Cisco Secure Access China User Guide

Cisco Secure Access
Updated March 12, 2025

Topics included

Part I: Cisco Secure Access China Help....16

1 Introduction to Cisco Secure Access China....18

Welcome to Cisco Secure Access China....19
Sign into Secure Access China with Security Cloud Sign On....19
Find Your Organization ID....20
Determine Your Current Package....21
Sign into Secure Access China....21
Find Your Organization....22
Determine Your Current Package....22
Secure Access China Single Sign-On Authentication....22
Configure Single Sign-On Authentication....22
Troubleshoot Single Sign On Authentication....24
Secure Access Regions....24

2 Getting Started....26

Get Started....27
Begin Secure Access Onboarding Workflow....27
Step 1 - Configure Network Connections....28
Step 2 - Configure Access to Resources....29
Step 3 - Configure End User Connectivity....30
Step 4 - Configure Endpoints and Network Sources....31
Secure Access China Overview....32
Prerequisites....36
What's Next....37
Quickstarts....37
Quickstart - Cisco Secure Client with Virtual Private Network....37
Quickstart - Cisco Secure Client with Internet Security....38
Quickstart - Browser with SAML Authentication....39
Prerequisites....39
Limitations and Range Limits....40
Limitations Due to Regulatory and Data Access Restrictions in China....40
Cisco Secure Client....40
Data Retention....40
Users and Groups....41
Network Requirements for Secure Access China....41
Cisco Secure Client and Captive Portal Detection....41
Cisco Secure Client and Device Host Names....42

Transport Layer Security Protocol Requirements....42
Secure Access Secure Web Gateway Services....42
Secure Access SaaS Tenants....43
Secure Access SAML Gateway Services....43
Secure Access SAML Identity Provider Domains....44
Secure Access SAML Gateway Client Certificate Revocation Services....45
Secure Access VPN Services....45
Secure Access VPN Client Certificate Revocation Services....45
Manage Network Connections....46
IPsec Network Tunnels....46
Network Tunnels (Deployed in Network Tunnel Groups)....46

3 Manage Network Tunnel Groups....48
Manage Network Tunnel Groups....49
Device Compatibility and Network Tunnels....49
Add a Network Tunnel Group....50
View Network Tunnel Group Details....53
Edit a Network Tunnel Group....55
Delete a Network Tunnel Group....56
Supported IPsec Parameters....57

4 Network Tunnel Configuration....60
Network Tunnel Configuration....61
Configure Tunnels with Catalyst SD-WAN cEdge and vEdge....61
Configure Tunnels with Cisco ISR....66
Configure Tunnels with Cisco Adaptive Security Appliance....70
Configure Tunnels with Cisco Secure Firewall....77
Configure Tunnels with Meraki MX....97
Establish a Tunnel....103

5 Manage Users and Groups....106
Manage Users and Groups....107
View User Details....107
View Group Details....109
Provision Token for Identity Provider....111
Import Users and Groups from CSV File....113
Provision Users and Groups from Okta....115
Provision Users and Groups from Azure....123
Provision Users and Groups....125
View Users and Groups in Secure Access....126

6 Provision Users and Groups from Active Directory....128
Provision Users and Groups from Active Directory....129

Prerequisites for AD Connectors....129
Connect Multiple Active Directory Domains....130
Manage AD Components....131
Manage AD Connectors....138
AD Connector Communication Flow and Troubleshooting....154
Next Steps....157

7 Configure Integrations with SAML Identity Providers....158
Configure Integrations with SAML Identity Providers....159
Prerequisites for SAML Authentication....159
Configure Azure AD for SAML....160
Configure Okta for SAML....167
Configure AD FS for SAML....173
Configure Duo Security for SAML....184
Configure Ping Identity for SAML....191
Configure OpenAM for SAML....196
SAML Certificate Renewal Options....201
Test SAML Identity Provider Integration....202
Delete SAML Identity Provider Integration....203
Use Cases....204
Configure Identity Providers for SAML Authentication....204

8 Manage End-User Connectivity....206
Manage End-User Connectivity....207
Virtual Private Networks Settings and Profiles....207
Internet Security....207

9 Manage DNS Servers....208
Manage DNS Servers....209
Prerequisites....209
Procedure....209

10 Manage Remote Access Virtual Private Networks....210
Manage Remote Access Virtual Private Networks....211
FQDNs for Network Connections....211
Manage IP Pools....212
Add an IP Pool....213
Manage VPN Profiles....219
Add VPN Profiles....219
Manage Machine Tunnels....226

11 Manage PAC Files....236

Manage PAC Files....237
Deploy the Secure Access PAC File for Windows....237
Deploy the Secure Access PAC File for macOS....238
Customize the Secure Access PAC File....240
What is a PAC file?....242
Known Limitations....242
Recommendations....242

12 Manage Internet Security....244
Manage Internet Security....245
Set Up Internet Security on User Devices....245
Manage Internet Security Bypass....246
Configure Cisco Secure Client Settings....251
Download Cisco Secure Client or Copy Secure Access PAC File URL....253
Add Bypass Domains and Set Up Internet Security....253
Next Steps....254

13 Manage Resources....256
Manage Resources....257
Resource menu items that can be used as sources in access rules:....257
Resource menu items that can be used as destinations in internet access rules:....257
Resource menu items that can be used as destinations in private access rules:....257
Additional resources....257

14 Manage Registered Networks....258
Manage Registered Networks....259
Add Network Resources....259
Update a Network Resource....262
Delete a Network Resource....264

15 Manage Internal Networks....266
Manage Internal Networks....267
Add Internal Network Resources....267
Update an Internal Network Resource....268
Delete an Internal Network Resource....269

16 Manage Destination Lists....270
Manage Destination Lists....271
Add a Destination List....271
Upload Destinations From a File....272
Edit a Destination List....274
Download Destinations to a CSV File....274

Control Access to Custom URLs....275
Wildcards in Destination Lists....279
Add Punycode Domain Name to Destination List....280
Troubleshoot Destination Lists....281
How to Format Your Destination List....282

17 Manage AAA Servers....284
Manage AAA Servers....285

18 Manage Application Lists....286
Manage Application Lists....287
Add an Application List....287
Application Categories....288
Delete an Application List....290

19 Manage Content Category Lists....292
Manage Content Category Lists....293
Available Content Categories....293
Add a Content Category List....297
Request a Category for an Uncategorized Destination....298
Dispute a Content Category....298
View Content Categories in Reports....299

20 Manage Tenant Control Profiles....304
Manage Tenant Control Profiles....305
Add a Tenant Controls Profile....305
Control Cloud Access to Dropbox....308
Control Cloud Access to Google G Suite....309
Control Cloud Access to Microsoft 365....311
Control Cloud Access to Slack....313
Use Tenant Controls in Access Rules....314
Review Tenant Controls Through Reports....315

21 Manage Network Devices....318
Manage Network Devices....319
How to Add a Network Device in Secure Access....319
Procedure for Managing Network Devices....319

22 Manage Roaming Devices....322
Manage Roaming Devices....323
View Internet Security Settings for Roaming Devices....323
Edit Internet Security Settings for Roaming Devices....324

Delete a Roaming Device....327

23 Manage Private Resources....328

Manage Private Resources....329

Add a Private Resource....329

Add a Private Resource Group....332

Step 1 – Configure Private Resources....333

Step 2 – Set Up Network Connections, VPN Profiles, and Certificates....333

Step 3 – Add Private Resources in Private Access Rules....333

24 Manage Connections to Private Destinations....334

Manage Connections to Private Destinations....335

Manage Branch Connections....335

25 Manage the Access Policy....338

Manage the Access Policy....339

About the Access Policy....339

Show Additional Data on Your Access Rules....341

Edit the Order of the Rules in Your Access Policy....344

Rule Defaults: Default Settings for Access Rules....344

Global Settings for Access Rules....346

Edit Rule Defaults and Global Settings....348

Edit the Default Access Rules....349

Private and Internet Access Rules in Your Policy....349

Default Access Rules in Your Policy....350

Rule Defaults and Global Settings....350

26 Get Started With Internet Access Rules....352

Get Started With Internet Access Rules....353

Components for Internet Access Rules....353

Default Settings for Internet Access Rules....358

Add an Internet Access Rule....359

About Configuring Sources in Internet Access Rules....366

About Configuring Destinations in Internet Access Rules....367

Advanced Application Controls....369

Global Settings for Internet Access Rules....374

Troubleshoot Internet Access Rules....374

27 Get Started With Private Access Rules....378

Get Started With Private Access Rules....379

Components for Private Access Rules....380

Default Settings for Private Access Rules....382

Add a Private Access Rule....383
About Configuring Sources in Private Access Rules....388
About Configuring Destinations in Private Access Rules....389
About Endpoint Requirements in Access Rules....390
Allowing Traffic from Users and Devices on the Network....390
Global Settings for Private Access Rules....390
Troubleshoot Private Access Rules....391

28 Manage Endpoint Security....394
Manage Endpoint Security....395
Endpoint Attributes....395
About Endpoint Posture....396
About Posture Profiles....397
Endpoint Posture Assessment....397

29 Manage VPN Connection Posture Profiles....398
Manage VPN Connection Posture Profile....399
Add a VPN Connection Posture Profile....399

30 Manage IPS Profiles....404
Manage IPS Profiles....405
How IPS Works....405
Decryption is Required for Effective Intrusion Prevention....405
Exceptions for Traffic That Should Not be Decrypted....406
IPS is Used in Both Types of Access Rules....406

31 Manage Web Profiles....408
Manage Web Profiles....409
Add a Web Profile....409
Functionality Included in a Web Profile....412
Decryption....413
SAML Authentication....414
Security and Acceptable Use Controls....414
End-User Notifications....415
Enable SafeSearch....415
Enable SafeSearch....415
Confirm That SafeSearch is Working....415

32 Manage Threat Categories....420
Manage Threat Categories....421
Threat Category Descriptions....421
Add a Threat Category List....421

Dispute a Threat Categorization....422
Default Threat Category List....422
Reporting on Threat Category Access Attempts....423

33 Manage File Inspection....424
Manage File Inspection....425
Enable File Inspection....425
Test File Inspection....426
Monitor File Inspection Activity....426
Troubleshoot and Monitor File Inspection....427
Overview of Configuring File Inspection 427
File Inspection Details....427

34 Manage File Type Controls....430
Manage File Type Controls....431
Enable File Type Controls....431
File Types to Block....432
Review File Type Controls Through Reports....433

35 Manage Notification Pages....438
Manage Notification Pages....439
Preview Notification Pages....439
Create Custom Block and Warn Pages....440
Allow Users to Contact an Administrator....442
To view notification pages displayed to end users:....444
To display custom notification pages to end users:....444
Warn Pages: More Information....444
About Block Pages for Private Access Traffic....445

36 Manage Traffic Decryption....446
Manage Traffic Decryption....447
Important Information About Do Not Decrypt Lists....447
Add a Do Not Decrypt List for Web Profiles....448
Internet Access Features Requiring Decryption....450
Internet Traffic That Should Not Be Decrypted....450
Decryption in Private Access Rules....451
Decryption Settings....451
Decryption Requires Certificates....451
Decryption Logging....452
Troubleshooting Decryption....452

37 Manage Certificates....454

Manage Certificates....455
Certificates for Internet Decryption....455
Install the Cisco Secure Access Root Certificate....456
Add Customer CA Signed Root Certificate....461
View the Cisco Trusted Root Store....464
Manage Certificates for Private Resource Decryption....466
Certificates for Private Resource Decryption....468
Certificates for SAML Authentication....468
Manage SAML Certificates for Service Providers....468
Manage SAML Certificates for Identity Providers....470
VPN Certificates for User and Device Authentication....473
Manage CA Certificates for VPN Connections....473
Certificate Installation Methods....477

38 Manage the Data Loss Prevention Policy....478
Manage the Data Loss Prevention Policy....479
Add a Real Time Rule to the Data Loss Prevention Policy....480
Understand Exclusions in a Real Time Rule....490
Supported Applications....490
Discovery Scan....493
Edit a Data Loss Prevention Rule....497
Delete a Data Loss Prevention Rule....498
Enable or Disable a Data Loss Prevention Rule....498
Supported File and Form Types....500
Best Practices for the Data Loss Protection Policy....500

39 Manage Data Classifications....502
Manage Data Classifications....503
Add a Data Classification....503
Copy and Customize a Built-In Data Classification....509
Delete or Edit a Classification....518
Create an Exact Data Match Identifier....520
Index Data for an EDM....525
Exact Data Match Field Types....529
Create an Indexed Document Match Identifier....531

40 Built-in Data Identifiers....538
Built-in Data Identifiers....539
Copy and Customize a Data Identifier....539
Create a Custom Dictionary....541
Custom Regular Expression Patterns....543
Individual Data Identifiers....544
Tolerances....545

41 Manage Logging....546
Manage Logging....547
Enable Logging....547
Enable Logging to Your Own S3 Bucket....548
Enable Logging to a Cisco-managed S3 Bucket....552
Stop Logging....556
Delete Logs....556
Log Formats and Versioning....557
Where are Logs Stored?....576

42 Manage API Keys....578
Manage API Keys....579
Add Secure Access API Keys....579
Add KeyAdmin API Keys....583

43 Manage Accounts....588
Manage Accounts....589
Add a New Account....589
Edit Account Settings....591
Delete an Account....592
Hide Sources with De-identification....592

Part II: Cisco Secure Client....596

44 Get Started with Cisco Secure Client on Windows and macOS....598
Get Started with Cisco Secure Client on Windows and macOS....599
Prerequisites....599
Download Cisco Secure Client....600
Download the OrgInfo.json File....601
Manual Installation of Cisco Secure Client (Windows and macOS)....603
Mass Deployment Overview....604
Mass Deployment (Windows)....606
Multi Deployment Support....609
Customize Windows Installation of Cisco Secure Client....614
Mass Deployment (macOS)....617
Customize macOS Installation of Cisco Secure Client....620
VPN Headend Deployment....627
Secure Firewall Management Center and Secure Firewall Threat Defense....627
Meraki Systems Manager (SM) Deployment....630
Migration from Umbrella Roaming Client....630
Install the Root Certificate for All Browsers....630

Cloud Management....631
Additional References....637
Remote Monitoring and Management Deployment Tutorials....638

45 Manage Internet Security on Cisco Secure Client....640
Manage Internet Security on Cisco Secure Client....641
Download the OrgInfo.json File....641
Umbrella Roaming Security Module Requirements....643
Domain Management....645
Interpret Internet Security Diagnostics....647
Customize Windows Installation of Cisco Secure Client....648
Customize macOS Installation of Cisco Secure Client....650

46 Manage Virtual Private Networks on Cisco Secure Client....658
Manage Virtual Private Networks on Cisco Secure Client....659
Download the Virtual Private Network XML Profile....659
CA Certificates for VPN Connections....660
Prerequisites....660

Part III: Reports....662

47 Monitor Secure Access with Reports....664
Monitor Secure Access China with Reports....665
Export Report Data to CSV....665
Bookmark and Share Reports....666
Report Retention....667
Schedule a Report....667
Update a Scheduled Report....671
Report Scheduling....673
Available Reports....674

48 Remote Access Log Report....676
Remote Access Log Report....677
View the Remote Access Log Report....677

49 Activity Search Report....682
Activity Search Report....683
View the Activity Search Report....683
View Activity Search Report Actions....690
Schedule an Activity Search Report....693
Use Search and Advanced Search....693

50 Security Activity Report....698
Security Activity Report....699
View Activity and Details by Filters....699
View Activity and Details by Event Type or Security Category....701
View an Event's Details....704
Search for Security Activity....707

51 Total Requests Report....710
Total Requests Report....711
Prerequisites....711
View Trends in the Total Requests Report....711

52 Activity Volume Report....716
Activity Volume Report....717
Prerequisites....717
View Requests by Volume of Activity....717
View Activity Volume by Threat Categories....718
View Activity Volume by Policy Traffic....719
View Trends....719

53 App Discovery Report....720
App Discovery Report....721
View the App Discovery Report....721
View the Highest Risk Apps....723
Review Apps in the Apps Grid....724
View App Details....728
Change App Details....730
Control Apps....734
Control Advanced Apps....736
View Traffic Data Through SWG Service....737

54 Top Destinations Report....742
Top Destinations Report....743
Destination Details....743
Prerequisites....747
View the Top Destinations Report....747
View Further Details....750

55 Top Categories Report....752
Top Categories Report....753
Category Details....753

Prerequisites....757
View the Top Categories Report....757
Top Categories Quick View....760
View Category in Other Reports....761

56 Data Loss Prevention Report....762
Data Loss Prevention Report....763
Prerequisites....763
Events....763

57 Admin Audit Log Report....766
Admin Audit Log Report....767
Export Admin Audit Log Report to an S3 Bucket....767
Prerequisites....768
Generate Admin Audit Log Report....768

Part I

Cisco Secure Access China Help

Topics:

- Introduction to Cisco Secure Access China
- Getting Started
- Manage Network Tunnel Groups
- Network Tunnel Configuration
- Manage Users and Groups
- Provision Users and Groups from Active Directory
- Configure Integrations with SAML Identity Providers
- Manage End-User Connectivity
- Manage DNS Servers
- Manage Remote Access Virtual Private Networks
- Manage PAC Files
- Manage Internet Security
- Manage Resources
- Manage Registered Networks
- Manage Internal Networks
- Manage Destination Lists
- Manage AAA Servers
- Manage Application Lists
- Manage Content Category Lists
- Manage Tenant Control Profiles
- Manage Network Devices
- 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 VPN Connection Posture Profiles
- Manage IPS Profiles
- Manage Web Profiles
- Manage Threat Categories
- Manage File Inspection
- Manage File Type Controls
- Manage Notification Pages
- Manage Traffic Decryption

Describes Cisco Secure Access China Help. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

- Manage Certificates
- Manage the Data Loss Prevention Policy
- Manage Data Classifications
- Built-in Data Identifiers
- Manage Logging
- Manage API Keys
- Manage Accounts

1 Introduction to Cisco Secure Access China

Topics:

- Welcome to Cisco Secure Access China
- Secure Access China Single Sign-On Authentication
- Secure Access Regions

Provides an overview of Introduction to Cisco Secure Access China, including Welcome to Cisco Secure Access China, Secure Access China Single Sign-On Authentication, and Secure Access Regions. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Welcome to Cisco Secure Access China

Describes Welcome to Cisco Secure Access China. Secure Access China, operated by Digital China Cloud, is Cisco's cloud-based platform that offers multiple levels of defense against internet-based threats.

Secure Access China, operated by Digital China Cloud, is Cisco's cloud-based platform that offers multiple levels of defense against internet-based threats. It 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 China, you can apply and enforce comprehensive security controls on collections of resources, users, and devices. The Secure Access policy serves as a container for your security configuration rules, allowing you to 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 China collates various reports and logs. The Secure Access China 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.

Sign into Secure Access China with Security Cloud Sign On

Describes Sign into Secure Access China with Security Cloud Sign On. Cisco Secure Access China supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access China console.

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

Prerequisites

Lists the prerequisites for sign into secure access. A valid Secure Access China account. For more information, see Manage Accounts.

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

Procedure

Provides instructions for sign into secure access. Sign in to Secure Access China 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.

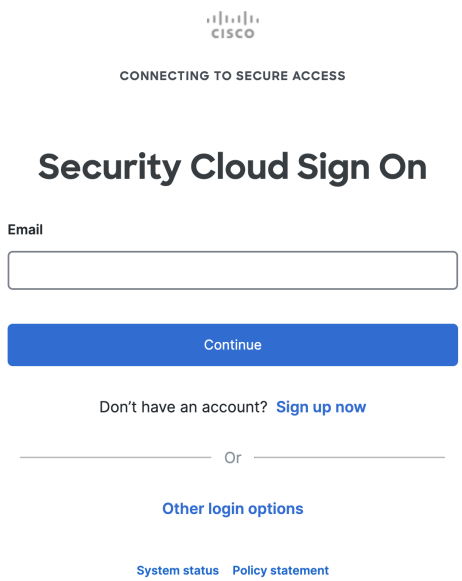
Sign in to Secure Access China through the Cisco Security Cloud Sign-On (SCSO) portal. If you do not have an SCSO account, follow the steps to Configure Single Sign-On Authentication.

1. Navigate to your Secure Access China organization at https://dashboard.ciscosecureaccess.cn<*org_number*>.

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

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

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



3. If you have an SCSO account, click **Continue** to sign in to Secure Access China.

Find Your Organization ID

Provides instructions for finding your Organization ID in Cisco Secure Access China. Every Secure Access organization (Org) is a separate instance of Secure Access China.

Every Secure Access organization (Org) is a separate instance of Secure Access China. 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.

Prerequisites

Lists the prerequisites for find your organization id. A minimum user role of Read Only. For more information, see Manage Accounts.

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

Procedure

Provides instructions for finding your organization id.

1. Sign in to Secure Access China.
2. Check the URL in the browser's address bar:

   ```
   https://dashboard.ciscosecureaccess.cn/org/<orgId>/#/<page>
   ```

   where `orgId` is your unique Secure Access China 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 China organization. Your organization name is listed under your account name.
4. Click **Switch Organizations** to change to another Secure Access China organization.
5. Locate **System Status**–the overall health status of Secure Access China.

Determine Your Current Package

Provides instructions for determining your Current Package in Cisco Secure Access China. Within your Cisco Secure Access China subscription, the Secure Access package determines the features available to you and your level of support.

Within your Cisco Secure Access China 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 China Subscription page.

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

Prerequisites

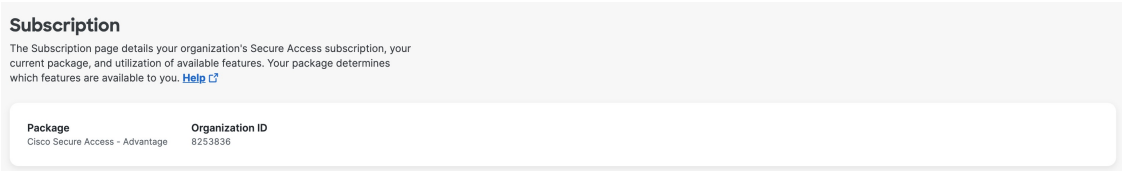
Lists the prerequisites for determine current package. A minimum user role of Read Only. For more information, see Manage Accounts.

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

Procedure

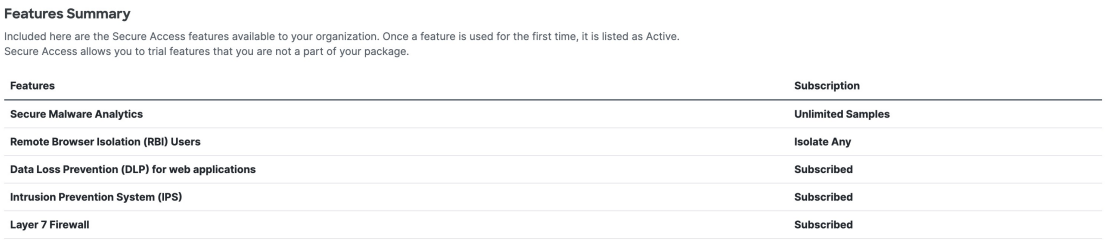
Provides instructions for determine current package. Navigate to Admin > Subscription and review the information about your current package. Package –The name of your package.

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 China.

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



Features	Subscription
Secure Malware Analytics	Unlimited Samples
Remote Browser Isolation (RBI) Users	Isolate Any
Data Loss Prevention (DLP) for web applications	Subscribed
Intrusion Prevention System (IPS)	Subscribed
Layer 7 Firewall	Subscribed

   - **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.

Sign into Secure Access China

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

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

Find Your Organization

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

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

Determine Your Current Package

Provides instructions for viewing your current Secure Access China package and directs readers to the package information used for setup decisions.

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

Secure Access China Single Sign-On Authentication

Describes Secure Access China Single Sign-On Authentication. Cisco Secure Access China supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access China console.

Cisco Secure Access China supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access China console. An administrator signs in to Secure Access China 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 China administrators through SCSO. For more information, see Cisco Security Cloud Sign On Identity Provider Integration Guide.

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

Any changes made in your organization's SAML identity provider (IdP) are synced with Secure Access China. 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 China. You must sign in to Secure Access China 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 China. The IdP that you set up in SCSO does not authorize an administrator's permissions to read, create, or update resources on Secure Access China. A Secure Access role defines the permissions on the Secure Access China account. For more information about user roles, see Manage Accounts.

Configure Single Sign-On Authentication

Provides instructions for configuring single Sign-On Authentication in Cisco Secure Access China. Cisco Secure Access China supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access China console.

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

Prerequisites

Lists the prerequisites for creating single sign on authentication account. A valid Secure Access China account. For more information, see Manage Accounts.

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

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

Provides instructions for adding your organization's identity provider in security cloud sign on. You can add an SAML identity provider (IdP) in SCSO for Secure Access China.

You can add an SAML identity provider (IdP) in SCSO for Secure Access China. 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

Provides instructions for adding administrators to secure access. When an administrator provisions a Secure Access China account, an email is sent from Secure Access China to the new administrator with the instructions to use SSO authentication to sign in to their Secure Access China Org.

A Cisco Secure Access China administrator can add additional administrators to their Secure Access China 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.

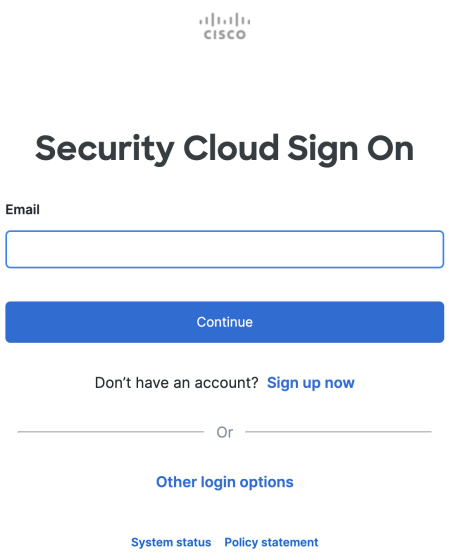
When an administrator provisions a Secure Access China account, an email is sent from Secure Access China to the new administrator with the instructions to use SSO authentication to sign in to their Secure Access China Org.

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

Procedure

Provides instructions for creating single sign on authentication account. Configure SSO authentication for Secure Access China through Cisco Security Cloud Sign On (SCSO).

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



1. Navigate to your Secure Access China organization at <https://dashboard.ciscosecureaccess.cn/org><org_number>.

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

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

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

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

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

4. Once you receive an email from Secure Access China 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.
5. Follow the steps to sign in to your Secure Access China Org. For more information, see Sign In to Secure Access with Security Cloud Sign On.

Troubleshoot Single Sign On Authentication

Provides instructions for troubleshooting single Sign On Authentication in Cisco Secure Access China. If you are unable to sign in to Secure Access China through Cisco Security Cloud Sign On, contact technical support provided by Digital China Cloud (DCC).

If you are unable to sign in to Secure Access China through Cisco Security Cloud Sign On, contact technical support provided by Digital China Cloud (DCC).

Secure Access Regions

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

Cisco Secure Access China has instances of regional network and computing data centers that protect and manage public and private resources. The Secure Access regions are located geographically around the world. Network branches, data centers, and user devices can connect to the Secure Access regions through the secure web gateway (SWG) and Virtual Private Networks (VPNs). Each region is highly available and composed of two or more physically independent data centers.

The Secure Access regions and data centers host the various IP addresses and fully-qualified domain names (FQDNs) for the Secure Access cloud services:

- **Secure Web Gateway**–For more information, see Secure Access Secure Web Gateway Services.
- **IPsec Tunnels**–For more information, see Add a Network Tunnel Group and View Network Tunnel Group Details.

2 Getting Started

Topics:

- Get Started
- Quickstarts
- Limitations and Range Limits
- Network Requirements for Secure Access China
- Manage Network Connections

Provides an overview of Getting Started in Cisco Secure Access China, including Get Started, Quickstarts, and Limitations and Range Limits. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started

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

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

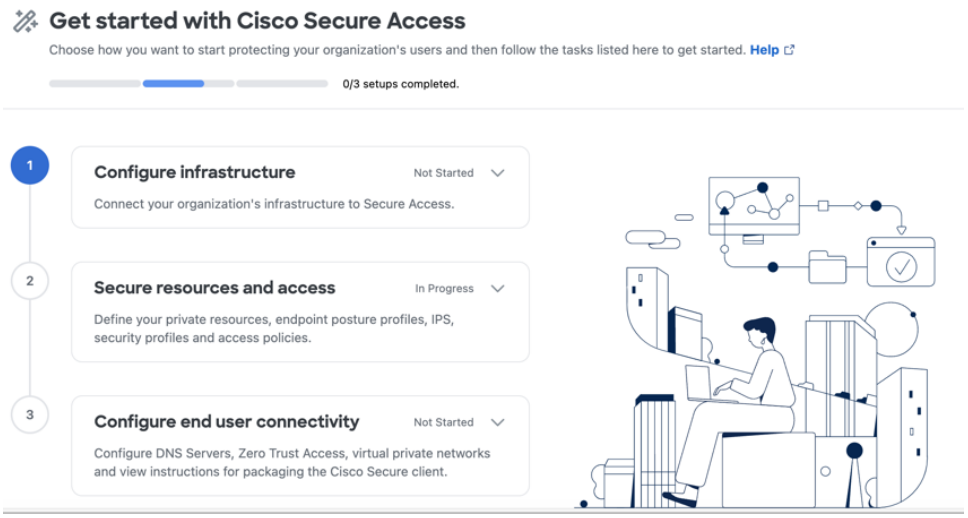
Secure Access China supports various network configurations and security controls through policy rules. The Secure Access policy defines how your organization manages network traffic, which sources can reach available resources. In a policy rule, you can combine settings from web profiles, posture profiles, 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.

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 China.

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

Provides instructions for configuring network Connections in Cisco Secure Access China. 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 China.

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 China. Once you complete the network connections deployment steps, provision users and groups from your organization in Secure Access China and configure integrations with SAML identity providers (IdPs). For more information, see Manage Network Connections.

Prerequisites

Lists the prerequisites for configuring network connections, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Task 1 – Add Network Connections

Outlines the first setup task for adding network connections and preparing the connectivity configuration for Secure Access China. for administrators to review.

Add Network Tunnel Groups

Provides instructions for adding 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.

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.

- Manage Network Connections

Task 2 – Provision Users and Groups

Outlines user and group provisioning options, including importing users and groups from CSV files or provisioning them from Okta for Secure Access China.

Provision users and groups from your organization in Secure Access China. 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

Outlines SAML identity provider integration for the organization and links to instructions for integrating identity providers and users with Secure Access China.

Integrate SAML identity providers (IdPs) and users in your organization in Secure Access China. 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

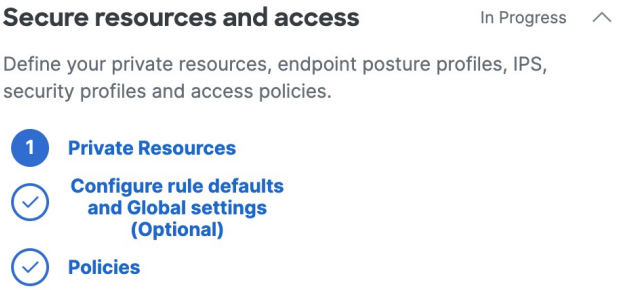
Outlines the next setup step for configuring access to resources after establishing network connections for Secure Access China. for administrators to review.

- Step 2 - Configure Access to Resources

Step 2 – Configure Access to Resources

Provides instructions for configuring access to Resources in Cisco Secure Access China. 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.

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

Lists the prerequisites for configuring access to resources, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Task 1 – Set Up Private Resources

Outlines the initial private resource setup task, including resource types and the configuration users need to connect to organizational subnets and applications.

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 – (Optional) Configure Rule Defaults and Global Settings

Outlines the optional task for configuring rule defaults and global settings used to control access to private resources in Secure Access China.

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

Manage Rule Defaults

Provides instructions for managing rule defaults. Manage IPS Profiles. Manage Web Profiles. Manage VPN Connection Posture Profiles. Manage Tenant Controls.

- Manage IPS Profiles
- Manage Web Profiles
- Manage VPN Connection Posture Profiles
- Manage Tenant Controls
- Manage Certificates
- Manage Threat Categories

Manage Global Settings

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

Outlines policy rule setup, including configuring and adding rules and using Manage the Access Policy to administer them in Secure Access China.

Configure and add rules to the Secure Access policy.

- Manage the Access Policy

What's Next

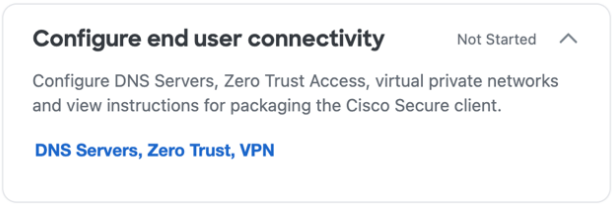
Outlines the next setup step: configure end-user connectivity after access to resources, as part of preparing Secure Access China. for administrators to review.

- Step 3 - Configure End User Connectivity

Step 3 - Configure End User Connectivity

Provides instructions for configuring end User Connectivity in Cisco Secure Access China. The Get Started with Secure Access workflow guides you through the tasks in the Configure End User Connectivity step–configure internet security, and virtual private networks (VPNs) access for user devices.

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



Prerequisites

Lists the prerequisites for configuring end user connectivity, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Task 1 – Configure Virtual Private Networks

Outlines the initial VPN setup task, including VPN settings and the Manage Remote Access Virtual Private Networks guidance for Cisco Secure Access China.

Set up virtual private networks (VPNs) settings.

- Manage Remote Access Virtual Private Networks

Task 2 – Configure Internet Security

Outlines the Internet Security setup task, including adding domains to the internal domains list and configuring Cisco Secure Client internet security settings.

Add domains to internal domains list and configure internet security settings for the Cisco Secure Client.

- Manage Internet Security

Configure Endpoints and Networks

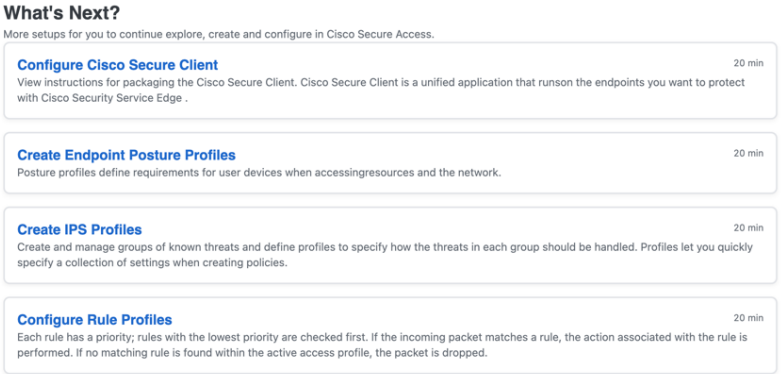
Outlines the step for configuring endpoints and network sources after setting up network connections in Secure Access China. for administrators to review.

- Step 4 – Configure Endpoints and Network Sources

Step 4 – Configure Endpoints and Network Sources

Provides instructions for configuring endpoints and Network Sources in Cisco Secure Access China, including Prerequisites, Add Networks to Secure Access China, and Set Up the Cisco Secure Client. It explains the sequence of actions and relevant settings presented in the procedure.

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 China, and configure IPS and endpoint posture profiles in policy rules.



Prerequisites

Lists the prerequisites for configuring endpoints and network sources, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Add Networks to Secure Access China

Provides links for adding networks to Secure Access China, including instructions for managing registered networks and internal networks. for administrators to review.

- Manage Registered Networks
- Manage Internal Networks

Set Up the Cisco Secure Client

Provides instructions for setting up the Cisco Secure Client. Download Cisco Secure Client. Download the OrgInfo.json File. Download the VPN XML File.

- Download Cisco Secure Client
- Download the OrgInfo.json File
- Download the VPN XML File
- Install the Cisco Secure Client

Add IPS Profiles

Provides instructions for adding IPS profiles and directs administrators to the Manage IPS Profiles topic for profile configuration details in Secure Access China.

- Manage IPS Profiles

Configure Rule Profiles

Directs administrators to the Manage the Access Policy topic for guidance on configuring rule profiles and managing access rules in Secure Access China.

- Manage the Access Policy

Secure Access China Overview

Describes Secure Access China Overview and outlines Prerequisites, Get Started Workflow, and Connectivity. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

The Cisco Secure Access China 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 China 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 China. For information about the Secure Access reports, see Get Started with Reports.

Prerequisites

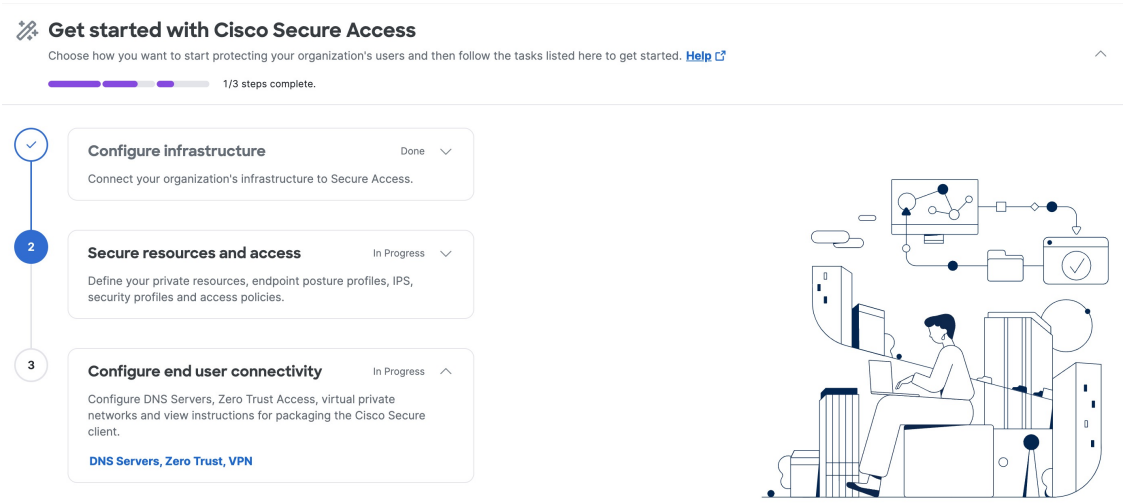
Lists the prerequisites for securing access overview. A minimum user role of Read Only. For more information, see Manage Accounts.

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

Get Started Workflow

Provides instructions for getting started workflow. The Getting Started with Secure Access Workflow describes the first configuration steps required to begin protecting your systems with Secure Access China.

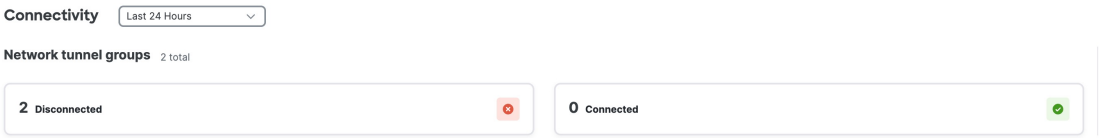
The **Getting Started with Secure Access Workflow** describes the first configuration steps required to begin protecting your systems with Secure Access China.



Connectivity

Describes the Connectivity status shown for configured Network Tunnel Groups and helps administrators review their organization?s connection state. for administrators to review.

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)**

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

Describes 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** section displays the number of access events–requests and blocks. It also displays the number IPS events–signature events.



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

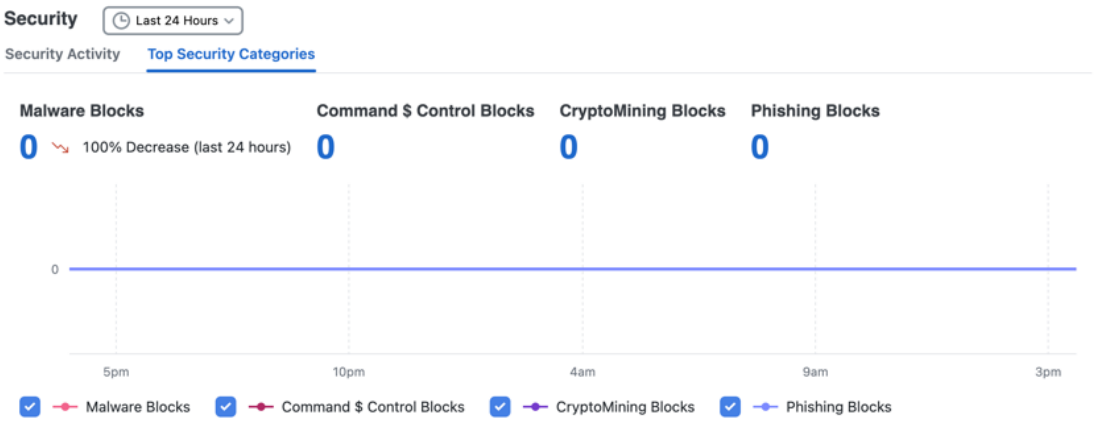


Users with the **Full Admin** or **Security Administrator** role can follow the **Certificates** link to update the certificate, or close the banner. If the certificate is not updated, a closed banner will reappear the next time the user opens the **Overview** page.

Top Security Categories

Describes the Top Security Categories display, which shows request counts for leading security categories and supports review of threat activity.

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



Users and Groups

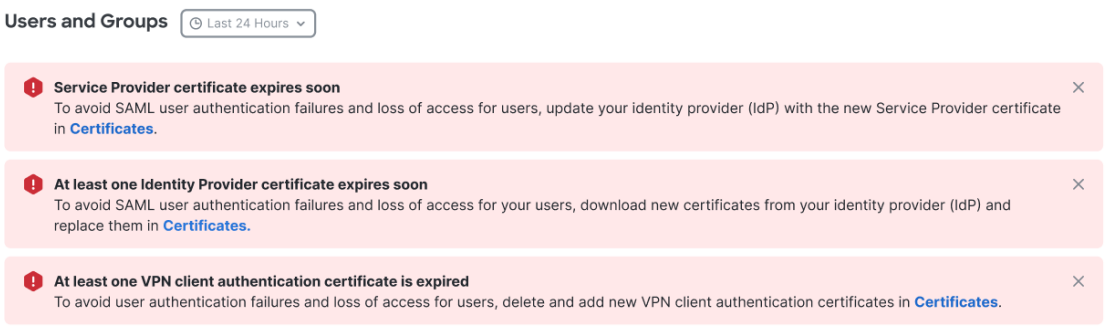
Describes users and Groups. The Users and Groups section displays the number of virtual private network (VPN) connections over time. This section also lists the top users in your organization who made the greatest number of requests in the selected time period.

The Users and Groups section displays the number of virtual private network (VPN) connections 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

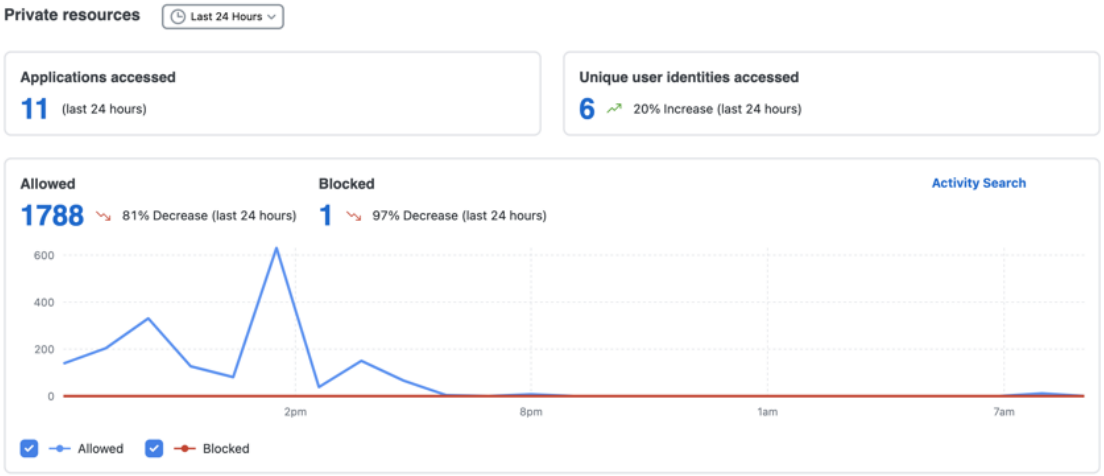
- VPN Certificates for User and Device Authentication

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.

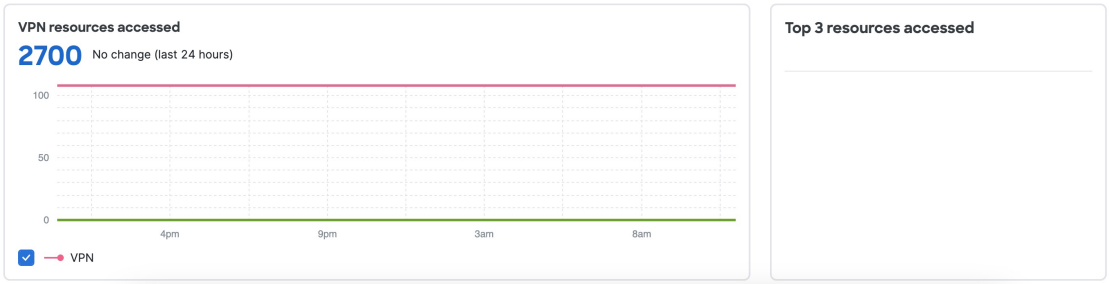
Private Resources

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 China and the method of the connection: virtual private network (VPN). The section also includes the top resources that received traffic.



Prerequisites

Lists the prerequisites for getting started secure access. Sign in to Secure Access China with single sign-on (SSO) authentication. For more information, see Sign Into Secure Access with Security Cloud Sign On.

- Sign in to Secure Access China 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 China subscription. For more information, see Determine Your Current Package.

What's Next

Describes 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 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.

Quickstarts

Describes Quickstarts in Cisco Secure Access China and outlines Prerequisites. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

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 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 Web profile and enable SAML authentication. For more information, see Quickstart – Browser with SAML Authentication.

Quickstart – Cisco Secure Client with Virtual Private Network

Describes Quickstart – Cisco Secure Client with Virtual Private Network in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for quickstart secure client vpn, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for quickstart secure client VPN. Deploy network tunnel groups in Secure Access China. For more information, see Manage Network Tunnel Groups.

1. Deploy network connectors in Secure Access China.
    - Deploy network tunnel groups in Secure Access China. 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 China. For more information, see Manage Users and Groups.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create a VPN endpoint posture profile for the user devices. For more information, see Add a VPN Connection Posture Profile.
5. Create a policy rule or add a VPN endpoint posture profile for the user devices to an existing Secure Access rule. For more information, see 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

Test Your Connectivity

Provides instructions for testing your connectivity. Check that you can reach private, SaaS, and internet resources protected by Secure Access China.

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

Quickstart – Cisco Secure Client with Internet Security

Describes Quickstart - Cisco Secure Client with Internet Security in Cisco Secure Access China. The Cisco Secure Client with Internet Security and secure web gateway (SWG)—connects user devices securely to internet resources.

The Cisco Secure Client with Internet 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.

Prerequisites

Lists the prerequisites for quickstart secure client internet security, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for quickstart secure client internet security. Deploy network tunnel groups in Secure Access China. For more information, see Manage Network Tunnel Groups.

1. Deploy network connectors in Secure Access China.
   - Deploy network tunnel groups in Secure Access China. 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 China. For more information, see Manage Users and Groups.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create a Web posture profile for the user devices. For more information, see Add a Web Profile.

5. Create a policy rule or add a Web profile for the user devices to an existing Secure Access rule. For more information, see Manage the Access Policy.
6. Deploy Cisco Secure Client with Umbrella on user devices in the organization.
    - Download Cisco Secure Client
    - Download the OrgInfo.json File
    - Install the Cisco Secure Client

Test Your Connectivity

Provides instructions for testing connectivity after setup by checking access to internet resources protected by Secure Access China. for administrators to review.

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

Quickstart – Browser with SAML Authentication

Describes Quickstart – Browser with SAML Authentication in Cisco Secure Access China. This Quickstart guide describes how to connect user devices securely to internet resources from a browser.

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 Web profile. Users are members of the organization that manages their devices.

Prerequisites

Lists the prerequisites for quickstart browser and saml, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for quickstart browser and SAML. Provision users and groups in Secure Access China. For more information, see Manage Users and Groups.

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

Test Your Connectivity

Provides instructions for testing connectivity after setup by checking access to internet resources protected by Secure Access China. for administrators to review.

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

Prerequisites

Lists the prerequisites for quickstarts secure access. Sign in to Secure Access China with single sign-on (SSO) authentication. For more information, see Sign Into Secure Access China with Security Cloud Sign On.

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

Limitations and Range Limits

Describes Limitations and Range Limits in Cisco Secure Access China. Secure Access China sets limitations by component and defines the amount of time that your data is available on our system.

Secure Access China 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 China.

Limitations Due to Regulatory and Data Access Restrictions in China

Describes limitations Due to Regulatory and Data Access Restrictions in China. Cisco Secure Access China has been customized to align with local restrictions and regulations. As such, the security enforcement in this product may be subject to certain limitations and is not identical to other Secure Access China instances.

- Cisco Secure Access China has been customized to align with local restrictions and regulations. As such, the security enforcement in this product may be subject to certain limitations and is not identical to other Secure Access China instances.
- Due to government restrictions, some disputes cannot be resolved because necessary data from customer environments will not be available.
- Disputes and categorization efforts requiring access to sites outside of China will not be resolved.
- Domestic Internet Service Providers (ISPs) in China implement Internet Content Provider (ICP) filtering to ensure that only domains and websites with valid ICP registrations are accessible over the public Internet, in accordance with Chinese regulations. For roaming users, enabling the Roaming Security Module allows access to ICP-registered destinations and enables customers to enforce their security policies. However, domains without ICP registration will likely continue to be blocked by the ISP's filtering system.

Cisco Secure Client

Describes Cisco Secure Client. Cisco Secure Access China applies private application configuration changes to the Cisco Secure Client every 30 minutes.

- Cisco Secure Access China applies private application configuration changes to the Cisco Secure Client every 30 minutes.
- Cisco Secure Access China excludes entitlement to the Secure Client Network Availability Module (both on-prem and cloud versions). Therefore, admins must not enable it.
- Customers must opt-out of the Customer Experience Feedback module to prevent their data from being exported outside of China. Failure to opt-out will result in customer data being exported outside of China. For more information, see Configure Customer Experience Feedback.

Data Retention

Summarizes data retention periods for DNS, web proxy, and firewall logs, including the 30-day retention period stated for these Secure Access China logs.

- Web proxy, firewall logs–Data retained for 30 days.

Internet Protocol Versions

Describes the internet protocol versions used for network destinations and explains their role in configuring Secure Access China connections. for administrators to review.

Feature	Limit
IPv4	Supported by all services.

Reports

Lists the reports available in Secure Access China, including Admin Audit Log, Total Requests, Top Destinations, Top Categories, and activity 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.

Users and Groups

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

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

Network Requirements for Secure Access China

Describes Network Requirements for Secure Access China. This document describes the network configurations that support connections to the Cisco Secure Access cloud services and other Secure Access services and applications.

This document describes the network configurations that support connections to the Cisco 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.

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:

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

Cisco Secure Client and Device Host Names

Describes Cisco Secure Client and Device Host Names. The Cisco Secure Client Umbrella Roaming Security module uses hostnames to register the device in Secure Access China. 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 China. 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 TLS 1.0 and TLS 1.1 protocols contain security vulnerabilities and do not support modern cryptographic algorithms.

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

Describes 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.

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

Explains that the Cisco Secure Client Umbrella Roaming Security module for macOS uses TLS 1.2 and describes the module?s transport security support.

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

Secure Access Secure Web Gateway Services

Provides instructions for securing 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 modules.

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

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 in your firewalls on ports 80 and 443 over TCP.

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

The following table contains the regional ingress IP addresses for the Secure Access Secure Web Gateway.

Region	IP Address
North	140.179.64.66
North	43.196.1.118
North	52.80.184.186
North	71.132.36.207

Secure Access SaaS Tenants

Provides instructions for securing 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 uses HTTPS to communicate with the Secure Web Gateway proxy services.

Microsoft 365

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

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

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

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

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

- 52.73.52.135
- 52.71.142.118
- 52.40.204.69
- 52.35.119.173
- 52.27.150.153

Secure Access SAML Gateway Services

Provides instructions for securing access saml gateway services. Required by Cisco Secure Client deployments with the Umbrella Roaming Security and Secure Access China integrations with SAML identity providers (IdPs).

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

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

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

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

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

Active Directory Federation Service SAML Identity Provider

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

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

Secure Access SAML Identity Provider Domains

Provides instructions for securing access saml identity provider domains. Required by Cisco Secure Client deployments with the Umbrella Roaming Security modules, and Secure Access China integrations with SAML identity providers (IdPs).

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

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

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

Azure AD SAML Identity Provider

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

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

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

Domain	Port/Protocol
msftauth.net	80/443 TCP

Secure Access SAML Gateway Client Certificate Revocation Services

Provides instructions for securing access saml gateway client certificate revocation services. Required by Cisco Secure Client deployments with the Umbrella Roaming Security modules, and Secure Access China integrations with SAML identity providers (IdPs).

Required by Cisco Secure Client deployments with the Umbrella Roaming Security modules, and Secure Access China 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

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

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

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

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

Secure Access VPN Client Certificate Revocation Services

Provides instructions for securing access vpn client certificate revocation services. Required by Cisco Secure Client deployments with the Virtual Private Network (VPN) module.

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

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

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

Manage Network Connections

Provides instructions for managing network Connections in Cisco Secure Access China. 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.

IPsec Network Tunnels

Describes iPsec Network Tunnels. User devices can read, write, and update private resources by setting up virtual private networks (VPNs) connections to Secure Access China through IPsec network tunnels.

Secure Access China 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 (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) 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) connections to Secure Access China through IPsec network tunnels.

Network Tunnels (Deployed in Network Tunnel Groups)

Describes network Tunnels (Deployed in Network Tunnel Groups). Characteristics of network tunnel groups:. You may be able to use existing infrastructure, without deploying additional devices.

Characteristics of network tunnel groups:

- Can route internet-bound traffic as well as traffic to private resources.
- Support VPN and branch-to-branch 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 China 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.

3 Manage Network Tunnel Groups

Topics:

- Manage Network Tunnel Groups

Provides an overview of Manage Network Tunnel Groups in Cisco Secure Access China, including Device Compatibility and Network Tunnels, Add a Network Tunnel Group, and View Network Tunnel Group Details. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Network Tunnel Groups

Provides instructions for managing network Tunnel Groups in Cisco Secure Access China. Tunnels and tunnel groups are core concepts in managing connections between your data centers and Cisco Secure Access China.

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

- Secure Access China 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) connections to Secure Access China 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 in Cisco Secure Access China. Secure Access China connects and secures traffic from IPsec tunnels established by various network devices.

Secure Access China 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 China.

IPsec Tunnel Requirements

Describes iPsec Tunnel Requirements. IPsec tunnels for Secure Access China must have an MTU that is no larger than 1280 bytes. Secure Access China automatically clamps the TCP MSS to 1240 or below.

IPsec tunnels for Secure Access China must have an MTU that is no larger than 1280 bytes. Secure Access China automatically clamps the TCP MSS to 1240 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 China, see the tunnel configuration topics found in Network Tunnel Configuration.

Supported Devices for Setting Up IPsec Tunnels

Describes supported Devices for Setting Up IPsec Tunnels. * Configure Tunnels with Meraki MX. * Configure Tunnels with Cisco ISR.

Secure Access China 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 China.

Platform	Software Version
Cisco Meraki MX *Configure Tunnels with Meraki MX	15.3
Cisco ISR-G2 * Configure Tunnels with Cisco ISR	15.4M3
Cisco ASA * Configure Tunnels with Cisco Adaptive Security Appliance (ASA)	Cisco ASA v9.8

Platform	Software Version
Cisco FTD	6.4+ (6.7 when using VTI)

* Configure Tunnels with Cisco Secure Firewall

Add a Network Tunnel Group

Provides instructions for adding a Network Tunnel Group in Cisco Secure Access China. To enable tunnel redundancy and high availability for IPsec tunnels connected to data center hubs, follow the steps to add a network tunnel group to Cisco Secure Access China.

To enable tunnel redundancy and high availability for IPsec tunnels connected to data center hubs, follow the steps to add a network tunnel group to Cisco Secure Access China.

Provisioning high-availability network tunnel groups at a hub site allows a group of tunnels to share a primary and secondary hub. Network devices that are capable of establishing an IPsec tunnel can join a network tunnel group using the credentials created when the tunnel group is deployed.

1. In Secure Access China, configure the attributes of the tunnel group and deploy the tunnel group. Once the tunnel group is deployed, the initial state of the tunnel group changes from **Unestablished** to **Inactive**.
2. Next, configure a tunnel in the network device that sends traffic to Secure Access China. Use the deployed tunnel group's attributes to associate the network tunnel to the tunnel group. The network tunnel group attributes required by network devices to establish the IPsec IKEv2 tunnel are: tunnel ID, tunnel passphrase, and IP Address of the Secure Access data center.
3. Enable user computers to connect securely to the tunnel and begin to send traffic to Secure Access China. Once Secure Access China receives and logs traffic from a network tunnel, the tunnel state is considered **Active**. View the events for the tunnel in the Secure Access China Overview and Activity Search.

Prerequisites

Lists the prerequisites for adding network tunnel group. Full Admin role in Secure Access China. For more information, see Manage Accounts.

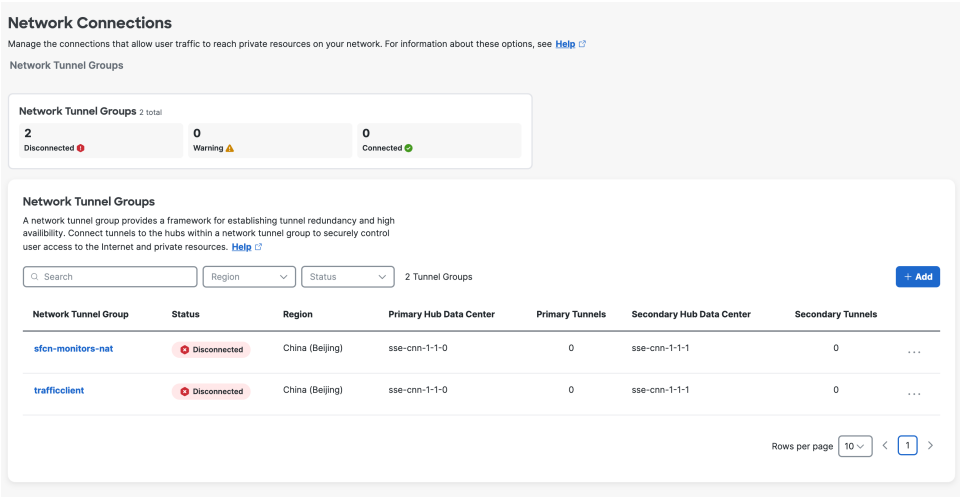
- Full Admin role in Secure Access China. For more information, see Manage Accounts.

Procedure

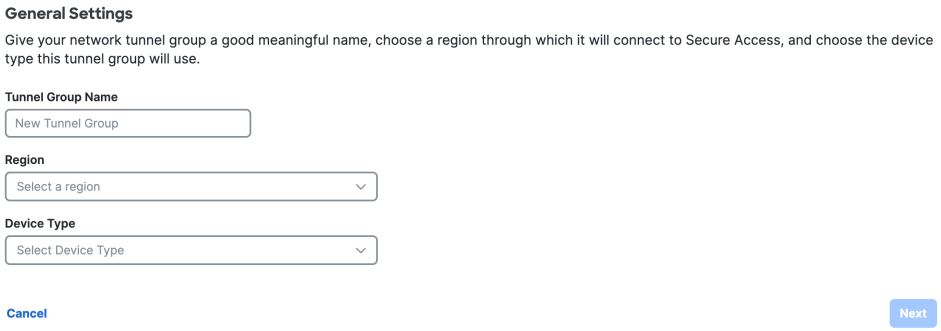
Provides instructions for adding network tunnel group. Add a network tunnel in Secure Access China for a device capable of establishing an IPsec IKEv2 tunnel.

Add a network tunnel in Secure Access China for a device capable of establishing an IPsec IKEv2 tunnel.

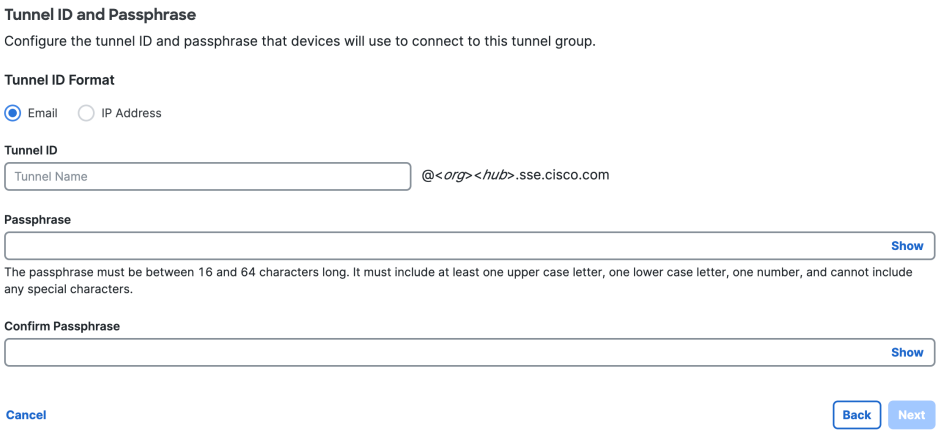
1. Navigate to **Connect > Network Connections > Network Tunnel Groups**.
2. Click **Add**.



3. Enter the **General Settings** for your tunnel group:
   a. Give your tunnel group a meaningful name.
   b. Choose a **Region**.
   c. Choose a **Device Type**.
   d. Click **Next**.

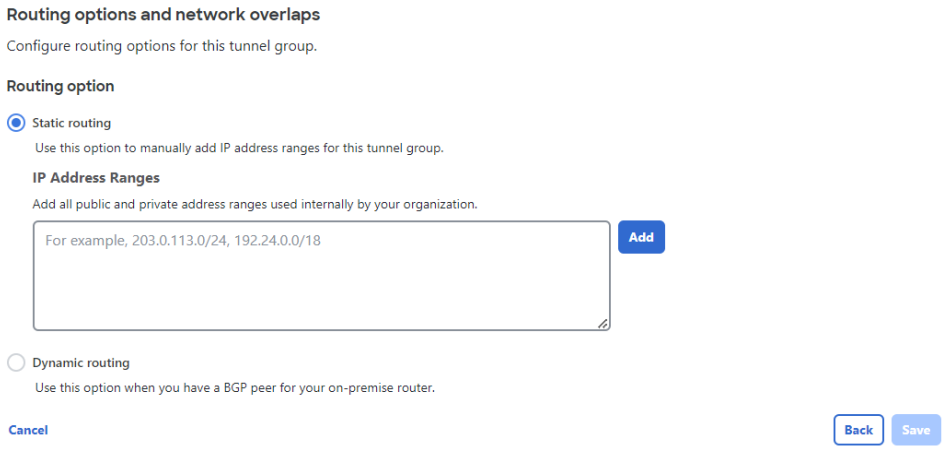


4. Enter the **Tunnel ID and Passphrase** for your tunnel group:
   a. Choose a **Tunnel ID Format**, either **Email** or **IP Address**. This field appears based on the **Device Type** chosen in the General Settings.
      - If the choice is email, use the format @.sse.cisco.com. Use the name you gave the tunnel group in **General Settings**.
      - If the choice is IP address, include both a primary and secondary IP address.
   b. Enter a **Passphrase**.
      - A tunnel passphrase is 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.
   c. Reenter your passphrase.
   d. Click **Next**.



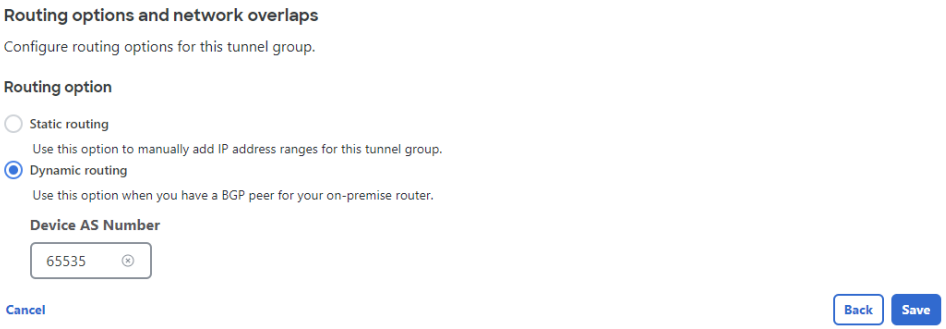
5. Choose the type of **Routing** for your tunnel group.

   a. Choose Static routing to manually add IP 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.

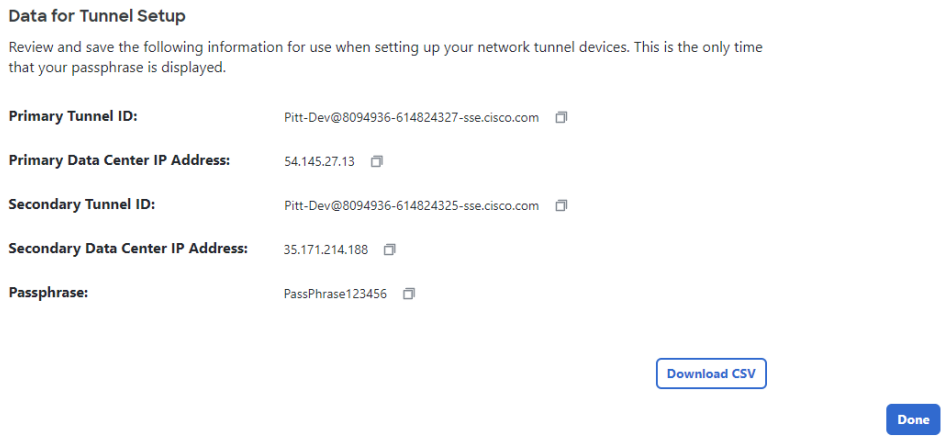
> **Note**
>
> You'll need the router's autonomous system (AS) number to use dynamic routing.



   c. Click **Next**.

6. On the **Data for Tunnel Setup** page, review the network tunnel information for completeness. Click the **Download CSV** button to save the information to use to configure and deploy a tunnel in a network device.

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



Configure Tunnel on Network Device

Provides instructions for configuring tunnel on network device. Follow the steps in one of the network device guides to deploy an IPsec tunnel with Secure Access China. For more information see Network Tunnel Configuration.

1. Follow the steps in one of the network device guides to deploy an IPsec tunnel with Secure Access China. For more information see Network Tunnel Configuration.

Verify Tunnel Traffic in Secure Access China

Provides instructions for verifying tunnel traffic in Secure Access China. After you add a tunnel to Cisco Secure Access and deploy a network tunnel with a compatible network device, check that Secure Access receives and logs traffic from the tunnel.

After you add a tunnel to Cisco Secure Access and deploy a network tunnel with a compatible network device, check that Secure Access receives and logs traffic from the tunnel.

1. Navigate to **Overview** and find your configured tunnel. Verify that the status of the tunnel is **Active**. For more information, see Secure Access China Overview.

View Network Tunnel Group Details

Provides instructions for viewing network Tunnel Group Details in Cisco Secure Access China. Once a network tunnel group is added to Cisco Secure Access China, you can view the configuration attributes of a deployed tunnel group.

Once a network tunnel group is added to Cisco Secure Access China, 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 China also lists the status of your organization's network tunnels and information about the attributes of the deployed tunnel groups in **Overview > Connectivity**.

Prerequisites

Lists the prerequisites for viewing network tunnel group details. A minimum role of Read Only in Secure Access China. For more information, For more information, see Manage Accounts.

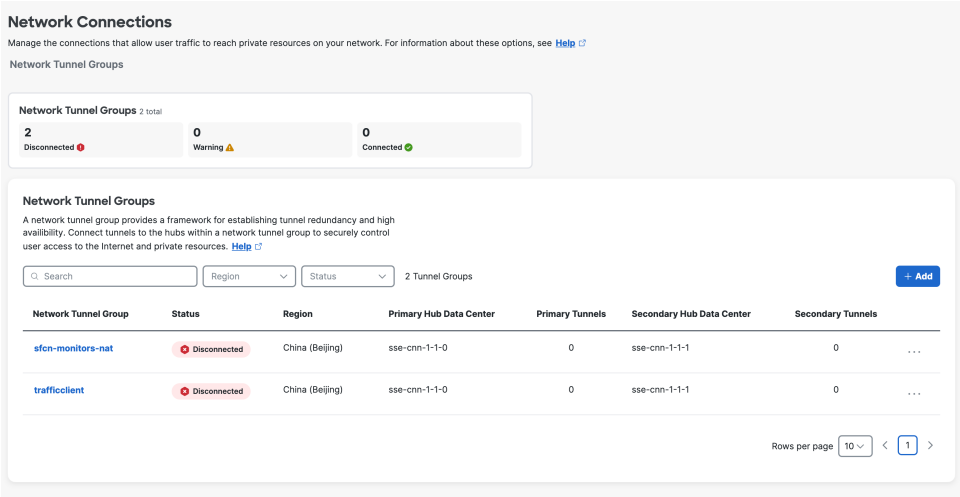
- A minimum role of Read Only in Secure Access China. For more information, For more information, see Manage Accounts.

Procedure

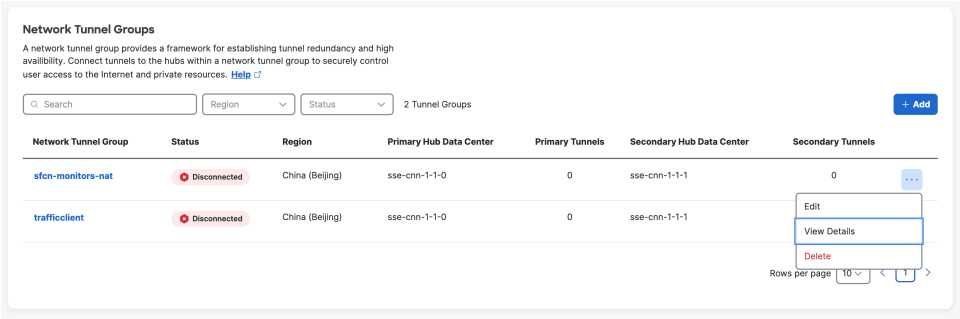
Provides instructions for viewing network tunnel group details. View the details of a deployed network tunnel group in Secure Access China.

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

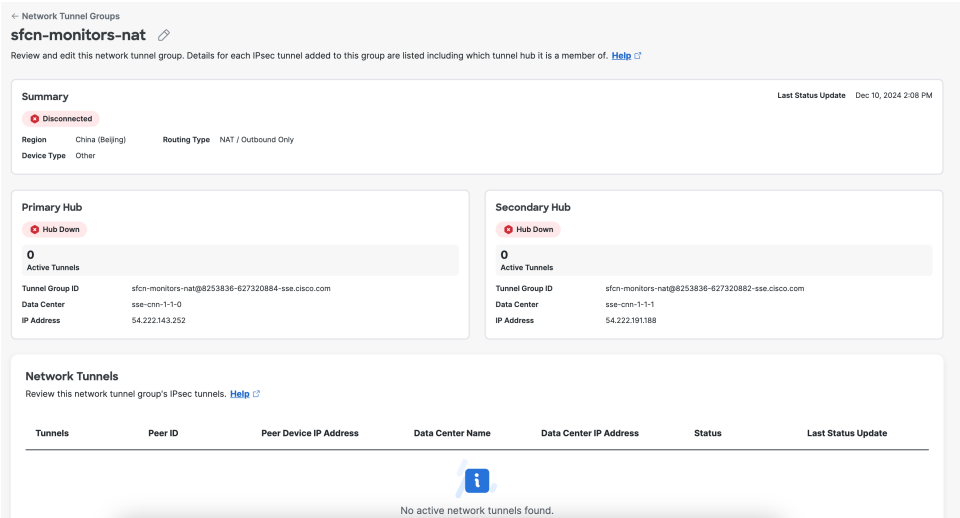
1. Navigate to **Connect > Network Connections > Network Tunnel Groups**.



2. Click the ellipsis (**...**), and then choose **View Details**.



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



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

Edit a Network Tunnel Group

Provides instructions for editing a Network Tunnel Group in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for editing network tunnel group. Full Admin role in Secure Access. For more information, see Manage Accounts.

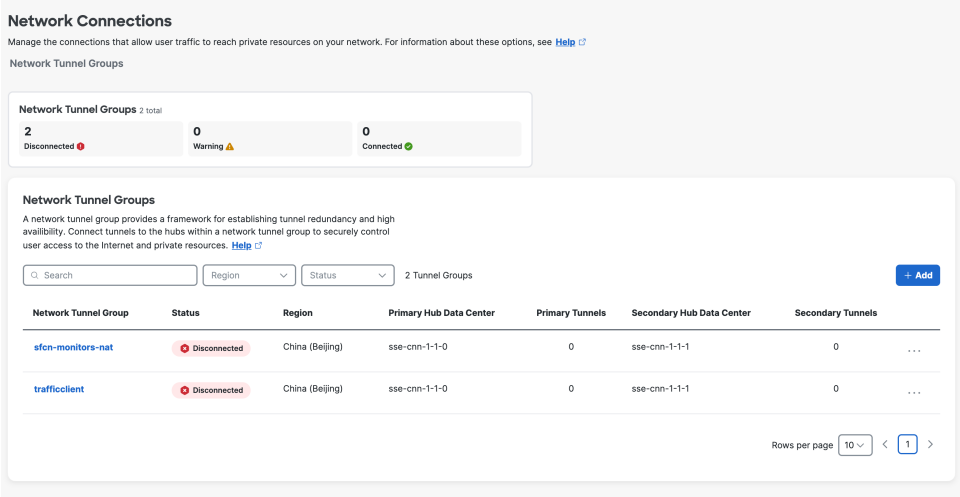
- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

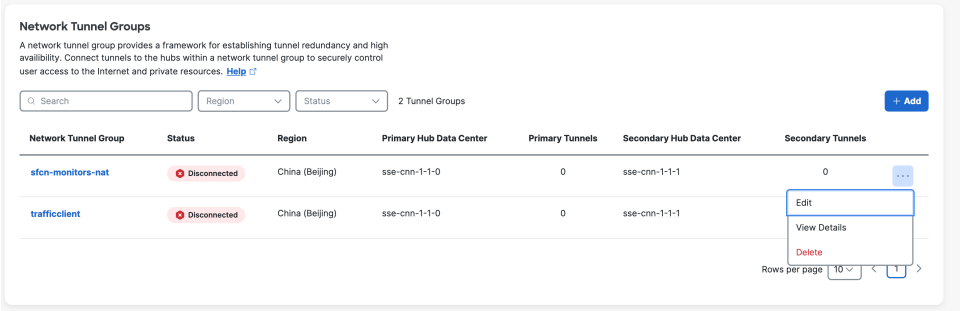
Provides instructions for editing network tunnel group. Edit the configuration attributes of a deployed network tunnel group in Secure Access.

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

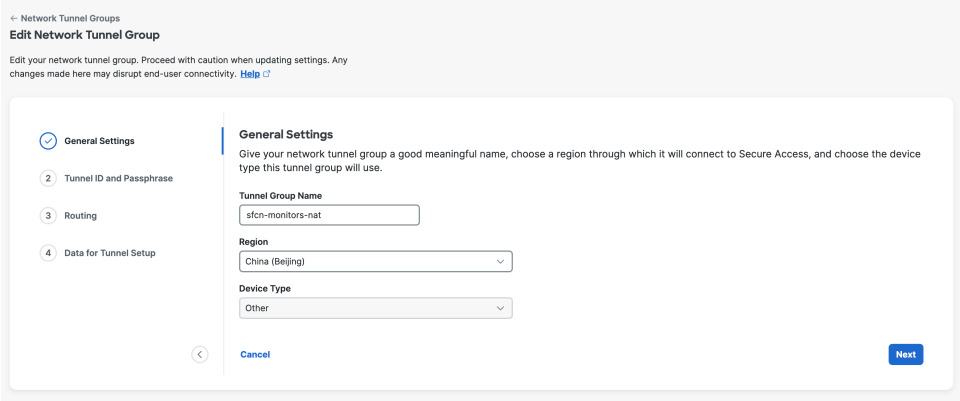
1. Navigate to **Connect > Network Connections** > **Network Tunnel Groups**.



2. Click the ellipsis (**...**), and then choose **Edit**.



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



4. Click **Save**.

Delete a Network Tunnel Group

Provides instructions for deleting a Network Tunnel Group in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for deleting network tunnel group. Full Admin role in Secure Access. For more information, see Manage Accounts.

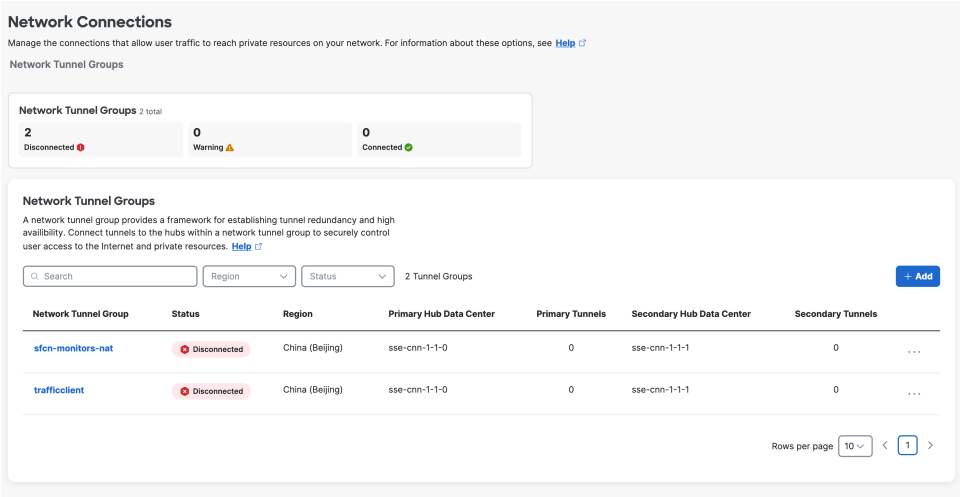
- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

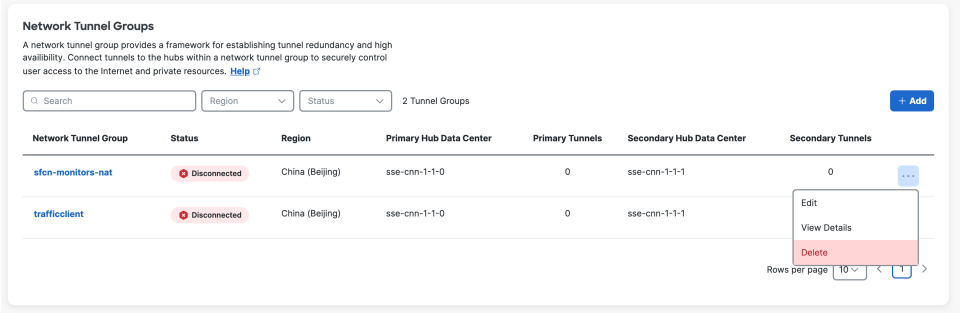
Provides instructions for deleting network tunnel group. Delete a network tunnel group from Secure Access. Navigate to Connect > Network Connections > Network Tunnel Groups.

Delete a network tunnel group from Secure Access.

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



2. Click the ellipsis (**...**), and then choose **Delete**.



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

Supported IPsec Parameters

Describes Supported IPsec Parameters in Cisco Secure Access China. Cisco Secure Access China uses the IPsec protocol for tunneling traffic.

Cisco Secure Access China 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)

Components	IKEv2 (Phase I) (no IKEv1 support)	ESP (Phase II)
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.

4 Network Tunnel Configuration

Topics:

- Network Tunnel Configuration

Provides an overview of Network Tunnel Configuration in Cisco Secure Access China, including Configure Tunnels with Catalyst SD-WAN cEdge and vEdge, Configure Tunnels with Cisco ISR, and Configure Tunnels with Cisco Adaptive Security Appliance. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Network Tunnel Configuration

Describes Network Tunnel Configuration in Cisco Secure Access China. You can establish an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel from a network device deployed in your environment to Cisco Secure Access.

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

Configure Tunnels with Catalyst SD-WAN cEdge and vEdge

Provides instructions for configuring tunnels with Catalyst SD-WAN cEdge and vEdge in Cisco Secure Access China. Follow these steps to connect a Cisco IOS XE Catalyst SD-WAN device through an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel to Cisco Secure Access.

Follow these steps to connect a Cisco IOS XE Catalyst SD-WAN device through an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel to Cisco Secure Access.

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

Prerequisites

Lists the prerequisites for configuring tunnels catalyst vedge. If you get a "Not Secure" warning when accessing the link, you can ignore it. When appears, enter your credentials.

- 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.

Step 1: Add a Network Tunnel Group in Secure Access

Describes 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.

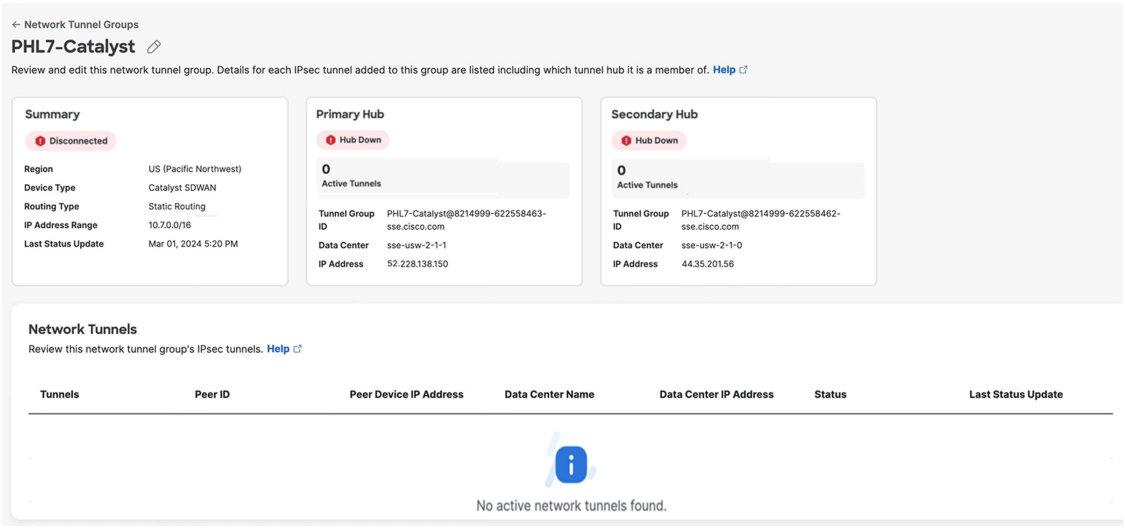
Tunnels and tunnel groups are core concepts in managing connections between your data centers and Cisco Secure Access. A network tunnel group provides the framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control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

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 Catalyst SD-WAN 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.

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



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

Step 2: Configure Cisco Catalyst SD-WAN Templates

Describes step 2: Configure Cisco Catalyst SD-WAN Templates. Configure a Catalyst SD-WAN tunnel to connect a Catalyst SD-WAN device to Cisco Secure Access.

Configure a Catalyst SD-WAN tunnel to connect a Catalyst SD-WAN device to Cisco Secure Access.

In Cisco Catalyst SD-WAN Manager, all the features are configured through templates. Once the Cisco Catalyst SD-WAN devices are registered with Cisco Catalyst SD-WAN Manager, you cannot configure anything through the CLI.

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

In SD-WAN Manager version 20.9, the SIG template is divided into several sections:

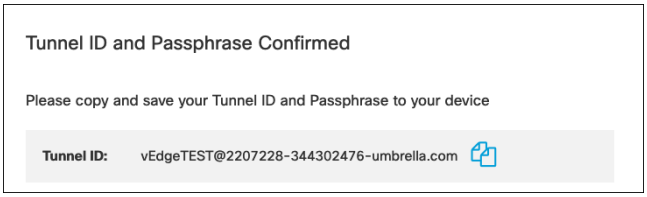
1. Device Type, Template Name, Description, and SIG Provider (Umbrella, Zscaler, or Generic).

> **Note**
>
> In version 20.4/17.4, the only two tunnel types that are offered are Umbrella and Third Party. You can configure Secure Access manual tunnels (IPSec or GRE) using the Third Party option. Starting in 20.5/17.5, the three tunnel types that are offered are Umbrella, Zscaler, and Generic. **To configure IPSec or GRE Secure Access tunnels, choose the Generic option.** You can configure Secure Access manual and automatic tunnels (IPSec or GRE) using the Generic option. Secure Access recommends you use automatic tunnels if available.

2. Tracker: Allows you to configure custom L7 health check tracker information.
3. Configuration: Allows you to specify different tunnel type (IPSec or GRE) and other tunnel characteristics, such as tunnel name, tracker name, tunnel source, whether the tunnel is attached to a primary or secondary data center (which is specified or discovered later) and advanced options, like IP MTU and other tunnel settings.
4. High Availability: Allows you to choose up to 4 active tunnels or 4 active/standby tunnel pairs by choosing the tunnels defined in the Configuration section under the Active or Backup column. You can also modify traffic ratios for the tunnels.
5. Advanced Settings (if applicable): Allows you to define primary or secondary data centers and Secure Access location name if desired, and advanced Secure Access settings (XFF Forwarding, Enable IPS Control, etc).

Define the Feature Template

1. Log into the Cisco Catalyst SD-WAN Manager console and navigate to **Configuration > Templates**.
2. Confirm that the **Feature Templates** tab is selected, then click **Add Template**.
3. Choose the device for which you are creating the template.
4. Under **VPN**, click **Cisco Secure Internet Gateway (SIG)**.
5. Under **Select Services** select device types, then choose **VPN Interface IPSec WAN**.
6. 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.
7. Choose the **Global Attribute** to change any IKE and IPSec defaults:
   a. **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.



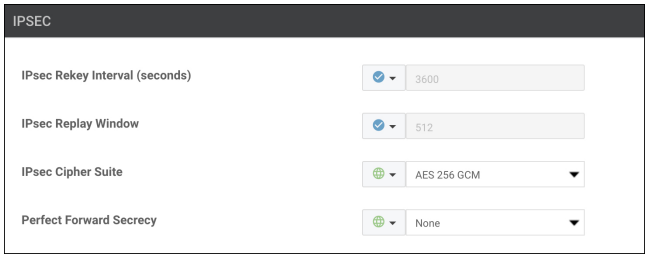
   b. **IPsec Settings**

- 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".

Important

Cipher Suite Encryption

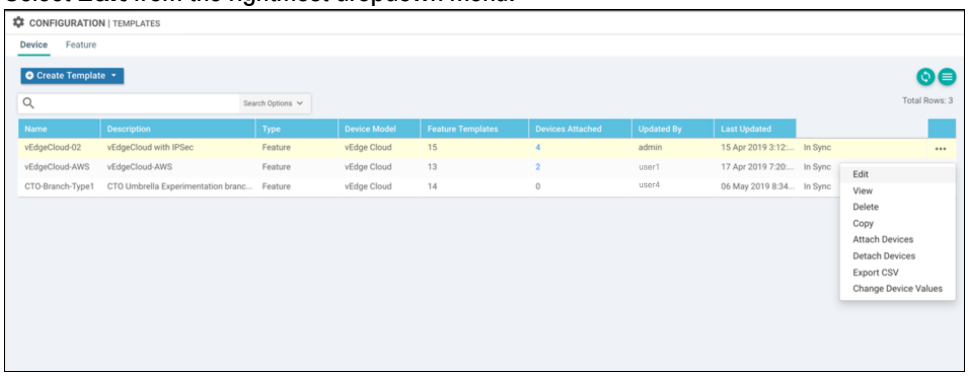
If performance is an issue with the default cipher, both `AES 256 CBC SHA1` and `Null SHA1` are also supported. You can test these to determine whether one offers better performance for a particular platform. Note that `Null SHA1` isn't necessarily faster than the default `AES 256 GCM` because of the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



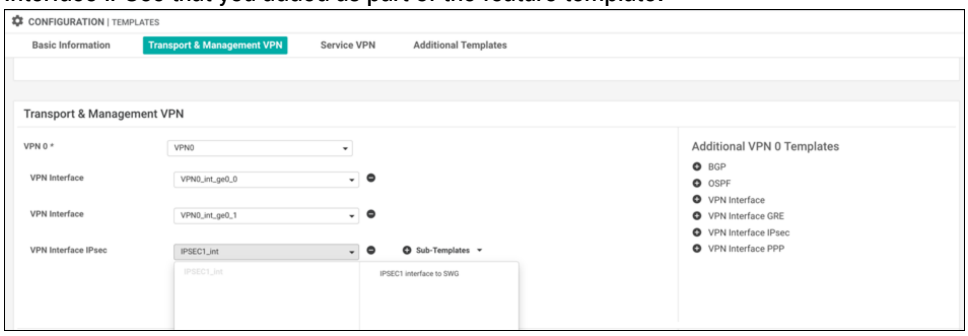
8. Click **Update** to save the configuration template.

Add the IPsec Interface Template

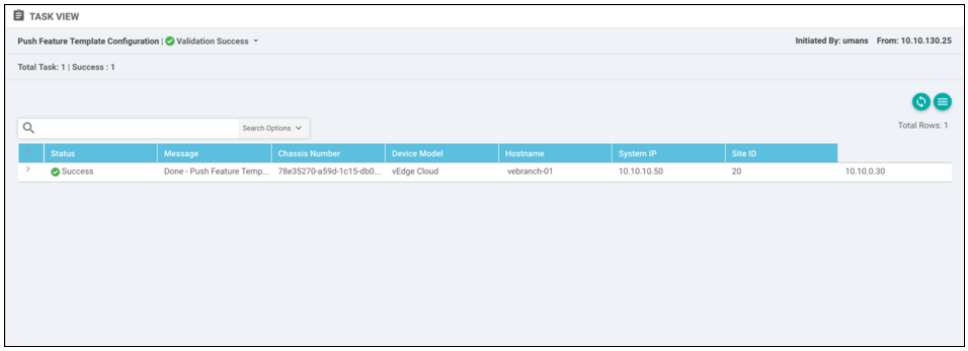
1. Navigate to **Configuration > Templates > Device** and then choose the device template for the CDFW tunnel.
2. Select **Edit** from the rightmost dropdown menu.



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.

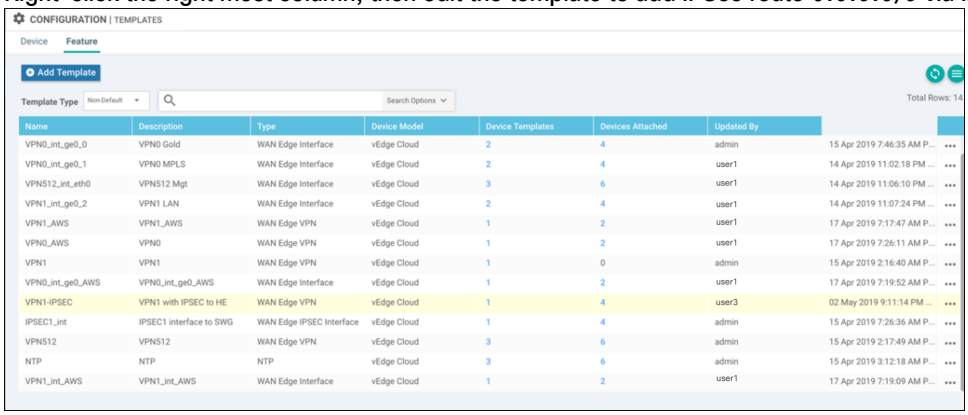


Configure Static Routes

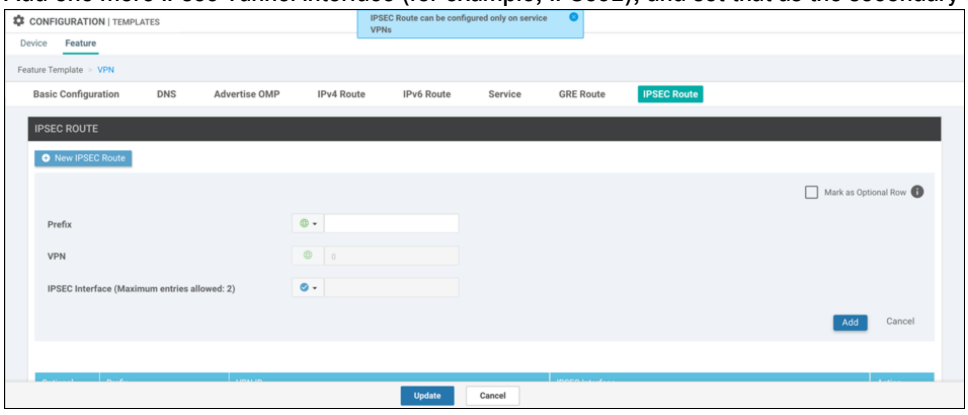
Provides instructions for configuring static routes. After configuring a template, you need to add static routes from the service VPN to redirect the traffic through the IPSec tunnel to CDFW headend.

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.

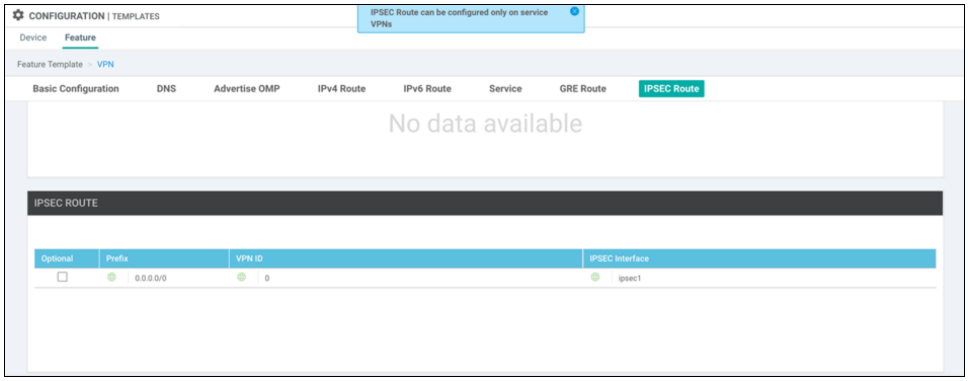
1. Navigate to **Configuration > Templates > Feature**.
2. Right-click the right most column, then edit the template to add *IPSec route 0.0.0.0/0 via IPSec1 Tunnel interface*.



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

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**.

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

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

     IF                                SOURCE                DEST                                                                                                TUNNEL
VPN  NAME    VERSION  SOURCE IP       PORT  DEST IP         PORT  INITIATOR SPI     RESPONDER SPI     CIPHER SUITE     DH GROUP        STATE           UPTIME      UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------------------------
0    ipsec3  2        173.37.56.164   4500  146.112.67.2    4500  f86fffc5e81d3c06  9fbdcdcfb30e72d4  aes256-cbc-sha1  14 (MODP-2048)  IKE_UP_IPSEC_UP  0:00:00:00  0:00:00:06
```

Configure Tunnels with Cisco ISR

Provides instructions for configuring tunnels with Cisco ISR in Cisco Secure Access China. 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

Lists the prerequisites for configuring tunnels Cisco ISR. The following prerequisites must be met for the tunnel to work successfully.

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

Licensing and Hardware

- 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

- 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. 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.

1. Follow the steps in Add Network Tunnel Group.

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

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.

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 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 146.112.0.0
  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 SFCN. 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

Provides instructions for testing the completed Secure Access China configuration and confirming that its configured services operate as expected. for administrators to review.

Check Tunnel Status

Provides instructions for checking tunnel status. Use the following command to verify the tunnel status on your ISR. show crypto session detail.

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

```
show crypto session detail
```

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, 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

Provides instructions for 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 Adaptive Security Appliance

Provides instructions for configuring tunnels with Cisco Adaptive Security Appliance in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for configuring tunnels Cisco asa. You must meet licensing, hardware, and network access prerequisites for the tunnel to work successfully.

You must meet licensing, hardware, and network access prerequisites 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.
- 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. 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:.

- 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. 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.

1. Follow the steps in Add Network Tunnel Group.

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

Configure ASA

Provides instructions for configuring asa. Validate that the command crypto isakmp identity is set to the default value " auto " to determine the correct ID Method for ISAKMP Peers.

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]
```

Important

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.

```
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
```

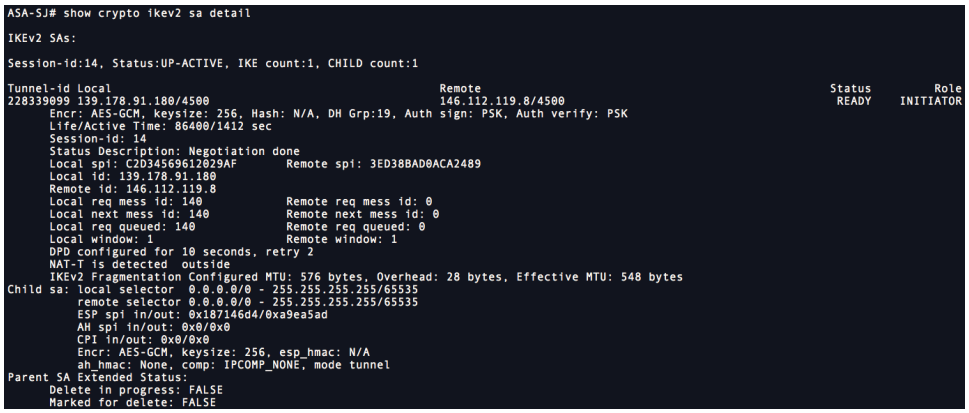
Test and Verify

Provides instructions for testing and verify. 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 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 Cisco Secure Firewall

Provides instructions for configuring tunnels with Cisco Secure Firewall in Cisco Secure Access China. Cisco Secure Firewall is a family of threat-focused next-generation firewalls.

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

Provides instructions for configuring firepower policy-based vpn. The Firepower configuration process consists of the following steps. To start at its IP address or FQDN; for example, https://FMC_IP_OR_FQDN.

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

Provides instructions for 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

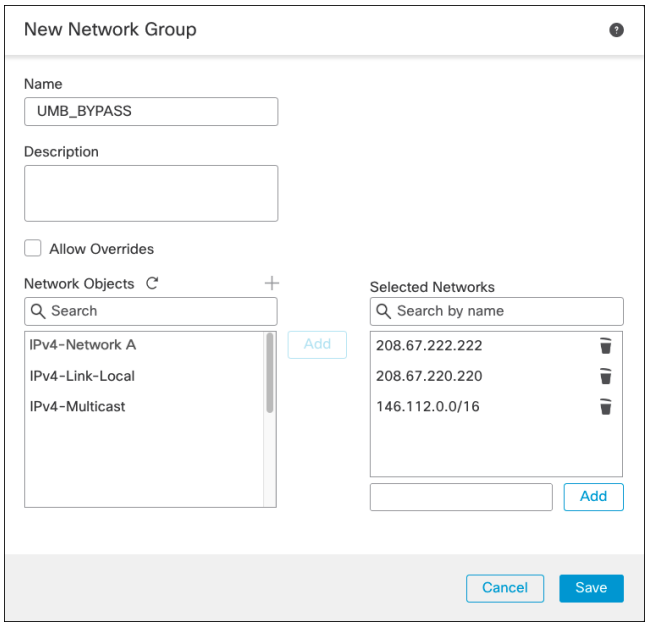
Provides instructions for adding network object. Navigate to Objects > Object Management > Network > Add Network > Add Group.

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.

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.



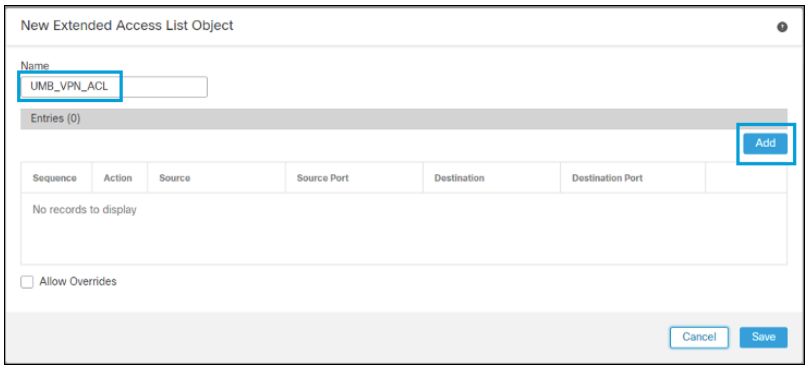
3. Optionally, add 146.112.0.0/16 as a network. Web traffic from endpoints with PAC file or Cisco Secure Client as well as proxy chaining traffic can then go outside the IPSec tunnel and achieve higher throughput.

Add Traffic Selector ACL

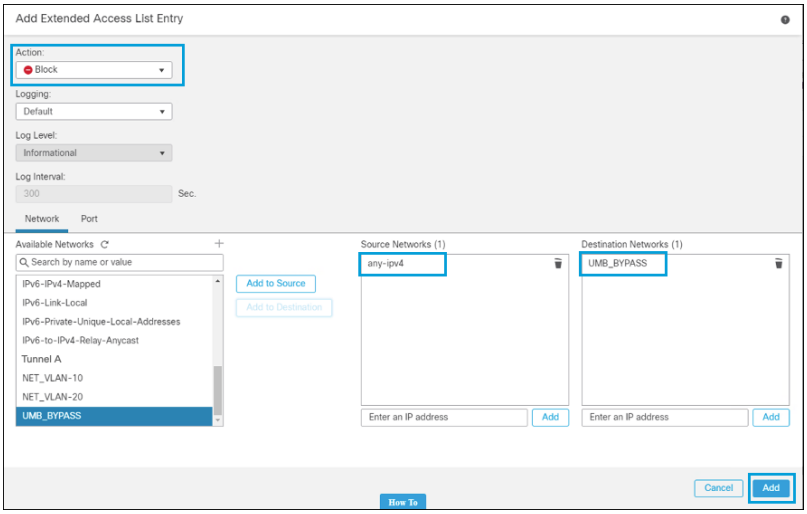
Provides instructions for adding traffic selector acl. This ACL is used in the IKEv2 security association negotiation as well as when Firepower makes decisions about when to encrypt traffic. It does not encrypt traffic denied in the ACL when the deny statement comes before the permit statement.

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.

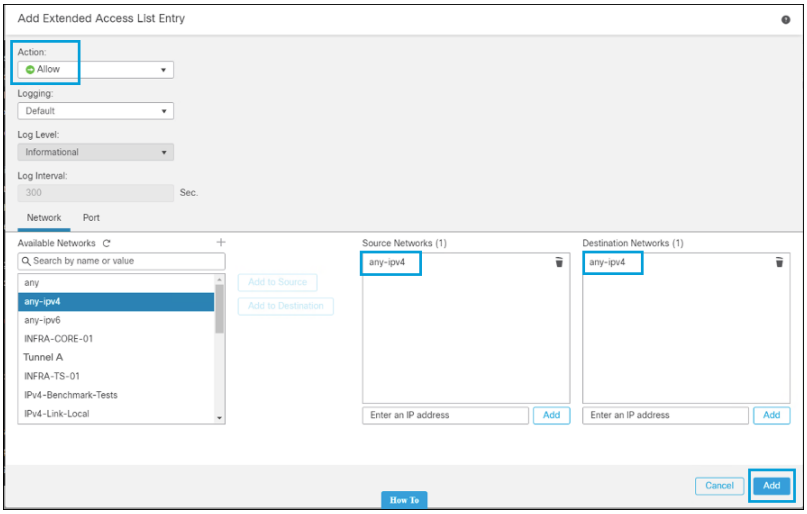
1. Navigate to **Objects > Object Management > Access List > Extended > Add Extended Access List**.
2. Enter a name for the ACL and then click **Add** to add the Access Control Entries (ACE).



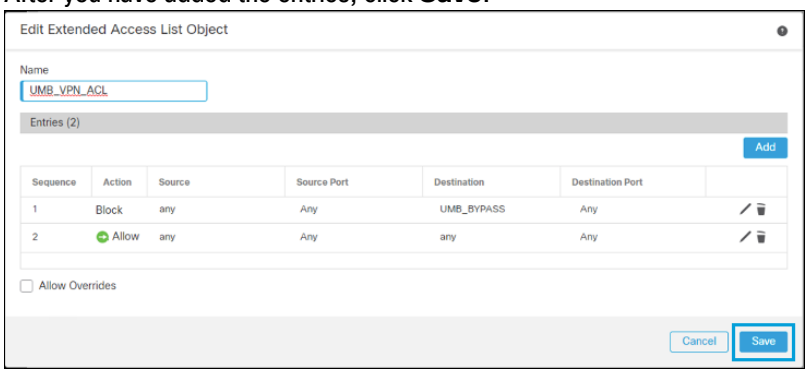
   a. The first entry denies traffic to the network object type group containing the Secure Access resolvers. Optionally, traffic to the `146.112.0.0/16` and `155.190.0.0/16` subnets can also be denied.



   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**.

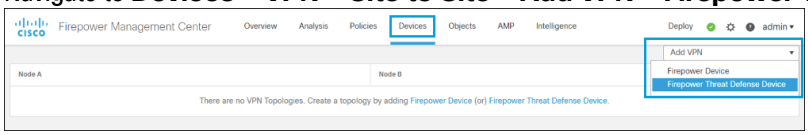


Configure Site-to-Site VPN

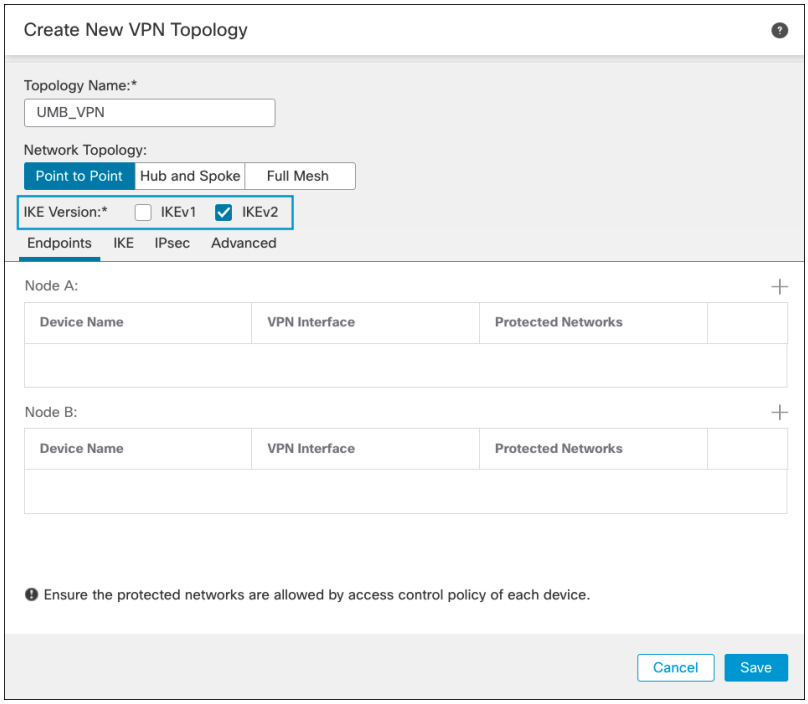
Provides instructions for configuring site-to-site vpn. You can now configure the site-to-site VPN. Enter a name for the topology. Check IKEv2 box (Secure Access supports IKEv2 only). For more information about supported protocols, see Supported IPSec Parameters.

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

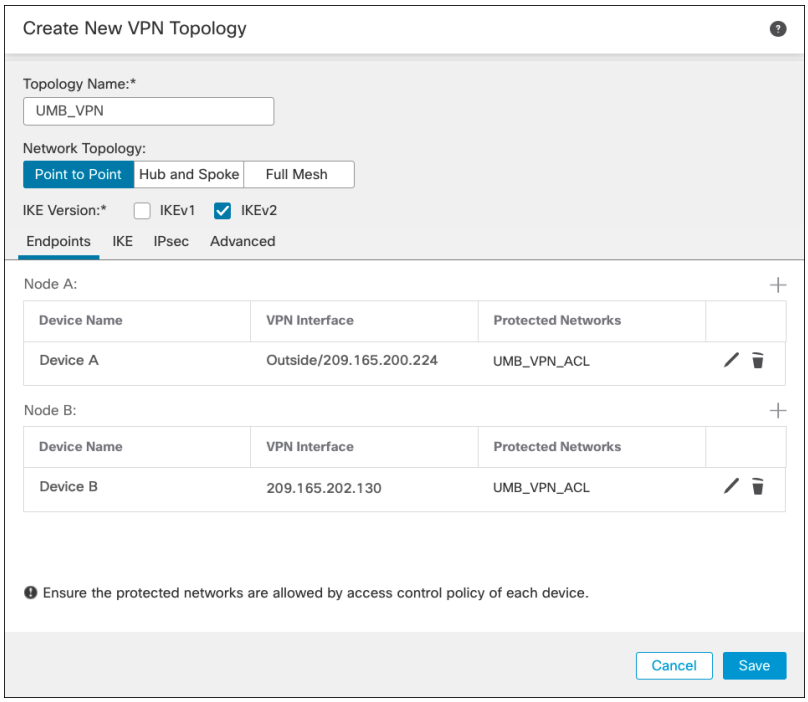
1. Navigate to **Devices > VPN > Site to Site > Add VPN > Firepower Threat Defense Device**.



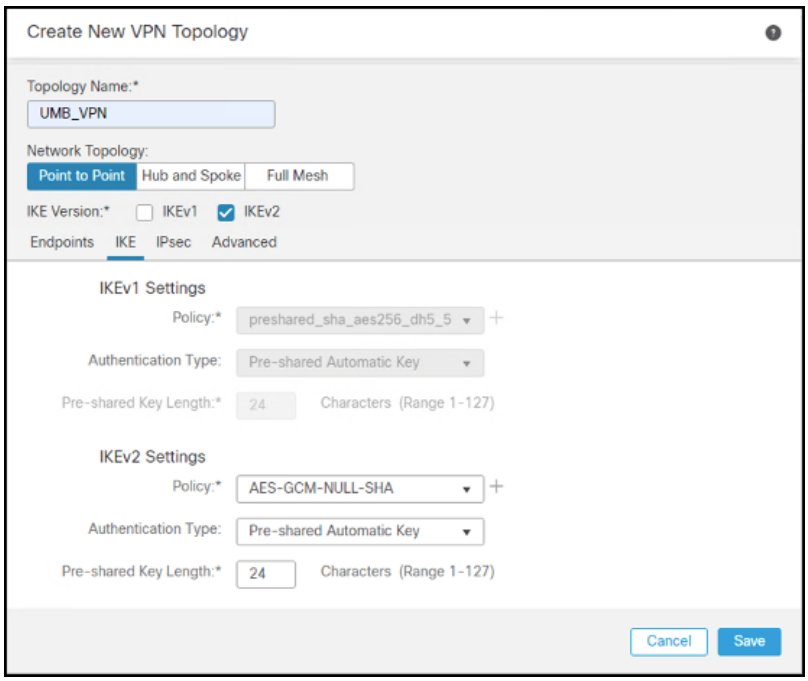
2. Enter a name for the topology. Check IKEv2 box (Secure Access supports IKEv2 only). For more information about supported protocols, see Supported IPSec Parameters.



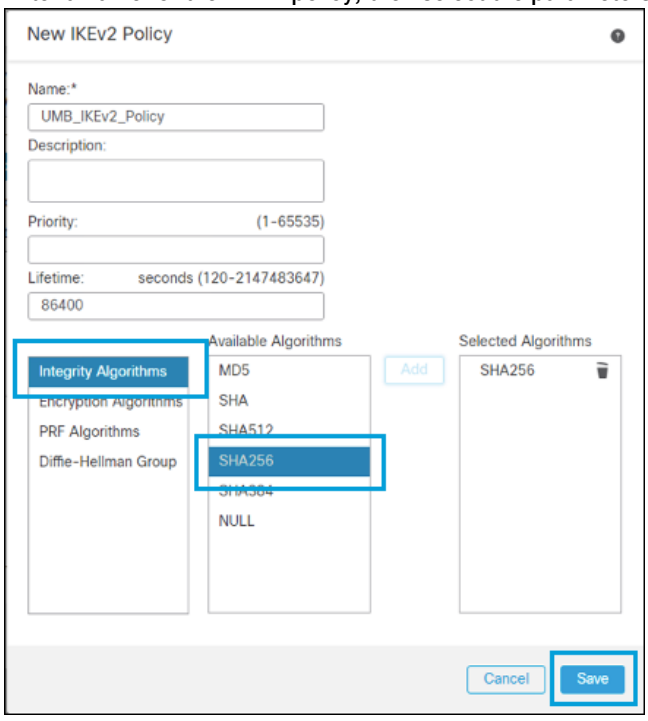
3. Add two peers: the local peer (FTD device) and the remote peer (Secure Access).
   a. Click **Add** for Node A and select the FTD device as the local peer and the interface sourcing the IPSec connection. The IP address is automatically populated.
   b. Under **Protected Networks**, select **Access 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**.



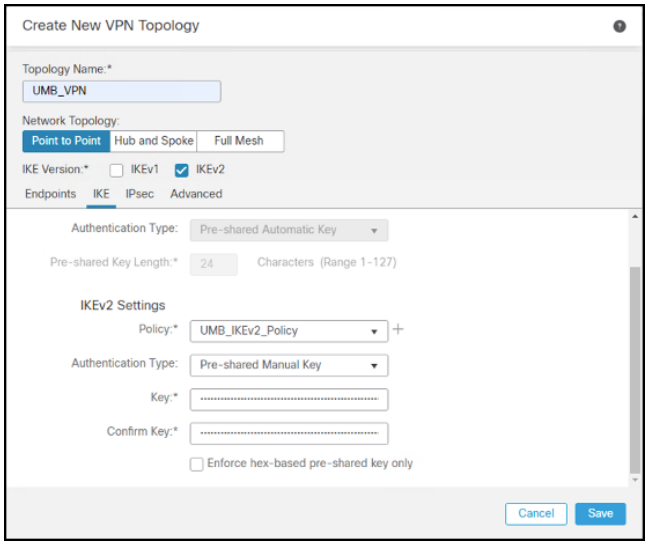
4. Click the **IKE** tab to add a new IKEv2 Policy containing the desired crypto algorithms. For more information about encryption supported by Secure Access, see Supported IPsec Parameters.



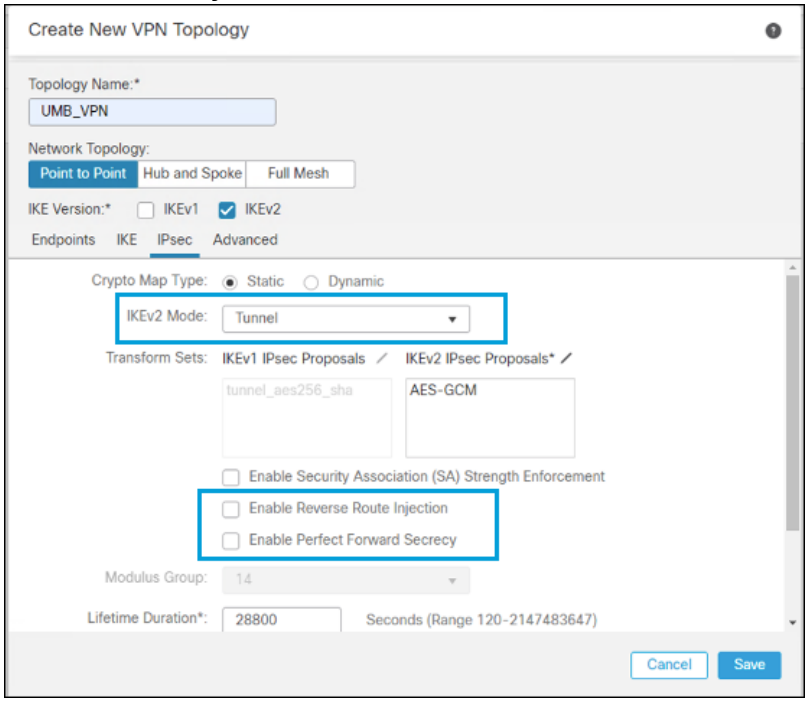
5. Enter a name for the IKEv2 policy, then select the parameters from the Supported IPsec Parameters.



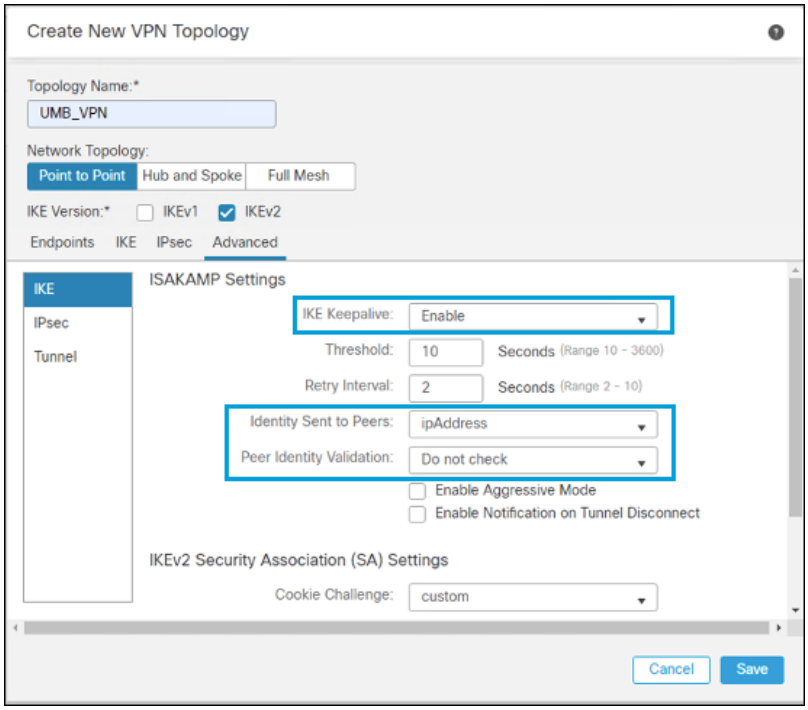
6. After saving the IKEv2 Policy, select it. Choose **Pre-shared Manual Key** from the **Authentication** drop-down menu and enter the key.



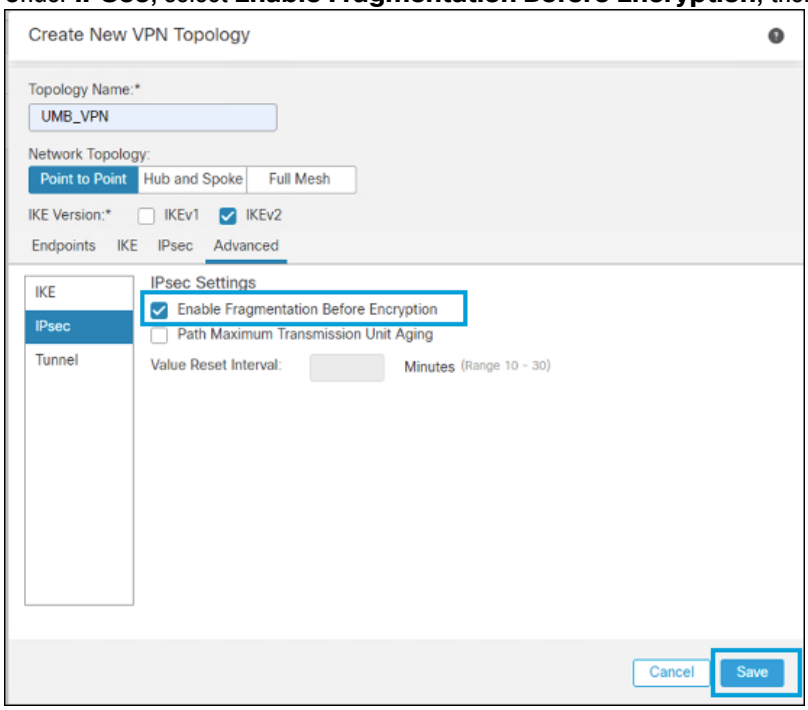
7. Under **IPSec Configuration**, add a new **IKEv2 IPsec Proposal** with your crypto algorithms or select an existing profile. Select **Tunnel** for **IKEv2 Mode** and uncheck **Enable Reverse Route Injection** and **Enable Perfect Forward Secrecy**.



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

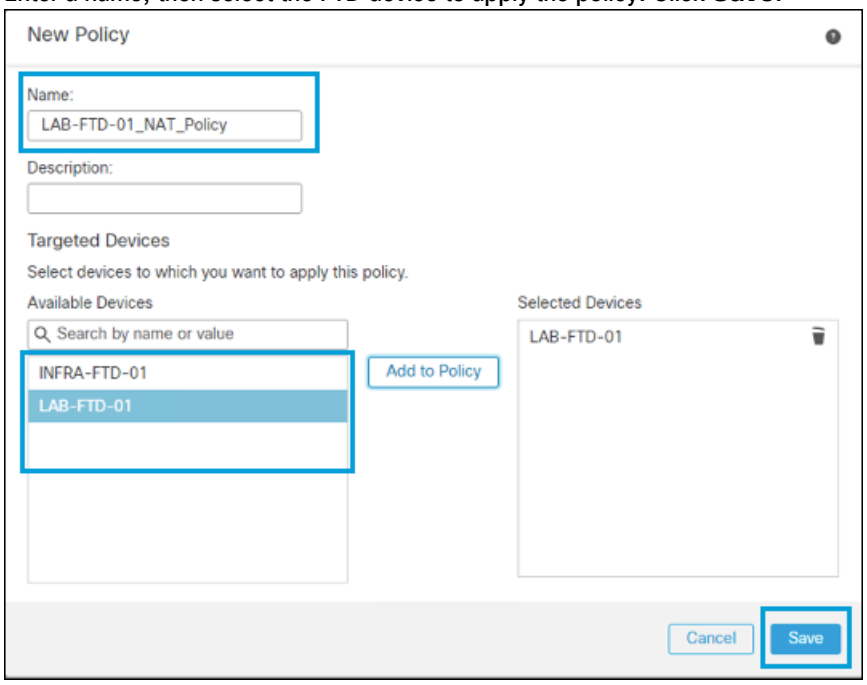
Provides instructions for configuring nat policy. This ensures that IP address only when the destination is the network object containing the resolver's IP address. Other destinations do not match the NAT statement.

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.

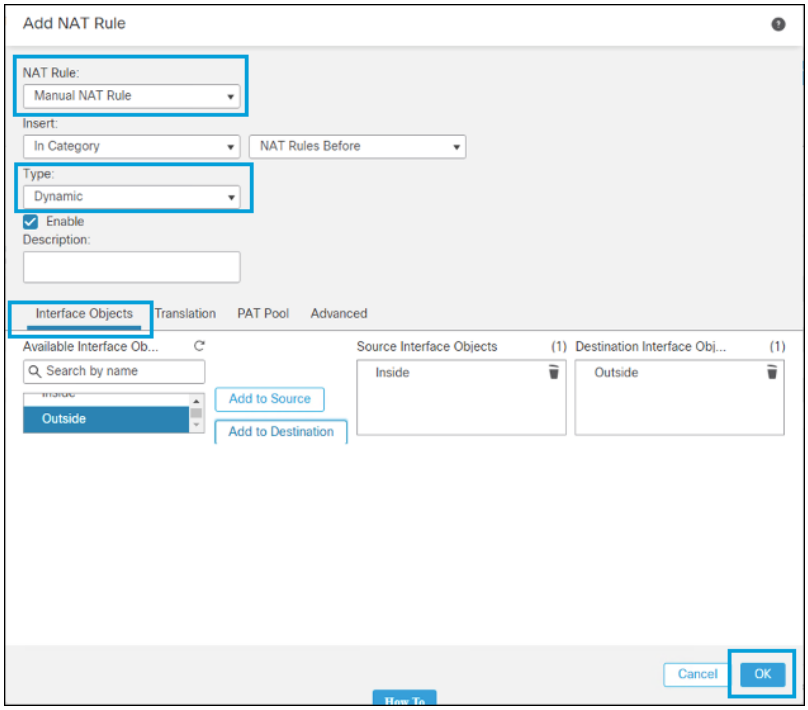
If you use the public IP in your internal network, you must NAT the traffic to a private IP address pool before sending the traffic to Secure Access, as most of the traffic goes through the Secure Access IPSec tunnel. It is easier to create NAT for the traffic not going through the tunnel and use no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

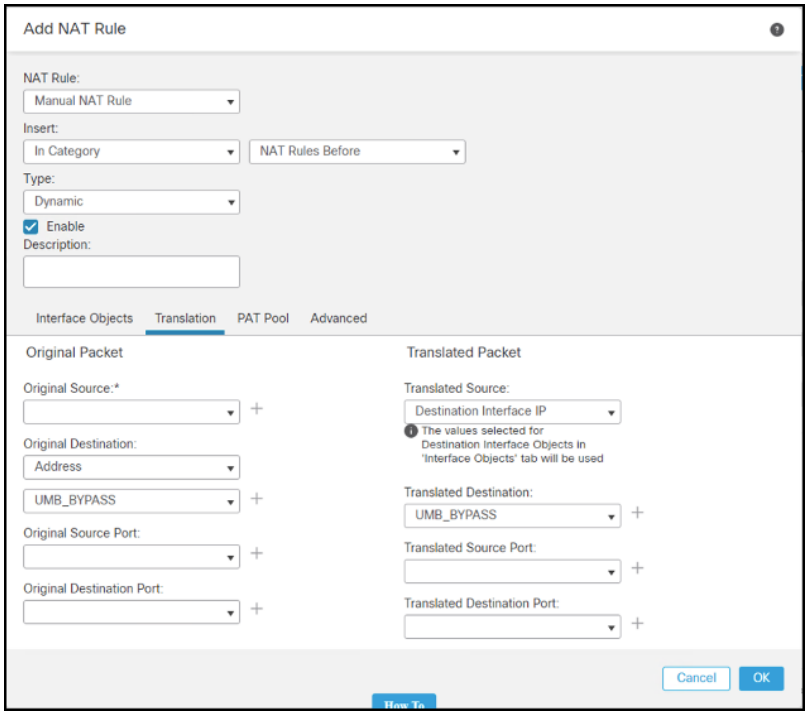


5. Under **Translations**, select a network object containing the internal subnet as the **Original Source**. Specify the Secure Access bypass network object you previously created as the **Original Destination**.**Important**

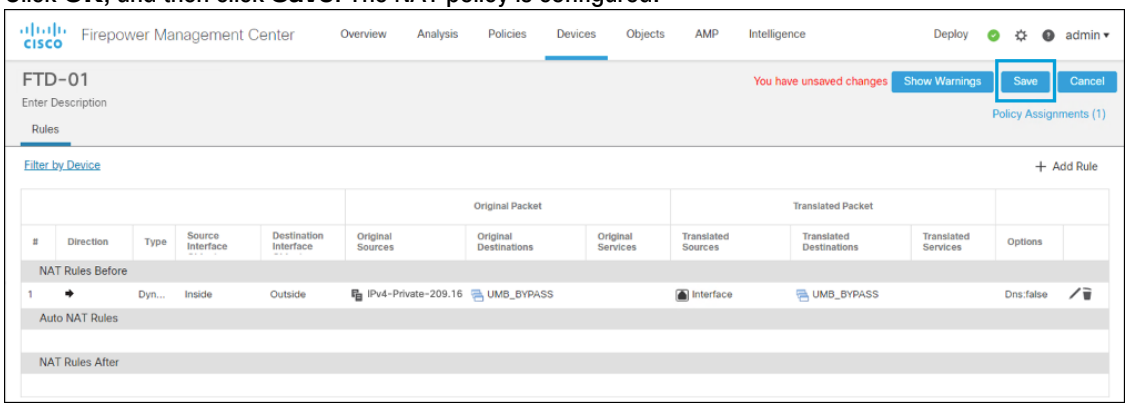
   This object contains the Secure Access resolvers' IP address, as well as (optionally) the `146.112.0.0/16` and `155.190.0.0/16` networks, plus any other traffic you may want to exempt from the tunnel. Using this object facilitates the configuration, because when hosts and subnets are added or removed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



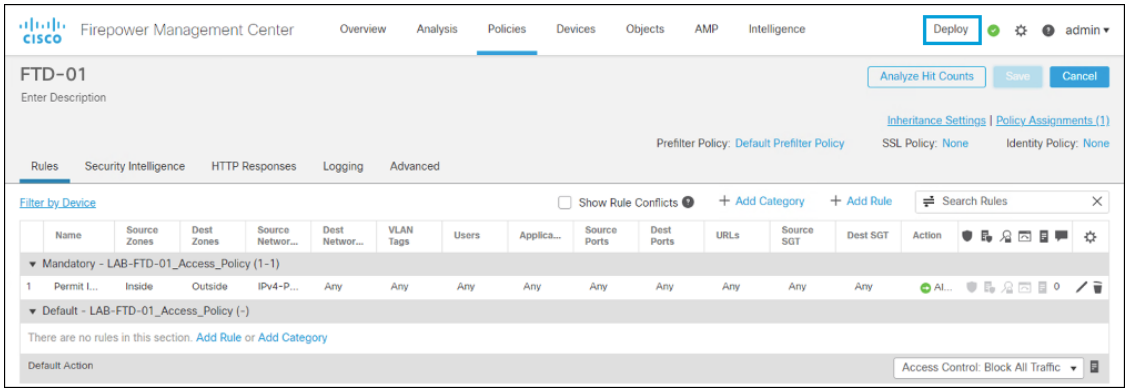
7. Click **OK**, and then click **Save**. The NAT policy is configured.



Configure Access Policy

Provides instructions for 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.



Important

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

Provides instructions for 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

Provides instructions for 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.

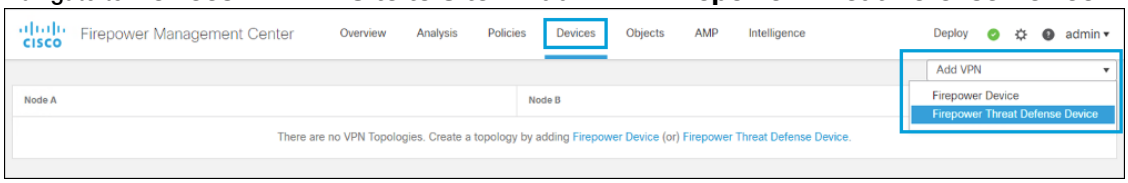
The new tunnel appears in Secure Access with a status of *UnEstablished*. The tunnel status is updated once the first IKEv2 INIT message containing the tunnel identity is received in one of the Secure Access data centers.

Configure Site-to-Site VPN

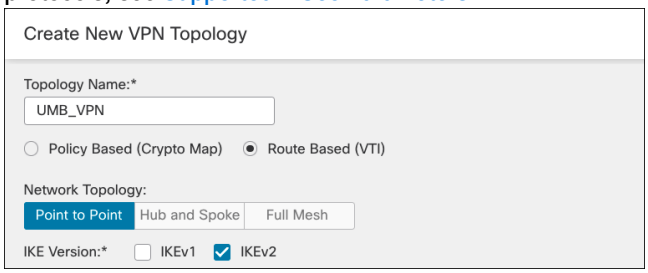
Provides instructions for configuring site-to-site vpn. You can now configure the site-to-site VPN. Navigate to Devices > VPN > Site to Site > Add VPN > Firepower Threat Defense Device.

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

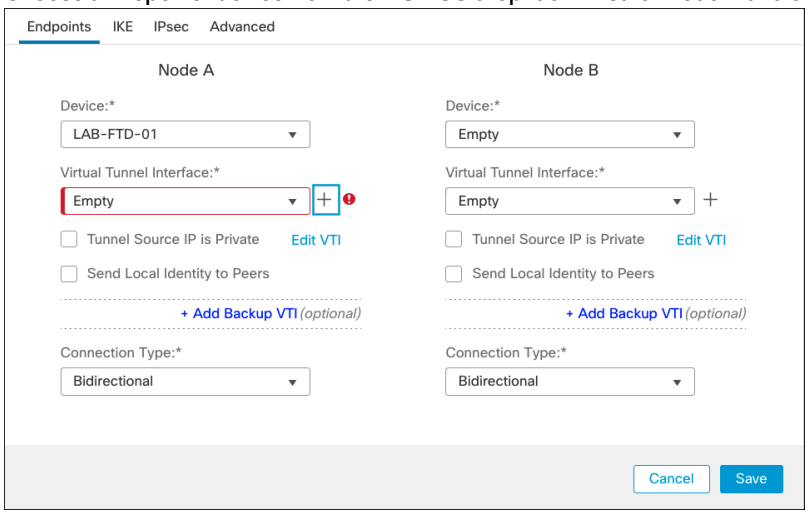
1. Navigate to **Devices > VPN > Site to Site > Add VPN > Firepower Threat Defense Device**.



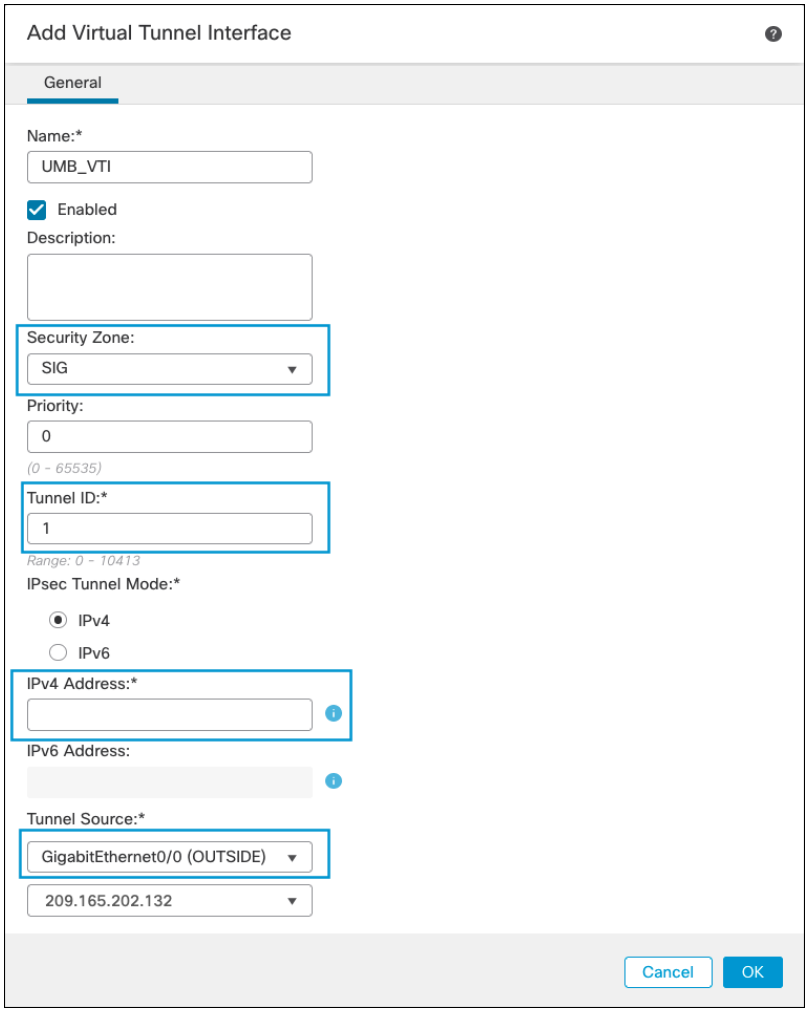
2. Enter a name for the topology, select **Route Based (VTI)**, and check IKEv2 box. For more information about supported protocols, see Supported IPSec Parameters.



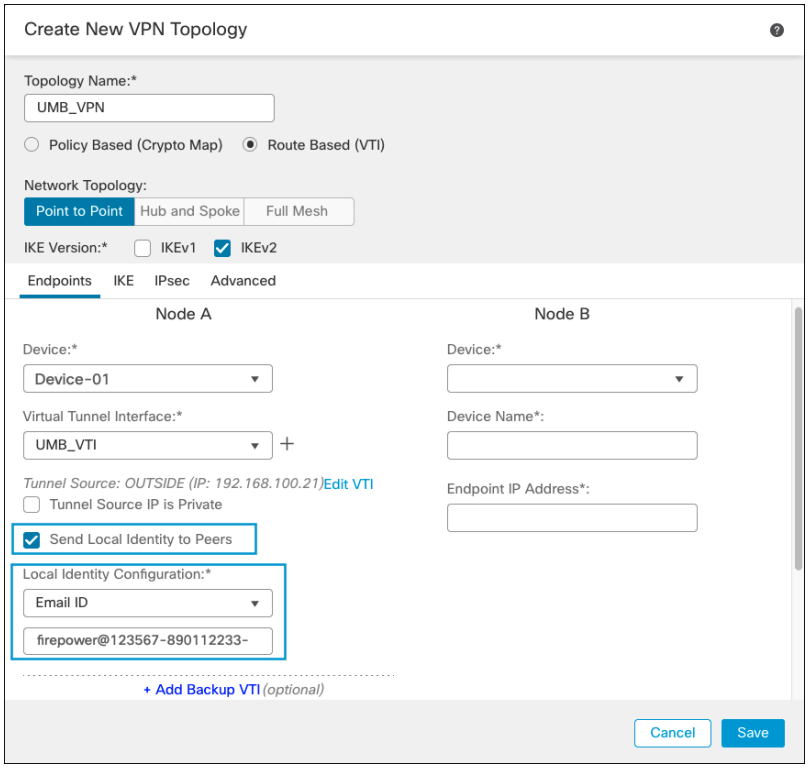
3. Choose a Firepower device from the **Device** drop-down list for Node A and click **Add** to add a Virtual Tunnel Interface.



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**.



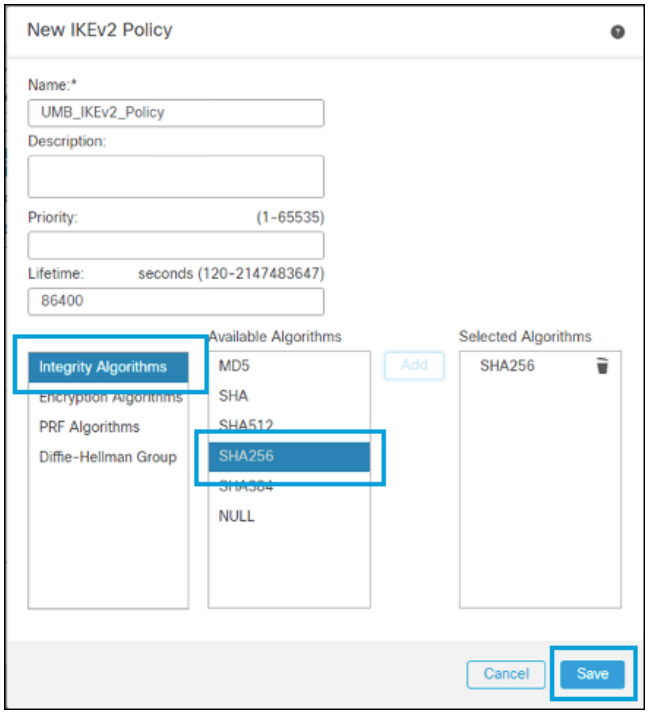
5. Select the VTI you just created, and under **Send Local Identity to Peers** select **Email ID** and type the previous created tunnel FQDN.



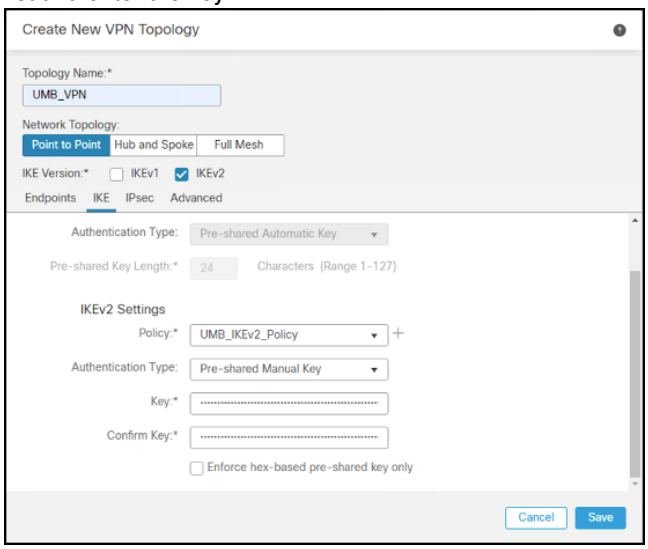
6. Under Node B, choose **Extranet** as the device, enter a name and IP address of a Secure Access data center.



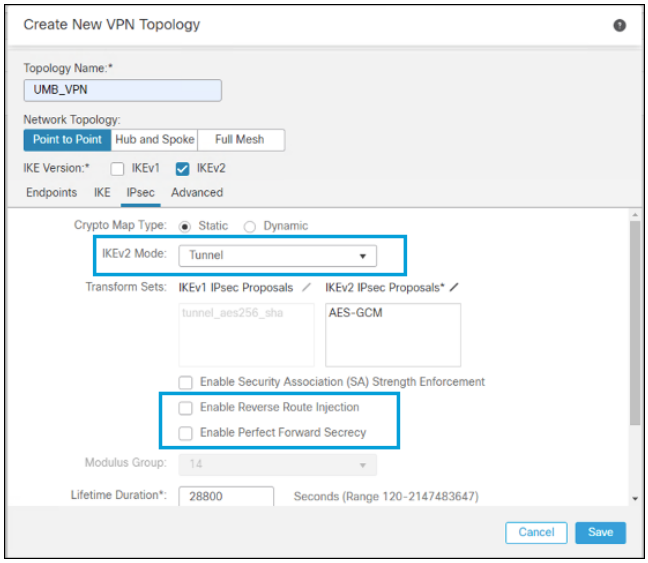
7. Enter a name for the IKEv2 policy, then select the parameters from the list.



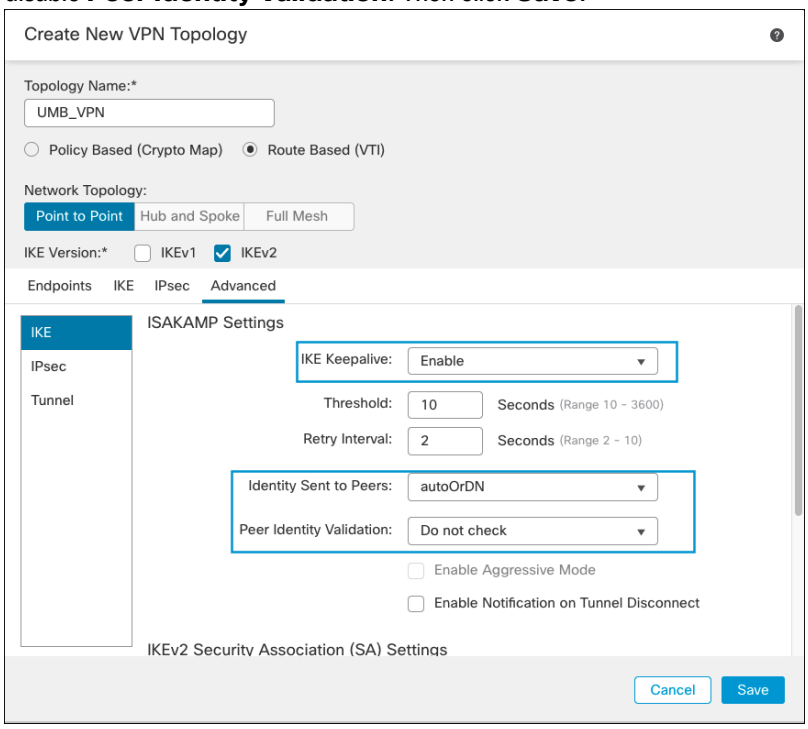
8. After saving the IKEv2 Policy, select it. Choose **Pre-shared Manual Key** from the **Authentication** drop-down list and enter the key.



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**.



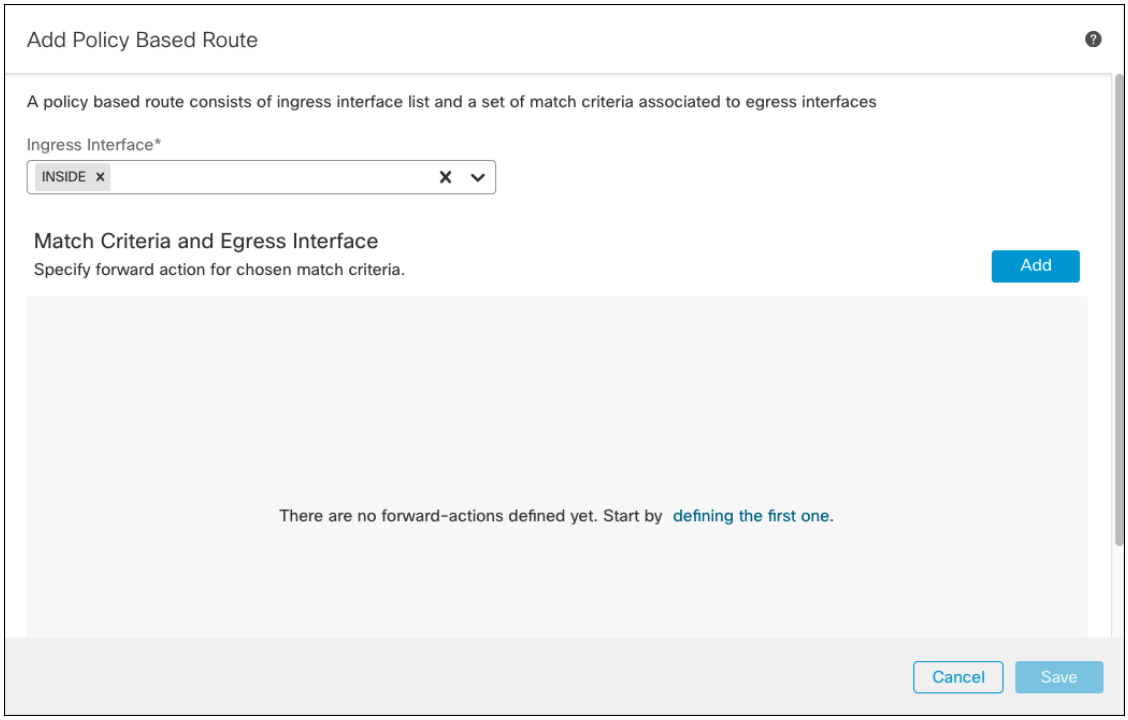
10. In the **Advanced** tab under IKE, enable **IKE Keepalive**. Select **autoOrDN** as the **Identity Sent to Peers**, and disable **Peer Identity Validation**. Then click **Save**.



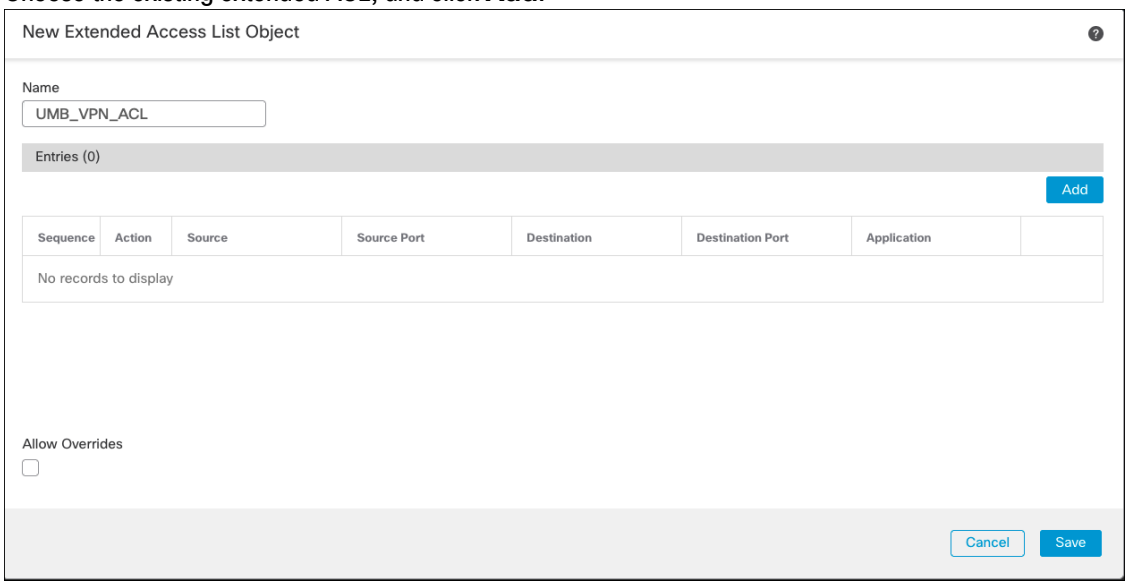
Configure Policy-based Routing

Provides instructions for configuring policy-based routing. 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.

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**.

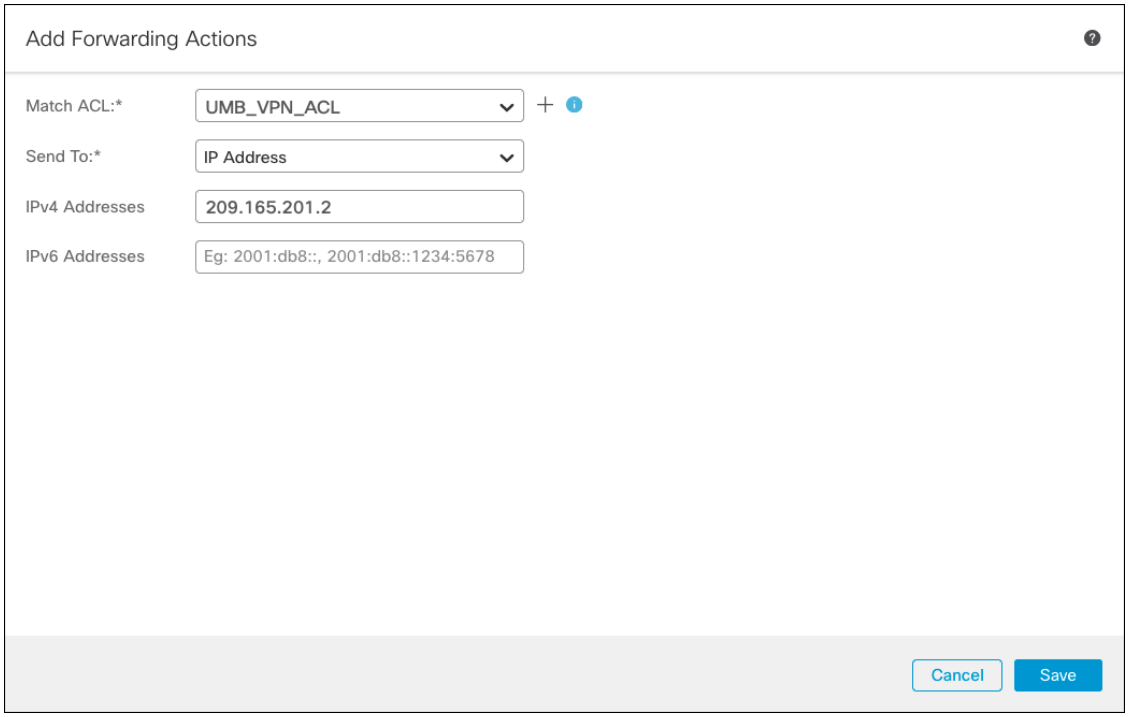


4. Choose the existing extended ACL, and click **Add**.



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

Provides instructions for 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.

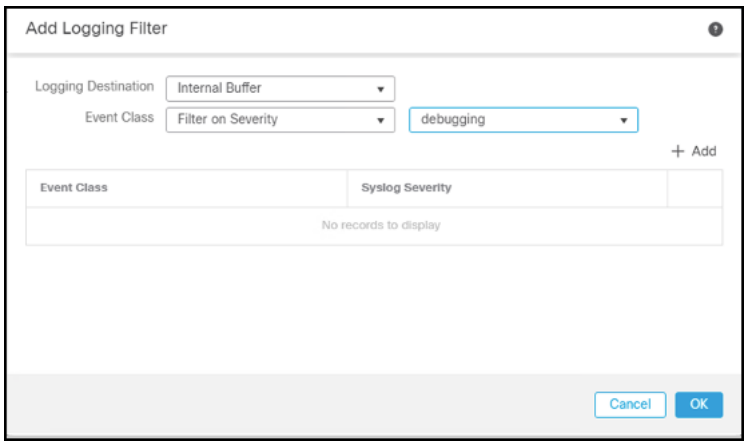
Cisco Secure Firewall Management Center has a VPN troubleshooting tab where VPN-related events are displayed. By default, only error messages are sent from FTD to Cisco Secure Firewall Management Center, as LINA code (ASA) is responsible for the IPSec tasks the same commands available for troubleshooting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

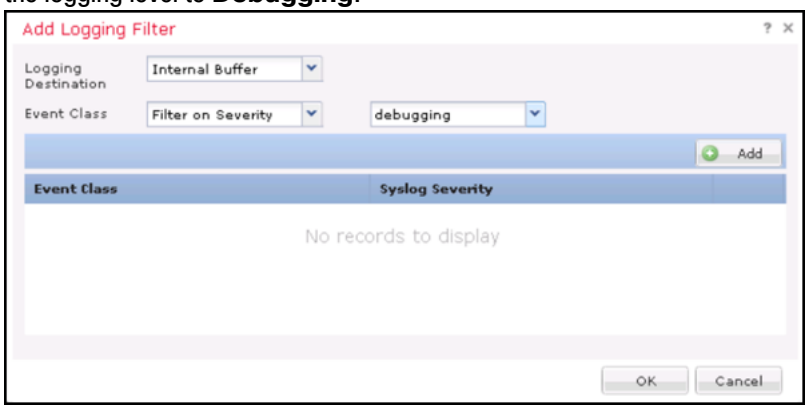
Enable Logging for Debugging

Provides instructions for enabling logging for debugging. 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.

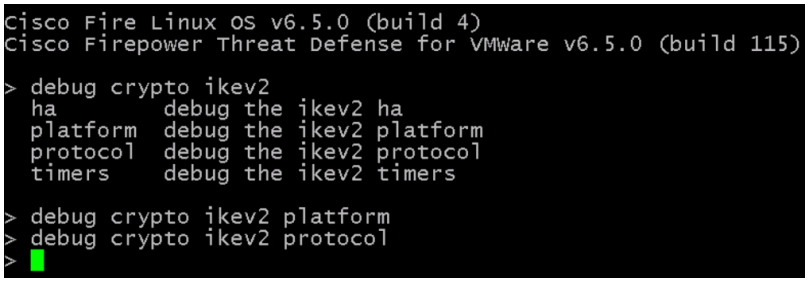
1. In Cisco Secure Firewall Management Center, navigate to **Devices > Platform Settings.**
2. Under **Basic Logging Settings**, add a logging destination.



