Cisco Umbrella DNS to Cisco Secure Access - DNS Defense Upgrade Guide

Cisco Secure Access
Updated October 1, 2026

1 Before You Begin

Topics:

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

Read the entire Upgrade Guide before attempting to upgrade Umbrella to Secure Access – DNS Defense.

Upgrade time will vary depending on the data and number of policies required to move over. Umbrella continues to operate during this process and your organization is always protected.

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

Important

You must have Full Admin access to start the upgrade to Secure Access.

- Welcome to Cisco Secure Access – DNS Defense
- QuickStart
- Create a Cisco Security Cloud Control Account
- Create Upgrade Manager in Umbrella
- Guidelines and Limitations

Is This Guide for You?

This offer is available to customers with Umbrella DNS Advantage, Umbrella DNS Essentials, MSP, and Multi-org.

This offer is available to customers with Umbrella DNS Advantage, Umbrella DNS Essentials, MSP, and Multi-org.

> **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**.

Welcome to Cisco Secure Access - DNS Defense

Experience enhanced security with Cisco Secure Access - DNS Defense.

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 DNS 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.

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

Why Choose Secure Access - DNS Defense?

- Seamless Transition: Enjoy a smooth upgrade to enhanced security measures without disruption to your operations.
- Connect Anywhere, Anytime: Gain secure access to applications and data from any location or device, making remote work effortless.
- Zero Trust Architecture: Connect to resources outside the company network without the need for a VPN, ensuring private applications are protected.
- Granular Access Control: Tailor access permissions based on user roles, device compliance, and other critical factors.
- Multi-Factor Authentication (MFA): Elevate your security with multiple verification steps to ensure only authorized access.
- Robust Policy Enforcement: Implement detailed security policies to manage user access and activity effectively.

Secure Access is your ideal partner for remote work scenarios, where secure and reliable access to corporate applications is crucial. With enhanced control over user access and activities, protect your internal resources with confidence.

Best Practices for the Upgrade

This topic outlines best practices to help you transition from Cisco Umbrella to Secure Access.

These are the best practices to help you transition from Cisco Umbrella to Secure Access.

- Upgrade during non-business hours.
- Use the migration tool to migrate a subset of devices at a time. This phased approach helps you validate the migration with a smaller group of devices before expanding to a full rollout.

  Migrating in stages allows you to test policies, confirm successful integration, and resolve any issues before migrating the remaining devices.
- Use the Redirecting Traffic feature to redirect a subset of identities at a time. We recommend a phased upgrade approach as this allows you to:
  - Test your internet access rules with a smaller group of identities.
  - Confirm successful integration of internet access rules.
  - Identify and address any issues early.

Upgrade Workflow

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

Procedure

1. Create a Cisco Security Cloud Control (SCC) account. You must receive a Welcome email with a subscription claim code to link a Secure Access account with your Umbrella instance. Follow the steps in 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 prerequisites in your Umbrella dashboard.
   - Enable Cisco Security Cloud Sign On for all users.
   - Update virtual appliances and Update Active Directory Connectors.
   - Update Chromebooks and Update mobile devices.
4. Start Upgrade

   Umbrella DNS policies and components are copied to Secure Access Internet Access Policy and settings.
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 - DNS Defense.

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

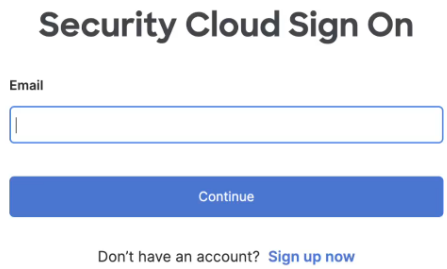
Cisco Security Cloud Control (SCC) provides centralized visibility and management for Cisco's security products. To upgrade from Umbrella DNS to Secure Access - DNS Defense, you'll need to create a Security Cloud Control account after receiving the Welcome email with your claim code. For more information, see Signing in to Security Cloud Control.

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.

