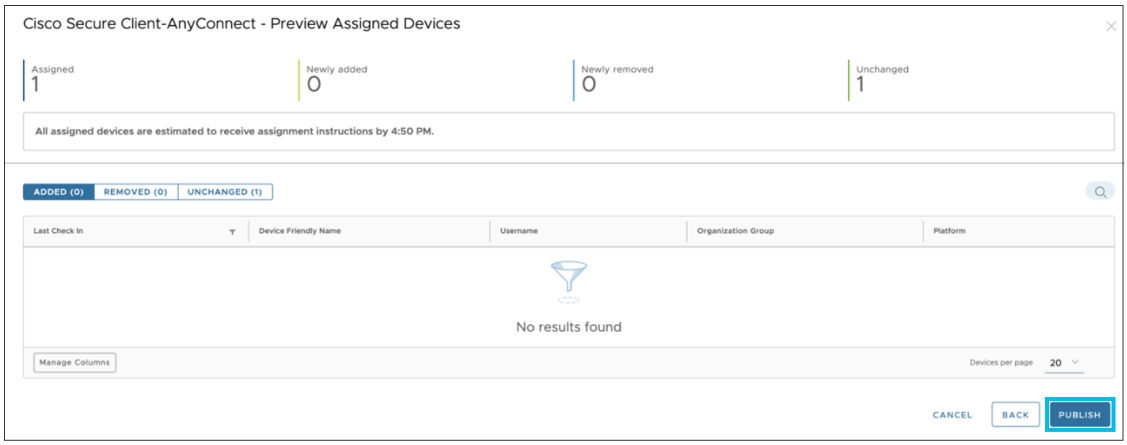


The Cisco Secure Client-AnyConnect app assignment is created.

13. Click **Save**.



14. Click **Publish** to publish the Cisco Secure Client Application.



What to do next

As the app delivery method is set to auto on the Distribution page the application gets installed automatically on the device and is displayed in both the console and your device.

Push the Cisco Root Certificate to Devices

Provides instructions for pushing the cisco root certificate to devices. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

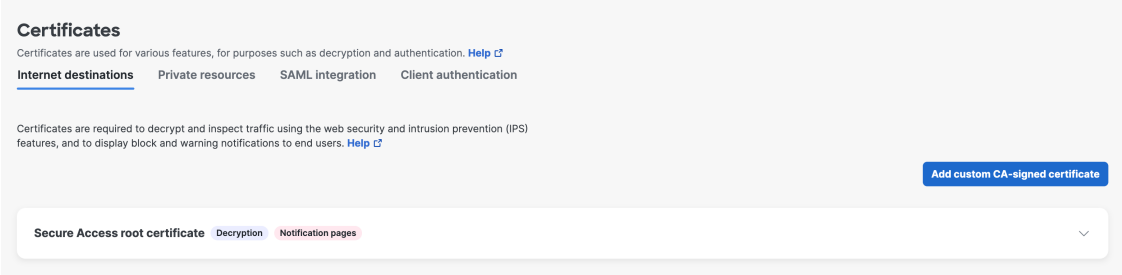
To support the display of block pages for HTTPS sites, HTTPS decryption if the Intelligent Proxy is used, and Trusted Network Detection if a VA is present you must push the Secure Access certificate to each of your managed devices.

Before you begin

- Full admin access to the Secure Access dashboard. See Manage Accounts.

Procedure

1. Navigate to **Secure** > **Settings** > **Certificate**.



2. Expand **Secure Access root certificate** and download the Cisco Secure Access root certificate.

   For more information about installing the root certificate, refer to Install the Cisco Secure Access Root Certificate.



3. Push the root certificate to all your devices from the MDM admin panel so that block pages can be displayed.

   This allows block pages for HTTPS sites to appear correctly, enables HTTPS decryption if the Intelligent Proxy is used, and enables Trusted Network Detection if a VA is present.

> **Note**
>
> If there is an Secure Access VA in your network and you want to use Trusted Network Detection, configure the VA as detailed in Configure Umbrella VA to Receive User-IP Mappings.

69 Manage Identities

Topics:

- Manage Identities

Describes the purpose and procedures for manage identities and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

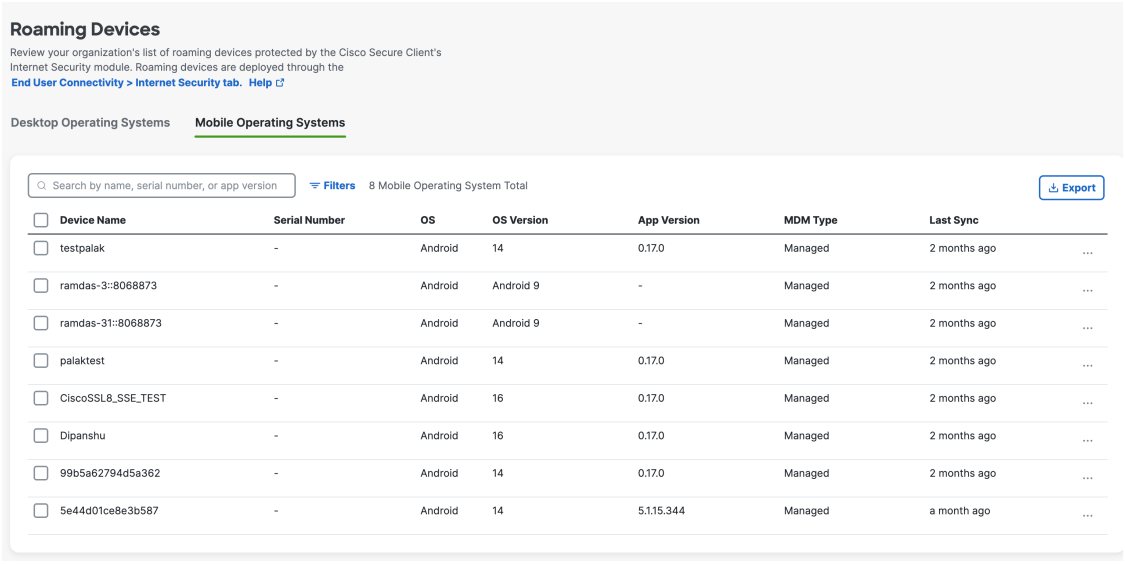
Manage Identities

Describes managing identities. To enable identity and be searchable in Secure Access, configure your Mobile Device Manager to share identity information. Identity can be any of the following based on what you choose to share with Secure Access:

To enable identity and be searchable in Secure Access, configure your Mobile Device Manager to share identity information. Identity can be any of the following based on what you choose to share with Secure Access:

- User email address
- Username
- Device serial number
- Any other unique device identifier

After you push the identities to Secure Access, they are listed in the Secure Access dashboard.



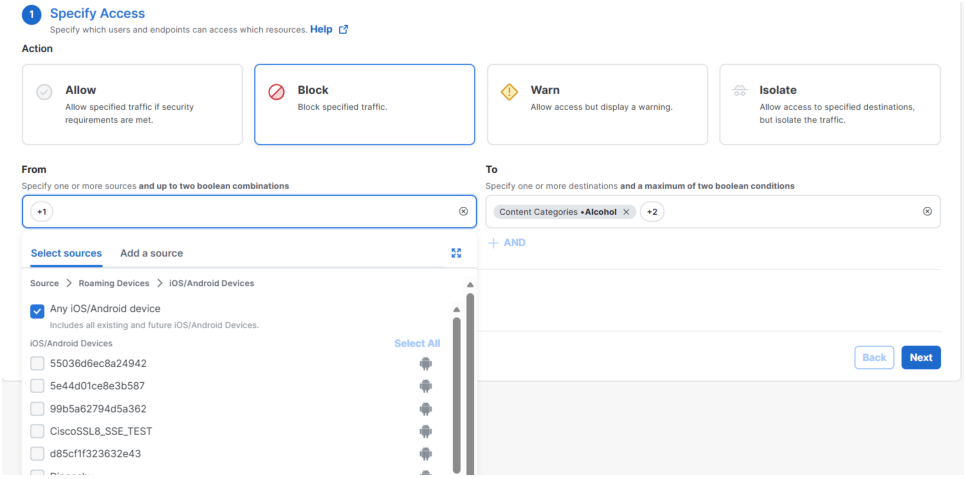
You can select user devices or use the user ID to search for them. To enable User Identities for Android clients, follow these steps.

Access User Identities on the Secure Access Dashboard

Describes accessing user identities on the secure access dashboard. You can configure internet access rules based on user identities or specific mobile devices.

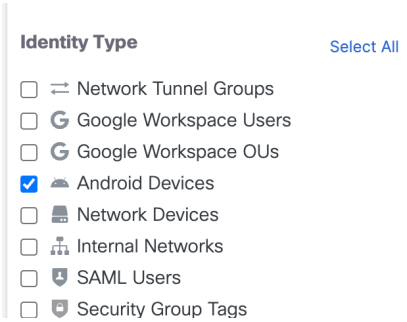
Configure Policy Based on User Identity

You can configure internet access rules based on user identities or specific mobile devices. The **Specify Access** page (**Secure** > **Access Policy** > **Add Rule** > **Internet Access**) allows you to select sources, such as roaming devices > Android devices, to include in your internet access rules.

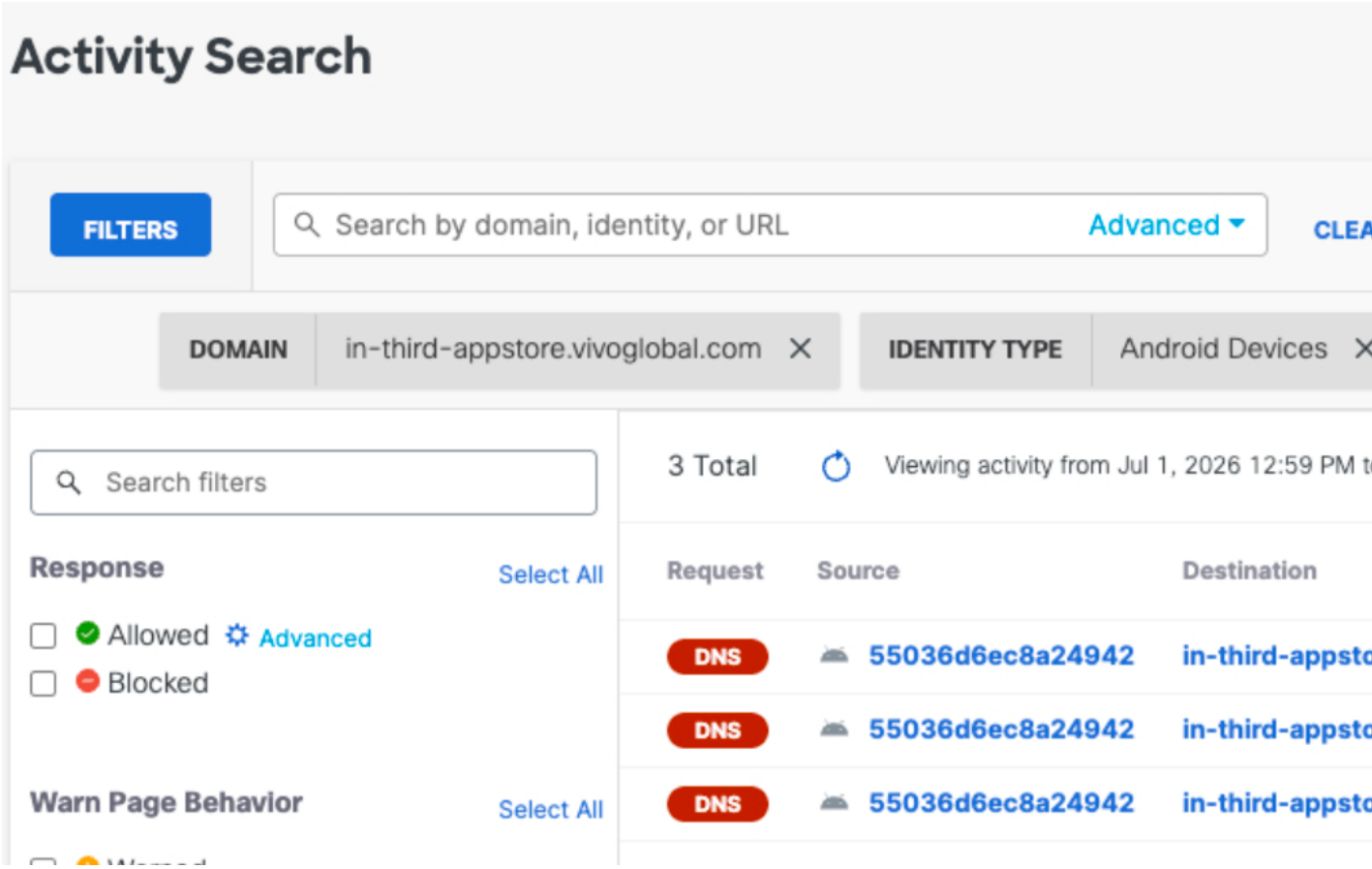


Monitor User Activity

As users start using the mobile device, you can monitor user activity through the Activity Search report. You can filter logs for the Android devices by selecting **Android Devices**.



You can see the user activity for the Allowed and Blocked.


Activity Search
FILTERS
Search by domain, identity, or URL
Advanced
CLEA
DOMAIN
in-third-appstore.vivoglobal.com
IDENTITY TYPE
Android Devices
Search filters
3 Total
Viewing activity from Jul 1, 2026 12:59 PM t
Response
Select All
Allowed
Advanced
Blocked
Warn Page Behavior
Select All
Request
Source
Destination
DNS
55036d6ec8a24942
in-third-appsto
DNS
55036d6ec8a24942
in-third-appsto
DNS
55036d6ec8a24942
in-third-appsto

70 Export Device Data to CSV

Topics:

- Export Device Data to CSV

Describes the purpose and procedures for export device data to csv and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

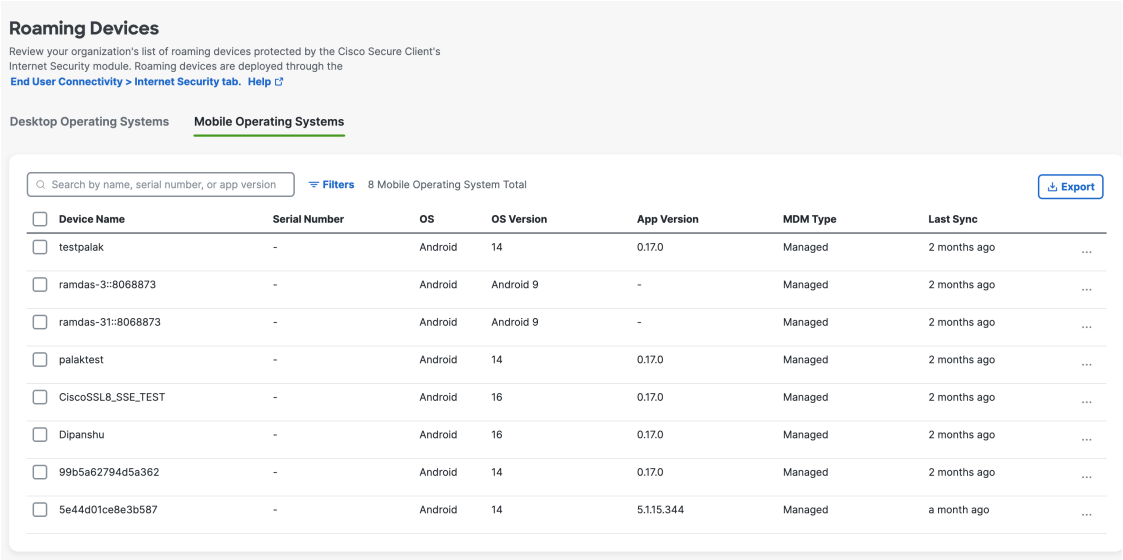
Export Device Data to CSV

Provides instructions for exporting device data to csv. The Export feature allows users to export device information to a CSV file, offering flexibility to export all devices, a specified number of devices, or devices that meet specific search criteria.

The Export feature allows users to export device information to a CSV file, offering flexibility to export all devices, a specified number of devices, or devices that meet specific search criteria. Once the export process is complete, the CSV file is downloaded to your **Downloads** folder.

Procedure

1. Navigate to **Resources** > **Sources and destinations** > **Roaming Devices**.
2. Click **Mobile Operating Systems**.



3. Choose one of the following export options as per your requirement:
   - Export All Devices
     - Click **Export** at the top of the table to export all devices.
   - Export Selected Devices
     - Check the required number of devices and click **Export Selected** to export a specific number of devices.
   - Export Devices Based on Search Criteria
     - Search by name, serial number, or app version in the search bar. To further refine your search, click **Filter** and specify a search criteria to filter the devices accordingly.
     - Click **Export** to export all the devices meeting the search criterial. Check the required number of devices, and click **Export Selected** to export a specific number of devices that meet the search criteria.

Once the export process is complete, the CSV file is downloaded to your **Downloads** folder.

71 Troubleshooting

Topics:

- Troubleshooting

Describes the purpose and procedures for troubleshooting and outlines related topics, requirements, and operational considerations in Cisco Secure Access. It also identifies related requirements, procedures, and operational considerations.

Troubleshooting

Describes troubleshooting. If you have difficulty validating the Secure Access module for Cisco Secure Client for Android OS after first installing it, review the following troubleshooting scenarios:

If you have difficulty validating the Secure Access module for Cisco Secure Client for Android OS after first installing it, review the following troubleshooting scenarios:

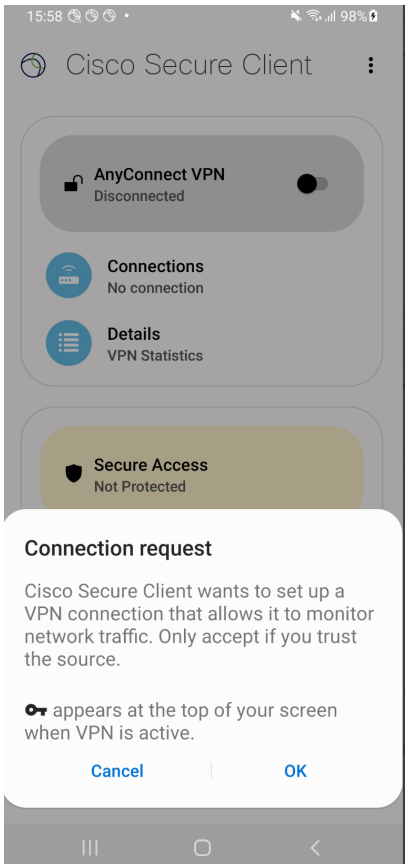
- First Launch of App
- Is this a VPN to Secure Access?
- An Internal Site Isn't Loading
- Configuration Issues
- Check for VPN Connection and Policy
- Check Block Page
- Get the Android ID
- Fail Close/Open Scenario
- Check Device Registration
- Missing CA Certificate
- Org ID on Policy Page is 0
- App Installation is Blocked
- Offboarding Users
- Known Issues

First Launch of App

Describes first launch of app. On the first launch, there should be a request for Cisco Secure Client VPN session as shown below. You must accept the connection request by clicking “OK” for the Secure Access protection to start.

On the first launch, there should be a request for Cisco Secure Client VPN session as shown below. You must accept the connection request by clicking “OK” for the Secure Access protection to start.

> **Note**
>
> **Mandatory Security Step**
>
> This cannot be bypassed; the behavior is built into Android OS for security reasons.

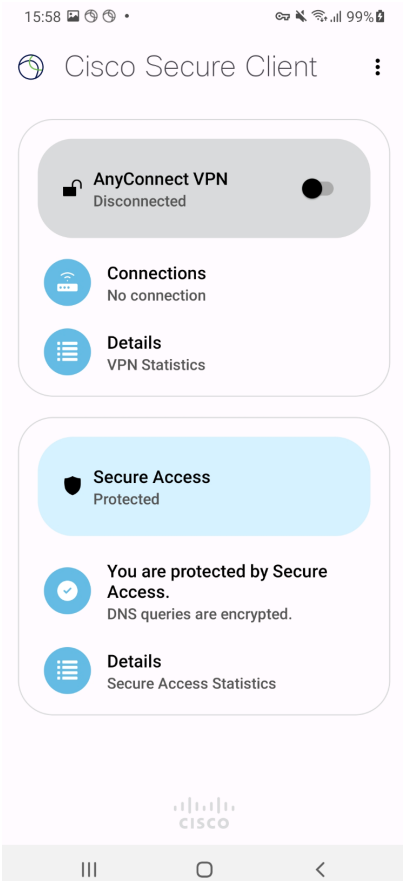


Is this a VPN to Secure Access?

Describes is this a vpn to secure access?. The Secure Access Module for Cisco Secure Client uses a VPN-like mechanism, but it is not in a traditional VPN.

The Secure Access Module for Cisco Secure Client uses a VPN-like mechanism, but it is not in a traditional VPN. This VPN-like mechanism is used to intercept DNS queries so that the module can process them (add metadata, encrypt and forward to Secure Access). The Android operating system's user interface does not show this distinction, so it appears as if a VPN were running.

When Secure Access protection starts, a green checkmark appears under the Secure Access UI subheading with the text “You are protected by Secure Access.”



An Internal Site Isn't Loading

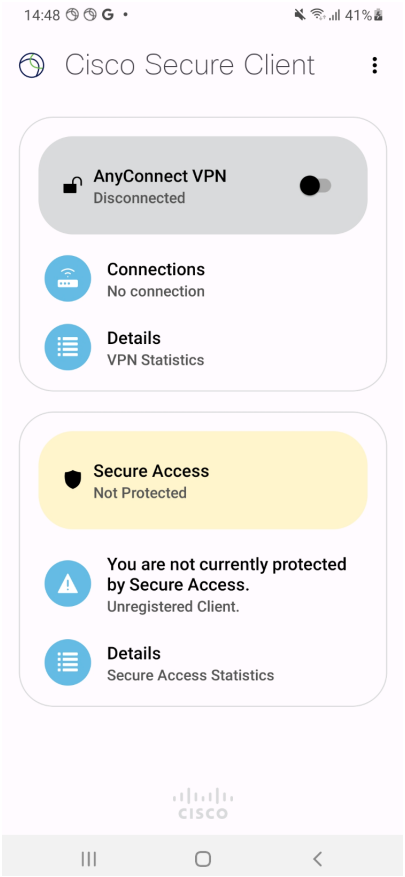
Describes an internal site isn't loading. The Secure Access module makes a best effort to automatically detect internal (intranet) sites and route DNS appropriately to the local DNS server. However, these mechanisms may not work in all scenarios.

The Secure Access module makes a best effort to automatically detect internal (intranet) sites and route DNS appropriately to the local DNS server. However, these mechanisms may not work in all scenarios. Therefore it's important to enter your internal / intranet domains in the Domain Management tools in the Secure Access dashboard. For more details, refer to Manage Domains.

Configuration Issues

Describes configuration issues. If the Secure Access Section in the Cisco Secure Client - AnyConnect app does not display a green checkmark, check the configuration details pushed from the MDM. If you don't have access, contact your administrator.

If the Secure Access Section in the Cisco Secure Client - AnyConnect app does not display a green checkmark, check the configuration details pushed from the MDM. If you don't have access, contact your administrator.



You can check if the configuration is available by clicking on the menu button at the top right in **Cisco Secure Client - AnyConnect** > **Diagnostics** > **Logging** and **System Information** > **System** > **Managed Configuration**.

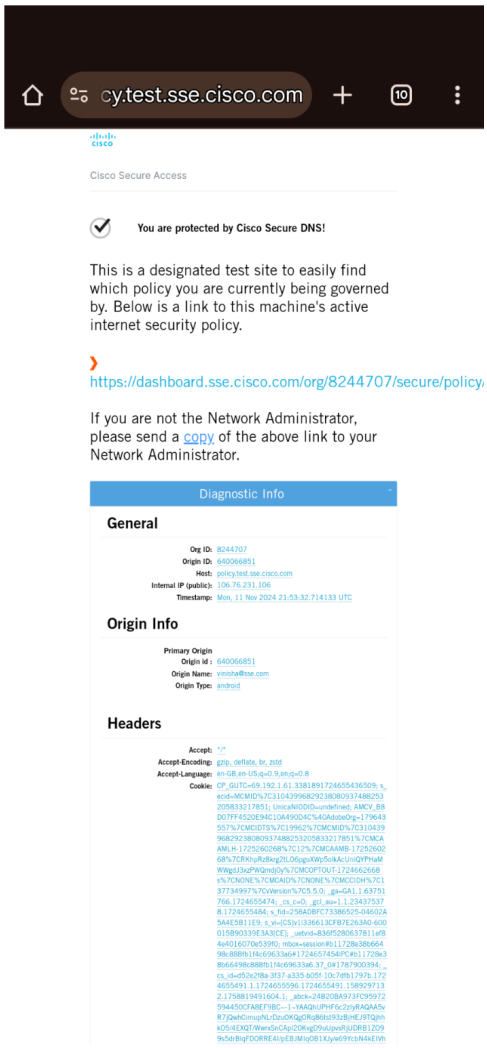
Verify that the managed configuration pushed by the administrator is available.

Check for VPN Connection and Policy

Provides instructions for checking for vpn connection and policy. Verify that the “key” icon (or something similar) is displayed in the notification panel for the VPN session created by Cisco Secure Client - AnyConnect.

Procedure

1. Verify that the “key” icon (or something similar) is displayed in the notification panel for the VPN session created by Cisco Secure Client - AnyConnect.
2. Open a browser.
3. Clear the cache.
4. Load `https://policy-debug.secureaccessfed.cisco/`. The page should load and display a URL to the active policy in the Secure Access dashboard. The format of the URL should be: `https://dashboard.secureaccessfed.cisco/org/<orgid>/#/configuration/policy/<policyid>`.
5. Verify that the organization ID displayed in the URL is the same as your Secure Access organization ID.



Check Block Page

Provides instructions for checking block page. Open http://www.internetbadguys.com/. You should see an Secure Access block page displaying the domain that was blocked along with the IP address of your device and the reasons for blocking.

Open `http://www.internetbadguys.com/`. You should see an Secure Access block page displaying the domain that was blocked along with the IP address of your device and the reasons for blocking. If you do not see the Secure Access block page, follow these steps:

Procedure

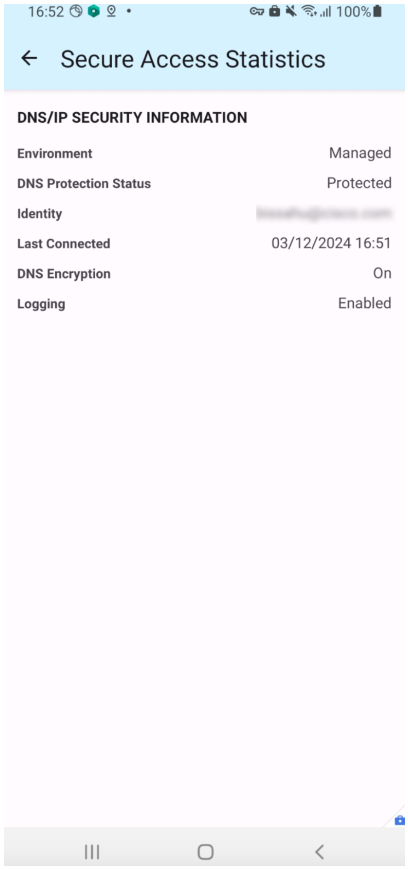
1. Select **Settings** > **Apps** > **Cisco Secure Client - AnyConnect** > **Force Close**.
2. Restart Cisco Secure Client - AnyConnect.
3. Reopen `http://www.internetbadguys.com/` and check for the Secure Access block page.

Get the Android ID

Provides instructions for get the android id. Launch Cisco Secure Client. Open Secure Access Security. Click Options, then open Secure Access Statistics. The Android ID is listed in that window.

Procedure

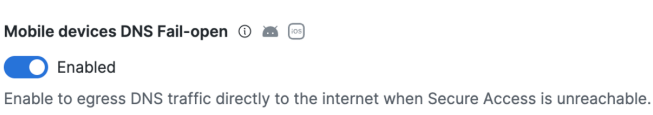
1. Launch Cisco Secure Client.
2. Open **Secure Access Security**.
3. Click **Options**, then open **Secure Access Statistics**. The Android ID is listed in that window.



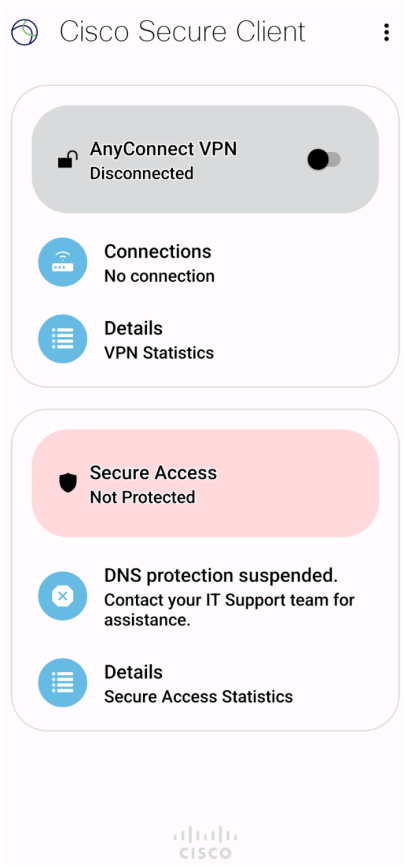
Fail Close/Open Scenario

Describes fail close/open scenario. Navigate to Cisco Secure Client settings Advanced , and enable the Mobile devices DNS Fail-open field to egress DNS traffic directly to the internet when Secure Access is unreachable.

Navigate to **Cisco Secure Client settings** > **Advanced**, and enable the **Mobile devices DNS Fail-open** field to egress DNS traffic directly to the internet when Secure Access is unreachable.



In case of internal errors, such as the Secure Access Resolver is not reachable or the DNSCrypt Certificate is not available, the Secure Access UI displays an error.



Check Device Registration

Provides instructions for checking device registration. Find the android_id for your Android device. Login to https://dashboard.secureaccessfed.cisco/, Choose the org id associated with the device.

Procedure

1. Find the `android_id` for your Android device.
2. Login to `https://dashboard.secureaccessfed.cisco/`,
3. Choose the `org id` associated with the device.
4. Navigate to **Resources** > **Roaming Devices** > **Mobile Operating Systems**.
5. Verify that the `android_id` is listed.

Missing CA Certificate

Provides instructions for missing ca certificate. If the Secure Access block page is not displayed but you see, instead, a warning about an insecure page, then there might be an error due to a missing Secure Access root certificate.

If the Secure Access block page is not displayed but you see, instead, a warning about an insecure page, then there might be an error due to a missing Secure Access root certificate.

Procedure

1. Download the Cisco Secure Access root certificate. For more information about downloading the root certificate, refer to Install the Cisco Secure Access Root Certificate.
2. Secure the device with your PIN, password or pattern lock.
3. Install the certificate you downloaded.
4. Select the certificate file.
5. Reload the block page in your browser.

Org ID on Policy Page is 0

Describes org id on policy page is 0. If the https://policy-debug.secureaccessfed.cisco/ URL shows 0 for the org id and bundle (policy) id, then refresh the page. Alternatively, clear the browser cache, try an incognito window, or try a different browser.

If the `https://policy-debug.secureaccessfed.cisco/` URL shows 0 for the org id and bundle (policy) id, then refresh the page. Alternatively, clear the browser cache, try an incognito window, or try a different browser.

App Installation is Blocked

Describes app installation is blocked. In order to download apps from the Google Play Store, a Gmail ID should be configured in the MDM.

In order to download apps from the Google Play Store, a Gmail ID should be configured in the MDM. If the ID is configured and the app still cannot be downloaded, the MDM admin may have chosen to disallow installation of apps from the Play Store.

Offboarding Users

Describes offboarding users. In order to fully remove an end user there are two steps: Delete the user from the Mobile Devices page in the Secure Access Dashboard.

In order to fully remove an end user there are two steps:

- Delete the user from the Mobile Devices page in the Secure Access Dashboard.
- Delete the Cisco Secure Access Module for Android OS from the user's device. This can be done by the MDM. The MDM app itself need not be removed from the user's device.

Known Issues

Describes known issues. App download fails in Google Play Store after enabling Cisco Secure client. This is a known limitation from Google on Android OS versions below v10. To avoid this, you must download Apps before enabling the Secure Access App.

- App download fails in Google Play Store after enabling Cisco Secure client. This is a known limitation from Google on Android OS versions below v10. To avoid this, you must download Apps before enabling the Secure Access App. Google has fixed this behavior in their Android OS 10. Check the issue tracker.
- In Android 10 and later, Google restricts reading serial numbers from the device. As a result, the *Serial number* field in the Secure Access dashboard displays “unknown” for Android 10 and later devices.
- Avoid using the *Wifi Assistant*; it may conflict with Cisco Secure Client - AnyConnect and DNS interception.
- Private DNS must be turned off for DNS interception to function properly.

- Click for information about Identify and Understand Unusual DNS Queries in Activity Reports.
- Huawei phones, when running in Work Profile mode, do not automatically start Cisco Secure Client - AnyConnect, even when the app was previously open. This does not apply to Huawei phones in Fully Managed mode.

Part V

Integrations

Topics:

- Secure Access Integrations

72 Secure Access Integrations

Topics:

- Integrate Catalyst SD-WAN with Secure Access

Describes the purpose and procedures for secure access integrations and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Integrate Catalyst SD-WAN with Secure Access

Describes integrating catalyst sd-wan with secure access. Cisco Catalyst SD-WAN integrates with Cisco Secure Access to share network context between the platforms for the purpose of applying consistent security enforcement for users, devices and workloads across the enterprise.

Cisco Catalyst SD-WAN integrates with Cisco Secure Access to share network context between the platforms for the purpose of applying consistent security enforcement for users, devices and workloads across the enterprise. Context-aware security policies become key for implementing and achieving a true zero-trust framework for the enterprise.

With this integration feature, administrators can automatically build tunnels with reliability to Secure Access from a Catalyst SD-WAN branch and share VPN ID/name context learned from the enterprise. Cisco Catalyst SD-WAN can be deployed and connected using either virtual or physical secure routers at branch offices, data center networks, and regional hubs. This integration allows IT teams to:

- Connect any user to any application, with integrated capabilities for multicloud, security, predictive operations, and enhanced network visibility on a Secure Access Service Edge (SASE)-enabled architecture.
- Ensure a predictable user experience for applications.
- Optimize Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS) connections.
- Offer integrated security, either on-premises or in the cloud.

This section describes how to enable inline context propagation, represented by VPN IDs.

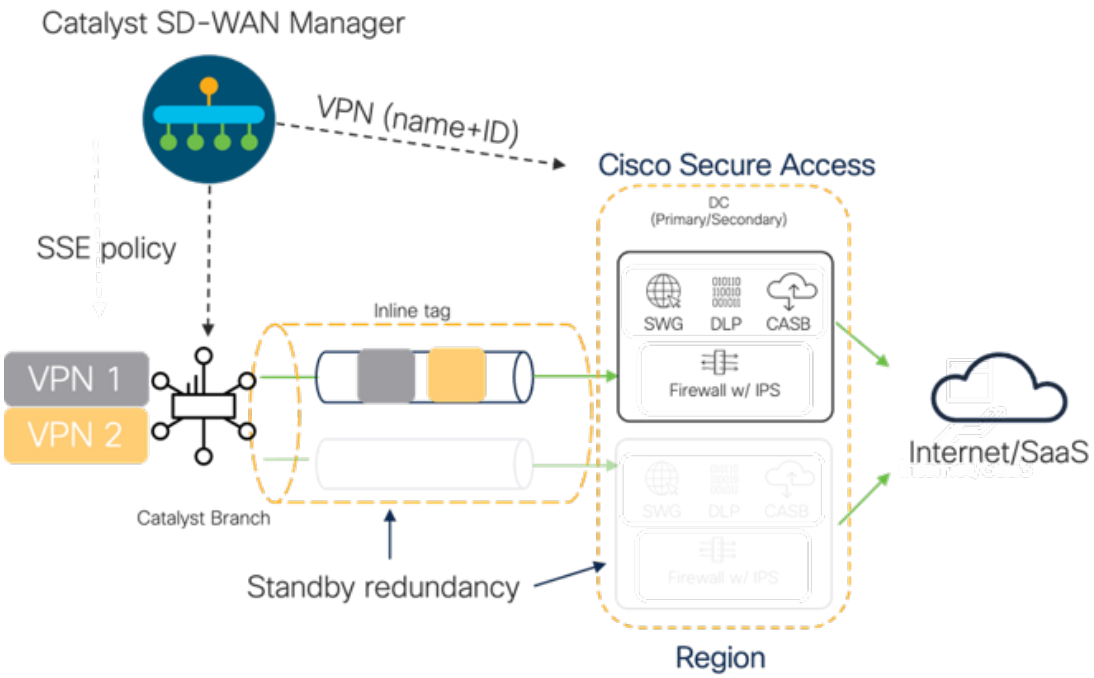
Solution Overview

Describes solution overview. Applying consistent security enforcement for users, devices, and workloads across the enterprise is top-of-mind for any CISO.

Applying consistent security enforcement for users, devices, and workloads across the enterprise is top-of-mind for any CISO. Whether the security enforcement is within the campus, branch, cloud, or data centers; consistent context-aware security policies are needed to implement and achieve a true zero-trust framework for an enterprise.

Use cases for context-aware security enforcement can revolve around employees, guests, or IoT networks behind a Catalyst SD-WAN branch that need to securely access internet/SaaS applications, with Cisco Secure Access providing cloud-based security enforcement.

With this integration, Cisco Secure Access administrators can use the rich enterprise context shared from Catalyst SD-WAN to configure simpler but granular policy control towards internet/SaaS for branch users.



Components and Prerequisites

Describes components and prerequisites. The components and prerequisites required for integrating Catalyst SD-WAN with Secure Access. The information in this integration section is based on the following components:

This topic describes the components and prerequisites required for integrating Catalyst SD-WAN with Secure Access.

Components Used

The information in this integration section is based on the following components:

- Cisco Catalyst SD-WAN release 20.15/17.15
- Cisco Secure Access
- Cisco ISE 3.1 patch or higher

Prerequisites

- A working knowledge of Cisco Catalyst SD-WAN configuration and features.
- A working knowledge of Cisco Secure Access.

Important

The information in this section is based on devices configured in a specific lab environment. All of the devices used started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any procedure or command.

Solution Workflow

Describes solution workflow. How context sharing between Catalyst SD-WAN and Secure Access works for VPN ID. Catalyst SD-WAN Manager integrates with Cisco Secure Access using SSE cloud credentials.

This topic describes how context sharing between Catalyst SD-WAN and Secure Access works for VPN ID.

1. Catalyst SD-WAN Manager integrates with Cisco Secure Access using SSE cloud credentials.
2. Cisco Secure Access learns VPN identities using APIs (out-of-band).
3. In Catalyst SD-WAN Manager, the Secure Service Edge policy group is configured to share VPN context in IPsec tunnels.
4. Once the tunnels are up, VPN ID context is shared in the IPsec metadata header inline.
5. VPN identities are leveraged in Secure Access internet access rules.
6. Packets with VPN ID context are then subject to Secure Access policy match as source objects.

Important

VPN ID context sharing is optional. Be aware that if the same VPN ID (*VPN 88* for example) is assigned across different branches, then traffic coming into Secure Access from these branches is subject to the same policy. A Secure Access policy rule cannot differentiate traffic between branches using the same VPN ID.

Related Information

Describes related information. Cisco Catalyst SD-WAN Getting Started Guide Cisco Catalyst SD-WAN Getting Started Guide Cisco Catalyst SD-WAN Security Configuration Guide Cisco Catalyst SD-WAN Security Configuration Guide

Cisco Catalyst SD-WAN Getting Started Guide Cisco Catalyst SD-WAN Getting Started Guide

Cisco Catalyst SD-WAN Security Configuration Guide Cisco Catalyst SD-WAN Security Configuration Guide

Cisco Catalyst SD-WAN Segmentation Configuration Guide Cisco Catalyst SD-WAN Segmentation Configuration Guide

Configure Context Sharing Between Catalyst SD-WAN and Secure Access

Describes configuring context sharing between catalyst sd-wan and secure access. Set up context sharing between Catalyst SD-WAN and Secure Access for VPN IDs.

This topic describes how to set up context sharing between Catalyst SD-WAN and Secure Access for VPN IDs.

Prerequisites

- Make sure DNS and ip domain-lookup command is configured on vpn0 for devices and cisco sd-wan manager with both having internet access.
- NAT needs to be enabled on the WAN of SD-WAN edge internet interface.
- Re-directing branch internet/SaaS-bound traffic from the branch LAN towards Cisco Secure Access can be done using the SSE default route in config-group or policy-group (data policy for specific application based redirect). See documentation for more details.
- Supported using config-group/policy-group infra only on Catalyst SD-WAN manager.

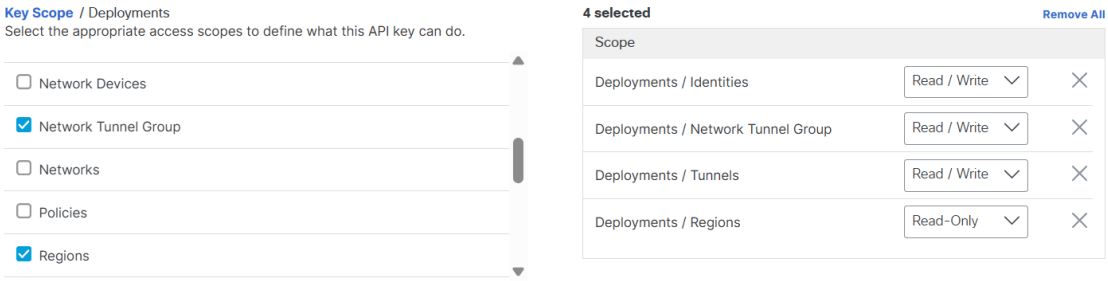
Generate API Key Pair for Context Sharing

Provides instructions for generating api key pair for context sharing. To configure the API keys needed for Catalyst SD-WAN Manager and Cisco Secure Access to share information, you need to generate key pair from Cisco Secure Access.

