Cisco Umbrella SIG Upgrade Guide to Cisco Secure Access

Cisco Secure Access
Updated November 17, 2026

1 Before You Begin

Topics:

- Is This Guide for You?
- Welcome to Cisco Secure Access
- Upgrade Workflow
- Guidelines and Limitations
- Create a Cisco Security Cloud Control Account
- Activate Upgrade Manager in Umbrella

Read the entire Upgrade Guide before attempting to upgrade from Umbrella SIG to Secure Access.

You must read the entire Upgrade Guide before attempting the upgrade.

You can also watch the Cisco Umbrella SIG to Secure Access Upgrade Walkthrough video, which demonstrates the complete upgrade process step-by-step.

- You must have Full Admin access to perform the ugrade to Secure Access.
- Upgrade time will vary depending on the data and number of policies that are copied over to Secure Access.
- Umbrella will continue to operate during the upgrade, and your organization is always protected.
- We recommend that you upgrade during nonbusiness hours.

Is This Guide for You?

See if you are eligible to upgrade from Cisco Umbrella SIG to Cisco Secure Access.

This guide is for Umbrella multi org customers, with Umbrella SIG Advantage or Umbrella SIG Essentials packages, upgrading to a Secure Access manager organization. Other package types, such as Umbrella for Managed Service Provider (MSP), are not eligible for this upgrade at this time. These packages will be eligible for upgrade in the future.

> **Note**
>
> Secure Access trial licenses are not supported for this upgrade. Upgrading requires an active, paid Secure Access subscription. Using a trial license may lead to expiration and potential disruption of your existing Umbrella dashboard access.

To identify your current Umbrella product, navigate to your managed organization Umbrella dashboard and select **Admin** > **Licensing**.

- **Full eligibility:** You are eligible for the automated upgrade if you have fewer than 50 network tunnels deployed and do not have any Catalyst SD-WAN tunnels (Viptela) deployed.
- **Limited eligibility:** If you have more than 50 network tunnels or have any Catalyst SD WAN tunnels deployed, your access to the automated upgrade is limited.

> **Note**
>
> Please contact your account team to discuss the upgrade options.

> **Note**
>
> Tunnel restrictions apply to the Secure Internet Gateway (SIG) migration process itself, regardless of whether it is standalone or Multi-Org. This means the tunnel limitations outlined in the Limited Availability section apply to SIG migration in both standalone and Multi-Org environments.

> **Note**
>
> For limited eligibility scenarios, you must perform a manual migration using a new instance. Do not use your existing Umbrella instance to claim your Secure Access license for these scenarios, as this may impact your existing Umbrella environment.

This upgrade allows you to begin using Secure Access without impacting the protections and access controls currently managed by Umbrella. Your existing Umbrella policies and rulesets remain in Umbrella and are not migrated to the Access Policy in Secure Access.

The full upgrade, which includes Secure Access internet access rules, will be available soon. Meanwhile, you can start creating private access rules within Secure Access.

To get started, complete all the prerequisites listed under Prerequisites. Once complete, follow the steps to Activate the Upgrade Manager and create your Secure Access account. After activation, you can explore the dashboard and set up private access rules.

If you are downgrading from an Advantage package (such as DNS-A or SIG-A) to an Essentials or lesser package (such as DNS-E or SIG-E) as part of your migration from Umbrella to Secure Access, you will lose access to certain features available in the higher-tier package.

Any features not included in your new Secure Access package will no longer be visible or functional after the migration.

Before proceeding with your downgrade:

- Review your current policies and configurations.
- Disable or remove any features that are not included in your new package to avoid unexpected changes.
- If you are unsure which features are supported in your new Secure Access package, please contact Cisco Support for assistance.

See Cisco Security Service Edge (SSE) Packages for an overview on different packages and covered features.

Welcome to Cisco Secure Access

Experience enhanced security with Cisco Secure Access.

> **Note**
>
> You must read the entire Upgrade guide before attempting to upgrade from Umbrella to Secure Access.

Experience enhanced security with Cisco Secure Access. Step into a new era of security with Secure Access, designed to offer more than just DNS-layer protection. This advanced solution delivers comprehensive protection, integrating the latest SIG Advantage or Essentials features to keep you one step ahead of cyber threats. Whether you're connecting from your office, home, or on the go, do so with confidence knowing you have unparalleled visibility and control.

Why Choose Secure Access?

As a valued Cisco Umbrella SIG customer, we are excited to support you in upgrading to Cisco Secure Access, a comprehensive solution designed to enhance your security posture with advanced access control, seamless connectivity, and robust threat protection. This transition empowers your organization with greater visibility, simplified management, and stronger enforcement of security policies across all users and devices, whether on-premises or remote. We are committed to making your upgrade experience smooth and successful, ensuring you maximize the benefits of Cisco's integrated security platform. Cisco Secure Access provides far more granular, identity- and device-aware control over who can access which specific internal private applications, regardless of where those applications are hosted.

Upgrade Workflow

This is a quick overview on the steps required to complete the upgrade.

Procedure

1. Create a Cisco Security Cloud Control account and a Cisco Security Cloud Sign On account. Follow the steps to Create a Cisco Security Cloud Control Account.

   For more information, see Claim a Subscription in Security Cloud Control Getting Started Guide for Existing Customers.

2. Activate Upgrade Manager
3. Complete all four prerequisite steps in your Umbrella dashboard.
   a. Enable Cisco Security Cloud Sign On for all users.
   b. Update virtual appliances and Update Active Directory Connectors.
   c. Update Chromebooks and Update mobile devices.
   d. Update SAML Metadata XML.
4. Start Upgrade

   Umbrella policies and components are copied to Secure Access as internet access rules and settings that all apply to a single Access policy.
5. Redirect Traffic

   Redirect your organization's identity traffic so that it is steered through Secure Access as sources.
6. Complete Upgrade and Close Umbrella

   Final step is to close your Umbrella account and only use Secure Access.

Guidelines and Limitations

Learn more about the guidelines and limitations when upgrading from Cisco Umbrella SIG to Cisco Secure Access.

Important

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 when you login to Secure Access dashboard > 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.

Table of Contents

- Umbrella Application Settings and Secure Access Application Lists
- Umbrella Policy and Rule Upgrade Behavior
- Umbrella Rulesets and Policy Components in Secure Access as Security Profiles and Internet and SaaS Resources
- Internet and SaaS Resources
- Block Page Bypass
- Content Categories
- Custom User Roles
- Destination Lists
- Domain Management
- Identities as Sources
- PAC Files
- Schedule Settings
- Security Profiles

- Selective Decryption Lists
- Static Keys
- Umbrella Legacy API Keys

Umbrella Application Settings and Secure Access Application Lists

(DNS) Application settings: and Application lists are managed separately in Umbrella and Secure Access. Changes made in one product are not reflected in the other. In Umbrella, a single DNS application setting may include both block and allow actions. In Secure Access, these actions are separated into distinct application lists, each supporting either block or allow for streamlined policy management.

(Firewall) Application settings: in Umbrella might not map directly to Secure Access. Even when category names are the same in both products, the applications assigned to those categories can differ.

For example, the Ad Publishing category in Umbrella includes 296 applications, while the same category in Secure Access includes 340 applications. As a result, the behavior of category-based firewall rules can change after upgrade. Review your internet access rules after upgrade and update them as needed to maintain the intended policy behavior.

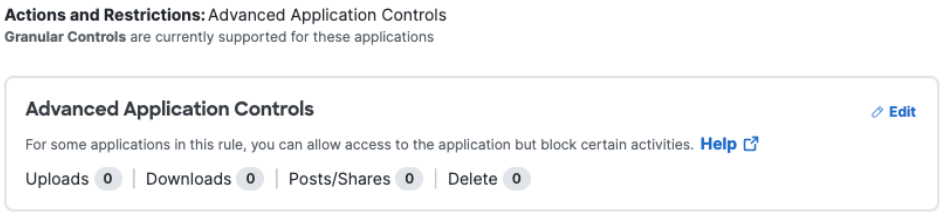
Secure Access does not include all Layer 7 applications available in Umbrella's Firewall policy because some applications are deprecated or discontinued.

Examples include Cisco Jabber, Google Hangouts, and AOL Messenger. For a list of applications that are not in Secure Access, see View Umbrella's Legacy Applications.

If you require access to a specific application, file a request through Cisco New Application Detector Request and contact Cisco Secure Access Support to let them know that you filed a New Application Detector Request. Both requests are required to enable review of the application and its classification in Secure Access.

(Web) Application settings: are synchronized between Umbrella and Secure Access. Changes made in one product will appear in the other.

In Secure Access, Advanced Application Control is located in the Access Policy page. Navigate to **Secure Access Policy** > **DNS Rule** > **Allow** > **Edit** > **Select Destinations** > **Internet Applications** > **Application Lists** > **Advanced Application Controls**. This section only appears if selected rule includes applications that allow granular controls on activities. See, Advanced Application Controls for more information.



Application Categories, Others: In Umbrella Firewall Policy, the categories description, Others may include a certain set of applications. In Secure Access, the category, Others contains a different set of applications. This means the grouping and categorization of applications have changed between the two products.

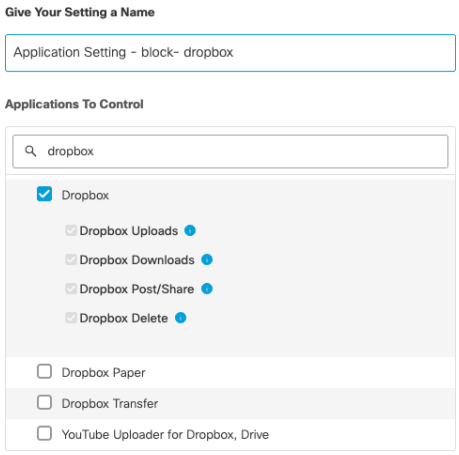
Review your applications carefully in Secure Access. Instead of relying on the category, **Others** as before–select the individual applications you want to control. This ensures your rules are precise and effective.

Some applications you used to find in the category, Others in Umbrella may now be listed under different categories in Secure Access. To add or manage applications: Navigate to: **Secure Access** > **Resources** > **Internet and SaaS Resources** > **Application Lists** and click **+ Add Here**, you can search for and add specific applications to your lists.

For more information on Application Lists in Secure Access, see Manage Application Lists and for category descriptions, see Application Categories.

Important Step Before Closing Umbrella Account: After moving your Umbrella traffic to Secure Access and just before completing the final step to close your Umbrella account in the Upgrade Manager, we recommend deselecting

all Advanced Application Controls in your Umbrella dashboard. This ensures there is no overlap in enforcement policies between the two products.



Umbrella Policy and Rule Upgrade Behavior

- Umbrella DNS, Web, and Firewall policies that do not include identities are not copied to Secure Access.
- Umbrella DNS, Web, and Firewall policies that are disabled are copied over to Secure Access and remain disabled.
- Secure Access does not support Intelligent Proxy. To replicate this level of DNS security we recommend downgrading your Secure Access subscription to Secure Access DNS Defense, which is a comparable level of DNS-layer protection, or upgrade to Secure Access and implement the Secure Access Secure Web Gateway (SWG) , where you can configure full web proxy capabilities that offer a more comprehensive security posture.

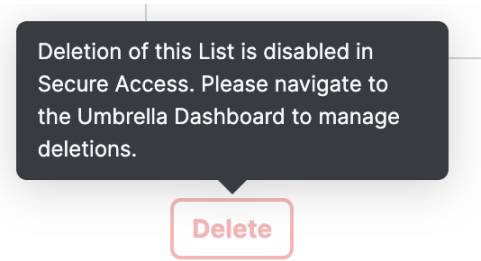
Umbrella Rulesets and Policy Components in Secure Access as Security Profiles and Internet and SaaS Resources

- **Rulesets Become Security Profiles**: After you complete the Start Upgrade step, your existing Umbrella Rulesets will automatically become Security Profiles in Secure Access.
- **Policy Component Restrictions**: While the Upgrade Manager is active, any Umbrella policy components shown in Security Profiles and Internet & SaaS Resources cannot be deleted in Secure Access.

Internet and SaaS Resources

Resources listed on the Internet and SaaS Resources page are reusable components (sometimes known as "objects") that can be used as destinations when configuring internet access rules. Internet and SaaS resources include:

- Destination Lists
- Application Lists
- Content Category Lists
- Tenant Controls



Block Page Bypass

Block Page Bypass Users and Codes are not copied over. For more information on the Secure Access feature, see Notification Pages.

Content Categories

Legacy Umbrella Content Categories will be upgraded to their equivalents in Secure Access. For more information see Available Content Categories.

After the upgrade, Umbrella content category name's in Secure Access will display a **(Web)** or **(DNS)** prefix. You can edit this prefix after the upgrade is complete and the Umbrella account is closed.

During the upgrade, the Delete button is disabled for DNS Content Categories; however, you can delete web content categories.

In Secure Access there is a category called, **Uncategorized** that is available in the web content categories, but not available for DNS content categories.

Custom User Roles

Custom user roles are not copied over. Secure Access has three roles:

- Full Admin
- Read-Only
- Security Administrator

For more information see, Manage Accounts.

Destination Lists

In Umbrella, if you have more than 250,000 destinations, you will not be able to upgrade to Secure Access until you reduce the number of destinations below this limit.

In Secure Access, destination lists are searchable by Destination List Name only, not by comments.

During the upgrade, the Delete button is disabled for DNS destination lists; however, you can delete web destination lists.

Secure Access allows you to add IPv6 addresses to destination lists. This feature is not supported in the Umbrella dashboard. If your traffic continues to route through Umbrella, IPv6 addresses may appear in Umbrella destination lists, but these destinations will not be evaluated.

After the upgrade, Umbrella destination lists in Secure Access will display a **(Web)** or **(DNS)** prefix. You can edit this prefix after the upgrade is complete and the Umbrella account is closed.