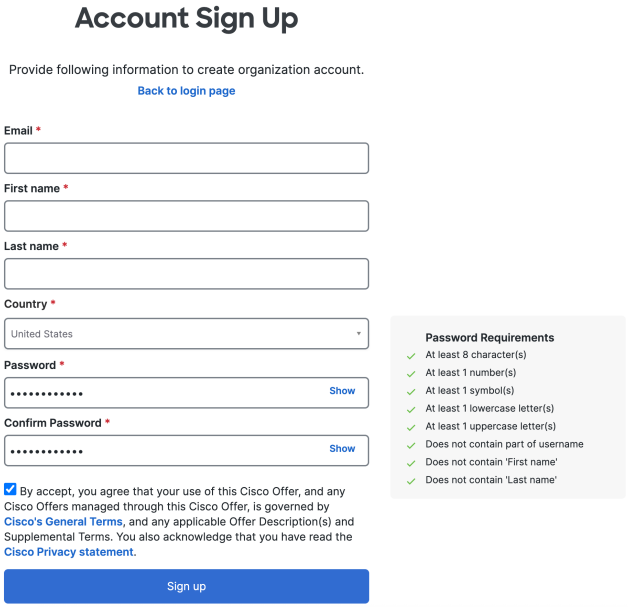
Finally, you'll need to setup multifactor authentication for added security, and we recommend using Duo.

Procedure

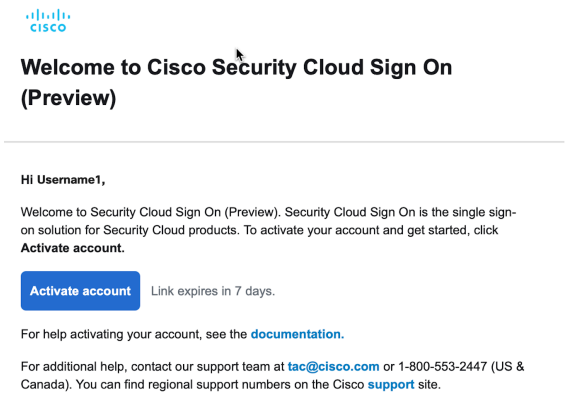
1. Create a Security Cloud Control (SCC) account by creating a Security Cloud Sign On account.
2. Click **Sign up now** to create a Security Cloud Sign On account.



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

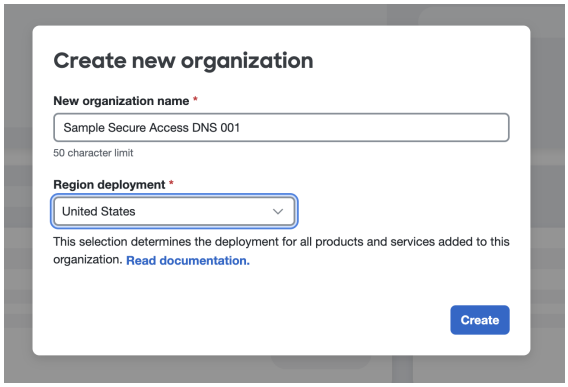


4. Look for the verification email to activate your account. Link expires in 7 days.



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 drop-down 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

Explains how to activate the Upgrade Manager.

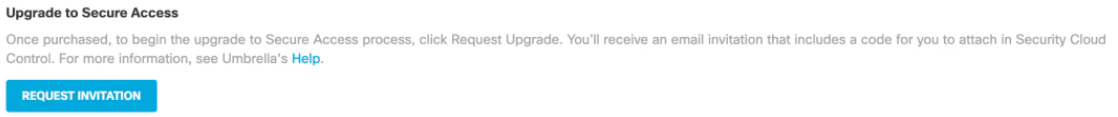
Before you begin

- **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 create a new Secure Access organization without linking your Umbrella organization.