To configure the API keys needed for Catalyst SD-WAN Manager and Cisco Secure Access to share information, you need to generate key pair from Cisco Secure Access.

Procedure

1. Log into Cisco Secure Access and navigate to **Admin** > **Management** > **API Keys**.
2. In the upper right, click the **Add** button.
3. Expand the **Key Scope** section and select the options **Identities**, **Network Tunnel Group**, and **Tunnels**.
4. Assign **Read/Write** permissions to the selected scopes.
5. Set **Regions** to **Read Only**.



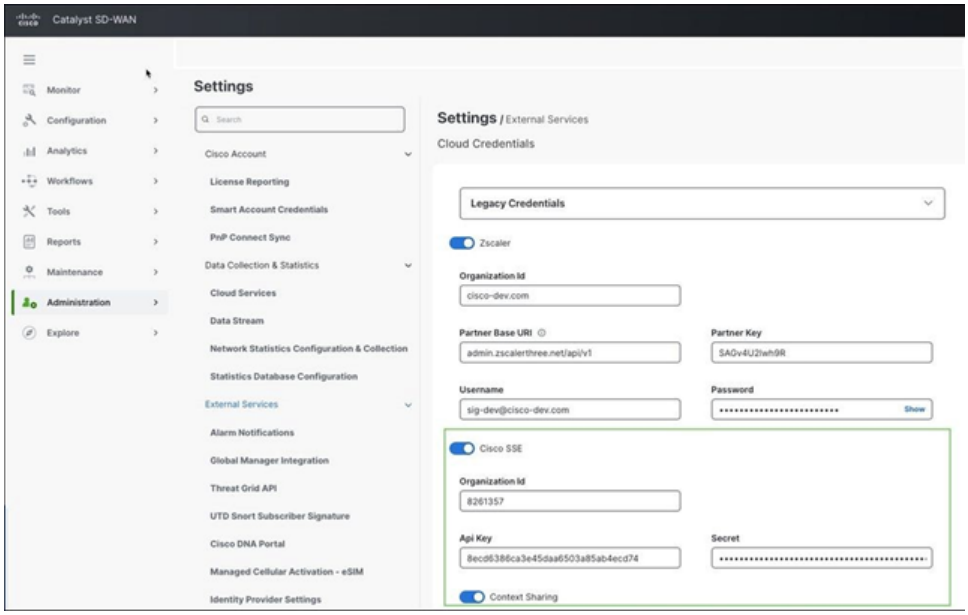
6. When all scopes are defined, click **CREATE KEY**. Copy and save the resulting key and secret.

Create Cisco Secure Access Credentials

Provides instructions for creating cisco secure access credentials. In another browser tab, log into Catalyst SD-WAN Manager, and navigate to Administration Settings Cloud Credentials

Procedure

1. In another browser tab, log into Catalyst SD-WAN Manager, and navigate to **Administration** > **Settings** > **Cloud Credentials**
2. Enable **Cisco SSE**.
3. Paste your Secure Access **Organization Id**, **Api key**, and **Secret**.
4. Enable **Context Sharing**.
5. Click **Add**.



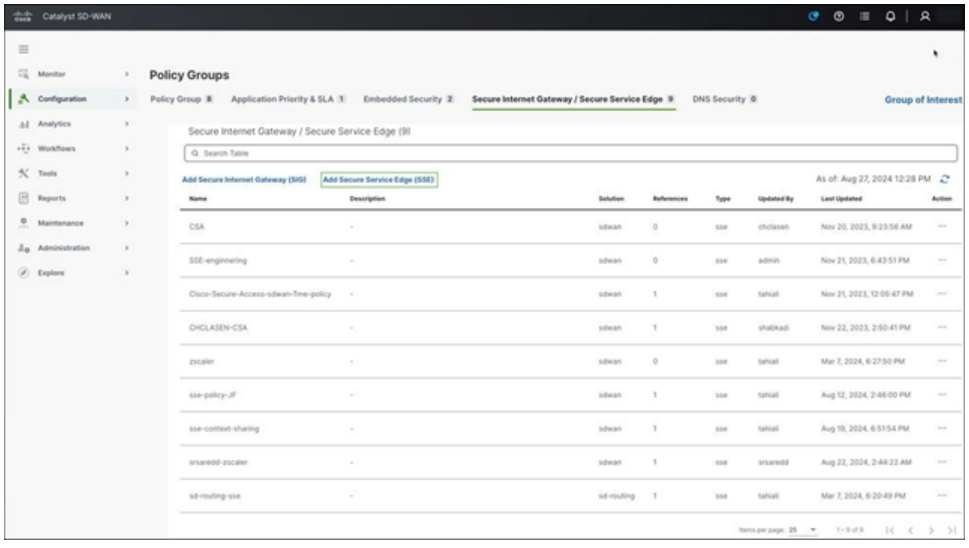
Add Secure Service Edge (SSE) Policy Group

Provides instructions for adding secure service edge (sse) policy group. Navigate to Configuration Policy Groups Secure Internet Gateway/Secure Service Edge .

Procedure

1. Navigate to **Configuration** > **Policy Groups** > **Secure Internet Gateway/Secure Service Edge**.
2. Click **Add Secure Service Edge (SSE)** to configure the SSE connectivity policy.

What to do next



Enable Context Sharing

Provides instructions for enabling context sharing. Under SSE Provider, select Cisco Secure Access. Under Context Sharing, enable VPN for context sharing for your SSE policy.

Procedure

1. Under SSE Provider, select **Cisco Secure Access**.
2. Under **Context Sharing**, enable **VPN** for context sharing for your SSE policy.
3. Click **Save**.

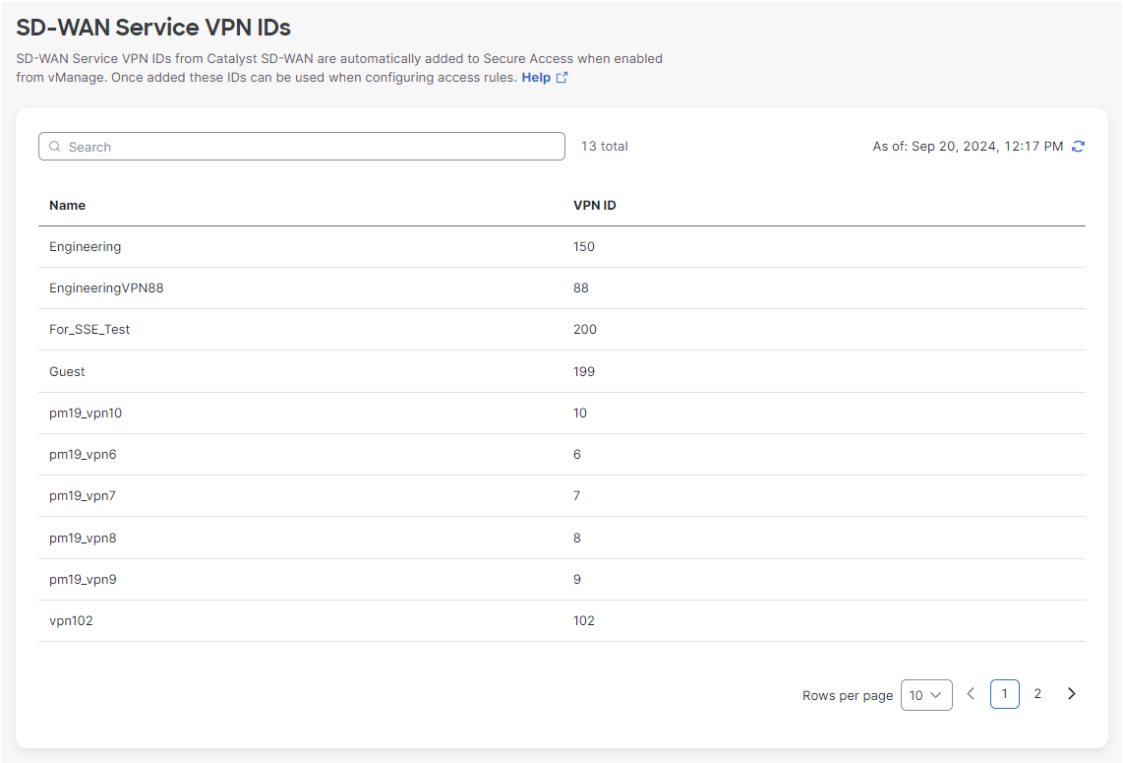
Verify Context Sharing in Secure Access

This topic describes how to verify context sharing between Catalyst SD-WAN and Secure Access for VPN IDs.

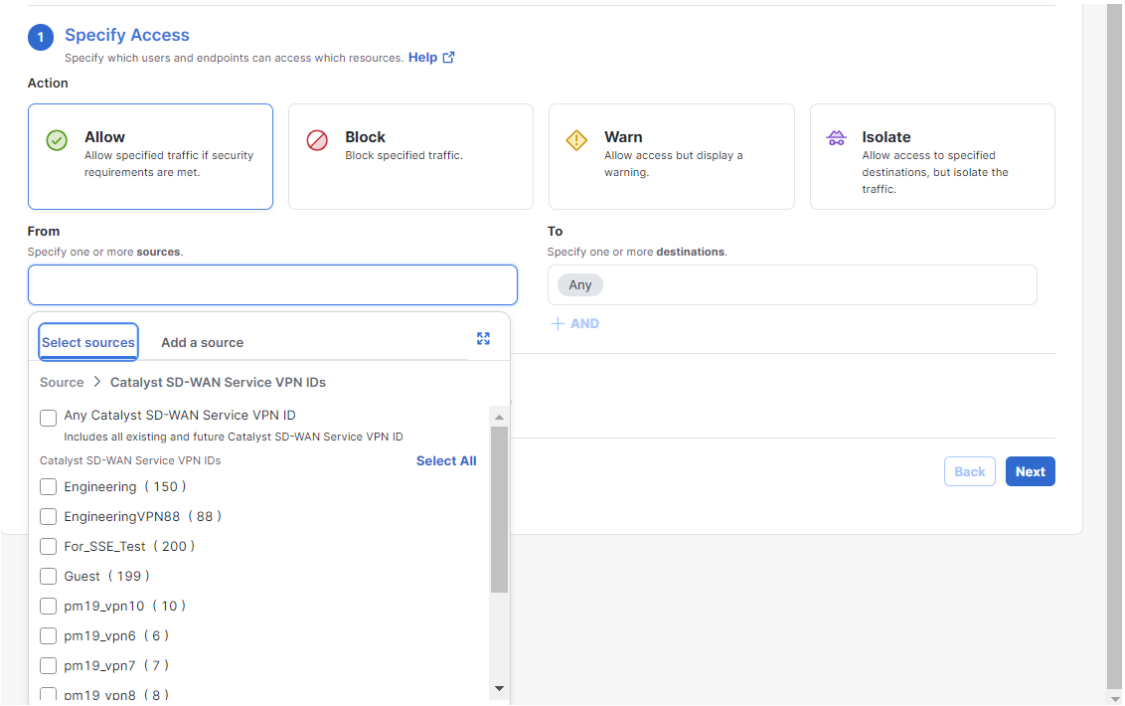
Service VPN IDs from Catalyst SD-WAN are automatically added to Secure Access as source resources when enabled from the SD-WAN Manager. Once added, these VPN IDs can be used when configuring access rules.

Procedure

1. Navigate to **Resources** > **Sources and Destinations** > **SD-WAN Service VPN IDs** to verify that the VPN IDs are shared as resources.



2. Navigate to **Secure** > **Policy** > **Access Policy**.
3. Click the **Add Rule** drop down and choose **Internet Access** to verify that the VPN IDs are shared as source objects for internet access rules.



4. From the **Select sources** drop down, choose **Catalyst SD-WAN Service VPN IDs** as a rule source.

   From there, you can select **Any Catalyst SD-WAN Service VPN ID**, which will include all existing and future VPN IDs in the rule. Alternately, you can select any (or all) existing VPN IDs for more granular internet access rules.

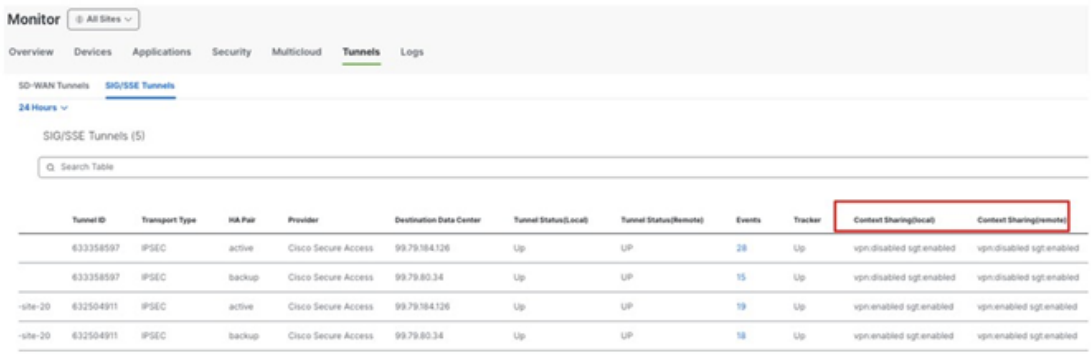
Monitor Context Sharing in SD-WAN Manager

Provides instructions for monitoring context sharing in sd-wan manager. You can view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device.

You can view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device.

Procedure

Under SD-WAN Manager Tunnel monitoring Dashboard.



Monitor Secure Access Tunnels using the CLI

Describes monitoring secure access tunnels using the cli. To view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device, use the show sse all command.

To view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device, use the `show sse all` command.

```
Device# show sse all

**************************************
   SSE  Instance Cisco-Secure-Access
**************************************
Tunnel name : Tunnel15000001
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN

Tunnel name : Tunnel15000002
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Backup
Local state: Up
Tracker state: Up
Destination Data Center: 44.241.136.173
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN
```

Activity Search in Secure Access

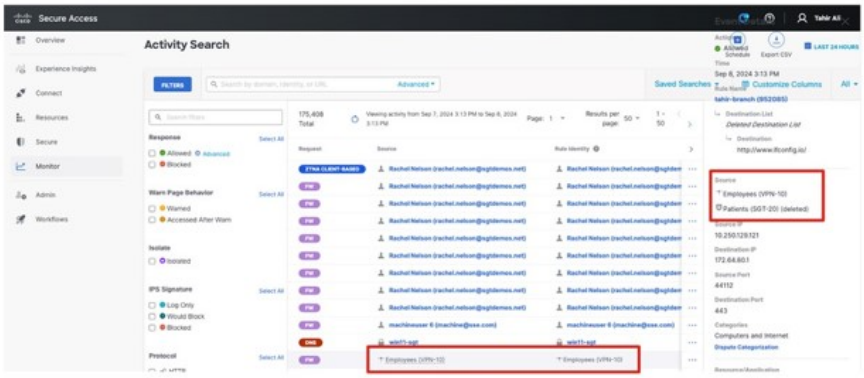
Provides instructions for activity search in secure access. To search for activity from the sources in your environment over a selected time period, use the Activity Search report. The report lists all security (and non-security) activity for the sources reporting to Secure Access for the selected time period.

To search for activity from the sources in your environment over a selected time period, use the Activity Search report. The report lists all security (and non-security) activity for the sources reporting to Secure Access for the selected time period.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.

   This takes you to the default view of the Activity Search report, which lists all of your identities and the internet requests or traffic events for your organization, tracked over time.



2. Hover over individual column values to apply it as a search filter or to exclude it from the search.

Part VI

Reports

Topics:

- Monitor Secure Access with Reports
- Remote Access Log Report
- Activity Search Report
- Security Activity Report
- Total Requests Report
- Activity Volume Report
- App Discovery Report
- Top Destinations Report
- Top Categories Report
- Cloud Malware Report
- Data Loss Prevention Report
- Admin Audit Log Report

73 Monitor Secure Access with Reports

Topics:

- Export Report Data to CSV
- Bookmark and Share Reports
- Report Scheduling
- Schedule a Report
- Update a Scheduled Report
- Report Retention

Introduces monitoring secure access with reports. Use Cisco Secure Access reports to monitor your Secure Access deployment and to better understand your Secure Access usage. Gain insights into request and block activity, determining which of your sources are generating blocked requests.

Use Cisco Secure Access reports to monitor your Secure Access deployment and to better understand your Secure Access usage. Gain insights into request and block activity, determining which of your sources are generating blocked requests. Reports help build actionable intelligence in addressing threats including changes in usage trends over time.

Available Reports

- **Remote Access Logs** – Lists users that have remotely connected to Secure Access and requested access to destinations.
- **Activity Search** –Search for activity from the sources in your environment over a selected time period.
- **Security Activity** –Lists security-related activity in your environment over a selected time period.
- **App Discovery** –Provides information about the cloud apps in use in your environment.
- **Top Destinations** –Lists the top traffic-generating sources over the selected time period. Filterable by source and destination.
- **Top Categories** –Lists the most popular security and content categories for your organization over the selected time period.
- **Data Loss Prevention** –Lists security events related to content classified as personally identifiable or sensitive information.
- **Cloud Malware** –Lists malicious files detected within your organization and provides details of the potential risk and exposure these files present.
- **Admin Audit Log** –Lists a record of any configuration changes made to your settings by any of your Secure Access administrators.

Export Report Data to CSV

Provides instructions for exporting report data to csv. Some reports let you export the results of a query to the CSV format.

Some reports let you export the results of a query to the CSV format. This lets you create other reports and graphs by feeding this data to other tools.

> **Note**
>
> The timezone of exported data is always the timezone selected for your account. You can change this for your account at **Admin** > **Accounts**.

Exportable reports:

- Activity Search
- Top Destinations
- Top Categories
- Top Identities
- Data Loss Prevention
- Cloud Malware

Troubleshooting

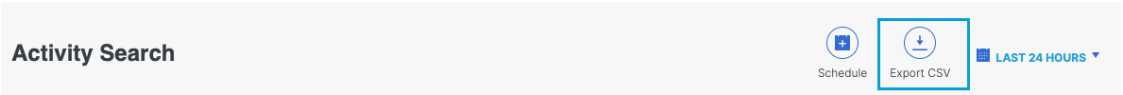
Depending on the time range and filters applied to the exported report, some report exports may take a very long period of time to generate and, in some cases, will time out. However, the 'time out' is not reflected in the dashboard. Instead, status is set to "Generating..." and persists. The report remains in this state without resolution. Typically, this happens somewhere between 12 to 24 hours after the report export is first begun. If this situation occurs, re-run the report export with a shorter date range, or more filters applied.

Before you begin

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

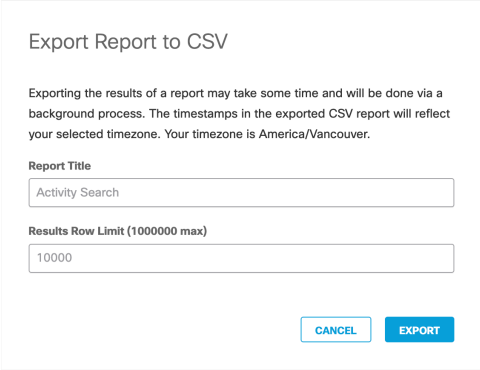
Procedure

1. Navigate to **Monitor** > **Reporting** > **report** and click **Export CSV** (or, in the case of the Data Loss Prevention and Cloud Malware reports, **Download**).

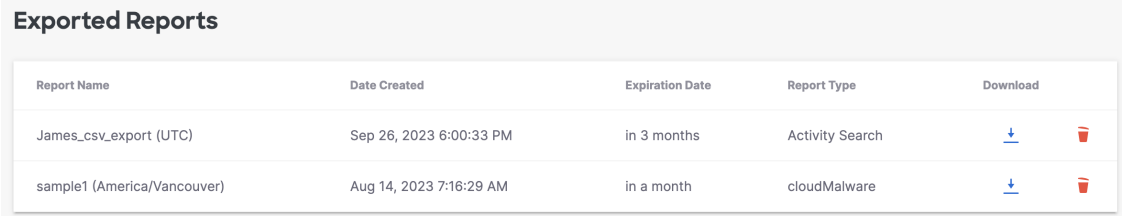


2. Give your report a good **Report Title**, add the number of rows of data to be returned, and click **Export**.

> **Note**
>
> When exporting to CSV, data is limited to a maximum of 1,000,000 rows. Due to the queue-based processing system, reports may experience significant latency. To minimize wait times, consider running reports for shorter time periods, reducing the number of rows to be exported, or applying more detailed filters. For efficient management of large datasets, check the last row of the initial report and then run the report again from that point for the next segment of data.



3. When you click **Export**, you are taken to the Exported Reports page, where you can download your CSV file.



4. Click the **Download** icon ( ).

   Your CSV file is automatically downloaded.

Bookmark and Share Reports

Describes bookmark and share reports. Secure Access stores the report state in the URL, making it easy to share a report with colleagues or bookmark a report for future use.

Secure Access stores the report state in the URL, making it easy to share a report with colleagues or bookmark a report for future use.

Procedure for Bookmark and Share Reports

Provides instructions for procedure for bookmark and share reports. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

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

Procedure

1. Navigate to **Monitor** > **Reports** > **report**.
2. Filter the report to display the data you need.
3. Use your browser's bookmark function. When you retrieve the bookmark the report will have the same filters applied. You can also share the URL of the page with any colleague in your organization with access to your dashboard. If the report has a relative date filter–last 24 hours, last 7 days, and so on–the relative date is applied. If the report has an absolute date filter (for example, Jan 7, 2019), the absolute filter is applied.

Report Scheduling

Describes report scheduling. Various reports in Secure Access can be configured so that Secure Access regularly emails you a summary of that report. You can configure filters for these reports so that they only contain the information you want.

Various reports in Secure Access can be configured so that Secure Access regularly emails you a summary of that report. You can configure filters for these reports so that they only contain the information you want. Each emailed report includes an HTML version of the report, a .ZIP file containing a CSV file with the entire data set, and a link to Secure Access and the report. See Schedule a Report.

Reports can be scheduled so that you receive an email daily, weekly, or monthly.

Note

You can unsubscribe from a report email through the **Unsubscribe** link at the bottom of every report email.

You can schedule the following reports:

- **Activity Search** –Activity from the identities in your environment over a selected time period. Filterable by identity name, destination, source IP, response, content category, and security category.
- **Total Requests** –Total requests for destinations from your organization over the selected time period. Filterable by identity.
- **Activity Volume** –Total queries within your organization broken down by security categories and results over the selected time period.
- **Top Destinations** –A list of the top traffic-generating identities over the selected time period. Filterable by identity and destination.
- **Top Categories** –A list of the top content categories for your organization over the selected time period. Filterable by identity and response.
- **Cloud Malware Report** –Provides an overview of malicious files within your environment and details the potential risk and exposure these files present.

Important

Cisco Secure Access uses SparkPost as the service to deliver email. Some mail filters, either at the local level or even at a transport layer (like an ISP) may block communications from SparkPost as marketing-related spam. If after scheduling your reports you do not receive them, check the spam filter at your mail server gateway. Whether your mail server gateway is hosted locally or in the cloud, it's likely the email was quarantined at that level.

Secure Access sends its reports from scheduled-reports-feedback@opendns.com.

Schedule a Report

Provides instructions for schedule a report. When scheduling a report, it's important to select filters so that you receive only the data that you want and that your reports don't exceed 10,000 rows–the limit of an emailed report.

When scheduling a report, it's important to select filters so that you receive only the data that you want and that your reports don't exceed 10,000 rows–the limit of an emailed report. As well, you want your scheduled report to be digestible and actionable by recipients. If you choose not to add filters, the report will apply to all traffic types for that report across your entire environment and may contain too much data to be readily read and interpreted by the recipient. With scheduled reports, you select filters for the report before you run the Schedule wizard.

> **Note**
>
> Once scheduled, if you do not receive the report, check the spam filter at your mail server gateway–whether it is hosted locally or hosted in the cloud. It's likely that the email was quarantined at that level.

Before you begin

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

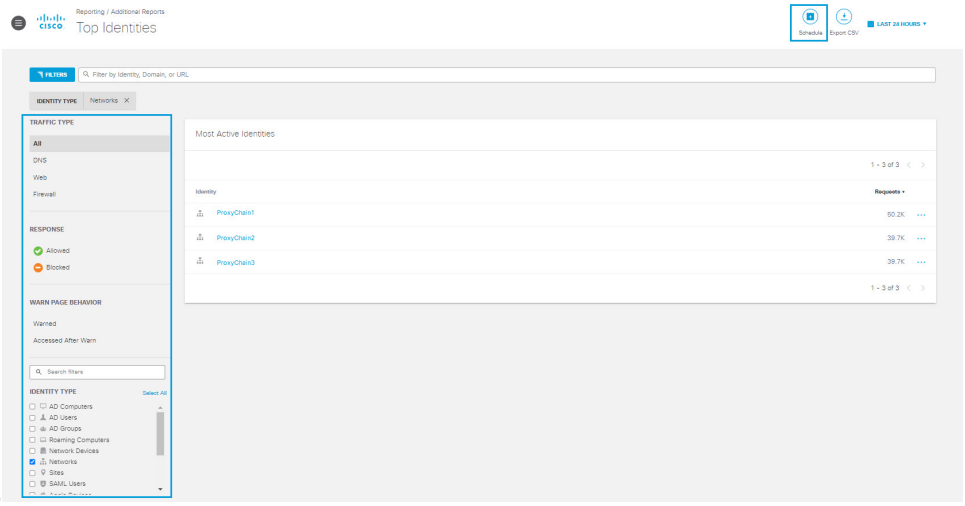
Procedure

1. Navigate to **Montior** > **Reporting** and select the report you want to schedule.

   For a list of schedulable reports, see Schedule Reports. (Screenshots in these instructions use the Top Identities report as an illustrative example.)

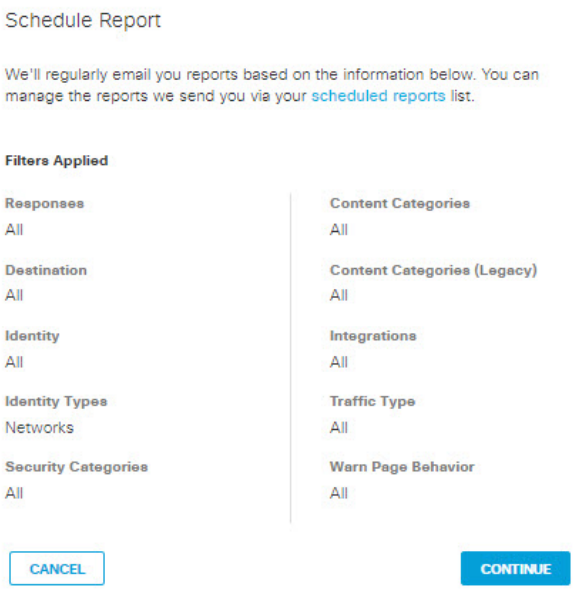
2. Select filters for the report and then click **Schedule**.

   Filters are applied to the report and the Scheduling wizard opens.



> **Note**
>
> The Top Threats report does not provide filters.

3. In the wizard, review filters and click **CONTINUE**.

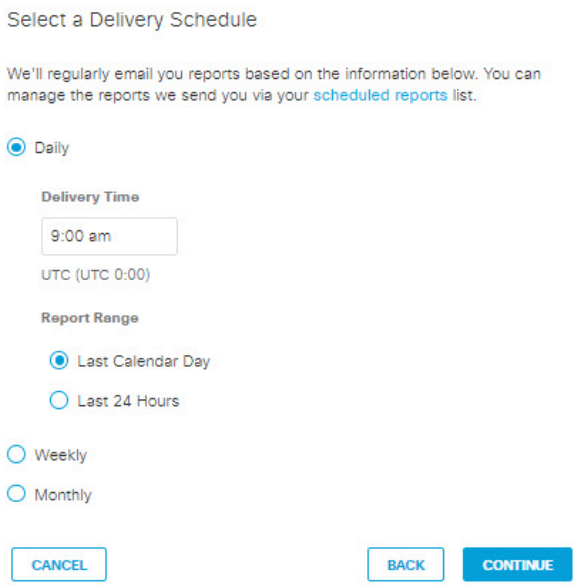


4. Select time parameters to set when and how often you want this report sent to recipients. Click **Continue**.

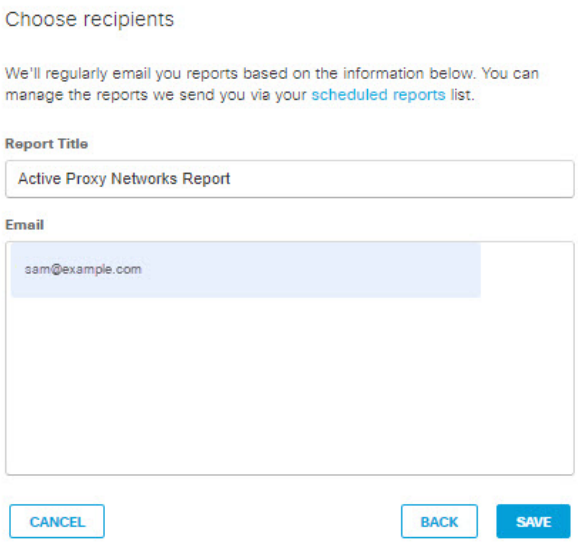
   For each time period, you can specify a time and range within that time period. Data is limited to 1,000,000 rows when exporting to CSV. If your report exceeds 1,000,000 rows, consider re-running the report with a shorter timeframe or with a more granular filter. It's a good idea to check the last row of your first report, then re-run the report from that time period for the next chunk of data.

> **Note**
>
> Delivery schedule defaults to the timezone of the user scheduling the report. If additional recipients need reports delivered at a different time, set up additional scheduled reports with the appropriate delivery schedule.

> **Note**
>
> Attempting to schedule a report for a time on the current day, regardless of whether the report is scheduled in the future from the current time on that same day, results in the report being scheduled on the next day at the earliest for weekly and monthly frequencies.

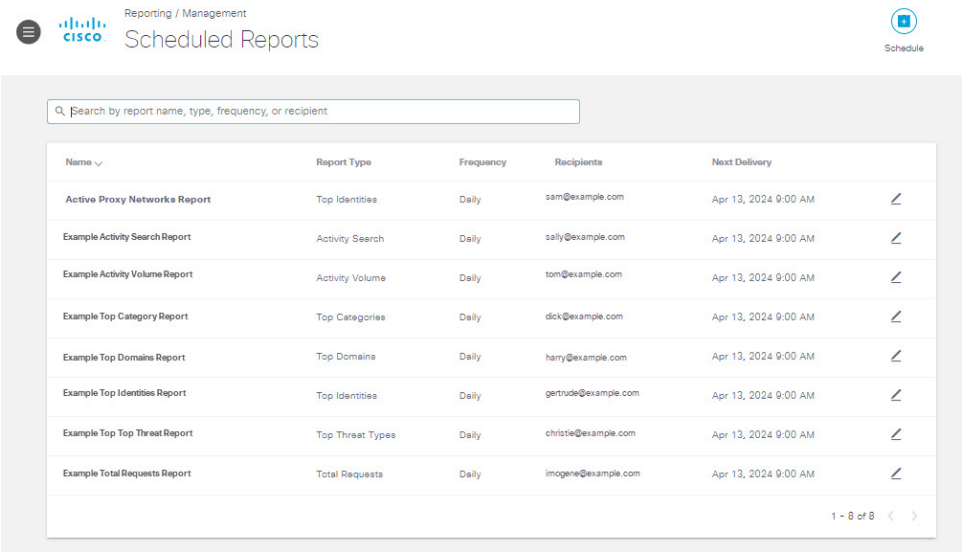


5. Give your report a good descriptive name, add email addresses for recipients of this report, and click **Save**. Enter as many recipients as you like separating addresses with commas or semicolons.



6. Your newly scheduled report is listed at **Reporting** > **Management** > **Scheduled Report**.

   You can update this schedule at any time. For more information, see Update a Scheduled Report.



Check Your Spam Folder

Describes checking your spam folder. Secure Access uses SparkPost as the service to deliver email. Some mail filters, either at the local level or even at a transport layer (for example, an ISP) may block communications from SparkPost as marketing-related spam.

Secure Access uses SparkPost as the service to deliver email. Some mail filters, either at the local level or even at a transport layer (for example, an ISP) may block communications from SparkPost as marketing-related spam. If you do not receive your scheduled reports, check the spam filter at your mail server gateway. Whether your mail server gateway is hosted locally or in the cloud, it's likely the email was quarantined at that level.

Unsubscribe From a Report

Describes unsubscribe from a report. You can unsubscribe from a scheduled report at any time by clicking the Unsubscribe link at the bottom of the email.

You can unsubscribe from a scheduled report at any time by clicking the **Unsubscribe** link at the bottom of the email.

Update a Scheduled Report

Describes updating a scheduled report. You can update your scheduled reports at any time. When you update filters for the scheduled report, the Scheduling wizard takes you to the report in question, where you can select filters as necessary and then save the updated schedule.

You can update your scheduled reports at any time. When you update filters for the scheduled report, the Scheduling wizard takes you to the report in question, where you can select filters as necessary and then save the updated schedule.

Procedure for Update a Scheduled Report

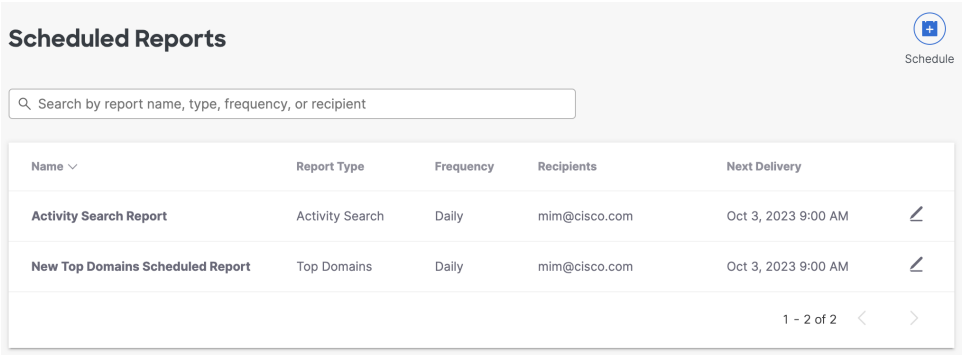
Provides instructions for procedure for update a scheduled report. Full Admin user role. For more information, see Manage Accounts. Navigate to Monitor Management Scheduled Reports and click a scheduled report. The Edit Scheduled Report modal opens and lists filters applied to the report.

Before you begin

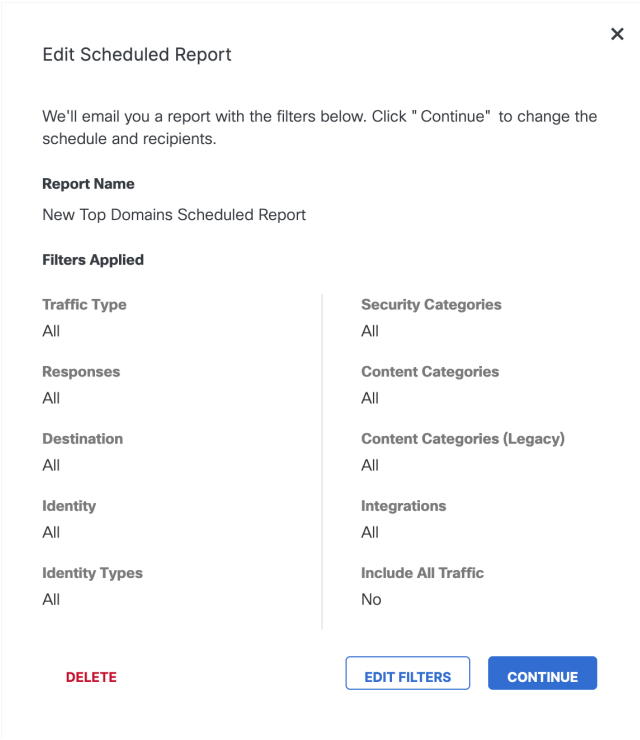
Full Admin user role. For more information, see Manage Accounts.

Procedure

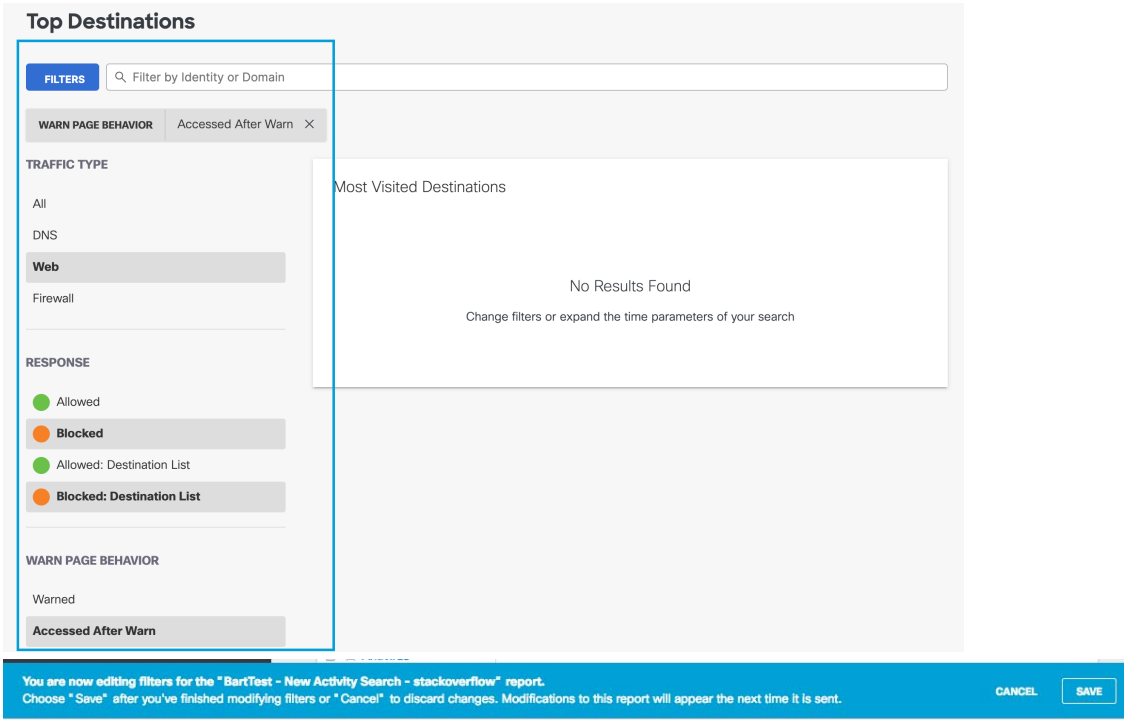
1. Navigate to **Monitor** > **Management** > **Scheduled Reports** and click a scheduled report. The Edit Scheduled Report modal opens and lists filters applied to the report.



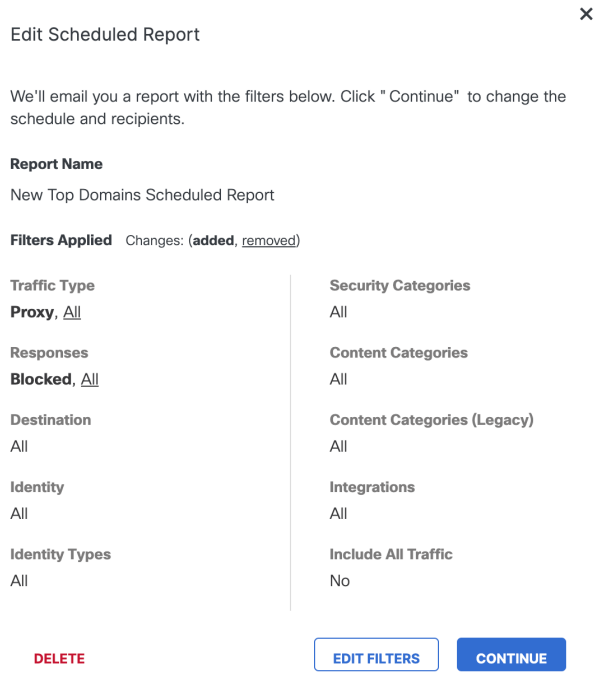
2. Optionally, click **Edit Filters**. The selected report's page opens.



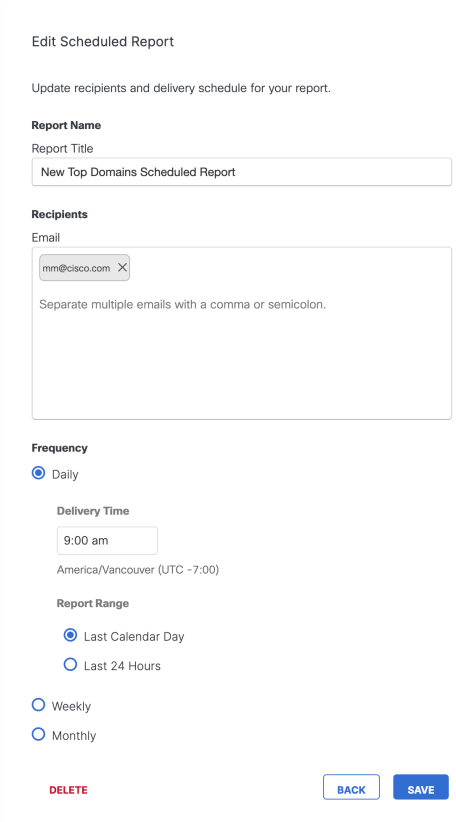
3. Select and apply filters for this report and click **Save**. The Scheduling wizard reopens listing updated filter selections.