Domain Management

Find the internal domain allow list by navigating to **Connect > End User Connectivity > Internet Security > Traffic Steering**.

Identities as Sources

When upgrading Umbrella DNS policies, web rules, or firewall rules to Secure Access, any policy or rule with more than 250 identities will cause the upgrade to fail. Secure Access supports a maximum of 250 sources per rule.

In Secure Access, the 250 source limit applies to the number of source entries in a rule, not to the total number of users within those entries. Each internet access rule can include up to 250 sources, counting both preconfigured source objects and sources entered directly in the rule.

For example:

- One user counts as one identity/source.

- One group counts as one identity/source.
- One network, tunnel group, or other source object counts as one identity/source.

This means that if you add a group to a rule, the group counts as a single source entry even if it contains multiple users.

Before the Upgrade:

Review your Umbrella policy or rule with more than 250 identities. If needed, you can:

- Remove any identities that are no longer required.
- Duplicate the policy or rule and remove some identities from each copy, effectively splitting the original rule into multiple smaller ones, each adhering to the 250 source limit.

PAC Files

Secure Access utilizes its own PAC (Proxy auto-configuration) files and does not support PAC files hosted by Umbrella.

To successfully upgrade to Secure Access, update your Secure Web Gateway (SWG) traffic:

1. **Update PAC File References**: Ensure your networks are configured to use the Secure Access PAC files instead of Umbrella-hosted PAC files.
2. **Download the Default PAC File**: You can download the default Secure Access PAC file by navigating to Manage PAC Files.
3. **Custom PAC Files Update Process**:
    - If you use custom Umbrella PAC files, first download them from the Umbrella Web Policy interface.
    - Update the proxy Fully Qualified Domain Name (FQDN) in each file to point to the Secure Access proxy FQDN.
    - Upload your modified PAC files to Secure Access by following the steps here, Upload Custom PAC Files to Secure Access.

Secure Access, has a different PAC file compared to the Umbrella-hosted PAC file and should be updated to include your network. To reuse custom Umbrella PAC files, download these files from Umbrella and then upload them to Secure Access. You also need to update the proxy FQDN in the custom PAC files before uploading to Secure Access.

In Secure Access navigate to **Connect > End User Connectivity > Internet Security > Deployment Options > Windows and macOS > View custom PAC files > Add custom PAC file**. For more information, see Manage PAC Files in Cisco Secure Access Help.

Schedule Settings

If you created a time schedule directly inside an Umbrella policy (not as a reusable schedule in Schedule Settings), that schedule remains embedded in the Umbrella policy and does not appear under Umbrella's Schedule Settings. However, once the upgrade begins, these unique schedules will appear in Secure Access as reusable schedules in Enablement Schedule. The schedule name will include the original Umbrella policy name (example, Inline Schedule For Rule 2) so you can identify its origin. These schedules will not appear in Umbrella's Schedule Settings for reuse.

Schedules Created Post-Upgrade:

Any schedule created in Umbrella's Schedule Settings after the upgrade will also appear in Secure Access Enablement Schedule. If a custom schedule is created directly in an Umbrella policy after the upgrade, it will not appear in the Enablement Schedule.

Secure Access Enablement Schedule have Start and End dates. When Umbrella schedules are transfer over, they will have a Start date but no End date. We recommend to review these schedules by navigating to **Resources > Settings > Enablement Schedule**.

Security Profiles

A Cisco Secure Access Security profile is a reusable component that you can use in the rules for the Access policy. A Security profile for internet access includes security controls and other settings such as acceptable use controls that you configure as a set.

> **Attention**
>
> While the Upgrade Manager is in progress, some security profiles are shared between the two platforms. To avoid any unintended changes to your policies, do not edit or delete any existing security profiles until the upgrade is finished. You can still create and manage new security profiles during this time–only existing ones are temporarily restricted.

Security Profiles include:

- Do Not Decrypt List
- SSO Authentication
- Security and Acceptable Use Controls
- End-User Notifications

For more information, see Security Profiles for Internet Access.

Selective Decryption Lists

What's Changing in Name:Umbrella's **Selective Decryption Lists** are now called **Do Not Decrypt Lists** in Secure Access.

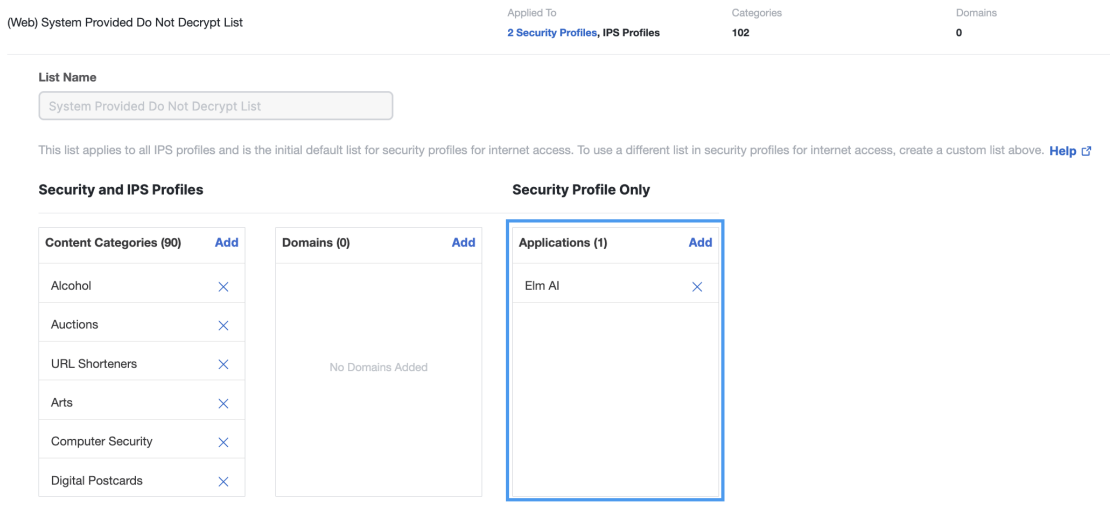
List Prefixes After Upgrade:After upgrading, your existing Umbrella lists will appear in Secure Access with a **(Web)** or **(DNS)** prefix. You can edit these prefixes once the upgrade is complete and your Umbrella account is closed.

Editing Restrictions During Upgrade:While the Upgrade Manager is running, you cannot make changes to Do Not Decrypt Lists linked to policies created in Umbrella. This restriction is lifted after you close your Umbrella account.

Content Categories Expansion:Umbrella has 102 content categories in its Selective Decryption Lists. Secure Access expands this to 144 categories. If you had all 102 categories selected in Umbrella, you will see all 144 categories selected after upgrade. For more information, see Available Content Categories in our Cisco Secure Access Help.

Application Visibility Behavior:

- **For Customers Upgrading from Umbrella**:You will continue to see the Applications List in the **System Provided Default Do Not Decrypt List**, just like in Umbrella. This means your existing behavior of adding applications to the default list remains unchanged. You can find this list in Secure Access under:**Secure > Settings > Do Not Decrypt Lists > System Provided Do Not Decrypt List**.
- **For Customers Directly Purchasing Secure Access**:The System Provided Default Do Not Decrypt List does not display an Applications List. This is the default behavior for new Secure Access customers who did not upgrade from Umbrella.



To learn more, see Important Information About Do Not Decrypt Lists in Secure Access Help.

Static Keys

In Secure Access, Static Key is found by navigating to **Connect > Users, Groups, and Endpoint Devices > Users > Configuration Management > Integrate Directories > IdP**. For more information, see Configure Identity Providers.

Umbrella Legacy API Keys

Legacy API keys will not transfer to Secure Access since Umbrella API was released in 2022. In Secure Access you continue to use API Keys, KeyAdmin Keys, and Static Keys. For more information see, Manage API Keys and Secure Access API Authentication.

View Umbrella's Legacy Applications

Lists legacy, deprecated, or discontinued Layer 7 applications from Umbrella Firewall policy that are not supported in the Secure Access application catalog.

Cisco Secure Access does not support the full suite of Layer 7 applications available in the Cisco Umbrella Firewall policy. Certain legacy, deprecated, or discontinued applications—such as Cisco Jabber, Google Hangouts, and AOL Messenger—are excluded from the Secure Access application catalog.

Table 1: List of applications not supported in Secure Access

Umbrella's Legacy Applications
Active Directory
ATEXSSTR
AOL Instant Messenger Text Chat
AOL Instant Messenger Audio
AOL Instant Messenger File Transfer
AOL Instant Messenger Video
AOL Protocol
Apple iOS updates
Apple Location Services
Apple Push Notification Service
AppleTV updates
Ares
Ariel1
asa-appl-proto
Audio Over HTTP
auth
auth-service
Ayiya IPv6 Tunneled
Babelgum

Umbrella's Legacy Applications
Backpage.com
Backup service
Systems and network monitoring tool
Binary over HTTP
World of Warcraft
Backroom SATNET Monitoring
Call of Duty
Control And Provisioning of Wireless Access Points Data Protocol
Coherent File Distribution Protocol
Common Internet File System
Cisco Collaboration Audio
Cisco Collaboration Control
Cisco Collaboration Video
Cisco Controller
Cisco IP Camera
Cisco IP SLA
Cisco Jabber Audio
Cisco Jabber Video
Cisco Media Audio
Cisco Media Video
Cisco NAC
Cisco NMSP
Cisco Phone Audio
Cisco Phone Control
Cisco RTMT
Cisco SD-WAN IPSec
cisco smart probe
Cisco Spark Audio
Cisco Spark Media
Cisco Spark Video
Citrix Audio
CMIP/TCP Agent
Conferencing Server
Conferencing

Umbrella's Legacy Applications
Connected Backup
Consumer Cloud Storage
Internet telephony tool
CORBA Internet Inter-ORB Protocol
Computer Protocol Heart Beat
Computer Protocol Network Executive
DameWare Mini Remote Control
Dantz Retrospect
DB service
DDM-Remote Relational Database Access
DECLadebug Remote Debug Protocol
Decvms-sysmgt
Desknet's
DHCP-Failover 2
DHCPv6 Client
DHCPv6 Server
Distributed Hash Table
errlog copy/server daemon
ESCP
Facebook Audio Streaming
Facebook Media Streaming
fasttrack-static
Filemaker relational database application
Filetopia
Flash Myspace
Flash Yahoo
Fring
Fring Video
Fring VoIP
File Transfer [Default Data]
Game-spy Online Gaming
generic-device
Genrad Mux
ggf-ncp

Umbrella's Legacy Applications
GhostSurf Anonymous Internet Surfing Application
GraphOn Login
Google Downloads Services
Google Services Audio
Google Services Media
Google Services Video
Grid FTP
GSS-HTTP
Google Talk Chat
Google Talk File Transfer
guruguru
H.245
Hangouts Audio
Hangout Chat
Hangout File Transfer
Hangouts Media
Hangouts Video
HELLO Port
hopopt
Hotmail Email Services
HP Performance Data Managed Node
HTTP Alternate
Local Network HTTP
HTTP Management
HTTP RPC Ep Map
IBM-DB2
ICQ File Transfer
IDPR Control Message Transport Protocol
IEEE MMS
Internet Audio Streaming Web Apps
Internet Video Streaming Web Apps
IP Messenger
Sun IPC server
Internet Packet Core Utility

Umbrella's Legacy Applications
IP-within-IP Encapsulation Protocol
IPv6 encapsulation
IPX in IP
Internet Security Association and Key Management Protocol
Isatap IPv6 Tunneled
iscsi-target
ISO Transport Service Access Point
ISO Transport Class 2 Non-Control over TCP
iTunes Media
Jabber Audio
Jabber Video
Kazaa2
KNET/VM Command/Message Protocol
Kuro
legent-1
Live Meeting
LiveStation
Locus PC-Interface Net Map Ser
MacOS Server Admin
Magenta Logic
Mail Service
Maplestory
Masqdialer
MATIP Type A
Memcomm
Megavideo
Meta5
Micro Focus COBOL
Microsoft-DS
MIT Dover Spooler
MPM [default send]
MS RPC IIS
Skype for Business (MS-Lync) Audio
Skype for Business (MS-Lync) Control

Umbrella's Legacy Applications
Microsoft Lync Media
Skype for Business (MS-Lync) Video
Microsoft Office Communications Server and File Transfer
Microsoft Remote Procedure Call
MS-RPC System Management Server
Microsoft SQL Monitor
MS Teams App Sharing
MS Teams Audio
MS Teams Media
MS Teams Video
Remote Desktop Protocol
Microsoft Global Catalog with LDAP/SSL
msg-auth
Windows Live Messenger File Transfer
Windows Live Messenger Video
My Jabber FT
NAMESERVER
nCube License Manager
net-assistant
NetApp SnapMirror
Network Basic Input/Output System
netrjs-1
netrjs-2
netrjs-3
netrjs-4
Windows Media
IBM NetView DM/6000 Server/Client
netviewdm3
networking-gnutella
NICNAME/WHOIS
notes
NovaStor Backup
NSW User System FE
OCS Amu

Umbrella's Legacy Applications
IBM Operations Planning and Control Start
IBM Operations Planning and Control Track
Microsoft System Center Operations Manager
Oracle Business Intelligence
Oracle E-Business Suite - Un-encrypted Traffic
Parsec Gameserver
passgo
passgo-tivoli
Perfect Dark
Ping
Proxy Server
Qbik GDP
Ringcentral Audio
Ring Central Media Protocol
Ringcentral Video
rsvp-encap-1
rsvp-encap-2
Real Time Messaging Protocol Encrypted
Real Time Messaging Protocol Tunneled
Sirius Systems
SCCP User Adaptation
Scoi2odialog
ftp protocol control over TLS/SSL
DEPRECATED, traffic will not match
Internet Message Access Protocol over TLS/SSL
Secure Simple Mail Transfer Protocol
telnet protocol over TLS
secure-vmtp
Internetwork Packet Exchange Protocol
Cray SFS config server
SGMP-TRAPS
Share
Secure SIP
Sixtofour IPv6 Tunneled

Umbrella's Legacy Applications
Slack Media
smartsdp
Songsari
Soulseek
IBM Informix SQL Interface
Sqli
sqlnet
REAL SQL Server
SRS Send
Local Network SSL
Statistical Conference Audio
Statistical Conference Video
Statistical Download
Statistical Peer-To-Peer
Statistics Server
STUN over TLS
SynOptics SNMP Broker Port
TAC News
tcp tunneled over dns
Tobit David Replica
Tobit David Service Layer
remote access and desktop sharing
Telepresence Audio
ticf-2
Timeserver
tlisrv
tnETOS
Tor
Traceroute Linux
Computer Supported Telecomunication Applications
Tunnel HTTP
List Processor
Unknown
Unix time

Umbrella's Legacy Applications
Ventrilo
Viber
Video Over HTTP
Virtual Places Chat
VNC over HTTP
WAP session service
WAP Secure Session Service
Waste
Web Analytics
WebRTC Audio
WebRTC Video
Webex Audio
Webex Video
whois++ Service
Wi-Fi Calling
Windows Update
eXtensible Data Transfer Protocol
Xerox
Xerox Internet Datagram Protocol
Yahoo VoIP Messenger
Art-Net
Local Operating Network
MikroTik Neighbor Discovery Protocol

Known Caveats

Warns that identity-based policy enforcement in Umbrella may not behave as expected after identity provider changes and before traffic redirection is complete, so policy testing should wait until redirection finishes.