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

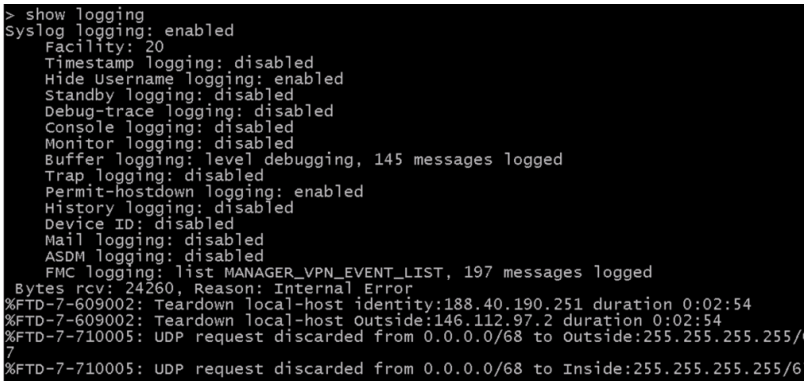


When logging is enabled, you can enable IKEv2 debug, SSH to FTD. Then enter type `debug crypto ikev2 platform` and `debug crypto ikev2 protocol`. These two debugging options provide detailed information about IKEv2 negotiation.



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

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



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



Configure Tunnels with Meraki MX

Provides instructions for configuring tunnels with Meraki MX in Cisco Secure Access China. 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 in the Secure Client to private applications on Meraki networks.

Prerequisites

Lists the prerequisites for manual Meraki mx. A Cisco Meraki MX/Z4 device (running MX 18.107+ firmware). A valid Cisco Secure Access account.

- 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.

Caveats and Considerations

Describes 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.

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

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.

Branch-to-Branch through Secure Access

Describes 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.

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

Provides instructions for securing internet access with non-meraki vpn. The following are requirements for this configuration:. No AutoVPN default route.

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

Describes 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.

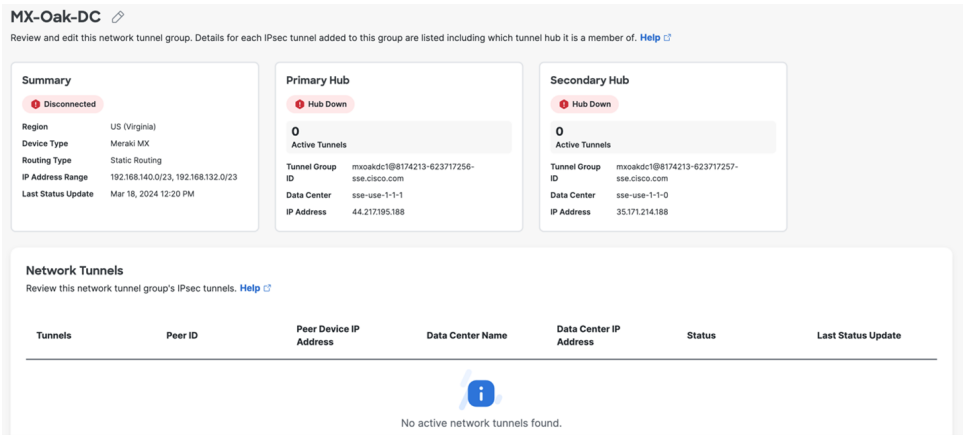
1. Follow the steps in Add a Network Tunnel Group.
2. Make note of the **Tunnel ID** and **Passphrase** you enter when configuring the network tunnel group. These values are needed when you configure your Meraki IPsec tunnel.

   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.

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.

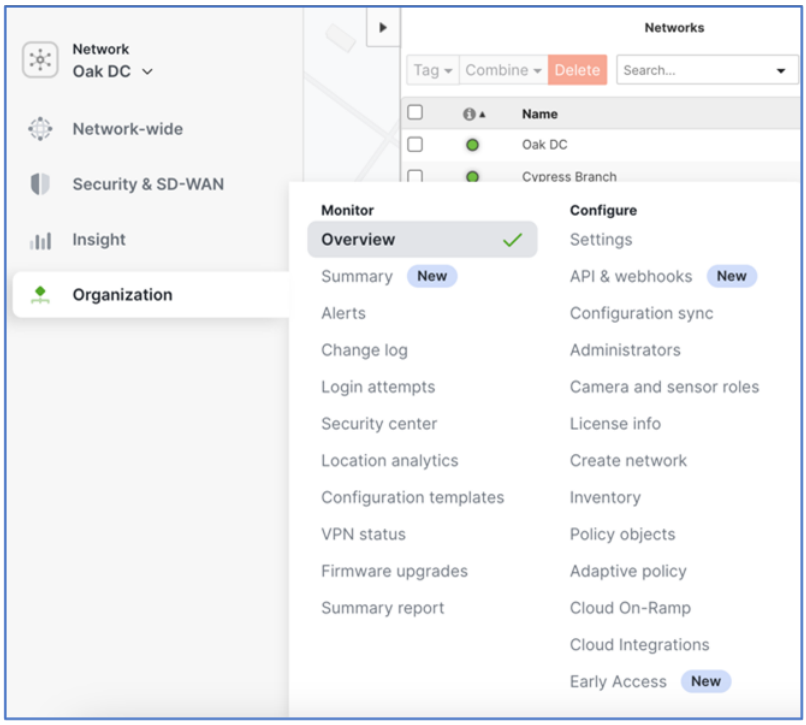
Step 2: Configure a Tunnel in Meraki MX

Describes 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.

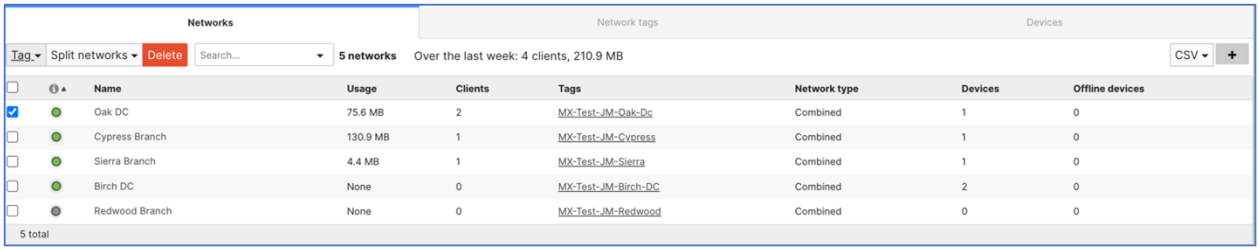
Configure a Meraki Third Party (non-Meraki) VPN tunnel to connect a Meraki MX/Z4 series device to Cisco Secure Access.

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.

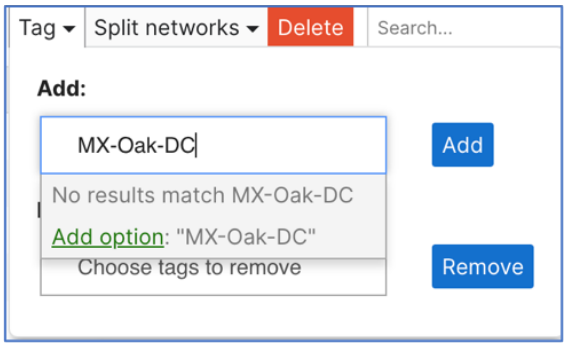


2. Select the desired network from the networks **Name** list. Select only the network that will connect to the Secure Access Network Tunnel Group.

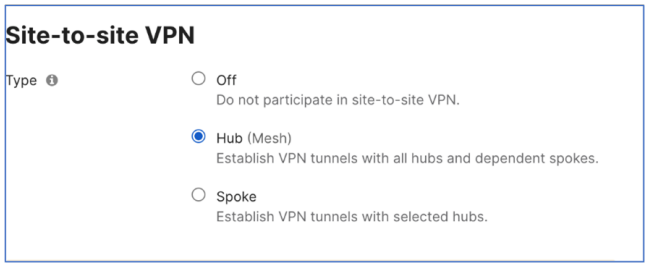


3. Add a Network tag to the selected network. Select the **Tag** dropdown menu from the top left. A tag can be created by typing into the field and then clicking **Add**.

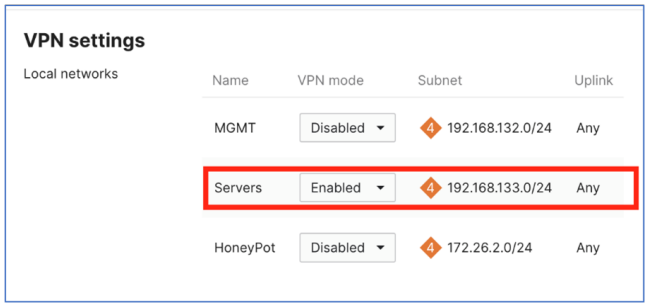
> **Note**
>
> It is recommended that the same name is used for the Meraki Network Tag as the Secure Access Network Tunnel Group.



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



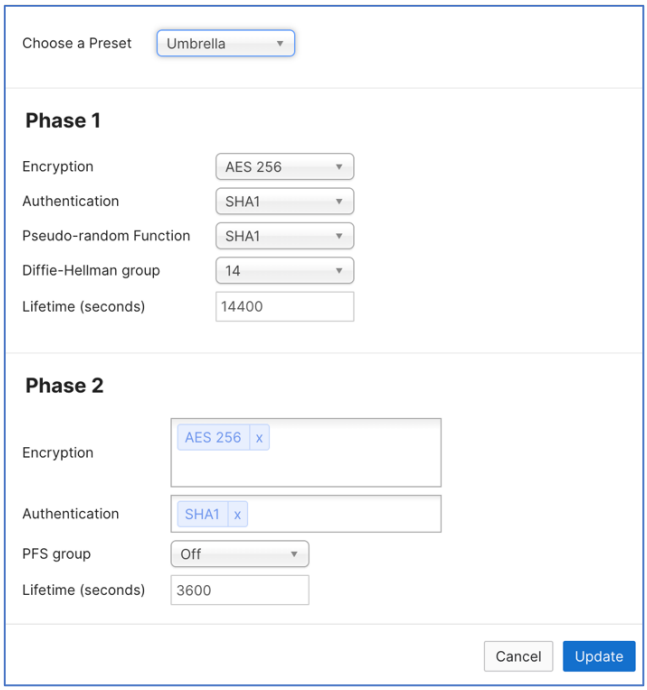
5. Next, in the same section, find the **VPN settings** and choose **Enabled** for the VLANs that will use the new Secure Access network tunnel group.



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.

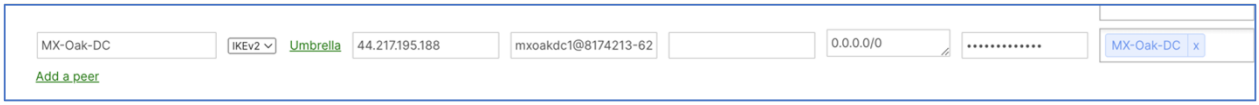


   - **Public IP**–IP address to connect to Secure Access Network Tunnel Group Primary Data Center IP.
   - **Local ID**–The Primary Tunnel ID for the Network Tunnel Group.
   - **Remote ID**–Leave this blank.

- **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.



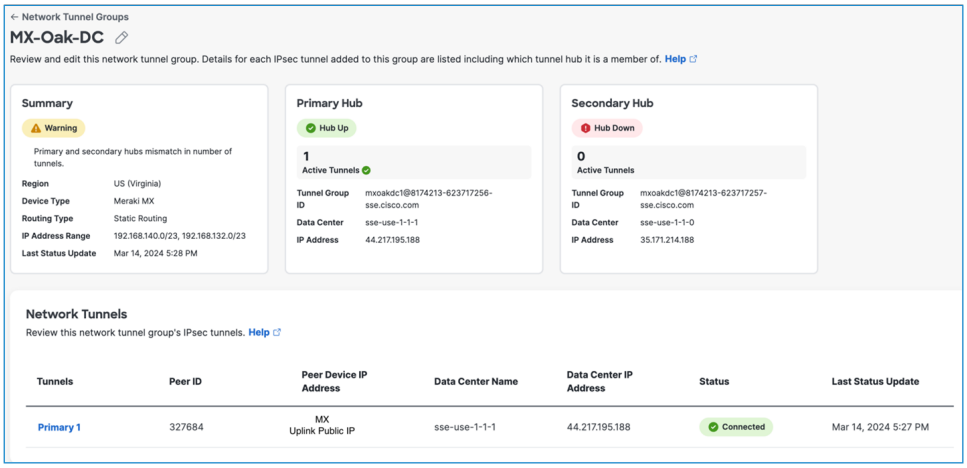
8. Click **Save**.

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

Verification and Troubleshooting

Describes 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.

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



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

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

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

Optional Configurations

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

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

Establish a Tunnel

Describes establish 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

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

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

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

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.

5 Manage Users and Groups

Topics:

- Manage Users and Groups

Provides an overview of Manage Users and Groups in Cisco Secure Access China, including View User Details, View Group Details, and Provision Token for Identity Provider. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Users and Groups

Provides instructions for managing users and Groups in Cisco Secure Access China. 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.

View User Details

Provides instructions for viewing user Details in Cisco Secure Access China. After an administrator provisions users in Secure Access China, you can view details about the users and identify the policy rules applied to the users.

After an administrator provisions users in Secure Access China, you can view details about the users and identify the policy rules applied to the users.

Prerequisites

Lists the prerequisites for viewing user details, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

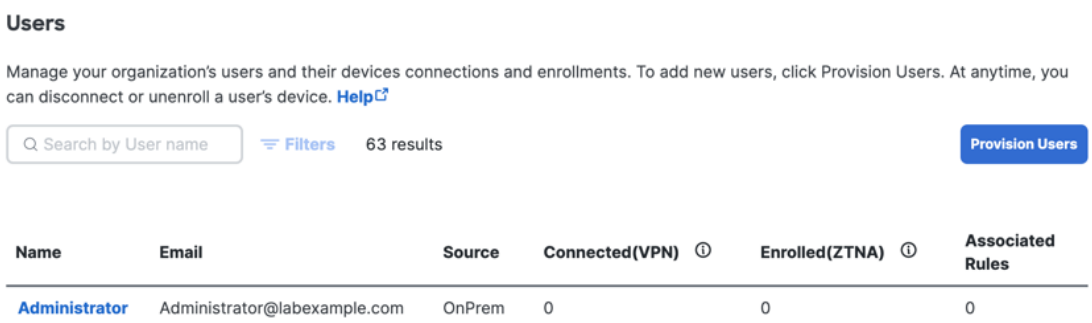
- Full Admin user role. For more information, see Manage Accounts.

Procedure

Provides instructions for viewing user details. View provisioned users and groups in Secure Access China. Navigate to Connect > Users and Groups.

View provisioned users and groups in Secure Access China.

1. Navigate to **Connect > Users and Groups**
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).
   - **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

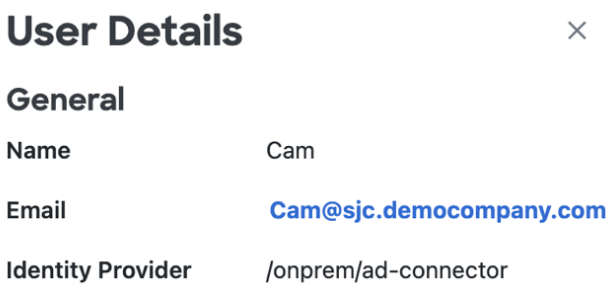
Describes the information shown for a user in the organization and helps administrators review that user?s details in Secure Access China.

The information about the user in the organization.

General User Details

Describes 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.

- **Name**–The name of the user.
- **Email**–The email of the user.
- **Identity Provider**–The identity provider that manages the user information.

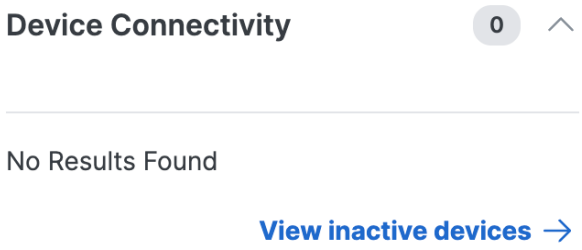


Device Connectivity

Describes device Connectivity. The list of devices associated with the user. Connection –The type of connection. IP address –The IP address of the device.

The list of devices associated with the user.

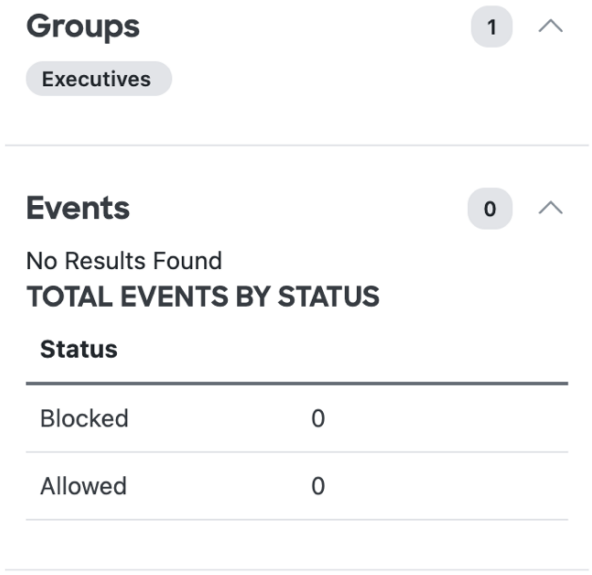
- **Connection**–The type of connection
- **IP address**–The IP address of the device.
- **OS Version**–The version of the device's operating system.



Groups and Events

Describes 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.

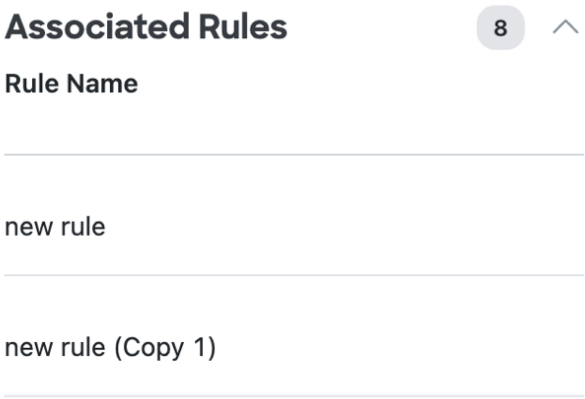
- **Groups**–The number of groups that include the user and the name of the groups.
- **Events**–The number of events created by the user and the status of the events.



Associated Rules

Describes the Secure Access policy rules applied to a user and helps administrators review the user?s associated access rules. for administrators to review.

The Secure Access policy rules applied to the user.



View Group Details

Provides instructions for viewing group Details in Cisco Secure Access China. After an administrator provisions groups in Secure Access China, you can view the details about the groups and identify the policy rules applied to the groups.

After an administrator provisions groups in Secure Access China, you can view the details about the groups and identify the policy rules applied to the groups.

Prerequisites

Lists the prerequisites for viewing group details, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

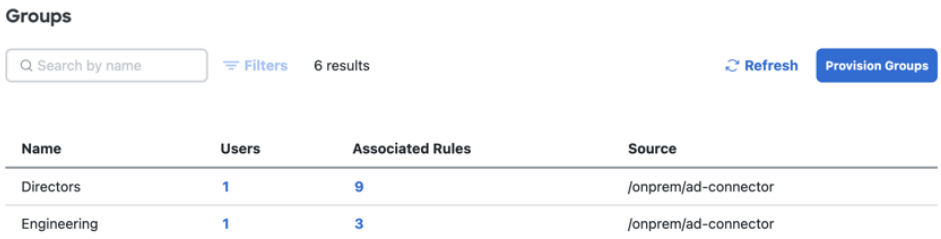
- Full Admin user role. For more information, see Manage Accounts.

Procedure

Provides instructions for viewing group details. View provisioned users and groups in Secure Access China. Name –The name of the group.

View provisioned users and groups in Secure Access China.

1. Navigate to **Connect > Users and Groups** 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.



2. Find a group in the organization and then click on the **Name** of the group to open the **Group Details**.

Group Details

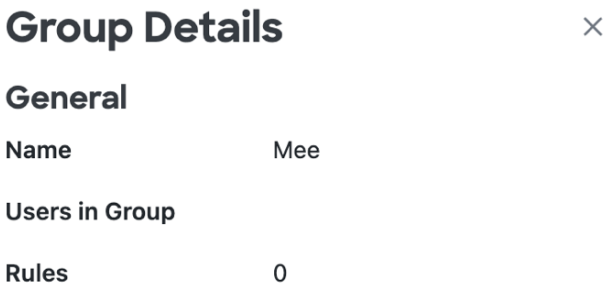
Describes the organization?s group information displayed in Secure Access China and helps administrators review group details and related access management.

The information about the organization's group.

General Group Details

Describes 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.

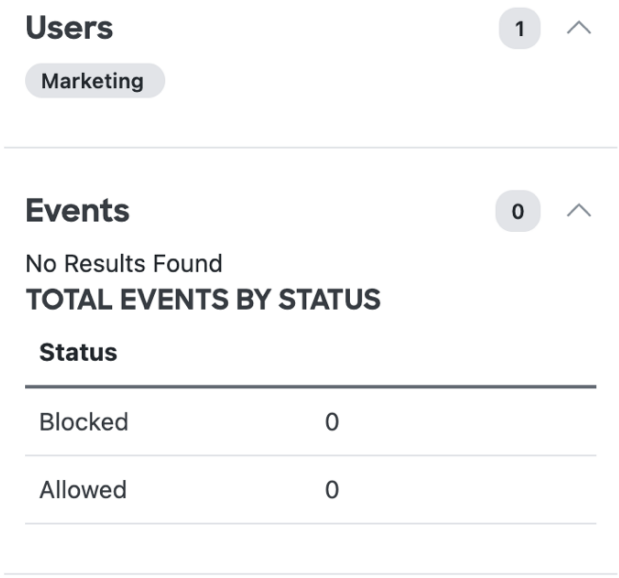
- **Name**–The name of the group.
- **Users in Group**–The number of users in the group and the label for the group.
- **Rules**–The number of rules that include this group.



Users and Events

Describes users and Events. The number of users in the group and the status of the events created by the users.

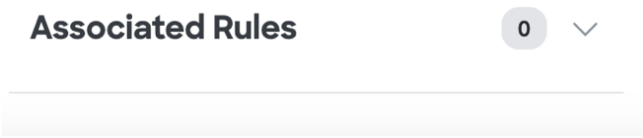
The number of users in the group and the status of the events created by the users.



Associated Rules

Describes the Secure Access policy rules applied to a group and shows administrators the number of associated rules. for administrators to review.

The number of Secure Access policy rules applied to the users in the group.



Provision Token for Identity Provider

Provides instructions for provisioning token for Identity Provider in Cisco Secure Access China. 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.

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

Lists the prerequisites for provisioning token for identity provider, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

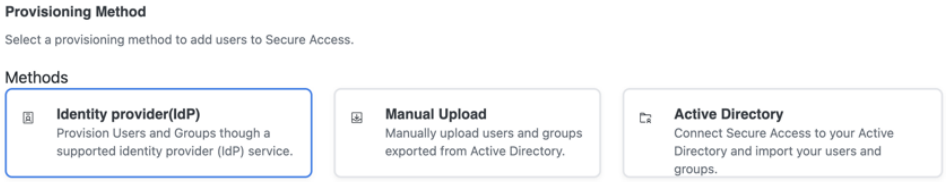
- Full Admin user role. For more information, see Manage Accounts.

Procedure

Provides instructions for provisioning token for identity provider. 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.

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.

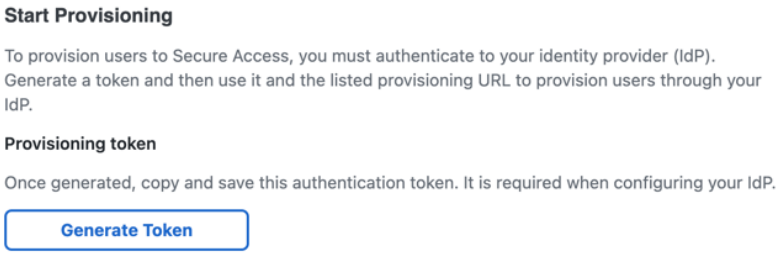
1. Navigate to **Connect > Users and Groups > Users** and click **Provision Users** or **Connect > Users and Groups > Groups** and click **Provision Groups**.
2. For **Provisioning Method**, click **Identity Provider**.



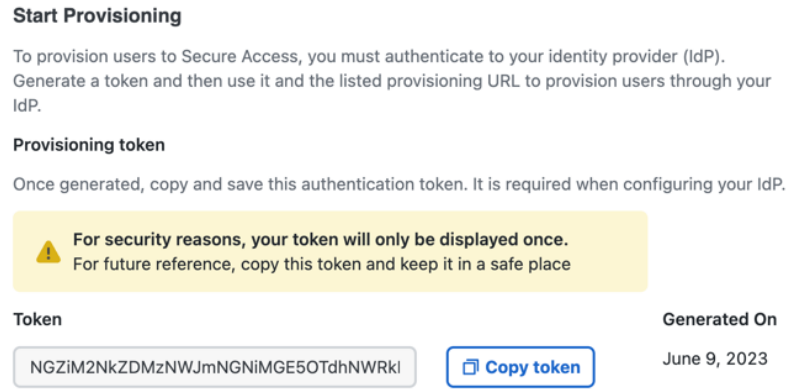
3. Choose an identity provider and then click **Next**.



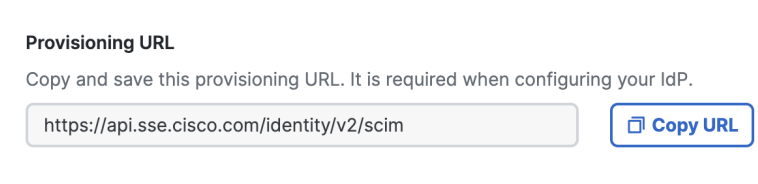
4. Click **Generate Token** to create a provisioning API access token for your integration with the IdP.



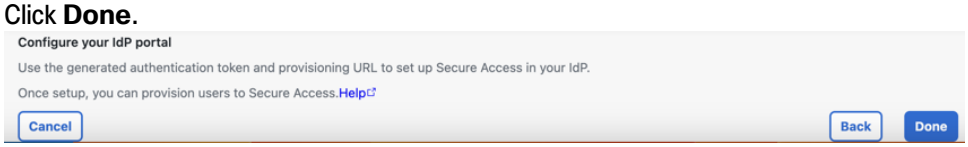
5. Click **Copy token** to copy the generated token. Save the token to your local system.



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

Provides instructions for 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

Import Users and Groups from CSV File

Provides instructions for importing users and Groups from CSV File in Cisco Secure Access China. Secure Access supports provisioning users and groups manually from a comma-separated values (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.

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

Lists the prerequisites for importing users from csv file, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

CSV File Format

Describes CSV File Format. The CSV file must include the users and groups information in a comma delimited format. Header row :.

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=SAMUser,CN=Users,DC=mycompany,DC=local",last_name_1,first_name_1,samuser@mycompany.com,samuser@mycompany.com,"CN=Group2,CN=Users,DC=mycompany,DC=com"
```

The following characters are not supported:

```
%<([{\\^-=$!|]})?*+>
```

CSV File Fields

Describes CSV File Fields. A user may belong to multiple groups, which are defined in the memberOf attribute. An example value of the memberOf field:.

Field	Required	Notes	Supported Number of Characters
DN		"CN=SAMLUser,CN=Users,DC=mycompany,DC=local"	64
sn	✔	The user's surname (family name or last name).	64
givenName	✔	The user's given name (legal first name).	64
userPrincipalName	✔	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	✔	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:

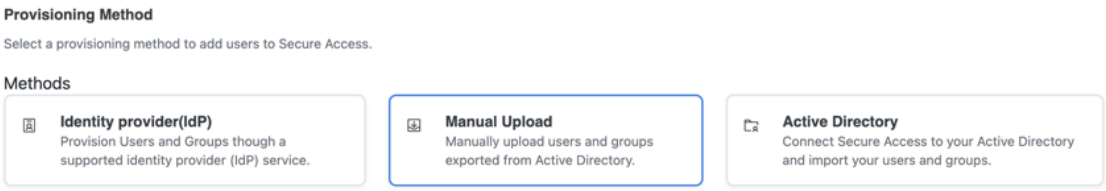
```
"CN=Group1,CN=Users,DC=dcloud,DC=local;CN=Group2,CN=Users,
DC=dcloud,DC=local;CN=Group3,CN=Users,DC=dcloud,DC=local;
CN=Group4,CN=Users,DC=dcloud,DC=local"
```

Procedure

Provides instructions for importing users from CSV file. Import users into Secure Access from a comma-separated values (CSV) file. Navigate to Connect > Users and Groups > Users and click Provision Users or Connect > Users and Groups > Groups and click Provision Groups.

Import users into Secure Access from a comma-separated values (CSV) file.

1. Navigate to **Connect > Users and Groups > Users** and click **Provision Users** or **Connect > Users and Groups > Groups** and click **Provision Groups**.
2. For **Provisioning Method**, click **Manual Upload** to provision users or groups in your organization.

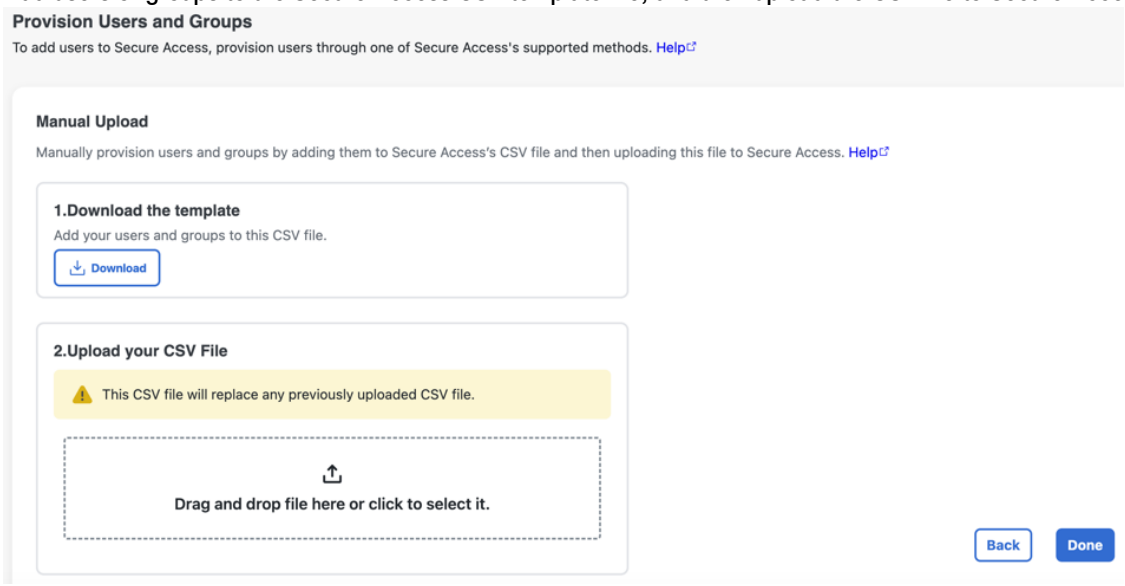


3. Click **Download** to save the Secure Access import template to your local system. The template is a CSV file that supports the following format:

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
```

4. Add users or groups to the Secure Access CSV template file, and then upload the CSV file to Secure Access.



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 and Groups to view the users and groups provisioned in your organization. See View User Details See View Group Details.

1. Navigate to **Connect > Users and Groups** to view the users and groups provisioned in your organization.
   a. See View User Details
   b. See View Group Details

Provision Users and Groups from Okta

Provides instructions for provisioning users and Groups from Okta in Cisco Secure Access China. Cisco Secure Access supports the provisioning of 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 for Secure Access** 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

Lists the prerequisites for provisioning users and groups from Okta. Full Admin user role. For more information, see Manage Accounts.

- 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 Cisco Active Directory 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

Describes limitations. 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 for Secure Access** 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 for Secure Access** 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. The Okta Active Directory agent does not synchronize the objectGUID attribute of users from on-premises AD to Okta by default.

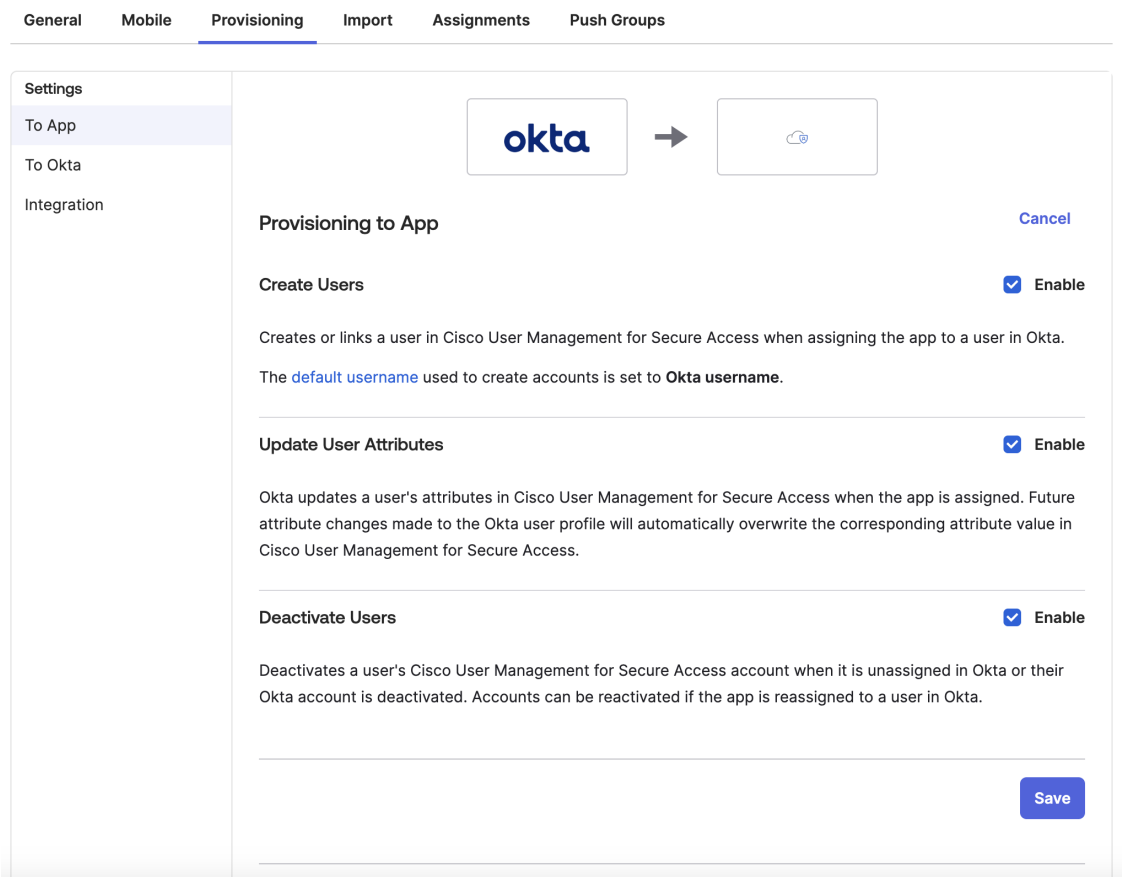
The on-premises Secure Access AD Connector and the Cisco Secure Client rely on the `objectGUID` attribute for user and group identification. Ensure that the `objectGUID` attribute of users is synchronized from Okta to Secure Access only if either of the following conditions are true:

- You have previously imported AD users to Secure Access using the on-premises Secure Access AD connector, are now importing the same user identities from Okta, and want the previously imported identities to be persisted for policy or reporting purposes.
- You have endpoints that authenticate against on-premises AD and run the Cisco Secure Client.

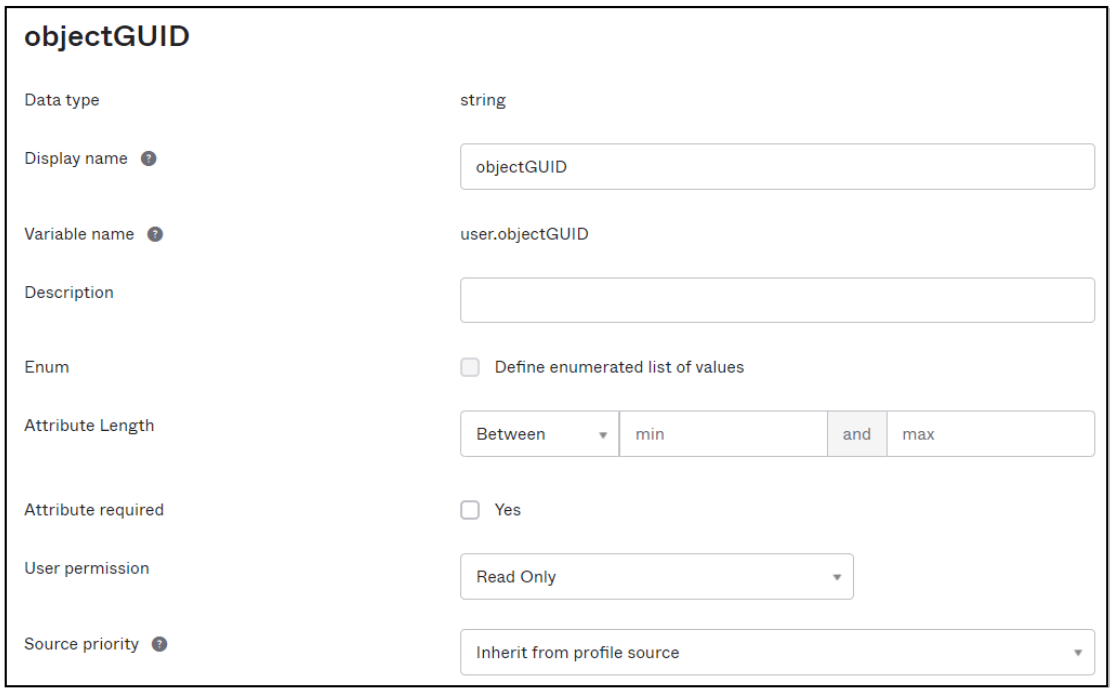
> **Note**
>
> Before setting up the import of the `objectGUID`, ensure that the on-premises Secure Access AD Connector that synchronizes these users and groups is switched off or that the Cisco Active Directory service on the connector machine is stopped.

The Okta Active Directory agent does not synchronize the `objectGUID` attribute of users from on-premises AD to Okta by default.

1. Navigate to the **Provisioning** tab on the **Cisco Secure Access User Management** 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 for Secure Access 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

Provides instructions for configuring the Cisco Secure Access app. Configure the Cisco User Management for Secure Access app on the Okta portal.

Configure the **Cisco User Management for Secure Access** app on the Okta portal.

> **Note**
>
> The **To Okta** setting is not supported on the **Cisco User Management for Secure Access** app.

Step 1 – Add the App to Okta

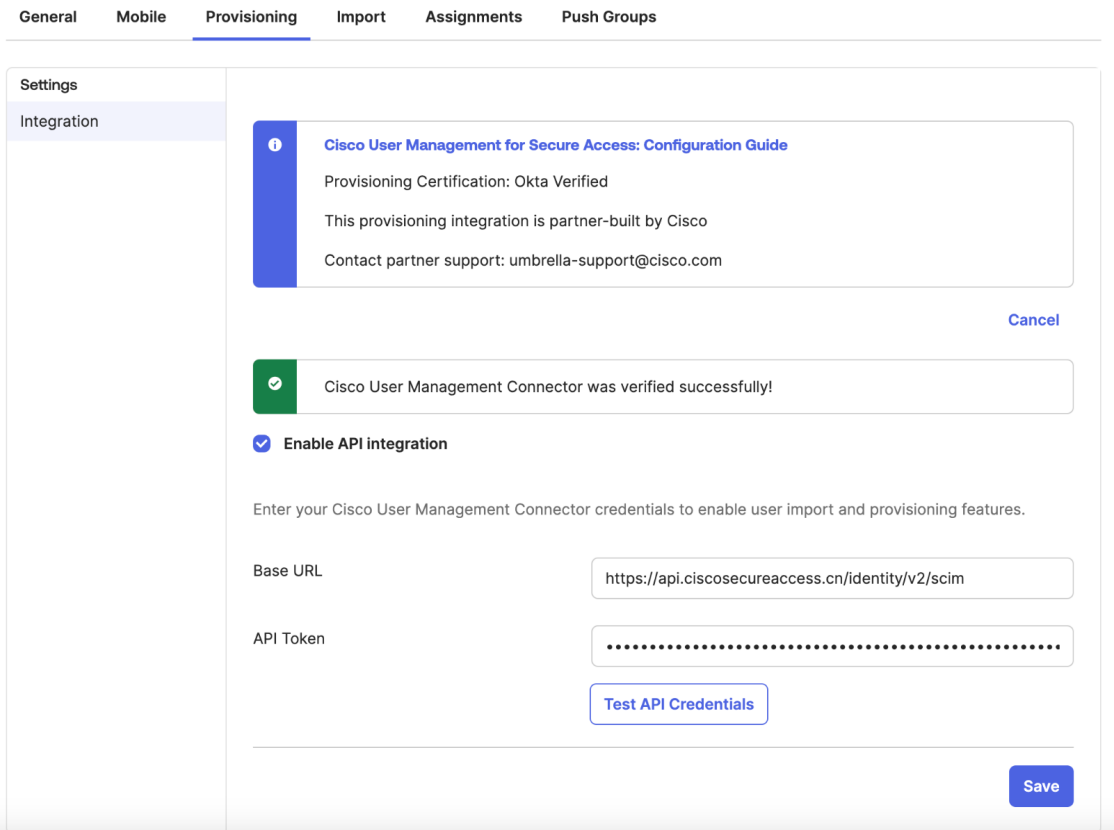
Describes step 1 - Add the App to Okta. Sign in to Okta and add the Cisco Secure Access User Management app to your instance of Okta.

1. Sign in to Okta and add the **Cisco Secure Access User Management** app to your instance of Okta.

Step 2 – Add the Secure Access SCIM Token to the App

Describes step 2 - Add the Secure Access SCIM Token to the App. Navigate to the Provisioning tab on the Cisco Secure Access User Management app in Okta.

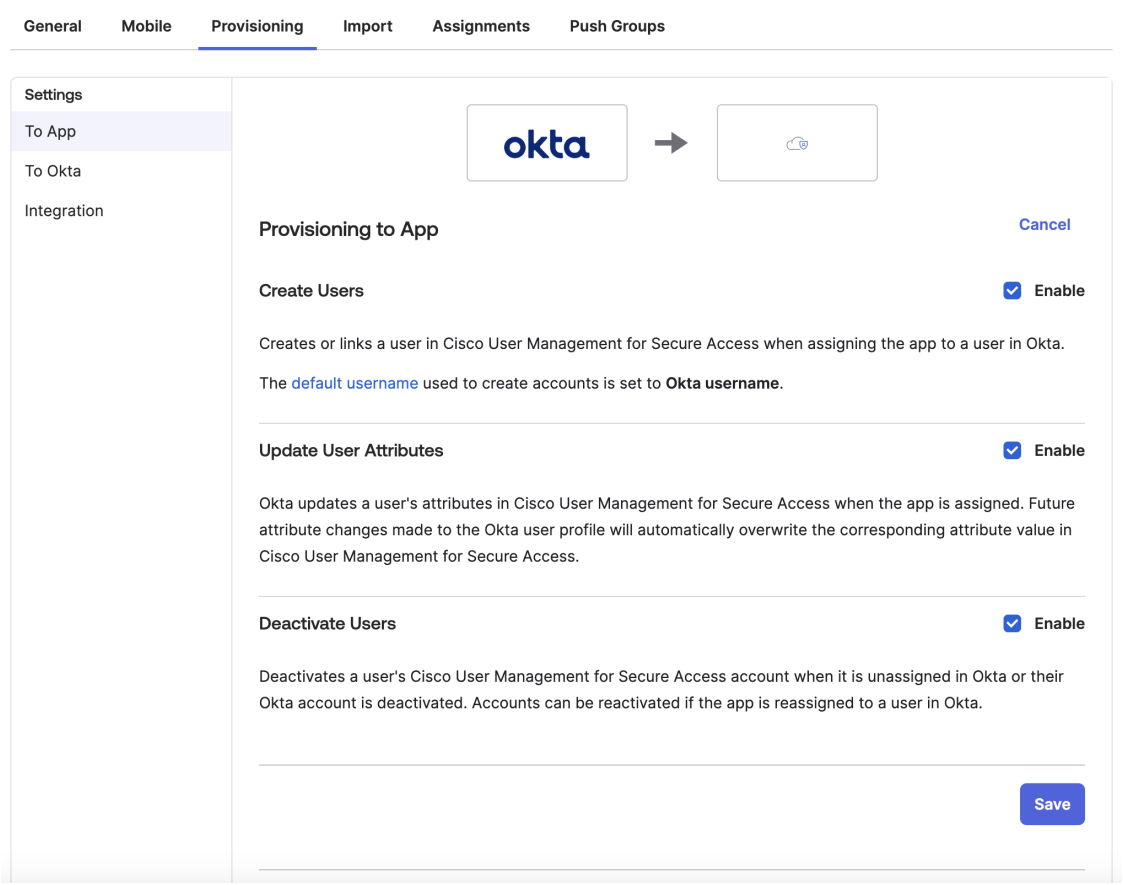
1. Navigate to the **Provisioning** tab on the **Cisco Secure Access User Management** app in Okta.
2. From **Settings > Integration**, select **Enable API Integration**, and then add the base URL (http://api.ciscosecureaccess.cn/identity/v2/scim) and Secure Access SCIM API token.
3. Click **Test API 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

Describes step 3 - Configure the Required User Options. Navigate to the Provisioning tab on the Cisco Secure Access User Management app in Okta.

1. Navigate to the **Provisioning** tab on the **Cisco Secure Access User Management** 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.

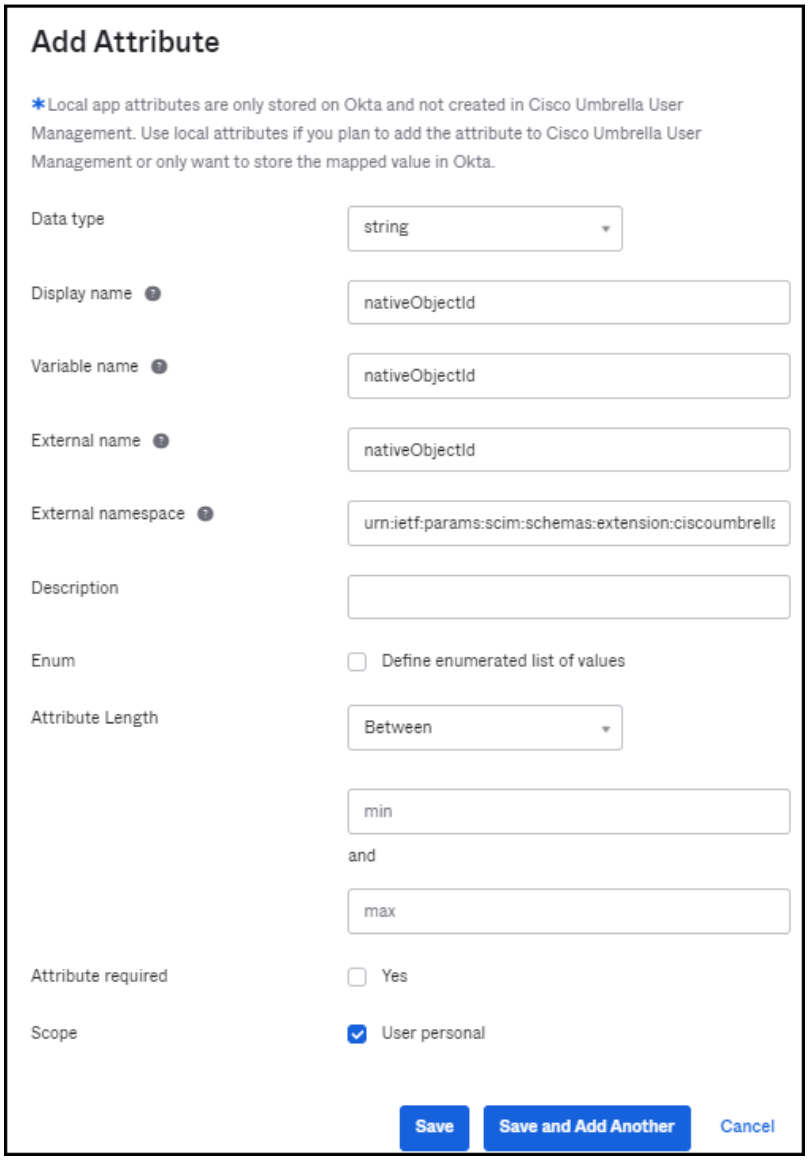


3. Verify that the following attributes are chosen for synchronization to Secure Access. Other attributes are not required. Secure Access does not list the **Given name** and **Family name** attributes for users. Secure Access only lists the **Display name** and **Username** attributes.
    - **Username**
    - **Given name**
    - **Family name**
    - **Display name**
    - **Primary email**

Step 4 – (Optional) Add a New Attribute and Create the User Profile Mapping

Describes step 4 - (Optional) Add a New Attribute and Create the User Profile Mapping. Navigate to the Provisioning tab on the Cisco Secure Access User Management app in Okta.

1. If you need to import the `objectGUID` attribute for users, add a new attribute and map the attributes in the profile mapping.



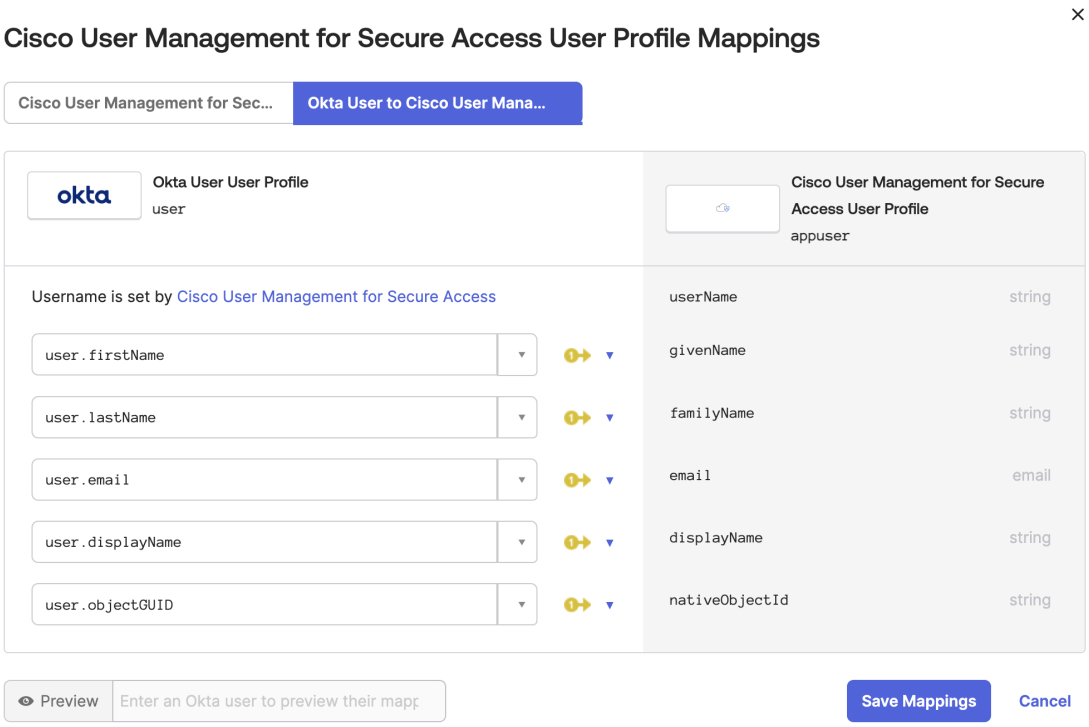
a. Navigate to the **Provisioning** tab on the **Cisco Secure Access User Management** app in Okta.
b. From **Settings > To App**, navigate to **Profile Editor**.
c. Click **Add Attribute**.

- Set **Display name**, **Variable name**, and **External name** to `nativeObjectId`.
- For **Scope**, click **User personal**.
- Set **External namespace** to `urn:ietf:params:scim:schemas:extension:ciscoumbrella:2.0:user`

d. Click **Save**.

2. Add the new user profile mapping.

a. Navigate to the **Provisioning** tab on the **Cisco Secure Access User Management** app in Okta.
b. From **Settings > To App**, navigate to **Profile Editor**.
c. For **Cisco User Management for Secure Access User Profile Mappings**, create a new **Okta User Profile** that maps the Okta User to the **Cisco User Management for Secure Access** user. The profile must map the `user.objectGUID` to `nativeObjectId`.
d. 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

Describes step 5 - Assign Users and Groups in the App. Once you complete the provisioning configuration, assign users in the Cisco User Management for Secure Access app.

Once you complete the provisioning configuration, assign users in the **Cisco User Management for Secure Access** app.

1. Navigate to the **Assignments** tab on the **Cisco Secure Access User Management** 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 Secure Access User Management** 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.

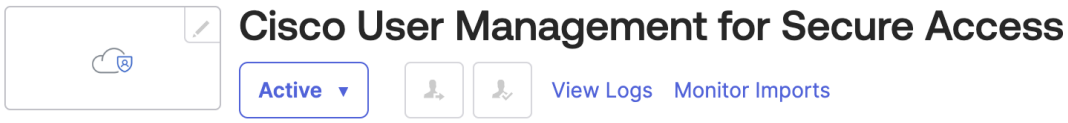
> **Note**
>
> Okta does not recommend pushing groups that are assigned to the app. If you have assigned the **Everyone** group to the app, you should not push the same group.

Step 6 – View Logs in the App

Describes step 6 – View Logs in the App. The app displays the progress of the provisioning. Navigate to View Logs on the Cisco User Management for Secure Access app in Okta. The app displays the progress of the provisioning.

1. Navigate to **View Logs** on the **Cisco User Management for Secure Access** 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 and Groups to view the users and groups provisioned from Okta. See View User Details See View Group Details.

1. Navigate to **Connect > Users and Groups** to view the users and groups provisioned from Okta.
   a. See View User Details
   b. See 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 Azure

Provides instructions for provisioning users and Groups from Azure in Cisco Secure Access China. Cisco Secure Access supports the provisioning of users and groups from Azure Active Directory (Azure AD).

Cisco Secure Access supports the provisioning of users and groups from Azure Active Directory (Azure AD). With your Secure Access System for Cross-domain Identity Management (SCIM) token, configure the **Cisco User Management for Secure Access** app on the Azure portal. Once you add users and groups in the app, Azure 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

Lists the prerequisites for provisioning users and groups from Azure. Full Admin user role. For more information, see Manage Accounts.

- Full Admin user role. For more information, see Manage Accounts.
- A valid Azure AD subscription with a premium Azure AD license.
- No concurrent provisioning of the same user or group identities from on-premises AD and Azure 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 Azure, ensure that the on-premises Secure Access AD connector is switched off or that the Cisco Active Directory service on the connector machine is stopped.
- For IP-to-user mapping deployments, you must use an on-premises Secure Access AD connector. Azure does not store the private IP to Active AD user mappings.
- Import the `ObjectGUID` attribute from Azure 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 Azure.
  - 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 Cisco Active Directory service on the connector machine is stopped.
  - To ensure that the `ObjectGUID` attribute for users is synchronized from Azure 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 Azure, you must reconfigure the policy to map it to the Azure 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 Azure, only group names are displayed on the policy page, for example: **ADGroup1**.

Limitations

Describes limitations. You can provision no more than 200 groups from Azure to Secure Access. Secure Access supports the provisioning of an unlimited number of users from Azure.

- You can provision no more than 200 groups from Azure to Secure Access. Secure Access supports the provisioning of an unlimited number of users from Azure.
- Concurrent synchronization of the same users and groups from the Secure Access AD Connector and the Cisco Secure Access Azure 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 Azure 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.
- Azure does not support nested group memberships for group-based assignment to any SaaS application.

Configure the Cisco User Management for Secure Access App

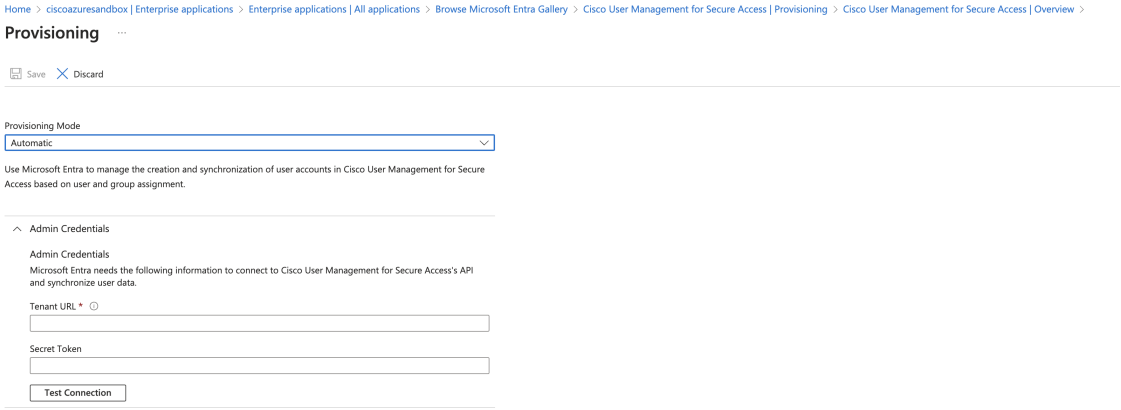
Provides instructions for configuring the cisco user management for secure access app. Navigate to the Cisco User Management for Secure Access app in Azure AD.

With your Secure Access SCIM token and API Identity URL, set up the Cisco Secure Access app in Azure AD and provision users and groups. For more information, see Tutorial: Configure Cisco Secure Access User Management for automatic user provisioning.

1. Navigate to the **Cisco User Management for Secure Access** app in Azure 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 Azure AD.



View Provisioned Users and Groups in Secure Access

Provides instructions for viewing provisioned users and groups in secure access. Navigate to Connect > Users and Groups to view the users and groups provisioned from Azure. See View User Details See View Group Details.

1. Navigate to **Connect > Users and Groups** to view the users and groups provisioned from Azure.
   a. See View User Details
   b. See 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 Azure 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 Azure 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

Provides instructions for provisioning users and groups. Import Users and Groups from CSV File. Provision Token for Identity Provider. Provision Users and Groups from Okta.

- 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

View Users and Groups in Secure Access

Provides instructions for viewing users and groups in Secure Access China and links to the detailed views for users and groups.

- View User Details
- View Group Details

6 Provision Users and Groups from Active Directory

Topics:

- Provision Users and Groups from Active Directory

Provides an overview of Provision Users and Groups from Active Directory in Cisco Secure Access China, including Prerequisites for AD Connectors, Connect Multiple Active Directory Domains, and Manage AD Components. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Provision Users and Groups from Active Directory

Provides instructions for provisioning users and Groups from Active Directory in Cisco Secure Access China. Provisioning users and groups from Active Directory (AD) to Cisco Secure Access requires the deployment of a Cisco AD Connector in your environment.

Provisioning users and groups from Active Directory (AD) to Cisco Secure Access requires the deployment of a Cisco AD Connector in your environment. The AD Connector securely retrieves non-sensitive user and group information from your instance of Microsoft AD and integrates the identities with Secure Access. Once your users and groups are provisioned in 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 in Cisco Secure Access China. 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

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

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.

> **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

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

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

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

- For downloading upgrades, allow traffic on 443 (TCP) to **disthost.umbrella.com**.

Connector Account

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

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

Provides instructions for connecting multiple Active Directory Domains in Cisco Secure Access China. 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.

> **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.

Manage AD Components

Provides instructions for managing AD Components in Cisco Secure Access China. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft AD.

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft AD. 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 China

Provides instructions for adding AD Components in Secure Access China. The integration of Active Directory (AD) with Cisco Secure Access China requires that you add the AD components—AD domains and domain controllers—in the organization's environment and register these AD components in Secure Access China.

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

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

Prerequisites

Lists the prerequisites for adding AD components in secure access. Full Admin user role. For more information, see Manage Accounts.

- 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.

Support for Multiple AD Domains and AD Forests

Describes support for Multiple AD Domains and AD Forests. To integrate multiple AD domains or AD forests with Secure Access China 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 China.

To integrate multiple AD domains or AD forests with Secure Access China 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 China.

Procedure

Provides instructions for adding AD components in secure access. Add your AD domain controllers or domains to Secure Access China. After you add the AD components you can view them in Secure Access China.

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

- 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 China
- Add a Domain in Secure Access China

Verify Auditing of Logon Events on Domain Controllers

Provides instructions for 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.

1. 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 China 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** 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 China, download the **Windows Configuration Script for Domain Controller** to the domain controllers in your environments.

1. Navigate to **Connect > Users and Groups > Users**, click **Provision Users**, and then click **Active Directory**.

   After an initial AD deployment, navigate to **Connect > Users and Groups > Users**, click **Configuration management**, and expand **Active Directory**.

2. For **Windows Configuration Script for Domain Controller**, click **Download**.



3. 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. Substitute the Windows configuration script filename (including the .wsf file extension) in the cscript command.

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 China. The configuration script prepares the domain controllers to communicate with the AD Connector.

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

   Important

   Before running the script, you must create the **Cisco_Connector**. 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 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 China. Registration only occurs if you accept this offer.

Repeat the steps to add your domain controllers in Secure Access China. 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.

Add a Domain Controller in Secure Access China

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

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

For LDAP or LDAPS AD queries, AD integration requires that you register an AD domain controller or AD domain in Secure Access China. 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.

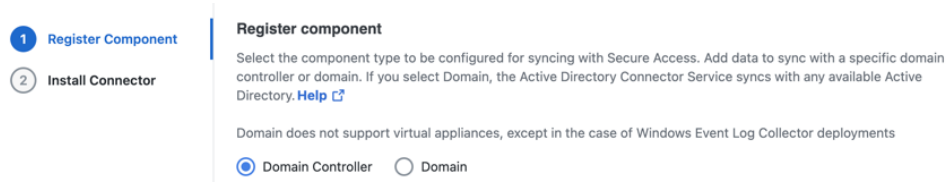
The Cisco AD Connector can only retrieve users and groups from a single domain controller. If you register multiple domain controllers in Secure Access China, the Cisco AD Connector only attempts to perform an LDAP sync against the first domain controller in the list. Ensure that the domain controller 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.

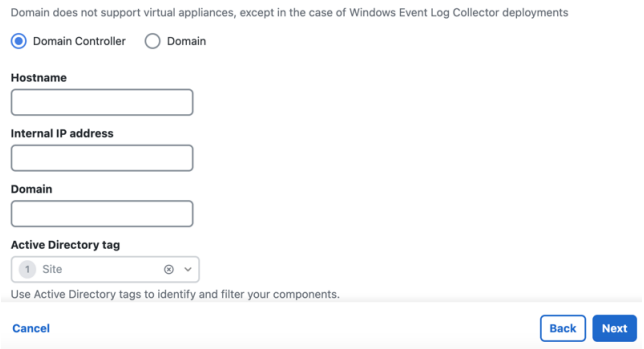
1. Navigate to **Connect > Users and Groups > Users**, click **Provision Users**, and then click **Active Directory**.

   After an initial AD deployment, navigate to **Connect > Users and Groups > Users**, click **Configuration Management**, and expand **Active Directory**.

2. Click **Next**.
3. Choose **Domain Controller** to register the AD domain controller in Secure Access China.



4. Enter the **hostname**, **internal IP address**, and **domain** of the domain controller.
5. For **Active Directory tag**, choose a Site to associate with the AD component.

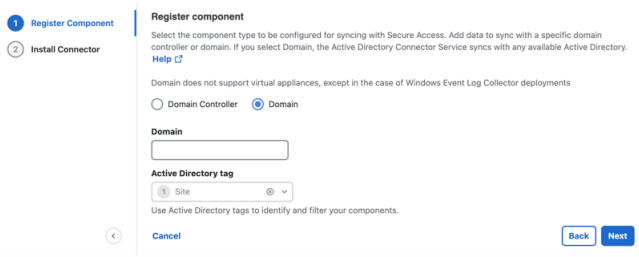


6. Click **Next**, and then follow the instructions to install the AD Connector.

Add a Domain in Secure Access China

Provides instructions for adding a domain in Secure Access China. Choose Domain to register the AD domain component. For Domain , enter the domain name.

1. Choose **Domain** to register the AD domain component.
2. For **Domain**, enter the domain name.
3. For **Active Directory tag**, choose a Site to associate with the AD component.
4. 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 in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for managing sites for AD components. 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.

- 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

Provides instructions for managing sites for AD components. Manage a Site for an AD component that is deployed in your on-premises environment.

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

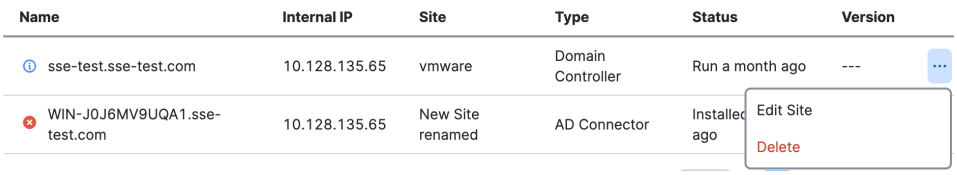
- Edit a Site

Edit a Site

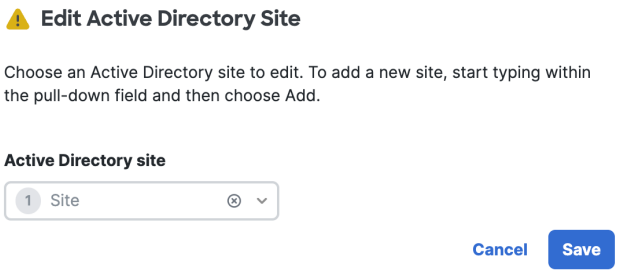
Provides instructions for editing a site. Choose a Site for the AD component in the organization on Secure Access. Navigate to Connect > Users and User Groups , click Configuration management , and then expand Active Directory.

Choose a Site for the AD component in the organization on Secure Access.

1. Navigate to **Connect > Users and User Groups**, 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 China

Provides instructions for viewing AD Components in Secure Access China. The integration of Active Directory (AD) with Cisco Secure Access requires that you add the organization's AD components on Secure Access China and integrate a Cisco AD Connector.

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

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

Prerequisites

Lists the prerequisites for viewing AD components in secure access. Full Admin user role. For more information, see Manage Accounts.

- 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

Provides instructions for viewing AD components in secure access. In Secure Access China, view the AD components and AD Connectors that you deployed.

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

View AD Components in Secure Access China

Provides instructions for viewing ad components in Secure Access China. It can take up to four hours for large numbers of AD user and group objects to synchronize for the first time.

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 China through the AD Connector successfully. Any subsequent changes should also sync successfully.

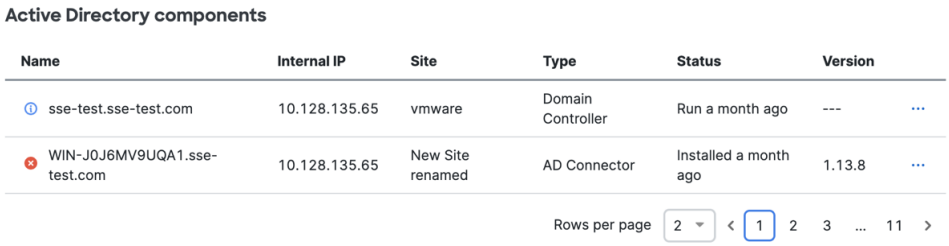
Note

If the AD Connector does not appear in Secure Access China 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.

1. Navigate to **Connect > Users and User Groups**, 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.
   - **Site**–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

Provides instructions for deleting AD Components in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for deleting ad components, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for deleting AD components. Remove a single AD component for the organization or delete all AD components that you registered with Secure Access.

Remove a single AD component for the organization or delete all AD components that you registered with Secure Access.

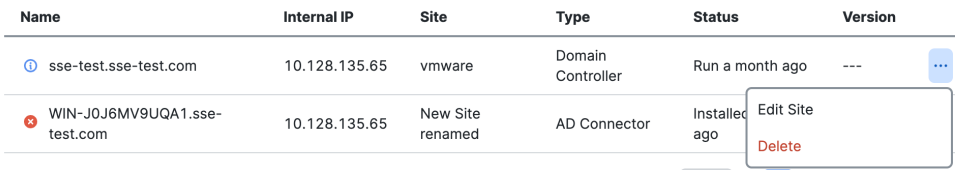
- Delete an AD Component
- Remove All AD Components

Delete an AD Component

Provides instructions for deleting an ad component. Delete a single AD component that was added in Secure Access. Navigate to Connect > Users and User Groups , click Configuration management , and then expand Active Directory.

Delete a single AD component that was added in Secure Access.

1. Navigate to **Connect > Users and User Groups**, 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**.



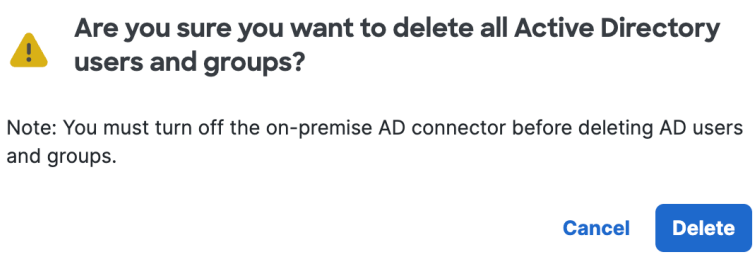
4. Click **Delete** to confirm the removal of the AD component in Secure Access.

Remove All AD Components

Provides instructions for removing all ad components. Remove all AD components for the organization in Secure Access. Navigate to Connect > Users and User Groups , click Configuration Management > Configurations , and then expand Active Directory.

Remove all AD components for the organization in Secure Access.

1. Navigate to **Connect > Users and User Groups**, click **Configuration Management > Configurations**, 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

Provides instructions for managing AD Connectors in Cisco Secure Access China. 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 and groups 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.

Configure Authentication for AD Connectors

Provides instructions for configuring authentication for AD Connectors in Cisco Secure Access China. Cisco Secure Access communicates with the deployed Cisco Active Directory (AD) Connectors in your environments.

Cisco Secure Access communicates with the deployed Cisco Active Directory (AD) Connectors in your environments. Secure Access makes software syncs and health checks to the AD Connectors and requires that API requests from the AD Connectors use authentication. For information about deploying the Cisco AD Connector, see Connect Active Directory to Secure Access.

To manage the authentication of the communications from the AD Connectors to Secure Access, we recommend that you configure API key credentials for your AD Connector deployments. Your API key credentials apply to all AD Connectors that are deployed in your environment.

How to Set Up Your API Credentials

Describes how to Set Up Your API Credentials. Secure Access client API key credentials are valid for 90 days. First, create the Secure Access Key Admin API key and secret.

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. Your Secure Access client API key credentials are stored in the AD Connectors that are deployed in the organization.

Important

Secure Access client API key credentials are valid for 90 days.

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.

Prerequisites

Lists the prerequisites for configuring authentication for AD connectors and vas. Full Admin user role. For more information, see Manage Accounts.

- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

Provides instructions for configuring authentication for AD connectors and vas. 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 AD Connectors that you deploy in your environments. The generated API credentials (key and secret) apply to all AD Connectors in the organization.

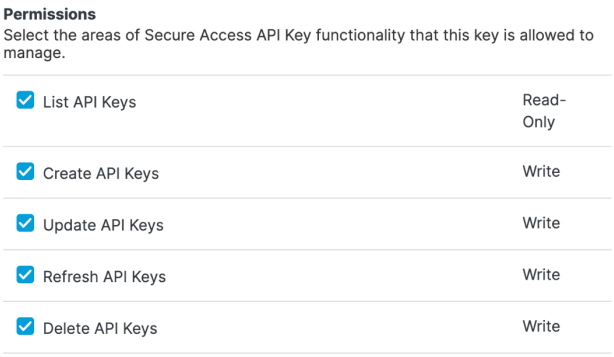
- Step 1 – Create the Key Admin API Key Credentials
- Step 2 – Add the Key Admin API Key Credentials

Step 1 – Create the Key Admin API Key Credentials

Describes 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.

1. 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.



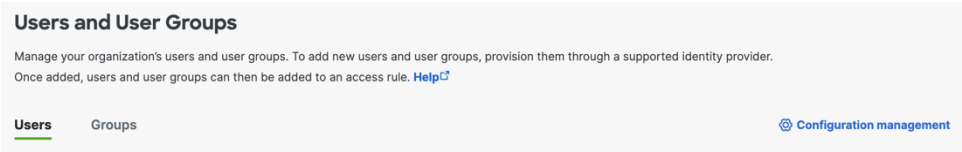
> **Note**
>
> Save your Key Admin API key and secret and use these credentials to configure the authentication for the AD Connectors in the organization.

Step 2 – Add the Key Admin API Key Credentials

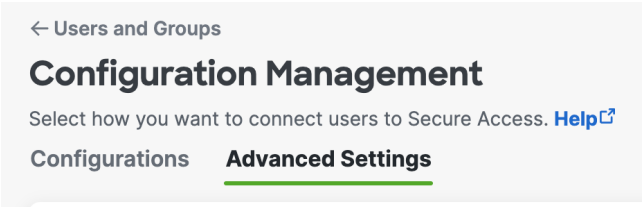
Describes step 2 – Add the Key Admin API Key Credentials. Add the Secure Access Key Admin API key and secret to the AD Connector in Users and Groups > Configuration Management > API Authentication . Then, generate a Secure Access client API key and secret.

Add the Secure Access Key Admin API key and secret to the AD Connector in **Users and Groups > Configuration Management > API Authentication**. Then, generate a Secure Access client API key and secret.

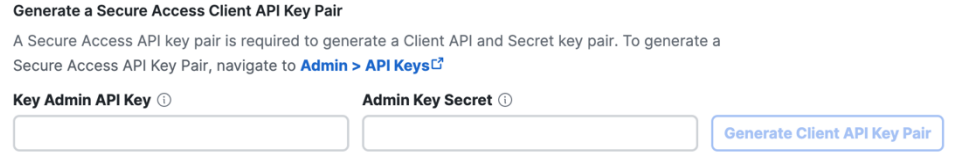
1. Navigate to **Connect > Users and User Groups > Configuration Management**.



2. Click **Advanced Settings**.

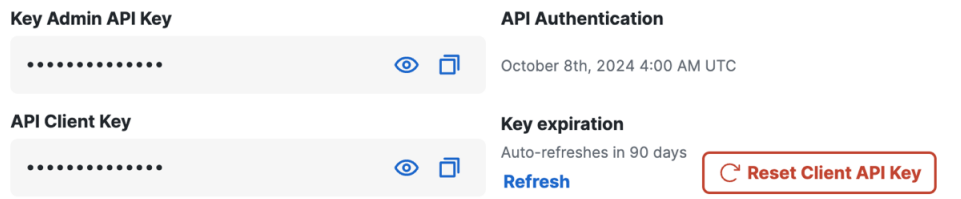


3. For **Key Admin API Key**, add the Key Admin API key, and for **Key Admin Key Secret**, add the Key Admin API key secret. For information about creating the Key Admin API key, see Step 1 – Create the Key Admin API Key Credentials.



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.

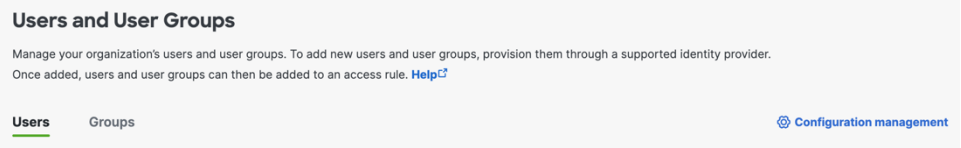


Refresh Client API Key and Secret

Describes refresh Client API Key and Secret. Refresh your Secure Access client API key and secret. Navigate to Connect > Users and User Groups > Configuration Management.

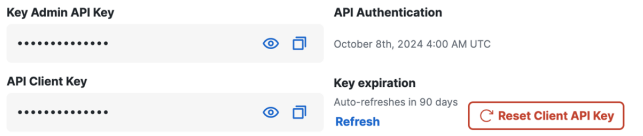
Refresh your Secure Access client API key and secret.

1. Navigate to **Connect > Users and User Groups > Configuration Management**.

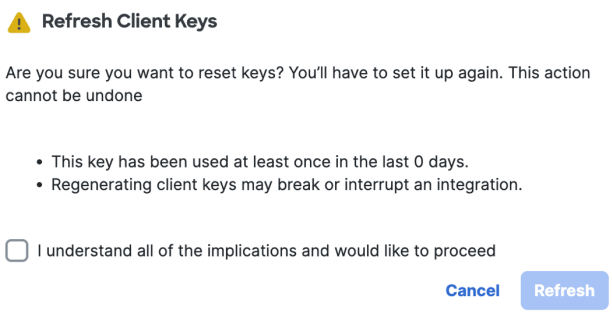


2. Click **Advanced Settings**.
3. Click **Refresh**.

   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

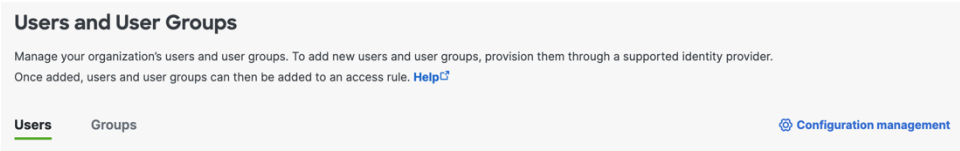
Describes reset Client API Key. Delete your Secure Access Key Admin API key and Secure Access client API key. Navigate to Connect > Users and User Groups > Configuration Management.

Delete your Secure Access Key Admin API key and Secure Access client API key.

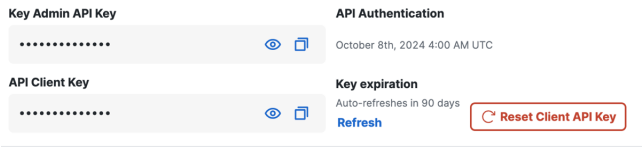
Important

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.

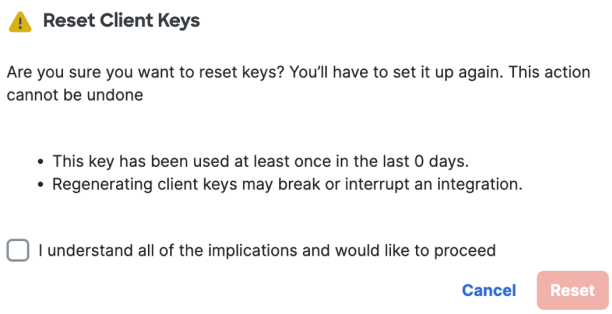
1. Navigate to **Connect > Users and User Groups > Configuration Management**.



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 in Cisco Secure Access China. You can schedule the date and time that Cisco Secure Access updates the Active Directory (AD) Connector software on your deployed Cisco 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. 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.

Prerequisites

Lists the prerequisites for configuring updates on AD connectors. 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.

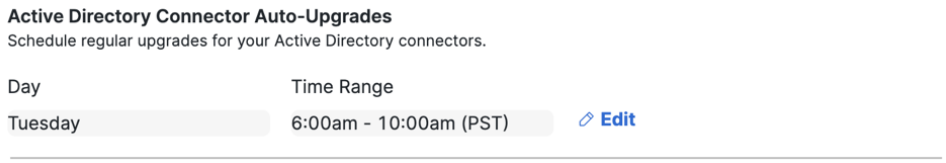
- Full Admin user role. For more information, see Manage Accounts.
- Deploy an AD Connector in your environment. For more information, see Connect Active Directory to Secure Access.

Procedure

Provides instructions for configuring updates on AD connectors. Select the day and time to update your deployed AD Connectors automatically.

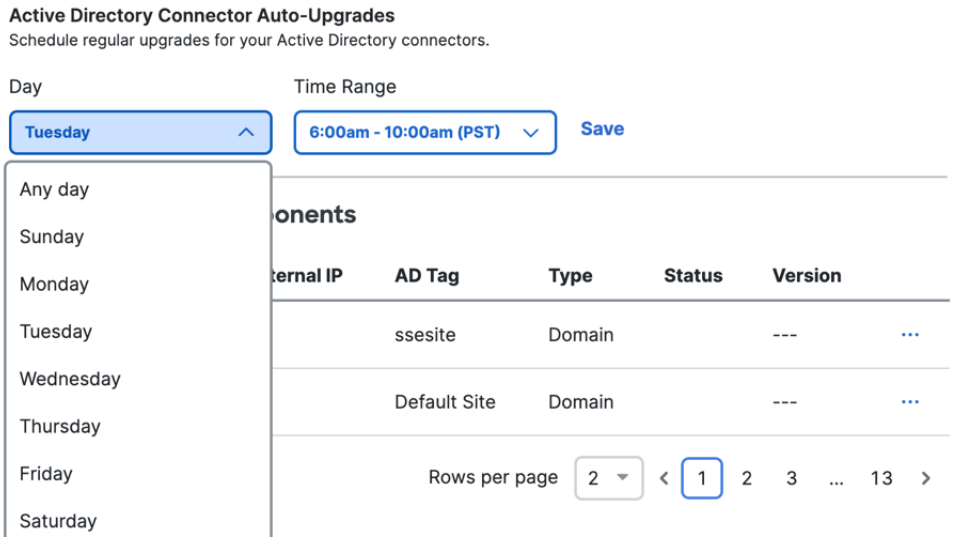
Select the day and time to update your deployed AD Connectors automatically.

1. Navigate to **Connect** > **Users and Groups** > **Configuration Management**.
2. For **Provisioning**, expand **Active Directory**.
3. Navigate to **Active Directory Connector Auto-Upgrades**, and then click **Edit**.



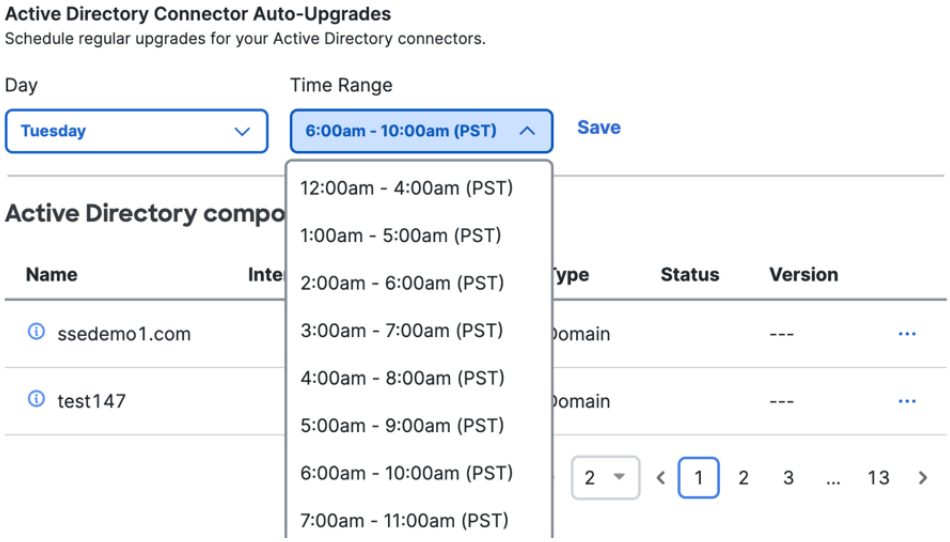
4. For **Day**, choose the day of the week to update the AD Connector software.

> **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

Provides instructions for 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 and groups 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.

Prerequisites

Lists the prerequisites for connecting active directory to secure access 1. Full Admin user role. For more information, see Manage Accounts.

- 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.
- (Optional) Configure software updates on the AD Connector. For more information, see Configure Updates on AD Connectors.

Procedure

Provides instructions for connecting active directory to secure access 1. Download the software package for the Cisco AD Connector and install an AD Connector in your environment.

Download the software package for the Cisco AD Connector and install an AD Connector in your environment.

- Step 1 – Download the Active Directory Connector
- Step 2 – Install the Active Directory Connector

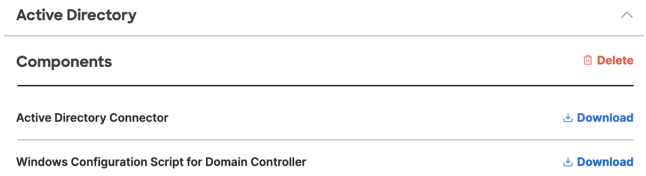
Step 1 – Download the Active Directory Connector

Describes 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.

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 and Groups > Users** and click **Provision Users**, or navigate to **Connect > Users and Groups > Groups** and click **Provision Groups**.
3. For **Provisioning Method**, click **Active Directory** or expand **Active Directory**.
4. For **Active Directory Connector**, click ** Download** to save the 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

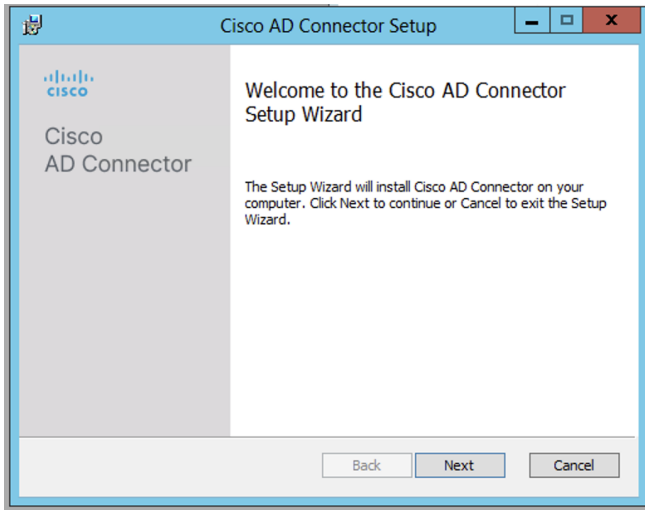
Describes step 2 – Install the Active Directory Connector. As an administrator, extract the contents of the Cisco AD Connector ZIP file to a folder on the server, and then navigate to that folder.

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.

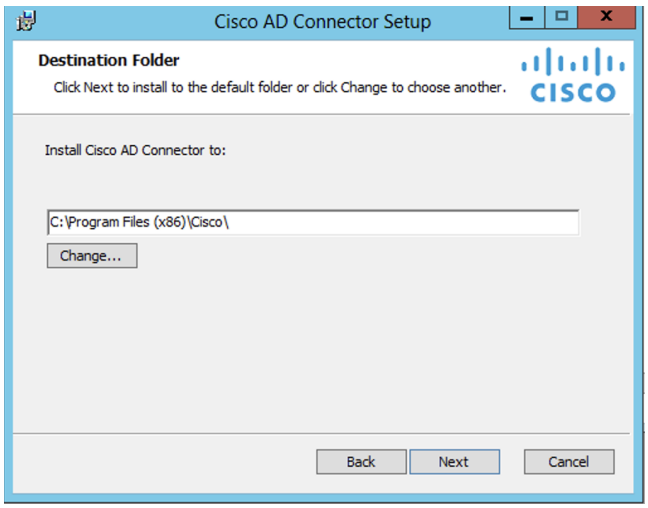
Note

If you run the AD Connector installer from the root directory of your server, you may encounter installation errors.

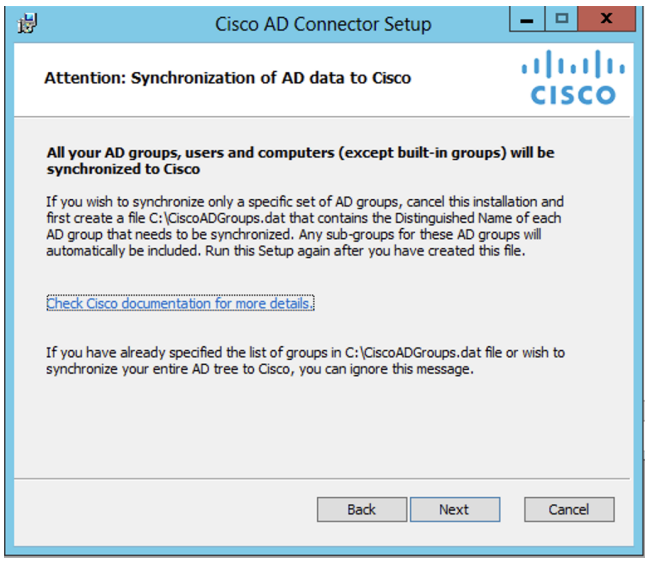
1. Run **setup.msi**, and then in the **Cisco AD Connector Setup** wizard, click **Next**.



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.

Rename Selective Sync File After Upgrading to AD Connector v1.14.4

Provides instructions for renaming 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. 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.

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**
>
> **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.

Supported Organizational Units

Describes supported organizational units for directory synchronization and identifies the organizational units available for Secure Access management. for administrators to review.

```
CN=My Group,OU=Organizational Unit,DC=sample,DC=local
```

Unsupported Organizational Units

Shows a distinguished name example for an unsupported organizational unit, such as OU=My OU,OU=Organizational Unit,DC=sample,DC=local, in directory synchronization. for administrators to review.

```
OU=My OU,OU=Organizational Unit,DC=sample,DC=local
```

Sample File Entries

Shows sample file entries and provides examples administrators can use when reviewing the supported file formats and data fields. for administrators to review.

```
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

Describes 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.

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.

Deploy LDIF Files for AD Connector

Provides instructions for deploying LDIF Files for AD Connector in Cisco Secure Access China. The Cisco Active Directory (AD) Connector integrates with Cisco Secure Access to provision the organization's users and groups from AD.

The Cisco Active Directory (AD) Connector integrates with Cisco Secure Access to provision the organization's users and groups from AD. You can install and configure the AD Connector to provision users and groups using LDAP Interchange Format (LDIF) source files. Once you deploy the LDIF files on your server, the AD Connector syncs the users and groups in your organization with Secure Access.

For information about deploying the AD Connector with LDAP or LDAPS, see Connect Active Directory to Secure Access.

Best Practices for LDIF Source Deployments

Describes best Practices for LDIF Source Deployments. If you use both deployment methods, you may add duplicate users and groups in your organization.

- 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

Describes deploy ldif files for AD connector. Requirements for deploying LDIF source files on your server:. LDIF can support multiple domains.

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

Lists known limitations for deploying LDIF source files with the AD Connector, including no support for selective groups-only sync or incremental sync.

- No support for selective groups-only sync.
- No support for incremental sync.

Prerequisites

Lists the prerequisites for deploying ldif files for AD connector. Full Admin user role. For more information, see Manage Accounts.

- 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

Provides instructions for deploying ldif files for AD connector. Download, install, and configure the Cisco AD Connector. Then, deploy the LDIF source files.

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

Describes 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.

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 and Groups > Users** and click **Provision Users**, or navigate to **Connect > Users and Groups > Groups** and click **Provision Groups**.
3. For **Provisioning Method**, click **Active Directory** or expand **Active Directory**.
4. For **Active Directory Connector**, click ** Download** to save the Cisco AD connector deployment 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.

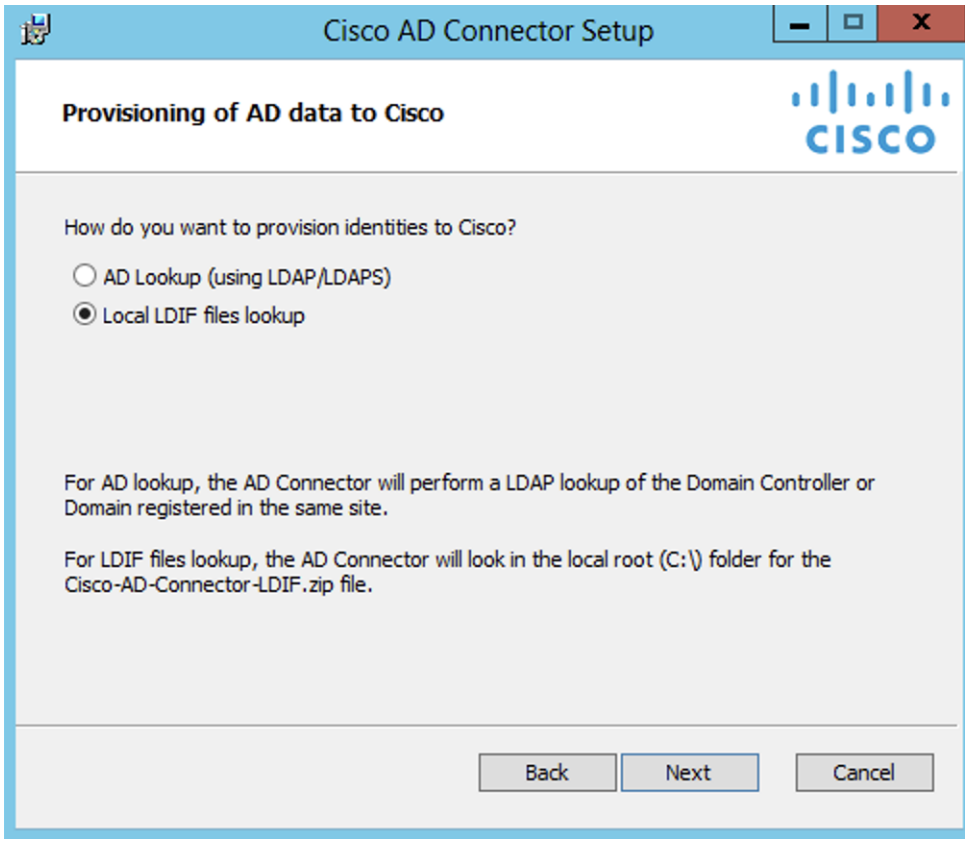
Step 2 - Install the Cisco AD Connector

Describes 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.

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**.



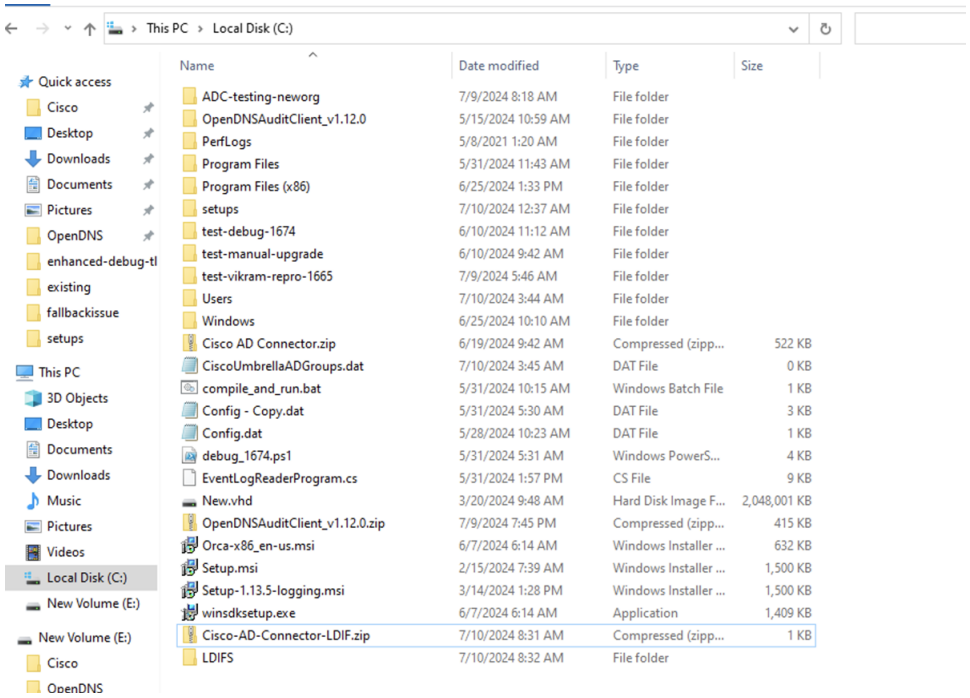
Step 3 – Deploy the LDIF Source Files

Describes step 3 – Deploy the LDIF Source Files. Deploy the LDIF source files on your server. For more information, see Best Practices for LDIF Source Deployments and Requirements.

Deploy the LDIF source files on your server. For more information, see Best Practices for LDIF Source Deployments and Requirements.

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**.

3. Once you create the ZIP file, the AD Connector automatically syncs the users and groups with Secure Access. Syncs occur every five minutes.



Troubleshooting

Describes provisioning errors that can occur when the AD Connector uses LDIF source files and provides context for troubleshooting those conditions.

Various configuration conditions of the AD Connector with LDIF source files can result in provisioning errors.

Scenario 1

Describes 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.

- 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

Describes 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.

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

Describes 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.

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

Describes 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.

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

Describes 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:.

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

Describes Change the Connector Account Password in Cisco Secure Access China. For regulatory compliance, you may need to change the password of the Cisco Active Directory (AD) Connector account.

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 cannot accurately identify Web requests with the AD users or groups, and cannot sync user and group changes from AD.

Prerequisites

Lists the prerequisites for changing the connector account password. Administrative privileges on the server where you will install the AD Connector.

- 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

Provides instructions for changing the connector account password. Sign in to the account from any system that is a member of the domain and then set the new password.

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**. 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 Active Directory Service** service.
6. Repeat steps 2 and 3 for each deployed AD Connector.

How to Connect Active Directory to Secure Access

Describes how to Connect Active Directory to Secure Access. Add domain controllers or domains in Secure Access for LDAP or LDAPS deployments. For more information, see Add AD Components 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.
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 and groups 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.

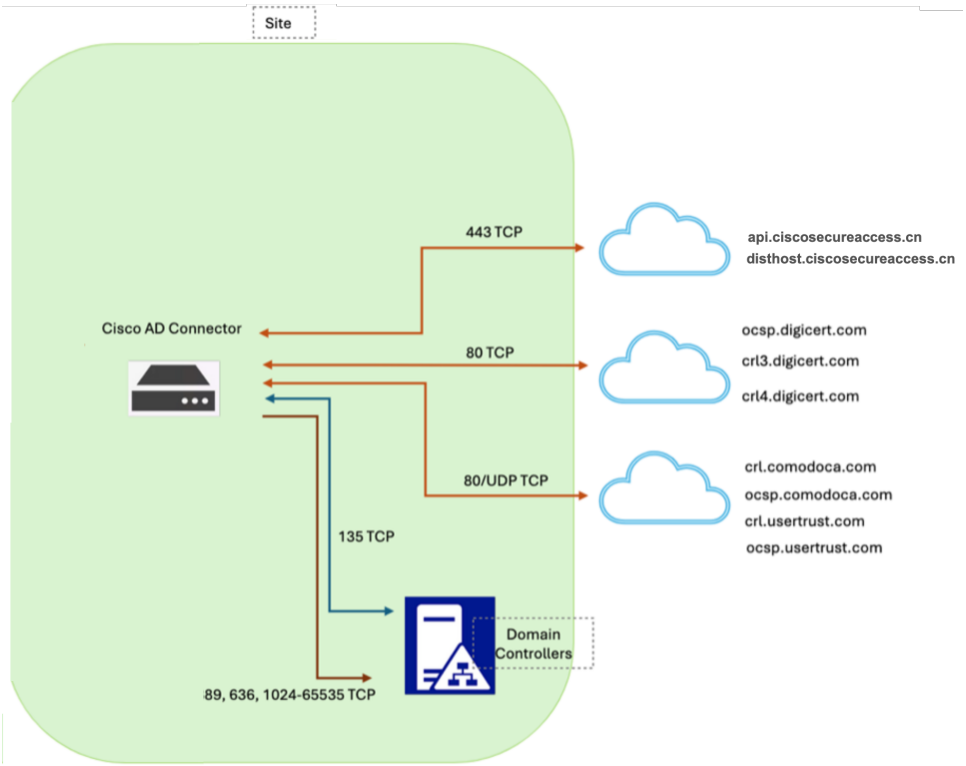
AD Connector Communication Flow and Troubleshooting

Describes AD Connector Communication Flow and Troubleshooting in Cisco Secure Access China. The Cisco Active Directory (AD) Connector is a Windows application and service that communicates with Cisco Secure Access China and AD domain controllers.

The Cisco Active Directory (AD) Connector is a Windows application and service that communicates with Cisco Secure Access China and AD domain controllers. The Cisco AD Connector only syncs the required AD User and Group attributes with Secure Access China.

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 China, and the steps that you can take to troubleshoot your Cisco AD Connector deployment.

The diagram includes the deployment of the Secure Access China Virtual Appliance.



Communication Flow

Describes communication Flow. The Cisco AD Connector retrieves the AD Users and Groups details only. Secure Access China stores these required attributes from each object:.

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, the Cisco AD Connector sends the AD data every five minutes using an HTTPS connection on TCP port 443. However, it can take an hour or longer for changes to reflect in Secure Access China.

Secure Access China stores these required attributes from each object:

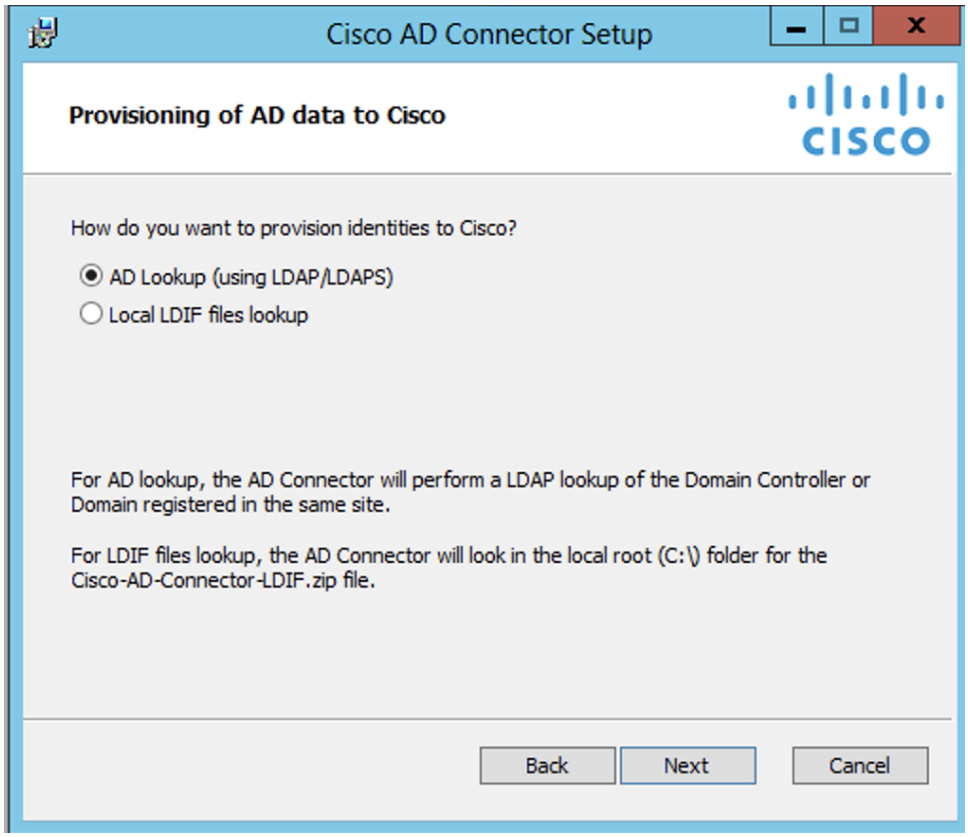
- `sAMAccountName`–The username that you use to sign into the Cisco AD Connector.
- `dn`–The distinguished name.
- `userPrincipalName`–The user's principal name.
- `memberOf`–The groups that include the user.
- `objectGUID`–The group ID of the object. This property is sent to Secure Access China as a 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 China 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\\CiscoADConnector\\ADSync`.

   Review the files in the **.ldif** files in the **ADSync** directory to confirm that the Cisco AD Connector synchronized the AD Users and Groups data to Secure Access China.

   > **Note**
   >
   > When you install the Cisco AD Connector, you have the option to turn off the local storage of `.ldif` files.



Troubleshooting

Provides recommendations for troubleshooting communication problems with the Cisco AD Connector and checking its communication flow and configuration. for administrators to review.

Recommendations for troubleshooting the communications with the Cisco AD Connector.

Network Requirements

Describes network Requirements. The Cisco AD Connector communicates with Secure Access China and the deployed domain controllers. Ensure that you allow certain domains and services on your firewalls. For more information, see Network Requirements for Secure Access China.

The Cisco AD Connector communicates with Secure Access China and the deployed domain controllers. Ensure that you allow certain domains and services on your firewalls. For more information, see Network Requirements for Secure Access China.

Table 1:

Port and Protocol	Source	Destination	Note
443/TCP	AD Connector	**api.ciscosecureaccess.cn** **disthost.ciscosecureaccess.cn**	• Initial registration with the Secure Access China • Automatic updates • Health status reporting in Secure Access China
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 China, we recommend that you check for any Layer-7 application proxies, which may block or drop data sent to Secure Access China. A common case is the **inspect** feature on Cisco devices that communicate on HTTP, or HTTPS. For more information, see Cisco Security Appliance Command Line Configuration Guide, Version 7.2.

Restart the Active Directory Connector

Describes restart the Active Directory Connector. You can restart the Cisco AD Connector service on the AD Connector server. Restarting the Cisco AD Connector triggers a full synchronization of the AD Users and Groups, not only the changes from the previous sync to Secure Access China.

You can restart the **Cisco AD Connector** service on the AD Connector server. Restarting the Cisco AD Connector triggers a full synchronization of the AD Users and Groups, not only the changes from the previous sync to Secure Access China.

If your Cisco AD Connector is not in the **Okay** state, contact Support.

Next Steps

Describes next Steps. Review the requirements for setting up the AD components and Cisco AD Connector in your environment. For more information, see Prerequisites for AD Connectors.

1. Review the requirements for setting up the AD components and Cisco AD Connector in your environment. For more information, see Prerequisites for AD Connectors.
2. Review how to connect multiple AD domains. For more information, see Connect Multiple Active Directory Domains.
3. Manage the AD components with Secure Access. For more information, see Manage AD Components.
4. Manage the AD Connectors. For more information, see Manage AD Connectors.
5. View the installed AD components. For more information, see View AD Components in Secure Access.
6. Troubleshoot the AD deployments. For more information, see AD Connector Communication Flow and Troubleshooting.

7 Configure Integrations with SAML Identity Providers

Topics:

- Configure Integrations with SAML Identity Providers

Provides an overview of Configure Integrations with SAML Identity Providers in Cisco Secure Access China, including Prerequisites for SAML Authentication, Configure Azure AD for SAML, and Configure Okta for SAML. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Configure Integrations with SAML Identity Providers

Provides instructions for configuring integrations with SAML Identity Providers in Cisco Secure Access China. 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, 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.

Prerequisites for SAML Authentication

Describes Prerequisites for SAML Authentication in Cisco Secure Access China. 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

Lists the Secure Access China service provider metadata values, including the entity ID and entity URL used to configure SAML identity providers.

- Secure Access China Entity ID– **saml.id.ciscosecureaccess.cn**
- Secure Access Entity URL–**fg.id.ciscosecureaccess.cn/gw/auth/acs/response**

Requirements

Describes prerequisites for SAML authentication. 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.

- If your organization integrates with AD FS, we recommend that you bypass web traffic to the **id.ciscosecureaccess.cn** domain on the Secure Access secure web gateway (SWG). Otherwise, send **id.ciscosecureaccess.cn** requests to the SWG, not directly to the internet. For more information about bypassing domains and Secure Access Web security, see Manage Internet Security.
- 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 Web Profile

Provides instructions for enabling saml and https inspection in the web profile. To obtain the user identity of a device through SAML, you must enable SAML and HTTPS inspection in the Web profile. For more information, see Manage Web Profiles.

- To obtain the user identity of a device through SAML, you must enable SAML and HTTPS inspection in the Web profile. For more information, see Manage Web 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 Azure AD for SAML

Provides instructions for configuring azure AD for SAML in Cisco Secure Access China. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the Azure AD SAML IdP with Secure Access by uploading the Azure AD XML metadata file to Secure Access, or alternatively add the Azure AD metadata in Secure Access manually.

For information about provisioning an organization's users from Azure AD in Secure Access, see Provision Users and Groups from Azure.

Prerequisites

Lists the prerequisites for configuring Azure for SAML. 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.

- 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.ciscosecureaccess.cn** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Internet Security.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access Web profile. For more information, see Manage Web 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 Web 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 Web 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 Internet Security.

We recommend that you bypass certain domains on the secure web gateway. For more information, see Manage Internet Security.

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

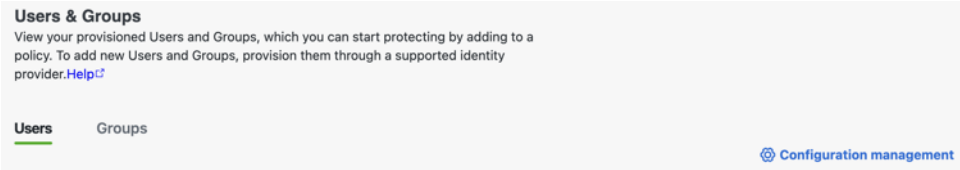
Provides instructions for configuring Azure for SAML. Step 1 – Choose an Authentication Method. Step 2 – Add an Identity Provider.

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Configure the Identity Provider's SAML Metadata

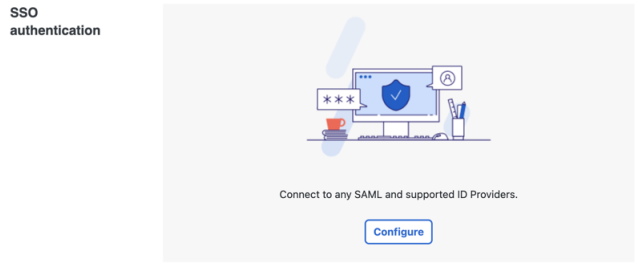
Step 1 – Choose an Authentication Method

Describes step 1 – Choose an Authentication Method. Navigate to Connect > Users and Groups and click Configuration Management. Navigate to SSO authentication and click Configure.

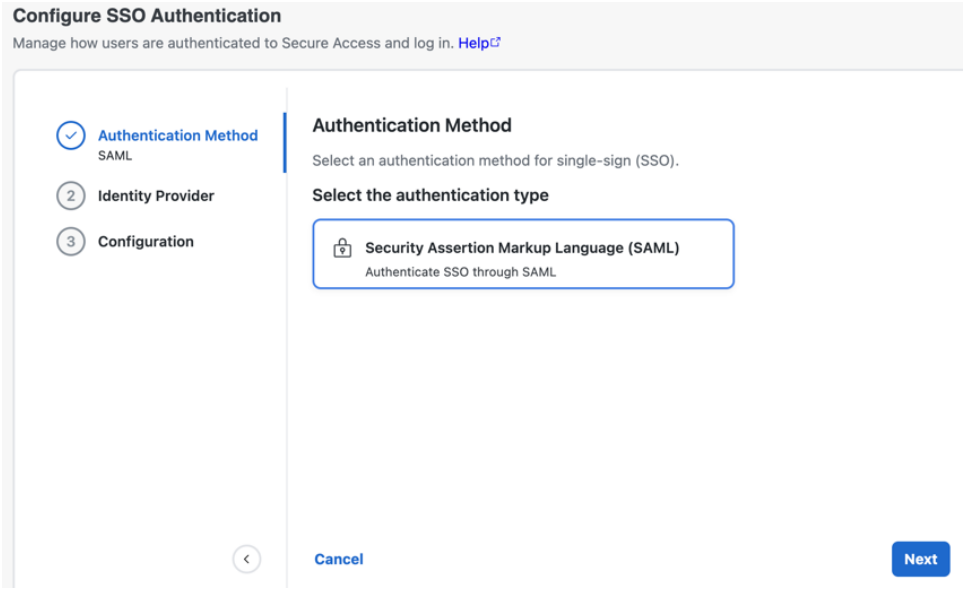
1. Navigate to **Connect > Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



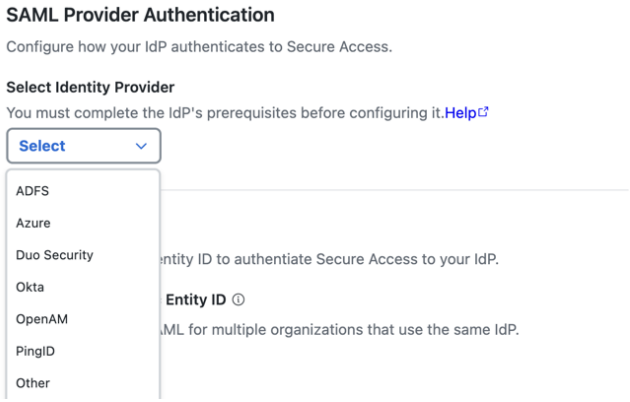
3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.



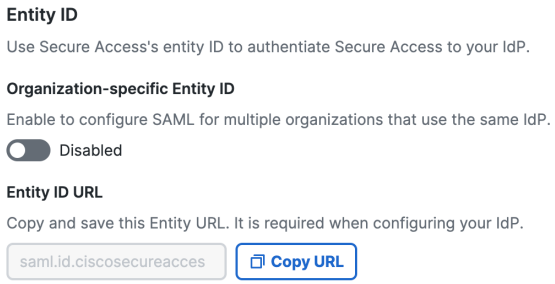
Step 2 – Add an Identity Provider

Describes step 2 - Add an Identity Provider. For Identity Provider , choose Azure . Secure Access supports various IdPs.

1. For **Identity Provider**, choose **Azure**. Secure Access supports various IdPs.



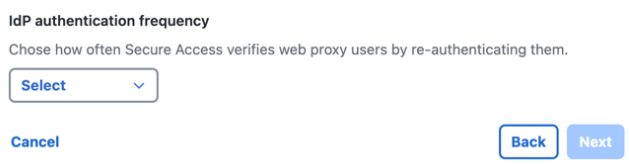
2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.id.ciscosecureaccess.cn**. 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.id.ciscosecureaccess.cn**.



4. Choose a time interval when a user must authenticate with Secure Access, or select **Never**.

   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 Azure AD. The Secure Access Metadata XML file includes the Secure Access root certificate.

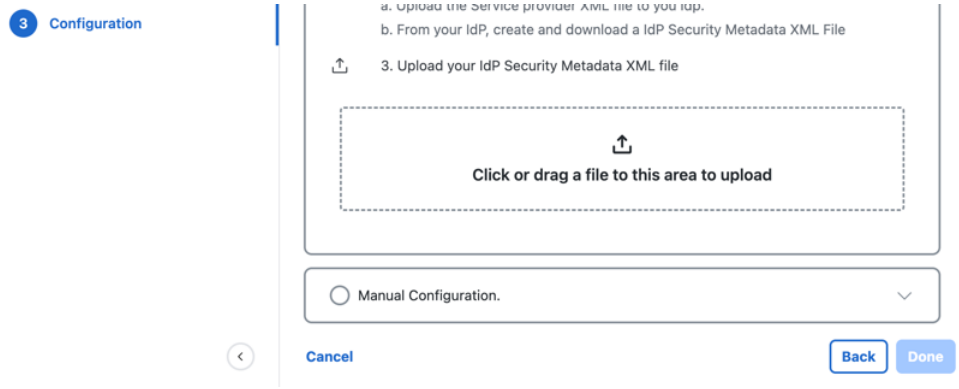
Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Azure AD. The Secure Access Metadata XML file includes the Secure Access root certificate.

> **Note**
>
> Azure AD (Microsoft Entra) 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

Describes 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_SSE_SP_Metadata XML file to your local device.

1. Check **Manual Configuration**, and then click **Download service provider XML file** to save the **Cisco_SSE_SP_Metadata** XML file to your local device.



2. Open the **Cisco_SSE_SP_Metadata** XML file.
3. Copy the certificates from the **Cisco_SSE_SP_Metadata** XML file to a new file and save. Use the certificate file in the next step when you create the app integration in Azure.

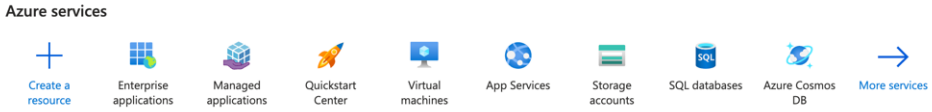
Step 3b – Add Secure Access Service Provider Metadata to Azure AD

Describes step 3b - Add Secure Access Service Provider Metadata to Azure AD. Add the Secure Access service provider metadata to your instance of Azure AD.

Add the Secure Access service provider metadata to your instance of Azure AD.

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.

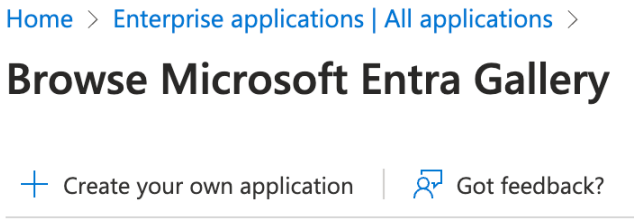
1. Sign in to Azure and navigate to **Azure services > Enterprise Applications**.



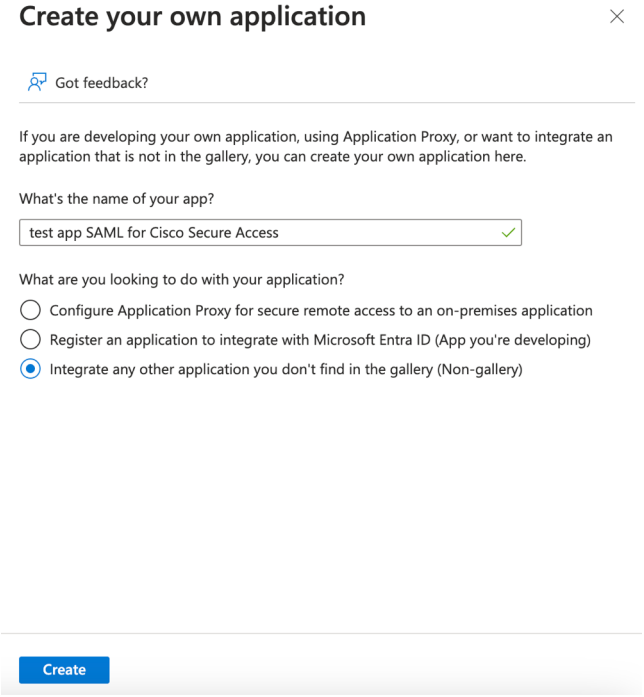
2. Select **New Application**.



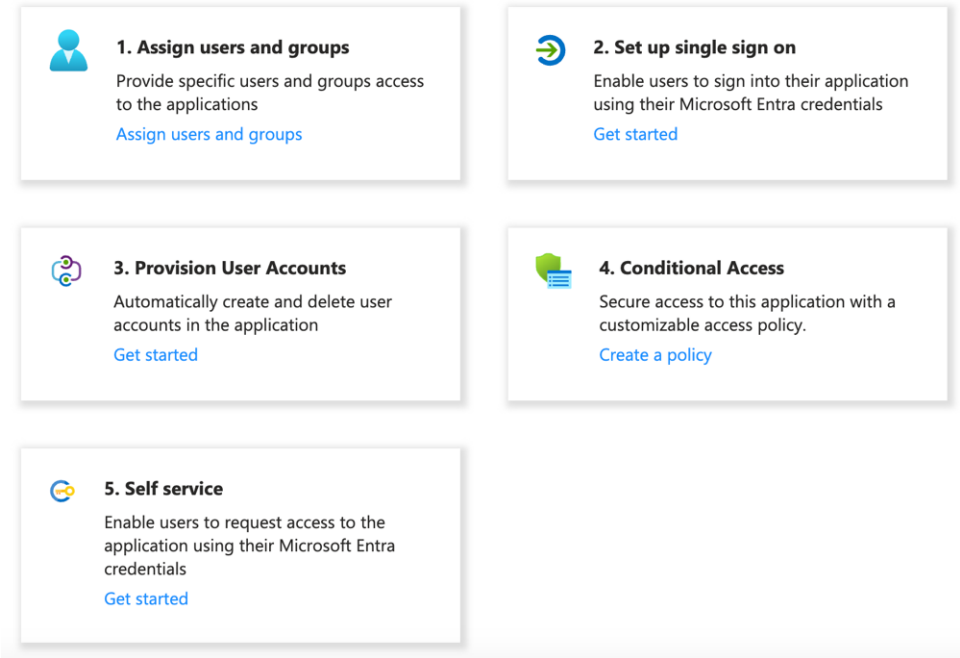
3. Select **Create your own Application**.



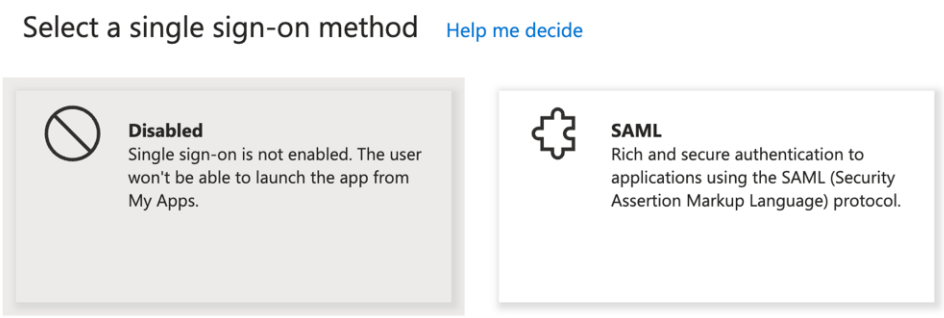
4. Give the new application a meaningful name, select **Integrate any other application you don't find in the gallery (Non-gallery)**, and then click **Create**.



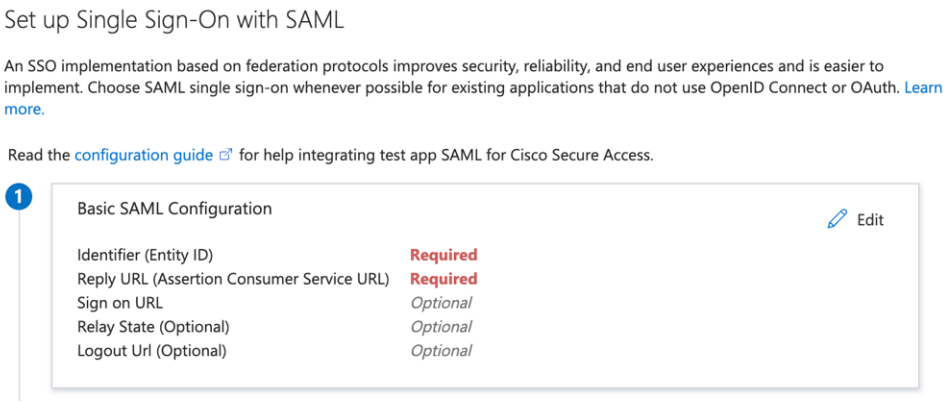
5. Navigate to **Getting Started**, and then click **Set up single sign on**.



6. Click **SAML** to select the sign-on method.

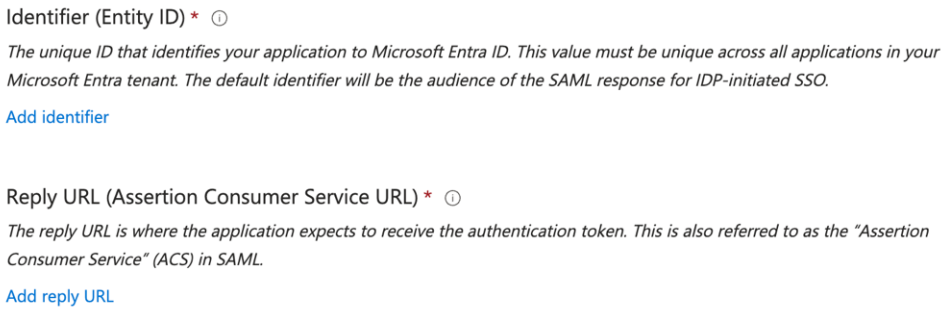


7. For **Basic SAML Configuration**, click **Edit**.

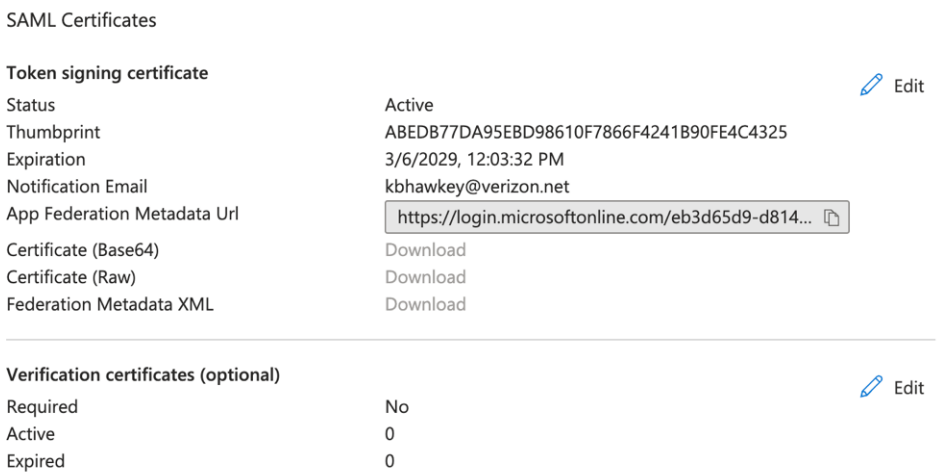


   a. For **Identifier (Entity ID)** (Microsoft Entra ID), click **Add identifier** and enter **saml.id.ciscosecureaccess.cn** in the text area.

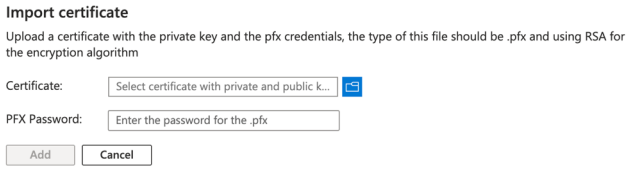
   b. For **Reply URL (Assertion Consumer Service URL)**, click **Add reply URL** and enter **https://fg.id.ciscosecureaccess.cn/gw/auth/acs/response**.



8. **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.



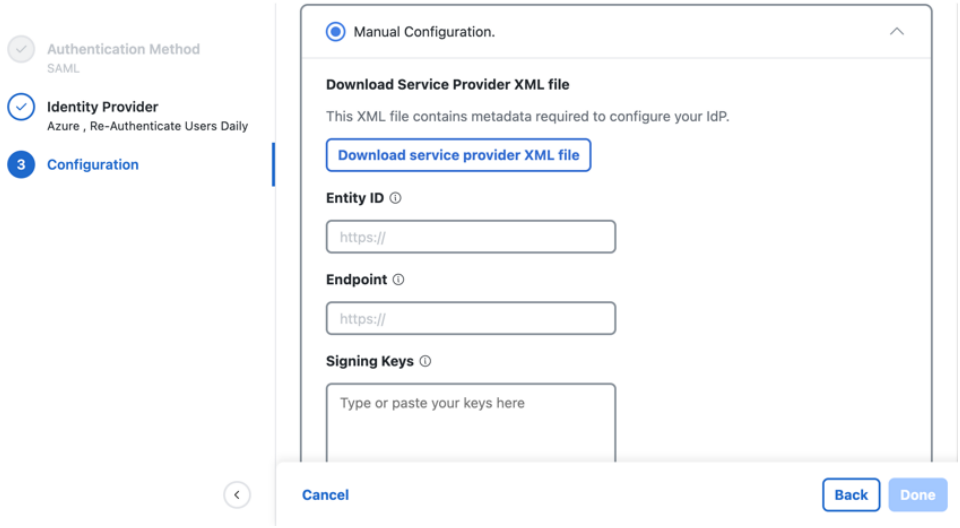
9. Download the **Federation Metadata XML** file. Use the file to upload the configured Azure SAML attributes to Secure Access.

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

Provides instructions for 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

Provides instructions for 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 Okta for SAML

Provides instructions for configuring okta for SAML in Cisco Secure Access China. 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.

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.

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.

Prerequisites

Lists the prerequisites for configuring Okta for SAML. Full Admin user role. For more information, see Manage Accounts. Send id.ciscosecureaccess.cn requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.

- Full Admin user role. For more information, see Manage Accounts.
- Send **id.ciscosecureaccess.cn** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Internet Security.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access web profile. For more information, see Manage Web 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.
- Enable HTTPS Inspection in the Secure Access Web 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 Web Profiles.
- You must install the Cisco Secure Access root certificate on all client machines that connect on networks or network tunnels where SAML is enabled. For more information, see Manage Certificates.

Procedure

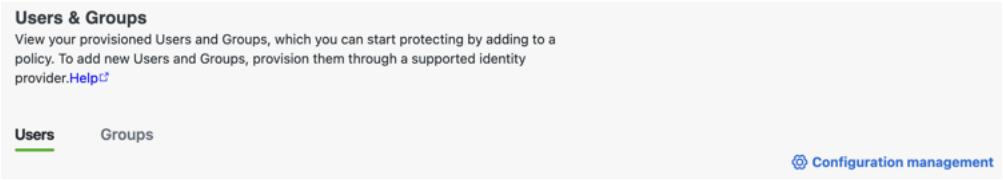
Provides instructions for configuring Okta for SAML. Step 1 – Choose an Authentication Method. Step 2 – Add an Identity Provider.

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Configure the Identity Provider's SAML Metadata

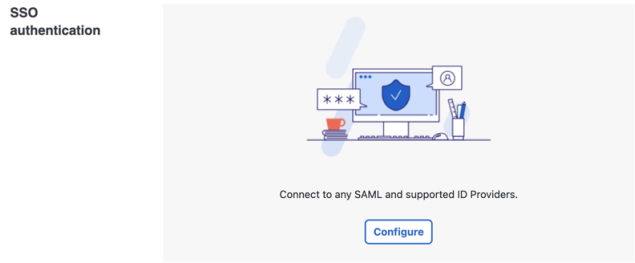
Step 1 – Choose an Authentication Method

Describes step 1 – Choose an Authentication Method. Navigate to Connect > Users and Groups and click Configuration Management. Navigate to SSO authentication and click Configure.

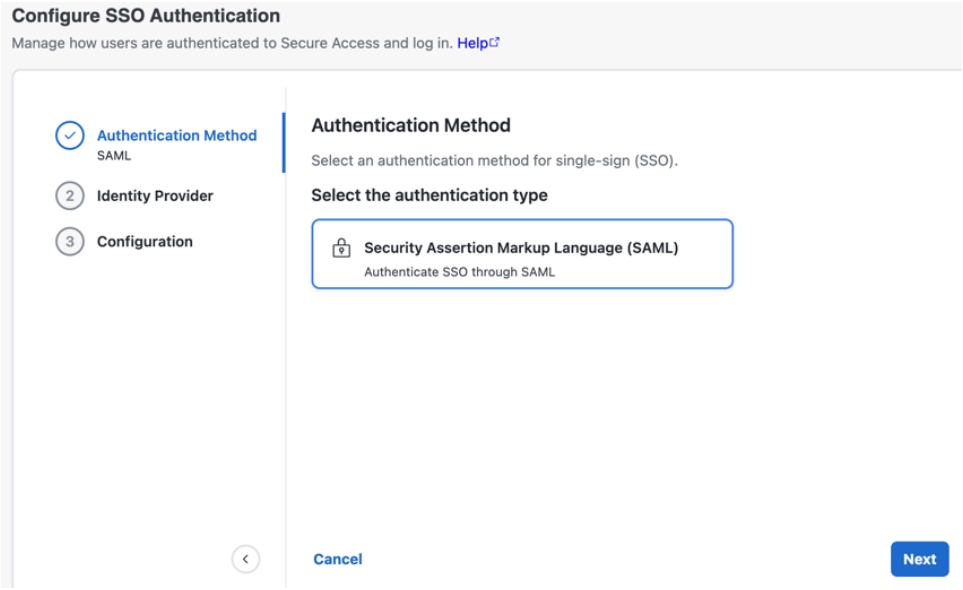
1. Navigate to **Connect > Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



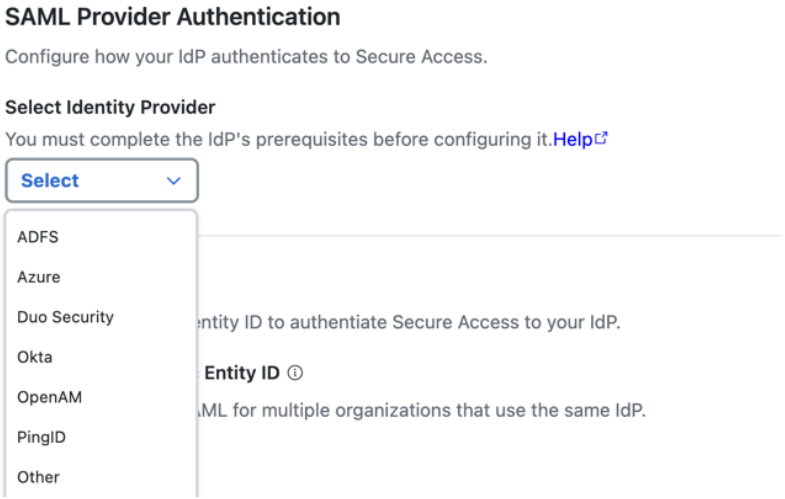
3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.



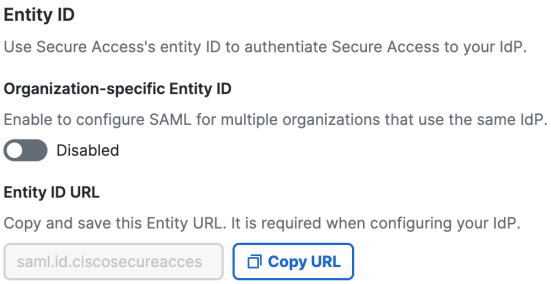
Step 2 – Add an Identity Provider

Describes step 2 - Add an Identity Provider. For Identity Provider , choose Okta . Secure Access supports various IdPs.

1. For **Identity Provider**, choose **Okta**. Secure Access supports various IdPs.



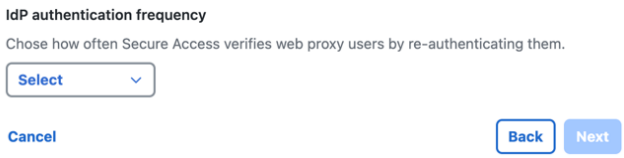
2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.id.ciscosecureaccess.cn**. 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.id.ciscosecureaccess.cn**.



4. Choose a time interval when a user must authenticate with Secure Access, or select **Never**.

   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_SSE_SP_Metadata XML file from Secure Access and use the service provider metadata to configure your instance of Okta.

Download the **Cisco_SSE_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.

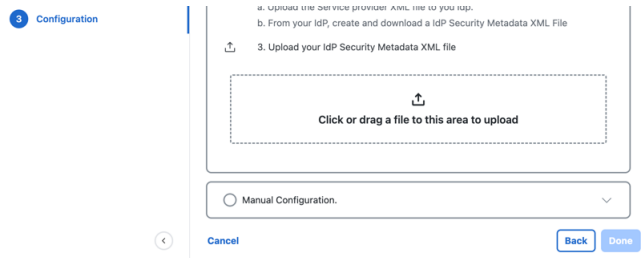
Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion.

> **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

Describes 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_SSE_SP_Metadata XML file to your local device.

1. Check **Manual Configuration**, and then click **Download service provider XML file** to save the **Cisco_SSE_SP_Metadata** XML file to your local device.



2. Open the **Cisco_SSE_SP_Metadata** XML file.
3. Copy the certificates from the **Cisco_SSE_SP_Metadata** XML file to a new file and save. Use the certificate file in the next step when you create the app integration in Okta.

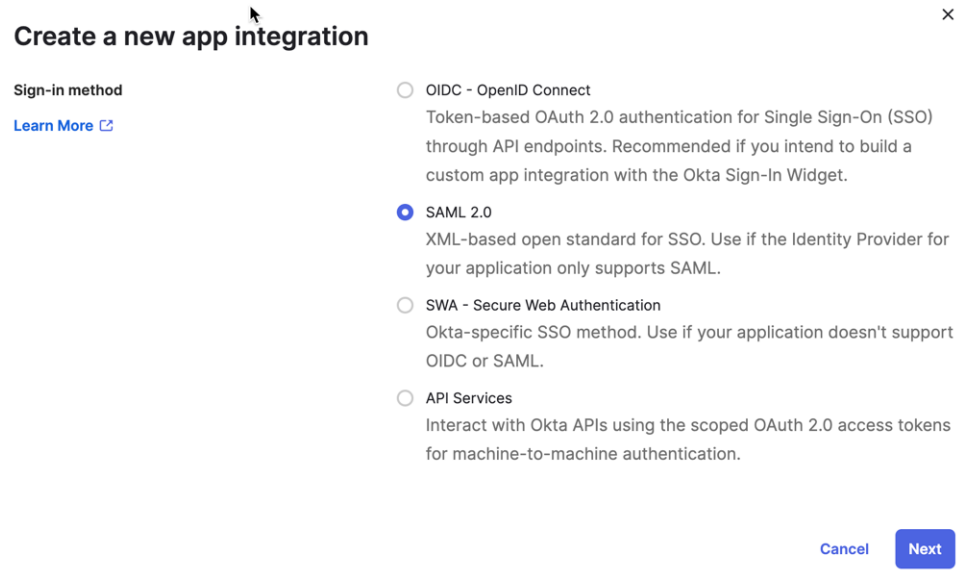
Step 3b – Add Secure Access Service Provider Metadata to Okta

Describes step 3b - Add Secure Access Service Provider Metadata to Okta. 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 can find the following steps described in the Okta Help. For more information, see Create a Basic Custom SAML Application Using SP Metadata File.

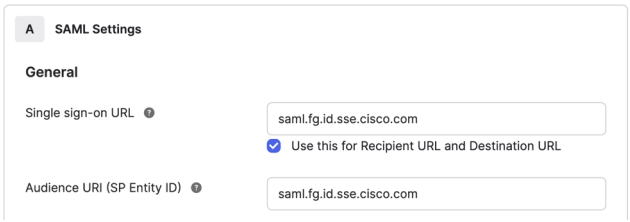
You must configure Secure Access as a generic SAML 2.0 application within Okta. Okta does not provide a method to upload Secure Access metadata for automatic configuration. Extract the **EntityID** and **AssertionConsumerService** values from the Secure Access metadata file and add these to the applicable fields in Okta. Contact Okta for assistance.

1. Sign in to your instance of Okta, then navigate to **Applications** > **Create a new app integration**.

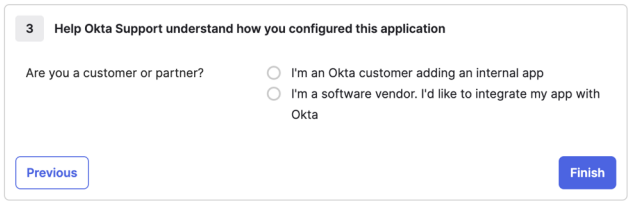


2. Click **SAML 2.0**, and then click **Next**.
3. For **General Settings**, add a name for the app integration, and then click **Next**.
4. For **SAML Settings > General**, enter the values from the service provider metadata file that you downloaded in Step 3a - Download the Secure Access Service Provider 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: `https://fg.id.ciscosecureaccess.cn/gw/auth/acs/response`.
   - For **Audience URI (SP Entity ID)**, add the value of the **entityID** element.

     The value should be something like: `saml.id.ciscosecureaccess.cn`.



5. Click **Show Advanced Settings**.
6. For **Signature Certificate**, upload the root certificate that you downloaded from the **Cisco_SSE_SP_Metadata** XML file. Click **Preview the SAML Assertion** to show the created metadata file, and then click **Next**.
7. Click **I'm an Okta customer adding an internal app**, and then click **Finish**.

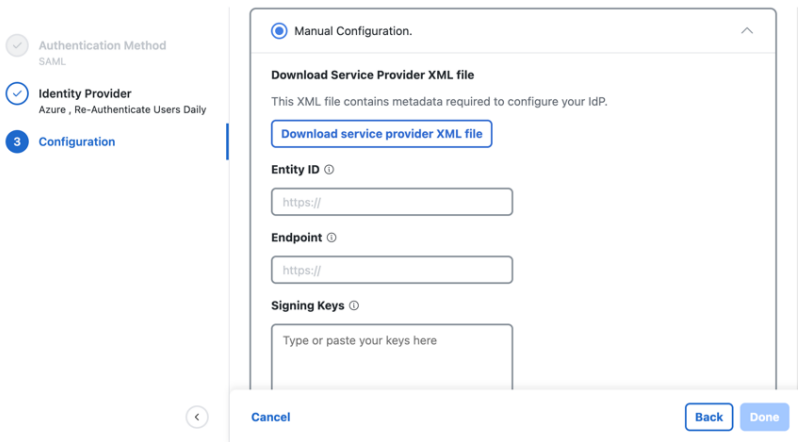


Step 3c – Add the Okta SAML Metadata to Secure Access

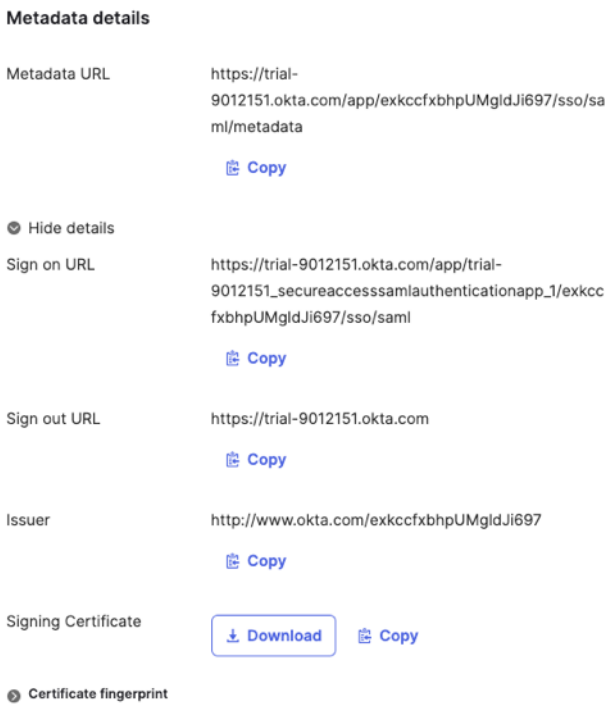
Describes step 3c - Add the Okta SAML Metadata to Secure Access. Complete the manual configuration of Okta in Secure Access. Enter your Okta SAML metadata for the following Secure Access settings:.

Complete the manual configuration of Okta in Secure Access. Enter your Okta SAML metadata for the following Secure Access settings:

- **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 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

Provides instructions for 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

Provides instructions for 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

Provides instructions for configuring AD FS for SAML in Cisco Secure Access China. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure Active Directory Federation Services (AD FS) with Secure Access by uploading the AD FS XML metadata file to Secure Access, or alternatively add the AD FS metadata in Secure Access manually.

For information about provisioning users from AD FS to Secure Access, see Provision Users and Groups from Active Directory.

Prerequisites

Lists the prerequisites for configuring adfs for SAML. Full Admin user role. For more information, see Manage Accounts. We recommend that you bypass web traffic to the id.ciscosecureaccess.cn domain on the Secure Access secure web gateway (SWG). For more information about domains and the SWG, see Manage Internet Security.

- Full Admin user role. For more information, see Manage Accounts.
- We recommend that you bypass web traffic to the **id.ciscosecureaccess.cn** domain on the Secure Access secure web gateway (SWG). For more information about domains and the SWG, see Manage Internet Security.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Internet Security.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access web profile. For more information, see Manage Web 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 Web 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 Web 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.

Procedure

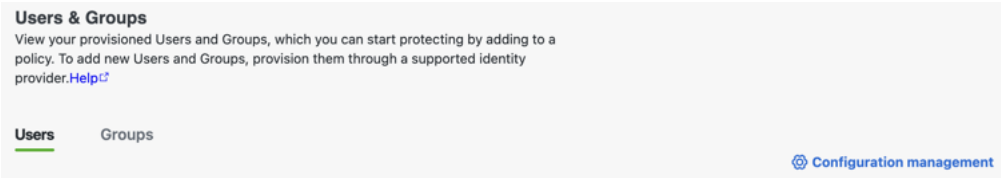
Provides instructions for configuring adfs for SAML. Step 1 – Choose an Authentication Method. Step 2 – Add an Identity Provider.

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

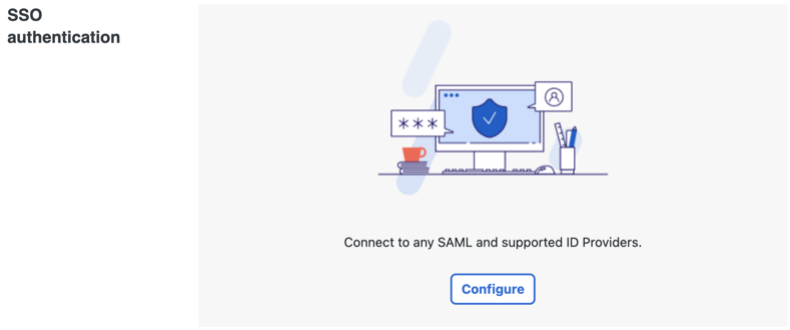
Step 1 – Choose an Authentication Method

Describes step 1 – Choose an Authentication Method. Navigate to Connect > Users and Groups and click Configuration Management. Navigate to SSO authentication and click Configure.

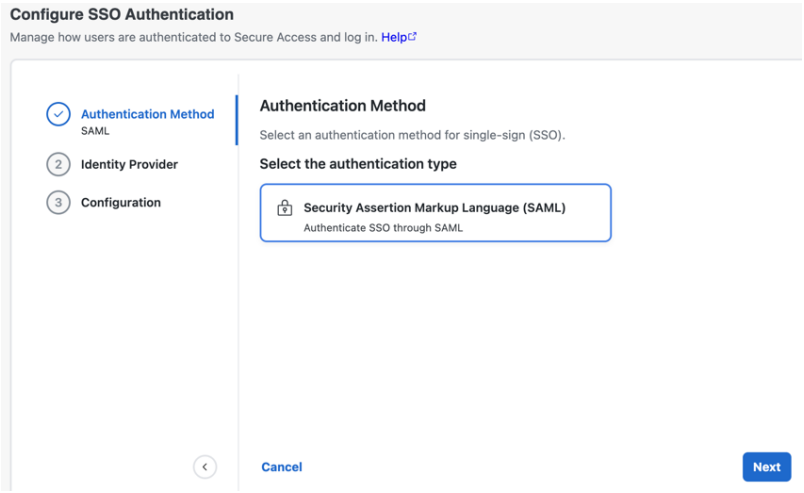
1. Navigate to **Connect > Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



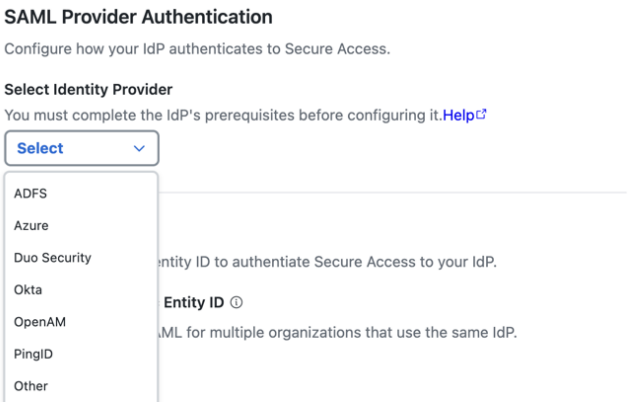
3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.



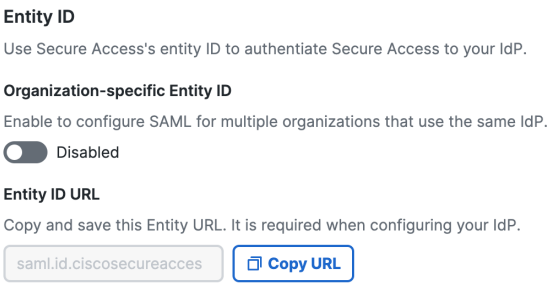
Step 2 – Add an Identity Provider

Describes step 2 - Add an Identity Provider. The time intervals are: Daily Weekly Monthly. For Identity Provider , choose ADFS . Secure Access supports various IdPs.

1. For **Identity Provider**, choose **ADFS**. Secure Access supports various IdPs.



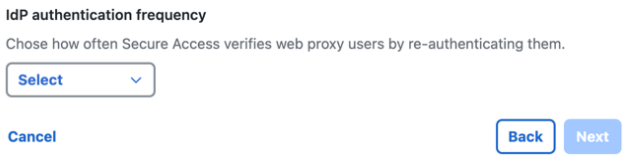
2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.id.ciscosecureaccess.cn**. 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.id.ciscosecureaccess.cn**.



4. Choose a time interval when a user must authenticate with Secure Access, or select **Never**.

   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. Then, either upload the AD FS SAML metadata XML file to Secure Access or add the SAML metadata directly in 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. 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.

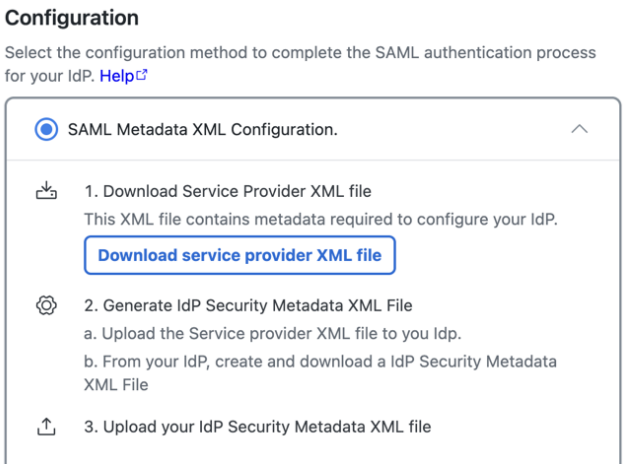
- Step 3a – Upload the Identity Provider's SAML Metadata XML File
- Step 3b – Add the Identity Provider's SAML Metadata

Step 3a – Upload the Identity Provider's SAML Metadata XML File

Describes 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.

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.



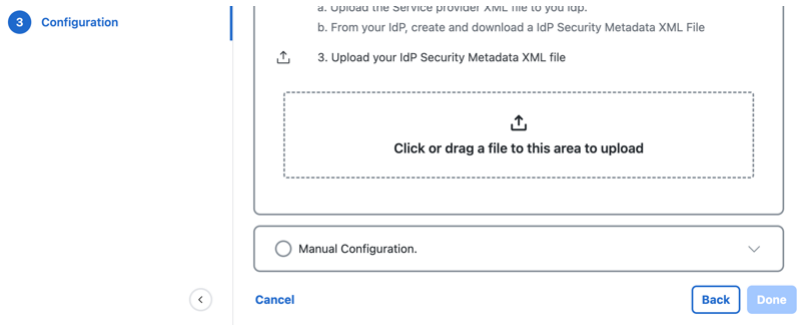
Step 3b – Add the Identity Provider's SAML Metadata

Describes 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.

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.

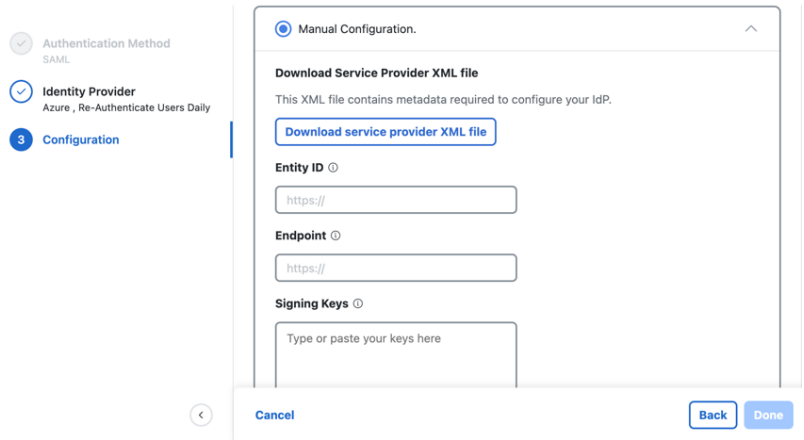
   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   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**.

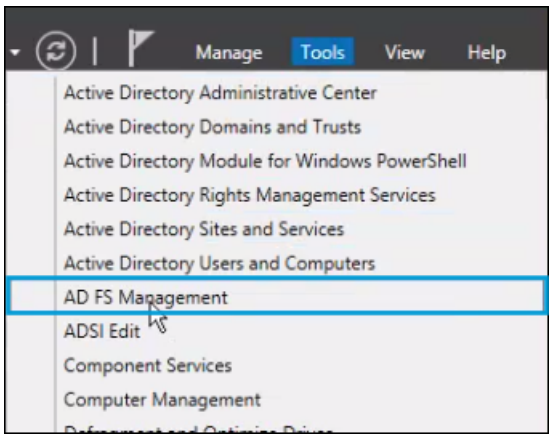
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
   - **Signed Authentication Request (optional)**–Choose whether you can sign the authentication request for the IdP.



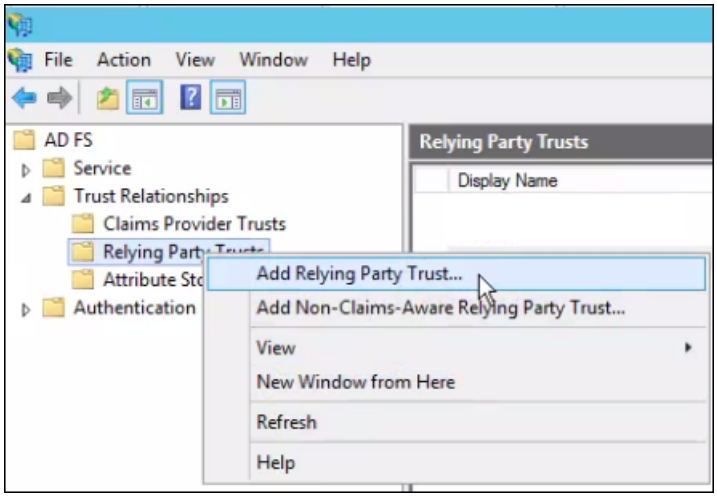
Configure Active Directory Federation Services

Provides instructions for configuring active directory federation services. Log into AD FS and navigate to Server Manager > Tools > AD FS Management.

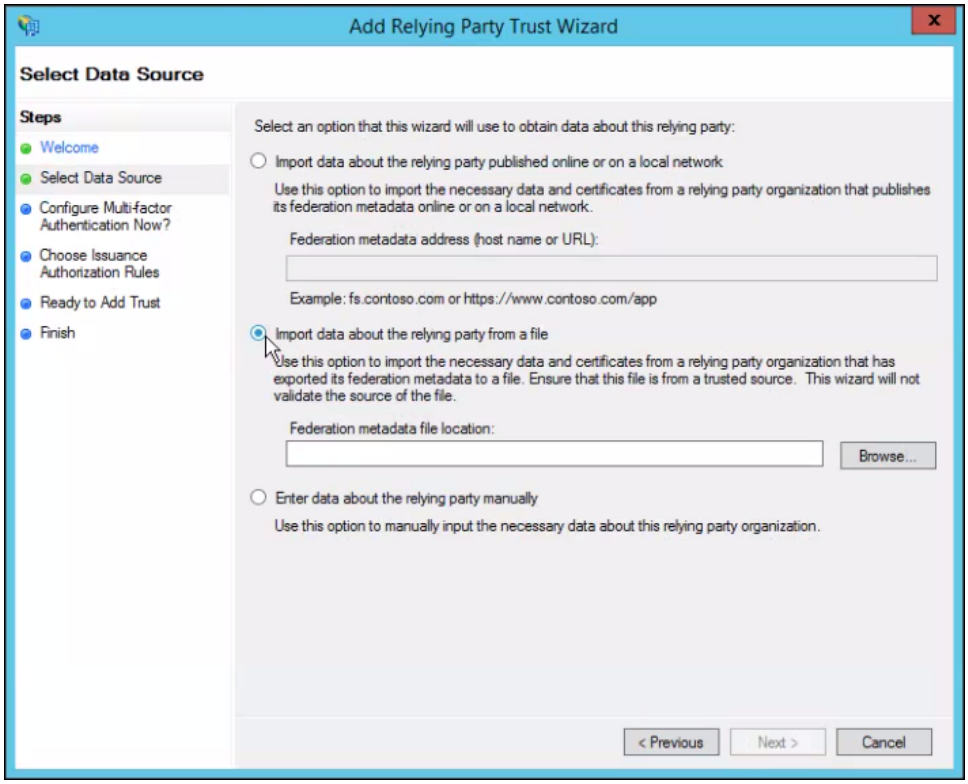
1. Log into AD FS and navigate to **Server Manager > Tools > AD FS Management**.



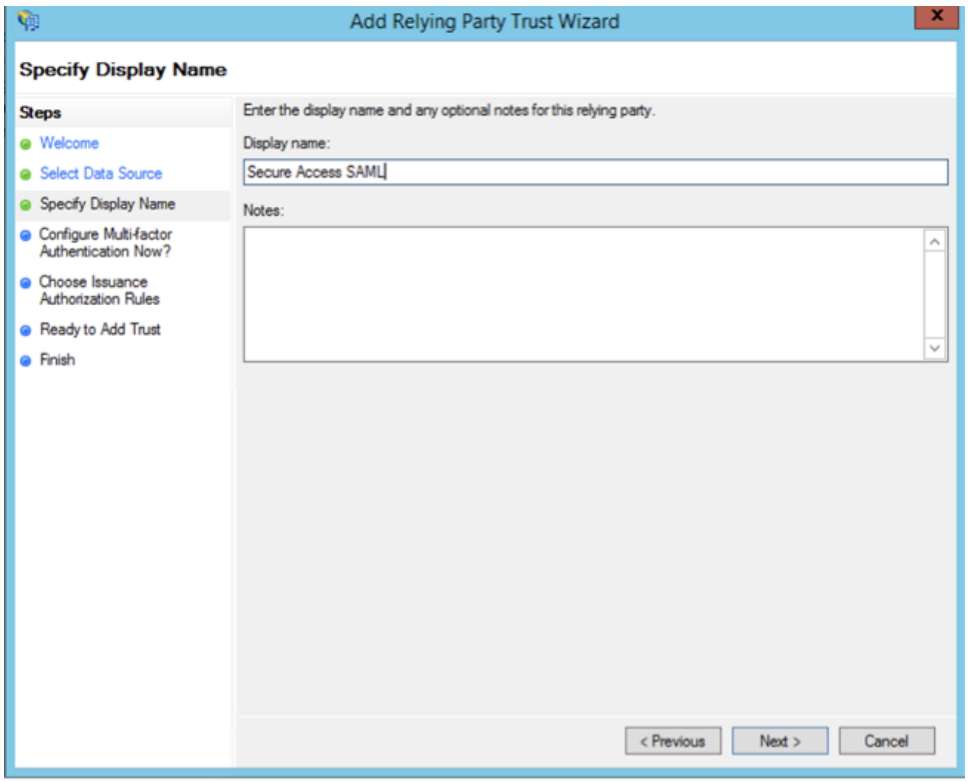
2. In the AD FS Manager, right-click on **Trust Relationships** and navigate to **Relying Party Trusts > Add Relying Party Trust** and select **Start**.



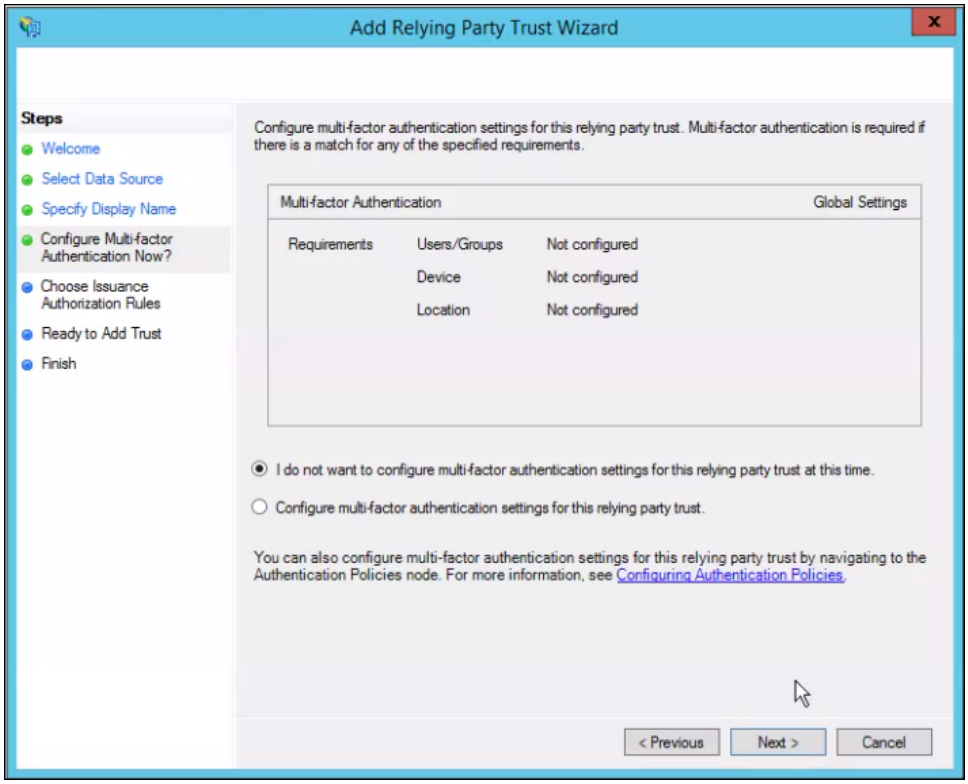
3. Choose **Import data about the relying party from a file** and browse for the **metadata.xml** file downloaded from Secure Access.



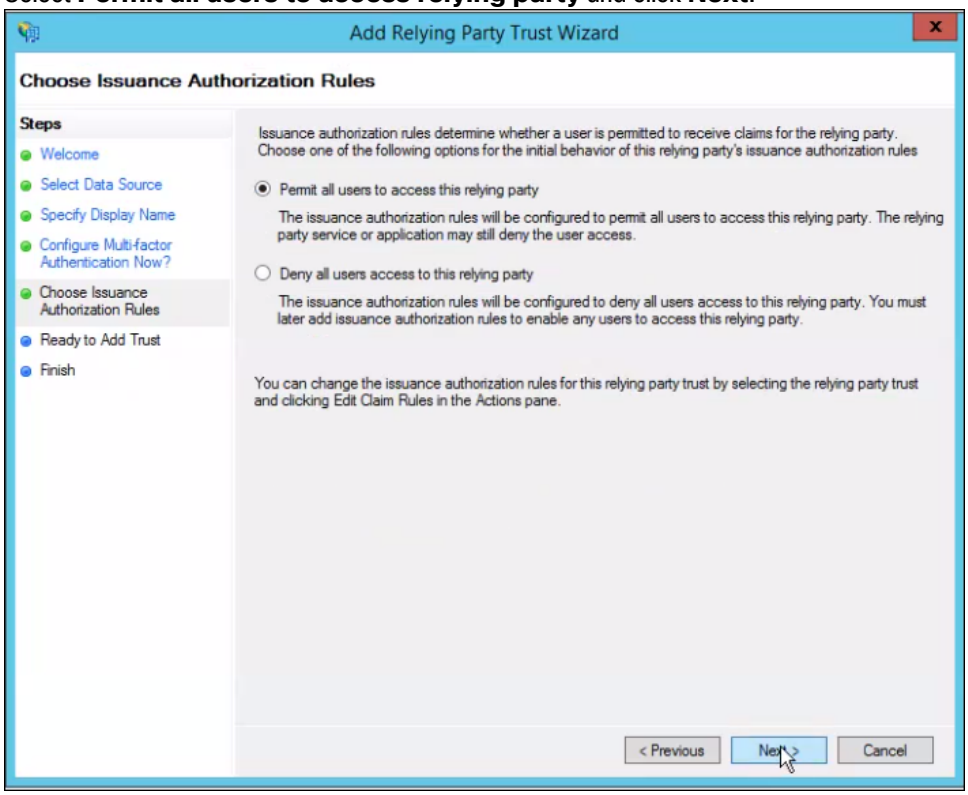
4. For **Display name**, provide a meaningful name for the trust connection, and then click **Next**.



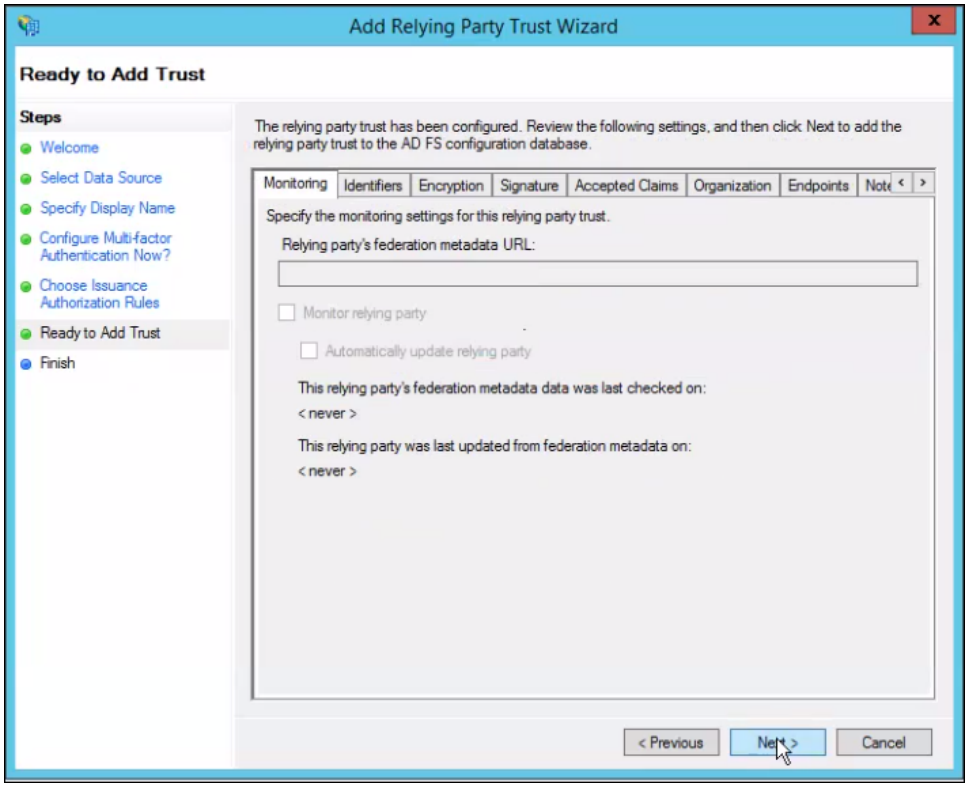
5. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time** and click **Next**.



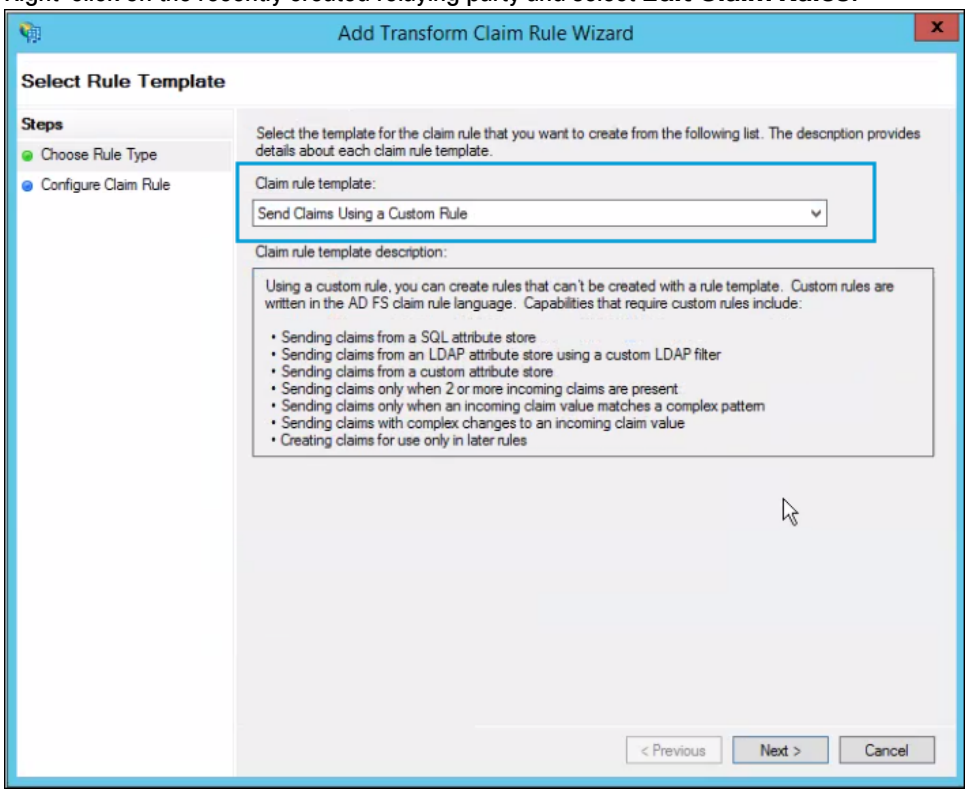
6. Select **Permit all users to access relying party** and click **Next**.



7. Verify settings and click **Next**.



8. Right-click on the recently created relaying party and select **Edit Claim Rules**.

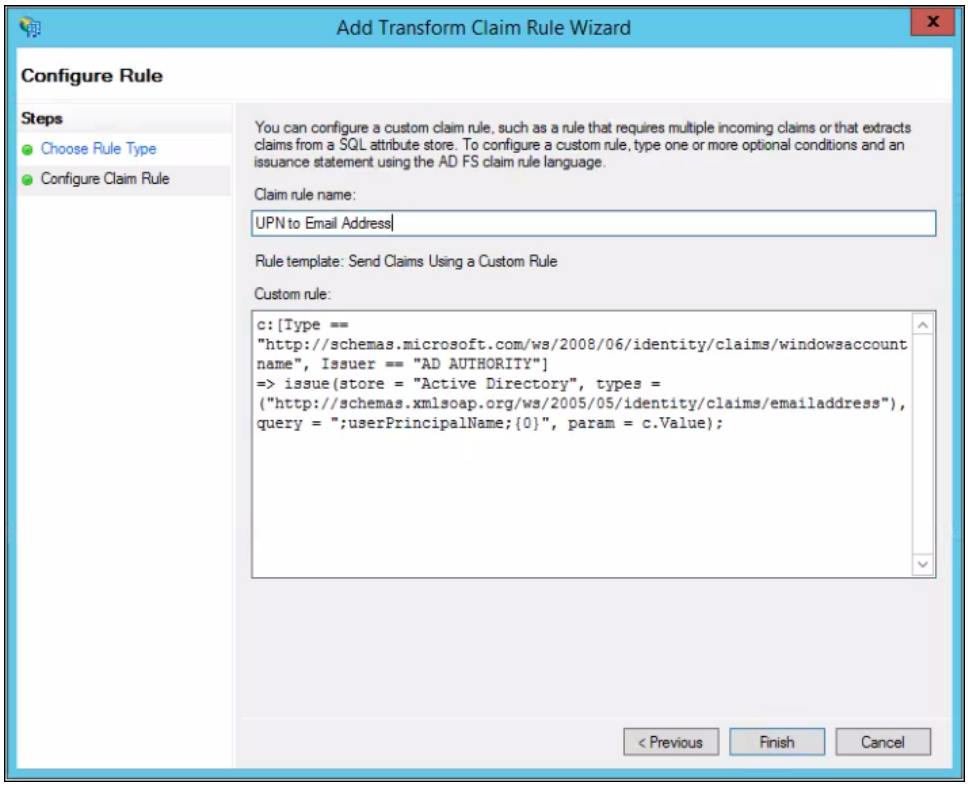


9. Under **Issuance Transform Rules**, click **Add Rule**, then choose **Send Claims Using a Custom Rule** with the following configuration:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
```

```
 Issuer == "AD AUTHORITY"]

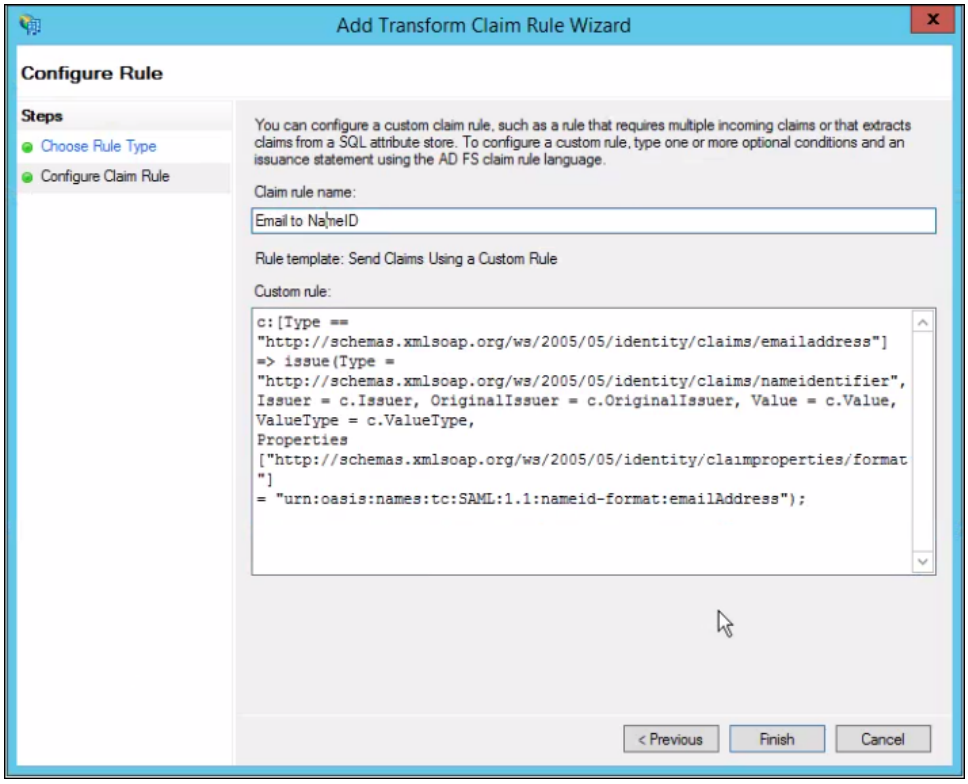
=> issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"), query
 = ";userPrincipalName;{0}", param = c.Value);
```



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

Provides instructions for 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

Provides instructions for 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

Provides instructions for configuring duo Security for SAML in Cisco Secure Access China. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the Duo Security SAML IdP with Secure Access by uploading the Duo Security XML metadata file to Secure Access, or alternatively add the Duo Security metadata in Secure Access manually.