4. Review filters and click **Continue**.

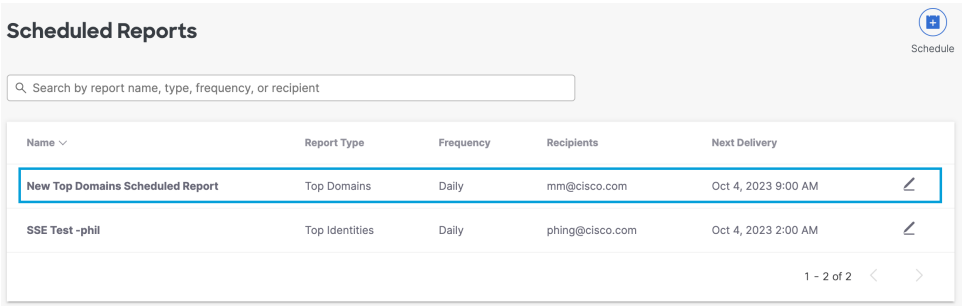


5. Update recipients (press **Enter** to add addresses), the report's delivery schedule, and click **Save**.



Your newly updated scheduled report is listed at **Monitor** > **Management** > **Scheduled Reports**.

> **Note**
>
> This updated report replaces the current report.



Report Retention

Describes report retention. The reporting of information begins as soon as you start sending traffic to Secure Access. The following reports are available for one calendar year:

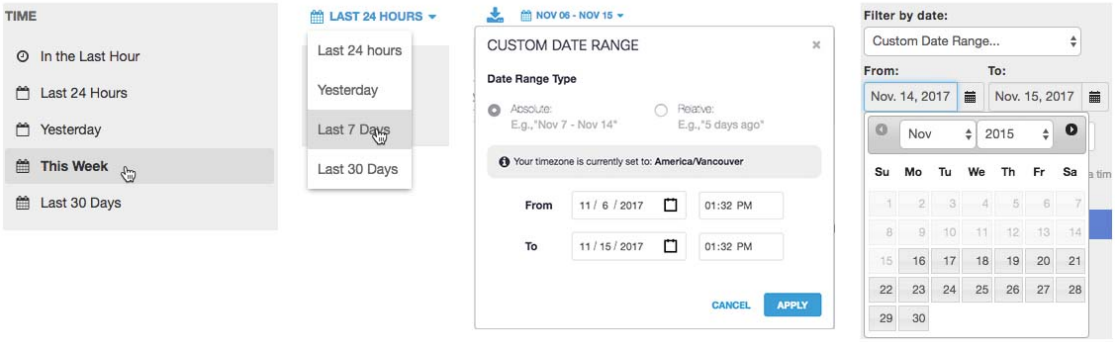
The reporting of information begins as soon as you start sending traffic to Secure Access.

The following reports are available for one calendar year:

- Top Destinations
- Top Categories

Activity Volume is retained for one calendar year.

You can review and filter reported data on various timelines. Timelines vary depending on the report, from the last hour to the last thirty days, and in some cases, custom date ranges in increments of time–up to 30 or 90 days–going back one year.



The following reports are limited to a 30-day search window:

- Top Destinations
- Security Activity
- Activity Search

> **Note**
>
> Secure Access does not retain Security Activity or Activity Search data for more than 30 days.

Admin Audit Log Retention

Describes admin audit log retention. The Admin Audit Log retains data for one year. You can access data in three-month increments. For more information, see the Admin Audit Log Report.

The Admin Audit Log retains data for one year. You can access data in three-month increments. For more information, see the Admin Audit Log Report.

74 Remote Access Log Report

Topics:

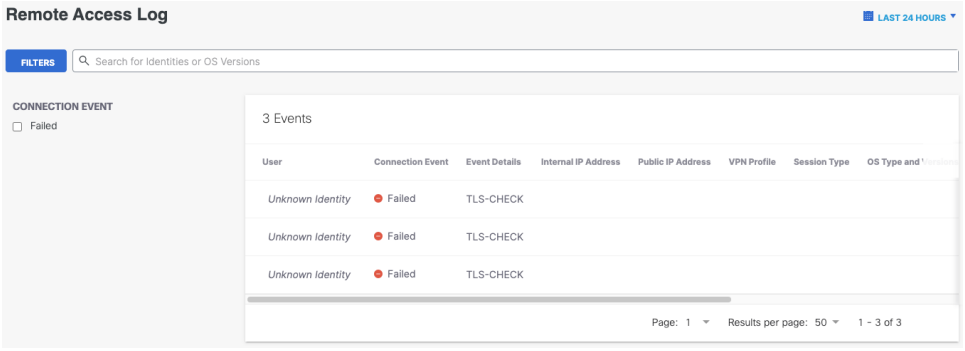
- Remote Access Log Report

Describes the purpose and procedures for remote access log report and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Remote Access Log Report

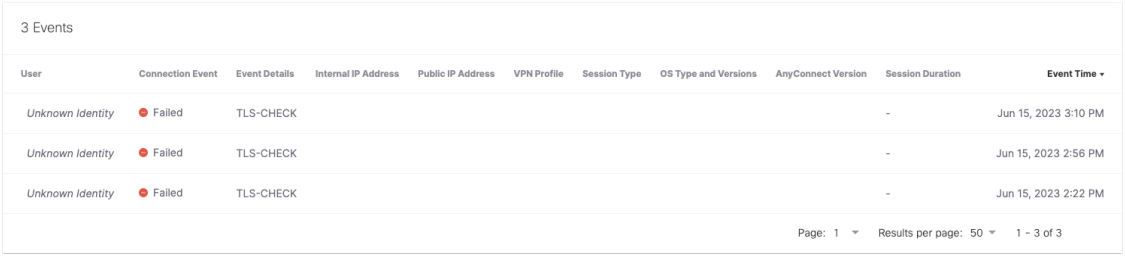
Describes remote access log report. The Remote Access Log report lists users that have remotely connected to Secure Access and requested access to destinations. Page displaying Remote Access Log report with users requesting access to Secure Access destinations

The Remote Access Log report lists users that have remotely connected to Secure Access and requested access to destinations.



Connection Events – Failed

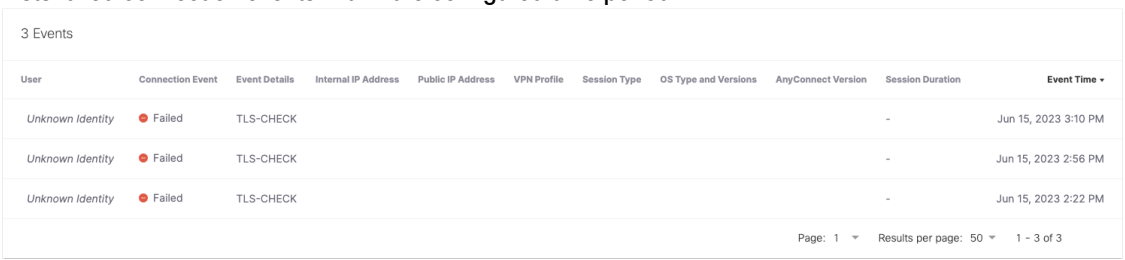
Lists failed connection events within the configured time period



Connection Events – Failed

Describes connection events – failed. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Lists failed connection events within the configured time period



75 Activity Search Report

Topics:

- View the Activity Search Report
- View Activity Search Report Actions
- Schedule an Activity Search Report
- Use Search and Advanced Search

Introduces activity search report. Find the result of every DNS, URL, and IPv4 or IPv6 request from your various sources in descending date and time. The report lists all security (and non-security) activity for the sources reporting to Secure Access for the selected time.

Find the result of every DNS, URL, and IPv4 or IPv6 request from your various sources in descending date and time. The report lists all security (and non-security) activity for the sources reporting to Secure Access for the selected time.

Refine your search using filters to help identify security issues that require attention.

View the Activity Search Report

Provides instructions for viewing the activity search report. The functions of the Activity Search report and where to find the report in Secure Access.

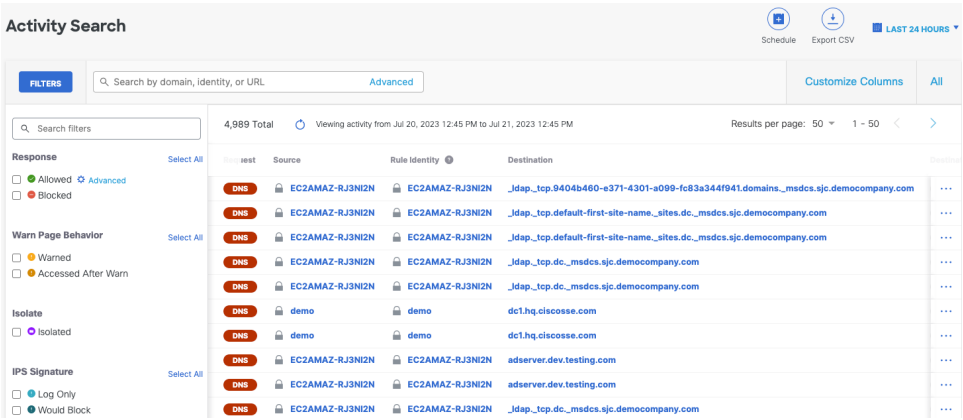
This topic explains the functions of the Activity Search report and where to find the report in Secure Access.

Before you begin

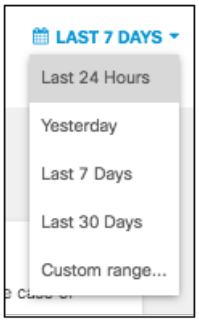
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

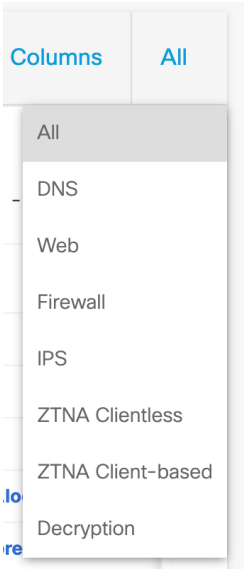
1. Navigate to **Monitor** > **Reports** > **Activity Search**. This takes you to the default view of the Activity Search report, which lists all of your identities and the internet requests or traffic events for your organization, tracked over time. The default is 24 hours.



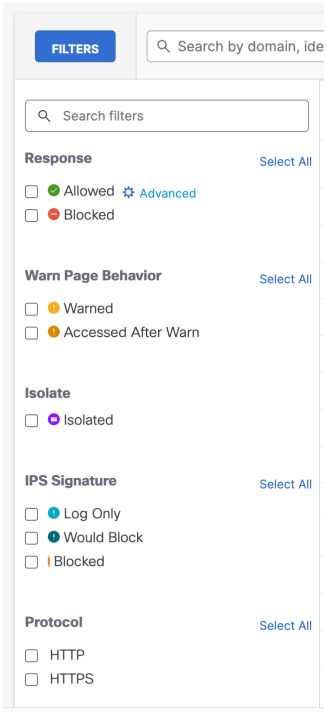
2. Choose a time frame to view the report. You can view the results for the last 24 hours (default), Yesterday, Last 7 Days, Last 30 Days, or a Custom range.



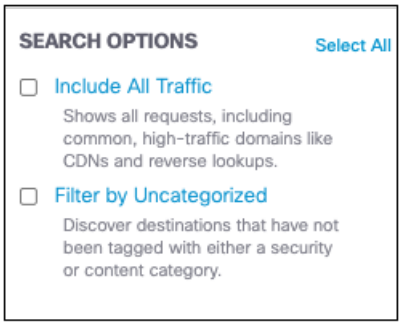
3. From the **Requests** menu, choose a request type or the default of **All**. Filters update to those that are relevant to the type of request chosen.



4. Select available filters based on the request type.



5. Optionally, select a **Search Options** filter:
   - **Include All Traffic**–Includes data from all domains including noisy domains that are filtered out by default.
   - **Filter by Uncategorized**–Includes destinations that are not classified under a specific security or content category.



Configure Columns to Display

Describes configuring columns to display. To change the layout of the data presented in the Activity Search Report, select Columns. Check or clear the information you want to see displayed, then click Apply.

To change the layout of the data presented in the Activity Search Report, select **Columns**. Check or clear the information you want to see displayed, then click **Apply**. You can also drag and drop items in the list to reorder their position on the page.

Column name	Column description
Request	When **All Requests** is selected, this column displays the type of request for each event. Event request types are DNS, Web, Firewall, IPS, ZTNA Clientless, ZTNA Client-based, and Decryption.
Source	The name of the source of the request. Applicable to all request types.
Rule Identity	The identity of the source that Secure Access used to determine which rule applied to the request. Applicable to DNS, Web, Firewall, and ZTNA requests. A request can have multiple identities. Click the row to view Event Details including all identities associated with a request. For more information, see View Activity Search Report Actions.
Destination	The destination of the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests.
Destination IP	The IPv4 or IPv6 address of the destination. Supports both compressed and long-form IPv6 address formats. Applicable to Web, Firewall, and Decryption requests.
Destination Port	The UDP/TCP port of the destination request. Applicable to client-based ZTA requests. For more information, see Comparison of Client-Based and Browser-Based Zero Trust Access Connections.
Destination Country	The two-character country identifier. Applicable to DNS, Web, and Firewall requests.
File Name	The name of the file involved with the activity, where applicable. Applicable to Web and Firewall requests. **Note** File Name will only populate for traffic matching rules with File Type Control or File Inspection enabled (you can enable File Type Control without blocking any file types by clicking enable and saving the rule.) If none of the rules have File Type Control enabled, the file name and extension fields remain blank.
Internal IP	The internal IPv4 or IPv6 address of the request. Supports both compressed and long-form IPv6 address formats. Applicable to DNS and Web requests.
External IP	The external IPv4 or IPv6 address of the request. Supports both compressed and long-form IPv6 address formats. Applicable to DNS and Web requests.
DNS Type	The DNS record type. Applicable to DNS requests.

Column name	Column description
Action	The request is either Blocked, or Allowed. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests. **Blocked – Certificate Error** indicates certificate and TLS error events when the request is processed by a ruleset with **HTTPS inspection** and **File Analysis** enabled.
Categories	Content and Security categories flagged with the activity. Applicable to DNS, Web, and Firewall requests.
Resource/Application	The resource or application involved with the activity, when applicable. Populates for traffic matching rules with Application Controls enabled. If no rules have Application Controls enabled, then the field will remain blank. Applicable to DNS, Web, Firewall, and ZTNA requests. For more information, refer to Advanced Application Controls.
Signature List Name	The Secure Access Intrusion Prevention System (IPS) signature list applied to the request. Applicable to IPS requests. For more information, refer to Manage IPS Profiles.
IPS Signature	The signature of the known threat that was blocked or logged by Secure Access IPS. Applicable to IPS requests. For more information, refer to Manage IPS Profiles.
Protocol	Displays whether the Web request protocol is HTTP or HTTPS, and whether the Firewall, IPS, or Decryption request protocol is TCP or UDP. Decryption request protocol includes the cryptographic protocol, such as TLS.
Rule Name	The name of the access rule applied to the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests. Click the rule name to view your Access Policy where the rule is configured. For more information, refer to Manage the Access Policy. Click the row to view Event Details including details of the rule (such as destination list or schedule applied). For more information, refer to View Full Details.
Application Category	If an application is involved with the activity, this column contains the categories associated with the application. Applicable to DNS, Web, and Firewall requests. For the full list of application categories, refer to Application Categories.
Application Protocol	If an application is involved with the activity, this column contains the protocol for the application (HTTP, SSL, RTP, DNS, or none). Applicable to Firewall requests.
Request Method	The HTTP method used by the request. Applicable to Web requests.
Referer	The URI from which the request originated. Applicable to Web requests.
Status Code	Standard HTTP status codes. Applicable to Web requests.
Content Type	The HTTP content type. Applicable to Web requests.
File Extension	The extension of the file involved in the activity, where applicable. Applicable to Web and Firewall requests.

Column name	Column description
OS	The operating system of the client's device. Applicable to ZTNA requests.
Browser	The client's browser. Applicable to ZTNA requests.
Location	The two-character country identifier. Applicable to ZTNA requests.
Location IP	The IPv4 or IPv6 address of the client. Supports both compressed and long-form IPv6 address formats. Applicable to ZTNA requests.
Date and Time	The date and time stamp of the request. Applicable to all request types.

From your search results, you can click an identity or destination and go to their respective detailed report.

View Activity Search Report Actions

Describes viewing activity search report actions. To learn more about the results of your activity search, click the View Actions icon for a result and choose an item from the menu.

To learn more about the results of your activity search, click the **View Actions** icon for a result and choose an item from the menu.

See Full Details

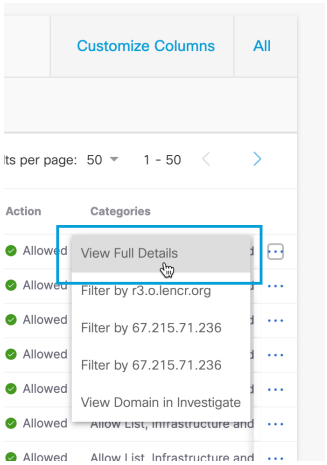
Provides instructions for see full details. A minimum user role of Read-only. For more information, see Manage Accounts. For each entry listed, from the View Actions icon, choose View Full Details.

Before you begin

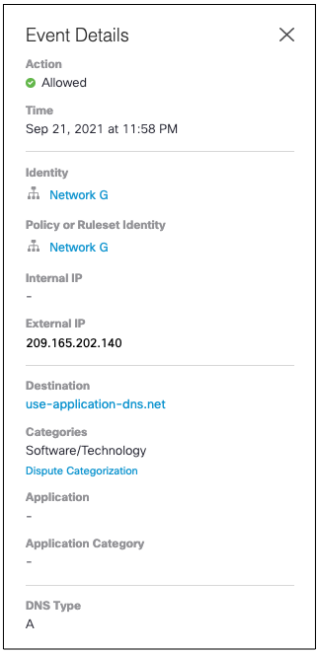
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

For each entry listed, from the **View Actions** icon, choose **View Full Details**.



The details of each activity result are displayed. The details listed depend on the event type.

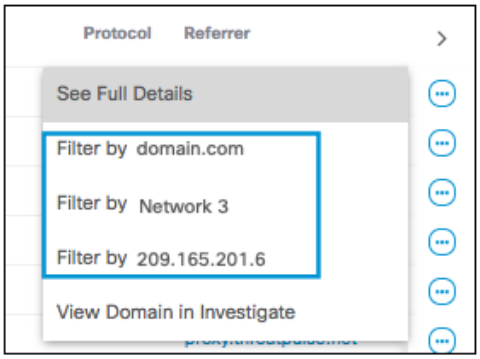


Filter Views

Describes filter views. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Where applicable, certain results can be filtered by the following:

- Application
- Destination
- URL
- Source
- External IP

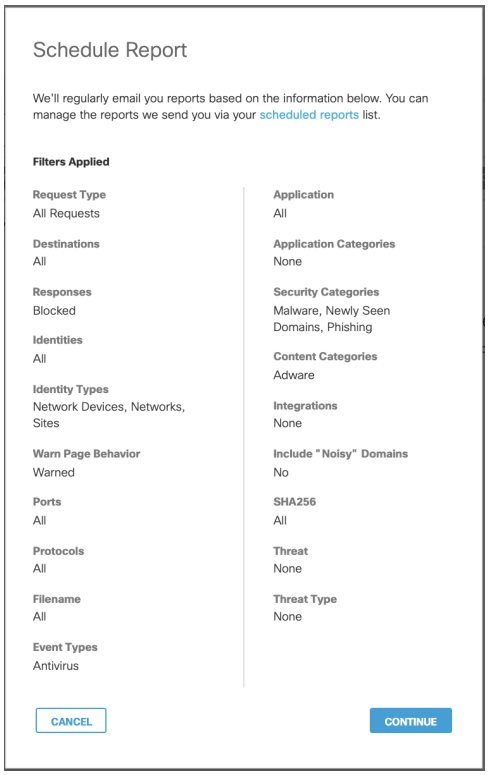


Schedule an Activity Search Report

Describes schedule an activity search report. You can schedule a report to be emailed to you at regular intervals. Your emailed report is a table showing an HTML version of the report and an attached CSV file containing the entire data set.

You can schedule a report to be emailed to you at regular intervals. Your emailed report is a table showing an HTML version of the report and an attached CSV file containing the entire data set. Also included in your email is a link to a live version of the same report. For more about scheduled reports, see Schedule a Report.

When scheduling a new report for Activity Search, any current filters selected apply.



Use Search and Advanced Search

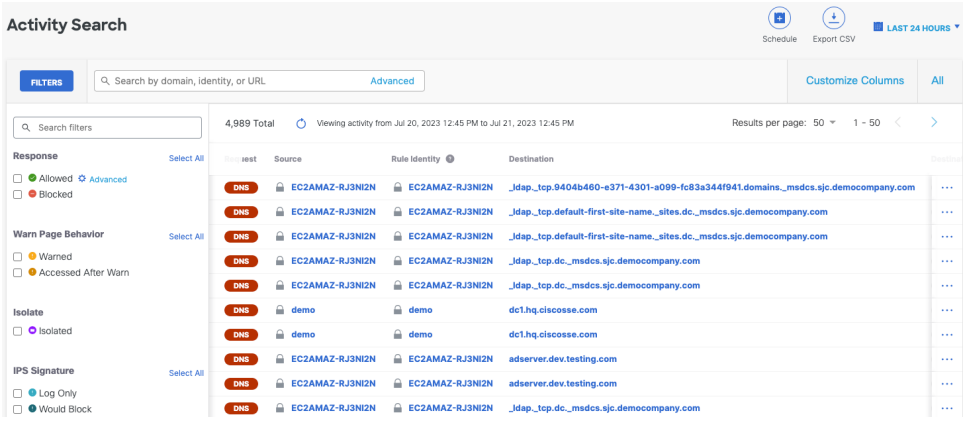
Describes using search and advanced search. In addition to using the filters to narrow the activity results in the Activity Search report, the Search and Advanced Search features provide further filtering of event details.

In addition to using the filters to narrow the activity results in the Activity Search report, the Search and Advanced Search features provide further filtering of event details. For example, you can search for events with specific domains but exclude subdomains you are not interested in. Wildcards available for some fields (Domains, URLs, and File names) allow you to search for all varieties within that field. For example, using `*.gif` in File Name will search for all files that are .gifs.

Search

Describes search. Search the report for domains, identities, or URLs. To search and filter the report by more options, such as threat type or file name, use Advanced Search.The Activity Search interface.

Search the report for domains, identities, or URLs. To search and filter the report by more options, such as threat type or file name, use Advanced Search.



Wildcards

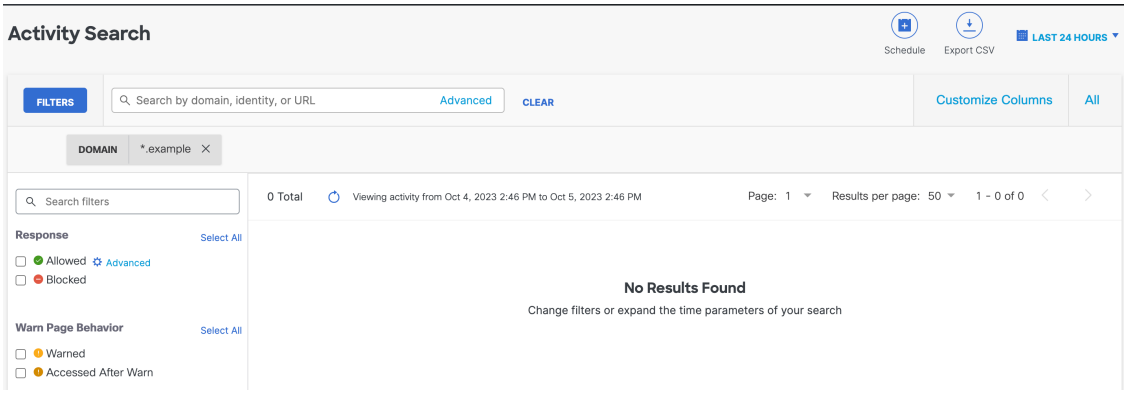
Describes wildcards. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Domains

Describes domains. Domains can be searched in the search bar or advanced search with the wildcard * to include or exclude subdomains.

Domains can be searched in the search bar or advanced search with the wildcard * to include or exclude subdomains. For example, `example.com` will search the top-level parent domain of Example, `*.example.com` will search for only the subdomains of Example, and `*example.com` will search for both the parent and subdomains of Example.

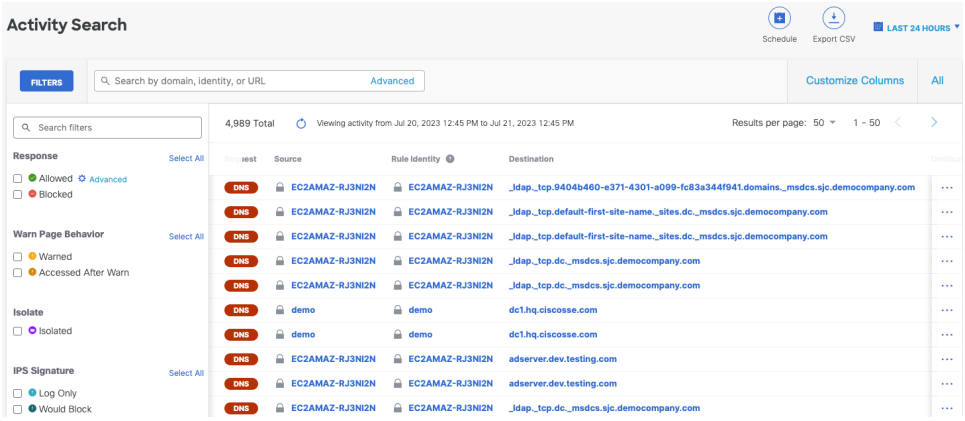
You can use wildcards to search by top-level domain. For example, `*.example` will search for all top-level domains that end in .example.



URLs

Describes urls. The wildcard * can be used in any part of the URL path to search for URLs containing certain terms. For example, example* will search for URLs containing "example".The Activity Search interface.

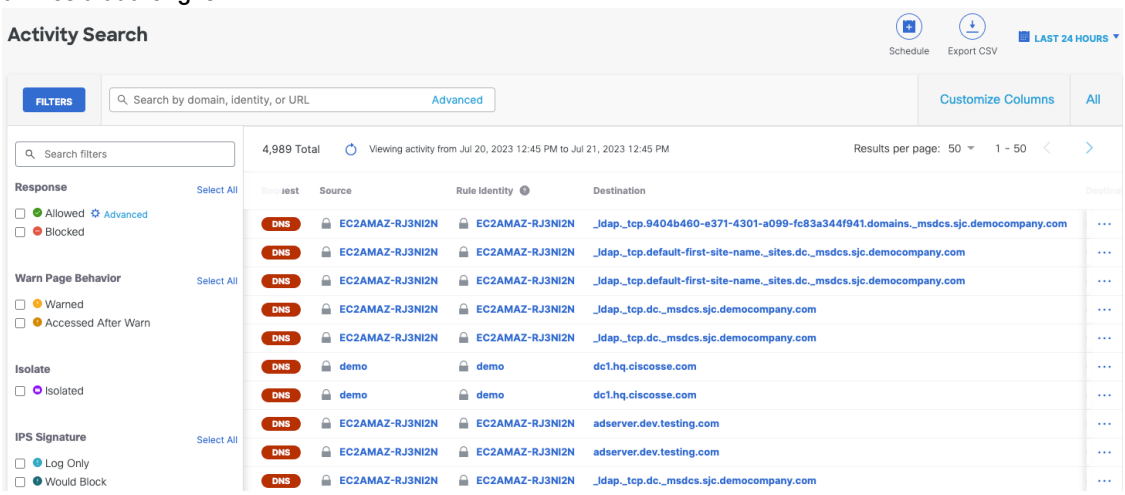
The wildcard * can be used in any part of the URL path to search for URLs containing certain terms. For example, `example*` will search for URLs containing "example".



File Names

Describes file names. File names can use the wildcard * to search for file types, in Advanced Search only. For example, *.gif will search for all files that are .gifs.The Activity Search interface.

File names can use the wildcard * to search for file types, in Advanced Search only. For example, `*.gif` will search for all files that are .gifs.



Advanced Search

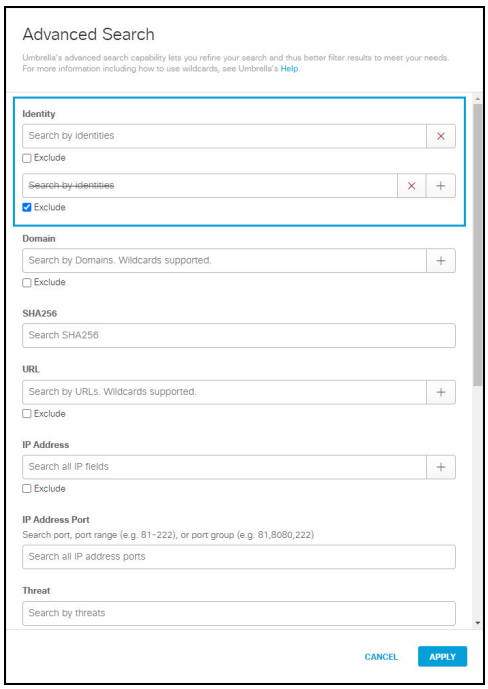
Provides instructions for advanced search. A minimum user role of Read-only. For more information, see Manage Accounts. In the search bar, click Advanced. The Advanced Search window opens.

Before you begin

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

Procedure

1. In the search bar, click **Advanced**. The Advanced Search window opens.



2. Add search parameters and click **Apply**. Available search parameters include:
    - **Identity**–Include or exclude identity sources in search results. Secure Access opens a menu listing sources as soon as you begin typing.
    - **Domain**–Include or exclude one or more domains in search results. When you add a domain, a new field appears so that you can add or exclude another domain.
    - **SHA256**–Search by the hash function.
    - **URL**–Include or exclude specific URLs in search results.
    - **IP Address**–Include or exclude events associated with specific IPv4 or IPv6 addresses on your network (either internal or public egress IP address). Supports both compressed and long-form IPv6 address formats. This does not provide the capability to search for destination IP addresses.
    - **IP Address Port**–Search by a firewall port number, port range (e.g. 81-222), or port group (e.g. 81, 8080, 222).
    - **Threat**–Search by threats.
    - **Threat Type**–Search by threat type. For more information, see Threat Category Descriptions.
    - **Public Application**–Search by any public application.
    - **File Name**–Search by the name of a file.
    - **IPS Signature List Names**–Search by default and custom IPS Signature List Names. For more information, see Manage IPS Profiles.
    - **IPS Signatures**–Search by IPS signatures. For more information, see Manage IPS Profiles.
    - **OS Type**–Search by operating system from which activity originated.
    - **Location**–Search by the location from which activity originated.
    - **Egress IP Type**–Search by the egress IPv4 or IPv6 addresses: shared or reserved. Supports both compressed and long-form IPv6 address formats.

- **Egress Data Center**—Search by the egress data center location from which activity originated.

76 Security Activity Report

Topics:

- View Activity and Details by Filters
- View Activity and Details by Event Type or Security Category
- View an Event's Details
- Search for Security Activity

Introduces security activity report. The Security Activity report highlights security events generated by your organization's sources visiting destinations flagged—but not necessarily blocked—by Secure Access security researchers as a threat.

The Security Activity report highlights security events generated by your organization's sources visiting destinations flagged—but not necessarily blocked—by Secure Access security researchers as a threat.

Activities captured by this report include attempts to access sites hosting malware or phishing sites, botnet activity on infected machines on your local network, and attempts to download malicious files.

View Activity and Details by Filters

Describes viewing activity and details by filters. The Security Activity report gives you the ability to monitor and discover threats to your organization by displaying traffic patterns. You can filter these results by event type, category, time period, and type of request.

The Security Activity report gives you the ability to monitor and discover threats to your organization by displaying traffic patterns. You can filter these results by event type, category, time period, and type of request.

> **Note**
>
> Secure Access reports are time-dependent. Secure Access time is UTC by default but can be changed to a different timezone on a per-user basis. Navigate to **Admin** > **Accounts** and update your account's time setting.

Procedure

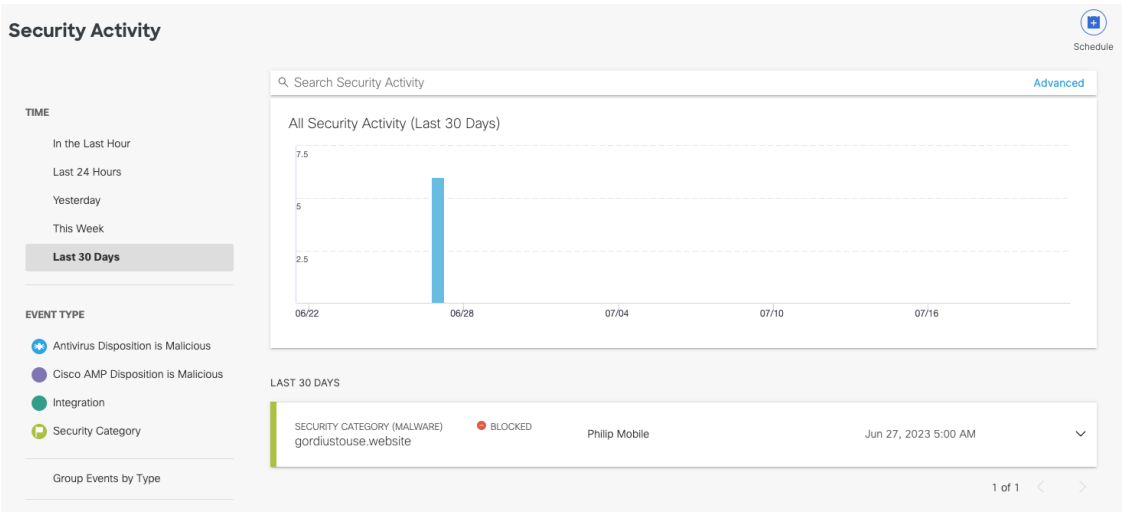
Provides instructions for procedure. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports Security Activity .

Before you begin

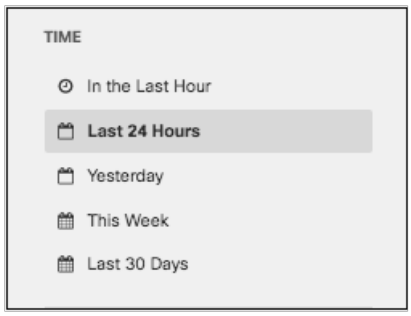
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

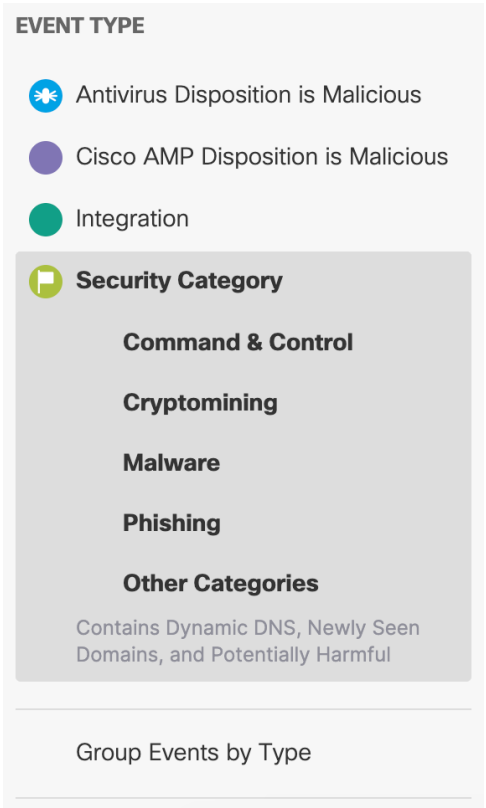
1. Navigate to **Monitor** > **Reports** > > **Security Activity**.



2. Choose a time period of events to view. You can generate a report to document activities for the last hour, the last 24 hours, the previous calendar day (yesterday), the last seven days, and the last month.

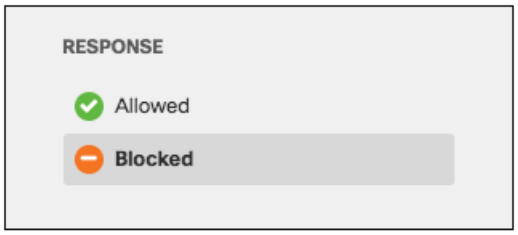


3. Choose which security event types or categories you want to view in the report. By default, all events and categories are selected to display activity for all event types.
   - **Antivirus Disposition is Malicious**–Lists events that have been filtered through a virus scan.
   - **Cisco AMP Disposition is Malicious**–Lists events that have been filtered through Cisco Advanced Malware Protection (AMP).
   - **Security Category**–Lists events allowed or blocked against selected security categories: Command and Control, Cryptomining, Malware, Phishing, and Other Categories (Contains Dynamic DNS, Newly Seen Domains, and Potentially Harmful).

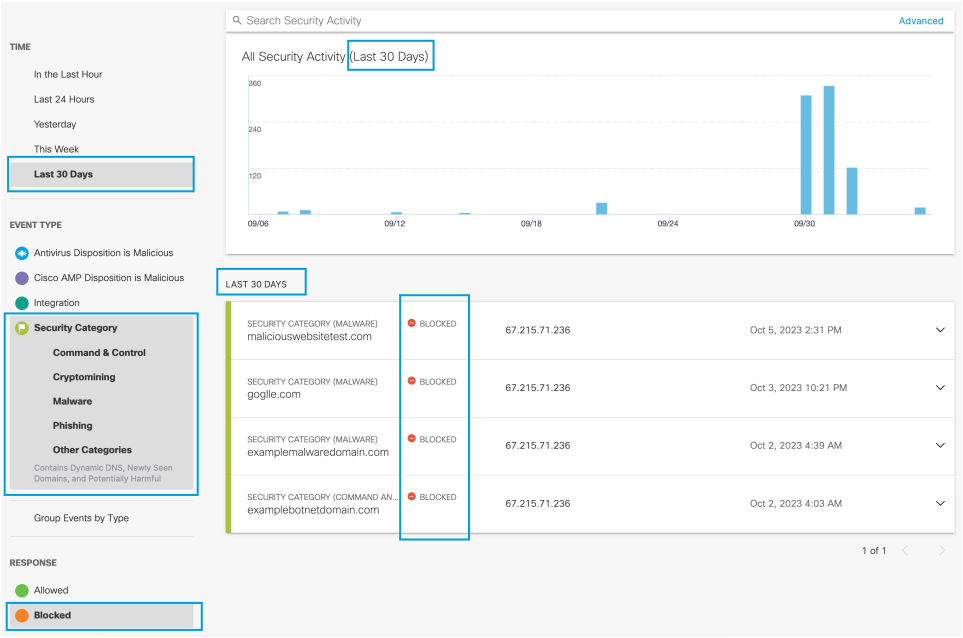


4. For **Response,** select **Allowed**, **Blocked**, or both.

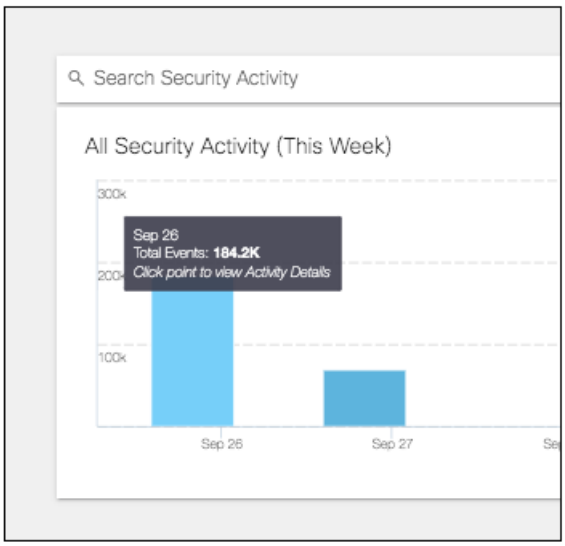
   If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response** > **Allowed**. Secure Access cannot allow viruses to pass through the system. These will always be blocked.



Once all filters have been selected, the activity graph and event details will reflect the chosen filters. The graph will display activities for the events selected during the configured time period. The event details cards will stack from most recent to oldest.



Hovering over a bar on the graph shows details for that time period (the hour or day). Clicking the details redirects you to the Activity Search report where you can view further details for that time period filtered by Response (if only one is selected) and the security categories selected.



View Activity and Details by Event Type or Security Category

Describes viewing activity and details by event type or security category. If you want to view data for individual event types or security categories in your environment to see which categories may pose more risk and at what times depending on trends, use the Group Events by Type feature.

If you want to view data for individual event types or security categories in your environment to see which categories may pose more risk and at what times depending on trends, use the **Group Events by Type** feature.