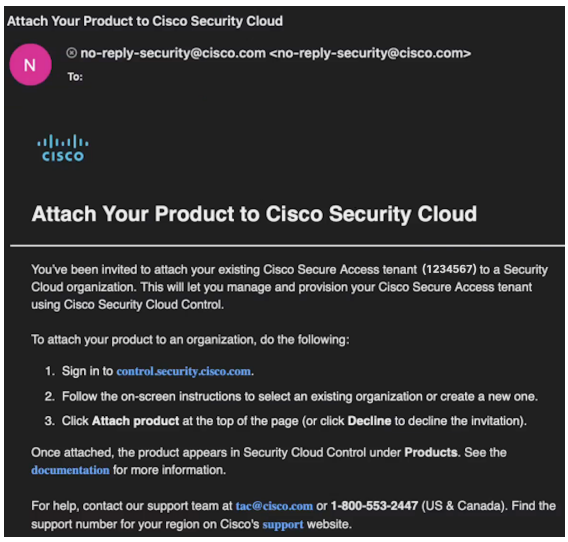
- The admin must receive a welcome email from Cisco Security Cloud containing a unique subscription claim code to upgrade to Secure Access – DNS Defense.
- The admin who receives the subscription claim code is responsible for completing the subsequent steps to activate the Upgrade Manager in Umbrella.

Procedure

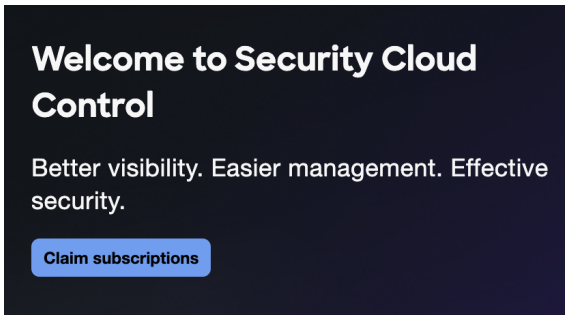
1. Login to your Umbrella account.
2. Navigate to **Admin > Licensing > Upgrade to Secure Access** and click **Request Invitation**.



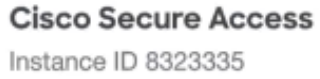
3. Check your email for an invitation to **Attach Your Product to Cisco Security Cloud**.



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**.

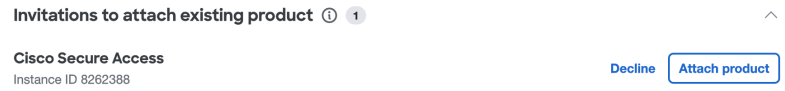


6. Check that **Cisco Secure Access Instance ID** is the same as your Umbrella organization ID.

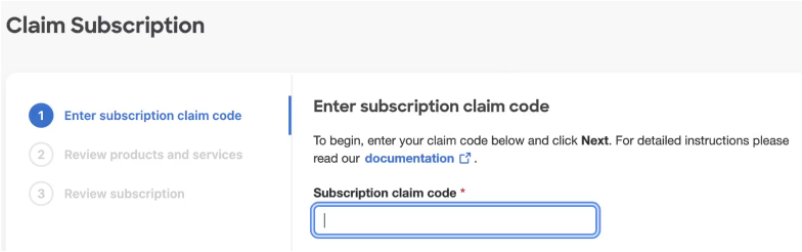


7. Click **Attach product** then click **Attach** to attach your Umbrella organization to the Secure Access instance.

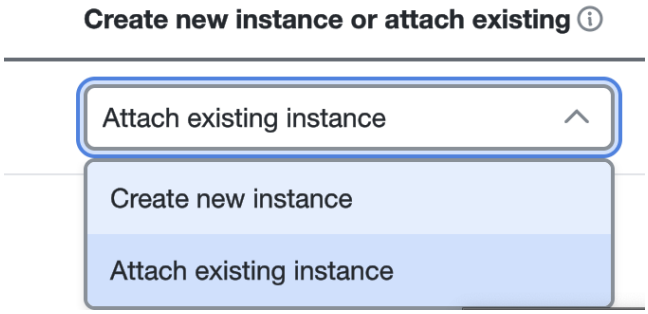
This action cannot be undone.



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



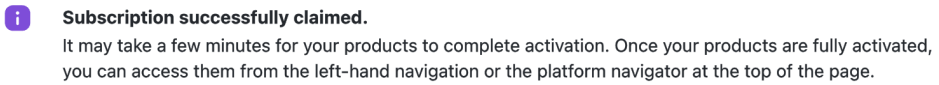
9. Click **Next** to begin the claim subscription work flow.
10. In the drop-down list select **Attach existing instance**.