Prerequisites

Lists the prerequisites for configuring Duo security for SAML. Full Admin user role. For more information, see Manage Accounts. Send id.ciscosecureaccess.cn requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.

- Full Admin user role. For more information, see Manage Accounts.
- Send **id.ciscosecureaccess.cn** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Internet Security.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access web profile. For more information, see Manage Web 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 Web 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 Web 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.

Procedure

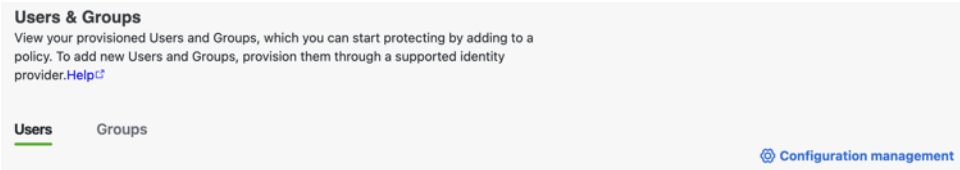
Provides instructions for configuring Duo security for SAML. Step 1 – Choose an Authentication Method. Step 2 – Add an Identity Provider.

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

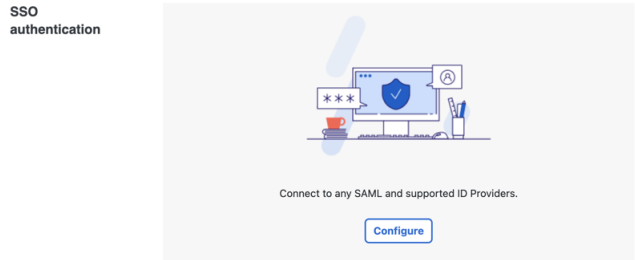
Step 1 – Choose an Authentication Method

Describes step 1 – Choose an Authentication Method. Navigate to Connect > Users and Groups and click Configuration Management. Navigate to SSO authentication and click Configure.

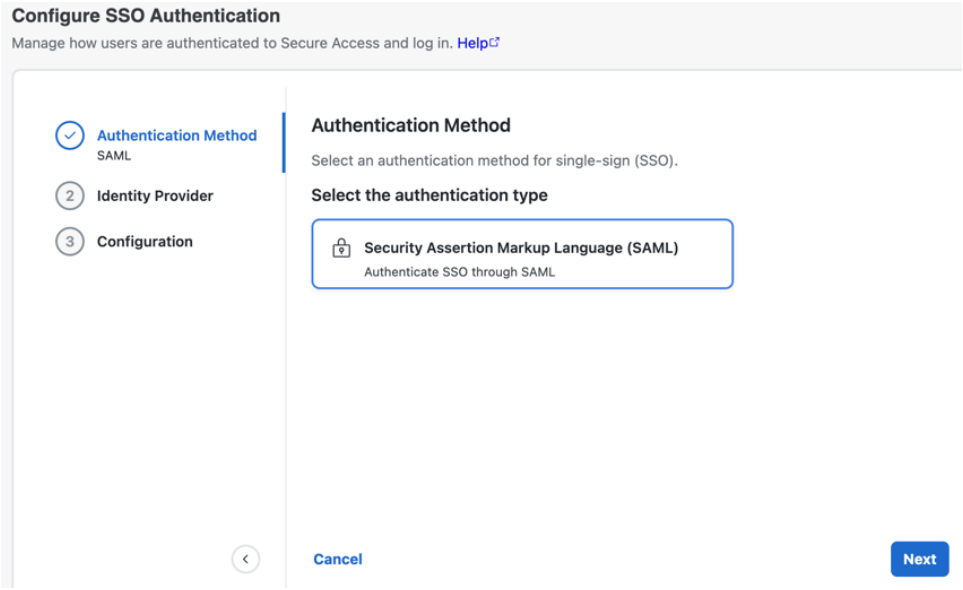
1. Navigate to **Connect > Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



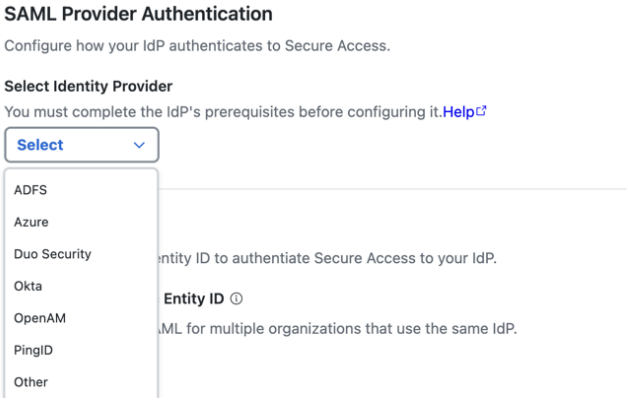
3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.



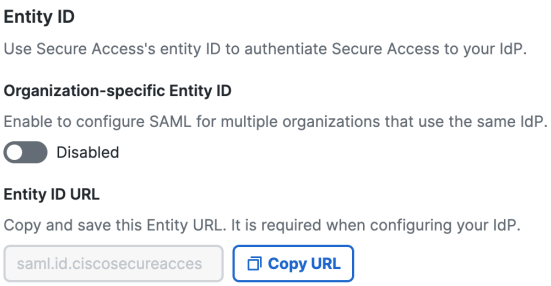
Step 2 – Add an Identity Provider

Describes step 2 – Add an Identity Provider. For Identity Provider , choose Duo Security . Secure Access supports various IdPs.

1. For **Identity Provider**, choose **Duo Security**. Secure Access supports various IdPs.



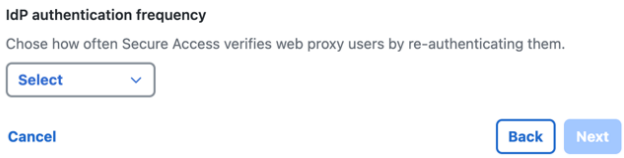
2. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.id.ciscosecureaccess.cn**. 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.id.ciscosecureaccess.cn**.



4. Choose a time interval when a user must authenticate with Secure Access, or select **Never**.

   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.

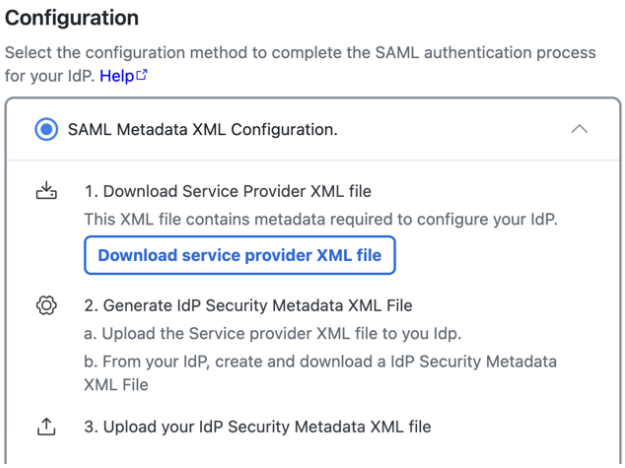
- Step 3a – Upload the Identity Provider's SAML Metadata XML File
- Step 3b – Add the Identity Provider's SAML Metadata

Step 3a – Upload the Identity Provider's SAML Metadata XML File

Describes 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.

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.

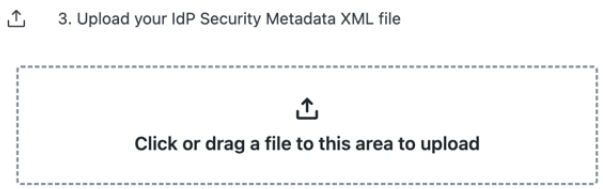
   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

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.



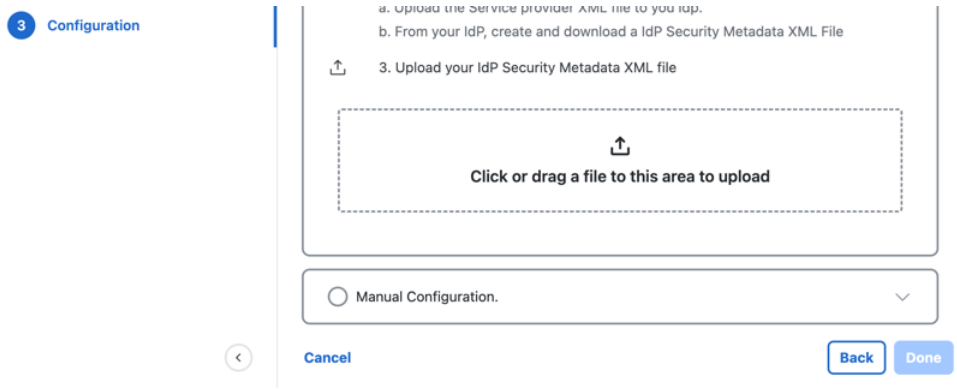
Step 3b – Add the Identity Provider's SAML Metadata

Describes 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.

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.

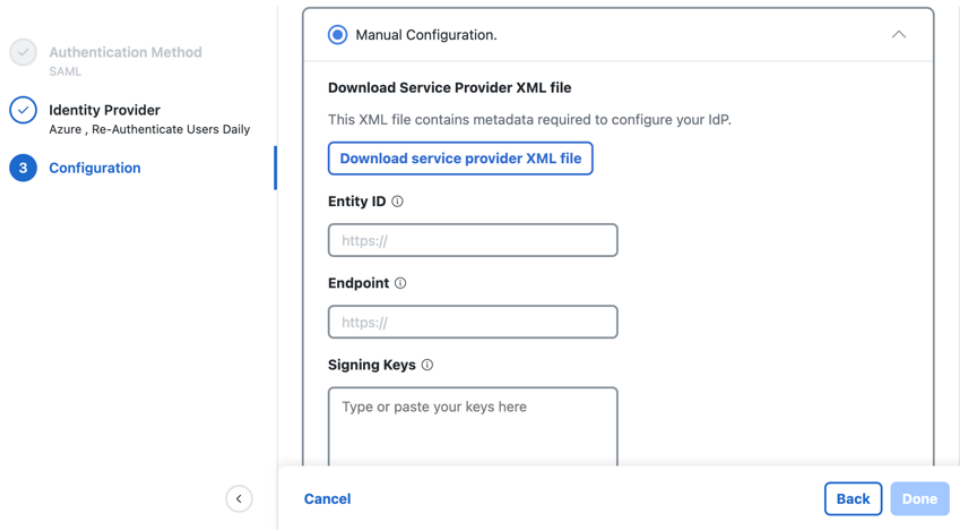
   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP signing certificate, refer to your vendor's documentation.

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**.

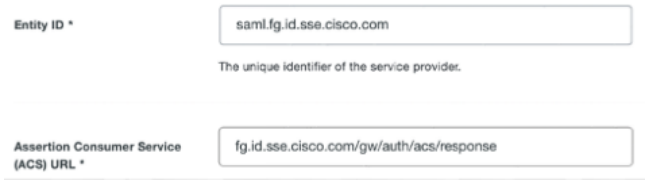
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
   - **Signed Authentication Request (optional)**–Choose 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. Enter an email address in the NameID attribute field. Click Download certificate to download the certificate, and then click Download XML to download the SAML Metadata file.

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.id.ciscosecureaccess.cn** and for **Assertion Consumer Service (ACS) URL**, enter **" fg.id.ciscosecureaccess.cn/gw/auth/acs/response**.



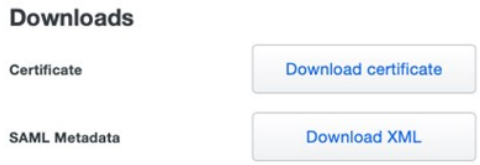
4. Enter an email address in the **NameID attribute** field.



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

Provides instructions for 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

Provides instructions for 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

Provides instructions for configuring ping Identity for SAML in Cisco Secure Access China. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity Provider (IdP) in Secure Access.

Configure the Ping Identity SAML IdP with Secure Access by uploading the Ping Identity XML metadata file to Secure Access, or alternatively add the Ping Identity metadata in Secure Access manually.

Prerequisites

Lists the prerequisites for configuring PingID for SAML. Full Admin user role. For more information, see Manage Accounts. Send id.ciscosecureaccess.cn requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.

- Full Admin user role. For more information, see Manage Accounts.
- Send **id.ciscosecureaccess.cn** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Internet Security.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access web profile. For more information, see Manage Web 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 Web 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 Web 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.

Procedure

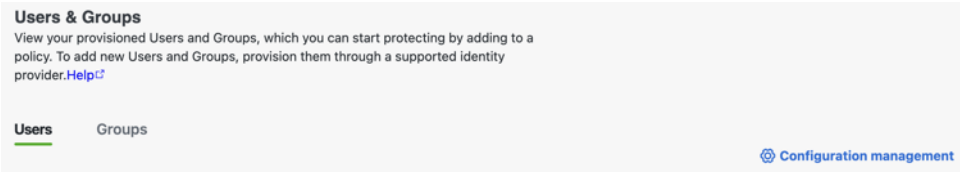
Provides instructions for configuring PingID for SAML. Step 1 – Choose an Authentication Method. Step 2 – Add an Identity Provider.

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

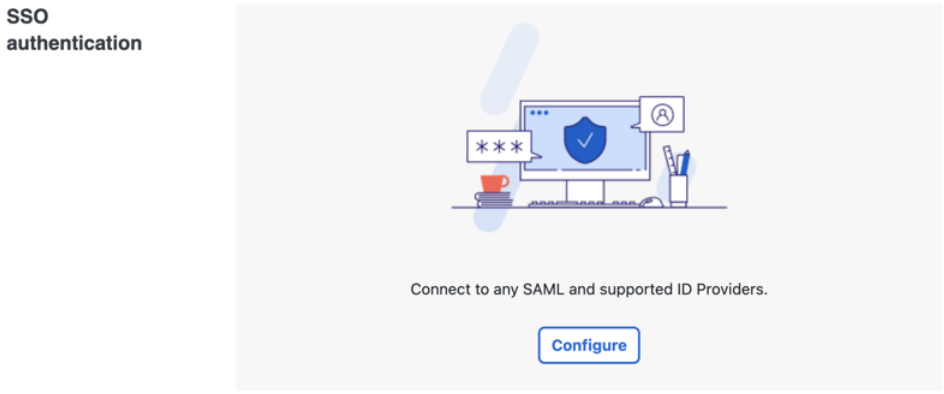
Step 1 – Choose an Authentication Method

Describes step 1 – Choose an Authentication Method. Navigate to Connect > Users and Groups and click Configuration Management. Navigate to SSO authentication and click Configure.

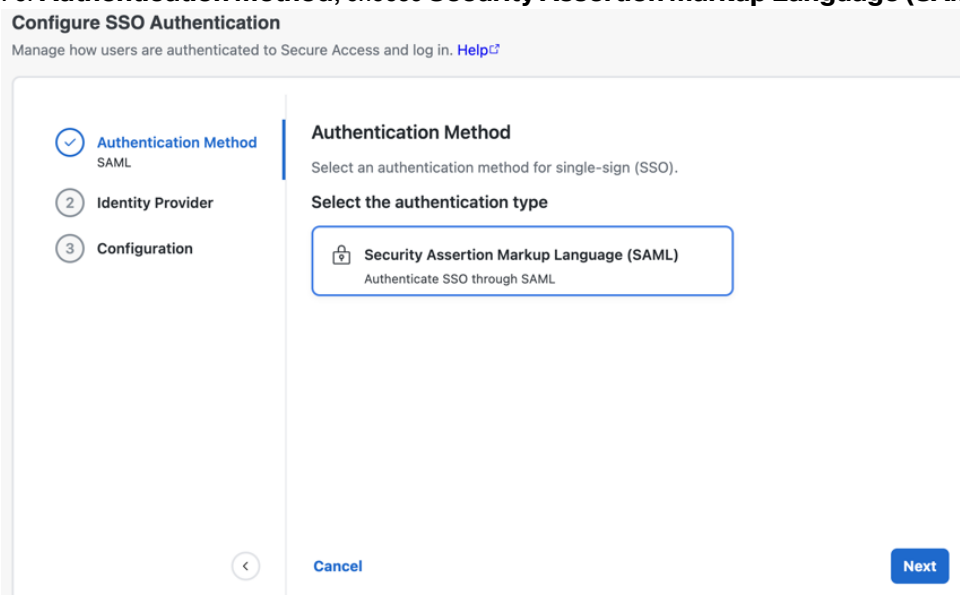
1. Navigate to **Connect > Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



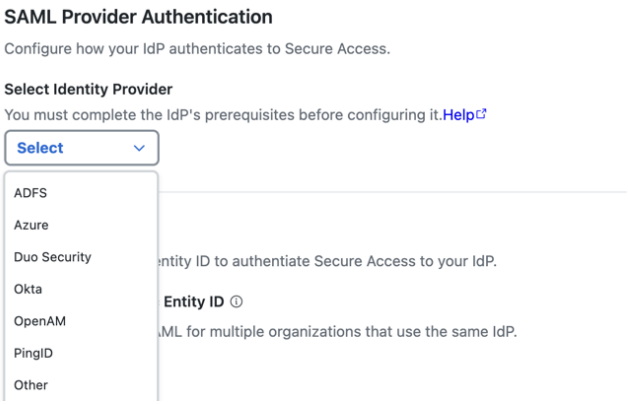
3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.



Step 2 – Add an Identity Provider

Describes step 2 – Add an Identity Provider. For Identity Provider , choose PingID . Secure Access supports various IdPs.

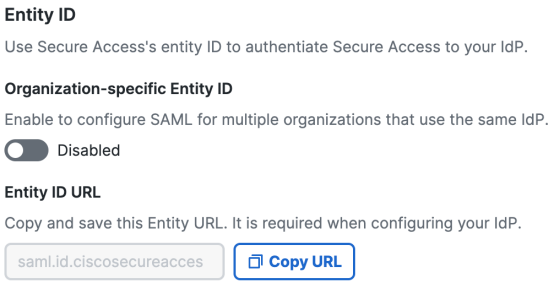
1. For **Identity Provider**, choose **PingID**. Secure Access supports various IdPs.



2. (Optional) Enable an organization-specific entity ID.

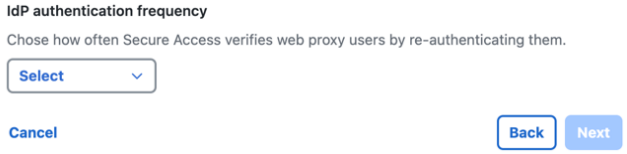
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access Orgs and need to configure SAML authentication for Secure Access Internet Security for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.id.ciscosecureaccess.cn**. Secure 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.id.ciscosecureaccess.cn**.



4. Choose a time interval when a user must authenticate with Secure Access, or select **Never**.
   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.

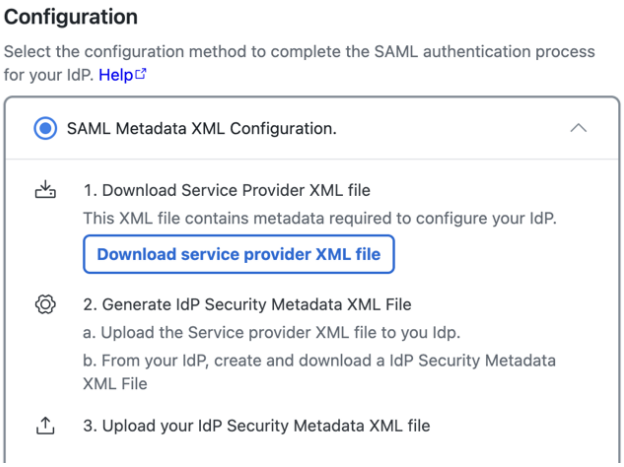
- Step 3a – Upload the Identity Provider's SAML Metadata XML File
- Step 3b – Add the Identity Provider's SAML Metadata

Step 3a – Upload the Identity Provider's SAML Metadata XML File

Describes 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.

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.

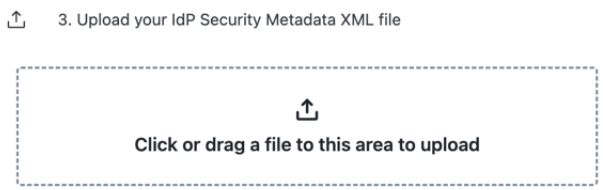
   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

3. Configure 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. 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.



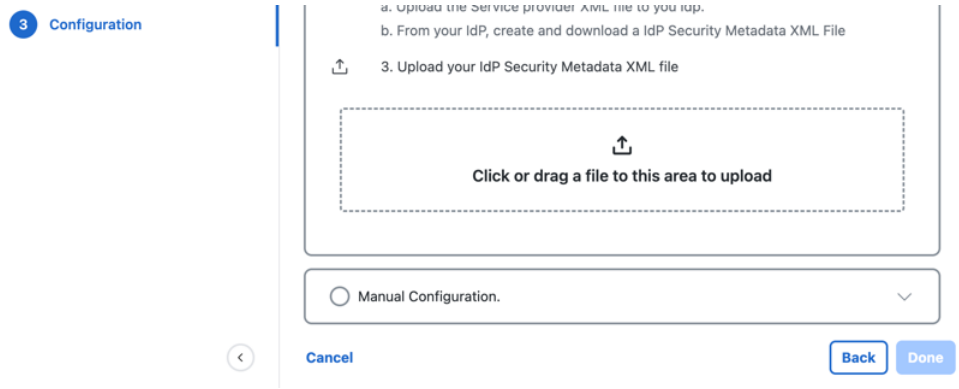
Step 3b – Add the Identity Provider's SAML Metadata

Describes 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.

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.

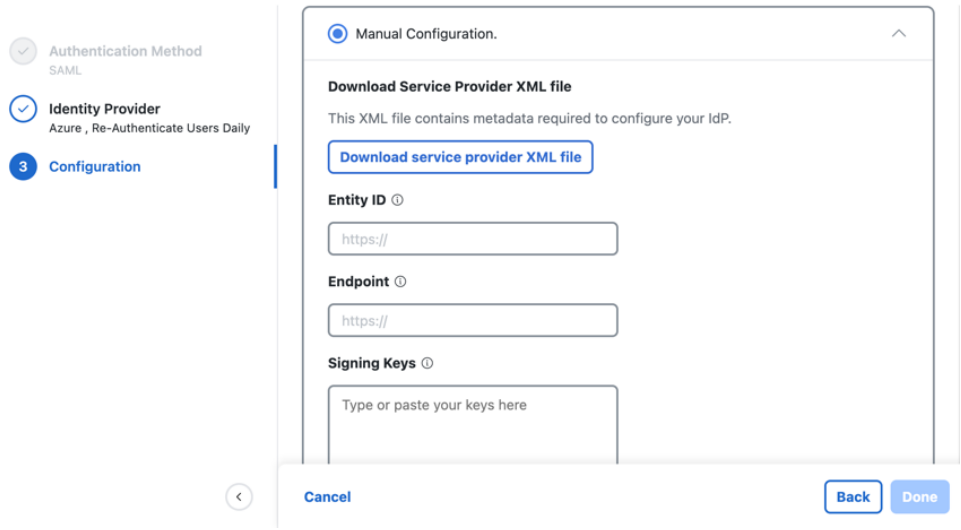
   Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP signing certificate, refer to your vendor's documentation.

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

Provides instructions for 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

Provides instructions for 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

Provides instructions for configuring openAM for SAML in Cisco Secure Access China. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the OpenAM SAML IdP with Secure Access by uploading the OpenAM XML metadata file to Secure Access, or alternatively add the OpenAM metadata in Secure Access manually.

Prerequisites

Lists the prerequisites for configuring openam for SAML. Full Admin user role. For more information, see Manage Accounts. Send id.ciscosecureaccess.cn requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.

- Full Admin user role. For more information, see Manage Accounts.
- Send **id.ciscosecureaccess.cn** requests to the Secure Access secure web gateway (SWG), not directly to the internet. For more information about domains and the SWG, see Manage Internet Security.

- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Internet Security.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Enable SAML in the Secure Access web profile. For more information, see Manage Web 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 Web 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 Web 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.

Procedure

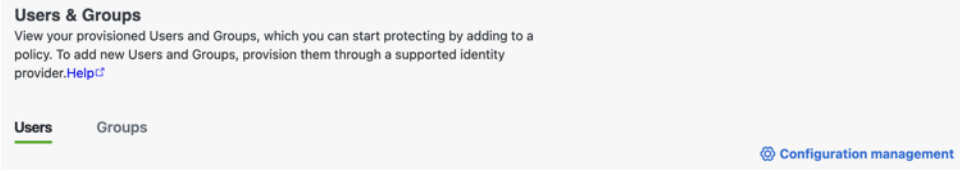
Provides instructions for configuring openam for SAML. Step 1 – Choose an Authentication Method. Step 2 – Add an Identity Provider.

- Step 1 – Choose an Authentication Method
- Step 2 – Add an Identity Provider
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

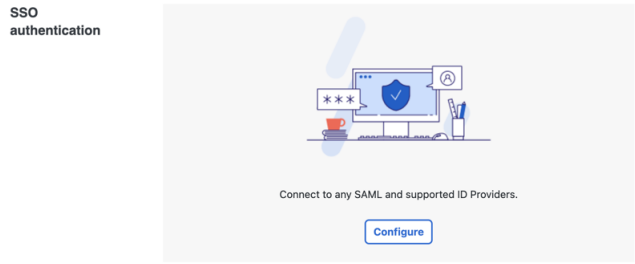
Step 1 – Choose an Authentication Method

Describes step 1 – Choose an Authentication Method. Navigate to Connect > Users and Groups and click Configuration Management. Navigate to SSO authentication and click Configure.

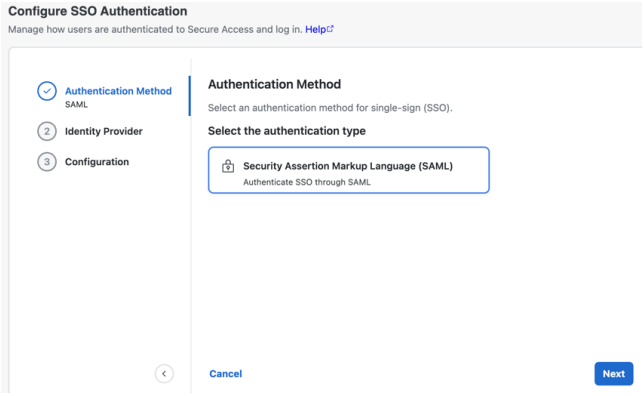
1. Navigate to **Connect > Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication** and click **Configure**.



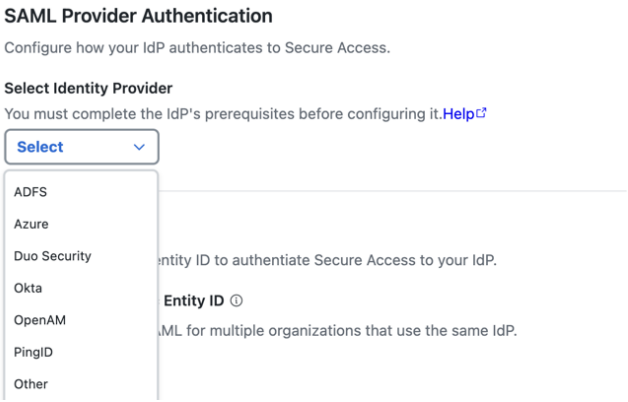
3. For **Authentication Method**, choose **Security Assertion Markup Language (SAML)**, and then click **Next**.



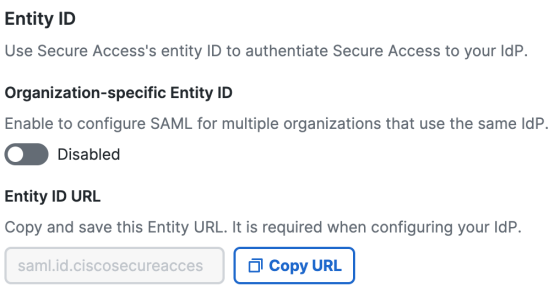
Step 2 – Add an Identity Provider

Describes step 2 - Add an Identity Provider. For Identity Provider , choose OpenAM . Secure Access supports various IdPs.

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 for these Orgs against the same IdP. The Secure Access SAML default common `EntityID` is **saml.id.ciscosecureaccess.cn**. 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.id.ciscosecureaccess.cn**.

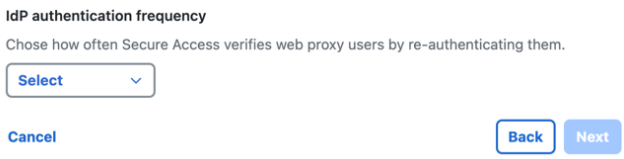


4. Choose a time interval when a user must authenticate with Secure Access, or select **Never**.

   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.

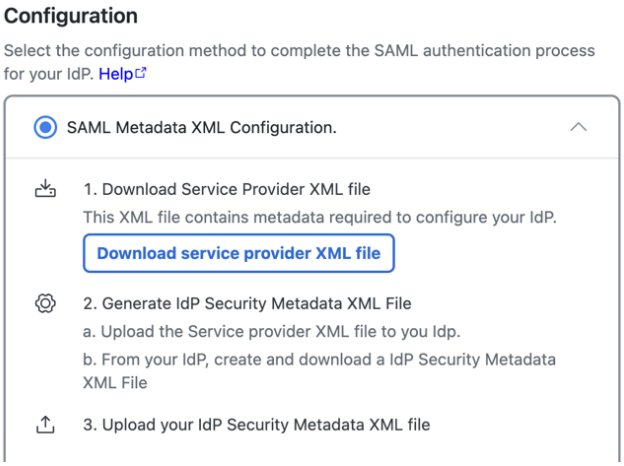
- Step 3a - Upload the Identity Provider's SAML Metadata XML File
- Step 3b - Add the Identity Provider's SAML Metadata

Step 3a – Upload the Identity Provider's SAML Metadata XML File

Describes 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.

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.

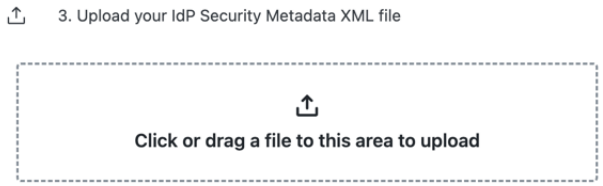
   The Secure Access service provider (SP) metadata includes the service provider Issuer ID, the assertion consumer endpoint URL information, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

   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.



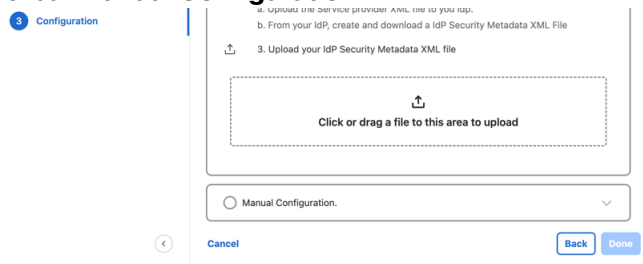
Step 3b – Add the Identity Provider's SAML Metadata

Describes 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.

1. Check **Manual Configuration**.



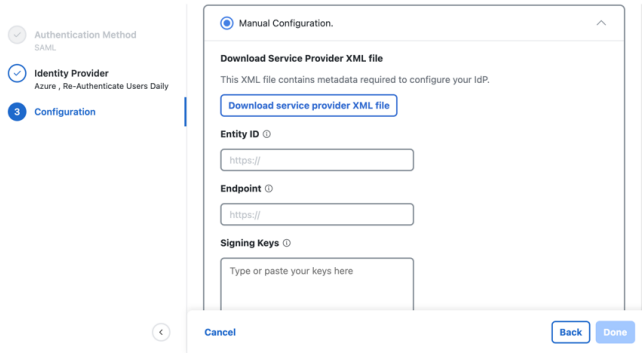
2. Click **Download service provider XML file** to save the Secure Access service provider XML metadata file to your local system.

   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

Provides instructions for 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

Provides instructions for 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 in Cisco Secure Access China. A SAML identity provider (IdP) may require the verification of a service provider's request signing certificate.

A SAML identity provider (IdP) may require the verification of a service provider's request signing certificate. When you integrate a SAML IdP with Secure Access, you may have to import the Secure Access certificate information in to your IdP platform.

> **Note**
>
> Many IdPs do not validate SAML request signatures and therefore these steps are not required. We recommend that you contact your IdP for confirmation.

There are two options for importing the certificate information into your IdP: Automatic Configuration and Manual Import.

Known Limitations

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.

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 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

Lists the prerequisites for SAML certificate renewal options. An IdP that supports automatic updates of a service provider's metadata from a URL, for example: AD FS and Ping Identity.

- 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://api.ciscosecureaccess.cn/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

Provides instructions for testing SAML Identity Provider Integration in Cisco Secure Access China. 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.

Prerequisites

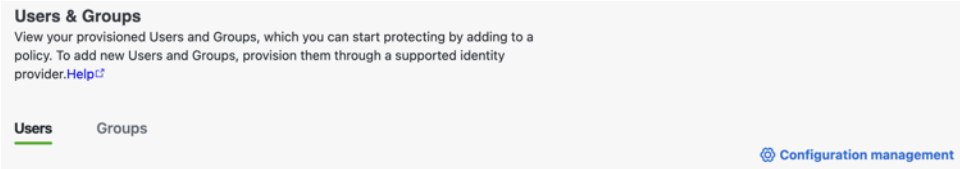
Lists the prerequisites for testing saml identity provider integration, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

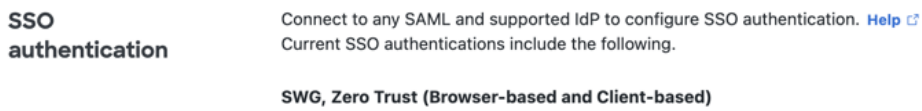
Procedure

Provides instructions for testing SAML identity provider integration. Navigate to Connect > Users and Groups and click Configuration Management. Navigate to SSO authentication.

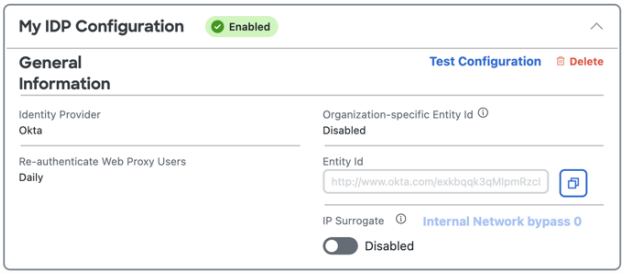
1. Navigate to **Connect > Users and Groups** and click **Configuration Management**.



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

Provides instructions for deleting SAML Identity Provider Integration in Cisco Secure Access China. 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.

Prerequisites

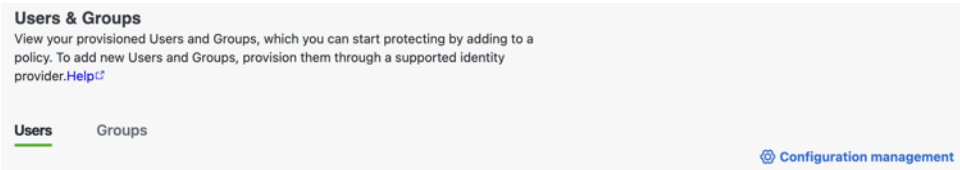
Lists the prerequisites for deleting saml identity provider integration, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

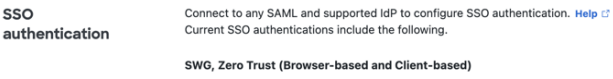
Procedure

Provides instructions for deleting SAML identity provider integration. Navigate to Connect > Users and Groups and click Configuration Management. Navigate to SSO authentication.

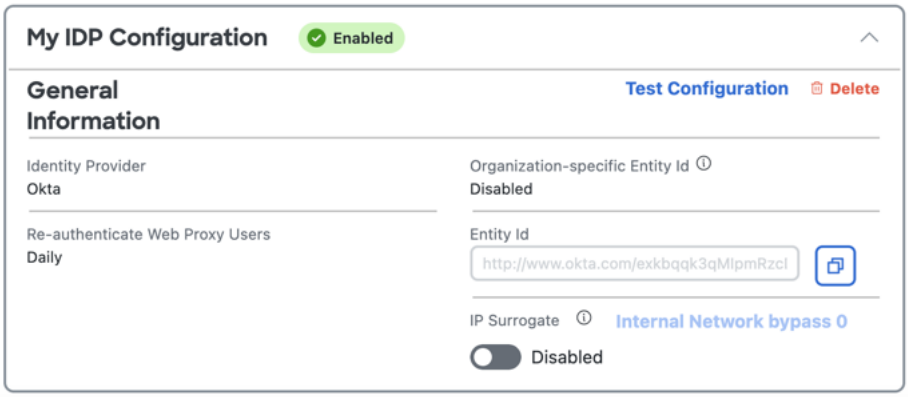
1. Navigate to **Connect > Users and Groups** and click **Configuration Management**.



2. Navigate to **SSO authentication**.



3. Click **Delete** to remove the integration between the IdP and Secure Access.



Use Cases

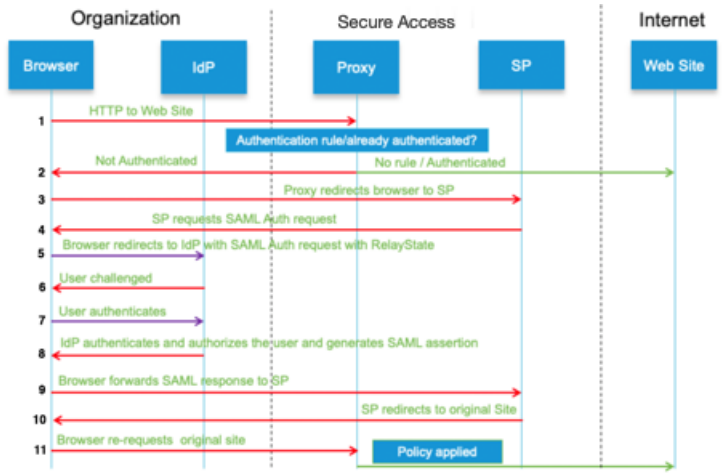
Provides instructions for using cases. Secure Access uses SAML authentication to provide seamless connections to web resources and private resources from user devices.

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

Provides instructions for securing internet access–networks and network tunnels. 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.

- 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 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



Configure Identity Providers for SAML Authentication

Provides instructions for 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

8 Manage End-User Connectivity

Topics:

- Manage End-User Connectivity

Provides an overview of Manage End-User Connectivity in Cisco Secure Access China. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage End-User Connectivity

Provides instructions for managing end-User Connectivity in Cisco Secure Access China. Secure Access provides secure connectivity to the internet and your digital resources.

Secure Access provides secure connectivity to the internet and your digital resources. To route network traffic from endpoints securely, you can:

- Manage 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

Virtual Private Networks Settings and Profiles

Describes virtual Private Networks Settings and Profiles. Configure VPN settings and profiles. For more information, see Manage Remote Access Virtual Private Networks.

Configure VPN settings and profiles. For more information, see Manage Remote Access Virtual Private Networks.

Internet Security

Describes internet Security. Steer traffic from endpoints to Secure Access or directly to the internet. For more information, see Manage Internet Security.

Steer traffic from endpoints to Secure Access or directly to the internet. For more information, see Manage Internet Security.

9 Manage DNS Servers

Topics:

- Manage DNS Servers

Provides an overview of Manage DNS Servers in Cisco Secure Access China. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage DNS Servers

Provides instructions for managing DNS Servers in Cisco Secure Access China. Add DNS servers to resolve DNS requests to internet resources.

Add DNS servers to resolve DNS requests to internet resources.

Prerequisites

Lists the prerequisites for adding dns servers, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

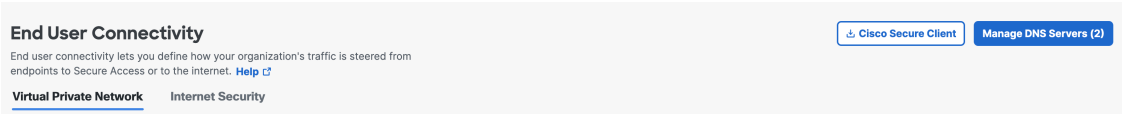
- Full Admin user role. For more information, see Manage Accounts.

Procedure

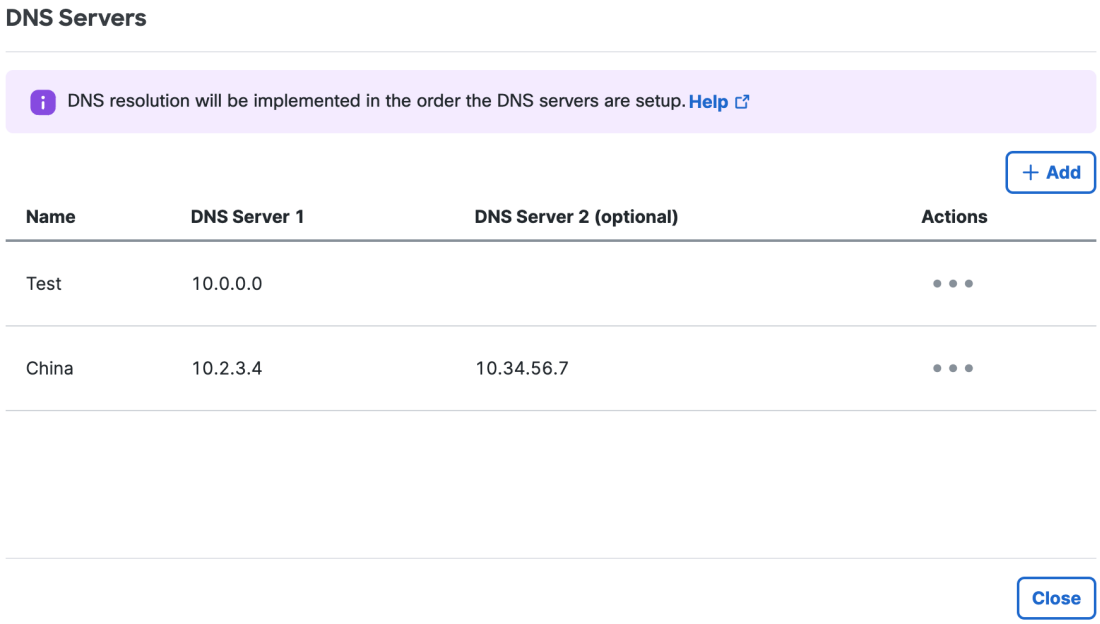
Provides instructions for adding DNS servers. Add an IP address or address range for a DNS server. Your DNS traffic routes through the DNS servers managed by Secure Access China.

Add an IP address or address range for a DNS server. Your DNS traffic routes through the DNS servers managed by Secure Access China.

1. Navigate to **Connect > End 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**.

10 Manage Remote Access Virtual Private Networks

Topics:

- Manage Remote Access Virtual Private Networks

Provides an overview of Manage Remote Access Virtual Private Networks in Cisco Secure Access China, including FQDNs for Network Connections, Manage IP Pools, and Add an IP Pool. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Remote Access Virtual Private Networks

Provides instructions for managing remote Access Virtual Private Networks in Cisco Secure Access China. 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:

FQDNs for Network Connections

Describes FQDNs for Network Connections in Cisco Secure Access China. A fully qualified domain name (FQDN) refers to the complete and unique address of an internet presence.

A fully qualified domain name (FQDN) refers to the complete and unique address of an internet presence. It consists of the host name and the domain, and is used to locate specific hosts online and access them using name resolution.

FQDN adds an extra layer of flexibility and precision when you create VPN profiles and access rules, providing enhanced security and simplifying network management. Secure Access offers a robust set of features to safeguard your infrastructure, and among them is the fully qualified domain name (FQDN) feature.

In the context of Secure Access remote access VPNs, FQDN enables you to create VPN profiles based on domain names rather than just IP addresses. This introduces a more flexible approach to controlling network traffic, as it allows for profiles to be defined based on specific services or applications hosted on those domains even when associated IP addresses change dynamically.

About Fully Qualified Domain Names (FQDNs)

Describes about Fully Qualified Domain Names (FQDNs). The benefits of using FQDN include:. Secure Access FQDN objects can be used within hierarchical, global, and regional network VPN policies to regulate traffic to or from specific domains, as discussed in the following sections.

“Fully qualified” refers to the unique identification that guarantees that all of the domain levels are specified. The fully qualified domain name consists of three or more labels: The top level domain, the domain names, optional subdomains, and the host name. If a domain name doesn’t specify all of the labels that are required for the FQDN, then this is called a “Partially Qualified Domain Name” (PQDN). This often means that only the host name is given. The generic name or the FQDN and its IP address is the “Fully Qualified Host Name” (FQHN).

The structure of an FQDN is predefined by the domain name system (DNS). The names of the individual levels in the domain name area are called “labels” and are separated from one another by dots. Each label must consist of 1 to 63 characters and the total FQDN may not exceed 255 characters in total. Only letters, numbers, or dashes can be used. Each label has to have either a letter or a number at the beginning.

The benefits of using FQDN include:

- FQDNs offer more reliability because they don't change when the underlying IP addresses change, such as traffic that’s routed through load balancers. This can help to reduce downtime and improve the reliability of your cloud workloads.
- FQDNs are more human-readable and easier to remember than IP addresses. This can make your VPN profiles and policies more readable and easier to maintain.
- FQDNs can help to improve the security of your applications by making it more difficult for DNS spoofing attacks.

Secure Access FQDN objects can be used within hierarchical, global, and regional network VPN policies to regulate traffic to or from specific domains, as discussed in the following sections.

Secure Access Global FQDN

Provides instructions for securing access global fqdn. Your Secure Access org is assigned a global FQDN available to copy and paste as needed. Navigate to Connect > End User Connectivity > Virtual Private Network to find the global FQDN.

Your Secure Access org is assigned a global FQDN available to copy and paste as needed. Navigate to **Connect > End User Connectivity > Virtual Private Network** to find the global FQDN.

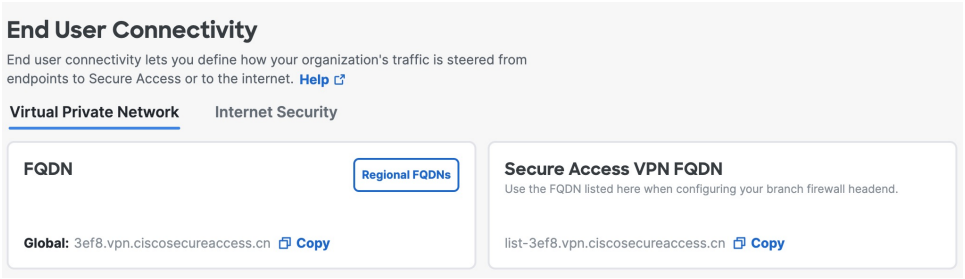
Secure Access Regional FQDNs

Provides instructions for securing access regional fqdns. Regional FQDNs let you create and enforce consistent VPN profiles across all subnetworks within a region in your Secure Access network. These profiles contain settings that can determine how VPN traffic traverses your network, including destination exceptions and DNS mode.

Regional FQDNs let you create and enforce consistent VPN profiles across all subnetworks within a region in your Secure Access network. These profiles contain settings that can determine how VPN traffic traverses your network, including destination exceptions and DNS mode.

When creating a VPN profile, you can opt to automatically add a region-specific FQDN to the hostname, which provides flexibility to clients when connecting to their VPN headend; see Step 1 - General Settings of the **Add VPN Profiles** topic.

Your Secure Access regional FQDNs are also available to copy and paste as needed. Navigate to **Connect > End User Connectivity > Virtual Private Network** and click **Regional FQDNs** from the global **FQDN** card to view the available regional FQDNs.



Secure Access VPN Headend FQDN

Provides instructions for securing access vpn headend fqdn. Your Secure Access org is assigned a VPN FQDN to use when configuring your branch firewall headend.

Your Secure Access org is assigned a VPN FQDN to use when configuring your branch firewall headend. This FQDN is available to copy and paste as needed. Navigate to **Connect > End User Connectivity > Virtual Private Network** to find the **Secure Access VPN FQDN** card.

Manage IP Pools

Provides instructions for managing IP Pools in Cisco Secure Access China. 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.

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 an IP Pool

Provides instructions for adding an IP Pool in Cisco Secure Access China. VPN profiles require IP addressing pools in order to be fully-functional.

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 China IP address pools.

Prerequisites

Lists the prerequisites for adding ip pool, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for adding IP pool. 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.

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.

Add an IP Pool

Provides instructions for adding an ip pool. To configure the VPN IP Pool, complete the following steps:. Take the following actions to manage IP pools.

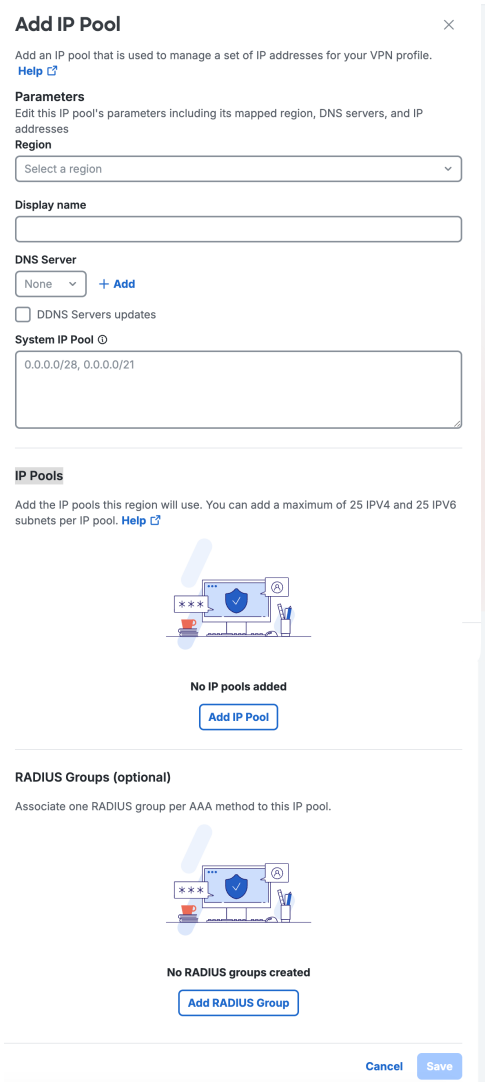
To configure the VPN IP Pool, complete the following steps:

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Under **Regions and IP Pools**, click **Manage**.

   The IP Pools page opens. Each region must have a unique IP pools configured. These IP pools are used to assign IP addresses to endpoint devices connecting via remote access VPN. Proper configuration ensures that VPN clients receive unique IP addresses from the pool associated with their region, preventing IP address conflicts and enabling efficient routing and management of remote access VPN connections.

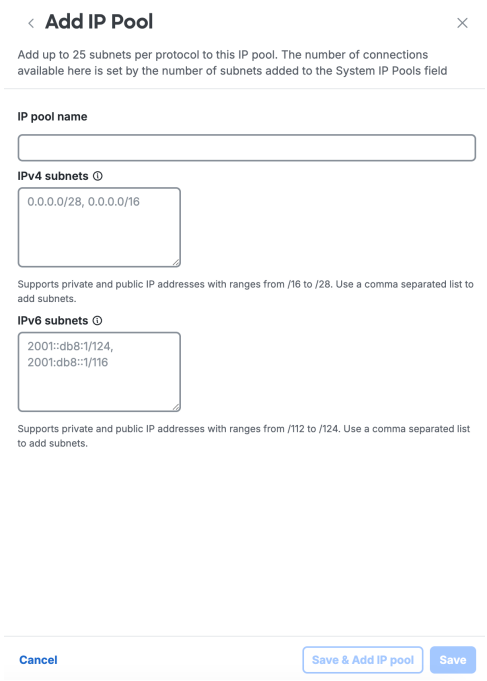
   Take the following actions to manage IP pools.

   - Click **Add IP Pool** to open a dialog for creating a new IP pool.
   - Click an existing IP pool's region name to view the **IP pool detailed information** pane.
   - Click the **pencil** icon to edit an IP pool.
3. Click **Add IP Pool**.
4. Configure IP pool Parameters :



- Select an available **Region**.
- Enter a **Display name**.
- Select a **DNS Server** pair from the dropdown, or click **+ Add** to create a new DNS pair.
- **DDNS Servers updates** (optional): Check the box to select an existing DDNS server, or click **+ Add** to create a new DDNS pair.
- **System IP pool** (optional): Add up to five subnets with IP ranges from /28 to /21 to grant Secure Access permission to obtain IP addresses for administrative connections to customer data centers. Subnets added as system IP pools count against the total number of IP pools available in the next step.

5. **IP pools**: Add the IP pools this region will use. You can add a maximum of 25 IPV4 and 25 IPV6 Subnets per IP pool.



- Enter an **IP pool name**.
- Add **IPV4 subnets** for remote access VPN user connections. Each user endpoint will receive an IPv4 address from the IP pool. You may add multiple comma-separated ranges from /28 to /16.
- Add **IPv6 subnets** (optional) for remote access VPN user connections. If configured, each user endpoint will receive an IPv6 address from the IP pool. You may add multiple comma-separated ranges from /124 to /112. The IPv6 user connection count must be greater than or equal to the IPv4 user connection count configured for this IP pool.
- Click **Save & Add IP Pool** to finish configuring a new IP pool.

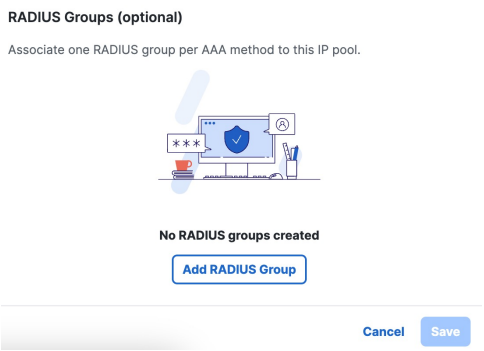
6. **RADIUS Groups** (optional): Select an existing RADIUS group or click **Add RADIUS Group** to associate a RADIUS group with this IP pool.
7. Click **Save** when you are done.

Add a RADIUS Group (optional)

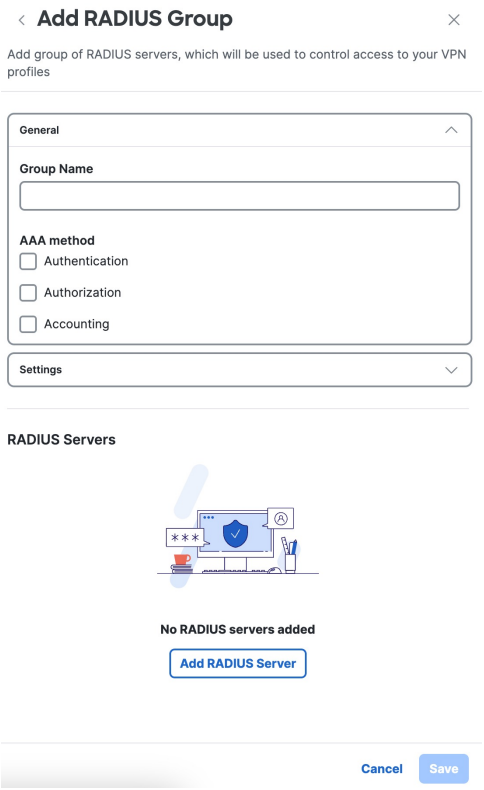
Provides instructions for adding a radius group (optional). This section describes how to configure a RADIUS group and add servers to the group. This RADIUS group can be applied to the Management IP pool being configured and mapped to other IP pools.

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.

1. Navigate to **Connect > End User Connectivity > Virtual Private Network**.
2. Click **Add IP Pool**. The **Regions and IP Pools** page appears
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**.



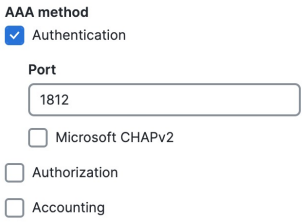
5. Choose the AAA methods to apply to this RADIUS Group. Choose at least one method.

> **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.

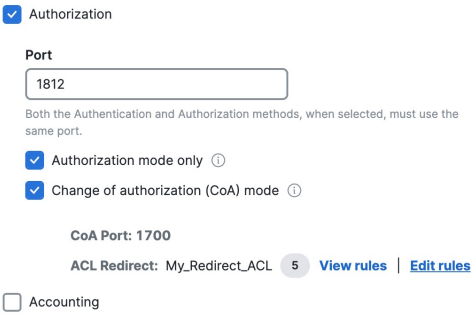


b. **Authorization**- Enter the RADIUS authorization **Port** number. The valid range is from 1 to 65535.

The default is 1812.

When you check **Authorization mode only**, no common password is required.

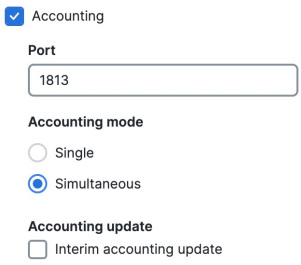
When you check **Change of authorization (CoA) mode**, the RADIUS server group will be registered for CoA notification. If you enable CoA, the listening port for RADIUS CoA requests uses the default of 1700. The ACL Redirect displays the number of rules defined for ACL redirect. Click **View rules** to view the rules, and **Edit rules** to edit the rules. Select the **Change of authorization (CoA) mode** 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.

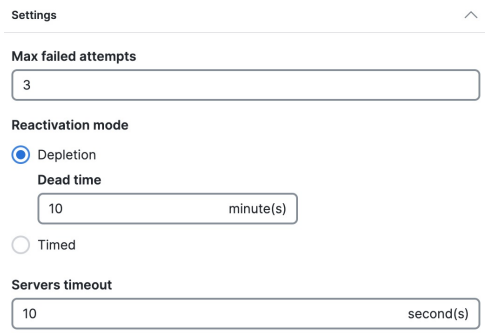
b. Choose **Depletion, Dead time** to reactivate failed servers only after all of the servers in the group are inactive.

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.

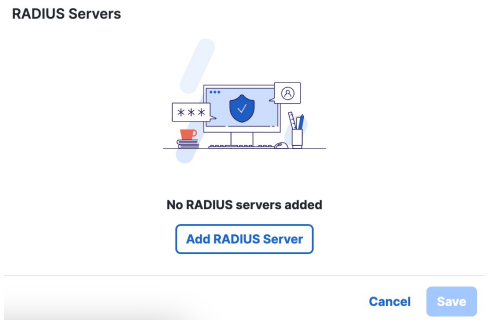
c. Choose **Timed** to reactivate failed servers after 30 seconds of down time.

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.

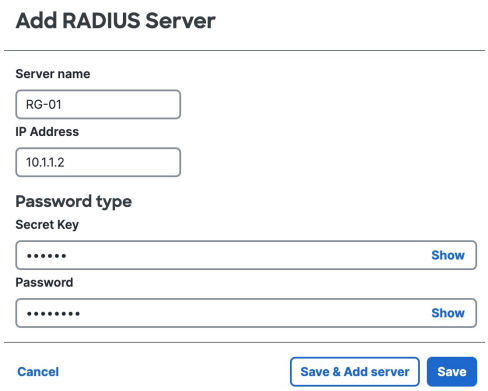


7. Scroll down to **RADIUS Servers** and click **Add RADIUS Server**.

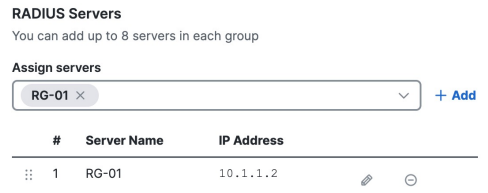
You can add up to eight servers to each RADIUS group.



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

Provides instructions for managing VPN Profiles in Cisco Secure Access China. 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 VPN Profiles

Provides instructions for adding VPN Profiles in Cisco Secure Access China. A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet.

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

Lists the prerequisites for adding VPN profiles, including a Full Admin role in Secure Access and the account role information in Manage Accounts.

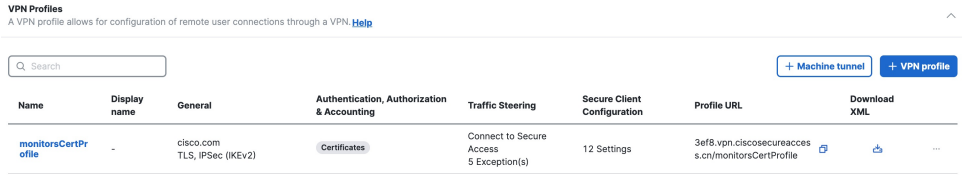
- Full Admin role in Secure Access. See Manage Accounts.

Step 1 – General Settings

Describes 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.

1. Navigate to **Connect > End User Connectivity > Virtual Private Network**.
2. In the **VPN Profiles** pane, click **+VPN profile**.



3. Enter a meaningful **VPN Profile name** for this profile.
4. Configure the **General settings** for this VPN profile:
5. Optionally, enter a **Display name** for this profile. This is a customizable and flexible label that is displayed to end-users of the Cisco Secure Client for ease-of-selection when choosing the appropriate profile.
6. Enter the **Default Domain**.
7. Choose a **DNS Server** from the drop-down, or click **Add** to add a new DNS server pair.

   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 **Profile Settings**, review the following settings and choose the options appropriate for this profile:

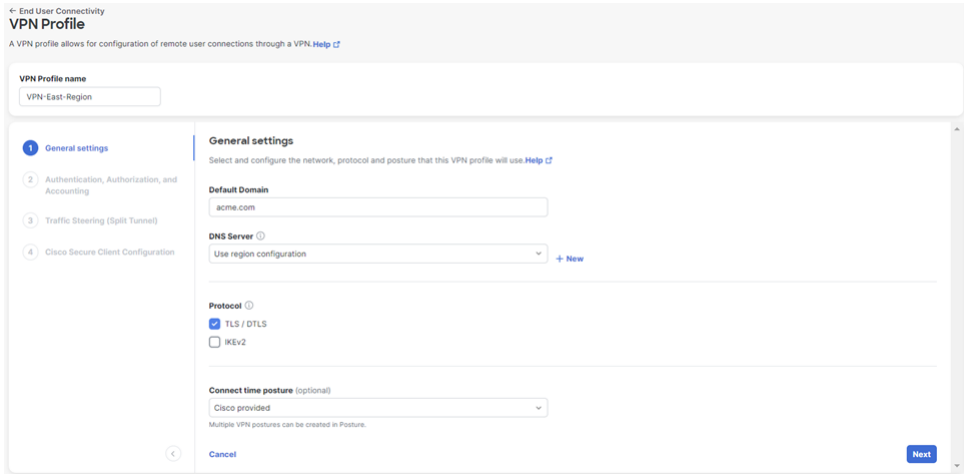
- Check **Include machine tunnel for this profile** to allow a client device to connect to Secure Access before a user initiates a login. Click **+ Add Machine Tunnel** to configure a machine tunnel if one does not exist for this profile; see Manage Machine Tunnels for information.
- Check **Include regional FQDN** to add a region-specific FQDN to the hostname, which provides flexibility to clients when connecting to their VPN headend.

9. 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.

10. Optionally, choose a **Connect time posture** from the drop-down.



11. 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.

Choose a configuration method from the **Protocols **drop-down to complete the authentication process for this VPN profile. Authentication is the way a user is identified before being allowed access to the network and network resources. Authentication requires valid user credentials, a certificate, or both. You can use authentication alone, or with authorization and accounting.

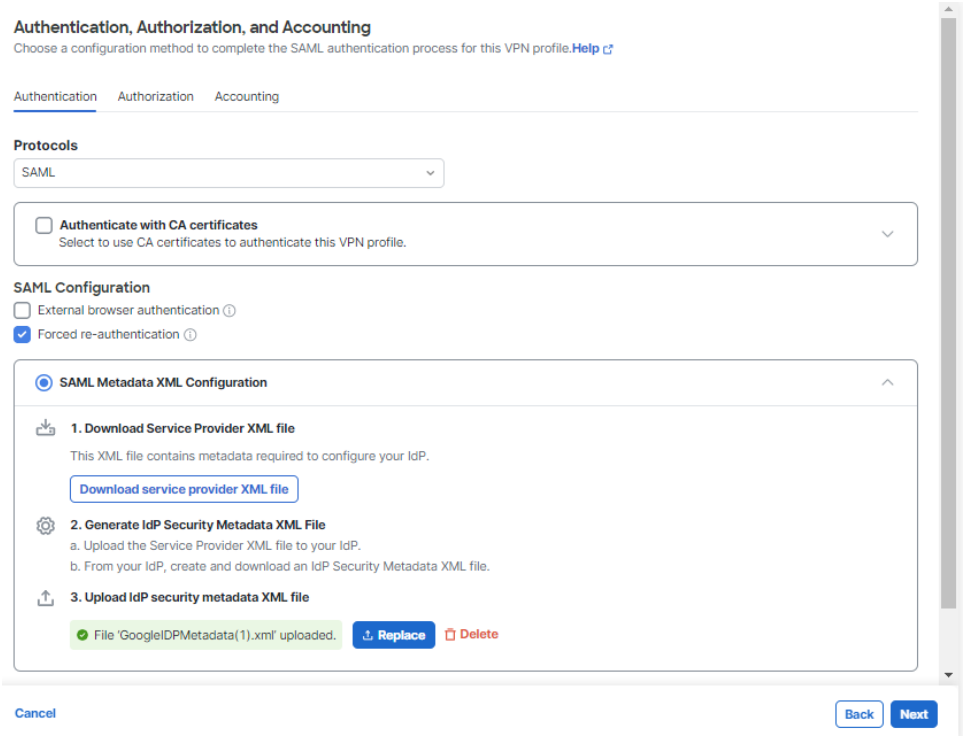
Choose from:

- SAML
- RADIUS
- Certificate

SAML

Explains how SAML authentication can be used to authenticate users and identifies the SAML option available in Secure Access China.

Use this option to authenticate users with SAML.



SAML Configuration

Describes SAML Configuration. When you choose SAML , each user is authenticated using the SAML single sign-on server. Forced re-authentication –Select this option to force a re-authentication whenever a VPN connection is initiated. Forced re-authentication is related to the Session Timeout setting; see Cisco Secure Client Configuration.

When you choose **SAML**, each user is authenticated using the SAML single sign-on server.

- **External browser authentication**–Select this option to have Secure Client use a local browser for authentication. When selected, Secure Client can support other SAML-based web authentication options, such as Single Sign On, biometric authentication, or other enhanced methods that are unavailable with an embedded browser.
- **Forced re-authentication**–Select this option to force a re-authentication whenever a VPN connection is initiated. Forced re-authentication is related to the Session Timeout setting; see Cisco Secure Client Configuration.

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**.

SAML Metadata XML Configuration

Describes SAML Metadata XML Configuration. Click the SAML Metadata XML Configuration option, provide your Service Provider XML file and follow the guidelines to complete your Identity Provider (IdP) setup.

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.

Manual Configuration

Describes manual Configuration. Click the Manual Configuration option complete the form with information obtained from your Service Provider (SP) and Identity Provider (IdP).

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.

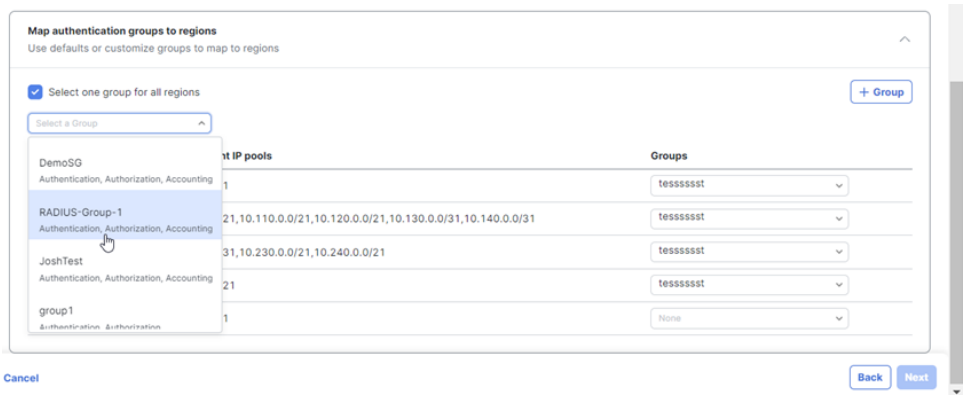
3. Obtain the following from the SAML IdP:
   a. Identity Provider Entity ID URL.
   b. Sign-in URL.
   c. Sign-out URL.
   d. IdP Certificate.
   e. Request Signature.

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.

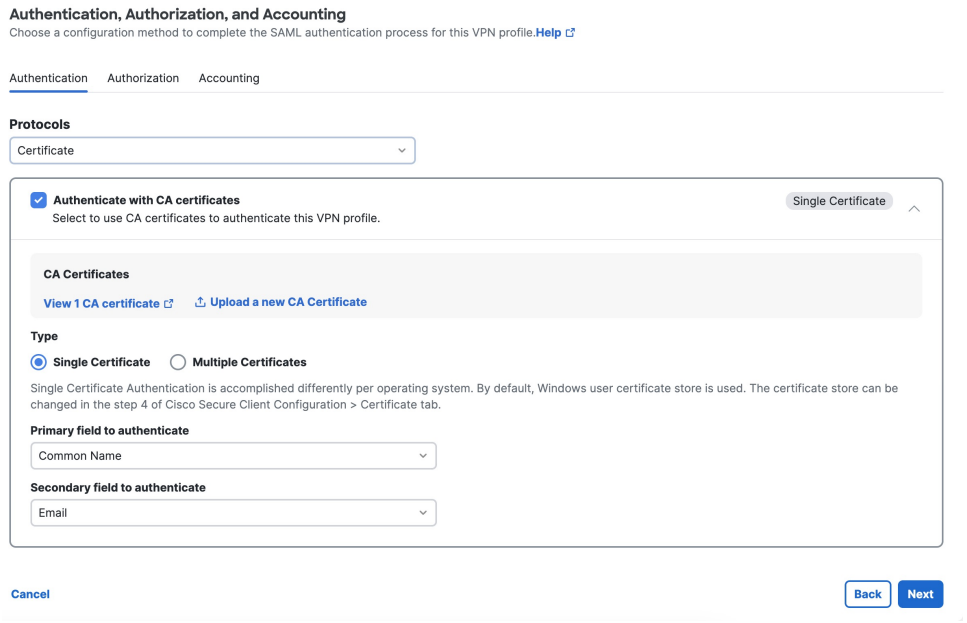
When you choose **RADIUS**, each user is authenticated using RADIUS group servers. RADIUS authentication for remote access VPNs supports **RADIUS**, **RADIUS+ Single CA certificate**, and **RADIUS+ Multiple CA Certificates**.



Certificate

Describes certificate. Use this option to authenticate users with trusted certificate authorities (CAs). Select Multiple Certificates authentication to authenticate the VPN client using the machine and user certificates.

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.

When **Multiple Certificates** authentication is enabled, you can select one of the following certificates to map the username and authenticate the VPN user:

- **First Cert**–Select this option from the **User certificate** drop-down list, to map the username from the machine certificate sent from the VPN client.
- **Second Cert**–Select this option from the **User certificate** drop-down list, to map the username from the user certificate sent from the client.

Note

Multiple certificate authentication utilizing a machine certificate requires that the **Windows certificate store override** option is enabled, and the **Client Certificate Store** option is set to **All** in Step 4 – Cisco Secure Client Configuration of the VPN profile configuration. See The Cisco Secure Client Profile Editor for complete information.

Note

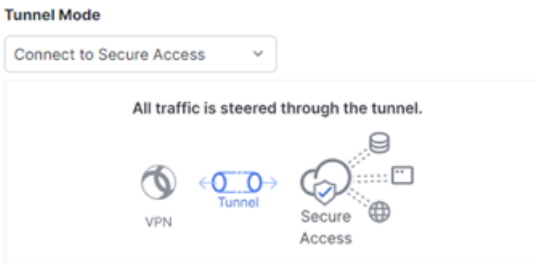
If you do not enable multiple certificate authentication, the user certificate (second certificate) is used for authentication by default.

Step 3 – Traffic Steering (Split Tunnel)

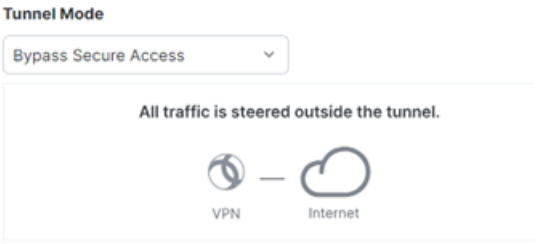
Describes step 3 – Traffic Steering (Split Tunnel). For Traffic Steering (Split Tunnel) , you can configure a VPN profile to maintain a full tunnel connection to Secure Access, or configure the profile to use a split tunnel connection to direct traffic through the VPN only if necessary.

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.

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.



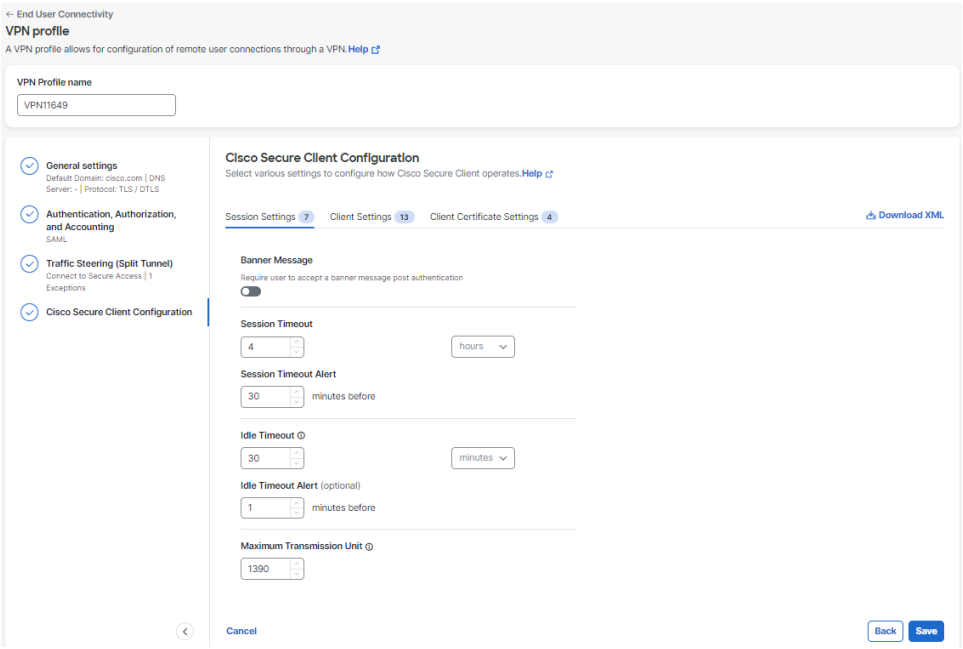
2. Depending on your selection, you can **Add Exceptions** to steer traffic inside or outside the tunnel. You can enter comma-separated IPs, domains, and network spaces.
3. For **DNS Mode**, you can accept the default DNS or choose to **Tunnel all DNS** traffic.
4. Click **Next** to configure the Cisco Secure Client.

Step 4 – Cisco Secure Client Configuration

Describes step 4 - Cisco Secure Client Configuration. You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN profile.

You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN profile.

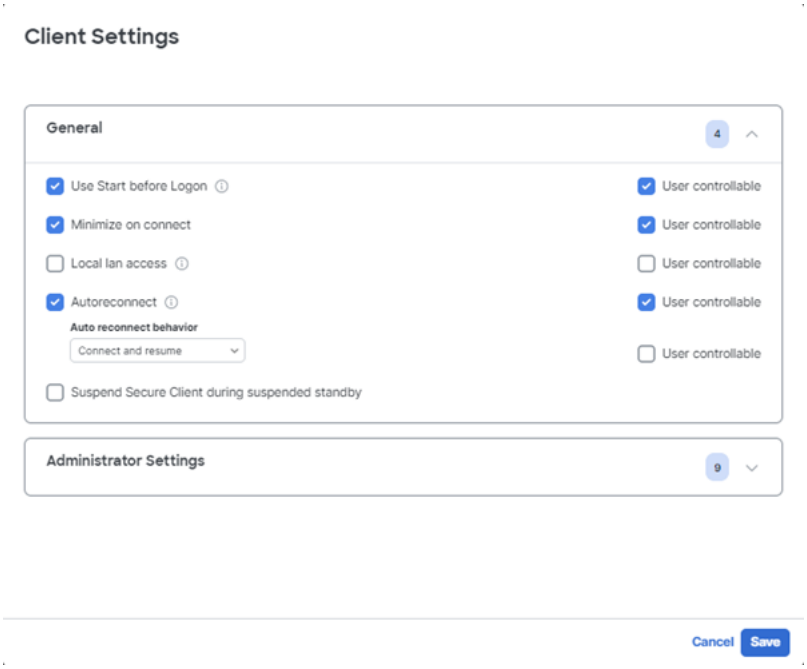
1. Click the **Session Settings** tab to modify session-specific settings:



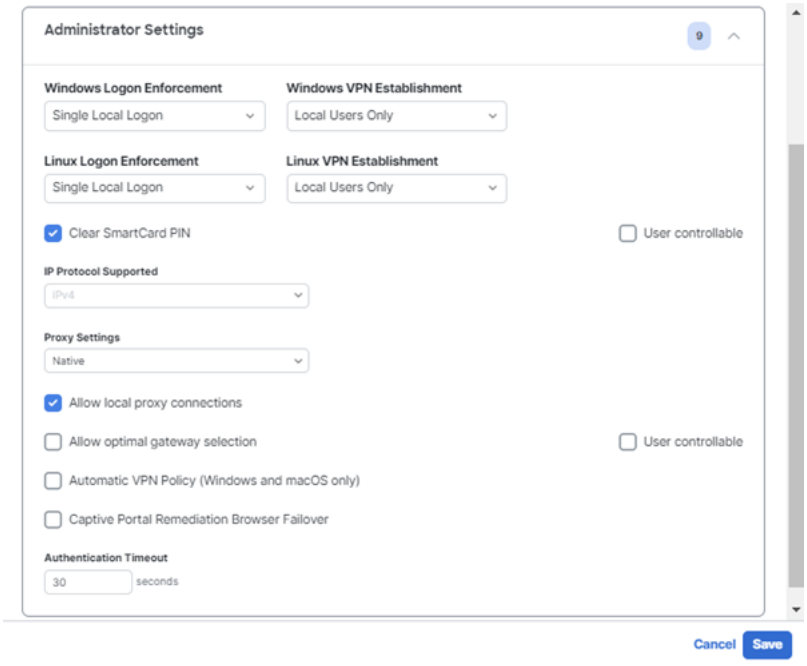
- **Banner Message**–Configure a banner message for the user to accept after Secure Client authentication.
- **Session Timeout**–Configure a time window after which the Secure Client session will end. The default is 4 hours.
- **Session Timeout Alert**–Configure the number of minutes before the session timeout to alert the user. The default is 30 minutes.
- **Idle Timeout**–Configure a time window for an idle Secure Client session, after which the session will end.
- **Idle Timeout Alert**–Configure the number of minutes before the idle session timeout to alert the user. The default is 1 minute.
- **Maximum Transmission Unit (MTU)**–Configure the largest packet size that can be transmitted through the VPN tunnel before fragmentation. Accepts a value between 576 and 1390.

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.



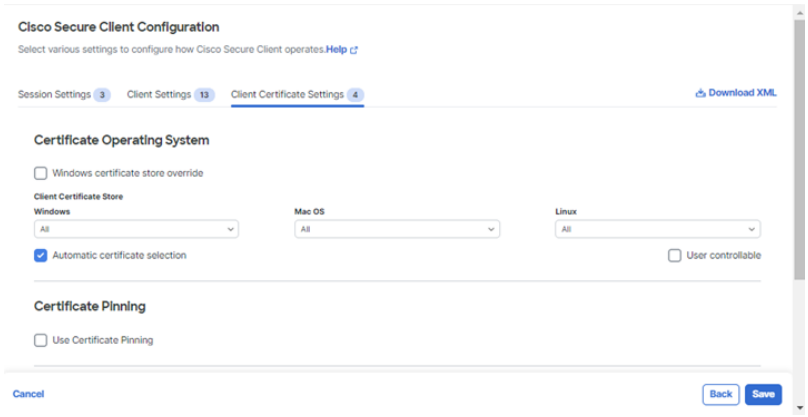
   b. Modify **Administrative Settings** as needed.



   c. Click **Save**.

3. Modify any **Client Certificate Settings** as needed.

> **Note**
>
> When the **Multiple Certificates** option is selected in Step 2 – Authentication, Authorization, and Accounting of the VPN profile configuration, enable the **Windows certificate store override** option, and set the **Client Certificate Store** option to **All**. See The Cisco Secure Client Profile Editor for complete information.



4. Click **Save** to complete the VPN Profile.

Manage Machine Tunnels

Provides instructions for managing machine Tunnels in Cisco Secure Access China. A Secure Access VPN machine tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user.

A Secure Access VPN machine tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. You can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint OS login scripts that require corporate network connectivity also benefit from this feature. For this tunnel to be created without user interaction, certificate-based authentication is used.

The Secure Access machine tunnel allows administrators to have the Cisco Secure Client connected without user intervention prior to when the user logs in. Secure Access machine tunnel is triggered when the endpoint is off-premise and disconnected from a user-initiated VPN. The Secure Access VPN machine tunnel is transparent to the end user and disconnects automatically when the user initiates VPN.

About the VPN Machine Tunnel

Describes about the VPN Machine Tunnel. The user initiates a VPN tunnel via the Secure Client, which triggers the machine tunnel termination. Upon machine tunnel termination, the user tunnel establishment continues as usual.

The Secure Client VPN agent service is automatically started upon system boot-up. It detects that the machine tunnel feature is enabled (via the VPN profile), therefore it launches the management client application to initiate a machine tunnel connection. The management client application uses the host entry from the VPN profile to initiate the connection. Then the VPN tunnel is established as usual, with one exception: no software update is performed during a machine tunnel connection since the machine tunnel is meant to be transparent to the user.

The user initiates a VPN tunnel via the Secure Client, which triggers the machine tunnel termination. Upon machine tunnel termination, the user tunnel establishment continues as usual.

The user disconnects the VPN tunnel, which triggers the automatic re-establishment of the machine tunnel.

For information about viewing connection events filtered by machine tunnel, see View the Remote Access Log Report.

Limitations

Describes limitations. A machine tunnel user with the email address machine@sse.com needs to be provisioned. For more information, see What to do Next.

- A machine tunnel user with the email address **machine@sse.com** needs to be provisioned. For more information, see What to do Next.
- User interaction is not supported.
- Certificate-based authentication through Machine Certificate Store (Windows) is only supported.
- Strict Server Certificate checking is enforced.
- A private proxy is not supported.
- A public proxy is not supported (ProxyNative value is supported on platforms where Native Proxy settings are not retrieved from the browser).
- Secure Client Customization Scripts are not supported.

Configure the VPN Machine Tunnel

Provides instructions for configuring the vpn machine tunnel. This section describes how to configure the Secure Access as the VPN gateway to accept connections from Secure Client through the VPN machine tunnel.

This section describes how to configure the Secure Access as the VPN gateway to accept connections from Secure Client through the VPN machine tunnel.

The following procedure explains how to add and configure the remote access VPN machine tunnel.

Prerequisites

Lists prerequisites for managing machine tunnels, including a Full Admin role in Secure Access and the account role information in Manage Accounts.

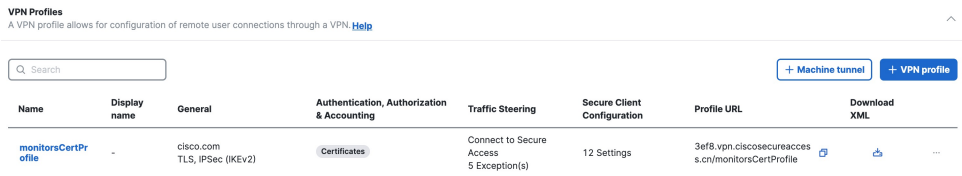
- Full Admin role in Secure Access. See Manage Accounts.

Step 1 – General Settings

Describes step 1 – General Settings. Configure the general settings, including the domain and the protocols this machine tunnel will use.

Configure the general settings, including the domain and the protocols this machine tunnel will use.

1. Navigate to **Connect > End User Connectivity > Virtual Private Network**.
2. In the **VPN Profiles** pane, click **+ Machine Tunnel**.



3. Configure the network and protocol settings for the machine tunnel:
   a. Enter the **Default Domain**.
   b. Choose a **DNS Server** from the drop-down, or click **Add**to add a new DNS server pair.

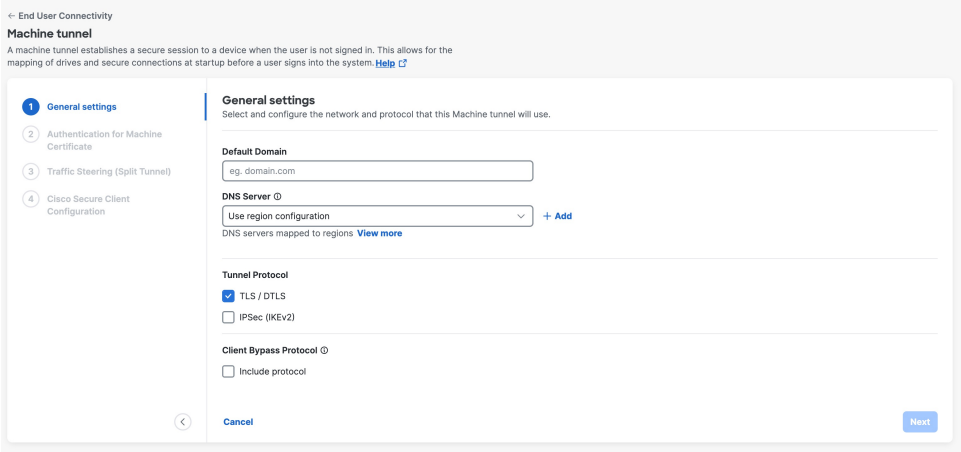
      The DNS server mapped through the **Manage IP Pool** page is set as the default server. Selecting another DNS server overwrites this default server.

c. Select the protocol that this machine tunnel will use:

- TLS/DTLS
- IPSec (IKEv2)

  At least one protocol must be selected.

d. Optionally, check **Include protocol** to enforce client bypass protocol.

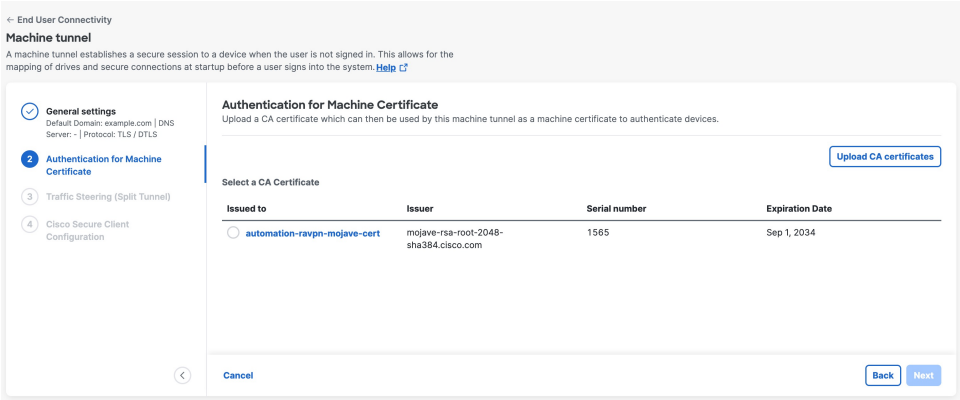


Step 2 – Authentication for Machine Certificate

Describes step 2 - Authentication for Machine Certificate. The machine tunnel is transparent to the end user and disconnects automatically when the user initiates a VPN session. For this tunnel to be created without user interaction, certificate-based authentication is used.

The machine tunnel is transparent to the end user and disconnects automatically when the user initiates a VPN session. For this tunnel to be created without user interaction, certificate-based authentication is used.

1. Choose CA certificates from the list, or click **Upload CA certificates**, which can then be used by the machine tunnel as a machine certificate to authenticate devices.



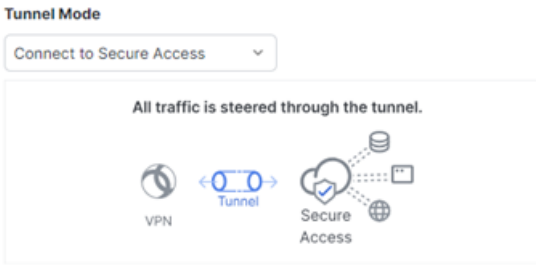
2. Click **Next** to configure the Traffic Steering.

Step 3 – Traffic Steering (Split Tunnel)

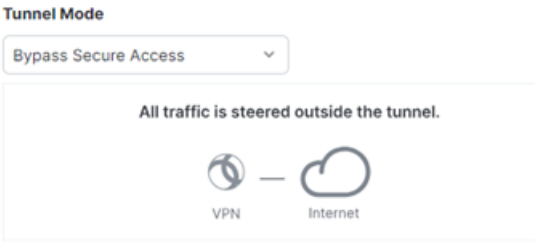
Describes step 3 - Traffic Steering (Split Tunnel). For Traffic Steering (Split Tunnel) , you can configure a machine tunnel to maintain a full tunnel connection to Secure Access, or configure it to use a split tunnel connection to direct traffic through the VPN only if necessary.

For **Traffic Steering (Split Tunnel)**, you can configure a machine tunnel to maintain a full tunnel connection to Secure Access, or configure it to use a split tunnel connection to direct traffic through the VPN only if necessary.

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.



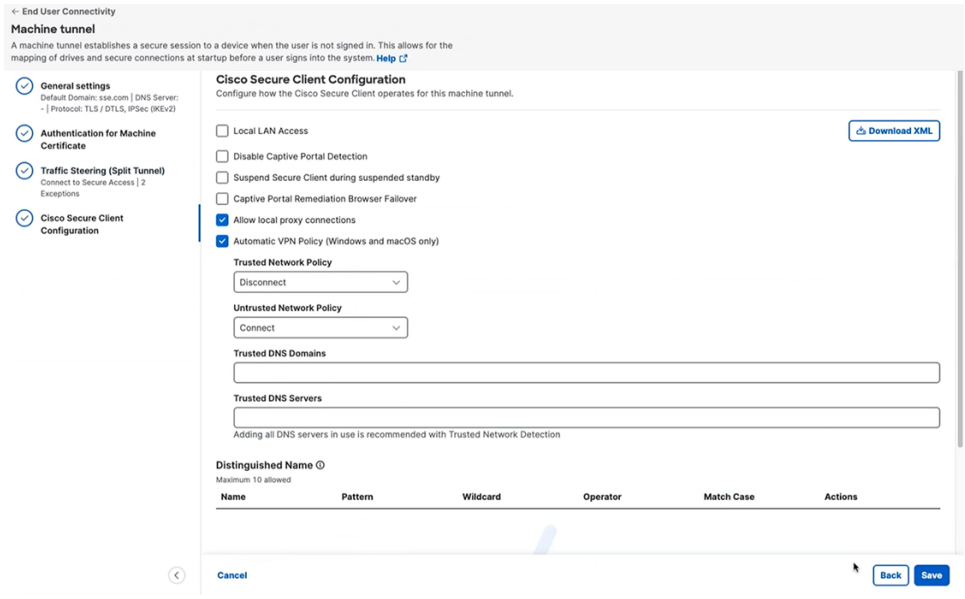
2. Depending on your selection, you can **Add Exceptions** to steer traffic inside or outside the tunnel. You can enter comma-separated IPs, domains, and network spaces.
3. For **DNS Mode**, you can accept the default mode or choose to **Tunnel all DNS** traffic.
4. Click **Next** to configure the Cisco Secure Client.

Step 4 – Cisco Secure Client Configuration

Describes step 4 – Cisco Secure Client Configuration. You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN machine tunnel.

You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN machine tunnel.

1. Review the options presented on the **Cisco Secure Client Configuration** tab.



2. Configure the options that are specific to your machine tunnel:

- **Local LAN Access**–Allows the user complete access to the local LAN connected to the remote computer during the VPN session to Secure Access.

> **Note**
>
> Enabling local LAN access can potentially create a security weakness from the public network through the user computer into the corporate network.

- **Disable Captive Portal Detection**–When Cisco Secure Client receives a certificate with a common name that does not match the Secure Access name, a captive portal is detected. This behavior prompts the user to authenticate. Some users using self signed certificates may want to enable connection to corporate resources behind an HTTP captive portal and should thus mark the **Disable Captive Portal Detection** checkbox. The administrator can also determine if they want the option to be user configurable and mark the checkbox accordingly. If user configurable is selected, the checkbox appears on the Preferences tab of the Cisco Secure Client UI.
- **Suspend Secure Client during suspended standby**– (Windows Only) Available only for devices that support Connected Standby. During Connected Standby, the operating system throttles system process, which can impact how packets are processed. With this option, you can disable VPN traffic when the system enters Connected Standby mode. The feature is disabled by default.
- **Captive Portal Remediation Browser Failover**–Allows the end user to use an external browser (after closing the Cisco Secure Client browser) for captive portal remediation.
- **Allow Local Proxy Connections**–By default, Cisco Secure Client lets Windows users establish a VPN session through a transparent or non-transparent proxy service on the local PC. Uncheck this parameter if you want to disable support for local proxy connections. Some examples of elements that provide a transparent proxy service include acceleration software provided by some wireless data cards, and network components on some antivirus software.
- **Automatic VPN Policy (Windows and macOS only)**–Enables Trusted Network Detection allowing Cisco Secure Client to automatically manage when to start or stop a VPN connection according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually. Setting an Automatic VPN Policy does not prevent users from manually controlling a VPN connection.

- **Trusted Network Policy**–Action Cisco Secure Client automatically takes on the VPN connection when the user is inside the corporate network (the trusted network).
  - Disconnect (Default)–Disconnects the VPN connection upon the detection of the trusted network.
  - Connect–Initiates a VPN connection upon the detection of the trusted network.
  - Do Nothing–Takes no action in the untrusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
  - Pause–Cisco Secure Client suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, Cisco Secure Client resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.
- **Untrusted Network Policy**–Cisco Secure Client starts the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.
  - Connect (Default)–Initiates the VPN connection upon the detection of an untrusted network.
  - Do Nothing–Takes no action in the trusted network. This option disables Always-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
- **Trusted DNS Domains**–DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *''.cisco.com*.

  Note

  Wildcards ('*') are **not** supported for DNS suffixes.

- **Trusted DNS Servers**–DNS server addresses (IP addresses separated by commas) that a network interface may have when the client is in the trusted network. For example: 192.168.1.2, 2001:DB8::1.

  Note

  Wildcards ('*') are **not** supported for DNS server addresses.

3. **Distinguished Name**–Specifies distinguished names (DNs) for exact match criteria in choosing acceptable client certificates. When you add multiple Distinguished Names, each certificate is checked against all entries, and all of them must match.

   Note

   A maximum of 10 distinguished names are allowed.

   - **Name**–The distinguished name (DN) to use for matching:
     - CN–Subject Common Name

- C–Subject Country
- DC–Domain Component
- DNQ–Subject Dn Qualifier
- EA–Subject Email Address
- GENQ–Subject Gen Qualifier
- GN–Subject Given Name
- I–Subject Initials
- L–Subject City
- N–Subject Unstruct Name
- O–Subject Company
- OU–Subject Department
- SN–Subject Sur Name
- SP–Subject State
- ST–Subject State
- T–Subject Title
- ISSUER-CN–Issuer Common Name
- ISSUER-DC–Issuer Component
- ISSUER-SN–Issuer Sur Name
- ISSUER-GN–Issuer Given Name
- ISSUER-N–Issuer Unstruct Name
- ISSUER-I–Issuer Initials
- ISSUER-GENQ–Issuer Gen Qualifier
- ISSUER-DNQ–Issuer Dn Qualifier
- ISSUER-C–Issuer Country
- ISSUER-L–Issuer City
- ISSUER-SP–Issuer State
- ISSUER-ST–Issuer State
- ISSUER-O–Issuer Company
- ISSUER-OU–Issuer Department
- ISSUER-T–Issuer Title
- ISSUER-EA–Issuer Email Address

4. Click **Save** to complete the VPN machine tunnel.

What to do Next

Describes what to do Next. You need to associate the machine tunnel with remote access VPN users. This is done by provisioning a machine tunnel user with a specific email (machine@sse.com) from your organization's identity provider (IdP), such as Active Directory.

You need to associate the machine tunnel with remote access VPN users. This is done by provisioning a machine tunnel user with a specific email (**machine@sse.com**) from your organization's identity provider (IdP), such as Active Directory. Secure Access supports various methods to provision users and groups.

Add the New Machine Tunnel User

Provides instructions for adding the user account required to configure a new Cisco Secure Client machine tunnel in Secure Access China.

Prerequisites

Lists the prerequisites for managing machine tunnels prerequisites 1. Full Admin user role. For more information, see Manage Accounts. An identity provider (IdP) configured and integrated with Secure Access. For more information, see Manage Users and Groups.

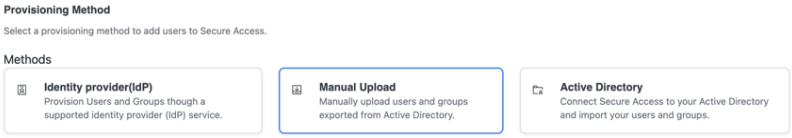
- Full Admin user role. For more information, see Manage Accounts.
- An identity provider (IdP) configured and integrated with Secure Access. For more information, see Manage Users and Groups.
- A configured machine tunnel applied to a VPN profile.

Procedure

Provides instructions for managing machine tunnels. To add the new machine tunnel user, provision the user through your supported identity provider (IdP). This example shows a manual upload of a CSV file.

To add the new machine tunnel user, provision the user through your supported identity provider (IdP). This example shows a manual upload of a CSV file.

1. Navigate to **Connect > Users and Groups > Users** and click **Provision Users**.
2. For **Provisioning Method**, click **Manual Upload** to provision the new machine tunnel user in your organization.

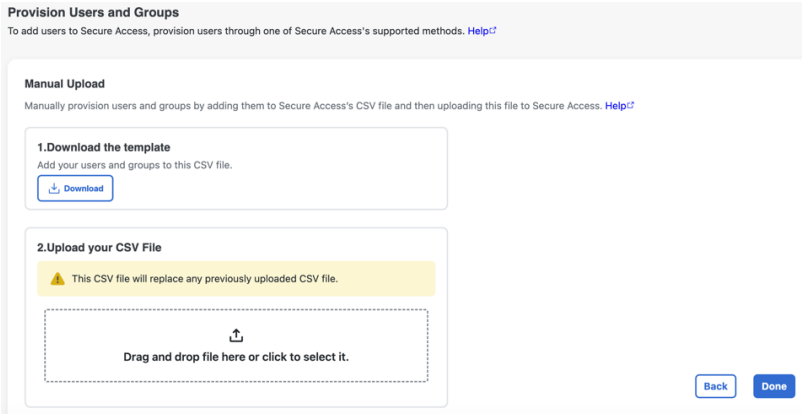


3. Click **Download** to save the Secure Access import template to your local system. The template is a CSV file that supports the following format:

```
DN,sn,givenName,userPrincipalName,mail,memberOf
```

   Note that **DN** and **memberOF** are not required. For complete information, see CSV File Format.

4. Add the machine tunnel user to the Secure Access CSV template file, and then upload the CSV file to Secure Access.

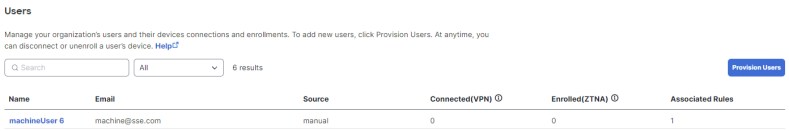


For example:

```
DN,sn,givenName,userPrincipalName,mail,memberOf
machineUser,6,machine@sse.com,machine@sse.com,adminGroup
```

5. Click **Done**.

   Once added, users and user groups can then be added to an access rule.



View Provisioned Users and Groups in Secure Access

Provides instructions for viewing provisioned users and groups in secure access. Navigate to Connect > Users and Groups to view the users and groups provisioned in your organization.

1. Navigate to **Connect > Users and Groups** to view the users and groups provisioned in your organization.
   a. See View User Details
   b. See View Group Details

11 Manage PAC Files

Topics:

- Manage PAC Files

Provides an overview of Manage PAC Files in Cisco Secure Access China, including Deploy the Secure Access PAC File for Windows, Deploy the Secure Access PAC File for macOS, and Customize the Secure Access PAC File. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage PAC Files

Provides instructions for managing PAC Files in Cisco Secure Access China. When configuring Cisco Secure Access Internet Security, you have several choices as to how you can send web traffic to Secure Access.

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).

Deploy the Secure Access PAC File for Windows

Provides instructions for 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 Internet Security.

Prerequisites

Lists the prerequisites for deploying secure access pac file for windows. 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.

- 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.

Procedure

Provides instructions for deploying secure access pac file for windows. 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.

> **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.

Copy the Secure Access PAC File URL

Describes 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.

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

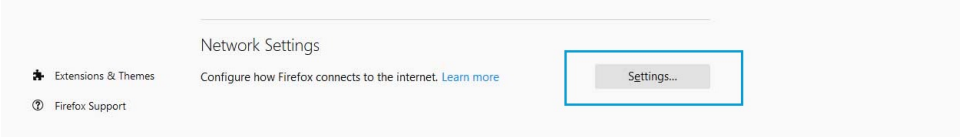
Provides instructions for deploying the secure access pac file url for chrome and edge browsers.

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.

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

Provides instructions for 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 Internet Security.

Prerequisites

Lists the prerequisites for deploying secure access pac file for mac. Full Admin user role. For more information, see Manage Accounts.

- 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.

Procedure

Provides instructions for deploying secure access pac file for mac. 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.

> **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.

Copy the Secure Access PAC File URL

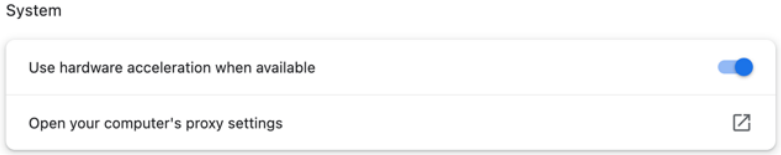
Describes copy the Secure Access PAC File URL. Navigate to Connect > End User Connectivity > Internet Security. Copy the Secure Access PAC file URL and save to your system.

1. Navigate to **Connect > End User Connectivity > Internet Security**.
2. Copy the Secure Access PAC file URL and save to your system.

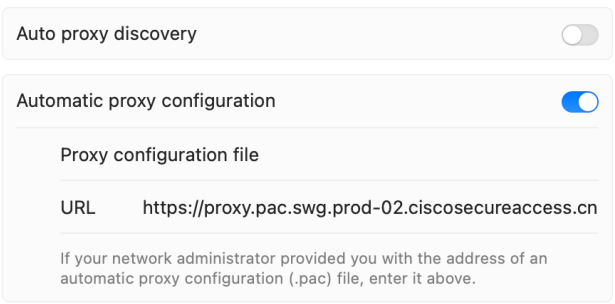
Deploy the Secure Access PAC File URL to Chrome

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.

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.

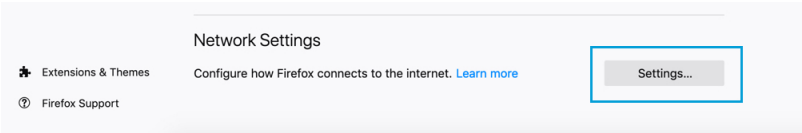


3. Click **OK** and then **Apply**.

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.

1. Open your Firefox browser, navigate to **Firefox > Preferences**, scroll to **Network Settings**, and click **Settings**.

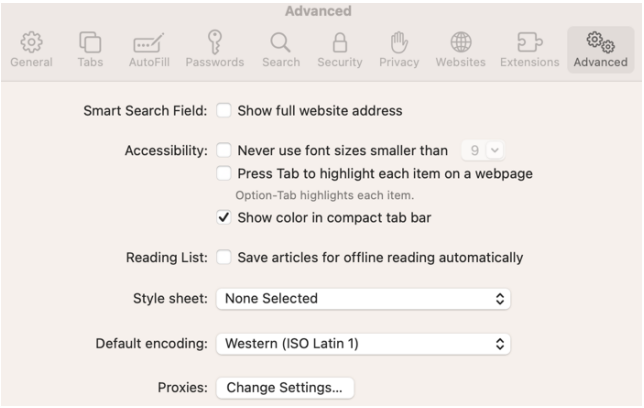


2. Check **Automatic Proxy Configuration URL** and paste the Secure Access PAC file URL.
3. Click **OK**.

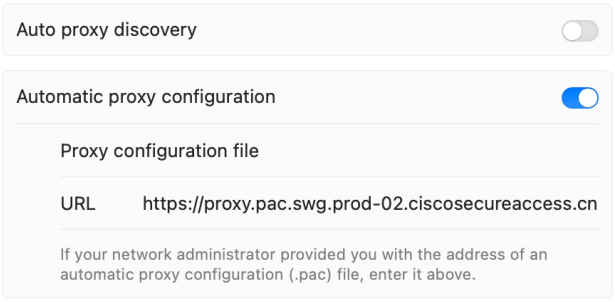
Deploy the Secure Access PAC File URL to Safari

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.

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

Provides instructions for customizing 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.

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 Internet Security.

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.

Prerequisites

Lists the prerequisites for customizing secure access pac file, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

- 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.

Procedure

Provides instructions for customizing 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.

Copy the Secure Access PAC File

Describes copy the Secure Access PAC File. Navigate to Connect > End User Connectivity > Internet Security. Copy the Secure Access PAC file URL.

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.

1. Paste the copied PAC URL into a browser's address bar and then press **Enter** or **Return** to download the PAC file.



Edit the PAC File

Provides instructions for 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.

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**.

```
//-----------------------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----------------------
```

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

Describes 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.

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

Describes 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.

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.

We recommend that you bypass the following domains directly to allow all traffic with TCP on ports 80 and 443:

- ocsp.int-x3.letsencrypt.org
- isrg.trustid.ocsp.identrust.com
- *.cisco.com
- *.opendns.com
- *.sse.com
- *.umbrella.com
- *.okta.com
- *.oktacdn.com
- *.pingidentity.com
- secure.aadcdn.microsoftonline-p.com

12 Manage Internet Security

Topics:

- Manage Internet Security

Provides an overview of Manage Internet Security in Cisco Secure Access China, including Set Up Internet Security on User Devices, Manage Internet Security Bypass, and Configure Cisco Secure Client Settings. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Internet Security

Provides instructions for managing internet Security in Cisco Secure Access China. You can manage the Cisco Secure Access Internet Security settings in Secure Access to protect the user devices in your organization.

You can manage the Cisco Secure Access Internet Security settings in Secure Access to protect the user devices in your organization.

> **Note**
>
> User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file for the browsers in the environment.

Set Up Internet Security on User Devices

Provides instructions for setting up internet Security on User Devices in Cisco Secure Access China. Before you add web security in Cisco Secure Access for end users, deploy the Cisco Secure Client or the Secure Access or custom PAC files in your environment.

Before you add web security in Cisco Secure Access for end users, deploy the Cisco Secure Client or the Secure Access or custom PAC files in your environment. User devices with the Cisco Secure Client installed must also deploy the Umbrella Roaming Security module.

This guide describes the steps to download the software package for the Cisco Secure Client or copy the URL for the Secure Access PAC file to your environment.

To complete the setup, we recommend that you provision users and groups from the organization in Secure Access. For more information, see Manage Users and Groups.

Prerequisites

Lists the prerequisites for setting up internet security on user devices. Full Admin user role. For more information, see Manage Accounts.

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

Visibility of User Identities in Policy Rules

Describes 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.

- Deploy the Secure Access Active Directory (AD) Connector. For more information, see Connect Active Directory to Secure Access.
- Provision users and groups in Secure Access. For more information, see Provision Users and Groups from Active Directory.

Procedure

Provides instructions for setting up internet security on user devices. Download the Secure Access OrgInfo.json file for the organization or copy the Secure Access PAC file URL. Use the deployment configuration files to set up the Cisco Secure Client or browsers on the user devices.

Download the Secure Access OrgInfo.json file for the organization or copy the Secure Access PAC file URL. Use the deployment configuration files to set up the Cisco Secure Client or browsers on the user devices.

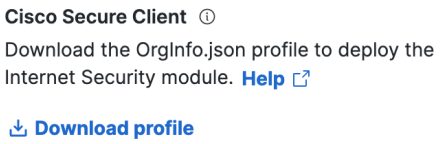
For more information about deploying PAC files with Secure Access, see Manage PAC Files.

Download the OrgInfo.json File

Provides instructions for downloading the orginfo.json file. Download the Secure Access OrgInfo.json file to the user devices where you have deployed the Cisco Secure Client. For more information about deploying the OrgInfo.json file, see Download the OrgInfo.json File.

1. Navigate to **Connect > End User Connectivity > Internet Security**.
2. For **Cisco Secure Client**, click **Download profile**.

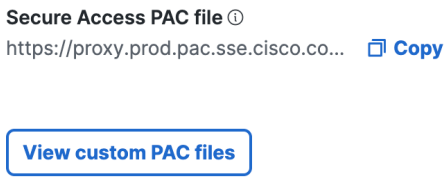
   Download the Secure Access OrgInfo.json file to the user devices where you have deployed the Cisco Secure Client. For more information about deploying the OrgInfo.json file, see Download the OrgInfo.json File.



Copy the PAC File URL

Describes copy the PAC File URL. Navigate to Connect > End User Connectivity > Internet Security. For Secure Access PAC file , click Copy to get the Secure Access PAC file URL. For more information about the Secure Access PAC file and deploying custom PAC files, see Manage PAC Files.

1. Navigate to **Connect > End User Connectivity > Internet Security**.
2. For **Secure Access PAC file**, click **Copy** to get the Secure Access PAC file URL. For more information about the Secure Access PAC file and deploying custom PAC files, see Manage PAC Files.



Manage Internet Security Bypass

Provides instructions for managing internet Security Bypass in Cisco Secure Access China. You can configure certain destinations in Cisco Secure Access to bypass internet security for end users.

You can configure certain destinations in Cisco Secure Access to bypass internet security for end users. Add a destination–an IP address, CIDR block, or domain–and manage how Secure Access resolves DNS requests to the destination. Traffic on a destination can bypass the Secure Web Gateway.

Add Destinations for Internet Security Bypass

Provides instructions for adding destinations for Internet Security Bypass in Cisco Secure Access China. You can configure certain destinations in Cisco Secure Access China to bypass internet security for end users.

You can configure certain destinations in Cisco Secure Access China to bypass internet security for end users. To bypass internet security on a destination, add an IP address, CIDR block, or domain in Secure Access China. After you add a destination to bypass internet security, you can view, edit, or delete the destination.

This guide describes the steps to add destinations in Secure Access China where DNS requests for the destinations bypass the Secure Web Gateway.

Prerequisites

Lists the prerequisites for adding destinations internet security bypass. Full Admin user role. For more information, see Manage Accounts. User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file on the browsers in the environment.

- Full Admin user role. For more information, see Manage Accounts.
- User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file on the browsers in the environment.

Procedure

Provides instructions for adding destinations internet security bypass. Add destinations in Secure Access China to bypass internet security. Traffic for destinations that are added in Secure Access China bypass the Secure Access DNS resolvers and Secure Web Gateway or the Secure Web Gateway only.

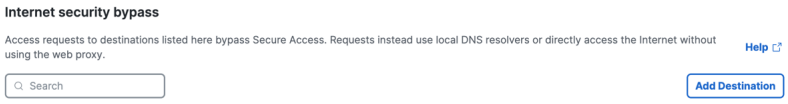
Add destinations in Secure Access China to bypass internet security. Traffic for destinations that are added in Secure Access China bypass the Secure Web Gateway only.

If you configure DNS requests to bypass the SWG, the queries are sent to the organization's local DNS resolvers.

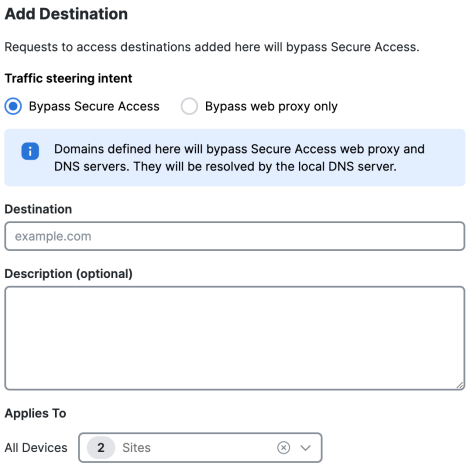
Steer Traffic to Secure Access China or Bypass Domains

Describes steer Traffic to Secure Access China or Bypass Domains. Navigate to Connect > End User Connectivity > Internet Security , and then click Add Destination.

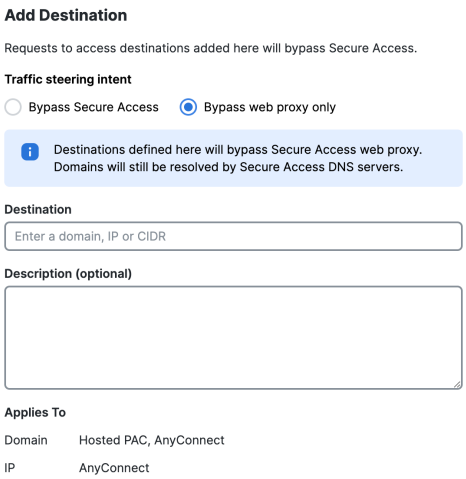
1. Navigate to **Connect > End User Connectivity > Internet Security** , and then click **Add Destination**.



2. Choose **Bypass Secure Access** to bypass the Secure Access SWG.
   a. For **Destination**, enter a domain name.
   b. (Optional) For **Description**, enter text that describes this domain.
   c. For **Applies To**, choose the Secure Access China Sites for all devices that should bypass the domain.



3. Choose **Bypass web proxy only** to bypass the Secure Web Gateway (SWG) only.
   a. For **Destination**, enter a domain name.
   b. (Optional) For **Description**, enter text that describes this destination.



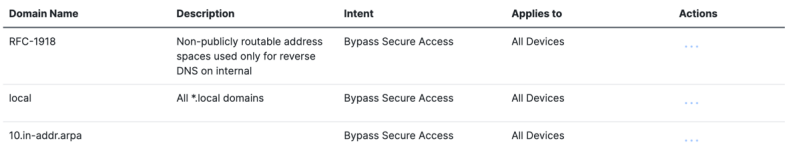
4. Click **Save**.

View Destinations for Internet Security Bypass

Provides instructions for viewing destinations for internet security bypass. After you add the destinations in Secure Access China to bypass internet security, you can view the details about the destinations.

After you add the destinations in Secure Access China to bypass internet security, you can view the details about the destinations.

1. Navigate to **Connect > End User Connectivity > Internet Security**.
2. View the domains that you added to the bypass internet security list in Secure Access China.
   - **Domain Name**–The name of the domain.
   - **Description**–The text that describes the domain.
   - **Intent**–The type of domain, for example: **Bypass Secure Access**.
   - **Applies to**–The name of a Site or the location of the Secure Access China Virtual Appliance (VA) deployment where the domain is bypassed.
   - **Actions**–The actions taken to manage the destination in Secure Access China.



Domain Name	Description	Intent	Applies to	Actions
RFC-1918	Non-publicly routable address spaces used only for reverse DNS on internal	Bypass Secure Access	All Devices	...
local	All *.local domains	Bypass Secure Access	All Devices	...
10.in-addr.arpa		Bypass Secure Access	All Devices	...

Edit Destinations for Internet Security Bypass

Provides instructions for editing destinations for Internet Security Bypass in Cisco Secure Access China. After you add a destination to bypass internet security in Cisco Secure Access China, you can edit the internet security bypass information for the destination.

After you add a destination to bypass internet security in Cisco Secure Access China, you can edit the internet security bypass information for the destination.

This guide describes the steps to edit destinations in Secure Access China that are configured to bypass internet security. You can modify the internet security information for destinations that bypass the Secure Access Secure Web Gateway (SWG).

Prerequisites

Lists the prerequisites for editing destinations for internet security bypass. Full Admin user role. For more information, see Manage Accounts.

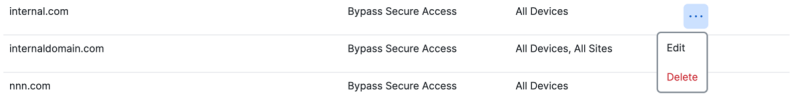
- Full Admin user role. For more information, see Manage Accounts.
- User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file on the browsers in the environment.

Procedure

Provides instructions for editing destinations for internet security bypass. Edit a destination that is configured to bypass internet security in Secure Access China.

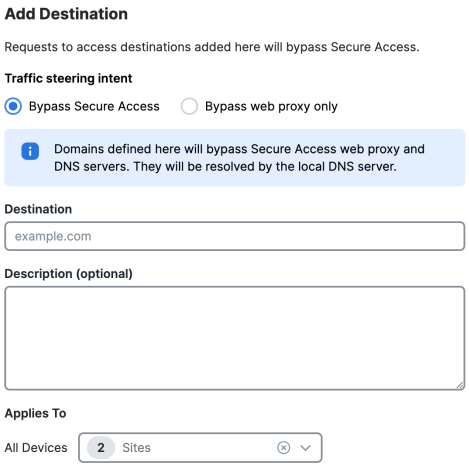
Edit a destination that is configured to bypass internet security in Secure Access China.

1. Navigate to **Connect > End User Connectivity > Internet Security**.
2. Navigate to **Internet security bypass**, navigate to a destination in the internet security bypass table, and then click the ellipsis (**...**).
3. Click **Edit** to modify the bypass information for the destination.



4. Navigate to **Traffic steering intent**.
5. Choose **Bypass Secure Access** to bypass the Secure Access Secure Web Gateway.

> **Note**
>
> DNS requests for the destination are resolved by the organization's local DNS servers.
>
> a. For **Destination**, enter a domain name.
> b. (Optional) For **Description**, enter text that describes this domain.
> c. For **Applies To**, choose the Sites in Secure Access China for all devices that should bypass the domain.



6. Choose **Bypass web proxy only** to bypass the Secure Web Gateway only.
7. Click **Save**.

Delete Destination for Internet Security Bypass

Provides instructions for deleting destination for Internet Security Bypass in Cisco Secure Access China. After you add a destination to bypass internet security in Cisco Secure Access China, you can remove the destination.

After you add a destination to bypass internet security in Cisco Secure Access China, you can remove the destination. As a result of removing the destination, the DNS requests for the destination will resolve to their local organization DNS resolvers.

Prerequisites

Lists the prerequisites for deleting destination for internet security bypass. Full Admin user role. For more information, see Manage Accounts.

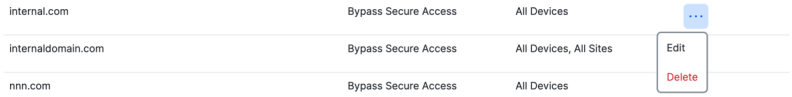
- Full Admin user role. For more information, see Manage Accounts.

Procedure

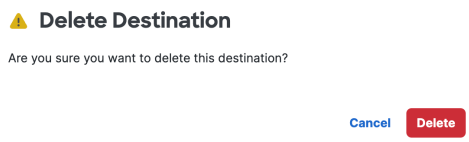
Provides instructions for deleting destination for internet security bypass. Remove a domain that is configured for internet security bypass in Secure Access China.

Remove a domain that is configured for internet security bypass in Secure Access China.

1. Navigate to **Connect > End User Connectivity > Internet Security**.
2. Navigate to **Internet security bypass**, navigate to a destination in the internet security bypass table, and then click the ellipsis (**...**).
3. Click **Delete**.



4. Click **Delete** to confirm the removal of the destination.



About Internet Security Bypass

Describes about Internet Security Bypass. If you bypass internet security in Secure Access, DNS requests for the destinations bypass the Secure Access DNS servers and Secure Web Gateway. T the organization's local DNS servers resolve the DNS requests.

Internet security bypass is supported on user devices with the Cisco Secure Client (formerly known as AnyConnect) deployed or browsers in the environment with a configured Secure Access or custom PAC file. User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module.

- If you bypass internet security in Secure Access, the organization's local DNS servers resolve the DNS requests.

Set Up Internet Security Bypass

Provides instructions for setting up internet security bypass. Add a destination in Secure Access to bypass internet security. For more information, see Add Destinations for Internet Security Bypass.

- Add a destination in Secure Access to bypass internet security. For more information, see Add Destinations for Internet Security Bypass.
- Edit a destination in Secure Access that is configured to bypass internet security. For more information, see Edit Destination for Internet Security Bypass.
- Delete a destination in Secure Access that is configured to bypass internet security. For more information, see Delete Destination for Internet Security Bypass.

Configure Cisco Secure Client Settings

Provides instructions for configuring cisco Secure Client Settings in Cisco Secure Access China. You can configure the Cisco Secure Access Internet Security in Secure Access for end users.

You can configure the Cisco Secure Access Internet Security in Secure Access for end users.

> **Note**
>
> User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file for the browsers in the environment.

This guide describes the steps to enable the DNS and web security settings and advanced internet security settings in Secure Access for the end user devices in the organization.

Prerequisites

Lists the prerequisites for configuring Cisco Secure Client settings, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for configuring Cisco Secure Client settings. Configure the Cisco Secure Client internet security settings. The advanced internet settings contains several fields that provide additional control over user authentication, traffic bypass, and VPN compatibility.

Configure the Cisco Secure Client internet security settings. The advanced internet settings contains several fields that provide additional control over user authentication, traffic bypass, and VPN compatibility.

Configure Security Settings

Provides instructions for configuring DNS and web security settings as part of setting up security features in Secure Access China.

- Configure DNS and Web Security

Configure Advanced Security Settings

Provides instructions for configuring advanced security settings. Use Active Directory for Access Policy. Third Party VPN compatibility. Configure Cisco Secure Client Settings.

- Use Active Directory for Access Policy
- Third Party VPN compatibility
- Configure Cisco Secure Client Settings
- Secure Web Gateway Backoff Settings

Configure Web Security

Provides instructions for configuring web security. Configure web security settings for the Cisco Secure Client. Enable the Web Security (port 80/443 traffic only) toggle button.

Configure web security settings for the Cisco Secure Client.

The Cisco Secure Client with the Umbrella Roaming Security module steers web traffic on ports 80/443 to the Secure Web Gateway (SWG). All web traffic is evaluated against the organization's policy and Internet Access rules when a VPN connection is not established.

> **Note**
>
> You can override this option on individual roaming devices.

- Enable the **Web Security (port 80/443 traffic only)** toggle button.

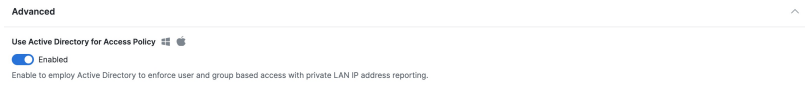


Use Active Directory for Access Policy

Provides instructions for using active directory for access policy. Enable the Cisco Secure Client to synchronize users and groups identities with the Secure Access Active Directory (AD) Connector. Secure Access applies Access rules for user identities, which are associated with devices that have deployed the Cisco Secure Client.

Enable the Cisco Secure Client to synchronize users and groups identities with the Secure Access Active Directory (AD) Connector. Secure Access applies Access rules for user identities, which are associated with devices that have deployed the Cisco Secure Client.

- Enable the **Use Active Directory for Access Policy** toggle button.



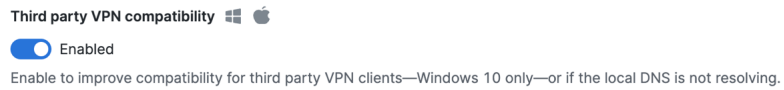
Third Party VPN Compatibility

Describes third Party VPN Compatibility. Improve compatibility for third-party VPN clients on Windows 10 only, or if the local DNS is not resolving resources.

Improve compatibility for third-party VPN clients on Windows 10 only, or if the local DNS is not resolving resources.

The Cisco Secure Client with the Umbrella Roaming Security module works with most VPN software. However, the Cisco Secure Client with the Umbrella Roaming Security module and other VPN profiles may not resolve local DNS queries correctly on a VPN connection with Windows 10. The local LAN may bind above the VPN, failing to resolve local DNS requests over the tunnel. Select this setting to apply the legacy binding order behavior.

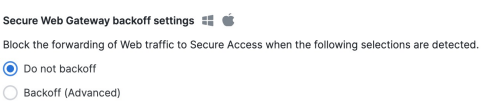
- Enable the **Third Party VPN Compatibility** toggle button.



Secure Web Gateway Backoff Settings

Provides instructions for securing web gateway backoff settings. Select Do not backoff to disable secure web gateway backoff. Bypass Web traffic from Secure Access for the following contexts:.

- Select **Do not backoff** to disable secure web gateway backoff.



- Select **Backoff (Advanced)**.

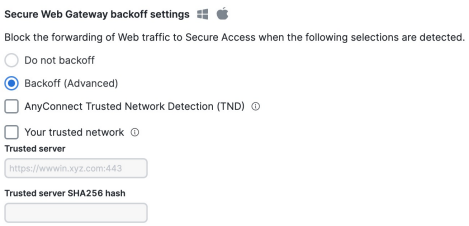
> **Note**
>
> The **AnyConnect Trusted Network Detection (TND)** and **Your trusted network** options are only supported with user devices that have version 5.1.3.62 or higher of the Cisco Secure Client with the Umbrella Roaming Security module deployed. For information about downloading the Cisco Secure Client software packages, see Cisco Secure Client Version 5.1.3.62.

Bypass Web traffic from Secure Access for the following contexts:

- Select **AnyConnect Trusted Network Detection (TND)** to disable web traffic forwarding from an endpoint to Secure Access if the network is trusted. This setting requires that you have the Trusted Network Detection (TND) setting enabled in the AnyConnect VPN profile for the user devices.
- Select **Your Trusted network** to enable endpoints to detect an organization's trusted network, which is identified by the **Trusted server** and **Trusted server SHA256 hash** fields. When the endpoint detects trusted networks, traffic from the endpoints bypass Secure Access and the endpoints rely on the network protections.
  - For **Trusted server**, enter the URL (`<domain>:<port>`) of the trusted network server, which hosts the trusted server certificate.

    This option disables redirects to Secure Access when on the trusted network identified by the trusted network server.
  - For **Trusted server SHA256 hash**, enter the SHA256 hash for the trusted network server's certificate.

    The ID of the trusted network server's certificate must match the configured SHA256 hash.



Download Cisco Secure Client or Copy Secure Access PAC File URL

Provides instructions for downloading Cisco Secure Client or copy secure access pac file url. To deploy the Secure Access Internet Security on user devices, first download and install the software package for the Cisco Secure Client or copy the URL for the Secure Access PAC file from Secure Access.

To deploy the Secure Access Internet Security on user devices, first download and install the software package for the Cisco Secure Client or copy the URL for the Secure Access PAC file from Secure Access.

You can also install custom PAC files in your environment. For more information about deploying PAC files, see Manage PAC Files.

Add Bypass Domains and Set Up Internet Security

Provides instructions for adding bypass domains and set up internet security. Once you install and deploy the Cisco Secure Client or the Secure Access or custom PAC files in the environment, add bypass domains in Secure Access.

Once you install and deploy the Cisco Secure Client or the Secure Access or custom PAC files in the environment, add bypass domains in Secure Access. Then, configure DNS and web security settings for the user devices in the organization.

Next Steps

Outlines follow-up tasks for internet security, including setting up user devices, managing internet security bypass, and configuring Cisco Secure Client settings.

- Set Up Internet Security on User Devices
- Manage Internet Security Bypass
- Configure Cisco Secure Client Settings

13 Manage Resources

Topics:

- Manage Resources

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

Manage Resources

Provides instructions for managing resources in Cisco Secure Access China. 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:

Lists resource menu items that can be selected as access rule sources, including registered networks, internal networks, and roaming devices.

- 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:. Content Category 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:

Lists resource menu items that can be selected as destinations in private access rules, including private resources managed in Secure Access China.

- 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.

14 Manage Registered Networks

Topics:

- Manage Registered Networks

Provides an overview of Manage Registered Networks in Cisco Secure Access China, including Add Network Resources, Update a Network Resource, and Delete a Network Resource. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Registered Networks

Provides instructions for managing registered Networks in Cisco Secure Access China. A resource is an internet capable entity that is managed by your organization.

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 IPv4 static IP addresses and dynamic IP addresses over IPv4. In Secure Access, all traffic originating from the public IP space is identified as coming from that network. The public IP space or IP range defines the scope of the network resource.

To start protecting the networks in your organization, see Add Network Resources.

Add Network Resources

Provides instructions for adding network Resources in Cisco Secure Access China. A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses.

A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access China supports IPv4 for both static IP addresses and dynamic IP addresses. In Secure Access China, 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 China. Once you've configured and added a network resource, build policy rules to extend Secure Access China'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

Lists the prerequisites for adding network resources. 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

Describes dynamic IP Address–IPv4 Only. Secure Access China 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.

Secure Access China 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 China 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 China 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 China does not support third-party DDNS clients.

Download the Cisco Dynamic IP Updater

Provides instructions for downloading the cisco dynamic ip updater. Download the Cisco Dynamic IP Updater for your system. Windows 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

Provides instructions for installing the cisco dynamic ip updater. Install the Cisco Dynamic IP Updater on one of the devices on your dynamic IP network.

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 China).
- Ensure that the device is always powered on or turned on before any other devices sign on to the network.

Procedure

Provides instructions for adding network resources. 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 China at the same time. Pre-registering networks ensures that all IP spaces that belong to your organization are added to Secure Access China. If you have more than one public egress IP in your organization, configure a network resource for each IP address.

- 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

Describes step 1 - Select the Network. First, determine the IP address of your network. Your IPv4 address and location are displayed.

First, determine the IP address of your network.

1. Go to http://www.whatismyip.com.

   Your IPv4 address and location are displayed.

2. In Secure Access China, navigate to **Resources > Registered Networks**.

   The public IP address of your network is listed at the top of the page.

> **Note**
>
> Depending on your package, if you attempt to add a network other than the one currently being used to access Secure Access China, Secure Access China 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.

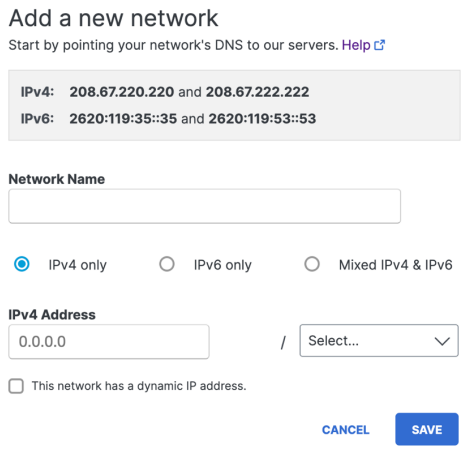
Step 2 – Configure the Network Resource

Describes step 2 – Configure the Network Resource. Select a protocol based on the IP address where you have configured your router.

Before you begin, determine if you have an IPv4 dynamic IP address. Secure Access China 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 China. Otherwise, Secure Access China 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.

1. Navigate to **Resources > Registered Networks** and click **Add**.
2. Give your network resource a descriptive **Network Name**.



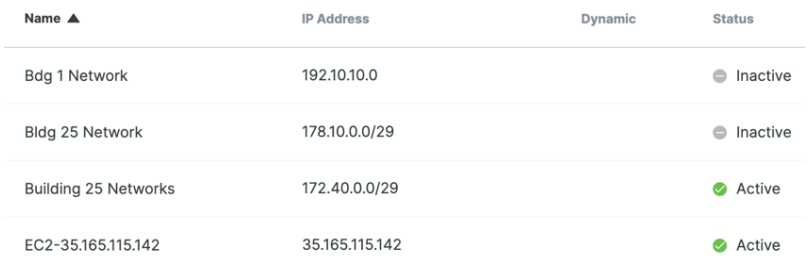
3. Choose an internet protocol: **IPv4**, **IPv6**, or **Mixed IPv4 & IPv6**.

   Select a protocol based on the IP address where you have configured your router.

4. Add the network's IP address and choose a subnet mask.
5. For IPv4 only, if you have a dynamic IP address, check **This network has a dynamic IP address**.

6. Click **Save**.

   Once Secure Access China validates your IP address, the network resource is listed at **Resources > Registered Networks**. Initially, Secure Access China lists the status of your network as **Inactive**. When Secure Access China 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.

> **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 China 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 China'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 China's global network.

> **Note**
>
> You may need to restart your client's network interface or your device.

Update a Network Resource

Provides instructions for updating a Network Resource in Cisco Secure Access China. Once you add a Registered Network resource—a public static or dynamic IP network—to Cisco Secure Access, you can update the resource.

Once you add a Registered Network resource—a public static or dynamic IP network—to Cisco Secure Access, you can update the resource.

Prerequisites

Lists the prerequisites for updating a network resource, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Edit the Registered Network Resource Name

Provides instructions for editing the registered network resource name. Navigate to Resources > Registered Networks. Click the pencil icon to edit the Network resource Name.

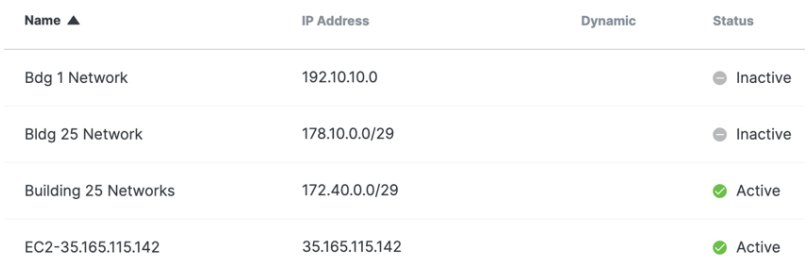
1. Navigate to **Resources > Registered Networks**.
2. Click the pencil icon to edit the Network resource **Name**.
3. Enter a descriptive name for the network and then click **Save**.

Update the Registered Network Resource

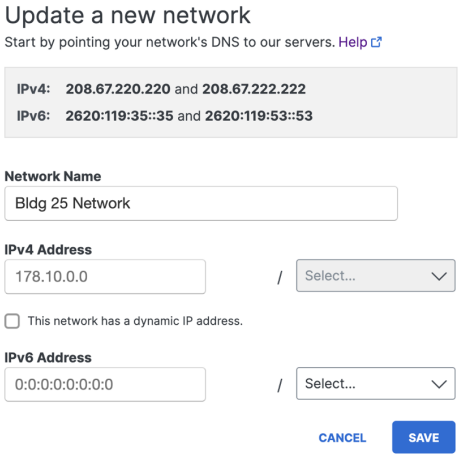
Provides instructions for updating the registered network resource. The + icon does not appear until you hover over the Network resource.

1. Navigate to **Resources > Registered Networks**.
2. Hover over a network resource and click the **+** to open the configuration dialog.

   The **+** icon does not appear until you hover over the Network resource.



3. Follow the steps in Add Network Resources to update the Registered Network resource.



Delete a Network Resource

Provides instructions for deleting a Network Resource in Cisco Secure Access China. 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.

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.