Procedure

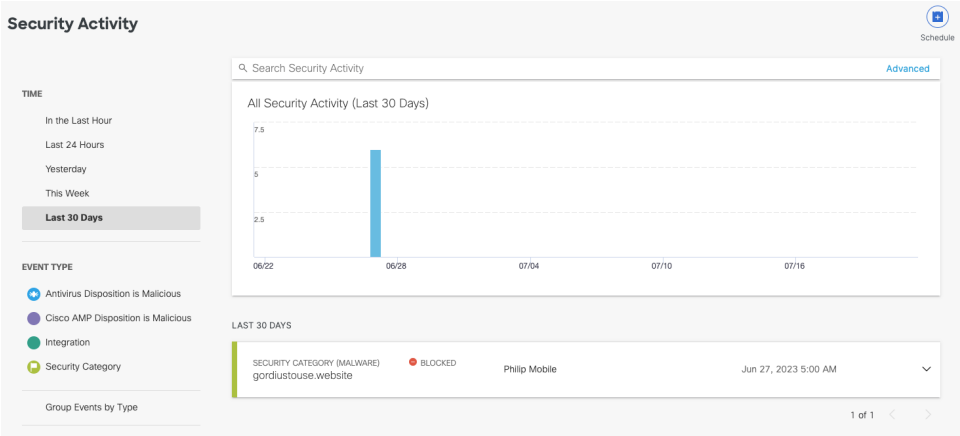
Provides instructions for procedure. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports Security Activity .

Before you begin

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

Procedure

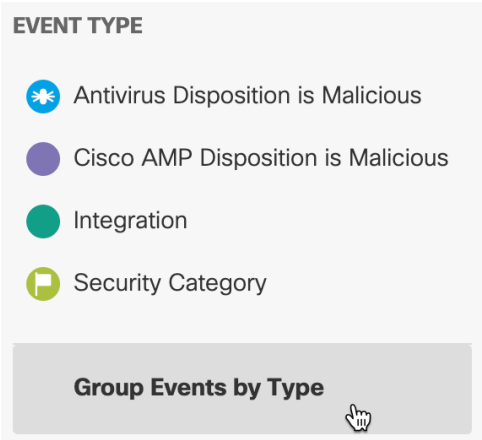
1. Navigate to **Monitor** > **Reports** > **Security Activity**.



2. Choose a time period of events to view. You can generate a report to document activities for the last hour, the last 24 hours, the previous calendar day (yesterday), the last seven days, or the last month.

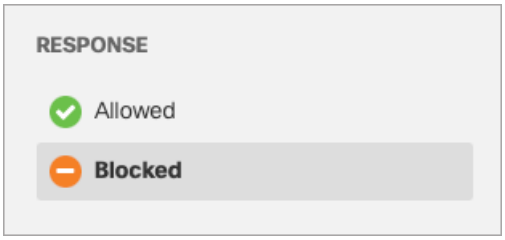


3. Select which security event types or categories you want to view in the report. By default, all events and categories are selected to display activity for all event types.

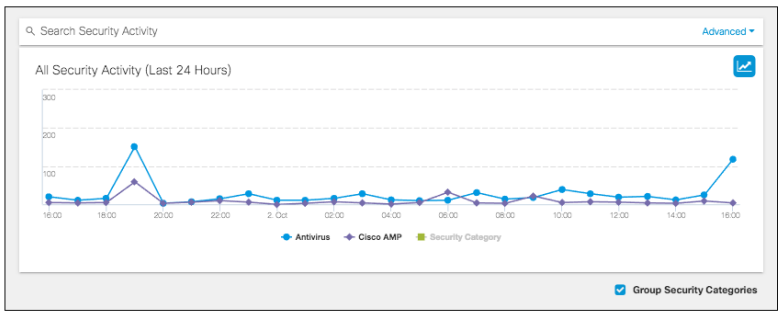


4. For **Response,** select **Allowed**, **Blocked**, or both.

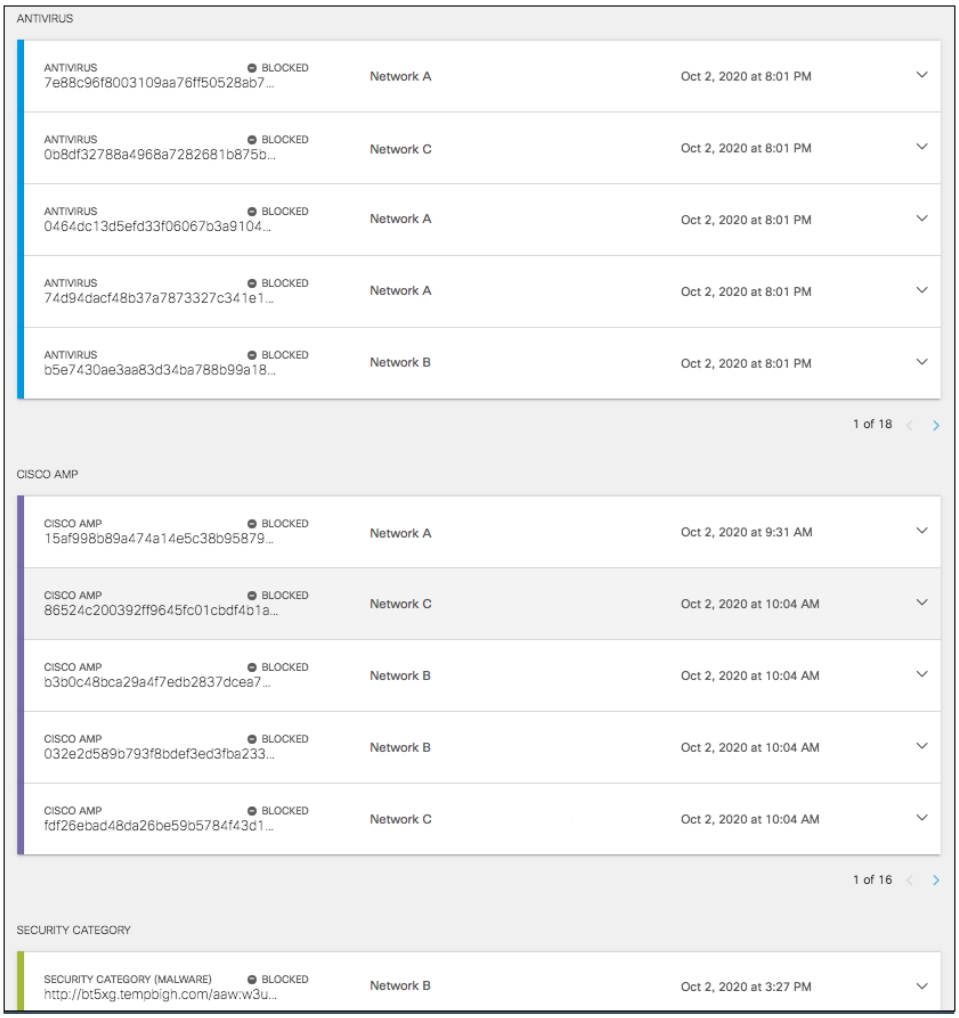
> **Note**
>
> If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response** > **Allowed**. Secure Access cannot allow viruses to pass through the system. These will always be blocked.



The activity graph updates to show each selected event type so you can compare activities for each type of security risk. You can click the event type on the graph or in the filter to view or hide the events in the graph.



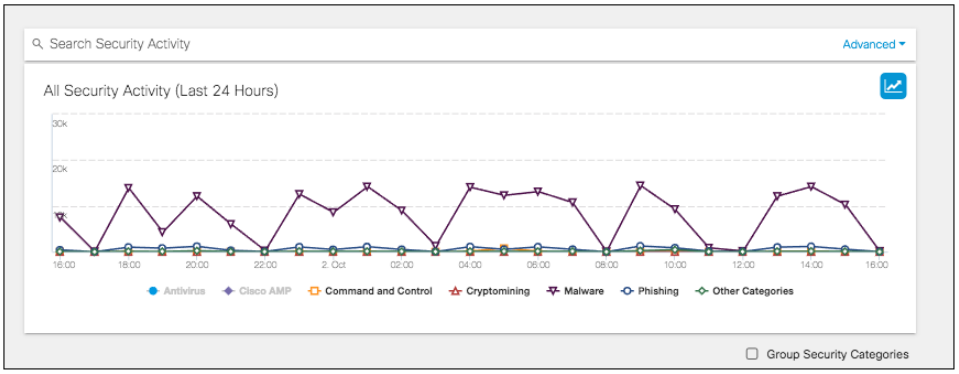
Grouping security categories also reorganizes the events' details cards by event type. By viewing event details by event type or category, you can see which categories were more active and perhaps causing more risk to the environment.



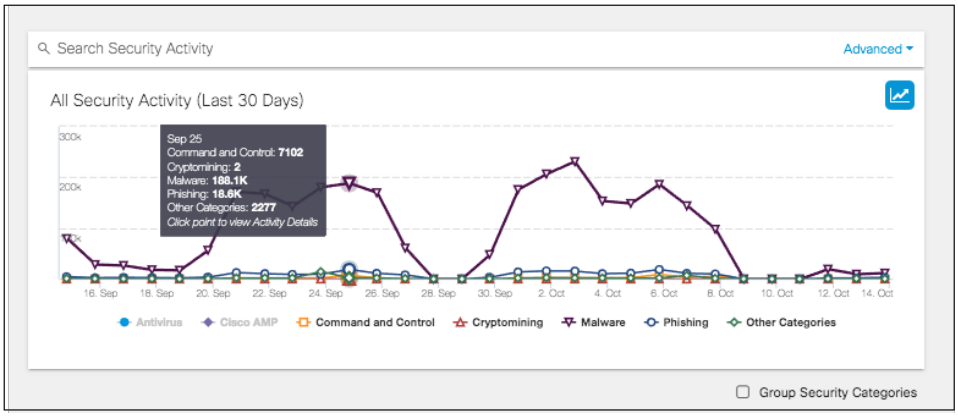
Group Security Categories

Describes group security categories. When Group Security Categories is unchecked, the selected security categories are shown individually on the Activity graph. This enables you to view which categories had more activity within the given time frame or where spikes in some categories occurred.

When **Group Security Categories** is unchecked, the selected security categories are shown individually on the Activity graph. This enables you to view which categories had more activity within the given time frame or where spikes in some categories occurred. Clicking the category name on the graph or in the Security Categories filter will show or hide that category's events on the graph.



Rolling over a point on the line graph provides a summary of the security events at that time by the categories selected. Clicking the details redirects you to the Activity Search report where you can further view the activity's details.



View an Event's Details

Describes viewing an event's details. In the Security Activity report, you can view the details of a security event, including date and time, destination, identity, and the event's result (Blocked or Allowed).

In the Security Activity report, you can view the details of a security event, including date and time, destination, identity, and the event's result (Blocked or Allowed).

Procedure

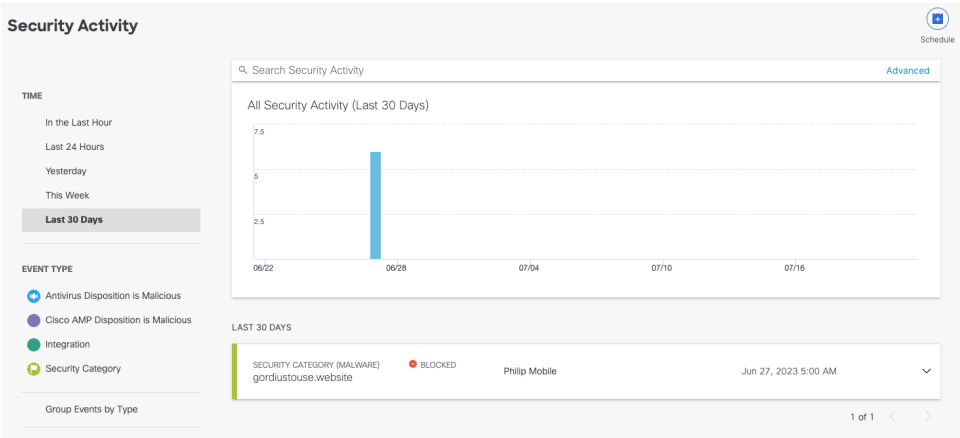
Provides instructions for procedure. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports Security Activity .

Before you begin

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

Procedure

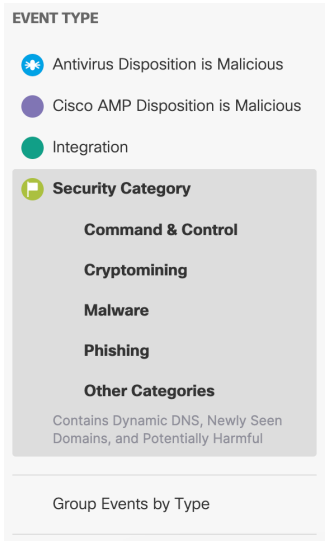
1. Navigate to **Monitor** > **Reports** > **Security Activity**.



2. Choose a time period of events to view. You can generate a report to document activities for the last hour, the last 24 hours, the previous calendar day (yesterday), the last seven days, and the last month.

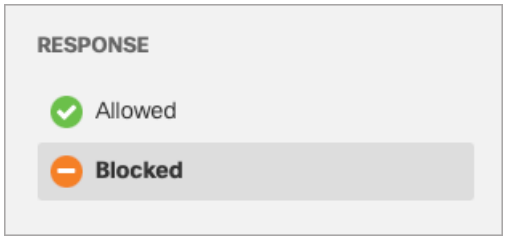


3. Select which security event types or categories you want to view in the report. By default, all events and categories are selected to display activity for all event types.

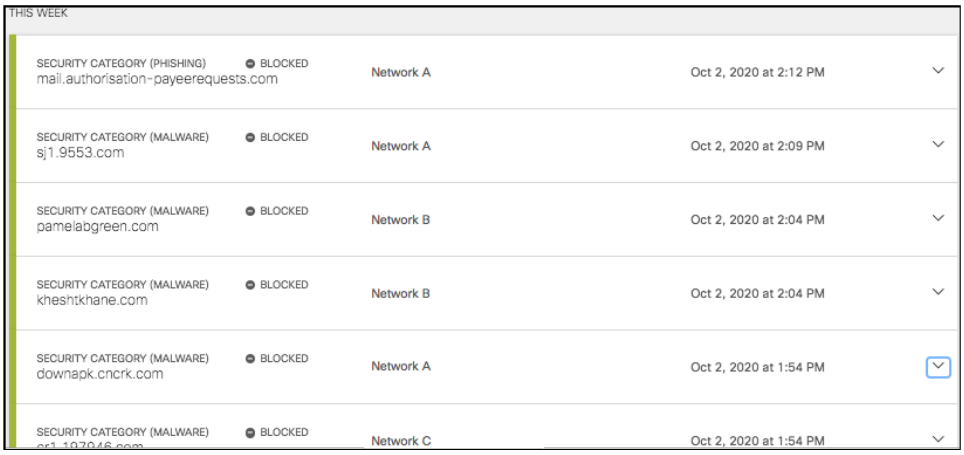


4. For **Response,** select **Allowed**, **Blocked**, or both.

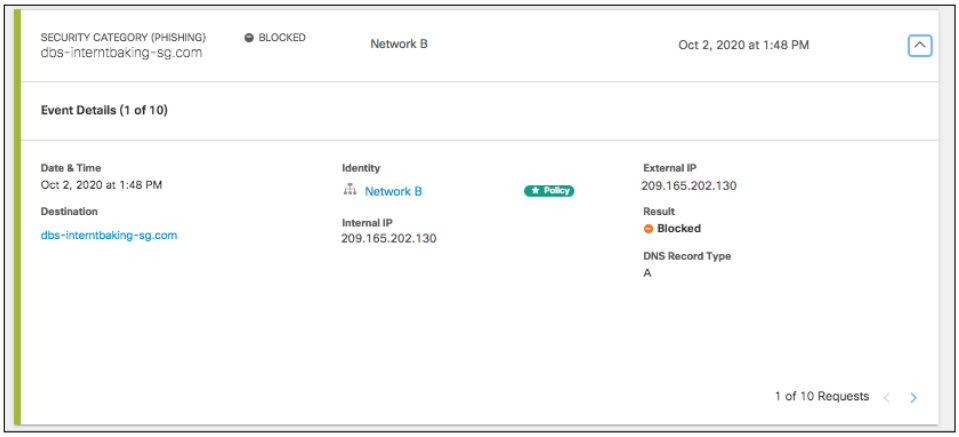
> **Note**
>
> If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response** > **Allowed**. Secure Access cannot allow viruses to pass through the system. These will always be blocked.



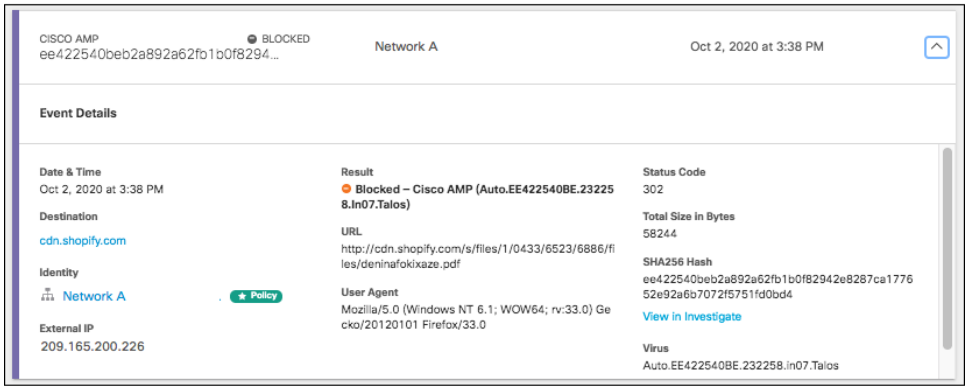
The list of events' details is stacked as cards and sorted by event type (if **Group Security Categories** is enabled).



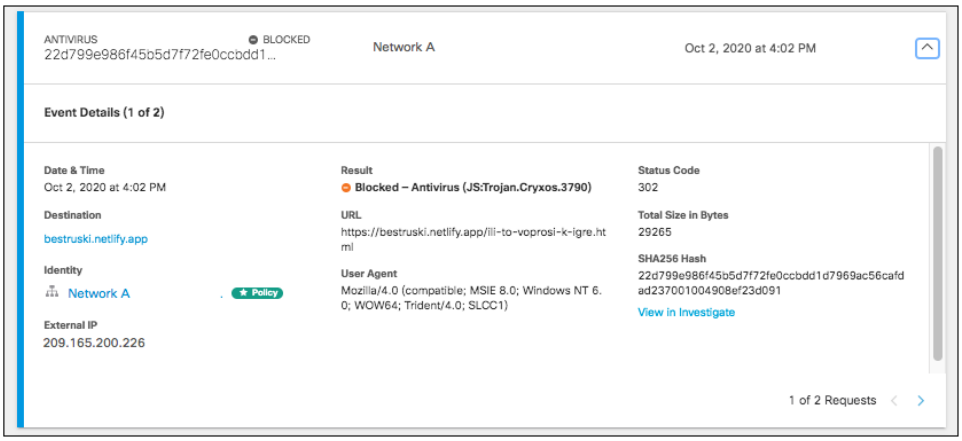
5. Click an event to view its details. Each security activity card groups an event by destination and lists the details of the event including date and time, destination, identity, and the event's result (Blocked or Allowed).



Details differ slightly between event type, but all list the destination and identity from which you can click through to the Destination Details and Identity Details.



Details for AMP and Antivirus events will also include the SHA256 Hash.



Search for Security Activity

Describes search for security activity. To view security activities for a specific source, use the search feature to filter the Activity chart and event details by source.

To view security activities for a specific source, use the search feature to filter the Activity chart and event details by source.

Procedure

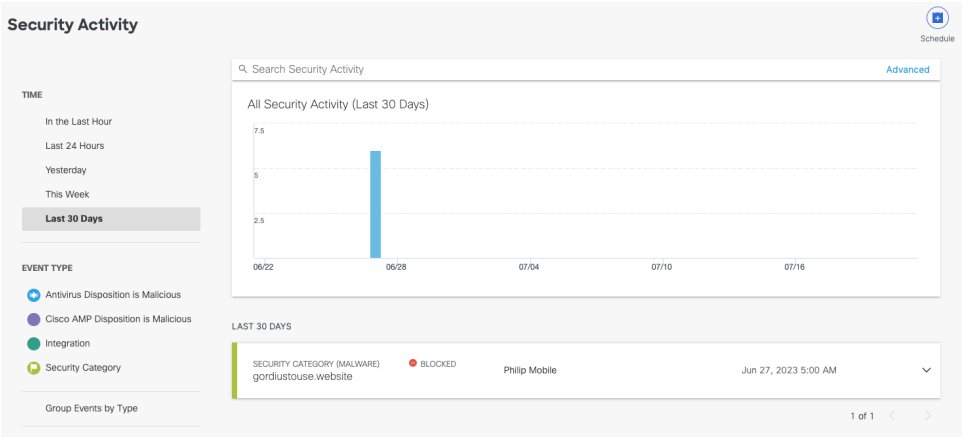
Provides instructions for procedure. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports Security Activity .

Before you begin

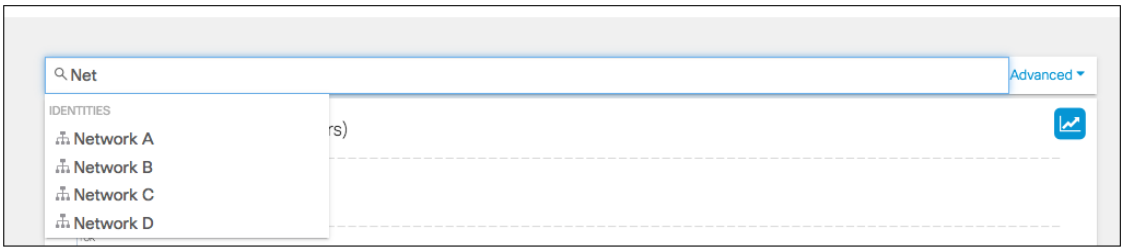
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Security Activity**.



2. Type the source's name in the search bar at the top of the page and press **Enter**. You can only filter by one source at a time.



Advanced Search

Provides instructions for advanced search. To search security activities by more specific fields other than the source, such as domain, URL, or threat type, use the Advanced Search feature.

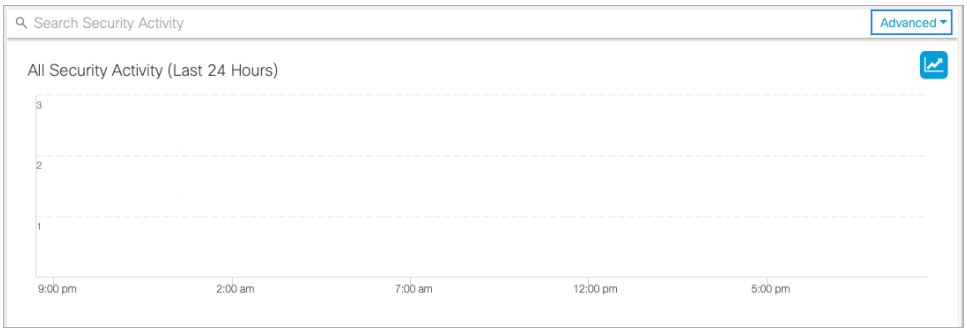
To search security activities by more specific fields other than the source, such as domain, URL, or threat type, use the Advanced Search feature.

Before you begin

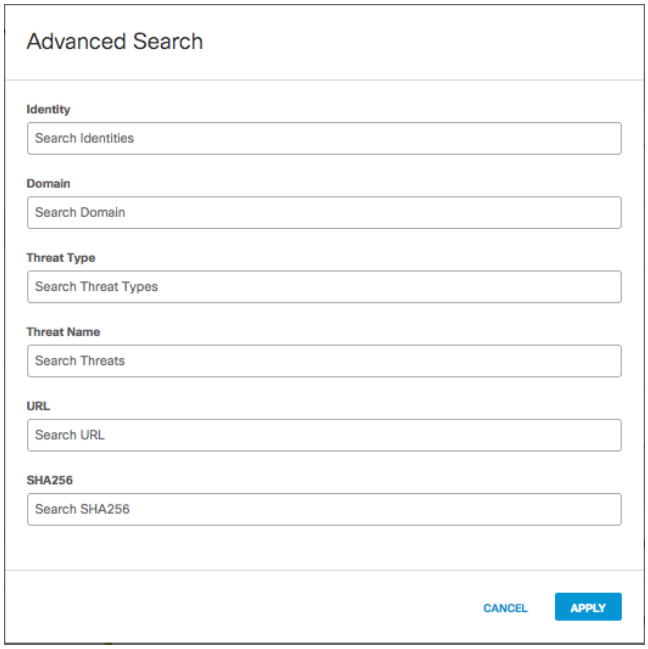
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. In the search bar, click **Advanced**.



2. Enter the fields of your search and then click **Apply**. You don't have to enter information for each search field, but remember that the more information you can provide, the more successful your search will be.


Advanced Search
Identity
Search Identities
Domain
Search Domain
Threat Type
Search Threat Types
Threat Name
Search Threats
URL
Search URL
SHA256
Search SHA256
CANCEL
APPLY

77 Total Requests Report

Topics:

- Total Requests Report

Describes the purpose and procedures for total requests report and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Total Requests Report

Describes total requests report. The Total Requests Report provides a visualization of traffic over a given time period. Based on selected categories, traffic type, and responses, you can see what traffic trends occur in your environment.

The Total Requests Report provides a visualization of traffic over a given time period. Based on selected categories, traffic type, and responses, you can see what traffic trends occur in your environment.

View Trends in the Total Requests Report

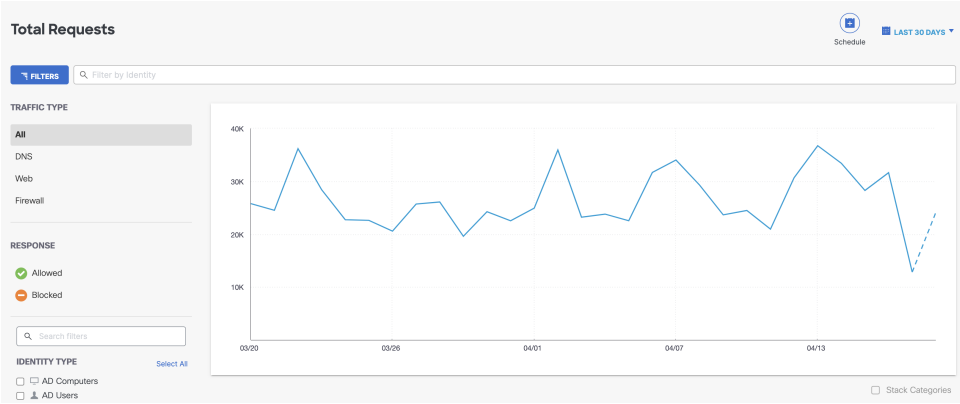
Provides instructions for viewing trends in the total requests report. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

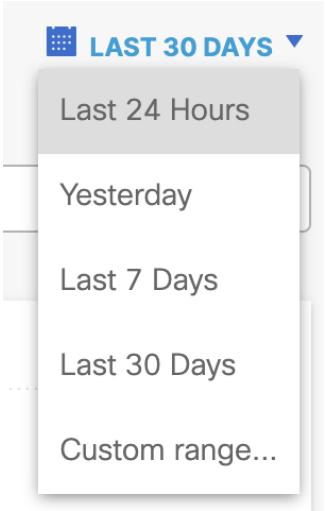
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

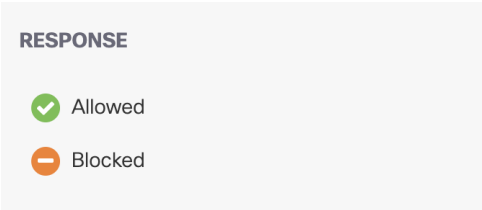
1. Navigate to **Monitor** > **Reports** > **Total Requests**. You will see filters to the left of the trend graph.



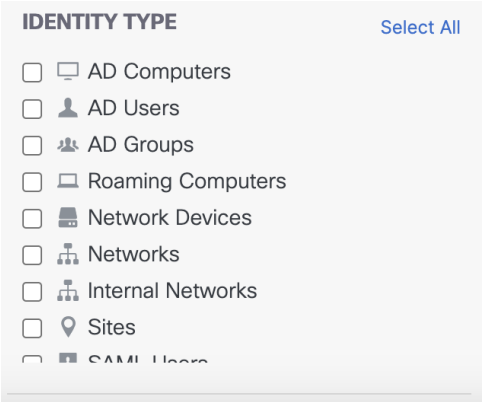
2. Choose a time frame to view the report's results. The Total Requests Report can be filtered by time: the last 24 hours, the previous calendar day (yesterday), the last seven days, and the last month.



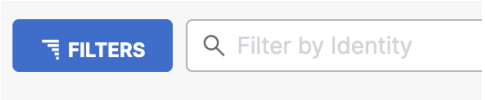
3. Filter the results by the type of response. You can filter by Blocked requests or Allowed requests. By default, nothing is selected, so all responses are shown.



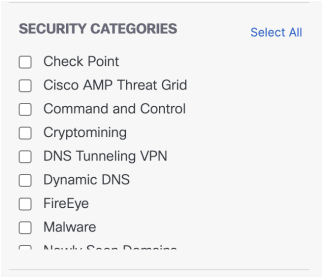
4. Filter by specific identity types.



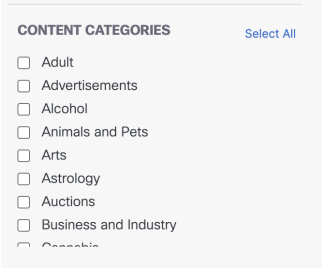
Alternatively, if you are looking for a specific identity to filter your results, enter it in the search bar.



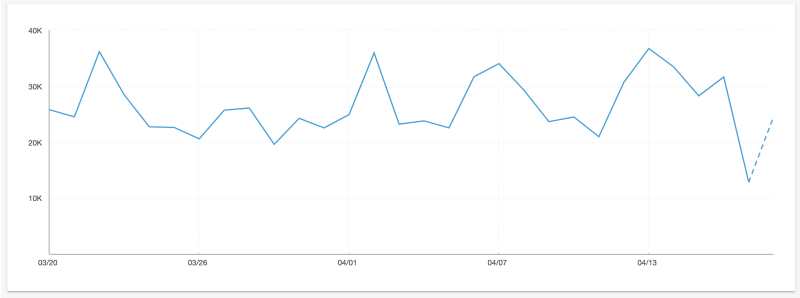
5. Filter by specific security categories. For more information about threat categories, see Manage Threat Categories and Threat Category Descriptions.



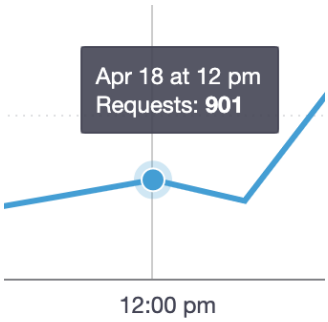
6. Filter by specific content categories. For a full list of content categories, see Available Content Categories.



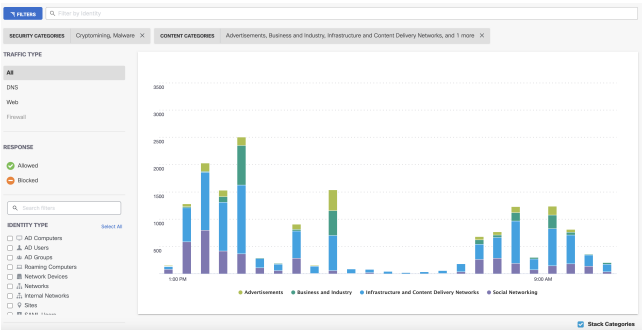
Once all filters have been selected and applied, the trend graph will update to reflect the appropriate total request data. When no security or content categories are selected, the graph remains a line that reflects the time frame, responses, and identity types selected.



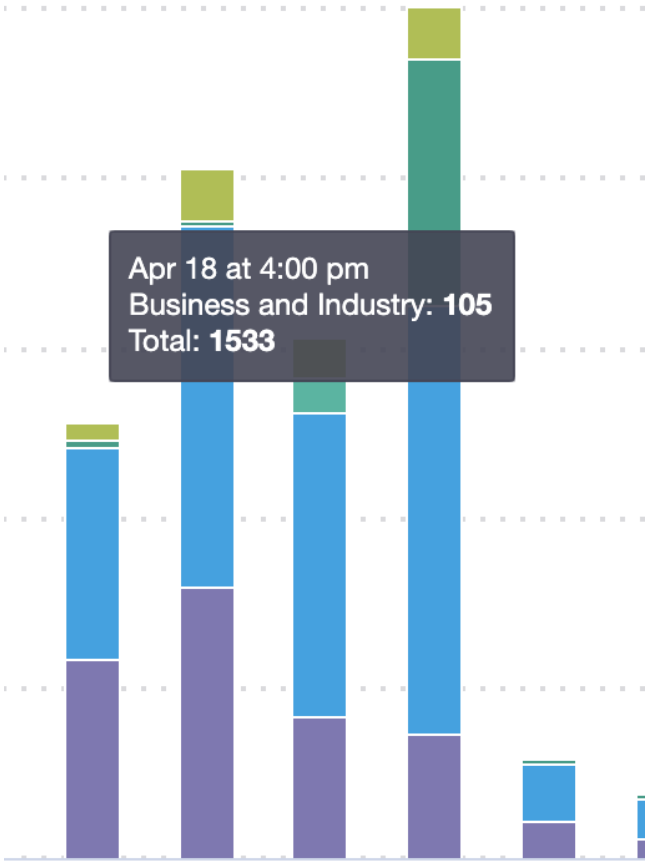
Hovering on a point on the graph will show the date, time and number of requests for that timestamp.



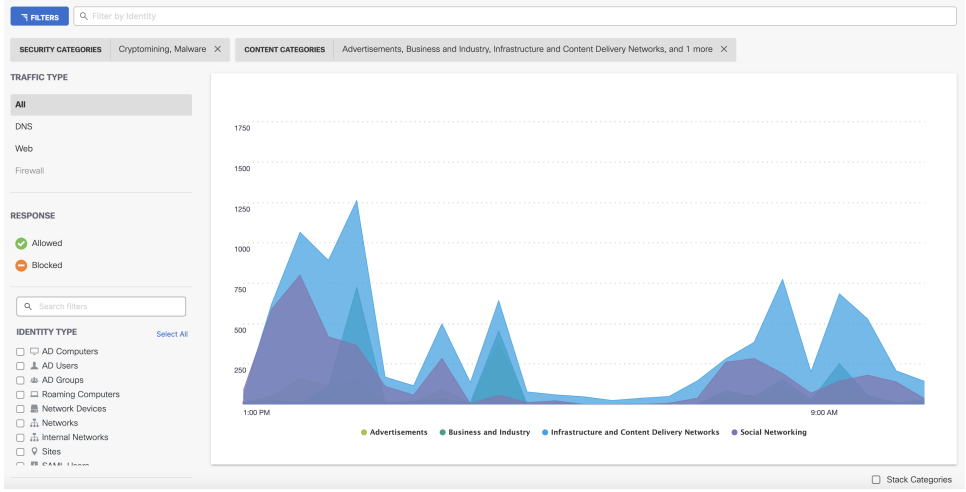
When you do filter by security or content categories, the trend graph will change to a bar graph of the requests for those categories within the selected time frame and other filters. Categories can be stacked if multiple categories showed traffic for those dates by clicking the **Stack Categories** checkbox.



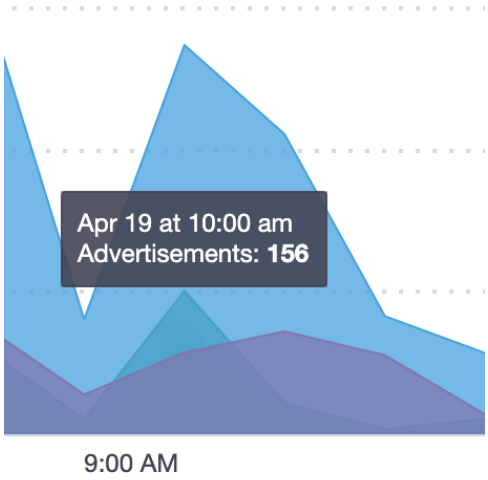
Hovering on a category for a specific date and time will show the total requests for that category as well as the overall total requests for that timestamp.



You can also choose to view the categories unstacked, by unchecking the **Stack Categories** checkbox.



Hovering on a point on the graph will show the total requests for that category at that time.



Clicking a category on either graph type will redirect you to the Category Details for that category.

78 Activity Volume Report

Topics:

- Activity Volume Report

Describes the purpose and procedures for activity volume report and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Activity Volume Report

Describes activity volume report. The Activity Volume Report provides an overall summary of traffic by security categories and policies affected by content categories and Destination Lists.

The Activity Volume Report provides an overall summary of traffic by security categories and policies affected by content categories and Destination Lists. You can view traffic allowed and blocked across these fields as well as the percentage of this traffic for each field and determine which activities may be a potential risk in the organization.

View Requests by Volume of Activity

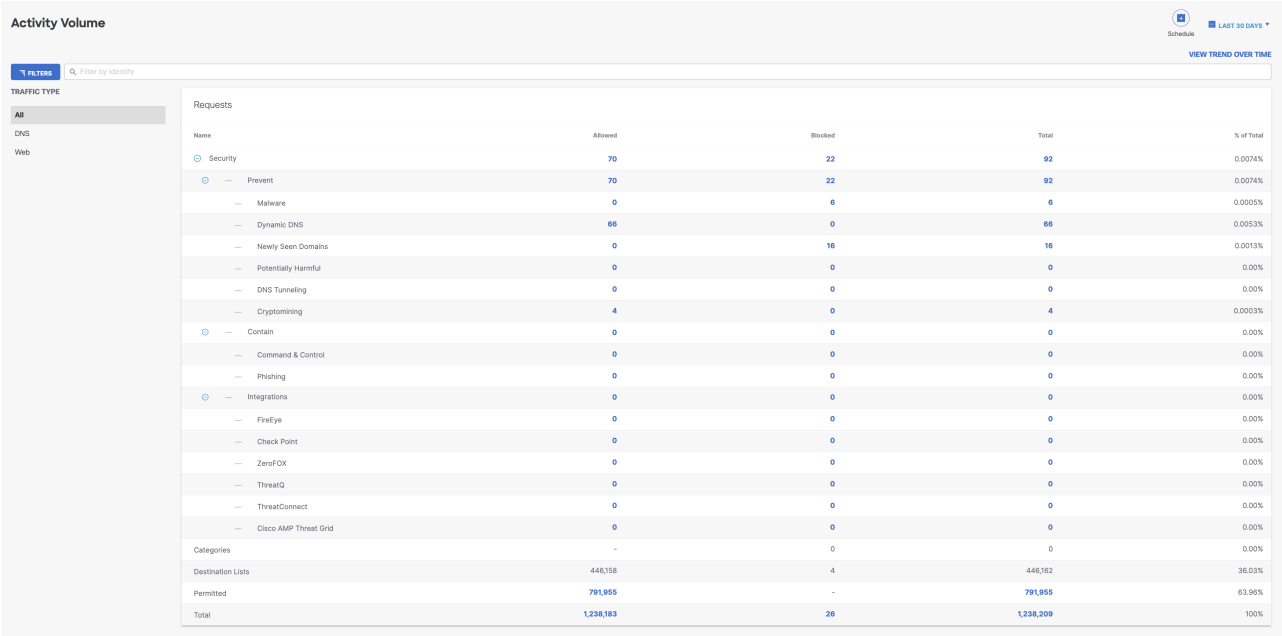
Provides instructions for viewing requests by volume of activity. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

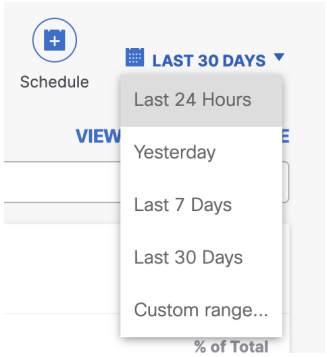
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

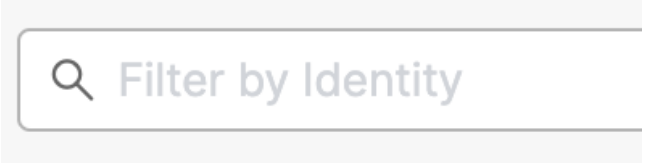
1. Navigate to **Monitor** > **Reports** > **Activity Volume**. You are presented with a chart that depicts categorized requests over time.



2. Choose a time frame to view the activity volume.The Activity Volume Report can be filtered by the Last 24 hours, Yesterday, Last 7 Days, Last 30 Days, or a custom range within the last 30 days.



3. If necessary, filter by a specific identity using the search tool.



The Activity Volume Report consists of three main fields of activity (Security, Categories, and Destination Lists), the total Permitted requests, and the Total requests of all traffic. Each field displays the number of requests Allowed, Blocked, the Total number of requests, and the Percentage of all requests that that field represents.

> **Note**
>
> Allowed Categories do not display any results.

Requests

Name	Allowed	Blocked	Total	% of Total
Security	70	22	92	0.0076%
Categories	-	0	0	0.00%
Destination Lists	434,626	4	434,630	35.86%
Permitted	777,295	-	777,295	64.13%
Total	1,211,991	26	1,212,017	100%

View Activity Volume by Threat Categories

Describes viewing activity volume by threat categories. The Security field contains two sub-fields of traffic data relating to potential security risks: Prevent and Contain. For more information about threat categories, see Threat Category Descriptions. Integrations are not applicable to Secure Access.

The Security field contains two sub-fields of traffic data relating to potential security risks: Prevent and Contain. For more information about threat categories, see Threat Category Descriptions. Integrations are not applicable to Secure Access.

Requests

Name	Allowed	Blocked	Total	% of Total
Security	70	22	92	0.0076%
Prevent	70	22	92	0.0076%
Contain	0	0	0	0.00%
Integrations	0	0	0	0.00%

Prevent

Describes prevent. The Prevent security section lists the threat categories utilized to prevent threats and risks in your environment. The chart provides the number of Allowed, Blocked, Total Requests, and the percentage of Total Requests for each category.