- **Policy enforcement during migration:**

  During the migration process, an intermediate phase exists between updating your identity provider configuration and completing traffic redirection. In this phase, authentication via your identity provider may succeed, but identity-based policy enforcement in Umbrella may not function as expected. This can result in traffic that was previously blocked or warned being allowed. Do not attempt to validate policy enforcement until traffic redirection is fully completed.

Create a Cisco Security Cloud Control Account

Cisco Security Cloud Control is a new security platform that allows you to manage your security products and achieve security outcomes from a single integrated interface.

Before you begin

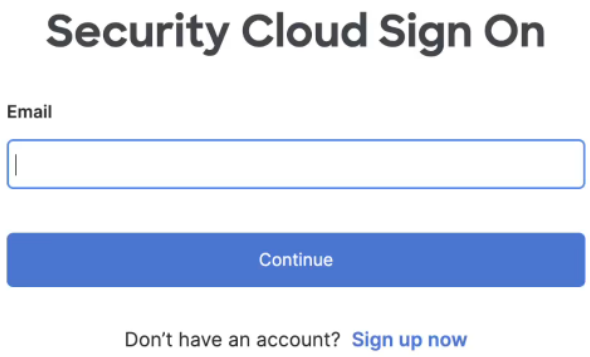
Cisco Security Cloud Control (SCC) provides centralized visibility and management for Cisco's security products. To upgrade from Umbrella SIG to Secure Access, create your SCC account after receiving the Welcome email with your claim code.

As part of this process, you'll create a Security Cloud Sign On account. Security Cloud Sign On is the solution to access multiple Cisco security and cloud services with one set of credentials.

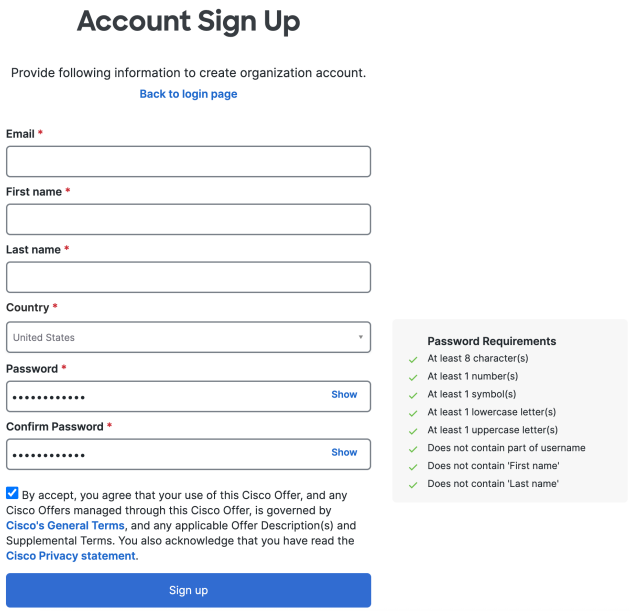
Finally, you'll need to setup multifactor authentication for added security, and we recommend using Duo.

Procedure

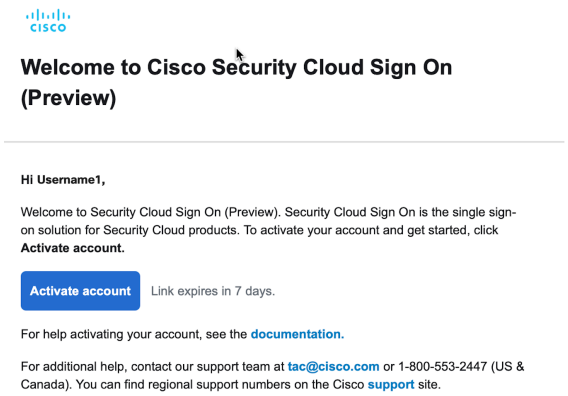
1. Create a Security Cloud Control (SCC) account by creating a Security Cloud Sign On account.
2. Click **Sign up now** to create a Security Cloud Sign On account.



3. Enter your information on the Account Sign Up page.

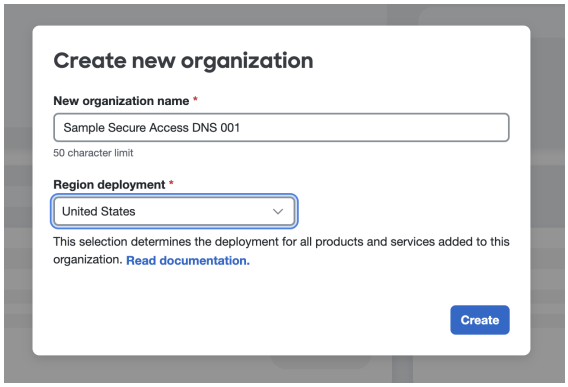


4. Look for the verification email to activate your account. Link expires in 7 days.



5. Enroll in multifactor authentication. We recommend using Duo
6. Add users to SCC, see Role-Based Access Control in an Organization.

   Add all Umbrella admins to avoid locking them out of Umbrella. All users must enroll in Duo unless you configure Identity Service Provider.
7. Follow these steps to integrate your Identity Service Provider.
8. Create a new organization name.



   The name of your new Secure Access organization should be the same as your Umbrella organization. See, Create an Organization for more information about organizations and regions.

   Select any region from the dropdown menu. The product is globally available, so your selection won't impact its functionality.

What to do next

Follow the next steps to add Upgrade Manager to your Umbrella dashboard.

Activate Upgrade Manager in Umbrella

This topic explains how to activate Upgrade Manager in Umbrella and create your Secure Access account.

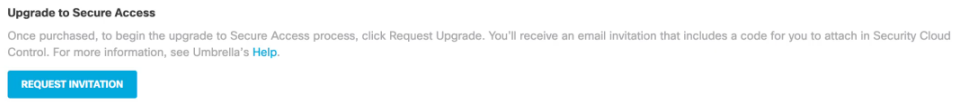
Before you begin

- **The admin activating the Upgrade Manager in Umbrella must use the same email address to create the Security Cloud Control (SCC) account.** Using a different email will prevent linking your Umbrella organization to the correct SCC account–causing the upgrade to fail and may create a new Secure Access organization without linking your Umbrella organization.

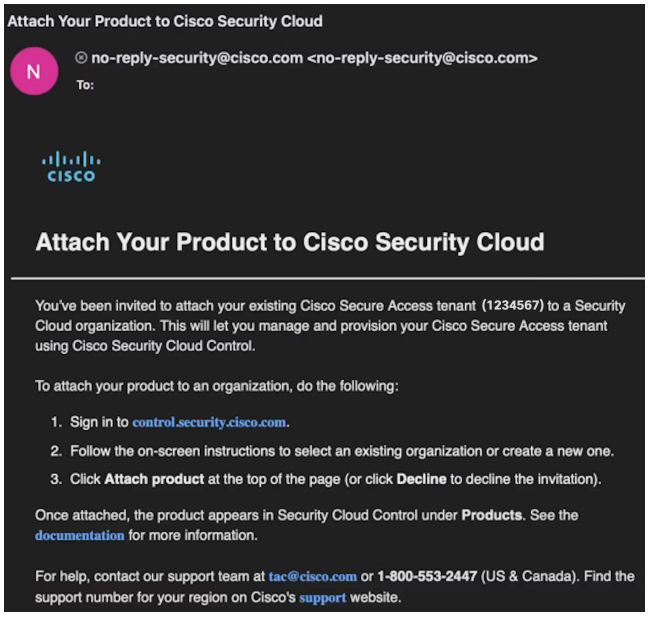
- The admin must receive a welcome email from Cisco Security Cloud containing a unique subscription claim code to upgrade to Secure Access.
- The admin who receives the subscription claim code is responsible for completing the subsequent steps to activate the Upgrade Manager in Umbrella.

Procedure

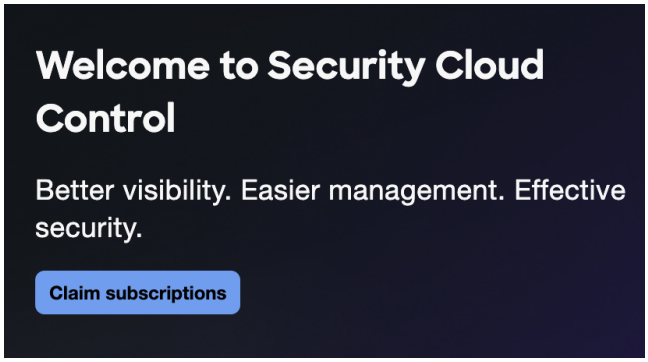
1. Login to your Umbrella account.
2. Navigate to **Admin > Licensing > Upgrade to Secure Access** and click **Request Invitation**.



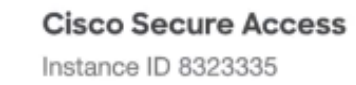
3. Check your email for an invitation to **Attach Your Product to Cisco Security Cloud**.



4. Click the link in your email to login to your Security Cloud Control account. The Umbrella admin activating the Upgrade Manager must use the same email address to create the Security Cloud Control account.
5. Click **Claim subscriptions**.

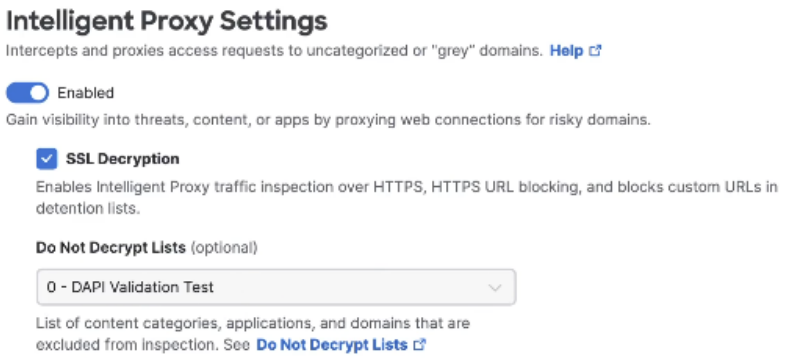


6. Check that **Cisco Secure Access Instance ID** is the same as your Umbrella organization ID.

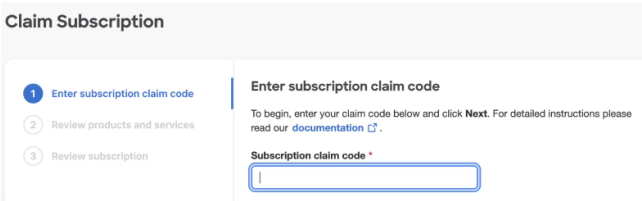


7. Click **Attach product** then click **Attach** to attach your Umbrella organization to the Secure Access instance.

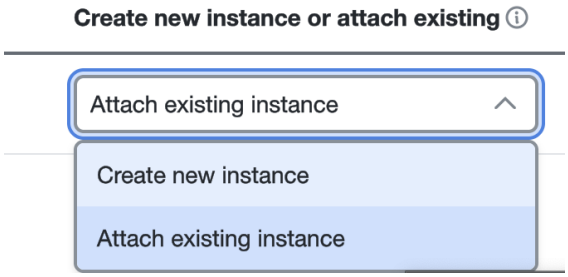
   This action cannot be undone.



8. Click **Claim subscription** and enter your subscription claim code.



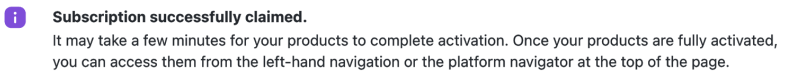
9. Click **Next** to begin the claim subscription workflow.
10. In the drop-down list select **Attach existing instance**.



Do not create a new instance, as doing so will not upgrade or link your existing Umbrella organization to Secure Access. Instead, it will create a separate Secure Access instance with a new organization ID that is not connected to your current Umbrella organization.

11. Click through **Claim** to associate the subscription details, including subscription ID and product licenses with your new Secure Access organization.

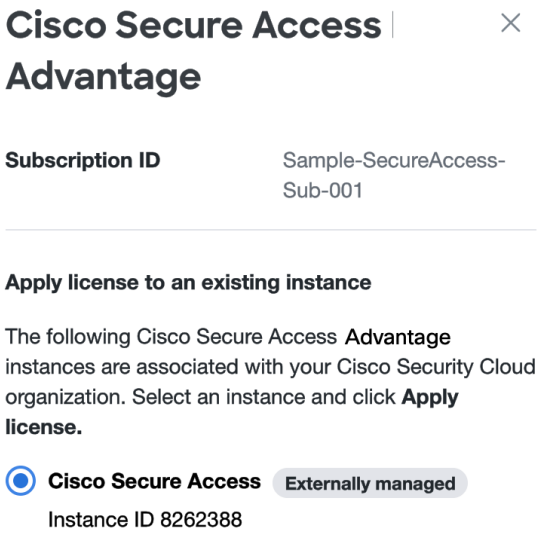
    Subscription successfully claimed. It may take a few minutes for your product to complete activation. Once your products are fully activated, you can access them from the left-hand navigation or the platform navigator at the top of the SCC page.