Do not create a new instance. A new organization will not upgrade to Secure Access – DNS Defense.

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

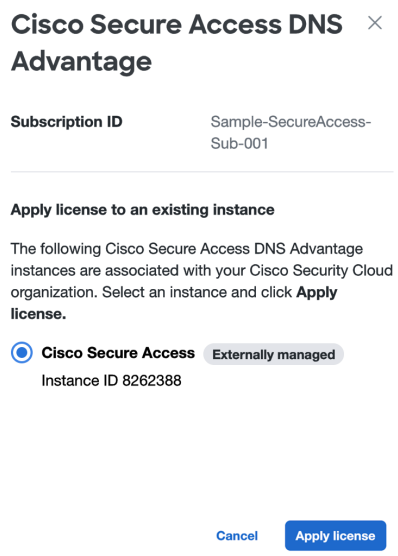
    Subscription successfully claimed. It may take a few minutes for your product to complete activation. Once your products are fully activated, you can access them from the left-hand navigation or the platform navigator at the top of the SCC page.



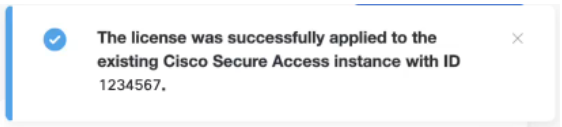
12. In **Product and service activation status**, click **Action required**.



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



A 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 and then Start Upgrade to create your new Secure Access organization.

Guidelines and Limitations

Learn more about the guidelines and limitations in Cisco Secure Access - DNS Defense.

Umbrella Application Settings and Secure Access Application Lists

After completing the Start Upgrade step, Umbrella Application settings become Secure Access Application lists. Application settings and Application lists are managed separately, and any changes made to the application categories are not reflected between the two dashboards. We recommend to not make any changes until you complete the last step in the Upgrade Manager and permanently close your Umbrella account.

An Application Setting in Umbrella with block and allow accesses are separated into two Application Lists in Secure Access. An Application List will only have block or allow to support Secure Access Internet Access rules.

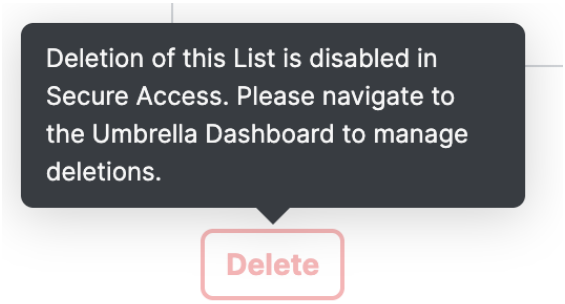
Umbrella Policy Upgrade Behavior

- Umbrella DNS policies that do not include identities are not copied to Secure Access.
- Umbrella DNS 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 Policies and Components in Security Profiles and Internet and SaaS Resources

Once the upgrade begins, **Delete** function is disabled for Umbrella policies in Secure Access until you complete Step 4 in the Upgrade Manger and close your Umbrella account. Additionally, the Umbrella policy components listed in Security Profiles and Internet and SaaS Resources cannot be deleted in Secure Access while the Upgrade Manager is active.



Block Page Bypass

Block Page Bypass is not copied over. For more information on the Secure Access feature, refer to Manage Notification Pages.

Custom User Roles

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

- Full Admin
- Read-Only

For more information, refer to Add a New Account.

Domain Management

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

Source Identity Limit of Secure Access Policy May Be Exceeded

Secure Access policies are rule-based, and each rule supports a maximum of **250 unique source identities**. When the Umbrella policy **[%POLICY NAME%]** is translated to Secure Access, the resulting rule may exceed this limit. You can continue with the migration. However, migration may fail if the Umbrella policy contains more than 250 unique source identities.

If the policy uses **All** as the source identity, you can safely ignore this warning. For example, an Umbrella policy may show a count greater than 250 when **All Roaming Computers** is selected, but this selection is translated as a single source identity.