Prerequisites

Lists the prerequisites for deleting a network resource, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

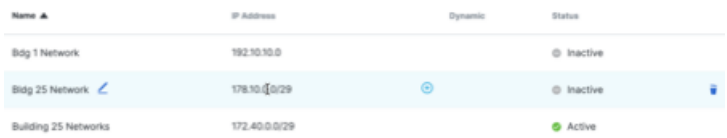
- Full Admin user role. For more information, see Manage Accounts.

Procedure

Provides instructions for deleting a network resource. The Network resource is deleted from Secure Access and is removed from any policy rules.

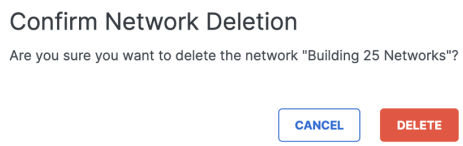
1. Navigate to **Resources > Registered Networks**.
2. Hover over a network resource and click the trash can icon (**Delete**).

> **Note**
>
> The trash can icon does not appear until you hover over the Network resource.



3. Click **Delete** to confirm.

   The Network resource is deleted from Secure Access and is removed from any policy rules.



15 Manage Internal Networks

Topics:

- Manage Internal Networks

Provides an overview of Manage Internal Networks in Cisco Secure Access China, including Add Internal Network Resources, Update an Internal Network Resource, and Delete an Internal Network Resource. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Internal Networks

Provides instructions for managing internal Networks in Cisco Secure Access China. A resource is an internet capable entity that is managed by your organization.

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 in Cisco Secure Access China. An Internal Network resource represents a private address space of IP addresses.

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 China.

To start protecting an internal network, add an Internal Network resource to Cisco Secure Access China. 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 China, 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 China Activity Search report.

Prerequisites

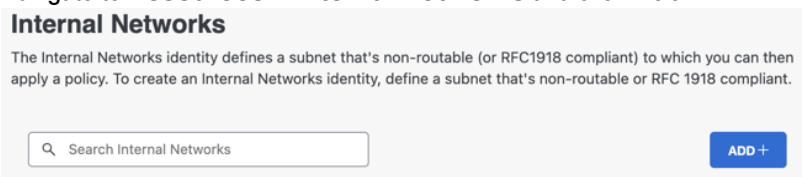
Lists the prerequisites for adding internal network resources, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

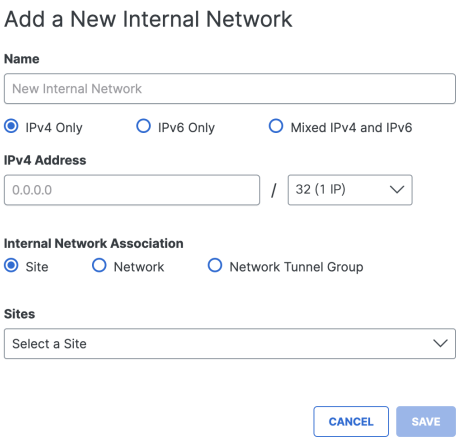
Procedure

Provides instructions for adding internal network resources. Navigate to Resources > Internal Networks and click Add. Give a descriptive internal network name for Name.

1. Navigate to **Resources > Internal Networks** and click **Add**.



2. Give a descriptive internal network name for **Name**.



3. Choose IP address version according to the IP address version defined in your network. Enter the IP address and choose the IP address range for the network in the respective fields..
4. For **Internal Network Association**, choose **Site**, **Network**, or **Network Tunnel Group**.
   a. Expand **Sites**, and then select the Site to associate with the Internal Network.
   b. Expand **Network**, and then select the Network resources to associate with the Internal Network resource. The **Network** radio button appears only when the **IPv4 Only** option is chosen.
   c. Expand **Network Tunnel Group**, and then select the Network Tunnel Groups to associate with the Internal Network resource. The **Network Tunnel Group** radio button appears for the **IPv4 Only** and **IPv6 Only** networks.
5. Click **Save**.

Update an Internal Network Resource

Provides instructions for updating an Internal Network Resource in Cisco Secure Access China. Once you add Internal Network resources to Cisco Secure Access, you can you can update the resource.

Once you add Internal Network resources to Cisco Secure Access, you can you can update the resource.

Prerequisites

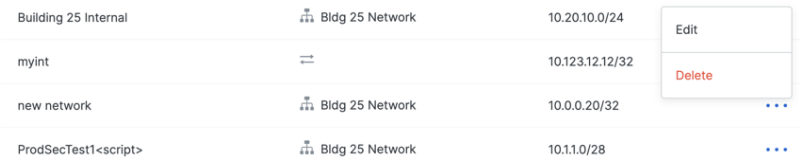
Lists the prerequisites for updating an internal network resource, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

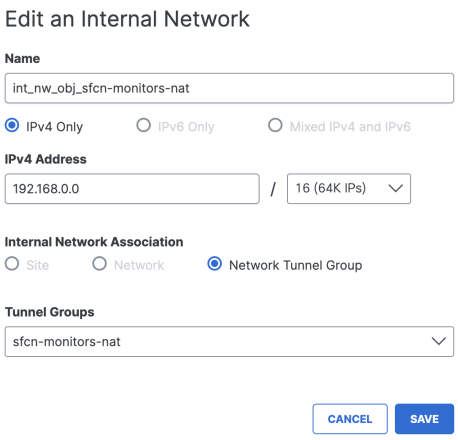
Procedure

Provides instructions for updating an internal network resource. Navigate to Resources > Internal Networks. For an Internal Network resource, click the ellipsis (…) and choose Edit to open the Internal Network resource.

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 in Cisco Secure Access China. Once you add Internal Network resources to Cisco Secure Access, you can remove an Internal Network resource from Secure Access.

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.

Prerequisites

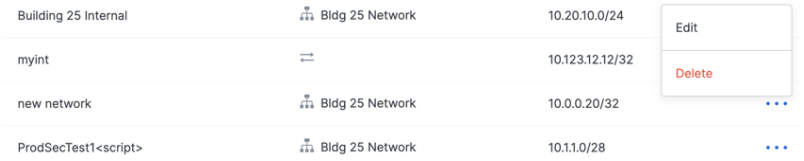
Lists the prerequisites for deleting an internal network resource, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for deleting an internal network resource. Navigate to Resources > Internal Networks. For an Internal Network resource, click the ellipsis (…) and choose Delete.

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.



16 Manage Destination Lists

Topics:

- Manage Destination Lists

Provides an overview of Manage Destination Lists in Cisco Secure Access China, including Add a Destination List, Upload Destinations From a File, and Edit a Destination List. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Destination Lists

Provides instructions for managing destination Lists in Cisco Secure Access China. A destination list is a collection of domains, URLs, IPv4 addresses, and CIDRs to which you want to apply the same internet access rules.

A destination list is a collection of domains, URLs, IPv4 addresses, and CIDRs to which you want to apply the same internet access rules.

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.

Add a Destination List

Provides instructions for adding a Destination List in Cisco Secure Access China. Cisco Secure Access China enables administrators to manage destinations grouped by destination lists.

Cisco Secure Access China 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.

Prerequisites

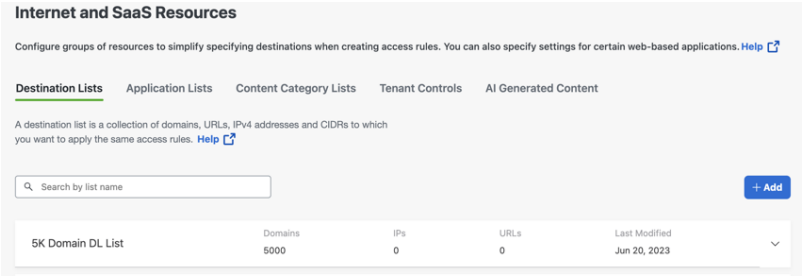
Lists the prerequisites for adding destination list. Full Admin role in Secure Access China. See Manage Accounts. For supported destination types and guidelines, see Manage Destination Lists.

- Full Admin role in Secure Access China. 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.

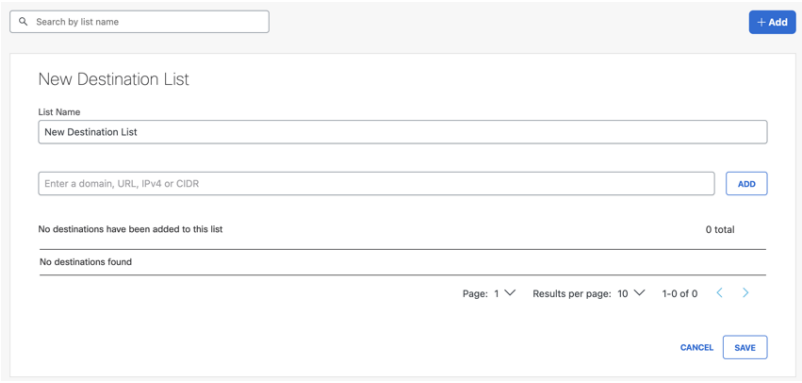
Procedure

Provides instructions for adding destination list. 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.

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 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 in Cisco Secure Access China. You can import destinations in bulk from a text file into an existing destination list.

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.

Prerequisites

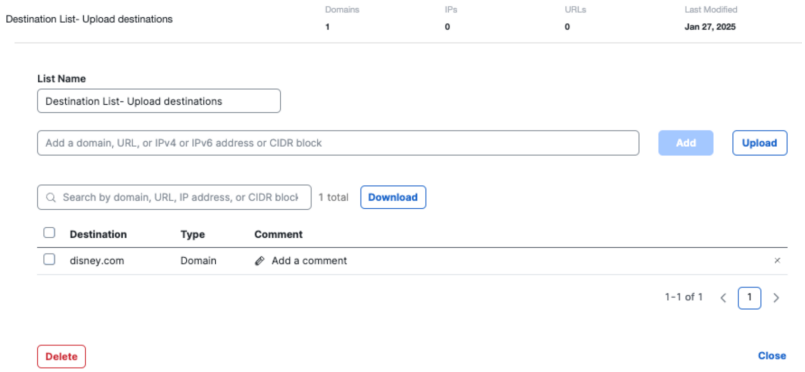
Lists the prerequisites for adding destinations in bulk. Full Admin role in Secure Access China. See Manage Accounts. For supported destination types and guidelines, see Manage Destination Lists.

- Full Admin role in Secure Access China. See Manage Accounts.
- For supported destination types and guidelines, see Manage Destination Lists.

Procedure

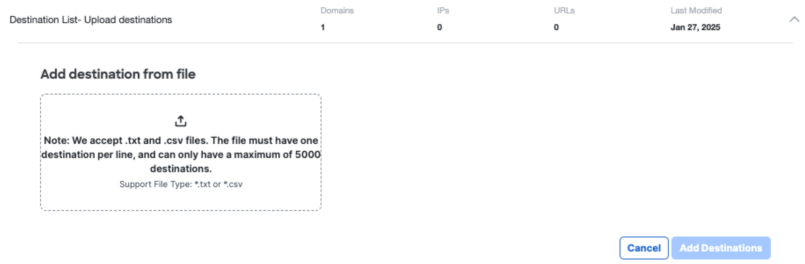
Provides instructions for adding destinations in bulk. The current uploader supports text and CSV files in the format of one destination per line. Excel files are not supported.

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 **Upload**.

   The current uploader supports text and CSV files in the format of one destination per line. Excel files are not supported.



5. Select or drag and drop a .txt file or csv file that contains your destinations.

   If you want to remove the file and choose a different file, click **Replace**.

6. Click **Add destinations**.

   Supported destinations in the file are added to your destination list.

   If your bulk upload includes unsupported destinations, the upload does not fail, but only supported destinations are added.

7. Immediately after uploading the destinations, look for a pop-up 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 in Cisco Secure Access China. A destination list can be edited at any time.

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.

Prerequisites

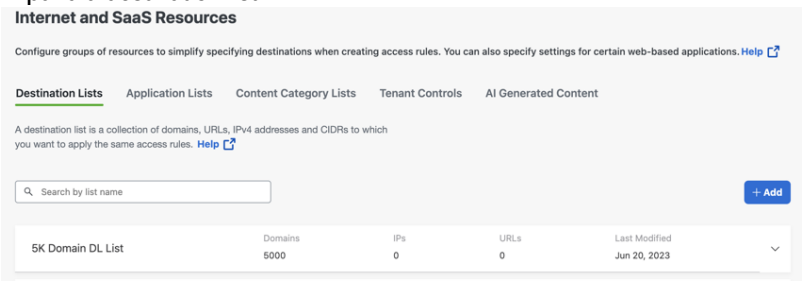
Lists the prerequisites for editing destination list, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

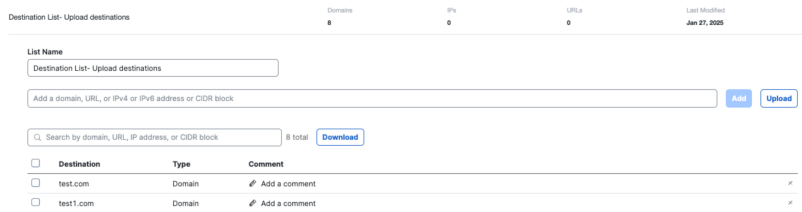
Provides instructions for editing destination list. You can upload destinations in bulk from a text or CSV file. For more information, see Upload Destinations from a File.

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists.**
2. Expand a destination list.



3. Make your changes.

> **Tip**
>
> You can upload destinations in bulk from a text or CSV file. For more information, see Upload Destinations from a File.



4. Click **Save**.

Download Destinations to a CSV File

Provides instructions for downloading destinations to a CSV File in Cisco Secure Access China. 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. Having a CSV file is useful for when you need to update destinations or to show others which destinations your are allowing and blocking without having to give others access to your Secure Access dashboard.

You can remove or add entries and then bulk upload it to the destination list. For more information, see Upload Destinations from a File.

Prerequisites

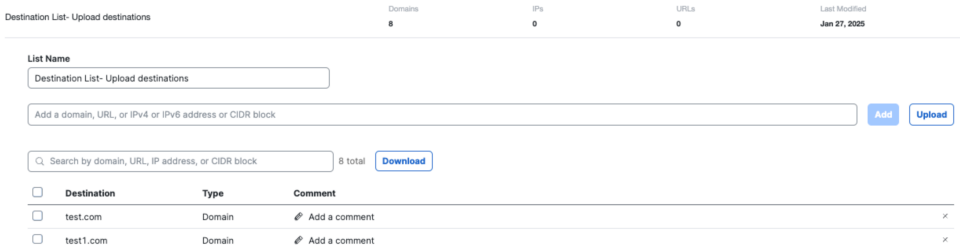
Lists the prerequisites for downloading destinations to csv file, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for downloading destinations to CSV file.

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.
2. Expand a destination list and click **Download**.



Control Access to Custom URLs

Describes Control Access to Custom URLs in Cisco Secure Access China. 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

Lists prerequisites for controlling access to custom URLs, including a root certificate for SSL decryption and protocol-agnostic destination list behavior for HTTP and HTTPS URLs.

- 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 blocking a url. To block a URL, you can add it to a blocked destination list or create a new blocked destination list for URLs.

To block a URL, you can add it to a blocked destination list or create a new blocked destination list for URLs.

To add a URL to an existing blocked destination list:

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.

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.

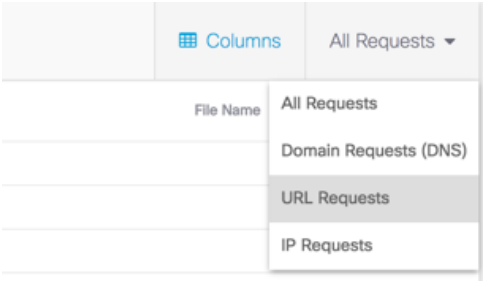
Also, check to see if you have a local–on-premise–proxy that is interfering.

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 for custom URLs.

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.opendns.com txt
```

Windows

```
nslookup proxy.opendnstest.com
```

```
nslookup -type=txt debug.opendns.com
```

Wildcards in Destination Lists

Describes Wildcards in Destination Lists in Cisco Secure Access China. Wildcards support top-level domains (TLDs) to allow broad allows or blocks for 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.

Note

Asterisks (*) are not supported.

Destination List Entry	Implied Wildcard
domain.com	*.domain.com/*
com	*.com/*
www.domain.com	*.[www.domain.com/\\]
	(http://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 Not Supported

Regular expressions in URL paths are not supported.

Add Punycode Domain Name to Destination List

Provides instructions for adding punycode Domain Name to Destination List in Cisco Secure Access China. 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?

Describes what is Punycode?. 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.

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

Describes examples of Unicode and Punycode Encoded Strings. Only one ASCII character. Only one emoji character. Only one Greek character.

Unicode	Punycode	Description
a	a-	Only one ASCII character.

Unicode	Punycode	Description
🙂	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.

Troubleshoot Destination Lists

Describes Troubleshoot Destination Lists in Cisco Secure Access China. When you add a malformed destination or unsupported type of destination to a destination list, you may encounter an error condition.

When you add a malformed destination or unsupported type of destination to a destination list, you may encounter an error condition. In most cases, Secure Access displays an error message that describes the reasons for the error condition.

Destination lists support the following destination types:

- Fully-qualified domain name (FQDN)
- IP address
- URL

For more information about destination lists, see Add a Destination List.

Destination Lists and Common Error Conditions

Action	Error Message	Additional Information
Added a URL to an allow list.	URLs in allow lists are not currently supported. Consider adding the domain only instead.	• Remove the URL and replace it with the domain for that URL.
Entered a destination that does not match the type and format expected by the destination list.	Invalid Domain, Invalid URL, Invalid IP	• Check the format and type of the destination that you added. • Enter the correct format of the destination.
Added a URL that has an error in the domain, path, or query.	Check to confirm that the URL was entered correctly.	• Secure Access requires that URLs follow RFC-3986 Uniform Resource Identifier (URI): Generic Syntax. • Check the characters in the URL. • Check the composition of the URL. • You can add a partial URL to leverage right-side wildcarding. For more information, see Control Access to Custom URLs.
Added a URL that is found in a high-volume domain list.	The URL belongs to a domain that does not present a security concern, but if proxied may impact Secure Access performance. Instead, consider adding only the domain.	• If you do not trust the destination, consider blocking the domain. • Generally, high-volume domains do not present a security risk and do not require additional inspection.

Action	Error Message	Additional Information
Added a destination that is found in the protected allow list.	The supplied destination matches the Secure Access global allow list and cannot be saved.	• Destinations in the protected allow list either host services other than HTTP or are critical to Secure Access operations. Secure Access only proxies services that use HTTP. • If the error occurs when you add a URL and you don't trust the destination, consider blocking the domain. • If you are not sure why the destination is considered protected, contact support.
Entered a URL that contains non-ASCII characters.	Invalid URL.	• Try percent-encoding the URL or block the domain.
Uploaded a list of destinations in which at least one of the URLs or domains contains an error.	There was an issue with one or more of the destinations in the uploaded list.	• A bulk upload error message. • Secure Access provides a link to the list of destinations that were not added from the uploaded destination list. • Correct or remove the destinations from your bulk upload list and try again. • Secure Access does not add destinations from an uploaded destination list unless all of the destinations are accepted.
Entered a destination that is not accepted by Secure Access.	Invalid destination.	• A generic error message. • Entered a destination that is not accepted by Secure Access. • You have encountered an error condition that is not categorized by Secure Access. We recommend that you contact Support.
Entered a destination that matches a destination in an existing destination list.	This destination already exists in the destination list.	• Secure Access does not add a destination that already appears in a destination list.

How to Format Your Destination List

Describes how to Format Your Destination List. Always enter domains in this format: domain.com Not: www.domain.com. Destination lists accept domain names that are encoded in Punycode. For more information, see Add Punycode Domain Name to Destination List.

Always enter domains in this format: `domain.com`Not: `www.domain.com`

Using the correct format ensures that `*.domain.com` is included in your destination list (a wildcard is implicit). However, if you only want to block **subdomain.domain.com**, you must be more specific when you define the entry.

Note

Destination lists accept domain names that are encoded in Punycode. For more information, see Add Punycode Domain Name to Destination List.

17 Manage AAA Servers

Topics:

- Manage AAA Servers

Provides an overview of Manage AAA Servers in Cisco Secure Access China. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage AAA Servers

Provides instructions for managing AAA Servers in Cisco Secure Access China. The authentication, authorization and accounting (AAA) server is a network server that is used for access control.

The authentication, authorization and accounting (AAA) server is a network server that is used for access control. Authentication identifies the user. Authorization implements policies that determine which resources and services an authenticated user may access. Accounting keeps track of time and data resources that are used for billing and analysis.

If you want to use an external AAA server, you must first create a AAA server group for the protocol that the external server uses, and add the server to the group. You can create more than one group per protocol, and separate groups for all protocols that you want to use. Each server group is specific to one type of server or service.

18 Manage Application Lists

Topics:

- Manage Application Lists

Provides an overview of Manage Application Lists in Cisco Secure Access China, including Add an Application List, Application Categories, and Delete an Application List. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Application Lists

Provides instructions for managing application Lists in Cisco Secure Access China. Secure Access organizes application-based resources into categories based on the type of processes or services provided, for example: shopping, education, or human resources.

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 in Cisco Secure Access China. Cisco Secure Access China application lists organize application-based destinations into categories based on the type of processes or services provided, for example: shopping, education, or human resources.

Cisco Secure Access China 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.

Prerequisites

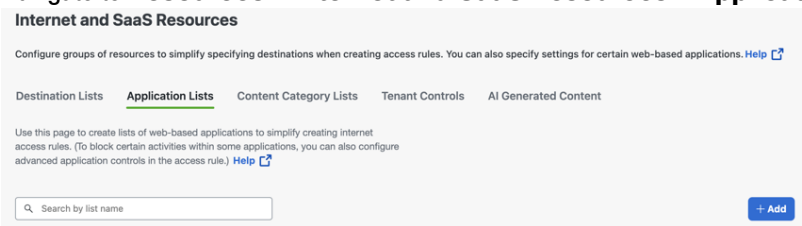
Lists the prerequisites for adding application list, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

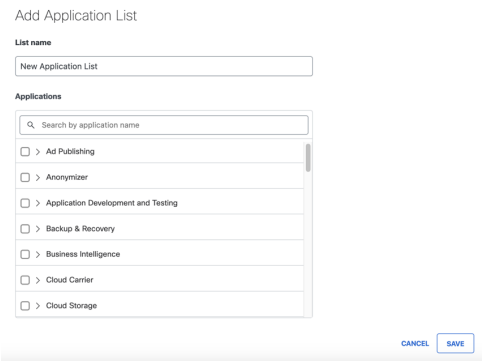
Procedure

Provides instructions for adding application list. This new Application list is now available as a destination when you add an internet access rule.

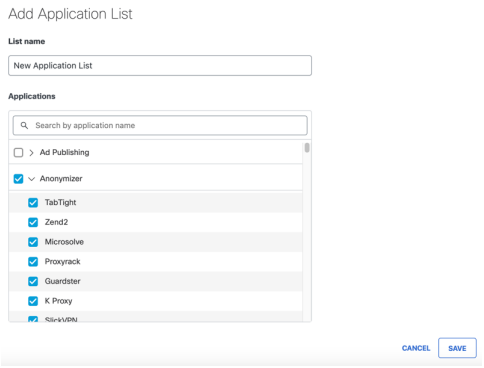
1. Navigate to **Resources** > **Internet and SaaS Resources** > **Application Lists** and click **Add**.



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 China 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**.

This new Application list is now available as a destination when you add an internet access rule.

(Optional) To allow access to an application but block uploading, downloading, posting, or sharing, configure the Advanced Application Controls section directly in an internet access rule. Not all applications support this feature. For details, see Advanced Application Controls.

Application Categories

Describes Application Categories in Cisco Secure Access China. The system is capable of discovering thousands of apps; these are divided into categories for ease of reference.

The system is capable of discovering thousands of apps; these are divided into categories for ease of reference. Categorization of discoverable apps is conducted by a team of researchers, and based on similarities among apps as well as a number of other quantitative application feature sets.

Category Descriptions

Describes category Descriptions. Discovered apps are assigned to the following categories:. 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.

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 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 Storage**–Applications that offer massively scalable storage capacity that can be used for applications, and file storage.
- **Collaboration**–Applications that enhance communication and collaboration in workgroups, within enterprises, and across enterprises.
- **Compute**–Fundamental computing resources for running cloud-based systems that can be dynamically provisioned and configured as needed.
- **Content Delivery Network (CDN)**–Applications that store content and files to improve the performance and cost of delivering content for web-based systems by offering a large distributed system of servers deployed in multiple data centers across the Internet.
- **Content Management**–Applications for managing the production of and access to content, enforcing document production workflows, and providing workspaces for groups or enterprises to find and access documents.
- **Customer Relationship Management (CRM)**–Applications that manage interactions with current and future customers, including organization and automation across sales, marketing, and customer service functions.
- **Database Management**–Applications offering scalable data management solutions for structured or unstructured data, relational database solutions or scalable non-SQL datastores.
- **E-Commerce**–Applications that facilitate the buying and selling of products or services.
- **Education**–Applications that provide educational or training courses, general learning opportunities or specific employee training independent of their location.
- **Enterprise Resource Planning (ERP)**–Applications that manage operations or management of a business; which can include internal and external resources, including tangible assets, financial resources, materials, and human resources.
- **Financial Services**–Applications for managing financial processes and information.
- **Games**–Online and mobile games.
- **Generative AI**–Applications that enable access to large language models (LLM) and artificial intelligence (AI) tools.
- **Healthcare**–Applications that provide access to health, medical, and personal fitness systems.
- **Hosting Services**–Applications that enable corporate or individual websites or other content to be accessible over the internet.
- **Human Resources**–Applications for managing human resources and HR functions.
- **IT Service Management**–Applications that support specific IT functions to plan, deliver, operate and control IT services.

- **Legal**–Applications that provide access to legal documents and public records and support legal content.
- **Marketing & Sales**–Applications that are specifically designed for marketing and sales functions.
- **Media**–Applications that host or stream media as a service.
- **Office Productivity**–Applications for producing information and other standard office-oriented tasks such as documentation, presentations, project management, and so on.
- **Others**–Used for those services where no existing categorization would fit.
- **P2P**–Peer to Peer torrents like apps and protocols.
- **Search**–Web or app-based search.
- **Security**–Applications that support security activities to ensure adherence to regulatory compliance rules and protect information, data applications, and infrastructure.
- **Service Management**–Applications that support general operational activities outside of the IT function.
- **Shopping**–Web or app-based basic online shopping.
- **Social Networking**–Applications that establish and maintain a connection among users that are tied in one or more specific types of interdependency.
- **Software Repository**–Software repositories.
- **Support**–Applications that provide access to customer support services.
- **Travel**–Applications that provide travel management services.
- **Web Content**–Mostly app-based services that provide content. It can be through a login or paid portal.
- **Website**–An online platform accessible via web browsers that provides information, services, or functionalities to users, often requiring a URL for access.

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 in Cisco Secure Access China. After you create an application list, you can delete the list from Secure Access.

After you create an application list, you can delete the list from Secure Access.

Prerequisites

Lists the prerequisites for deleting application list, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for deleting application list. Navigate to Resources > Internet and SaaS Resources > Application Lists. Expand an application list, and then click Delete.

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.

19 Manage Content Category Lists

Topics:

- Manage Content Category Lists

Provides an overview of Manage Content Category Lists in Cisco Secure Access China, including Available Content Categories, Add a Content Category List, and Request a Category for an Uncategorized Destination. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Content Category Lists

Provides instructions for managing content Category Lists in Cisco Secure Access China. Secure Access classifies internet destinations using content-based categories.

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 in Cisco Secure Access China. You can use the following content categories as destinations in internet access rules.

You can use the following content categories as destinations in internet access rules. Web sites that Cisco Talos classifies as belonging to a category destination are handled by the rule.

- **Adult**–Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers), general information about sex, non-pornographic in nature, genital piercing, adult products or greeting cards, information about sex not in the context of health or disease.
- **Advertisements**–Banner and pop-up advertisements that often accompany a web page, other advertising websites that provide advertisement content. Advertising services and sales are classified as Business and Industry.
- **Alcohol**–Alcohol as a pleasurable activity, beer and wine making, cocktail recipes, liquor sellers, wineries, vineyards, breweries, alcohol distributors. Alcohol addiction is classified as Health and Medicine. Bars and restaurants are classified as Dining and Drinking.
- **Animals and Pets**–Information about domestic animals, livestock, service animals, pets and their care. Veterinary services, medicines, and animal health. Pet and animal training, aquariums, zoos, and animal shows. Includes animal shelters, humane societies, animal centric charities, and sanctuaries, bee keeping, training, and animal husbandry; dinosaurs and extinct animals.
- **Arts**–Galleries and exhibitions, artists and art, photography, literature and books, performing arts and theater, musicals, ballet, design, architecture. Cinema and television are classified as Entertainment.
- **Astrology**–Astrology, horoscope, fortune telling, numerology, psychic advice, tarot.
- **Auctions**–Online and offline auctions, auction houses, and classified advertisements.
- **Business and Industry**–Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital, office supplies, industrial equipment (process equipment), machines and mechanical systems, heating equipment, cooling equipment, materials handling equipment, packaging equipment, manufacturing: solids handling, metal fabrication, construction and building, passenger transportation, commerce, industrial design, construction, building materials, shipping and freight (freight services, trucking, freight forwarders, truckload carriers, freight and transportation brokers, expedited services, load and freight matching, track and trace, rail shipping, ocean shipping, road feeder services, moving and storage).
- **Cannabis**–Websites that focus on the recreational and medicinal consumption of cannabis. Sites may include marketing, discussions about legal and regulatory issues, growth and production, paraphernalia, research, and investment in the cannabis industry. Dispensaries, cannabinoid (CBD oil, THC, etc.) based products are also included.
- **Chat and Instant Messaging**–Web-based instant messaging and chat rooms.
- **Cheating and Plagiarism**–Promoting cheating and selling written work, such as term papers, for plagiarism.
- **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.
- **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 Sites (Germany)**–URLs that are restricted in Germany due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Sites (Great Britain)**–URLs that are restricted in Great Britain due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Sites (Italy)**–URLs that are restricted in Italy due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Sites (Poland)**–URLs that are restricted in Poland due to content which may be unlawful as determined by the regional government.
- **Religion**–Religious content, information about religions, religious communities.
- **SaaS and B2B**–Web portals for online business services.
- **Safe for Kids**–Directed at, and specifically approved for, young children.
- **Science and Technology**–Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar subjects, space exploration, meteorology, geography, energy (fossil, nuclear, renewable), communications (telephones, telecommunications).
- **Search Engines and Portals**–Search engines and other initial points of access to information on the Internet.
- **Sex Education**–Factual websites dealing with sex, sexual health, contraception, pregnancy.
- **Shopping**–Bartering, online purchasing, coupons and free offers, general office supplies, online catalogs, online malls.
- **Social Networking**–Social networking. See also Professional Networking.
- **Social Science**–Sciences and history related to society, archaeology, anthropology, cultural studies, history, linguistics, geography, philosophy, psychology, women's studies.
- **Society and Culture**–Family and relationships, ethnicity, social organizations, genealogy, seniors, child-care.
- **Software Updates**–Websites that host updates for software packages.

- **Sports and Recreation**–All sports, professional and amateur, recreational activities, fishing, fantasy sports, public parks, amusement parks, water parks, theme parks, spas.
- **Streaming Audio**–Real-time streaming audio content including Internet radio and audio feeds.
- **Streaming Video**–Real-time streaming video including Internet television, web casts, and video sharing.
- **Terrorism and Violent Extremism**–Terrorist or extremist websites that promote death or violence as part of their ideology. Sites may contain graphic or disturbing images, videos, and text. Some sites may not advocate terrorism but share first-hand material of a violent nature.
- **Tobacco**–Pro-tobacco websites, tobacco manufacturers, pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as Health and Medicine.
- **Transportation**–Personal transportation, information about cars and motorcycles, shopping for new and used cars and motorcycles, car clubs, boats, airplanes, recreational vehicles (RVs), and other similar items. Note, car and motorcycle racing is classified as Sports and Recreation.
- **Travel**–Business and personal travel, travel information, travel resources, travel agents, vacation packages, cruises, lodging and accommodation, travel transportation, flight booking, airfares, car rental, vacation homes.
- **Uncategorized**–Any site (domain, URL, or IP address) that has not been categorized–that does not match a security or content category–is blocked. Note that Cisco Talos does not categorize IP addresses as content, only domains, and URLs. IP addresses found to be malicious are placed into a relevant security category. If a URL does not resolve to a content category, Umbrella looks for the URL's domain for a category. If the domain is not categorized then Umbrella treats the URL as uncategorized.

  Note

  Use caution when enabling this category as it will match any domain or URL that has not been categorized by Cisco Talos. This may have unintended results, blocking access to sites not meant to be blocked. Before enabling this setting, we recommend that you first monitor your "Uncategorized" traffic through the Activity Search report. This will help you determine what type of impact that enabling the Uncategorized content category will have on your organization. For more information about monitoring uncategorised traffic, see Activity Search Report.

- **URL Shortener**–Domains used to shorten long URLs, brand URLs, or may obscure the final destination of a hyperlink.
- **Weapons**–Information relating to the purchase or use of conventional weapons such as gun sellers, gun auctions, gun classified ads, gun accessories, gun shows, and gun training, general information about guns, other weapons may be included. Government military websites are classified as Military.
- **Web Cache and Archives**–Cached or archived web content often stored for preservation or to decrease load times.
- **Web Hosting**–Website hosting, bandwidth services.
- **Web Page Translation**–Translation of web pages between languages.
- **Web-based Email**–Public web-based email services. Websites enabling individuals to access their company or organizations email service are classified as Organizational Email.

To make a request to categorize an uncategorized destination:

1. Log into talosintellgence.com with your cisco.com credentials.
2. Click **My Account** .
3. Submit a request to recategorize the domain.

Add a Content Category List

Provides instructions for adding a Content Category List in Cisco Secure Access China. Content category lists allow you to speed rule creation and apply rules consistently to groups of categories.

Content category lists allow you to speed rule creation and apply rules consistently to groups of categories.

Prerequisites

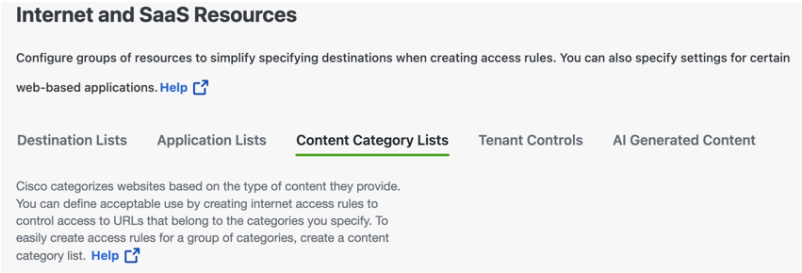
Lists the prerequisites for adding content category list, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

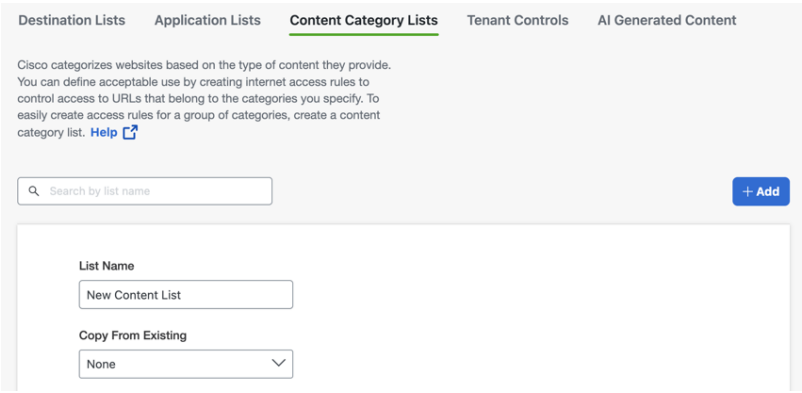
Procedure

Provides instructions for adding content category list. The new Content Category list is now available as a destination in internet access rules.

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

Describes Request a Category for an Uncategorized Destination in Cisco Secure Access China. You can contact your sales representative to request categorization of an uncategorized destination.

You can contact your sales representative to request categorization of an uncategorized destination.

Dispute a Content Category

Describes Dispute a Content Category in Cisco Secure Access China. Secure Access uses the content categories that are maintained by Technical Assistance Center (TAC).

Secure Access uses the content categories that are maintained by Technical Assistance Center (TAC). If you disagree with a destination's content-category classification, you can dispute it by contacting your sales representative.

View Content Categories in Reports

Provides instructions for viewing content Categories in Reports in Cisco Secure Access China. You can view information about content categories, such as requests that Secure Access China blocked because of content categories.

You can view information about content categories, such as requests that Secure Access China blocked because of content categories.

Prerequisites

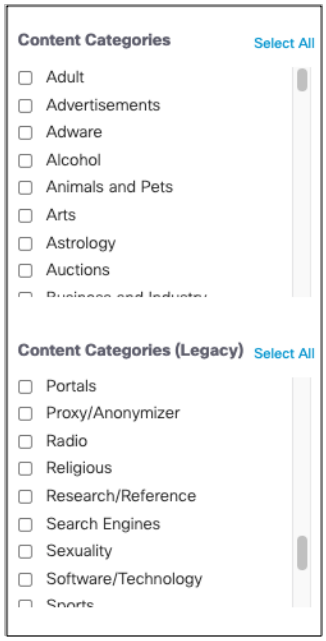
Lists the prerequisites for viewing content categories in reports. A minimum user role of Read-only. For more information, see Manage Accounts.

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

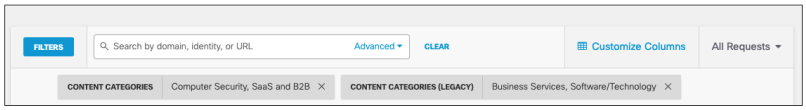
View Content Categories in Activity Search Report

Provides instructions for viewing content categories in activity search report. Your filtered categories appear at the top of the report.

1. Navigate to **Monitor > Activity Search**.
2. Scroll down to Content Categories and select your desired filters.



Your filtered categories appear at the top of the report.



The Categories column of the report displays both legacy and new Talos content categories.

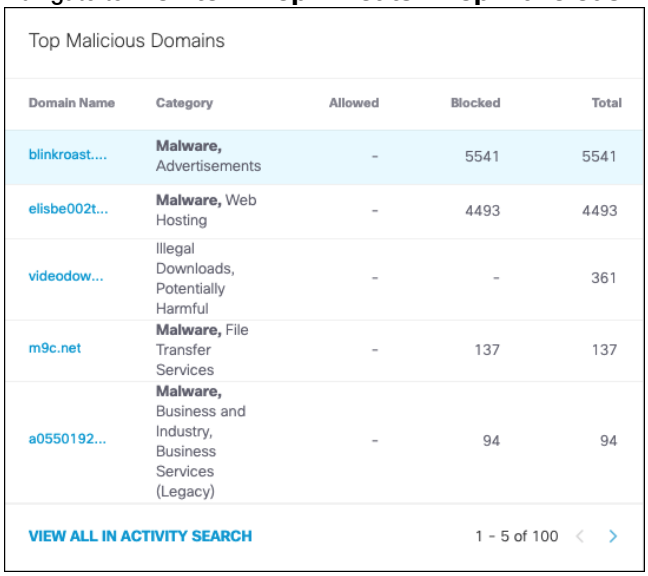


Categories
Software/Technology (Legacy), Business Services (Legacy), Computer Security, SaaS and B2B
Software/Technology (Legacy), Business Services (Legacy), Computer Security, SaaS and B2B
Software/Technology (Legacy), Business Services (Legacy), Computer Security, SaaS and B2B
Software/Technology (Legacy), Business Services (Legacy), Computer Security, SaaS and B2B
Software/Technology (Legacy), Cloud and Data Centers
Software/Technology (Legacy), Cloud and Data Centers
Software/Technology (Legacy), SaaS and B2B
Software/Technology (Legacy), Computers and Internet
Software/Technology (Legacy), Computers and Internet
Software/Technology (Legacy), SaaS and B2B

View Content Categories in Top Threats Report

Provides instructions for viewing content categories in top threats report. Navigate to Monitor > Top Threats > Top Malicious Domains.

1. Navigate to **Monitor > Top Threats > Top Malicious Domains**.



Top Malicious Domains

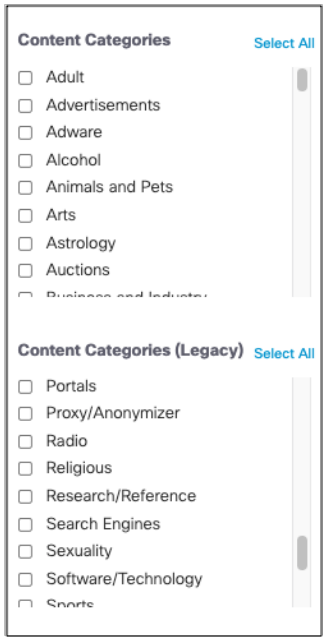
Domain Name	Category	Allowed	Blocked	Total
blinkroast....	**Malware,** Advertisements	-	5541	5541
elisbe002t...	**Malware,** Web Hosting	-	4493	4493
videodow...	Illegal Downloads, Potentially Harmful	-	-	361
m9c.net	**Malware,** File Transfer Services	-	137	137
a0550192...	**Malware,** Business and Industry, Business Services (Legacy)	-	94	94

VIEW ALL IN ACTIVITY SEARCH 1 - 5 of 100

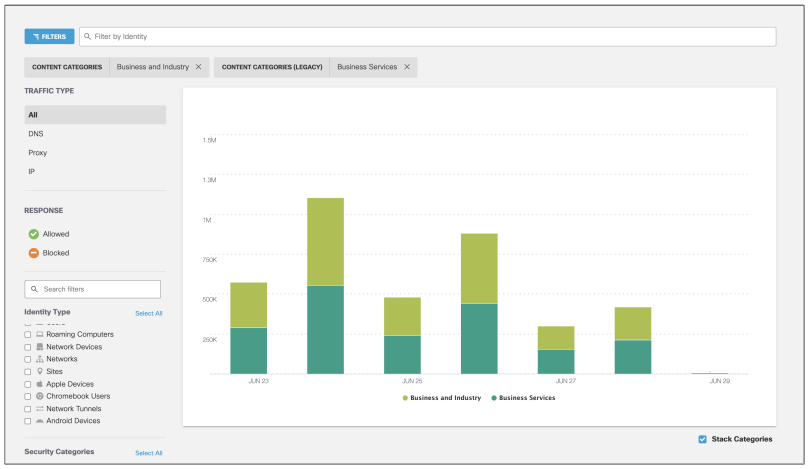
View Content Categories in Total Requests Report

Provides instructions for viewing content categories in total requests report. The graph displays data for the selected Talos content categories.

1. Navigate to **Monitor > Additional Reports > Total Requests**.
2. Filter by content categories. Click **Apply**.



The graph displays data for the selected Talos content categories.

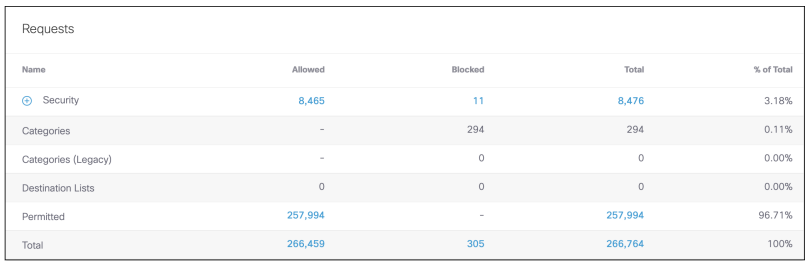


View Content Categories in Activity Volume Report

Provides instructions for viewing content categories in activity volume report. The table displays data for both the Talos content categories.

1. Navigate to **Monitor > Additional Reports > Activity Volume**.

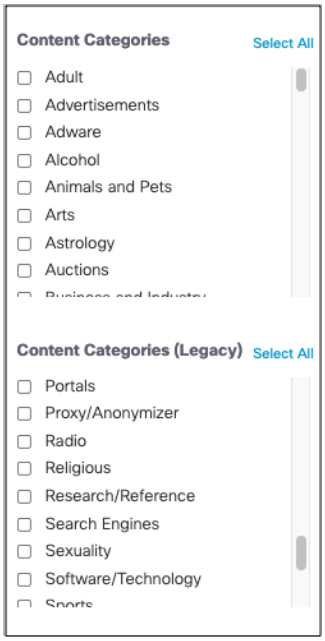
   The table displays data for both the Talos content categories.



View Content Categories in Top Destinations Report

Provides instructions for viewing content categories in top destinations report. The category column of the report displays the Talos content categories.

1. Navigate to **Monitor > Top Destinations**.
2. Filter by content categories.



The category column of the report displays the Talos content categories.

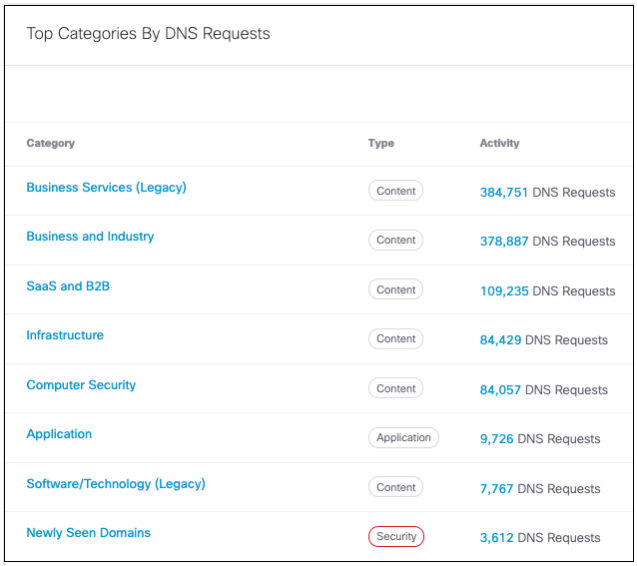


View Content Categories in Top Categories Report

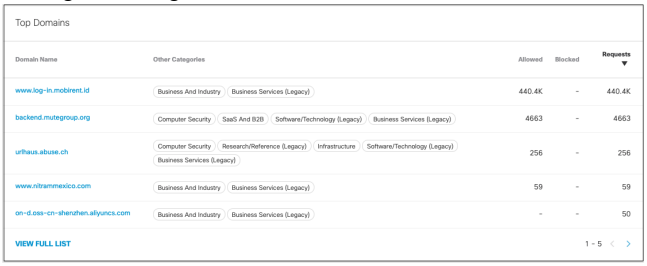
Provides instructions for viewing content categories in top categories report. The category column of the report displays the Talos content categories.

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.



20 Manage Tenant Control Profiles

Topics:

- Manage Tenant Control Profiles

Provides an overview of Manage Tenant Control Profiles in Cisco Secure Access China, including Add a Tenant Controls Profile, Control Cloud Access to Dropbox, and Control Cloud Access to Google G Suite. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Tenant Control Profiles

Provides instructions for managing tenant Control Profiles in Cisco Secure Access China. Secure Access tenant controls allow you to provision connectivity for users to certain SaaS applications in the cloud.

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 in Cisco Secure Access China, including Prerequisites and Procedure. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access tenant controls allow you to provision connectivity for users to the following SaaS applications and suites in the cloud:

- Dropbox
- Google G Suite
- Microsoft 365
- 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.

Prerequisites

Lists the prerequisites for adding tenant controls profile. The following data is required to configure tenant controls and allow access to cloud-based applications and suites:.

- 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:

- **Dropbox–Tenant Name** and **Team ID**.
- **Google G Suite–Domains**. Scroll to "Use a web proxy server to block accounts" in G Suite Admin Help.
- **Microsoft 365–Tenant Domain** and **Tenant Directory ID**. See also, Azure Active Directory documentation.
- **Slack–Workspace ID**. For more information, see Approve Slack workspaces for your network.

For more information, see the application's documentation or contact the application's Support.

Procedure

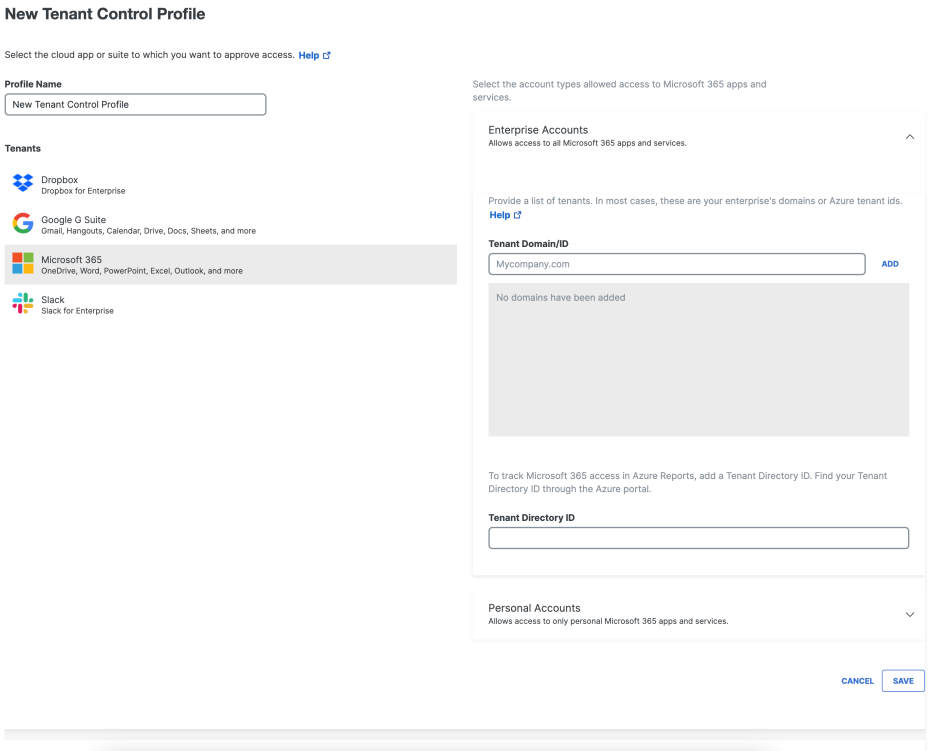
Provides instructions for adding tenant controls profile. Dropbox – Tenant Name and Team ID. Microsoft 365 – Tenant Domain and, optionally, Tenant Directory ID . See also, Azure Active Directory documentation.

1. Navigate to **Resources > Internet and SaaS Resources**.

2. Click **Tenant Controls**.
3. Click the default **Global Tenant Controls** profile.
   a. Alternatively, click **Add.**



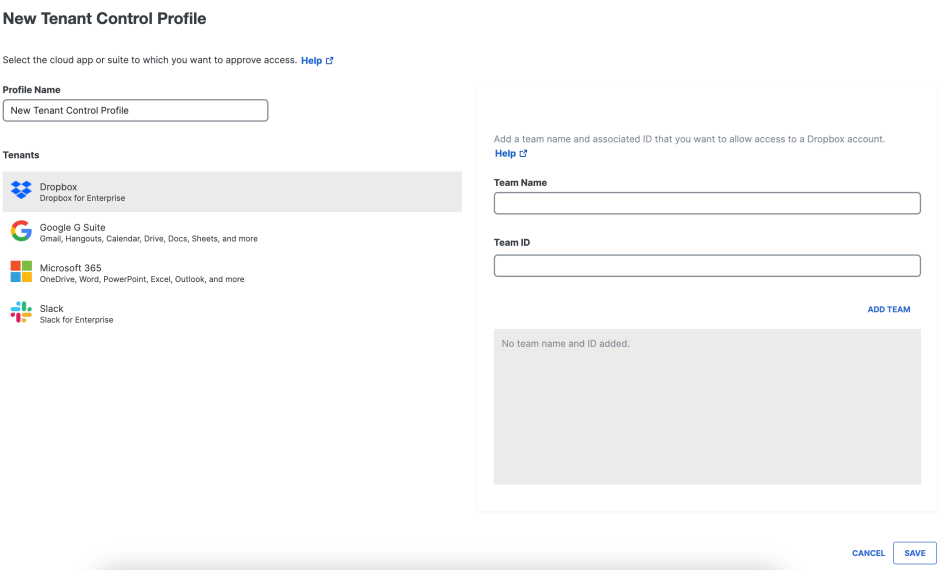
4. Give your configuration a descriptive **Profile Name.**
5. Select a tenant.



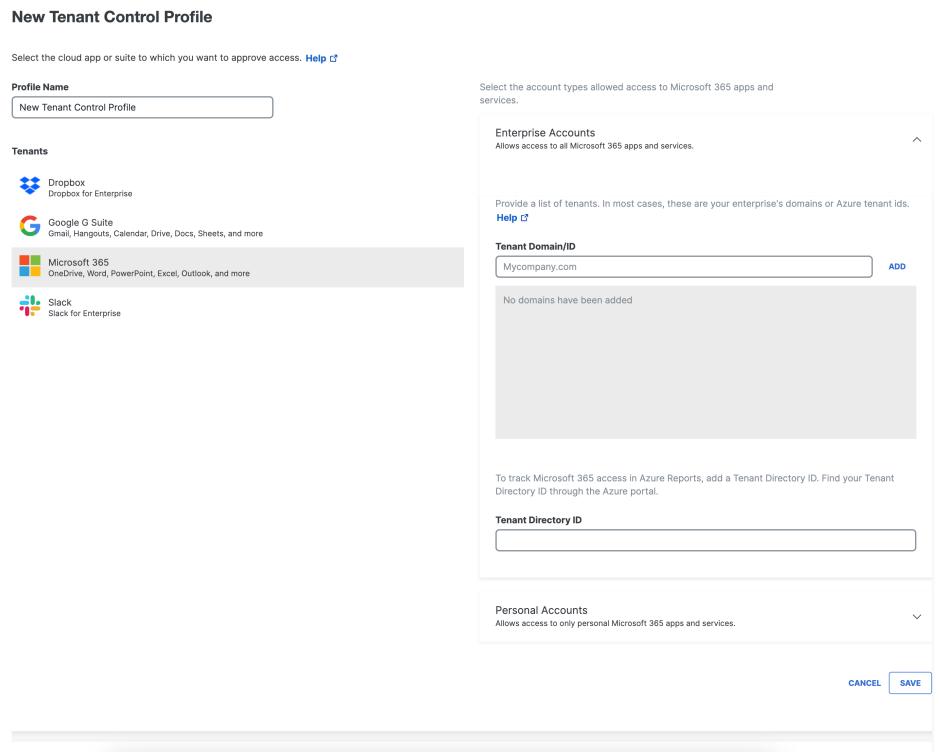
6. In the right pane, add specific data and domain information to grant access to those tenants from within your organization.

> **Note**
>
> If you aren't sure what information to enter for a tenant, see the application's documentation or contact the application's Support.

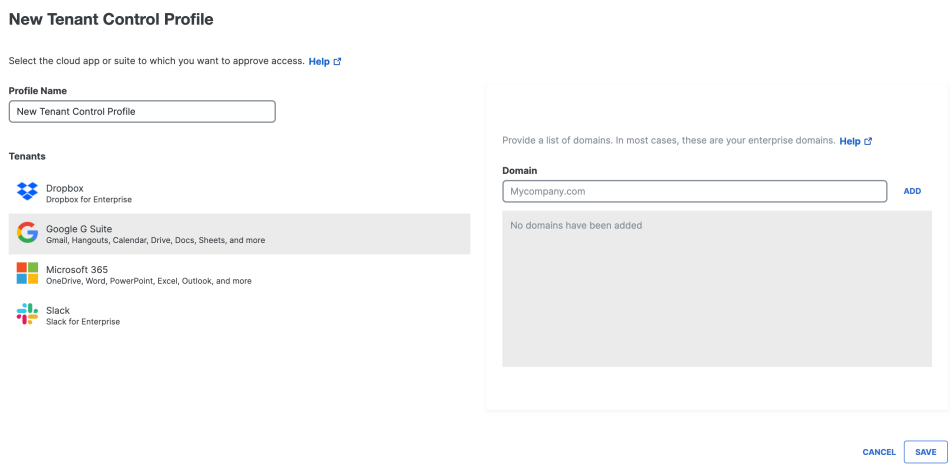
- **Dropbox–Tenant Name** and **Team ID**.



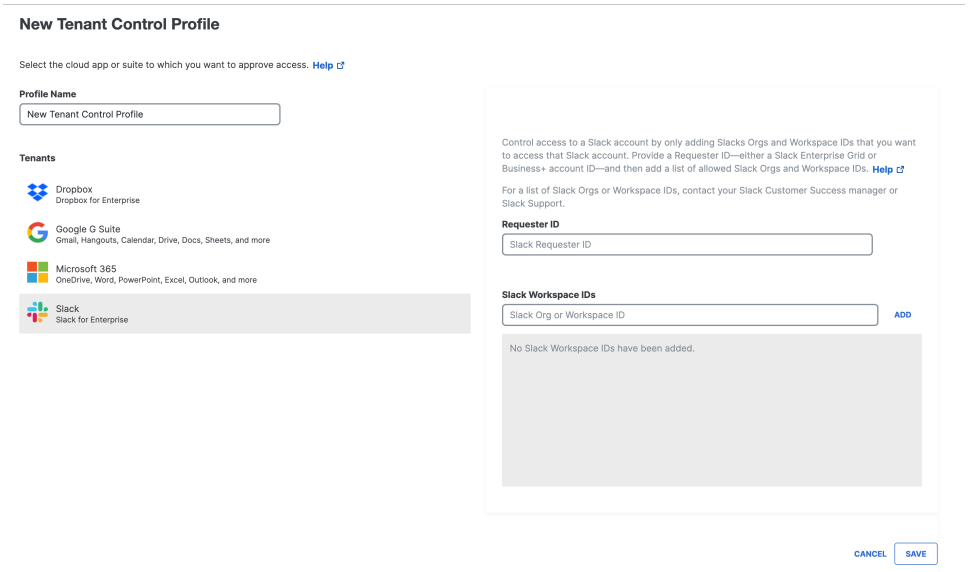
- **Microsoft 365–Tenant Domain** and, optionally, **Tenant Directory ID**. See also, Azure Active Directory documentation.



- **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.



7. After you've configured access to applications, click **Save**.

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 Dropbox

Describes Control Cloud Access to Dropbox in Cisco Secure Access China. The Secure Access tenant controls profile manages access to the cloud-based application Slack.

The Secure Access tenant controls profile manages access to the cloud-based application Slack.

Prerequisites

Lists the prerequisites for control cloud access dropbox. Dropbox requires the following data to configure tenant controls for access to the cloud-based application:.

Dropbox requires the following data to configure tenant controls for access to the cloud-based application:

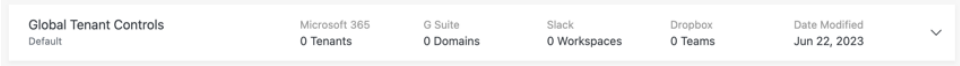
- **Tenant Name**
- **Team ID**

Procedure

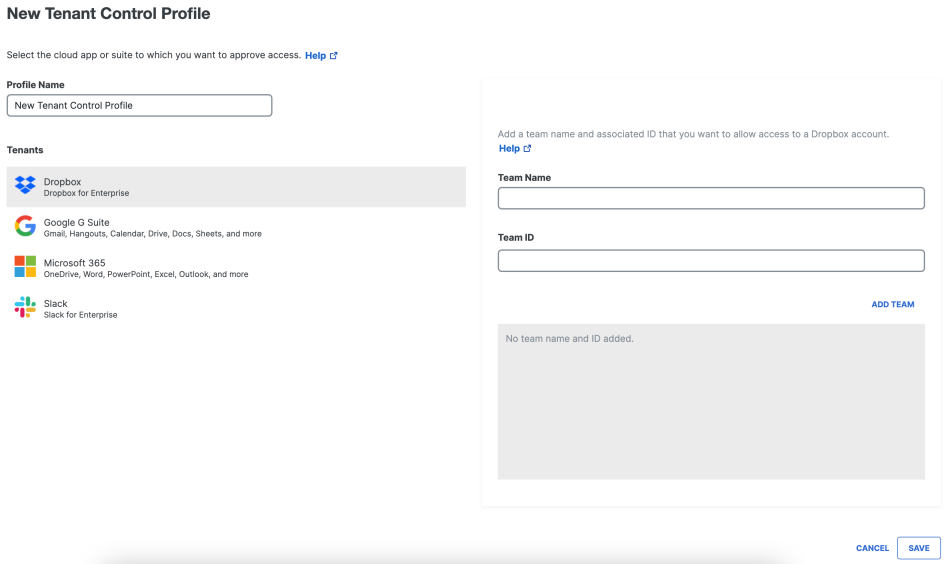
Provides instructions for control cloud access dropbox. The new Tenant Controls profile is now available when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

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 **Tenant Name** and a **Team ID**.



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 Google G Suite

Describes Control Cloud Access to Google G Suite in Cisco Secure Access China. The Secure Access tenant controls profile manages access to the cloud-based application Google G Suite.

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.

Prerequisites

Lists the prerequisites for control cloud access google gsuite. 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:.

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

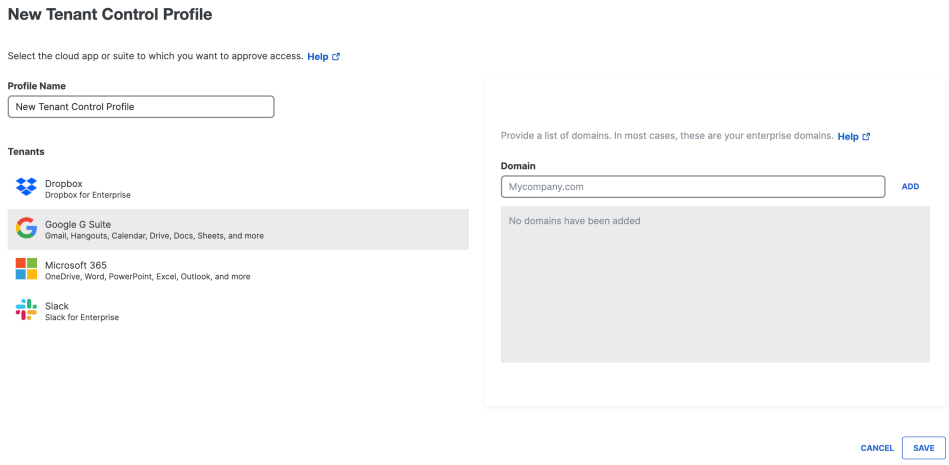
Provides instructions for control cloud access google gsuite. This new Tenant Controls setting is now available for selection when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

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 Microsoft 365

Describes Control Cloud Access to Microsoft 365 in Cisco Secure Access China. Use a tenant-control profile to manage access to the cloud-based application Microsoft 365.

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.

Prerequisites

Lists the prerequisites for control cloud access microsoft 365. Microsoft 365 requires the following data to configure tenant controls for access to the cloud-based application:.

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

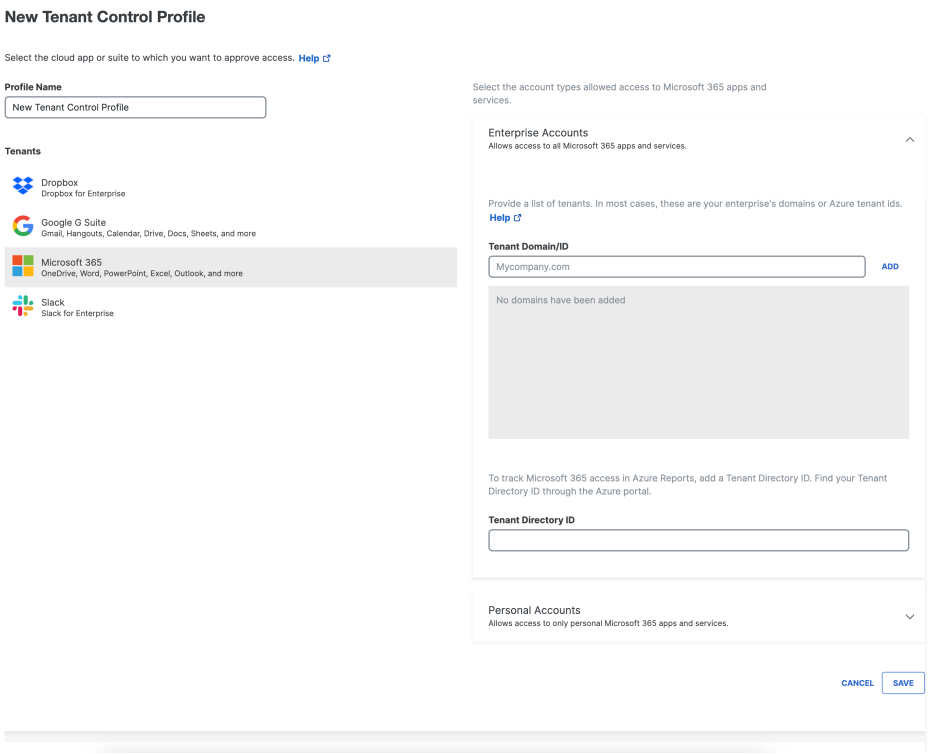
Provides instructions for control cloud access microsoft 365. This ID is used to track Office 365 access in Azure Reports.

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**.

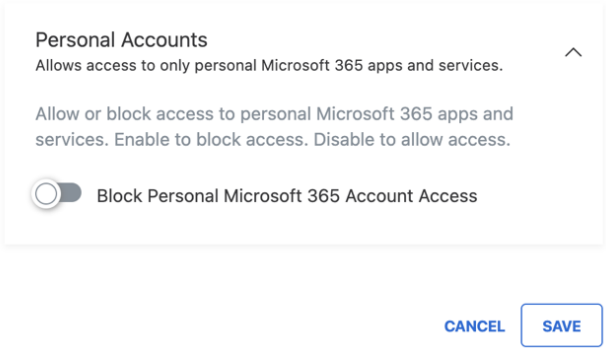
> **Note**
>
> You can add multiple Tenant Domains.

   b. Optionally, add your organization's **Tenant Directory ID** for Microsoft 365.

      This ID is used to track Office 365 access in Azure Reports.

> **Note**
>
> For more information about how to acquire the Tenant Directory ID, see Microsoft's documentation or contact Microsoft Support.

6. Optionally, expand **Personal Accounts** and click the toggle to block access to Personal Microsoft 365 accounts.



7. Click **Save**.

   Result: 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 Slack

Describes Control Cloud Access to Slack in Cisco Secure Access China. The Secure Access tenant controls profile manages access to the cloud-based application Slack.

The Secure Access tenant controls profile manages access to the cloud-based application Slack.

Prerequisites

Lists the prerequisites for control cloud access slack. Slack requires the following data to configure tenant controls for access to the cloud-based application:.

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.

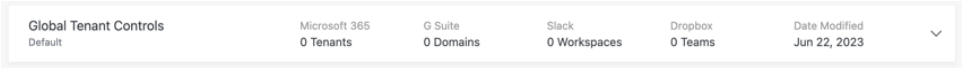
Procedure

Provides instructions for control cloud access slack. 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.

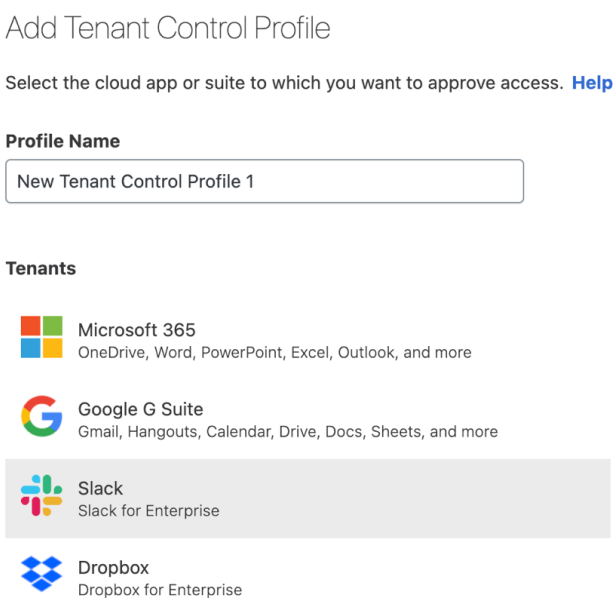
1. Navigate to **Resources > Internet and SaaS Resources.**
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

   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.

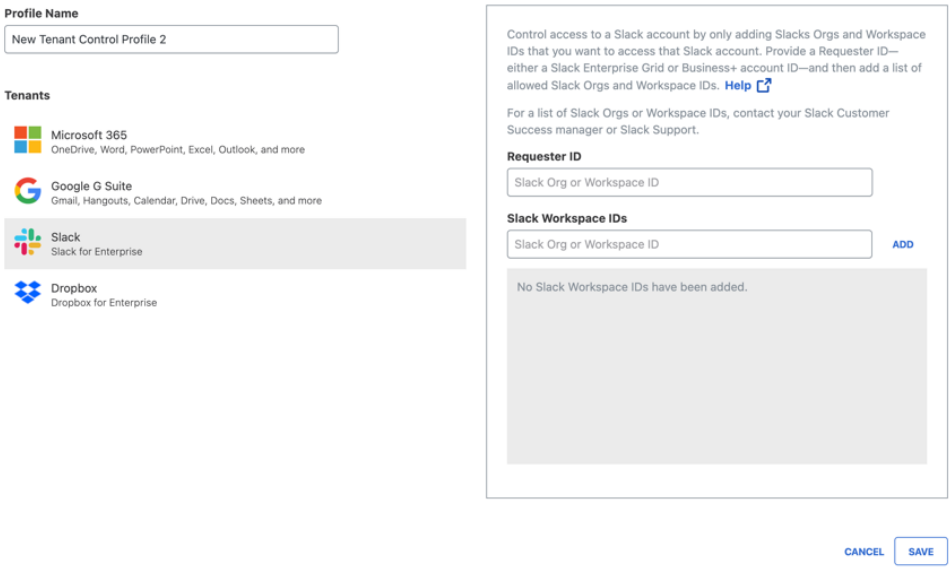


4. Give your configuration a descriptive **Profile Name** and select **Slack**.



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.

Use Tenant Controls in Access Rules

Describes Use Tenant Controls in Access Rules in Cisco Secure Access China. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

To use tenant controls in internet-access rules:

- Add tenant control profiles for the applications that require such controls.
- Decryption must be enabled for the rule. Make sure it is enabled in the web profile selected in the rule.
- The option to select a tenant control profile appears in the Security Controls section of the rule (after you choose destinations and then click Next.)

- If you enable Microsoft 365 Compatibility in Global Settings:

  Microsoft 365 Compatibility is compatible with Tenant Controls. However, when Tenant Controls are configured for Microsoft 365, Secure Access decrypts three Microsoft login domains (login.microsoftonline.com, login.microsoft.com, and login.windows.net) for the purpose of tenant enforcement. The domain is detected by analyzing the SNI (Server Name Indication) TLS extension. Some applications may not send SNI information in which case the exclusion does not apply.

  For more information about Microsoft 365 Compatibility, see Global Settings for Access Rules.

Review Tenant Controls Through Reports

Describes Review Tenant Controls Through Reports in Cisco Secure Access China. 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.

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.

Prerequisites

Lists prerequisites for reviewing tenant controls, including a minimum Read-only role and the account role details in Manage Accounts. for administrators to review.

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

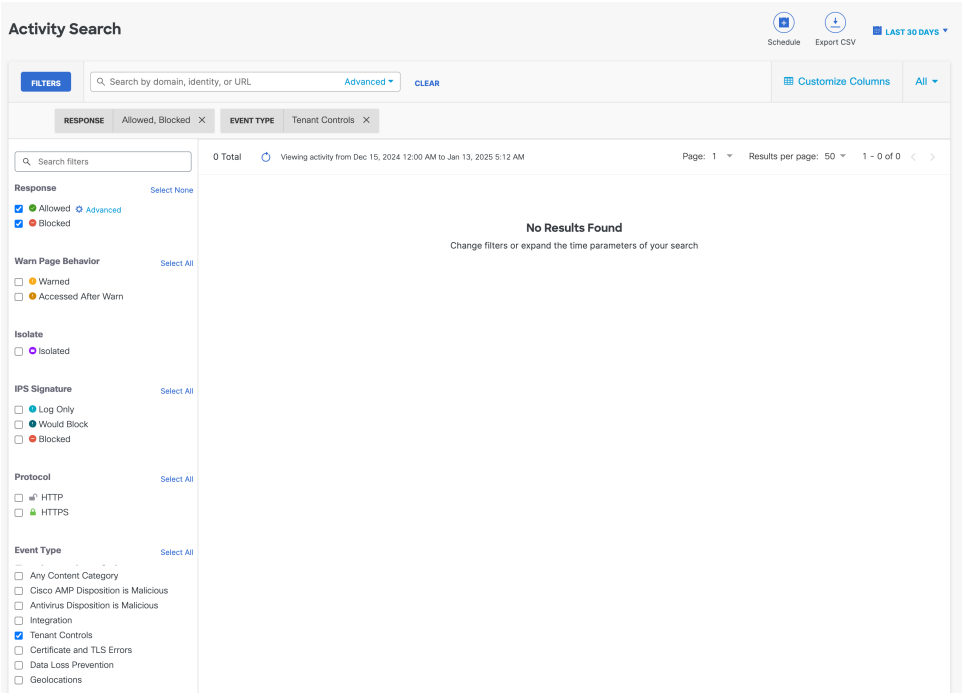
Procedure

Provides instructions for reviewing tenant controls. Since the blocking of tenants occurs at the vendor level, Secure Access displays tenant controls as Allowed in Activity Search.

1. Navigate to **Monitor > Activity Search**.
2. In the **Response** filter, select **Allowed** or **Blocked**.



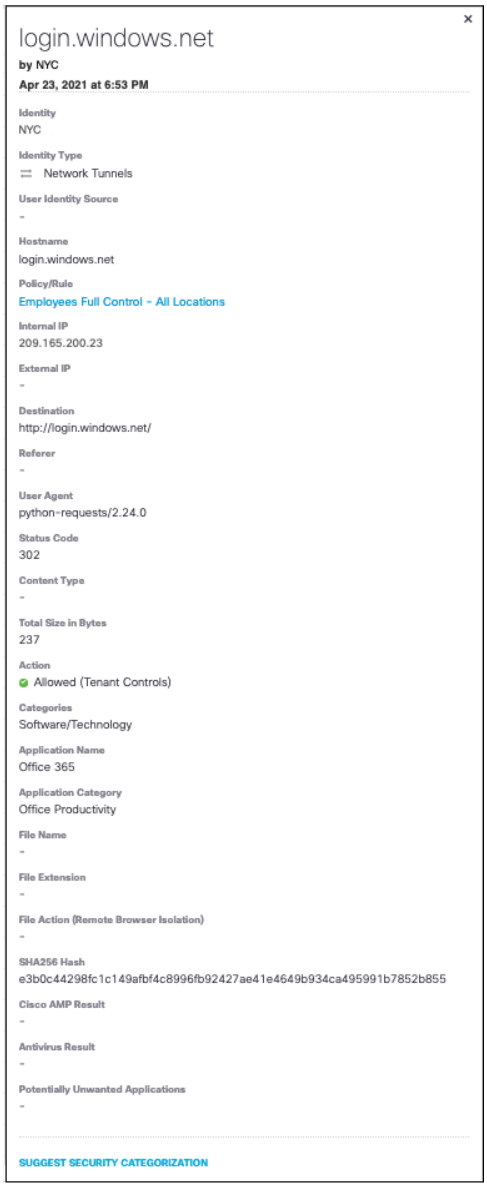
3. Under **Event Type**, select **Tenant Controls**.



Note

Since the blocking of tenants occurs at the vendor level, Secure Access displays tenant controls as Allowed in Activity Search.

4. To access detailed information about a tenant-control event, from the Action menu, choose **View Further Details**.


login.windows.net
by NYC
Apr 23, 2021 at 6:53 PM
Identity
NYC
Identity Type
Network Tunnels
User Identity Source
-
Hostname
login.windows.net
Policy/Rule
Employees Full Control - All Locations
Internal IP
209.165.200.23
External IP
-
Destination
http://login.windows.net/
Referer
-
User Agent
python-requests/2.24.0
Status Code
302
Content Type
-
Total Size in Bytes
237
Action
Allowed (Tenant Controls)
Categories
Software/Technology
Application Name
Office 365
Application Category
Office Productivity
File Name
-
File Extension
-
File Action (Remote Browser Isolation)
-
SHA256 Hash
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Cisco AMP Result
-
Antivirus Result
-
Potentially Unwanted Applications
-
SUGGEST SECURITY CATEGORIZATION

21 Manage Network Devices

Topics:

- Manage Network Devices

Provides an overview of Manage Network Devices in Cisco Secure Access China, including How to Add a Network Device in Secure Access and Procedure for Managing Network Devices. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Network Devices

Describes Manage Network Devices in Cisco Secure Access China. In Cisco Secure Access, you can add a hardware or virtual network device—for example, a router, switch, access point, or firewall—that routes DNS traffic to Secure Access's recursive DNS servers.

In Cisco Secure Access, you can add a hardware or virtual network device—for example, a router, switch, access point, or firewall—that routes DNS traffic to Secure Access's recursive DNS servers. Some network devices may also:

- Encrypt DNS traffic.
- Add internal IP addresses to DNS requests.
- Enable a policy for traffic by network segment or service set identifier (SSID).

After you add the network device in Secure Access, you can select the network device as a source component on the internet access rules in the Access policy. For more information, see Add an Internet Access Rule. You can also view the properties of a network device, and edit or remove the device in Secure Access.

> **Note**
>
> You can only deploy a network device when the device is on-network. You may deploy a network device as an alternative to a Secure Access Virtual Appliance (VA).

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Add the network device in Secure Access. For more information, see How to Add a Network Device in Secure Access.

How to Add a Network Device in Secure Access

Provides instructions for adding a Network Device in Secure Access. Create a Secure Access API key with the Deployments Network Devices key scope.

Procedure

1. Create a Secure Access API key with the **Deployments** > **Network Devices** key scope. For more information, see Manage API Keys.
2. Before you register the network device in Secure Access, add your username and password or Secure Access Network Devices API key and secret to the device.
3. On the device, use the Cisco Secure Access Network Devices API to add the network device in Secure Access. For more information, see Secure Access Network Devices API.

Procedure for Managing Network Devices

Describes Procedure for Managing Network Devices in Cisco Secure Access China. After you add a network device in Secure Access, you can view the properties of the device and edit or remove the device.

After you add a network device in Secure Access, you can view the properties of the device and edit or remove the device.

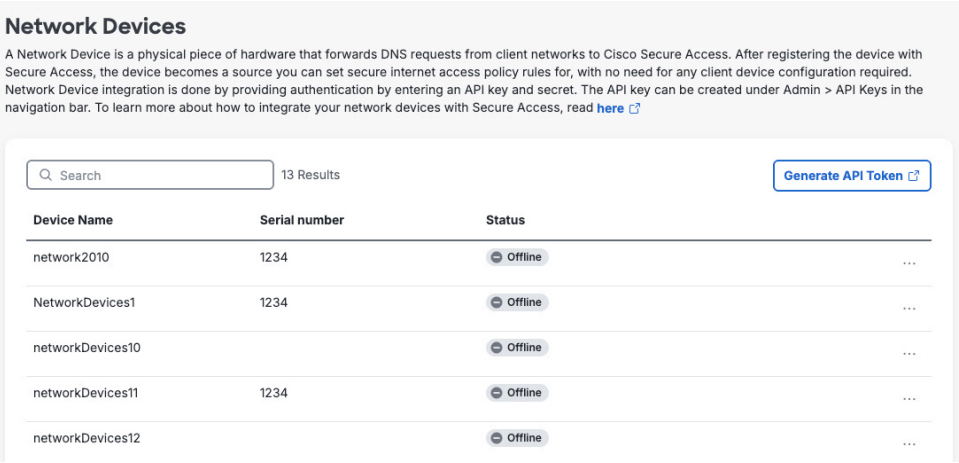
- View the Network Devices in Secure Access
- Edit a Network Device
- Remove a Network Device

View the Network Devices in Secure Access

Provides instructions for viewing the Network Devices in Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Network Devices**.
2. Navigate to a network device. The properties of the network device are:
   - **Device Name**–The name of the network device.
   - **Serial number**–The serial number of the network device.
   - **Status**–The status of the network device: **Online** or **Offline**.

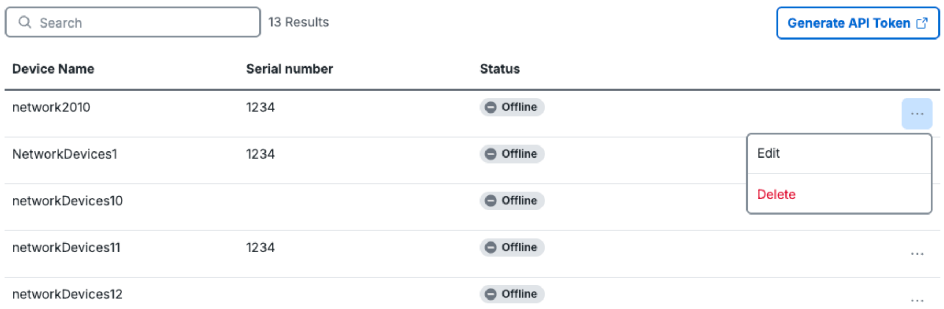


Edit a Network Device

Provides instructions for editing a Network Device in Cisco Secure Access China. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Network Devices**.
2. Navigate to a network device, click on the ellipsis (**...**), and then choose **Edit**.



3. For **Device Name**, enter a descriptive name for the network device. The device's name must be unique for all network devices in the organization.



4. Click **Update**.

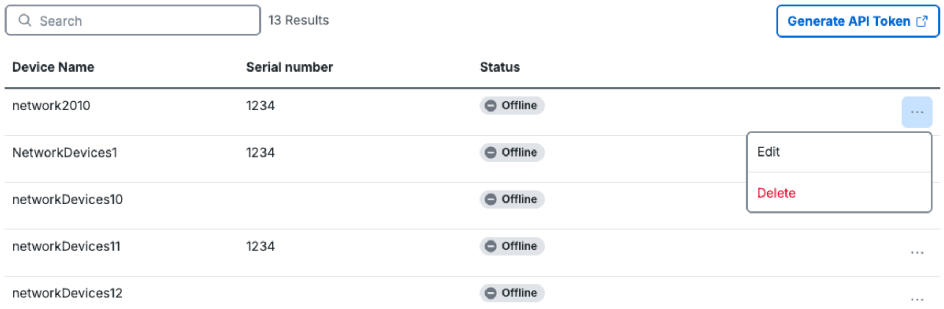
Remove a Network Device

Provides instructions for removing a Network Device in Cisco Secure Access China. It explains the sequence of actions and relevant settings presented in the procedure.

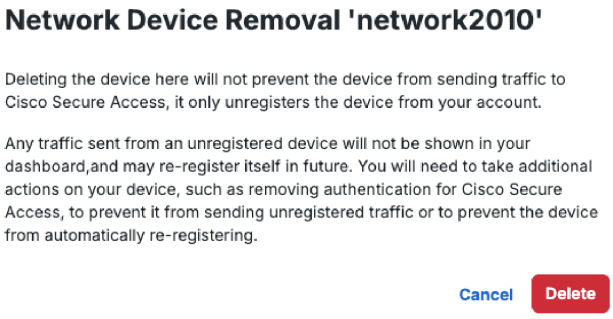
Deleting a network device in Secure Access does not prevent the device from sending traffic to Secure Access. To remove a network device fully, remove the authentication (username and password or API token) from the device first. If you are decommissioning the device, take the device offline. Otherwise, even if it is deleted in Secure Access, the device reappears when the network device sends additional traffic.

Procedure

1. Navigate to **Resources** > **Network Devices**.
2. Navigate to a network device, click on the ellipsis (**...**), and then choose **Delete**.



3. Click **Delete** to confirm the removal of the network device.



22 Manage Roaming Devices

Topics:

- Manage Roaming Devices

Provides an overview of Manage Roaming Devices in Cisco Secure Access China, including View Internet Security Settings for Roaming Devices, Edit Internet Security Settings for Roaming Devices, and Delete a Roaming Device. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Roaming Devices

Provides instructions for managing roaming Devices in Cisco Secure Access China. Cisco Secure Access Roaming Devices represent user devices that have deployed the Cisco Secure Client with the Umbrella Roaming Security module.

Cisco Secure Access Roaming Devices represent user devices that have deployed the Cisco Secure Client with the Umbrella Roaming Security module. The Cisco Secure Client syncs with Secure Access China to manage the Web security on the device. As part of the sync, a Roaming Device resource is added to Secure Access China. 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 China, 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

Provides instructions for viewing internet Security Settings for Roaming Devices in Cisco Secure Access China. A Roaming Device resource represents a user device that has deployed the Cisco Security Client with the Umbrella Roaming Security module.

A Roaming Device resource represents a user device that has deployed the Cisco Security Client with the Umbrella Roaming Security module.

The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices. The Umbrella Roaming Security module includes:

- Web security

Once deployed, the Cisco Secure Client registers the user device with Secure Access China. Cisco Secure Access China adds the device to the list of Roaming Device resources managed by the organization. Cisco Secure Client syncs with Secure Access China periodically and the device's web traffic is protected by the organization's policy rules. As an administrator, you can override, enable, or disable the internet security settings for the roaming devices in the organization.

Prerequisites

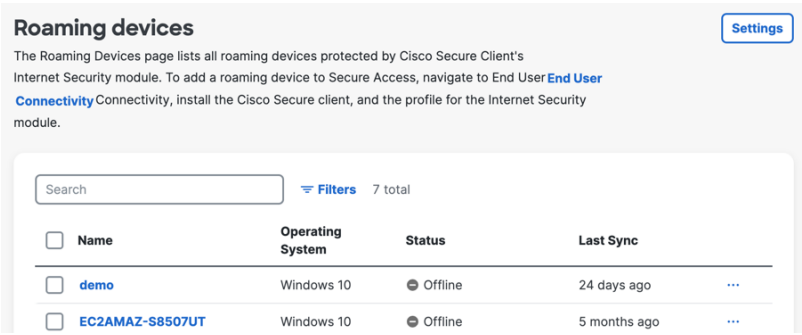
Lists the prerequisites for viewing roaming device internet security settings. Full Admin user role. For more information, see Manage Accounts.

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

Procedure

Provides instructions for viewing roaming device internet security settings. Navigate to Resources > Roaming Devices. Click a device name to open the Roaming Device resource.

1. Navigate to **Resources > Roaming Devices**.
2. Click a device name to open the Roaming Device resource.

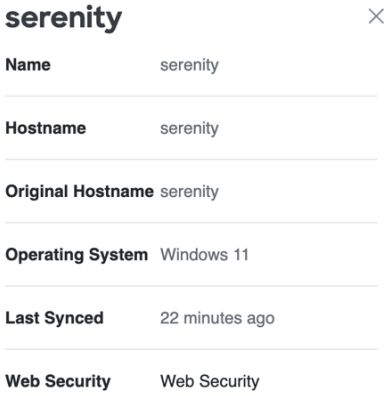


3. The Roaming Device resource displays the device's internet security details.

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
- **Last Synced**–last date when Cisco Secure Client received a sync from Secure Access China
- **Web Security**–specifies whether Cisco Secure Client has internet security deployed



Security Information – IPv4

Describes security Information - IPv4. Status –specifies whether the device is protected by Secure Access internet security. Last Active Policy –specifies the name of the last active Secure Access policy.

- **Status**–specifies whether the device is protected by Secure Access internet security.
- **Last Active Policy**–specifies the name of the last active Secure Access policy.



Edit Internet Security Settings for Roaming Devices

Provides instructions for editing internet Security Settings for Roaming Devices in Cisco Secure Access China. The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices.

The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices. The Umbrella Roaming Security module includes:

- Web security

You must activate the Secure Web Gateway (SWG) internet security settings in your instance of Secure Access China.

Secure Access China has various options to configure the Internet Security settings on Roaming Devices:

- Always enable the Secure Web Gateway settings for all Roaming Devices

- Always Override the Secure Web Gateway settings for all Roaming Devices
- Use the Secure Web Gateway settings in the default policy rule

Prerequisites

Lists the prerequisites for editing roaming devices internet security settings. Full Admin role in Secure Access China. For more information, see Manage Accounts.

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

Procedure

Provides instructions for editing roaming devices internet security settings. You can override the internet security settings globally or disable the Cisco Secure Client Umbrella Roaming Security module on individual Roaming Devices.

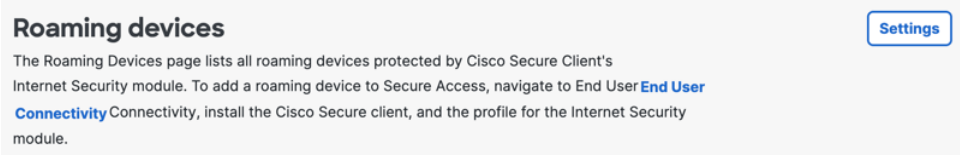
You can override the internet security settings globally or disable the Cisco Secure Client Umbrella Roaming Security module on individual Roaming Devices. Unless configured, all devices follow the global settings for internet security in the Cisco Secure Client Umbrella Roaming Security module settings.

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 China internet security is disabled globally, the devices that are enabled through the override remain enabled.

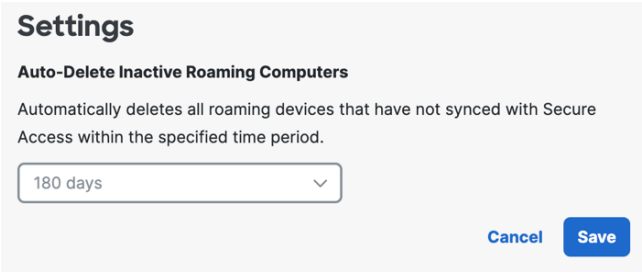
Edit the Auto-Delete Interval for Roaming Devices

Provides instructions for editing the auto-delete interval for roaming devices. The time intervals to sync roaming devices with Secure Access China are:.

1. Navigate to **Resources** > **Roaming Devices**.
2. Click **Settings** to set the auto-delete interval setting.

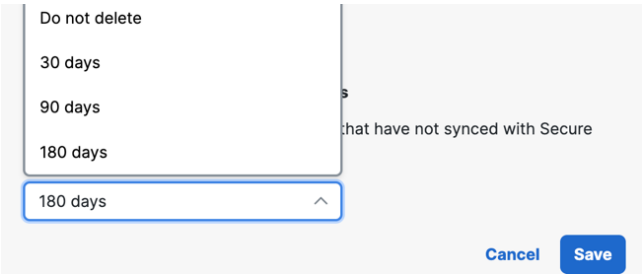


3. From the dropdown, choose **Do not delete** or the time period that the roaming devices must sync with Secure Access China before the devices are deleted from the organization, and then click **Save**.



The time intervals to sync roaming devices with Secure Access China 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 China in 30 days.
- **90 days**–delete the Roaming Devices in the organization if the devices have not synced with Secure Access China in 90 days.
- **180 days**–delete the Roaming Devices in the organization if the devices have not synced with Secure Access China in 180 days.



Disable the Internet Security Settings

Provides instructions for disabling the internet security settings. 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.

1. Navigate to **Resources > Roaming Devices**.
2. Select the devices to disable the SWG setting.
3. From the **Action** menu, select **Disable SWG**.

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. 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.

1. Navigate to **Resources > Roaming Computers**.
2. Select the devices for which you want to enable the SWG module. You can select up to 100 devices at a time on the page.
3. From the **Action** menu, select **Enable SWG**.

> **Note**
>
> The Action menu does not appear until you select a device.

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. Select the checkbox at the top of the column to select all devices on the page.

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.

1. Navigate to **Resources > Roaming Computers**.
2. Select the devices for which you want to remove the SWG override. You can select up to 100 devices at a time on the page.

> **Note**
>
> Select the checkbox at the top of the column to select all devices on the page.

3. From the **Action** menu, select **Follow Global Settings**. You can select up to 100 devices at a time on the page.

Delete a Roaming Device

Provides instructions for deleting a Roaming Device in Cisco Secure Access China. An administrator can delete a Roaming Device resource in Secure Access.

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.

Prerequisites

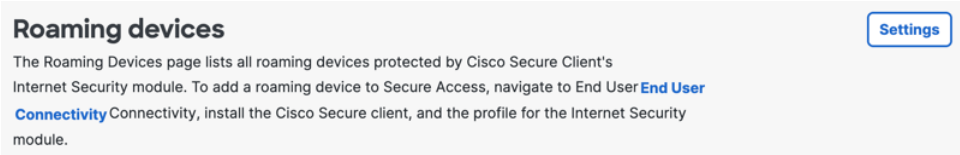
Lists the prerequisites for deleting a roaming device, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for deleting a roaming device. Navigate to Resources > Roaming Devices. Click the ellipsis (...) to open the action menu, and then click Delete.

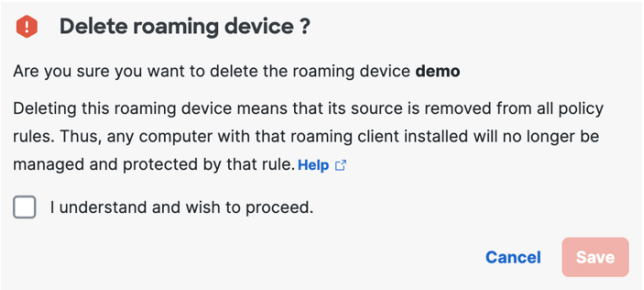
1. Navigate to **Resources** > **Roaming Devices**.



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**.



23 Manage Private Resources

Topics:

- Manage Private Resources

Provides an overview of Manage Private Resources in Cisco Secure Access China, including Add a Private Resource and Add a Private Resource Group. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Private Resources

Provides instructions for managing private Resources in Cisco Secure Access China. You can configure and add private resources to your organization.

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

Add a Private Resource

Provides instructions for adding a Private Resource in Cisco Secure Access China, including Prerequisites and Procedure. It explains the sequence of actions and relevant settings presented in the procedure.

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.

Prerequisites

Lists the prerequisites for adding private resources. Full Admin user role. For more information, see Manage Accounts. Gather IP or CIDR addresses for your private resources.

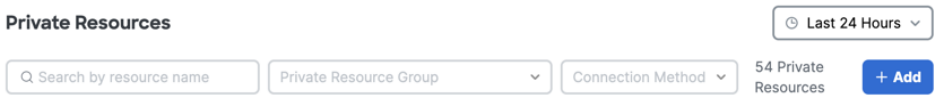
- Full Admin user role. For more information, see Manage Accounts.
- Gather IP or CIDR addresses for your private resources.
- If you will specify resource addresses using domain names (FQDNs), you must add at least one internal DNS server that can route traffic to your resource. For more information, 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.
- Plan your private resource configurations to avoid configuration conflicts such as duplicate or overlapping addresses.

Procedure

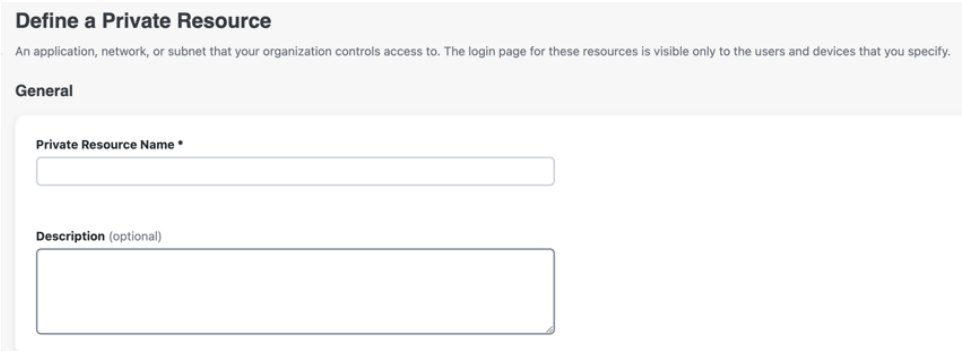
Provides instructions for adding private resources. Configure a resource controlled by your organization. For Internally Reachable Address , enter an IP address, FQDN, wildcard FQDN (in the format *.example.com), protocol, and port or port ranges.

Configure a resource controlled by your organization.

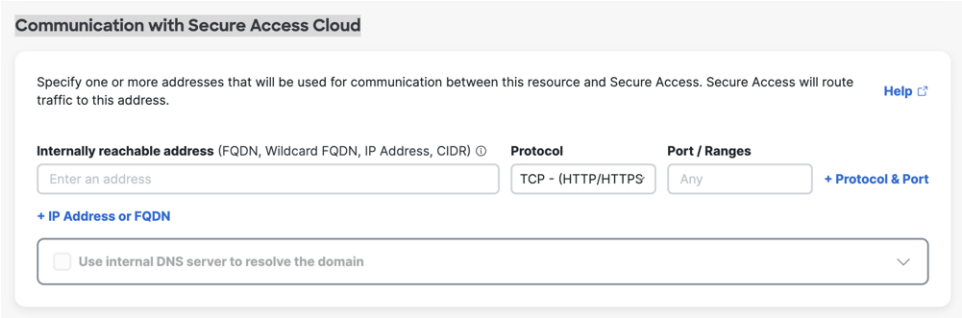
1. Navigate to **Resources** > **Private Resources** , choose **Private Resources**, and then click **+Add**.



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 **Communication with Secure Access Cloud**.



For **Internally Reachable Address**, enter an IP address, FQDN, wildcard FQDN (in the format *.example.com), protocol, and port or port ranges.

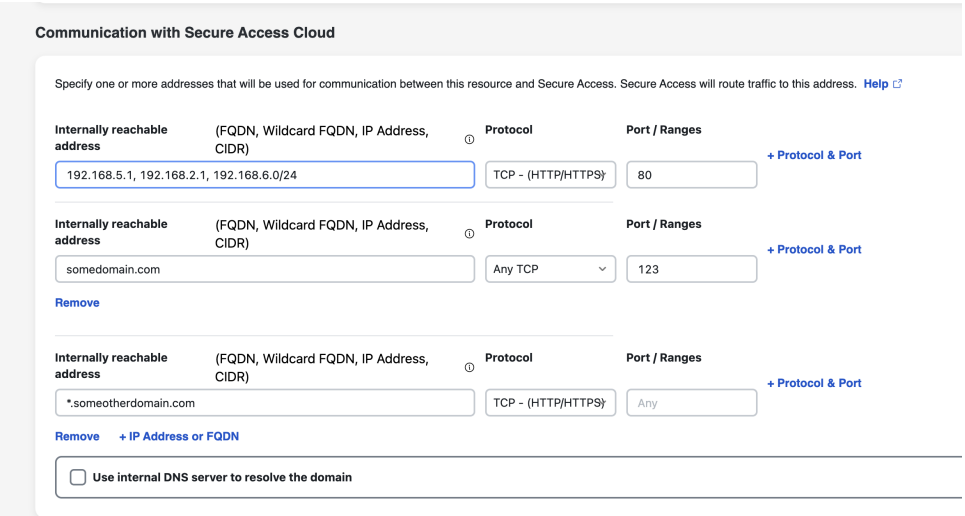
The address you provide does _not _ need to be publicly accessible from outside the network.

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:

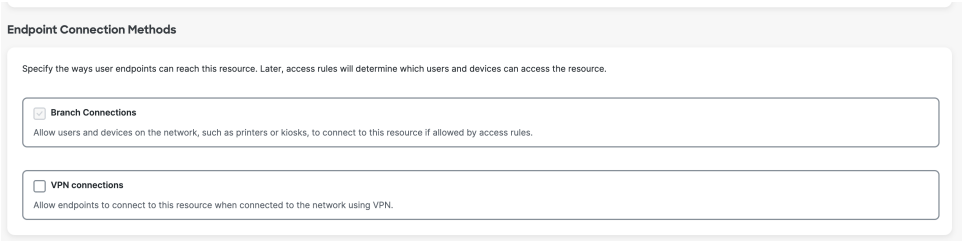
- In each address line, you can specify a single IP address (no address ranges) or CIDR block, or a comma-separated list of addresses or CIDR blocks, or an FQDN with or without wildcard. Add addresses and FQDNs as separate lines.
- If the address includes a wildcard FQDN, the wildcard must be the first 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 **+ Network IP or FQDN** and add a separate address line for each port.
- Select a protocol that includes TCP and does not include UDP.
- Example configurations:



If you 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.

- Branch Connections
- VPN connections



4. Branch connections are configured for all private resources. For more information, see Manage Branch Connections.
5. Select VPN connections to allow endpoints to communicate to this resource when connected to the network using VPN.
6. 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.

What To Do Next

- Configure requirements that you want to apply to this resource, such as endpoint requirements (using posture profiles) and intrusion prevention (IPS profiles). See Components for Private Access Rules.
- After you have configured other requirements, add private access rules to allow users and devices to access this resource. See Manage Private Access Rules.
- When you are ready for end-users to access the resource, if you have enabled browser-based access, give your users the dummy URL that you configured in this procedure.

Add a Private Resource Group

Provides instructions for adding a Private Resource Group in Cisco Secure Access China. You can create private resource groups with private resources and use these components as destinations in private access rules.

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.

Prerequisites

Lists the prerequisites for adding resource groups, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

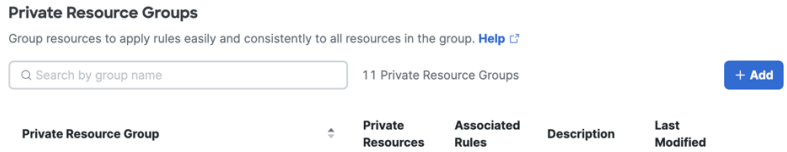
- Full Admin user role. For more information, see Manage Accounts.

Procedure

Provides instructions for adding resource groups. Configure a resource group with the private resources in your organization. The description is optional.

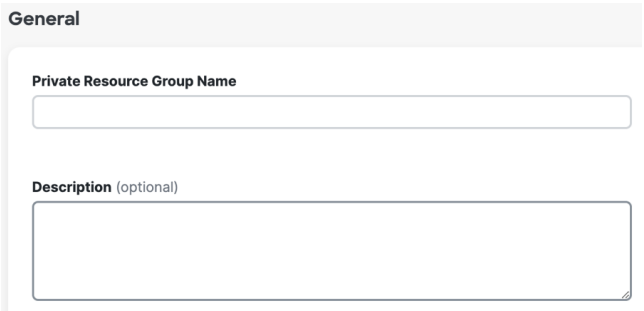
Configure a resource group with the private resources in your organization.

1. Navigate to **Resources** > **Private Resources**, choose **Private Resource Groups**, and then click **+Add**.



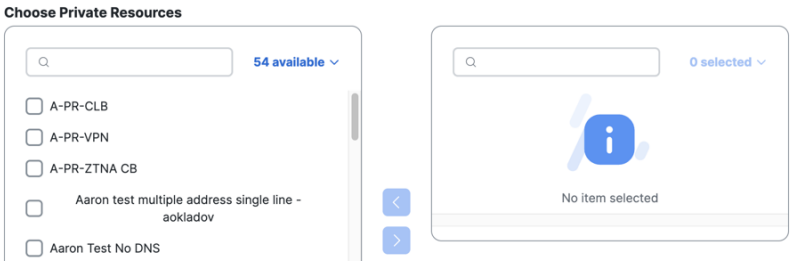
2. For **Private Resource Group Name**, enter a meaningful name for the resource group. For **Description**, we recommend that you provide information such as the purpose of the resource group.

> **Note**
>
> The description is optional.



3. For **Choose Resources**, add 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**.

Step 1 – Configure Private Resources

Describes 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.

1. Understand your connection options

Specify connection requirements for private resources where you want to allow access.

- For more information, see Manage Branch Connections.

1. Add Private Resources

- Work with resource owners to gather the information needed to configure each resource. For more information, see Add Private Resources.

Step 2 — Set Up Network Connections, VPN Profiles, and Certificates

Describes step 2 – Set Up Network Connections, VPN Profiles, and Certificates. 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.

1. 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.

2. 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

Describes 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.

1. 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.

24 Manage Connections to Private Destinations

Topics:

- Manage Connections to Private Destinations

Provides an overview of Manage Connections to Private Destinations in Cisco Secure Access China, including Manage Branch Connections. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Connections to Private Destinations

Provides instructions for managing connections to Private Destinations in Cisco Secure Access China. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access supports several types of connections to private resources:

- **VPN**–Remote Access Virtual Private Network
- **Branch Network**

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.

Manage Branch Connections

Provides instructions for managing branch Connections in Cisco Secure Access China. Secure Access protects users and devices that are connected on an organization's branch and internal networks.

Secure Access protects users and devices that are connected on an organization's branch and internal networks. An enterprise may have multiple branch offices distributed across various geographical locations. Each branch office may allow connections only to certain applications and services managed by the organization and block connections to other private resources.

When on a branch network protected by Secure Access, users and devices can connect seamlessly to the internet and private applications and services. You can control how users and devices connect to private resources by adding private access policy rules for network sources and destinations. For example, you can define policy rules that block or allow access to private resources from IOT devices, kiosks, or printers.

Endpoint Connection Methods

Describes endpoint Connection Methods. Secure Access supports various types of network connections to private resources:. When you add a private resource to Secure Access, Secure Access automatically enables Branch Connections to the private destination.

Secure Access supports various types of network connections to private resources:

- **Branch connections**
- **VPN connections**

When you add a private resource to Secure Access, Secure Access automatically enables **Branch Connections** to the private destination.

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.

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.

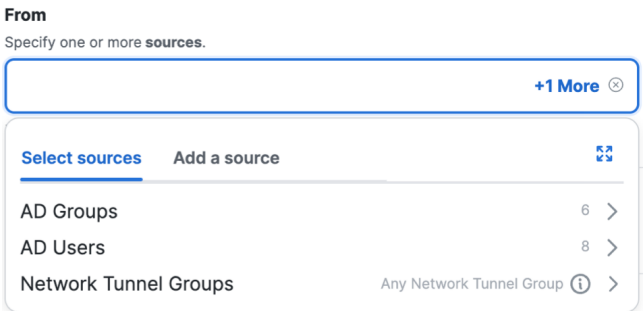
Users, groups, and devices on your corporate networks, including branch offices, can always connect to a private resource if allowed by private access rules. When users, groups, and user devices connect to private resources from a branch network, Secure Access does not evaluate the device's endpoint 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.

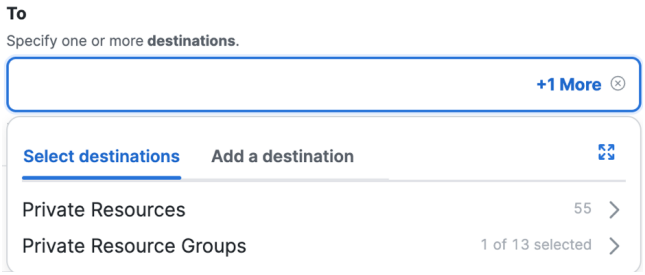


Destinations for Branch Network Connections

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. Network Tunnel Group.

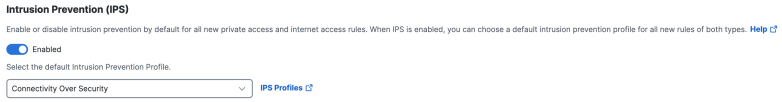
Secure Access supports connections from Branch network source components to various destination components.

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

Provides instructions for 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.

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.

25 Manage the Access Policy

Topics:

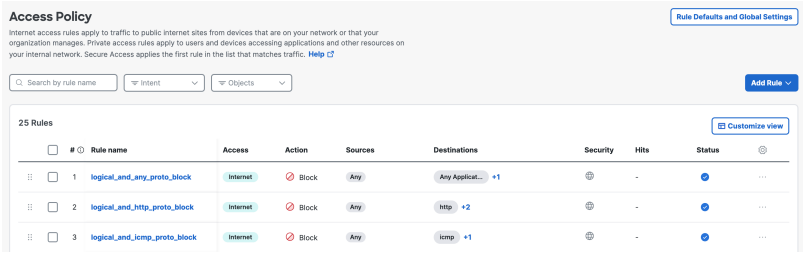
- Manage the Access Policy

Provides an overview of Manage the Access Policy in Cisco Secure Access China, including About the Access Policy, Show Additional Data on Your Access Rules, and Edit the Order of the Rules in Your Access Policy. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage the Access Policy

Provides instructions for managing the Access Policy in Cisco Secure Access China. Secure Access has a single unified policy, which consists of policy rules and settings.

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.



About the Access Policy

Describes About the Access Policy in Cisco Secure Access China. The Cisco Secure Access policy is the collection of your internet and private access rules, rule defaults, and global settings.

The Cisco Secure Access policy is the collection of your internet and private access rules, rule defaults, and global settings. The policy displays your configured rule data and allows you to choose how to prioritize the rules in your policy. Once you add a rule, you can edit various components on the rule. You decide how to view and manage your rules that best meets your organization's access controls to resources.

Best Practices

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.

    Rule Defaults
  - **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.

    Custom

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.

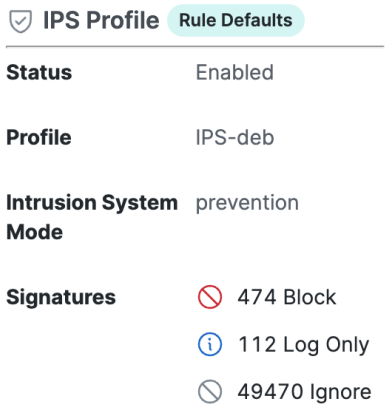


- **#**–The pound sign (hash symbol) indicates the priority of the rule.
- **Rule name**–The name that you assigned to the rule.
- **Access**–The type of access rule either **Internet** or **Private**.
- **Action**–The type of action on the rule.
  - For internet access rules: **Allow**, **Block**, **Isolate**, 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.

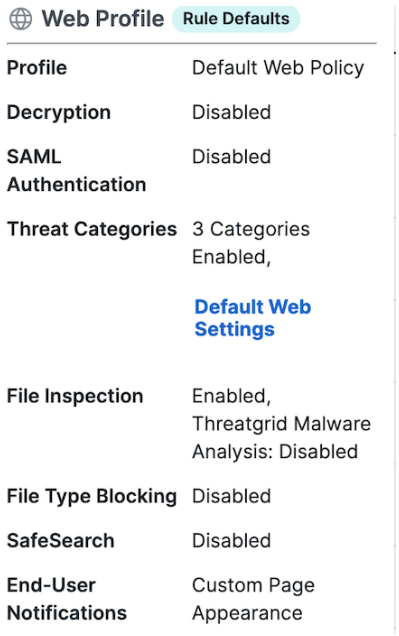


Security controls are the globally-configured profiles that are enabled on the rule: Intrusion Prevention (IPS), Web, and Tenant profiles. Hover over the security icon to display the profile information for the rule.

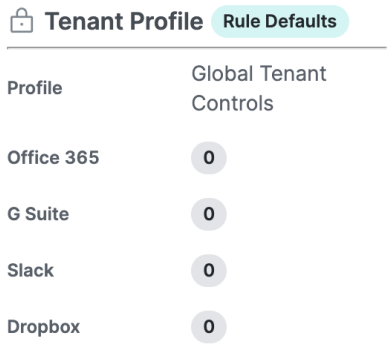
- **IPS Profile**. For more information, see Manage IPS Profiles.



- **Web Profile**. For more information, see Manage Web Profiles.



- **Tenant Profile**. For more information, see Manage Tenant Control Profiles.



- **Hits**–The number of times Secure Access China 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

Describes Show Additional Data on Your Access Rules in Cisco Secure Access China. The Cisco Secure Access policy table lists the configured properties, security controls, logging, and status information for your internet and private access rules.

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.

Prerequisites

Lists the prerequisites for show additional data on access rules. Full Admin user role. For more information, see Manage Accounts.

- Full Admin user role. For more information, see Manage Accounts.
- Your policy has at least one configured access rule.

Procedure

Provides instructions for show additional data on access rules. 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.

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.

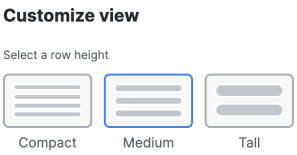


1. Navigate to **Secure** > **Access Policy**, and then click **Customize view**.

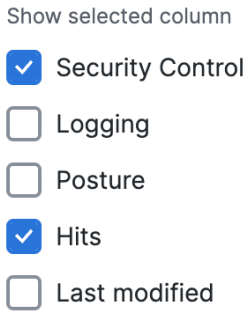


2. (Optional) For **Select a row height**, choose the height of the rows in the policy table.

   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.

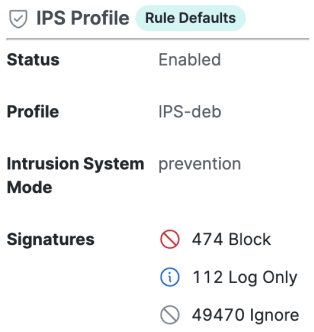


   - **Security**–The security controls applied to the rule.

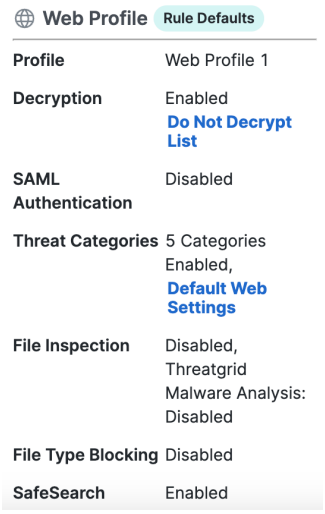


Security controls are the globally-configured profiles that are enabled on the rule: Intrusion Prevention (IPS), Web, and Tenant profiles. Hover over the security icon to display the profile information for the rule.

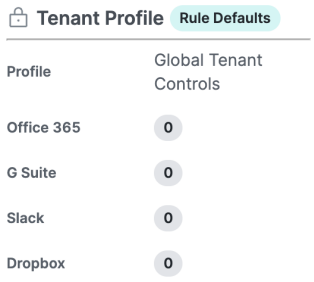
- **IPS Profile**. For more information, see Manage IPS Profiles.



- **Web Profile**. For more information, see Manage Web Profiles.

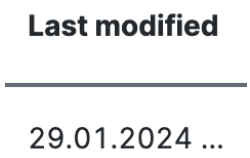


- **Tenant Profile**. For more information, see Manage Tenant Control Profiles.



- **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 defaults** to show the policy table with the default rule data view or click anywhere on the page outside of the **Customize View** component to enable your selections and close the window.



Edit the Order of the Rules in Your Access Policy

Provides instructions for editing the Order of the Rules in Your Access Policy in Cisco Secure Access China. 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 in Cisco Secure Access China. 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. 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.

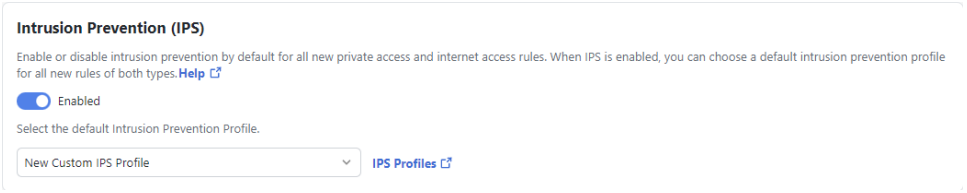
For example, if you change the default IPS Profile from **Balanced Security and Connectivity** to **Maximum Security**, the IPS profile in all existing rules that are configured to use the default IPS Profile will now use the **Maximum Security** settings for IPS.

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.

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.

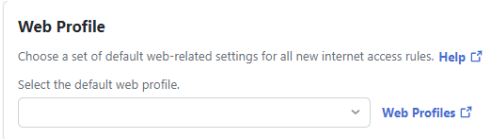


For more information, see Manage IPS Profiles.

Web Profile

Describes web Profile. A Web profile provides a set of web-related settings. Choose a profile to apply to all new internet access rules.

A Web profile provides a set of web-related settings. Choose a profile to apply to all new internet access rules.

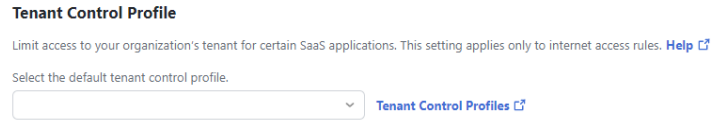


For more information, see Manage Web Profiles.

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, see Manage Tenant Controls.

Global Settings for Access Rules

Describes Global Settings for Access Rules in Cisco Secure Access China and outlines Microsoft 365 Compatibility, Tenant Controls, and Limitations. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Global Settings affect all rules of the applicable type (internet access rules and/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.

To change these settings, see Edit Rule Defaults and Global Settings.

Global Settings for Access Rules

Describes global Settings for Access Rules. Microsoft 365 Compatibility. Secure Access Packages and Feature Availability Not all of the features described here are available to all Secure Access packages.

- Microsoft 365 Compatibility
- Decryption
- Decryption Logging
- Certificate Pinning

> **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.

Microsoft 365 Compatibility

Describes microsoft 365 Compatibility. This setting applies only to web security features, not to IPS. The domains are excluded from HTTPS decryption and content filtering.

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

Describes tenant Controls. If you use tenant controls for Microsoft 365, see additional information at Use Tenant Controls in Access Rules.

If you use tenant controls for Microsoft 365, see additional information at Use Tenant Controls in Access Rules.

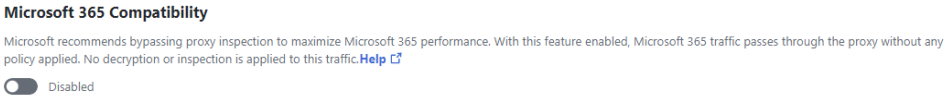
Limitations

Describes limitations. 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.

- 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

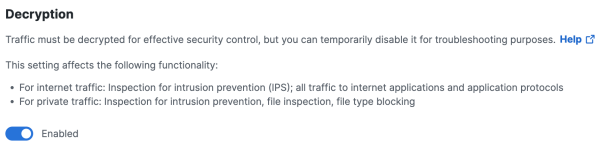
Describes decryption. Traffic must be decrypted for effective security control, but you can temporarily disable decryption for troubleshooting purposes. This setting applies to the following functionality:.

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.



Decryption Logging

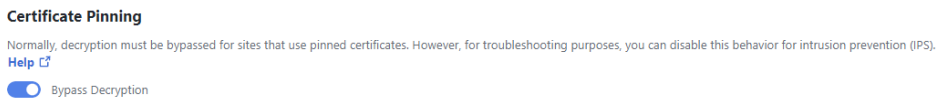
Describes decryption Logging. You can enable or disable decryption logging globally in Global Settings, for traffic to private resources or internet destinations or both.

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 in Cisco Secure Access China. Before you change the default rule settings on the Cisco Secure Access policy, see Important Information About Changing Rule Defaults.

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.

Prerequisites

Lists the prerequisites for editing rule defaults and global settings. Full Admin user role. For more information, see Manage Accounts.

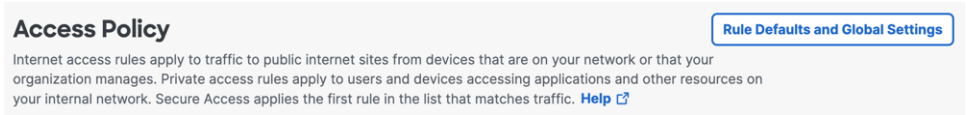
- Full Admin user role. For more information, see Manage Accounts.
- If you are changing the rule defaults, understand the ramifications of doing so. For more information, see Important Information About Changing Rule Defaults.
- Review the settings available on each policy rule:
  - Rule Defaults
  - Global Settings

Procedure

Provides instructions for editing rule defaults and global settings. To change rule defaults or global settings:. For details about each setting, see:.

To change rule defaults or global settings:

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

Provides instructions for editing the Default Access Rules in Cisco Secure Access China, including Default Internet Access Rule, Default Private Access Rule, and To View or Edit Default Access Rules. It explains the sequence of actions and relevant settings presented in the procedure.

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

Describes 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.

- 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

Describes 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.

- 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

Describes to View or Edit Default Access Rules. To view or edit a default access rule:. Navigate to Secure > Access Policy.

To view or edit a default access rule:

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.

Private and Internet Access Rules in Your Policy

Describes private and Internet Access Rules in Your Policy. There are two types of access rules:. To create and work with these rules, see Get Started with Private Access Rules.

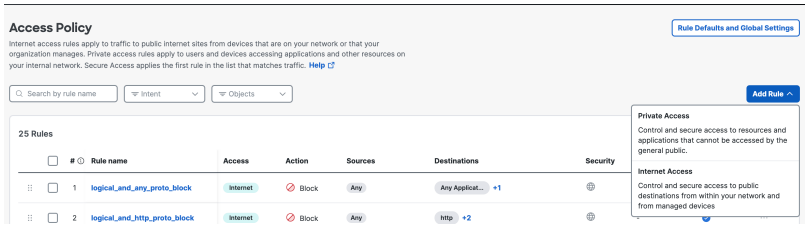
There are two types of access rules:

- **Private access rules**–Controls access to applications hosted from your data center and private clouds.

To create and work with these rules, 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

Describes 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.

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.



Rule Defaults and Global Settings

Describes 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.

- For more information, see Global Settings for Access Rules.
- For more information, see Rule Defaults: Default Settings for Access Rules.

26 Get Started With Internet Access Rules

Topics:

- Get Started With Internet Access Rules

Provides an overview of Get Started With Internet Access Rules in Cisco Secure Access China, including Components for Internet Access Rules, Default Settings for Internet Access Rules, and Add an Internet Access Rule. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started With Internet Access Rules

Describes Get Started With Internet Access Rules in Cisco Secure Access China. Internet access rules specify how traffic to internet destinations should be handled.

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.

   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.

   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.

   See Edit the Default Access Rules

5. **Add internet access rules**

   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.

   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.

   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 in Cisco Secure Access China. 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

Provides instructions for 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.

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

Provides instructions for configuring intrusion prevention (ips) profiles. You can choose a different IPS profile for each access rule based on the balance of convenience vs. risk appropriate for the particular traffic.

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

Provides instructions for 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 Web Profiles

Configure Threat Category Settings

Provides instructions for 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

Provides instructions for configuring SAML authentication, which is required for some web security features; see Manage Web Profiles for related settings.

SAML authentication is required for some web security features.

See Manage Web Profiles

Set Up Certificates for Decrypting Internet Traffic

Provides instructions for 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

Provides instructions for 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 web profile.

For details, see Important Information About Do Not Decrypt Lists.

(Optional) Configure Custom End-User Block and Warn Notifications

Provides instructions for configuring custom end-user block and warn notifications for blocked or warned internet destinations; notifications require decryption. for administrators to review.

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 Web Profiles

Provides instructions for configuring web 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.

  See Manage File Inspection.

- **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 web profile that you will choose in a rule. See Manage Web Profiles.

Tenant Controls

Describes tenant Controls. If your company uses Microsoft 365, Slack, Google G-Suite, or Dropbox, see Manage Tenant Control Profiles .

If your company uses Microsoft 365, Slack, Google G-Suite, or Dropbox, see Manage Tenant Control Profiles.

Default Settings for Internet Access Rules

Describes Default Settings for Internet Access Rules in Cisco Secure Access China. 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 **Rule Defaults and Global Settings**, 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.

- **Web Profile**

  Specify a default set of settings that control security and other interactions for end users accessing the internet.

  For more information about web profiles, see Manage Web 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 in Cisco Secure Access China. The Cisco Secure Access policy is a collection of an organization's internet and private access rules.

The Cisco Secure Access policy is a collection of an organization's internet and private access rules. To start protecting user devices that connect to the Internet, add internet rules to the organization's Access policy.

This guide describes the steps to add an internet access rule and configure security controls and profiles.

Prerequisites

Lists the prerequisites for adding an internet access rule. Prerequisites for internet access rules are similar to but different from prerequisites for private access rules.

- Full Admin user role. For more information, see Manage Accounts.
- At a minimum, you should configure the source and destination components and rule settings before creating internet access rules.
  - For more information, see Components for Internet Access Rules.
  - For more information, see Default Settings for Internet Access Rules.
- For other factors involved in creating and enforcing internet access rules, see Manage Internet Access Rules.
- In general, decryption is required to properly process HTTPS traffic, including traffic that will be blocked. For more information, see Security Profile.

> **Note**
>
> Prerequisites for internet access rules are similar to but different from prerequisites for private access rules.

Procedure

Provides instructions for adding an internet access rule. Navigate to Secure > Access Rules. Click Add Rule > Internet Access.

1. Navigate to **Secure > Access Rules**.
2. Click **Add Rule > Internet Access**.

   At the top of the rule is a summary section. The **Summary** describes the security controls that you configure on this rule.

3. Configure access criteria. For more information, 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. For more information, see Security Control Options.
6. Click **Save**.
7. (Optional) Enable or disable the rule using the toggle at the top of the page.
8. (Important) Additional rules are required for most traffic.

Access Options

Lists access rule configuration options, including rule action, sources, destinations, endpoint requirements, logging settings, rule summary, and advanced application controls.

- Disable or enable the rule
- Logging settings
- Summary
- Rule name
- Rule order
- Rule action
- Pre-Configured Sources
- Composite Sources
- Pre-Configured Destinations
- Composite Destinations
- Advanced Application Controls

Disable or Enable the rule

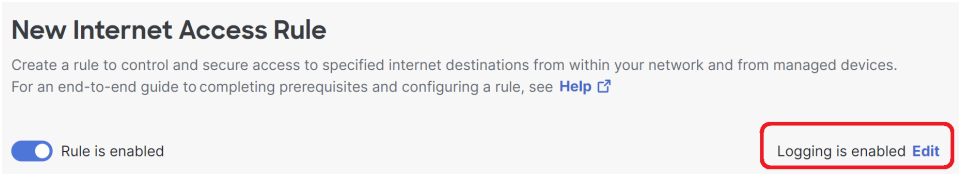
Provides instructions for disabling or enable the rule. After you configure the rule and click Save , the rule will take effect only if this toggle shows as Enabled.

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 China applies the first rule in the list on the Access Policy page that matches the traffic.

Specify where you want this rule in the overall rule order.

Secure Access China applies the first rule in the list on the Access Policy page that matches the traffic.

Order your rules so that more specific rules are above more general rules that might also apply to the traffic.

For important guidelines, see Edit the Order of Rules on the Access Policy Page.

Rule action

Describes rule action. 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 applications and application categories as well as content categories and content category lists.
  - You can configure a custom warning notification that Secure Access China 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** - Currently, Remote Browser Isolation is not supported.

Pre-Configured Sources

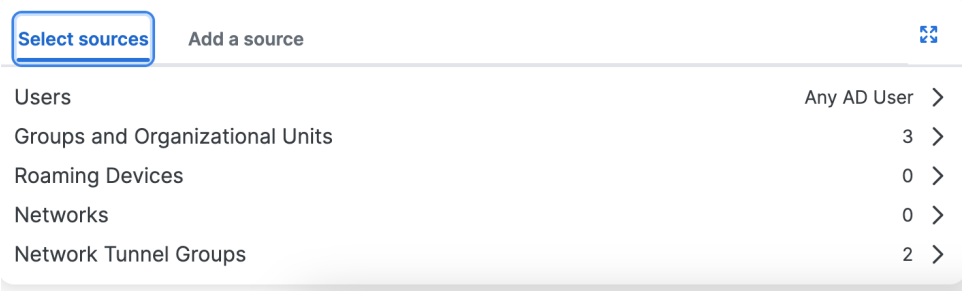
Describes pre-Configured Sources. We recommend that you create reusable components rather than adding source IP addresses directly to a rule. For more information, see Components for Internet Access Rules.

We recommend that you create reusable components rather than adding source IP addresses directly to a rule. For more information, see Components for Internet Access Rules.

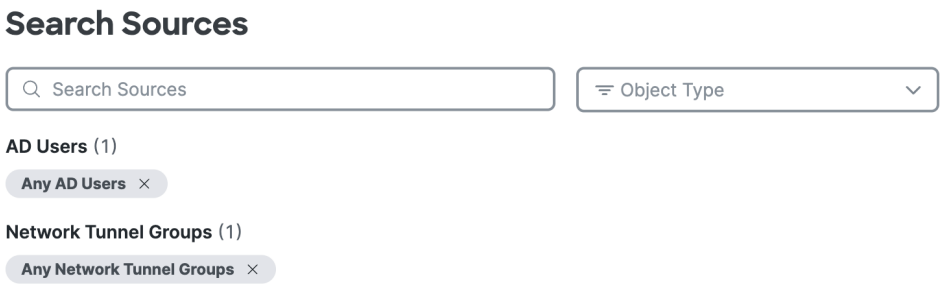
> **Note**
>
> The arrows out icon opens a window to configure the sources in your rule.

1. Navigate to **Secure > Access Policy > Add Rule > Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **From**.
3. For **Select sources**, click in the white space beside the default value ("Any") and choose the configured source components in your organization.

For descriptions of the different types of sources, including links to how to create reusable sources, see Components for Internet Access Rules.



4. After you add a source component, click **+More** to view the list of sources that you added to the rule.
   a. Click on the **X** to remove a previously added source, then click **Done**



Composite Sources

Describes composite Sources. Secure Access China does not support a comma-separated list of wildcard masks. Navigate to Secure > Access Policy > Add Rule > Internet Access.

You can add Sources directly on an internet rule. This option is useful if you need to quickly address a specific issue that arises, for example to immediately block a particular user's access to an internet destination. For more information about configuring sources, see About Configuring Sources for Internet Access Rules.

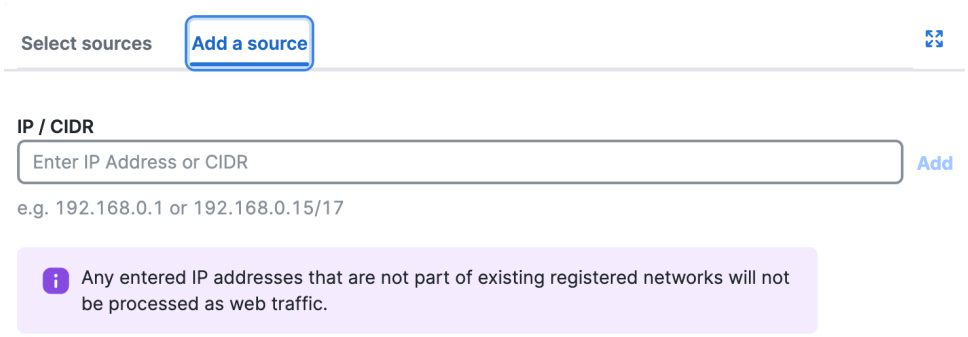
Important

Secure Access China does not support a comma-separated list of wildcard masks.

1. Navigate to **Secure > Access Policy > Add Rule > Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **From**.
3. For **Add a source**, enter an IPv4 address or CIDR block.

   For example:

   - IPv4 address–**1.2.3.4**
   - CIDR block–**1.2.3.4/24**



4. Click **Add**.
5. After you add a composite source, click **+More** to view the list of sources that you added to the rule.
   a. Click on the **X** to remove a previously added source, then click **Done**.



Pre-Configured Destinations

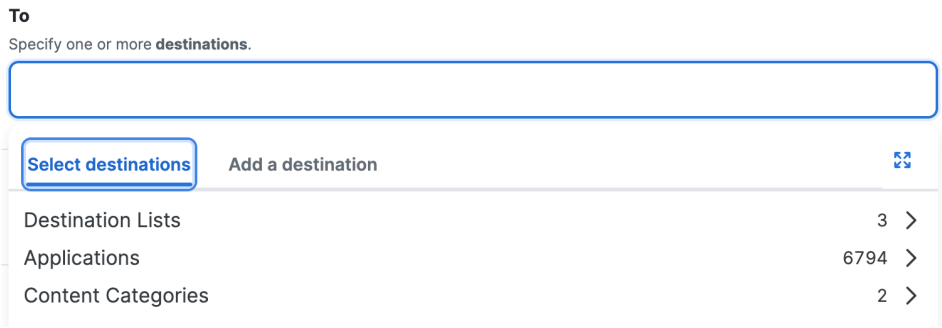
Describes pre-Configured Destinations. We recommend that you create reusable components rather than adding destinations directly in a rule. For more information, see Components for Internet Access Rules.

We recommend that you create reusable components rather than adding destinations directly in a rule. For more information, see Components for Internet Access Rules.

The rule action sets the the destination options that are available on the rule. Usually you will select destinations that you or others have previously configured.

> **Note**
>
> The arrows out icon opens a window to configure the destinations in your rule.

1. Navigate to **Secure > Access Policy > Add Rule > Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.
3. Click **Select destinations**, click in the white space beside the default value ("Any") and choose the configured destinations in your organization.



4. After you add a destination component, click **+More** to view the list of destinations that you added to the rule.
   a. Click on the **X** to remove a previously added destination, then click **Done**.



Composite Destinations

Describes composite Destinations. You can add destinations directly on an internet rule. For more information, see About Configuring Destinations for Internet Access Rules.

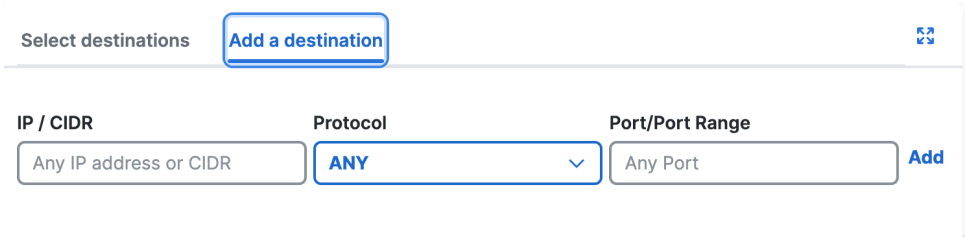
You can add destinations directly on an internet rule. For more information, see About Configuring Destinations for Internet Access Rules.

1. Navigate to **Secure > Access Policy > Add Rule > Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.
3. Click **Add a destination**.
   a. For **IP or CIDR**, enter an IPv4 address or CIDR block.

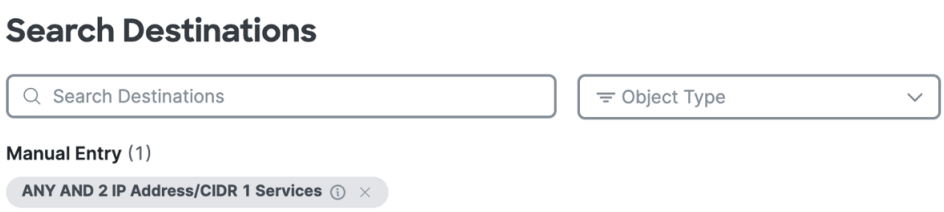
      For example:

      - IPv4 address–**1.2.3.4**
      - CIDR block–**1.2.3.4/24**

   b. For **Protocol**, choose from one of the supported protocols: **ANY**, **TCP**, **UDP**, or **ICMP**.
   c. For **Port/Port Range**, enter a port or range of ports separated by a hyphen (**-**).
   d. When you finish adding the composite destination, click **Add**.



4. After you add a destination component, click **+More** to view the list of destinations that you added to the rule.
   a. Click on the **X** to remove a previously added destination, then click **Done**.



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.

For more information, see Advanced Application Controls.

Security Control Options

Lists security control options, including Intrusion Prevention, security profiles, tenant control profiles, and advanced security controls. for administrators to review.

- 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.

For more information, 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 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.

Tenant Control Profile

Describes tenant Control Profile. Tenant controls affect access to Microsoft 365, Google G Suite, Slack, and Dropbox. For additional requirements, see Use Tenant Controls in Access Rules.

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 Get Started with Internet Access Rules and review additional steps you should take after configuring a rule.

Return to Get Started with Internet Access Rules and review additional steps you should take after configuring a rule.

About Configuring Sources in Internet Access Rules

Describes About Configuring Sources in Internet Access Rules in Cisco Secure Access China. Secure Access internet rules enable you to configure DNS and Web security for your organization's web traffic.

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.

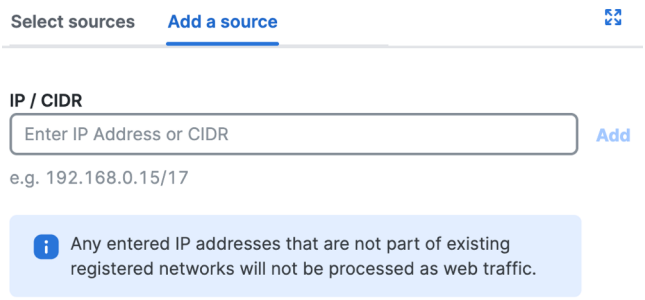
If you select Network Tunnel Groups, Secure Access secures and controls access from traffic from IPsec tunnels established by your supported network devices. If you need to know what tunnels are included in a group, navigate to **Connect > Network Connections > Network Tunnel Groups** and look at the 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

Describes IP Addresses and CIDR Blocks. Sources accept private non-routable IPs (RFC-1918 compliant) or IPs for Registered Networks in Secure Access.

- 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.

About Configuring Destinations in Internet Access Rules

Describes About Configuring Destinations in Internet Access Rules in Cisco Secure Access China. Secure Access China internet rules enable you to configure Web security for your organization's web traffic.

Secure Access China internet rules enable you to configure 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 China 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. 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.

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 China combines the entries into a set using the boolean OR operator.

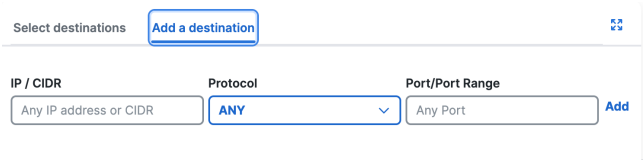
You can add destinations directly in a rule rather than choosing destination components. However, this is generally not recommended. Destinations that you add to a rule are not reusable components, are not dynamically updated, and cannot be used in any other rule.

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 China does not accept private non-routable addresses for destinations, only public IP addresses. Secure Access China does not require that your destination IP address is the IP of a Registered Network in Secure Access China.

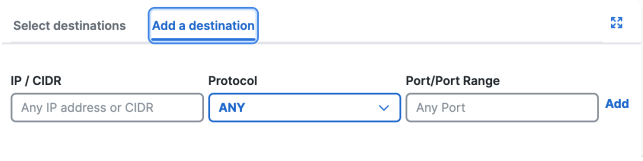
- Destinations accept IP addresses and CIDR blocks.
  - Secure Access China does not accept private non-routable addresses for destinations, only public IP addresses.
  - Secure Access China does not require that your destination IP address is the IP of a Registered Network in Secure Access China.



Ports

Explains port handling for internet access rule destinations and identifies ports 80 and 443 as ports accepted directly on a rule.

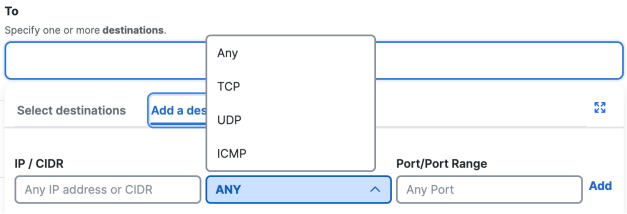
- Destinations accept ports 80 and 443 directly on an internet access rule.



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 in Cisco Secure Access China. 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

Lists cloud storage applications and shows the available upload, download, posting, sharing, and delete actions for each application category. for administrators to review.

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
SmugMug	Cloud Storage	Yes	Yes		Yes
SlideShare	Cloud Storage	Yes	Yes		Yes
4shared	Cloud Storage	Yes			Yes

Collaboration

Describes collaboration. Cisco Webex Teams. 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.

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

Lists content management categories and identifies the supported application actions, including upload, download, and posting or sharing content. for administrators to review.

Applications	Category	Upload	Download	Post/Share
Egnyte Connect	Content Management	Yes		
Lucidchart	Content Management	Yes		
Pastebin	Content Management	Yes		

Media

Lists media applications and shows the available upload, download, posting, sharing, and delete actions for each application category. for administrators to review.

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. Only for Gmail attachment uploads. Only for Mail.ru attachment uploads. Yes Only for Gmail attachment uploads. Yes Only for Mail.ru attachment uploads.

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

Lists peer-to-peer applications and shows the available upload, download, posting, sharing, and delete actions for each application category. for administrators to review.

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

Lists social networking applications and shows the available upload, download, posting, sharing, and delete actions for each application category. for administrators to review.

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

Applications	Category	Upload	Download	Post/Share
Twitter	Social Networking	Yes		Yes

Prerequisites

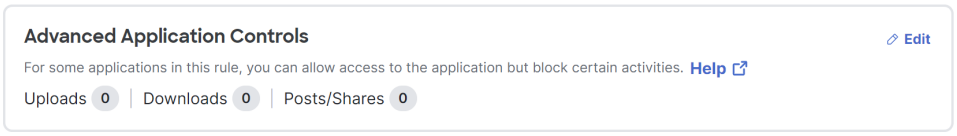
Lists the prerequisites for advanced application controls, including the Full Admin user role and the access role details in Manage Accounts.

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

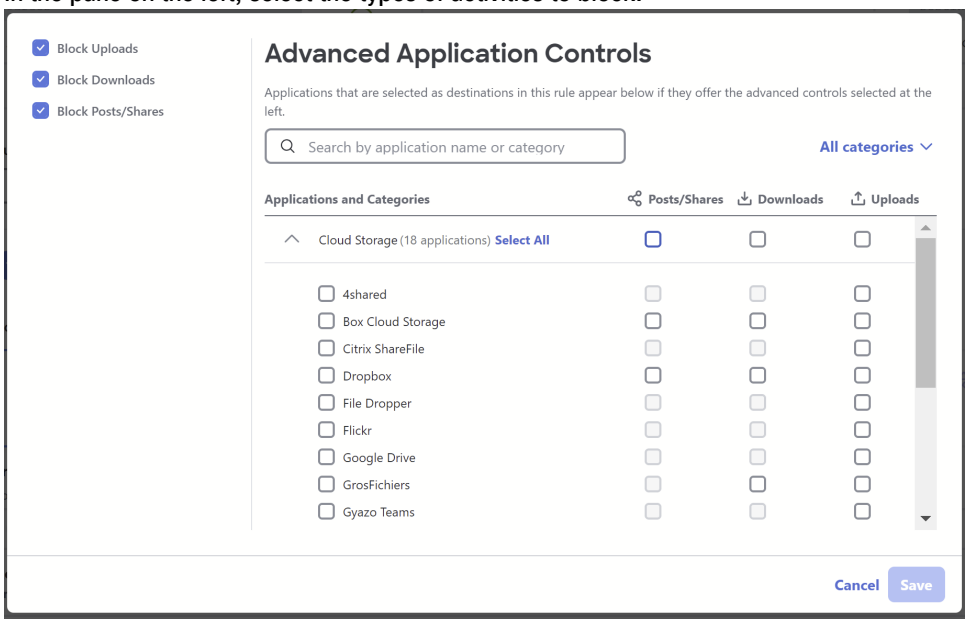
Procedure

Provides instructions for advanced application controls. Repeat as needed for each category in the All categories list. 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.

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 web profile selected in the rule.

If advanced application control is not working as expected, check the following:

- Decryption must be enabled in the web profile selected in the rule.
- The site must not be on the **Do Not Decrypt** list selected in the web 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.

Global Settings for Internet Access Rules

Describes Global Settings for Internet Access Rules in Cisco Secure Access China. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Global settings generally apply to all rules. However, some settings apply only to private access rules, not to internet access rules.

Do not change global settings unless you have a specific reason to do so.

If your company uses either of the following, verify that the applicable global settings are correct for your company:

- Microsoft 365 applications
- Applications that use pinned certificates

Decryption-related settings:

- Decryption for IPS

  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.

Troubleshoot Internet Access Rules

Provides instructions for troubleshooting internet Access Rules in Cisco Secure Access China, including General troubleshooting tips, Problems while creating the rule, and The Next button is unavailable. It explains the sequence of actions and relevant settings presented in the procedure.

To troubleshoot internet 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 the rule

Introduces issues that can arise while creating an access rule and directs administrators to the related rule configuration and troubleshooting guidance.

The Next button is unavailable

Describes 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 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 Web Profile, including in the web 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 web 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.

27 Get Started With Private Access Rules

Topics:

- Get Started With Private Access Rules

Provides an overview of Get Started With Private Access Rules in Cisco Secure Access China, including Components for Private Access Rules, Default Settings for Private Access Rules, and Add a Private Access Rule. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started With Private Access Rules

Describes Get Started With Private Access Rules in Cisco Secure Access China. 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.

   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.

   See Default Settings for Private Access Rules.

4. **Add private access rules**

   Generally, you will create rules to allow access to private resources.

   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**.

   See Edit the Default Access Rules.

6. **Edit the global settings**

   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.

   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.

   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.

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 in Cisco Secure Access China. You can create access rules by adding rule components that you or others have configured to a rule.

You can create access rules by adding rule components that you or others have configured to a rule. Components described in this topic are reusable. You can use the same component (such as a source) in multiple rules, speeding and simplifying rule creation. For example, you can define a set of users as a source, then use the same source in an internet access rule and in a private access rule for the same set of users. Some components are profiles, or groups of settings bundled together that you choose as a unit when configuring a rule.

Sources

Describes sources. 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 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:

- **VPN posture profiles**: For end-user devices that are connected to the network using remote access VPN.
- **Branch connections**: For end-user devices that are connected to these resources from a branch network.

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

Explains the security controls used by private access rules and compares their range with the more varied controls used for internet access rules.

Private access rules have (and need) less varied security controls than internet access rules.

Intrusion Prevention (IPS)

Describes 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.

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 in Cisco Secure Access China. 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 > Policy > Access Policy**, click**Rule Defaults and Global Settings**, then click the **Rule Defaults** tab.

The following settings apply to private access rules:

- **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.

- **Web Profile**

  Specify a default set of settings that control security and other interactions for end users accessing the internet.

  For more information about web profiles, see Manage Web Profiles.

- **Tenant Control Profile**

  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.

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

Provides instructions for adding a Private Access Rule in Cisco Secure Access China. Cisco Secure Access China connects users, devices, both public and branch networks, and network tunnels to private resources in your enterprise.

Cisco Secure Access China 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 China enables Branch network connections to the resource.

Once you add your sources and private resources to Secure Access China, 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 China 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

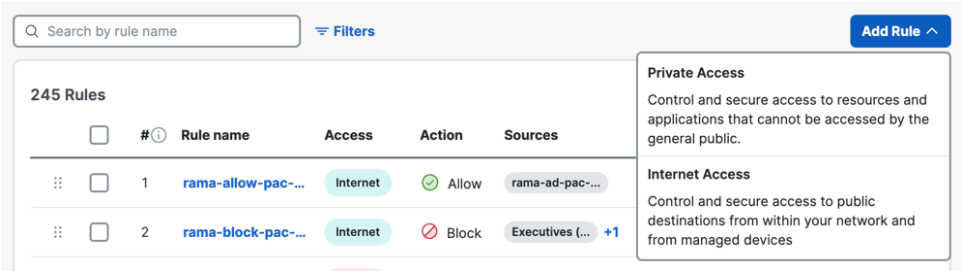
Lists the prerequisites for adding a private access rule. Full Admin user role. For more information, see Manage Accounts. Add sources to your organization. For more information, see Components for Private Access Rules.

- 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. 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.

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.

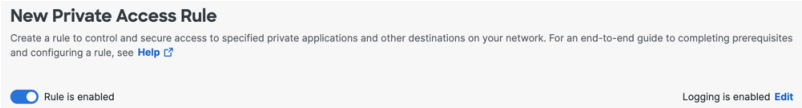


Enable the Rule and Edit Your Logging Settings

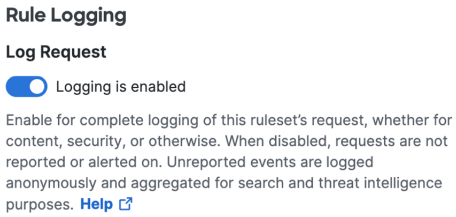
Provides instructions for enabling the rule and edit your logging settings. Toggle the rule to enable it. After you configure and save the rule to your policy, the rule is enabled.

1. Toggle the rule to enable it. After you configure and save the rule to your policy, the rule is enabled.

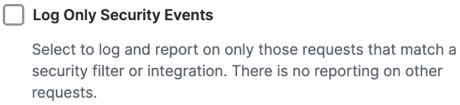
   You can toggle off the rule at any time to disable it.



1. Click **Edit** to manage your logging settings on the access rule.
   a. For **Log Request**, toggle off or on to choose whether Secure Access China logs the events for the traffic managed by the access rule.



   b. For **Log Only Security Events**, select whether Secure Access China 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.

1. 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.

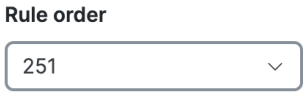


Choose a Rule Order

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 China.

1. For **Rule order**, choose a new priority for the rule, or keep the rule order assigned to the rule by Secure Access China.

When you add a new rule, Secure Access China assigns the next lowest priority to the rule. Secure Access China 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.



Step 1 — Specify Access Options

Outlines the first access rule configuration step and identifies the rule action, sources, destinations, and endpoint requirements to specify. for administrators to review.

- Rule Action
- Sources
- Destinations
- Endpoint Requirements

Rule Action

Describes rule Action. Note: When the action is Allow and the traffic does not pass the security controls defined in the rule, Secure Access China blocks the traffic.

1. Choose **Allow** or **Block** to assign how Secure Access China applies the configured components in the access rule. **Note:** Secure Access China blocks the traffic in your organization to private destinations unless an access rule allows the connections.

Note: When the action is **Allow** and the traffic does not pass the security controls defined in the rule, Secure Access China blocks the traffic.

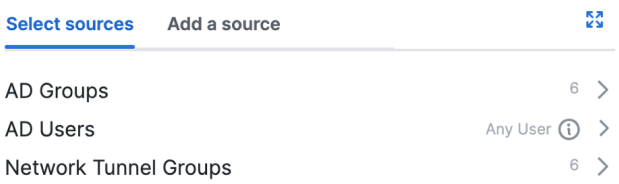
Sources

Describes 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.

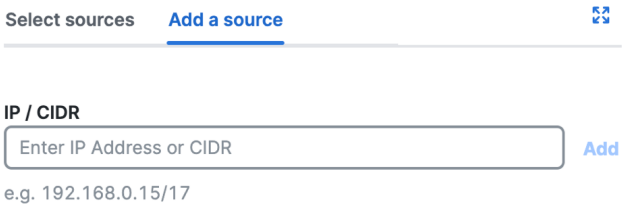
> **Note**
>
> The connection methods for a destination depend on the type of sources that you choose. If you select Users or User Groups, you can choose destinations enabled for virtual private networks (VPNs) connections, not Branch connections.

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**.

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 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.

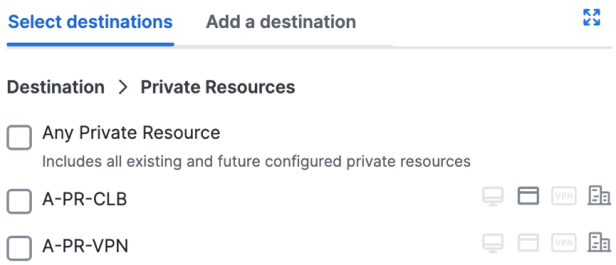
1. For **Select destinations**, click in the white space beside the default value ("Any") and choose the configured **Private Resource Groups** and **Private Resources** in your organization. When you finish choosing your private resources, click **Done**.

   Note

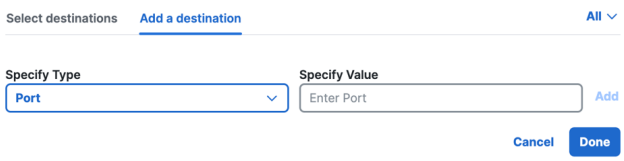
   The arrows out icon opens a window to configure the destinations in your rule.

   a. For each **Private Resource**, hover over the network connections icons.

      Secure Access China 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**.



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.

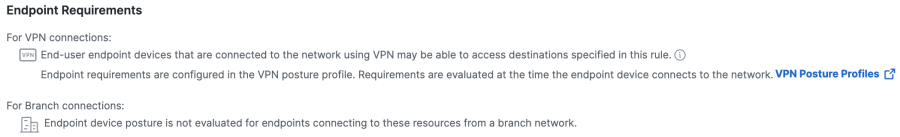
For more information, see About Configuring Destinations in Private Access Rules.

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.



Step 2 — Configure Security Control Options

Describes step 2 – Configure Security Control Options. Intrusion prevention is the only security control option needed for private access rules.

Intrusion prevention is the only security control option needed for private access rules.

Intrusion Prevention (IPS)

Describes intrusion Prevention (IPS). We recommend that you do not disable your IPS Profiles. For more information, see Manage IPS Profiles.

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**.

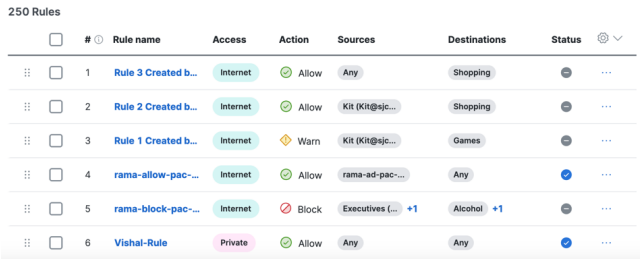
> **Note**
>
> We recommend that you do not disable your IPS Profiles. For more information, see Manage IPS Profiles.

Summary

Describes summary. After you add a rule to your policy, you can edit the rule and then view the rule summary.

After you add a rule to your policy, you can edit the rule and then view the rule summary.

1. Navigate to **Secure > Access Policy**.
2. Navigate to a rule, and then click on the horizontal elipsis (**...**) to expand the rule menu.



3. Click **Edit** to open the rule and view the rule summary.



The summary contains the components that you configured on the access rule:

- **Sources**
- **Action**
- **Security Controls**
- **Destinations**

If you see an **Upgrade** button, this means that your organization has an opportunity to upgrade to a subscription that offers additional functionality.

About Configuring Sources in Private Access Rules

Describes About Configuring Sources in Private Access Rules in Cisco Secure Access China. Let the following information guide you when you add sources to a private access rule.

Let the following information guide you when you add sources to a private access rule.

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 in Cisco Secure Access China. Let the following information guide you when you add destinations to a private access rule.

Let the following information guide you when you add destinations to a private access rule.

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 (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.

Important

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 in Cisco Secure Access China. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Important

Note about traffic handling

If endpoints do not meet the requirements specified in posture profiles, traffic is handled differently for VPN connections:

- **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 Cisco Secure Access China. 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 in Cisco Secure Access China. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Global settings generally apply to all rules. However, some settings apply only to internet access rules, not to private access rules.

The following global settings apply to private access rules:

- **Decryption for IPS**

  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

Provides instructions for troubleshooting private Access Rules in Cisco Secure Access China, including General Troubleshooting Tips, Problems While Creating a Rule, and Next button is not available. It explains the sequence of actions and relevant settings presented in the procedure.

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

Introduces issues administrators may encounter while creating an access rule and provides a place to review related rule configuration guidance.

Next button is not available

Describes 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.

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 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.
- 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.

28 Manage Endpoint Security

Topics:

- Manage Endpoint Security

Provides an overview of Manage Endpoint Security in Cisco Secure Access China, including Endpoint Attributes. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Endpoint Security

Provides instructions for managing endpoint Security in Cisco Secure Access China. Secure Access is a converged cloud security solution that enables fast, reliable, and secure private network connections to your applications.

Secure Access is a converged cloud security solution that enables fast, reliable, and secure private network connections to your applications. End users are assured of a secure, transparent user experience, anywhere they work – office, home, or on the road. User devices can read, write, and update private resources by setting up virtual private networks (VPNs) connections to Secure Access through IPsec network tunnels.

Endpoint Attributes

Describes Endpoint Attributes in Cisco Secure Access China and outlines Supported Operating Systems, Firewall Conditions, and Endpoint Security Agents. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

The following sections describe the endpoint attributes that are evaluated.

Supported Operating Systems

Describes supported Operating Systems. This option checks for the existence of any required operating systems that are needed on the endpoint device.

This option checks for the existence of any required operating systems that are needed on the endpoint device.

The operating system hosts and manages your data, applications, and connected devices. Inadequate protections for the operating system could also affect the performance of all of these components and ultimately affect productivity of your users and the organization.

The following sections describe the supported operating systems and package dependencies for Secure Access posture profiles.

- 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

Describes 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.

This option checks for the existence of a firewall on the endpoint device.

- Windows
  - Require the platform-native firewall to be running on the endpoint device.
- Mac OS X
  - Require the platform-native firewall to be running on the endpoint device.

Endpoint Security Agents

Describes endpoint Security Agents. This option checks for the existence of an endpoint security agent required to be running on the endpoint device.

This option checks for the existence of an endpoint security agent required to be running on the endpoint device.

System Password Enforcement

Describes the endpoint requirement that checks whether a system password is required on the device before applying the access rule.

This option checks whether a system password is required on the endpoint device.

Disk Encryption

Describes 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.

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

Describes the endpoint requirement that checks whether a required web browser is present on the device before applying the rule.

This option checks for the existence of a required web browser on the endpoint device.

Windows Registry Conditions

Describes windows Registry Conditions. This option checks for the existence of a registry key or the value of the registry key on the endpoint device.

This option checks for the existence of a registry key or the value of the registry key on the endpoint device.

File Conditions

Describes 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.

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

Describes process Conditions. This option checks if an application or process is running or not running on the endpoint device.

This option checks if an application or process is running or not running on the endpoint device.

Certificate Conditions

Explains how certificate conditions check that required server certificates are present and valid on an endpoint device before applying the endpoint requirement.

This option checks if any required server certificates are present and valid on the endpoint device.

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.

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.

29 Manage VPN Connection Posture Profiles

Topics:

- Manage VPN Connection Posture Profile

Provides an overview of Manage VPN Connection Posture Profiles in Cisco Secure Access China, including Add a VPN Connection Posture Profile. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage VPN Connection Posture Profile

Provides instructions for managing VPN Connection Posture Profile in Cisco Secure Access China. Posture profiles define requirements for user devices when accessing resources and the network.

Posture profiles define requirements for user devices when accessing resources and the network.

Profiles in this list apply when users access specific resources using VPN. The VPN client must be installed on the end-user device. Requirements are checked when the device connects to the network.

VPN Posture Attributes

- Operating System
- Endpoint security agent
- Windows registry entries
- Firewall
- Disk encryption
- Files
- Processes
- Certificates

Add a VPN Connection Posture Profile

Provides instructions for adding a VPN Connection Posture Profile in Cisco Secure Access China. 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.

Prerequisites

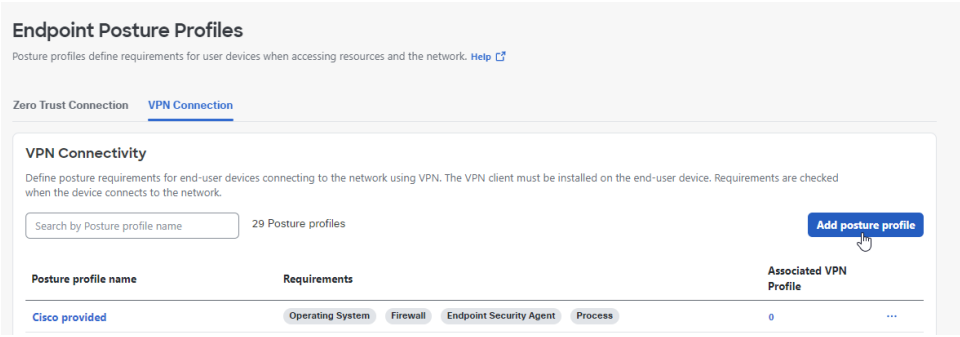
Lists the prerequisites for adding VPN posture profile. Valid credentials for the Secure Access dashboard. Full Admin role in Secure Access. For more information, see Manage Accounts.

- Valid credentials for the Secure Access dashboard.
- Full Admin role in Secure Access. For more information, see Manage Accounts.

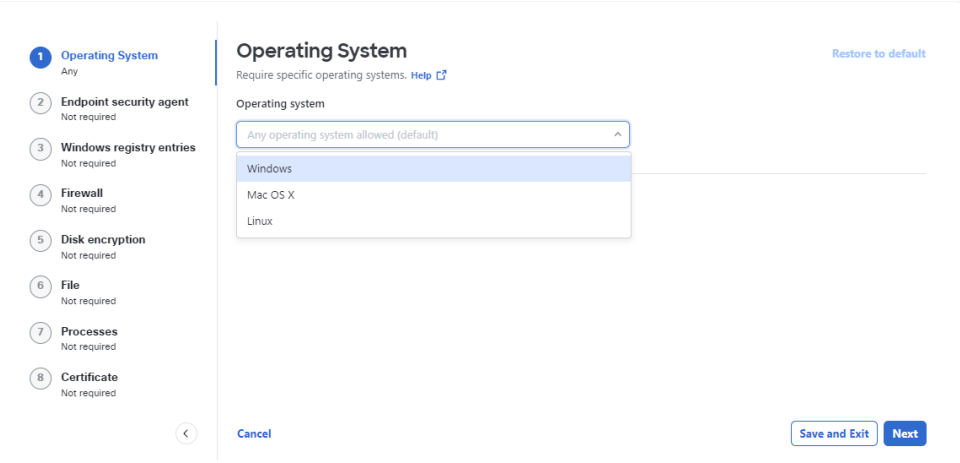
Procedure

Provides instructions for adding VPN posture profile. For VPN Connection , click Add Posture Profile. 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.

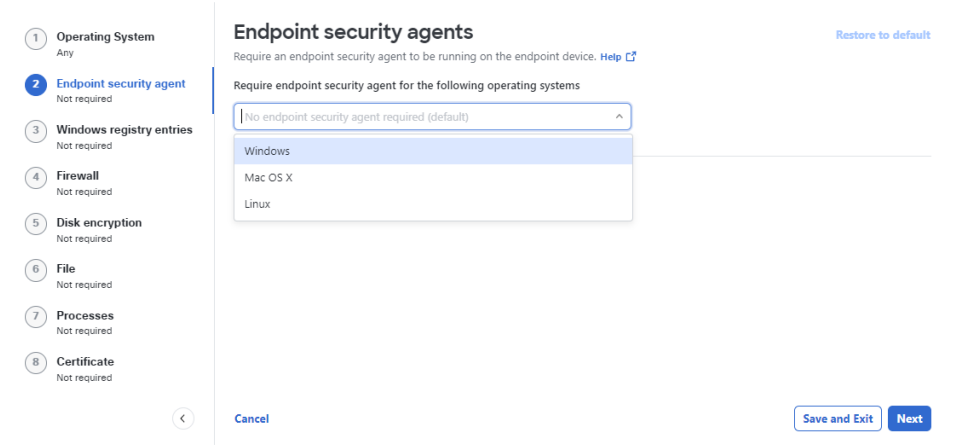
1. Navigate to **Secure > Profiles > Endpoint Posture Profiles**.
2. For **VPN Connection**, click **Add Posture Profile**.



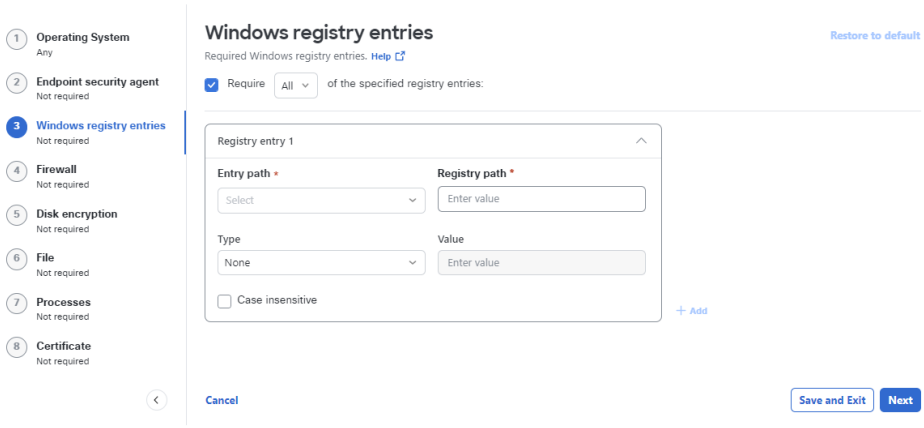
3. Give your posture profile a good descriptive **Name**.
4. For the **Operating System** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select endpoint security agents. See Supported Operating Systems.



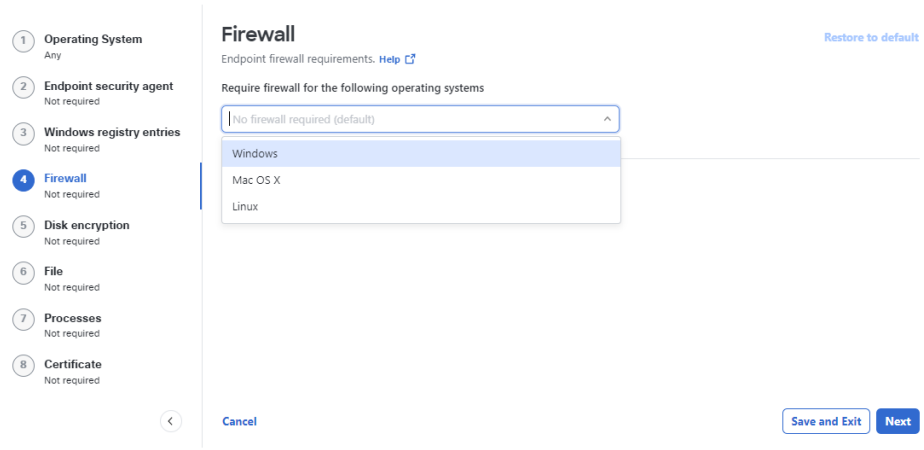
5. For the **Endpoint security agent** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select Windows registry entries. See Endpoint Security Agents.



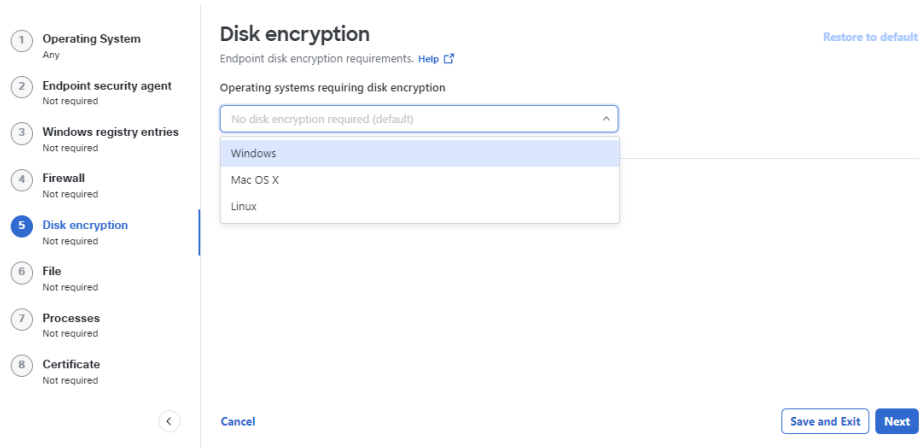
6. For the **Windows registry entries** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select endpoint firewalls. See Windows Registry Entries.



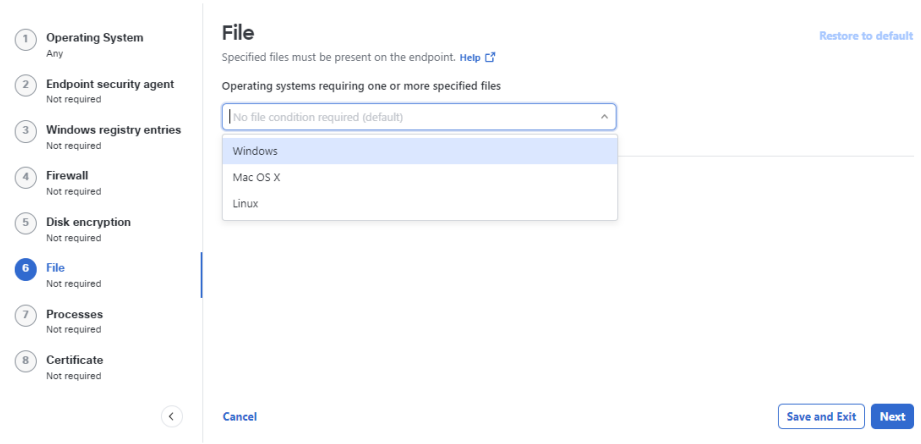
7. For the **Firewall** option, choose the firewall for your profile. Click **Save and Exit** or **Next** to select disk encryption. See Firewall Requirements.



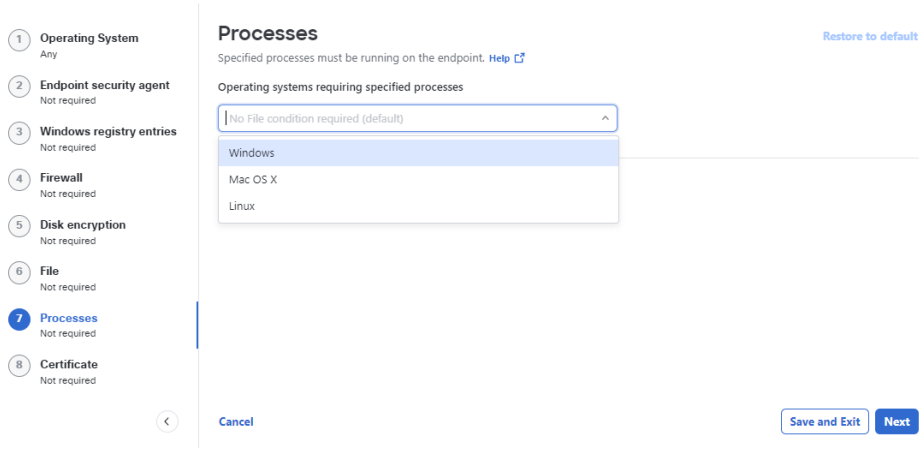
8. For the **Disk encryption** option, choose the disk encryption package(s) for your profile. Click **Save and Exit** or **Next **to configure any OS file requirements. See Disk Encryption.



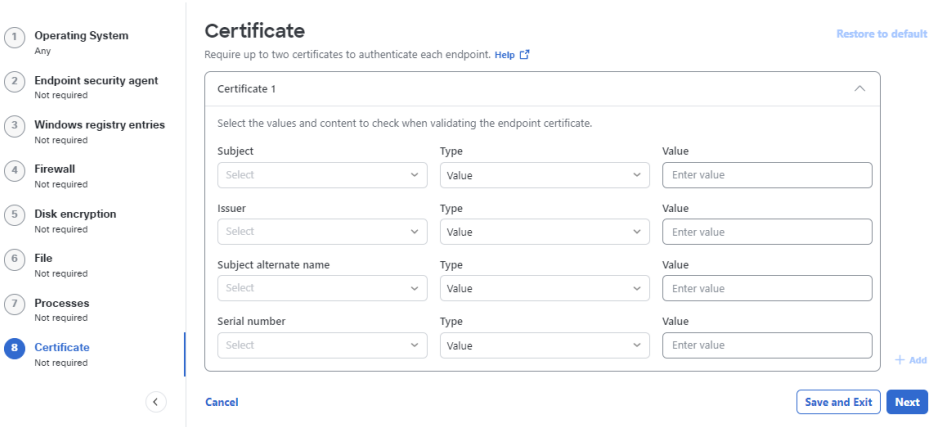
9. For the **File** option, specify any files that are required for the operating system. Click **Save and Exit** or **Next **to configure any OS process requirements. See File Requirements.



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.

30 Manage IPS Profiles

Topics:

- Manage IPS Profiles

Provides an overview of Manage IPS Profiles in Cisco Secure Access China. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage IPS Profiles

Provides instructions for managing IPS Profiles in Cisco Secure Access China. Secure Access's Intrusion Prevention System (IPS) protects your network and assets from known threats.

Secure Access's Intrusion Prevention System (IPS) protects your network and assets from known threats. You define IPS profiles with signature lists that group these threats and allow you to specify how each threat should be handled. You then specify an IPS profile in each access rule.

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

Describes hit Counts. Hit counts represent the amount of times signatures were detected on your network for a certain period.

Hit counts represent the amount of times signatures were detected on your network for a certain period. By default, hit count durations for all lists are set to the last 24 hours. Each list's hit count duration can be changed to the last five minutes, last hour, yesterday, or the last 30 days. Hit counts may also be reset at any time.

Cisco-Provided IPS Signature Lists

Describes Cisco-Provided IPS Signature Lists. 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.

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.

  See Certificates for Internet Decryption.

- Certificates required for decrypting traffic to private destinations.

  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.

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.

31 Manage Web Profiles

Topics:

- Manage Web Profiles
- Enable SafeSearch

Provides an overview of Manage Web Profiles in Cisco Secure Access China, including Enable SafeSearch. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Web Profiles

Provides instructions for managing web Profiles in Cisco Secure Access China. A web profile is a set of security controls and other settings such as acceptable use controls that you configure as a set, then use as a unit in internet access rules.

A web profile is a set of security controls and other settings such as acceptable use controls that you configure as a set, then use as a unit in internet access rules. For example, you can use different web profiles for different sets of users, or for different types of destinations.

You can configure up to 100 web profiles and use each profile in one or more internet access rules.

Secure Access comes with a partially configured web profile; you must either configure that profile to suit your needs or create a different web profile and designate that profile as the default web profile.

To configure web profiles, see detailed information in Add a Web Profile.

Add a Web Profile

Provides instructions for adding a Web Profile in Cisco Secure Access China. A Web profile is a set of security controls and other settings that you can use in internet access rules.

A Web profile is a set of security controls and other settings that you can use in internet access rules. To add a Web profile, navigate to **Secure > Profiles > Web Profiles**.

> **Note**
>
> For detailed information about each of the features you will configure in a web profile, see Manage Web Profiles.

Prerequisites

Lists the prerequisites for adding web profile. Full Admin user role. For more information, see Manage Accounts. Familiarize yourself with the options you will configure in the profile. See Manage Web Profiles.

- Full Admin user role. For more information, see Manage Accounts.
- Familiarize yourself with the options you will configure in the profile. See Manage Web Profiles.
- Configure prerequisite functionality and components that you will select in a web profile:
  - Add a Do Not Decrypt List for Web Profiles
  - Create the list of Threat Categories that you will choose in the web profile.
  - (Optional) Create custom Notification Pages that Secure Access will display when rules that use this web profile match traffic that blocks access or displays a warning. Customizations can include the logo, message, and contact information of your choice.

Procedure

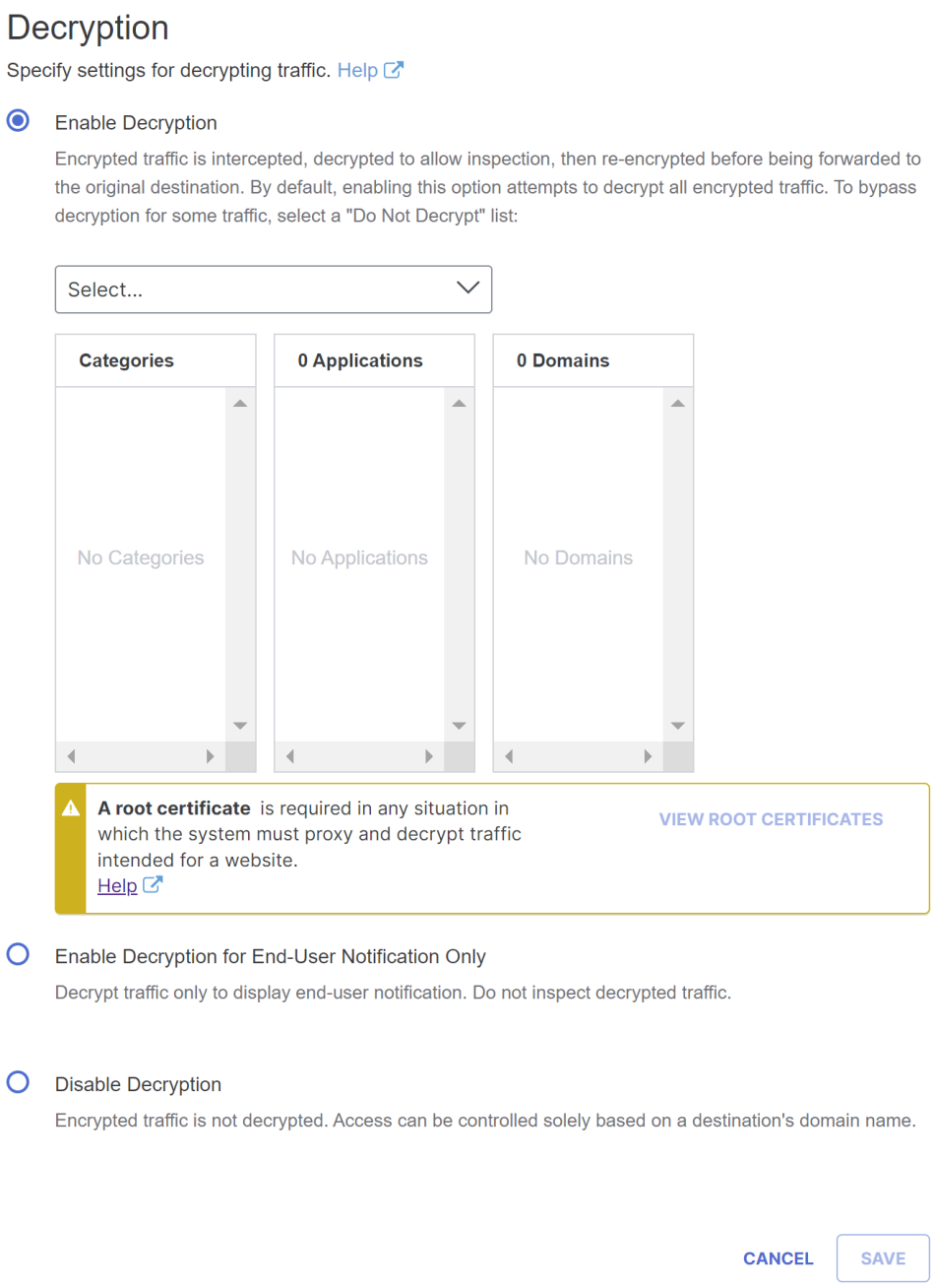
Provides instructions for adding web profile. Navigate to Secure > Profiles > Web Profiles . Click Add. Choose Decryption settings, including a Do Not Decrypt list.

1. Navigate to **Secure > Profiles > Web Profiles**. Click **Add**.
2. Choose Decryption settings, including a Do Not Decrypt list.

   Decryption is required for most web security features to work properly. For more information about decryption, see Manage Traffic Decryption.

For guidance on which option to choose in this section, see Manage Web Profiles.

a. Next to the **Decryption** setting, click **Edit** to modify the setting.



b. Choose a decryption option.

1. **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.
2. **Enable Decryption for End-User Notification Only** - Decrypt traffic only to display end-user notification. Do not decrypt traffic for inspection.

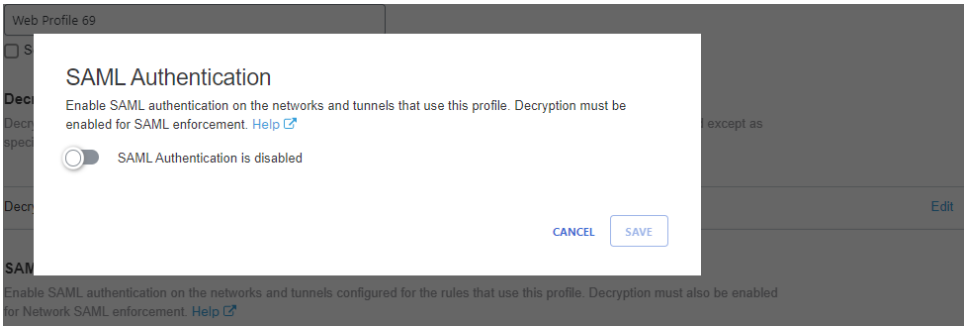
> **Note**
>
> A root certificate is required in any situation in which the system must proxy and decrypt traffic intended for a website.

3. **Disable Decryption** - Encrypted traffic is not decrypted. Access can be controlled solely based on a destination's domain name.

c. If you enabled decryption, choose a Do Not Decrypt list. For more information.

3. Enable or disable SAML Authentication.

a. Next to the **SAML Authentication** setting, click **Edit** to modify the setting. For guidance on which option to choose, see Manage Web Profiles.



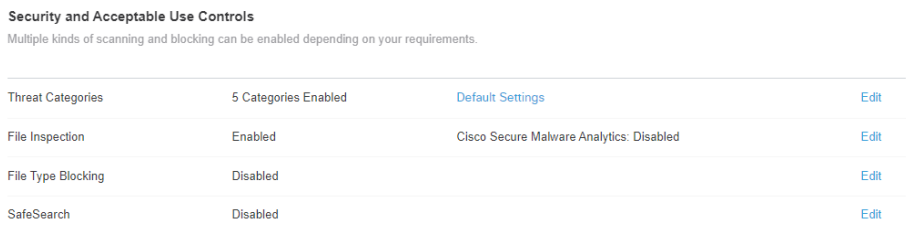
b. Enable or disable the setting.

c. If you enable this option, be sure that decryption is enabled in the same web profile.

4. Configure **Security and Acceptable Use Controls**.

Multiple kinds of scanning and blocking can be enabled depending on your requirements. For links to more details about each, see Manage Web Profiles.

Available controls are:



Click **Edit** beside each setting to choose options.

Choose options:

a. For Threat Categories: Choose from existing lists of threat categories, to block access to known malicious sites and potentially risky sites, based on threat category.

b. For File inspection: Choose the file inspection tool(s) to protect traffic that matches rules that use this web profile.

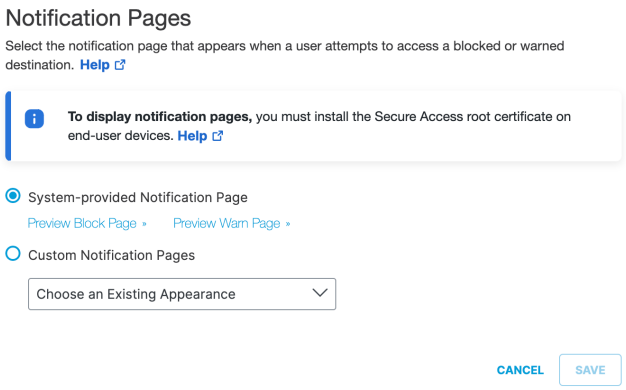
c. For File type blocking: Choose file types to block, even if the original filename extension has been altered. You can enable categories of file type (such as executables or video) and individual file type extensions.

d. For SafeSearch: Enable this option to filter out offensive, explicit, unsafe, and harmful search results in Google, YouTube, Yahoo, and Bing.

5. Configure End-User Notifications

   Block and Warn pages will be displayed in the end-user's web browser, based on the action configured in each rule in which the web profile is used. For more information, see Manage Notification Pages.

6. Next to the **Notification Pages** setting, click **Edit**.



7. Choose one of the two options. Each option includes a Block notification and a Warn notification.
   a. **System-provided Notification Pages**.
   b. **Custom Notification Pages**.
8. If you chose custom pages, choose the pages you want to display.
9. To preview the pages you have selected, click the **Preview** links.
10. Click **Save**.

Next steps

Describes next steps. Configure functionality elsewhere in the product that is needed for your selected features to work. For example:.

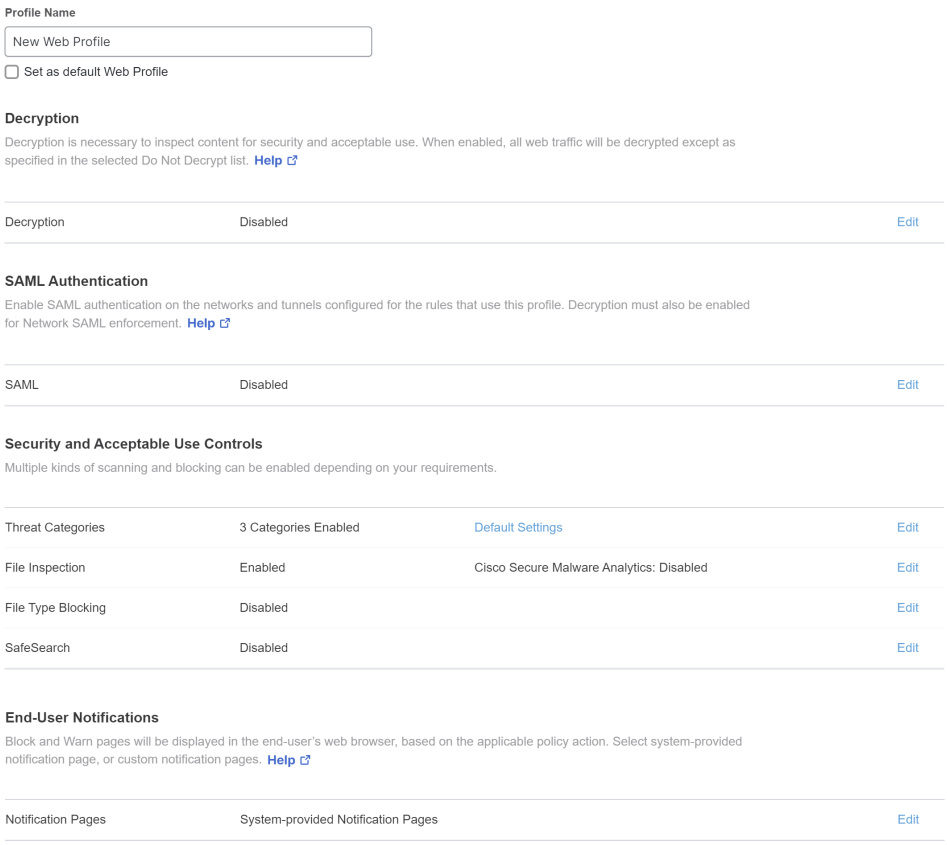
Configure functionality elsewhere in the product that is needed for your selected features to work. For example:

- **Traffic decryption**: Decryption requires certificates. For more information, see Certificates for Internet Decryption.
- **SAML user authentication**: If you will enable this option in a web profile, ensure that SAML authentication is configured for your Secure Access deployment, and enable SAML for the Cisco Secure Client roaming security module. For more information, see Configure Integrations with SAML Identity Providers.
- **Notification pages**: To display notification pages, you must install a Secure Access root CA certificate on all end-user devices. This may not be the same certificate you use for decrypting internet traffic. For more information, see Certificates for Internet Decryption.
- Add the web profile to one or more internet access rules.

Functionality Included in a Web Profile

Describes the settings and security controls available in a web profile and explains how administrators configure web security behavior. for administrators to review.

You can configure various settings and security controls on a web profile.



Decryption

Describes decryption. Decryption is necessary for proper functioning of all features enabled in the web profile. When enabled, all web traffic will be decrypted except as specified in the selected Do Not Decrypt list. For more information about decryption, see Manage Traffic Decryption.

Decryption is necessary for proper functioning of all features enabled in the web profile. When enabled, all web 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 web 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.

SAML Authentication

Describes SAML Authentication. If your organization uses SAML authentication, you should generally enable this option on the networks and tunnels configured for the rules that use this profile.

If your organization uses SAML authentication, you should generally enable this option on the networks and tunnels configured for the rules that use this profile.

Requirements for Enabling SAML Authentication

Describes requirements for Enabling SAML Authentication. Configure SAML authentication to authorize connections to the secure web gateway from user devices on networks and network tunnels. For more information, see Configure Integrations with SAML Identity Providers.

- Configure SAML authentication to authorize connections to the secure web gateway from user devices on networks and network tunnels. For more information, see Configure Integrations with SAML Identity Providers.
- Decryption must also be enabled for network SAML enforcement.

Requirements for Disabling SAML Authentication

Describes requirements for Disabling SAML Authentication. For example, if the rule source includes:. For example, if users should not be identified for privacy or confidentiality reasons, such as by regulation or policy.

- Decryption is disabled in the web profile, or is enabled only for notifications.
- The web 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. These controls include the following:. 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 an access rules.

These controls include the following:

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 anayze files for suspicious behaviors.	Manage File Inspection

Option	Description	More Information
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 an access rules.

End-User Notifications

Describes end-User Notifications. You configure two types of end-user notifications in web profiles:. For details, see Manage Notification Pages. 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 web profiles:

- 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 details, see Manage Notification Pages.

Enable SafeSearch

Provides instructions for enabling safeSearch in Cisco Secure Access China. SafeSearch is a search engine filter that blocks search results for explicit content such as pornography, violence, gore, and other offensive adult content.

SafeSearch is a search engine filter 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 enduser device for any applicable search engine or site.

Enable SafeSearch

Provides instructions for enabling safesearch. When you enable SafeSearch in a web profile, you must also enable decryption in the same web profile. For more information, see Manage Traffic Decryption.

When you enable SafeSearch in a web profile, you must also enable decryption in the same web profile. For more information, see Manage Traffic Decryption.

To enable SafeSearch and decryption, see Add a Web Profile.

Confirm That SafeSearch is Working

Provides instructions for confirming that safesearch is working. Tests must be done through a source that is included in an access rule that is configured to use a web profile in which SafeSearch is enabled.

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.

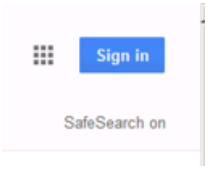
Tests must be done through a source that is included in an access rule that is configured to use a web profile in which SafeSearch is enabled.

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.

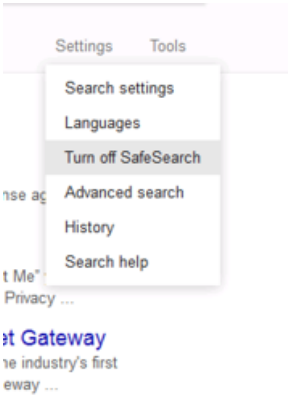
After attempting a search in Google, a **SafeSearch on** indicator should be displayed.

Figure 1: google_safeseach.png



In the browser, under **Settings**, if you select **Turn off SafeSearch**, it has no effect and explicit sites are not listed in searches.

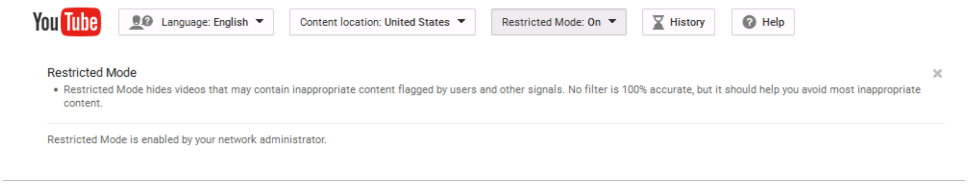
Figure 2: turnoff_safesearch.png



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".

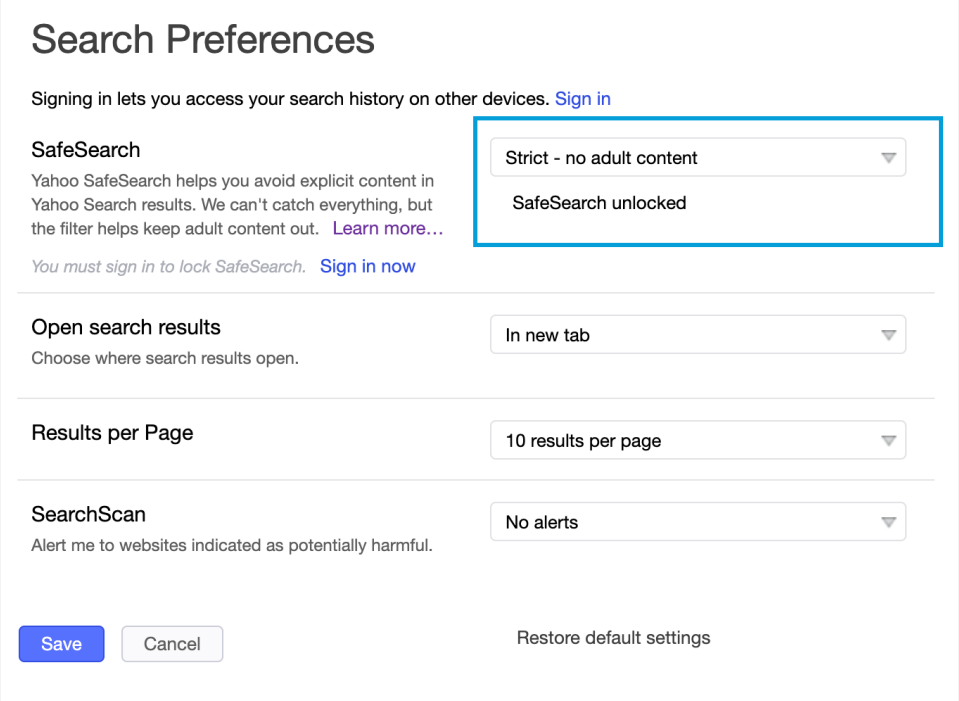


Yahoo

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.

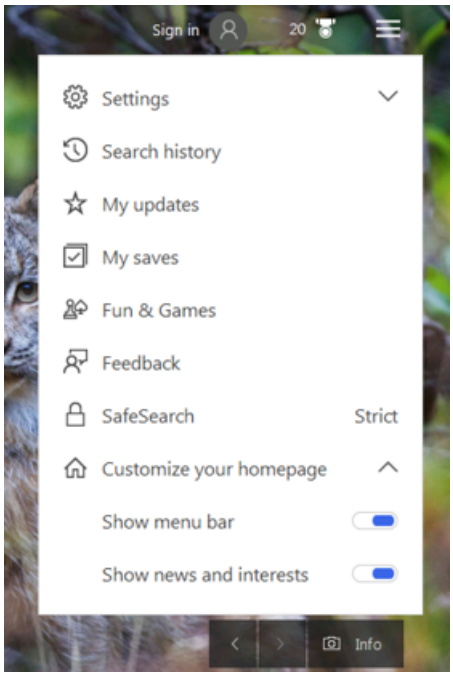


Bing

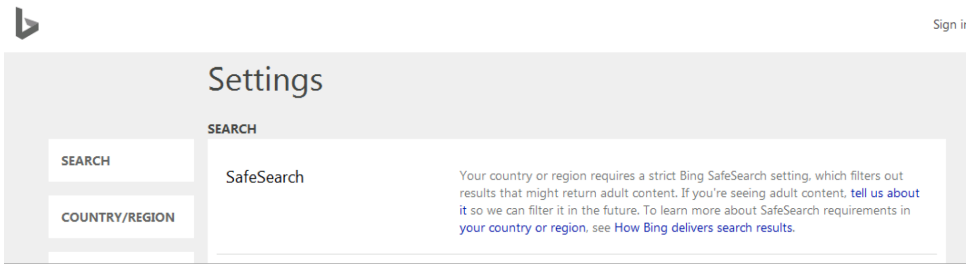
Describes bing. From the menu icon, Bing displays that SafeSearch is set to “Strict”. Clicking SafeSearch takes you to a page describing SafeSearch, but there is no disable option.

From the menu icon, Bing displays that SafeSearch is set to “Strict”.

Figure 3: safesearch_bing.png



Clicking **SafeSearch** takes you to a page describing SafeSearch, but there is no disable option.


Sign i
Settings
SEARCH
SEARCH
COUNTRY/REGION
SafeSearch
Your country or region requires a strict Bing SafeSearch setting, which filters out results that might return adult content. If you're seeing adult content, tell us about it so we can filter it in the future. To learn more about SafeSearch requirements in your country or region, see How Bing delivers search results.

32 Manage Threat Categories

Topics:

- Manage Threat Categories

Provides an overview of Manage Threat Categories in Cisco Secure Access China, including Threat Category Descriptions, Add a Threat Category List, and Dispute a Threat Categorization. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Threat Categories

Provides instructions for managing threat Categories in Cisco Secure Access China. 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 web profile, then specify a web profile in each internet access rule.

For a list of all threat categories and a description of each, see Threat Categories.

Threat Category Descriptions

Describes Threat Category Descriptions in Cisco Secure Access China. Malware—Blocks requests to access servers hosting malware and websites compromised through any application, protocol, or port.

- **Malware**—Blocks requests to access servers hosting malware and websites compromised through any application, protocol, or port. Recommended.
- **Command Control Callbacks**—Prevents compromised devices from communicating with command and control servers through any application, protocol or port. Also, this setting helps identify potentially infected machines on your network. Recommended.
- **Phishing Attacks**—Blocks access to fraudulent websites that are designed to steal personal information. Recommended.
- **Potentially Harmful Domains**—Blocks access to domains that exhibit suspicious behavior and may be part of an attack.
- **Newly Seen Domains**—Blocks access to domains that are being queried through Secure Access for the first time and for which Secure Access has not yet seen a client lookup. Not all new domains are necessarily harmful; blocking access to this category may block access to legitimate sites.
- **Dynamic DNS**—Blocks access to sites that host dynamic DNS content. Not all sites in this category are necessarily harmful; blocking access to this category may block access to legitimate sites.
- **DNS Tunneling VPN**—Blocks VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These services can be used to bypass corporate policies regarding access and data transfers.
- **Cryptomining**—Blocks access to crypto mining pools where "miners" group together and share resources—processing power—to better gather and share cryptocurrencies. Also blocks known web crypto mining source code repositories.

Add a Threat Category List

Provides instructions for adding a Threat Category List in Cisco Secure Access China. You can create different threat category lists to use in different web profiles, which you can then use in different internet access rules.

You can create different threat category lists to use in different web 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.

Prerequisites

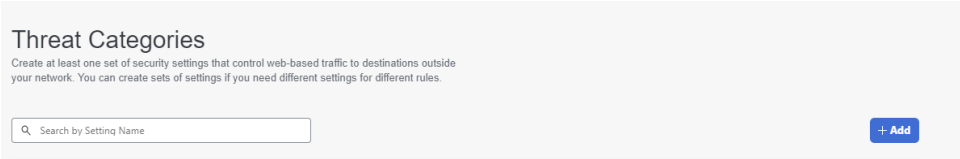
Lists the prerequisites for adding threat category set, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

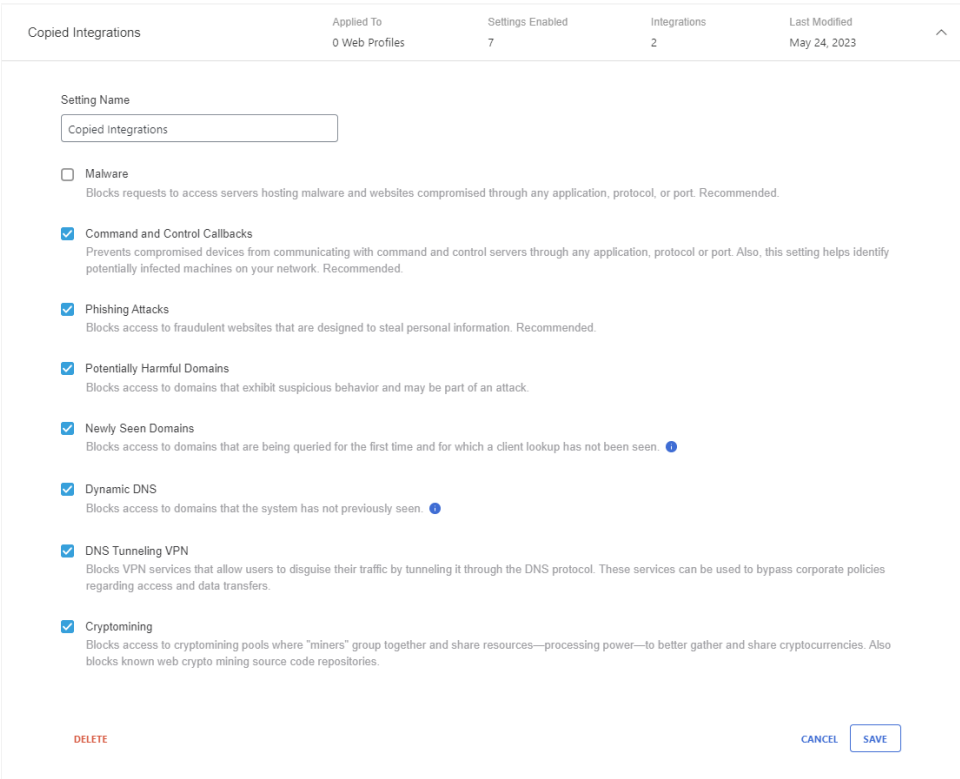
Provides instructions for adding threat category set. Navigate to Secure> Settings > Threat Categories and click Add. Give your setting a good descriptive Setting Name.

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 Web profile.

Dispute a Threat Categorization

Describes Dispute a Threat Categorization in Cisco Secure Access China. When a destination is classified in a category which you disagree with, you can dispute the categorization.

When a destination is classified in a category which you disagree with, you can dispute the categorization. Secure Access and Technical Assistance Center (TAC) share a unified set of threat categories. You can submit a category dispute request through your sales representative.

Default Threat Category List

Describes default Threat Category List. A default threat category list ships with Secure Access. This default list is included in the default web profile and by default in all web profiles that you create.

A default threat category list ships with Secure Access. This default list is included in the default web profile and by default in all web 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 web profiles.

The following threat categories are enabled in the threat categories list that is included by default in web profiles: Malware, Command Control Callbacks, and Phishing.

Reporting on Threat Category Access Attempts

Describes reporting on Threat Category Access Attempts. When traffic is blocked based on one of these categories, Secure Access generates a reporting event.

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 web profile selected for your rule, it is still reported as an allowed visit to a destination that matches one of the threat categories.

33 Manage File Inspection

Topics:

- Manage File Inspection

Provides an overview of Manage File Inspection in Cisco Secure Access China, including Enable File Inspection, Test File Inspection, and Monitor File Inspection Activity. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage File Inspection

Provides instructions for managing file Inspection in Cisco Secure Access China. Protect your network from malicious files using file inspection.

Protect your network from malicious files using file inspection.

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 File Inspection for evaluating files for malicious content:

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.

Enable File Inspection

Provides instructions for enabling file Inspection in Cisco Secure Access China. To inspect files for threats, enable the file inspection features in a web profile, then assign the web profile to an internet access rule.

To inspect files for threats, enable the file inspection features in a web profile, then assign the web profile to an internet access rule.

File Inspection uses multiple features to evaluate for malicious files. For details, see Manage File Inspection.

Once inspections are complete, a file is either delivered to the end user or the connection is terminated and the user is shown a block page.

Once you have enabled File Inspection, to monitor and review Umbrella's inspection activities, use the Security Activity and Activity Search reports.

Prerequisites

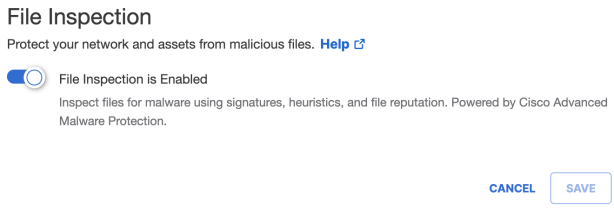
Lists the prerequisites for enabling file inspection. Full Admin user role. For more information, see Manage Accounts. Determine which options you want to enable. For details, see Manage File Inspection.

- Full Admin user role. For more information, see Manage Accounts.
- Determine which options you want to enable. For details, see Manage File Inspection.
- Certificates are required to decrypt traffic and detect files, and to display block notifications. For more information, see Certificates for Internet Decryption.

Procedure

Provides instructions for enabling file inspection. Enable File Inspection if it is not already enabled:. Navigate to Secure > Profiles > Web Profiles.

1. Navigate to **Secure > Profiles > Web Profiles**.
2. Click **+Add** or expand an existing web 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. In the same Web profile, ensure that Decryption is enabled.
7. Choose a Web profile that has file inspection enabled when you configure internet access rules.

Test File Inspection

Provides instructions for testing file Inspection in Cisco Secure Access China. After setting up file inspection, we recommend that you check your configured web profile and internet access rules.

After setting up file inspection, we recommend that you check your configured web profile and internet access rules. You can evaluate File Inspection by pointing your browser to one of our test files.

Prerequisites

Lists the prerequisites for testing file analysis. To ensure that the traffic is not blocked by other security features, test the web 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.

- 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 web profile with File Inspection enabled.

  To ensure that the traffic is not blocked by other security features, test the web 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 testing file analysis. Browse to one of Cisco's EICAR test files. Clear text test file. Encrypted test file.

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.

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 blocking page diagnostic information. 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.

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.

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). If a file is malware, Secure Access returns a block page. The block page diagnostic information lists the `Server` as `mps`.

Monitor File Inspection Activity

Provides instructions for monitoring file Inspection Activity in Cisco Secure Access China. There are several places to monitor file inspection activity.

There are several places to monitor file inspection activity.

Monitor and Review File Inspection

Provides instructions for monitoring and review file inspection. To review inspection activity at any time, use the Security Activity and Activity Search reports.

To review inspection activity at any time, use the Security Activity and Activity Search reports.

Troubleshoot and Monitor File Inspection

Provides instructions for troubleshooting and Monitor File Inspection in Cisco Secure Access China. It explains the sequence of actions and relevant settings presented in the procedure.

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 web profile that has file inspection 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).

Overview of Configuring File Inspection

Describes overview of Configuring File Inspection. To configure these features:. Enable file inspection in a web profile and configure the features.

To configure these features:

- Enable file inspection in a web profile and configure the features
- Ensure that decryption is enabled in the web profile
- Configure block notification pages and choose the applicable page in the web profile
- Associate the web profile with an internet acces rule. See Manage Web 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)

Describes Cisco Advanced Malware Protection (AMP). When File Inspection is enabled, Secure Access uses AMP to scan for malicious files.

When File Inspection is enabled, Secure Access uses AMP to scan for malicious files.

AMP is built on an extensive collection of real-time threat intelligence and dynamic malware analytics supplied by the Talos Security Intelligence and Research Group 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

Describes antivirus Scanner. When File Inspection is enabled, an antivirus scanner attempts to scan all files. The system begins streaming large files from the proxy to the user after scanning up to 50 MB to ensure that the user starts receiving the download while scanning continues in the background.

When File Inspection is enabled, an antivirus scanner attempts to scan all files. The system begins streaming large files from the proxy to the user after scanning up to 50 MB to ensure that the user starts receiving the download while scanning continues in the background. If a file is identified as malicious, the connection is immediately terminated. For larger files, the user may initially experience a brief lag, but should still receive the entire file as quickly as normal—unless it's malicious. Secure Access only scans the first 50 MB and does not scan the content of any files over 50 MB. For more information on file scanning size, see Limitations and Range Limits.

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.

34 Manage File Type Controls

Topics:

- Manage File Type Controls

Provides an overview of Manage File Type Controls in Cisco Secure Access China, including Enable File Type Controls, File Types to Block, and Review File Type Controls Through Reports. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage File Type Controls

Provides instructions for managing file Type Controls in Cisco Secure Access China. Cisco Secure Access provides security use controls in the Web profile.

Cisco Secure Access provides security use controls in the Web 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

Provides instructions for enabling file Type Controls in Cisco Secure Access China. Cisco Secure Access provides security use controls in the Web profile.

Cisco Secure Access provides security use controls in the Web profile. One of the security controls–File Type Blocking–defines access to certain types of files. Once **File Type Blocking** is enabled, if a user device attempts to download a selected file type, Secure Access presents a Block page instead of the requested resource.

Secure Access checks a file based on its file extension and detects whether the extension has been changed. For example, if a .gif file extension is changed to .xyz, Secure Access can detect that the file is a .gif.

> **Note**
>
> Blocking some file types may cause a website not to display correctly.

Prerequisites

Lists the prerequisites for enabling file type control. Full Admin user role. For more information, see Manage Accounts. You must enable decryption in the same Web profile.

- Full Admin user role. For more information, see Manage Accounts.
- You must enable decryption in the same Web profile.

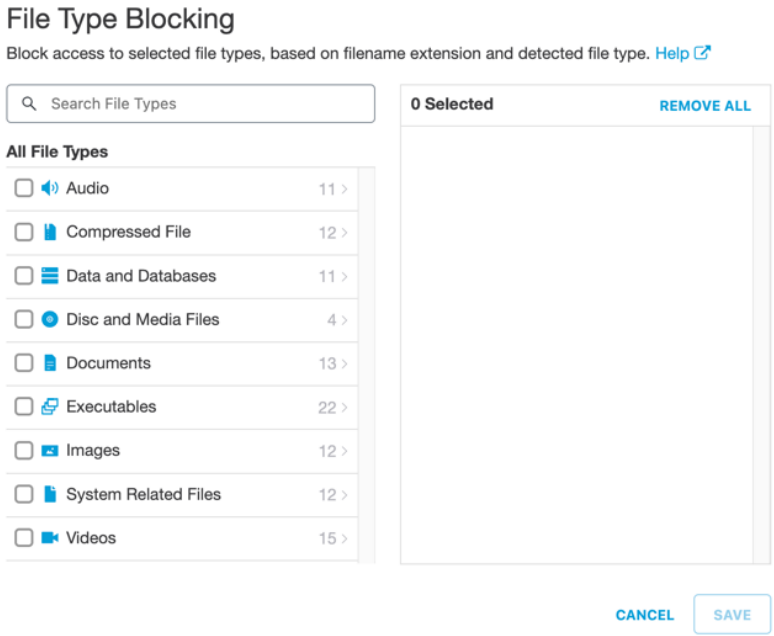
Procedure

Provides instructions for enabling file type control. Use this web profile in an access rule to apply it to traffic.

1. Navigate to **Secure > Web Profiles**.
2. Add a web profile or expand an existing web profile.
3. For **Security and Acceptable Use Controls > File Type Blocking**, click **Edit**.

4. 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 this web profile in an access rule to apply it to traffic.

File Types to Block

Describes File Types to Block in Cisco Secure Access China. You can block the following file types in a Web profile.

You can block the following file types in a Web profile.

Audio	Compressed	Data and Database	Disc and Media	Documents	Executable	Image	System-related	Video
aif	7z	csv	dmg	doc	apk	ai	bak	avi
cda	arj	dat	iso	docm	bat	bmp	cab	flv
m4a	deb	db	toast	docx	bin	gif	cpl	gat
mid	gz	log	vcd	dotm	cgi	ico	cur	h264
mp3	pak	mdb		pdf	com	jpeg	drv	m4v
mpa	pkg	nzb		pop	dll	jpg	emu	mkv
ram	rar	sav		potm	exe	png	icns	mov
snd	rar	sql		pptx	hta	ps	ini	mp4
wav	rpm	tar		rtf	jar	psd	ps1	mpeg
wma	tar.gz	torrent		tex	js	rm	scr	qtm
wpl	tbz			xls	moo	svg	sys	rm
	z			xlsm	msi	tif	tmp	rv
	zip			xlsx	pif	tiff		ssm
					pl			vob
					prg			wmv
					py			
					sh			
					swf			
					vb			
					vbs			
					vm			
					wsf			

Review File Type Controls Through Reports

Describes Review File Type Controls Through Reports in Cisco Secure Access China. File types enabled through Web profiles are listed in the Activity Search Report.

File types enabled through Web profiles are listed in the Activity Search Report.

Prerequisites

Lists the prerequisites for reviewing file type controls through reports. A minimum user role of Read-only. For more information, see Manage Accounts.

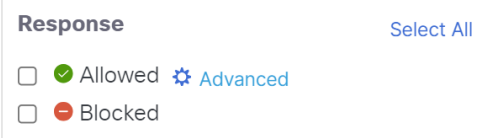
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

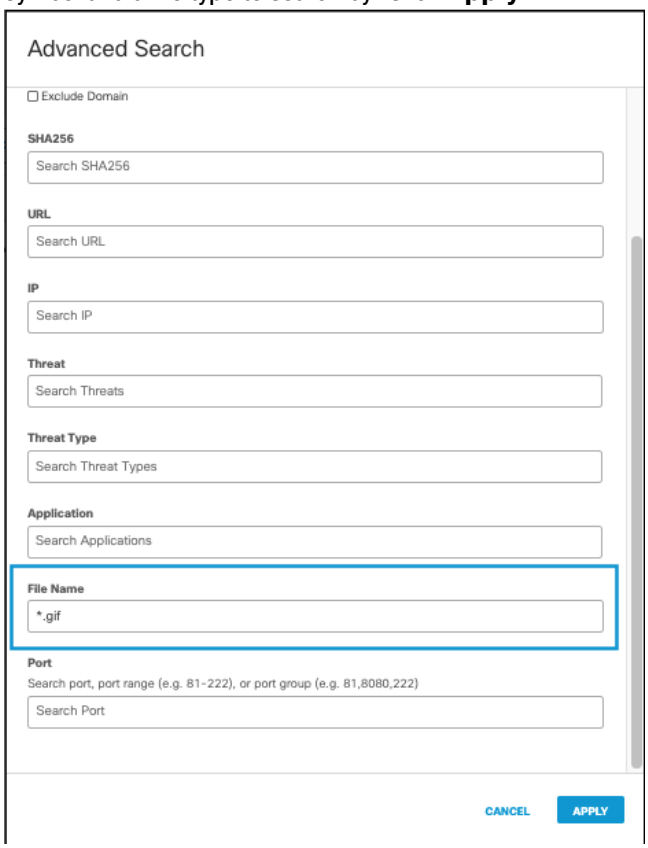
Provides instructions for reviewing file type controls through reports. The results will filter by events where files of that type were blocked.

1. Navigate to **Monitor > Activity Search**.

2. Under the **Response** filter, choose **Blocked**.

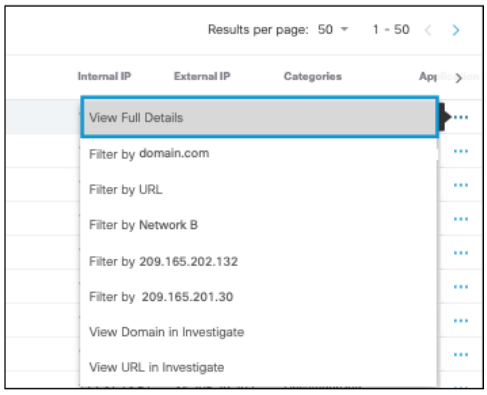


3. Click **Advanced** in the search bar to bring up the Advanced search. Under **File Name**, enter the asterisk wildcard symbol and a file type to search by. Click **Apply**.

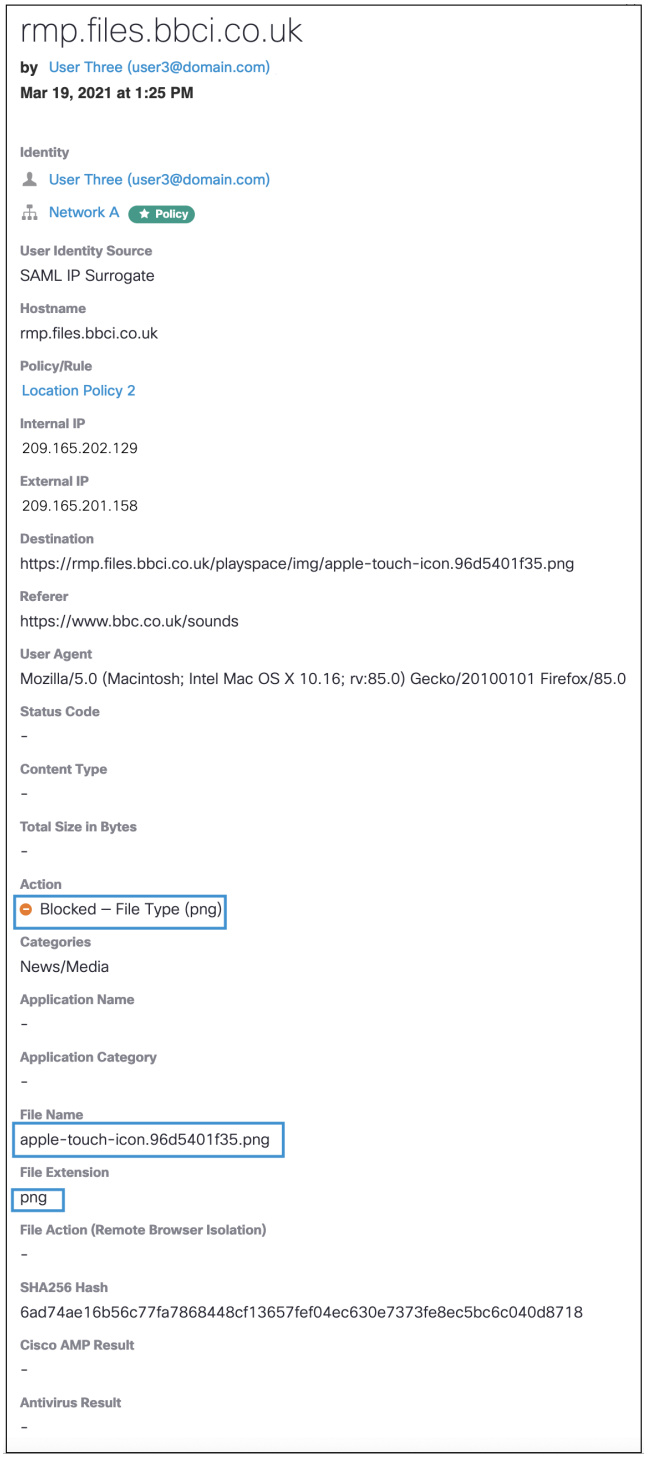


The results will filter by events where files of that type were blocked.

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.

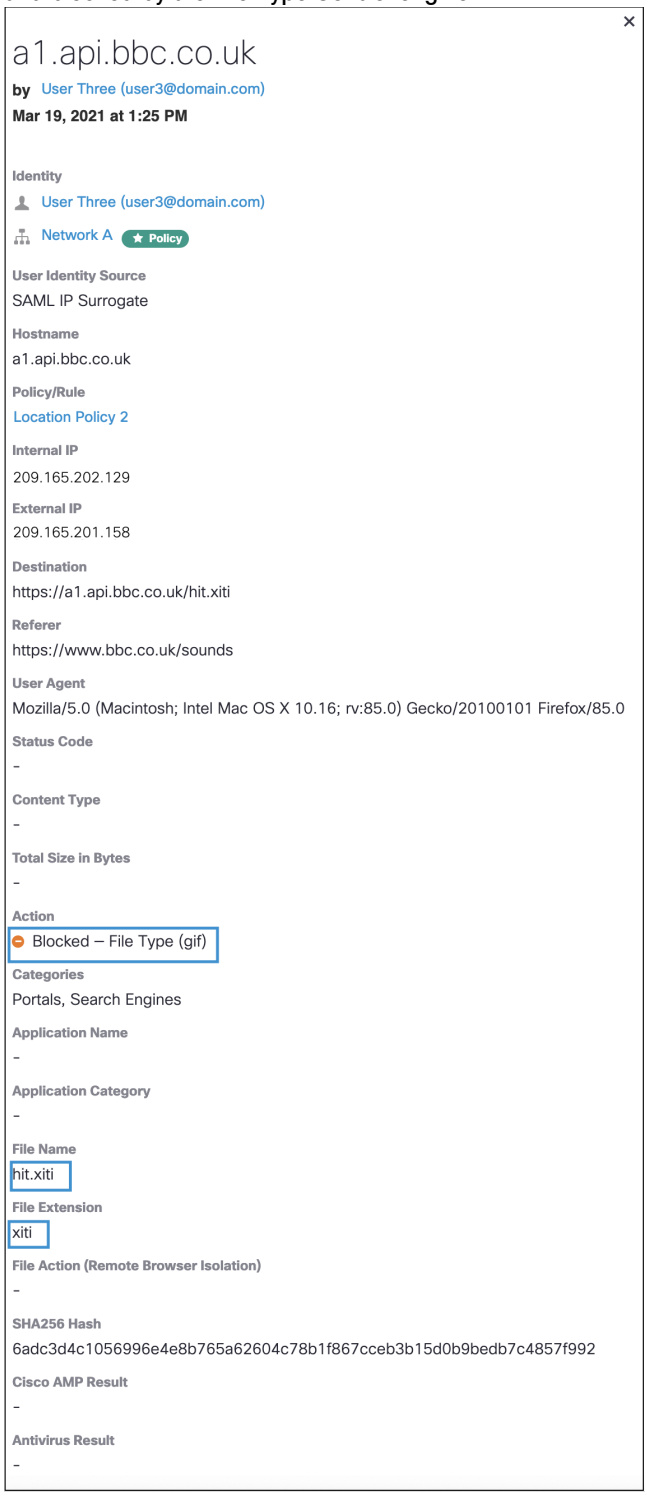


In cases where the file extension is displayed in the file extension column but does not match the extension shown against the file type block control action, the file type control block action should be trusted because it is more accurate and based on the detection engine.

For example, the file extension listed here is shown as a *.xiti*.

News/Media	https://rmp.files.bbci.co.uk/playspace/js/vendors-sounds.0dcc01359227adc46...	js	Allowed	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
News/Media	https://rmp.files.bbci.co.uk/playspace/img/apple-touch-icon.96d5401f35.png	png	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129

When you examine the details, however, you discover that the file type is actually a *.gif*, which was successfully detected and blocked by the File Type Control engine.



35 Manage Notification Pages

Topics:

- Manage Notification Pages

Provides an overview of Manage Notification Pages in Cisco Secure Access China, including Preview Notification Pages, Create Custom Block and Warn Pages, and Allow Users to Contact an Administrator. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Notification Pages

Provides instructions for managing notification Pages in Cisco Secure Access China, including To view notification pages displayed to end users, To display custom notification pages to end users, and Warn Pages: More Information. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access displays notification pages to end users when users try to:

- Access a destination that is blocked by web 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 web profile is associated with a single notification page configuration that includes both Block and Warn pages.

Preview Notification Pages

Describes Preview Notification Pages in Cisco Secure Access China and outlines Prerequisites and Procedure. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

There are several places to preview notification pages. Use this procedure to preview default and custom pages from a web profile.

Prerequisites

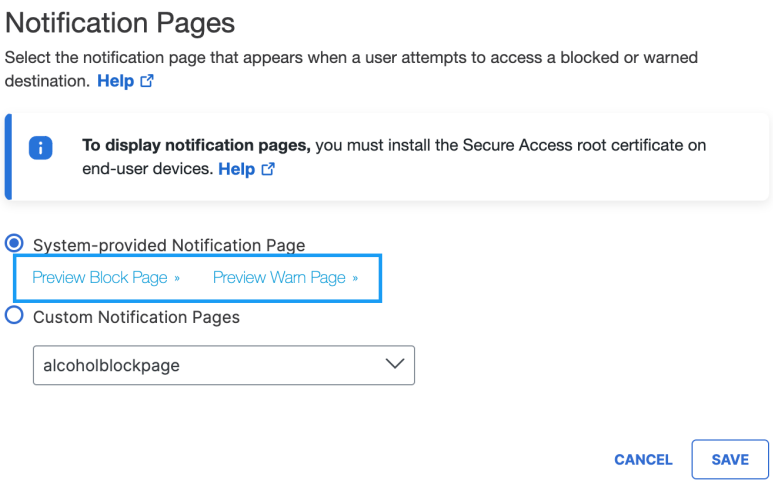
Lists the prerequisites for preview notification pages, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

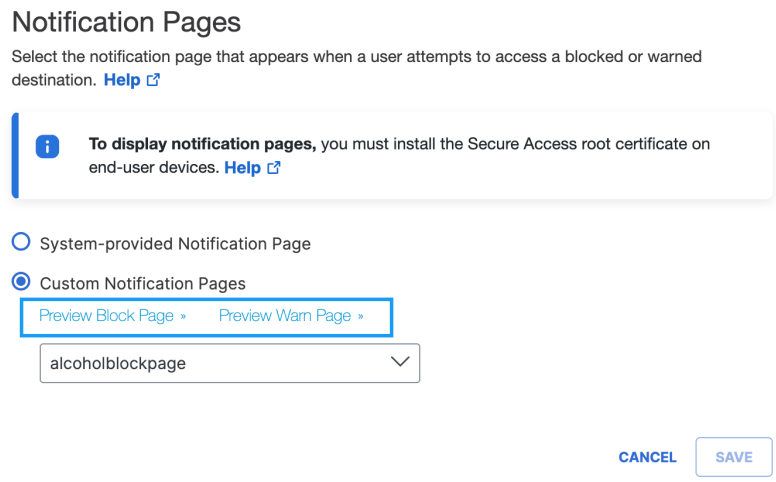
Procedure

Provides instructions for preview notification pages. Navigate to Secure > Profiles > Web Profiles. Scroll down to End-User Notifications and click Edit.

1. Navigate to **Secure > Profiles > Web Profiles**.
2. Click **Add**.
3. Scroll down to **End-User Notifications** and click **Edit**.
4. To preview the default notification pages:
   a. Make sure **System-provided Notification Pages** is selected.
   b. Click the blue Preview links (one each for Block and Warn pages.)



5. To preview a custom notification page:
   a. Select **Custom Notification Pages**.
   b. Choose the notification page design you want to preview.
   c. Click the blue Preview links (one each for Block and Warn pages.)



You can also preview notification pages on the **Secure > Settings > Notification Pages** page.

Create Custom Block and Warn Pages

Provides instructions for creating custom Block and Warn Pages in Cisco Secure Access China. 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 a Web profile.

Prerequisites

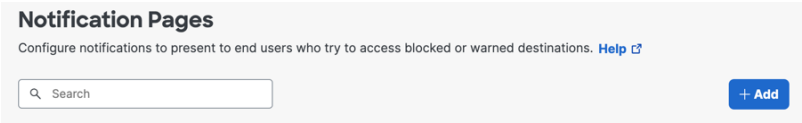
Lists the prerequisites for creating a custom block page. Full Admin user role. For more information, see Manage Accounts. Gather your logo, help desk email address, and any other information you want to provide.

- 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: PNG and JPEG are supported. Images larger than 125x70 pixels will be cropped and resized.

Create Custom Block and Warn Pages

Provides instructions for creating custom block and warn pages. If this is a new configuration, name this set of notification pages.

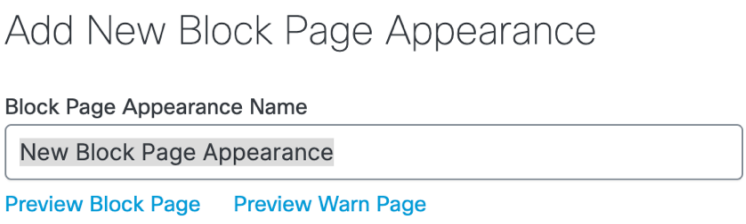
1. Navigate to **Secure > Settings > Notification Pages**.
2. Click **+Add**, or expand the setting you want to edit. The settings on the page are optional.



3. If this is a new configuration, name this set of notification pages.
4. Provide a logo. Secure Access notification pages support PNG and JPEG. Images larger than 125x70 pixels will be cropped and resized.
5. If you want to allow end users to contact an administrator from a block message, provide the email address that user messages will be forwarded to. For more information, see .Allow Users to Contact an Administrator on page 442
6. Expand **Block Page Appearance**.
   a. If you want to display a unique message based on the reason for the block, click **Differently** and click a Block reason.
   b. Click **Show a block page with a custom message**.
   c. 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.
7. Expand **Warn Page Appearance**.
   a. Click **Show a warn page with a custom message**.
   b. 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.

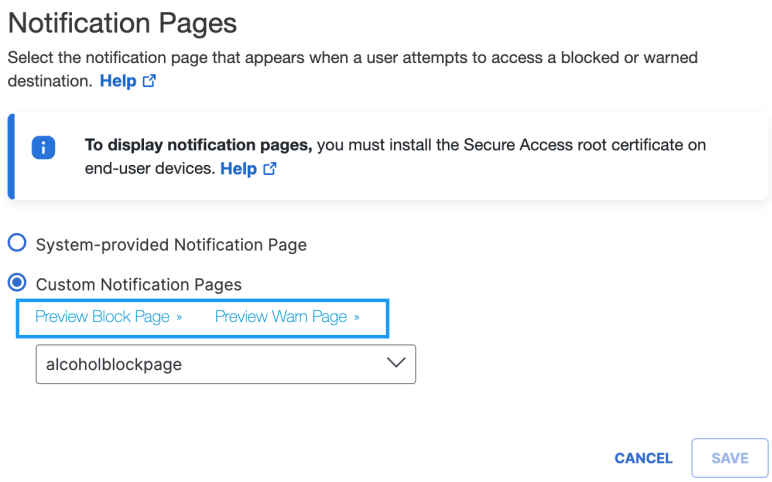


9. Click **Save**.

Link a Custom Notification Page Appearance to a Web Profile

Describes link a Custom Notification Page Appearance to a Web Profile. Navigate to Secure > Profiles > Web Profiles and expand the profile you'd like to link.

1. Navigate to **Secure > Profiles > Web 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**.

Next Steps

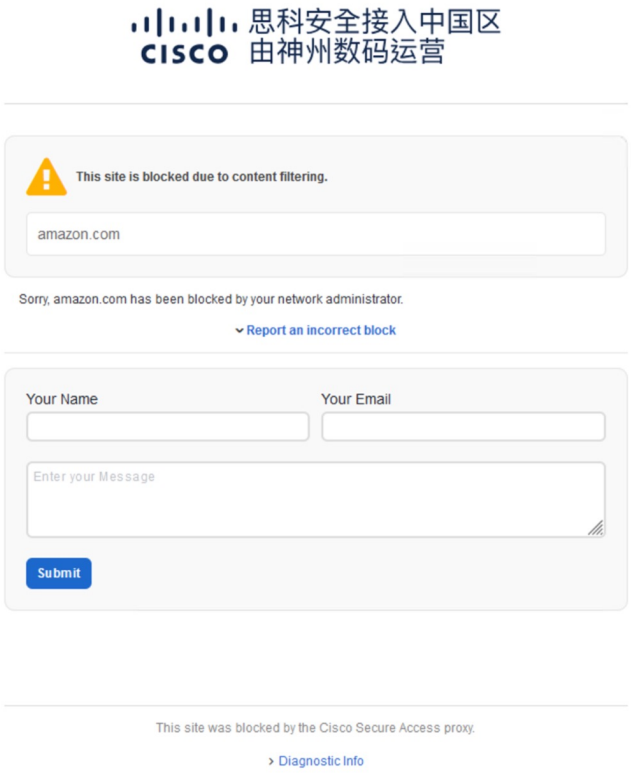
Outlines the next steps for completing custom notification pages, including the remaining requirements described in Manage Notification Pages. for administrators to review.

Complete the remaining requirements described in Manage Notification Pages.

Allow Users to Contact an Administrator

Provides instructions for allowing users to Contact an Administrator in Cisco Secure Access China. 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.

Prerequisites

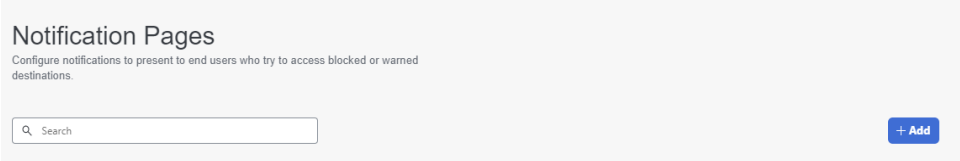
Lists the prerequisites for allowing users to contact an administrator. Full Admin user role. For more information, see Manage Accounts.

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

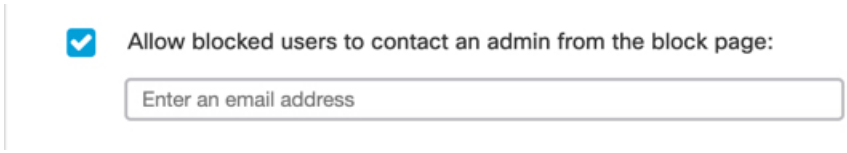
Procedure

Provides instructions for allowing users to contact an administrator. The following is an example of an email sent to an administrator when a user sent a message from a block page:.

1. Navigate to **Secure > Settings > Notification Pages** and click the setting you want to edit.

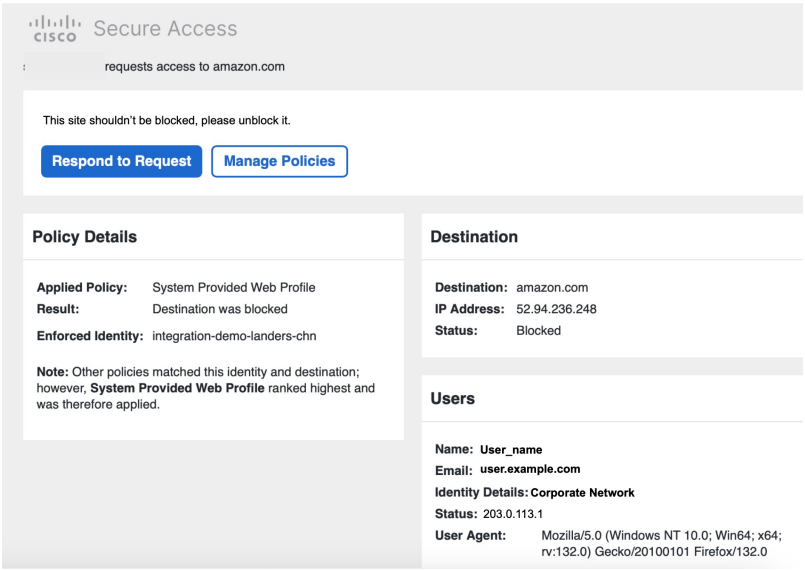


2. Select **Allow blocked users to contact an admin from the block page** to allow end-users to contact an administrator from your organization. You can only add one email.



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:



To view notification pages displayed to end users:

Describes to view notification pages displayed to end users:. See Preview Notification Pages. You can view the default and any custom pages.

- See Preview Notification Pages.
- You can view the default and any custom pages.

To display custom notification pages to end users:

Describes to display custom notification pages to end users:. If user devices do not have the necessary certificate, users will see standard browser error when they try to access a blocked destination.

- 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 web profiles to use custom notification pages. See Add a Web Profile.
- In the default web profile, choose the block and warn pages to display when traffic matches internet access rules that use the default web profile. To choose a default web profile, see Edit Rule Defaults and Global Settings.
- Configure internet access rules to use the web 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.

Warn Pages: More Information

Describes warn Pages: More Information. 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.

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

Describes 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.

The notification pages described in this section do not apply to private access rules. See Manage Private Access Rules.

36 Manage Traffic Decryption

Topics:

- Manage Traffic Decryption

Provides an overview of Manage Traffic Decryption in Cisco Secure Access China, including Important Information About Do Not Decrypt Lists and Add a Do Not Decrypt List for Web Profiles. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Traffic Decryption

Provides instructions for managing traffic Decryption in Cisco Secure Access China. Decryption is used for various purposes in Secure Access.

Decryption is used for various purposes in Secure Access. You will configure decryption when you configure those features.

Important Information About Do Not Decrypt Lists

Describes Important Information About Do Not Decrypt Lists in Cisco Secure Access China. Traffic that is not decrypted cannot be effectively inspected for threats.

Traffic that is not decrypted cannot be effectively inspected for threats.

However, in order to comply with confidentiality regulations in some locations, certain traffic should not be decrypted. You can use Do Not Decrypt lists to specify these destinations.

Do Not Decrypt lists apply only to destinations in internet access rules, and they are used for both web security and intrusion prevention (IPS) features.

Currently, IPS profiles and web profiles support Do Not Decrypt lists differently:

- All IPS profiles use a single Do Not Decrypt list.
- Each web 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 China. 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 web 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 web 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 web 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 web security features, or you can create additional do-not-decrypt

lists for use in web 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 web profile. See Add a Do Not Decrypt List for Web 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. Initially, this list is empty. Add the destinations that are important to your organization.

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 Web Profiles

Provides instructions for adding a Do Not Decrypt List for Web Profiles in Cisco Secure Access China. 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 web 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.

Prerequisites

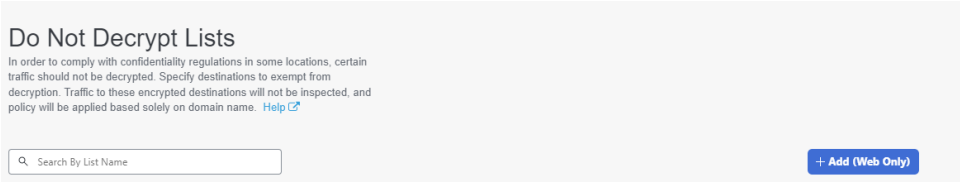
Lists the prerequisites for adding web selective decryption list, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

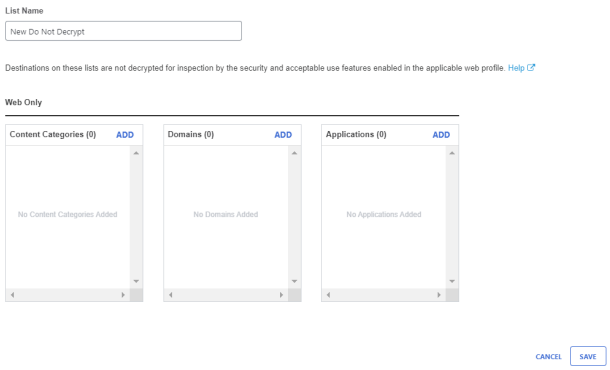
Procedure

Provides instructions for adding web selective decryption list. Navigate to Secure > Settings > Do Not Decrypt Lists and click Add.

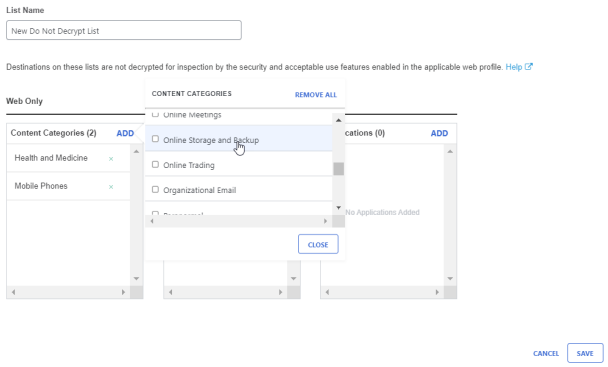
1. Navigate to **Secure > Settings > Do Not Decrypt Lists** and click **Add**.



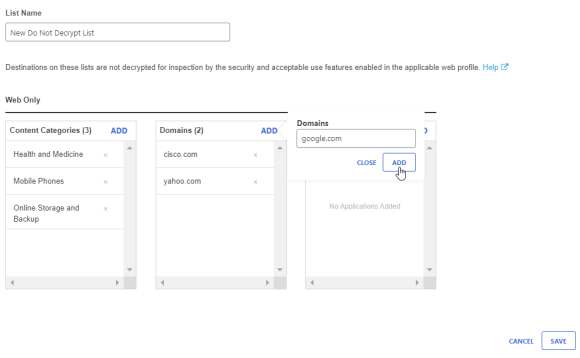
2. Give your list a good descriptive **List Name**.



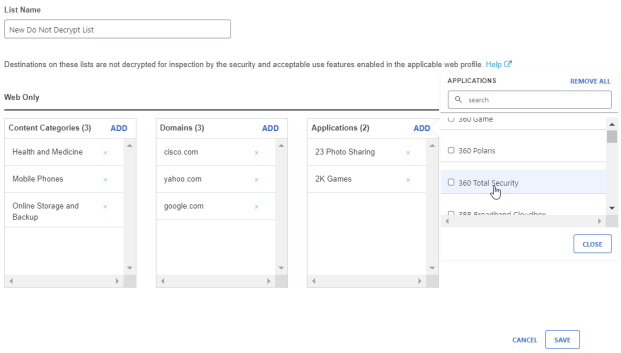
3. Add content categories, applications, and domains that will be exempt from decryption:
   a. **Click Add, select Categories to be exempt from HTTPS inspection and then click Close.**



   b. Click **Add**, add a **Domain** to exempt it from HTTPS inspection and then click **Add**.



   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 Web profiles to the Access policy.

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.

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 web profiles)

  Decryption is required for inspection by the security and acceptable use features.

- File inspection and enforcement of file type controls

  See Manage File Inspection and Manage File Type Control.

- Destinations that are derived from SAML configurations

- Displaying block and warning notifications to end users

  When a destination triggers a warning page, users can only access that destination by clicking the link in the warning notification. See Manage Notification Pages.

- 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:. Traffic to confidential internet destinations, based on laws, regulations, or policy.

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:. Do Not Decrypt Lists for Web Profiles. This setting affects decryption for Intrusion Prevention (IPS) only.

Decryption-specific settings appear in the following components:

- Web profile
- Do Not Decrypt Lists for Web Profiles
- Private Resource
- Global Settings

  This setting affects decryption for Intrusion Prevention (IPS) only.

  It applies to both private and internet destinations.
- 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.

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.

37 Manage Certificates

Topics:

- Manage Certificates

Provides an overview of Manage Certificates in Cisco Secure Access China, including Certificates for Internet Decryption, Install the Cisco Secure Access Root Certificate, and Add Customer CA Signed Root Certificate. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Certificates

Provides instructions for managing certificates in Cisco Secure Access China, including Certificate Installation Methods. It explains the sequence of actions and relevant settings presented in the procedure.

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.

Certificates for Internet Decryption

Describes Certificates for Internet Decryption in Cisco Secure Access China and outlines Certificates for Displaying Notifications, Certificates for Decrypting Internet Traffic, and Option 1: Distribute Self-Signed Certificates to End-User Devices. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Certificates are required for secure internet access. Specifically, certificates are required to decrypt traffic in order to inspect it for threats, and to present notifications to end users when access is blocked or triggers a warning. Web security features and the intrusion prevention (IPS) feature all require decryption in order to be effective.

End-user devices that connect to resources through Secure Access must trust the connection with Secure Access. You must set up certificates to establish this trust.

For internet traffic, depending on the features you need, there are two ways for end-user devices to validate the certificate that Secure Access presents to end-user devices that connect to internet resources through Secure Access:

1. You can install the self-signed Secure Access certificate into the browser trust stores of all end-user endpoint devices, or
2. You can sign the Secure Access certificate using your corporate certificate authority (CA) so that it can be validated by an existing certificate in the trust store of end-user devices. This method also allows you to easily revoke the certificate if needed, without having to update all end-user devices.

Certificates for Displaying Notifications

Describes certificate distribution for displaying notifications and explains the option to distribute self-signed certificates to end-user devices. for administrators to review.

You can use only this method:

- Option 1: Distribute Self-Signed Certificates to End-User Devices

Certificates for Decrypting Internet Traffic

Describes certificates for Decrypting Internet Traffic. You can use either of these methods:. Option 1: Distribute Self-Signed Certificates to End-User Devices.

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

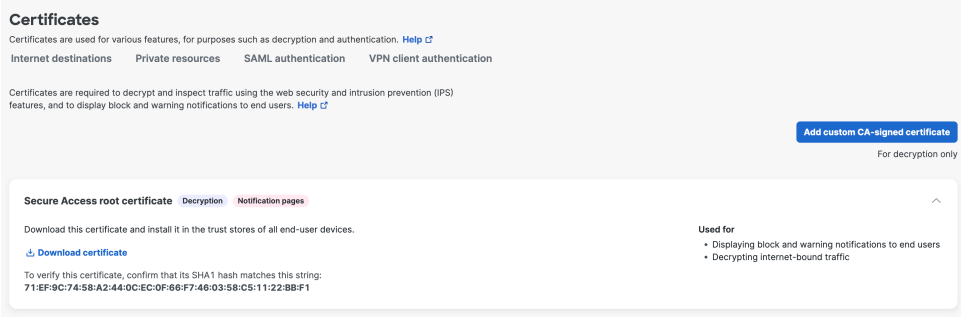
Describes option 1: Distribute Self-Signed Certificates to End-User Devices. Download the Secure Access certificate. Install the downloaded certificate in the trust store of all devices in your organization.

Prerequisites

- 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. This certificate cannot be used to display notifications. For more information, see Add Customer CA Signed Root Certificate .

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

Provides instructions for 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.

Prerequisites

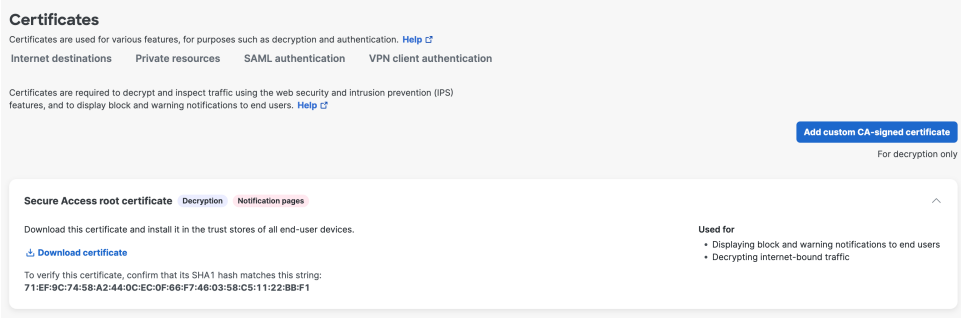
Lists the prerequisites for installing the Cisco Secure Access root certificate. You must have administrative privileges on the devices in the organization or network administrative permissions over the network.

- You must have administrative privileges on the devices in the organization or network administrative permissions over the network.
- Full Admin user role. For more information, see Manage Accounts.

Download the Cisco Secure Access Root Certificate

Provides instructions for downloading the Cisco Secure Access root certificate. Navigate to Secure > Certificates > Internet destinations , and then expand Secure Access root certificate.

1. Navigate to **Secure** > **Certificates** > **Internet destinations**, and then expand **Secure Access root certificate**.



2. Click **Download certificate** to download the **Cisco_Secure_Access_CN_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 Prerequisites.

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_CN_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**.

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.s for managing Group Policy.

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 Prerequisites.

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_CN_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**.

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

Provides instructions for 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.

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 Prerequisites.

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 Prerequisites.

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.

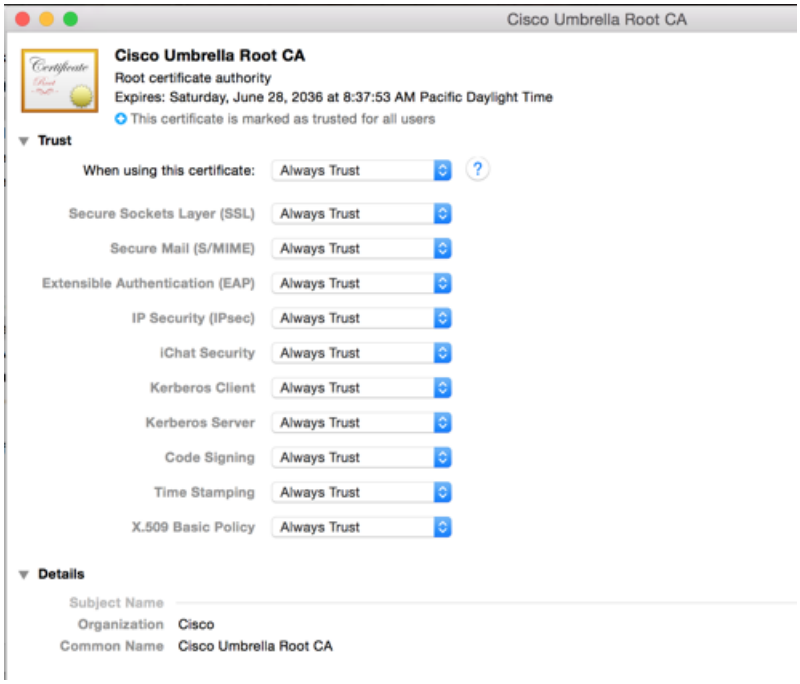
   To interact with the Firefox certificate store from the command line, use the **certutil** tool from the NSS Tools package. For more information, see Using the Certificate Database Tool.

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 Prerequisites.

Before you begin, download the Cisco Secure Access root certificate. See Prerequisites.

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 Prerequisites.

1. 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 Prerequisites.

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_CN_Root_CA.cer** file and click **Open**.
7. Select **Trust this CA to identify Websites**.
8. Click **OK**.

Add Customer CA Signed Root Certificate

Provides instructions for adding customer CA Signed Root Certificate in Cisco Secure Access China. 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 China.

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 China.

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 China 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 China 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 China.

Prerequisites

Lists the prerequisites for adding customer ca signed root certificate. A Certificate Signing Request (CSR) file downloaded from Secure Access China.

- A Certificate Signing Request (CSR) file downloaded from Secure Access China.
- Microsoft Certificate Services, Active Directory Certificate Services, or OpenSSL to sign the CSR with your CA.

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 China 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

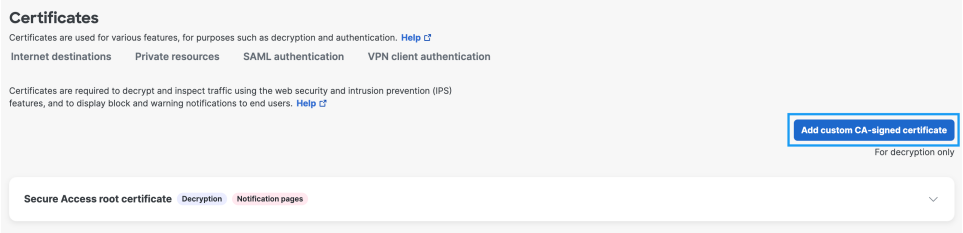
Provides instructions for installing root certificate in browsers. For information about how to install certificates in browsers, see Install the Cisco Secure Access Root Certificate.

For information about how to install certificates in browsers, see Install the Cisco Secure Access Root Certificate.

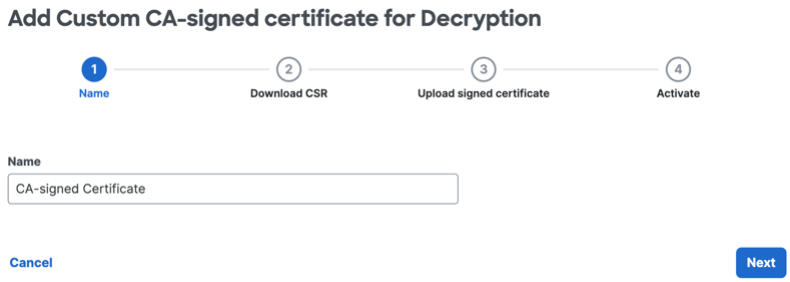
Procedure

Provides instructions for adding customer ca signed root certificate. Navigate to Secure > Settings > Certificates and click the Internet destinations tab. Click Add custom CA-signed certificate.

1. Navigate to **Secure > Settings > Certificates** and click the **Internet destinations** tab. Click **Add custom CA-signed certificate**.



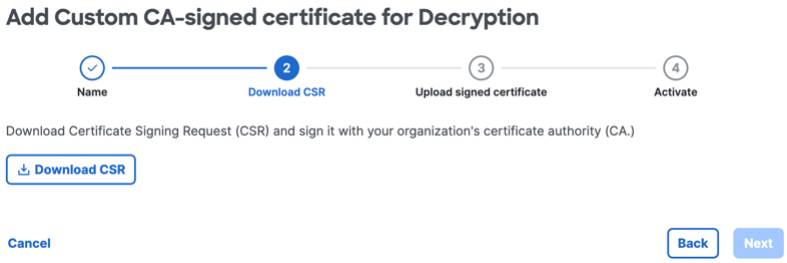
2. Enter a descriptive name for your certificate, and then click **Next**.



3. Click **Download CSR** to save the Secure Access Certificate Signing Request (.csr) file to the local system, and then click **Next**.

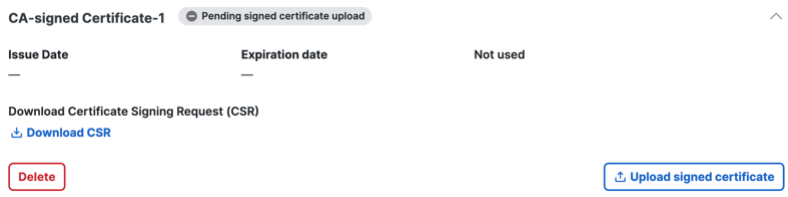
   Use a tool such as Microsoft Certificate Services or OpenSSL to sign the CSR with your corporate certificate signing authority (CA).

> **Note**
>
> You must download the Secure Access China CSR file to complete the step.



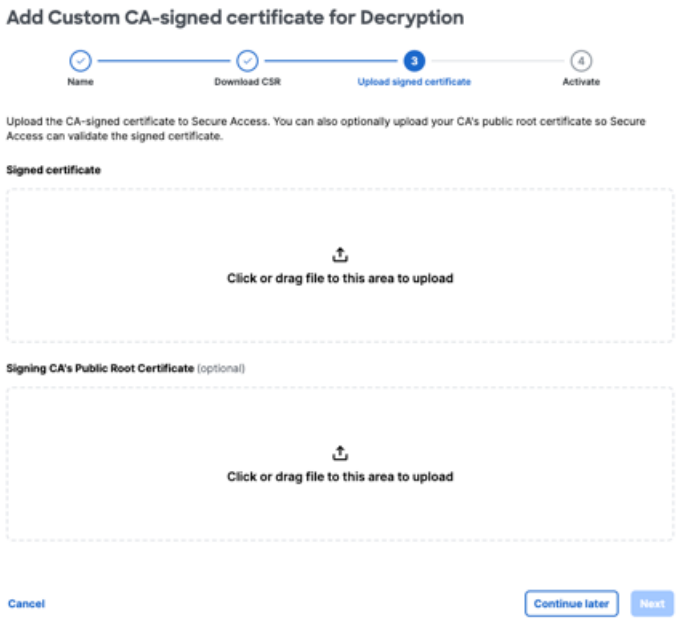
4. Sign the downloaded CSR file with your corporate certificate authority (CA).
5. Once you have signed the downloaded .csr file, click **Upload signed certificate**.

   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 China CSR or drag the signed certificate file onto Secure Access China, and then click **Next**.

   You can optionally also upload your signing certificate authority's public root certificate to Secure Access China. This allows Secure Access China 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 China, and then click **Start using for decryption**.

View the Cisco Trusted Root Store

Provides instructions for viewing the Cisco Trusted Root Store in Cisco Secure Access China. A root certificate is required when Secure Access proxies and decrypts HTTPS traffic intended for a website.

A root certificate is required when Secure Access proxies and decrypts HTTPS traffic intended for a website. Cisco provides trusted root store bundles, which contain information about certificates used by Cisco products. Within a bundle, you can view the list of trusted Cisco Certification Authorities (CA), type of root certificate, and certificate fingerprint (SHA-1).

The Secure Access trusted root certificate information is stored in the Cisco Trusted Union Root bundle. The Cisco Trusted Union Root bundle is a PKCS#7 bundle file (.p7b). The Cisco Trusted Union Root bundle is signed with a digital signing certificate, which you use to verify the bundle.

Prerequisites

Lists the prerequisites for viewing Cisco trusted root store. You must have administrative privileges on the devices in the organization or network administrative permissions over the network.

- You must have administrative privileges on the devices in the organization or network administrative permissions over the network.
- Use a version of OpenSSL v1.0 or greater to extract the root bundle.

Download the Cisco Trusted Union Root Bundle

Provides instructions for downloading the cisco trusted union root bundle. Navigate to the Cisco Cryptographic Services site at Cisco PKI: Policies, Certificates, and Documents.

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

Provides instructions for extracting certificate files from a bundle so they can be reviewed and used in certificate configuration for Secure Access China.

Step 1: Extract the Signing Certificate

Describes 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.

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

Provides instructions for extracting PEM-formatted certificates from a certificate bundle as part of preparing certificates for Secure Access configuration. for administrators to review.