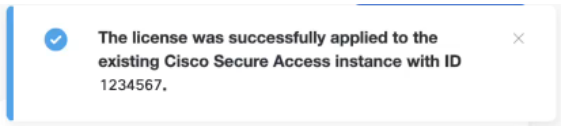
12. In **Product and service activation status**, click **Action required**.



13. Click **Apply license** to link Cisco Secure Access to your existing Umbrella account.



a) A notification informs you that your license was successfully applied to the Cisco Secure Access instance.



14. Login to Umbrella dashboard to see **Upgrade Manager** in the left-hand navigation.



15. Click **Upgrade Manager** to begin the process of completing the necessary prerequisites before creating your new Secure Access organization.

    Next steps, see Prerequisites for Upgrade and then Start Upgrade to create your new Secure Access organization.

2 Prerequisites for Upgrade

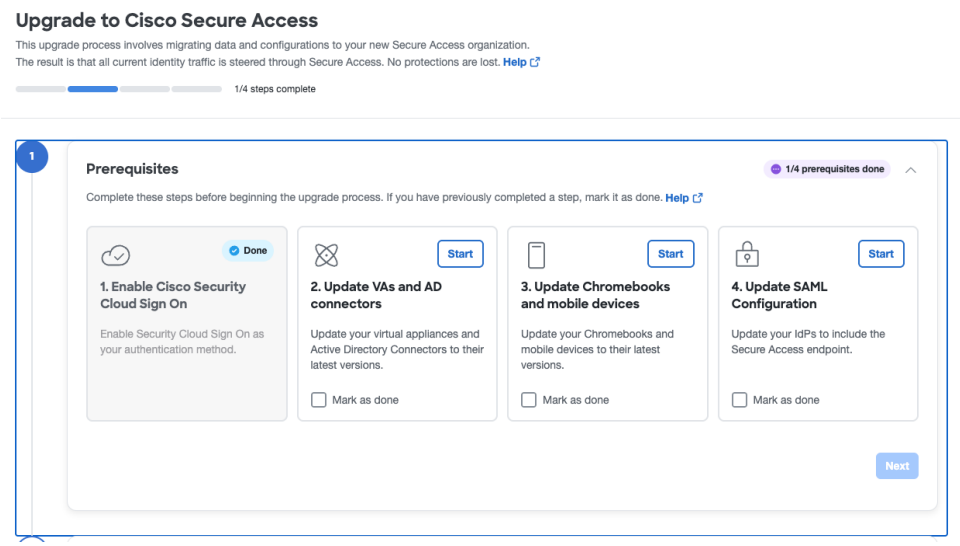
Topics:

- Enable Cisco Security Cloud Sign On
- Overview of Virtual Appliance Updates
- Overview of Active Directory Connector Updates
- Update Chromebooks
- Update Mobile Device
- Overview to Update SAML Metadata XML

You must complete all the prerequisites before upgrading to Secure Access.

The prerequisite steps listed below need to be completed before you can begin the next step to Start Upgrade.

1. Enable Cisco Security Cloud Sign On.
2. Update Virtual Appliances and Update Active Directory Connectors.
3. Update Chromebooks and Update Mobile Devices.
4. Update SAML Metadata XML.



Note

Add any additional registered network devices using the legacy API before upgrading. For guidance on setting up network devices with legacy APIs, see the Hardware integration section at https://securitydocs.cisco.com/docs/umbrella-sig/olh/152032.dita.

Enable Cisco Security Cloud Sign On

Prerequisite: Enable Cisco Security Cloud Sign On

Cisco Security Cloud Sign On (SCSO) allows you to access Cisco Security products with one set of credentials from any device. Security Cloud Control is the platform where you manage those products and achieve security outcomes through a single integrated interface, while Cisco Security Cloud Sign On provides seamless authentication across them.

As part of the upgrade to Secure Access, Umbrella admins must enable Cisco Security Cloud Sign On and create Security Cloud Control accounts before completing SAML authentication.

This is a required prerequisite for Umbrella admins. Complete this step before the upgrade helps ensure that administrators can access Security Cloud Control while the upgrade is in progress and prevents admin lockout from the Umbrella organization.

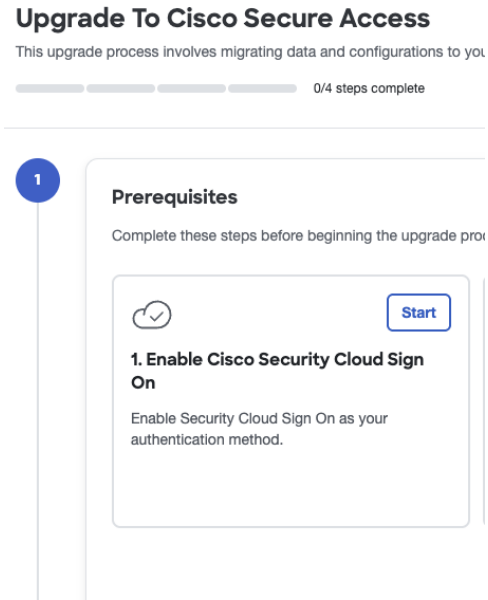
If your organization already uses an identity provider (IdP) with Umbrella, Cisco recommends configuring Cisco Security Cloud Sign On to use that same IdP when possible. Do not remove your existing Umbrella IdP configuration unless explicitly required.

Before proceeding, verify that your Umbrella admin accounts also exist in Security Cloud Control, either as manually created users or as users provisioned through your IdP. To avoid access issues, use the same administrator email address in both Umbrella and Security Cloud Control.

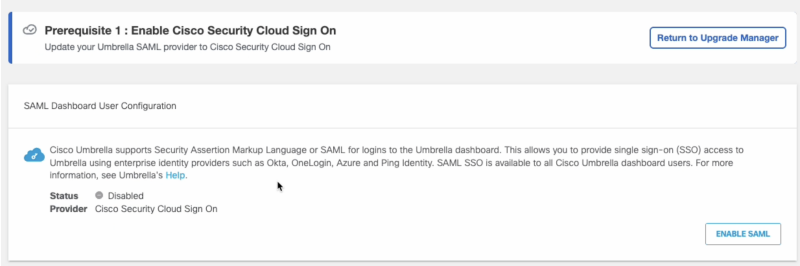
For more information, see Overview of Security Cloud Sign On in our Security Cloud Control Getting Started Guide for Existing Customers.

Procedure

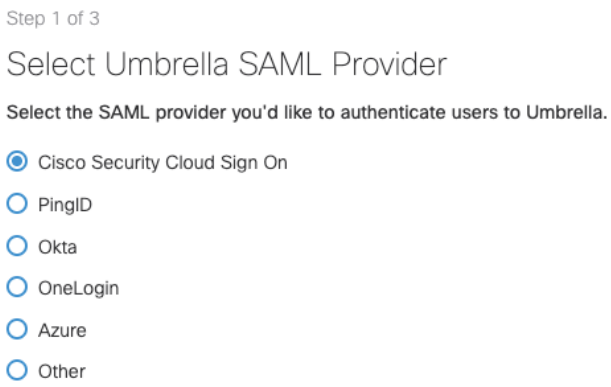
1. Navigate to **Upgrade Manager**. Click **Start** for **Enable Cisco Security Cloud Sign On**.



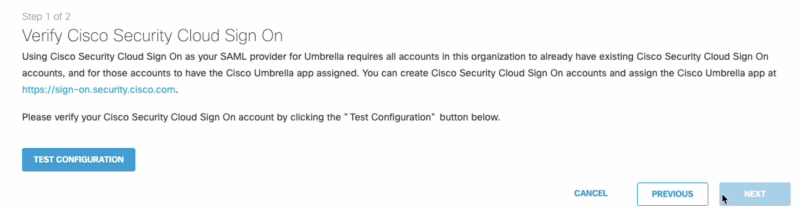
2. Click **Enable SAML**.



3. Click Cisco Security Cloud Sign On to create a SCSO account for all users in Umbrella. In the following window click **Sign up now**. For more information about creating accounts, see Invite a User.

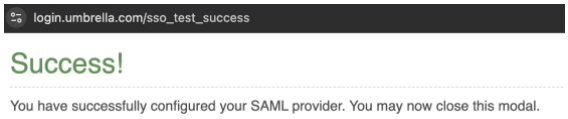


4. After the accounts are created, return to **Upgrade Manager > Prerequisite > Enable Cisco Security Cloud Sign On > Start**. Click **Test Configuration**.

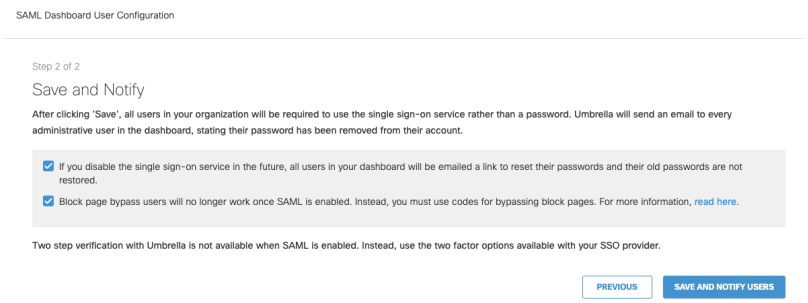


The **Test Configuration** must be performed and successful for the set-up to complete.

Once the authentication is complete, a success modal appears.



5. Click **Next**. Check both boxes to acknowledge the information and click **Save and Notify Users**.
   - This single sign-on service will now be required going forward.
   - Umbrella will send an email to all dashboard users (not end-users) and a message to all admins in the dashboard to inform them of the mandatory single sign-on (SSO) and that passwords are no longer accepted.
   - If SSO is disabled in the future all users will be emailed a link to reset their passwords as old passwords will not be accepted.
   - Block page bypass users will no longer function once SAML is enabled.



6. Click **Return to Upgrade Manager** and **Enable Cisco Security Cloud Sign On** step will change from Start to **Done**.



What to do next

Follow the next steps to check that your Virtual Appliances and Active Directory connectors are up to date.

After you enabled Cisco Security Cloud Sign On:

- Cisco Security Cloud Sign On becomes the required sign-in method for Umbrella dashboard users going forward.
- Umbrella sends an email to all dashboard users (not end-users) to inform them of the mandatory single sign-on (SSO) and that passwords are no longer accepted.
- If SSO is disabled later, all users will receive an email with a link to reset their passwords because previous passwords are no longer valid.
- Block page bypass users no longer function once SAML is enabled.

Overview of Virtual Appliance Updates

Check that your virtual appliances are updated.

New virtual appliance (VAs) software versions become available automatically and are usually applied without any intervention required. To ensure the high availability of DNS services, you must have two VAs running for automatic updates to take place.

Both the connector and the VA are capable of automatic updates. To download updates, these components require access to the following URLs:

- 443 (TCP) to disthost.opendns.com
- 443 (TCP) to disthost.umbrella.com

If you would like to find out more about upcoming versions, including release notes, see Service Updates. Click **Follow** to receive update notifications.

Update Your Virtual Appliance

Virtual Appliance updates are usually automatically updated but can be manually updated.

We recommend updating your VAs to v3.7.1 (or above) and configure Enhance Authentication.

In order for new versions to be automatically installed on the VAs, we require that a **minimum of two VAs be installed**. You must have two VAs in place so that there is no downtime or interruption in service during the update process.

Performing an "in-place" manual update of a VA results in up to **15 minutes of downtime**, during which you will not be able to perform DNS queries on the network and effectively will not have internet service.

Follow these steps to update your Virtual Appliances:

Procedure

1. Update Virtual Appliances
2. Configure Authentication for Virtual Appliances

Overview of Active Directory Connector Updates

Ensure that your Active Directory Connectors are updated.

The Cisco Active Directory (AD) Connector integrates with Umbrella to provision users and groups from your organization. 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 Umbrella.

Configure Automatic Updates on Active Directory Connectors

These are the steps to set up automatic updates for AD Connectors.

Schedule the date and time that Umbrella updates the Cisco AD Connector software on your deployed AD Connectors. When scheduled, Umbrella checks if the AD Connector has the latest version of the software. If a new version is available, Umbrella removes the installed AD Connector software from your systems and deploys the latest version of the AD Connector.

Before you begin

You must have Full Admin access in Umbrella.

Procedure

1. Navigate to **Deployments > Configuration > Sites and Active Directory** and click **Settings**.
2. Navigate to **Active Directory Connector Auto-Upgrades**, and click **Edit**.
3. 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, Umbrella attempts to redeploy the AD Connectors with the latest version of the software.

4. 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**.

Upgrade Active Directory Connectors Manually

Provides steps for manually upgrading an outdated Active Directory Connector in Umbrella, from locating the connector and confirming the available version to monitoring upgrade progress.

Before you begin

You must have Full Admin access in Umbrella.

Procedure

1. Navigate to **Deployments > Configuration > Sites and Active Directory**.
2. In the **Version** field, click the red exclamation symbol for the AD connector with the outdated version.

   A confirmation message appears indicating the available AD connector version to upgrade and a warning about few minutes of downtime during the AD connector upgrade.
3. Click **Upgrade**.

   The manual upgrade in progress is indicated by the running clock symbol in the **Version** field.

Update Chromebooks

Check that all Chromebooks and Cisco Chromebook clients are updated.

Ensure that all Chromebook Operating Systems and Chromebook clients are updated. Google is responsible for updating the software in Chromebooks. When Cisco updates the Cisco Security for Chromebook client in the Chrome Web Store, the upgrade is automatically pushed by Google to all the Chromebooks. This process can take several hours. See Chromebook Client FAQs for more information.