The Prevent security section lists the threat categories utilized to prevent threats and risks in your environment. The chart provides the number of Allowed, Blocked, Total Requests, and the percentage of Total Requests for each category. The data here provides an insight as to which categories receive the most requests which can determine if policies need to be updated or configured differently.

Prevent	70	22	92	0.0076%
Malware	0	6	6	0.0005%
Dynamic DNS	66	0	66	0.0054%
Newly Seen Domains	0	16	16	0.0013%
Potentially Harmful	0	0	0	0.00%
DNS Tunneling	0	0	0	0.00%
Cryptomining	4	0	4	0.0003%

Contain

Describes contain. The Contain section lists two threat categories in which threats are contained and prevented from spreading in your environment. The chart provides the number of Allowed, Blocked, Total Requests, and the percentage of Total Requests for each category.

The Contain section lists two threat categories in which threats are contained and prevented from spreading in your environment. The chart provides the number of Allowed, Blocked, Total Requests, and the percentage of Total Requests for each category.

Contain	0	0	0	0.00%
Command & Control	0	0	0	0.00%
Phishing	0	0	0	0.00%

View Activity Volume by Policy Traffic

Describes viewing activity volume by policy traffic. The Categories and Destination Lists fields provide an insight into traffic where requests were allowed or blocked due to policies configured with content categories and destination lists.

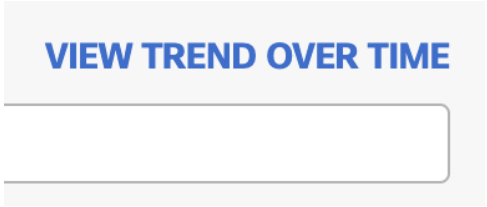
The Categories and Destination Lists fields provide an insight into traffic where requests were allowed or blocked due to policies configured with content categories and destination lists. The chart provides the number of Allowed, Blocked, Total Requests, and the percentage of Total Requests for each field. This information shows what types of policies are receiving the most traffic and may need more efficient management.

Categories	-	0	0	0.00%
Destination Lists	434,626	4	434,630	35.86%

View Trends

Describes viewing trends. Click the View Trend Over Time button to be redirected to the Total Requests Report for an enhanced visualization of traffic trends over a given period of time.

Click the View Trend Over Time button to be redirected to the Total Requests Report for an enhanced visualization of traffic trends over a given period of time.



79 App Discovery Report

Topics:

- View the App Discovery Report
- View the Highest Risk Apps
- Review Apps in the Apps Grid
- View App Details
- Change App Details
- Control Apps
- Control Advanced Apps
- View Traffic Data Through SWG Service

Introduces app discovery report. Monitor the cloud apps in use by your organization with the App Discovery report. Apps can be blocked through rules when risk levels are unacceptable or when an app category is inappropriate for your organization. For more information, see Control Apps.

Monitor the cloud apps in use by your organization with the App Discovery report. To effectively reduce the risk introduced by apps, monitor app use and look for a reduction over time in the number of DNS requests made by apps with high and very high-risk assessments. You can monitor this with the App Discovery report.

Apps can be blocked through rules when risk levels are unacceptable or when an app category is inappropriate for your organization. For more information, see Control Apps.

App Discovery data is aggregated and processed once a day. It may take up to 24 hours for new data to populate an App Discovery report. Logging of traffic is required for App Discovery to function.

View the App Discovery Report

Describes viewing the app discovery report. Monitor the cloud apps in use by your organization with the App Discovery report.

Monitor the cloud apps in use by your organization with the App Discovery report. To effectively reduce the risk introduced by apps, monitor app use and look for a reduction over time in the number of DNS requests made by apps with high and very high-risk assessments.

View the App Discovery Report

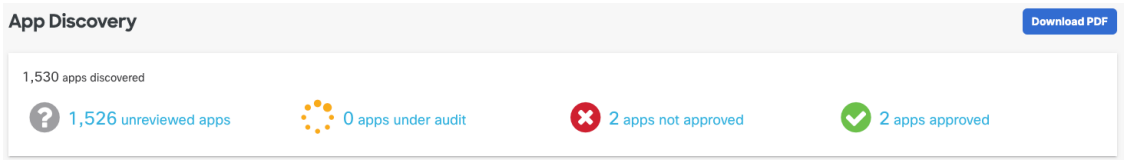
Provides instructions for viewing the app discovery report. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

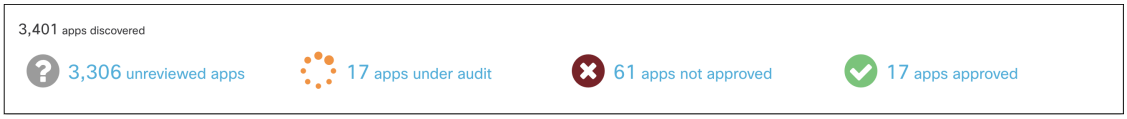
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **App Discovery**.



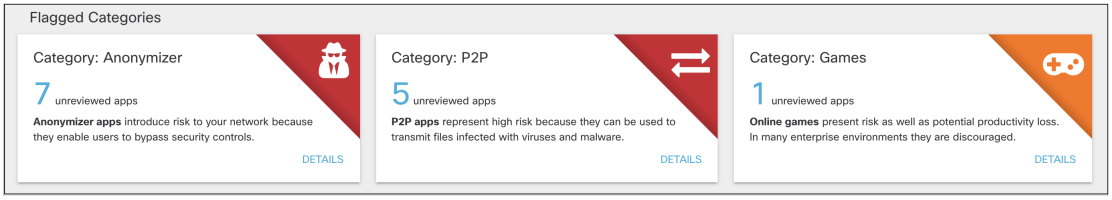
2. View the discovered apps in your environment.
   - **Unreviewed**–The app has not yet been assigned any label.
   - **Under Audit**–The app is currently being reviewed.
   - **Not Approved**–The app should not be approved for use in your environment.
   - **Approved**–The app may be used in your environment.



> **Note**
>
> Once an app has been given a label, it cannot be set back to Unreviewed. You can use the Under Audit label for apps that still need review. When you set an app to Not Approved, it is *not* automatically blocked from use.

> **Note**
>
> Labels within the App Discovery report are used to help review apps in your environment. You must configure application settings within a policy to block apps. For more information, see Control Apps.

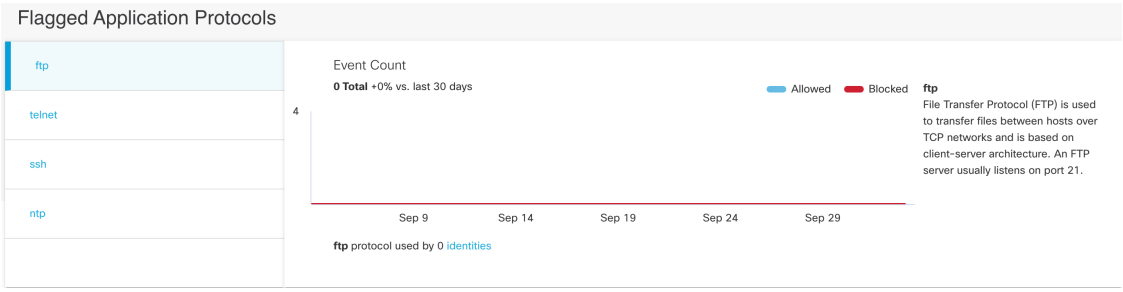
3. View the flagged categories. Cisco's Cloud Security researchers categorize apps according to function, source, and other factors. The categories of most interest (and most risk) are:
   - **Anonymizers**–Services that provide an anonymous proxy tool that attempts to make activity on the Internet untraceable. Apps in this category can introduce data exfiltration risks.
   - **Cloud Storage**–Applications that offer massively scalable storage capacity that can be used for applications and file storage. Apps in this category can also be used for data exfiltration.
   - **Collaboration**–Apps that may store sensitive data in unreliable services or unsecured environments.
   - **Games**–Online and mobile games. While games are not notable for data exfiltration risks, some can be used as attractive ways to introduce malware.
   - **Media**–Apps that can contribute to productivity loss and are frequently managed as unwanted bandwidth consumers.
   - **P2P**–Peer to Peer torrents like apps and protocols. These apps can be used for data exfiltration.
   - **Social Networking**–Can be used to transmit sensitive data as well as contribute to productivity loss.



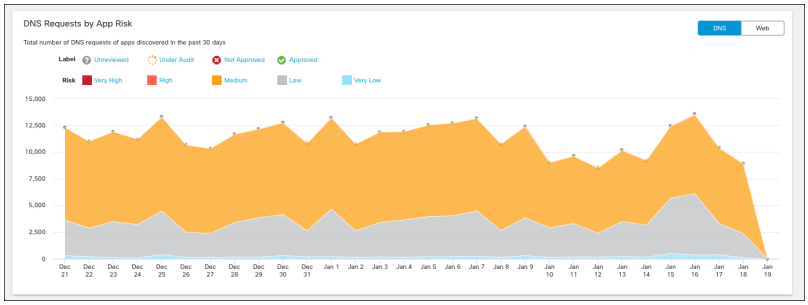
For a complete list of application categories, see Application Categories

4. View the flagged application protocols. These protocols are flagged based on the protocol used by the application.

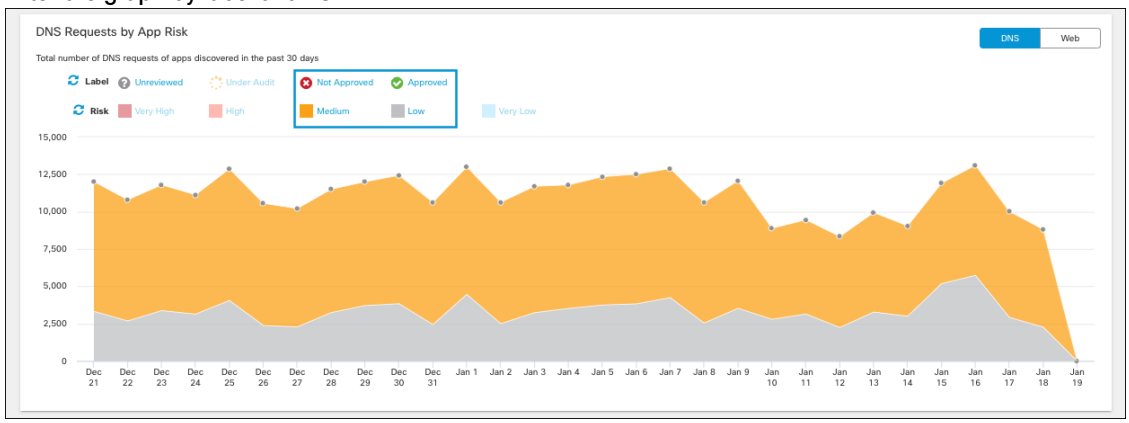
> **Note**
>
> Dismissing a flagged app card hides it from the overview. It does not label or block the app.



5. View DNS requests and traffic by App Risk. The graph shows the total number of DNS requests for apps discovered in the past 30 days. Secure Access assigns a risk score to apps based on several factors. The DNS requests made by a high-risk app can be considered more problematic than the same number of requests made by an app with a lower risk score.



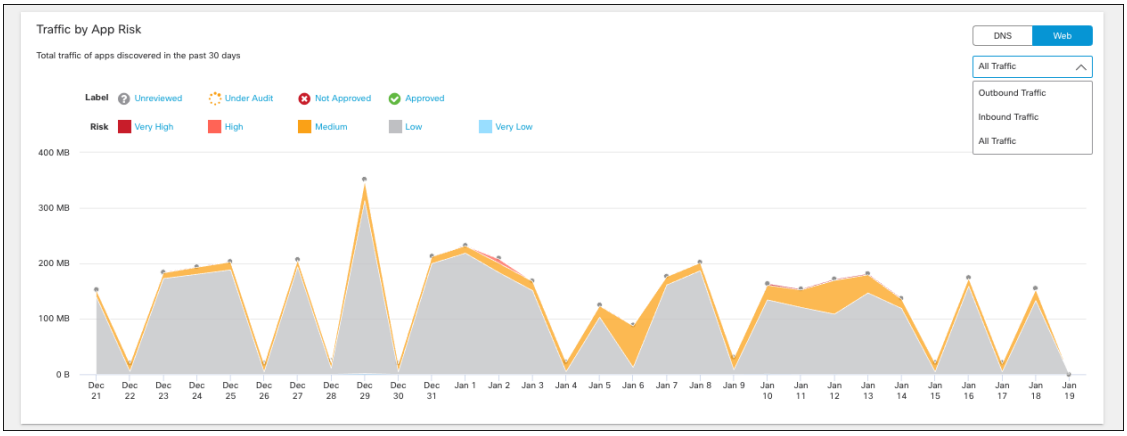
a. Filter the graph by label and risk.



b. Select Web and review Traffic (bytes in and out) by App Risk for the last 30 days.

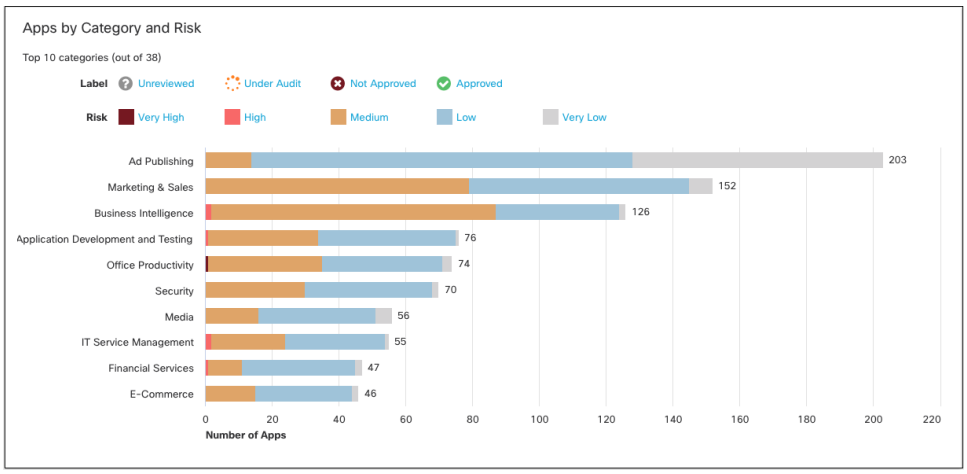


c. View All Traffic, Outbound Traffic or Inbound Traffic.

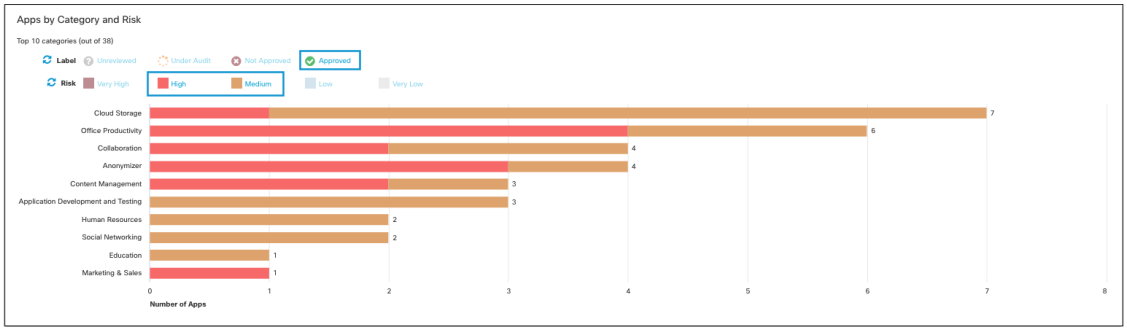


6. View apps by category and risk.

Click a bar on the chart to view apps in that category in the App Grid.



a. Filter by label and risk.



View the Highest Risk Apps

Describes viewing the highest risk apps. You can view the highest-risk apps in the App Discovery Report by filtering for apps with the highest number of DNS requests.

You can view the highest-risk apps in the App Discovery Report by filtering for apps with the highest number of DNS requests.

The App Discovery report is used to help review apps in your environment. To block risky apps, you must configure application settings within a policy rule to control apps.

Procedure

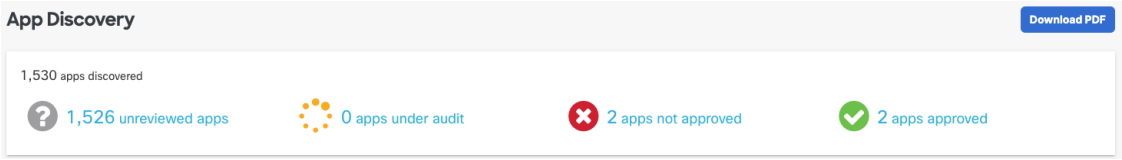
Provides instructions for procedure. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports App Discovery .

Before you begin

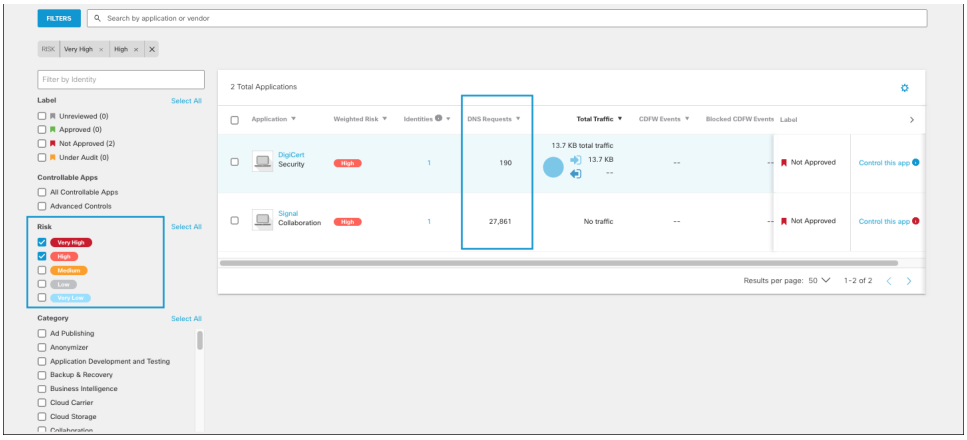
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **App Discovery**.



2. From the overview, click **Unreviewed Apps**. The App Grid appears depicting data for the last 90 days.
3. Filter the list by selecting **Very High** or **High** from the Risk menu. Only the riskiest apps will be listed.
4. Filter the list by **DNS Requests** to display the apps with the highest number of requests at the top.



The apps at the top of the list should now represent the highest number of DNS requests made by the riskiest apps.

Review Apps in the Apps Grid

Describes reviewing apps in the apps grid. The Apps Grid provides an overall view of application activity in your environment and the potential risk indicated by this traffic.Packages and Feature AvailabilityNot all of the features described here are available to all Secure Access packages.

The Apps Grid provides an overall view of application activity in your environment and the potential risk indicated by this traffic.

> **Note**
>
> Packages and Feature Availability
>
> Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Your Current Package.
>
> If you encounter a feature here that you do not have access to, contact your sales representative for more information.

Procedure

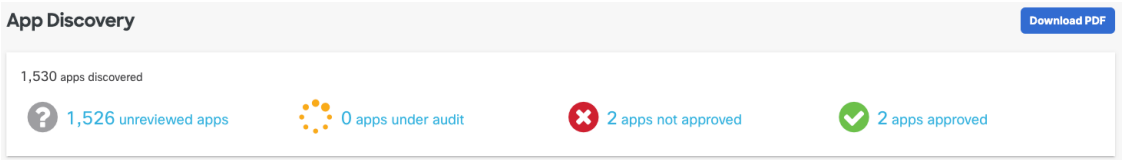
Provides instructions for procedure. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports App Discovery and click one of the app labels to open the Apps Grid.

Before you begin

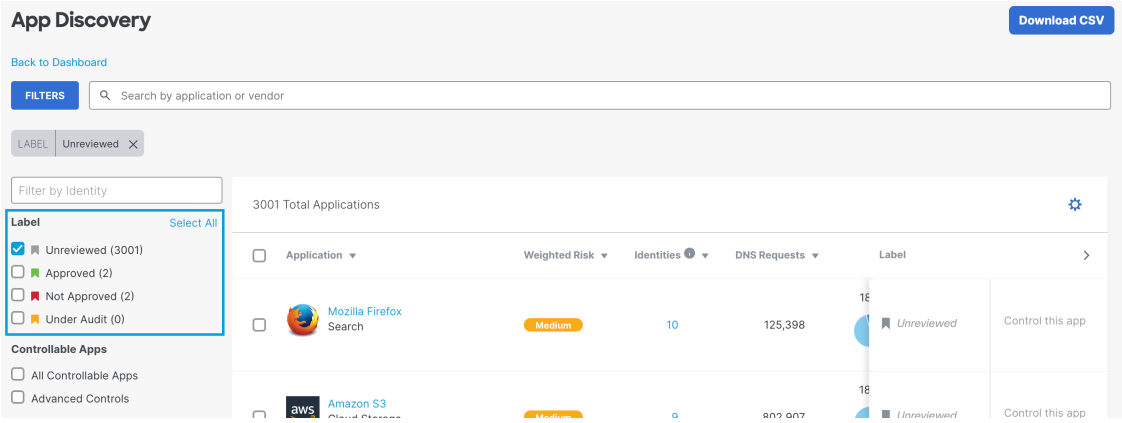
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



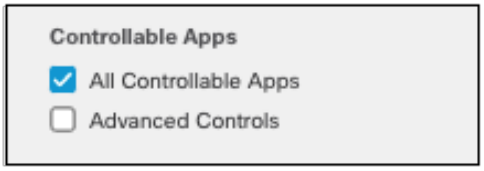
2. Filter by label.
   - **Unreviewed**–The app has not yet been assigned any label.
   - **Approved**–The app may be used in your environment.
   - **Not Approved**–The app should not be approved for use in your environment.
   - **Under Audit**–The app is currently under review.



> **Note**
>
> When you set an app to Not Approved or Approved, it is *not* automatically blocked or allowed. Labels within the App Discovery report are used to help review apps in your environment. You must configure application settings within a policy to block apps. For more information, see Control Apps.

3. Filter by Controllable Apps.

   You can filter the apps listed by apps that are controllable and apps that have advanced app controls.



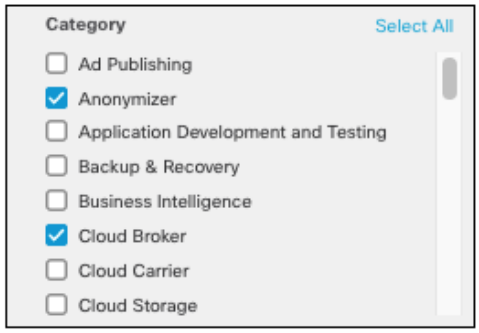
4. Filter by Risk.

   For more information on how risk is calculated, see Risk Details.



5. Filter by category.

   For more information on app categories, see Application Categories.

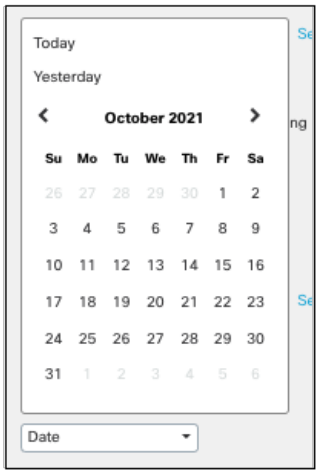


6. Filter by app type.

   - **SaaS**–Software as a service
   - **PaaS**–Platform as a service
   - **IaaS**–Infrastructure as a service



7. Filter by date. The app grid will display data for 24 hours based on the date selected. The default is the current date.



Configure Columns to Display

Provides instructions for configuring columns to display. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

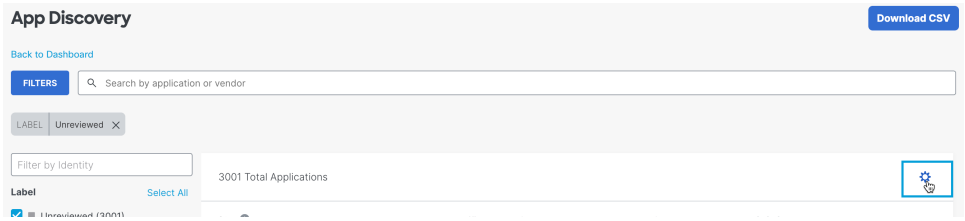
You can customize what columns are displayed.

Before you begin

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

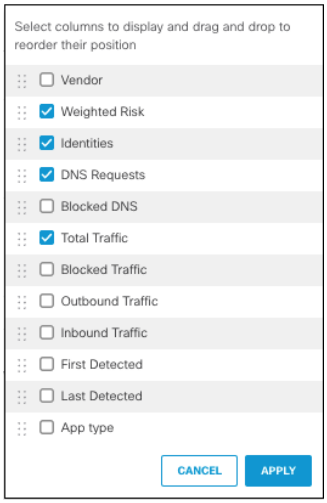
Procedure

1. Click the **Actions** icon.



2. Select columns to display and click **Apply**.

> **Note**
>
> Rearrange the order of settings by dragging and dropping the column fields.



- **App Type**–The type of app: SaaS, PaaS or IaaS.
- **Blocked DNS**–The percentage of DNS requests blocked by Secure Access based on policy configurations.
- **Blocked Traffic**–The percentage of all traffic blocked.
- **DNS Requests**–The number of DNS requests for this app.
- **First Detected**–The date the app was first detected.
- **Identities**–The number of identities affected by the app. Click this number to view the app's details and the list of identities with requests for that app.
- **Inbound Traffic**–Bytes inbound.
- **Last Detected**–The date the app was last detected.
- **Outbound Traffic**–Bytes outbound.
- **Total Traffic**–The total number of bytes inbound and outbound for this app in your environment.
- **Vendor**–The vendor that owns the app.
- **Weighted Risk**–The risk the app poses to the environment.

Change the Label of an App

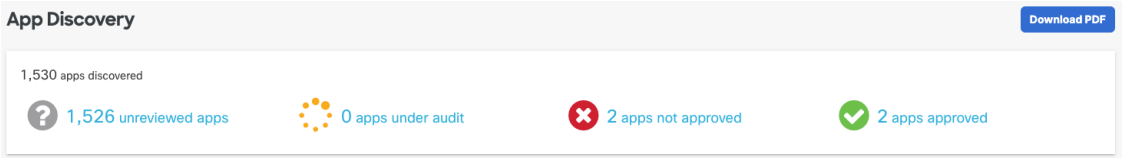
Provides instructions for changing the label of an app. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

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

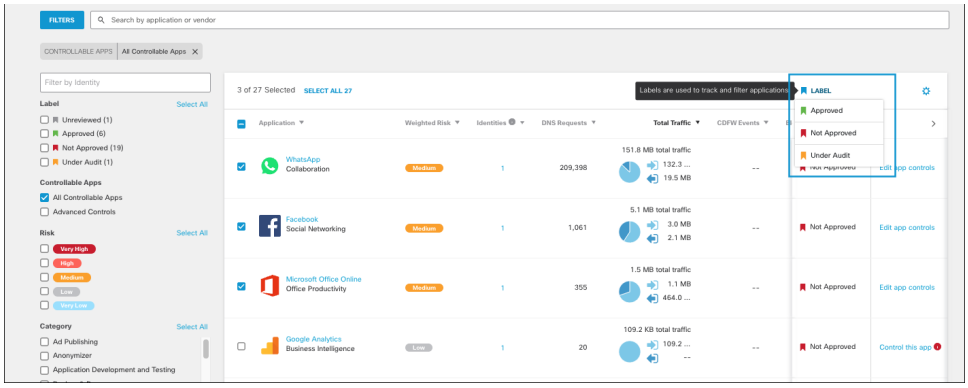
Procedure

1. Navigate to **Reporting** > **Core Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



2. Check the checkbox for the app or apps you want to change the label of, click the **Label** drop-down menu, and select the new label.

> **Note**
>
> Once an app has been given a label, it cannot be set back to Unreviewed. You can use the Under Audit label for apps that still need review.



View App Details

Describes viewing app details. The details page for an app lists summary information about the app, including: The risk score for the app, and the details on how it was calculated.

The details page for an app lists summary information about the app, including:

- The risk score for the app, and the details on how it was calculated.
- The identities that have made DNS requests and seen traffic for the app.
- The detailed attributes of the app, which can help you perform a risk/benefit analysis of permitting the app to be used in your environment.

Procedure

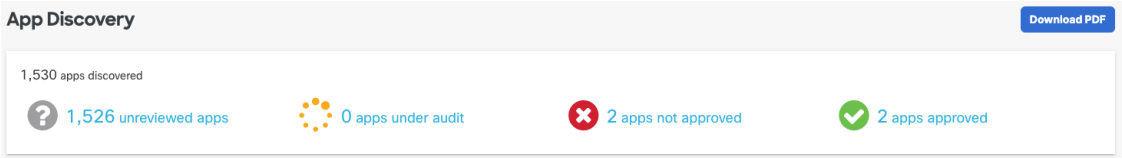
Provides instructions for procedure. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports App Discovery and click one of the app labels to open the Apps Grid.

Before you begin

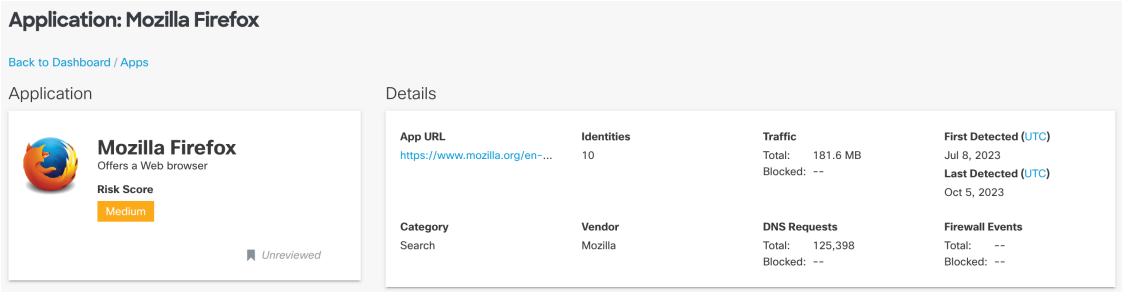
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

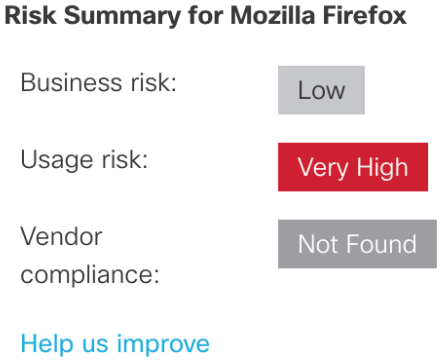
1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



2. Click the name of an app to view its details for the last 90 days.
3. View the initial details of the app, including the name and a description of the app.



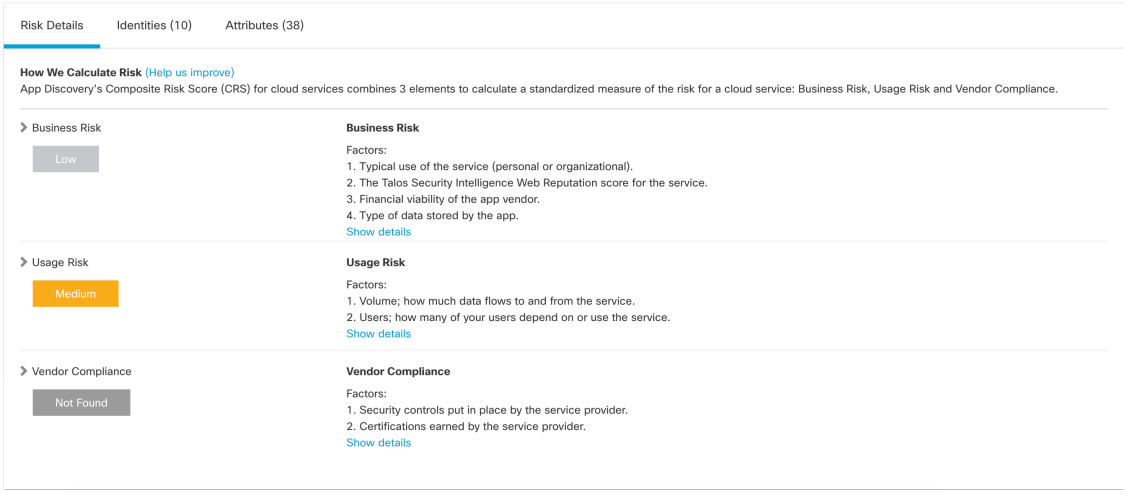
- **Risk Score**–The overall score calculated from the risk details.



- **Unreviewed**, **Approved**, **Not Approved**, or **Under Audit**– Current status od the app. Click **Control this app** to edit the label or control the app. For more information, see Control Apps.
- **App URL**–The URL of the app.
- **Category**–The category the app falls under. For more information, see Application Categories.
- **Identities**–The number of sources that accessed the app.
- **Vendor**–The owner of the app.
- **Traffic**–The number of bytes of total traffic and bytes blocked.
- **DNS Requests**–The total number of DNS requests and the percentage of requests blocked by Secure Access.
- **First Detected**–The date the app was first detected.
- **Last detected**–The date the app was last detected.

4. Click **Risk Details**.

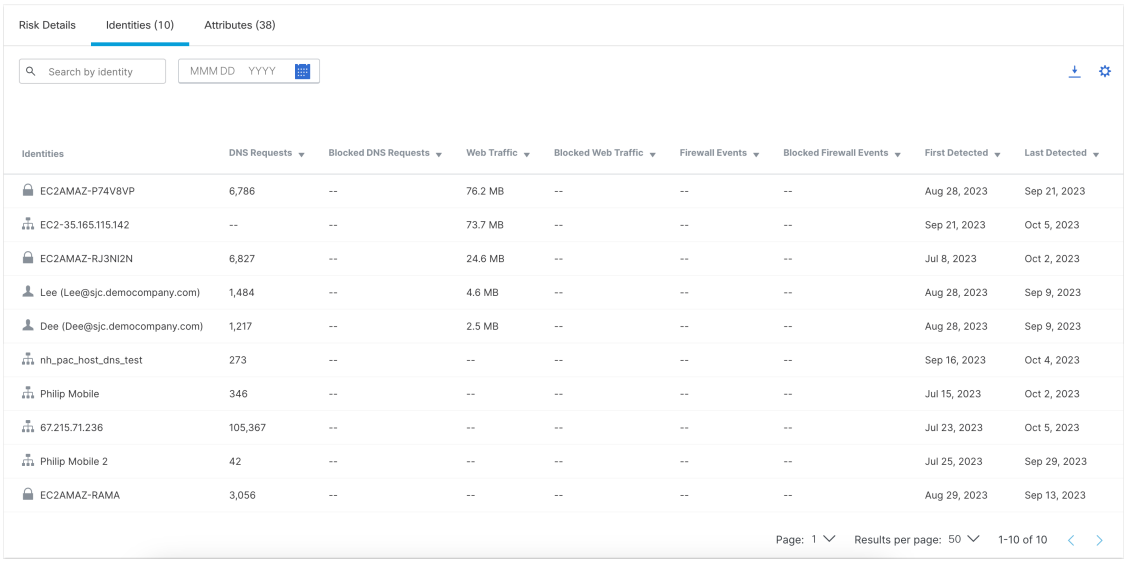
   The Risk Details tab displays the app's risk score and how it was calculated, including Business Risk, Usage Risk, and Vendor Compliance.



5. Click **Itenities**.

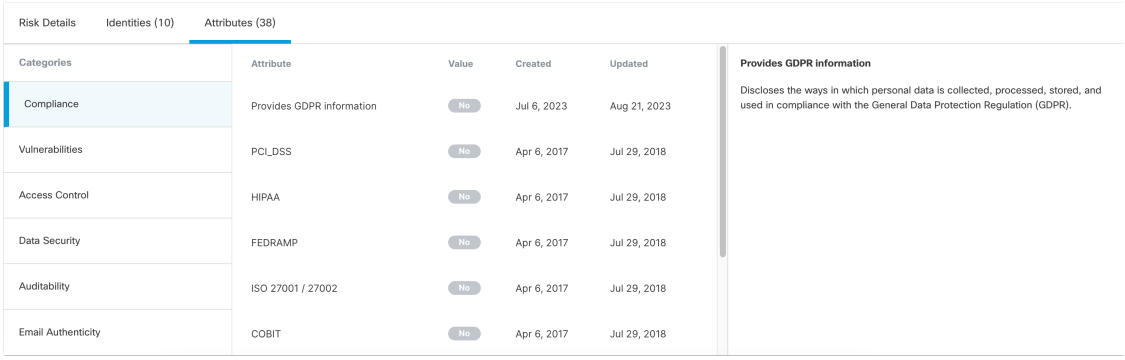
   The Identities tab lists your organization's sources that have made DNS requests and traffic for this app.

   Click the Download CSV icon to download this information as a CSV file.



6. Click **Attributes**.

   The Attributes tab lists the various attributes associated with this app.



For each displayed attribute, Secure Access shows whether the attribute applies to the application and the dates when the attribute information was collected and updated. Use the attributes to evaluate the risk that the application will expose your environment to data breaches, identity theft, financial fraud, and other cyber threats.

The attribute categories are:

- **Compliance attributes** – Indicate whether the application complies with the requirements of a number of certifications such as GDPR, HIPAA, and FEDRAMP.
- **Vulnerabilities attributes** – Indicate whether the application is vulnerable to exploits that attackers could use to compromise the security of the affected systems, steal sensitive data, or cause other types of damage.
- **Access control attributes** – Indicate the methods the application supports to manage and restrict access based on a user's identity, role, and authorization level.
- **Data security attributes** – Indicate the practices and technologies the application uses to protect data from unauthorized access, use, disclosure, modification, or destruction.
- **Auditability attributes** – Indicate the abilities the application provides for an administrator to review the activity and transactions of a system, to ensure that it is operating in a compliant and secure manner.
- **Email authenticity attributes** – Indicate what methods the app provides to verify that email is actually from the sender that it claims to be from, and that the message has not been tampered with or altered in any way during transit.

Change App Details

Describes changing app details. You can change details about apps from within the App Discovery Report: You can change the review status label assigned to an app.

You can change details about apps from within the App Discovery Report:

- You can change the review status label assigned to an app. Labels help you keep track of the review status of apps, so you know which ones are approved for use in your environment. The possible label values are:
  - **Unreviewed**–The app has not yet been assigned any label.
  - **Approved**–The app may be used in your environment.
  - **Not Approved**–The app should not be used in your environment.
  - **Under Audit**–The app is currently under review.

> **Note**
>
> App labels are primarily used for tracking and filtering, to help you keep track of the app review process within your organization. They do not of themselves control access to an app. However, if you establish an app risk profile app risk profile that uses Label Status as a criteria, and that profile is used in an internet access rule, that rule may cause an application to be blocked or allowed based on the value of its app label.

- You can change the risk score for the app, overriding the value calculated by Umbrella. The possible risk scores are:
  - Very High
  - High
  - Medium
  - Low

- Very Low

> **Note**
>
> Changing the risk score for an app does not change whether Secure Access blocks or allows the app. (You must configure application settings within a policy to block apps. For more information, see Manage the Access Policy or Manage Security Profiles for Internet Access.) Secure Access provides risk scores strictly for your own information, to help you keep track of the risk levels for different apps and decide whether to block or allow them. You can accept the risk levels calculated by Secure Access, or assign different risk scores based on the risk tolerances within your organization.

Change the Risk Score for an App

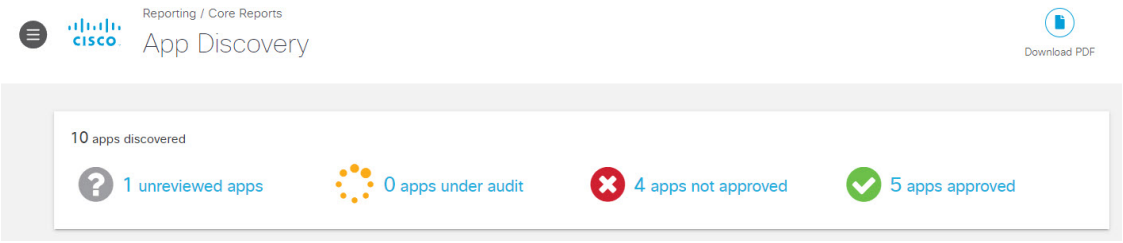
Provides instructions for changing the risk score for an app. A minimum of Read Only access to the Secure Access dashboard. See Manage Accounts.

Before you begin

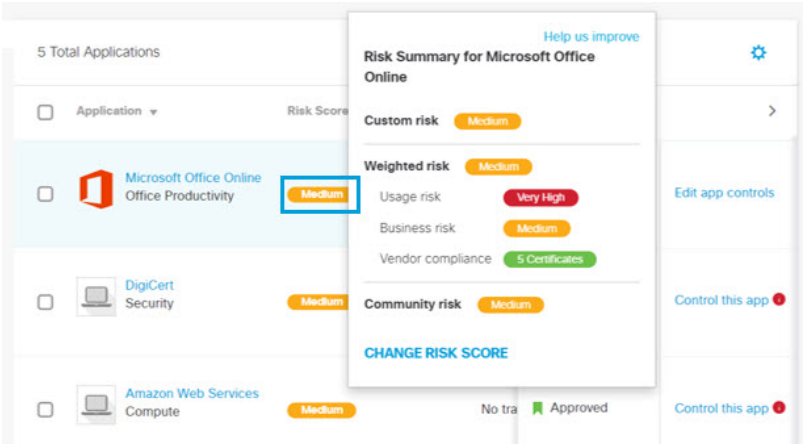
A minimum of Read Only access to the Secure Access dashboard. See Manage Accounts.