Internet and SaaS Resources

Internet and SaaS Resources page contains 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

Legacy Umbrella Content Categories

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

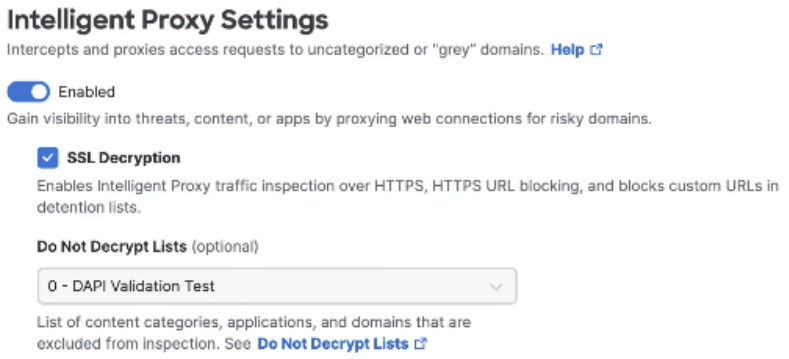
Security Profiles

A Cisco Secure Access Security profile is a reusable component that you can use for the rules in the Access policy. A Security profile for internet access rules includes security controls and other settings such as acceptable use controls that you configure as a set. For more information, refer to Add a Security Profile for Internet Access. Security Profiles include:

- Threat Categories
- File Inspection
- SafeSearch
- Do Not Decrypt List
- Notification Pages

Selective Decryption

Umbrella's Selective Decryption is upgraded to Do Not Decrypt List in Secure Access. While the Upgrade Manager is running, you can not make changes to the Do Not Decrypt List that is linked to a policy created in Umbrella. This option is enabled once you close your Umbrella account. For more information, refer to Enable the Intelligent Proxy and Do Not Decrypt Lists.



Static Keys

In Secure Access, Static Key is found by navigating to Connect > Users, Groups > Configuration Management > Integrate Directories > IdP. For more information, refer to Provision Token for Identity Provider.

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, refer to Manage API Keys and Secure Access API Authentication.

2 Prerequisites

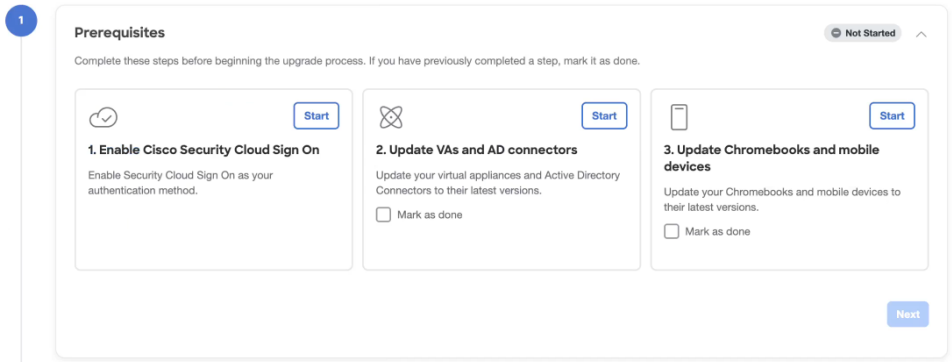
Topics:

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

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

Before upgrading to Secure Access - DNS Defense, ensure that all prerequisites are complete.

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



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.

Note

If you are upgrading from an Umbrella DNS-only package to **Secure Access - Essentials** or **Secure Access - Advantage**, instead of **Secure Access - DNS Defense**, disable **Intelligent Proxy** in your existing Umbrella DNS policies before migration.

During migration from DNS-only to full Secure Access, the Umbrella DNS Intelligent Proxy is upgraded to a full proxy, rather than the selective proxy used in DNS-only deployments. Disabling Intelligent Proxy in advance is recommended to help avoid unexpected proxy behavior after migration.

Enable Cisco Security Cloud Sign On

This topic describes how to enable Cisco Security Cloud Sign On and create Security Cloud Control accounts for your Umbrella administrators.

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.