Procedure

1. Update Chromebook Operating Systems to version 122 or above.

2. Update Cisco Security for Chromebook client to 2.1.1 or above.

Update Mobile Device

Check that all mobile devices and clients are up to date before attempting the upgrade.

Ensure that all mobile devices and clients are up to date before attempting the upgrade. You can proceed to the next step if you have no mobile devices or clients set up.

For more information, see Managed Android Device

For more information, see Managed iOS Device

For more information, see Unmanaged Mobile Device Protection

Overview to Update SAML Metadata XML

This is the last step in the prerequisites – to update the end-user SAML configuration in your IdP.

If you have SAML integrations set up in Umbrella, you must update your IdPs to include Secure Access endpoints to prevent user lockouts. Any changes made to your SAML configuration in Umbrella will also appear in Secure Access. If you delete SAML in Secure Access, the configurations will be deleted in the Umbrella dashboard.

Updated Service Provider SAML Metadata

- Entity ID–saml.fg.id.sse.cisco.com
- Entity URL–fg.id.sse.cisco.com/gw/auth/acs/response

Manual Import

If your identity provider (IdP) does not allow you to upload the Secure Access Metadata XML file and instead requires you to manually enter the information, then review these topics:

For Umbrella, see Provision Identities Through Manual Import.

For Secure Access, see SAML Certificate Renewal Options.

Download SAML Metadata XML

This topic goes over the steps to download the Secure Access SAML Metadata XML to update your IdP to integrate with Secure Access (SAML).

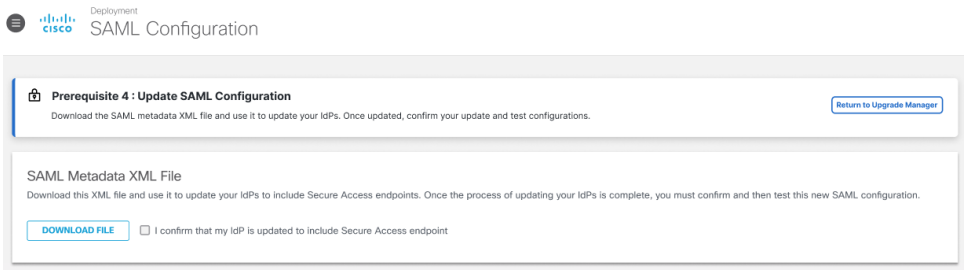
To update your identity providers (IdPs) for Secure Access, download the Secure Access metadata XML file located in your Umbrella dashboard. This file contains important metadata, including the service provider Issuer ID, assertion consumer endpoint URL, and Secure Access SAML signing certificate. Once the configuration is successful, your Entity ID will change to **saml.fg.id.sse.cisco.com**. After updating your IdPs with this information, be sure to test the new SAML configuration before marking this step as complete. If you mark this step as complete before integrating Secure Access XML file to your IdPs, may result in your users getting locked out of Umbrella.

We recommend performing these actions during a scheduled maintenance window to minimize disruption to end users, as changing the Entity ID may temporarily affect user access.

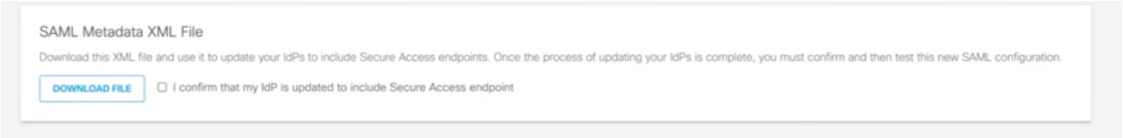
Before you begin
This prerequisite step only appears if you have SAML configured.

Procedure

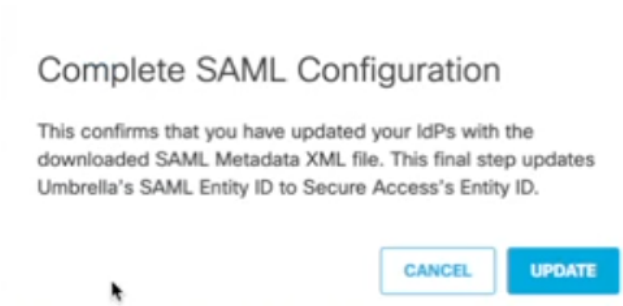
1. In the Umbrella dashboard navigate to **Upgrade Manager** > **4. Update SAML Configuration** > Click **Start**.
2. Click **Download File** to download the Secure Access SAML metadata XML File.



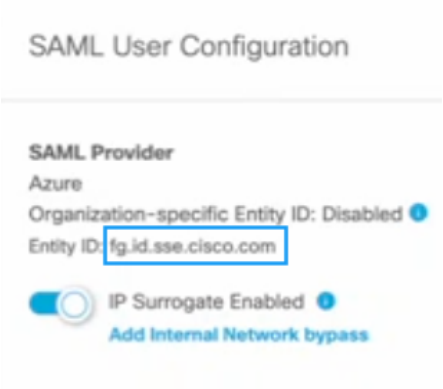
   a) For more information on configuring your IdP and exporting your IdP metadata refer to your vendor's documentation.
3. Check the box **I Confirm that my IdP is updated to include Secure Access endpoint** after you configured Secure Access metadata files with your IdPs.



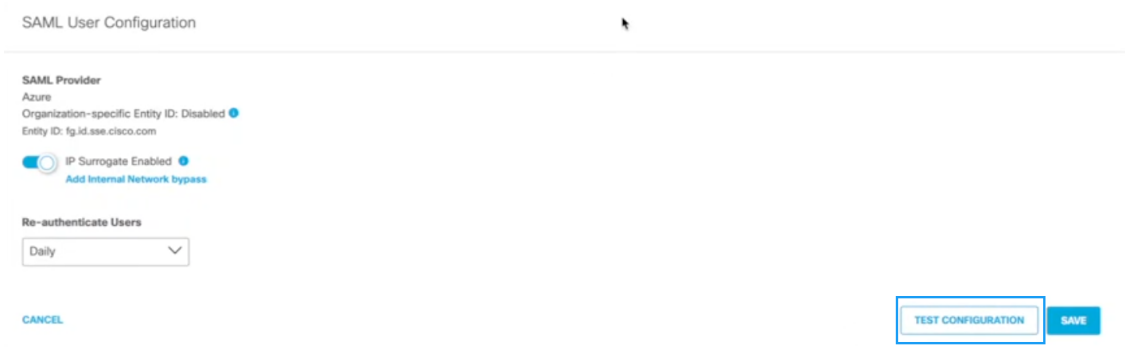
4. Another pop-up message appears to confirm that your IdP is updated. Click **Update**.



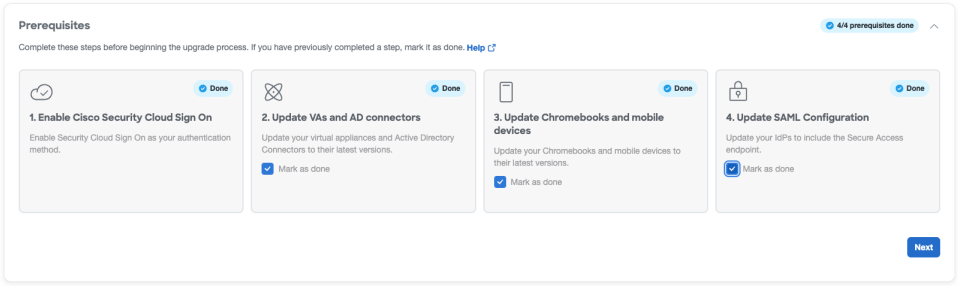
5. Umbrella's Entity ID changes to Secure Access' Entity ID.



6. Click **Test Configuration** to test whether a user can authenticate with the configured IdP.



7. Navigate to **Upgrade Manager > 4. Download SAML Metadata XML** and check the box next to **Mark as done**.



What to do next

SAML Integrations in Secure Access are found by navigating to **Connect > Users and User Groups, and Endpoint Devices** > click **Configuration management** > **SSO authentication**. To learn more about SAML configurations in Secure Access see, Configure Integrations with SAML Identity Providers.**Important**

Deleting your default SAML configuration in Secure Access will also remove the configuration from the Umbrella dashboard—unless you set up OpenID Connect (OIDC) in Secure Access. Umbrella does not support OIDC. If you integrate an OIDC identity provider (IdP) in Secure Access, it will not appear in Umbrella, and all SAML configuration changes must be managed through Secure Access. For more information about OIDC, see Configure Integrations with OIDC Identity Providers.

3 Overview to Start Upgrade

Topics:

- Start Upgrade to Secure Access
- Getting Started with Internet Access Rules
- Manage Umbrella Certificates

This step creates a new Secure Access organization and transfers over your Umbrella configurations.

In this step, you are creating a Secure Access account, and your existing Umbrella DNS, Web, and Firewall policies are unified into a single set of internet access rules within the Access Policy.

Your **Data Loss Prevention (DLP) policy** is copied to Secure Access and is not merged into the Access Policy. DLP policy retains its original configuration, and enforcement continues independently from the internet access rules. While your Upgrade Manager is active, your DLP policy is shared between Umbrella and Secure Access. Any changes made in one product will affect the other until you permanently close your Umbrella account.

Internet Access Rules

This integration eliminates the previous distinction between DNS, Web, and Firewall policies, as each new Internet Access Rule can comprehensively manage both DNS-layer, web-layer, and Firewall traffic components.

For example, while traditional Umbrella required creating separate DNS, Web, and Firewall policy rules to block a specific application like social media, Secure Access achieves this with a single, unified internet access rule.

This streamlined "single pane of glass" approach significantly reduces complexity, enhances operational efficiency by eliminating duplicate configurations, and provides a more robust, easier-to-manage security posture.

Umbrella DNS Policies become Secure Access internet access rules.

Umbrella Web Policy becomes Secure Access internet access rules.

Umbrella Firewall Policy becomes Secure Access internet access rules.

Umbrella DNS policies + Web Policy = Secure Access internet access rules.

Umbrella DNS policies + Web Policy + Firewall Policy = Secure Access internet access rule

Start Upgrade: After completing the prerequisites, the next step is to Start Upgrade. This step creates a new Secure Access organization and transforms your existing Umbrella DNS policies, Web policy, Firewall policy, and configurations into the Secure Access dashboard.

Continuous Protection: Umbrella continues to operate and protect your organization during the upgrade.

Simplified Policy Management: The traditional Umbrella DNS policies, Web policy, and Firewall policy are configured separately. Secure Access consolidates all your internet access rules into one Access Policy. There is no distinction between DNS policies, Web policy, and Firewall policy–just one set of internet access rules that combine all policy components.

Review and Reorder Rules: After the upgrade, your Umbrella DNS, Web, and Firewall policies are converted into internet access rules. Depending on the original configuration, a single Umbrella policy or rule might be split into multiple internet access rules.

You must review your rules in Secure Access to confirm they align with your security goals. Secure Access enforces the first matching rule in the policy list-meaning rules at the top take precedence over those below-reordering your rules may be required. Properly order your rules to ensure your intended protections and access controls are maintained.

Note

Minimize changes in Umbrella during the upgrade process. While it is possible to make changes, please be aware that not all changes will reflect in Secure Access post upgrade. To ensure a smooth transition and consistent security enforcement, it's best to limit changes during this period.

Why Order Matters

- When network traffic (like your internet request or an attempt to access an internal server) comes into a system with an access policy, the system evaluates the traffic against the rules in the order they are listed, from top to bottom.
- The first rule that matches the characteristics of the traffic is applied.
- Once a match is found and an action (allow or deny) is taken, the system stops processing further rules for that specific piece of traffic.
- This means if you have a very broad "allow" rule at the top of your list, it might accidentally permit traffic that a more specific "deny" rule further down the list was intended to block. Conversely, a broad "deny" rule at the top could block legitimate traffic that a more specific "allow" rule was supposed to permit.

Start Upgrade to Secure Access

Start Upgrade, generates your new Secure Access organization and copies your Umbrella policies and configurations.

Before you begin

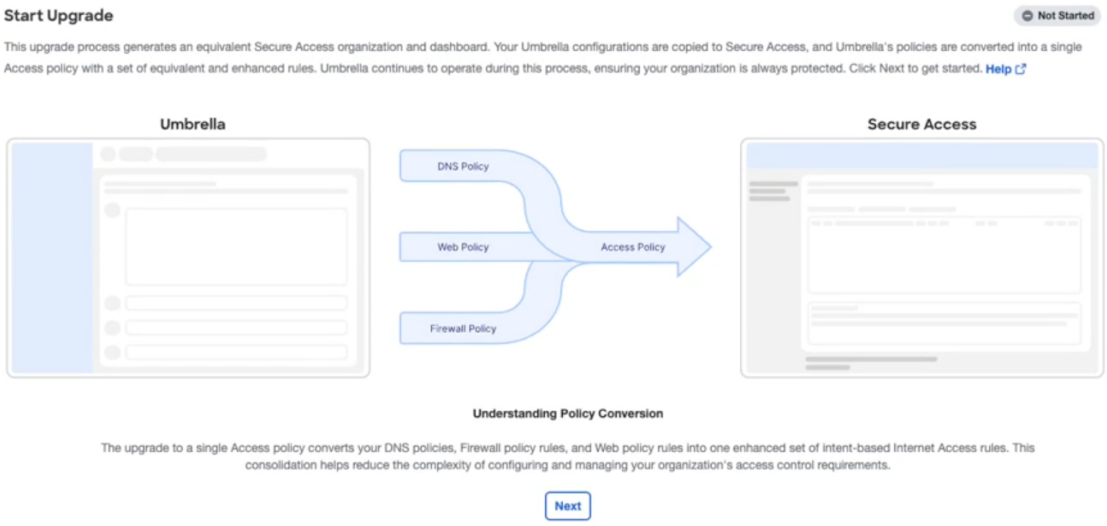
In this step you are creating a new Secure Access dashboard and transferring your existing Umbrella policies and policy components.