```
# 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

Provides instructions for generating individual certificate files from a certificate bundle for use in Secure Access certificate configuration. for administrators to review.

Linux

Describes Linux endpoint support and summarizes the platform context for deploying or configuring Cisco Secure Client on Linux devices. for administrators to review.

```
# 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

Describes macOS endpoint support and summarizes the platform context for deploying or configuring Cisco Secure Client on macOS devices. for administrators to review.

```
# 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

Provides instructions for 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 Certificates for Private Resource Decryption

Provides instructions for managing certificates for Private Resource Decryption in Cisco Secure Access China. Secure Access's Intrusion Prevention System (IPS) can protect your private resources.

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.

Prerequisites

Lists the prerequisites for managing certificates private resource decryption, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

- 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.

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.

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.

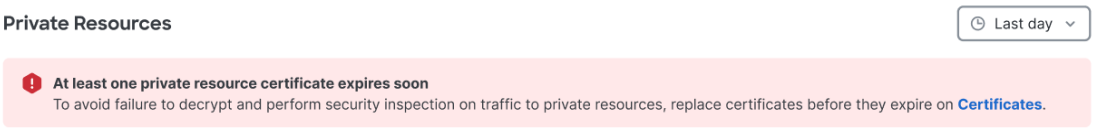
Procedure

Provides instructions for managing certificates used to decrypt traffic to private resources and support certificate-based inspection in Secure Access China.

View Notifications About Expired Private Resource Certificates

Provides instructions for 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 Option 2: Upload a certificate and key to the Certificates page on page 467, 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.

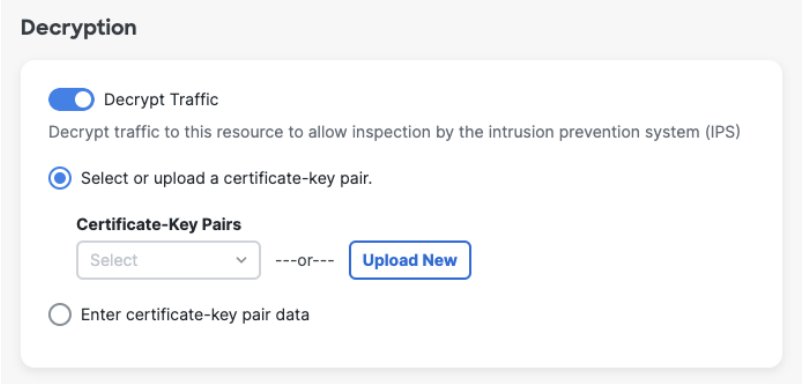
Upload Private Resource Certificates

Provides instructions for uploading certificates for private resources so Secure Access China can use them for private resource connectivity and inspection.

Option 1: Upload or enter a certificate-key pair directly to the private resource

Describes option 1: Upload or enter a certificate-key pair directly to the private resource. Navigate to Resources > Private Resources.

1. Navigate to **Resources > Private Resources**.
2. Click an existing private resource or add a new private resource.
3. Scroll down to **Decryption**.
4. Enable the **Decrypt Traffic** field. The certificate-key configuration options are displayed.

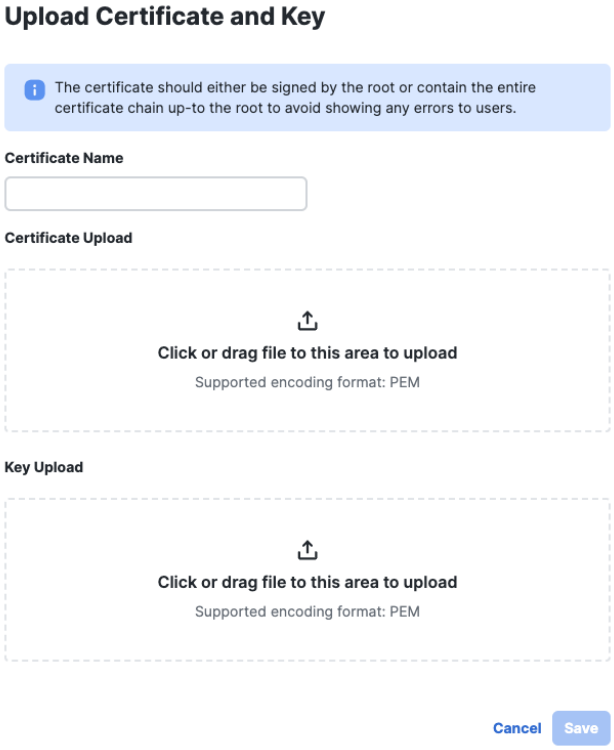


5. Select an existing certificate, upload a new certificate, or paste certificate values.
6. Click **Save**.

Option 2: Upload a certificate and key to the Certificates page

Describes option 2: Upload a certificate and key to the Certificates page. Navigate to Secure > Settings > Certificates and click Private resources.

1. Navigate to **Secure > Settings > Certificates** and click **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.

Certificates for Private Resource Decryption

Describes Certificates for Private Resource Decryption in Cisco Secure Access China. 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 in Cisco Secure Access China. 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—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

Provides instructions for managing SAML Certificates for Service Providers in Cisco Secure Access China. 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:

- Networks and network tunnels protected by Internet Security
- Virtual Private Networks (VPNs) with a configured VPN profile

Prerequisites

Lists the prerequisites for certificates SAML service providers. 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.

- 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

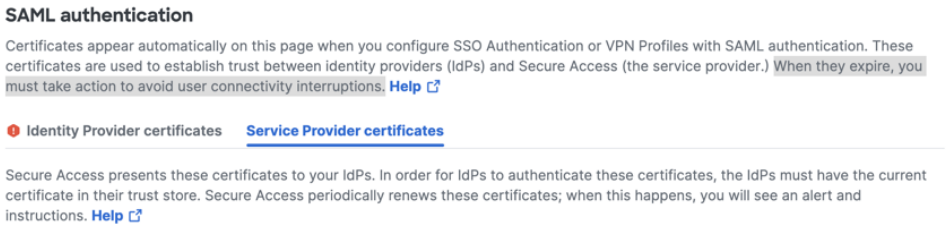
Provides instructions for certificates SAML service providers. Download service provider certificates. View notifications about the expiration of Secure Access certificates that are deployed in SAML IdP integrations and VPN Profiles.

- Download service provider certificates.
- View notifications about the expiration of Secure Access certificates that are deployed in SAML IdP integrations and VPN Profiles.

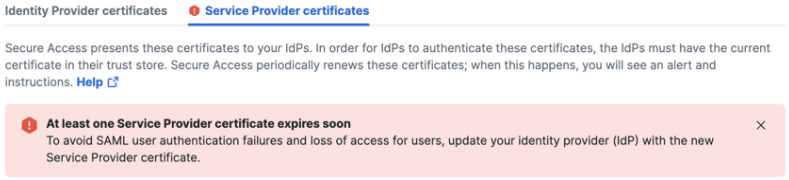
View Notifications About Expired Service Provider Certificates

Provides instructions for viewing notifications about expired service provider certificates. Navigate to Secure > Certificates > SAML authentication > Service Provider Certificates.

1. Navigate to **Secure > Certificates > SAML authentication > Service Provider Certificates**.



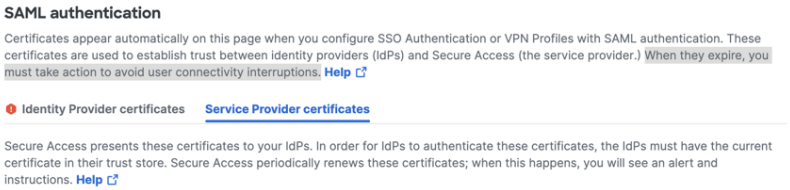
2. Secure Access displays any notifications about certificates that may expire.



Download Web Security Service Provider Certificates

Provides instructions for downloading web security service provider certificates. For Automatic Configuration , copy the Automatic Certificate Updates URL and upload the Secure Access XML Metadata file to your SAML IdP.

1. Navigate to **Secure > Certificates > SAML authentication > Service Provider Certificates**.



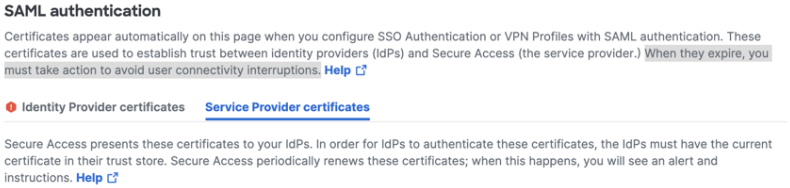
2. Upload a new Secure Access service provider certificate to the SAML IdP.
   a. For **Automatic Configuration**, copy the **Automatic Certificate Updates URL** and upload the Secure Access XML Metadata file to your SAML IdP.
   b. b. For **Manual Configuration**, in the list of certificates, click **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 authentication > Service Provider Certificates.

1. Navigate to **Secure > Certificates > SAML authentication > Service Provider Certificates**.



2. For **VPN Service Provider**, click **download** on a certificate in the list to save the certificate to your local system. Then, upload the certificate to the SAML IdP.

- **Subject name**–The certificate's common name, which defines the entity that manages the certificate.
- **Serial number**–The serial number of the certificate.
- **Expiration date**–The date when the certificate is no longer valid.



Manage SAML Certificates for Identity Providers

Provides instructions for managing SAML Certificates for Identity Providers in Cisco Secure Access China. 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:

- Networks and network tunnels protected by Internet Security
- Virtual Private Networks (VPNs) with a configured VPN profile

Prerequisites

Lists the prerequisites for certificates SAML IdP. 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.

- 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

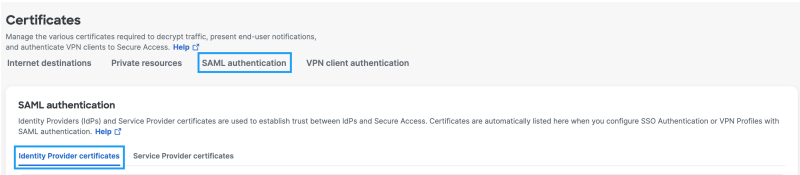
Provides instructions for certificates SAML IdP. Manage IdP certificates integrated with Secure Access. View notifications about the expiration of Secure Access certificates that are deployed in SAML IdP integrations and VPN Profiles.

- Manage IdP certificates integrated with Secure Access.
- View notifications about the expiration of Secure Access certificates that are deployed in SAML IdP integrations and VPN Profiles.

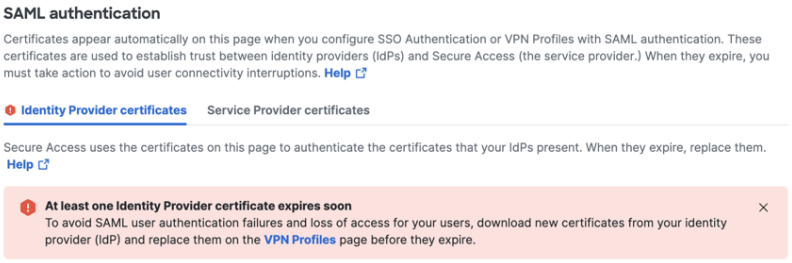
View Notifications About Expired Identity Provider Certificates

Provides instructions for viewing notifications about expired identity provider certificates. Navigate to Secure > Certificates > SAML authentication > Identity Provider certificates.

1. Navigate to **Secure > Certificates > SAML authentication > Identity Provider certificates**.



2. Secure Access displays any notifications about expiring certificates.



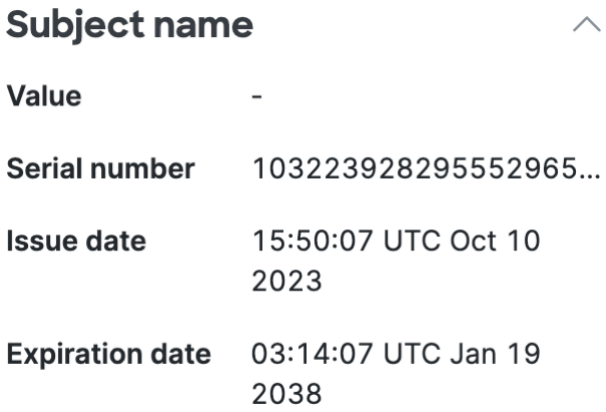
Manage Virtual Private Network Identity Provider Certificates

Provides instructions for managing virtual private network identity provider certificates. 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:.

1. Navigate to **Secure > Certificates > SAML Authentication > 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.

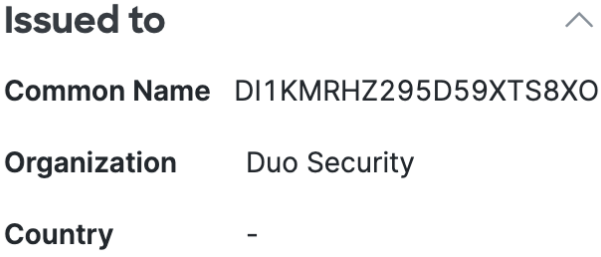


4. **Issued to** is the entity that uses the certificate to build a trust relationship with Secure Access. For **Issued to**, get the following certificate details:

   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.

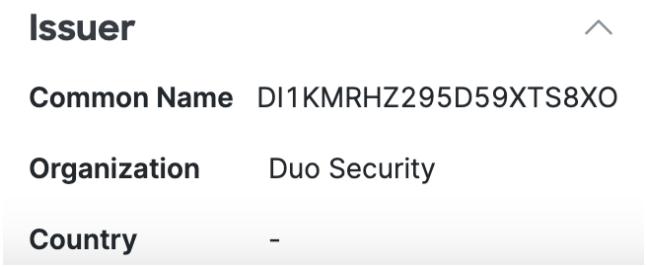


5. **Issuer** is the entity (trusted authority) that issues the certificate. For **Issuer**, get the following certificate details:

   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.



VPN Certificates for User and Device Authentication

Describes VPN Certificates for User and Device Authentication in Cisco Secure Access China. Users that connect over virtual private networks (VPNs) to private resources are protected by Cisco Secure Access.

Users that connect over virtual private networks (VPNs) to private resources are protected by Cisco Secure Access. The user devices must trust their network communications with Secure Access.

To set up the trust between Secure Access and the user devices in the organization that connect over a VPN, install a certificate signed by your organization's Certificate Authority (CA) on all devices and upload your organization's signed CA root certificate to Secure Access. CA root certificates enable Secure Access to authenticate users and devices that connect over VPNs.

Once you upload signed CA certificates for VPN connections to Secure Access, you can view the details about the certificates, revoke a certificate, and delete a certificate. For more information about VPN Certificate Authority certificates, see Manage CA Certificates for VPN Connections.

Manage CA Certificates for VPN Connections

Provides instructions for managing CA Certificates for VPN Connections in Cisco Secure Access China. When devices connect to networks using virtual private networks (VPNs), Cisco Secure Access authenticates the users and devices through the organization's Certificate Authority (CA) certificate.

When devices connect to networks using virtual private networks (VPNs), Cisco Secure Access authenticates the users and devices through the organization's Certificate Authority (CA) certificate.

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.
2. Upload your organization's signed CA root certificate to Secure Access.

Prerequisites

Lists the prerequisites for certificates for vpn, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Install a Certificate Authority Certificate on User Devices

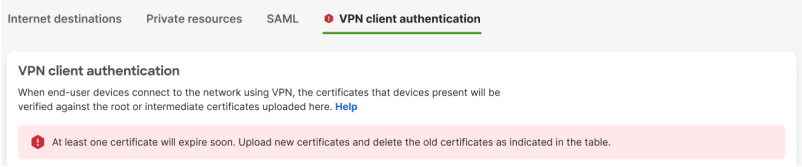
Provides instructions for installing a certificate authority certificate on user devices. Install your corporate Certificate Authority (CA) root certificate on the user devices in your organization. For information about installing certificates on devices, see Install the Cisco Secure Access Root Certificate.

Install your corporate Certificate Authority (CA) root certificate on the user devices in your organization. For information about installing certificates on devices, see Install the Cisco Secure Access Root Certificate.

View Notifications About Expired VPN Certificate Authority Certificates

Provides instructions for viewing notifications about expired vpn certificate authority certificates. Navigate to Secure > Certificates > VPN client authentication.

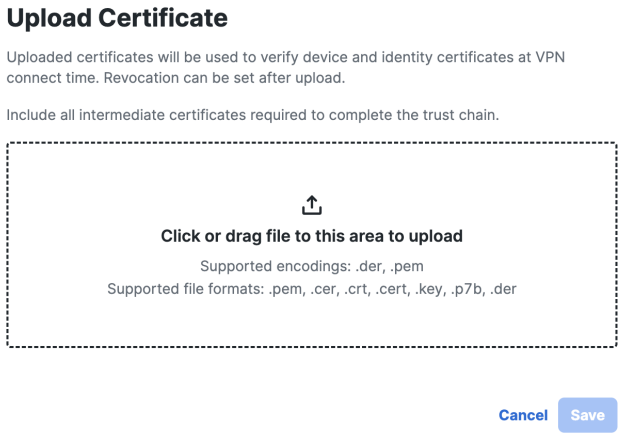
1. Navigate to **Secure > Certificates > VPN client authentication**.
2. Secure Access displays a banner if a certificate has expired or will expire within 90 days:



Upload VPN Certificate Authority Certificates

Provides instructions for uploading vpn certificate authority certificates. Navigate to Secure > Certificates > VPN client authentication. Click Upload Certificate.

1. Navigate to **Secure > Certificates > VPN client authentication**.
2. Click **Upload Certificate**.

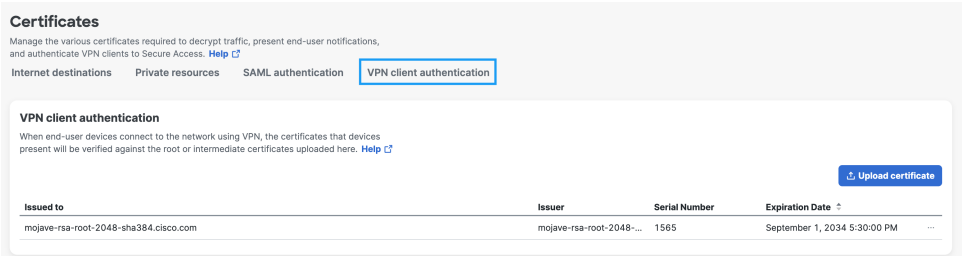


3. Upload your signed CA root certificate, and then click **Save**.

View VPN CA Certificates

Provides instructions for viewing vpn ca certificates. Issued to –The name issued to the VPN CA certificate. Issuer –The CA that issued the certificate.

1. Navigate to **Secure > Certificates > VPN Client Authentication**. Secure Access lists the certificates uploaded by your organization.



Issued to–The name issued to the VPN CA certificate.

Issuer–The CA that issued the certificate.

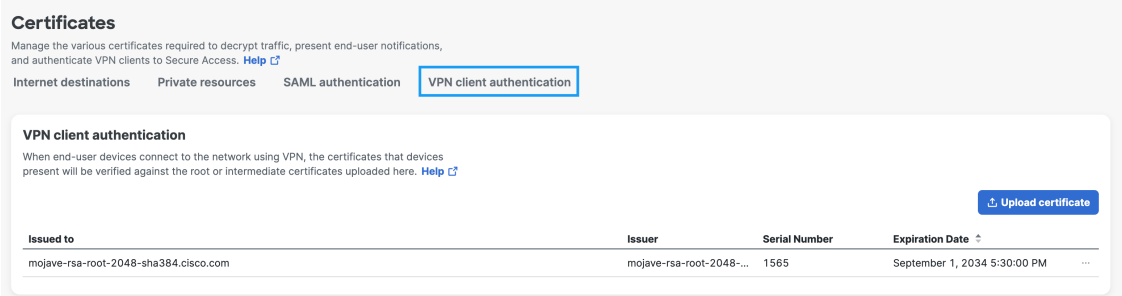
Serial–The serial number of the certificate.

Expiration–The date when the certificate is no longer valid.

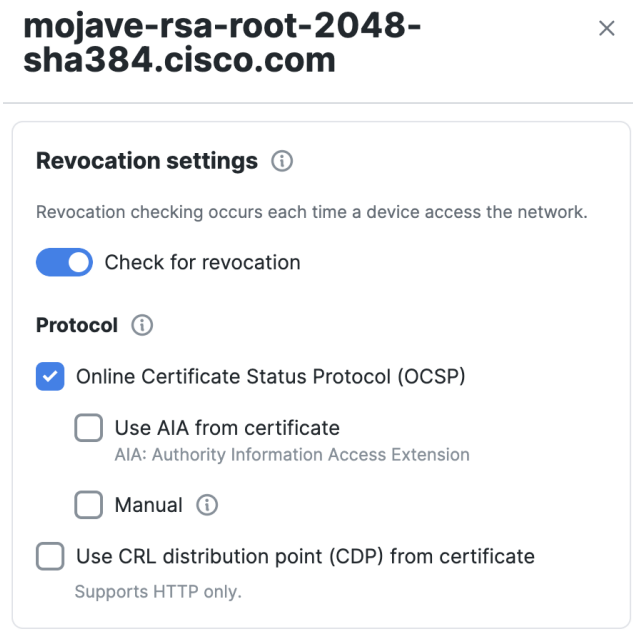
Manage Certificate Revocation Settings

Provides instructions for managing certificate revocation settings. Navigate to Secure > Certificates > VPN Client Authentication. Click on an VPN CA certificate Issued to link to open the certificate details.

1. Navigate to **Secure > Certificates > VPN Client Authentication**.
2. Click on an VPN CA certificate **Issued to** link to open the certificate details.



3. For **Revocation settings**, enable **Check for revocation**.
4. For **Protocol**, check **Online Certificate Status Protocol**,a. Check **Use AIA from certificate**.b. Check **Manual**.0o9=0-=
5. For **Protocol**, check **Use CRL distribution point (CFP) from certificate**.



6. Click **Save**.

View the CA Certificate Details

Provides instructions for viewing the ca certificate details. Type –The type of the certificate. Serial Number –The serial number of the certificate.

1. **General** certificate details:

   Type–The type of the certificate.

   Serial Number–The serial number of the certificate

   Public Key Type–The type of the public key.

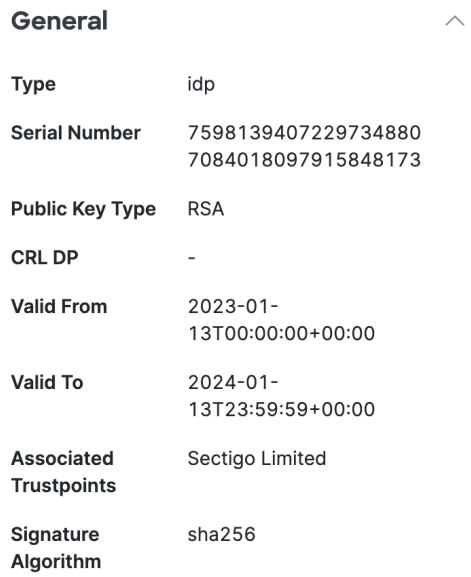
   CRL DP–Certificate Revocation List (CRL) Distribution Point. The location where you can check the revocation of the certificate.

   Valid From–The date from which the certificate is valid.

   Valid To–The date when the certificate is not valid.

   Associated Trustpoints

Signature Algorithm–The cryptographic hash algorithm (Secure Hashing Algorithm 256).



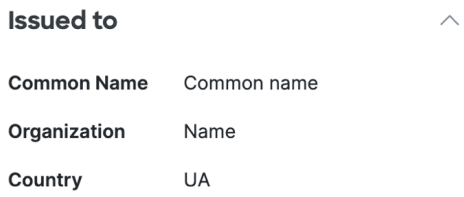
2. **Issued to** certificate details.

   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.

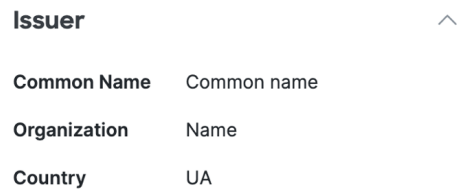


3. **Issuer** certificate details. The issuer is the entity (trusted authority) that issues the certificate.

   Common Name–The fully-qualified domain name that is secured by the certificate.

   Organization–The organization that issued the certificate.

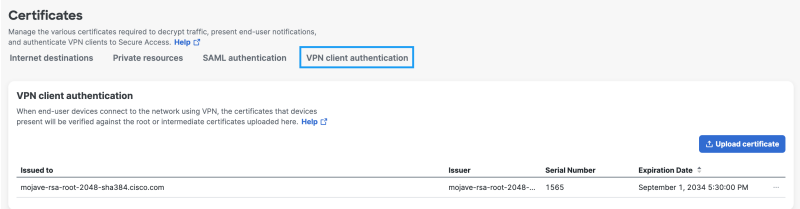
   Country–The country where the certificate was issued specified in the two-character country code.



Delete a VPN Certificate

Provides instructions for deleting a vpn certificate. Navigate to Secure > Certificates > VPN Client Authentication. Click on an VPN CA certificate Issued to link to open the certificate details, and then click Delete . Click Delete again to confirm the removal of the certificate.

1. Navigate to **Secure > Certificates > VPN Client Authentication**.



2. To remove a certificate, follow the steps in one of the options:
   a. Click on an VPN CA 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 the ellipsis (...) and select **Delete**. Click **Delete** again to confirm the removal of the certificate.

Certificate Installation Methods

Describes 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).

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.

38 Manage the Data Loss Prevention Policy

Topics:

- Manage the Data Loss Prevention Policy

Provides an overview of Manage the Data Loss Prevention Policy in Cisco Secure Access China, including Add a Real Time Rule to the Data Loss Prevention Policy, Understand Exclusions in a Real Time Rule, and Supported Applications. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage the Data Loss Prevention Policy

Provides instructions for managing the Data Loss Prevention Policy in Cisco Secure Access China. Not all of the features described here are available to all Secure Access packages.

> **Note**
>
> Secure Access Packages and Feature Availability
>
> Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine 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 **Real Time** DLP rules to inspect the web traffic traversing the proxy. 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.

Data violations detected through the Real Time rules are logged as part of the unified Events view of the Data Loss Prevention Report.

Discovery Scans 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.

Real Time 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 in Cisco Secure Access China. 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.

Prerequisites

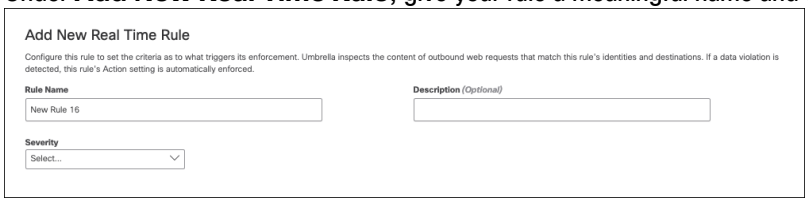
Lists the prerequisites for adding a data protection policy, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- Full Admin user role. For more information, see Manage Accounts.

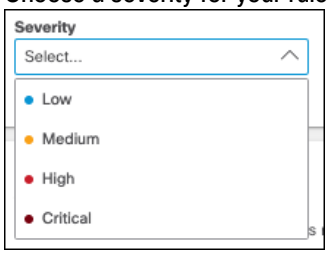
Procedure

Provides instructions for adding a data protection policy. When All Destinations is selected, you can select the type of data Secure Access China monitors:.

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.



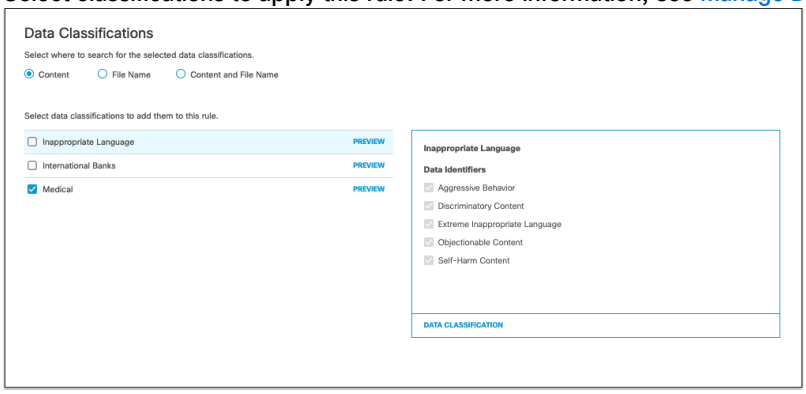
3. Choose a severity for your rule based on the risk involved or importance within the ruleset.



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 China 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**.

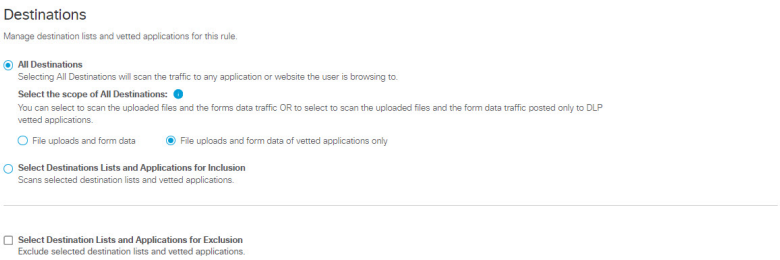
- **All Destinations**–Monitors all outbound web requests or blocks all file uploads that originate from the selected identities for this rule.

  When **All Destinations** is selected, you can select the type of data Secure Access China monitors:

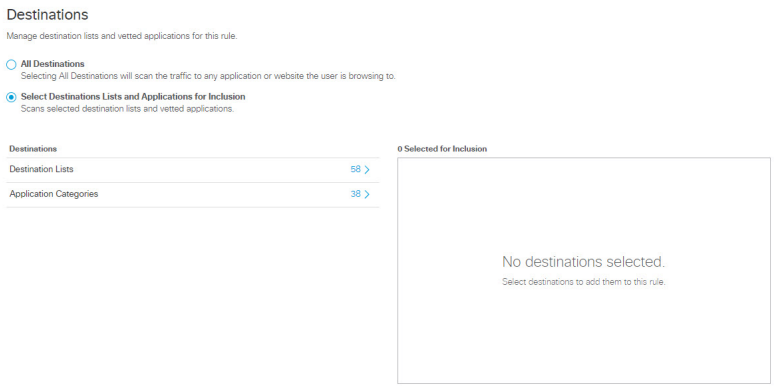
  - Choose **File uploads and form data** to monitor all uploaded files and forms data for all web destinations users visit.**Important**

    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.

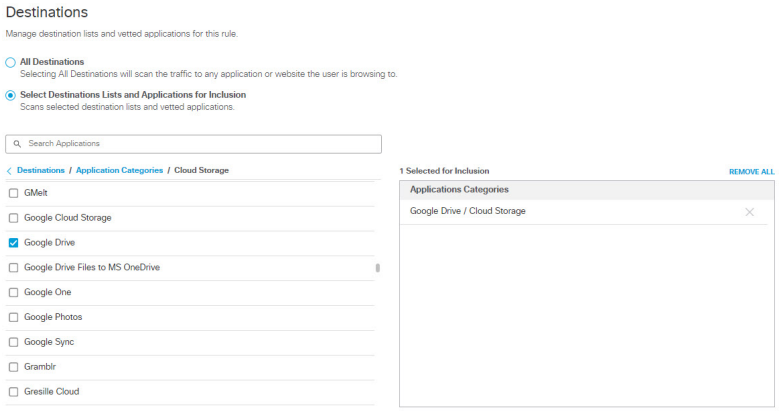


- **Select Destination Lists and Applications for Inclusion**–Monitors all web requests and blocks all file uploads matching the identities selected on the rule, the selected destination lists, and supported applications.

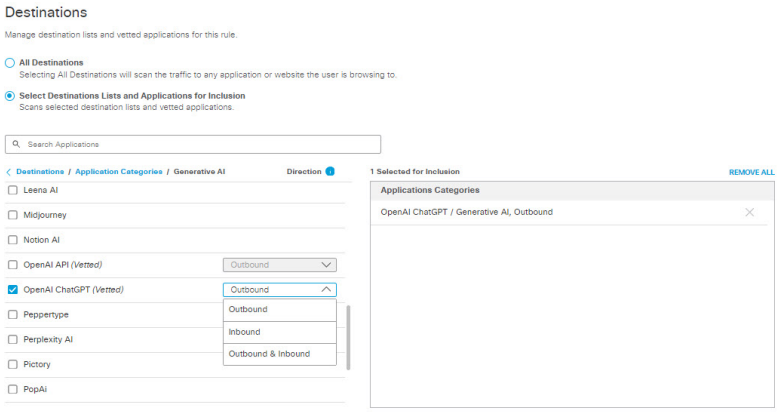


- To add applications for inclusion, under **Destinations** expand **Application Categories**. (See Application Categories) for a list of available categories.) Expand categories and check the boxes for the applications you want to add to the rule. You can search for an application by entering at least three consecutive letters from the application name in the search box.

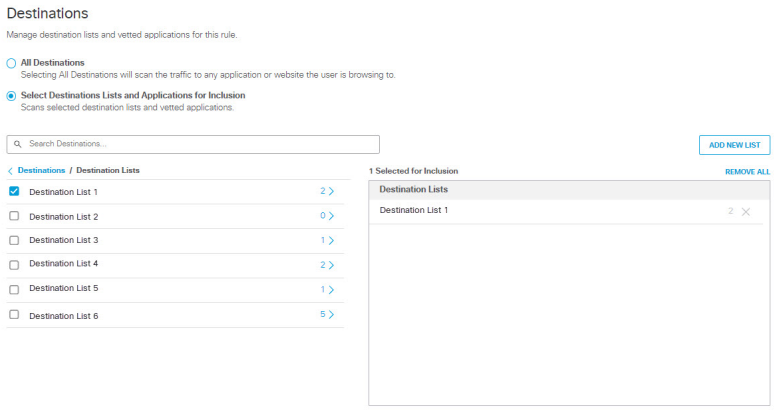
> **Note**
>
> It is not possible to search for an application with fewer than three letters in its name–for example, "QQ" or "YY." These applications must be manually selected from the hierarchy under their respective categories, or wildcarded in search–for example, "QQ*". This behavior is by design.



- Note that for some applications (**OpenAI API** and **OpenAI ChatGPT**, for example) you can choose to scan any one of three traffic options: **Outbound** (from your system to the application), **Inbound** (from the application to your system), or **Outbound and Inbound**.

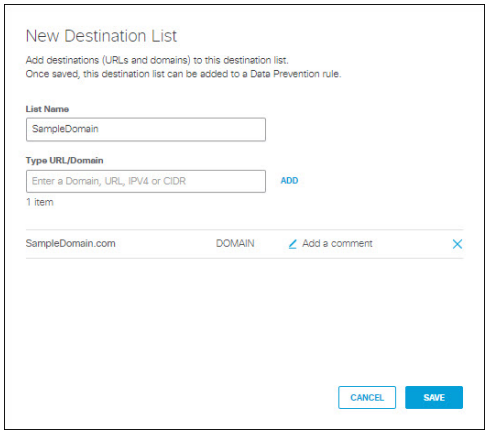


- To add destination lists for inclusion, under **Destinations** expand **Destination Lists** and check the boxes for the destination lists you want to add to the rule.

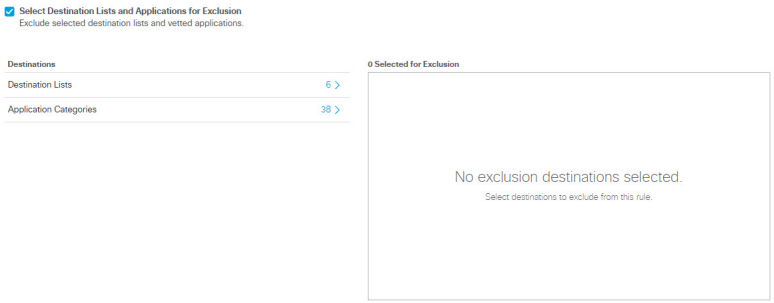


- To create a new destination list and add it for inclusion, under **Destinations** expand **Destination Lists** and click **ADD NEW LIST.** Under **List Name** enter a unique name for the list. For each URL/Domain to be in the list, enter a domain name, URL, IPV4 address or CIDR, and click **Add**. Click **Save** when done.

> **Note**
>
> Adding a new destination list to the rule here automatically adds it for inclusion.

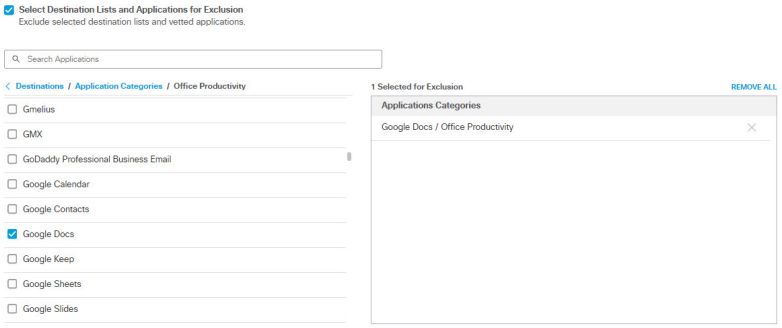


9. Check the checkbox **Select Destination Lists and Applications for Exclusion** to select destinations and applications to exclude from this rule.

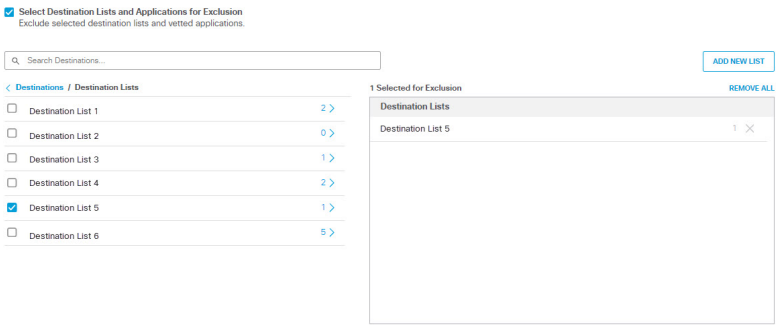


- To exclude applications, under **Destinations** expand **Application Categories**. (See Application Categories for a list of available categories.) Expand categories and check the boxes for the applications you want to exclude from the rule. You can search for an application by entering at least three 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.

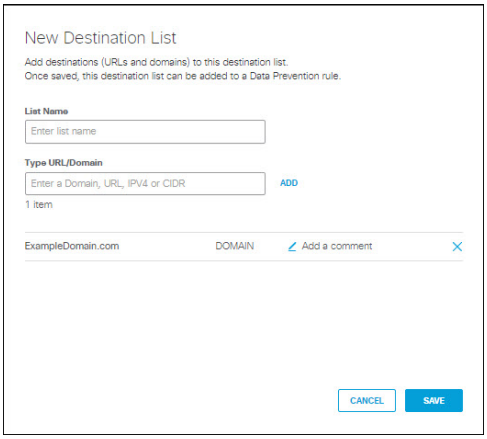


- To exclude destination lists, under **Destinations** expand **Destination Lists** and check the boxes for the destination lists you want to exclude from the rule.



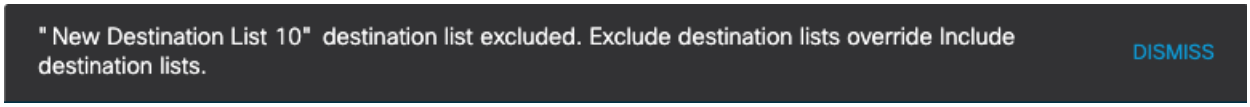
- To create a new destination list and exclude it, under **Destinations** expand **Destination Lists** and click **ADD NEW LIST.** Under **List Name** enter a unique name for the list. For each URL/Domain to be in the list, enter a domain name, URL, IPV4 address or CIDR, and click **Add**. Click **Save** 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.

Figure 4: toast pop up.png



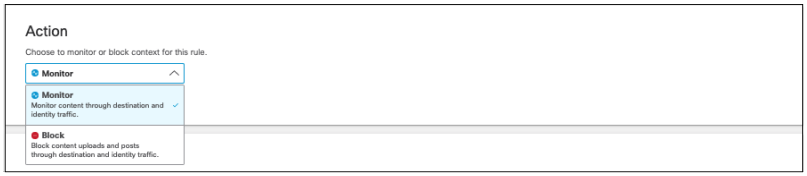
10. Under **Action**, from the drop-down list, choose **Monitor** or **Block**.

    - **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.

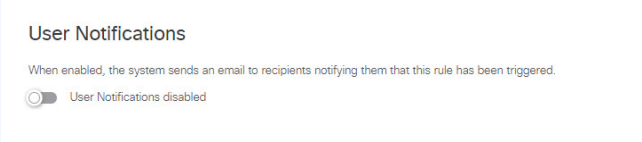
    - **Block**–Block file uploads.

      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.

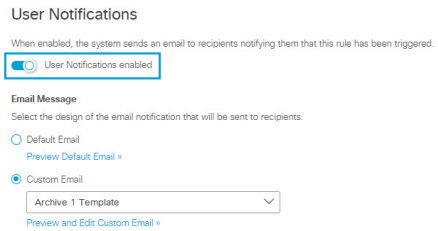


> **Note**
>
> Limited Availability
>
> Secure Access China can optionally block all password-protected files directed to destinations configured in the DLP rules. If enabled, this feature impacts all file types and all users and cannot be configured for finer granularity. This feature is not generally available; contact Secure Access China 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.
>
> 
>

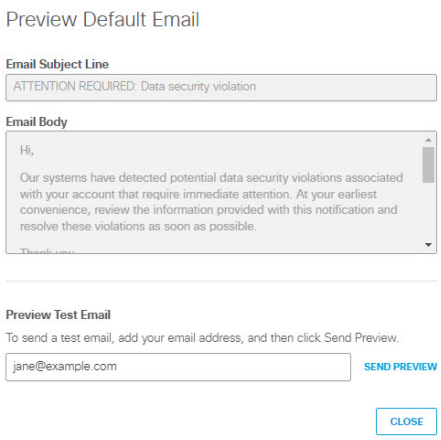
a. Enable user notifications.



b. Choose the email template:

To Use the Default Email Template:

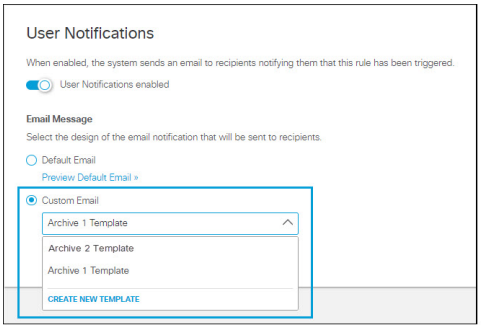
1. Click **Default Email**.
2. To preview the content of the email that will be send to users, click on **Preview Default Email**. You can review the email subject line and text, but you cannot change it.

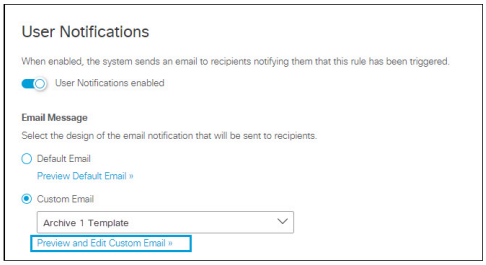


3. iii. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)
4. iv. Click **CLOSE** to return to the Data Loss Prevention Policy page.

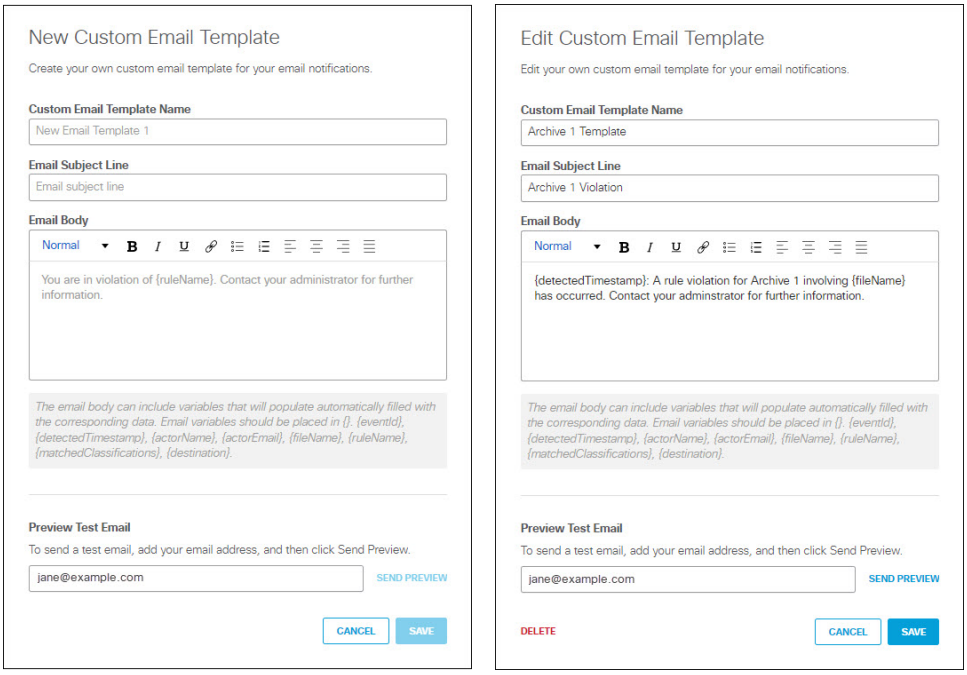
To Use a Custom Email Template:

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 China gets this information from the authenticated Active Directory.)
- **{actorEmail}** - Email address of the user whose action triggered the violation. (Secure Access China 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. 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 in Cisco Secure Access China. 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 China then inspects the web request for matches with the rule's configured data classifications and file labels. Exclusions enable you to narrow your data criteria monitoring to specific applications and destinations. For example, if you have the rule to monitor data classifications for an application, but want to exclude some domains or URLs from being scanned, you can exclude a destination list with those domains. Traffic through that application will be scanned with the exception of the destination list excluded.

Within the context of a Real Time rule, exclusions will always override inclusions. For example, if a rule states that a domain on one list is excluded but the same domain is included on another destination list, the domain will automatically be excluded from the rule.

Supported Applications

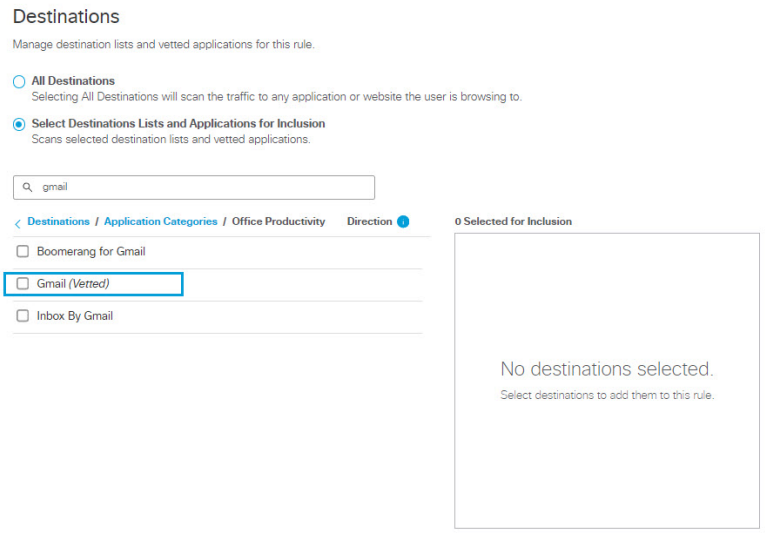
Describes Supported Applications in Cisco Secure Access China. The Real Time DLP rules inspect the content of all Secure Access proxied web requests matching the resources and destinations selected in the Real Time rules of the Data Loss Prevention (DLP) policy.

The Real Time DLP rules inspect the content of all Secure Access proxied web requests matching the resources and destinations selected in the Real Time rules of the Data Loss Prevention (DLP) policy. When a Real Time DLP rule is configured with **Select Destination Lists and Applications for Inclusion**, Secure Access scans for data violations every web request matching the rule's applicable resources and targeting a destination matching the rule-configured destinations. A web request can be a web form or a file upload. File uploads can be scanned for matches with the selected data classifications in the file content, file name, or either. Moreover, a file upload can be scanned for the presence of document properties matching the rule's File Labels settings. For more information, see Add a Real Time Rule to the Data Loss Prevention Policy.

Verified applications also support other workflows besides file uploads. For example, if the rule is configured to **Select Destination Lists and Applications for Inclusion** and Yahoo Mail is chosen as an application to scan for content,

the policy can scan for file uploads, emails sent, and draft emails saved. Violations within these workflows are then blocked or monitored, depending on the action selected in the rule. However, some applications have limitations when scanning for file names of file uploads. For example, the DLP policy can scan Dropbox for file uploads, but the file name can not be scanned.

The DLP Real Time rules support thousands of applications, divided into categories for ease of reference. Before January of 2024, DLP supported a more limited set of applications; the table below lists those applications and the limitations on their support. These applications appear in the GUI with the notation *(Vetted)*, as shown in the example below:



The list of apps marked *Vetted* in the GUI, and their workflow limitations, is listed below:

Application	Supported Workflows	File Name Limitations
Box Cloud Storage	File upload	
ChatGPT	Create conversation	
OpenAI ChatGPT API	Request and Response of Chat and Completions	
Concur Invoice	Receipt upload	
Confluence	File upload; edit a file **Note** To scan file uploads, you must select Atlassian and Confluence as destinations for the DLP rule.	
DLPTest.com	Submit test message; File upload	

Application	Supported Workflows	File Name Limitations
Dropbox	File upload; File upload add comment; File upload update comment **Note** Dropbox Paper is not supported using Real Time DLP.	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;	
PasteBin	Post a message	

Application	Supported Workflows	File Name Limitations
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	

Discovery Scan

Describes Discovery Scan in Cisco Secure Access China. Discovery Scan inspects the content of all files in the tenant that are modified over the selected date range.

Discovery Scan inspects the content of all files in the tenant that are modified over the selected date range. As files in the selected tenant are scanned upon content change and context (sharing) change, Secure Access assesses the file. If Secure Access detects a violation, the offending file is listed in the Data Loss Prevention Report.

This topic walks you through how to initiate a scan and how to cancel an ongoing scan.

> **Note**
>
> A discovery scan must be triggered around 24 hours after tenant authorization as the system evaluates and enumerates the users in the organization. Any triggering beforehand might not include all users. Secure Access performs discovery scans on 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

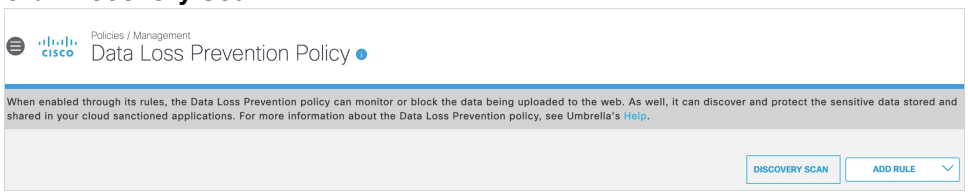
Lists the prerequisites for initiate discovery scan. You must authenticate a tenant for at least one of the platforms Secure Access supports: Google Drive, Microsoft 365, Dropbox, and Box.

- You must authenticate a tenant for at least one of the platforms Secure Access supports: Google Drive, Microsoft 365, Dropbox, and Box.

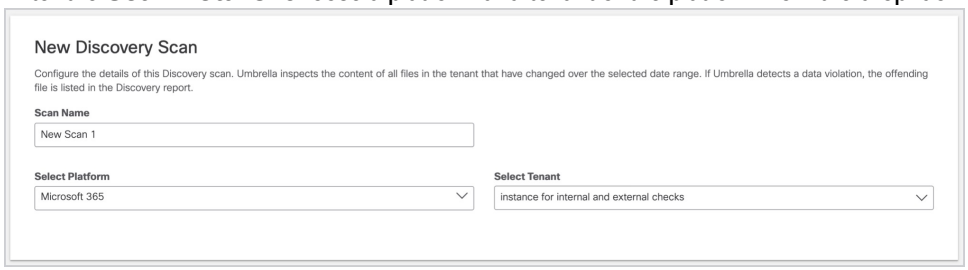
Initiate a Discovery Scan

Describes initiate a Discovery Scan. Select where in uploaded files you would like the scan to search for the data classifications that you choose.

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**.
2. Click **Discovery Scan**.



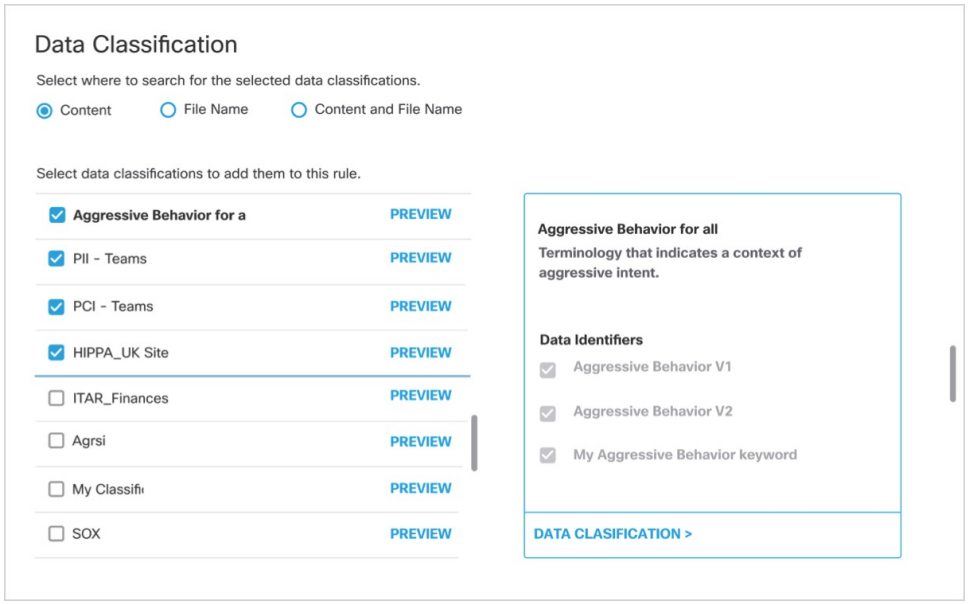
3. Enter the **Scan Details**. Choose a platform and tenant of the platform from the drop-down lists.



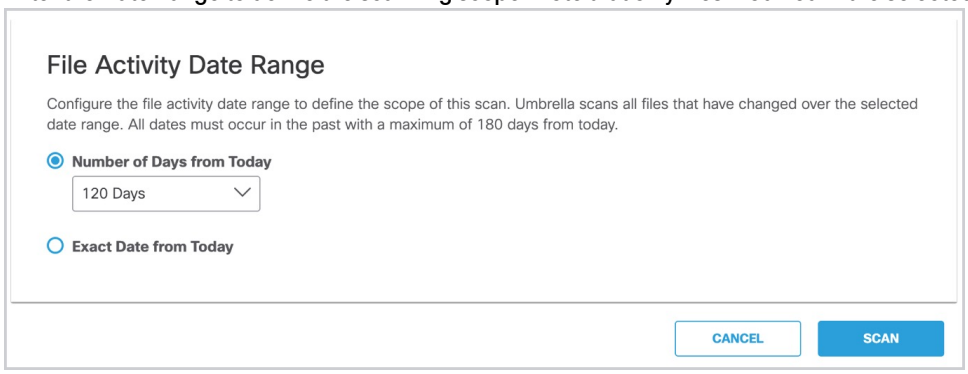
4. Select where in uploaded files you would like the scan to search for the data classifications that you choose.
   - **Content**–(Default) Searches only the content of files for the selected data classifications.
   - **File Name**–Searches only file names for the selected data classifications.
   - **Content and File Name**–Searches content and file names for the selected data classifications. Both content and file name do not need to match for the scan to apply, only one or the other.