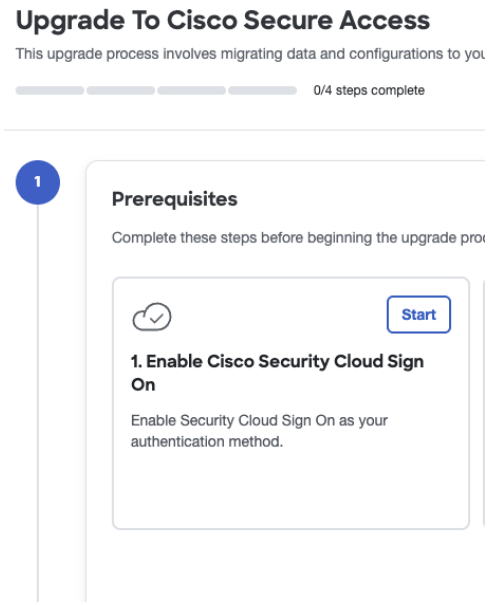
Before you begin

- Full admin user role is required.
- **Existing SAML configuration:** If your organization already uses an identity provider (IdP) with Umbrella, you must configure that same IdP in Security Cloud Control before you enable this feature. This ensures that your existing authentication flow remains intact and prevents administrator lockout. Do not remove your existing Umbrella IdP configuration unless explicitly required.
- **User account verification:** Verify that your Umbrella admin accounts also exist in Security Cloud Control, either as manually created users or as users provisioned through your IdP. Use the same administrator email address in both Umbrella and Security Cloud Control to avoid access issues.

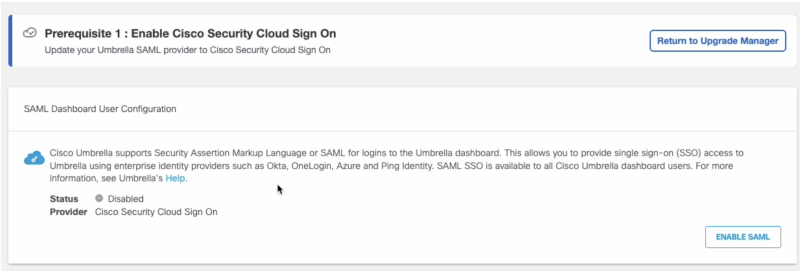
  For more information, see Overview of Security Cloud Sign On in our Security Cloud Control Getting Started Guide for Existing Customers.

Procedure

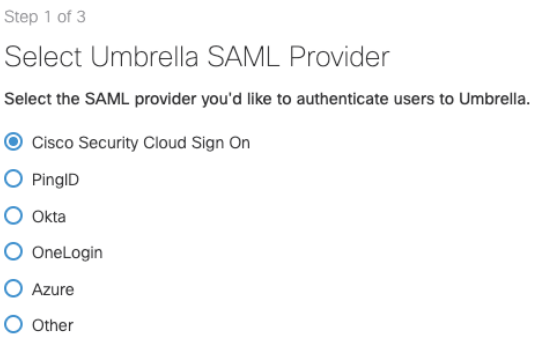
1. Navigate to **Upgrade Manager**. In the **Enable Cisco Security Cloud Sign On** prerequisite step, click **Start**.



2. Click **Enable SAML**.

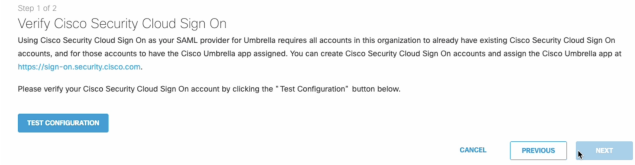


3. Perform one of the following actions based on your current configuration:
   - **If you do not have SAML configured:** Click Cisco Security Cloud Sign On to create a Security Cloud Sign On account for all Umbrella dashboard users. In the following window, click **Sign up now**. For more information about creating accounts, see Invite a User.

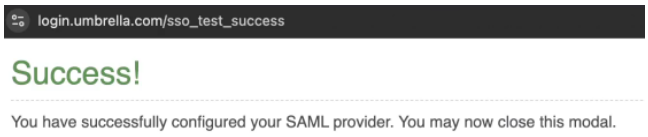
   - **If you already have SAML configured:** Ensure your existing IdP is configured in Security Cloud Control, then proceed to link your accounts.