Procedure

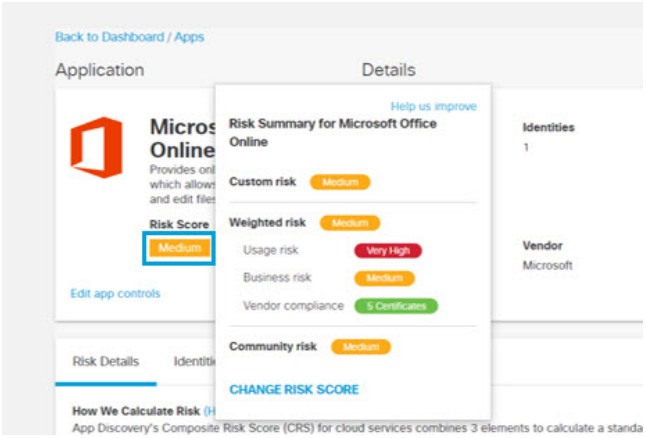
1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



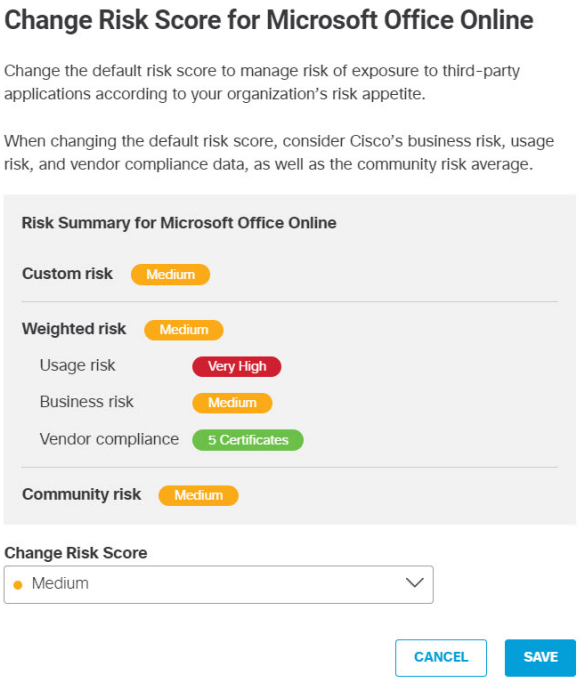
2. You have two choices:
   - To change the risk score for an app from the Apps Grid, hover over the risk score for an app to view its Risk Summary.



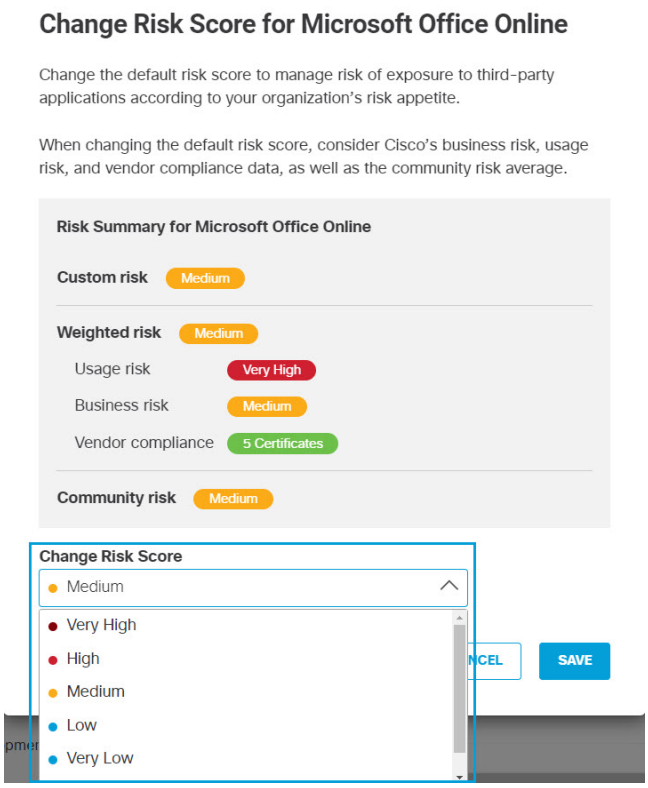
   - To change the risk score for an app from its Details page, click the name of the app on the Apps Grid, then from the Details page hover over the risk score to view the Risk Summary.



3. From the Risk Summary, click on **CHANGE RISK SCORE** to display the Risk Score Change dialog.



4. Select the new value to assign:
   - Very High
   - High
   - Medium
   - Low
   - Very Low



5. Click **SAVE**.

Change the Label of an App

Provides instructions for changing the label of an app. Labels within the App Discovery report help you keep track of the review status of apps, so you know which ones are approved for use in your environment. You can change the label for an app anytime.

Labels within the App Discovery report help you keep track of the review status of apps, so you know which ones are approved for use in your environment. You can change the label for an app anytime.

> **Note**
>
> App labels are primarily used for tracking and filtering, to help you keep track of the app review process within your organization. They do not of themselves control access to an app. However, if you establish an app risk profile that uses Label Status as a criteria, and that profile is used in an internet access rule, that rule may cause an application to be blocked or allowed based on the value of its app label.

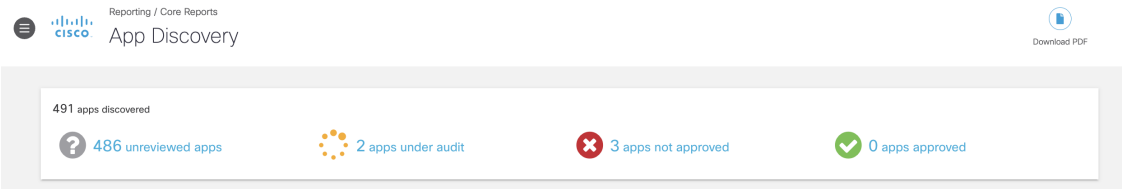
> **Note**
>
> Once an app has been given a label, it cannot be set back to **Unreviewed**. You can use the **Under Audit** label for apps that still need review.

Before you begin

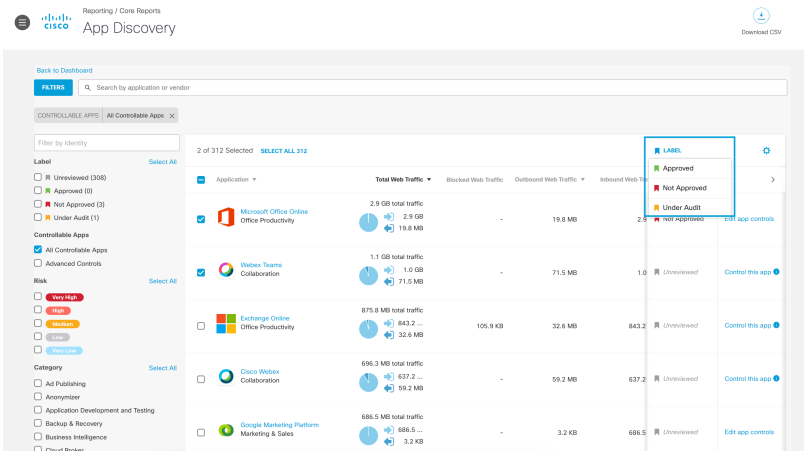
A minimum of Read Only access to the Secure Access dashboard. See Manage Accounts.

Procedure

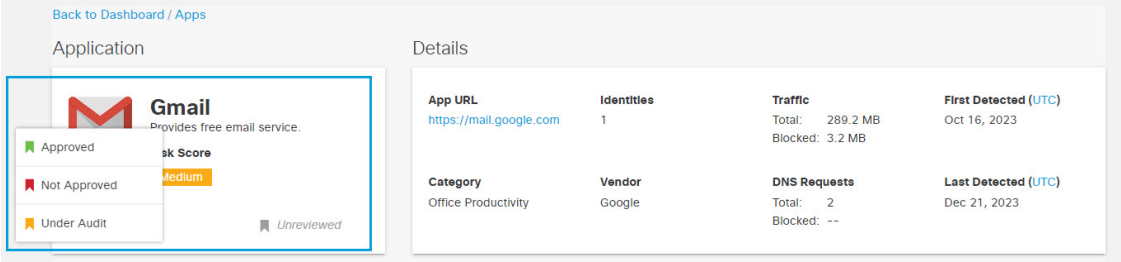
1. Navigate to **Reporting** > **Core Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



2. You have two choices:
   a. To change the label for an app from the Apps Grid, hover over its label to view the label menu.



   b. To change the label for an app from its Details page, click the name of the app on the Apps Grid, then on the Details page hover over the label to view the Label menu.



3. From the Label menu, select your choice of new value to assign:
   - **Approved**–The app may be used in your environment.
   - **Not Approved**–The app should not be approved for use in your environment.
   - **Under Audit**–The app is currently under review.

Control Apps

Describes control apps. You can control applications through rules and through the App Discovery report in View App Details and the App Grid. The application settings are a rule component that enables controlling of supported apps, regardless of usage, at the policy level.

You can control applications through rules and through the App Discovery report in View App Details and the App Grid. The application settings are a rule component that enables controlling of supported apps, regardless of usage, at the policy level. The App Discovery report allows you to review apps in your organization and control apps individually.

> **Note**
>
> App blocking requires enablement within a rule. Apps that are not present in application settings, or do not have the **Edit app controls**, **Control this app**, or **Block this app** options in App Discovery cannot be blocked. If you need to block an app we don't have yet, contact Support to request it.

Procedure

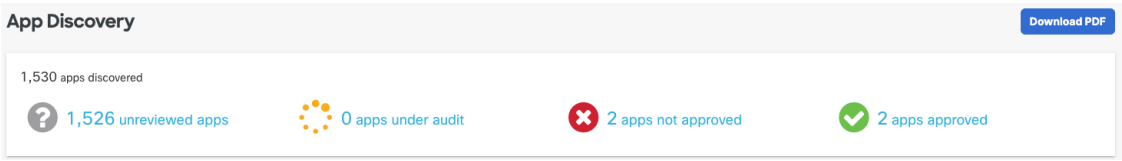
Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. Navigate to Monitor Reports App Discovery .

Before you begin

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

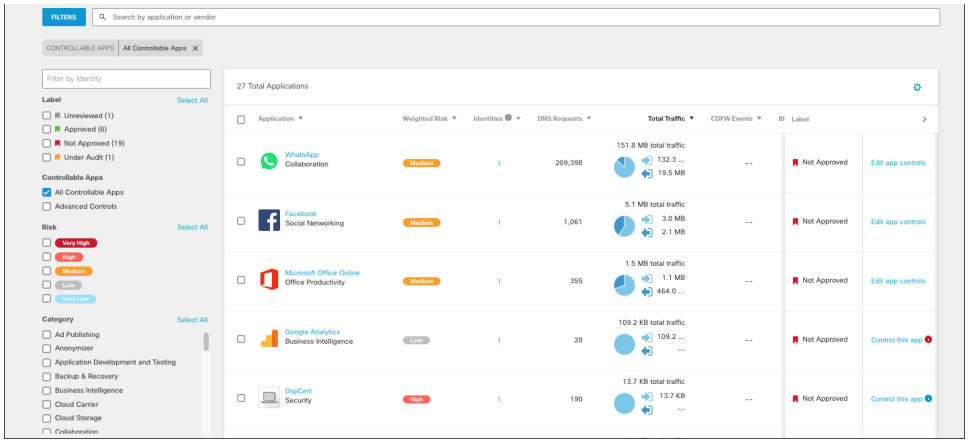
Procedure

1. Navigate to **Monitor** > **Reports** > **App Discovery**.



2. From the overview, click **Unreviewed Apps**. The App Grid appears depicting data for the last 90 days.

3. Select a **Controllable Apps** filter: **All Controllable Apps** or **Advanced Controls**.

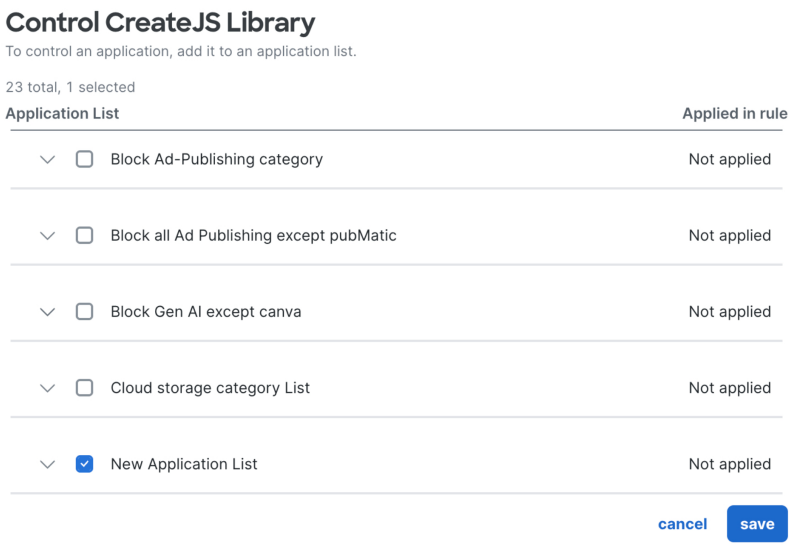


4. Click **Edit App Controls**, **Control This App**, or **Block This App**.

   - **Block This App**–Appears when a block has not been configured for this app, or a red tooltip icon will appear if the app setting is configured but has not yet been applied to a policy.
   - **Control This App**–Appears when **Block** or **Allow** have not been configured for this app, or a red tooltip icon will appear if the app setting is configured but has not yet been applied to a policy.
   - **Edit App Controls**–Appears when the app has already had settings configured but can be edited.

5. On clicking **Control This App**, the **Control Application Name** window appears. Choose one or more application lists to add this application to and click **Save**. Once saved, the internet access rules set for the application lists are applied to the application.

   The application can only be added to application lists currently active in a policy.



Control Application Lists

Describes control application lists. You can also configure a rule to block lists of applications and lists of application categories. For more information, see Manage Application Lists and Add an Application List.

You can also configure a rule to block lists of applications and lists of application categories. For more information, see Manage Application Lists and Add an Application List.

For more information about applying application lists to rules, see Manage the Access Policy.

Control Advanced Apps

Describes control advanced apps. Applications within App Discovery can be blocked or allowed based on risk assessment. In addition to blocking all content for an application, you have the option to instead block only specific content, such as file uploads or posts.

Applications within App Discovery can be blocked or allowed based on risk assessment. In addition to blocking all content for an application, you have the option to instead block only specific content, such as file uploads or posts.

> **Note**
>
> Secure Access Packages
>
> Advanced App Controls are not available to all Secure Access packages. To determine your current package, navigate to **Admin** > **Licensing**. For more information, see Determine Your Current Package

You can edit the controls of apps with advanced app controls while reviewing applications in the App Discovery Report. You can filter out apps with advanced controls and edit their application settings in the Apps Grid, or edit the application settings in the app's Details page.

Procedure

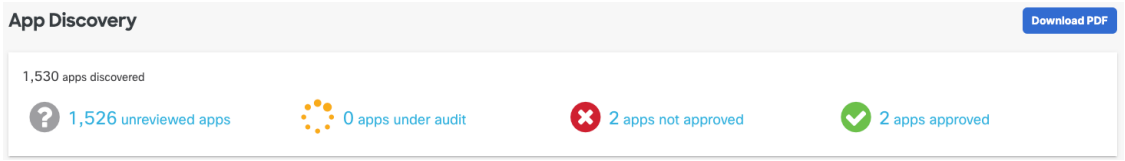
Provides instructions for procedure. Full Admin user role. For more information, see Manage Accounts. Navigate to Monitor Reports App Discovery .

Before you begin

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

Procedure

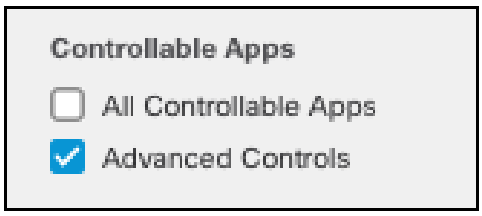
1. Navigate to **Monitor** > **Reports** > **App Discovery**.



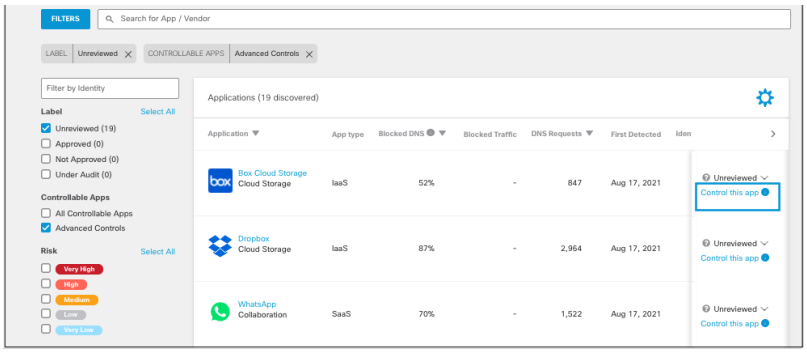
2. Click any of the discovered apps labels to enter the Apps Grid.



3. Choose **Advanced Controls** under the **Controllable Apps** filter.

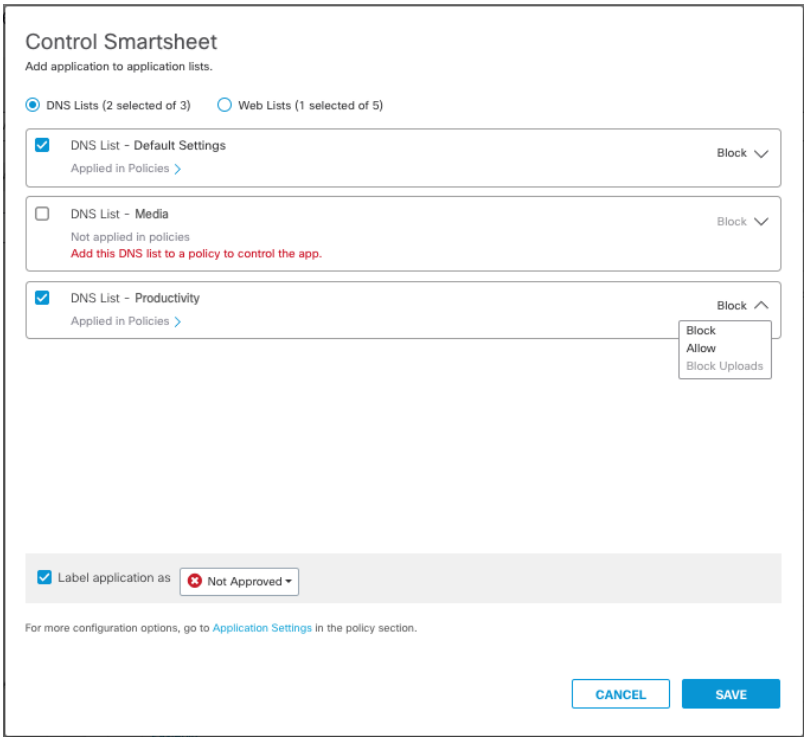


4. Choose an app to control and click **Control this app**.

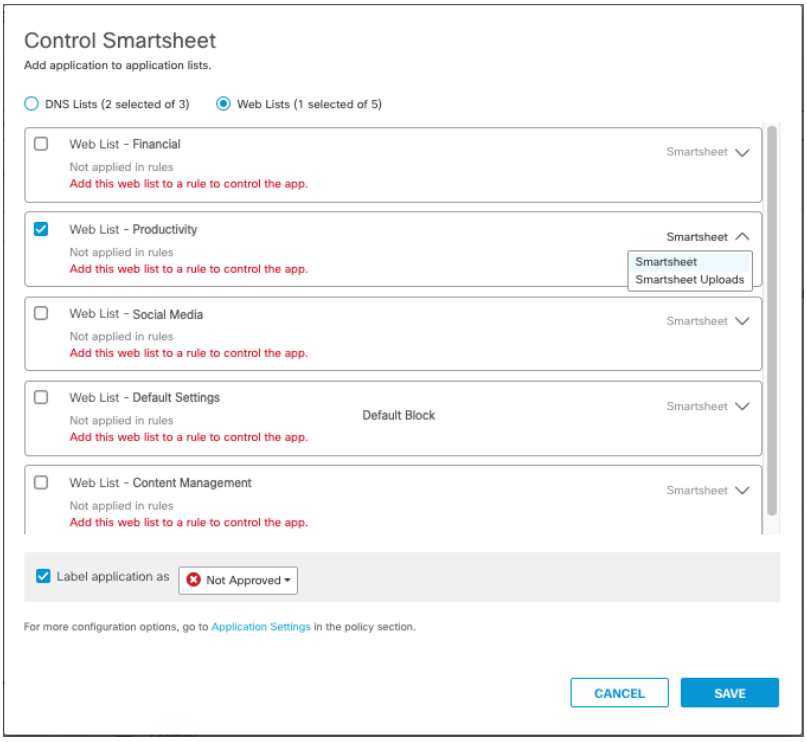


5. The application settings window appears with options for the various policies affected by the app. The app can only be added to application lists currently active in a policy.

   a. For DNS application settings, choose **Block**, **Allow**, or **Block Uploads** (if applicable).



   b. For Web application settings, choose to block all content from the app, or to block specific types of content such as uploads.



6. Choose a label to help with filtering and reporting and then click **Save**.

View Traffic Data Through SWG Service

Describes viewing traffic data through swg service. App Discovery provides traffic data through the Secure Web Gateway (SWG) service. Traffic is reported in bytes in and bytes out.

App Discovery provides traffic data through the Secure Web Gateway (SWG) service. Traffic is reported in bytes in and bytes out.

View Traffic

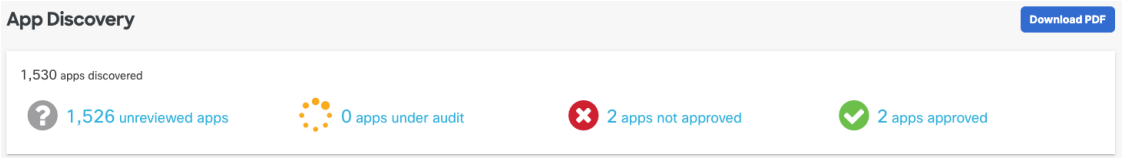
Provides instructions for viewing traffic. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports App Discovery and locate the DNS Requests by App Risk graph.

Before you begin

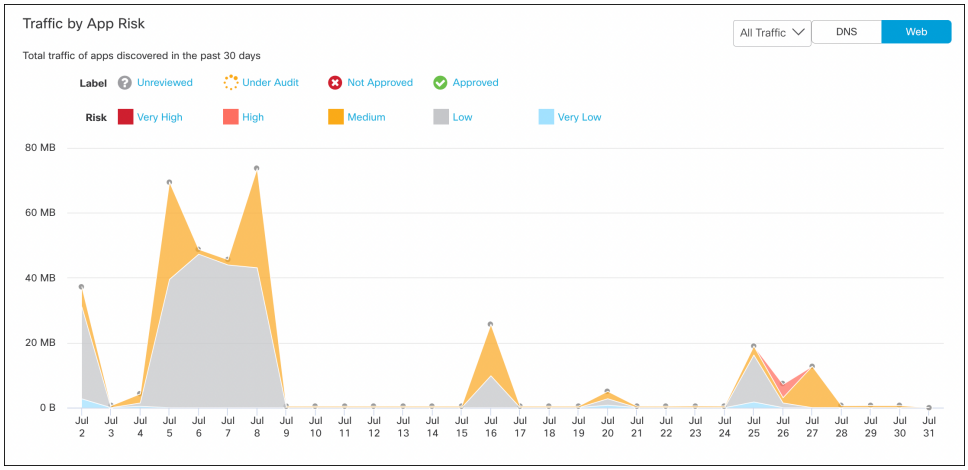
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

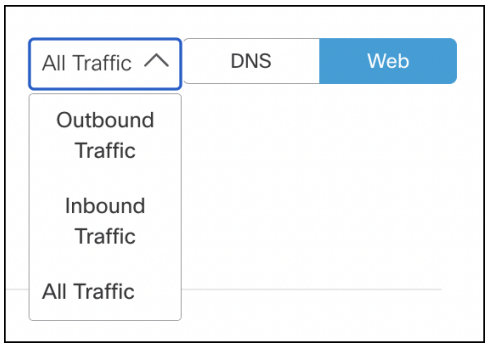
1. Navigate to **Monitor** > **Reports** > **App Discovery** and locate the DNS Requests by App Risk graph.



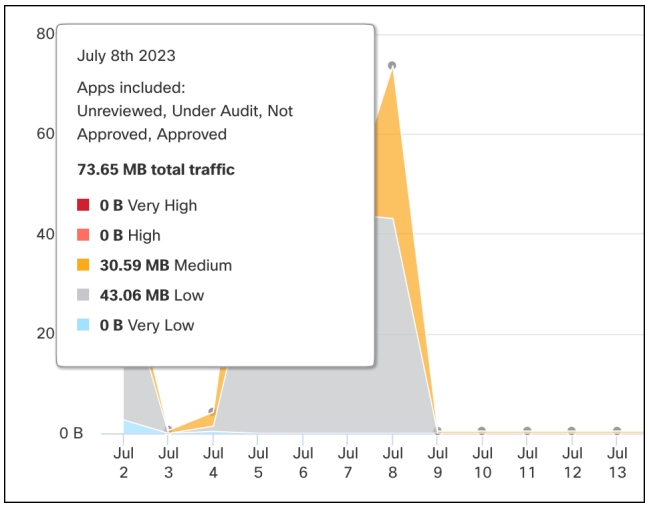
2. Click **Web** to display Traffic by App Risk.



3. Click **All Traffic** to open the drop-down and then choose to view **All Traffic**, **Inbound Traffic**, or **Outbound Traffic**.



4. Hover on a point in the graph to view details about the traffic by app risk for that date.



View Traffic in the Apps Grid

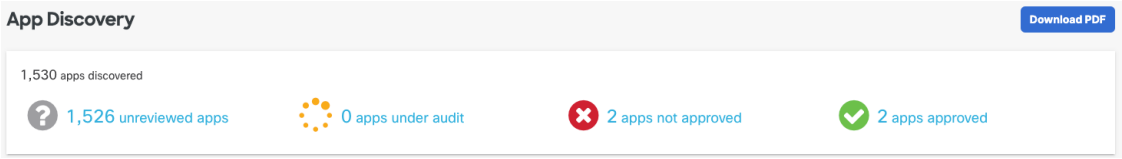
Provides instructions for viewing traffic in the apps grid. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

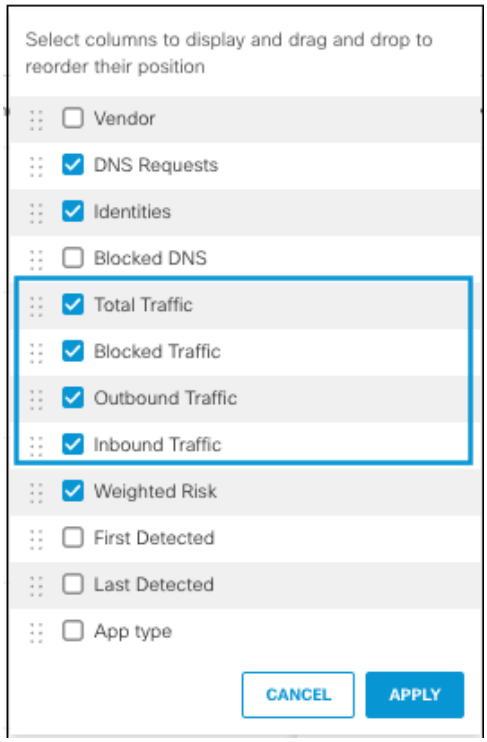
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

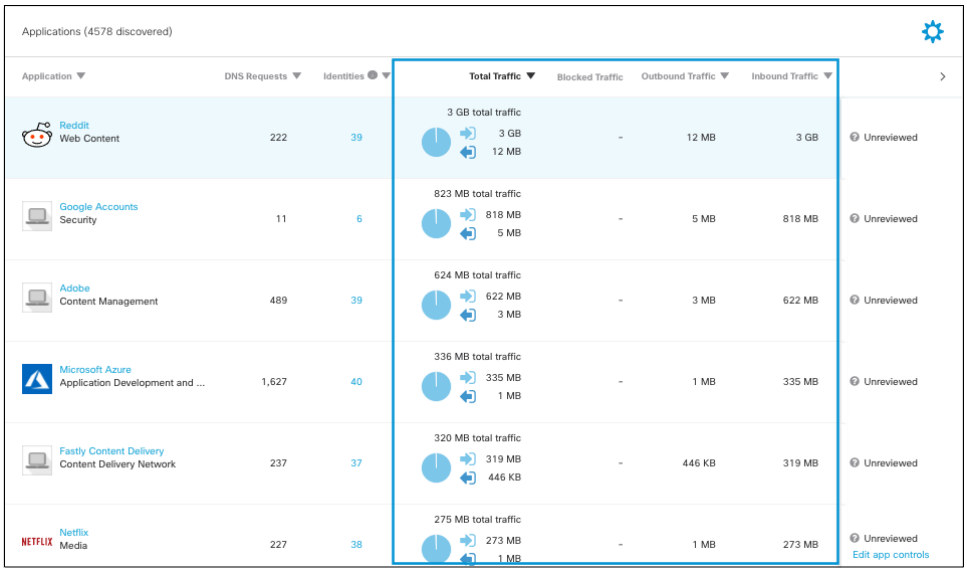
1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



2. Click the action menu to open the drop-down of options for columns displayed in the grid. Select the columns relevant to traffic and then click **Apply**.



3. View the traffic, bytes in and out, of applications by total, outbound, or inbound traffic.



View Traffic in the App Details

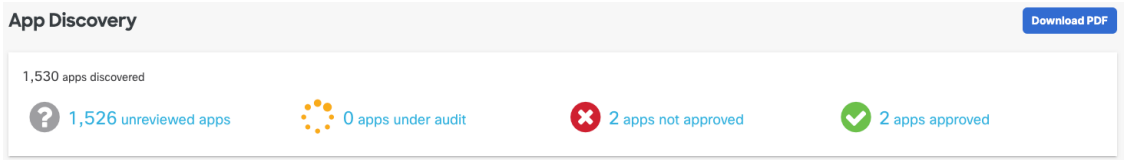
Provides instructions for viewing traffic in the app details. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

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

Procedure

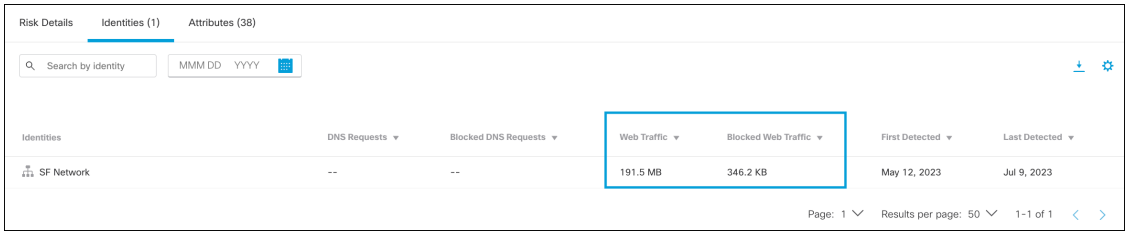
1. Navigate to **Reporting** > **Core Reports** > **App Discovery** and click the name of an app to view its details for the last 90 days.



   Details include the total and blocked traffic in bytes.



2. Navigate to the **Identities** section of the app details and view the total Traffic and Blocked Traffic.



80 Top Destinations Report

Topics:

- Top Destinations Report

Describes the purpose and procedures for top destinations report and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Top Destinations Report

Describes top destinations report. The Top Destinations report lists the top domains your organization has made access requests to over the selected time period. It is filterable, schedulable, and you can export the results to a CSV file.

The Top Destinations report lists the top domains your organization has made access requests to over the selected time period. It is filterable, schedulable, and you can export the results to a CSV file.

View the Top Destinations Report

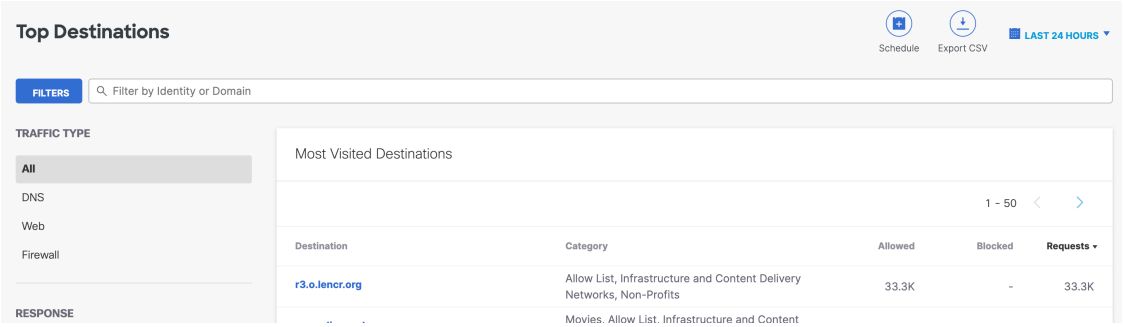
Provides instructions for viewing the top destinations report. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

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

Procedure

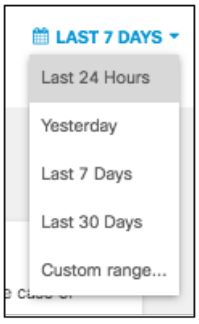
1. Navigate to **Monitor** > **Reports** > **Top Destinations**. The report displays a chart of the most visited destinations.



The following information is displayed for each destination:

- **Destination**–The domain.
- **Category**–The category, such as Malware, Business Services, Phishing, and so on.
- **Allowed**–The number of requests to that destination that were allowed.
- **Blocked**–The number of requests to that destination that were blocked.
- **Requests**–The number of requests for the domain for the selected period.

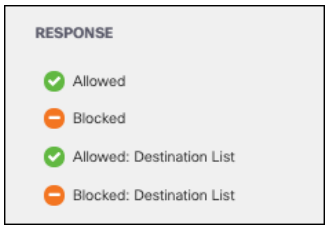
2. Choose a time frame within which data is displayed.



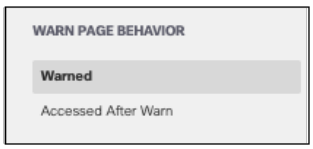
3. Choose whether to view results for All types of traffic, DNS, Web, or Firewall.



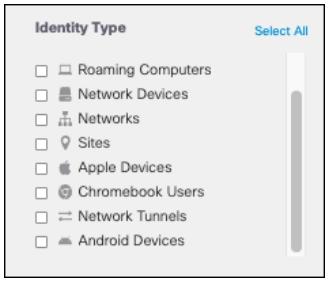
4. Filter results by the response type. Select Allowed, Blocked, Allowed: Destination List, or Blocked: Destination List. By default, nothing is selected, so all responses are shown.



5. Filter results by requests that were warned or accessed after a warning.



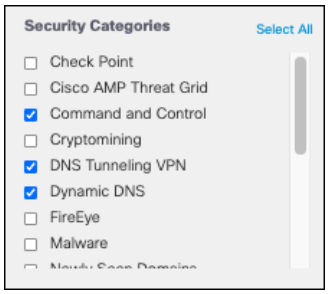
6. Filter by specific identity types and click **Apply**.



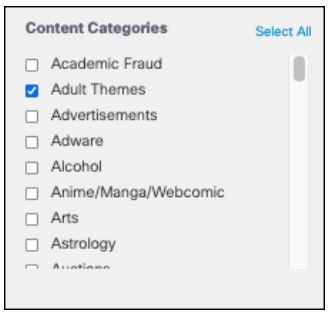
Alternatively, if you are looking for a specific identity to filter your results, enter it in the search bar. You can also filter by a specific domain.



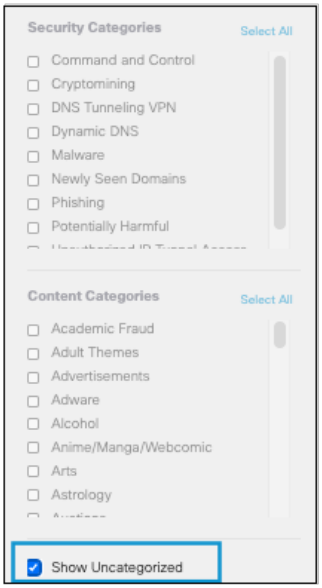
7. Filter by specific security categories and click **Apply**. For more information, see Threat Categories.



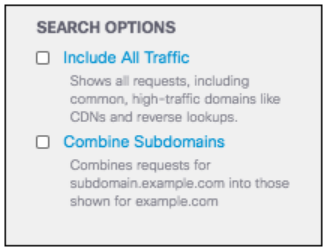
8. Filter by specific content categories and click **Apply**. For more information about content categories, see Manage Content Categories.



Alternatively, selecting **Show Uncategorized** deselects all security and content categories and only displays requests not matching any category.



9. Choose to optionally filter results by search options.
   - **Include All Traffic**–Includes data from all domains including noisy domains filtered out by default.
   - **Combine Subdomains**–Combines all subdomain requests from a parent domain and lists the combined requests under the parent domain.



Once you have chosen applicable filters, the report updates to reflect the data narrowed by those filters.



View Further Details

Describes viewing further details. Clicking any destination in the report table redirects you to the Destination Details for that domain.

Clicking any destination in the report table redirects you to the Destination Details for that domain.

Destination Details

Describes destination details. The Destination Details report provides access to information about the destinations that your identities are visiting, determining which are the most actively requested and when this activity occurs. Here you can explore activity at the domain level, determining who has visited the selected domain and when.

The Destination Details report provides access to information about the destinations that your identities are visiting, determining which are the most actively requested and when this activity occurs. Here you can explore activity at the domain level, determining who has visited the selected domain and when. This detailed information can help you determine if any computer or networks may be compromised or are connecting to known malicious sites so that you can better protect yourself and others.

View the Destination Details

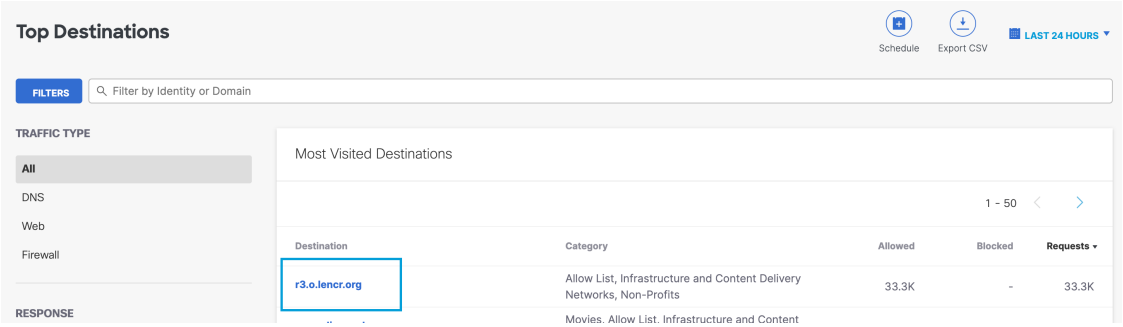
Provides instructions for viewing the destination details. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports Top Destinations and click a Destination

Before you begin

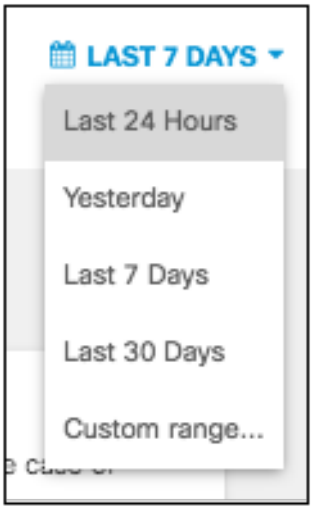
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Top Destinations** and click a **Destination**

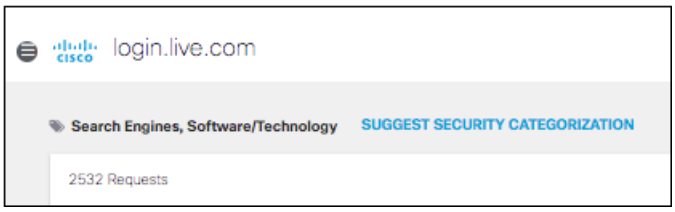


2. Choose a time frame within which data is displayed.

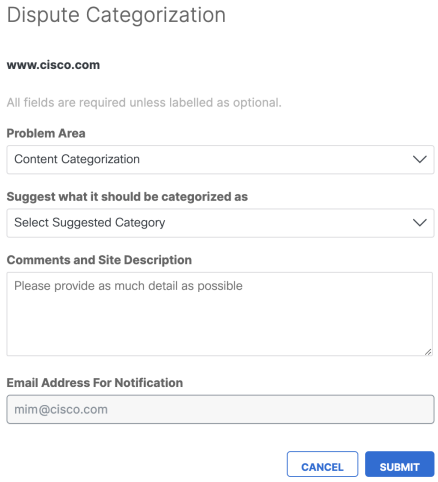


3. View the destination's content and threat categories.

   At the top of the report, under the domain for the destination you are viewing, are any categories associated with the destination. For category definitions, see Manage Content Categories and Manage Threat Categories.



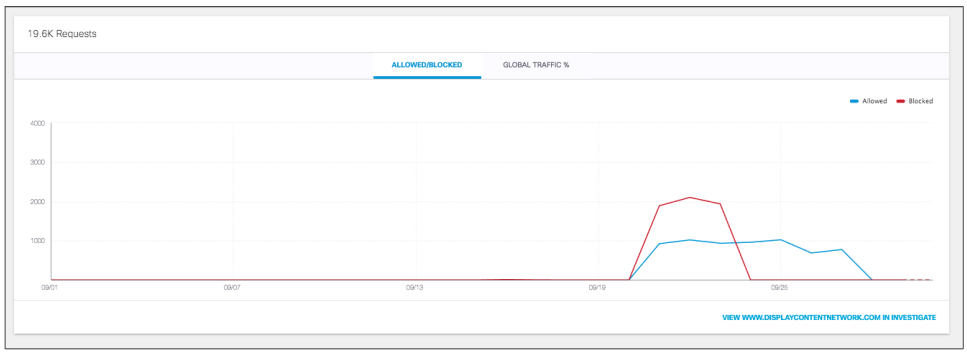
   If you believe this destination belongs in a security category, click **Suggest Security Categorization**, fill out the request form that creates an internal Secure Access ticket for a security researcher to review, and click **Submit**.