> **Note**
>
> Choosing Content, File Name, or Content and File Name refers to scanning file uploads for the selected data classifications and configured file labels.

5. Select the required **Data Classification** of your choice. You can select multiple tenants.

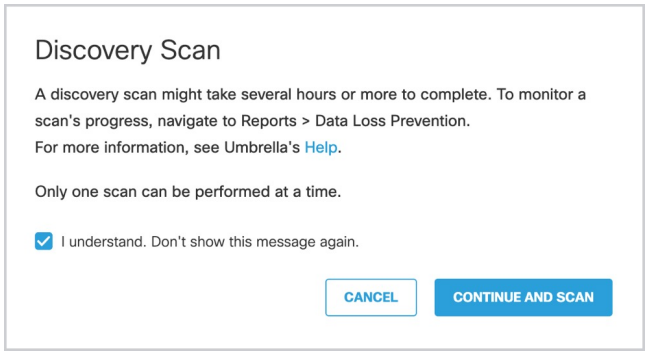


6. Enter the Date Range to define the scanning scope. Note that only files modified in the selected date range are scanned.



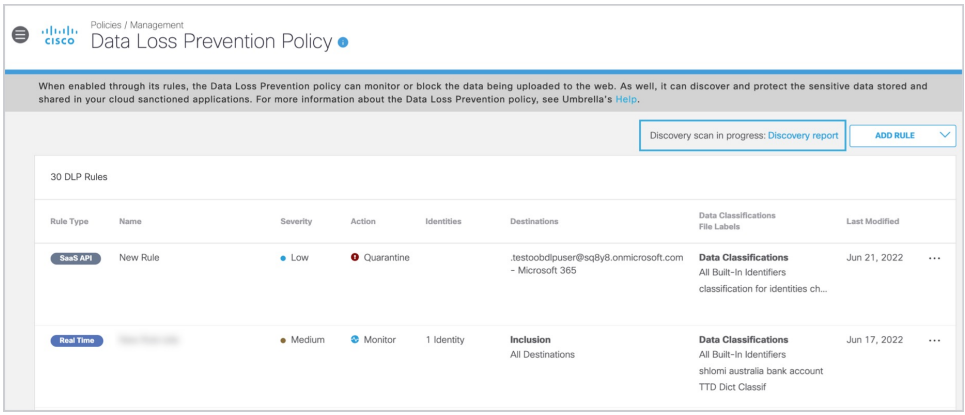
7. Click **Scan** to initiate.
8. Click **Continue and Scan**.

> **Note**
>
> Only one scan executes at a time. The scan might take a while. Once completed, you can initiate another scan.



9. Click **Discovery Report** to view the progress of the scan results.

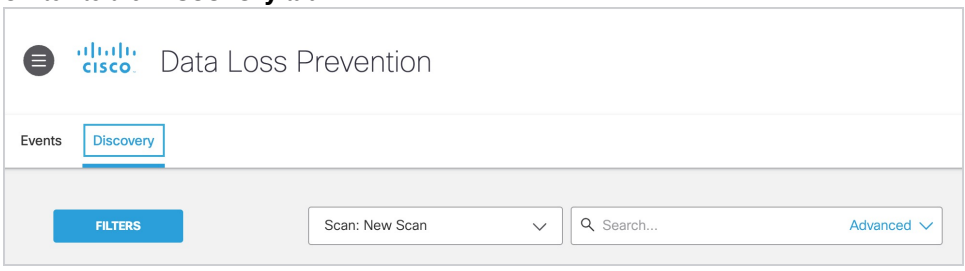
   For more information on DLP reports, refer to DLP Report.



Cancel a Discovery Scan

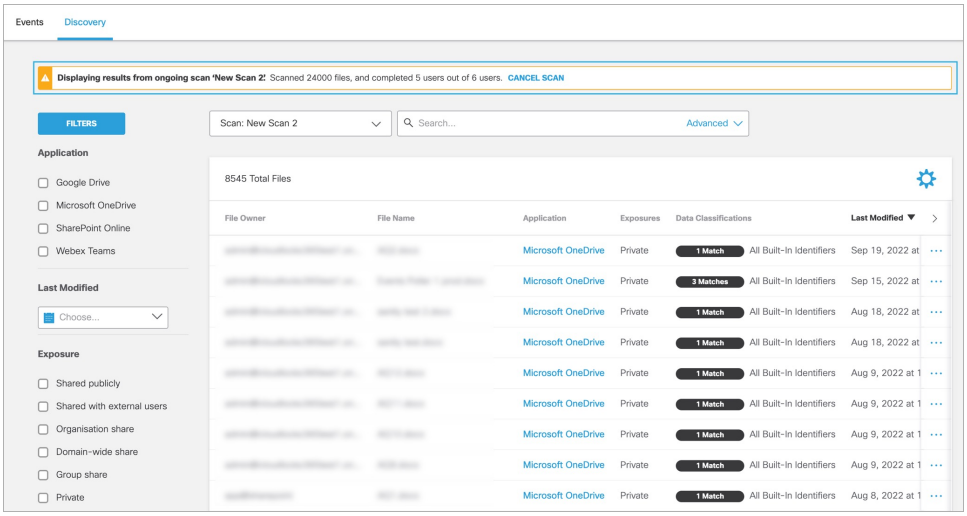
Describes cancel a Discovery Scan. Click Cancel Scan . Results of the ongoing scan are displayed in the ribbon. Note that the cancelation of a scan might take a few minutes.

1. Navigate to **Reporting** > **Additional Reports** > **Data Loss Prevention**.
2. Switch to the **Discovery** tab.

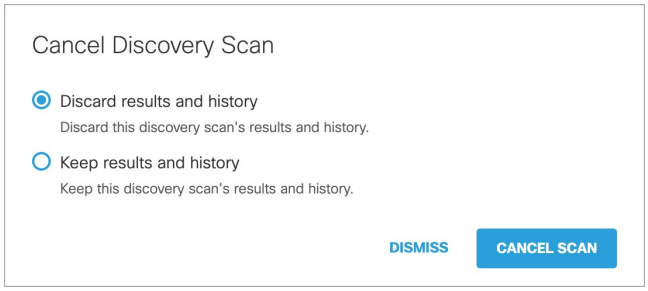


3. Click **Cancel Scan**. Results of the ongoing scan are displayed in the ribbon.

   Note that the 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

Provides instructions for editing a Data Loss Prevention Rule in Cisco Secure Access China, including Prerequisites and Procedure. It explains the sequence of actions and relevant settings presented in the procedure.

After adding a Real Time 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.

Prerequisites

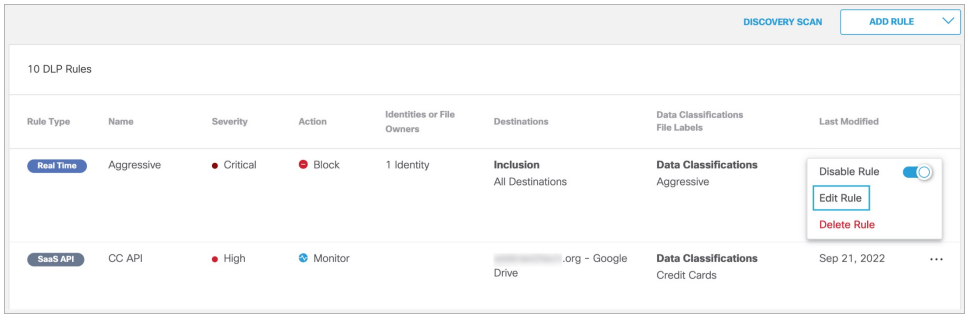
Lists the prerequisites for editing a data loss prevention rule. Full admin access to the Secure Access dashboard. See Manage Accounts.

- Full admin access to the Secure Access dashboard. See Manage Accounts.
- For Real Time DLP rules, HTTPS Inspection must be enabled either on the Web Default Policy, or at least one web policy ruleset where the same identity is configured in a DLP rule. For example, if the identity "Network A" is configured for a DLP rule, it must also be configured for a web policy ruleset where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.

Procedure

Provides instructions for editing a data loss prevention rule. Navigate to Secure > Policy > Data Loss Prevention Policy. Click the More Actions menu, and select Edit Rule.

1. Navigate to **Secure > Policy > Data Loss Prevention Policy**.
2. Click the **More Actions** menu, and select **Edit Rule**.



3. Make the changes and click **Save**.

Delete a Data Loss Prevention Rule

Provides instructions for deleting a Data Loss Prevention Rule in Cisco Secure Access China. You can delete a Data Loss Prevention rule at any time.

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.

Prerequisite

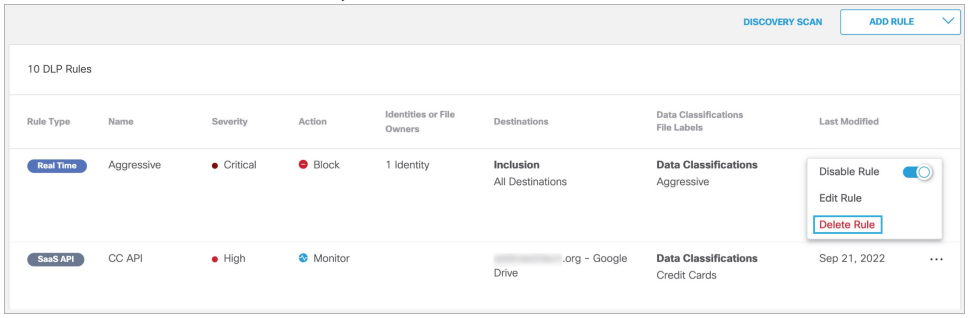
Lists prerequisites for the task, including the Full Admin user role and the account access information provided in Manage Accounts.

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

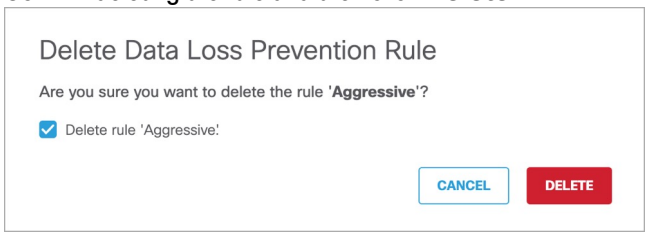
Procedure

Provides instructions for deleting a data loss prevention rule. Navigate to Secure > Policy > Data Loss Prevention Policy. Click the More Actions menu, and click Delete Rule.

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

Provides instructions for enabling or Disable a Data Loss Prevention Rule in Cisco Secure Access China. Newly added rules are automatically enabled for the Data Loss Prevention policy.

Newly added rules are automatically enabled for the Data Loss Prevention policy. When you navigate to **Secure > Policy > Data Loss Prevention Policy**, disabled rules appear faded. Note that enabling or disabling a rule does not impact any running Discovery Scan, it only impacts incoming events for the scan.

Prerequisites

Lists the prerequisites for enabling or disable a data loss prevention rule. Full Admin user role. For more information, see Manage Accounts.

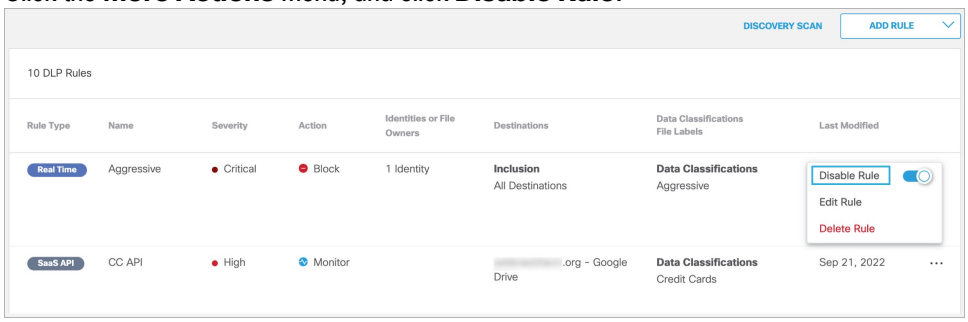
- Full Admin user role. For more information, see Manage Accounts.
- For Real Time DLP rules, HTTPS Inspection must be enabled either on the Web Default Policy, or at least one web policy ruleset where the same identity is configured in a DLP rule. For example, if the identity "Network A" is configured

for a DLP rule, it must also be configured for a web policy ruleset where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.

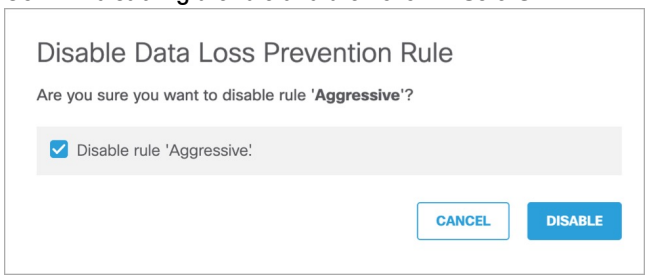
Disable a Rule

Provides instructions for disabling a rule. Navigate to Secure > Policy > Data Loss Prevention Policy. Click the More Actions menu, and click Disable Rule.

1. Navigate to **Secure > Policy > Data Loss Prevention Policy**.
2. Click the **More Actions** menu, and click **Disable Rule**.



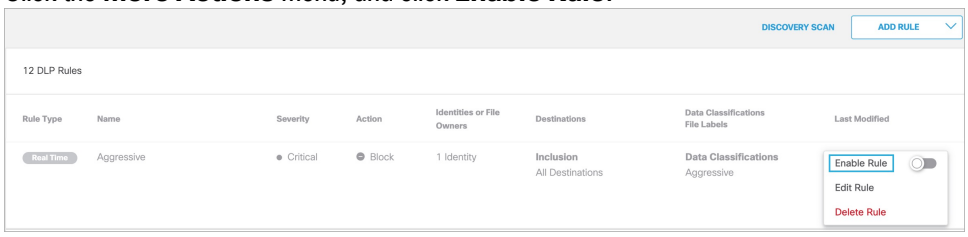
3. Confirm disabling the rule and then click **Disable**.



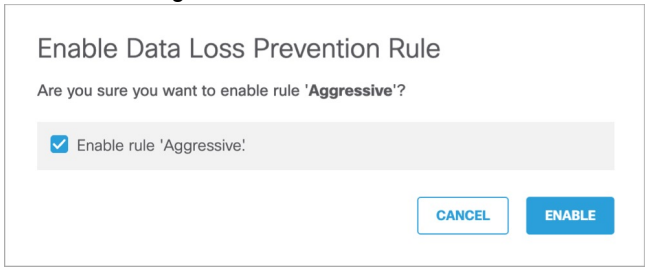
Enable a Rule

Provides instructions for enabling a rule. Navigate to Secure > Policy > Data Protection Policy. Click the More Actions menu, and click Enable Rule.

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 in Cisco Secure Access China. The Data Loss Prevention policy can monitor or block the data being uploaded to the web.

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
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 in Cisco Secure Access China. Some of the Data Loss Prevention policy's built-in identifiers have the potential to produce false positives if not customized to narrow the scope of the inspection.

Some of the Data Loss Prevention policy's built-in identifiers have the potential to produce false positives if not customized to narrow the scope of the inspection. The following are recommended to reduce the number of false positives in these classifications. For more information on customizing an identifier, see Copy and Customize a Data Identifier.

Threshold

The default threshold for built-in identifiers without tolerance is 1. This means that the policy will search for content where the identifier is met only once within a file. Increasing the threshold will scan content for instances where the identifier is met more than once, creating fewer false positives for each individual instance of the identifier. A threshold of 10, for example, only monitors or blocks a file if 10 instances of the identifier are found in the file.

Proximity Terms

Proximity keywords reduce false positives by requiring identifiers to match within 10 terms of specified words.

For example, a Canadian bank account identifier will search for a pattern matching Canadian bank account numbers and transit numbers. A document containing several random numbers matching that pattern could produce false positives, however, if proximity terms such as "Canada" and "bank" are added to the customized identifier, the scope of the inspection is reduced.

39 Manage Data Classifications

Topics:

- Manage Data Classifications

Provides an overview of Manage Data Classifications in Cisco Secure Access China, including Add a Data Classification, Copy and Customize a Built-In Data Classification, and Delete or Edit a Classification. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Data Classifications

Provides instructions for managing data Classifications in Cisco Secure Access China. The Data Loss Prevention (DLP) policy monitors or blocks content based on the rules configured for the policy.

The Data Loss Prevention (DLP) policy monitors or blocks content based on the rules configured for the policy. The rules use *data identifiers* and *data classifications*, which describe the type of data to be monitored or blocked. The file and form types supported by the DLP policy are listed here.

Data identifiers describe the content the Data Loss Prevention Policy monitors or blocks. Data identifiers can describe Personal Information Identifiers (PII) that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers. Data identifiers can also describe certain content an organization may wish to monitor or block within its network traffic, such as discriminatory or aggressive content. 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 Add a Data Classification.)
- You can create a custom data classification based on a built-in data classification provided by Secure Access. (See Copy and Customize a Built-In Data Classification).
- You can apply a built-in data classification provided by the system.

Secure Access provides four different built-in data classifications. You can apply these directly to your DLP rules or copy them and customize the copies to create your own data classifications. Each of the built-in data classifications has a different set of built-in data identifiers associated with it. .

Add a Data Classification

Provides instructions for adding a Data Classification in Cisco Secure Access China. You can create a data classification to help you monitor content with specific characteristics.

You can create a data classification to help you monitor content with specific characteristics. Custom data classifications can be used in real time rules 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.

The system offers built-in data identifiers you can choose from:

Built-In Identifiers

Describes 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.

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

Describes custom Identifiers. You can create custom identifiers to match specific terms and pattern expressions of your choosing. See Create a Custom Identifier.

You can create custom identifiers to match specific terms and pattern expressions of your choosing. See Create a Custom Identifier .

Exact Data Match Identifiers

Describes 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.).

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

Describes 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.

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.

Prerequisites

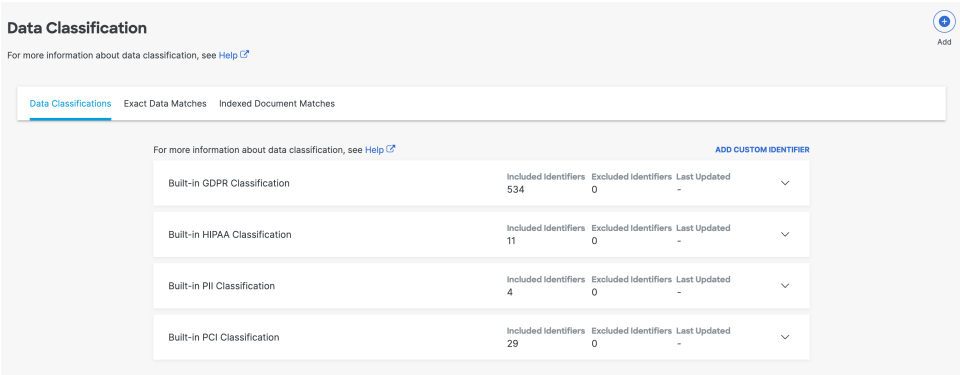
Lists the prerequisites for adding a data classification without a template. Full Admin user role. For more information, see Manage Accounts.

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

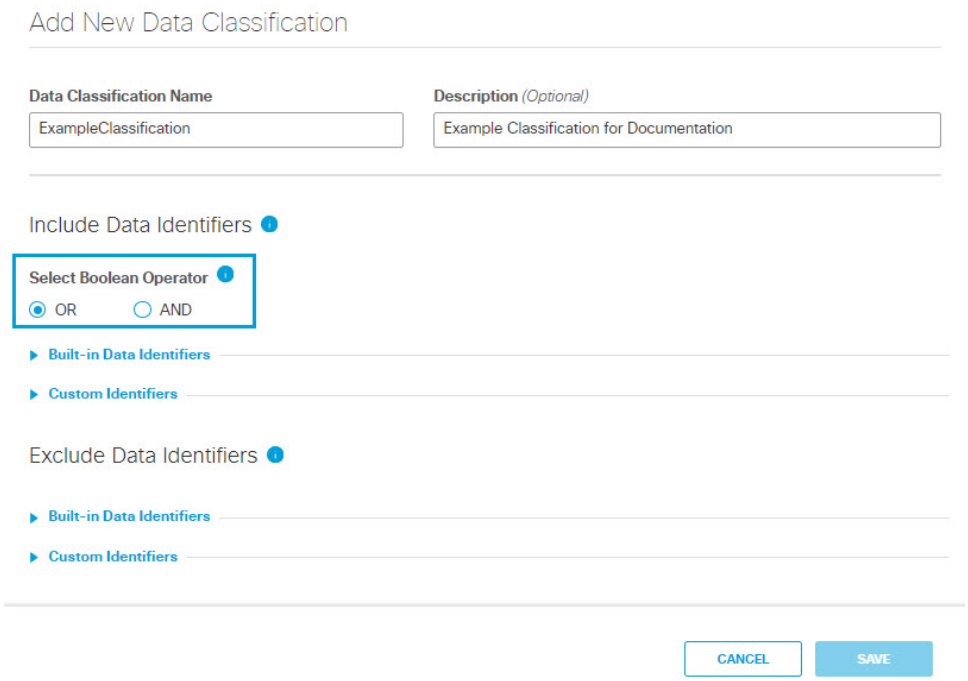
Procedure

Provides instructions for adding a data classification without a template. OR –At least one of the data identifiers included must match during rule evaluation.

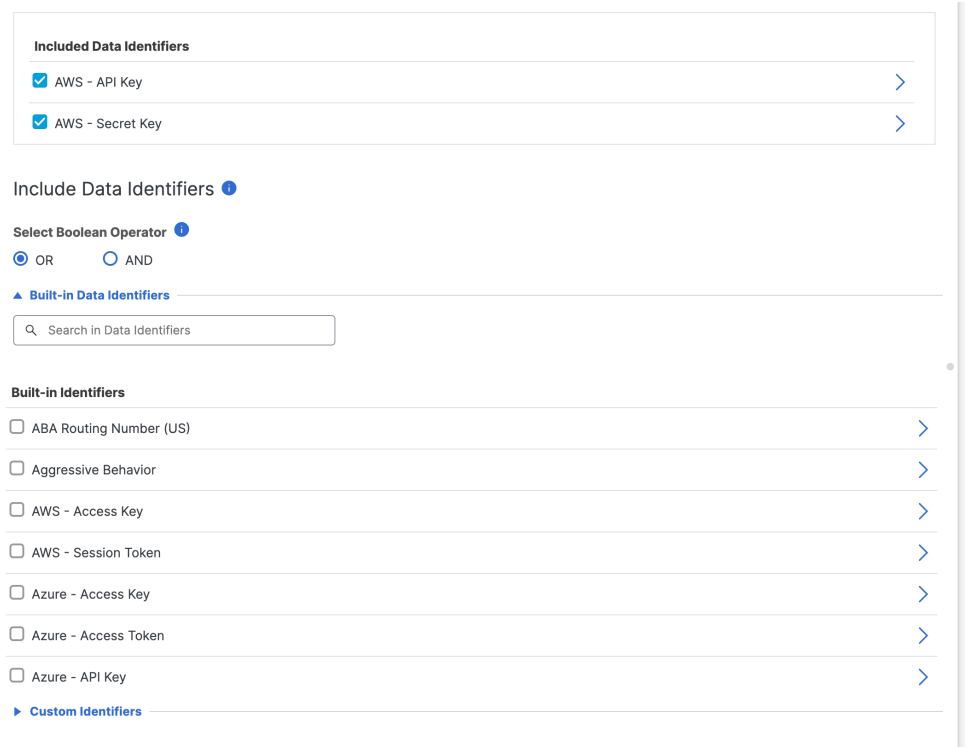
1. Navigate to **Secure > Settings > Data Classification > Data Classifications**. Click **Add**.



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 enter custom identifiers to include in the data classification.

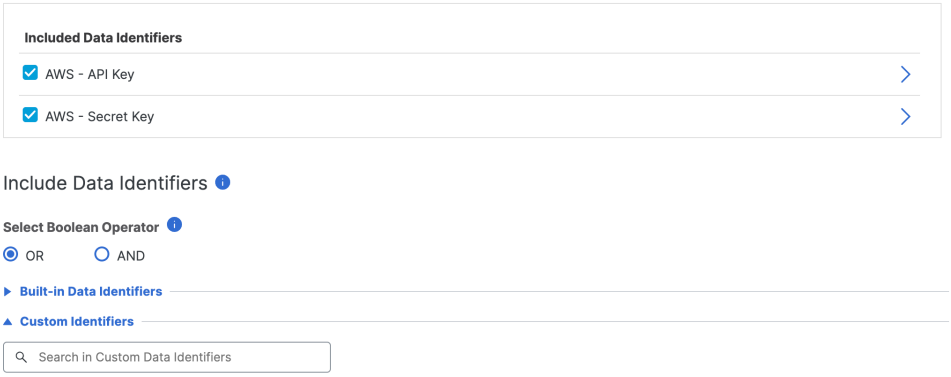
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

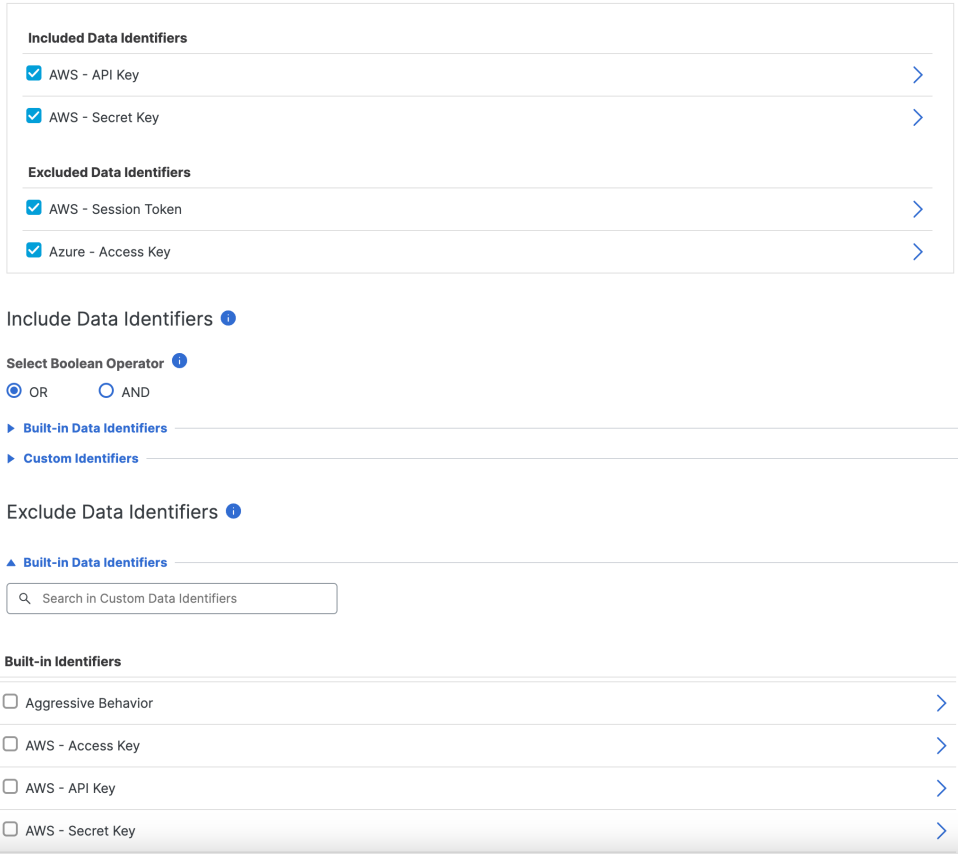
> **Note**
>
> Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

- 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:

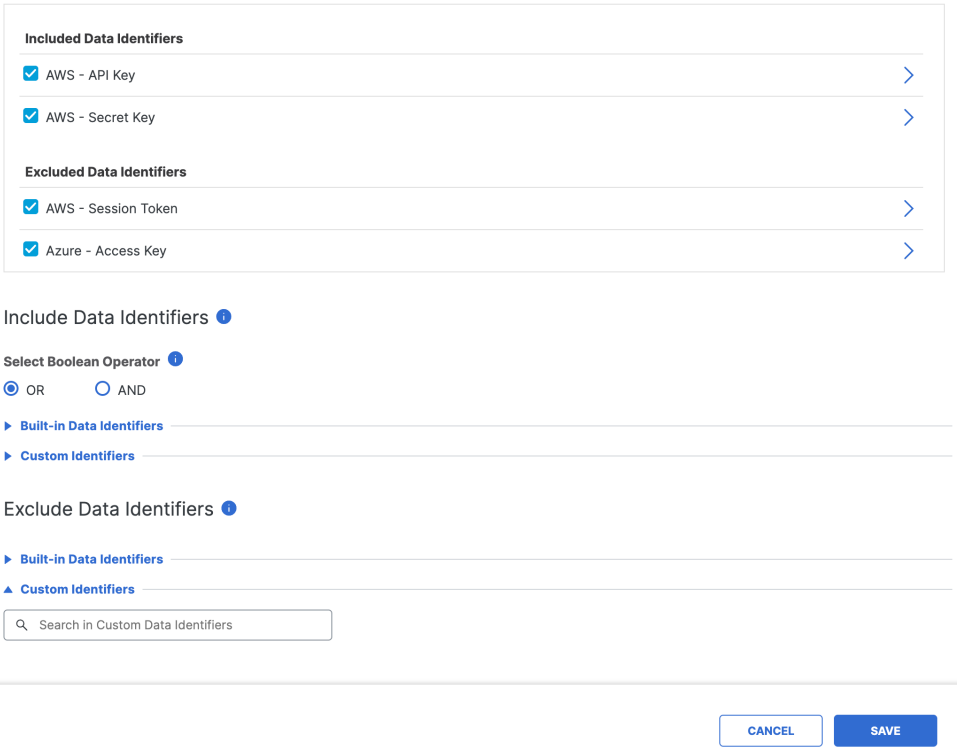
   - Custom Identifiers
   - Exact Data Match Identifiers

     Note

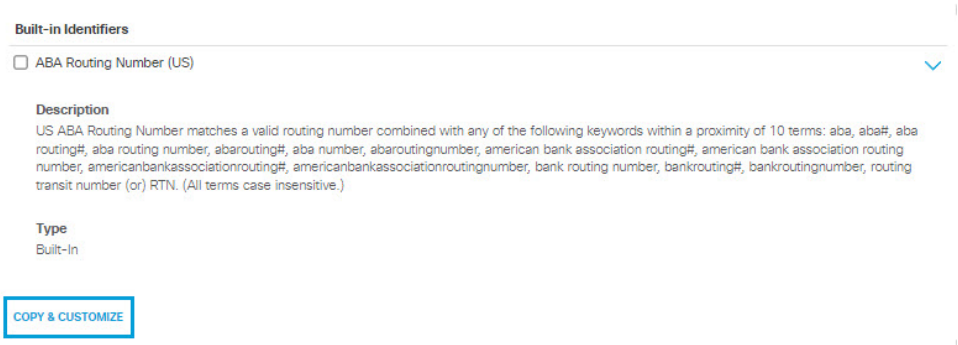
     Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

   - Indexed Document Match Identifiers

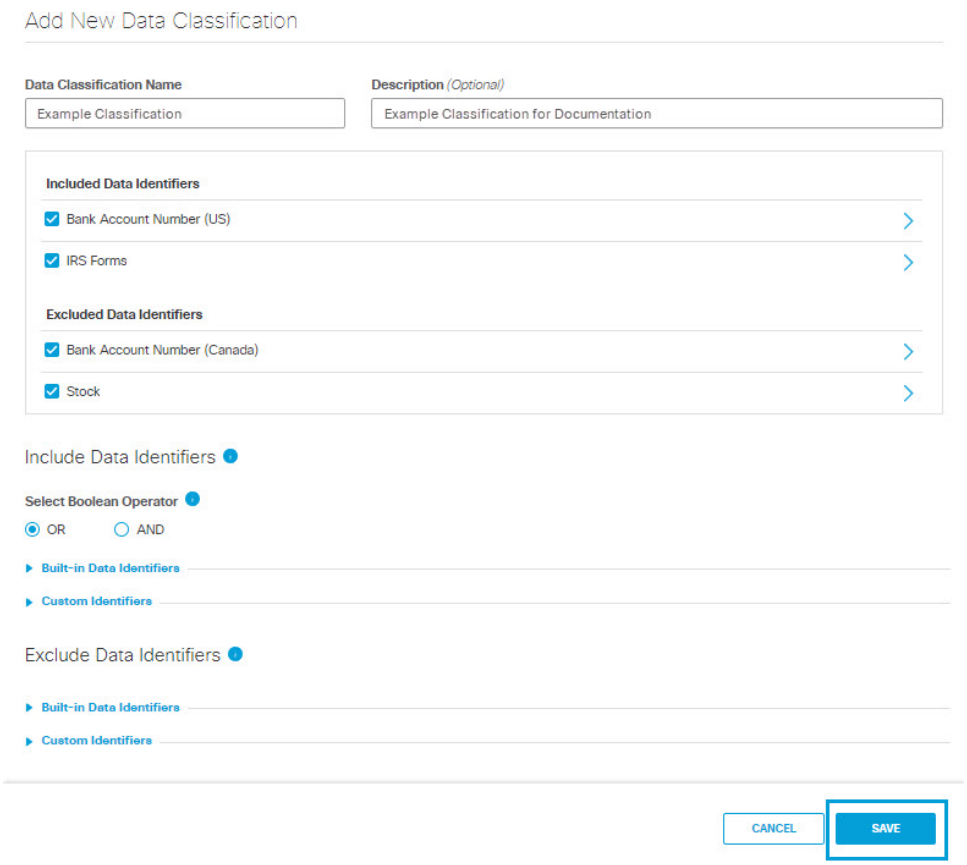
> **Note**
>
> Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)



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**.



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, or initiate a new Discovery Scan.

Copy and Customize a Built-In Data Classification

Describes Copy and Customize a Built-In Data Classification in Cisco Secure Access China. The system provides four different built-in data classifications you can use in real time rules and discovery scans.

The system provides four different built-in data classifications you can use in real time 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.

. You can create custom data classifications based on any of the 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 offers built-in data identifiers you can choose to remove from or add to your customized version of a built-in data classification:

- Built-In Identifiers

  These identify data using pattern matching and dictionary lookups. The descriptions shown in the GUI provide details about the type of data they match. For more information, see Built-In Data Identifiers.

- Machine Learning Identifiers

  These identify data based on AI analysis of example documents. For example, the identifier for Patent Files has been trained to recognize documents that are likely patent applications. For more information, see Built-In Data Identifiers.-->

The system offers three types of data identifiers you can create yourself applying different methods of data analysis. You can add these to your customized version of a built-in data classification:

- Custom Identifiers

  You can create custom identifiers to match specific terms and pattern expressions of your choosing. See Create a Custom Identifier .

- Exact Data Match Identifiers

  Exact Data Match Identifiers use fingerprinting to identify data in structured documents that match criteria you define. (See Create an Exact Data Match Identifier for more information.)

- Indexed Document Match Identifiers

  Indexed Document Match Identifiers use fingerprinting to identify data in unstructured documents that match criteria you define. See Create an Indexed Document Match Identifier for more information.

To delete or edit a data classification, see Delete or Edit a Classification.

Prerequisites

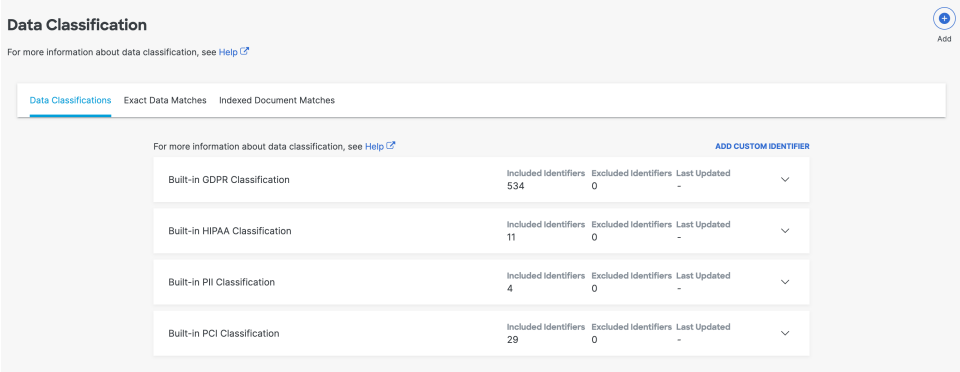
Lists the prerequisites for adding a data classification using a template. Full Admin user role. For more information, see Manage Accounts.

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

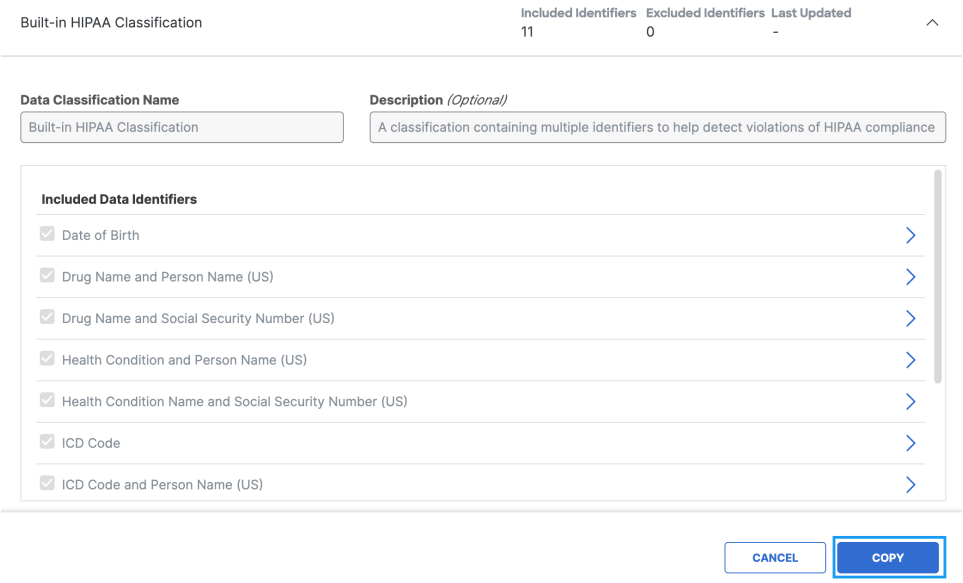
Procedure

Provides instructions for adding a data classification using a template. Expand Custom Identifiers and select additional data identifiers. (Custom Identifiers , Exact Data Match Identifiers , and Indexed Document Match Identifiers).

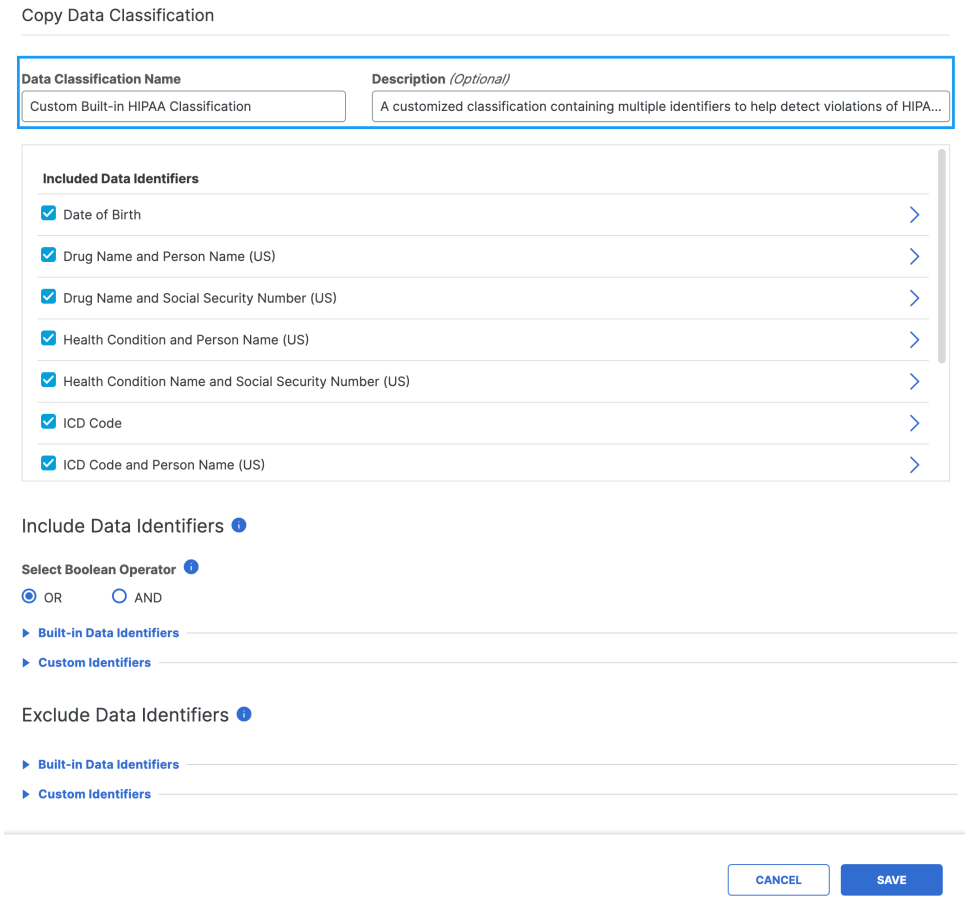
1. Navigate to **Secure > Settings > Data Classification > Data Classifications**.



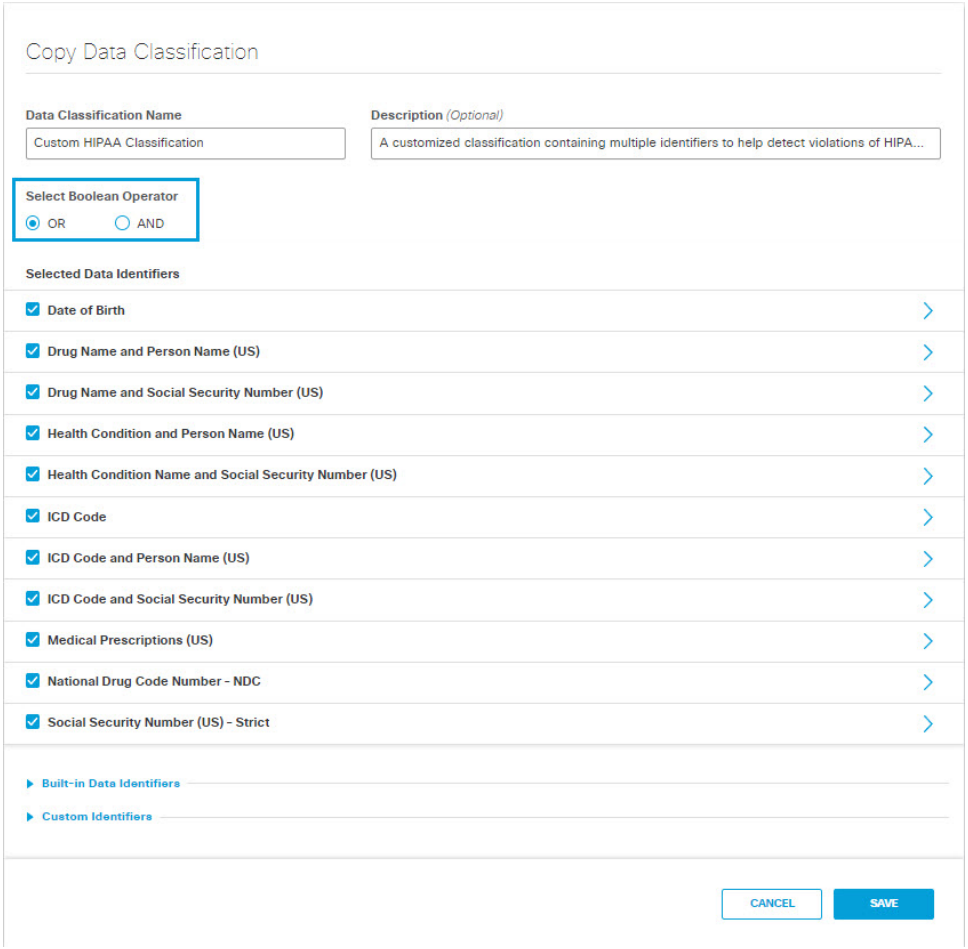
2. Expand one of the built-in data classifications and click **Copy**.



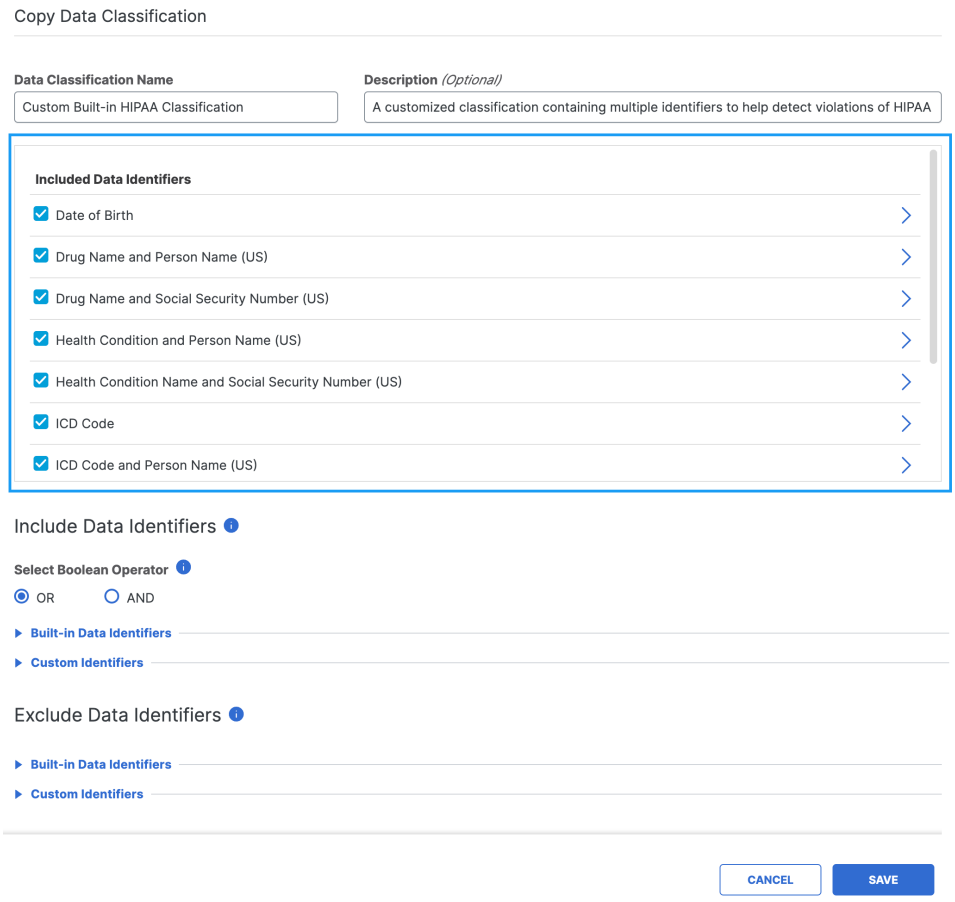
3. Give the new data classification a meaningful name and description.



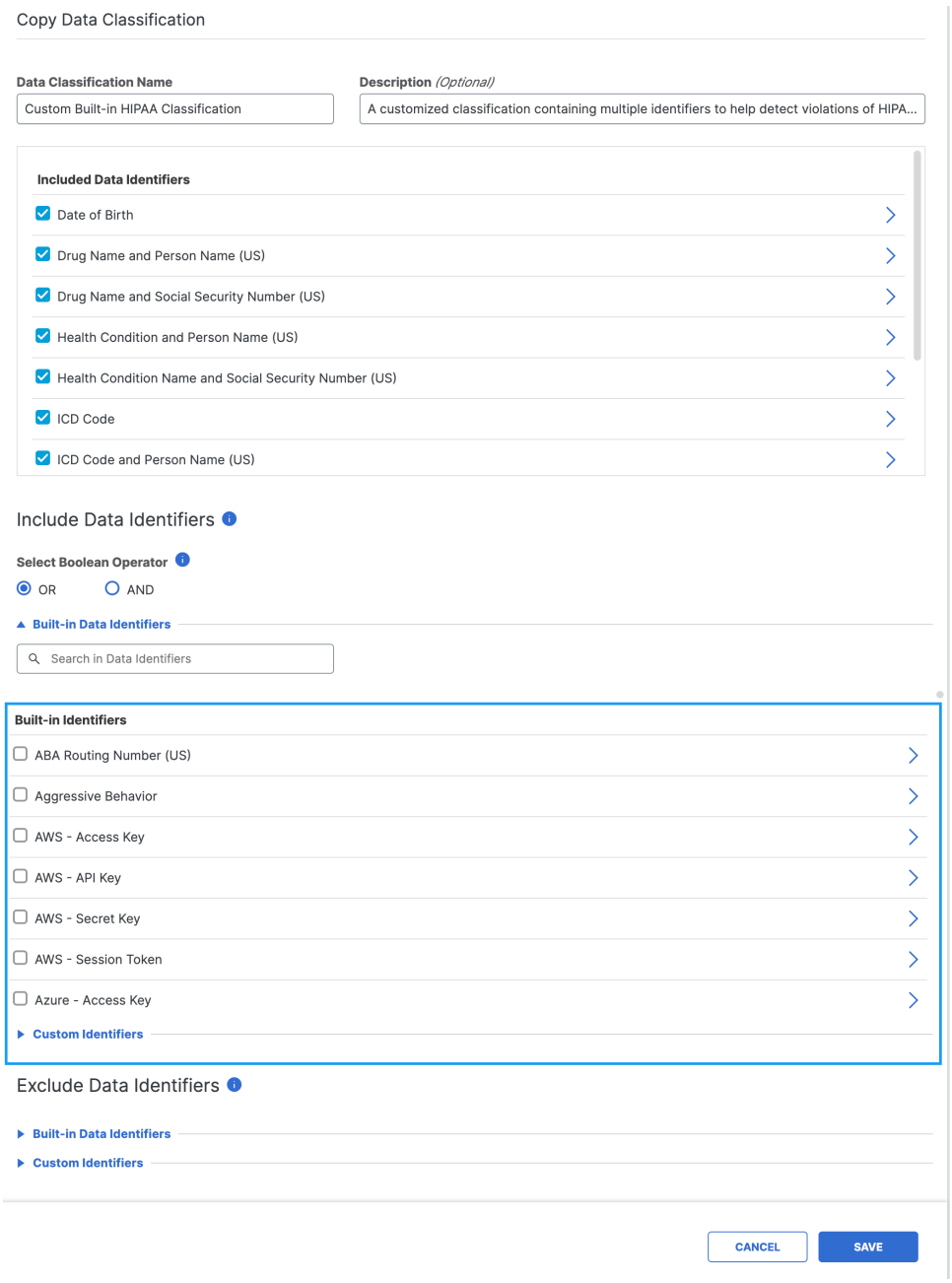
4. Make the desired changes to the new data classification. Choose from the following:
   - Change the Boolean operator
     - **OR**–At least one of the data identifiers selected must match during rule evaluation.
     - **AND**–All of the data identifiers selected must match during rule evaluation.



- Deselect pre-selected data identifiers.



- Expand **Built-in Data Identifiers** and select additional data identifiers.

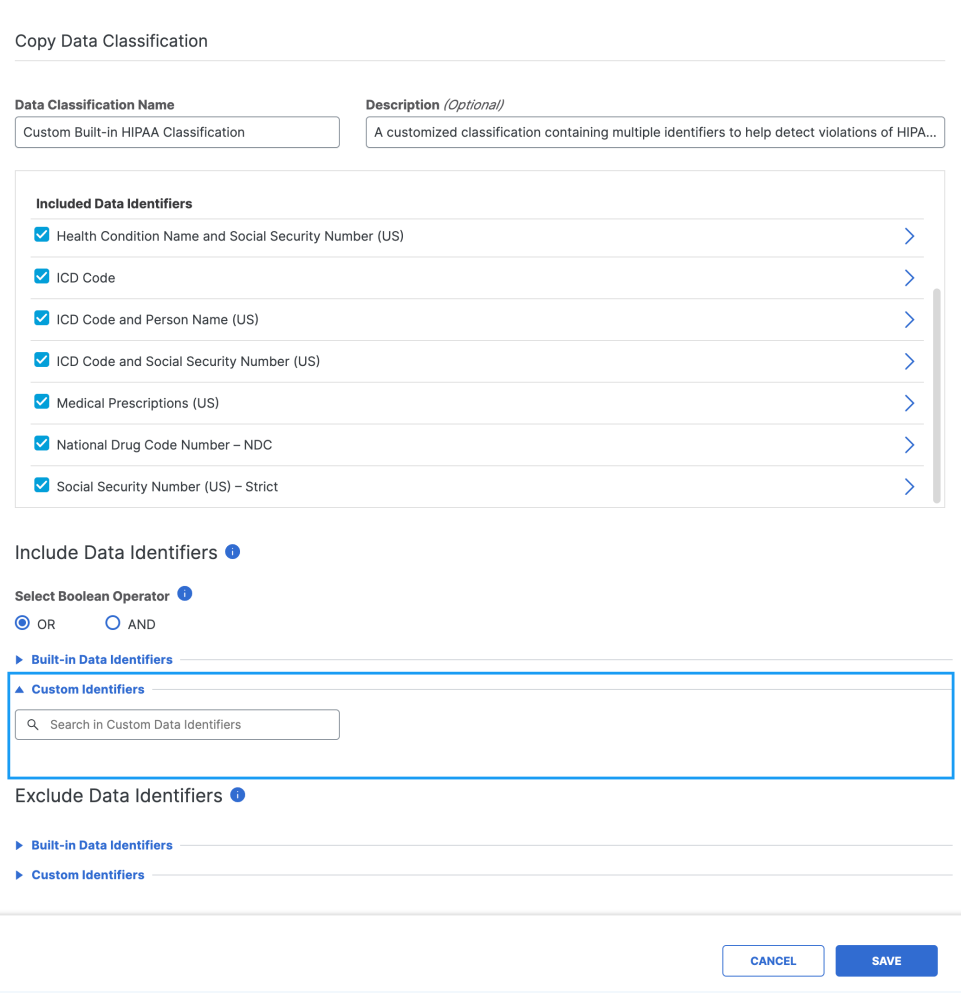


- Expand **Custom Identifiers** and select additional data identifiers.

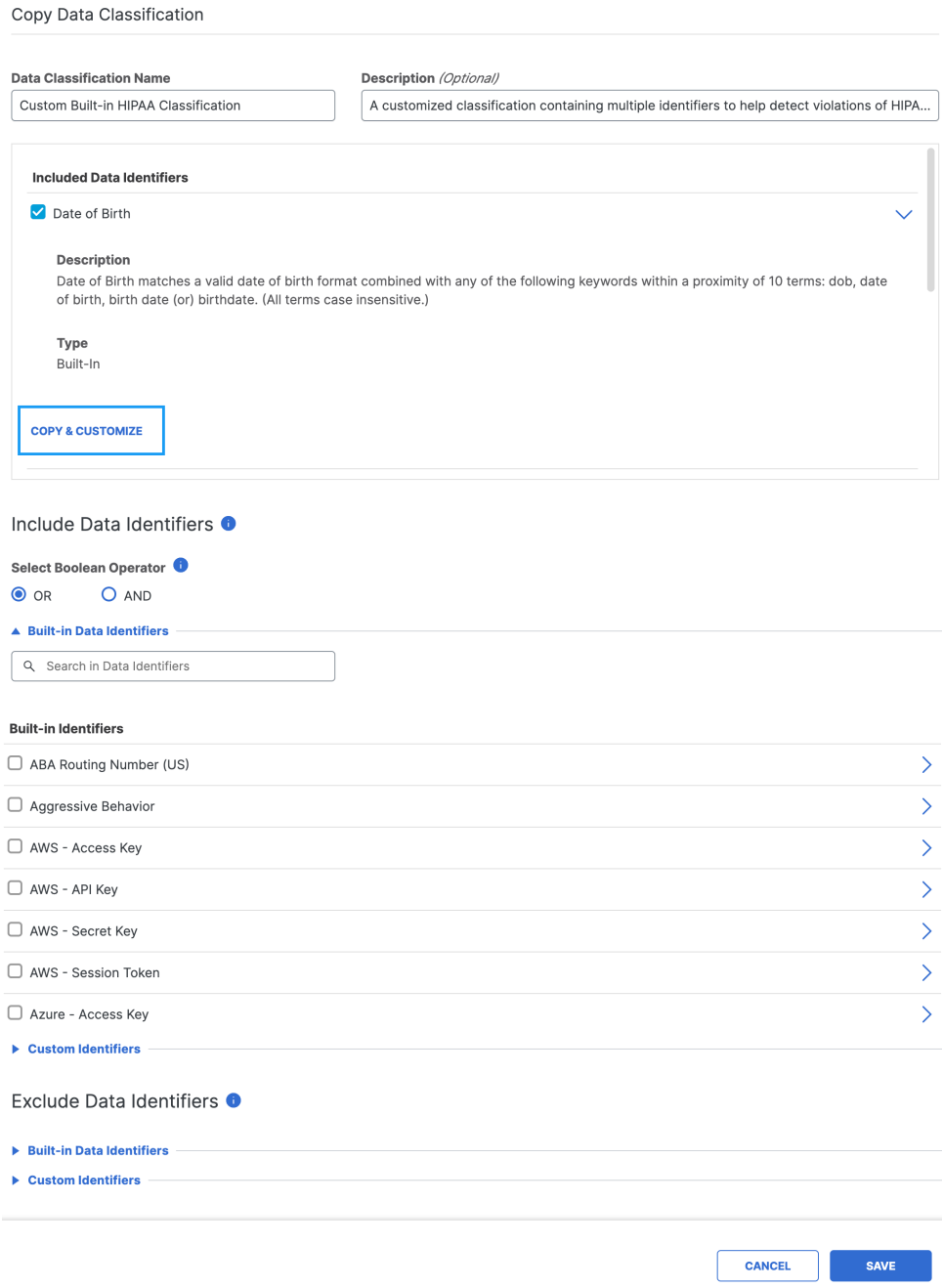
  (**Custom Identifiers**, **Exact Data Match Identifiers**, and **Indexed Document Match Identifiers**).

Note

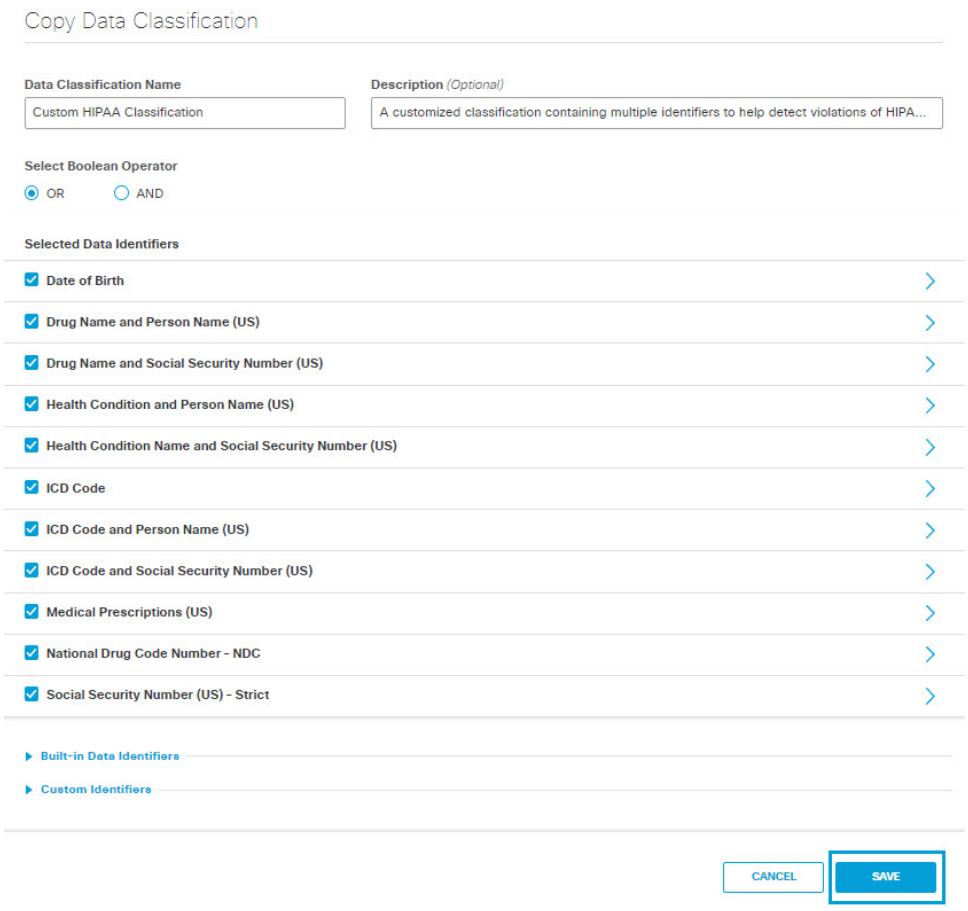
Exact Data Match Identifiers and Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier or Create an Indexed Document Match Identifier for more information.)



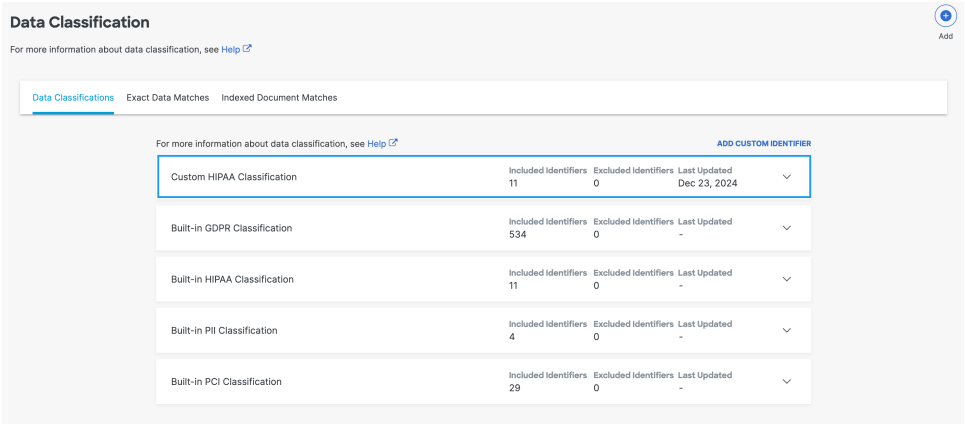
- You may expand any built-in data identifier and click **COPY & CUSTOMIZE** to create a new customized data identifier. See Copy and Customize a Data Identifier.


Copy Data Classification
Data Classification Name
Custom Built-in HIPAA Classification
Description (Optional)
A customized classification containing multiple identifiers to help detect violations of HIPA...
Included Data Identifiers
Date of Birth
Description
Date of Birth matches a valid date of birth format combined with any of the following keywords within a proximity of 10 terms: dob, date of birth, birth date (or) birthdate. (All terms case insensitive.)
Type
Built-In
COPY & CUSTOMIZE
Include Data Identifiers
Select Boolean Operator
OR
AND
Built-in Data Identifiers
Search in Data Identifiers
Built-in Identifiers
ABA Routing Number (US)
Aggressive Behavior
AWS - Access Key
AWS - API Key
AWS - Secret Key
AWS - Session Token
Azure - Access Key
Custom Identifiers
Exclude Data Identifiers
Built-in Data Identifiers
Custom Identifiers
CANCEL
SAVE

5. Click **Save**.



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 or initiate a new Discovery Scan.



Delete or Edit a Classification

Provides instructions for deleting or Edit a Classification in Cisco Secure Access China. After adding a data classification, you can delete or edit it at any time.

After adding a data classification, you can delete or edit it at any time. To add a data classification, see Add a Data Classification or Copy and Customize a Built-In Data Classification.

> **Note**
>
> You cannot edit or delete a built-in data classification.

Prerequisites

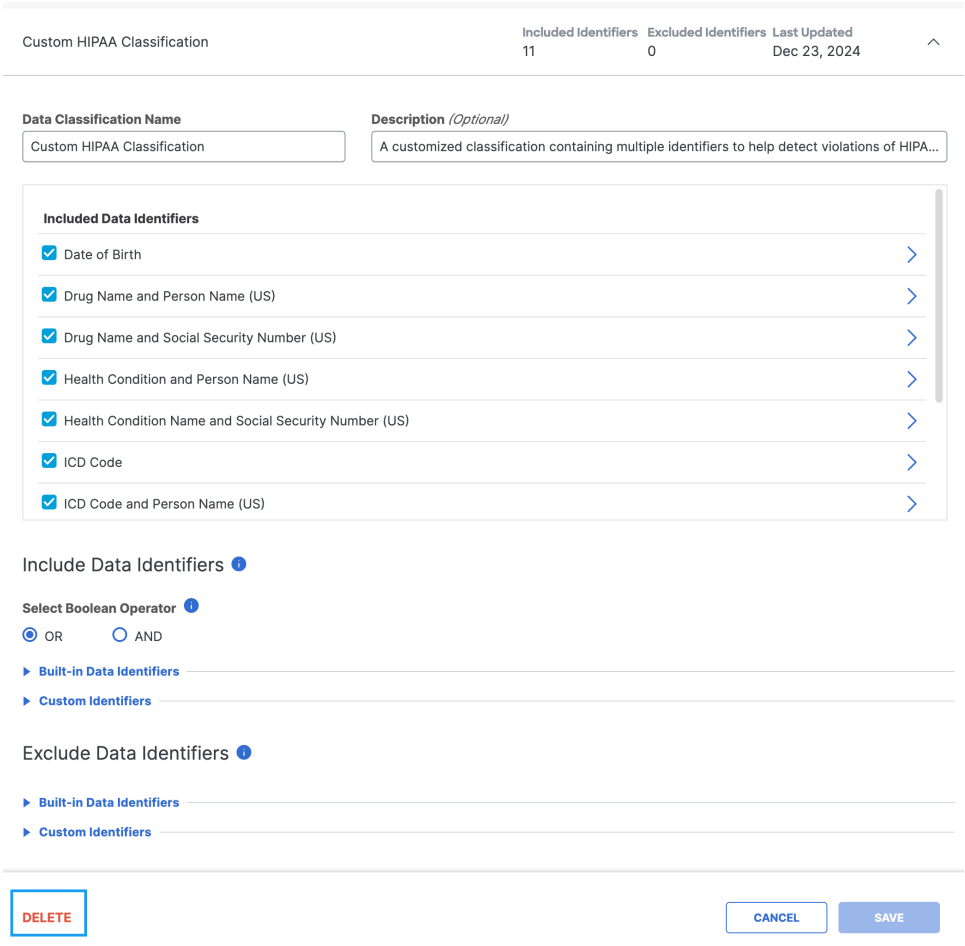
Lists the prerequisites for deleting or edit a classification, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

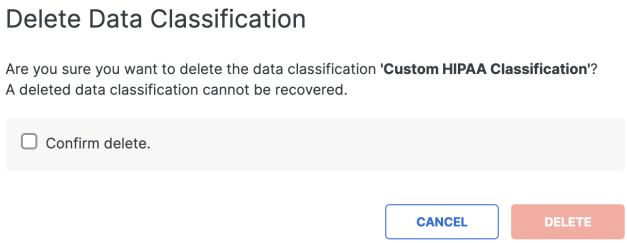
Delete a Classification

Provides instructions for deleting a classification. Navigate to Secure > Settings > Data Classification . Click Data Classifications. Expand a data classification and click Delete.

1. Navigate to **Secure > Settings > Data Classification**. Click **Data Classifications**.
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. You may not edit a built-in data classification. Navigate to Secure > Settings > Data Classification > Data Classifications.

> **Note**
>
> You may not edit a built-in data classification.

1. Navigate to **Secure > Settings > Data Classification > Data Classifications**.
2. Expand a data classification.
3. Edit the data classification as needed and click **Save**.

Create an Exact Data Match Identifier

Provides instructions for creating an Exact Data Match Identifier in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for creating an exact data match identifier. Full Admin user role. For more information, see Manage Accounts.

- Full Admin user role. For more information, see Manage Accounts.
- JVM version 17+
- The template CSV you upload must meet the following requirements:
  - The file can not be larger than 10 KB.
  - The second and ensuing rows may contain sample data; be aware, however, that this data will not be indexed unless it also appears in the source data CSV file.
- The DLP indexer supports data files with up to 55 million records. The exact records limit is determined by the total number of columns and the number of those are of Alphanumeric type. The indexer displays the exact limit when attempting to load a file that exceeds it. If your dataset is larger than the limit, you need to split the records into multiple files. For errors received when indexing a large file, see Memory Tuning for DLP Exact Data Matching Indexer.
- Both the template and source data CSV files must meet the following requirements:
  - A multi-term (multi-word) field can contain a maximum of 6 space-separated words.
  - The data file must contain only 1 byte or 2 byte UTF-8 encoded characters.
  - The first row of data must have between 1 and 50 fields and each row must have the same number of fields.
  - The first row of data must specify the name of each field, and each value must be unique.
  - Data in the second and ensuing rows must comply with the EDM field types and supported formats (see Exact Data Match Field Types).
  - The field names in the sample data template must match the field names in the actual data source file. The field names must appear in the same order in both files.

Caution

Do *not* create, edit, or view the template or source data CSV file using Microsoft Excel, as this may corrupt the file. Use a text editor.

Note

If any of the values provided in the source file to the DLP indexer fail to be validated as per the supported format, then the DLP indexer will skip that record and proceed with indexing the remaining records. The indexer also behaves in this manner for any records that may exceed the template-defined fields, and for empty rows or records with empty primary values. The position of the skipped records in the file will be provided as part of the output of the DLP indexer.

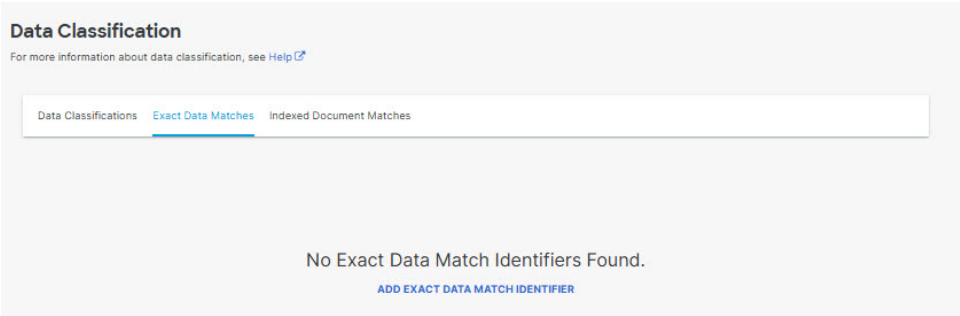
The following procedure uses the following example CSV file for both the template and indexed source data:

```
Email,SSN,Passport number - US,Credit card number
r_t@gmail.com, 113011111,123456789USA1234567U1234567, 5205105105105109
r_ppp@gmail.com, 248257990,123456789USA1234567U1234567, 4532237384050172
r_opop@gmail.com, 363265019,123456789USA1234567U1234567, 4532549977031249
ppo_t@gmail.com, 417279936,123456789USA1234567U1234567, 4539157470627290
```

Procedure

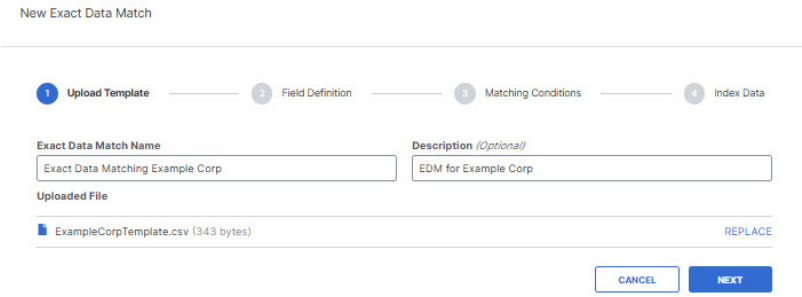
Provides instructions for creating an exact data match identifier. Provide a name and description for the exact data match, then upload sample data and click Next . Do not upload any real data in the CSV. Use only sample data for the template.

1. Navigate to **Secure > Settings > Data Classification > Exact Data Matches** and click **ADD EXACT DATA MATCH IDENTIFIER**.



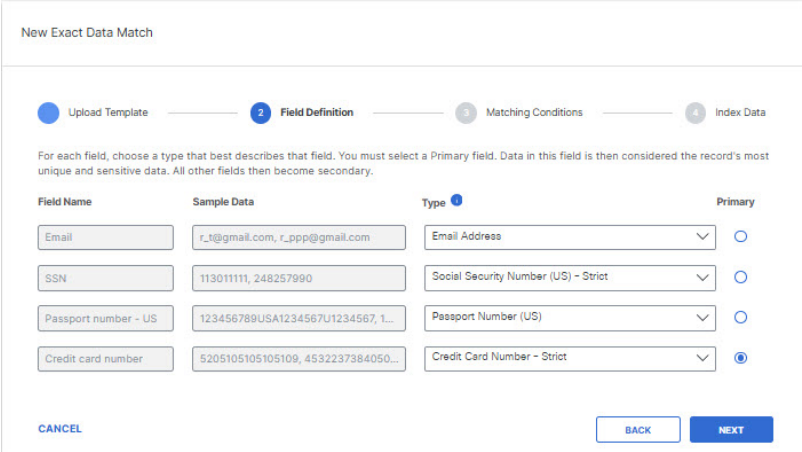
2. Provide a name and description for the exact data match, then upload sample data and click **Next**.

> **Note**
>
> Do not upload any real data in the CSV. Use only sample data for the template.



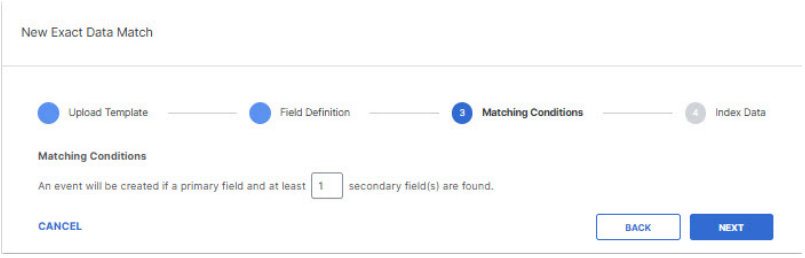
3. From the drop-down menu, choose the type of data of each field.

   The available field types are described in Exact Data Match Field Types:



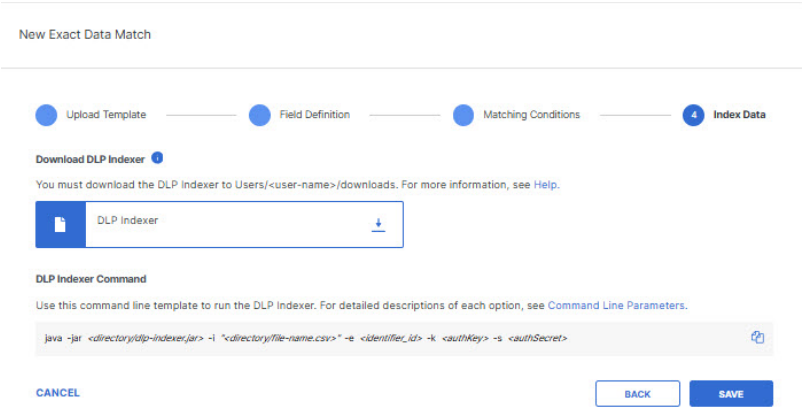
4. Select the Primary field that must be found with other data fields for the identifier to match and click **Next**. The primary field should be the field in the record to always match. The secondary fields are the number of fields in the record that should be present with the primary field to match.
5. Enter the minimum number of secondary fields required to be found within 10 terms of the primary field for a match. You can have no secondary field, or up to as many fields in the record that are not the primary field. For example, if at least 3 secondary fields are required, then the identifier will trigger an event only when 3 or more additional fields are found with the primary field. If the .csv file has only 1 column, then the secondary option is greyed-out and automatically set to 0. Click **Next**.

> **Note**
>
> The secondary fields must each be a different identifier.



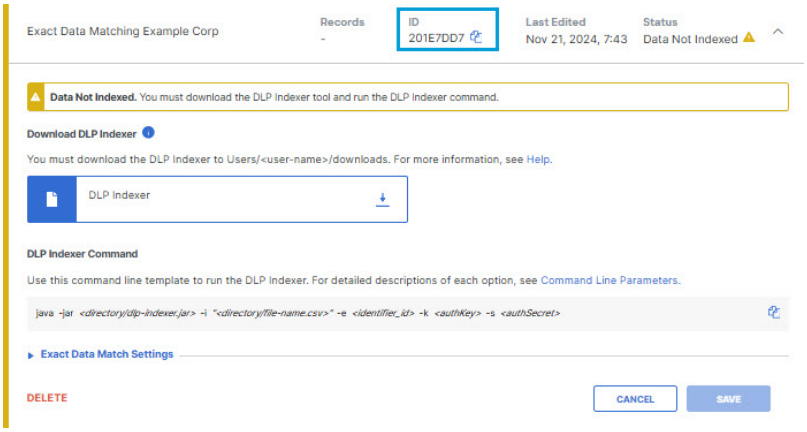
6. Click the download icon to download the DLP indexer. Then click **Save**.

> **Note**
>
> You can click on **Command Line Parameters** to view information about the command line arguments required to run the indexer.

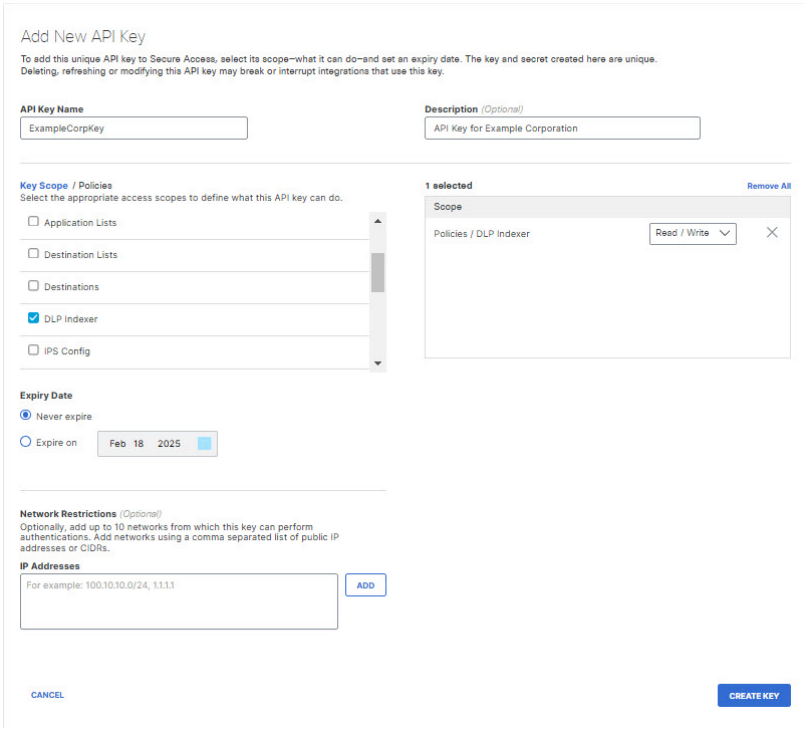


7. The EDM Identifier now has a status of **Data Not Indexed**. You can expand the listing to view the details about the EDM Identifier. When the EDM identifier status is **Data Not Indexed**, you can edit the field types, the primary field selection, and the matching conditions, but the EDM Identifier cannot be added to a data classification. Make note of the ID for th EDM Identifier; you will need it to run the DLP indexer.

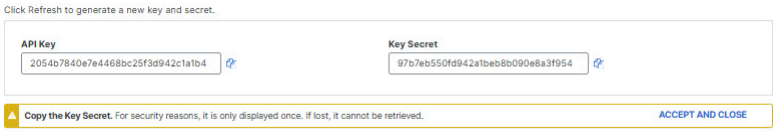
> **Note**
>
> The display page does not display the full EDM identifier ID; use the **Copy** icon to copy the ID



8. Create an API key and secret for the EDM data indexer.
   a. Navigate to **Admin > API Keys** and click **Open API Keys**.
   b. Click **Add** and provide an **API Key Name** and **Description** for the API Key.
   c. Select **Policies > DLP Indexer** for the scope and choose **Read/Write** for the permissions. Then click **Create Key**.



   d. Copy and save the API Key and Secret somewhere safe, as you will need them to run the DLP Indexer.



9. Click **ACCEPT AND CLOSE**.
10. Use the Secure Access DLP Indexer to index your data records. For more information on the indexer, see Index Data for an EDM.

    a. Move the indexer from the Downloads folder to a convenient location, such as the folder where the data records are stored.

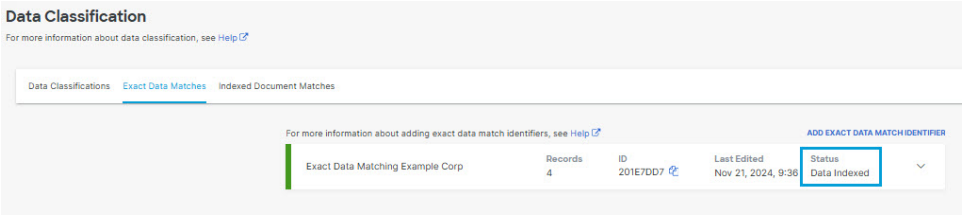
    b. Run the indexer in a terminal window with the following command:

    java -jar <*directory_path*>\dlp-indexer.jar -i " <*directory_path*>\<*source_file*>.csv" -e <*edm_template-id*> -k <*authKey*> -s <*authSecret*>

    where:

    - **<*directory_path*>\dlp-indexer.jar** –the relative path to the location of the DLP indexer
    - **" <*directory_path*>\<*source_file*>.csv"** –the relative path to the csv spreadsheet with the actual data records
    - **<*edm_template-id*>** –the ID of the EDM Identifier retrievable from the Umbrella UI (see Step 7)
    - **<*authKey*>** –the API Key previously saved at Step 8d
    - **<*authSecret*>** –the API Secret previously saved at Step 8d

    The EDM Identifier now has a status of **Data Indexed**.



The EDM Identifier now has a status of **Data Indexed**.

> **Note**
>
> When the EDM has a status of **Data Indexed**, you can add the EDM to a data classification but you can not edit the field types, primary field selection, or matching condition.

If you update your source file with new or changed records, you need to run the DLP indexer again on that file using the same EDM Identifier ID, API Key, and API Secret. This ensures that policies configured to use the EDM Identifier are updated to reflect the new data fingerprints. For more information, see Update the Indexed Data Set Periodically.

Index Data for an EDM

Describes Index Data for an EDM in Cisco Secure Access China. The DLP indexer creates irreversible fingerprints of critical data structured in records with a consistent format and uploads them to Secure Access to establish a custom EDM Identifier.

The DLP indexer creates irreversible fingerprints of critical data structured in records with a consistent format and uploads them to Secure Access to establish a custom EDM Identifier. EDM Identifiers enable Secure Access to protect sensitive data by using data fingerprinting techniques as opposed to pattern matching techniques.

EDM Identifiers can be added to a Data Classification (see Manage Data Classifications) as custom identifiers; DLP rules that use these identifiers can monitor and/or block files that match the data you have indexed.

You need to run the DLP indexer in two different circumstances:

- When you initially create an EDM Identifier, you run the indexer on the data set you want to detect. This topic provides basic information for running the indexer, but for a description of the process to use the indexer within the context of creating an EDM Identifier, see Create an Exact Data Match Identifier. You cannot use the indexer to create an EDM Identifier without also performing the steps described in that topic.
- When the data set to be detected changes, you run the indexer to produce an updated version of the EDM Identifier. This process is described in Update the Indexed Data Set Periodically.

> **Note**
>
> To see a summary of the indexer options available, invoke the indexer with the **-h** option. (**java -jar <*directory-path*>\dlp-indexer.jar -h**.)

Prerequisites

Lists the prerequisites for index data for an edm. A multi-term (multi-word) field can contain a maximum of 6 space-separated words.

- 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. Be sure you have the API key and secret. (See Step 8 in Create an Exact Data Match 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. For the full procedure to create an EDM identifier, see Create an Exact Data Match Identifier.

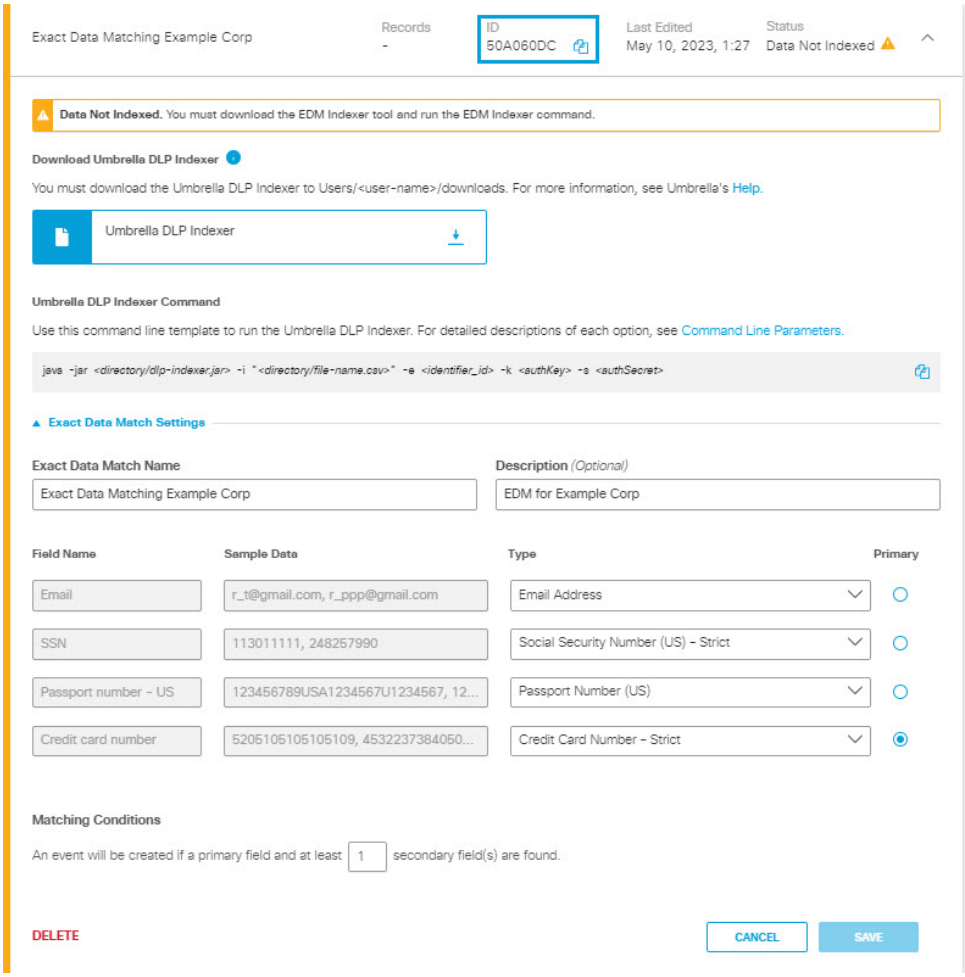
1. Review the Prerequisites, especially:
   - Be sure you have the API key and secret. (See Step 8 in Create an Exact Data Match Identifier.)
   - Be sure you have the EDM Identifier ID. (See Step 7 in Create an Exact Data Match Identifier.)

1. 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 preiodically updating the indexed data set.

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.

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

Describes 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:

- Confirm you have the latest version of the Java Development Kit installed.
- Confirm that you have your PATH system variable set correctly:

  1. 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**
  2. 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 Secure Access Support to assist you with troubleshooting.

Exact Data Match Field Types

Describes Exact Data Match Field Types in Cisco Secure Access China. When creating an Exact Data Match (EDM) template, you must choose an EDM type for each field provided.

When creating an Exact Data Match (EDM) template, you must choose an EDM type for each field provided. The EDM types are similar to the Built-in Data Identifiers in that specific patterns must be found to match the identifier. Unlike Built-In Identifiers, EDM types do not use keywords to find data matches.

Supported EDM Types

Describes supported EDM Types. ABA Routing Number (US) – A 9-digit number used by banks to identify specific financial institutions in the United States.

- **ABA Routing Number (US)**– A 9-digit number used by banks to identify specific financial institutions in the United States.
- **Alphanumeric**–Up to 6 words composed of 1 and 2-byte UTF-8 encoded characters, delimited by spaces.

- **Bank Account Number (US)**–A 5-digit number denoting a bank account number issued in the United States.
- **Carte nationale d'identité sécurisée – CNIS (France)**–A 12-digit number denoting the French national identity card number.
- **Credit Card Number**–A valid 15 or 16-digit credit card number that passes the Luhn validation and includes any of the following delimiters: space, no space, ~, or -.
- **Date**–A date value matching one of the following formats where the `<delimiter>` is no space, /, or -. :
- the European format of `<dd><delimiter><mm><delimiter><yyyy>` or
- the American format of `<mm><delimiter><dd><delimiter><yyyy>`
- **Email Address**–A valid email address using ASCII characters.
- **Fiscal Identification Number – Número de identificación fiscal – NIF (Spain)**– A number issued to Spanish nationals for identification purposes. The pattern matches`<ddddddddd><a>` where:
  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
- **ICD Code**–A number matching the pattern of one of the typical International Classification of Diseases (ICD) codes.
- **Individual Taxpayer Identification Number – ITIN (US)**–A United States tax processing number issued by the Internal Revenue Service (IRS). The pattern must match the format of `<ddd><delimiter><dd><delimiter><dddd>` where:
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, or -
- **International Bank Account Number – IBAN (UK)**–An international bank account number for the UK. The pattern matches a format of `<aadd><delimiter><aaaadddd><delimiter><dddd><delimiter><dddd><delimiter><dd>` where:
  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, or -
- **IP Address**–A valid IPv4 address.
- **National Drug Code Number (NDC)**–Segments of the National Drug Code (NDC) used in the united States to identify drugs for human use. The pattern matches a format of `<ddddd><delimiter><ddd><delimiter><dd>` where:
  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is ~ or -
- **National Insurance Number – NINO (UK)**–An identification number issued to individuals by the United Kingdom Department for Work and Pensions. The pattern matches with a format of `<aa><delimiter><dd><delimiter><dd><delimiter><dda>` where:
  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, -, or .
- **Passport Number (US)**–An identification number issued to citizen and non-citizen nationals of the United states. The pattern must match a format of `<ddddddddd>USA<ddddddd>U<ddddddd>` where `d` is any ASCII digit from 0 to 9.
- **Passport Number (UK)**–An identification number that serves as proof of nationality or immigration status in the United Kingdom. The pattern must match one of the following formats:
  - a 9-digit number
  - `<ddddddddd>GBR<ddddddd>U<ddddddd>` where `d` is any ASCII digit from 0 to 9

- **Postcode (UK)**– A number matching the typical UK postal code patterns, where the number can include a space between the inward and outward segments.
- **Social Security Number - INSEE (France)**– National identification numbers for The National Institute of Statistics and Economic Studies issued at birth to French nationals. The number can be 12 or 15 digits. The pattern matches a format of `<ddddddddddddd><delimiter><dd>` where:
  - d is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~
- **Social Security Number (US) – Strict**–An identification number issued in the United States to citizens, permanent residents, and temporary working residents. The pattern matches `<aaa><delimiter><dd><delimiter><dddd>` where:
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, -, or .

Create an Indexed Document Match Identifier

Provides instructions for creating an Indexed Document Match Identifier in Cisco Secure Access China. 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:

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.)

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**.)

Prerequisites

Lists the prerequisites for creating an indexed document match identifier. Full Admin user role. For more information, see Manage Accounts.

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

- JVM version 17+
- The source file(s) you index must be in one of the formats supported by the DLP policy, listed here.

Limitations

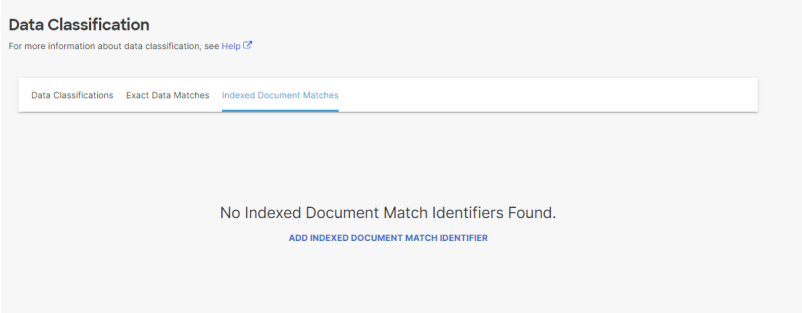
Describes limitations. The total amount of indexed text for all the IDMs in your organization must not exceed 1 GB. You can increase this limit at no cost; contact customer support. The DLP indexer displays an error message if you exceed your allotted quota.

- 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.

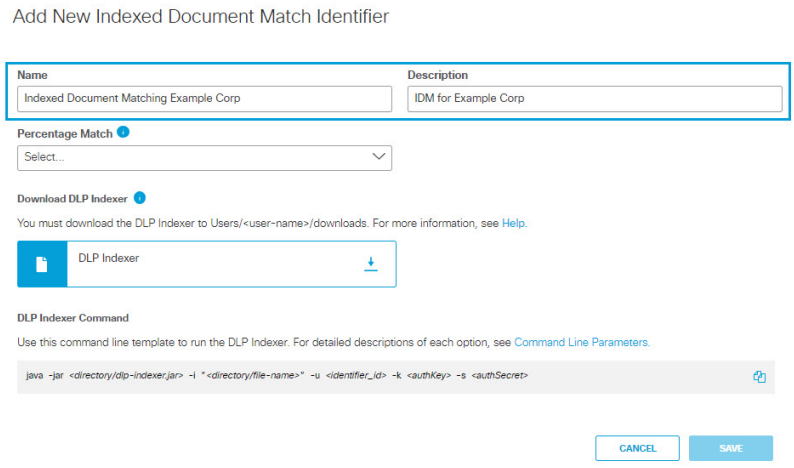
Create an Indexed Document Match Identifier

Provides instructions for creating an indexed document match identifier. High: 80% or more of the scanned document must match a document indexed for the IDM.

1. Navigate to **Secure > Settings > Data Classification > Indexed Document Matches** and click **ADD INDEXED DOCUMENT MATCH IDENTIFIER**.

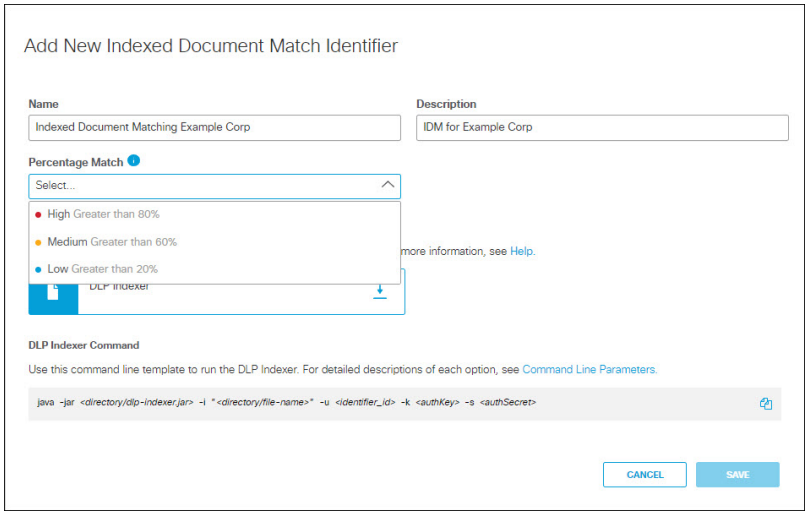


2. Provide a name and description for the Indexed Document Match Identifier.



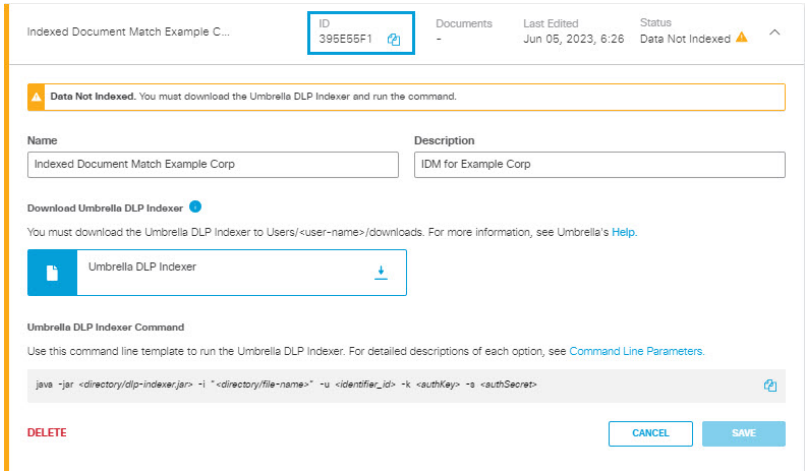
3. Select the level of percentage match required for a scanned document to be considered a match against a document included in the IDM:
   - High: 80% or more of the scanned document must match a document indexed for the IDM.
   - Medium: 60% or more of the scanned document must match a document indexed for the IDM.

- Low: 20% or more of the scanned document must match a document indexed for the IDM.

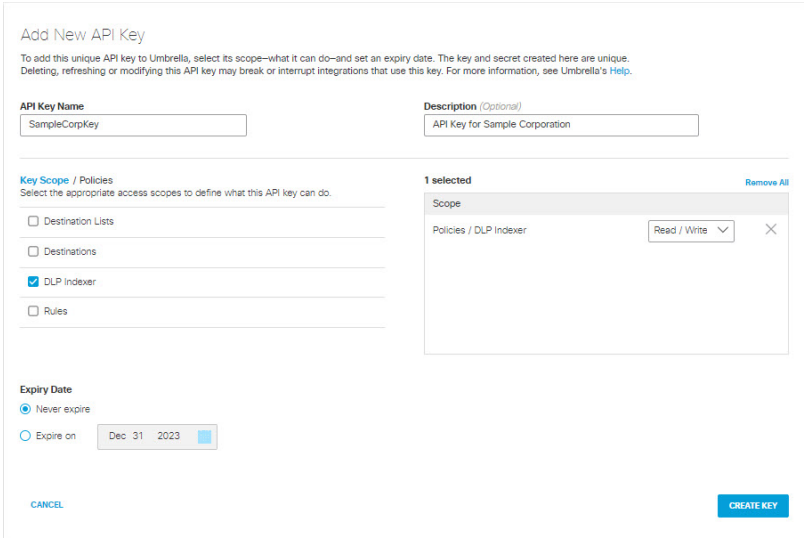


4. If you have not already downloaded the Umbrella DLP indexer, click the download icon to do so.
5. Click **Save.**
6. The Indexed Document Match Identifier now has a status of **Data Not Indexed.** You can expand the listing to view the details about the IDM Identifier. After you have indexed the IDM 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.

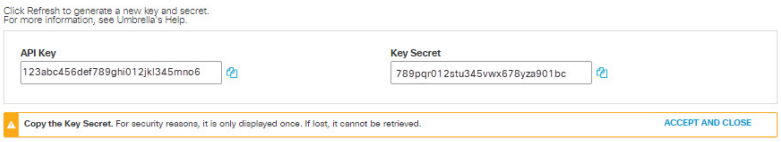
> **Note**
>
> The display page does not display the full IDM Identifier ID; use the **Copy** icon to copy the ID.



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.

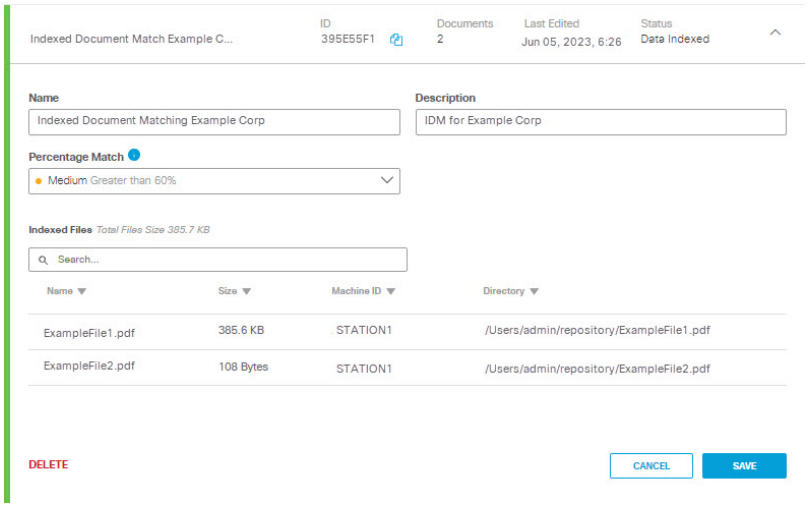


8. Use the Umbrella DLP indexer to fingerprint your example files.

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.



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

Provides instructions for monitoring the indexed data set and re-index as needed. 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.

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

Describes 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:

- Confirm you have the latest version of the Java Development Kit installed.
- Confirm that you have your PATH system variable set correctly:

  1. Check the location where you have Java installed.

     - For Windows this is normally **C:\Program Files\Java\jdk-<version-number>\bin</version-number>**

- For Linux this is normally **/usr/java/jdk-<version-number>/bin</version-number>**

2. 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.

40 Built-in Data Identifiers

Topics:

- Built-in Data Identifiers

Provides an overview of Built-in Data Identifiers in Cisco Secure Access China, including Copy and Customize a Data Identifier, Create a Custom Dictionary, and Custom Regular Expression Patterns. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Built-in Data Identifiers

Describes Built-in Data Identifiers in Cisco Secure Access China. Secure Access provides a wide selection of built-in data identifiers you can choose to incorporate into DLP policy to classify a wide range of sensitive data, both structured and unstructured.

Secure Access provides a wide selection of built-in data identifiers you can choose to incorporate into DLP policy to classify a wide range of sensitive data, both structured and unstructured.

The built-in identifier can classify specific data values based on pattern matching, bloom filters, and dictionaries incorporating proximity terms.

The ML Document Classification are built-in identifiers based on LLM (Large Language Model) that was trained to classify unstructured sensitive data based on its true context.

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.

Copy and Customize a Data Identifier

Describes Copy and Customize a Data Identifier in Cisco Secure Access China. You can copy and customize your own data identifier based on threshold and proximity.

You can copy and customize your own data identifier based on threshold and proximity. For a list of built-in data identifiers, see Built-in Data Identifiers.

Prerequisites

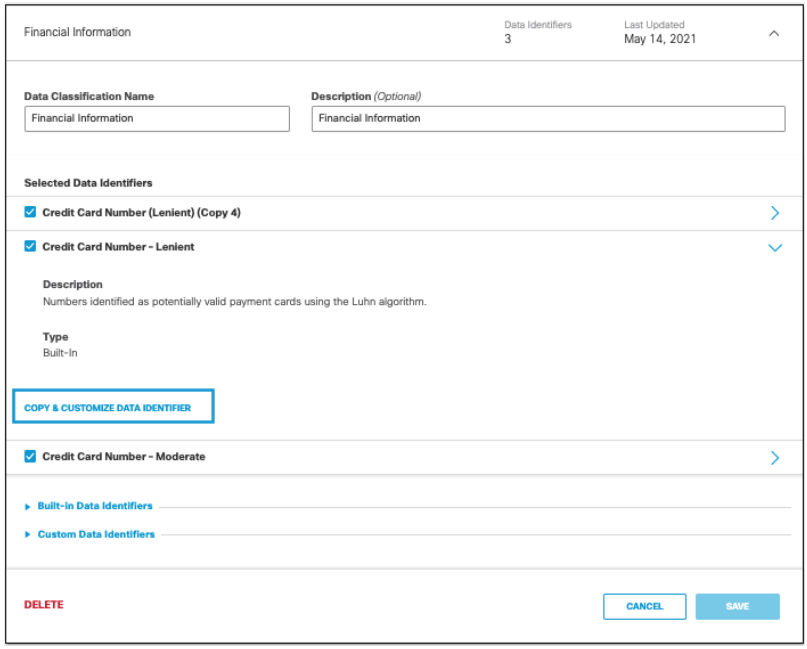
Lists the prerequisites for copy and customize a data identifier. Full Admin user role. For more information, see Manage Accounts.

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

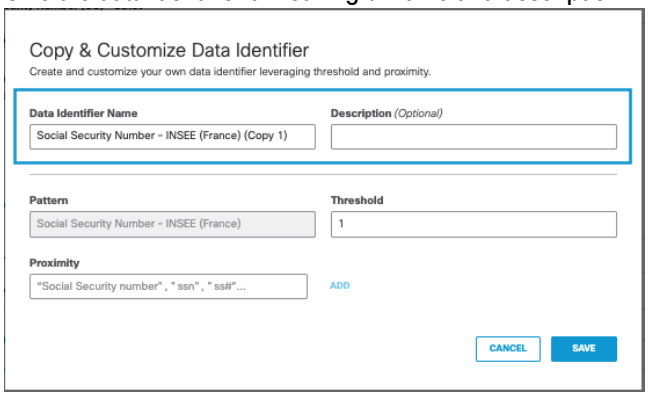
Procedure

Provides instructions for copy and customize a data identifier. For Threshold , add the number of instances of this identifier you would like matched in a document before it is activated.

1. Navigate to **Secure > Settings > Data Loss Prevention Classifications**.
2. Expand a data classification.
3. Expand a data identifier and click **Copy and Customize Data Identifier**.

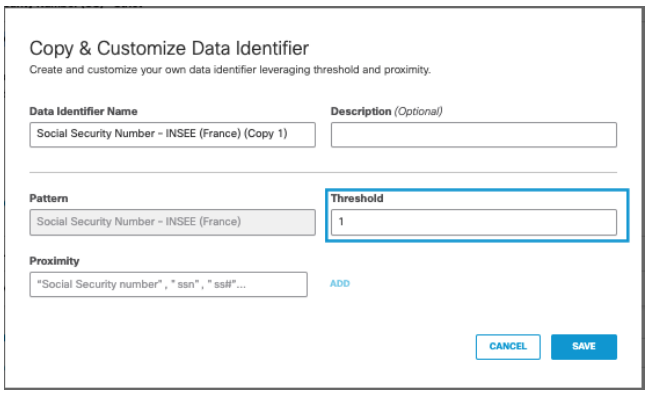


4. Give the data identifier a meaningful name and description.



5. For **Threshold**, add the number of instances of this identifier you would like matched in a document before it is activated.

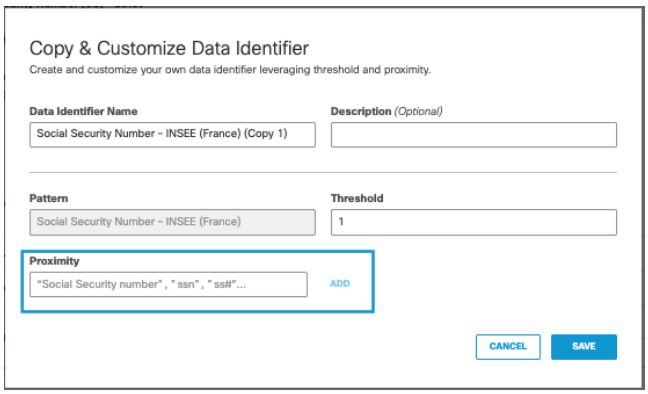
   A threshold of 10, for example, only monitors or blocks a file if 10 instances of the identifier are found in the file.



6. For **Proximity**, add proximity keywords to match against the pattern. The keywords need to be found within 10 terms of the original pattern.

   For example, add keywords such as "Visa" and "Mastercard" to match against a credit card identifier.

   Then click **Add**.



7. Click **Save**.

   The custom identifier appears under Custom Data Identifiers when creating or editing a classification.

> **Note**
>
> Pattern
>
> The pattern field is the built-in regular expression designed for this identifier and cannot be edited.

Create a Custom Dictionary

Provides instructions for creating a Custom Dictionary in Cisco Secure Access China. You can add terms and expression patterns to a custom dictionary, which can be used when editing or creating a data classification.

You can add terms and expression patterns to a custom dictionary, which can be used when editing or creating a data classification. To add a data classification, see Add a Data Classification.

Prerequisites

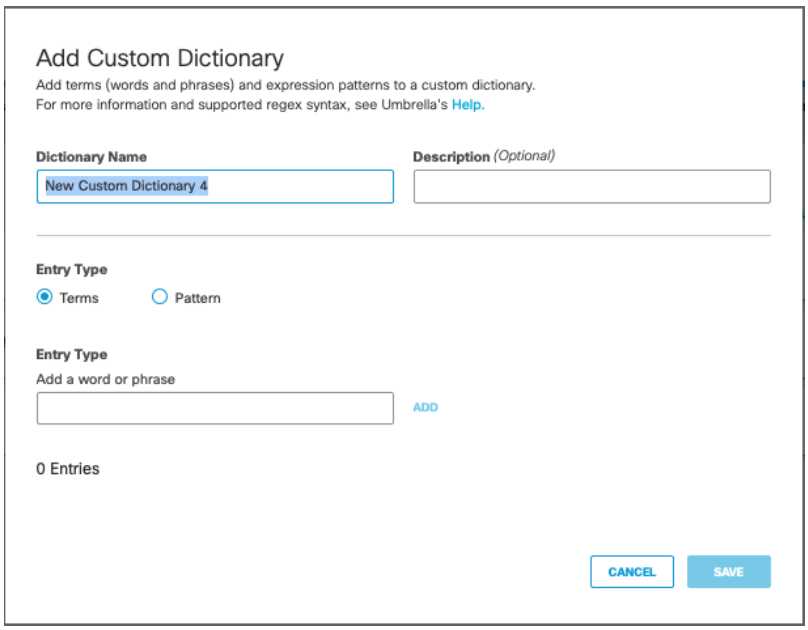
Lists the prerequisites for creating a custom dictionary, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for creating a custom dictionary. Enter sample text in the Test box. Click Test to verify the pattern matches, then click Add.

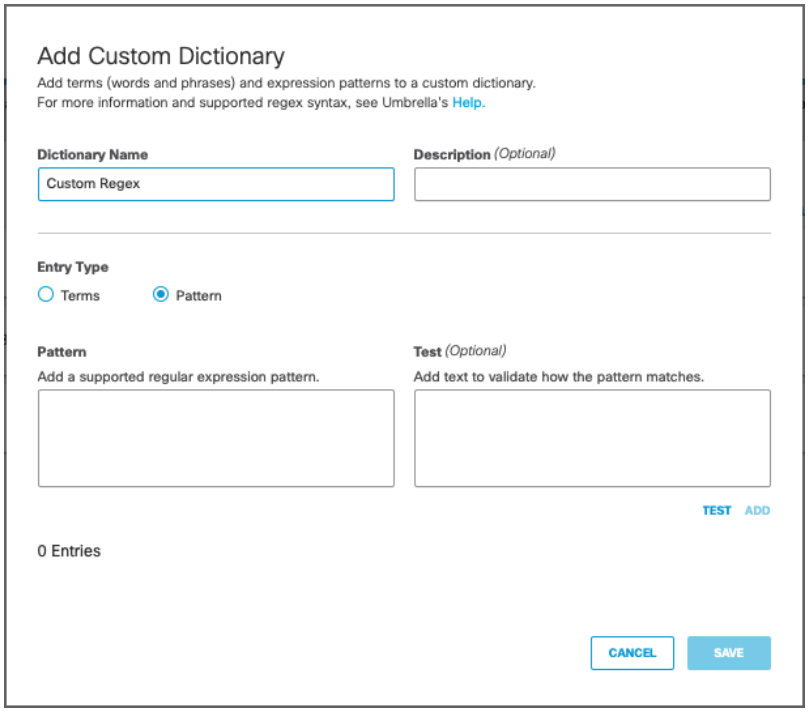
1. Navigate to **Secure > Settings > Data Loss Prevention Classifications**.
2. Click **Add Custom Dictionary**.
3. Give the custom dictionary a meaningful name and description.



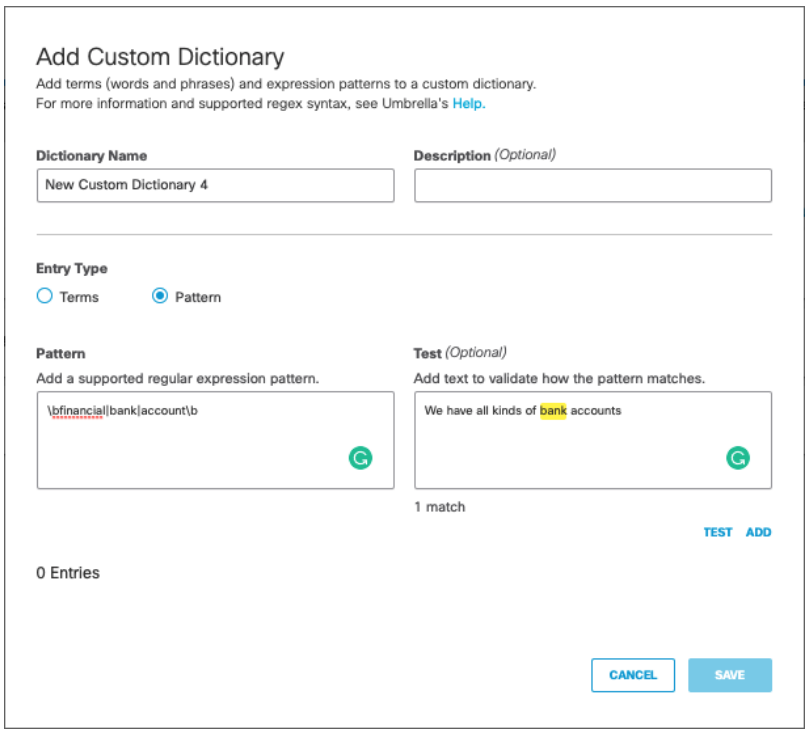
4. Add terms and patterns to your custom dictionary.

> **Note**
>
> Terms and patterns cannot be uploaded or entered as a CSV. Each term must be entered individually.

   a. For **Terms**, add up to 100 terms and click **Add** for each term.
   b. For **Pattern**, enter 3-150 characters of a regular expression. You can add up to 10 patterns to a custom dictionary. For more information, see Custom Regular Expression Patterns.



Enter sample text in the **Test** box. Click **Test** to verify the pattern matches, then click **Add**.



5. Click **Save**.

   Your custom dictionary appears under **Custom Data Identifiers** when editing or creating a classification.

Custom Regular Expression Patterns

Describes Custom Regular Expression Patterns in Cisco Secure Access China. 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 that apply when administrators create custom regular expression patterns for matching traffic in Secure Access China. for administrators to review.

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. The following must be used for these character definitions:. 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. | alternations have a maximum of 20 per pattern.

- 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 in Cisco Secure Access China and outlines Drug Name, Health Condition, and ICD-10 Code. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

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.

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.

41 Manage Logging

Topics:

- Manage Logging

Provides an overview of Manage Logging in Cisco Secure Access China, including Enable Logging, Enable Logging to Your Own S3 Bucket, and Enable Logging to a Cisco-managed S3 Bucket. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Logging

Provides instructions for managing logging in Cisco Secure Access China. Secure Access allows for the logging of events and traffic.

Secure Access allows for the logging of events and traffic.

Only event data is stored in a data warehouse. This is any data that might appear in a Secure Access report.

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 in Cisco Secure Access China. Secure Access allows for the logging of events and traffic through a policy's 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.

Prerequisites

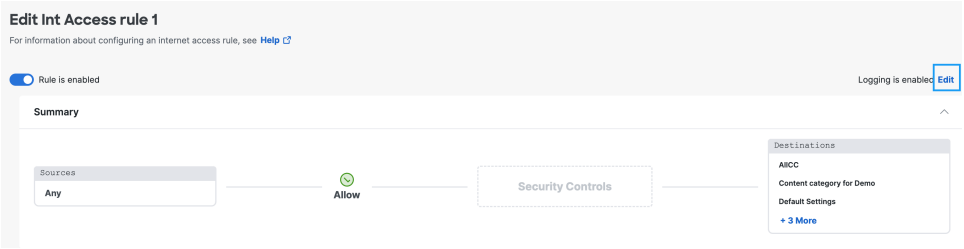
Lists the prerequisites for enabling logging, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

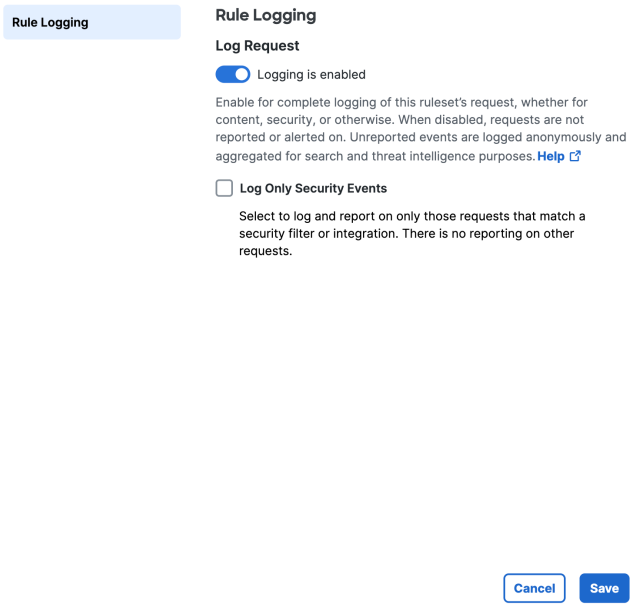
Procedure

Provides instructions for enabling logging. Disabling logging for a ruleset impacts reporting as nothing is logged to report on. For each rule, click Edit and make changes as needed.

1. For each rule, click **Edit** and make changes as needed.



2. Make changes as needed and click **Save**.



Settings are:

- **Log Requests** – Logs 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.

> **Note**
>
> Disabling logging for a ruleset impacts reporting as nothing is logged to report on.

Enable Logging to Your Own S3 Bucket

Provides instructions for enabling logging to Your Own S3 Bucket in Cisco Secure Access China. You can configure Secure Access to log events to an Amazon S3 bucket that you manage.

You can configure Secure Access to log events to an Amazon S3 bucket that you manage. To enable logging to a self-managed Amazon S3 bucket, follow the prerequisite steps to set up an AWS account and create an Amazon S3 bucket. Once you have created an S3 bucket in Amazon, configure Secure Access to use it for the storage of logs.

Prerequisites

Lists the prerequisites for enabling logging to your own S3 bucket. Amazon requires a credit card in case your usage exceeds free plan usage.

- Full Admin user role. For more information, see Manage Accounts.
- A login to Amazon AWS service (http://aws.amazon.com/console/). If you don't have an account, Amazon provides free sign-up for S3.

> **Note**
>
> Amazon requires a credit card in case your usage exceeds free plan usage.

- A bucket configured in Amazon S3 to be used for storing logs. For more information, see Amazon's S3 documentation.

> **Note**
>
> Periods in S3 bucket names are not supported.

JSON Bucket Policy

Describes jSON Bucket Policy. When you set up your Amazon S3 bucket, you must add a bucket policy that accepts uploads from Secure Access.

When you set up your Amazon S3 bucket, you must add a bucket policy that accepts uploads from Secure Access. Copy the following preconfigured JSON and substitute your S3 bucket name for `bucketname`. Then, paste the Secure Access S3 bucket policy into your Amazon S3 bucket policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-cn:iam::146618076670:role/CICDBotRole"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws-cn:s3:::test-stats-api-prod-4/*"
        },
        {
            "Sid": "2",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws-cn:iam::146618076670:role/CICDBotRole"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws-cn:s3:::test-stats-api-prod-4/*"
        },
        {
            "Sid": "8",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws-cn:iam::146618076670:role/CICDBotRole"
            },
            "Action": "s3:DeleteObject",
            "Resource": "arn:aws-cn:s3:::test-stats-api-prod-4/*"
        },
        {
            "Sid": "3",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-cn:iam::146618076670:role/CICDBotRole"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws-cn:s3:::test-stats-api-prod-4"
        },
        {
            "Sid": "4",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-cn:iam::146618076670:role/CICDBotRole"
            },
```

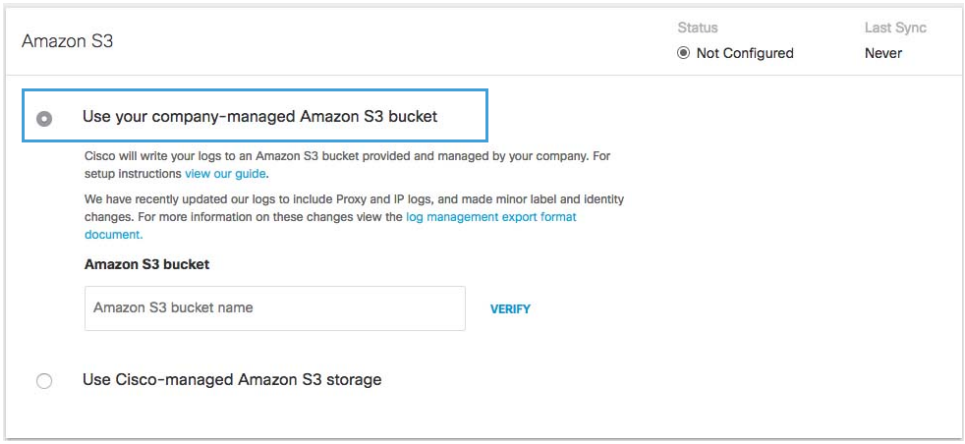
```
            "Action": "s3:ListBucket",
            "Resource": "arn:aws-cn:s3:::test-stats-api-prod-4"
        }
    ]
}
```

Procedure

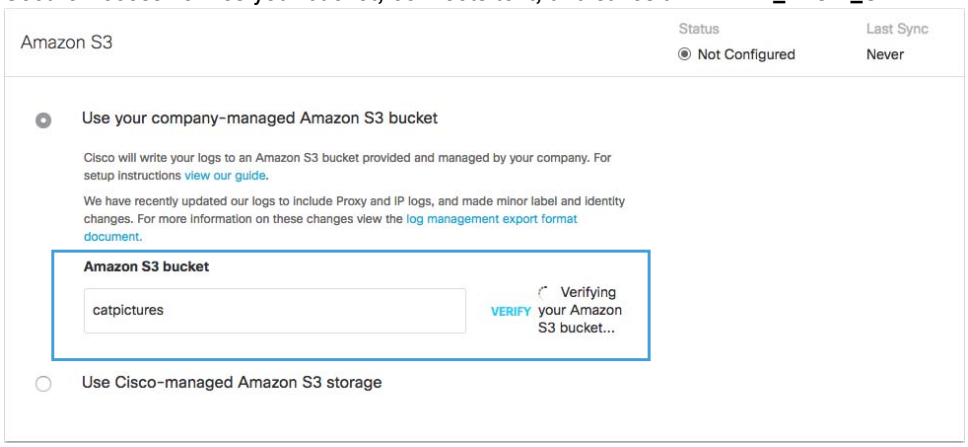
Provides instructions for enabling logging to your own S3 bucket. Note: You must first configure a bucket in Amazon S3. For more information, see Amazon's S3 documentation.

Note: You must first configure a bucket in Amazon S3. For more information, see Amazon's S3 documentation.

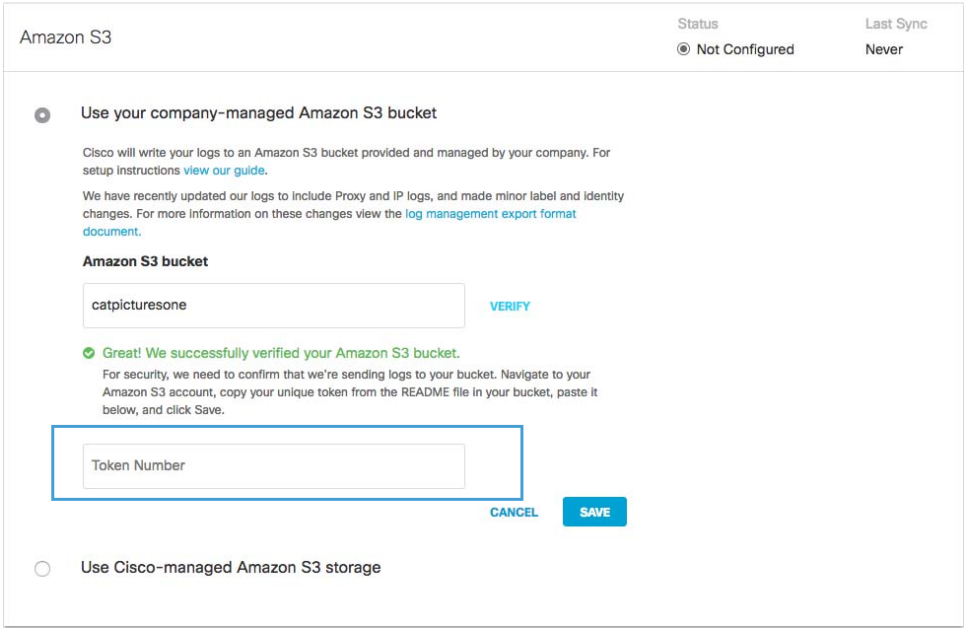
1. Navigate to **Admin > Log Management** and in the **Amazon S3** area select **Use your company-managed Amazon S3 bucket**.



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-west-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

Provides instructions for downloading files from the s3 bucket locally. You can use (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

Lists the prerequisites for enabling logging to your own S3 bucket prerequisites 1. 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.

- 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-west-1/dnslogs
/opt/splunk/etc/apps/TA-cisco_umbrella/data/
```

Enable Logging to a Cisco-managed S3 Bucket

Provides instructions for enabling logging to a Cisco-managed S3 Bucket in Cisco Secure Access China. You can configure Secure Access to log events to an Amazon S3 bucket that Cisco manages.

You can configure Secure Access to log events to an Amazon S3 bucket that Cisco manages. Cisco configures all Cisco-managed buckets to use Amazon Server-Side Encryption with S3-Managed Keys (SSE-S3, AES-256). The encryption and keys are managed by AWS, meaning Cisco and the customer don't exchange keys, but the data is still encrypted at rest. More information can be found on the AWS website by searching for "SSE-S3, AES-256".

Secure Access provides access to Cisco Managed S3 buckets using Amazon's IAM system. When the S3 bucket is provisioned, Secure Access provides the KEY and SECRET directly to you through the Secure Access Log Management UI. Secure Access does not store your keys during the generation process. If you lose your keys, you can not recover them. Instead, you must rotate the keys using the Secure Access Log Management UI.

The Cisco IAM user can write files to the S3 bucket, and the customer IAM user can read from the bucket. Customers can rotate their keys at any time.

Customer logs are also encrypted in transit between Cisco's Log Management infrastructure and S3.

Prerequisites

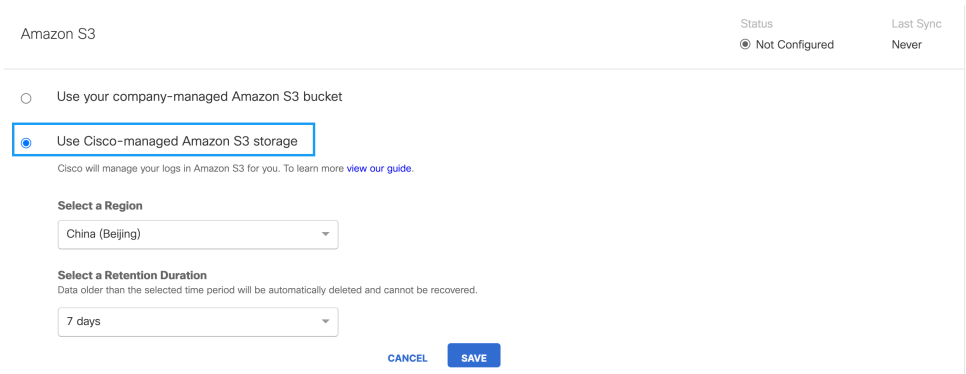
Lists the prerequisites for enabling logging to a Cisco managed S3 bucket. Full Admin user role. For more information, see Manage Accounts.

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

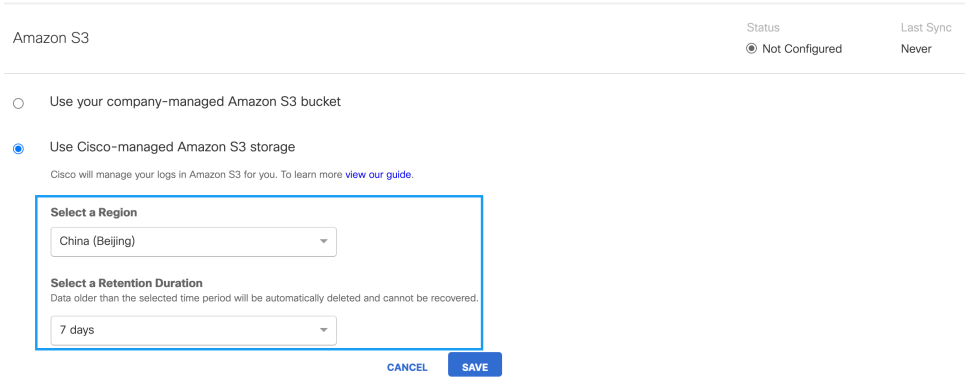
Procedure

Provides instructions for enabling logging to a Cisco managed S3 bucket. Secure Access activates its ability to export to an AWS S3 account. When activation is complete, the Amazon S3 Summary page appears.

1. Navigate to **Admin > Log Management** and in the **Amazon S3** area select **Use a Cisco-managed Amazon S3 bucket**.

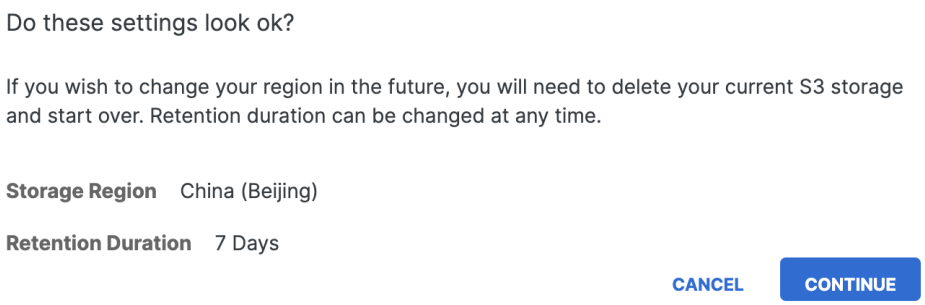


2. Select a **Region** and a **Retention Duration**.

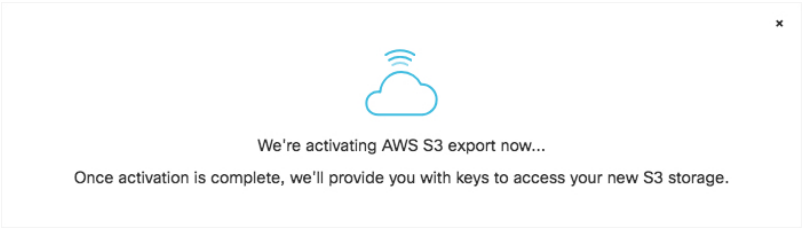


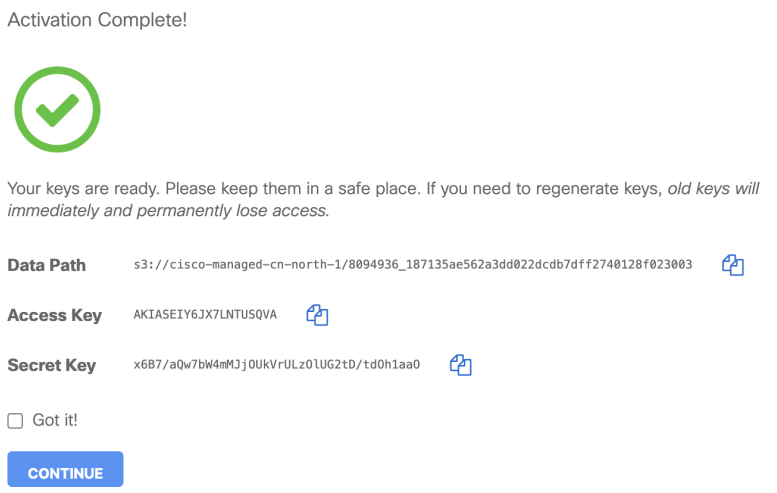
- **Select a Region**–Regional endpoints are important to minimize latency when downloading logs to your servers. The regions match those available in Amazon S3; however, not all regions are available. For example, China is not listed. Pick a region that is closest to you. If you wish to change your region in the future, you will need to delete your current settings and start over.
- **Select a Retention Duration**–Select 7, 14, or 30 days. Beyond the selected time period, all data will be purged and cannot be retrieved. We recommend a smaller time period if your ingestion cycle is regular. The retention duration can be changed at any time.

3. Click **Save** and then **Continue** to confirm your settings.



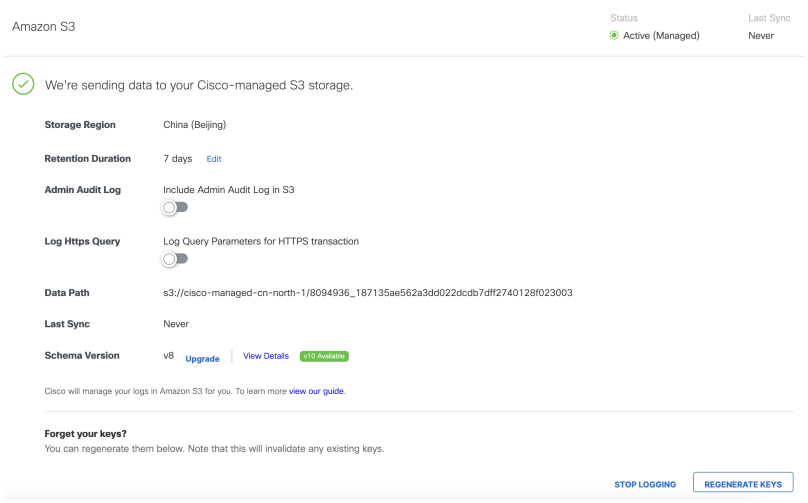
Secure Access activates its ability to export to an AWS S3 account. When activation is complete, the Amazon S3 Summary page appears





4. Copy credentials from this page and store them in a safe place. This is the only time that the **Access** and **Secret** keys are made available to you. These keys are required to access your S3 bucket and download logs. If you lose these keys, they must be regenerated.
5. Once keys are copied and safe, select **Got it** and then click **Continue**.

> **Note**
>
> **Continue** is unavailable until you check **Got it**.



S3 Bucket Data Path

Describes S3 Bucket Data Path. The Secure Access Amazon S3 Summary page provides the Data Path to your Amazon bucket. A Secure Access data path contains the following path fields:.

The Secure Access Amazon S3 Summary page provides the **Data Path** to your Amazon bucket. A Secure Access 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 the AWS S3 bucket managed by Cisco (`cisco-managed`), a dash (-), and the **AWS region**.

2. **AWS S3 bucket directory prefix**–the directory prefix (customer folder name) to the Cisco-managed AWS S3 bucket.

Sample S3 Bucket Data Path:

```
cisco-managed-us-west-1/2069997_6ff2802af17337def701c2e7816cf14913zf848a
```

Use the data path to your Cisco-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 Umbrella logs found in your AWS S3 bucket. For more information, see Cisco Cloud Security App for Splunk.

Download Files From the S3 Bucket Locally

Provides instructions for downloading files from the s3 bucket locally. You can use (CLI) to download files from a Cisco-managed S3 bucket to your local directory.

You can use the Amazon command-line interface (CLI) to download files from a Cisco-managed S3 bucket to your local directory.

Prerequisites

Lists the prerequisites for enabling logging to a Cisco managed S3 bucket prerequisites 1. Run the AWS CLI to download your files from a Cisco-managed S3 bucket to your local directory. To run the AWS CLI command in test mode (without syncing files), use the --dryrun flag.

- Install the AWS CLI to your system. For more information, see Installing or updating the latest version of the AWS CLI.

Run the AWS CLI to download your files from a Cisco-managed S3 bucket to your local directory. To run the AWS CLI command in test mode (without syncing files), use the `--dryrun` flag.

AWS CLI command syntax:

```
aws s3 sync s3://DATAPATH/ /path/to/local/directory/
```

Note: You must append a forward slash (**/**) to the DATAPATH.

Detailed sample command:

```
aws s3 sync
s3://cisco-managed-us-west-1/2069997_6ff2802af17337def701c2e7816cf14913zf848a/
 /opt/splunk/etc/apps/TA-cisco_umbrella/data/
```

Best Practices: Download Files From the S3 Bucket

Describes best Practices: Download Files From the S3 Bucket. When you delete downloaded files from the local directory, only delete files that are older than the Retention Duration value configured in Secure Access. Otherwise, the next sync command will download the deleted files again.

- When you download files from a Cisco-managed S3 bucket, ensure that you only download one copy of each log file. If you download log files multiple times, Cisco reserves the right to suspend the download of logs from a Cisco-managed S3 bucket (through the rotation of keys or other methods).
- When you delete downloaded files from the local directory, only delete files that are older than the **Retention Duration** value configured in Secure Access. Otherwise, the next sync command will download the deleted files again.

Stop Logging

Describes Stop Logging in Cisco Secure Access China and outlines Prerequisites and Procedure. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

You can stop logging at any time. When logging is stopped, Secure Access immediately stops sending logs to your S3 storage.

Prerequisites

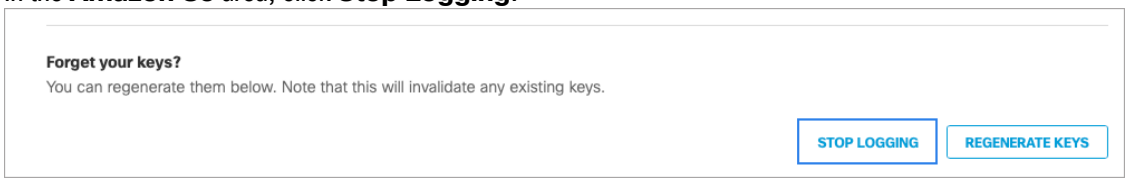
Lists the prerequisites for stopping logging, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

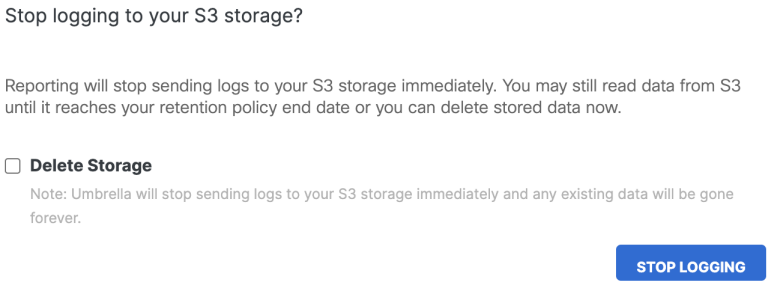
Procedure

Provides instructions for stopping logging. Navigate to Admin > Log Management. In the Amazon S3 area, click Stop Logging. Click Stop Logging to confirm your request.

1. Navigate to **Admin > Log Management**.
2. In the **Amazon S3** area, click **Stop Logging**.



3. Click **Stop Logging** to confirm your request.



Delete Logs

Provides instructions for deleting logs in Cisco Secure Access China. You can delete previous log data when you stop logging.

You can delete previous log data when you stop logging. See Stop Logging.

Prerequisites

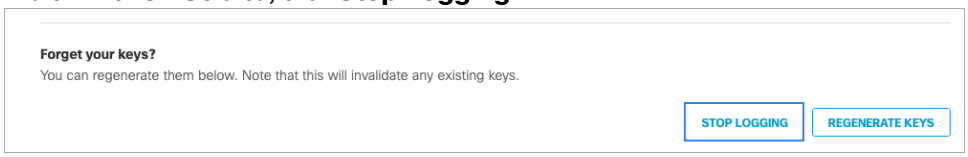
Lists the prerequisites for deleting logs, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

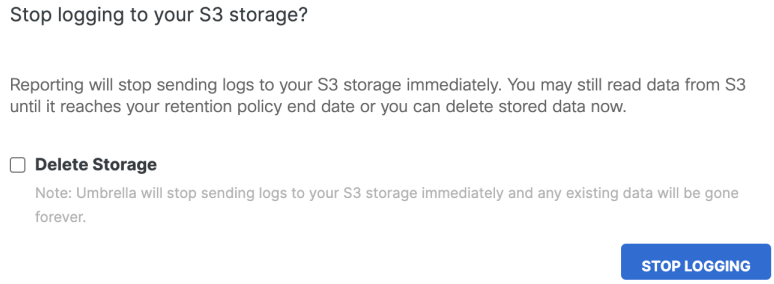
Procedure

Provides instructions for deleting logs. You can restart logging at any time. Navigate to Admin > Log Management. In the Amazon S3 area, click Stop Logging.

1. Navigate to **Admin > Log Management**.
2. In the **Amazon S3** area, click **Stop Logging**.



3. Check **Delete Storage**, then click **Stop Logging & Delete** to confirm your request. Logging of activity data stops and all activity logs are deleted.



4. Click **Start Logging** to resume logging.

   You can restart logging at any time.

Log Formats and Versioning

Describes Log Formats and Versioning in Cisco Secure Access China. Cisco Secure Access stores zipped comma-separated values (CSV) log files in either Cisco's managed AWS S3 bucket or your own AWS S3 bucket.

Cisco Secure Access stores zipped comma-separated values (CSV) log files in either Cisco's managed AWS S3 bucket or 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.

Admin Audit Log Formats

Describes Admin Audit Log Formats in Cisco Secure Access China. 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 575.

Example

Shows a sample v4 through v10 Admin Audit Log event and illustrates the format of event records available in the Admin Audit Log.

An example of a v4 through v10 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

Describes order of Fields in Admin Audit Log. Not all fields 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.

> **Note**
>
> Not all fields 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.

V10 Log Format

Describes v10 Log Format. The CSV fields in the header row of the Admin Audit log. Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.

The CSV fields in the header row of the Admin Audit log.

```
id,timestamp,email,user,type,action,logged in from,before,after
```

The description of each field and the log version in which each field was released, from **version 4** up to **version 10**. 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

Field name	Description	Release version
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 Cloud Firewall Log Formats in Cisco Secure Access China. Cloud firewall logs show traffic that has been handled by Secure Access cloud-delivered firewall.

Cloud firewall logs show traffic that has been handled by Secure Access cloud-delivered firewall. For information about the size of a log file, see Estimate the Size of a Log.

Example

Shows an example v10 Cloud Firewall log event and illustrates the field structure used in Cloud Firewall log records for reference.

An example v10 Cloud Firewall log.

```
timestamp,origin IDs,identities,identity type,direction,protocol,packet
size,source IP,source port,destination IP,destination port,data center,rule
ID,action,fqdns,destination list IDs,first packet timestamp,last packet
timestamp,packets sent,packets received,bytes sent,bytes received,fw event
id,destination country,app id,aws region,private app group id,private
flow,posture id,casi category ids,traffic source,content category ids,content
 category list ids,organization id
"2024-06-14 18:59:57","[211039844]","Passive Monitor", "SFCN Tunnel
[illegible]
```

Order of Fields in the Cloud Firewall Log

Describes order of Fields in the Cloud Firewall Log. Not all fields 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.

> **Note**
>
> Not all fields 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.

V10 Log Format

Describes v10 Log Format. The CSV fields in the header row of the Cloud Firewall logs. The description of each field and the log version in which each field was released, up to version 10 . For more information about log versions, see Find Your Log Schema Version.

The CSV fields in the header row of the Cloud Firewall logs.

```
timestamp,origin ids,identities,identity type,direction,protocol,packet
size,source ip,source port,destination ip,destination port,data center,rule
```

```
id,action,fqdns,destination list ids,first packet timestamp,last packet
timestamp,packets sent,packets received,bytes sent,bytes received,fw event
id,destination country,app id,aws region,private app group id,private
flow,posture id,casi category ids,traffic source,content category ids,content
 category list ids,organization id
```

The description of each field and the log version in which each field was released, up to **version 10**. 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 SFCN Tunnel Device.	v5
direction	The direction of the packet. It is destined either towards the internet or to the customer's network.	v1
protocol	The actual protocol of the traffic. Valid values are: `TCP, UDP, or ICMP`.	v1
packet size	The size in bytes of the packet sent to the SFCN.	v1
source ip	The internal IP address of the user-generated traffic towards the SFCN. If the traffic goes through NAT before it comes to SFCN, it will be the NAT IP address.	v1
source port	The internal port number of the user-generated traffic towards the SFCN.	v1
destination ip	The destination IP address of the user-generated traffic towards the SFCN.	v1
destination port	The destination port number of the user-generated traffic towards the SFCN.	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

Field name	Description	Release version
packets received	The number of packets received during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
bytes sent	The number of bytes sent during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
bytes received	The number of bytes received during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
fw event id	The ID of the firewall event. Populated only for traffic handled by Cisco Secure Firewall.	v9
destination country	The ISO-3166 alpha-2 two-character identifier of the country associated with the destination IP.	v10
app id	The unique application ID identified for the current session.	v10
aws region	The AWS region that stores your VPN logs.	v10
private app group id	The unique ID of the private resource group ID that the private resource belongs to.	v10
private flow	TRUE if Secure Access applied a private access rule to the user-generated traffic, and FALSE if Secure Access applied an internet access rule.	v10
posture id	The unique ID of the endpoint posture profile.	v10
casi category ids	Name of the Application category to which the App ID belongs.	v10
traffic source	The source of the user-generated traffic. Valid values are `0 - Unknown, 1 - VPN,2 - ZTNA, 3 - Network Tunnel`.	v10
content category ids	ID of one or more content categories matched by the rule.	v10
content category list ids	ID of one or more content category lists that include categories matched by the rule.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v10

Data Loss Prevention (DLP) Log Formats

Describes Data Loss Prevention (DLP) Log Formats in Cisco Secure Access China. The Cisco Secure Access DLP logs show information about DLP events where data identifiers were triggered and a violation occurred.

The Cisco Secure Access DLP logs show information about DLP events where data identifiers were triggered and a violation occurred. DLP logs are available in all log format versions. For information about the size of a log file, see Estimate the Size of a Log.

> **Note**
>
> A single DLP event can present in multiple rows of the logs when different data identifiers and file labels are triggered for the same content. Rows related to the same content or event have the same Unique Event ID.

Example

Shows an example v10 DLP log event and illustrates the record format used for Data Loss Prevention log entries. for administrators to review.

An example of a v10 DLP log event.

```
timestamp,event type,unique event
id,severity,identity,owner,name,application,destination,action,rule,data
classification,data identifier,content type,file size,sha 256 hash,file
label,application category name,traffic direction,private resource name,private
 resource group name,destination protocol,destination ip,destination
port,organization id
"2022-02-15 12:05:45","Real
 PCI Classification","Credit Card Number -
Strict","text/html","48","abbd2352c3cfea8846871928bf99ca24dc3a6f162170926649381a6d968869ab",

"Confidential","","","dlpprivateresource","","https","127.0.0.1","443","8247177"
```

Order of Fields in the DLP Log

Describes order of Fields in the DLP Log. Not all fields 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.

> **Note**
>
> Not all fields 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.

V10 Log Formats

Describes v10 Log Formats. The CSV fields in the header row of the DLP logs. Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.

The CSV fields in the header row of the DLP logs.

```
timestamp,event type,unique event
id,severity,identity,owner,name,application,destination,action,rule,data
classification,data identifier,content type,file size,sha 256 hash,file
label,application category name,traffic direction,private resource name,private
 resource group name,destination protocol,destination ip,destination
port,organization id
```

The description of each field and the log version in which each field was released, up to **version 10**. 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.	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`, `Medium`, `High`, 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
file size	The size of the file in bytes.	v6
sha 256 hash	The hex digest of the response content.	v6
file label	The file name label that matched on the file properties.	v7
application category name	The category of the requested web application. For more information, see Application Categories.	v10
traffic direction	Direction of traffic. (Applies only to some applications, such as OpenAI API and OpenAI ChatGPT.)	v10
private resource name	The name of the private resource.	v10
private resource group name	The private resource group name if the matched rule destination was a private resource group.	v10
destination protocol	The protocol of the destination.	v10
destination ip	The IP address of the destination.	v10
destination port	The port of the destination.	v10

Field name	Description	Release version
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v10

IPS Log Formats

Describes IPS Log Formats in Cisco Secure Access China. The Cisco Secure Access IPS logs show the traffic, events, and possible threats detected by the Secure Access Intrusion Prevention System.

The Cisco Secure Access IPS logs show the traffic, events, and possible threats detected by the Secure Access Intrusion Prevention System. For information about the size of a log file, see Estimate the Size of a Log.

Example

Shows an example v10 IPS log and illustrates the field format used in Intrusion Prevention System log records. for administrators to review.

Example of a v10 IPS log.

```
timestamp,identities,identity types,generator id,signature id,signature
message,signature list id,severity,attack classification,cves,ip
protocol,session id,source ip,source port,destination ip,destination
port,action,operation mode,policy resource id,direction,firewall rule id,ips
config type,aws region,application id,casi category ids,data center,organization
 id
"2024-09-11 23:17:13","Firewall Tunnel Name","Network
Tunnels","1","16606","SERVER-ORACLE BEA WebLogic Server Plug-ins Certificate
overflow attempt","50516","HIGH","Attempted User Privilege
Gain","cve-2009-1016","TCP","12345","123.123.123.123","80","1.1.1.1","40762","Would
 Block","IDS","50516","S2C","21171","PROFILE","eu-central-2b","","","","8151514"
```

Order of Fields in the IPS Log

Describes order of Fields in the IPS Log. Not all fields 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.

> **Note**
>
> Not all fields 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.

V10 Log Format

Describes v10 Log Format. The CSV fields in the header row of the IPS log. The description of each field and the log version in which each field was released, up to version 10 . For more information about log versions, see Find Your Log Schema Version.

The CSV fields in the header row of the IPS log.

```
timestamp,identities,identity types,generator id,signature id,signature
message,signature list id,severity,attack classification,cves,ip
protocol,session id,source ip,source port,destination ip,destination
port,action,operation mode,policy resource id,direction,firewall rule id,ips
config type,aws region,application id,casi category ids,data center,organization
 id
```

The description of each field and the log version in which each field was released, up to **version 10**. 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
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

Field name	Description	Release version
firewall rule id	The ID of the rule that matches the firewall session.	v9
ips config type	The type of the IPS configuration. Valid values are: `CONFIG`, `PROFILE`, and `UNKNOWN`.	v9
aws region	The AWS region where Secure Access stores your logs.	v9
application id	The ID of the destination application.	v10
casi category ids	The name of the Application category to which the App ID belongs.	v10
data center	The name of the data center that processed the user-generated traffic.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v10

Remote Access VPN Log Formats

Describes Remote Access VPN Log Formats in Cisco Secure Access China. The Cisco Secure Access remote access virtual private network (VPN) logs show the VPN session connection events, which are managed by the Secure Access VPN services.

The Cisco Secure Access remote access virtual private network (VPN) logs show the VPN session connection events, which are managed by the Secure Access VPN services. Some relevant fields to aid debugging and trouble-shooting VPN sessions include:

- Display Username for Failed Events – Significantly improves how quickly issues can be tracked and addressed.
- ASA Syslog Message ID Extraction Support – Offers detailed insights by identifying the specific sys-log messages used in the remote access logs.
- Device ID – Includes the device ID with every event, providing critical help to network administrators in numerous ways.
- Failed Events for Posture – Provides vital information for effective triage during failed connection attempts.

For information about the size of a log file, see Estimate the Size of a Log.

Examples

Describes examples. An example v10 Secure Access VPN log of a CONNECTED event. An example v10 Secure Access VPN log of a DISCONNECTED event.

An example v10 Secure Access VPN log of a **CONNECTED** event.

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons
"2024-09-11
14:51","[redacted]","us-1","CONNECTED","[redacted]","7","[redacted]","8368","35","us","","46","R2","[redacted]","2.12.12.13","10.10.10.10","","","Mac
 OS X
14.6.1","5.1.2.42","ASA-5-109201","DEVICE-M-L9XH","","n/a","n/a","10","","","[]"
```

An example v10 Secure Access VPN log of a **DISCONNECTED** event.

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons
"2024-09-11
22:52","hostexample","user-1","DISCONNECTED","[295782]","7","sample-uid","8263","35","us","","48","TK2","CiscoSecureAccessVPN","24.123.123.123","10.10.1.10","2024-09-11 19:54:52","User
 Requested","Mac OS X
14.6.1","5.0.05040","ASA-4-113019","DEVICE-M-F1PG","","n/a","n/a","10","","","[]"
```

An example v10 Secure Access VPN log of a failed **AUTHORIZATION-CHECK** event.

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons
"2024-09-11
21:40:51","hostexample","user-1","FAILED","[296758]","7","sample-uid","8263","35","us","","48","TK2","CiscoSecureAccessVPN","24.123.123.123","10.10.1.10","","","Mac
 OS X
14.6.1","5.1.2.42","ASA-5-109201","DEVICE-M-L9XH","","n/a","n/a","10","","","["AUTHORIZATION-CHECK"]"
```

An example Secure Access VPN log of a failed **CERT-AUTH-CHECK** event.

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons
"2024-09-11
21:40:51","hostexample","user-1","FAILED","[296758]","7","sample-uid","8263","35","us","","48","TK2","CiscoSecureAccessVPN","24.123.123.123","10.10.1.10","","","Mac
 OS X
14.6.1","5.1.2.42","ASA-5-109201","DEVICE-M-L9XH","","n/a","n/a","10","","","["CERT-AUTH-CHECK"]"
```

Order of Fields in the RAVPN Log

Describes order of Fields in the RAVPN Log. Not all fields 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.

> **Note**
>
> Not all fields 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.

V10 Log Format

Describes v10 Log Format. The CSV fields in the header row of the RAVPN logs. The description of each field and the log version in which each field was released, up to version 10 . For more information about log versions, see Find Your Log Schema Version.

The CSV fields in the header row of the RAVPN logs.