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

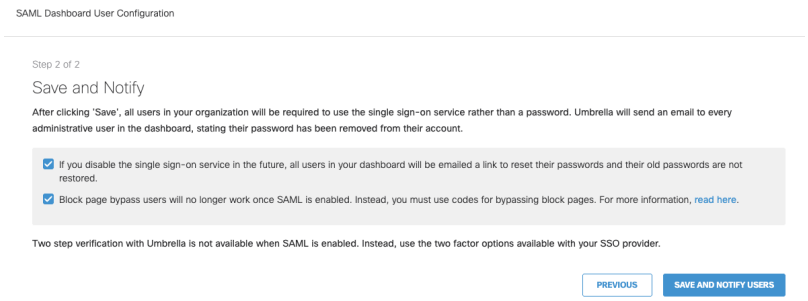
   

   The **Test Configuration** must be performed and successful for the set-up to complete.

   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**.



6. Click **Return to Upgrade Manager** and **Enable Cisco Security Cloud Sign On** step changes 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:

- Update Virtual Appliances
- 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

Use this procedure to manually upgrade Active Directory Connectors.

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.

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

3 Start Upgrade

Topics:

- Upgrade to Secure Access - DNS Defense
- Getting Started with Internet Access Rules
- Understanding Access Policy Enforcement: Secure Web Gateway Enabled

This step creates a new Secure Access organization and copies over your Umbrella configuration.

Starting the upgrade process generates a new Secure Access - DNS Defense organization. Umbrella continues to operate during this process and your organization is always protected.

Umbrella DNS policies and components are copied over to Secure Access as internet access rules, Settings, Internet and SaaS Resources. After the upgrade, an Umbrella DNS policy can be split into multiple rules in Secure Access. You need to review the order of the rules and test to ensure this is how you want the traffic handled.

Upgrade to Secure Access - DNS Defense

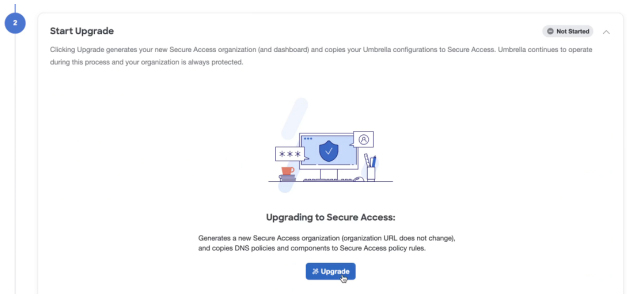
Clicking Upgrade generates your new Secure Access organization and copies over your Umbrella configurations.

Before you begin

We recommend to not make any changes to your policies while your upgrade from Umbrella to Secure Access is in progress. To avoid any unintended changes to your policies, please do not edit or delete any existing security profiles until the upgrade is finished. Policies created in Umbrella post transition will not be synced to Secure Access. See Get Started with Internet Access Policy for the new policy components mapping.

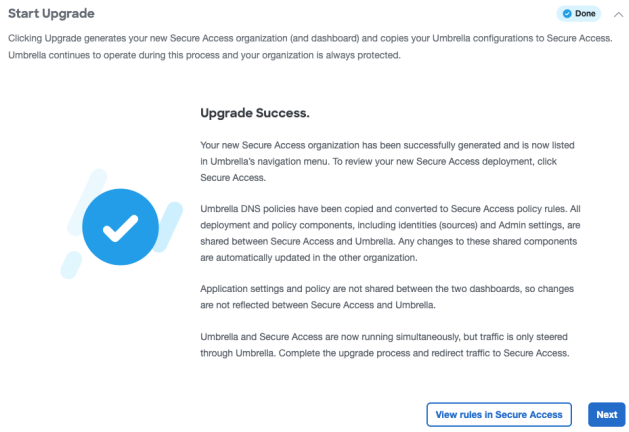
Procedure

1. Click **Upgrade** to begin. Do not exit the page during the upgrade. All changes will be lost and must restart from the beginning. The upgrade time depends on the number of policies that are copied over from Umbrella to Secure Access.