Any Umbrella DNS policies, Web policy, and Firewall policy, created after the upgrade will not sync to Secure Access.

We recommend making all policy component changes in your new Secure Access dashboard. Changes made in Umbrella after the upgrade may not appear in Secure Access, and changes in Secure Access may not reflect in Umbrella. For details on which component changes are shared between Secure Access and Umbrella, refer to the Guidelines and Limitations.

Procedure

1. Navigate to **Upgrade Manager** > **Start Upgrade** > Click **Next**.

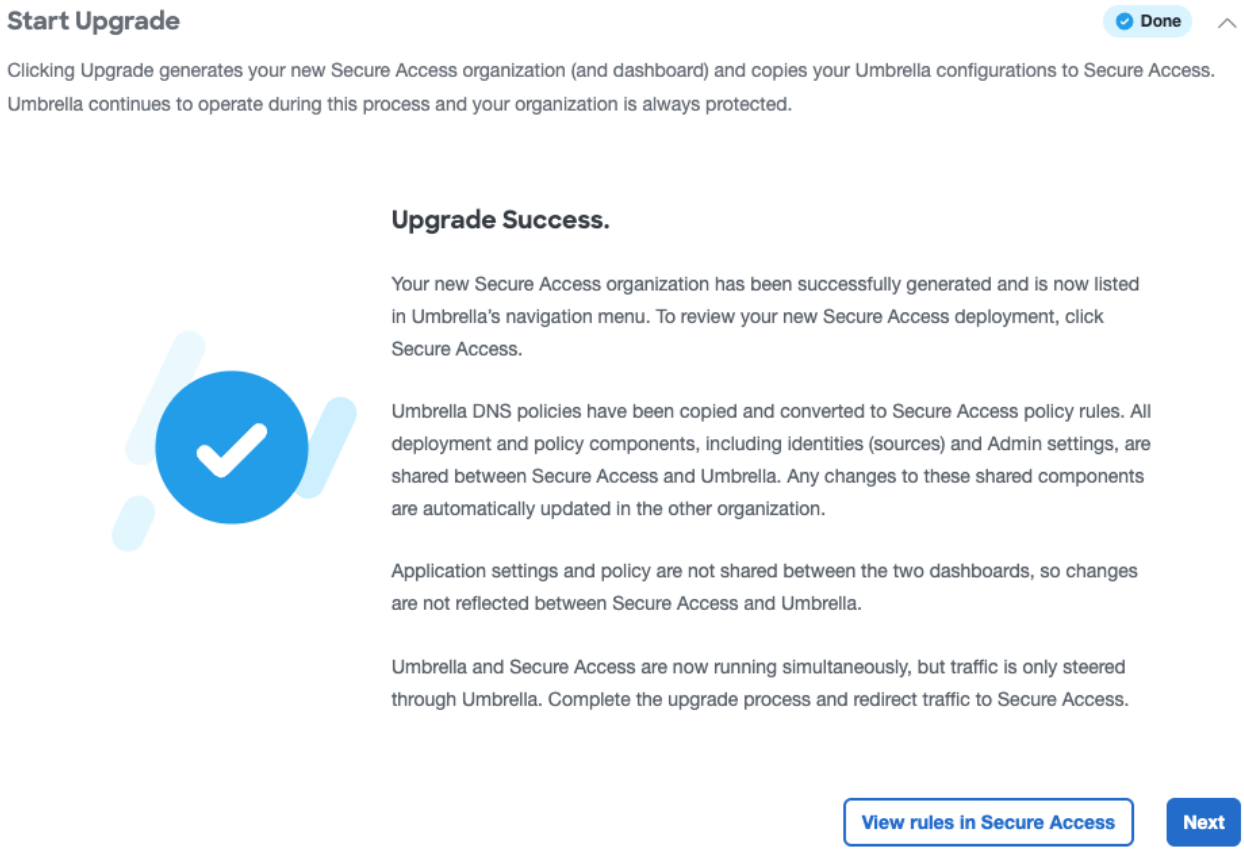


2. Click **Upgrade** to begin.

   The upgrade time depends on the number of policies that are copied from Umbrella to Secure Access. You can navigate away and return to the page at any time to monitor the upgrade status.

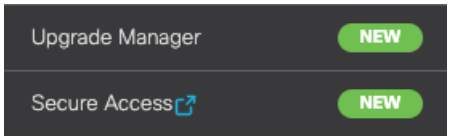
3. **Upgrade Success** appears once the upgrade is complete. Your new Secure Access organization is now successfully generated.

   If you see Upgrade Failed try to click Upgrade again, or contact Support.



4. Click **View rules in Secure Access** to navigate to your new Secure Access dashboard or click **Next** to go to **Redirect Traffic.**

   Secure Access shortcut appears in the left-hand navigation next time you login to Umbrella.

   Check that your Umbrella policies have copied over as rules in Secure Access. To learn more about the new mapping, see Internet Access Rules.

   For more information on how to create new internet access rules, see Get Started with Internet Access Rules in Cisco Secure Access Help.

What to do next

When you upgrade to Secure Access, you must review your policy rules because Secure Access processes traffic based on the first matching rule in your policy list.

Rules placed higher take precedence, so prioritizing critical allow or block rules ensures your policies are enforced correctly and prevents unintended access or threats.

New allow rules (with destinations as ANY) may be created from the translated stack of rules. This could prevent rules below from being processed. Taking time to review and, if needed, reorder your rules after the upgrade helps ensure they are applied as intended in Secure Access and maintains your expected security outcomes.

Important Login Instructions for Secure Access During Upgrade

While the Upgrade Manager is active, Secure Access is only accessible through your Umbrella dashboard login.

Direct login at Cisco Secure Access may cause redirection loops and is unsupported. Until Step 4: Complete Upgrade and Close Umbrella is finished, the Umbrella dashboard is the only supported login method.

Getting Started with Internet Access Rules

Umbrella DNS policies, Web policy, and Firewall policy are now Secure Access internet access rules. An internet access rule can now be enforced at the DNS layer, web proxy layer, and firewall layer.

The conversion to Secure Access internet access rules unifies policies from Umbrella DNS, Web, and firewall-significantly expanding their enforcement. Now, these consolidated rules can be applied across the DNS, web proxy, and firewall layers, offering more comprehensive control.

This upgrade introduces a fundamental change in policy structure, unlike Umbrella where a single policy or rule could contain multiple block and allow components, Secure Access employs a single Access policy model where each individual rule is configured exclusively to either block or allow traffic.

> **Note**
>
> Secure Access uses a unified policy model where rule order determines traffic precedence. Review and test your rules thoroughly before manually reordering them, as moving a rule can change how traffic is handled and may inadvertently allow traffic that was previously blocked.

The order of rules on the Policy page is crucial for how traffic is managed. Traffic is processed by the first rule in the list that matches, and any rules below that matched rule have no effect on that traffic. It is important to arrange your rules so that more specific rules are placed above more general rules. Essential rules, such as those blocking access to sites you want to restrict for all users, should be positioned at the top. If no rule matches the traffic, Secure Access applies the default access rule for the traffic type (internet or private access), located at the bottom of the Access policy page.

Misconfigurations can lead to unintended events, such as unprotected resources or users accessing blocked destinations, so careful planning and design of your rules before implementation is essential. Test your rules by creating a new identity in Umbrella and redirecting the traffic to Secure Access. Follow these steps to Redirect Umbrella Traffic to Secure Access Sources.

Migration order

During the transition, Umbrella DNS, Web, and Firewall policies are transformed into multiple rules in Secure Access, similar to this order depending on how you selected your policies to copy into Secure Access:

1. Umbrella Web Policy sourced rules.
2. Umbrella Web Default Policy sourced rule.
3. Umbrella DNS Policy sourced rules.
4. Umbrella DNS Default Policy sourced rule.
5. Umbrella Firewall Policy sourced rules.
6. Umbrella Firewall Default Policy sourced rule.

For more information, see our Cisco Secure Access guidebook on Get Started With Internet Access Rules and Manage the Access Policy.

Table 2: Policy Components Mapping

Umbrella Policy Components	Secure Access Internet Access Rules
Policies	Access Policy
DNS policies	Internet Access Rules
Web policy	Internet Access Rules
Firewall policy	Internet Access Rules
Application Settings	Application List
Block Page Appearance	Notification Page
Content Categories	Content Categories
Destination Lists	Destination Lists
Identities	Sources
Mobile Device and Roaming Computer	Roaming Device
Security Settings	Threat Categories
Selective Decryption	Do Not Decrypt List

Umbrella DNS Policies to Internet Access Rules: What You Need to Know

Umbrella DNS policies become internet access rules in the Access policy.

After the upgrade, an Umbrella DNS policy can be split into multiple internet access rules in Secure Access. The policy is split in this specific order:

1. Allow Rule (Primary): The first rule is an allow rule that permits traffic as specified in the original Umbrella policy.
2. Block Rule (Secondary): The second rule is a block rule that enforces restrictions on traffic as defined in the original Umbrella policy.
3. Allow Rule (Default): A third rule may be introduced as an implicit allow rule to ensure policy evaluation is consistent with Umbrella's policy model. This rule accounts for scenarios where no explicit match is found for a destination and prevents unintended traffic disruptions.
    - Does not terminate rule evaluation on the enforcement side, enabling further analysis of traffic.
    - Allows general access to safe and non-malicious websites by default. Websites are permitted unless explicitly flagged as malicious by Cisco's threat intelligence.
    - The default rule applies to all sources from the original Umbrella policy until custom rules are configured.
    - Destinations are set to Any.

    How the Default Rule Operates:

    - If the Allow rule (Default) is matched, no rules beyond it will be evaluated during the same query cycle.
    - However, the rule allows subsequent evaluations for the same query under specific circumstances, such as: When analyzing CNAME records and after retrieving resolved IP addresses from DNS resolution.

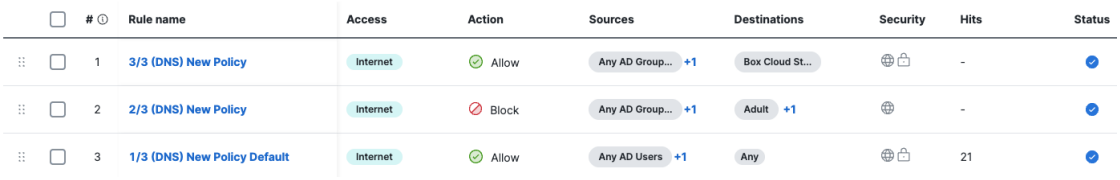
> **Note**
>
> The sources remain the same in these newly separated rules.

Umbrella DNS Policy upgraded to Secure Access Rules

Example: An Umbrella policy named, **New Policy** has AD Groups, AD Users, AD Computers as identities, Content Category blocks all adult related websites and illegal activity, and Application Settings allows Box Cloud Storage.

Umbrella policy appears in Secure Access' Access Policy:

1. 1st rule's name, **3/3 (DNS) New Policy**. Sources: AD Groups, AD Users, AD Computers. **Allow** Application List: Box Cloud Storage.
2. 2nd rule's name is **2/3 (DNS) New Policy**. Sources: AD Groups, AD Users, AD Computers. **Block** Content Category List: all adult related websites and illegal activity.
3. 3rd rule's name is **1/3 (DNS) New Policy Default**. Sources: AD Groups, AD Users, AD Computers. **Allow** destinations: Any.



For more information on creating new internet access rules, see our Cisco Secure Access Help guidebook on Get Started With Internet Access Rules and Manage the Access Policy.

Umbrella Firewall Policy to Internet Access Rules: What You Need to Know

Umbrella Firewall, Web, and DNS policies are copied to Secure Access as internet access rules. These rules can now be enforced across the DNS layer, web proxy layer, and firewall layer, providing multi-layered security coverage.

When you upgrade from Umbrella to Secure Access, your existing firewall rules become internet access rules. Internet access rules can be enforced by DNS, Web, and firewall layers. This change brings several important differences you need to know to ensure your rules continue to protect your network effectively.

What's changing:

1. **Firewall rule name change:** We add a prefix, **(Firewall)** to your rule name to help you easily identify it among the other rules in Secure Access. You can edit or remove the name once you close your Umbrella account.
2. **Bulk Firewall Rule Actions:** Umbrella supports bulk actions for firewall rules, but this capability is not available in Secure Access. You must manage internet access rules individually after migration.
3. **Firewall Rule Schedule Translation:** When migrating firewall rules, Secure Access translates the schedule to apply the start and end times to every day within the specified period. This differs from Umbrella, where start and end times apply only to the first and last days of the period. As a result, the migrated rule may be active for a broader duration than originally intended.
4. **Firewall Rules May Be Split into Multiple Internet Access Rules:** Firewall rules containing applications may be divided into separate internet access rules based on two distinct destinations:
   - Application Protocols refers to the specific communication rules and standards used by software to exchange data over a network, such as HTTP or FTP.

- Internet Applications are the actual software programs or services (YouTube or Facebook) that use these protocols to provide functionality to users.

5. **Internal Networks and Tunnel Identity Differences:**
   - In Umbrella, Firewall rules support internal networks by allowing the selection of **All Tunnels** as a source. Policies can apply broadly to all network tunnels without specifying each tunnel individually.
   - In Secure Access, the **All Tunnels** identity is not supported as a single entity. Instead, the equivalent rule criteria is expressed as a logical AND operator by combining:
     - **Network Objects** or inline source IP (such as CIDR IP addresses representing internal networks) AND
     - **Network Tunnel Groups** (select Any Network Tunnel Groups).

     Example: The source criteria in Secure Access would be represented as CIDR IP addresses AND Any Network Tunnel Groups.

6. **Changes to Destinations in Internet Access Rules:** In Umbrella, the destinations field can include IP addresses, ports, Application Protocols, and Internet Applications.