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons
```

The description of each field and the log version in which each field was released, up to **version 10**. 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 fully-qualified domain name (FQDN) of the user device or virtual machine (VM) that generates the events.	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.	v9
retention days	The number of days that AWS S3 stores your Secure Access VPN log.	v9
storage location	The two-character label that identifies the location of your Cisco-managed VPN logs. Configure the storage location on Secure Access for your organization. The storage location options are: eu or us.	v9
msp organization id	The Secure Access managed organization ID.	v9
session id	The unique ID of the VPN session.	v9
session type	The protocol used by the device with the VPN session, for example: `TLS`.	v9
vpn profile	The name of the VPN connection profile that establishes a VPN session.	v9

Field name	Description	Release version
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
asa syslog id	The ID of the Cisco ASA syslog used to generate this log event.	v10
device id	The ID of the device with the Cisco Secure Client and VPN module.	v10
machine id	The ID of the client machine used for authentication.	v10
public ipv6	The public IP v6 address of the device with the Cisco Secure Client and VPN module.	v10
assigned ipv6	The IP v6 address assigned to the device with the Cisco Secure Client and VPN module.	v10
security group tag	Security group tag matched as a source by a rule.	v10
dap record name	The posture profile assessed by Cisco Secure Client HostScan.	v10
dap connection type	The RAVPN session connection type.	v10
failed reasons	The error codes for failed remote connection requests.	v10

Web Log Formats

Describes Web Log Formats in Cisco Secure Access China. 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

Shows an example v10 Web log event and illustrates the record structure used for Web log entries in Secure Access China.

An example of a v10 Web log event.

```
timestamp,policy identity label,internal client ip,external client
ip,destination ip,content type,action,url,referer,user agent,status code,request
 size,response size,response body size,sha—sha256,categories,av
detections,puas,amp disposition,AMP malware name,amp score,policy identity
type,blocked categories,identities,identity types,request method,dlp
status,certificate errors,file name,ruleset id,rule ID,destination list
ids,isolate action,file action,warn status,forwarding method,producer,msp
organization id,geo location of blocked destination countries,application
```

```
ids,hostname,data center,egress,server name,time based rule,security
overridden,detected response file type,warn categories,organization id
"2024-09-11 11:48:11","TheComputerName","192.192.192.135","1.1.1.91",
"3.4.5.6","","ALLOWED",""https://unitedstates.smartscreen.microsoft.com"","www.google.com","Mozilla/5.0>
 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/61.0.3163.100 Safari/537.36","200","562","1489","","","Search
Engines","","","","","","Roaming Computer","","TheComputerName,
ADSite,Network","Roaming Computer, Site,
Network","GH","","","tej","","","","scanned","download_original_file","warn session","","SWA","","","","sgroup-proxy-https-8c1-684-1.sgp.s1","ALL","true","unitedstates.smartscreen.microsoft.com","false","false","","","2403"
```

Order of Fields in the Web Log

Describes order of Fields in the Web Log. Not all fields 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.

> **Note**
>
> Not all fields 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.

V10 Log Format

Describes v10 Log Format. The CSV fields in the header row of the Web log. The description of each field and the log version in which each field was released, up to version 10 . For more information about log versions, see Find Your Log Schema Version.

The CSV fields in the header row of the Web log.

```
timestamp,policy identity label,internal client ip,external client
ip,destination ip,content type,action,url,referer,user agent,status code,request
 size,response size,response body size,sha—sha256,categories,av
detections,puas,amp disposition,AMP malware name,amp score,policy identity
type,blocked categories,identities,identity types,request method,dlp
status,certificate errors,file name,ruleset id,rule ID,destination list
ids,isolate action,file action,warn status,forwarding method,producer,msp
organization id,geo location of blocked destination countries,application
ids,hostname,data center,egress,server name,time based rule,security
overridden,detected response file type,warn categories,organization id
```

The description of each field and the log version in which each field was released, up to **version 10**. 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

Field name	Description	Release version
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
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: `RoamingComputer`, `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
file name	The name of the file.	v6

Field name	Description	Release version
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. Currently, Remote Browser Isolation (RBI) is not supported.	v8
file action	The action taken on a file in a remote browser isolation session. Valid values are: `UNKNOWN, DETECT, BLOCK, MALWARE_CLOUD_LOOKUP, MALWARE_WHITELIST, CLOUD_LOOKUP_TIMEOUT, CUSTOM_DETECTION, CUSTOM_DETECTION_BLOCK, ARCHIVE_BLOCK_DEPTH_EXCEEDED, ARCHIVE_BLOCK_ENCRYPTED, ARCHIVE_BLOCK_FAILED_TO_INSPECT, TID_BLOCK`	v8
warn status	The Warn page's state associated with the request.	v8
forwarding method	The method used to forward the proxy events. Example: Secure Web Appliance.	v9
producer	The producer of the proxy events.	v9
msp organization id	The Secure Access parent organization ID.	v10
geo location of blocked destination countries	The ISO-3166 IDs of one or more countries where destination IPs blocked by policy are located.	v10
application ids	The ID of the destination application.	v10
hostname	The hostname of the user device.	v10
data center	The name of the data center that processed the user-generated traffic.	v10
egress	TRUE indicates that the egress IP was a reserved IP.	v10
server name	The name of the server according to the TLS protocol server name indication (SNI), if present, or from the server's SAN certificate common name (CN).	v10
time based rule	TRUE indicates that a the rule was applied due to a time condition.	v10
security overridden	TRUE indicates that security filtering was explicitly overridden and not applied during enforcement.	v10
detected response file type	The file type that resulted in a blocked response. Examples: `exe, avi`.	v10
warn categories	The ID of one or more content categories in lists matched for a Warn action by the rule.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v10

Prerequisites

Lists the prerequisites for log formats and versioning. Full Admin user role. For more information, see Manage Accounts. Configure logging to an Amazon S3 bucket. See Enable Logging to Your Own S3 Bucket or Enable Logging to a Cisco-managed S3 Bucket.

- Full Admin user role. For more information, see Manage Accounts.
- Configure logging to an Amazon S3 bucket. See Enable Logging to Your Own S3 Bucket or Enable Logging to a Cisco-managed S3 Bucket.

Log File Name Formats

Describes log File Name Formats. 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.

- **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`

Subfolders

Describes subfolders.

Logs are uploaded to AWS S3 buckets in the appropriate subfolder with the following naming format.

```
<subfolder>/<YYYY>-<MM>-<DD>/<YYYY>-<MM>-<DD>-<hh>-<mm>-<xxxx>.csv.gz
```

Secure Access names a log subfolder (`<subfolder>`) with one of the following folder names:

- `proxylogs`
- `firewalllogs`
- `iplogs`
- `auditlogs`
- `dlplogs`
- `vpnlogs`

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

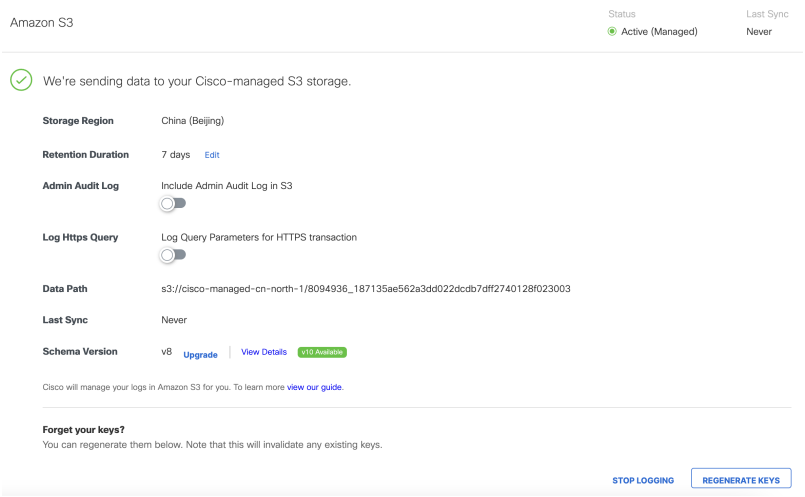
Describes log Schema Versions. v2 –For customers who have configured their own S3 bucket after November 2017, or are using a Cisco-managed bucket. This version is inclusive of everything in version 1.

- **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`.
  - 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.

View Your Log Schema Version and Last Sync Time

Provides instructions for viewing your log schema version and last sync time. Navigate to Admin > Log Management . In the Amazon S3 area, Secure Access displays the log Schema Version in use and Last Sync time.

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 ("").

- Admin Audit Log Formats
- Cloud Firewall Log Formats
- Data Loss Prevention (DLP) Log Formats
- IPS Log Formats
- Remote Access VPN Log Formats
- Web 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.

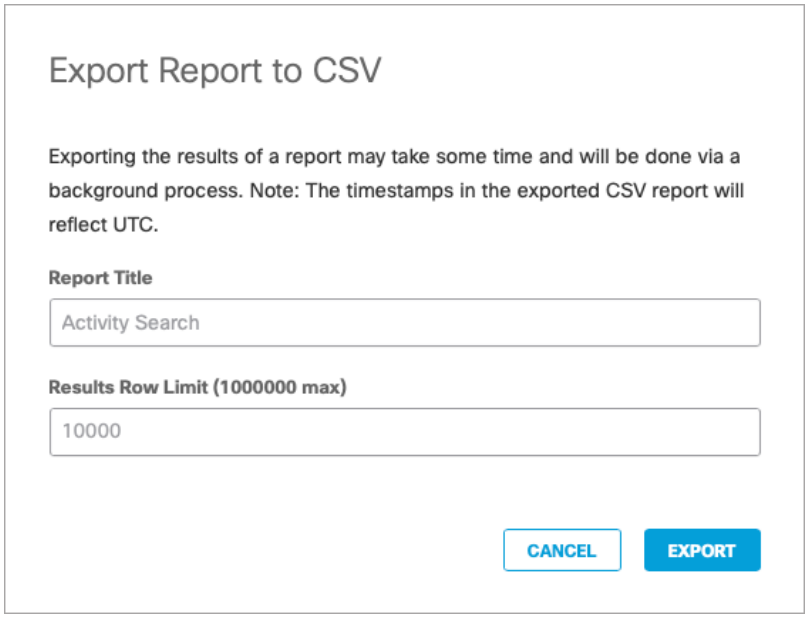
1. Download one of your Secure Access log files. The Secure Access log file is a comma-separated values (CSV) file.
2. Count the number of rows in the CSV file minus one for the header row.The number of rows is equivalent to the number of events in the twenty-four hour period.
3. Multiply the number 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

Describes estimate the Size of an Exported Report. Navigate to Monitor > Activity Search. For Filters, run a report for the last 24 hours and then click the Export CSV icon.

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.

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.

Where are Logs Stored?

Describes where are Logs Stored?. You can also optionally configure logging so that logs are also stored to an Amazon S3 bucket –either your own or one managed by Cisco.

When you create a policy, activity logs are saved by default to the China (Beijing) location of the Secure Access data warehouse.

You can also optionally configure logging so that logs are also stored to an Amazon S3 bucket–either your own or one managed by Cisco.

Logging to Amazon S3

Describes logging to Amazon S3. As well as storing logs to one of its data warehouses, Secure Access can store logs to an Amazon S3 bucket.

As well as storing logs to one of its data warehouses, Secure Access can store logs to an Amazon S3 bucket.

By having your logs uploaded to an S3 bucket, you can then automatically download logs so that you can keep them in perpetuity in backup storage outside of the Secure Access data warehouse storage system. Saving to an S3 bucket also gives you the ability to ingest logs through your SIEM or another security tool. This can help you determine if any security events in your Secure Access logs coincide with events in other security tools.

Secure Access Amazon S3 options:

- A self-managed bucket–You own the Amazon S3 bucket, including its configuration and management.
- A Cisco-managed bucket–Cisco Secure Access owns the bucket and sets the configuration and management of it.

Advantages and Disadvantages of Configuring a Cisco-Managed Bucket

Describes advantages and Disadvantages of Configuring a Cisco-Managed Bucket. Easy to set up and manage. Included with your Secure Access license.

- Easy to set up and manage.
- Included with your Secure Access license.
- You cannot add anything to your bucket besides log files from Secure Access and the bucket cannot be used by another application.

- Some SIEM integration types (such as QRadar) may require advanced privileges for the user accessing the S3 bucket (beyond the basic Read permissions) and as such, may not work with this feature.
- You cannot get support from Amazon directly for advanced configuration assistance, such as automation or help with the command line.
- Data can only be stored offline for a maximum of 30 days.

42 Manage API Keys

Topics:

- Manage API Keys

Provides an overview of Manage API Keys in Cisco Secure Access China, including Add Secure Access API Keys and Add KeyAdmin API Keys. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage API Keys

Provides instructions for managing API Keys in Cisco Secure Access China. 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

Provides instructions for 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.

Prerequisites

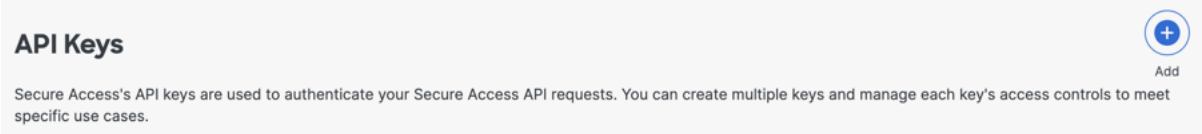
Lists the prerequisites for adding secure access api keys, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

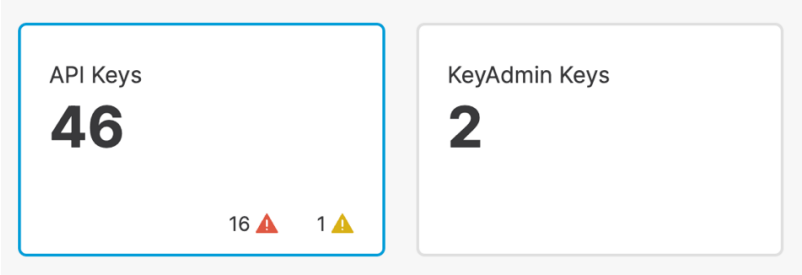
Add API Key

Provides instructions for adding api key. (Optional) For Network Restrictions , enter a comma-separated list of public IP addresses or CIDRs, then click Add.

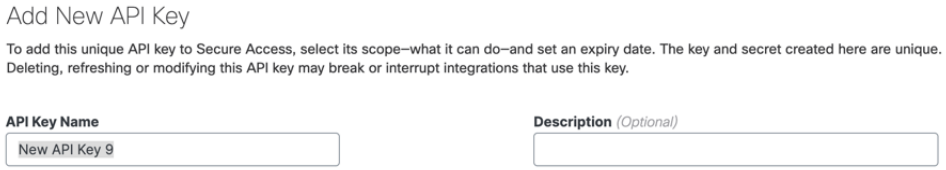
1. Navigate to **Admin > API Keys**.



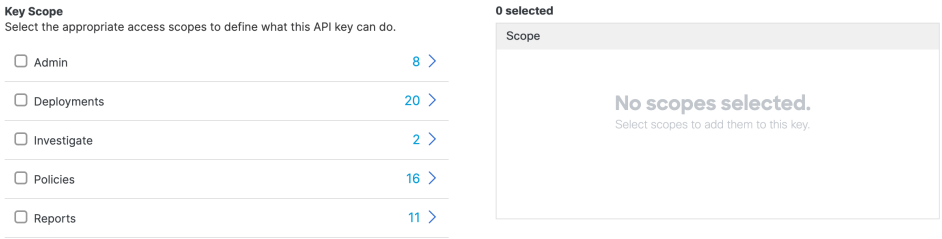
2. Click **API Keys** and then click **Add**.The number of expired API keys appears next to the red triangle. The number of API keys that expire within 30 days appears next to the yellow triangle.



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.

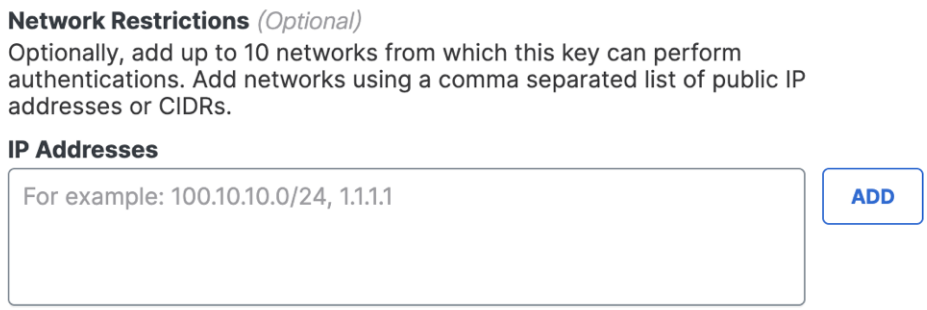


5. Choose **Read-Only** or **Read / Write** for the selected scope and resource.
6. For **Expiry Date**, choose an expiration date or choose **Never expire**.



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**.

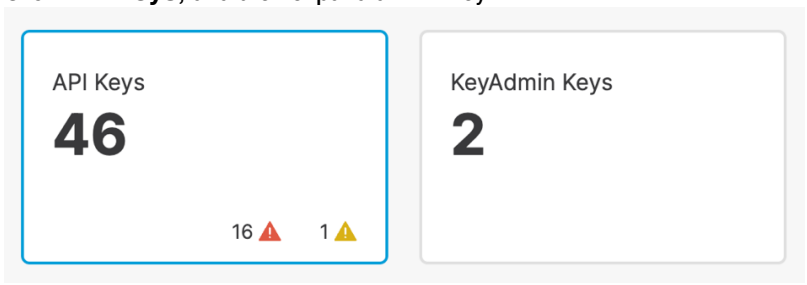
9. Copy and save your **API Key** and **Key Secret**.
10. Click **Accept and Close**.



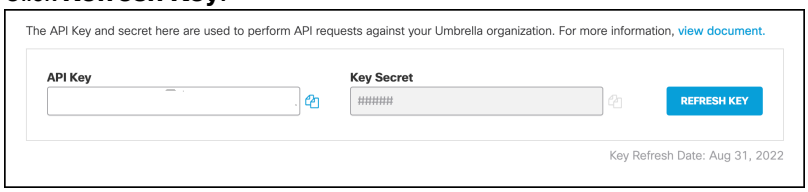
Refresh API Key

Describes refresh API Key. Navigate to Admin > API Keys. Click API Keys , and then expand an API key.

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**.

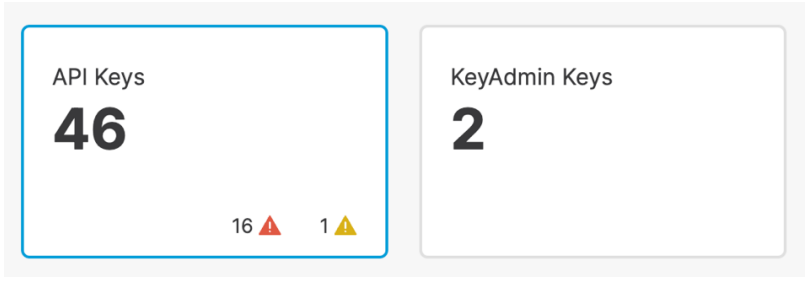


Update API Key

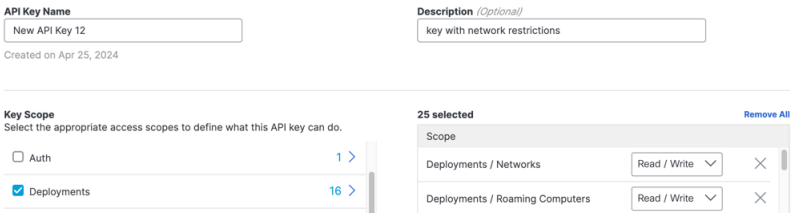
Provides instructions for updating api key. You can modify one or multiple settings on your API key. Modify the API Key Name , Description , and selected scopes and permissions in Key Scope.

You can modify one or multiple settings on your API key.

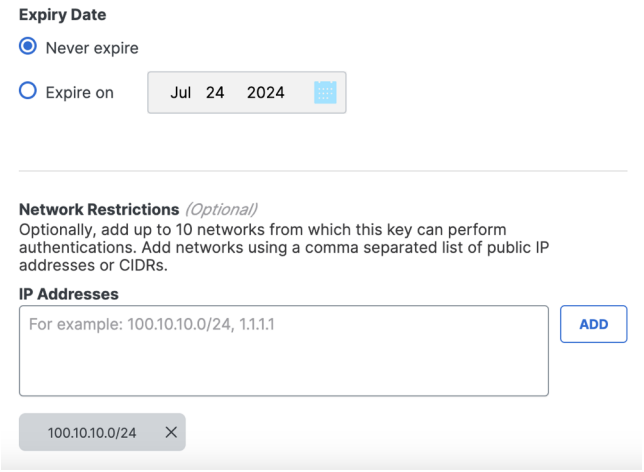
1. Navigate to **Admin > API Keys**.
2. Click **API Keys**, and then expand an API key.



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.

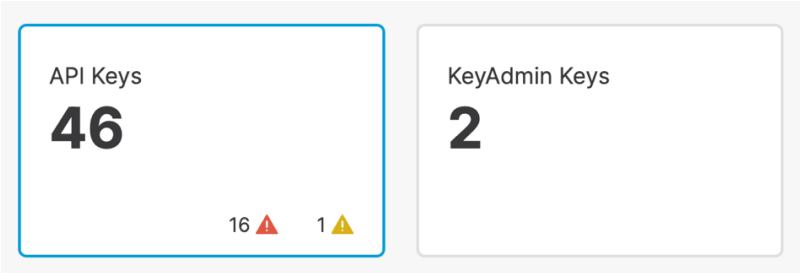


6. Click **Save**.

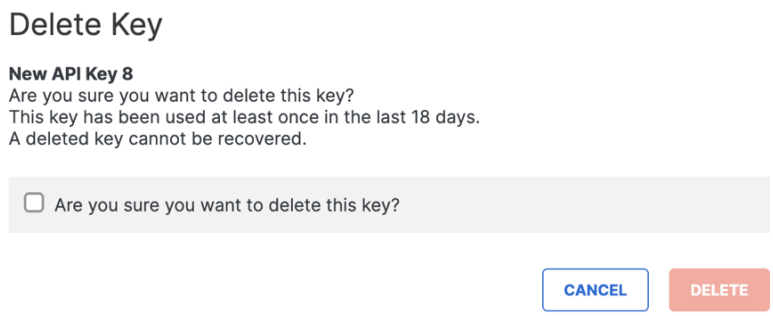
Delete API Key

Provides instructions for deleting api key. Navigate to Admin > API Keys. Click API Keys , and then expand an API key.

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

Provides instructions for adding keyAdmin API Keys in Cisco Secure Access China. The Secure Access Key Admin API enables you to create and manage Secure Access 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. 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

Provides instructions for 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.

Prerequisites

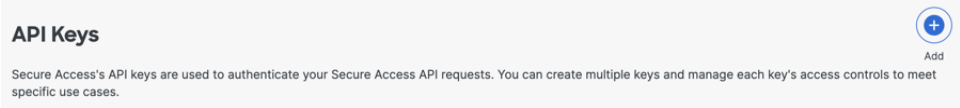
Lists the prerequisites for adding secure access keyadmin API keys. Full Admin user role. For more information, see Manage Accounts.

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

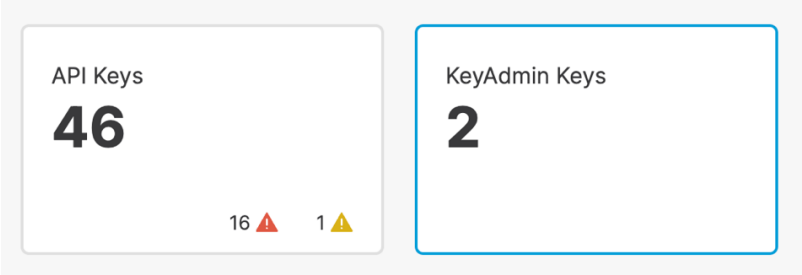
Add KeyAdmin API Key

Provides instructions for adding keyadmin api key. Navigate to Admin > API Keys. 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.

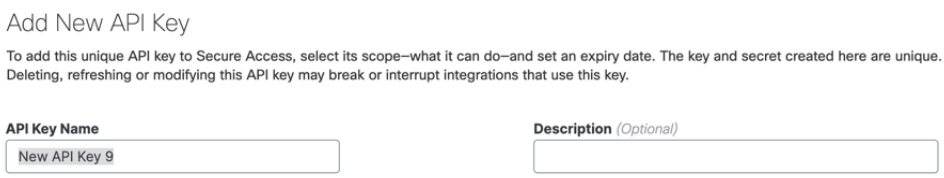
1. Navigate to **Admin > API Keys**.



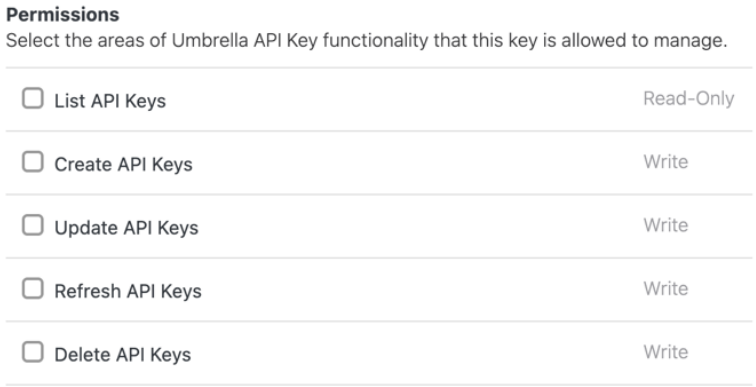
2. Click **KeyAdmin Keys** and then click **Add**.The number of expired API keys appears next to the red triangle. The number of API keys that expire within 30 days appears next to the yellow triangle.



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.

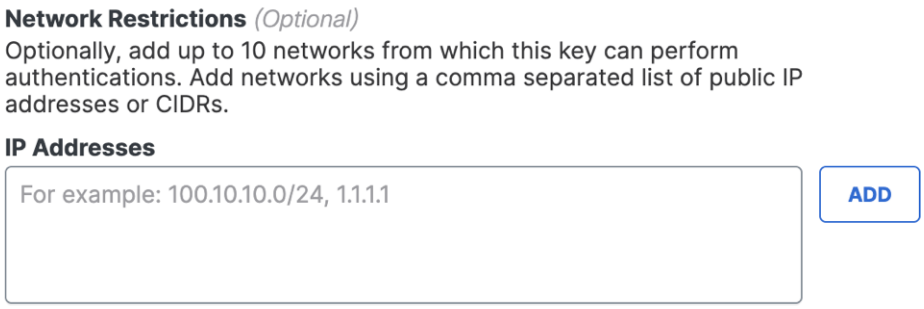


5. For **Expiry Date**, choose the expiration date for the key, or choose **Never expire**.



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.



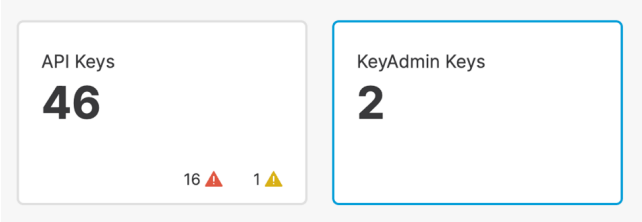
7. Click **Create Key**.
8. Copy and save your **KeyAdmin Key** and **Key Secret**.
9. Click **Accept and Close**.



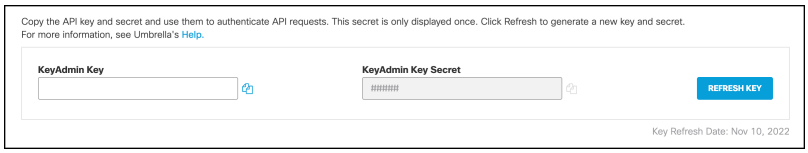
Refresh KeyAdmin API Key

Describes refresh KeyAdmin API Key. Navigate to Admin > API Keys. Click KeyAdmin Keys , and then expand an API key.

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**.

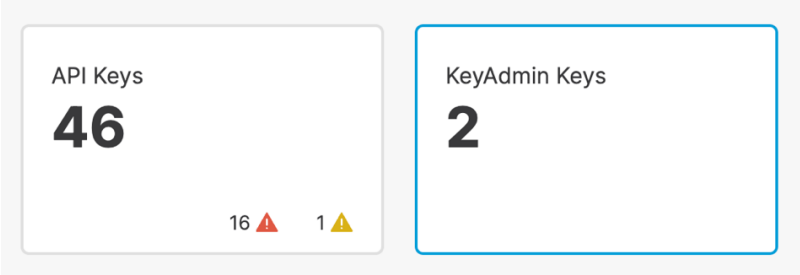


Update KeyAdmin API Key

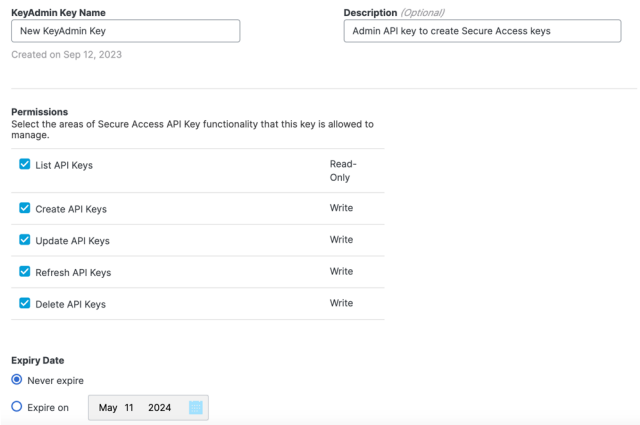
Provides instructions for updating keyadmin api key. You can modify one or multiple settings on your API key. Navigate to Admin > API Keys.

You can modify one or multiple settings on your API key.

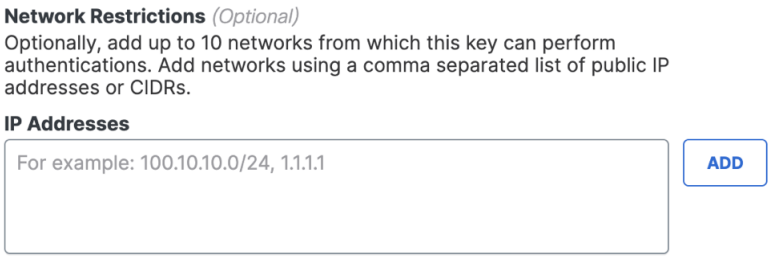
1. Navigate to **Admin > API Keys**.
2. Click **KeyAdmin Keys**, and then expand an API key.



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.

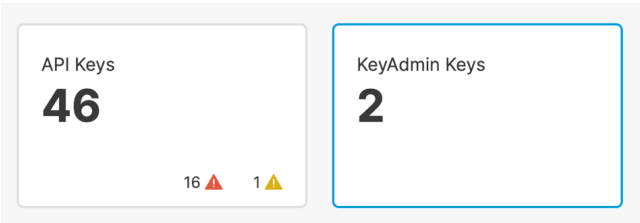


5. Click **Save**.

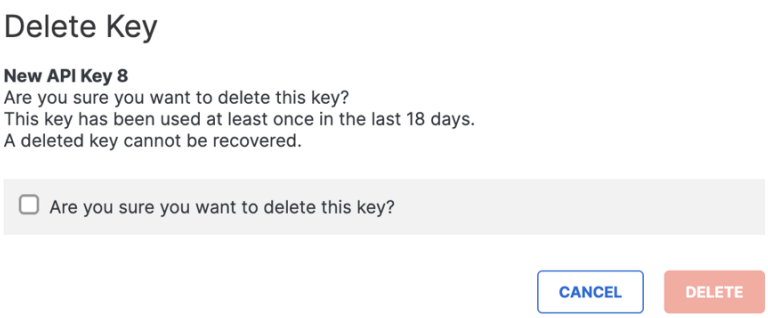
Delete KeyAdmin API Key

Provides instructions for deleting keyadmin api key. Navigate to Admin > API Keys. Click KeyAdmin Keys , and then expand an API key.

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.


Delete Key
New API Key 8
Are you sure you want to delete this key?
This key has been used at least once in the last 18 days.
A deleted key cannot be recovered.
Are you sure you want to delete this key?
CANCEL
DELETE

43 Manage Accounts

Topics:

- Manage Accounts

Provides an overview of Manage Accounts in Cisco Secure Access China, including Add a New Account, Edit Account Settings, and Delete an Account. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

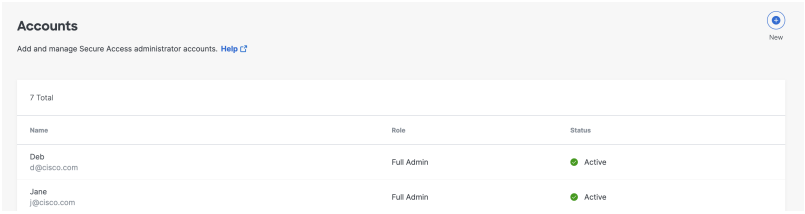
Manage Accounts

Provides instructions for managing accounts in Cisco Secure Access China. 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

Provides instructions for adding a New Account in Cisco Secure Access China. You can add users to your instance of Cisco Secure Access China by adding a new account.

You can add users to your instance of Cisco Secure Access China 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 China configurations.

Prerequisites

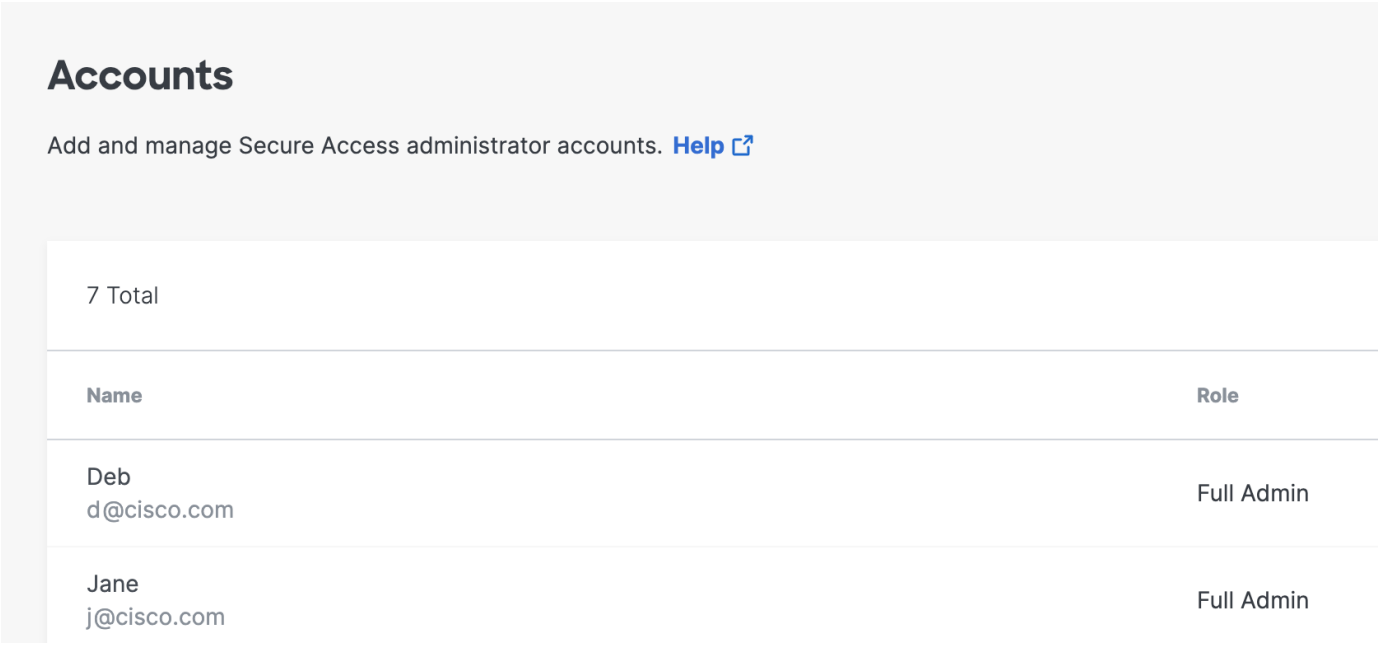
Lists the prerequisites for adding a new account, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for adding a new account. User roles are:. After a user creates a password and signs in, the user has access to your instance of Secure Access China. The user's role controls their level of access.

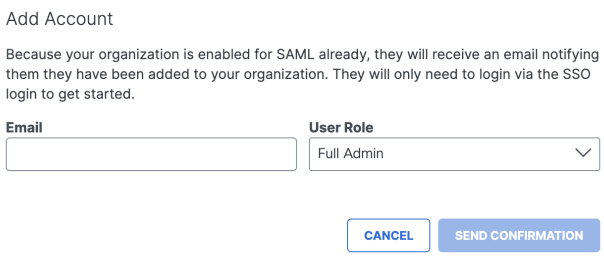
1. Navigate to **Admin > Accounts** and click **New**.



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 China. This includes the ability to add users and assign roles.
   - **Read-Only**–Grants limited access to Secure Access China. 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.

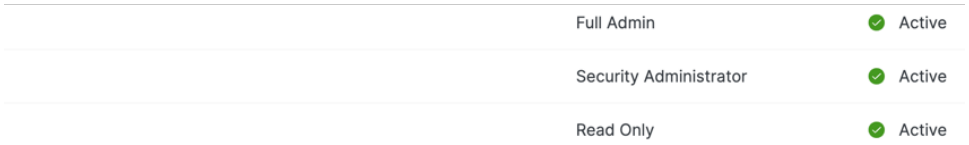


3. A message is sent to the new user's email address with instructions for setting a password.

> **Note**
>
> When the new user clicks **Confirm Invite**, Secure Access China redirects them to the Secure Access China login page.

After a user creates a password and signs in, the user has access to your instance of Secure Access China. The user's role controls their level of access.

Once the account is added, its status is **Active** and you can edit the account. For more information, see Edit Account Settings.



Edit Account Settings

Provides instructions for editing account Settings in Cisco Secure Access China. With administrator rights, you can change an account's settings at any time.

With administrator rights, you can change an account's settings at any time.

Prerequisites

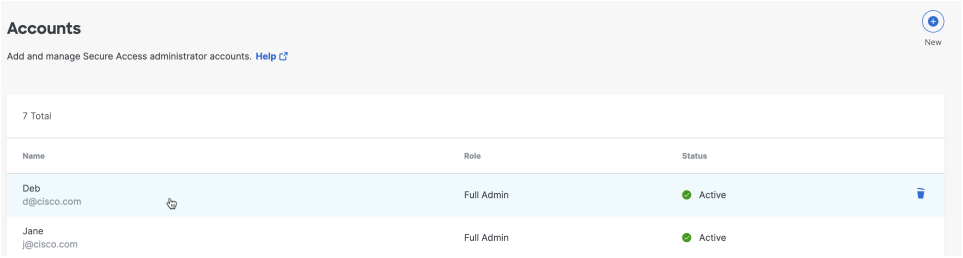
Lists the prerequisites for editing an account, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

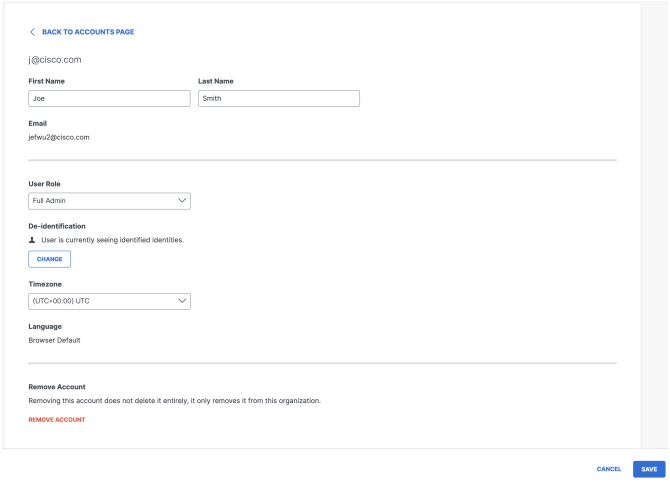
Procedure

Provides instructions for editing an account. The following account settings can be changed:. Navigate to Admin > Accounts and click a listed account entry.

1. Navigate to **Admin > Accounts** and click a listed account entry.



2. Update account settings as needed.



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

Provides instructions for deleting an Account in Cisco Secure Access China. After adding a user to your instance of Secure Access, you can delete their account at any time.

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.

Prerequisites

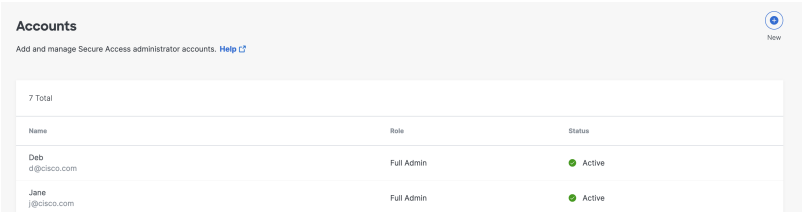
Lists the prerequisites for deleting an account, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

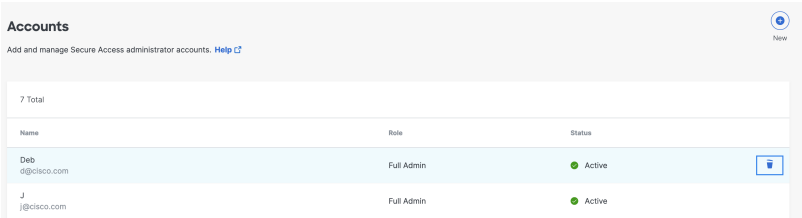
Prerequisites

Lists the prerequisites for deleting an account prerequisites 1. Navigate to Admin > Accounts. Hover over the account that you want to delete and then click the delete icon next to the account.

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.



3.

Hide Sources with De-identification

Describes Hide Sources with De-identification in Cisco Secure Access China. Some regions or organizations require restrictions to hide the sources of users making internet requests.

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.



> **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.

Prerequisites

Lists the prerequisites for hide sources with de identification, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Source Types

Describes source Types. The following source types are de-identified:. internal IP addresses. GSuite users and groups. SAML-obtained users and groups.

The following source types are de-identified:

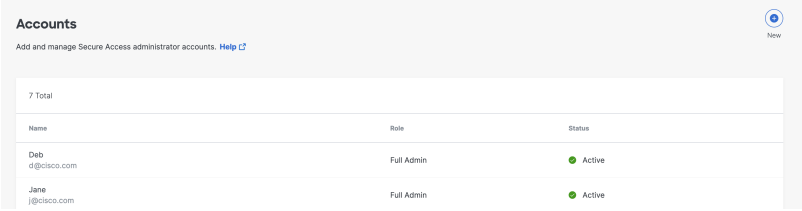
- AD usernames
- computer/hostnames
- internal IP addresses
- Chromebook identities
- mobile identities
- GSuite users and groups
- SAML-obtained users and groups
- internal IP addresses

Enable De-identification

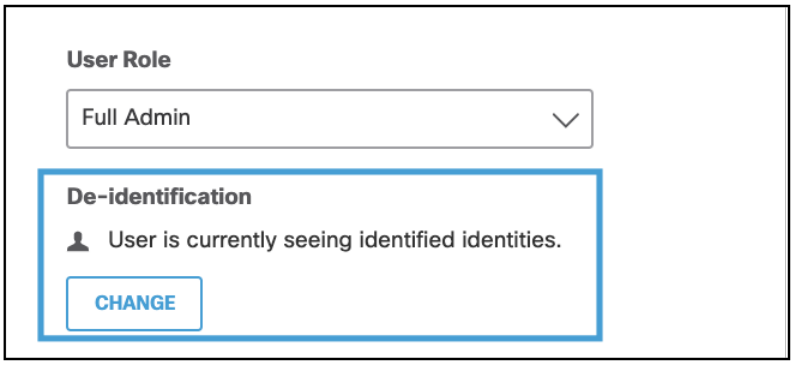
Provides instructions for enabling de-identification. De-identification is enabled and source (identity) names are replaced with a hash. You cannot enable de-identification for your own account.

1. Navigate to **Admin > Accounts** and click an account name.

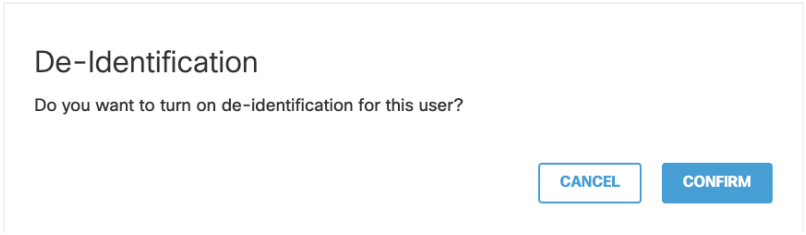
> **Note**
>
> You cannot enable de-identification for your own account.



2. Under **De-identification** click **Change**.



3. Click **Confirm**.



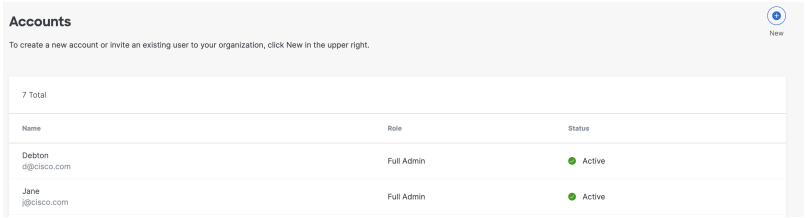
De-identification is enabled and source (identity) names are replaced with a hash.

Disable De-identification

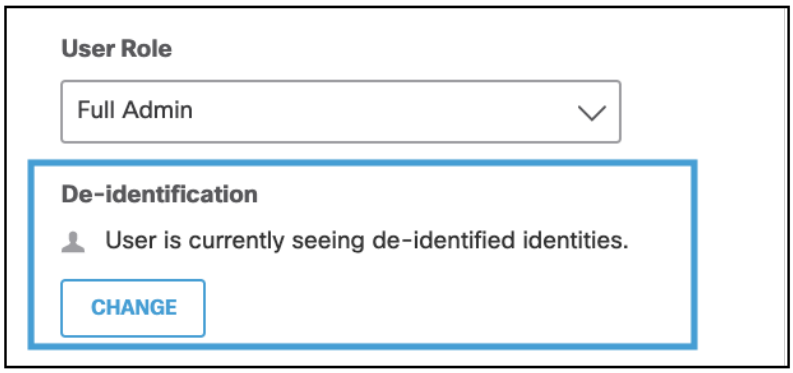
Provides instructions for disabling de-identification. De-identification is disabled and the account can view identity names. You cannot enable de-identification for your own account.

1. Navigate to **Admin > Accounts** and click an account name.

> **Note**
>
> You cannot enable de-identification for your own account.



2. Under **De-identification** click **Change**.



3. Click **Confirm**.



De-identification is disabled and the account can view identity names.

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.

Part II

Cisco Secure Client

Topics:

- Get Started with Cisco Secure Client on Windows and macOS
- Manage Internet Security on Cisco Secure Client
- Manage Virtual Private Networks on Cisco Secure Client

Describes Cisco Secure Client in Cisco Secure Access China. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

44 Get Started with Cisco Secure Client on Windows and macOS

Topics:

- Get Started with Cisco Secure Client on Windows and macOS

Provides an overview of Get Started with Cisco Secure Client on Windows and macOS in Cisco Secure Access China, including Install the Cisco Secure Client, Download Cisco Secure Client, and Download the OrgInfo.json File. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started with Cisco Secure Client on Windows and macOS

Describes Get Started with Cisco Secure Client on Windows and macOS in Cisco Secure Access China. Cisco Secure Client provides security to user devices on any network from any location.

Cisco Secure Client provides security to user devices on any network from any location. User devices can connect to private resources through VPNs, or access internet resources protected by the Cisco Secure Access 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.

Secure Client features:

- Endpoint compliance
- User identity verification and device communications managed by 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.

Prerequisites

Describes Prerequisites in Cisco Secure Access China. Cisco Secure Client provides security to user devices on any network, whether the device connects to private resources using VPN or the secure web gateway (SWG).

Cisco Secure Client provides security to user devices on any network, whether the device connects to private resources using VPN or 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.

Secure Access Requirements

Provides instructions for securing access requirements. Full Admin user role. For more information, see Manage Accounts. Administrative privileges on the user device.

- Full Admin user role. For more information, see Manage Accounts.
- Administrative privileges on the user device.

Download the Cisco Secure Client Pre-Deployment Package

Provides instructions for downloading the Cisco Secure Client pre-deployment package. Install Cisco Secure Client packages for Windows and MacOS. For more information, see Download Cisco Secure Client.

Install Cisco Secure Client packages for Windows and MacOS.

- macOS– `cisco-secure-client-macos-5.1.0.136-predeploy-k9.pkg`
- Windows– `cisco-secure-client-win-5.1.0.136-predeploy-k9.msi`

For more information, see Download Cisco Secure Client.

Install the Cisco Secure Client

Provides instructions for installing the Cisco Secure Client. 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.

1. 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.

Download Cisco Secure Client

Provides instructions for downloading cisco Secure Client in Cisco Secure Access China. This topic explains your options for downloading the Cisco Secure Client pre-deployment package in Secure Access China.

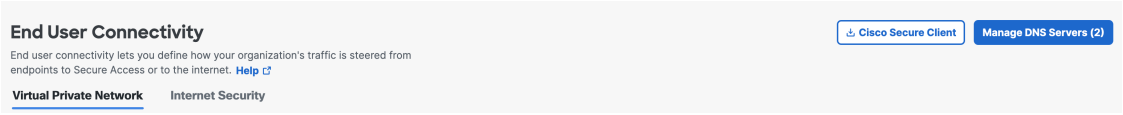
This topic explains your options for downloading the Cisco Secure Client pre-deployment package in Secure Access China.

- **Option 1**: Download any version of Secure Client using the link in Secure Access China to Cisco Software Central. You will need a valid service contract that is associated with your Cisco.com profile.
- **Option 2**: Download the current version of Secure Client using the shortcut buttons in Secure Access China.

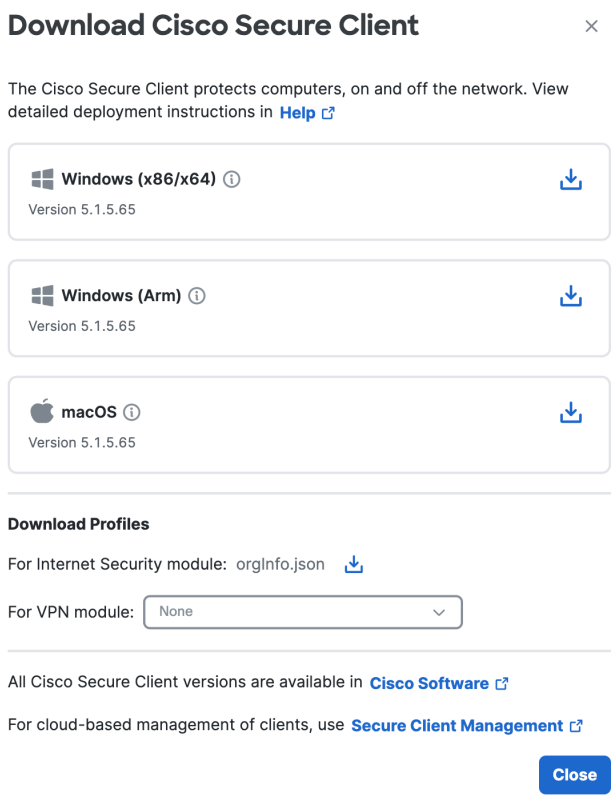
Procedure

Provides instructions for downloading Cisco Secure Client. In Secure Access China, navigate to Connect > End User Connectivity. On the End User Connectivity page, click Cisco Secure Client.

1. In Secure Access China, 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:



> **Note**
>
> The supported version of Cisco Secure Client is 5.1.8, so it is recommended to download this version to ensure optimal functionality. Client support for multiple deployments is available starting with Cisco Secure Client release 5.1.8 on Windows and macOS. This enables roaming users to connect to the appropriate Secure Access deployment based on their current location.

- 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 the current version of Secure Client, click the download button.

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 China which VPN profiles to enforce. You created the VPN profiles in the End-User Connectivity module of Secure Access China (**show menu path)**
5. Click **Close**.
6. Distribute Secure Client on all end-user devices.

Download the OrgInfo.json File

Provides instructions for downloading the OrgInfo.json File in Cisco Secure Access China. You can deploy various modules with the Cisco Secure Client.

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 (Web security) requires the Secure Access China **OrgInfo.json** file. The Secure Access China **OrgInfo.json** file associates a Cisco Secure Client deployment with the Umbrella Roaming Security module to a Secure Access China user and organization. Once the module is deployed on the Cisco Secure Client, Secure Access China 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 China to install the Cisco Secure Client Umbrella module, the roaming device is managed by that instance of Secure Access China 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 China to the device.

Prerequisites

Lists the prerequisites for downloading the orginfo json, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for downloading OrgInfo.json, the Cisco Secure Client internet security profile used to configure the client deployment for Secure Access China.

Download the Cisco Secure Client internet security profile (**OrgInfo.json**).

Step 1 – Download the OrgInfo.json File

Describes step 1 – Download the OrgInfo.json File. Navigate to Connect > End User Connectivity > Internet Security. For Cisco Secure Client, click Download Profile to save the OrgInfo.json file to the local system.

1. Navigate to **Connect > End User Connectivity > Internet Security**.
2. For Cisco Secure Client, click **Download Profile** to save the **OrgInfo.json** file to the local system.

Step 2 – Copy the OrgInfo.json File to the Target Directory

Describes step 2 – Copy the OrgInfo.json File to the Target Directory. You have two options for copying the OrgInfo.json file:.

You have two options for copying the OrgInfo.json file:

1. **Using the Profiles Directory**

   Cisco Secure Client is available as a .zip file (for Windows) or a .dmg file (for macOS), each containing installer packages. Within the extracted archive, you will find a subdirectory named Profiles. Copy OrgInfo.json to the profile directory for the Umbrella module at Profiles\umbrella to ensure that the profile is automatically installed during product installation.

2. **Using the Installation Directory**

   Alternatively, you can copy the OrgInfo.json file directly to the location of the Cisco Secure Client runtime directory at:

```
Windows: %ProgramData%\Cisco\Cisco Secure Client\Umbrella
macOS: /opt/cisco/secureclient/umbrella/
```

> **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.

When you deploy the OrgInfo.json file for the first time, the Cisco Secure Client copies the OrgInfo.json file to the data subdirectory (see below), 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. The data subdirectory is:

For Cisco Secure Client 5.1.7 or earlier:

```
Windows: %ProgramData%\Cisco\Cisco Secure Client\Umbrella\data
macOS: /opt/cisco/secureclient/umbrella/data
```

For Cisco Secure Client 5.1.8 or later:

```
Windows: %ProgramData%\Cisco\Cisco Secure
Client\Umbrella\data\regionaldata\<region_name>
macOS: /opt/cisco/secureclient/umbrella/data/regionaldata/<region_name>
```

Note

The region_name in the directory should match the region tag found in the **OrgInfo.json** file. If the region tag is missing, it is assumed to be “global”.

Manual Installation of Cisco Secure Client (Windows and macOS)

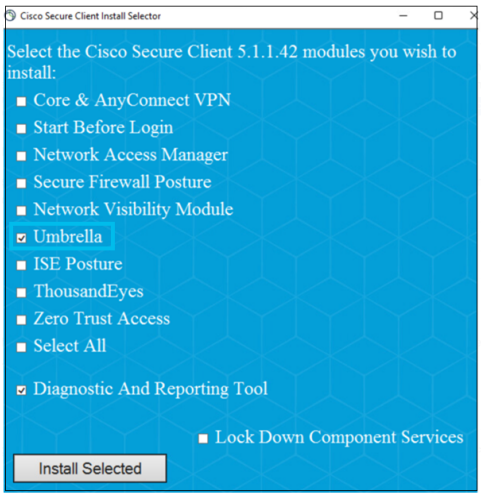
Describes Manual Installation of Cisco Secure Client (Windows and macOS) in Cisco Secure Access China. Install Cisco Secure Client If you choose only the Umbrella option, the VPN functionality in Cisco Secure Client will be disabled.

Procedure

1. **Install Cisco Secure Client**

Note

- If you choose only the Umbrella option, the VPN functionality in Cisco Secure Client will be disabled. However, the core VPN service will still be installed, as Umbrella shares some underlying functionality with this service.
- Unchecking the Core & AnyConnect VPN option will hide the VPN from the graphical user interface (GUI). The VPN service (csc_vpnagent) will continue to run in the background, but it will not be visible in the GUI.
- We highly recommend that you select Diagnostics and Reporting Tool for troubleshooting capabilities.



2. **Install Umbrella Profile**

After installing Cisco Secure Client, install the Umbrella profile (OrgInfo.json), downloaded from your Umbrella dashboard. Copy the profile to the correct folder to register and activate Umbrella:

Windows	`%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json`
macOS	`/opt/cisco/secureclient/umbrella/OrgInfo.json`

Mass Deployment Overview

Describes Mass Deployment Overview in Cisco Secure Access China and explains Profile Installation and Customization Options. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Remote Installation

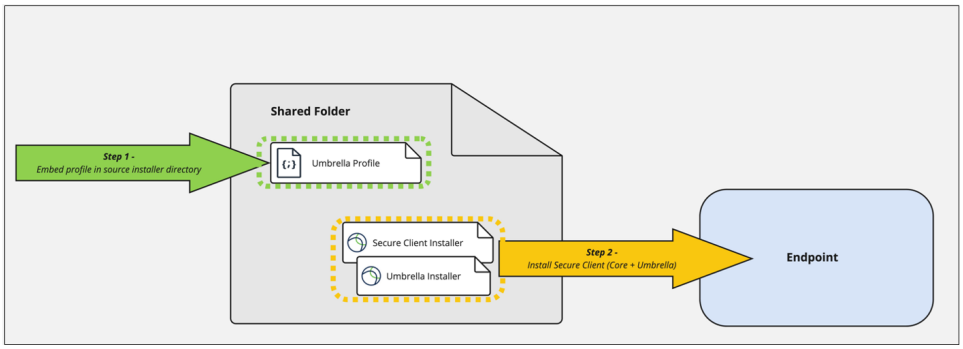
Cisco Secure Client can be deployed with endpoint management software designed to remotely install applications. This includes tools such as Unified Endpoint Management (UEM) and Remote Management and Monitoring (RMM). The remote installation options outlined below includes installing both the Cisco Secure Client software and the Umbrella profile (OrgInfo.json), similar to the steps followed in the manual deployment process.

Scripted Installation	• Cisco Secure Client is installed by endpoint management software. • The Umbrella profile information is copied to the endpoint by a **post install** script or task.
Mass Deployment Package	• The installation package or source is modified, and the Umbrella configuration profile is bundled with this package or source prior to installation. • The customized package can be installed by endpoint management software with the profile that is already included.
VPN Headend Deployment	(This option is suitable for customers using Secure Client for VPN.) • The software and profile are uploaded to the VPN headend. • Umbrella is automatically downloaded and installed when the corresponding user connects to the VPN.
RMM Deployment	This option is suitable for managed service providers.) • Cisco Secure Client can be deployed to multiple end customers using RMM tools.

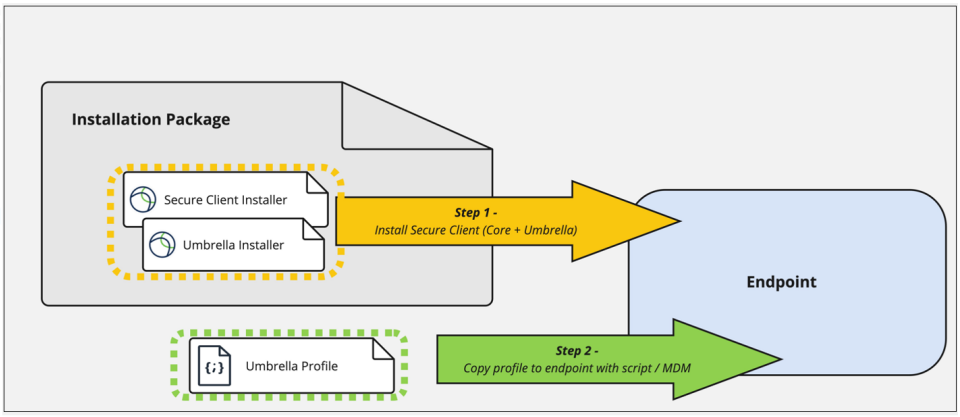
Profile Installation

Installing your Umbrella organization profile (OrgInfo.json) is a mandatory step in the deployment process because this file uniquely identifies your Umbrella organization and is required for the Cisco Secure Client to register with Umbrella. The following diagrams show the two main ways in which the Umbrella organization profile can be distributed.

- **Bundle Profile** – The profile (OrgInfo.json) is bundled with the installation package prior to installation.



- **Copy Profile** : The profile (OrgInfo.json) is copied to a location in the endpoint (programmatically) after installation. (MDM – Managed Device Manager).



Customization Options

Before performing a mass deployment of Cisco Secure Client, you may consider the following common installation customizations.

1. Select Cisco Secure Client Modules

Choose which Cisco Secure Client modules you want to install. For a minimum installation (Umbrella protection only) you must install two modules:

- Core & AnyConnect VPN module
- Umbrella module

Choose the modules using the following methods.

Windows	Using a 'Pre-Deployment' package, the modules are provided as individual Microsoft Software Installer (MSIs). Only install the desired .msi files. A minimum of two .msi files must be installed (Core VPN + Umbrella module.
macOS	Using a 'Pre-Deployment' package Cisco Secure Client (and its modules) are installed using a single .dmg image. An 'install_choices.xml' file can be provided to the macOS installer to disable unwanted modules. Alternatively, use a 'Web Deployment' package, install each Cisco Secure Client module using a separate .dmg image. A minimum of two .dmg image files must be installed (Core VPN + Umbrella module).

2. Disable VPN Functionality

The Core Secure Client VPN module must be installed for the Umbrella module to function. However, the VPN functionality itself is not required and can be disabled (for macOS and Windows) such that it is not available to users. Each of the installation methods on this page provide options for disabling Cisco Secure Client VPN.

You can disable the VPN functionality using one of these methods:

- During manual installation uncheck the Core & AnyConnect VPN (for Windows and macOS).
- Disable the VPN functionality within a customized .dmg package (macOS).
- Disable the VPN functionality by deploying a special VPN profile (Windows and macOS).

For more information, see How to Disable VPN Functionality in Cisco Secure Client.

3. **Lockdown Services (Windows)**

   On Windows, you can customize the installation to prevent users from tampering with Cisco Secure Client. To do this, modify any of the **msiexec** commands and provide these additional MSI parameters:

   - **LOCKDOWN=1** : Prevents the service from being stopped.
   - **ARPSYSTEMCOMPONENT=1** : Hides the program from **Programs and Features** in Windows.

   For more information, see Command Line installation and RMM reference.

Mass Deployment (Windows)

Describes Mass Deployment (Windows) in Cisco Secure Access China and explains Add Umbrella Profile. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

(Optional) Package Customization

You have the option to bundle the Umbrella profile within the installation source directory before running the Cisco Secure Client installer. The profile will then be automatically imported during installation. This method creates a preconfigured deployment package, which can be executed without any additional script or configuration. However, note that for this method to work, one of the following is required:

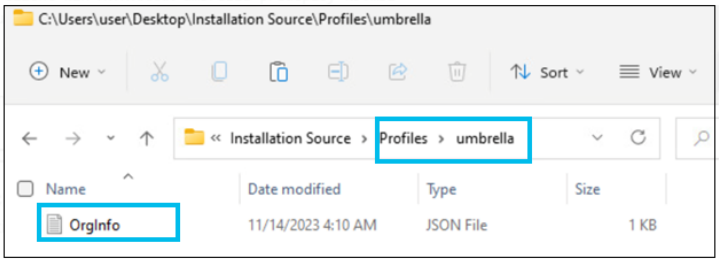
- A shared network folder to act as the installation source.
- Endpoint management software that can create and distribute multifile installation packages.

> **Note**
>
> See the following examples of software that can distribute multifile installation packages using the Windows Content Prep Tool or Jamf Composer:
>
> - Secure Client Umbrella Roaming Security Module Provisioning via MS Intune (Windows).
> - How to deploy Cisco Secure Client via JAMF (MacOS).
>
> For more information, see Customize Windows Installations of Secure Client.

Add Umbrella Profile

Add the OrgInfo.json file to a \\Profiles\\umbrella subdirectory within the installation package. The source installation folder must have the following contents:

```
cisco-secure-client-win-X.X.XXXXX-core-vpn-predeploy-k9.msi
cisco-secure-client-win-X.X.XXXXX-umbrella-predeploy-k9.msi
\\Profiles\\umbrella\\OrgInfo.json
```



For more information, see Automated deployment tutorial with bundled Umbrella profile.

Automated Installation (Windows)

Describes Automated Installation (Windows) in Cisco Secure Access China. Cisco Secure Client can be installed using an unattended process that uses a script and follows the same workflow as the manual installation process.

Cisco Secure Client can be installed using an unattended process that uses a script and follows the same workflow as the manual installation process.

Install Cisco Secure Client

Use the following msiexec commands to install the required modules (Core + Umbrella):

```
msiexec /i "cisco-secure-client-win-5.X.XXXX-core-vpn-predeploy-k9.msi" /passive
 PRE_DEPLOY_DISABLE_VPN=1 /lvx_ vpninstall.log
msiexec /i "cisco-secure-client-win-5.X.XXXX-umbrella-predeploy-k9.msi" /passive
 PRE_DEPLOY_DISABLE_VPN=1 /lvx_ umbrellainstall.log
```

For more information, see Command-Line and RMM.

Note

The PRE_DEPLOY_DISABLE_VPN=1 parameter disables the VPN functionality for customers not using Cisco Secure Client for VPN access. Note, however, that the Core VPN module must be installed.

Install the Umbrella Profile

This step is necessary unless the profile is already bundled within the installation package (see Package Customization). After installation, copy the Umbrella profile (downloaded from your Umbrella dashboard) to the correct folder in the local device to register and activate Umbrella. This can be done with a task or post install script.

Copy the Umbrella profile to the following location:

```
%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json
```

Note

How to deploy Secure Client with Microsoft GPO article provides information on how to create an Umbrella profile using Microsoft Group Policy.

Instead of copying the Umbrella profile, you can create it with a script if your management software supports post-installation scripts.

The following example shows how to create an Umbrella profile using PowerShell. Replace DEPLOYMENT_KEY, ORG_ID, FINGERPRINT, and USER_ID values with the ones from your profile (OrgInfo.json) file:

Note

The deployment key feature has been carefully designed for backward compatibility:

- Cisco Secure Client 5.1.7 or earlier will continue to use the legacy User ID and fingerprint for registration purposes regardless of whether a deployment key is present.
- Cisco Secure Client 5.1.8 or later will use the deployment key regardless of whether the User ID and fingerprint are present. If the deployment key is not present then the legacy User ID and fingerprint will be used for registration purposes.

```
$org_file = "%PROGRAMDATA%\\Cisco\\Cisco Secure Client\\Umbrella\\OrgInfo.json"

$data=@"
{
    "deploymentKey” : “DEPLOYMENT_KEY",
    "organizationId" : "ORG_ID",
    "fingerprint" : "FINGERPRINT",
    "userId" : "USER_ID"
}
"@

if(-not(Test-Path -Path $org_file))
{
 $data > $org_file
}
```

(Optional) Disable VPN Functionality (Post installation)

If the VPN functionality was not disabled during installation, it can optionally be disabled with a post-installation task or script. You can disable the Secure Client VPN functionality after installation by creating a special profile, VPNDisable_ServiceProfile.xml.

```
%ProgramData%\Cisco\Cisco Secure
Client\VPN\Profile\**VPNDisable_ServiceProfile.xml**
```

Instead of copying the VPN profile, it can also be created with a script. This is useful if your endpoint management software supports post install scripts. The following example shows how to create the VPNDisable_ServiceProfile.xml using bash script.

```
$profile_file = "%PROGRAMDATA%\\Cisco\\Cisco Secure Client\\VPN\\Profile\\
VPNDisable_ServiceProfile.xml "
$data=@"
{
?\<xml version="1.0" encoding="utf-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">

  <ClientInitialization>
    <ServiceDisable>true</ServiceDisable>
  </ClientInitialization>
</AnyConnectProfile>
}
"@
```

```
if(-not(Test-Path -Path $profile_file))
{
 $data > $profile_file
}
```

For more information, see How to Disable VPN Functionality in Cisco Secure Client.

Multi Deployment Support

Describes Multi Deployment Support in Cisco Secure Access China. Cisco supports multiple deployments of Cisco Secure Access to address the requirements of our multinational customers.

Cisco supports multiple deployments of Cisco Secure Access to address the requirements of our multinational customers. While the foundational mechanisms remain consistent, each deployment comprises unique dashboards and connection endpoints configured to meet the specific requirements of each deployment. The main deployment, known as the Global deployment, is distinct and isolated from other regional deployments, such as the one in China, which meets local operational needs. For instance, the China-specific deployment does not offer Domain Name System (DNS) protection but does provide Secure Web Gateway (SWG) protection.

Client support for multiple deployments is available from Cisco Secure Client Release 5.1.8 on Windows and macOS. This enables roaming users to connect to the appropriate Secure Access deployment based on their current location.

To ensure a seamless experience when roaming between different Secure Access deployments–such as transitioning from Global deployment to one in China or vice versa–IT staff must properly provision the Cisco Secure Client installation. This involves configuring the client with multiple OrgInfo.json files, which contain the necessary configurations for the client to register and connect seamlessly to various Secure Access deployments. By provisioning clients in this manner, users can maintain consistent and reliable connectivity protection, regardless of their location, enhancing productivity and minimizing disruptions.

Manage Device Deployment

Provides instructions for managing device Deployment in Cisco Secure Access China. The Deployment Keys feature provides an effective way to manage device registration within organizations while mitigating unauthorized access.

The **Deployment Keys** feature provides an effective way to manage device registration within organizations while mitigating unauthorized access. This feature introduces the concept of a **deployment key** that can be activated, deactivated,and revoked. By utilizing deployment keys, administrators gain control over the credentials used by devices during registration for Secure Access protection. A deployment key is a field in the OrgInfo.json file, which is used when registering devices to your organization's network. This feature ensures that only authorized devices are enrolled by requiring an active deployment key for registration.

This feature facilitates seamless device registration and ongoing validation while offering the flexibility to deactivate keys when necessary. If any unauthorized devices try to connect, administrators can swiftly deactivate the current deployment key and delete the suspected devices from the dashboard, ensuring a secure and efficient network environment. The devices will not be able to re-register with the now-deactivated deployment key. Administrators can then activate a new deployment key. This allows IT teams to maintain operational continuity while safeguarding against unauthorized access.

Prerequisites for Device Deployment Management

Describes prerequisites for Device Deployment Management. For the Global deployment, the Deployment key feature is optional. In other deployments, such as in China, the deployment key feature is mandatory, and is automatically enabled.

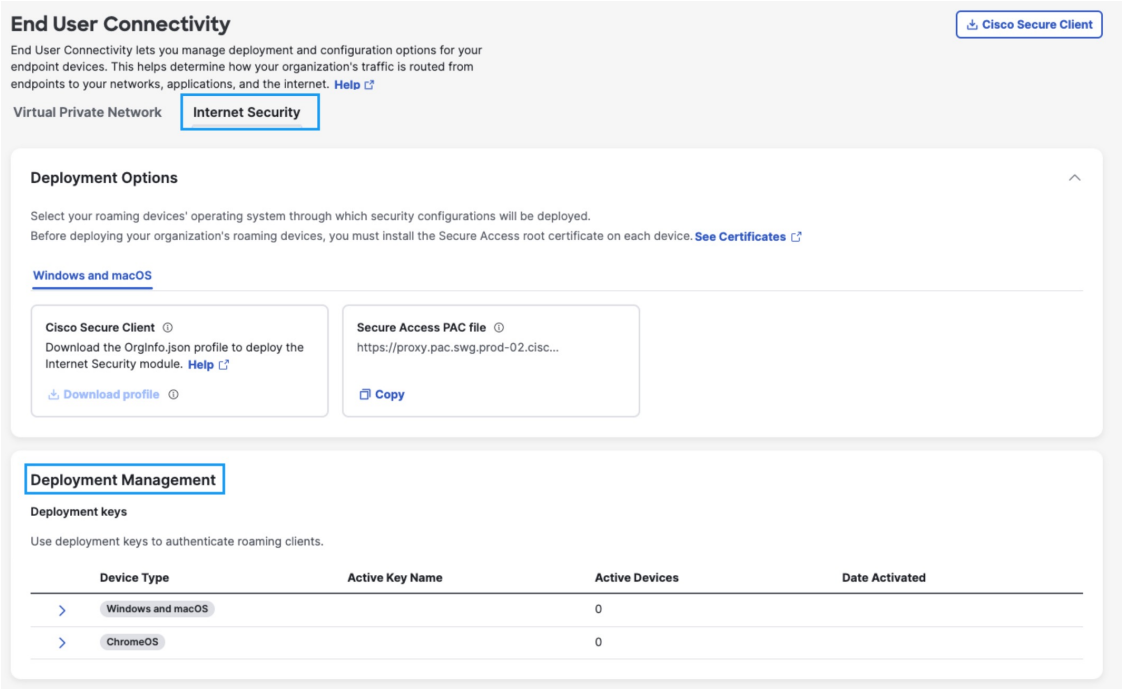
- Uninstall all the existing Cisco Secure Client installations.
- Enable the **Deployment Key** feature (**Connect > End User Connectivity > Internet Security**) if it is disabled.

> **Note**
>
> For the Global deployment, the **Deployment key** feature is optional. In other deployments, such as in China, the deployment key feature is mandatory, and is automatically enabled.

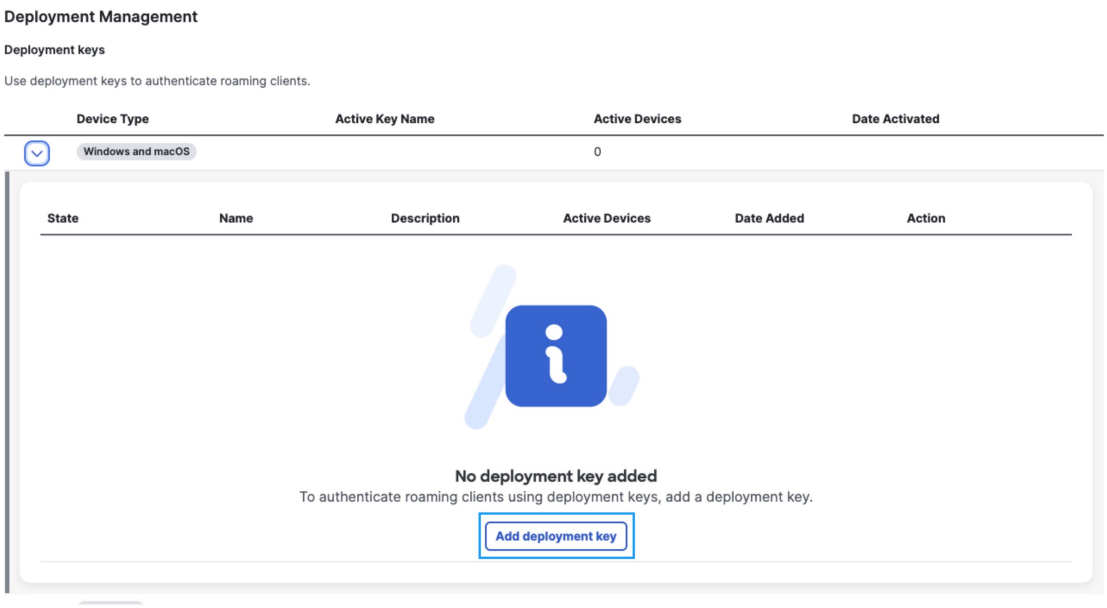
Add and Activate Deployment Key

Provides instructions for adding and activate deployment key. Only one deployment key can be active at a time for each device type.

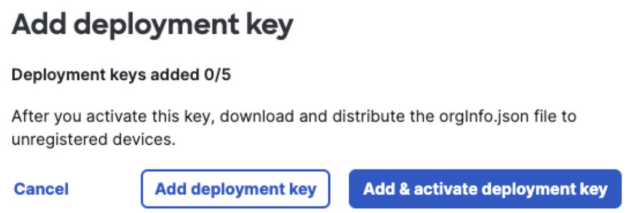
1. From the Secure Access China dashboard, navigate to **Connect > End User Connectivity**.
2. Click **Internet Security**.
3. In the **Deployment Management** section, expand the device type.



4. Click **Add deployment key**.



5. In the **Add deployment key** window, click **Add & activate deployment key** to create and activate a deployment key for inclusion in your organization's OrgInfo.json file.

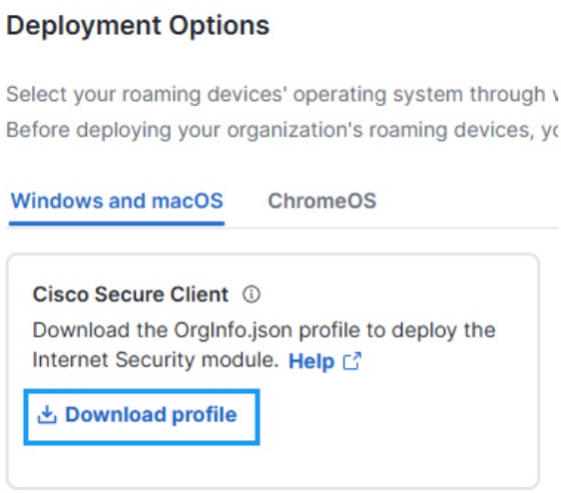


You can choose to add the deployment key immediately, but activate it later. In such a scenario, click **Add deployment key**. The deployment key is added to the table. When you are ready to activate the deployment key, click **Activate** in the **Action** column.

Important

- Only one deployment key can be active at a time for each device type.
- You can add up to five deployment keys per device type. To remove a key, contact Cisco support or your Account Manager.
- The deployment key name includes a random number to ensure its uniqueness.

If your Secure Access deployment requires a deployment key, or if your organization has already enabled them, the OrgInfo.json file can only be downloaded when there is an active deployment key (see image below). For more information on how to download the OrgInfo.json file, see Download the OrgInfo.json File.



Manage Deployment Key Compromise

Provides instructions for managing deployment key compromise. If you determine that a key has been compromised, take action to protect your network's integrity and security. Compromised keys can pose significant risks, as they may allow unauthorized access to your network.

If you determine that a key has been compromised, take action to protect your network's integrity and security. Compromised keys can pose significant risks, as they may allow unauthorized access to your network.

This section outlines the necessary actions to be taken to ensure network security and continuity, including deactivating compromised keys, understanding the effects on existing clients, and steps for activating and distributing a new key for secure device registration.

1. **Deactivate the Compromised Key:** As a first step, deactivate the compromised key. This action prevents any further device registrations using the deactivated key, ensuring that your network remains secure.

   To deactivate a deployment key, perform the following steps:

   a. From the Secure Access China dashboard, navigate to **Connect > End User Connectivity**.
   b. Click **Internet Security.**
   c. In the **Deployment Management** section, expand the device type.
   d. Click **Deactivate** in the **Action** column.

   Upon deactivating the compromised deployment key, it is important to consider its implications on both existing clients and the registration of new devices:

   - **Effect on existing clients:** It's important to note that deactivating a key will not disrupt the operation of clients already using it. These clients will continue to function normally, minimizing any potential impact on your current network operations.
   - **Limitations for new devices:** However, deactivated keys cannot be used for registering new devices. This means that any device attempting to register itself with the deactivated key will be unable to do so.

   > **Note**
   >
   > Devices that are deleted from the dashboard will automatically get reregistered when the Umbrella module is restarted, but only if the deployment key in their OrgInfo.json file is active.

2. **Activate the new deployment key:** To facilitate the registration of new devices, you must activate a different deployment key. This new key will replace the compromised one and will be used for future device registrations.

3. **Download a new profile:** After the new key is activated, download a new profile, specifically the OrgInfo.json file. This file contains the updated information, including the new active deployment key.
4. **Distribute the new profile to new devices:** Distribute the updated OrgInfo.json profile to any new devices that need to connect to your network. This ensures that they have the correct and secure credentials to register and operate within your network environment.
5. **Update the OrgInfo.json file for registered devices:** For devices that are already registered and need the OrgInfo.json file to be updated, place the new file in the correct subdirectory within the *Umbrella/data/regionaldata/<region_name>* directory, where the original OrgInfo.json file was located.

   After updating the file, restart the Cisco Secure Client–Umbrella Agent Windows service to apply the changes. The *region_name* in the directory should match the region tag found in the OrgInfo.json file. If the region tag is missing, it is assumed to be "global".

   > **Note**
   >
   > The OrgInfo.json file is case-sensitive only in the region-specific subdirectory, not in the Umbrella directory.

Delete a Deployment Key

Provides instructions for deleting a deployment key. To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

Activate DNS and SWG Protection

Provides instructions for activating dns and swg protection. Follow these instructions to activate DNS and SWG protection across multiple deployments:.

Follow these instructions to activate DNS and SWG protection across multiple deployments:

- **Primary OrgInfo.json file:** Ensure that there is a main OrgInfo.json file in the Umbrella runtime directory.

  For Windows, you can find the Primary OrgInfo.json file in: *%ProgramData%|Cisco|Cisco Secure Client|Umbrella*.

  For macOS, you can find the Primary OrgInfo.json file in: */opt/cisco/secureaccess/umbrella.*

- **Additional OrgInfo.json files:** Add OrgInfo.json files from other Secure Access deployments to the same directory. The file name must follow the format OrgInfo.*<custom_name>*.json, where custom name can include letters (a-z, A-Z), numbers (0-9), underscores (_), or dashes (-), for example, OrgInfo.global_org_55.json and OrgInfo.china_org_11.json.

Name and Deployment Identification

Describes name and Deployment Identification. The following information outlines the requirements and process for naming and identifying deployments using OrgInfo.json files. These steps ensure accurate identification and processing of Secure Access deployments across supported regions:.

The following information outlines the requirements and process for naming and identifying deployments using OrgInfo.json files. These steps ensure accurate identification and processing of Secure Access deployments across supported regions:

- Each OrgInfo.json file must include a "region" tag to identify its originating Secure Access deployment.
- Supported regions are "global" and "china." Any unrecognized region defaults to "global".
- If the "region" tag is missing, it is assumed to be "global" for backward compatibility purposes.
- Only one OrgInfo.json file is supported per deployment.

- After starting the Cisco Secure client, the client examines the Umbrella runtime directory to locate and process the OrgInfo.json files. These files are then organized into directories corresponding to each deployment, as identified by their "region" tags.

> **Note**
>
> OrgInfo.json files in the Umbrella directory are ignored by the Secure Client after the initial setup is complete.

- Cisco has implemented a location detection service that uses DNS to determine the current "region." The service returns a text record indicating the region name. Currently, "global" and "china" are the only supported regions.
- After the location is obtained, the client uses the matching OrgInfo.json going forward. This mechanism is designed to be forward-looking, with support for future deployments.

File Management

Describes file Management. This section explains how files and runtime data are stored and managed in the directory structure and provides instructions for updating the OrgInfo.json file in case of a deployment key change.

This section explains how files and runtime data are stored and managed in the directory structure and provides instructions for updating the OrgInfo.json file in case of a deployment key change.

- The *Umbrella/data/regionaldata/<region_name>* directory stores the files and relevant runtime data.
- To update an OrgInfo.json file because of a deployment key change, replace the OrgInfo.json file in the *Umbrella/data/regionaldata/<region_name>* directory while the Secure Client is not running. Ensure the client is stopped before making any changes to avoid conflicts or unexpected behavior. For more information on a deployment key change, see Manage Deployment Key Compromise.

Adhering to these guidelines ensures that organizations can configure their Cisco Secure Client for multi-deployment support, enabling efficient roaming and protection across different Secure Access deployments.

Customize Windows Installation of Cisco Secure Client

Provides instructions for customizing windows Installation of Cisco Secure Client in Cisco Secure Access China. 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 Web security), and DART (diagnostics) modules. By default, the Cisco Secure Client deploys with the VPN module.

Requirements

Describes customize windows Cisco Secure Client. Windows 8.1 or newer. The 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

Prerequisites

Lists the prerequisites for customizing windows Cisco Secure Client. Download the OrgInfo.json file from Secure Access China. For more information, see Download the OrgInfo.json File.

- Download the **OrgInfo.json** file from Secure Access China. 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

Provides instructions for customizing windows Cisco Secure Client. You can deploy the Cisco Secure Client for Windows with several options including:.

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. 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.

1. 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`.

> **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. Run the Windows installer to deploy the Cisco Secure Client Umbrella Roaming Security module.

1. Run the Windows installer to deploy the Cisco Secure Client Umbrella Roaming Security module.

```
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

Describes (Optional) Deploy the Cisco Secure Client DART Module. Run the Windows installer to deploy the Cisco Secure Client DART (diagnostics and troubleshooting) package.

1. Run the Windows installer to deploy the Cisco Secure Client DART (diagnostics and troubleshooting) package.

```
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

Describes 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.

1. 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.

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. 1 - Do not add domains. 1 - Do not re-query. DNS search suffixes are sent to local resolvers, unless this functionality is disabled.

> **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.
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.

Mass Deployment (macOS)

Describes Mass Deployment (macOS) in Cisco Secure Access China. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

(Optional) Package Customization

We recommend that on macOS platform, you customize the installation package before performing a mass deployment. For detailed instructions see Customize the macOS installation of Cisco Secure Client. You can customize the macOS installer image (.dmg file) to embed the Umbrella profile (OrgInfo.json) within it before deployment. The profile will then be automatically imported during installation. The package can also include customizations to (optionally) disable the Secure Client VPN functionality. You can use this customization to create a preconfigured deployment package that can be executed without additional scripts. For detailed instructions see Customize the macOS installation of Cisco Secure Client.

Add Umbrella Profile

Use the macOShdiutil command to create and mount a writable version of the .dmg image.

```
hdiutil convert cisco-secure-client-macos-<version>-predeploy-k9.dmg -format
UDRW -o csc-writeable.dmg
hdiutil attach csc-writeable.dmg
```

You can then add the Umbrella profile (OrgInfo.json) to the package in the following location:

/Volumes/Cisco\ Secure\ Client\ <version>/Profiles/Umbrella/OrgInfo.json

(Optional) Disable VPN Functionality

You can edit the following file (within the mounted DMG image) to disable the VPN functionality.

```
/Volumes/Cisco\ Secure\ Client\ <version>/Profiles/ACTransforms.xml
```

Add the following configuration to ACTransforms.xml:

```
<Transforms>
<DisableVPN>true</DisableVPN>
<DisableCustomerExperienceFeedback>true</DisableCustomerExperienceFeedback>
</Transforms>
```

Save the .dmg image

Eject the mounted disk image and convert it back to a read-only format.

diskutil eject /Volumes/Cisco\\ Secure\\ Client\\ <version> hdiutil convert csc-writeable.dmg -format UDRO -o csc-readable.dmg

The resulting file (csc-readable.dmg) can be distributed to users for manual installation or used as part of the Automated Installation process.

Automated Installation (macOS)

Describes Automated Installation (macOS) in Cisco Secure Access China. You can install Cisco Secure Client using a scripted, unattended process that follows the same workflow as the standard manual installation.

You can install Cisco Secure Client using a scripted, unattended process that follows the same workflow as the standard manual installation.

(Optional) Disable VPN Functionality (Post-Installation)

If the VPN functionality is not disabled during installation, it can be (optionally) disabled with a post-installation task or script. The Secure Client VPN functionality can be disabled after installation by creating a special profile, VPNDisable_ServiceProfile.xml. Place the profile in the following directory: /opt/cisco/secureclient/vpn/profile/VPNDisable_ServiceProfile.xml Instead of copying the umbrella profile, you can create it with a script. This is useful for management software that supports post-install script. The following example shows how to create the VPNDisable_ServiceProfile.xml using a bash script.

```
# !/bin/bash

profile_file="/opt/cisco/secureclient/vpn/profile/VPNDisable_ServiceProfile.xml"

data="<?xml version="1.0" encoding="utf-8"?>\\n
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">\\n
  <ClientInitialization>\\n
    <ServiceDisable>true</ServiceDisable>\\n
  </ClientInitialization>\\n
</AnyConnectProfile>\\n"

if ! test -f $profile_file; then
 echo -e $data > $profile_file
fi
```

For more information, see How to Disable VPN Functionality in Cisco Secure Client.

Allow Secure Client System Extensions

By default, macOS requires users to accept the activation of a new system extension. As a result, users are presented with a dialog box when they first install Cisco Secure Client. Users must follow the prompts to allow the Cisco Secure Client - Socket Filter' extension. Alternatively, the system extension can be approved centrally by the administrator using endpoint management, or device management suites if the device is managed by UEM tools. For more information, see the advice in Approving the Cisco Secure Client System Extension.

Installation (Pre-Deployment Package)

Cisco Secure Client (and its modules) are provided as a single 'pre-deployment' .dmg package. You must provide the attached **install_choices.xml** file to customize the installation so that only the necessary modules are installed. The attached **install_choices.xml** is preconfigured to install the minimum modules (Core VPN + Umbrella). This installation method is possible only if you are performing a scripted installation or if your endpoint management tool supports the **-applyChoiceChangesXML** parameter. Example:

```
hdiutil attach
~/Downloads/cisco-secure-client-macos-X.X.XXXX-core-vpn-predeploy-k9.dmg

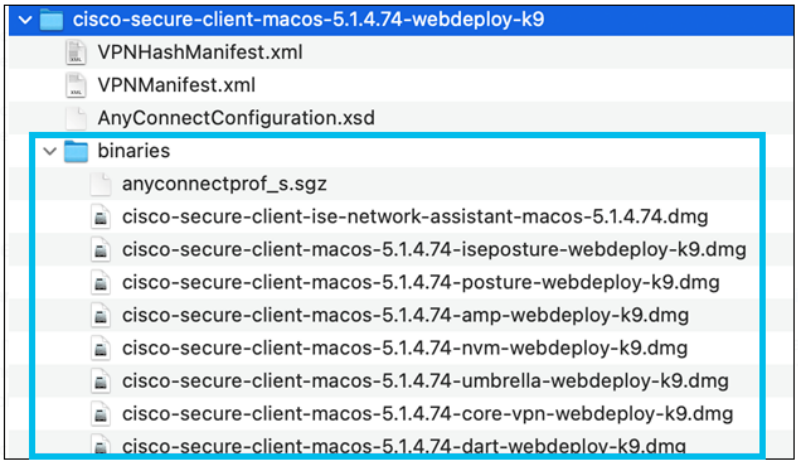
sudo installer -pkg /Volumes/Cisco\\ Secure\\ Client\<version>/Cisco\\ Secure\\
 Client.pkg -applyChoiceChangesXML ~/Downloads/install_choices.xml -target /
```

Note

The 'install_choices.xml' file is used to install the Core Secure Client and Umbrella modules. Additionally, it can be edited to include the installation of other Secure Client modules as well.

Installation (Web Deployment Package)

Cisco also provides a web deployment package that contains each Cisco Secure Client module as individual .dmg files. This alternative is only recommended if your endpoint management tool can't supply the required **-applyChoiceChangesXML** parameter to select the corresponding modules. Download the alternative headend (webdeploy) package (.pkg) and extract it with the macOS archive utility. Locate the relevant .dmg files in the binaries/ directory of the extracted package.



Both the Core VPN module and the Umbrella module must be installed separately as shown in the following examples:

```
hdiutil attach cisco-secure-client-macos-X.X.XXXX-core-vpn-webdeploy-k9.dmg
sudo installer -pkg /Volumes/Cisco\\ Secure\\ Client\\ -\\ AnyConnect\\ VPN\\
 X.X.X.XX/ -target /

hdiutil attach cisco-secure-client-macos-X.X.XXXX-umbrella-webdeploy-k9.dmg
sudo installer -pkg /Volumes/Cisco\\ Secure\\ Client\\ -\\ Umbrella\\ X.X.X.XX/
 -target /
```

Install Umbrella Profile

This is necessary unless the profile is already bundled with the installation package, see Package Customization. After installation, copy the Umbrella profile to the correct folder on the local machine to register and activate the Umbrella module. This method is useful for endpoint management software that can push the files to the endpoint. The profile must be placed in the following location: /opt/cisco/secureclient/umbrella/OrgInfo.json Instead of copying the umbrella profile, you can create it with a script. This is useful if your endpoint management tools support **post-install** scripts. The following example shows how to create the OrgInfo.json file using a bash script. Replace DEPLOYMENT_KEY, ORG_ID, FINGERPRINT, and USER_ID values with the ones from your profile.

Note

The deployment key feature has been carefully designed for backward compatibility:

- Cisco Secure Client 5.1.7 or earlier will continue to use the legacy User ID and fingerprint for registration purposes regardless of whether a deployment key is present.
- Cisco Secure Client 5.1.8 or later will use the deployment key regardless of whether the User ID and fingerprint are present. If the deployment key is not present then the legacy User ID and fingerprint will be used for registration purposes.

```
# !/bin/bash

orginfo_file="/opt/cisco/secureclient/umbrella/OrgInfo.json"
data="{\\n
    "deploymentKey" : "DEPLOYMENT_KEY",\\n
    "organizationId" : "ORG_ID",\\n
    "fingerprint" : "FINGERPRINT",\\n
    "userId" : "USER_ID"\\n
}"
if ! test -f $orginfo_file; then
 echo -e $data > $orginfo_file
fi
```

Note

The Meraki Systems Manager (SM) Deployment guide explains how to deploy the Umbrella profile using scripts.

Related information

mass-deployment-macos.dita#Cisco_a6139912-27a1-4115-bb0e-fda3a53c2c4f/package on page 617

Customize macOS Installation of Cisco Secure Client

Provides instructions for customizing macOS Installation of Cisco Secure Client in Cisco Secure Access China. 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 China 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 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 customize macOS Cisco Secure Client. 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

Prerequisites

Lists the prerequisites for customizing macOS Cisco Secure Client. Download the OrgInfo.json file from Secure Access China. For more information, see Download the OrgInfo.json File.

- Download the **OrgInfo.json** file from Secure Access China. 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

Provides instructions for customizing macOS Cisco Secure Client. Choose the modules to install with the Cisco Secure Client on a macOS device.

Choose the modules to install with the Cisco Secure Client on a macOS device.

Step 1 – Make the DMG Package Writeable

Describes 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.

1. Open a **Terminal** and set the DMG file to Read/Write.

```
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

Describes 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.

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

Describes how to copy OrgInfo.json to Cisco Secure Client Installation Directory.

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 China to **Volumes/Profiles**.

Step 4 – (Optional) Hide the VPN Module

Describes 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**.

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

Describes 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.

- To skip a module, define the module with `0`.
- To install a module, define the module with `1`.

> **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

Describes step 6 - Set Up the Correct Extension Permission Settings. Follow the payload guidance in Cisco Secure Client Extension Approval using MDM to deploy the System Extension settings.

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

Describes 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.

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 /
```

VPN Headend Deployment

Describes VPN Headend Deployment in Cisco Secure Access China. Customers utilizing the Secure Client VPN functionality can deploy the Umbrella module directly from their VPN headend, a method known as web deployment.

Customers utilizing the Secure Client VPN functionality can deploy the Umbrella module directly from their VPN headend, a method known as web deployment. This configuration is performed on the VPN server.

- Clients with existing AnyConnect Secure Client deployments can automatically download the Umbrella module and profile when they initiate a connection to the VPN.
- Cisco Secure Client can also be installed through a self-service workflow, where each user visits the HTTP web portal hosted on the VPN headend.
- This web deployment method allow you to update Cisco Secure Client and the Umbrella module software versions by centrally uploading new versions to the VPN server.

For more information, see Web Deployment of Cisco Secure Client.

Secure Firewall Management Center and Secure Firewall Threat Defense

Describes Secure Firewall Management Center and Secure Firewall Threat Defense in Cisco Secure Access China. This configuration guide covers the steps to provision the Umbrella Module in the Secure Firewall Management Center for version 6.5 or later.

This configuration guide covers the steps to provision the Umbrella Module in the Secure Firewall Management Center for version 6.5 or later. The provisioned module is applied to Secure Firewall Threat Defense managed by the management center.

Prerequisites to provision the Umbrella Module

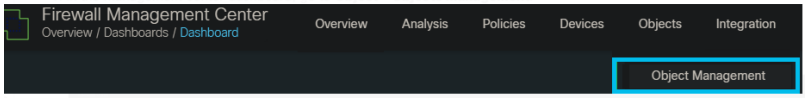
- Access to the Cisco Umbrella Dashboard.
- Access to management center or threat defense, as this version adds support for additional AnyConnect modules. For versions earlier than 6.7, FlexConfig can be used to deploy the module, you can refer to the Cisco documentation for details.
- Umbrella Module Profile (orginfo.json).
- AnyConnect VPN module configuration is already complete and functional on the management center or threat defense.

Procedure to enable Secure Client Umbrella Module in Management Center and Threat Defense

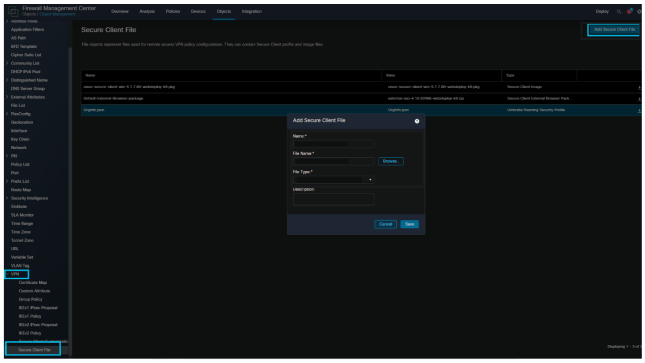
Follow these steps to enable Secure Client Umbrella Module in the management center:

Procedure

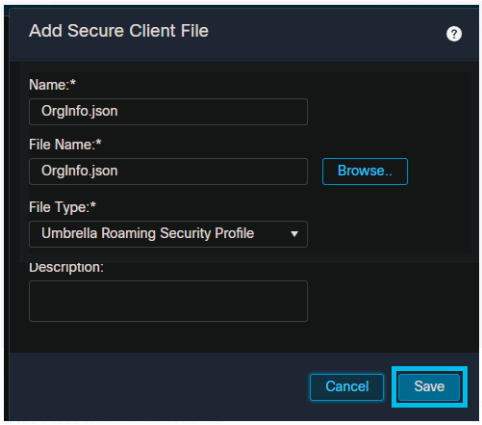
1. In the management center dashboard, go to **Object** > **Objects Management**.



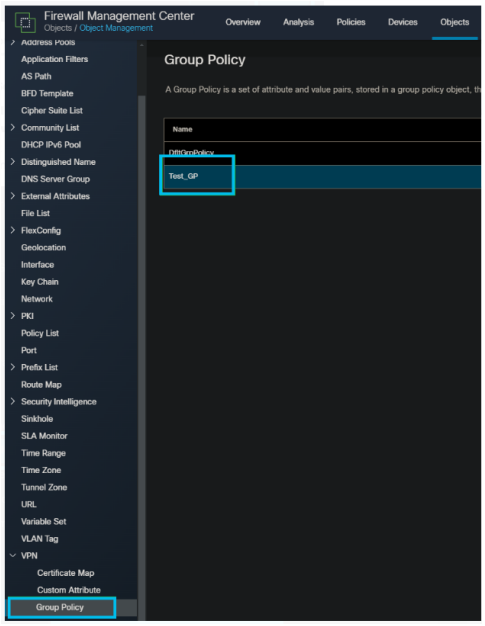
2. Navigate to **VPN** > **Secure Client File**.
3. On the **Secure Client File** page, click the **Add Secure Client File**.



4. In the Add Secure Client File window, complete the fields, including the following:
   a) Set a name for the profile (locally significant). From the **File Name**, click **Browse** to choose the JSON file that was downloaded from the Cisco Umbrella dashboard.
   b) From the **File Type** drop-down list, choose **Umbrella Roaming Security Profile**, and click **Save**.

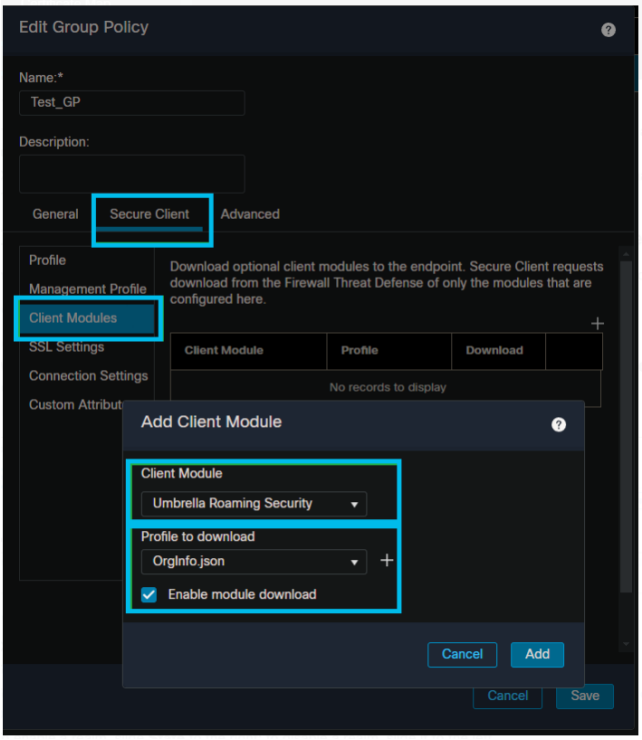


5. On the Group Policy window, click **Group Policy**, and then select the group policy that you're using to deploy Umbrella ("Test_GP" in this case).



6. Click the **Secure Client** tab, and then click **Client Modules**. Click **+** button to add a client module.
   a) In **Add Client Module**, from the **Client Module** drop-down list, choose **Umbrella Roaming Security**, and from **Profile to download** drop-down list, choose the profile that was added under step 4.

b) Check **Enable module download** checkbox so that users connecting through Secure Client will automatically download the Umbrella JSON profile.

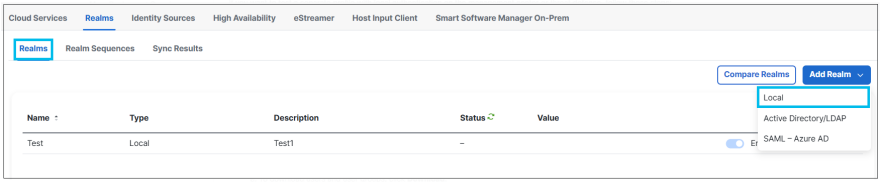


What to do next

(OPTIONAL) VPN Local Authentication (Management Center 7.0 or later required)

If you want to test a separate profile with local authentication on the management center or threat defense, follow these steps:

1. Create a local realm.
   a. Local usernames and passwords are stored in local realms.
   b. When you create a realm **Integration** > **Other Integrations** > **Realms** and select or create a new **LOCAL realm** type, you are prompted to add one or more local users.
   c. click **Add Realm** > **Local** to create a local realm.



2. Manage a local realm
   a. Click **Integration** > **Other Integrations** > **Realms**.
   b. To delete a realm, click **Delete**.
   c. To edit a realm, click **Edit** next to the realm and make changes as described in Create an LDAP Realm or an Active Directory Realm and Realm Directory.
   d. To enable a realm, slide **State** to the right; to disable a realm, slide it to the left.
   e. To download users and user groups, click **Download**.
   f. To copy a realm, click **Copy**.

Meraki Systems Manager (SM) Deployment

Describes Meraki Systems Manager (SM) Deployment in Cisco Secure Access China. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Deploying Cisco Meraki Systems Manager (SM) consists of the following steps:

1. Consult our command line parameters reference and confirm if any additional MSI arguments are desired. Examples include hiding from Add/Remove programs and installing without the VPN core.
2. Add a new application to the Meraki SM portal for deployment for the Cisco Secure Client core module MSI.
3. Repeat the process for the Umbrella Module MSI as a second application. For the Umbrella module, add the following command line execution, replacing <OrgInfo.json> with the contents of your organization's Umbrella profile OrgInfo.json file:

```
echo <OrgInfo.json> > "C:\ProgramData\Cisco\Cisco Secure
Client\Umbrella\OrgInfo.json"
```

An example command line execution is below:

```
echo {    "organizationId" : "12345",    "fingerprint" :
"12345123451234512345",    "userId" : "12345"} > "C:\ProgramData\Cisco\Secure
 Client\Umbrella\OrgInfo.json"
```

Migration from Umbrella Roaming Client

Describes Migration from Umbrella Roaming Client in Cisco Secure Access China. The standalone Umbrella Roaming module is approaching end of support and is directly replaced by the Umbrella Roaming module in Cisco Secure Client.

The standalone Umbrella Roaming module is approaching end of support and is directly replaced by the Umbrella Roaming module in Cisco Secure Client. The Umbrella Roaming module in Cisco Secure Client provides a more robust handling of DNS and web traffic using the Cisco Secure Client's underlying driver technologies. Cisco Secure Client provides a greater level of compatibility and reliability than the legacy Roaming Client. For more information, see Benefits from upgrading Cisco Umbrella Roaming Client to Cisco Secure Client.

To upgrade an existing Roaming Client computer to the Umbrella Roaming module in Cisco Secure Client, install Cisco Secure Client using any of the previous guides of Deploy Umbrella module in Cisco Secure Client.

- The existing Umbrella profile information (OrgInfo.json) from Roaming Client will be retained.
- The standalone Umbrella Roaming Client will be automatically removed during installation.
- Under no circumstances should both the Umbrella Roaming Client and Umbrella module be running. Ensure you have disabled any deployment tasks for the Umbrella Roaming Client to prevent re-installation.

Install the Root Certificate for All Browsers

Provides instructions for installing the Root Certificate for All Browsers in Cisco Secure Access China, including Inspect and Decrypt HTTPS Traffic and Render Block and Warn Pages. It explains the sequence of actions and relevant settings presented in the procedure.

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

Describes inspect and Decrypt HTTPS Traffic. Inspect HTTPS traffic and perform SSL decryption. If you do not enable HTTPS inspection, Secure Access China is unable to perform file inspection, URL matching, advanced application controls, or provide URL level visibility for HTTPS communications.

Inspect HTTPS traffic and perform SSL decryption.

1. Install a Secure Access root certificate for each browser on a user device.
2. Enable **HTTPS inspection** in the Web profile for the Secure Access secure web gateway (SWG).

   If you do not enable HTTPS inspection, Secure Access China is unable to perform file inspection, URL matching, advanced application controls, or provide URL level visibility for HTTPS communications.
3. Enable **Decryption** in the Web profile for the Secure Access secure web gateway (SWG).

For more information, see Manage Web 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 China 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 China does not downgrade the HTTPS protocol to HTTP when serving a block page. Thus, if a root certificate is not installed, the web browser displays a certificate warning to the user. For more information, see Manage Notification Pages.

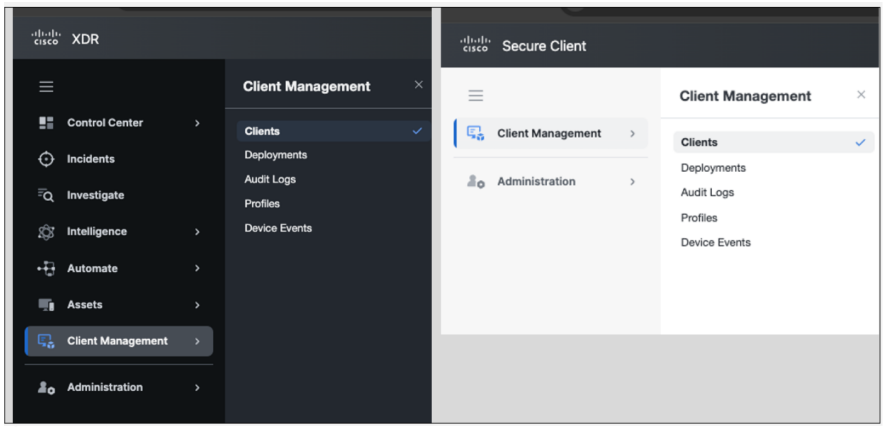
Cloud Management

Describes Cloud Management in Cisco Secure Access China. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Overview

Cisco Secure Client can now be deployed from Cisco cloud utilizing Cisco XDR or Cisco Secure Client Cloud Management. Cisco XDR is a cloud-based security solution that simplifies operations by helping security teams detect, prioritize, and respond to threats. It integrates Cisco and third-party tools into a single platform for comprehensive threat management. Cisco Secure Client with Client Management is the next-generation Secure Mobility Client that combines the existing features of both AnyConnect and Secure Endpoint with a Cloud Management solution in a single, unified end-user interface. For customers who are not using Cisco XDR, Cisco offers Cisco Secure Client Cloud Management at no additional cost. This service is available to those with an active Cisco Secure Client or Umbrella license. Both solutions support the creation and uploading of Cisco Secure Client profiles, including the Umbrella Orginfo.json file. Deployments can then be configured to specify Cisco Secure Client modules using these profiles. The Cloud Management module is essential, enabling the client to check in with the cloud every 2, 4, 6, or 8 hours. This ensures that clients remain up to date, as any changes to their deployment are pushed during these check-ins. Additionally, administrators receive a client inventory that displays installed versions, modules, and the last check-in time.

The following image shows the XDR Client Management and Cisco Secure cloud management:



Deploying Cisco Secure Client

In this instance, XDR will be utilized; However, the procedure remains the same when using Cisco Secure Client Cloud Management too.

Profiles

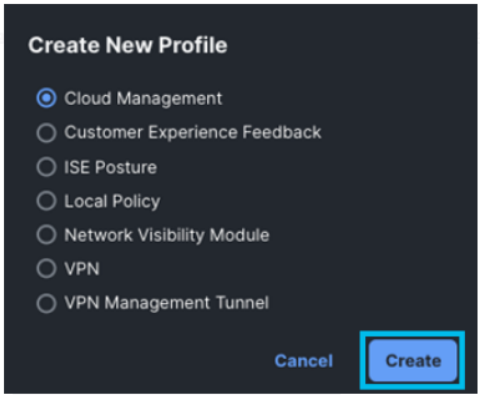
The Profiles page provides a list of all the Cisco Secure Client profiles in your Cisco XDR organization and allows you to create profiles that control the Cisco Secure Client endpoint software. We recommend that you start by gathering existing profiles or using the profile editor in Client Management to create new ones. The online profile editor can create profiles for the modules listed here. For the Network Access Manager (802.1x supplicant) and the Umbrella Orginfo.json, these profiles must be uploaded.

Note

There are only two default profiles, and this is directly from the XDR Client Management Help. The NVM Cloud Default Profile is mandatory but the Cloud Managment default profile is optional. Cisco XDR includes the following default profiles to help you get started with Cisco Secure Client deployments:

- Cloud Management Default Profile
- NVM Cloud Default Profile

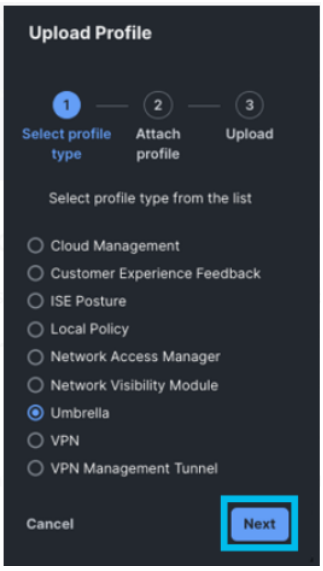
  The default profiles are associated with the XDR default deployment, which can be installed on your endpoints to improve detections and enrich incidents in Cisco XDR. These profiles can also be applied to any user created deployments. For more information, see XDR Profiles.



Uploading the Orginfo.json profile

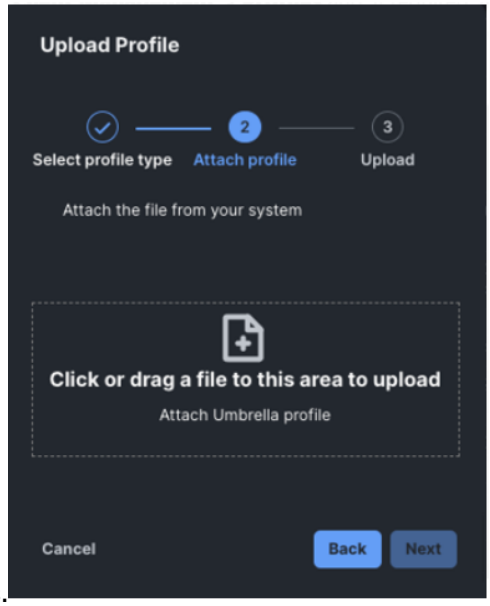
Upload the rginfo.json file that you previously downloaded from the Umbrella dashboard.

1. Navigate to **Client Management > Profiles > Upload**, select **Umbrella** from the list and click **Next**.

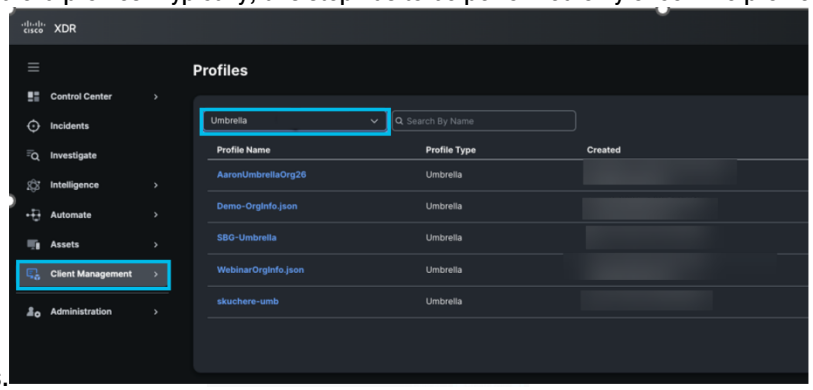


   A pop-up is displayed.

2. You can either drag and drop the Orginfo.json file or navigate to its location to add this profile and make it available for deployments.



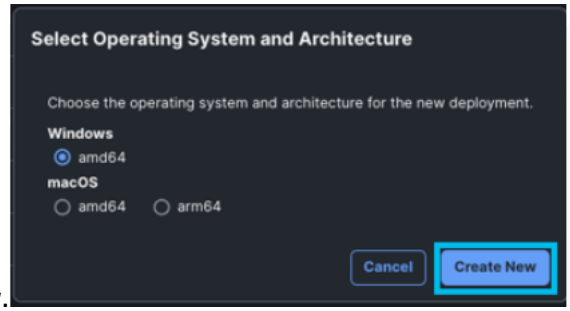
3. After the file is uploaded, go to **Client Management > Profiles** and, if required, apply a filter for Umbrella to display only the available Umbrella profiles. Typically, this step has to be performed only once. The profiles can be used in multiple deployments.



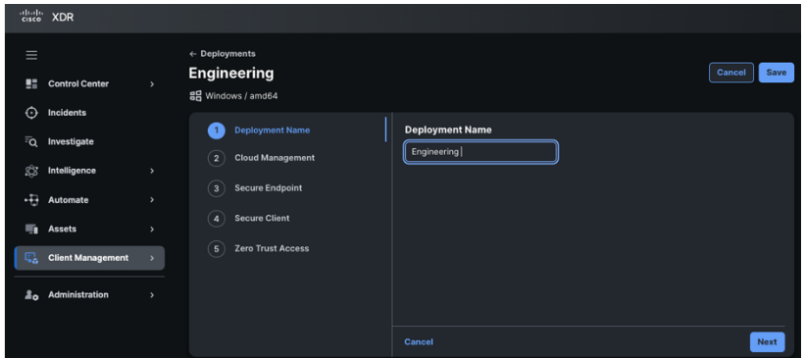
Create a Deployment

The Deployments page provides a list of all the Cisco Secure Client deployments in your Cisco XDR organization and allows users to define a list of all the packages and related profiles that must be installed on all the computers in a specific deployment within an organization (for example, QA department).

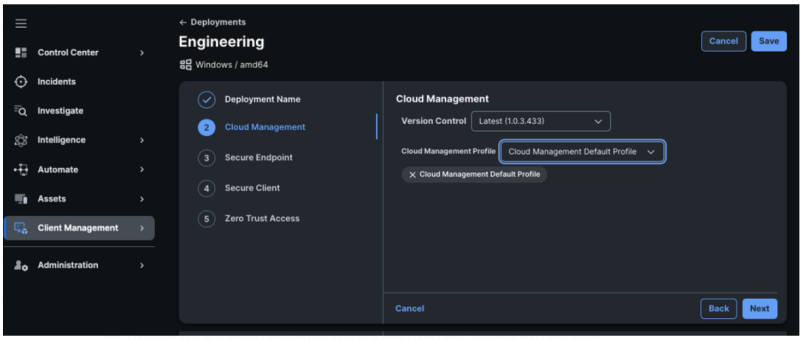
1. To create a new deployment, navigate to **Client Management > Deployments** and click **New**. You can also edit existing deployments from the list displayed.
2. When prompted, select the operating system for the deployment, that is, either **Windows or macOS**. In this example, **Windows** is selected.



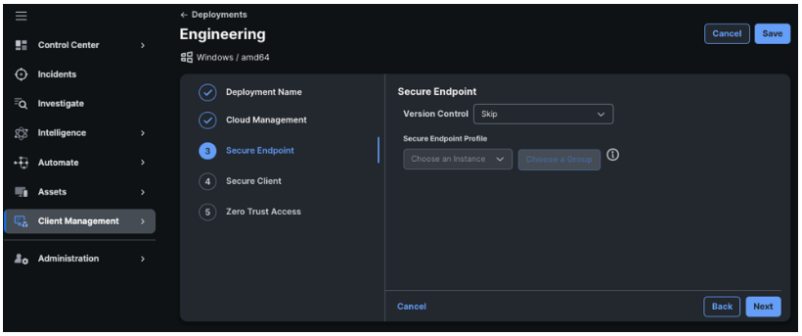
3. Click **Create New**.
4. **Specify** a name for the deployment: This name will be included in the file name of the final package after the deployment configuration is complete.



Every deployment includes the Cloud Management module and profile. Choose a version for both the Cloud Management module and the Cloud Management profile. While the default Cloud Management profile typically works well, administrators have the option to create a custom profile, if needed. For example, you might want different check-in intervals or update Windows for certain user groups.



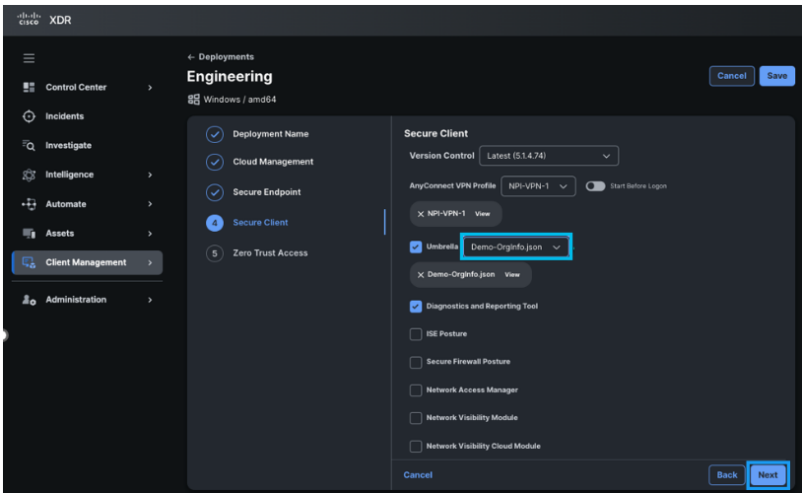
5. From the **Version Control** drop-down list, choose the Secure Endpoint connector version that you want to deploy. If you prefer to not include the Secure Endpoint module, choose **Skip** and proceed. In this example, **Skip** is chosen.



Next, configure the Cisco Secure Client section to include AnyConnect VPN, Umbrella, and DART in the deployment.

> **Note**
>
> If you don't plan to use AnyConnect VPN, you can skip adding a VPN profile. After completing the cloud deployment, push the **VPNDisable_ServiceProfile.xm** file to the VPN profile directory (as described earlier in Customize Windows Installation of Cisco Secure Client guide). This hides the AnyConnect VPN tile in the GUI.

To complete the Cisco Secure Client section of the deployment, we selected an existing VPN profile that was either uploaded or created in Client Management using the profile editor. Along with the VPN profile, we enabled the DART and the Umbrella module, specifying the previously uploaded Umbrella OrgInfo.json profile. This configuration generates a deployment package that includes the specified modules and profiles upon installation.

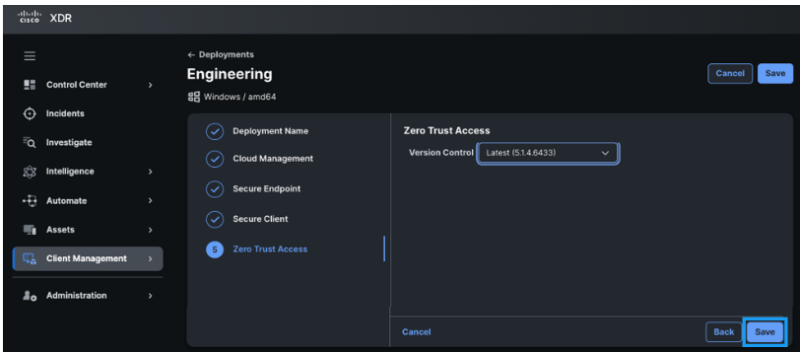


6. After completing the deployment configuration, click **Next**.

For Windows deployments, the administrator will have the option to add the Zero Trust Access (ZTA) module for Cisco Secure Client. While the ZTA module is supported on macOS through other deployment methods, it is not yet supported for cloud deployments using XDR or Cisco Secure Cloud Client Management. The ZTA module is designed to work seamlessly with the Cisco Secure Access solution.

ZTA focuses on knowing, understanding, and controlling who and what is on your network:

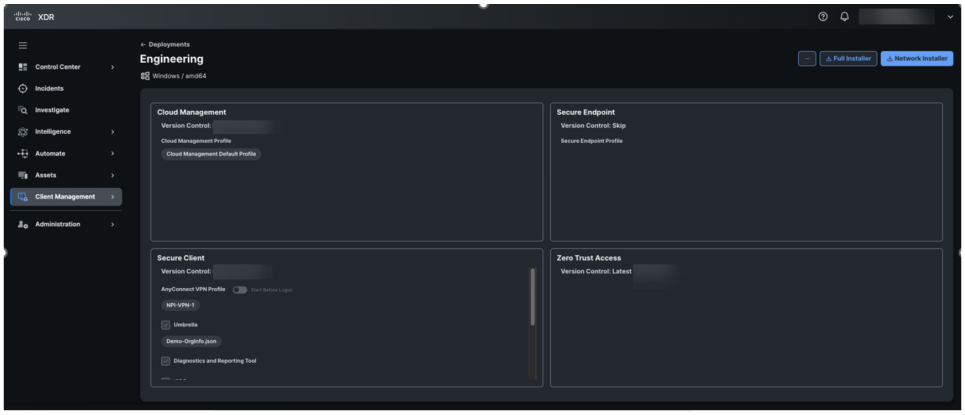
- It grants appropriate access based on role or function.
- It controls application access at the network layer.
- By assuming that the network layer is untrustworthy, it helps prevent unauthorized access and breaches.



7. When you click **Save** it finalizes the deployment configuration and presents the Administrator with two installation package options – Network Installer or Full Installer.

   - **Network Installer**: A streamlined installer that includes only the Cloud Management client. When using the Network Installer, it will download the remaining components specified in the deployment in the background.
   - **Full Installer**: A comprehensive package that includes all the installers and profiles configured for the deployment. It is larger than the Network Installer, and when used, it installs the Cloud Management client along with all associated packages from the deployment.

     Both the Full and Network installers will link the device to the deployment from which the installer was created. Whenever the device connects to the cloud, it checks the installed packages against the deployment requirements. The device then updates the packages and profiles to match the deployment, but does not downgrade any packages that are newer than those specified in the deployment.

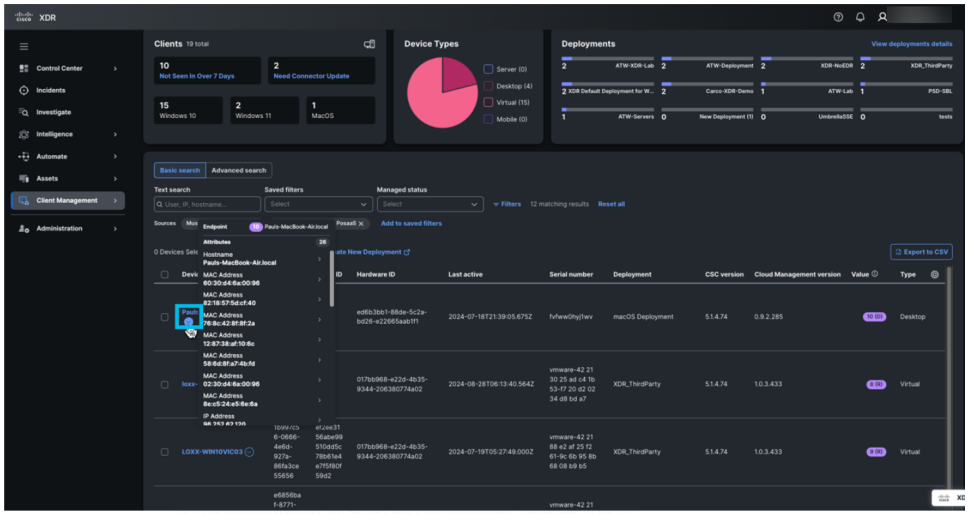


Post Deployment

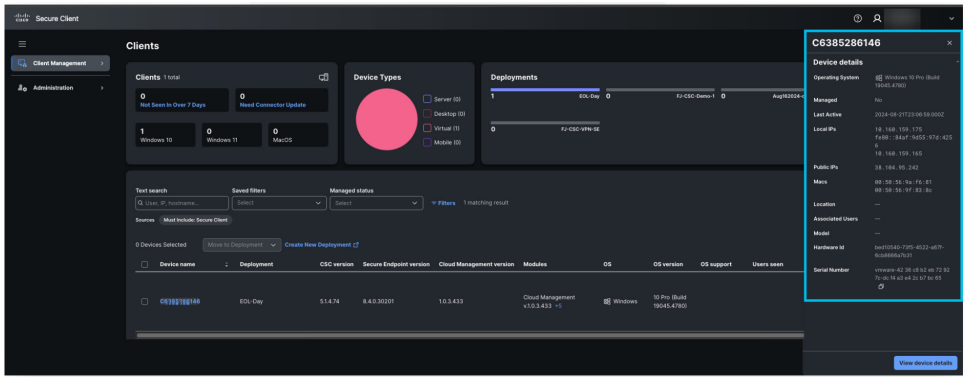
After deploying Cisco Secure Client with Cloud Management, both Cisco XDR and Cisco Secure Client Cloud Management offer valuable insights into the clients deployed to the cloud. The administrator can access a comprehensive inventory of these clients by navigating to Client Management > Clients. A table lists all the Cisco Secure Client devices in your organization along with their data. The following information is also displayed:

- The total number of devices found.
- The number of devices selected.
- **Move to Deployment**: Click to move selected devices to a specific deployment.
- **Create New Deployment**: Click to open the Deployments page. From this page, Admin users can define a list of all the packages and related profiles that must be installed on all the computers in a specific deployment within an organization.
- **Export to CSV**: Click to download the table contents to a spreadsheet. Note that only the contents of the table will be downloaded.

1. Each device includes a pivot menu icon that enables you to take action on it. You can perform some actions directly using pivot menu or pivot to the integrated product to perform additional actions.



The behavior varies slightly when performed in Cisco Secure Client Cloud Management. However, the Administrator can switch to a detailed view for more information.



Additional Reference

For more information about Cisco Secure Client Cloud Management, please refer to the FAQ.

Additional References

Describes Additional References in Cisco Secure Access China. The following guides provide in-depth information for customers deploying Cisco Secure Client with endpoint management, systems management, or device management tools.

The following guides provide in-depth information for customers deploying Cisco Secure Client with endpoint management, systems management, or device management tools.

Command Line and RMM Reference (Windows)	Provides information about installing Cisco Secure Client using the CLI (Windows)
Customize Windows Installations of Cisco Secure Client (Windows)	Provides command-line reference for installing Cisco Secure Client. Includes customizations for disabling the VPN functionality and locking down Cisco Secure Client services
Customize MacOS installations of Cisco Secure Client	Provides detailed instructions for creating a mass deployment package for macOS. Includes customizations for disabling VPN functionality and approving Cisco Secure Client extensions.

VPN Headend Installation (Windows)	Provides customers who are using Secure Client VPN functionality to deploy Umbrella from their VPN headend. This will automatically download the software and profile when connecting to VPN.
Meraki Systems Manager (SM) (Windows)	Provides information about how to deploy the Umbrella profile (OrgInfo.json) on Windows computers using post-install scripts.
Microsoft InTune (Windows)	Provides a tutorial for Intune (Windows clients). The software and Umbrella profile are packaged together using the Content Prep tool and delivered to Windows endpoints.
Microsoft InTune (macOS)	Provides a tutorial for Intune (macOS clients). A mass deployment package is created and deployed with a scripted task.
Shared Folder Installation (Windows)	Provides an example on how to install from a shared folder installation source using a script. In this example, the script is triggered using a scheduled task (Windows group policy).
GPO Installation (Windows)	Provides Cisco Secure Client to deploy as an application package using Windows group policy (GPO). The Umbrella profile is deployed to the endpoint using Windows group policy (GPO).
JAMF (macOS)	Provides a tutorial for JAMF (macOS Clients). The software, profile, and install choices (module selection) are bundled together using the JAMF composer.
Deploy Cisco Secure Client	Provides instructions for installing Cisco Secure Client and all modules (non-Umbrella specific) from cisco.com.

Remote Monitoring and Management Deployment Tutorials

Describes Remote Monitoring and Management Deployment Tutorials in Cisco Secure Access China. The following tutorials are suitable for MSPs using Remote Monitoring and Management (RMM) to deploy the Umbrella Roaming Security Module to multiple end customers.

The following tutorials are suitable for MSPs using Remote Monitoring and Management (RMM) to deploy the Umbrella Roaming Security Module to multiple end customers. A different Umbrella profile (OrgInfo.json) can be supplied for each customer in the RMM tool.

ConnectWise	Cisco-provided sample ConnectWise configuration templates.
Kaseya	Cisco-provided sample Kaseya configuration templates.

45 Manage Internet Security on Cisco Secure Client

Topics:

- Manage Internet Security on Cisco Secure Client

Provides an overview of Manage Internet Security on Cisco Secure Client in Cisco Secure Access China, including Download the OrgInfo.json File, Umbrella Roaming Security Module Requirements, and Domain Management. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Internet Security on Cisco Secure Client

Provides instructions for managing internet Security on Cisco Secure Client in Cisco Secure Access China. 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 China.

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 China. 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:

- Web security–Secure web gateway (SWG)

Once deployed, Cisco Secure Client registers the user device with Secure Access China 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 China. 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.

Download the OrgInfo.json File

Provides instructions for downloading the OrgInfo.json File in Cisco Secure Access China. You can deploy various modules with the Cisco Secure Client.

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 (Web security) requires the Secure Access China **OrgInfo.json** file. The Secure Access China **OrgInfo.json** file associates a Cisco Secure Client deployment with the Umbrella Roaming Security module to a Secure Access China user and organization. Once the module is deployed on the Cisco Secure Client, Secure Access China 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 China to install the Cisco Secure Client Umbrella module, the roaming device is managed by that instance of Secure Access China 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 China to the device.

Prerequisites

Lists the prerequisites for downloading the orginfo json, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

Provides instructions for downloading OrgInfo.json, the Cisco Secure Client internet security profile used to configure the client deployment for Secure Access China.

Download the Cisco Secure Client internet security profile (**OrgInfo.json**).

Step 1 – Download the OrgInfo.json File

Describes step 1 - Download the OrgInfo.json File. Navigate to Connect > End User Connectivity > Internet Security. For Cisco Secure Client, click Download Profile to save the OrgInfo.json file to the local system.

1. Navigate to **Connect > End User Connectivity > Internet Security**.
2. For Cisco Secure Client, click **Download Profile** to save the **OrgInfo.json** file to the local system.

Step 2 – Copy the OrgInfo.json File to the Target Directory

Describes step 2 - Copy the OrgInfo.json File to the Target Directory. You have two options for copying the OrgInfo.json file:.

You have two options for copying the OrgInfo.json file:

1. **Using the Profiles Directory**

   Cisco Secure Client is available as a .zip file (for Windows) or a .dmg file (for macOS), each containing installer packages. Within the extracted archive, you will find a subdirectory named Profiles. Copy OrgInfo.json to the profile directory for the Umbrella module at Profiles\umbrella to ensure that the profile is automatically installed during product installation.

2. **Using the Installation Directory**

   Alternatively, you can copy the OrgInfo.json file directly to the location of the Cisco Secure Client runtime directory at:

```
Windows: %ProgramData%\Cisco\Cisco Secure Client\Umbrella
macOS: /opt/cisco/secureclient/umbrella/
```

> **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.

When you deploy the OrgInfo.json file for the first time, the Cisco Secure Client copies the OrgInfo.json file to the data subdirectory (see below), 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. The data subdirectory is:

For Cisco Secure Client 5.1.7 or earlier:

```
Windows: %ProgramData%\Cisco\Cisco Secure Client\Umbrella\data
macOS: /opt/cisco/secureclient/umbrella/data
```

For Cisco Secure Client 5.1.8 or later:

```
Windows: %ProgramData%\Cisco\Cisco Secure
Client\Umbrella\data\regionaldata\<region_name>
macOS: /opt/cisco/secureclient/umbrella/data/regionaldata/<region_name>
```

> **Note**
>
> The region_name in the directory should match the region tag found in the **OrgInfo.json** file. If the region tag is missing, it is assumed to be “global”.

Umbrella Roaming Security Module Requirements

Describes Umbrella Roaming Security Module Requirements in Cisco Secure Access China. 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

Summarizes network requirements for the Roaming Security module and identifies the connectivity settings needed for its operation with Cisco Secure Client.

Secure Access and SAML Identity Provider Domains

Provides instructions for securing access and saml identity provider domains. When using an SSL-VPN, add the IP address of the VPN head-end to the external domains settings. For more information, see Manage Internet Security.

- 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 Internet Security.

Transport Layer Security Protocol

Describes the Transport Layer Security protocol requirements referenced by Secure Access network guidance and explains where administrators can find the related requirements.

- For more information, see Network Requirements for Secure Access: Transport Layer Security Protocol.

Network Access

Summarizes network access requirements for the Roaming Security module, including connectivity needed for Cisco Secure Client to reach internal domains.

Host Names

Describes 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.

- The Cisco Secure Client Umbrella Roaming Security module uses hostnames for registration. All machines must have a hostname that is unique within your organization.

HTTP and HTTPS

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

The Cisco Secure Client Umbrella Roaming Security module uses HTTP (80/TCP) and HTTPS (443/TCP) to communicate with Secure Access China 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 China
- 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 China.

Secure Access Client Certificate Revocation Services

Provides instructions for securing access client certificate revocation services. For more information, see Network Requirements for Secure Access: Client Certificate Revocation Services.

For more information, see Network Requirements for Secure Access: Client Certificate Revocation Services.

Roaming Security DNS Requirements

Describes roaming Security DNS Requirements. 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 only supports dual-stack IPv4/IPv6 for macOS and Windows. Standalone support for IPv6 for both macOs and Windows is not supported.

Internal Domains

Describes internal Domains. 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 China. The Cisco Secure Client's Umbrella module syncs with Secure Access periodically to check for new internal domains. This is a **critical** part of the setup process. We recommend that you populate the list of internal domains before you deploy the Umbrella (Roaming Security) module. For more information, see Domain Management.

Domain Management

Describes Domain Management in Cisco Secure Access China. Cisco Secure Access provides the option to manage domains when endpoints connect to internet resources with the Cisco Secure Client or a PAC file.

Cisco Secure Access provides the option to manage domains when endpoints connect to internet resources with the Cisco Secure Client or a PAC file. Domain management allows DNS queries for certain domains to query the local network's DNS servers.

If you do not specify a list of internal domains, all DNS queries are sent directly to Secure Access China, 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 China syncs newly added domains to Cisco Secure Clients within about one hour. For more information, see Manage Internet Security.

DNS Suffixes

Describes DNS Suffixes. 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 to Secure Access China.

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 China.

Operational Flow

Explains how Cisco Secure Client handles internal and external DNS queries as users connect to VPN or wireless networks. for administrators to review.

The Cisco Secure Client can handle internal and external DNS queries gracefully.

Configure Internal Domains

Explains how the Cisco Secure Client internal domains list is populated from Secure Access China internal domains and DNS suffixes configured on endpoints. The list supports access to internal resources on newly seen networks.

The Cisco Secure Client's internal domains list is populated by two sources:

- Syncs from the Secure Access China internal domains list.
- The DNS Suffixes list located in the local computer's networking configuration settings.

Cisco Secure Client and External Queries

Describes 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 China.

External DNS queries that do not match a domain located on either of the internal domains lists are sent straight to Secure Access China.

Cisco Secure Client and Internal Queries

Describes 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.

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.

Advanced Topics

Introduces advanced Cisco Secure Client topics and explains internal domains, query handling, and expected behavior on newly encountered networks. for administrators to review.

The following section focuses on more in-depth information and logic with internal domains and expected behavior.

Unencrypted

Describes unencrypted. Although the Cisco Secure Client is able to send encrypted DNS queries to Secure Access China ** when in the encrypted state**, domains listed on the bypass domains list are sent unencrypted, because they are not sent to Secure Access China.

Although the Cisco Secure Client is able to send encrypted DNS queries to Secure Access China ** when in the encrypted state**, domains listed on the bypass domains list are sent unencrypted, because they are not sent to Secure Access China.

DNS Suffixes (Continued)

Describes DNS Suffixes (Continued). There are implications that should be considered with DNS Suffixes. 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.

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 China. 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 China.
- If you use DNS suffixes to rely on internal domain resolution instead of populating the internal domains list in Secure Access China, 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 China internal domains list always sends unencrypted traffic on *all* networks.

> **Note**
>
> During the deployment of the Cisco Secure Client on user devices, you can disable the feature that adds the domains contained in the DNS suffixes list.

Interpret Internet Security Diagnostics

Describes Interpret Internet Security Diagnostics in Cisco Secure Access China. 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 web traffic.

When deployed on a user device, the Cisco Secure Client with the Umbrella (Roaming Security) module can generate detailed diagnostic reports about the device's 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.

Prerequisites

Lists the prerequisites for interpreting Cisco Secure Client diagnostics, including administrative privileges on the user device to access the diagnostic information.

- Administrative privileges on the user device.

Procedure

Provides instructions for interpreting diagnostics by generating the Cisco Secure Client diagnostic report on the user device and reviewing its output.

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. From the Cisco Secure Client menu, select Diagnostics and Reporting Tool , and then select Run.

1. From the Cisco Secure Client menu, select **Diagnostics and Reporting Tool**, and then select **Run**.
2. Send the generated **.zip** file to the support team.

Generate the Diagnostic Report on the Command Line

Provides instructions for generating the diagnostic report on the command line. Find the Cisco Secure Client Umbrella module diagnostic tool on your system and run the Cisco Secure Client's DART executable.

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 the support team.

Customize Windows Installation of Cisco Secure Client

Provides instructions for customizing windows Installation of Cisco Secure Client in Cisco Secure Access China. 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 Web security), and DART (diagnostics) modules. By default, the Cisco Secure Client deploys with the VPN module.

Requirements

Describes customize windows Cisco Secure Client. Windows 8.1 or newer. The 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

Prerequisites

Lists the prerequisites for customizing windows Cisco Secure Client. Download the OrgInfo.json file from Secure Access China. For more information, see Download the OrgInfo.json File.

- Download the **OrgInfo.json** file from Secure Access China. 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

Provides instructions for customizing windows Cisco Secure Client. You can deploy the Cisco Secure Client for Windows with several options including:.

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. 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.

1. 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`.

> **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. Run the Windows installer to deploy the Cisco Secure Client Umbrella Roaming Security module.

1. Run the Windows installer to deploy the Cisco Secure Client Umbrella Roaming Security module.

```
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

Describes (Optional) Deploy the Cisco Secure Client DART Module. Run the Windows installer to deploy the Cisco Secure Client DART (diagnostics and troubleshooting) package.

1. Run the Windows installer to deploy the Cisco Secure Client DART (diagnostics and troubleshooting) package.

```
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

Describes 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.

1. 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.

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. 1 - Do not add domains. 1 - Do not re-query. DNS search suffixes are sent to local resolvers, unless this functionality is disabled.

> **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.
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

Provides instructions for customizing macOS Installation of Cisco Secure Client in Cisco Secure Access China. 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 China 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 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 customize macOS Cisco Secure Client. 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

Prerequisites

Lists the prerequisites for customizing macOS Cisco Secure Client. Download the OrgInfo.json file from Secure Access China. For more information, see Download the OrgInfo.json File.

- Download the **OrgInfo.json** file from Secure Access China. 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

Provides instructions for customizing macOS Cisco Secure Client. Choose the modules to install with the Cisco Secure Client on a macOS device.

Choose the modules to install with the Cisco Secure Client on a macOS device.

Step 1 – Make the DMG Package Writeable

Describes 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.

1. Open a **Terminal** and set the DMG file to Read/Write.

```
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

Describes 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.

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

Describes how to copy OrgInfo.json to Cisco Secure Client Installation Directory.

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 China to **Volumes/Profiles**.

Step 4 – (Optional) Hide the VPN Module

Describes 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**.

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

Describes 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.

- To skip a module, define the module with `0`.
- To install a module, define the module with `1`.

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

Describes step 6 - Set Up the Correct Extension Permission Settings. Follow the payload guidance in Cisco Secure Client Extension Approval using MDM to deploy the System Extension settings.

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

Describes 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.