View the Request Traffic

Describes viewing the request traffic. The traffic graph displays the traffic for the type selected (blocked, allowed, or both) within the selected time period. This enables you to visualize when there are more active requests for this destination and if these requests are allowed or blocked.

The traffic graph displays the traffic for the type selected (blocked, allowed, or both) within the selected time period. This enables you to visualize when there are more active requests for this destination and if these requests are allowed or blocked.



View Requests by Blocked or Allowed

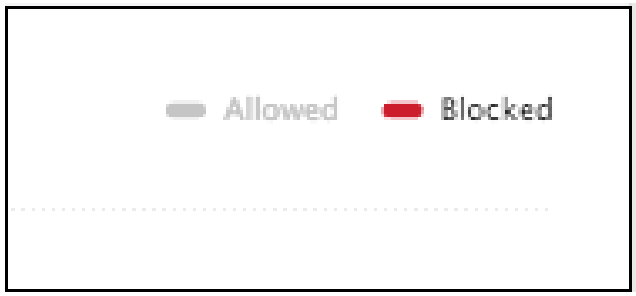
Provides instructions for viewing requests by blocked or allowed. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

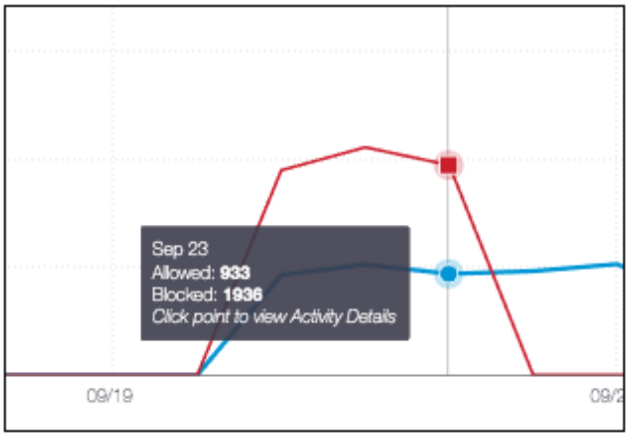
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click on **Allowed**, **Blocked**, or both to view those requests in the traffic graph. The graph displays the number of blocked and allowed requests for the destination that you are viewing within the selected time period. You can choose to see both Allowed and Blocked requests or one or the other individually. By default, only Allowed are shown initially.



2. Hover over a point on the graph to reveal the date and time and the number of Blocked and Allowed requests at that point. Clicking the point will redirect you to the Activity Search Report filtered by this domain and the Response (Blocked or Allowed) selected.



View Requests Through Global Traffic %

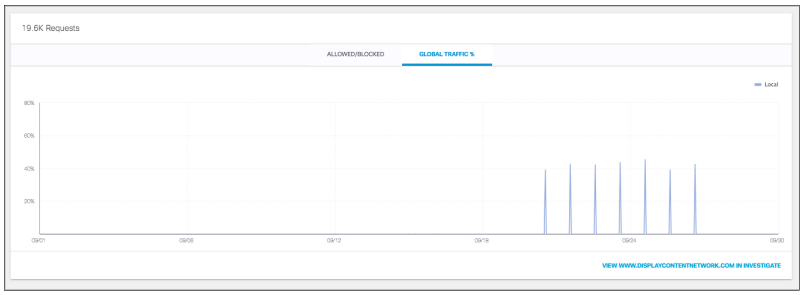
Provides instructions for viewing requests through global traffic %. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

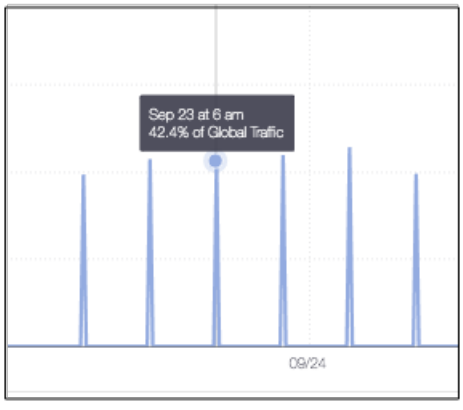
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click **Global Traffic %** on the traffic graph. The Global Traffic % chart displays the percentage of global traffic to this specific destination that is comprised of local traffic from your organization's Identities.



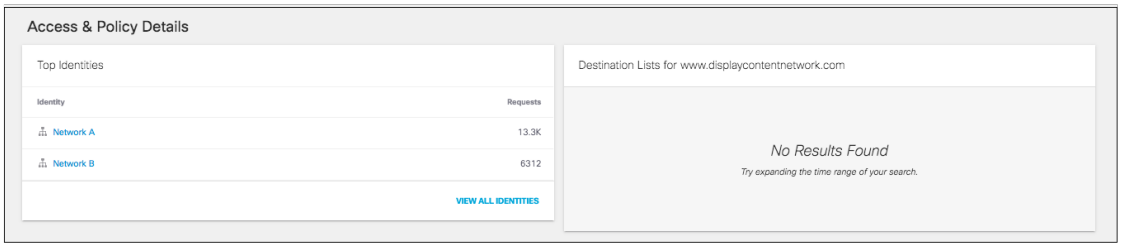
2. Hover on a point to view the date, time, and percentage of global traffic at that time.



View the Access and Policy Details

Provides instructions for viewing the access and policy details. The Access and Policy Details presents information related to identities accessing the destination and if the destination belongs to any Destination List policies.

The Access and Policy Details presents information related to identities accessing the destination and if the destination belongs to any Destination List policies.



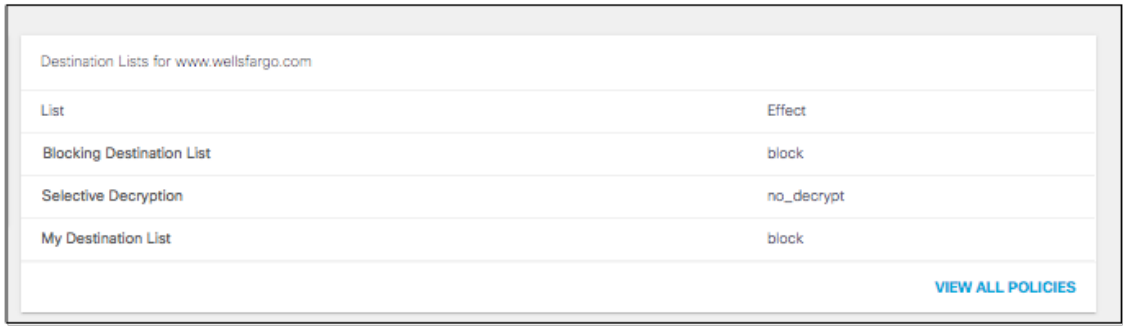
Procedure

1. Navigate to the **Access & Policy Details** > **Top Identities**.

   The Top Identities lists the sources that had the most requests for access to this destination.

2. Navigate to the **Access & Policy Details** > **Destination Lists**.

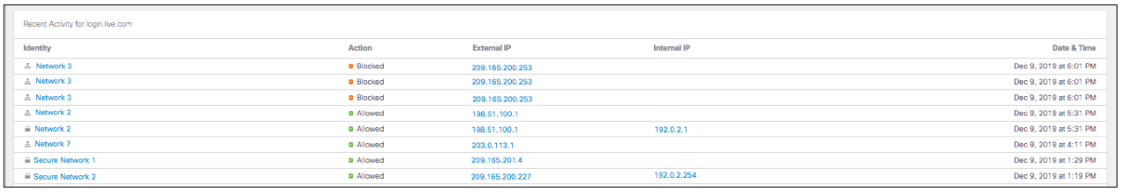
   The Destination Lists table shows if this domain belongs to any Destination Lists in your rules and what effect that list would have on the domain.



View Recent Activity

Describes viewing recent activity. The Recent Activity chart lets you investigate DNS activity for this destination. You can view the identities that requested the destination, the action (response) to that request (Blocked or Allowed), the external and internal IP addresses, and the date and time of the request.

The Recent Activity chart lets you investigate DNS activity for this destination. You can view the identities that requested the destination, the action (response) to that request (Blocked or Allowed), the external and internal IP addresses, and the date and time of the request. Viewing this information enables you to make decisions about how to best maintain your destination lists. Click **View All Activity** to open the Activity Search Report filtered by this domain.



View the Most Visited URL Paths

Describes viewing the most visited url paths. This chart lists the most frequently visited URL paths for this domain and the number of requests for each path within the requested time period.

This chart lists the most frequently visited URL paths for this domain and the number of requests for each path within the requested time period.



Most Visited URL Paths

Url Path	Requests
/RST2.srf	132
/	81
/oauth20_logout.srf	3
/oauth20_authorize.srf	3
/oauth20_desktop.srf	3
/login.srf	2
/me.srf	2

81 Top Categories Report

Topics:

- Top Categories Report

Describes the purpose and procedures for top categories report and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Top Categories Report

Describes top categories report. The Top Categories report is a list of the top security and content categories by DNS and firewall requests for your organization over the selected period.Packages and Feature AvailabilityNot all features described here are available to all Secure Access packages.

The Top Categories report is a list of the top security and content categories by DNS and firewall requests for your organization over the selected period.

> **Note**
>
> Packages and Feature Availability
>
> Not all features described here are available to all Secure Access packages. For more information, see Determine Your Current Package. If you encounter a feature described here that you do not have access to, contact your sales representative for more information.

View the Top Categories Report

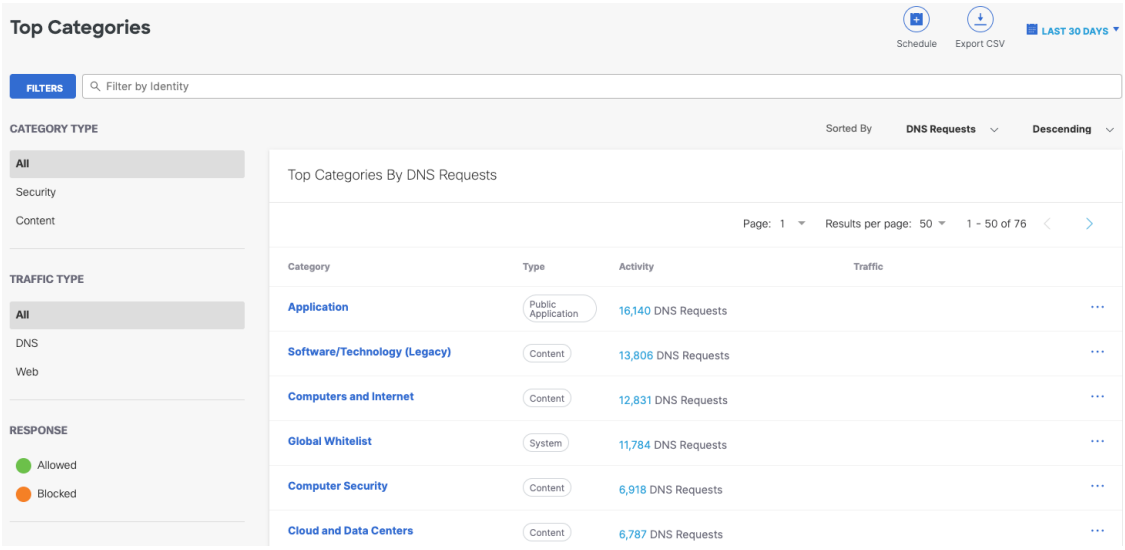
Provides instructions for viewing the top categories report. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

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

Procedure

Navigate to **Monitor** > **Reports** > **Top Categories**.



Report Fields

Provides instructions for report fields. A minimum user role of Read-only. For more information, see Manage Accounts. Category–The threat or content category item. Clicking a category name redirects you to the Category Details section. Type–The type of category: security, content, or application.

Before you begin

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

- **Category**–The threat or content category item. Clicking a category name redirects you to the Category Details section.
- **Type**–The type of category: security, content, or application.
- **Traffic**–The total bandwidth of proxy requests uploaded and downloaded for this category.
- **Activity**–The number of requests for the category for the selected period. Clicking the number of requests reveals more information:

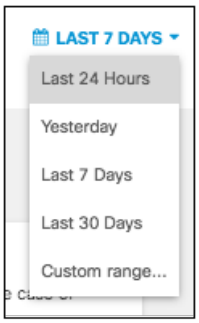
  The total requests for the selected period.

  which of the requests were blocked and which were allowed

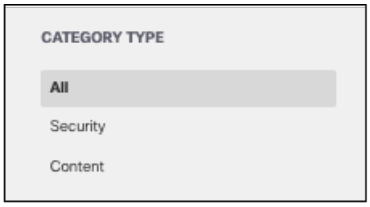
  The most active identities (the identities that have requested the category the most).

Procedure

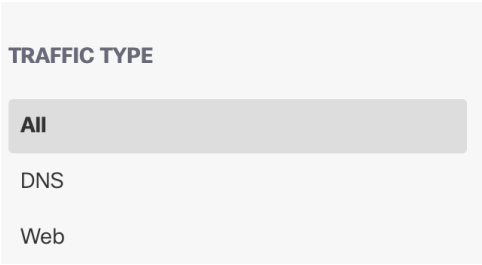
1. Choose a time frame within which to view the result. You can view the report for the last 24 hours, the previous day (yesterday), last week, the last 30 days, or a custom range within the last 30 days.



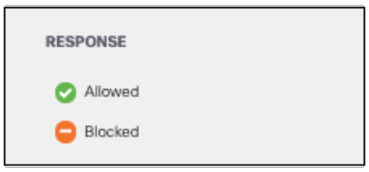
2. Filter the top categories by category type. You can view Security categories, Content categories, or both. By default, **All** is selected, so that both security and content categories are shown.



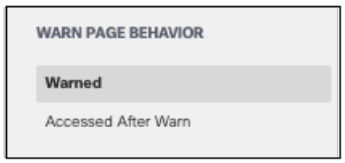
3. Filter top categories by traffic type. You can filter by DNS, Web, or both (All).



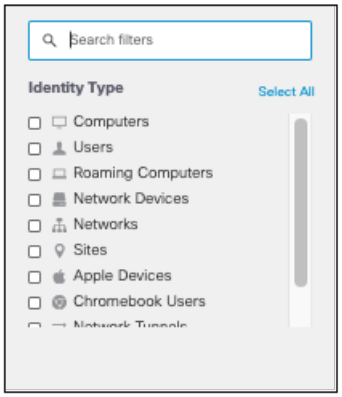
4. Filter top categories by response type. You can view categories from requests that were Allowed, Blocked, or both. By default, neither is selected, so all responses are shown.



5. Filter requests that were warned or accessed after a warn.



6. Choose identity types to filter results and click **Apply**. By default, no identity types are selected, so all identity types are shown.



You also have the option to search by identity if you know the identity name.



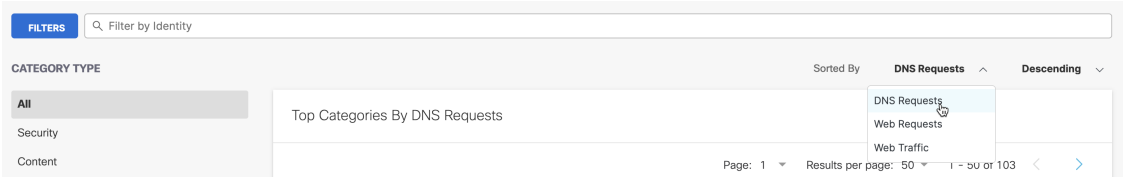
7. Choose how to sort the top category results.

Sort by Traffic

Describes sort by traffic. DNS Requests–Show DNS requests first. Web Requests–Show Web requests first. Web Traffic–Show Web traffic first.

- **DNS Requests**–Show DNS requests first.

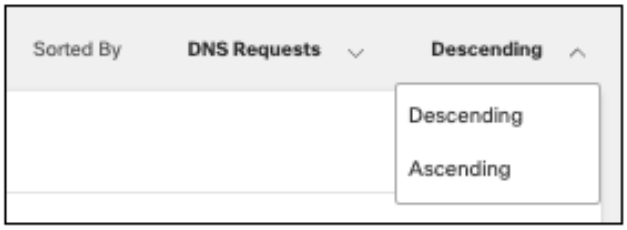
- **Web Requests**–Show Web requests first.
- **Web Traffic**–Show Web traffic first.



Ascending or Descending Order

Describes ascending or descending order. Descending–Show the results in descending order. By default, descending is selected. Ascending–Show the results in ascending order. The Top Cat Sort Ascenddescend interface.

- **Descending**–Show the results in descending order. By default, descending is selected.
- **Ascending**–Show the results in ascending order.



Once you have chosen all filters and sorting options, the report will reflect the appropriate results.

Top Categories Quick View

Provides instructions for top categories quick view. The quick view for Top Categories displays the most active identities and their respective requests for each individual category.

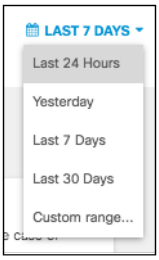
The quick view for Top Categories displays the most active identities and their respective requests for each individual category.

Before you begin

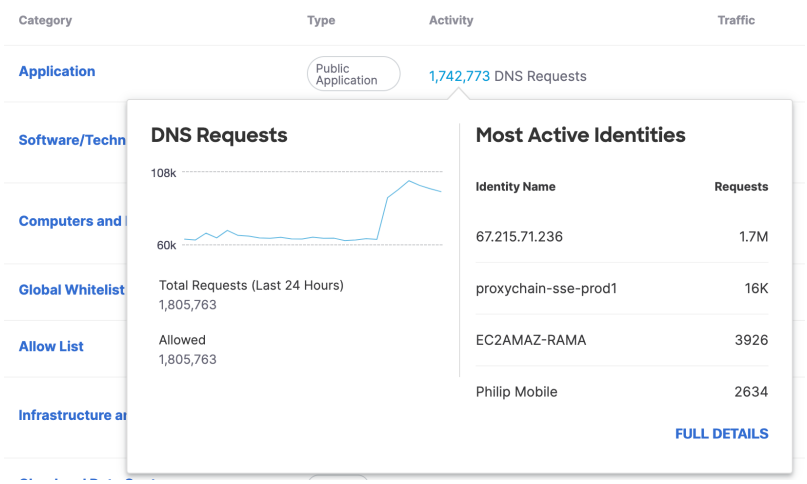
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Choose a time frame within which to view the quick view details. You can see details for the last 24 hours, the previous calendar day (yesterday), the last 7 days, the last 30 days, or a custom range within the last 30 days.



2. Click the number of requests (DNS or Web) in the **Activity** column of the category you wish to examine. A modal appears with a graph displaying the total requests of that traffic type over the selected time period and the total number of allowed requests. The most active identities with requests in this category are also displayed.



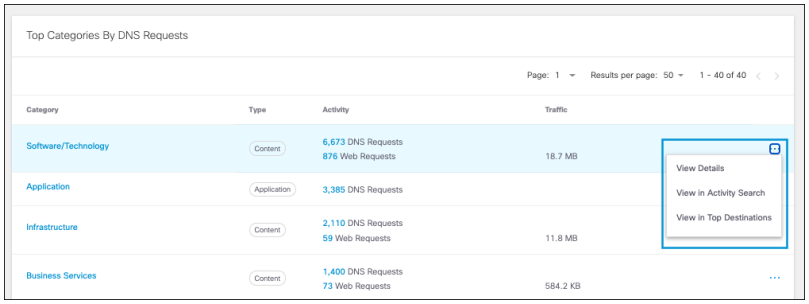
3. Optionally, click **Full Details** to open the Category Details for this category.

View Category in Other Reports

Describes viewing category in other reports. Viewing the category in other reports provides you with insights into how your organization accesses a destination category and what activities are involved. In the Top Categories report, each category can be explored further by accessing the View Menu.

Viewing the category in other reports provides you with insights into how your organization accesses a destination category and what activities are involved. In the Top Categories report, each category can be explored further by accessing the View Menu. Clicking this menu (the "...") reveals three options:

- **View Details** – Redirects you to that category's details.
- **View in Activity Search** –Redirects you to the Activity Search report filtered by that category.
- **View in Top Destinations** –Redirects you to the Top Destinations report filtered by this category.



Category Details

Describes category details. The Category Details for an individual category provide you with a focused view of the category's traffic and related sources and domains for a selected time period.

The Category Details for an individual category provide you with a focused view of the category's traffic and related sources and domains for a selected time period.

View a Category's Details Overview

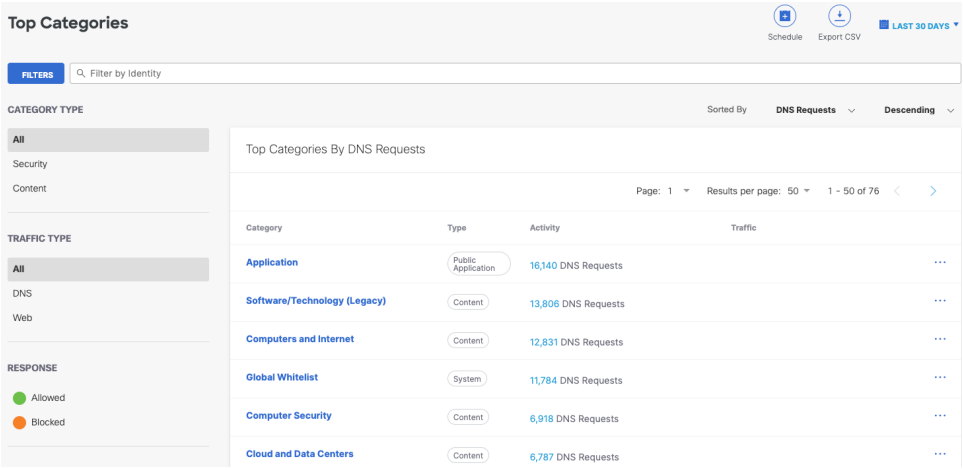
Provides instructions for viewing a category's details overview. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

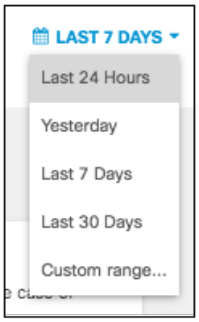
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Top Categories** and click one of the listed categories.



2. Choose a time period within which to view the results. The details can be filtered by the last 24 hours, the previous calendar day (yesterday), the last seven days, the last 30 days, or a custom range within the last 30 days.



View a Category's Traffic

Describes viewing a category's traffic. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

The first graph depicts the traffic over a selected time period for this category.

View the Activity Breakdown

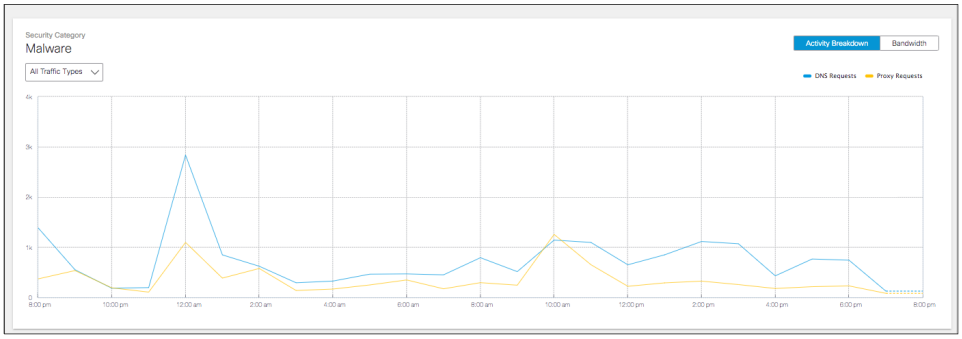
Provides instructions for viewing the activity breakdown. A minimum user role of Read-only. For more information, see Manage Accounts. Click a category and navigate to the traffic graph on the details page. Select Activity Breakdown.

Before you begin

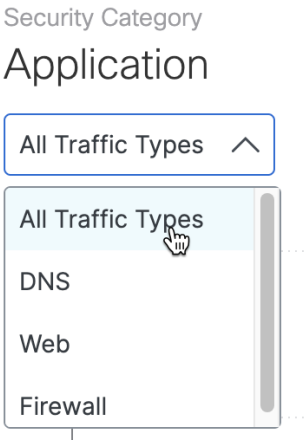
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

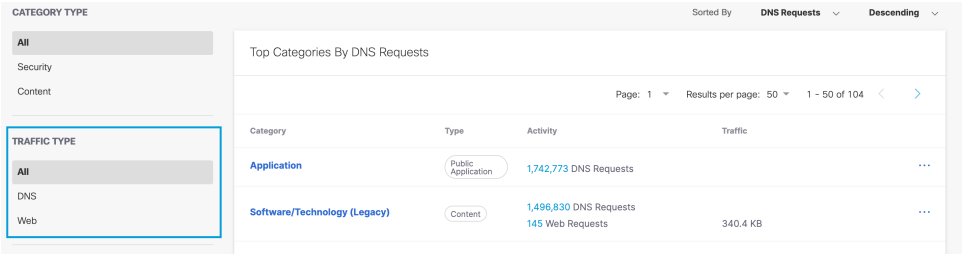
1. Click a category and navigate to the traffic graph on the details page. Select **Activity Breakdown**. The Activity Breakdown displays the number of DNS requests and proxy transactions for the selected time period.



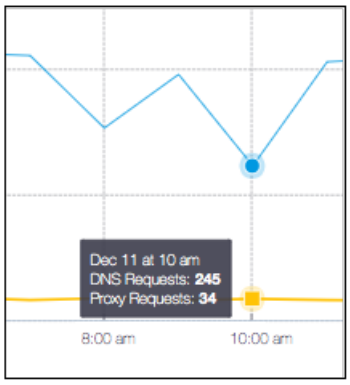
2. Filter the Activity Breakdown to view All Traffic Types (default), DNS, Web, or Firewall.



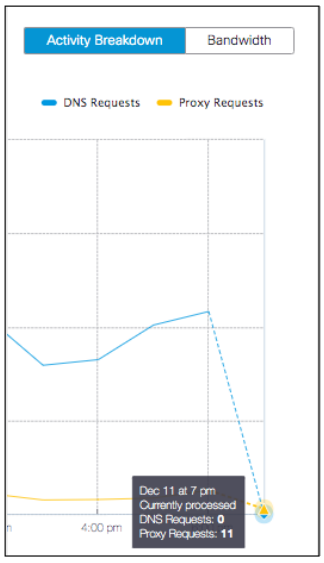
You can also choose the traffic type to filter before redirecting to the category details from the Top Category report. IP requests are not an option in Category Details.



3. Hover over a date and time to reveal details about the requests made at that time.



The dotted line provides available data that is still being processed. Hover over the point on the graph to see how many requests are currently processed.



View the Traffic Bandwidth

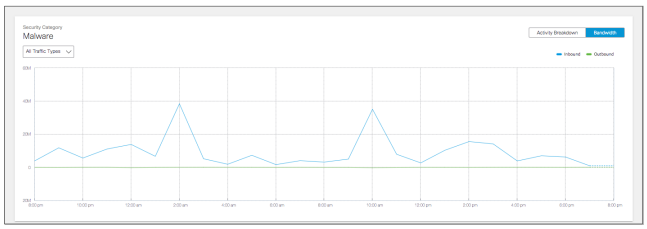
Provides instructions for viewing the traffic bandwidth. A minimum user role of Read-only. For more information, see Manage Accounts. Click a category and navigate to the traffic graph on the details page. Select Bandwidth.

Before you begin

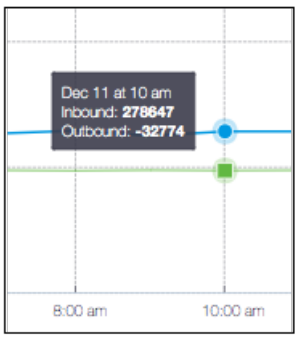
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

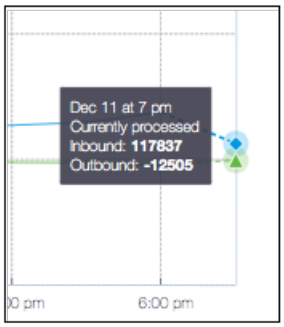
1. Click a category and navigate to the traffic graph on the details page. Select **Bandwidth**. For proxy transactions, the bandwidth view of the line graph shows the number of inbound and outbound traffic for the selected time period.



2. Hover over a specific date and time to reveal details about the traffic at that time.



The dotted line provides available data that is still being processed. Hover over the point along the graph to see the inbound and outbound traffic details currently processed.



View a Category's Identities

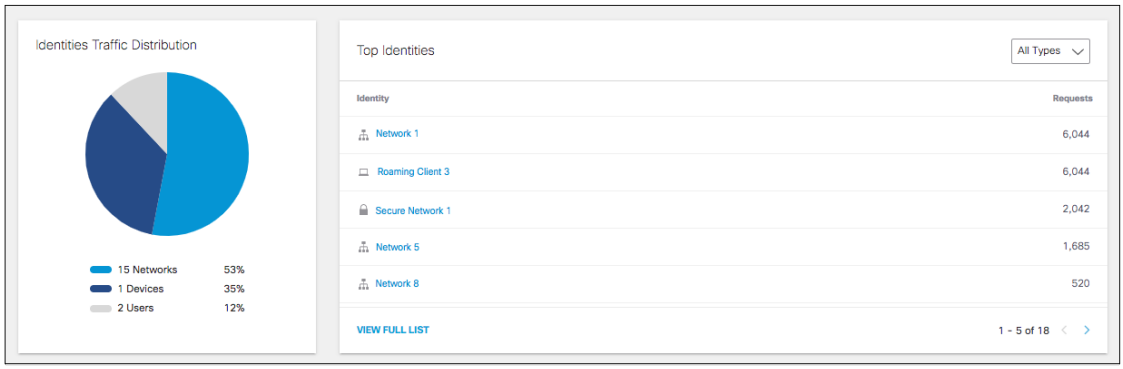
Provides instructions for viewing a category's identities. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to the identities section of the report.

Before you begin

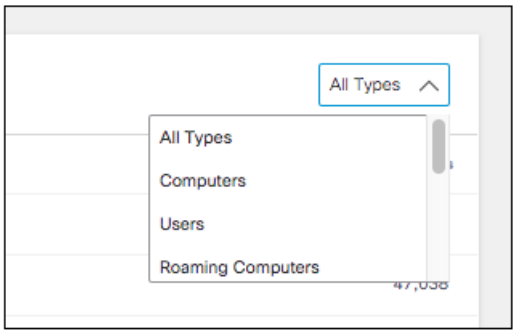
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to the identities section of the report.
2. View the Identities Traffic Distribution. The pie chart provides a breakdown of the identity types that have made requests for the category for the selected time period.
3. View the top identities making requests associated with this category.
   - **Identity**–The name of the identity.
   - **Requests**–The number of category requests the identity has made during the selected period.



You can filter which identity types are listed by selecting an identity type from the drop-down.



View the Category's Top Domains

Provides instructions for viewing the category's top domains. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

Navigate to the **Top Domains** section of the report. This list depicts the top domains where requests were flagged for this category:

- **Domain Name**–The domain name, such as example.com.
- **Other Categories**–If there are other categories associated with the domain in addition to the current category being viewed, they are listed here.
- **Allowed**–The number of requests allowed for this domain for the selected time period.
- **Blocked**–The number of requests blocked for this domain for the selected time period.
- **Requests**–The number of requests made for this domain for the selected period.



Click a domain to open the Destination Details. Click **View Full List** to open the Top Destinations Report filtered by this category.

82 Cloud Malware Report

Topics:

- Cloud Malware Report

Describes the purpose and procedures for cloud malware report and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Cloud Malware Report

Describes cloud malware report. The Cloud Malware Report provides an overview of malicious files within your environment and details the potential risk and exposure these files present. For setup instructions, see Enable Cloud Malware Protection.

The Cloud Malware Report provides an overview of malicious files within your environment and details the potential risk and exposure these files present. For setup instructions, see Enable Cloud Malware Protection.

View the Cloud Malware Report

Provides instructions for viewing the cloud malware report. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

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

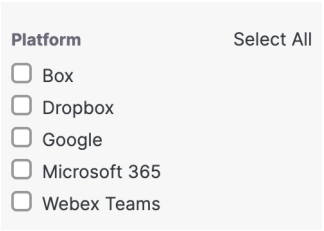
Procedure

1. Navigate to **Monitor** > **Reports** > **Cloud Malware**.

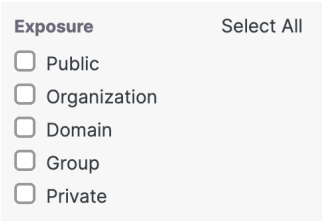


2. View the report's overview of information about the malicious files in your organization.
   - **Total files scanned**–The total number of files in the organization scanned for potential malware. This will also show a status as to whether the scan is complete or in progress.
   - **Platforms**–The platforms where malicious files were found.
   - **Malware found**–The total number of files found deemed malicious.
   - **Users with malware**–The number of users in your environment whose files contain malware.

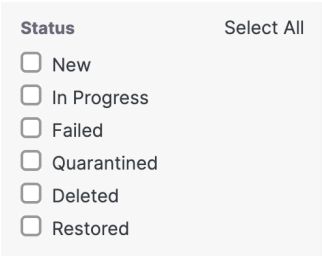
3. Filter by platform. The platforms available for Cloud Malware are Box, Dropbox, Google, Microsoft Office 365 (both OneDrive and SharePoint), and Webex Teams. You can filter your malicious files' results by selecting any or all of the platforms listed.



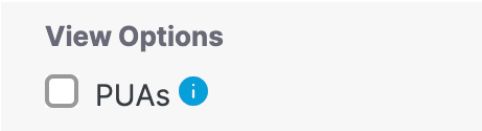
4. Filter by exposure. You can filter your malicious files by the type of exposure they pose to the environment. By default, none are selected, so all exposure types are presented.



5. Filter by status. Each file displays a status depending on whether it is newly discovered, a quarantine is in progress or failed, or that the file was successfully quarantined or deleted.



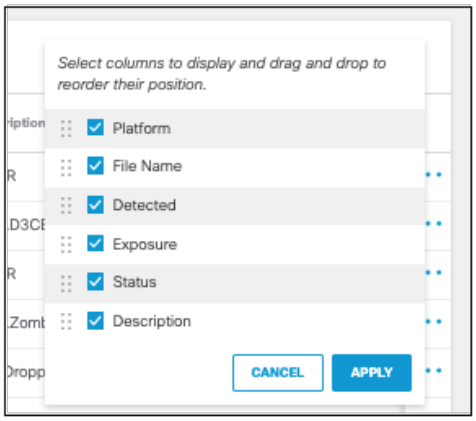
6. Optionally, you can choose to view suspect Potential Unwanted Applications.



7. Sort columns by detection or status.



Click the settings menu icon to select which columns to display and organize them as you choose.



Use the Cloud Malware Report

Describes using the cloud malware report. It also identifies related requirements, procedures, and operational considerations. It also identifies related requirements and procedures for Secure Access administrators.

Quarantine a Malicious File

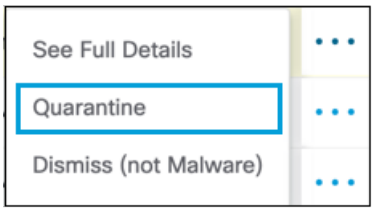
Provides instructions for quarantine a malicious file. On the Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive, when a malicious file presents a potential risk and needs remediation, you can manually quarantine the file. Only the integration user for the platform will have access to the quarantined files.

On the Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive, when a malicious file presents a potential risk and needs remediation, you can manually quarantine the file. Only the integration user for the platform will have access to the quarantined files.

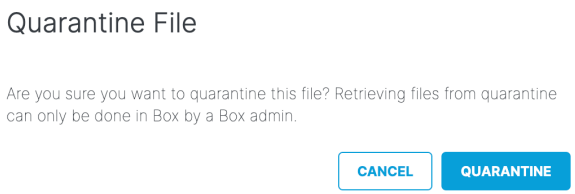
Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click the Action Menu to the right of the file that needs to be quarantined, then select **Quarantine**.



2. A modal appears to verify if this is the file to be quarantined. Click **Quarantine**. The status will update in the report to *Quarantine in Progress* while the quarantine is processing. This process can take up to five minutes; when complete, the status will update to **Quarantined**.



Note

- For Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive:
  - The file identified as exposing sensitive data is moved to the Cisco_Quarantine/DLP folder Secure Access created in the root path of the Global Admin who authorized the tenant.
  - The user who authorizes access to Secure Access will have access to the quarantine folder. All other accesses and collaborators are removed. Thus, we recommend that the admin add the relevant DLP Admins as additional collaborators to the folder.

What to do next

- Quarantine attempts may fail if the files have been locked or blocked by settings within their native platforms. Settings local to the platform where a file resides take precedence over Secure Access' ability to detect or remediate DLP violations or malware.

Restore a Quarantined File

Provides instructions for restore a quarantined file. On the Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive platforms, you can restore a file that has previously been quarantined.

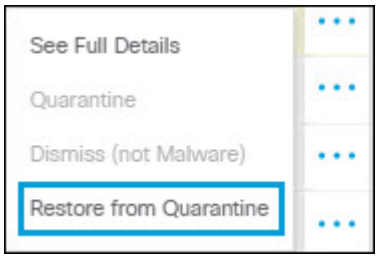
On the Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive platforms, you can restore a file that has previously been quarantined.

> **Note**
>
> Once a file has been quarantined and then restored, it cannot be quarantined again.

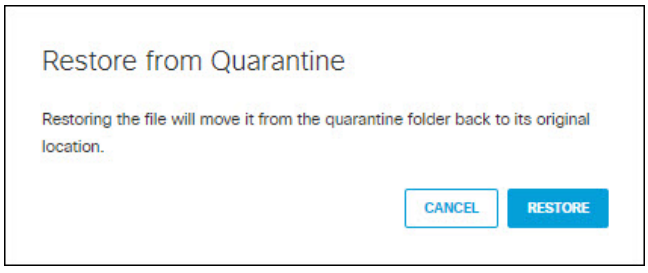
Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click the Action Menu to the right of the file that needs to be quarantined, then select **Restore from Quarantine**.



2. A dialog box appears to verify the file is to be restored. Click **RESTORE**. The status will update to **Restoration in Progress** while the file is being processed. This can take up to five minutes; when complete, the status will update to **Restored**.



> **Note**
>
> If your Cloud Malware deployment processes files from Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive and you restore a quarantined file that still violates rule criteria, the system will quarantine that file again. To prevent the system from quarantining the file again, remove the file's violation, or update the rule's criteria.

Delete a Malicious File

Provides instructions for deleting a malicious file. For the Webex Teams platform, when a malicious file presents a potential risk and needs remediation, you can delete the file.

For the Webex Teams platform, when a malicious file presents a potential risk and needs remediation, you can delete the file.

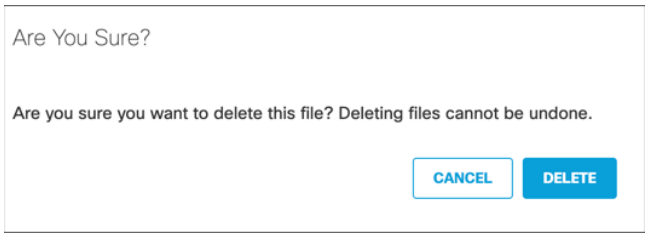
Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click the Action Menu for the file that needs to be quarantined and choose **Delete**.



2. A modal appears to verify if this is the file to be deleted. Click **Delete**. The report status is updated to *Deleted*.



Dismiss an Item from the Report

Provides instructions for dismiss an item from the report. When a reported file is found to not present a risk, you can dismiss the file from the report.

When a reported file is found to not present a risk, you can dismiss the file from the report.

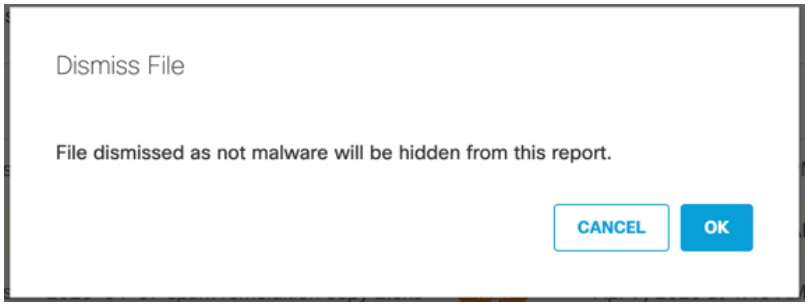
Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click the Action Menu for the file that needs to be removed from the report and choose **Dismiss**.



2. A modal appears to verify if this is the file to be dismissed. Click **OK**. The file is removed from the report.



Export a Cloud Malware Report

Provides instructions for exporting a cloud malware report. You can export your Cloud Malware report to a CSV file for your records.