   In Secure Access, the use of logical AND for destinations is only supported for certain destination types.
   - Logical AND for destinations allows these combinations: **Application Protocol**, **Network Object**, and **Service Object**.
   - Logical AND is **not supported** for Internet Applications. When configuring internet access rules, you can combine Network Objects AND Service Objects, but you cannot AND Internet Applications.

7. **Umbrella Network Tunnels Become Network Tunnel Groups:**
   - Tunnel ID and passphrases change.
   - You must configure and manage network tunnel groups by setting up primary and secondary hubs, and authentication.
   - For detailed steps and guidance, refer to the Cisco Umbrella SIG Upgrade Guide to Cisco Secure Access on, Upgrade to Network Tunnel Groups.
   - In the Secure Access Help guidebook learn more on how to Manage Network Tunnel Groups.

8. **IPS Signature List Renamed to IPS Profile:** IPS Signature List is now called IPS Profile. Find and manage these profiles under **Secure** > **Profiles** > **IPS Profiles**.

Umbrella Firewall Policy as Internet Access Rules in Secure Access

Example: An Umbrella firewall rule named, Company Block App Rule, is configured to block Application Protocol for DNS and block Internet Application for all E-Commerce. The identities are Network Tunnel New York and IP address: 209.165.201.1.

The Umbrella firewall rule is copied to Secure Access and becomes two internet access rules:

1. First rule's name is: 1/2 (Firewall) Company Block App Rule – Application Protocols.
   - This rule is configured to block Application Protocol for DNS.
   - The sources are Network Tunnel New York and IP address: 209.165.201.1.

2. Second rule's name is: 2/2 (Firewall) Company Block App Rule – Internet Applications.
   - This rule is configured to block Internet Application for all E-Commerce.
   - The sources are Network Tunnel New York and IP address: 209.165.201.1.

Umbrella Web Policy to Internet Access Rules: What You Need to Know

Umbrella Web Policy as Internet Access Rules in Secure Access.

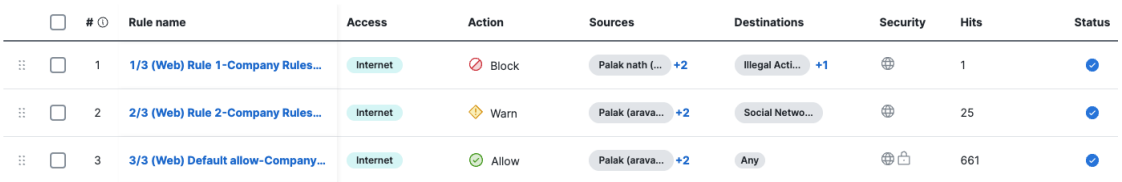
In Umbrella, the Web Policy, is made up of rulesets and rules that set various security, permission, and access controls for your identities. A ruleset may contain a rule with a block action and a second rule with a warn action. In Secure Access, this ruleset is separated into multiple rules depending on the type of rule actions and the valid compatibility of sources.

Umbrella Web Policy as Internet Access Rules in Secure Access

Example: An Umbrella Web ruleset named, **Company Ruleset** has two rules. Each rule has the same identities: G Suite Users, G Suite OUs, and Chromebooks. Rule 1: blocks all adult related websites and illegal activity listed in Content Category. Rule 2: warns users when accessing any Social Networking websites listed in Application Settings.

Umbrella's Web rule in Secure Access' Access Policy:

1. 1st rule's name, **1/3 (Web) Rule 2 - Company Ruleset**. Sources: G Suite Users, G Suite OUs, and Chromebooks. Block all adult related websites and illegal activity listed in Content Category.
2. 2nd rule's name, **2/3 (Web) Rule 1 - Company Ruleset**. Sources: G Suite Users, G Suite OUs, and Chromebooks. Warns users when accessing Social Networking websites listed in Application Settings.
3. 3rd rule's name, **3/3 (Web) Default allow - Company Ruleset**. Sources: G Suite Users, G Suite OUs, and Chromebooks. Destinations set to Allow Any. The default rule allows general access to non-malicious and safe websites. By default, most websites are allowed unless they are explicitly flagged as malicious by Cisco's threat intelligence. This new rule applies to the sources from the separated ruleset and destination is set to Any. This default rule is added to ensure your policy continues to work like it did in Umbrella. It covers situations where none of your specific rules, within the ruleset, match a destination. Without this rule, some user traffic might be blocked unexpectedly. Instead, when no explicit rule applies, traffic from matching sources will still be allowed–just like in your previous Umbrella Web policy.



Data Loss Prevention Policy: What You Need to Know

During the upgrade to Secure Access, your Data Loss Prevention (DLP) policy is uniquely shared between Umbrella and Secure Access, meaning any changes made in one product immediately impact both. This differs from DNS, Web, and Firewall policies which remain separate.

When you upgrade to Secure Access, it is important to understand how your Data Loss Prevention (DLP) policy is handled while the Upgrade Manager is active.

Shared DLP Policy: Unlike DNS, Web, and Firewall policies where Umbrella and Secure Access each keep their own separate copies, your DLP policy is shared between both products. This means there is a single DLP policy that applies to both Umbrella and Secure Access.

Impact of Changes: Since the DLP policy is shared, any changes you make to the DLP policy on either Umbrella or Secure Access will immediately affect enforcement on both products. All DLP rule updates are synchronized and will impact both products.

Policy Translation and Network Tunnel Groups: During the upgrade, the translation process attaches Network Tunnel Groups only to Umbrella DLP rules that had network tunnels configured. This ensures that your network tunnels continue to be managed properly within the DLP rules.

In summary, when you upgrade, remember that while DNS, Web, and Firewall policies operate independently on Umbrella and Secure Access, your DLP policy is unified and shared. Therefore, any updates you make to DLP rules on one product

will be reflected on the other, and network tunnel groups are linked only to those Umbrella DLP rules with existing network tunnels.

See our Secure Access Help guidebook for more information on how to Manage the Data Loss Prevention Policy.

Converting Ruleset and Rule Identities to Secure Access Sources

Explains how Umbrella ruleset and rule identities combine with a logical AND when converted to Secure Access internet access rules, which use sources instead of rulesets.

In Umbrella's Web policy, ruleset identities are configured followed by rule identities. The Umbrella rules match only when the ruleset identity and the rule identity match for a transaction.

Secure Access does not have rulesets. To achieve the same behavior in Secure Access, Umbrella's rulesets and rules are converted into internet access rules, and the two identities are combined with the logical AND operator.

Navigate to our Cisco Secure Access Help guidebook for more information on, Using Network Objects for Sources in Access Rules.

Manage Umbrella Certificates

Overview on installing the Umbrella Root Certificate in Secure Access.

Once you complete the Upgrade, Umbrella's root certificate and your CA signed root certificate are imported to Secure Access and used to decrypt web traffic. You can still edit and delete the certificates in Umbrella. However, to add or renew certificates, you must log in to Secure Access. Refer to the next topic for instructions on adding a certificate in Secure Access.

Install Umbrella Root Certificate

Learn how to install the Umbrella root certificate in Secure Access.

The procedure on this page describes how to download and install the root certificate in Secure Access if your Umbrella root certificate is expiring, or you need to install a new root certificate. Existing and new certificates are used for all Umbrella and Secure Access traffic.

When upgrading from Umbrella SIG to Secure Access, you will continue to use the Umbrella root certificate. Although the Secure Access User Guide refers to the Secure Access root certificate, you will use the Umbrella root certificate instead. In the documentation, replace any instance of **Cisco_Secure_Access_Root_CA.cer** with **Cisco_Umbrella_Root_CA.cer**.

Procedure

1. In Secure Access, navigate to **Secure > Certificates > Internet destinations**.
2. Expand **Umbrella root certificate**, and download the Cisco Umbrella root certificate.

What to do next

See Manage Certificates and Add Custom CA Signed Root Certificate in the Secure Access User Guide.

4 Overview of Redirecting Traffic

Topics:

- Redirect Umbrella Traffic to Secure Access Sources
- Overview on Network Tunnels: From Umbrella to Secure Access Architecture
- Upgrading Network Tunnels: From Umbrella to Secure Access

Redirect your organization's traffic through Secure Access.

In this step, select the Umbrella identities you want to upgrade to Secure Access. Once upgraded, traffic for these identities are steered through Secure Access only.

Umbrella identities are referred to as sources in Secure Access.

While Dual View is active, even new sources created in Secure Access (Registered Networks or Roaming Devices) require you to return to the Upgrade Manager in Umbrella to complete Step 3: Redirect Traffic.

This is essential as the Upgrade Manager functionality maintains the connection of all sources to your Umbrella account until redirection.

To fully transition to your Secure Access dashboard, complete these steps:

- Step 3. Redirect Traffic: Redirect Umbrella identities to Secure Access sources.
- Step 4. Complete Upgrade and Close Umbrella: Deactivate and permanently close your Umbrella account.

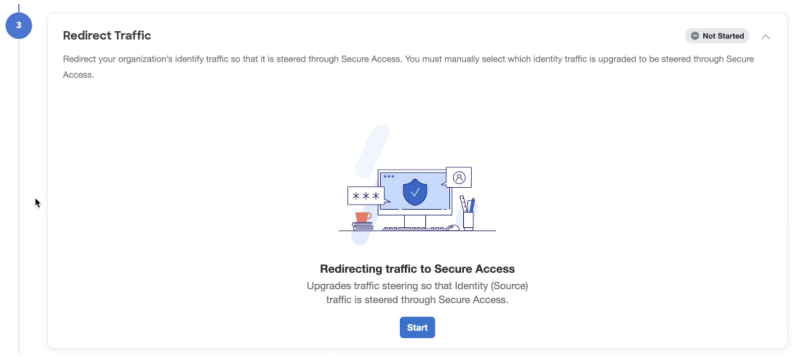
Redirect Umbrella Traffic to Secure Access Sources

Redirect Umbrella's identity traffic to start steering through Secure Access.

In this step, you are switching traffic from Umbrella to Secure Access. You can reverse traffic in this step at any time, until you complete the upgrade and close your Umbrella account. If desired, you can also create a new identity in Umbrella to test functionality in Secure Access.

Procedure

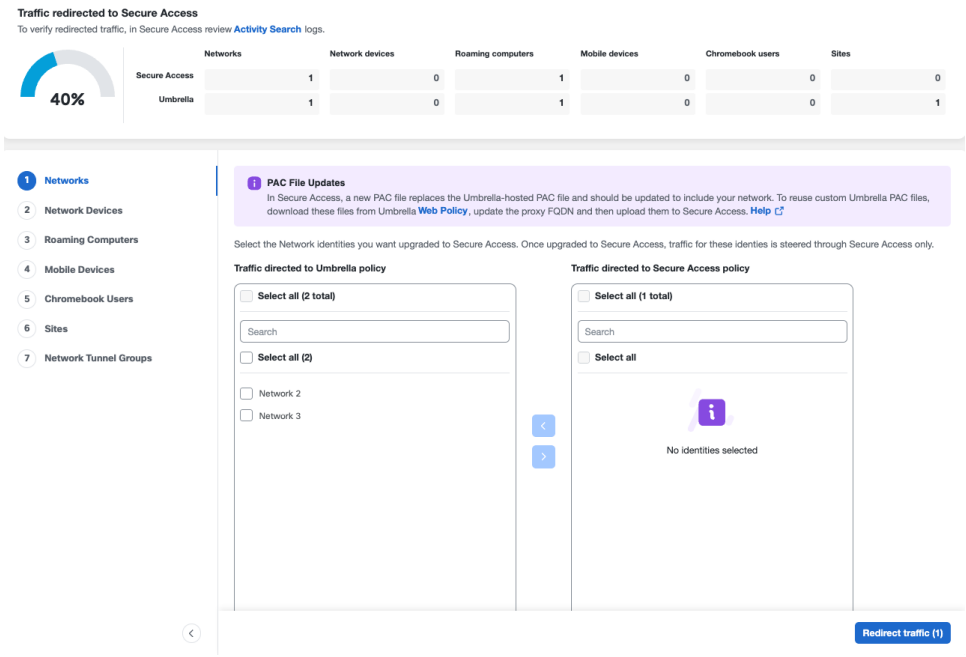
1. In **Redirect Traffic**, click **Start**.



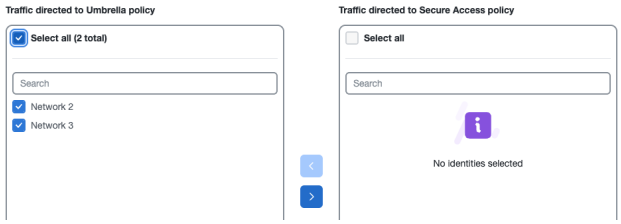
   The **Redirect Traffic to Secure Access** page displays the following identity types with traffic that you can redirect to Secure Access.

   - Networks
   - Network Devices
   - Roaming Computers
   - Mobile Devices
   - Chromebook Users
   - Sites
   - Network Tunnel Groups

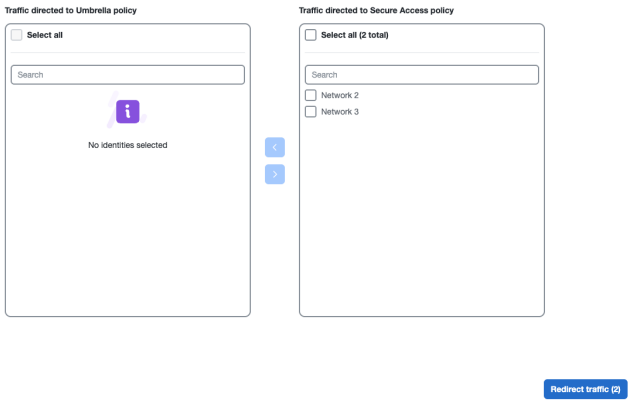
2. Click an identity type. A list of the available identities of that identity type will appear in **Traffic directed to Umbrella policy**.