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 /
```

46 Manage Virtual Private Networks on Cisco Secure Client

Topics:

- Manage Virtual Private Networks on Cisco Secure Client

Provides an overview of Manage Virtual Private Networks on Cisco Secure Client in Cisco Secure Access China, including Download the Virtual Private Network XML Profile and CA Certificates for VPN Connections. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Virtual Private Networks on Cisco Secure Client

Provides instructions for managing virtual Private Networks on Cisco Secure Client in Cisco Secure Access China. 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 China. 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.

Download the Virtual Private Network XML Profile

Provides instructions for downloading the Virtual Private Network XML Profile in Cisco Secure Access China. The Cisco Secure Client supports the use of various profiles to configure the deployment of the client modules.

The Cisco Secure Client supports the use of various profiles to configure the deployment of the client modules. A Cisco Secure Client module may require a certain profile present to install the module successfully.

The Cisco Secure Client virtual private network (VPN) module requires the VPN XML profile. Cisco Secure Client installs with the VPN module. You can download the Cisco Secure Client VPN profile from Secure Access China. For more information, see Download the Cisco Secure Client VPN Profile.

The Cisco Secure Client VPN profile configures the VPN module on the user device and connects clients securely to resources protected by Secure Access China.

Prerequisites

Lists the prerequisites for downloading Cisco Secure Client VPN profile. Full Admin user role. For more information, see Manage Accounts.

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

Procedure

Provides instructions for downloading Cisco Secure Client VPN profile. Download the Cisco Secure Client VPN profile to the user device.

Download the Cisco Secure Client VPN profile to the user device.

Step 1 – Download the Cisco Secure Client VPN Profile

Describes step 1 – Download the Cisco Secure Client VPN Profile. The Cisco Secure Client VPN profile describes the connection and security metadata for the VPN module.

The Cisco Secure Client VPN profile describes the connection and security metadata for the VPN module.

1. Navigate to **Connect > End User Connectivity > Virtual Private Network**.
2. For a VPN profile, click **Download XML** to save the Cisco Secure Client VPN profile to the local system.

Step 2 – Copy the VPN Profile to the Target Directory

Describes step 2 – Copy the VPN Profile to the Target Directory. Copy the Cisco Secure Client VPN XML file to the Cisco Secure Client VPN profile directory on the user devices.

Copy the Cisco Secure Client VPN XML file to the Cisco Secure Client VPN profile directory on the user devices.

OS	Location	File	Description
Windows	**%Program Data%\Cisco\Cisco Secure Client\VPN\Profile**	AnyConnect VPN Profile	
macOS	**/opt/cisco/secureclient/vpn/profile**	AnyConnect VPN Profile	

CA Certificates for VPN Connections

Describes CA Certificates for VPN Connections in Cisco Secure Access China. To authenticate users and devices when connected over a virtual private network (VPN), Secure Access China 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 China must have the root certificate authority (CA) certificate for the user devices.

Set up the trust between Secure Access China 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 China. For more information, see VPN Certificates for User and Device Authentication.

Prerequisites

Lists the prerequisites for managing virtual private network on Cisco Secure Client. For more information about the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

- 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.

Part III

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
- Data Loss Prevention Report
- Admin Audit Log Report

Describes Reports in Cisco Secure Access China. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

47 Monitor Secure Access with Reports

Topics:

- Monitor Secure Access China with Reports

Provides an overview of Monitor Secure Access with Reports, including Export Report Data to CSV, Bookmark and Share Reports, and Report Retention. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Monitor Secure Access China with Reports

Provides instructions for monitoring secure Access China with Reports. Use Cisco Secure Access China reports to monitor your Secure Access China deployment and to better understand your Secure Access China usage.

Use Cisco Secure Access China reports to monitor your Secure Access China deployment and to better understand your Secure Access China 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.

Export Report Data to CSV

Provides instructions for exporting report Data to CSV in Cisco Secure Access China. 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

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.

Prerequisites

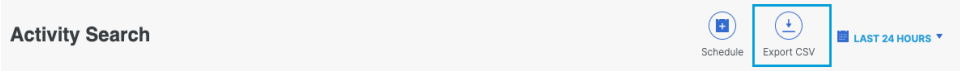
Lists the prerequisites for exporting report data to CSV. A minimum user role of Read-only. For more information, see Manage Accounts.

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

Procedure

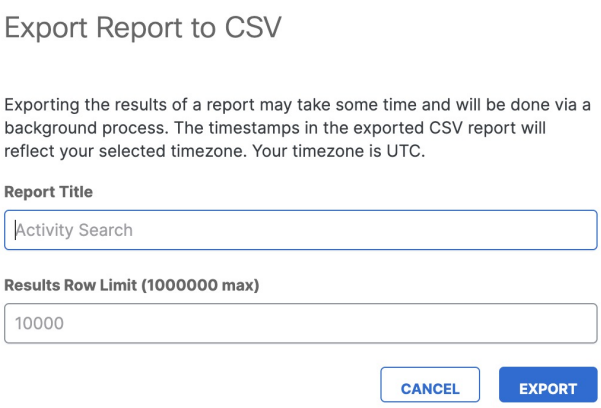
Provides instructions for exporting report data to CSV. Give your report a good Report Title , add the number of rows of data to be returned, and click Export.

1. Navigate to **Reporting > <*report*>** and click **Export CSV** (or, in the case of the Data Loss Prevention, **Download**).

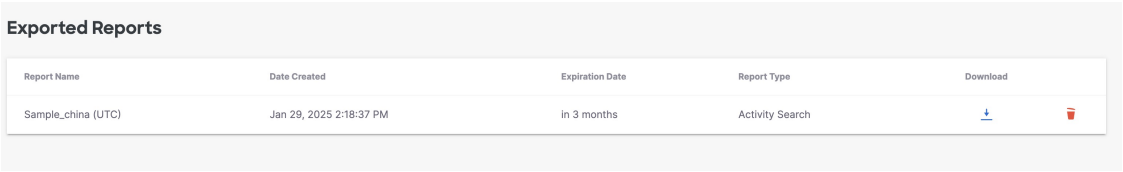


2. Give your report a good **Report Title**, add the number of rows of data to be returned, and click **Export**.

> **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 in Cisco Secure Access China. Secure Access China 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 China stores the report state in the URL, making it easy to share a report with colleagues or bookmark a report for future use.

Prerequisites

Lists the prerequisites for bookmark and share reports. A minimum user role of Read-only. For more information, see Manage Accounts.

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

Procedure

Provides instructions for bookmark and share reports.

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, 2025), the absolute filter is applied.

Report Retention

Describes Report Retention in Cisco Secure Access China. The reporting of information begins as soon as you start sending traffic to Secure Access China.

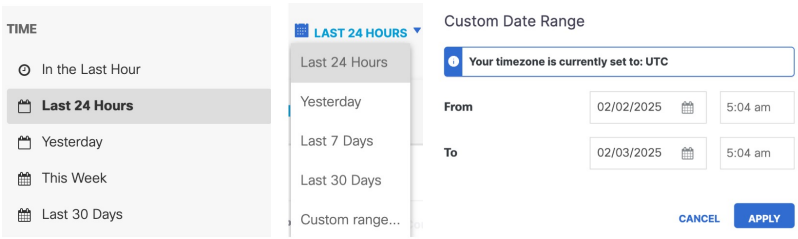
The reporting of information begins as soon as you start sending traffic to Secure Access China.

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 China 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 Ausdit 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 Ausdit Log Report.

Schedule a Report

Describes Schedule a Report in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for scheduling a report, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

Procedure

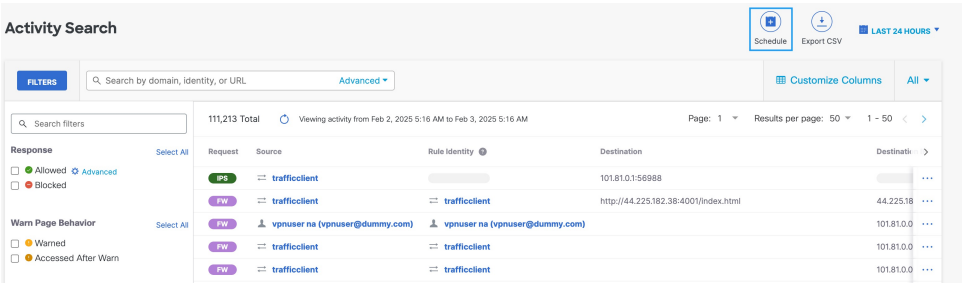
Provides instructions for scheduling a report. Navigate to Reporting and select the report you want to schedule. For a list of schedulable reports, see Report Scheduling . (Screenshots in these instructions use the Top Identities report as an illustrative example.).

1. Navigate to **Reporting** and select the report you want to schedule.

   For a list of schedulable reports, see Report Scheduling. (Screenshots in these instructions use the Top Identities report as an illustrative example.)

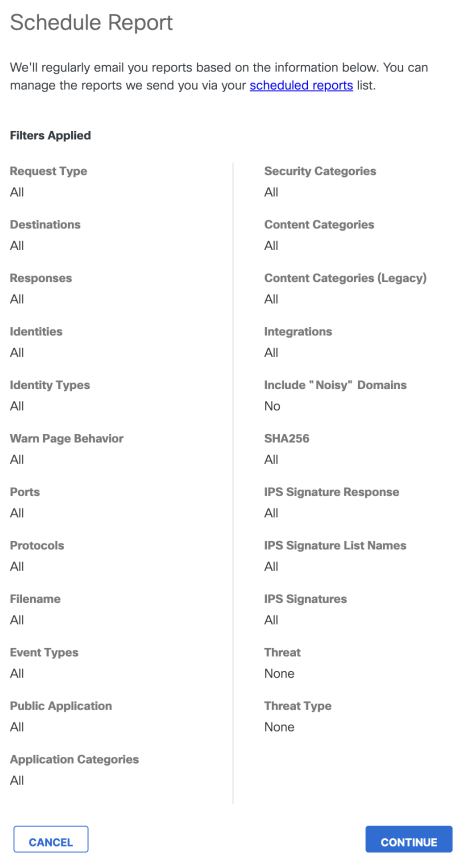
2. Select filters for the report and then click **Schedule**.

   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**.

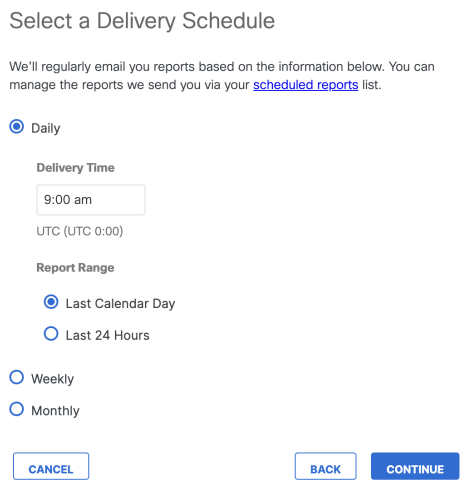


4. Select time parameters to set when and how often you want this report sent to recipients. Click **Continue**.

   For each time period, you can specify a time and range within that time period.

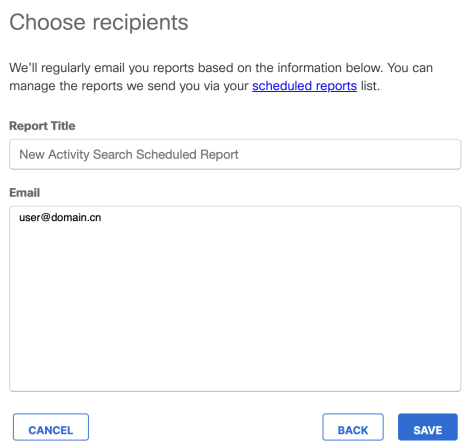
   The time of delivery defaults to the logged-in user's Umbrella's timezone, but if recipients are in different time zones, you can configure them to receive reports during their work hours. If the recipient is an administrator or helpdesk staff expected to take action on information in the report, we recommend setting up a second report with the delivery time adjusted for the recipient's region.

> **Note**
>
> Attempting to schedule a report for a time on the current day, regardless of whether the report is scheduled in the future from the current time on that same day, results in the report being scheduled on the next day at the earliest for weekly and monthly frequencies.



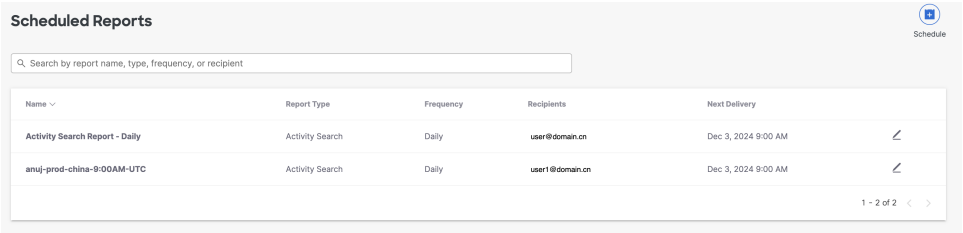
5. Give your report a good descriptive name, add email addresses for recipients of this report, and click **Save**.

   Enter as many recipients as you like separating addresses with commas or semicolons.



6. Your newly scheduled report is listed at **Monitor > Management > Scheduled Reports**.

   You can update this schedule at any time. For more information, see Update a Scheduled Report.



Check Your Spam Folder

Provides instructions for checking your spam folder. Secure Access China uses SendCloud 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 China uses SendCloud 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.

Update a Scheduled Report

Provides instructions for updating a Scheduled Report in Cisco Secure Access China. You can update your scheduled reports at any time.

You can update your scheduled reports at any time. When you update filters for the scheduled report, the Scheduling wizard takes you to the report in question, where you can select filters as necessary and then save the updated schedule.

Prerequisites

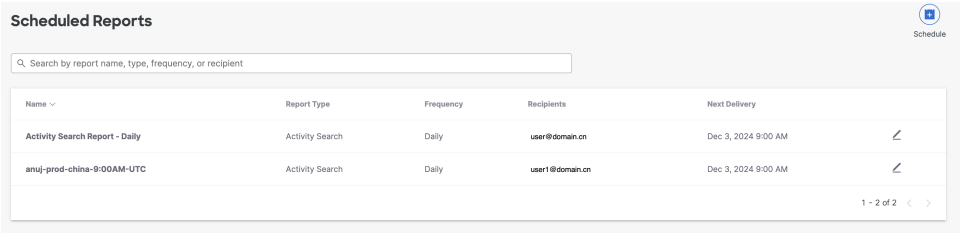
Lists the prerequisites for updating a scheduled report, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

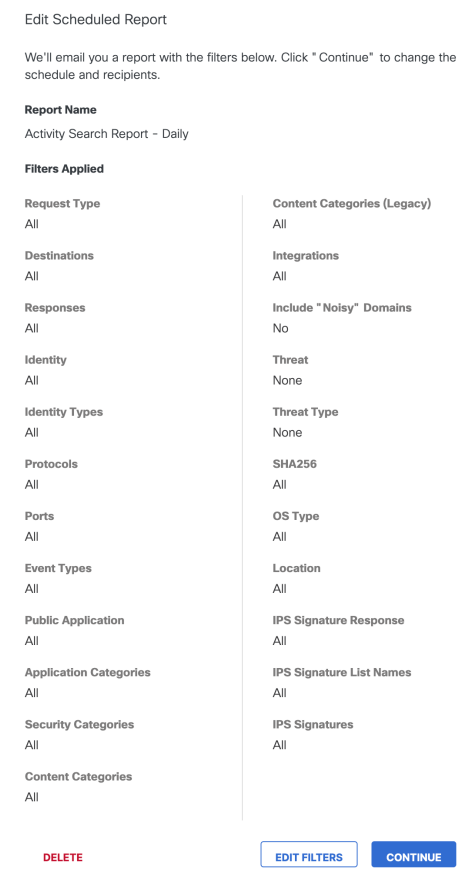
Procedure

Provides instructions for updating a scheduled report. The Edit Scheduled Report modal opens and lists filters applied to the report.

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.

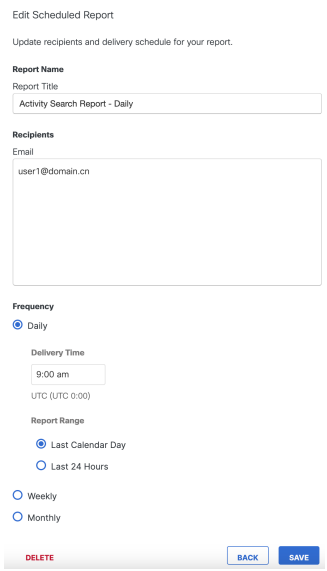
3. Select and apply filters for this report and click **Save**.

   The Scheduling wizard reopens listing updated filter selections.



You are now editing filters for the "Activity Search Report - Daily" report.
Choose "Save" after you've finished modifying filters or "Cancel" to discard changes. Modifications to this report will appear the next time it is sent.
CANCEL
SAVE

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 Scheduling

Describes Report Scheduling in Cisco Secure Access China. Various reports in Secure Access China can be configured so that Secure Access China regularly emails you a summary of that report.

Various reports in Secure Access China can be configured so that Secure Access China 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 China and the report. See Schedule a Report.

Reports can be scheduled so that you receive an email daily, weekly, or monthly.

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 Desinations–A list of the top traffic-generating identities over the selected time period. Filterable by identity and destination.
- Top Categories–A list of the top content categories for your organization over the selected time period. Filterable by identity and response.
- Data Loss Prevention – Lists data violations detected through the DLP Real Time rules.

Important

Cisco Secure Access China 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 China sends its reports from scheduled-reports-feedback@ciscosecureaccess.cn.

Available Reports

Describes available Reports. – Lists users that have remotely connected to Secure Access China and requested access to destinations. Remote Access Logs.

- **Remote Access Logs** – Lists users that have remotely connected to Secure Access China 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.
- **Admin Audit Log** –Lists a record of any configuration changes made to your settings by any of your Secure Access China administrators.

48 Remote Access Log Report

Topics:

- Remote Access Log Report

Provides an overview of Remote Access Log Report in Cisco Secure Access China, including View the Remote Access Log Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Remote Access Log Report

Describes Remote Access Log Report in Cisco Secure Access China. The Remote Access Log report lists users that have remotely connected to Secure Access China and requested access to destinations.

The Remote Access Log report lists users that have remotely connected to Secure Access China and requested access to destinations. Some relevant fields to aid debugging and trouble-shooting remote access 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.

Refine your search using filters to help identify security issues that require attention.

View the Remote Access Log Report

Provides instructions for viewing the Remote Access Log Report in Cisco Secure Access China. The Remote Access Log report lists users' connection events that are related to remote access, tracked over distinct time periods.

The Remote Access Log report lists users' connection events that are related to remote access, tracked over distinct time periods.

Prerequisites

Lists the prerequisites for viewing the remote access log report. A minimum user role of Read-only. For more information, see Manage Accounts.

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

View the Remote Access Log Report

Provides instructions for viewing the remote access log report. Connection Event lets you filter by the outcome of a VPN connection event. Possible values are: Connected, Disconnected, Failed, Warning, and Unknown.

1. Navigate to **Monitor > Reports > Remote Access Logs**.
2. Choose a time frame of remote access events.
3. Use the search bar to find remote access events by identity (user or device name) or endpoint device OS version.
4. Refine your search using the following filters to help identify security issues that require attention.
    - **Connection Event** lets you filter by the outcome of a VPN connection event. Possible values are: Connected, Disconnected, Failed, Warning, and Unknown.

      > **Note**
      >
      > A Warning outcome only results when a DDNS update has failed (see **Event Details** below).

    - **Machine Tunnel** lets you filter by VPN connections made by a machine tunnel. For more information about the Secure Access China machine tunnel, see Manage Machine Tunnels.
    - **OS Types and Versions** lets you filter by any client OS values that are in the current Remote Access Log data set.

- **Secure Client Versions** lets you filter by any Cisco Secure Client values that are in the current Remote Access Log data set.
- **Event Details** lets you filter by the combination of any reasons for connection failure or disconnection that are in the current Remote Access Log data set. Possible values:
  - Addr Assignment Fail
  - Access Allowed
  - Administrator Reset
  - Authentication Check
  - Authorization Check
  - Cert Auth Check
  - Certificate Expired
  - Client Type Not Supported
  - Connection Lost
  - Connection Preempted
  - DDNS Update Failed
  - Geocompliance Check
  - Geocompliance Service Unavailable
  - IKE Delete
  - IKEV2 Check
  - IPSec Error
  - Max Time Exceeded
  - Port Error
  - Posture Check
  - Posture Check Failed
  - SA Expired
  - Static IP Addr Assignment Fail
  - TLS Check
  - Unknown Disconnection Reason
  - Unknown Failed Reason
  - User Requested
- **Identities** lets you filter by connection events with Security Group Tags (SGT) you have configured rules to traffic originating from IP addresses in network segments that include SGTs. When present, SGTs will be appended to the **User** column value.

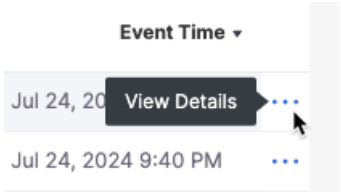
> **Note**
>
> Each filter is dynamic, except for **Identities**, and will only display filter option values that are present in the connection data. If no option values are present in the data for a filter, that filter will remain hidden.

View Event Details

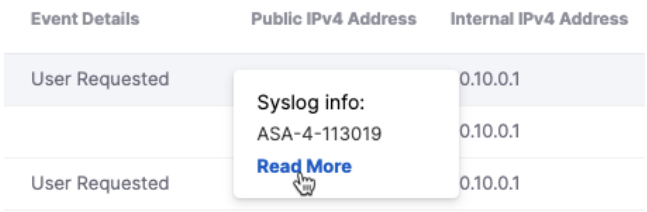
Provides instructions for viewing event details. There are two options to view details of an event. Option 1 : Click the View Details icon (the blue ellipsis at the right end of each row).

There are two options to view details of an event.

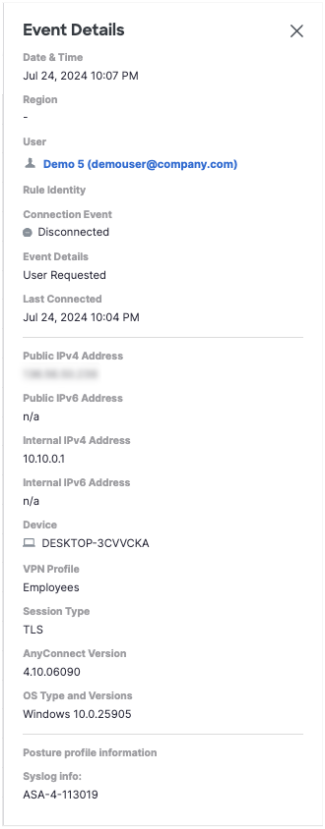
1. **Option 1**: Click the **View Details** icon (the blue ellipsis at the right end of each row).



2. **Option 2:** Hover over an **Event Details** field in any row, then click **Read More** below the ASA syslog message ID.



Result: The **Event Details** drawer displays detailed information about an individual event.


Event Details
Date & Time
Jul 24, 2024 10:07 PM
Region
-
User
Demo 5 (demouser@company.com)
Rule Identity
Connection Event
Disconnected
Event Details
User Requested
Last Connected
Jul 24, 2024 10:04 PM
Public IPv4 Address
Public IPv6 Address
n/a
Internal IPv4 Address
10.10.0.1
Internal IPv6 Address
n/a
Device
DESKTOP-3CVVCKA
VPN Profile
Employees
Session Type
TLS
AnyConnect Version
4.10.06090
OS Type and Versions
Windows 10.0.25905
Posture profile information
Syslog info:
ASA-4-113019

49 Activity Search Report

Topics:

- Activity Search Report

Provides an overview of Activity Search Report in Cisco Secure Access China, including View the Activity Search Report, View Activity Search Report Actions, and Schedule an Activity Search Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Activity Search Report

Describes Activity Search Report in Cisco Secure Access China. Find the result of every URL and IP request from your various sources in descending date and time.

Find the result of every URL and IP 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 China 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 in Cisco Secure Access China. This topic explains the functions of the Activity Search report and where to find the report in Secure Access China.

This topic explains the functions of the Activity Search report and where to find the report in Secure Access China.

Prerequisites

Lists the prerequisites for viewing the activity search report. A minimum user role of Read-only. For more information, see Manage Accounts.

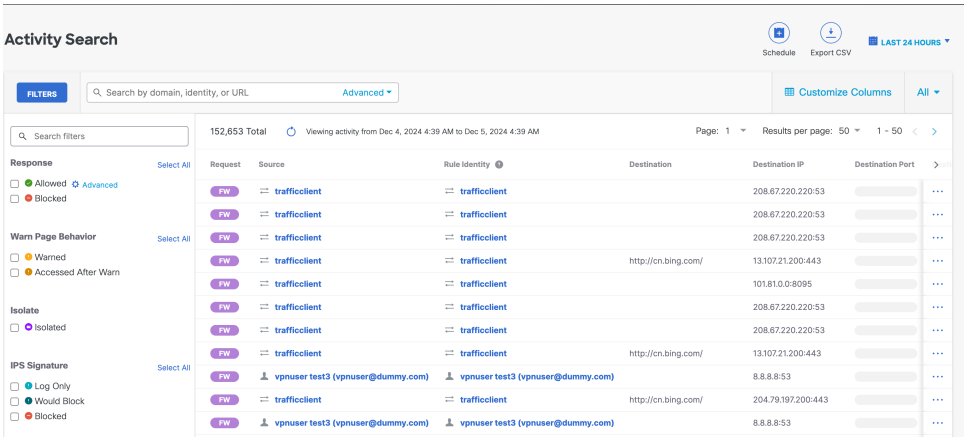
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

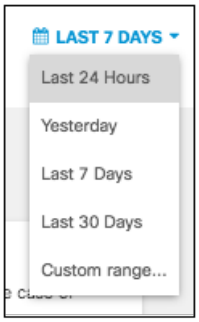
Provides instructions for viewing the activity search report 1. Navigate to Monitor > Reports > Activity Search. Choose a time frame to view the report. You can view the results for the last 24 hours (default), Yesterday, Last 7 Days, Last 30 Days, or a Custom range.

1. Navigate to **Monitor > Reports > Activity Search**.

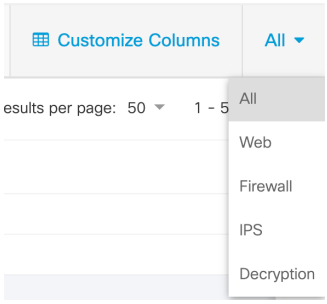
   This takes you to the default view of the Activity Search report, which lists all of your identities and the internet requests or traffic events for your organization, tracked over time. The default is 24 hours.



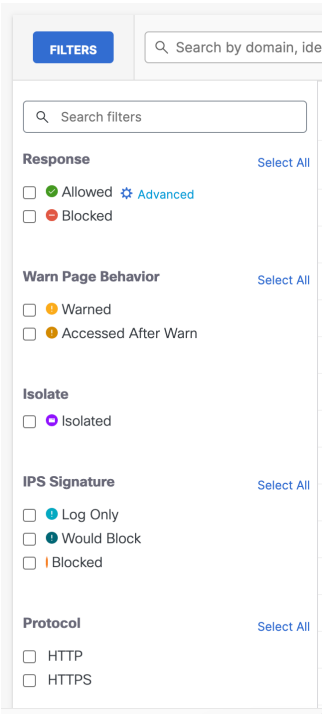
2. Choose a time frame to view the report. You can view the results for the last 24 hours (default), Yesterday, Last 7 Days, Last 30 Days, or a Custom range.



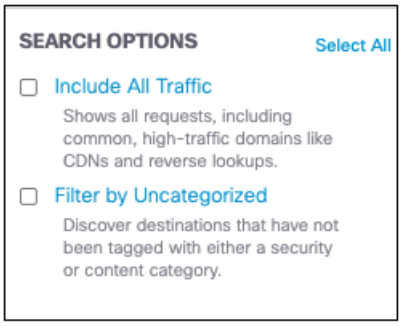
3. From the **Requests** menu, choose a request type or the default of **All**. Filters update to those that are relevant to the type of request chosen.



4. Select available filters based on the request type.



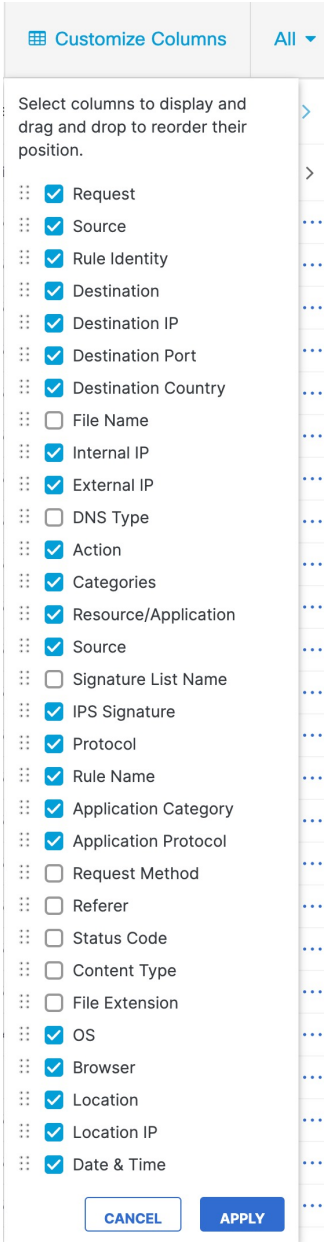
5. Optionally, select a **Search Options** filter:
   - **Include All Traffic**–Includes data from all domains including noisy domains that are filtered out by default.
   - **Filter by Uncategorized**–Includes destinations that are not classified under a specific security or content category.



Configure Columns to Display

Provides instructions for configuring columns to display. The identity of the source that Secure Access China used to determine which rule applied to the request. Applicable to Web and Firewall requests.

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 Web, Firewall, IPS, 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 China used to determine which rule applied to the request. Applicable to Web and Firewall 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.

Column name	Column description
Destination	The destination of the request. Applicable to Web, Firewall, and IPS 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.
Destination Country	The two-character country identifier. Applicable to 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 Web request.
External IP	The external IPv4 or IPv6 address of the request. Supports both compressed and long-form IPv6 address formats. Applicable to Web request.
Action	The request is either Blocked or Allowed. Applicable to Web, Firewall, and IPS requests. **Note:** Certificate and TLS error events display as **Blocked – Certificate Error**. These errors will only be displayed where the request is processed by a ruleset that has 'HTTPS inspection' and 'File Analysis' enabled.
Categories	Content and Security categories flagged with the activity. Applicable to Web and Firewall requests. Click **Dispute Categorization** in the Event Details navigation drawer to suggest a different category for a Source.
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 Web and Firewall requests. For more information, see 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, see 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, see Manage IPS Profiles.
Protocol	Displays whether the Web request protocol is HTTP or HTTPS, and whether the Firewall, IPS, or Decryption request

Column name	Column description
	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 Web, Firewall, and IPS requests. Click the rule name to view your Access Policy where the rule is configured. For more information, see 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, see View Activity Search Report Actions.
Application Category	If an application is involved with the activity, this column contains the categories associated with the application. Applicable to Web, and Firewall requests. For the full list of application categories, see Application Categories.
Application Protocol	If an application is involved with the activity, this column contains the protocol for the application (HTTP, SSL, RTP, 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.
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 Actions

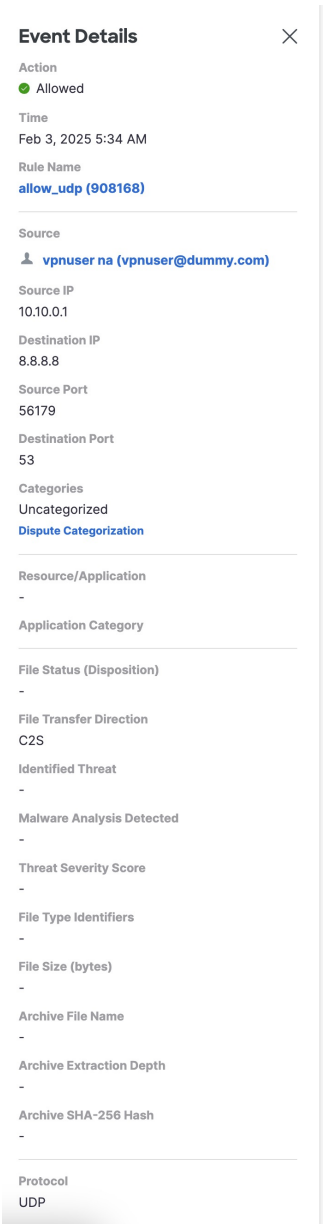
Provides instructions for viewing actions. To learn more about the results of your activity search, click the View Actions icon (the blue ellipsis at the right of each item in the search results) for a result and choose an item from the menu.

To learn more about the results of your activity search, click the **View Actions** icon (the blue ellipsis at the right of each item in the search results) for a result and choose an item from the menu.

View Full Details

Provides instructions for viewing full details. With View Actions, you can view the full details of each activity result:. The detail fields available depend on the type of event.

With View Actions, you can view the full details of each activity result:



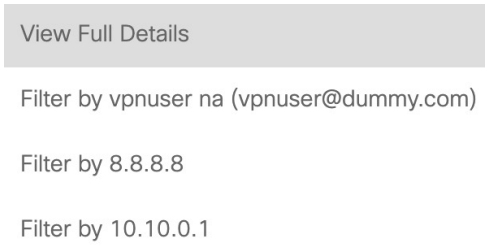
The detail fields available depend on the type of event.

Filter Views

Provides instructions for filtering views. Where applicable, the viewing of results can be filtered by the following:. Filter by Application.

Where applicable, the viewing of results can be filtered by the following:

- Filter by Application
- Filter by Destination
- Filter by URL
- Filter by Identity
- Filter by External IP

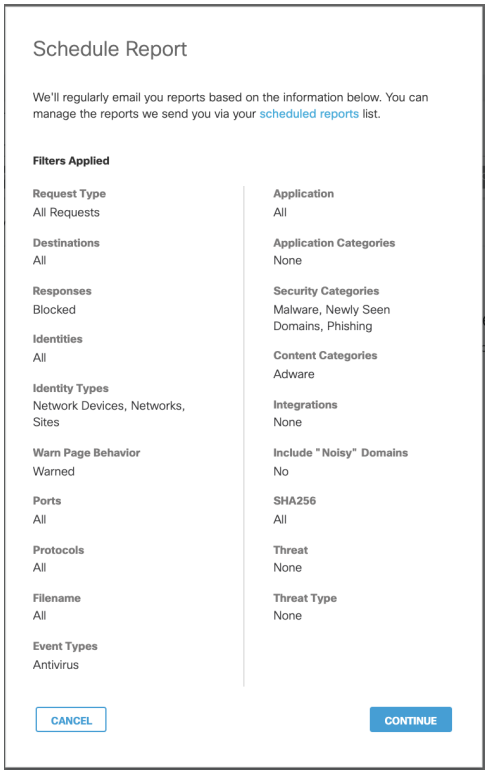


Schedule an Activity Search Report

Provides instructions for scheduling an activity search report. When scheduling a new report for Activity Search, any current filters selected apply.

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.



View Activity Search Report Actions

Provides instructions for viewing activity Search Report Actions in Cisco Secure Access China. 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.

Prerequisites

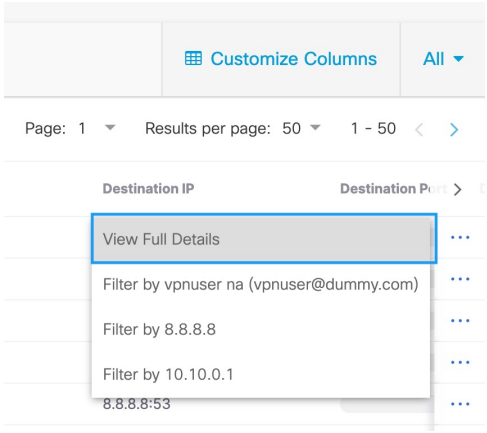
Lists the prerequisites for viewing actions, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

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

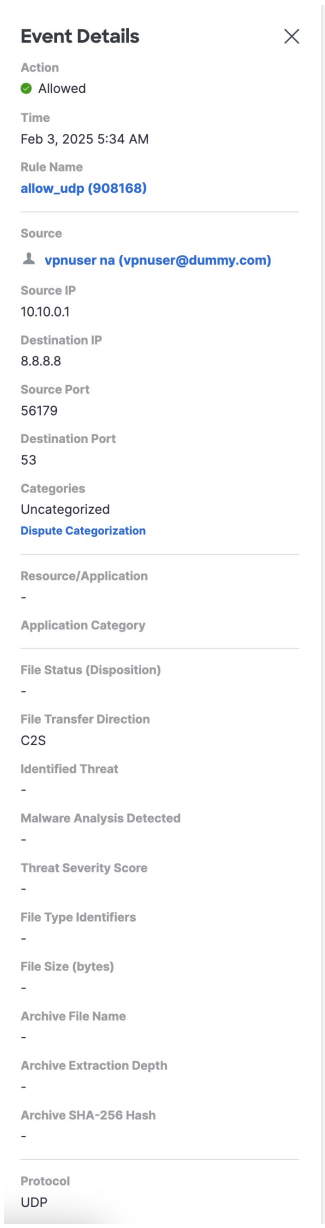
See Full Details

Describes see Full Details. The details of each activity result are displayed. The details listed depend on the event type.

1. 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.

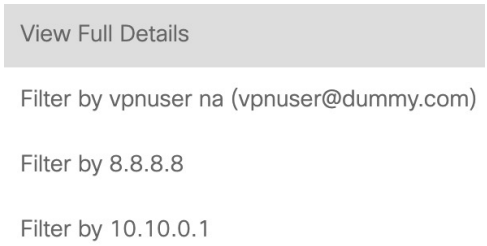


Filter Views

Describes filters for narrowing report results by application, destination, URL, source, external IP, and other available fields when applicable. for administrators to review.

Where applicable, certain results can be filtered by the following:

- Application
- Destination
- URL
- Source
- External IP

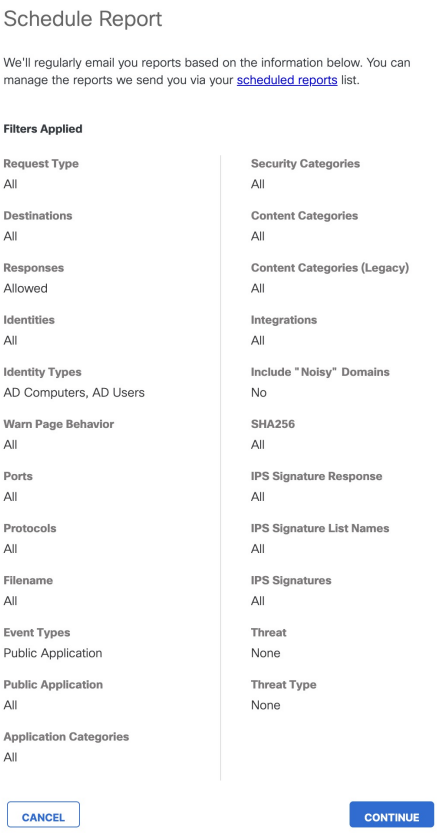


Schedule an Activity Search Report

Describes Schedule an Activity Search Report in Cisco Secure Access China. You can schedule a report to be emailed to you at regular intervals.

You can schedule a report to be emailed to you at regular intervals. Your emailed report is a table showing an HTML version of the report and an attached CSV file containing the entire data set. Also included in your email is a link to a live version of the same report. For more about scheduled reports, see Schedule a Report.

When scheduling a new report for Activity Search, any current filters selected apply.



Use Search and Advanced Search

Describes Use Search and Advanced Search in Cisco Secure Access China. 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.

Note

Packages and Feature Availability

Not all of the features described here are available to all Secure Access China 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.

Prerequisites

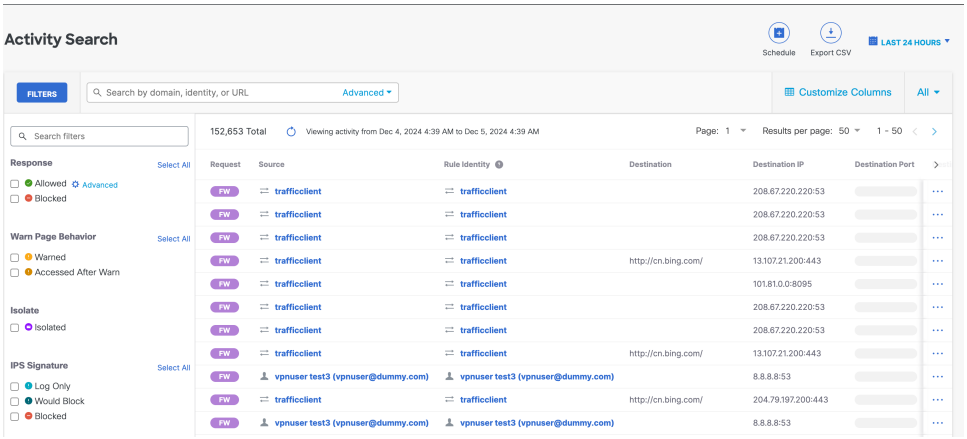
Lists the prerequisites for advanced search, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

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

Search

Provides instructions for searching. 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.

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

Explains how wildcard characters match multiple values in Advanced Search, including searches across domains, URLs, and file names such as *.gif.

Domains

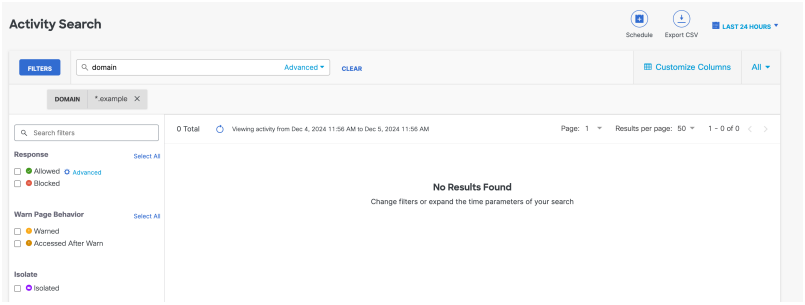
Describes domains. Domains can be searched in the search bar or advanced search with the wildcard * to include or exclude subdomains.

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.

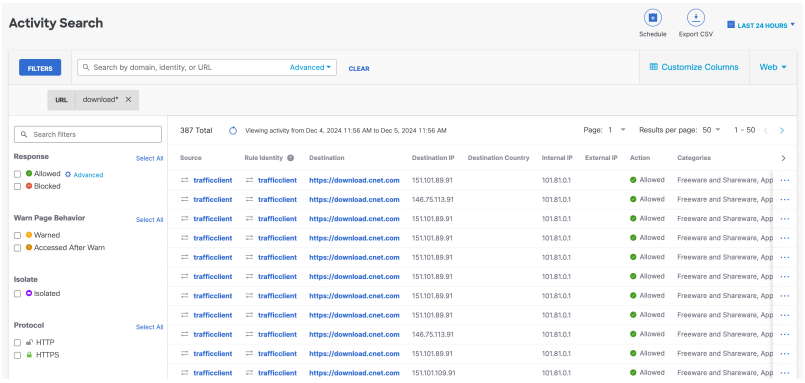


URLs

Describes URLs. The wildcard * can be used in any part of the URL path to search for URLs containing certain terms.

The wildcard * can be used in any part of the URL path to search for URLs containing certain terms.

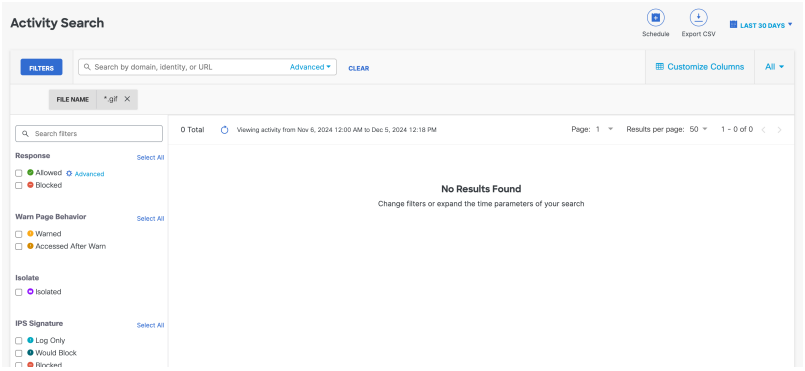
For example, `download*` will search for URLs containing "download".



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.

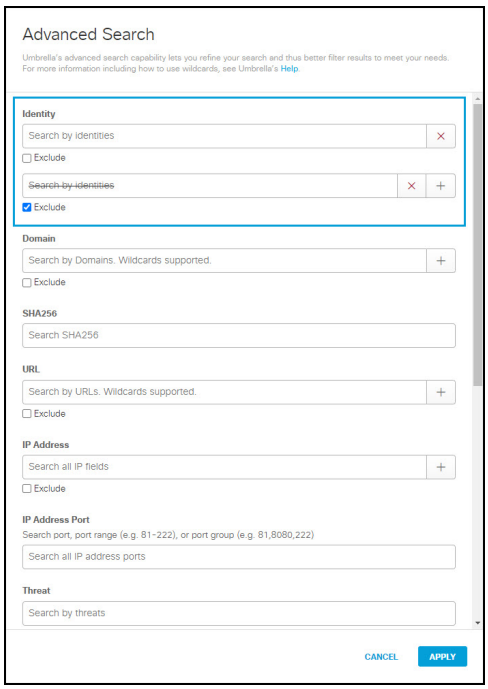
File names can use the wildcard * to search for file types, in Advanced Search only. For example, `*.gif` will search for all files that are .gifs.



Advanced Search

Describes advanced Search. In the search bar, click Advanced. The Advanced Search window opens. Add search parameters and click Apply.

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 sources from your search. Secure Access China opens a menu listing sources as soon as you begin typing.
   - **Domain**–You can search for more than one domain at a time. 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**–Search by specific URL path.
   - **IP Address**–Search for events associated with IP addresses on your network (either internal or public egress IP address). This does not provide the capability to search for destination IP addresses.
   - **IP Address Port**–Search by a firewall port number.
   - **Threat**–Search by threats.
   - **Threat Type**–Search by threat type. For more information, see Threat Category Descriptions.
   - **Public Application**–Search by public application.
   - **Application Group**–Search by application group.
   - **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.
   - **IPS Signatures**–Search by IPS signatures. For more information, see Manage IPS.
   - **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 IP addresses: shared or reserved.
   - **Egress Data Center** – Search by the egress data center location from which activity originated.

50 Security Activity Report

Topics:

- Security Activity Report

Provides an overview of Security Activity Report in Cisco Secure Access China, including View Activity and Details by Filters, View Activity and Details by Event Type or Security Category, and View an Event's Details. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Security Activity Report

Describes Security Activity Report in Cisco Secure Access China. The Security Activity report highlights security events generated by your organization's sources visiting destinations flagged–but not necessarily blocked–by Secure Access China 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 China 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

Provides instructions for viewing activity and Details by Filters in Cisco Secure Access China. The Security Activity report gives you the ability to monitor and discover threats to your organization by displaying traffic patterns.

The Security Activity report gives you the ability to monitor and discover threats to your organization by displaying traffic patterns. You can filter these results by event type, category, time period, and type of request.

> **Note**
>
> Secure Access China 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.

Prerequisites

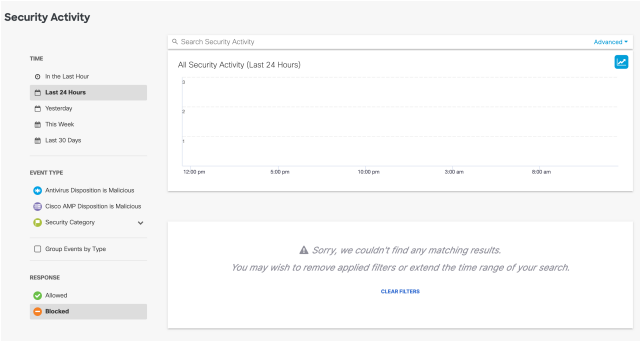
Lists the prerequisites for viewing activity and details by filters. A minimum user role of Read-only. For more information, see Manage Accounts.

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

Procedure

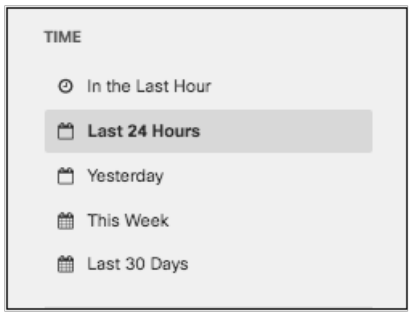
Provides instructions for viewing activity and details by filters. For Response, select Allowed , Blocked , or both. Navigate to Monitor > Reports > Security Activity.

1. Navigate to **Monitor > Reports > Security Activity**.

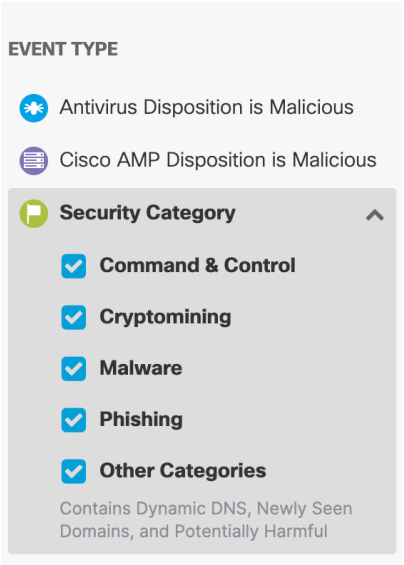


2. Choose a time period of events to view. You can generate a report to document activities for the last hour, the last 24 hours, the previous calendar day (yesterday), the last seven days, and the last month.

Figure 5: sec act time.png



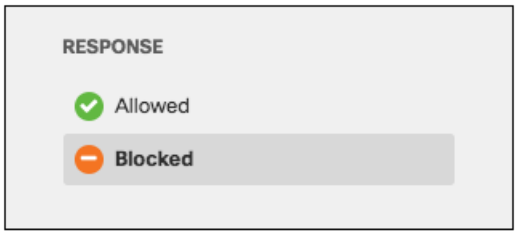
3. Choose which security event types or categories you want to view in the report. By default, all events and categories are selected to display activity for all event types.
   - **Antivirus Disposition is Malicious**–Lists events that have been filtered through a virus scan.
   - **Cisco AMP Disposition is Malicious**–Lists events that have been filtered through Cisco Advanced Malware Protection (AMP).
   - **Security Category**–Lists events allowed or blocked against selected security categories: Command and Control, Cryptomining, Malware, Phishing, and Other Categories (Contains Dynamic DNS, Newly Seen Domains, and Potentially Harmful).



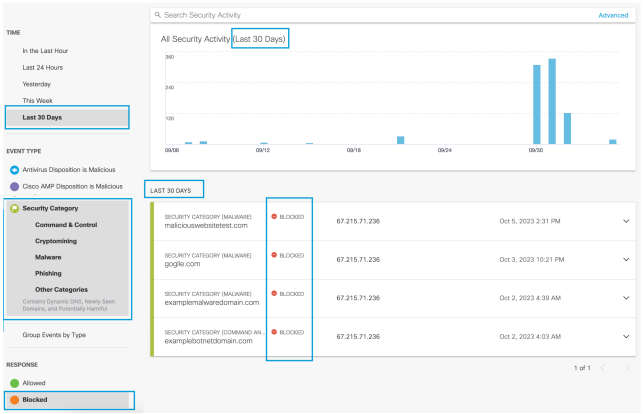
4. For **Response,** select **Allowed**, **Blocked**, or both.

> **Note**
>
> If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response > Allowed**. Secure Access China cannot allow viruses to pass through the system. These will always be blocked.

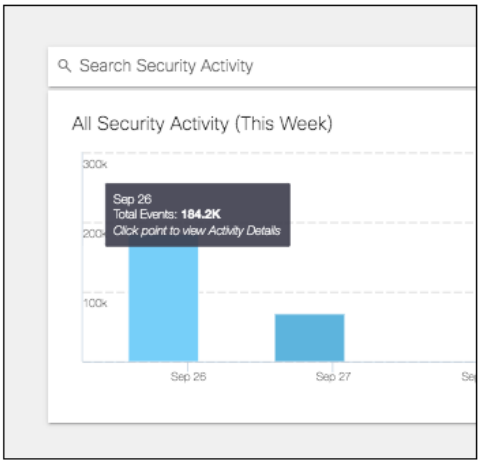
Figure 6: sec act response filter.png



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

Provides instructions for viewing activity and Details by Event Type or Security Category in Cisco Secure Access China, including Prerequisites, Procedure, and Group Security Categories. It explains the sequence of actions and relevant settings presented in the procedure.

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.

Prerequisites

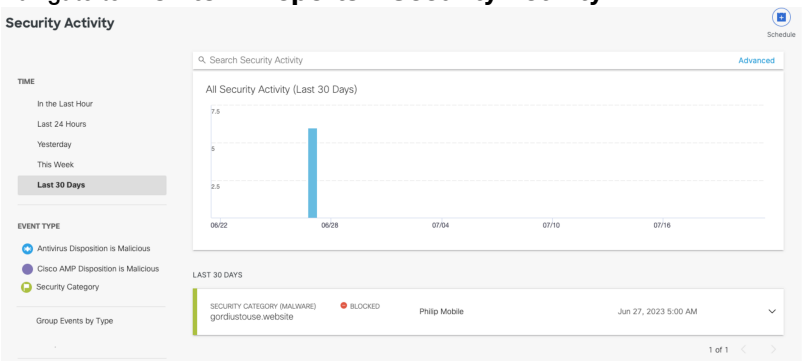
Lists the prerequisites for viewing activity and details by event type or security category. A minimum user role of Read-only. For more information, see Manage Accounts.

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

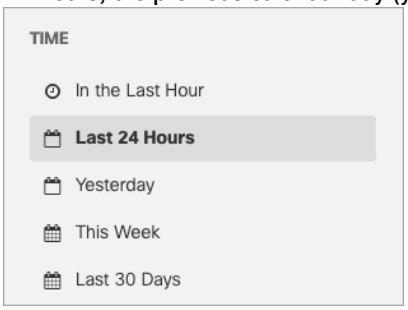
Procedure

Provides instructions for viewing activity and details by event type or security category. For Response, select Allowed , Blocked , or both.

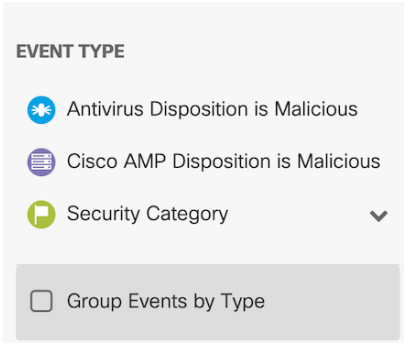
1. Navigate to **Monitor > Reports > Security Activity**.



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.

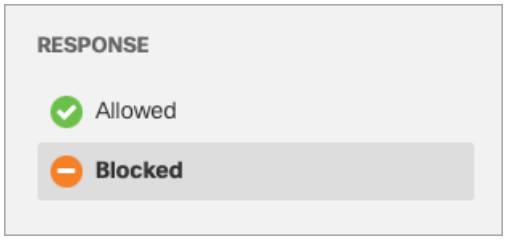


3. Select which security event types or categories you want to view in the report. By default, all events and categories are selected to display activity for all event types.

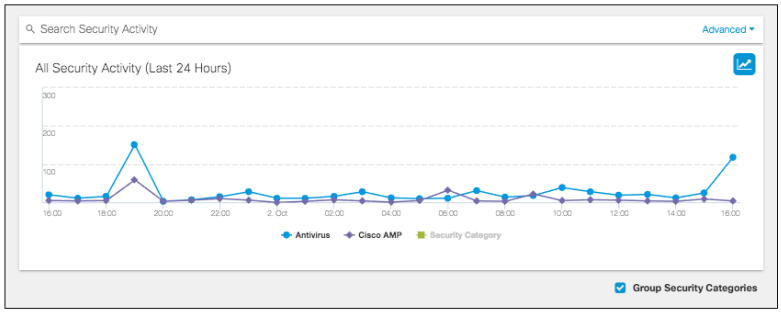


4. For **Response,** select **Allowed**, **Blocked**, or both.

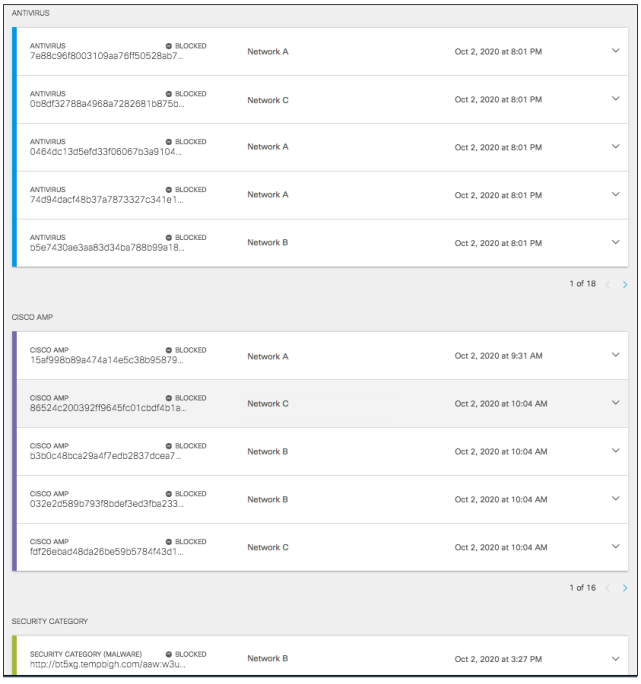
> **Note**
>
> If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response > Allowed**. Secure Access China cannot allow viruses to pass through the system. These will always be blocked.



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.



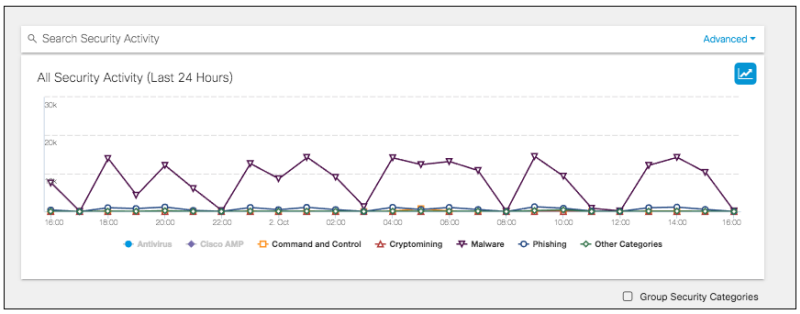
Grouping security categories also reorganizes the events' details cards by event type. By viewing event details by event type or category, you can see which categories were more active and perhaps causing more risk to the environment.



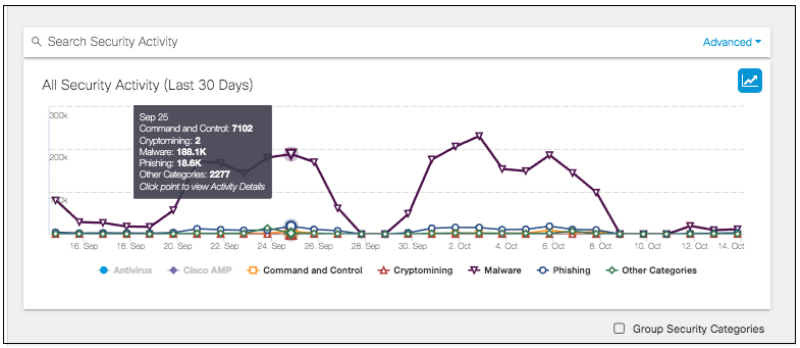
Group Security Categories

Describes group Security Categories. 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.

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

Provides instructions for viewing an Event's Details in Cisco Secure Access China. 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).

Prerequisites

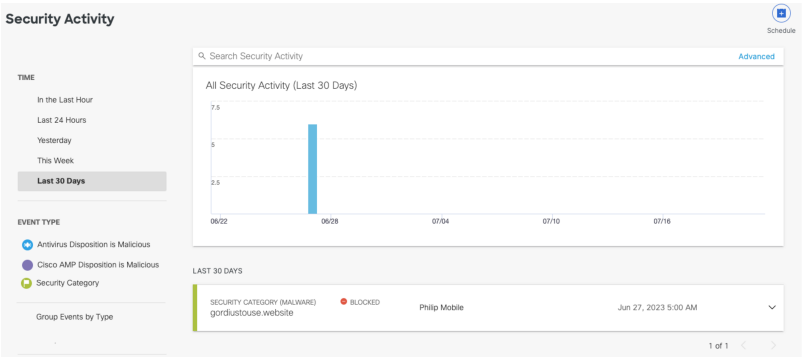
Lists the prerequisites for viewing an events details. A minimum user role of Read-only. For more information, see Manage Accounts.

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

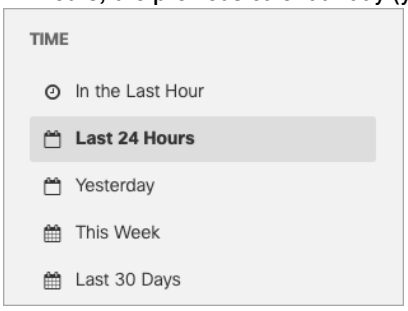
Procedure

Provides instructions for viewing an events details. For Response, select Allowed , Blocked , or both. The list of events' details is stacked as cards and sorted by event type (if Group Security Categories is enabled).

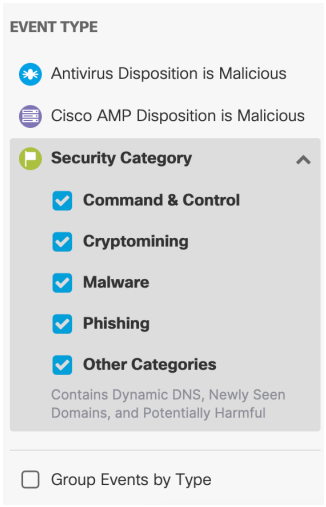
1. Navigate to **Monitor > Reports > Security Activity**.



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.

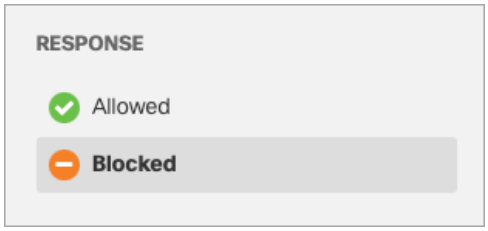


3. Select which security event types or categories you want to view in the report. By default, all events and categories are selected to display activity for all event types.

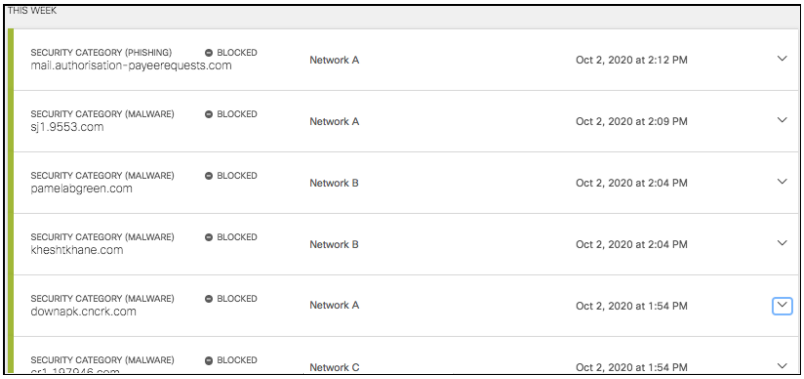


4. For **Response,** select **Allowed**, **Blocked**, or both.

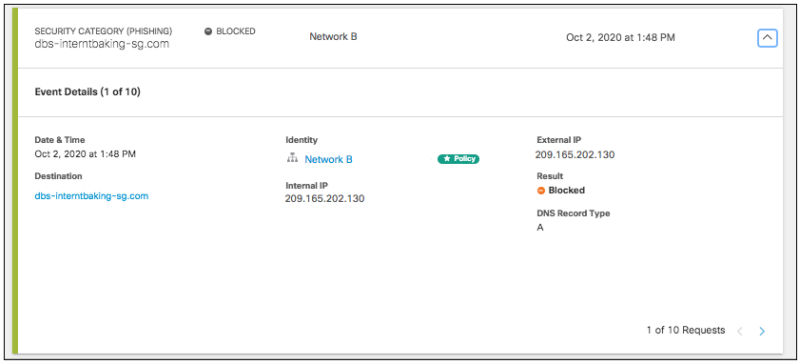
> **Note**
>
> If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response > Allowed**. Secure Access China cannot allow viruses to pass through the system. These will always be blocked.



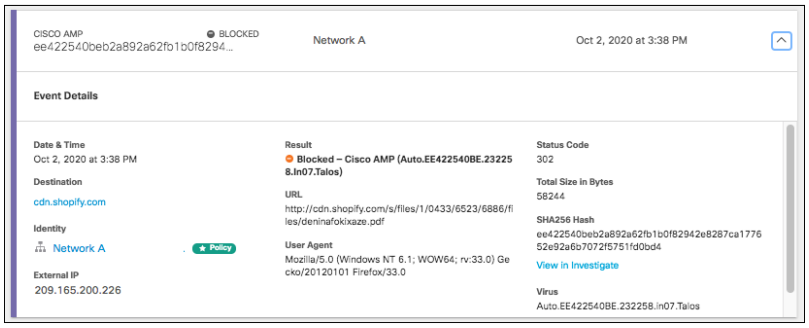
The list of events' details is stacked as cards and sorted by event type (if **Group Security Categories** is enabled).



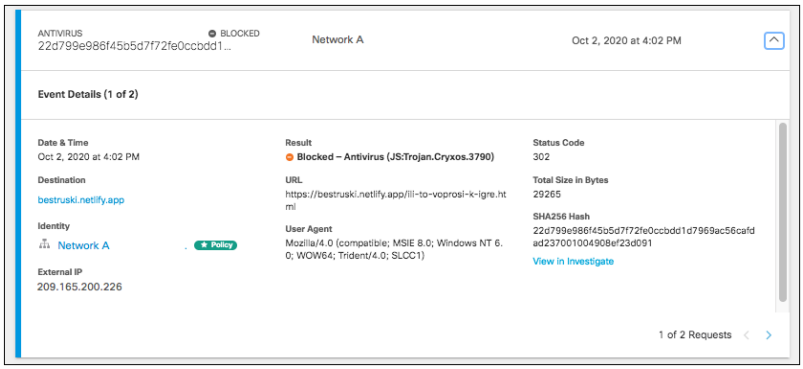
5. Click an event to view its details. Each security activity card groups an event by destination and lists the details of the event including date and time, destination, identity, and the event's result (Blocked or Allowed).



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 in Cisco Secure Access China. To view security activities for a specific source, use the search feature to filter the Activity chart and event details by source.

To view security activities for a specific source, use the search feature to filter the Activity chart and event details by source.

Prerequisites

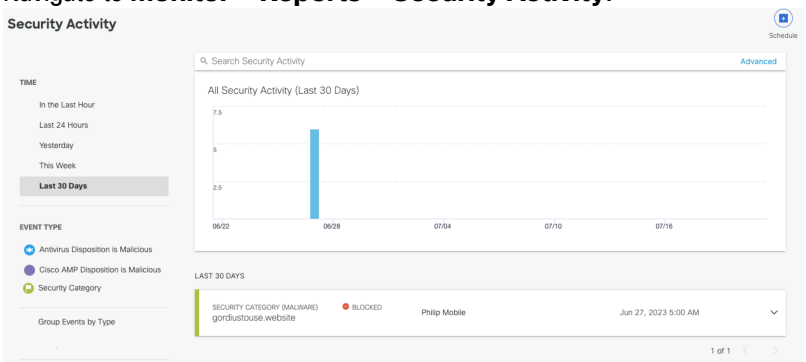
Lists the prerequisites for searching for security activity. A minimum user role of Read-only. For more information, see Manage Accounts.

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

Procedure

Provides instructions for searching for security activity. Navigate to Monitor > Reports > Security Activity. 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.

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.

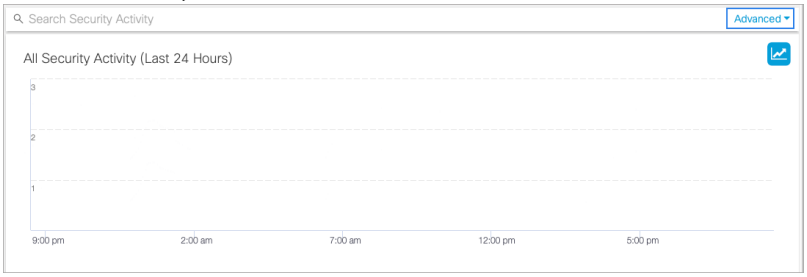


Advanced Search

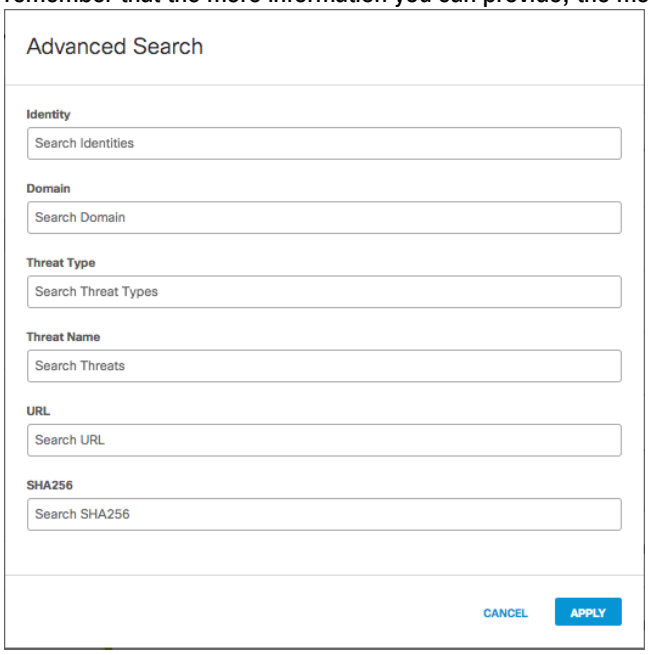
Describes advanced Search. To search security activities by more specific fields other than the source, such as domain, URL, or threat type, use the Advanced Search feature.

To search security activities by more specific fields other than the source, such as domain, URL, or threat type, use the Advanced Search feature.

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.



51 Total Requests Report

Topics:

- Total Requests Report

Provides an overview of Total Requests Report in Cisco Secure Access China. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Total Requests Report

Describes Total Requests Report in Cisco Secure Access China. The Total Requests Report provides a visualization of traffic over a given time period.

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.

Prerequisites

Lists the prerequisites for total requests report, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

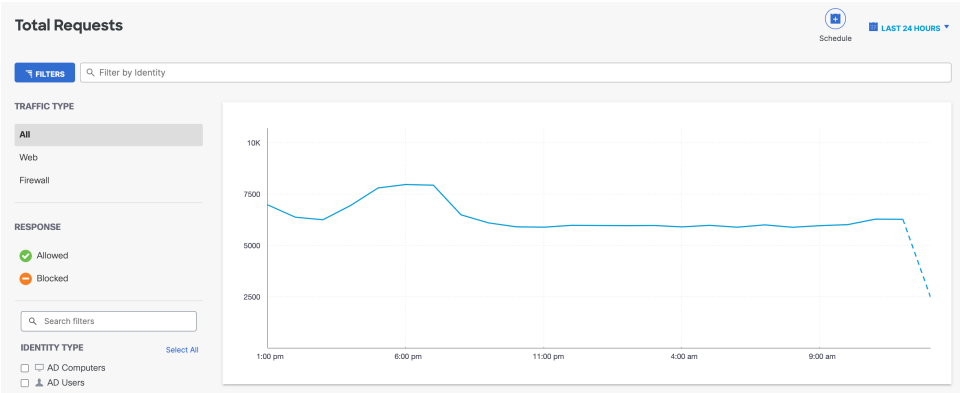
- A minimum user role of Read-only. For more information, see Manage Accounts.

View Trends in the Total Requests Report

Provides instructions for viewing trends in the total requests report. Navigate to Monitor > Reports > Total Requests. You will see filters to the left of the trend graph.

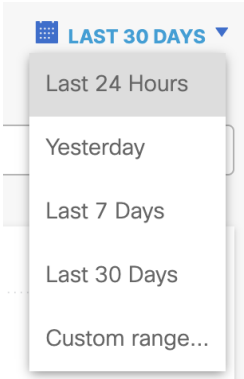
1. Navigate to **Monitor > Reports > Total Requests**.

   You will see filters to the left of the trend graph.



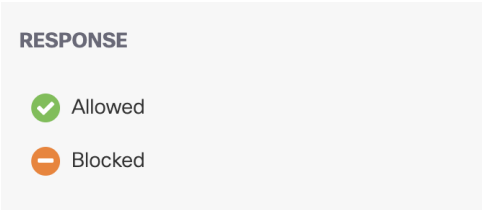
2. Choose a time frame to view the report's results.

   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.

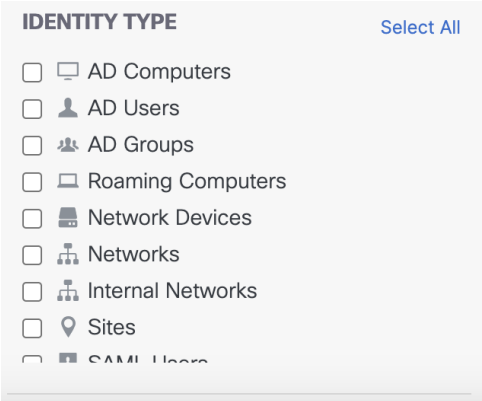


3. Filter the results by the type of response.

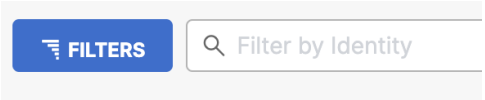
   You can filter by Blocked requests or Allowed requests. By default, nothing is selected, so all responses are shown.



4. Filter by specific identity types.

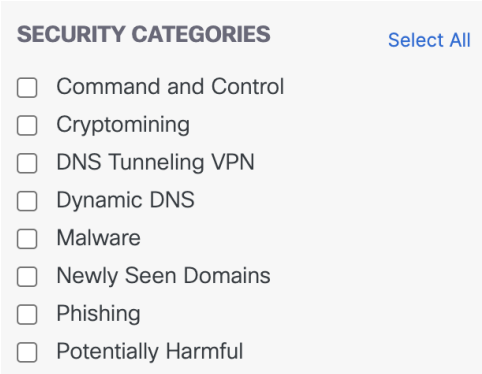


Alternatively, if you are looking for a specific identity to filter your results, enter it in the search bar.



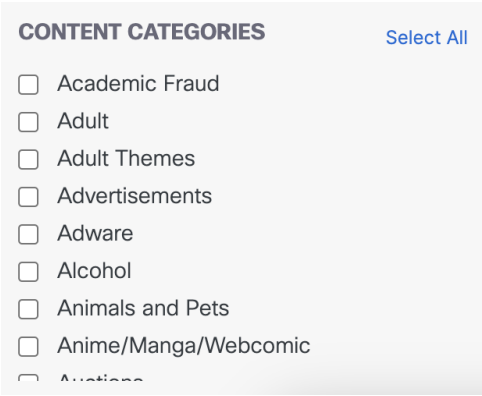
5. Filter by specific security categories.

For more information about threat categories, see Manage Threat Categories and Threat Category.

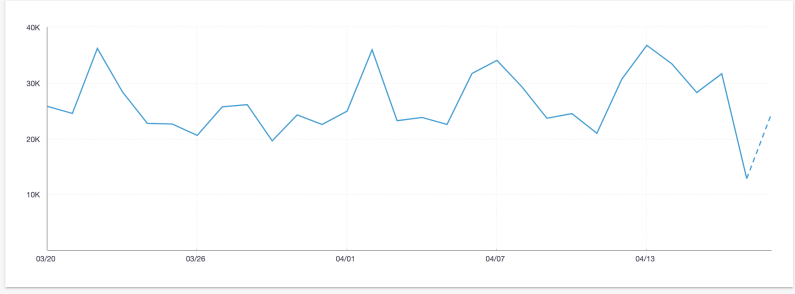


6. Filter by specific content categories.

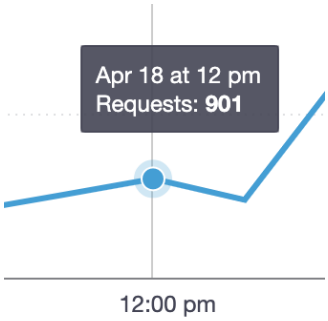
For a full list of content categories, see Available Content Categories.



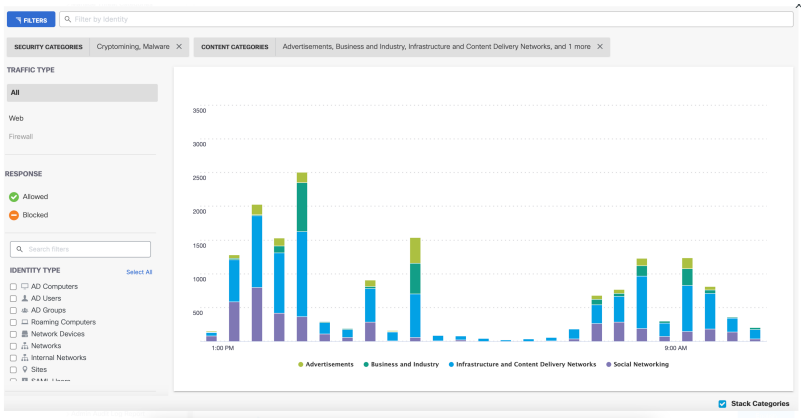
Once all filters have been selected and applied, the trend graph will update to reflect the appropriate total request data. When no security or content categories are selected, the graph remains a line that reflects the time frame, responses, and identity types selected.



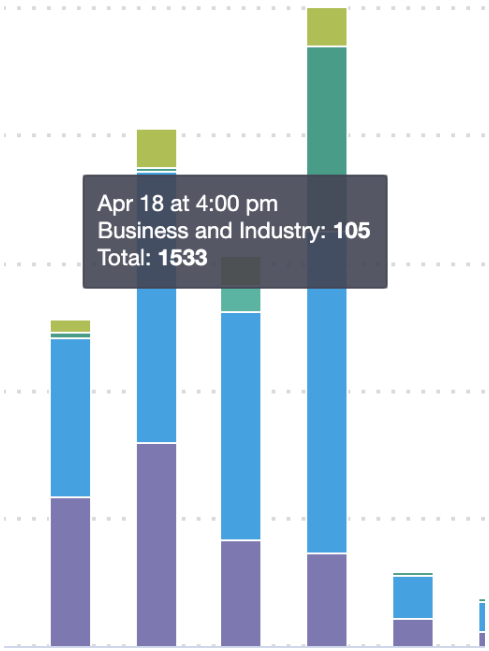
Hovering on a point on the graph will show the date, time and number of requests for that timestamp.



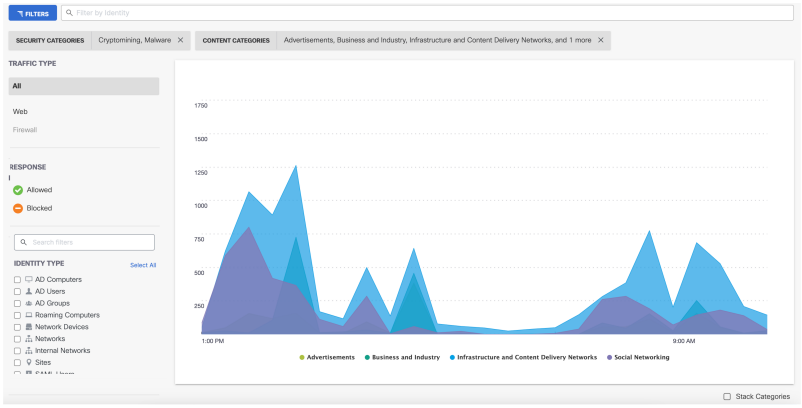
When you do filter by security or content categories, the trend graph will change to a bar graph of the requests for those categories within the selected time frame and other filters. Categories can be stacked if multiple categories showed traffic for those dates by clicking the **Stack Categories** checkbox.



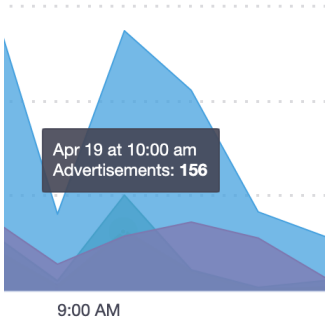
Hovering on a category for a specific date and time will show the total requests for that category as well as the overall total requests for that timestamp.



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.

52 Activity Volume Report

Topics:

- Activity Volume Report

Provides an overview of Activity Volume Report in Cisco Secure Access China. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Activity Volume Report

Describes Activity Volume Report in Cisco Secure Access China. 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.

Prerequisites

Lists the prerequisites for activity volume report, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

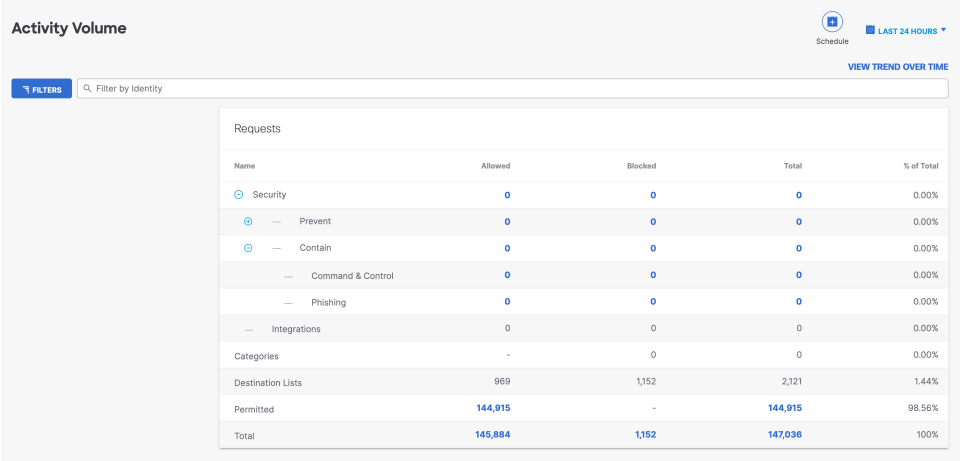
- A minimum user role of Read-only. For more information, see Manage Accounts.

View Requests by Volume of Activity

Provides instructions for viewing requests by volume of activity. Navigate to Monitor > Reports > Activity Volume. You are presented with a chart that depicts categorized requests over time.

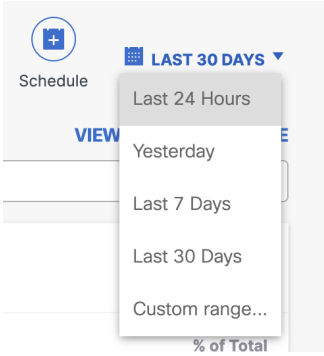
1. Navigate to **Monitor > Reports > Activity Volume**.

   You are presented with a chart that depicts categorized requests over time.

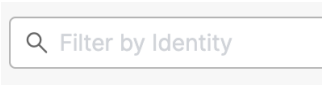


2. Choose a time frame to view the activity volume.

   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

Provides instructions for 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 China.

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 China.

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

Provides instructions for preventing. The Prevent security section lists the threat categories utilized to prevent threats and risks in your environment.

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

Provides instructions for 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.

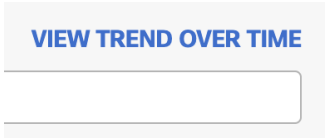
The Categories and Destination Lists fields provide an insight into traffic where requests were allowed or blocked due to policies configured with content categories and destination lists. The chart provides the number of Allowed, Blocked, Total Requests, and the percentage of Total Requests for each 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

Provides instructions for 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.



53 App Discovery Report

Topics:

- App Discovery Report

Provides an overview of App Discovery Report in Cisco Secure Access China, including View the App Discovery Report, View the Highest Risk Apps, and Review Apps in the Apps Grid. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

App Discovery Report

Describes App Discovery Report in Cisco Secure Access China. 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.

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

Provides instructions for viewing the App Discovery Report in Cisco Secure Access China. 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.

Prerequisites

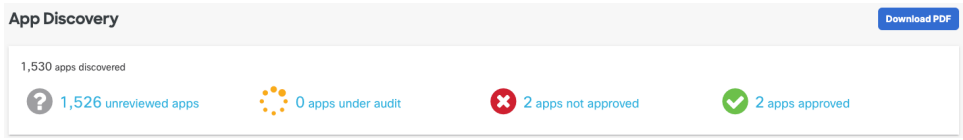
Lists the prerequisites for viewing the dashboard, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

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

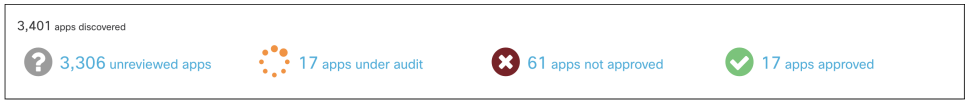
View the App Discovery Report

Provides instructions for viewing the app discovery report. Navigate to Monitor > Reports > App Discovery. View the discovered apps in your environment.

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.

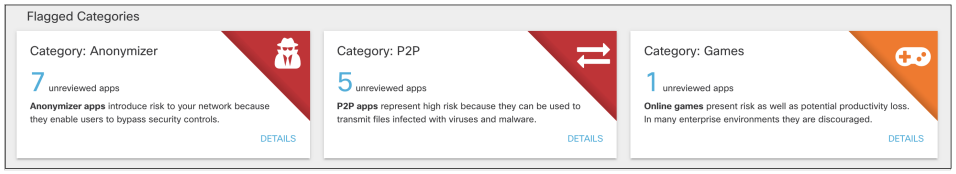


> **Note**
>
> Once an app has been given a label, it cannot be set back to Unreviewed. You can use the Under Audit label for apps that still need review. When you set an app to Not Approved, it is *not* automatically blocked from use. Labels within the App Discovery report are used to help review apps 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.

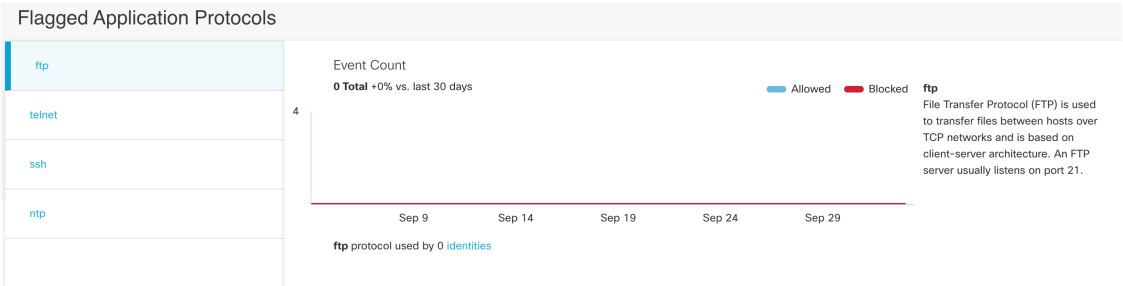


   For a complete list of application categories, see Application Categories.

4. View the flagged application protocols.

   These protocols are flagged based on the protocol used by the application.

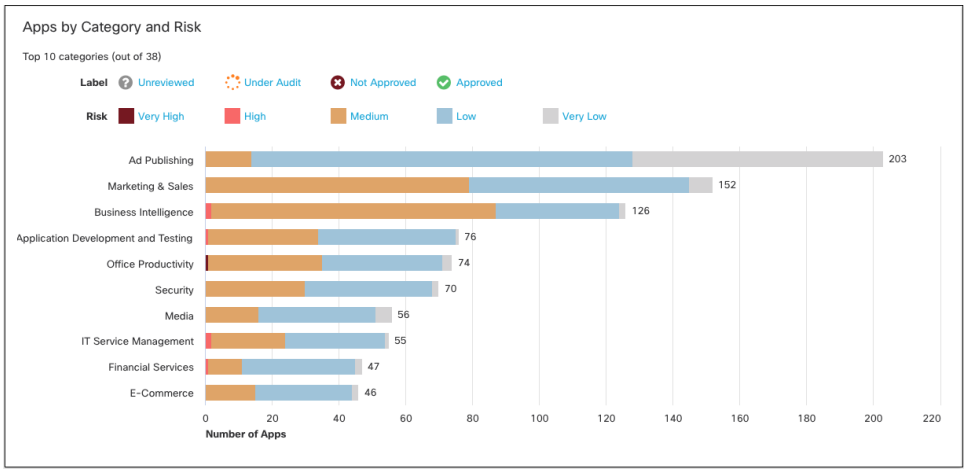
> **Note**
>
> Dismissing a flagged app card hides it from the overview. It does not label or block the app.



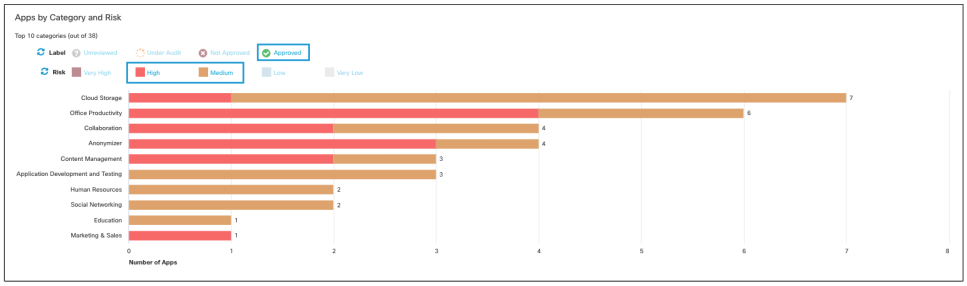
5. Choose **Web** to view the web traffic by App Risk. You can further filter the data by choosing **All Traffic**, **Outbound Traffic**, or **Inbound Traffic** from the drop-down list. Choose **Firewall** to view Firewall Events by App Risk.

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

Provides instructions for viewing the Highest Risk Apps in Cisco Secure Access China. 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.

Prerequisites

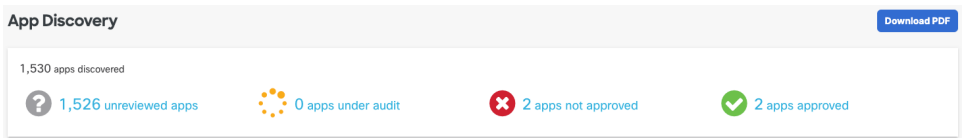
Lists the prerequisites for find the highest risk apps. A minimum user role of Read-only. For more information, see Manage Accounts.

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

Procedure

Provides instructions for find the highest risk apps. Navigate to Monitor > Reports > App Discovery. From the overview, click Unreviewed Apps . The App Grid appears depicting data for the last 90 days.

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.

Review Apps in the Apps Grid

Describes Review Apps in the Apps Grid in Cisco Secure Access China. The Apps Grid provides an overall view of application activity in your environment and the potential risk indicated by this traffic.

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 China 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.

Prerequisites

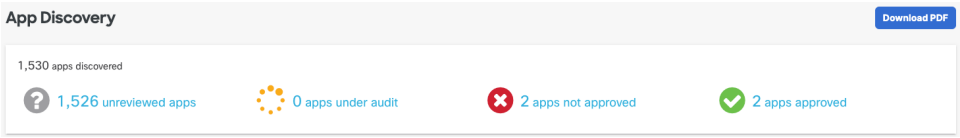
Lists the prerequisites for reviewing apps in the app grid. A minimum user role of Read-only. For more information, see Manage Accounts.

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

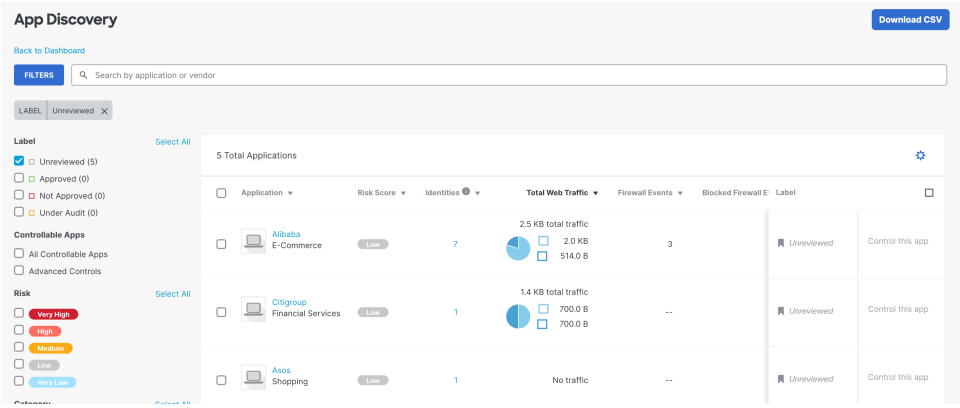
Procedure

Provides instructions for reviewing apps in the app grid. Navigate to Monitor > Reports > App Discovery and click one of the app labels to open the Apps Grid.

1. Navigate to **Monitor > Reports > App Discovery** and click one of the app labels to open the Apps Grid.



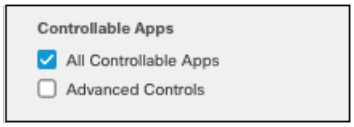
2. Filter by label.
   - **Unreviewed**–The app has not yet been assigned any label.
   - **Approved**–The app may be used in your environment.
   - **Not Approved**–The app should not be approved for use in your environment.
   - **Under Audit**–The app is currently under review.



> **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.

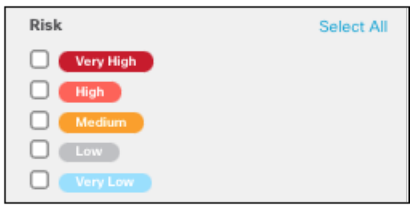
3. Filter by Controllable Apps.

   You can filter the apps listed by apps that are controllable and apps that have advanced app controls.

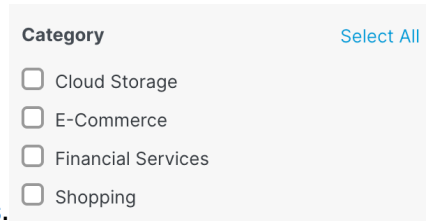
   

4. Filter by Risk.

   For more information on how risk is calculated, see Risk Details.

5. Filter by category.

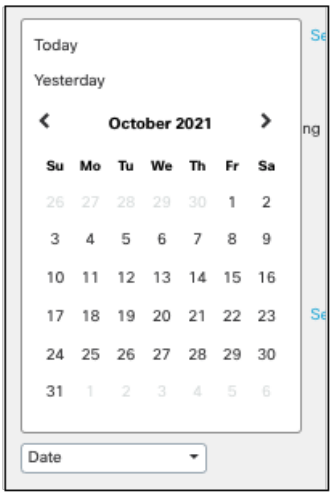
   For more information on app categories, see Application Categories.

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. You can customize what columns are displayed. Click the Actions icon. Select columns to display and click Apply.

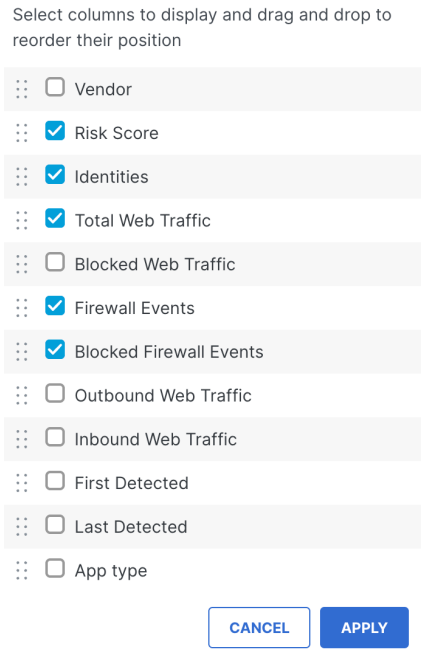
You can customize what columns are displayed.

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.

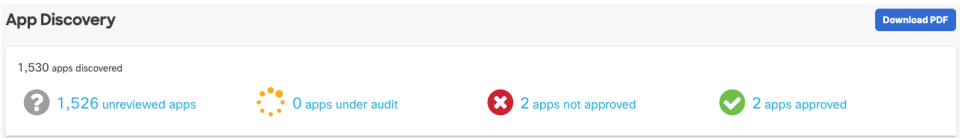


- **App Type**–The type of app: SaaS, PaaS or IaaS.
- **Blocked Traffic**–The percentage of all traffic blocked.
- **First Detected**–The date the app was first detected.
- **Identities**–The number of identities affected by the app. Click this number to view the app's details and the list of identities 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

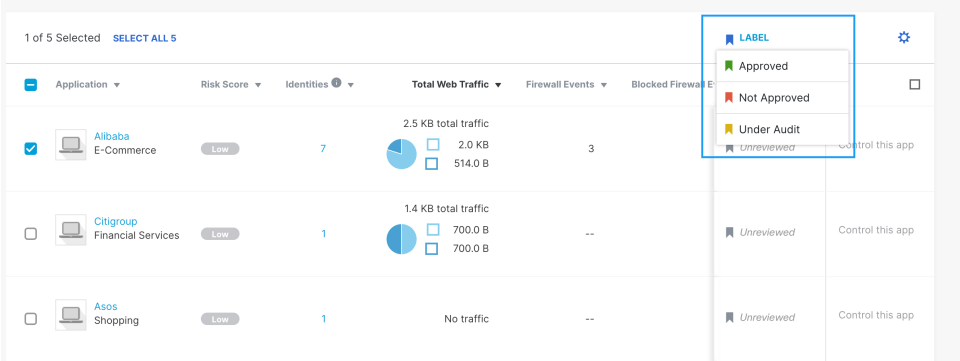
Provides instructions for changing the label of an app. Navigate to Reporting > Core Reports > App Discovery and click one of the app labels to open the Apps Grid.

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

Provides instructions for viewing app Details in Cisco Secure Access China, including Prerequisites and Procedure. It explains the sequence of actions and relevant settings presented in the procedure.

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 detailed attributes of the app, which can help you perform a risk/benefit analysis of permitting the app to be used in your environment.

Prerequisites

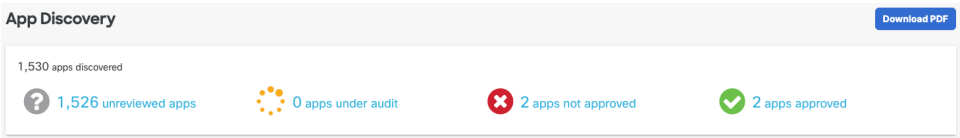
Lists the prerequisites for gather details about an app. A minimum user role of Read-only. For more information, see Manage Accounts.

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

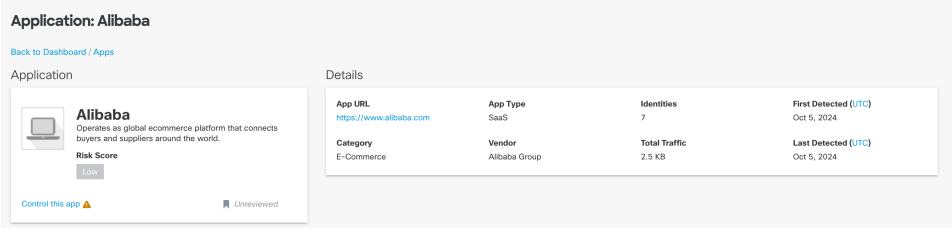
Procedure

Provides instructions for gather details about an app. Navigate to Monitor > Reports > App Discovery and click one of the app labels to open the Apps Grid.

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.



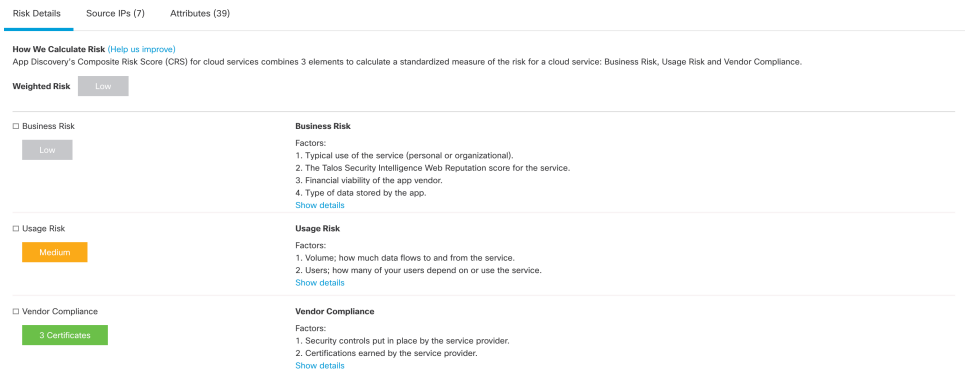
- **Risk Score**–The overall score calculated from the risk details.



- **Unreviewed**, **Approved**, **Not Approved**, or **Under Audit** – Current status of 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.
- **First Detected**–The date the app was first detected.
- **Last detected**–The date the app was last detected.

4. Click **Risk Details**.

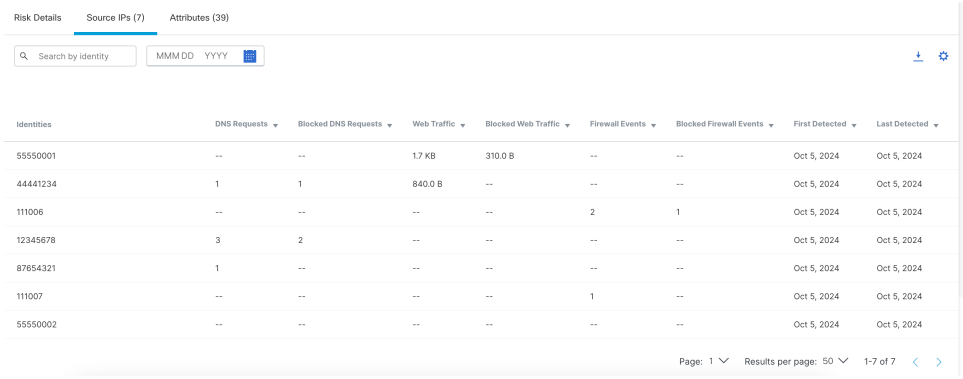
   The Risk Details tab displays the app's risk score and how it was calculated, including Business Risk, Usage Risk, and Vendor Compliance.



5. Click **Source IPs**.

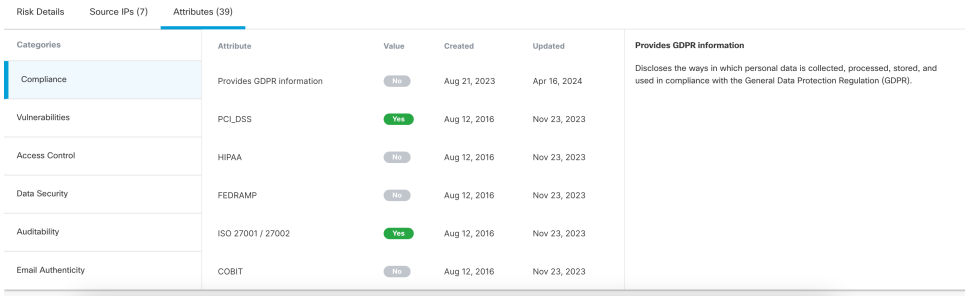
   The Source IPs tab lists your organization's sources that have made DNS requests and traffic for this app.

   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.



   Attributes are divided into categories. Click a category name to view the attributes associated with it. (Not all applications will show all attribute categories.)

   For each displayed attribute, Secure Access China 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 Change App Details in Cisco Secure Access China and outlines Prerequisites, Change the Risk Score for an App, and Change the Label of an App. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

You can change details about apps from within the App Discovery Report:

- You can change the review status label assigned to an app. Labels help you keep track of the review status of apps, so you know which ones are approved for use in your environment. The possible label values are:
  - **Unreviewed**–The app has not yet been assigned any label.
  - **Approved**–The app may be used in your environment.
  - **Not Approved**–The app should not be used in your environment.
  - **Under Audit**–The app is currently under review.

> **Note**
>
> Changing the label for an app does not change whether Umbrella blocks or allows the app. (You must configure application settings within a policy to block apps. For more information, see Manage the Access Policy. Labels are strictly for your own information, to help you keep track of the app review process within your organization.

- 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 Umbrella blocks or allows the app. (You must configure application settings within a policy to block apps. For more information, see Manage the Access Policy.) Umbrella 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 Umbrella, or assign different risk scores based on the risk tolerances within your organization.

Prerequisites

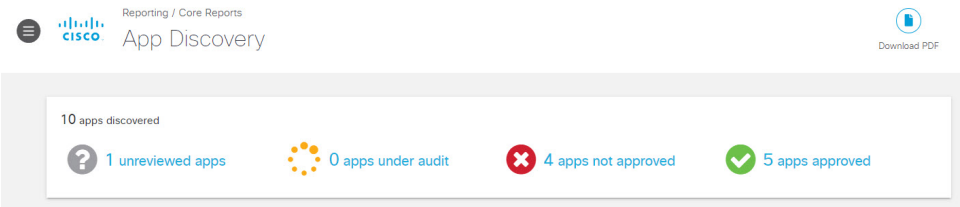
Lists the prerequisites for changing app details. A minimum of Read Only access to the Umbrella dashboard. See Manage Accounts.

- A minimum of Read Only access to the Umbrella dashboard. See Manage Accounts.

Change the Risk Score for an App

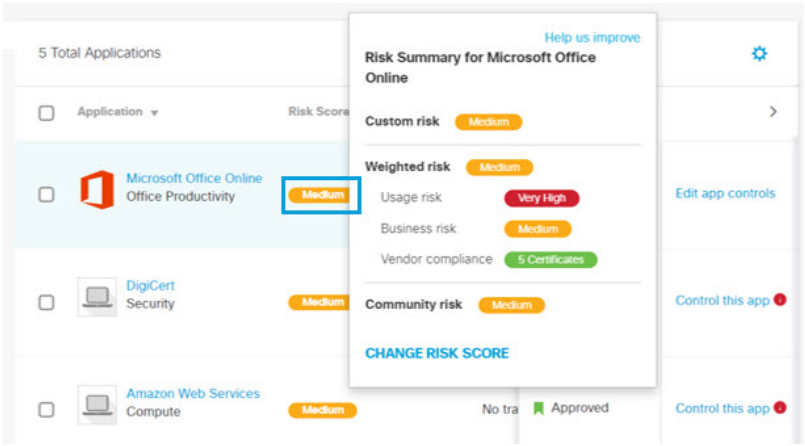
Provides instructions for changing the risk score for an app. Navigate to Monitor > Reports > App Discovery and click one of the app labels to open the Apps Grid.

1. Navigate to **Monitor > Reports > App Discovery** and click one of the app labels to open the Apps Grid.

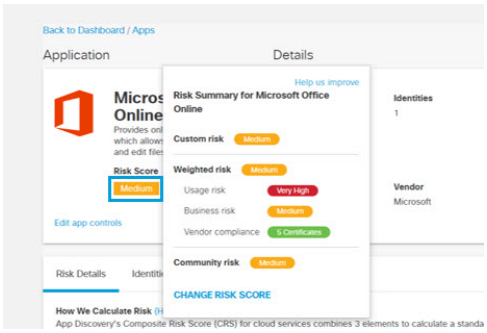


2. You have two choices:

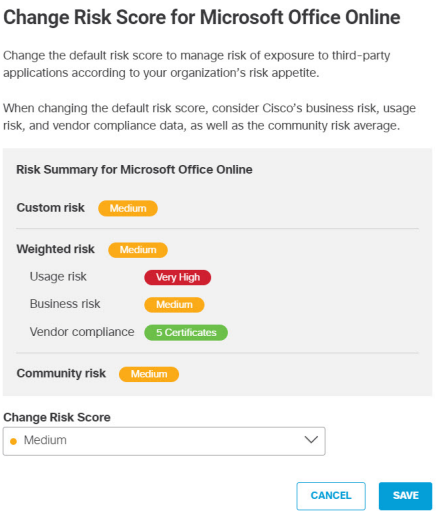
   a. To change the risk score for an app from the Apps Grid, hover over the risk score for an app to view its Risk Summary.



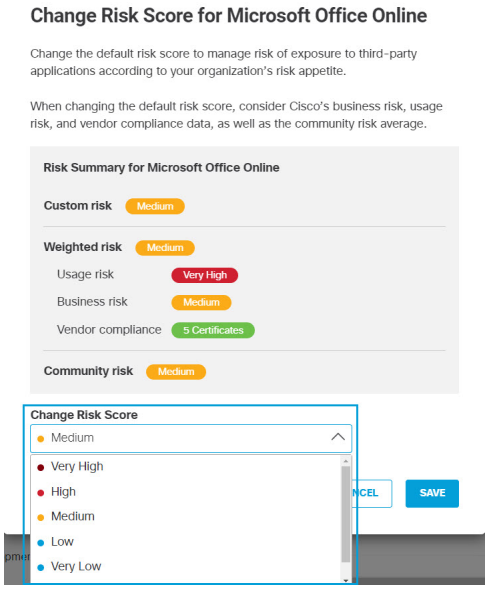
   b. To change the risk score for an app from its Details page, click the name of the app on the Apps Grid, then from the Details page hover over the risk score to view the Risk Summary.



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**.

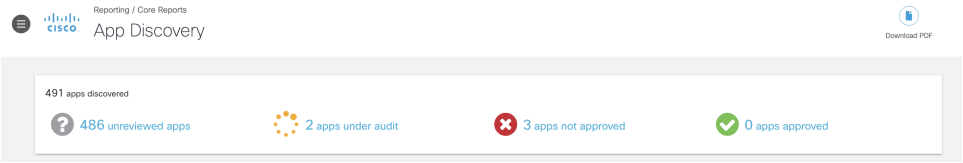
Change the Label of an App

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.

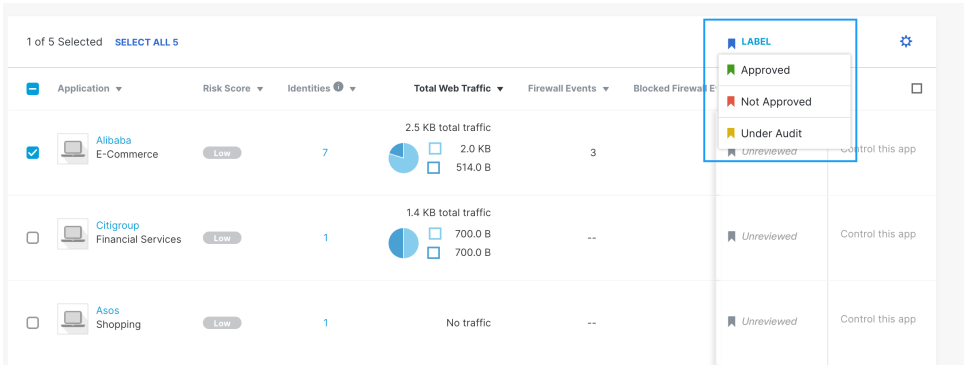
> **Note**
>
> Once an app has been given a label, it cannot be set back to **Unreviewed**. You can use the **Under Audit** label for apps that still need review.

1. Navigate to **Reporting** > **Core Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.

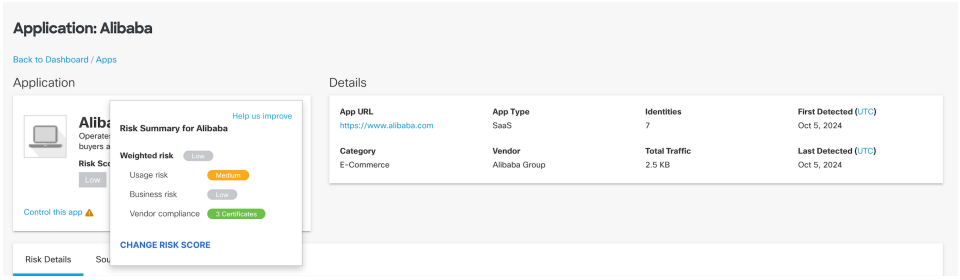


2. You have two choices:

   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 in Cisco Secure Access China. You can control applications through rules and through the App Discovery report in the app details and the App Grid.

You can control applications through rules and through the App Discovery report in the 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.

Prerequisites

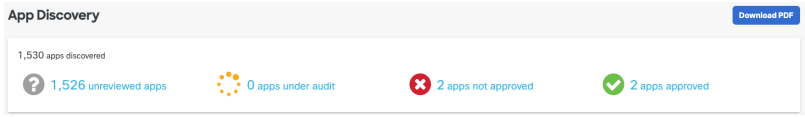
Lists the prerequisites for blocking apps, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

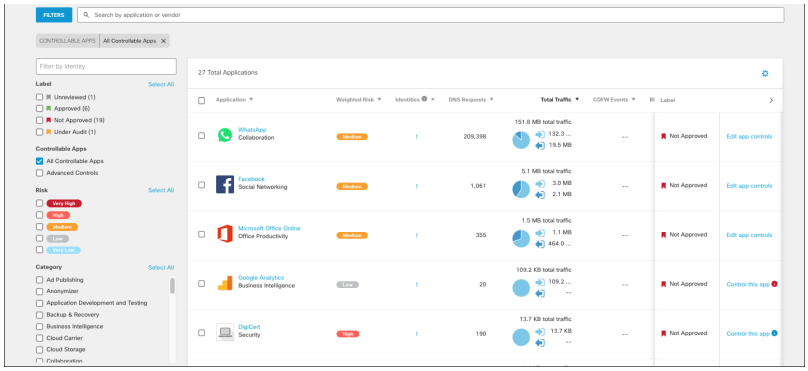
Procedure

Provides instructions for blocking apps. Navigate to Monitor > Reports > App Discovery. From the overview, click Unreviewed Apps . The App Grid appears depicting data for the last 90 days.

1. Navigate to **Monitor** > **Reports** > **App Discovery.**

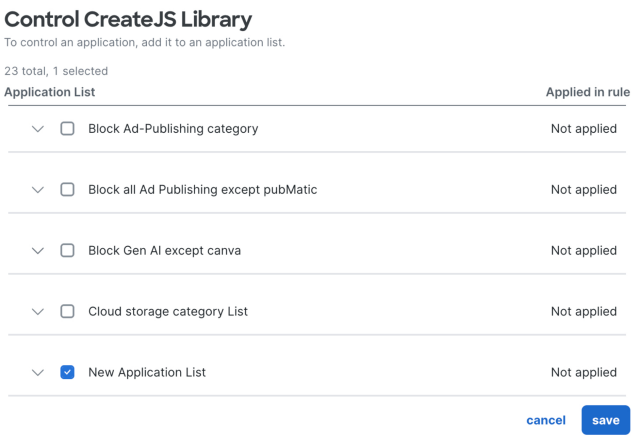


2. From the overview, click **Unreviewed Apps**. The App Grid appears depicting data for the last 90 days.
3. Select a **Controllable Apps** filter: **All Controllable Apps** or **Advanced Controls**.



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

You can also configure a rule to block lists of applications and lists of application categories. For more information, see Manage Application Lists and Add an Application List.

For more information about applying application lists to rules, see Manage the Access Policy.

Control Advanced Apps

Describes Control Advanced Apps in Cisco Secure Access China. Applications within App Discovery can be blocked or allowed based on risk assessment.

Applications within App Discovery can be blocked or allowed based on risk assessment. In addition to blocking all content for an application, you have the option to instead block only specific content, such as file uploads or posts.

> **Note**
>
> Secure Access China Packages
>
> Advanced App Controls are not available to all Secure Access China 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.

Prerequisites

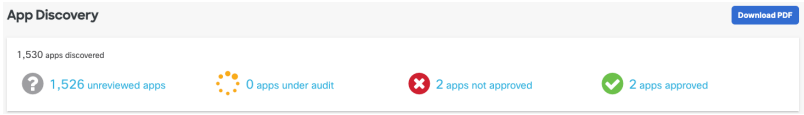
Lists the prerequisites for control advanced apps, including the Full Admin user role; see Manage Accounts for details about available roles and account access.

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

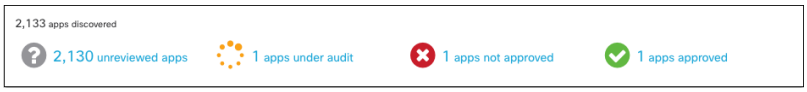
Procedure

Provides instructions for control advanced apps. Navigate to Monitor > Reports > App Discovery. Click any of the discovered apps labels to enter the Apps Grid.

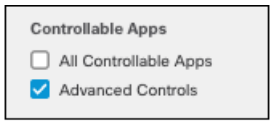
1. Navigate to **Monitor > Reports > App Discovery**.



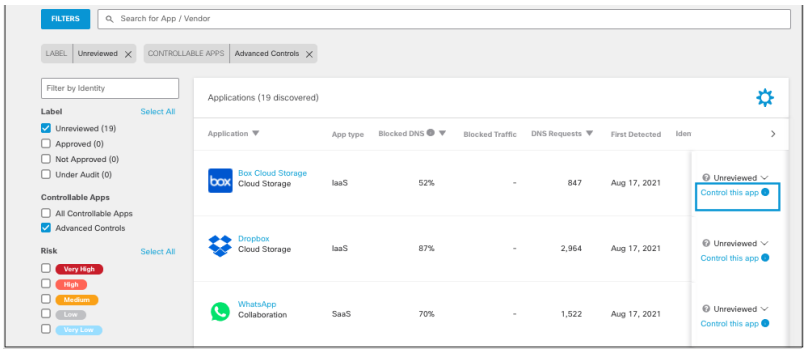
2. Click any of the discovered apps labels to enter the Apps Grid.



3. Choose **Advanced Controls** under the **Controllable Apps** filter.

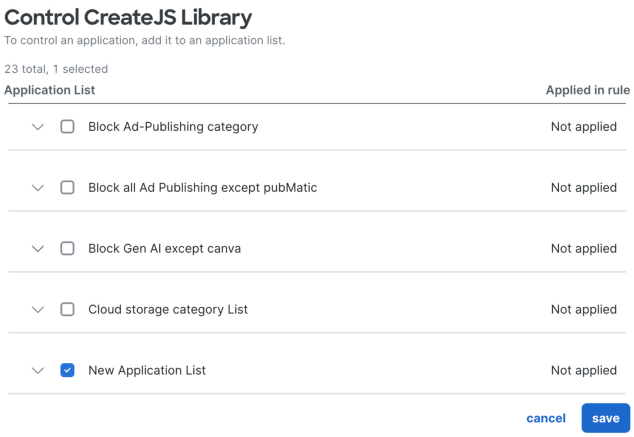


4. Choose an app to control and click **Control this app**.



5. 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.



View Traffic Data Through SWG Service

Provides instructions for viewing traffic Data Through SWG Service in Cisco Secure Access China. App Discovery provides traffic data through the Secure Web Gateway (SWG) service.

App Discovery provides traffic data through the Secure Web Gateway (SWG) service. Traffic is reported in bytes in and bytes out.

Prerequisites

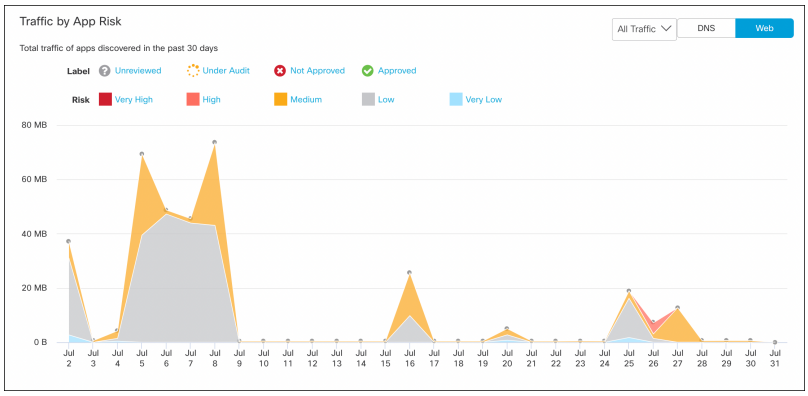
Lists the prerequisites for traffic data through SWG. A minimum user role of Read-only. For more information, see Manage Accounts.

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

View Traffic

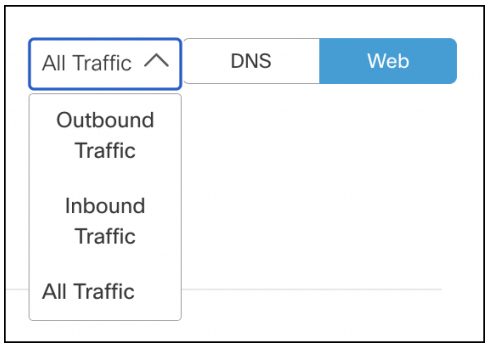
Provides instructions for viewing traffic. Navigate to Monitor > Reports > App Discovery and locate the Traffic by App Risk graph.

1. Navigate to **Monitor > Reports > App Discovery** and locate the **Traffic by App Risk** graph.

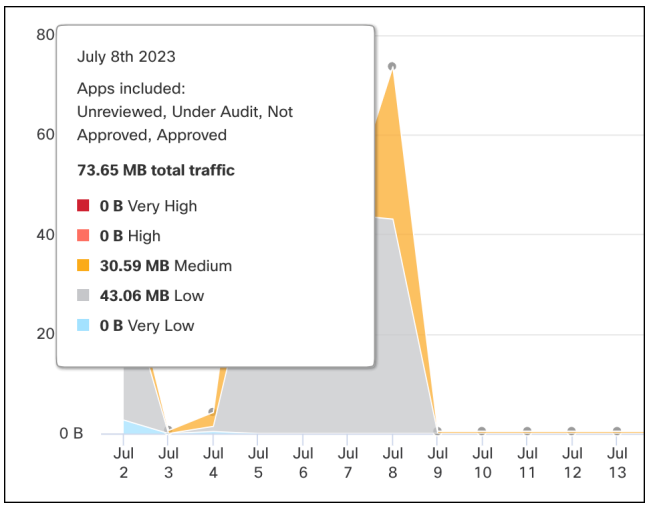


   If the **Firewall Events by App Risk** graph is displayed, click **Web** to display Traffic by App Risk.

2. Click **All Traffic** to open the drop-down and then choose to view **All Traffic**, **Inbound Traffic**, or **Outbound Traffic**.



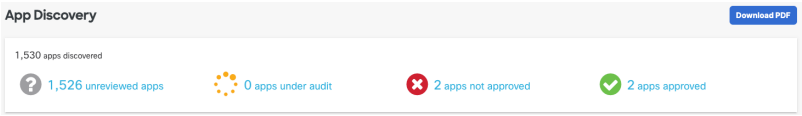
3. Hover on a point in the graph to view details about the traffic by app risk for that date.



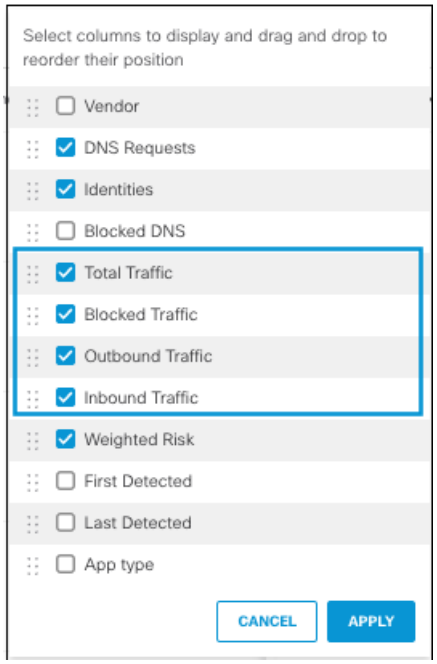
View Traffic in the Apps Grid

Provides instructions for viewing traffic in the apps grid. Navigate to Monitor > Reports > App Discovery and click one of the app labels to open the Apps Grid.

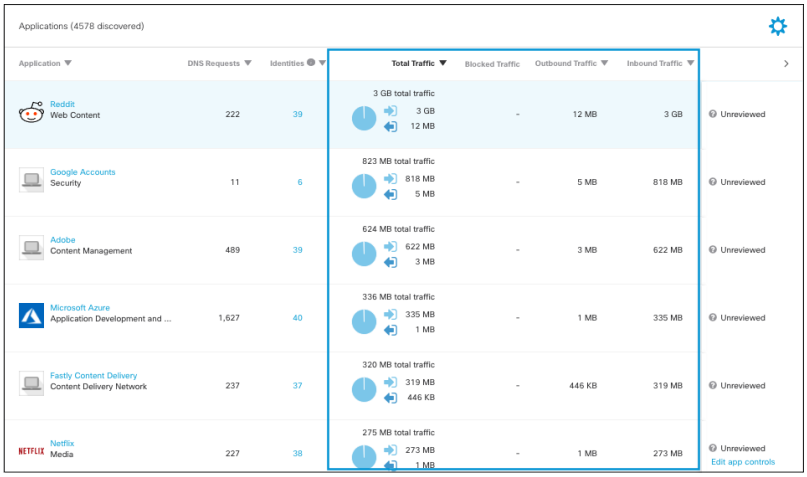
1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



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**.



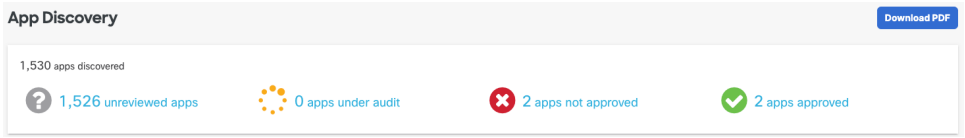
3. View the traffic, bytes in and out, of applications by total, outbound, or inbound traffic.



View Traffic in the App Details

Provides instructions for viewing traffic in the app details. Navigate to Reporting > Core Reports > App Discovery and click the name of an app to view its details for the last 90 days.

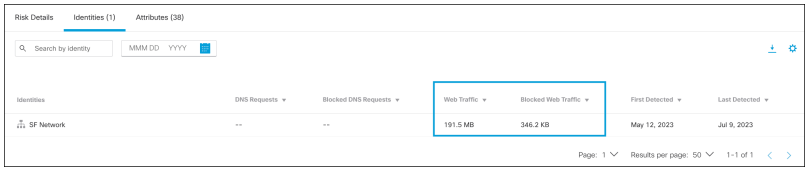
1. Navigate to **Reporting > Core Reports > App Discovery** and click the name of an app to view its details for the last 90 days.



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.



54 Top Destinations Report

Topics:

- Top Destinations Report

Provides an overview of Top Destinations Report in Cisco Secure Access China, including Destination Details. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Top Destinations Report

Describes Top Destinations Report in Cisco Secure Access China. The Top Destinations report lists the top domains your organization has made access requests to over the selected time period.

The Top Destinations report lists the top domains your organization has made access requests to over the selected time period. It is filterable, schedulable, and you can export the results to a CSV file.

Destination Details

Describes Destination Details in Cisco Secure Access China. The Destination Details report provides access to information about the destinations that your identities are visiting, determining which are the most actively requested and when this activity occurs.

The Destination Details report provides access to information about the destinations that your identities are visiting, determining which are the most actively requested and when this activity occurs. Here you can explore activity at the domain level, determining who has visited the selected domain and when. This detailed information can help you determine if any computer or networks may be compromised or are connecting to known malicious sites so that you can better protect yourself and others.

Prerequisites

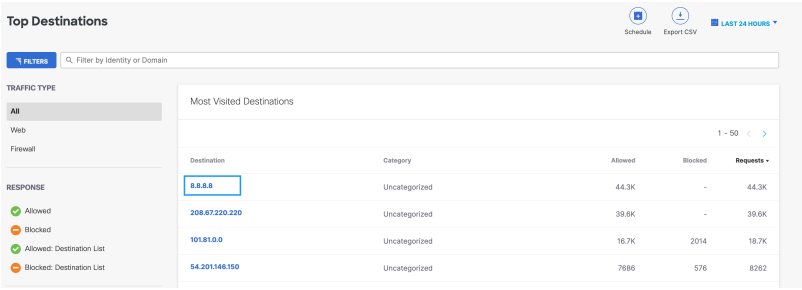
Lists the prerequisites for destination details, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

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

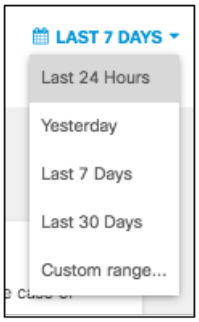
View the Destination Details

Provides instructions for viewing the destination details. 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.

1. Navigate to **Monitor > Reports > Top Destinations** and click a **Destination**

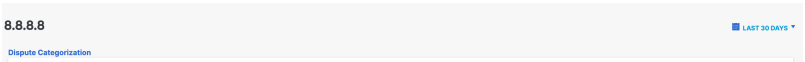


2. Choose a time frame within which data is displayed.

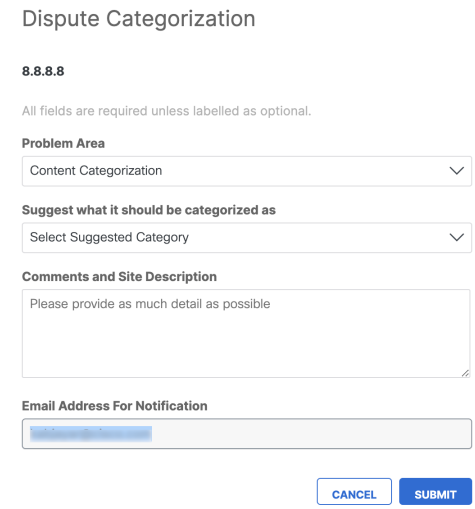


3. View the destination's content and threat categories.

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.



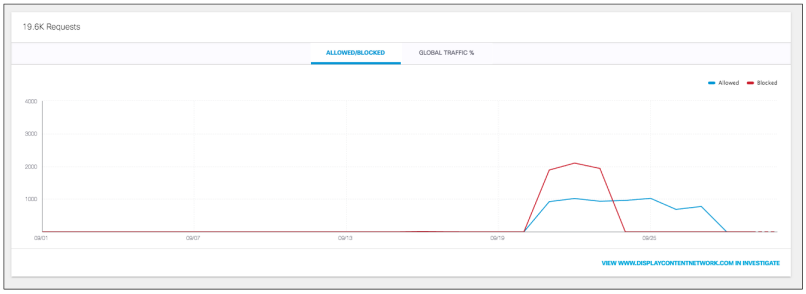
If you believe this destination belongs in a security category, click **Dispute Categorization**, fill out the request form that creates an internal Secure Access China ticket for a security researcher to review, and click **Submit**.



View the Request Traffic

Provides instructions for 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.

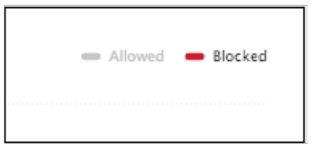


View Requests by Blocked or Allowed

Provides instructions for viewing requests by blocked or allowed. Click on Allowed , Blocked , or both to view those requests in the traffic graph.

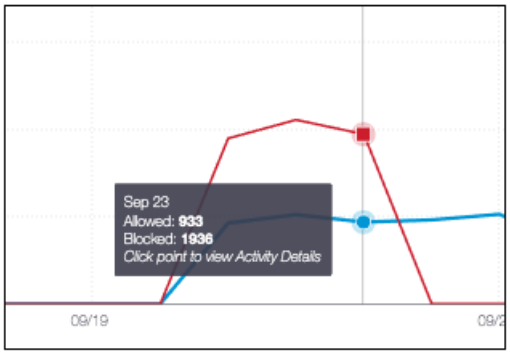
1. Click on **Allowed**, **Blocked**, or both to view those requests in the traffic graph.

   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.

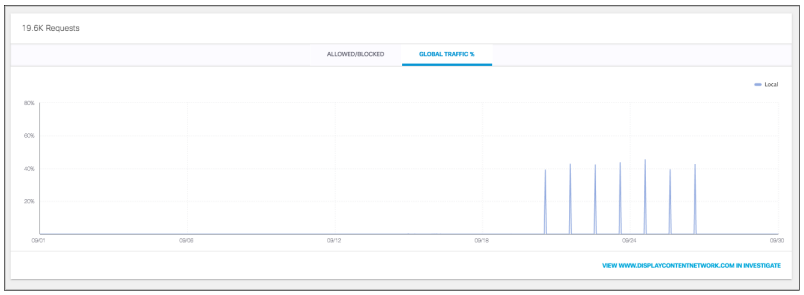


View Requests Through Global Traffic %

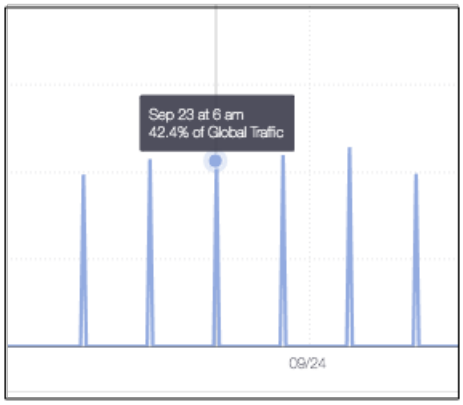
Provides instructions for viewing requests through global traffic %. Click Global Traffic % on the traffic graph. The Global Traffic % chart displays the percentage of global traffic to this specific destination that is comprised of local traffic from your organization's Identities.

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.



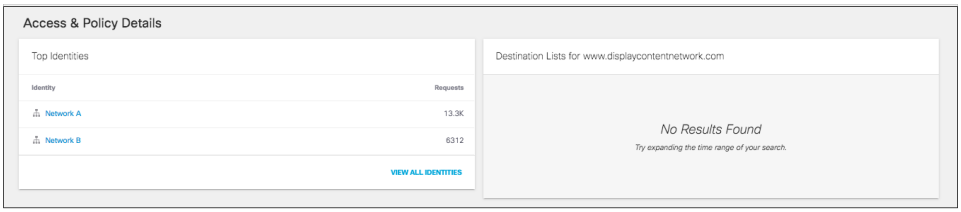
2. Hover on a point to view the date, time, and percentage of global traffic at that time.



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.

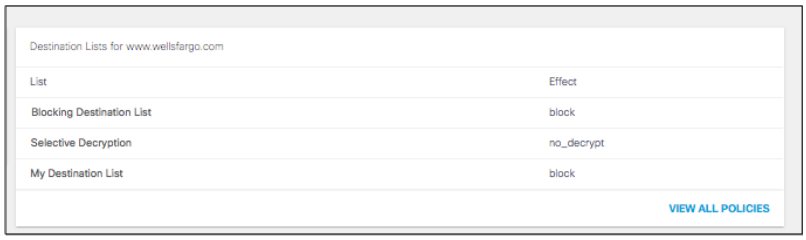


1. Navigate to the **Access & Policy Details** > **Top Identities**.

   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**.

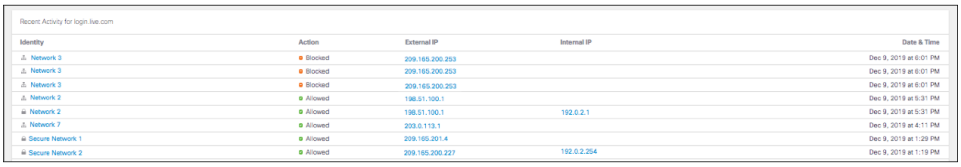
   The Destination Lists table shows if this domain belongs to any in your rules and what effect that list would have on the domain.



View Recent Activity

Provides instructions for 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.

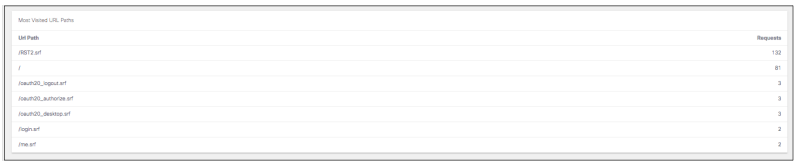
The Recent Activity chart lets you investigate DNS activity for this destination. You can view the identities that requested the destination, the action (response) to that request (Blocked or Allowed), the external and internal IP addresses, and the date and time of the request. Viewing this information 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

Provides instructions for 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.



Prerequisites

Lists the prerequisites for top destinations report, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

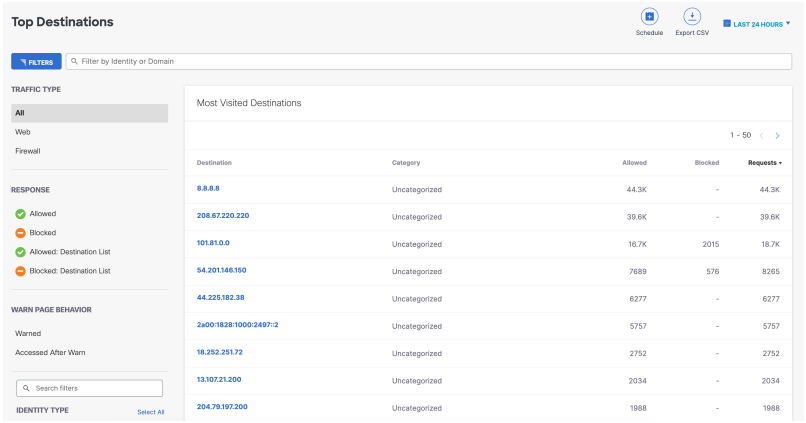
- A minimum user role of Read-only. For more information, see Manage Accounts.

View the Top Destinations Report

Provides instructions for viewing the top destinations report. Navigate to Monitor > Reports > Top Destinations. The report displays a chart of the most visited destinations.

1. Navigate to **Monitor > Reports > Top Destinations**.

   The report displays a chart of the most visited destinations.

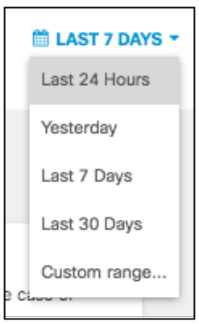


   The following information is displayed for each destination:

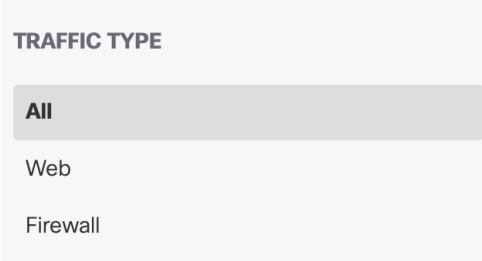
   - **Destination**–The domain.
   - **Category**–The category, such as Malware, Business Services, Phishing, and so on.
   - **Allowed**–The number of requests to that destination that were allowed.
   - **Blocked**–The number of requests to that destination that were blocked.
   - **Requests**–The number of requests for the domain for the selected period.

2. Choose a time frame within which data is displayed.

   Figure 7: time .png



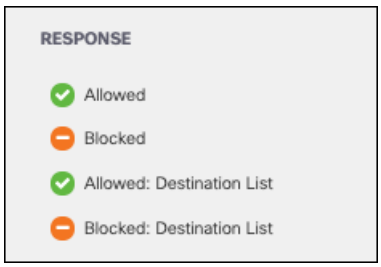
3. Choose whether to view results for All types of traffic, Web, or Firewall.



4. Filter results by the response type.

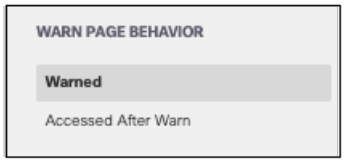
   Select Allowed, Blocked, Allowed: Destination List, or Blocked: Destination List. By default, nothing is selected, so all responses are shown.

   Figure 8: updated response type.png

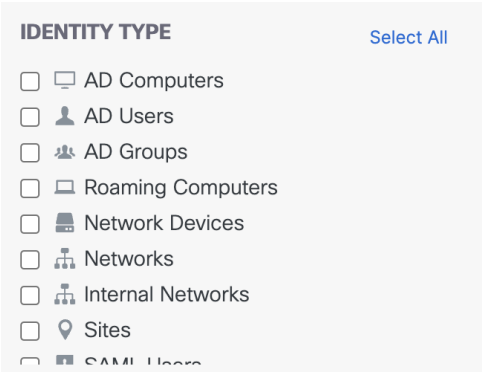


5. Filter results by requests that were warned or accessed after a warning.

   Figure 9: warn filter.png

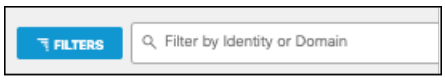


6. Filter by specific identity types and click **Apply**.



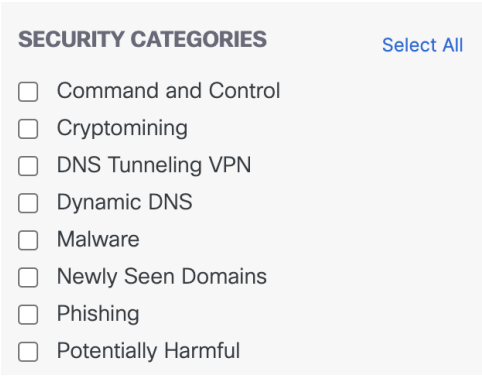
   Alternatively, if you are looking for a specific identity to filter your results, enter it in the search bar. You can also filter by a specific domain.

   Figure 10: identity:domain filter.png



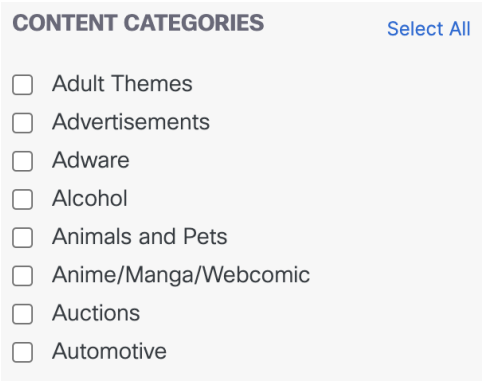
7. Filter by specific security categories and click **Apply**.

   For more information, see Threat Categories.

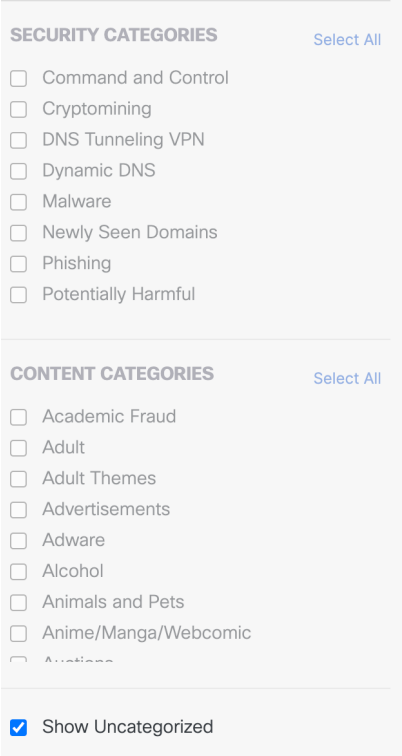


8. Filter by specific content categories and click **Apply**.

   For more information about content categories, see Manage Content Categories.



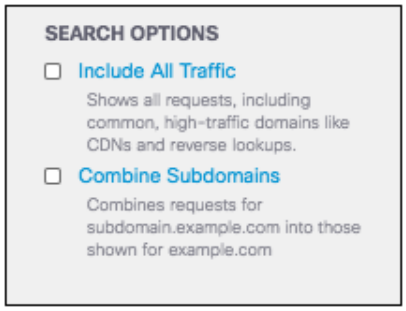
   Alternatively, selecting **Show Uncategorized** deselects all security and content categories and only displays requests not matching any category.



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.

Figure 11: filters.png



View Further Details

Provides instructions for 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.

55 Top Categories Report

Topics:

- Top Categories Report

Provides an overview of Top Categories Report in Cisco Secure Access China, including Category Details. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Top Categories Report

Describes Top Categories Report in Cisco Secure Access China. The Top Categories report is a list of the top security and content categories by firewall requests for your organization over the selected period.

The Top Categories report is a list of the top security and content categories by 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 China 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.

Category Details

Describes Category Details in Cisco Secure Access China. 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.

Prerequisites

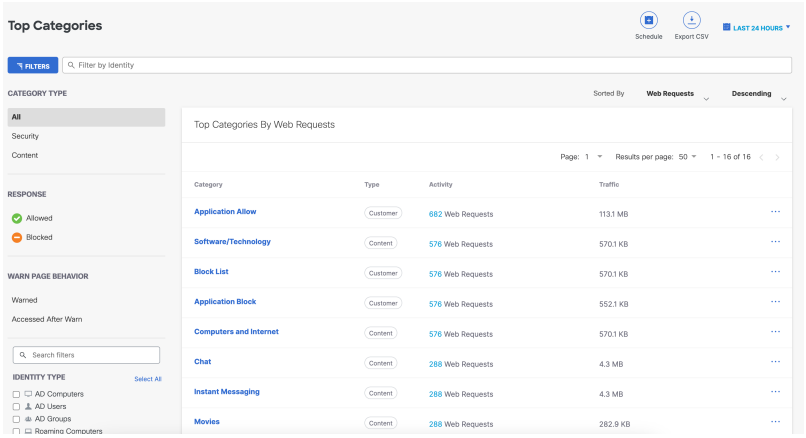
Lists the prerequisites for category details, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

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

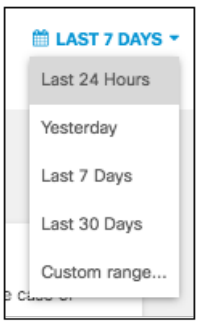
View a Category's Details Overview

Provides instructions for viewing a category's details overview. Navigate to Monitor > Reports > Top Categories and click one of the listed categories.

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

Provides instructions for viewing a category's traffic. The first graph depicts the traffic over a selected time period for this category.

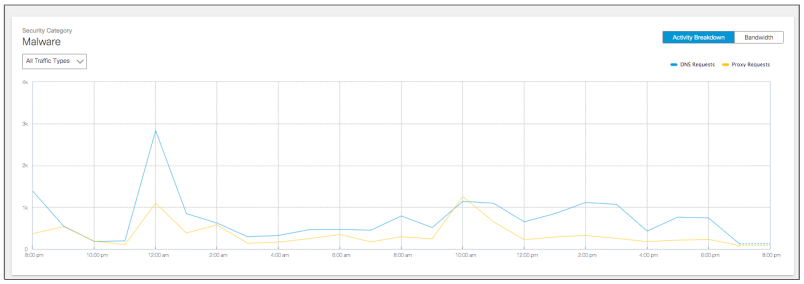
The first graph depicts the traffic over a selected time period for this category.

View the Activity Breakdown

Provides instructions for viewing the activity breakdown. Click a category and navigate to the traffic graph on the details page. Select Activity Breakdown.

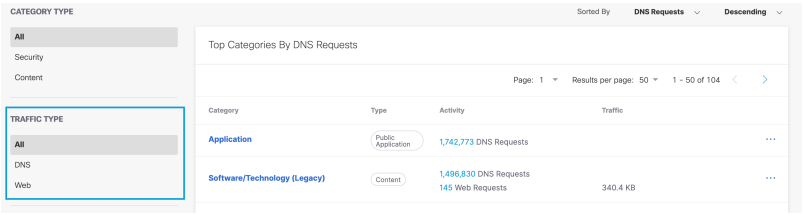
1. Click a category and navigate to the traffic graph on the details page. Select **Activity Breakdown**.

   The Activity Breakdown displays the number of web requests and proxy transactions for the selected time period.

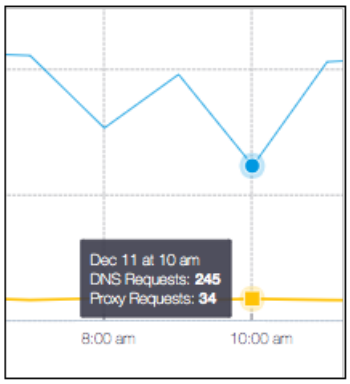


2. Filter the Activity Breakdown to view All Traffic Types (default), Web, or Firewall.

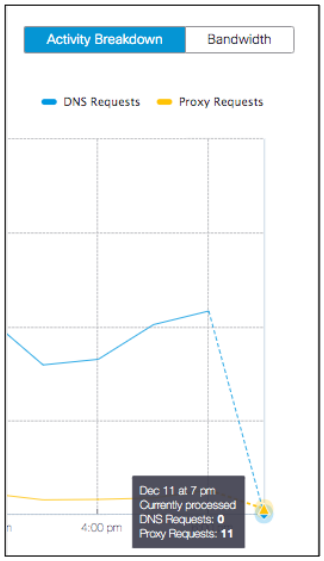
   You can also choose the traffic type to filter before redirecting to the category details from the Top Category report. IP requests are not an option in Category Details.



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.

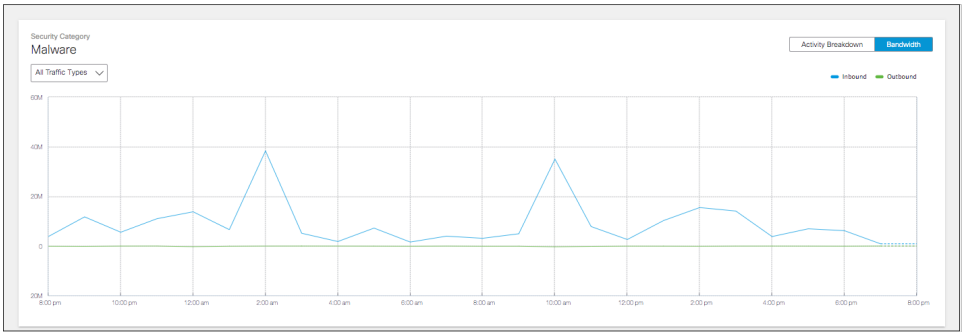


View the Traffic Bandwidth

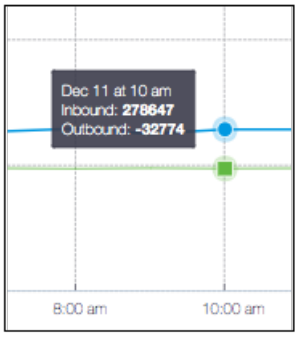
Provides instructions for viewing the traffic bandwidth. Click a category and navigate to the traffic graph on the details page. Select Bandwidth.

1. Click a category and navigate to the traffic graph on the details page. Select **Bandwidth**.

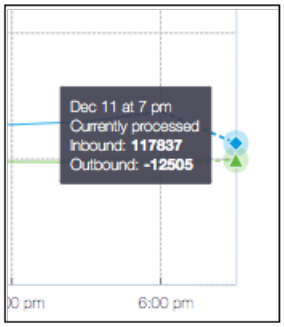
   For proxy transactions, the bandwidth view of the line graph shows the number of inbound and outbound traffic for the selected time period.



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.

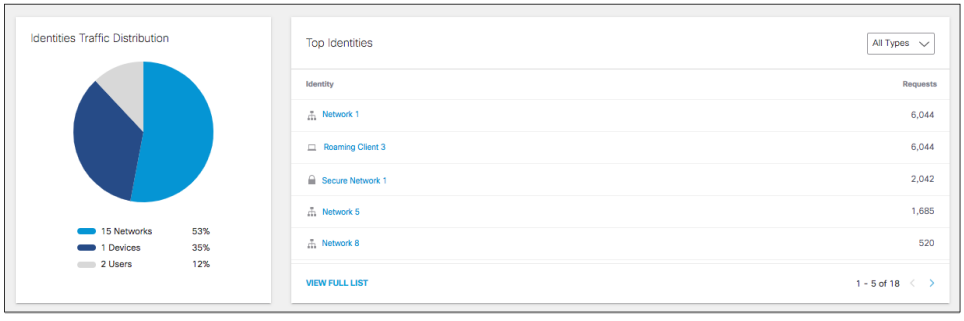


View a Category's Identities

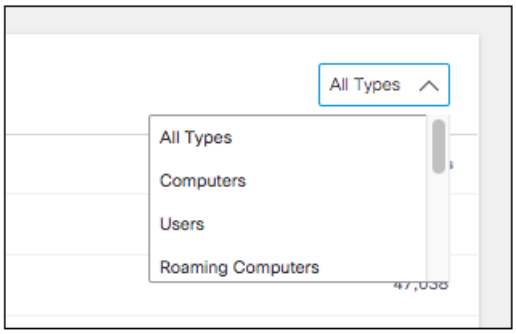
Provides instructions for viewing a category's identities. Navigate to the identities section of the report. View the Identities Traffic Distribution.

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. Navigate to the Top Domains section of the report. This list depicts the top domains where requests were flagged for this category:.

1. 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.

Prerequisites

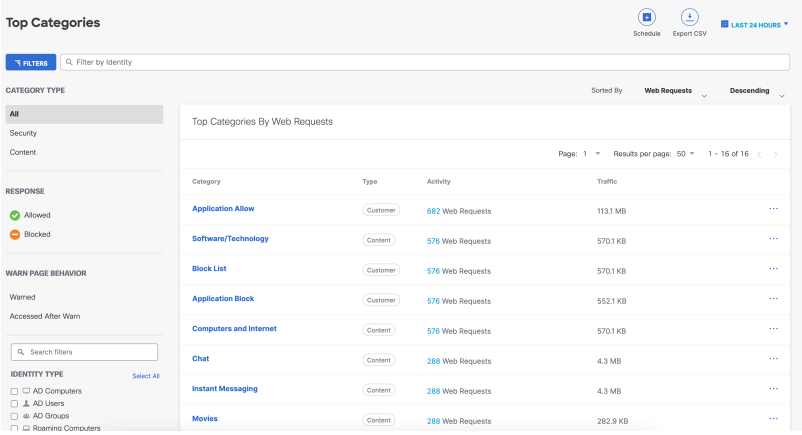
Lists the prerequisites for top categories report, including a minimum Read-only user role; see Manage Accounts for details about available roles and account access.

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

View the Top Categories Report

Provides instructions for viewing the top categories report. Navigate to Monitor > Reports > Top Categories. Category –The threat or content category item. Clicking a category name redirects you to the Category Details section.

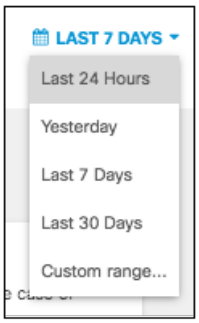
1. Navigate to **Monitor > Reports > Top Categories**.



Report Fields

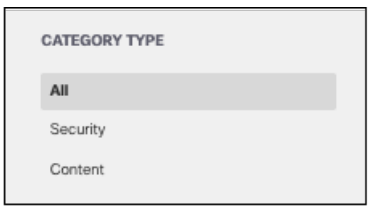
- **Category**–The threat or content category item. Clicking a category name redirects you to the Category Details section.
- **Type**–The type of category: security, content, or application.
- **Traffic**–The total bandwidth of proxy requests uploaded and downloaded for this category.
- **Activity**–The 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)

2. 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.



3. 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.

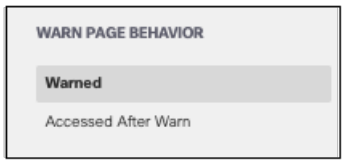


4. Filter top categories by response type.

You can view categories from requests that were Allowed, Blocked, or both. By default, neither is selected, so all responses are shown.

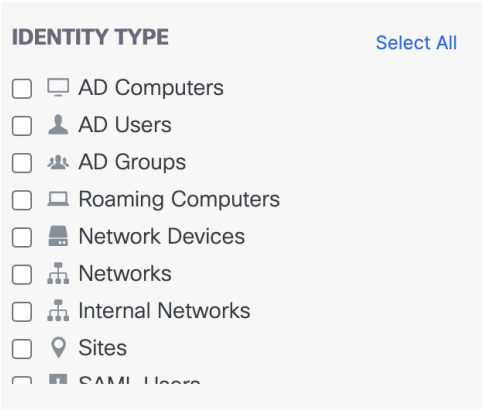


5. Filter requests that were warned or accessed after a warn.



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.

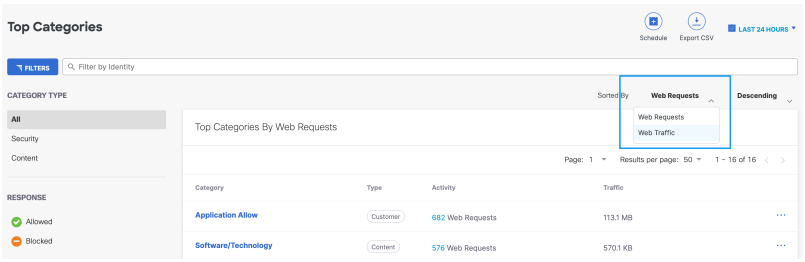


7. Choose how to sort the top category results.

Sort by Traffic

Provides instructions for sorting report traffic. Choose Web Requests to list web requests first, or Web Traffic to list web traffic first, when reviewing the traffic data.

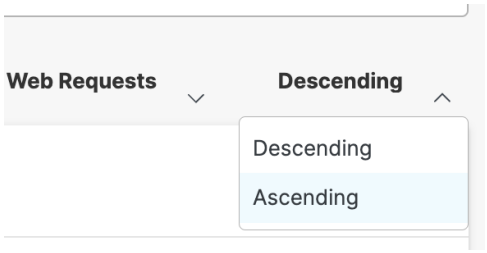
- **Web Requests**–Show Web requests first.
- **Web Traffic**–Show Web traffic first.



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.

- **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.

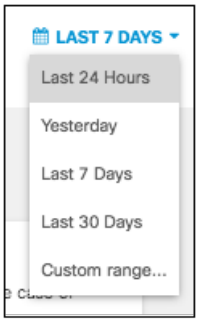
Top Categories Quick View

Describes 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.

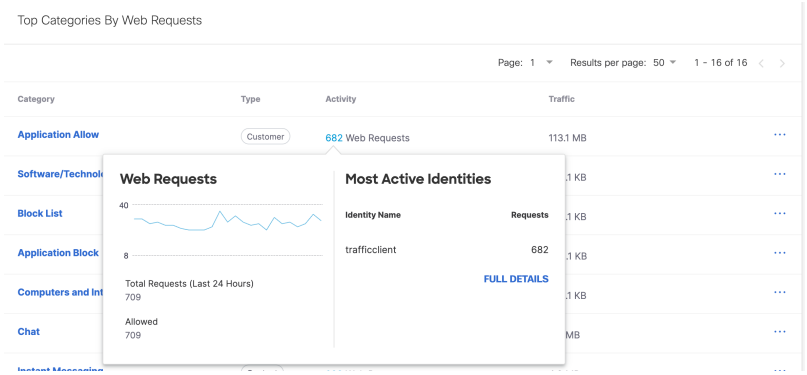
1. Choose a time frame within which to view the quick view details.

   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 in the **Activity** column of the category you wish to examine.

   A modal appears with a graph displaying the total requests of web 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.



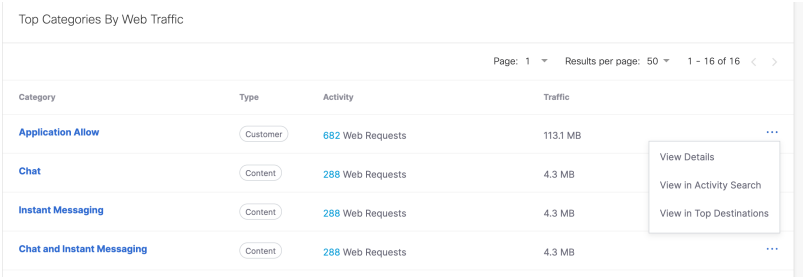
3. Optionally, click **Full Details** to open the Category Details for this category.

View Category in Other Reports

Provides instructions for viewing category in other reports. View Details – Redirects you to that Category Details. View in Activity Search –Redirects you to the Activity Search Report filtered by that category.

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 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.



56 Data Loss Prevention Report

Topics:

- Data Loss Prevention Report

Provides an overview of Data Loss Prevention Report in Cisco Secure Access China. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Data Loss Prevention Report

Describes Data Loss Prevention Report in Cisco Secure Access China. Data violations detected through the Real Time rules are logged as part of the unified Events view of the Data Loss Prevention Report.

Data violations detected through the Real Time rules are logged as part of the unified Events view of the Data Loss Prevention Report.

> **Note**
>
> Administrators with De-identification enabled will continue to see identifiable information in the Data Loss Prevention Report.

Prerequisites

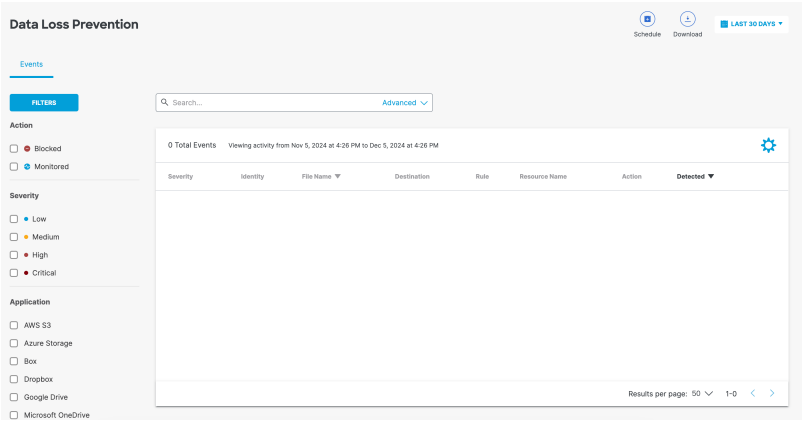
Lists the prerequisites for data loss prevention report. A minimum user role of Read-only. For more information, see Manage Accounts.

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

Events

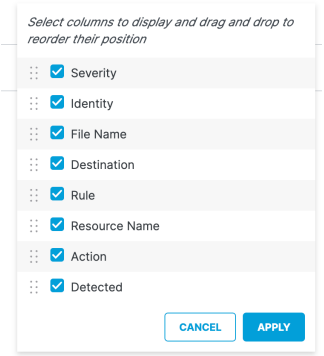
Describes events. Navigate to Monitor > Reports > Data Loss Prevention. Select a time frame to view reports generated in a specific date range. You can also choose a custom date range.

1. Navigate to **Monitor** > **Reports** > **Data Loss Prevention**.



2. 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:
   - **Action** – Whether the content is monitored or blocked
   - **Severity** – The severity of the rule that triggered the event.
   - **Application** – Application for which the DLP rule is applied.
   - **Identity Type** – The type of identity involved in the event.
   - **Application Categories** - The category of the application involved in the event.
4. Click the gear icon to customize and sort the columns of your report.
   - **Severity** –The severity of the rule that triggered the event.
   - **Identity or File Owner** –The identity that made the request.

- **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*.
- **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** – Action triggered by the rule on detecting a violation.
- **Detected** – The date and time of detection.

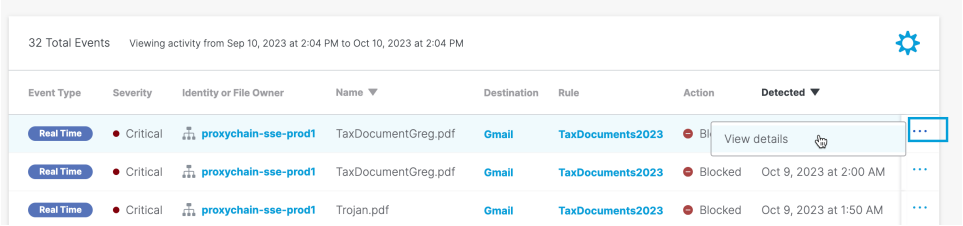


5. Click the action menu icon (three dots) to view further details of an event.

View Details

Provides instructions for viewing details. Click View details. The Event Details window displays some of the same content as the report table, with additional information:.

1. Click **View details**.



2. The Event Details window displays some of the same content as the report table, with additional information:

- **Application**–The application where the file was uploaded or posted.
- **Destination URL**–The URL of the destination for the event.
- **Rule Triggered**–The rule that triggered the event.
- **Classification**–The classification that matched the content found in the event. Clicking the caret displays the excerpts where the matches were found.
- **SHA256 Hash**–The unique SHA256 hash for the file.

Event Details

Detected
Oct 9, 2023 at 2:00 AM

Action
Blocked

Name
TaxDocumentGreg.pdf

Identity
proxychain-sse-prod1

Application
Gmail

Destination URL
mail.google.com

Rule
TaxDocuments2023

Severity
Critical

Classification

TaxDocuments2023

1 Match TaxDocuments2023

XXX....

Content Type
application/pdf

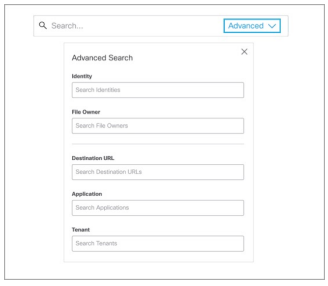
Total Size in Bytes
30.3 KB

SHA256 Hash
5fe79bac153faefeb06459408bec44f...

Copy

Unique Event ID
00f7c83d-a8c2-413b-bfcc-cd2cb3a...

Copy



57 Admin Audit Log Report

Topics:

- Admin Audit Log Report

Provides an overview of Admin Audit Log Report in Cisco Secure Access China, including Export Admin Audit Log Report to an S3 Bucket. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Admin Audit Log Report

Describes Admin Audit Log Report in Cisco Secure Access China. The Admin Audit log records changes that your administrative team has made to your organization's Secure Access China settings.

The Admin Audit log records changes that your administrative team has made to your organization's Secure Access China 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.

Export Admin Audit Log Report to an S3 Bucket

Provides instructions for exporting admin Audit Log Report to an S3 Bucket in Cisco Secure Access China, including Prerequisites and Procedure. It explains the sequence of actions and relevant settings presented in the procedure.

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

Prerequisites

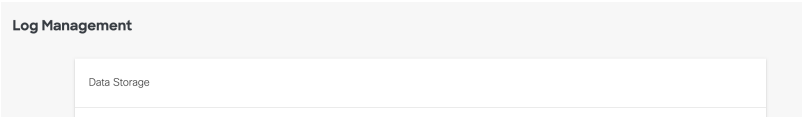
Lists the prerequisites for exporting admin audit logs. Logging is enabled. See Manage Logging. A minimum user role of Read-only. For more information, see Manage Accounts.

- Logging is enabled. See Manage Logging.
- A minimum user role of Read-only. For more information, see Manage Accounts.

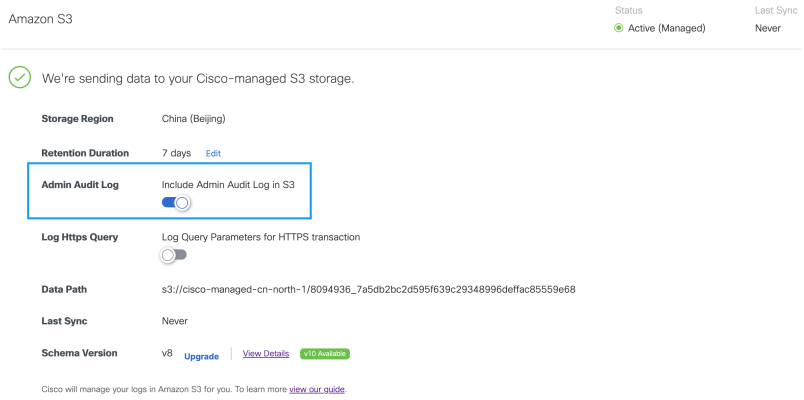
Procedure

Provides instructions for exporting admin audit logs. Secure Access China saves your Admin Audit logs to the auditlogs folder. Navigate to Admin > Log Management.

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 China saves your Admin Audit logs to the auditlogs folder.

Prerequisites

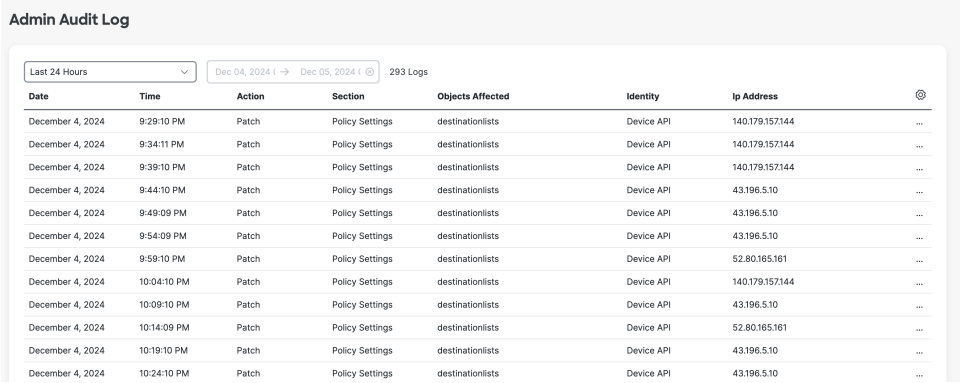
Lists the prerequisites for admin audit log report. A minimum user role of Read-only. For more information, see Manage Accounts.

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

Generate Admin Audit Log Report

Provides instructions for generating admin audit log report. Navigate to Monitor > Management > Admin Audit Log. Click … to view further details of an event.

1. Navigate to **Monitor > Management > Admin Audit Log**.



2. Click **...** to view further details of an event.