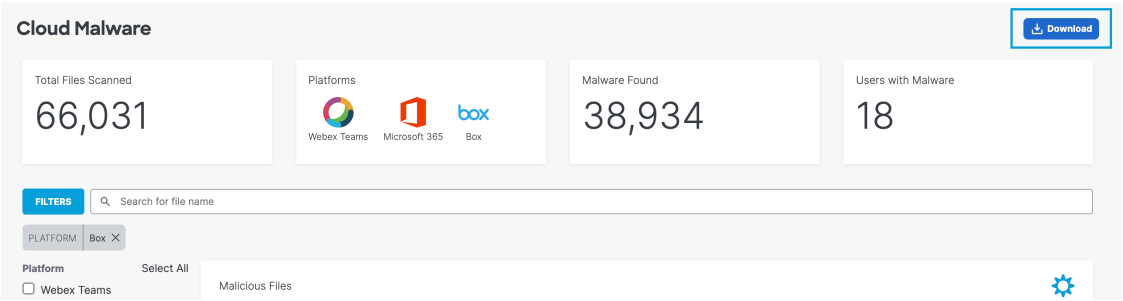
You can export your Cloud Malware report to a CSV file for your records.

Before you begin

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

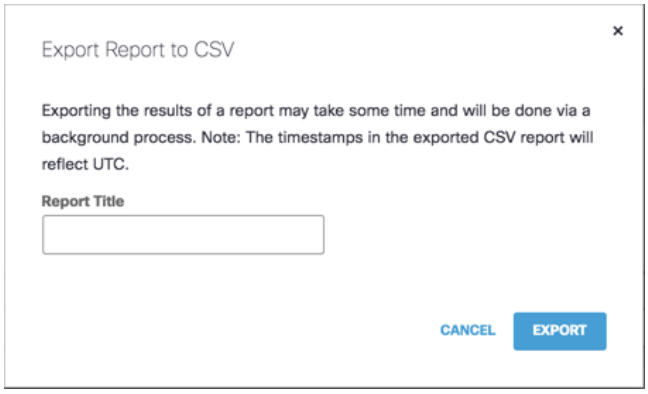
Procedure

1. Click **Download**.



2. Give your report a title and click **Export**.

> **Note**
>
> Data is limited to 1,000,000 rows when exporting to CSV.



3. When you click **Export**, you are taken to the Exported Reports page. Click the download icon in the download column to download the CSV file.

83 Data Loss Prevention Report

Topics:

- Data Loss Prevention Report

Describes the purpose and procedures for data loss prevention report and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Data Loss Prevention Report

Describes data loss prevention report. Data violations detected through the Real Time and SaaS API rules are logged as part of the unified Events view of the Data Loss Prevention Report.

Data violations detected through the Real Time and SaaS API rules are logged as part of the unified Events view of the Data Loss Prevention Report.

The Data Loss Prevention reports window includes these tabs:

- Events
- View a Discovery Scan on page 1104

> **Note**
>
> Administrators with De-identification enabled will continue to see identifiable information in the Data Loss Prevention Report.

View Events

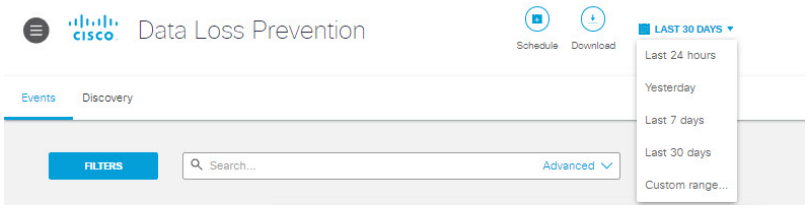
Provides instructions for viewing events. A minimum user role of Read-only. For more information, see Manage Accounts. Navigate to Monitor Reports Data Loss Prevention .

Before you begin

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

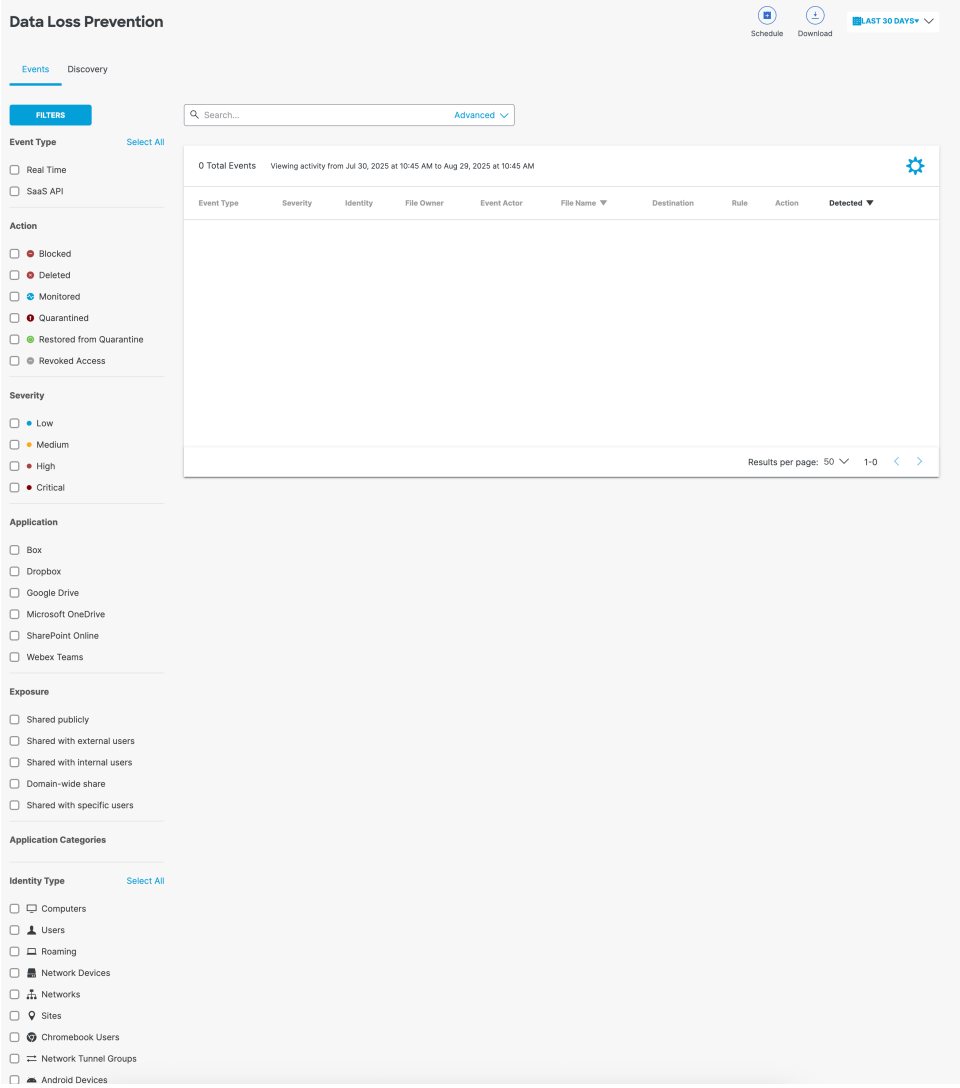
Procedure

1. Navigate to **Monitor** > **Reports** > **Data Loss Prevention**.
2. On the **Events** tab, select a time frame to view reports generated in a specific date range. You can also choose a custom date range.



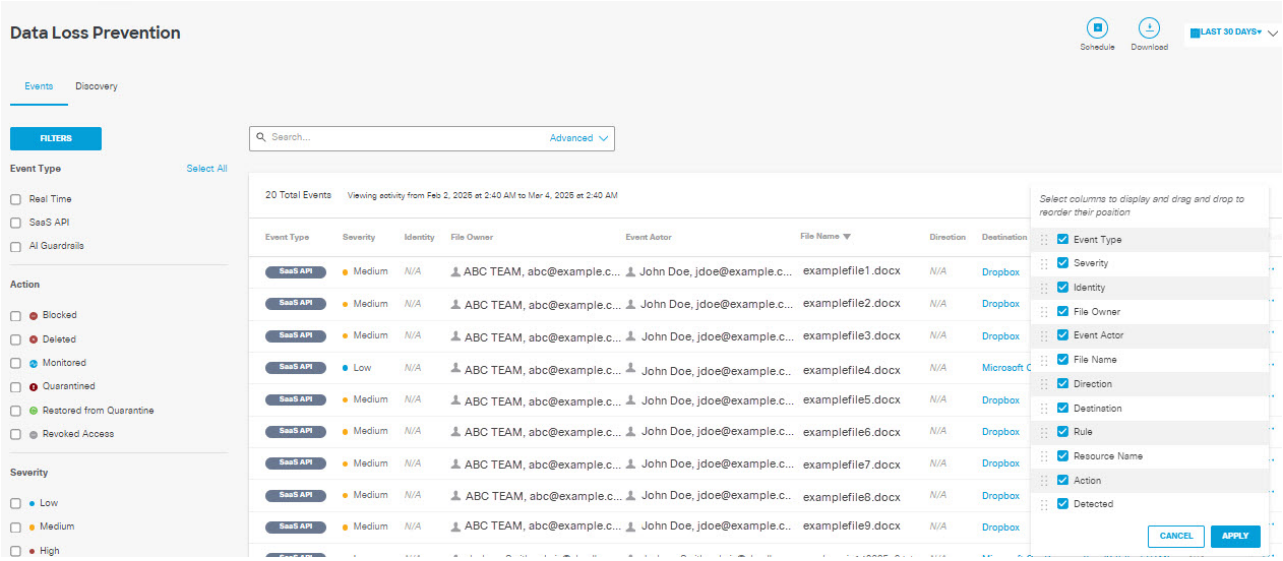
3. Use the available **Filters** for better search results; choose from those listed below:
   - **File Size**–Indicates the size of the file that triggered the event.
   - **Event Type**–Indicates the type of rule that triggered the event: Real Time (for private or internet resources) or SaaS API.
   - **Action**–The action the system has applied to the content: blocked, deleted, monitored, quarantined, restored from quarantine, revoked access.
   - **Severity**–The severity of the rule that triggered the event.
   - **Application**–Application for which an SaaS API rule is applied.
   - **Exposure**–Exposure of the content scanned.

- **Identity Type**–The type of identity involved in the event.
- **Application Categories**– The category of the application involved in the event. This filter displays only events that occurred after this filter was added to Secure Access, in January of 2024.



4. Click the gear icon to customize and sort the columns of your report.
   - **Event Type**– Indicates the type of rule that triggered the event: Real Time or SaaS API.
   - **Severity**–The severity of the rule that triggered the event.
   - **Identity** –The identity that made the request.
   - **File Owner**–The owner of the file that created the violation in the vendor.
   - **Event Actor**– The user who performs an action that triggers a rule violation.
   - **File Name**–The name of the file or attachment where a classification match was found. (This includes attachments to Outlook email messages.) When content is found in a message, a post, or form data, the File name displays *Message*, *Content*, or *Form*.
   - **Destination**–The destination where the content was scanned.
   - **Rule**–The rule that triggered the event.

- **Resource Name**–For AWS S3 this displays the S3 bucket associated with the content that triggered the violation. For Azure Storage this displays the storage account or container associated with the content that triggered the violation. For other applications, this displays "N/A."
- **Action**–The action triggered by the rule on detecting a violation.
- **Detected**–The date and time of detection.



5. Click the action menu icon (three dots) to view further details of an event. See View Details

---

View Details

Provides instructions for viewing details. A minimum user role of Read-only. For more information, see Manage Accounts. Click the action menu icon (three dots) for any event to view a menu of options. Click View details.

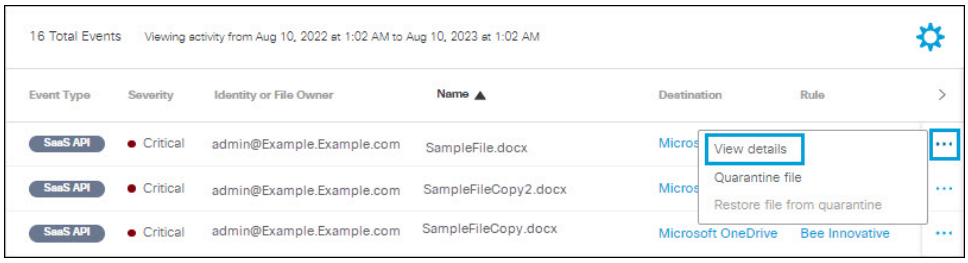
Before you begin

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

Procedure

---

1. Click the action menu icon (three dots) for any event to view a menu of options. Click **View details**.

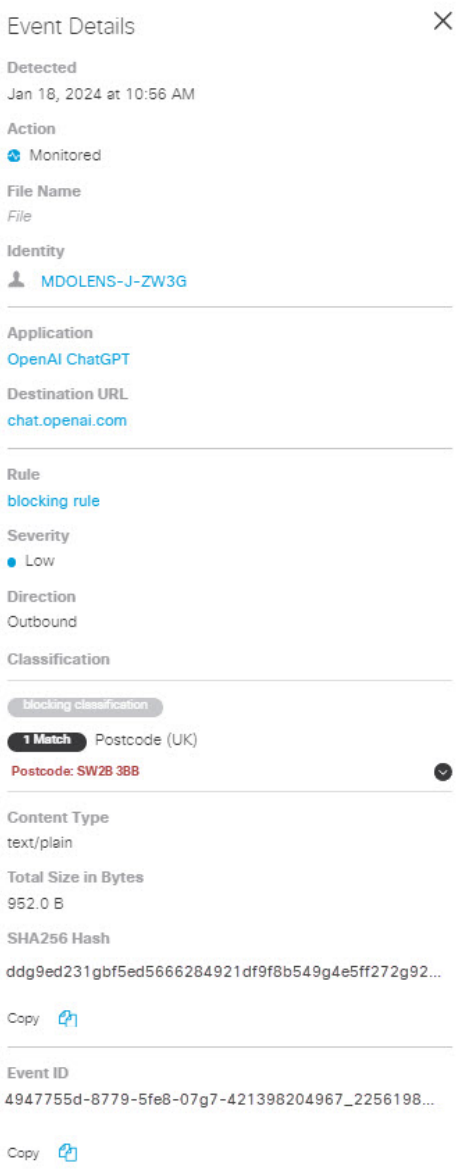


2. The Event Details window displays some of the same content as the report table, with additional information which varies depending upon the Event Type:

   Real Time Events

   - **Detected**–The date and time the content was detected.
   - **Action**–The action triggered by the rule on detecting a violation.

- **File Name**–The name of the file where a classification match was found. When content is found in a message or a post, the File name displays *Content*.
- **Identity**–The identity that made the request.
- **Private Resource**–The private resource where the file was uploaded or posted.
- **Private Resource Group** – The private resource group where the file was uploaded or posted.
- **Destination URL**– For private resources or private resource groups, the URL where the file was uploaded or posted.
- **Destination Port**– For private resources or private resource groups, the port where the file was uploaded or posted.
- **Destination Protocol**– For private resources or private resource groups, the protocol used to upload or post the file.
- **Destination IP**– For private resources or private resource groups, the IP address where the file was uploaded to posted.
- **Application**–The application where the file was uploaded or posted.
- **Application Category**–The category for the application where the file was uploaded or posted.
- **Destination URL**–The URL of the destination for the event.
- **Rule**–The rule that triggered the event.
- **Severity**–The severity of the rule that triggered the event.
- **File Label**–File label names in the value of the file's document properties. This includes Microsoft Office Document Properties, Microsoft Office Sensitivity Labels, and AdobePDF Document Properties.
- **Direction**–Direction of traffic.
- **Classification**–The classification that matched the content found in the event. Clicking the caret will display the excerpts where the matches were found.
- **Content Type**–The type of data that triggered the event.
- **Total Size in Bytes**–The size of the file that triggered the event.
- **SHA256 Hash**–The unique SHA256 hash for the file. (You may copy this using the **Copy** icon.)
- **Event ID**–A unique identifier for the event. (You may copy this using the **Copy** icon.)



SaaS API Events

A timeline of events associated with the file.

- **Application**–The application where the file was uploaded or posted.
- **Tenant**–The Secure Access tenant associated with the event.
- **Resource ID**– The URL for the resource associated with the content that triggered the violation. For Azure S3 the resource is an S3 bucket. For Azure Storage the resource is a storage account or container. For other applications, this does not apply.
- **Resource Name**–For AWS S3 this displays the S3 bucket associated with the content that triggered the violation. For Azure Storage this displays the storage account or container associated with the content that triggered the violation. For other applications, this does not apply.
- **Destination URL**–The URL of the destination for the event.

> **Note**
>
> (For some platforms, a single file or message can trigger multiple events that show the same Destination URL for each event.)

- **File/Message Direction**–The direction of the message or file that triggered the event: **Incoming** or **Outgoing**.

> **Note**
>
> For Outlook, this will always be **Outgoing**.

- **Rule**–The rule that triggered the event.
- **Severity**–The severity of the rule that triggered the event.
- **Exposure**–An indication of who can see the file–internal or external users.
- **Classification**–The classification that matched the content found in the event. Clicking the caret will display the excerpts where the matches were found.
- **Content Type**–The type of data that triggered the event.
- **Total Size in Bytes**–The size of the file that triggered the event.
- **SHA256 Hash**–The unique SHA256 hash for the file.
- **Unique Event ID**–A unique identifier for the event.

Delete File

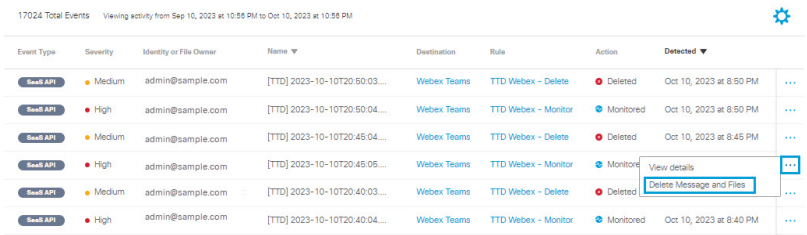
Provides instructions for deleting file. For SaaS API events on Webex Teams and Slack, when a message is monitored and a rule violation is detected, you can manually delete the message or file.

For SaaS API events on Webex Teams and Slack, when a message is monitored and a rule violation is detected, you can manually delete the message or file.

Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click the action menu (three dots) for any Webex Teams event that is not marked **Deleted** to view a menu of options. Click **Delete Message and Files**.



2. Click **Delete** to confirm.

Quarantine File

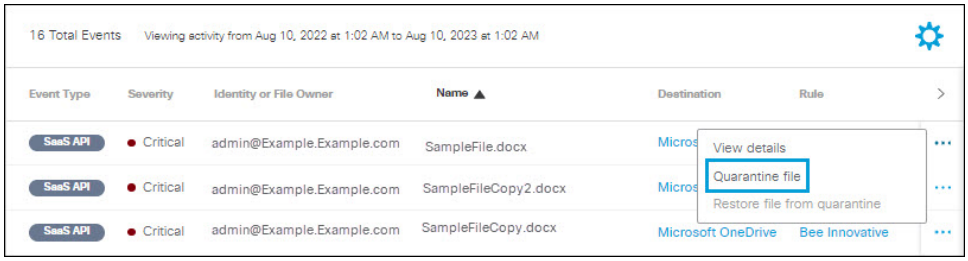
Provides instructions for quarantine file. For SaaS API events on Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive, when a file is monitored and a rule violation is detected, you can manually quarantine the file.

For SaaS API events on Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive, when a file is monitored and a rule violation is detected, you can manually quarantine the file.

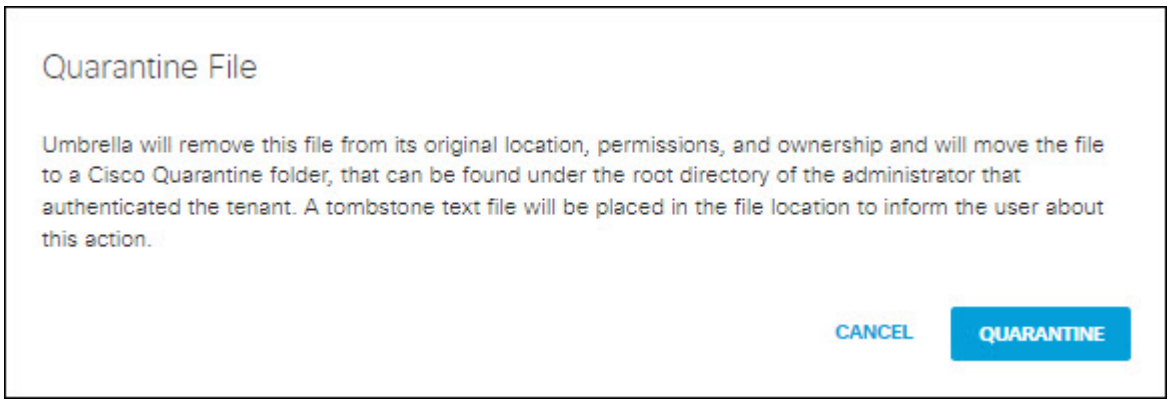
Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click the action menu icon (three dots) for any event to view a menu of options. Click **Quarantine file**.



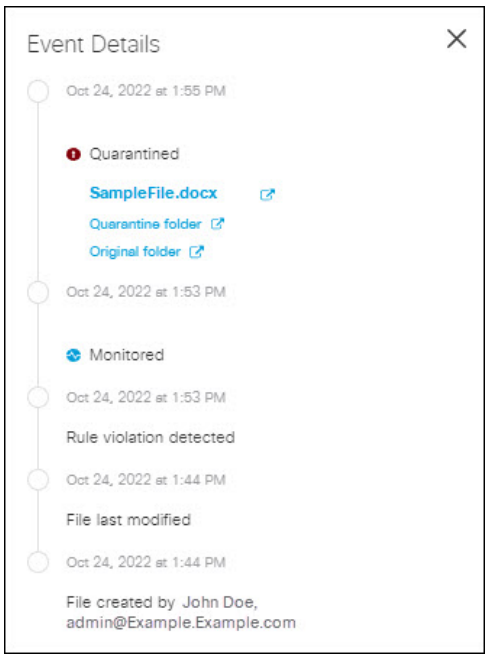
2. Click **Quarantine**.



Note

- For Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive:
  - The file identified as exposing sensitive data is moved to the Cisco_Quarantine/DLP folder Secure Access created in the root path of the Global Admin who authorised the tenant.
  - The user who authorizes access to Secure Access will have access to the quarantine folder. All other accesses and collaborators are removed. Thus, we recommend that the admin add the relevant DLP Admins as additional collaborators to the folder.
- For ServiceNow:
  - The file identified as exposing sensitive data is moved to a table named **Cisco_Quarantine_Malware** which can be access only by the admin user who authorized the ServiceNow tenant.
  - A footprint is attached to the notesactivities area of the table the file is attached to. This footprint will notify users that the file has been identified as malware, and for more information they should contact their administrator.

3. The file is now quarantined. Under Events Details, click **Quarantine Folder** to navigate to the quarantined folder.



Restore File from Quarantine

Provides instructions for restore file from quarantine. When a quarantined file is restored, the original location of the file, ownership and permissions are also restored.

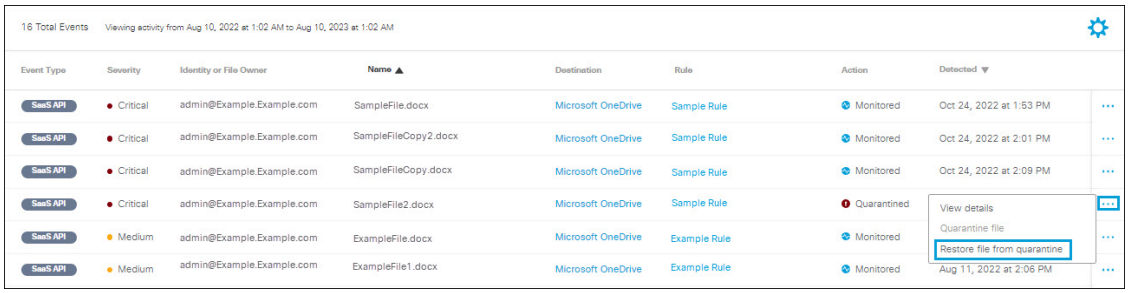
When a quarantined file is restored, the original location of the file, ownership and permissions are also restored.

Before you begin

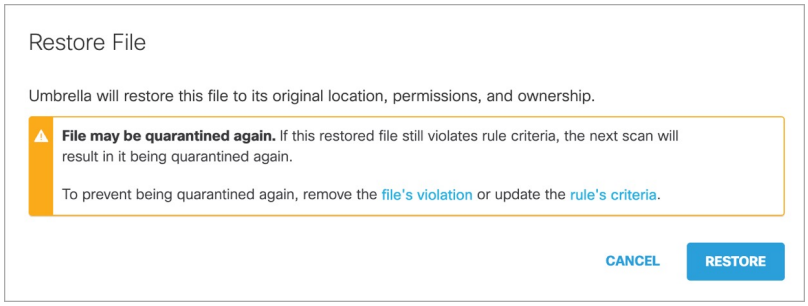
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

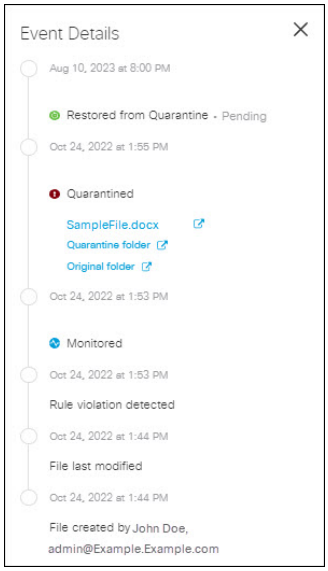
1. Click the action menu icon (three dots) for any event to view a menu of options. Click **Restore file from quarantine**.



2. Click **Restore** to proceed.



3. The file is now restored. You can access the file in its original location under **Event Details**.



Note

If your DLP rules process files from Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive and you restore a quarantined file that still violates rule criteria, the system will quarantine that file again. To prevent the system from quarantining the file again, remove the file's violation, or update the rule's criteria.

Use Advanced Search

Provides instructions for using advanced search. A minimum user role of Read-only. For more information, see Manage Accounts. You can search the Data Loss Prevention Reports by keywords to find specific events.

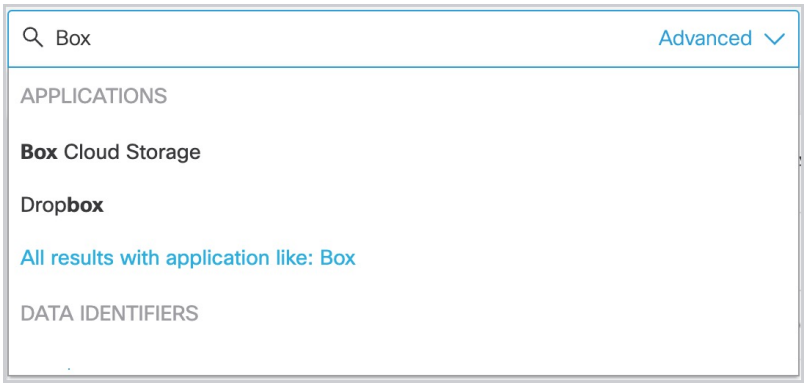
Before you begin

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

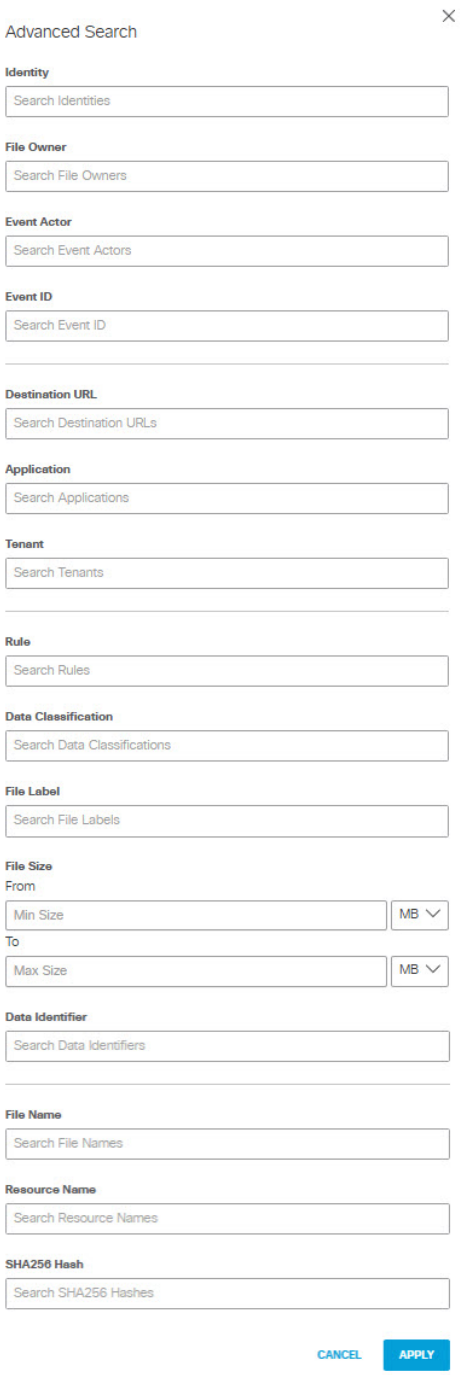
Procedure

---

1. You can search the Data Loss Prevention Reports by keywords to find specific events.



2. Alternatively, click **Advanced** in the search bar to bring up the advanced search. You can search the report choosing any of the following event criteria:
   - **Identity**
   - **File Owner**
   - **Event Actor**
   - **Event ID**
   - **Destination URL**
   - **Application**
   - **Direction** (Applies only to some applications, such as OpenAI API and OpenAI ChatGPT.)
   - **Tenant**
   - **Rule**
   - **Data Classification**
   - **File Label**
   - **File Size** (When searching for files meeting size criteria, You can choose to include only files that are greater than a minimum size you specify, or include files that are within a range of sizes you specify. (If you specify a maximum size without specifying a minimum size, the minimum size defaults to 0.) You can specify file sizes in KB or MB. The system scans only up to the first 50 MB of plain text for any file; if you specify a minimum size > 50 MB, Secure Access does not scan for other criteria.)
   - **Data Identifier**
   - **File Name**
   - **Resource Name** (applies to AWS S3 or Azure Storage tenants only)
   - **SHA256 Hash**
3. Click **Apply** to apply the filters to the report.



View a Discovery Scan

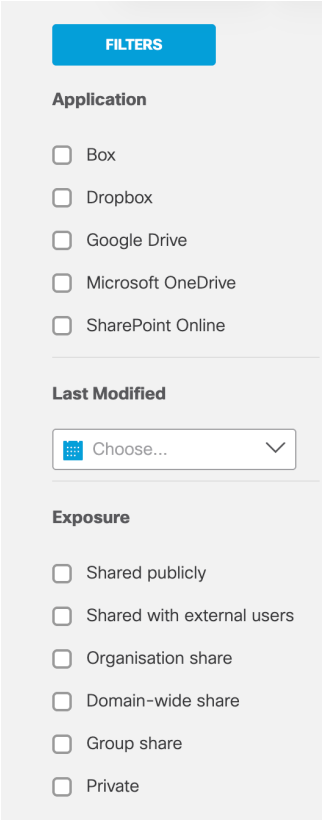
Provides instructions for viewing a discovery scan. You must initiate a discovery scan as described in Discovery Scan. Navigate to Monitor Reports Data Loss Prevention. Click the Discovery tab.

Before you begin

You must initiate a discovery scan as described in Discovery Scan.

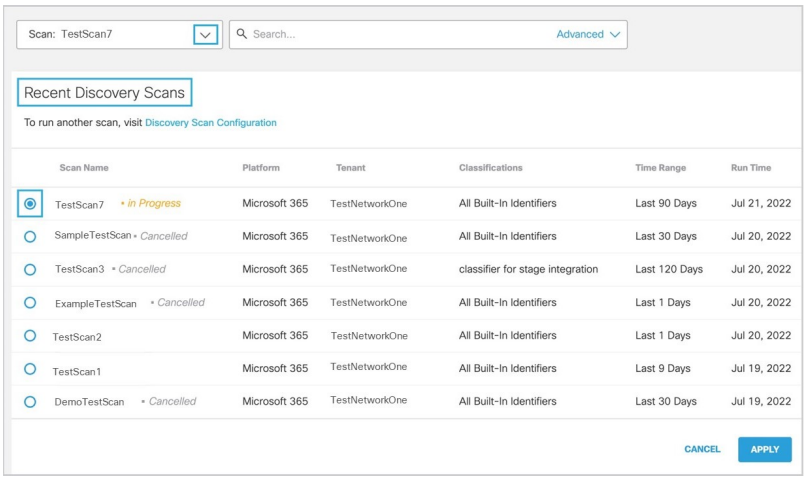
Procedure

1. Navigate to **Monitor** > **Reports** > **Data Loss Prevention.** Click the **Discovery** tab.
2. Use **Filters** to filter the data by **Application** , **Last Modified**, and **Exposure**.

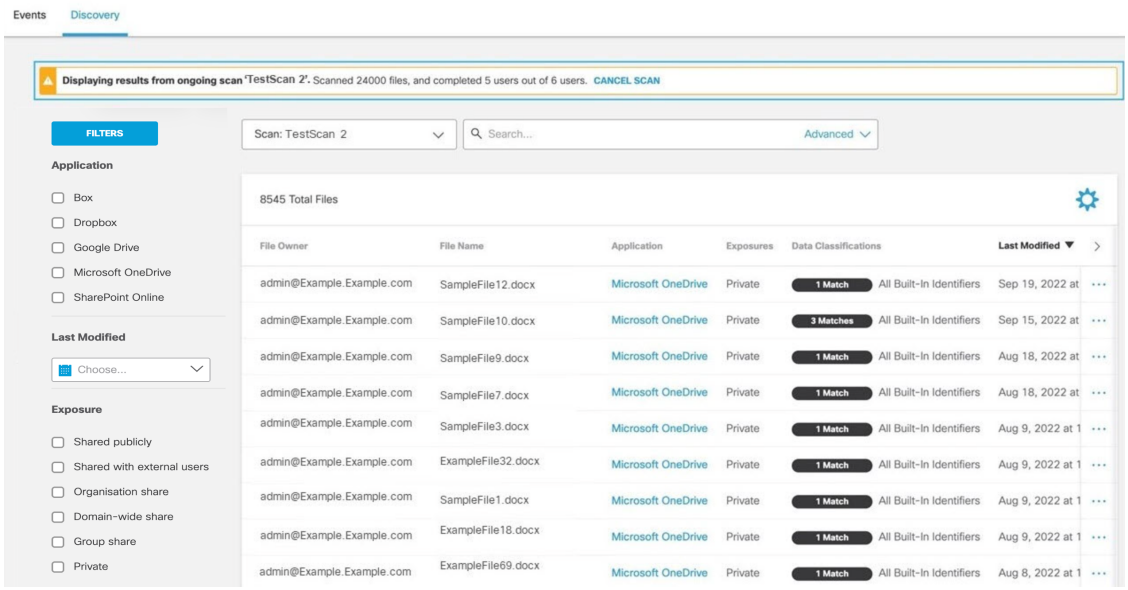


3. Choose a **Scan** from the drop-down. Click **Apply** to view the details.

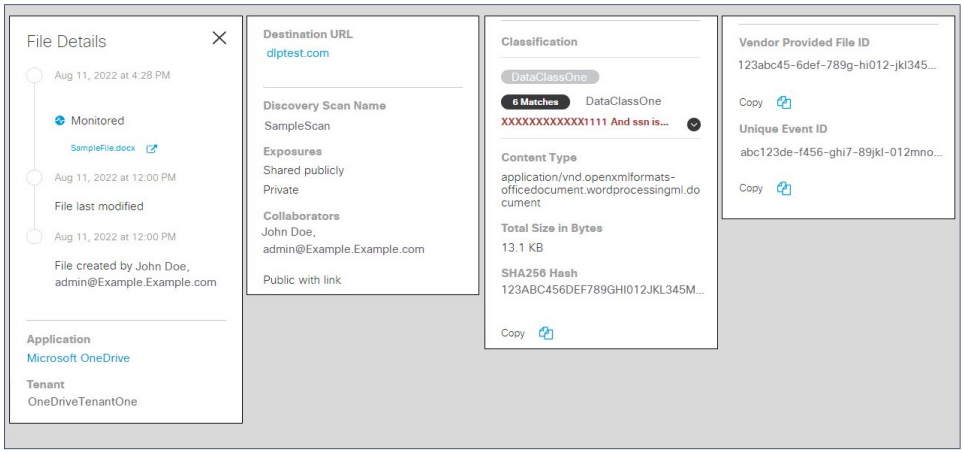
> **Note**
>
> Up to 10 recent scans are displayed. The next triggered Discovery Scan removes the oldest scan results in the list.



4. If there is an ongoing scan, the results are displayed. Click **Cancel Scan** to stop the ongoing scan. (You can only run one scan at a time.)



5. Click the action menu icon (three dots) to view further details of a file.



84 Admin Audit Log Report

Topics:

- Admin Audit Log Report

Describes the purpose and procedures for admin audit log report and outlines related topics, requirements, and operational considerations in Cisco Secure Access.

Admin Audit Log Report

Describes admin audit log report. The Admin Audit log records changes that your administrative team has made to your organization's Secure Access settings. Logs appear when change events occur, such as adding a user or modifying a rule. You can access data in 90-day increments.

The Admin Audit log records changes that your administrative team has made to your organization's Secure Access settings. Logs appear when change events occur, such as adding a user or modifying a rule. You can access data in 90-day increments. For more information about the details of the logs, see Log Formats and Versioning.

Generate Admin Audit Log Report

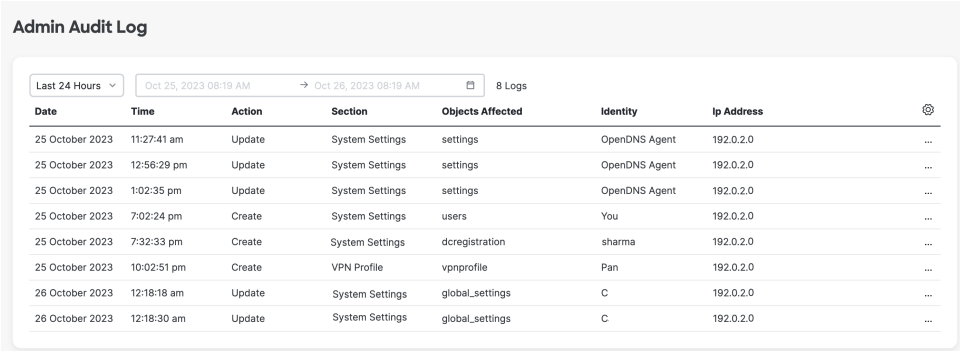
Provides instructions for generating admin audit log report. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

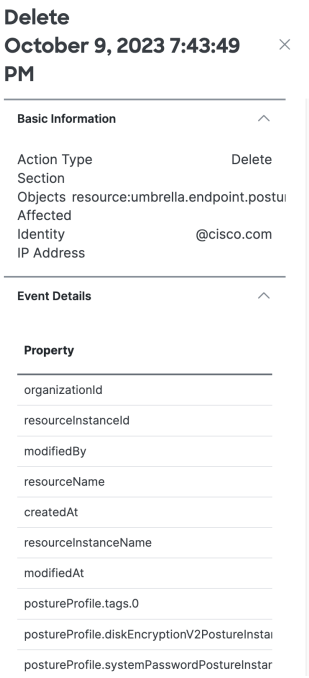
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Management** > **Admin Audit Log**.



2. Click an **Action** to view further details of an event.



Export Admin Audit Log Report to an S3 Bucket

Describes exporting admin audit log report to an s3 bucket. The Admin Audit log includes: Policies, Identities, or Block Pages that were Created

The Admin Audit log includes:

- Policies, Identities, or Block Pages that were Created
- Policies, Identities, or Block Pages that were Changed
- Policies, Identities, or Block Pages that were Deleted

Procedure

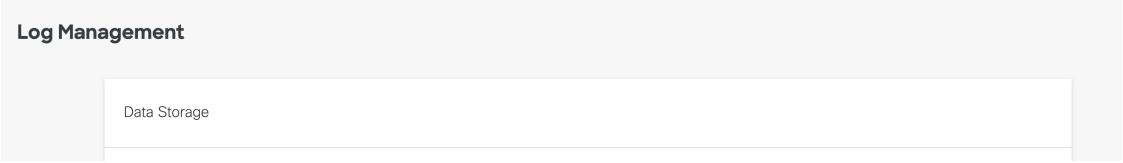
Provides instructions for procedure. Logging is enabled. See Manage Logging. A minimum user role of Read-only. For more information, see Manage Accounts.

Before you begin

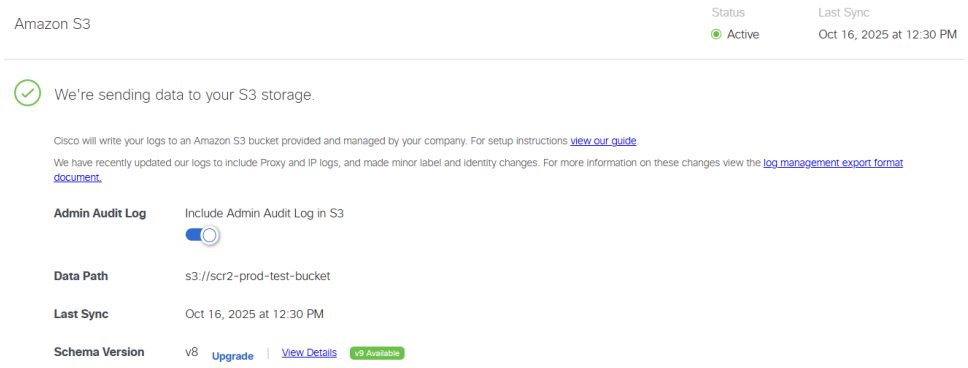
- Logging is enabled. See Manage Logging.
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Log Management**.



2. For your activated S3 bucket, navigate to **Admin Audit Log**. Enable the exportation of Admin Audit Log reports to your S3 bucket.



Secure Access saves your Admin Audit logs to the auditlogs folder.