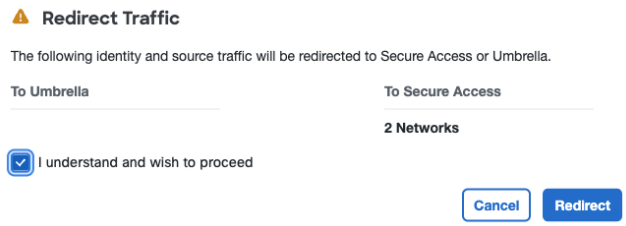
3. Select the identities to redirect traffic to Secure Access.



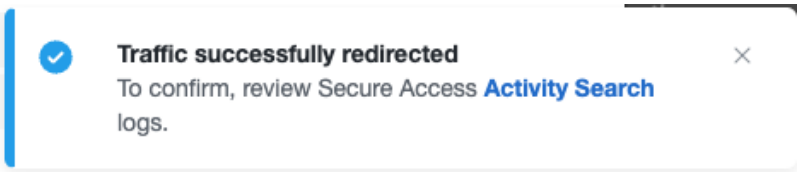
4. Click the arrow to move the selected identities to **Traffic directed to Secure Access policy**.



5. Click **Redirect Traffic**.
6. A pop-up message states, **The following identity and source traffic will be redirected to Secure Access or Umbrella.**



7. Check **I understand and wish to proceed**.
8. Click **Redirect**. Once the authentication is complete, a success modal appears: **Traffic successfully redirected**.



What to do next

View the Activity Search report in Secure Access to verify that the sources traffic are successfully redirected. In the left-hand navigation click **Secure Access > Reports > Activity Search**. For more information, see View and Customize the Activity Search Report.

Overview on Network Tunnels: From Umbrella to Secure Access Architecture

This section details the fundamental shift from Umbrella network tunnels to Secure Access network tunnel groups, emphasizing the critical role of primary and secondary hubs for enhanced redundancy and failover. It outlines the upgrade process, including the configuration of new IPSec tunnels, passphrases, and the necessary review of internet access rules, all while ensuring continuous service during the transition.

It is important to understand the fundamental changes involved when upgrading from Umbrella network tunnels to Secure Access network tunnel groups.

Setting up a primary and secondary hub in your network tunnel groups is essential for you to achieve successful deployment. **You must establish two tunnels for each network tunnel group**.

This configuration introduces fundamental improvements over Umbrella's network tunnels by enhancing redundancy and failover capabilities by using multiple hubs rather than a single tunnel. The primary hub handles traffic under normal conditions, while the secondary hub ensures high availability by automatically taking over if the primary fails. This setup minimizes service interruptions by leveraging tunnel auto-reconnect and failure detection timers, thereby providing continuous, reliable connectivity for branch devices and improving overall business continuity. For more information, see Manage Network Tunnel Groups.

In Step 2. Start Upgrade, the Upgrade Manager copies your Umbrella network tunnels as network tunnel groups in Secure Access.

In Step 3. Redirect Traffic:

- Establish new IPSec tunnels to redirect your network traffic securely.
- Umbrella Tunnel ID changes to a new Tunnel Group ID in Secure Access.
- Create new passphrases.
- Primary and secondary hubs must be configured.
- Internet access rules must be reviewed to fit the Secure Access framework.

- Changes made in Secure Access must also be applied to your endpoint devices, including updating IP addresses and passphrases.

Your existing Umbrella tunnels will remain operational and protected throughout the transition, ensuring uninterrupted service.

Upgrading Network Tunnels: From Umbrella to Secure Access

Guides you through converting Umbrella network tunnels to Secure Access network tunnel groups, editing group settings, configuring tunnel IDs and passphrases, and setting routing for NAT/Outbound traffic.

When upgrading from Cisco Umbrella SIG to Secure Access, the Upgrade Manager copies your Umbrella network tunnels as network tunnel groups in Secure Access. Next, you need to establish new IPSec tunnels to the network tunnel groups to complete the upgrade and redirect your network traffic securely.

Procedure

1. In Umbrella, click **Upgrade Manager** > **Step 3. Redirect Traffic** > **Start** > **Network Tunnel Groups** > **Start**. This brings you to the network tunnel groups page in the Secure Access dashboard.
2. To edit a network tunnel group, click the **ellipsis** (...) > **Edit**.
3. In **General Settings**, edit the Tunnel Group Name, Region, and Device Type.

   The prefix **SSE –** is automatically added to each network tunnel group name. For more information, see Reference: Network Tunnel Group Requirements and Best Practices.
4. Tunnel ID and Passphrase changes
   a) If you are using an IP address, add a second IP address for the secondary hub. Always ensure Tunnel IDs (IP addresses) are unique within your network to avoid conflicts.
   b) Change the original Umbrella passphrase to a new one.
5. In **Routing**, the routing type is always set to default to enable NAT/Outbound only.

What to do next

For detailed information on network tunnel groups, review the Cisco Secure Access Help guidebook on Manage Network Tunnel Groups.

Reference: Network Tunnel Group Requirements and Best Practices

This document provides crucial guidelines for managing network tunnel groups when upgrading to Secure Access from Umbrella.

Understand Network Tunnel Group Naming Requirements in Secure Access

When upgrading to Secure Access, it is important to follow these naming guidelines for network tunnel groups to ensure a smooth transition:

In Step 3: Redirect Traffic, Umbrella network tunnels are copied to Secure Access and automatically have the prefix "**SSE –**" added to their names.

- **New network tunnel groups** created in Secure Access, manually add the prefix, "**SSE –**".
- **Purpose**: This prefix clearly distinguishes Secure Access tunnels from existing Umbrella tunnels.
- **Retention**: Do not remove the prefix "**SSE –**".

- **Deployment Note**: Although Umbrella network tunnels and Secure Access network tunnel groups are visible in both dashboards, deployment is specific: Umbrella network tunnels can only be assigned to Umbrella policies, and Secure Access network tunnel groups exclusively to Secure Access rules.

Avoid Duplicate Tunnel Names

Do not use the same network tunnel name in Secure Access that's already used for Umbrella network tunnels.

- Using identical names can cause conflicts and confusion when managing tunnels across two dashboards.
- Unique names help maintain clear separation and simplify troubleshooting.

Region

Region will be preconfigured based on the last tunnel establishment that was made, but this can be changed by selecting from the drop-down list.

Consolidating Multiple Umbrella Tunnels into a Single Network Tunnel Group

You can simplify your network by combining many Umbrella tunnels into just one Secure Access network tunnel group with primary and secondary hubs for redundancy. This reduces the number of tunnels you manage while keeping your bandwidth intact. Only consolidate if it fits your business needs, especially when you have many tunnels because of bandwidth.

Simplified Tunnel Management

In Umbrella, multiple network tunnels are required to achieve higher bandwidth (four tunnels to reach 1 Gbps). In Secure Access, these multiple tunnels can be consolidated into a single network tunnel group, which simplifies management.

Consolidation of Tunnels

For example, if you have four Umbrella tunnels (Tunnel 1, Tunnel 2, Tunnel 3, Tunnel 4), each is initially copied over as separate network tunnel groups (NTG 1, NTG 2, NTG 3, NTG 4) in Secure Access. Then you can delete NTG 2 through NTG 4 and only keep NTG 1, reducing complexity. After deleting these additional network tunnel groups, you must update your internet access rules accordingly to reflect the changes in your tunnel configuration.

Redundancy with Primary and Secondary Hubs

Each network tunnel group includes a primary hub and secondary hub for redundancy, ensuring high availability and failover capabilities within a single tunnel group.

Scalability for Larger Deployments

If you have more than 4 and fewer than 400 Umbrella tunnels, you still only need one network tunnel group in Secure Access. This network tunnel group can support up to 200 tunnels, with up to 100 tunnels connected to the primary hub and up to 100 connected to the secondary hub.

Tunnel Count Efficiency

The number of Secure Access tunnels per hub is approximately the Umbrella tunnel count divided by four. This means fewer tunnels to manage while maintaining or improving bandwidth and redundancy. (Secure Access tunnel count per hub = Umbrella tunnel count / 4).

Policy Adjustments

After consolidation, you will need to update your internet access rules to reference the single network tunnel group instead of multiple individual tunnels.

SAML Authentication Redirects

When user traffic is distributed across multiple network tunnel groups without proper consolidation, you may notice an increase in SAML authentication redirects. This occurs each time traffic switches between different or unintended network tunnel groups; the system initiates additional redirects to the IdP for SAML authentication.

To minimize redirects, consolidate your tunnels into fewer network tunnel groups. Proper consolidation ensures that user traffic remains within the same network tunnel group, reducing the number of SAML authentication redirects. By consolidating your tunnels correctly, you ensure that the number of redirects is the same experience as in Umbrella.

5 Reports

Topics:

- Reports in Cisco Secure Access

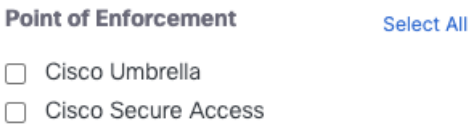
Describes how reports show Umbrella and Secure Access activity during the upgrade transition, including use of the Point of Enforcement filter and its availability after Umbrella is closed.

Reports in Cisco Secure Access

Learn about the reports during the upgrade transition to Cisco Secure Access .

All Umbrella reports are available in Secure Access. For more information, see Monitor Secure Access with Reports. You can generate reports for a specific time period, with a maximum range of the last 90 days.

While the Upgrade Manager is running, you can use reports to monitor Secure Access and Umbrella usage by using the **Point of Enforcement** filter. Point of Enforcement filter allows you to select which product's traffic path you wish to view.



Important

Point of Enforcement filter is not available once you permanently shut down Umbrella. For more information, see Complete Upgrade and Close Umbrella.

6 Complete Upgrade and Close Umbrella

Topics:

- Close Umbrella

Last step to complete the upgrade process.

The last step is to close your Umbrella account once you have completed the prerequisites, upgraded all policy rules, and directed all traffic to Secure Access.

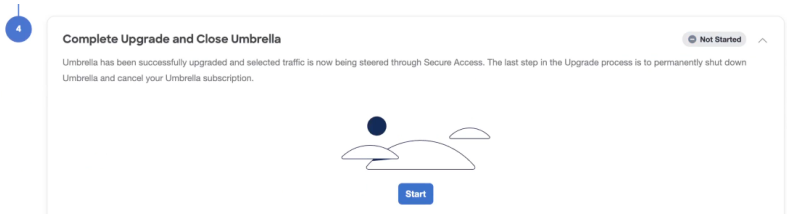
Close Umbrella

This is the last step to shut down Umbrella and cancel your Umbrella subscription.

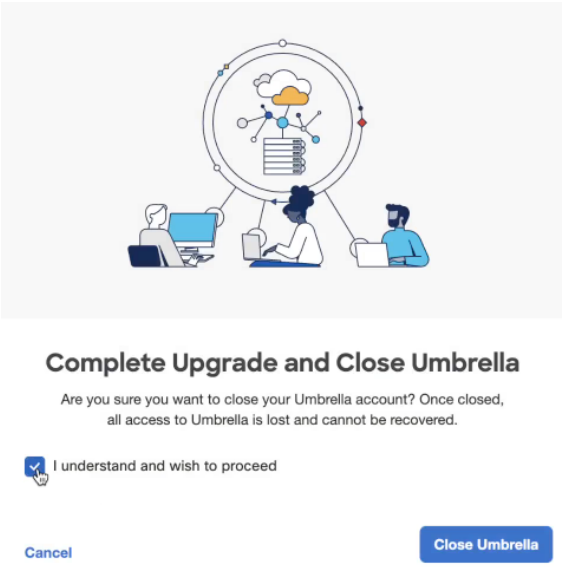
Umbrella is successfully upgraded and selected traffic are now steered through Secure Access. The last step in the Upgrade Manager is to permanently shut down Umbrella and cancel your Umbrella subscription.

Procedure

1. Click **Start**.



2. Check **I understand and wish to proceed**.



3. Click **Close Umbrella**.

   Your Umbrella account is closed, and your organization is fully protected with Secure Access.

7 Troubleshoot Overview

Topics:

- Troubleshoot Upgrade Manager

The following topic explains how to troubleshoot for customers upgrading from Cisco Umbrella SIG to Cisco Secure Access.

The following topic discusses possible scenerios where you may need to troubleshoot when upgrading.

Troubleshoot Upgrade Manager

Review scenarios in this topic if you experience any issues during the upgrade.

Issue	Solution
What if I never received the subscription claim code for Security Cloud Control (SCC)?	• Check your spam inbox. • You may not be the admin linked to the account at the time of purchase. Contact your sales representative for more information.
What if Step 2 **Start Upgrade** shows **Upgrade Failed**?	If another admin tried to edit or add a policy during the Upgrade process, the policy translation may fail. Try to refresh your web browser or delete the policy before attempting Step 2 of the upgrade again.
Can I change my Organization name?	• In Security Cloud Control you can change the Organization name by selecting your organization in the left-hand column > Platform management> Product Subscriptions > Subscriptions > Click pencil icon to edit > Save. • Changing the Organizaation name in SCC will not change the name in Secure Access. Contact Secure Access Support to request a change.
Umbrella admins are locked out of the Umbrella dashboard.	You must send invites to Umbrella admins to create their own Security Cloud Control accounts. Authentication will now happen through Security Cloud Control. See, Invite a User.
What if I clicked **Request Invitation** to Upgrade to Secure Access, but I am not the Admin who received the initial Security Cloud Control email with the Subscription Claim Code?	The Admin who received the initial Security Cloud Control email would create an account, add you as a new user, and you will activate the upgrade to Secure Access by entering the Subscription Claim Code in SCC.
What if I accidentally created a new Secure Access instance instead of attaching the existing?	Contact Secure Access Support
What if I linked the subscription claim code to the wrong Umbrella organization?	Contact Secure Access Support
Who should I contact if I have any technical issues?	Contact Secure Access Support