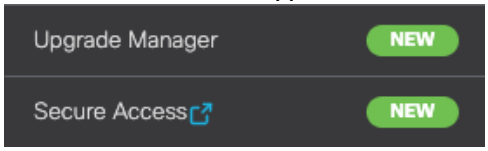
2. **Upgrade Success** appears once the upgrade is complete.

   Your new Secure Access organization has been successfully generated.



3. 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 rules, see Get Started with Internet Access Rules.

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

---

What to do next

Start redirecting your Umbrella identities to Secure Access in the next step.

Important Login Instructions for Secure Access During Upgrade

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

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 are now Secure Access internet access rules in the access policy.

When upgrading from Umbrella to Secure Access, you will see a change in how policies are structured. Unlike Umbrella, where a policy may include multiple block and allow components, Secure Access employs a unified policy model. Each rule within this model can be configured to either block or allow traffic. During the transition, an Umbrella policy is transformed into a maximum of three distinct rules in Secure Access, following 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.

   Non-terminal Allow: To support the implicit allow rule, Secure Access introduced the Non-terminal Allow feature. This feature ensures that the default rule:

   - 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 Non-terminal Allow rule 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.

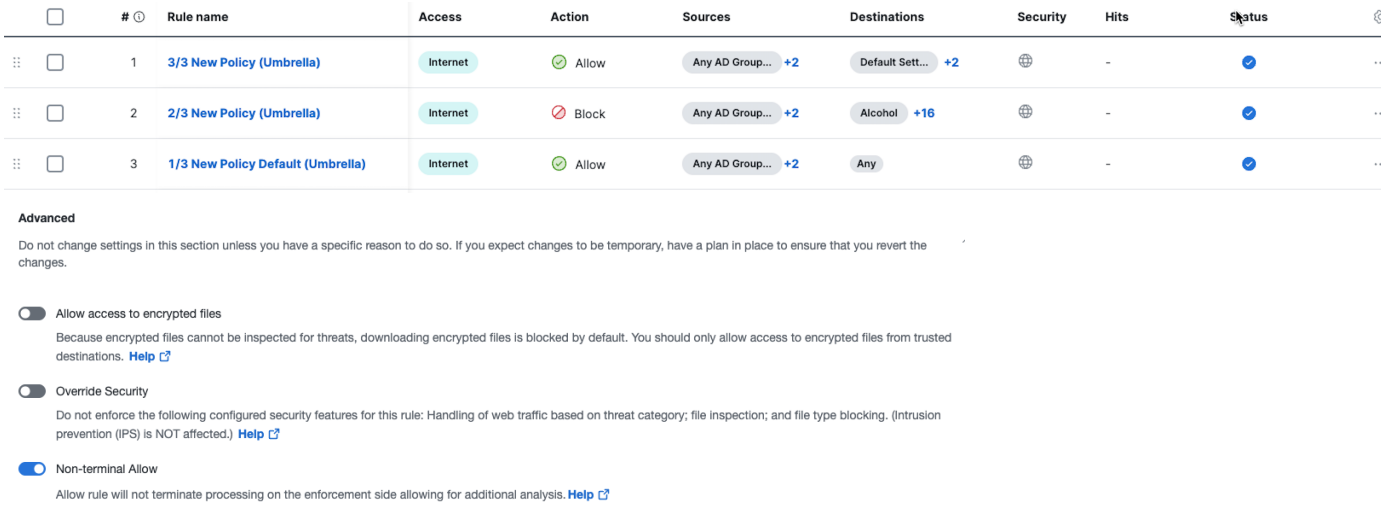
   > **Note**
   >
   > The sources remain the same in these newly separated rules.

Umbrella 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 New Policy (Umbrella)**. Sources: AD Groups, AD Users, AD Computers. Allow Application List: Box Cloud Storage.
2. 2nd rule's name is **2/3 New Policy (Umbrella)**. 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 New Policy Default (Umbrella)**. Sources: AD Groups, AD Users, AD Computers. Allow Any. To see **Non-terminal Allow** navigate to **Secure > Access Policy > Click Edit next to the Default (Umbrella) rule > Configure Security > Next > Advanced > Non-terminal Allow**.



For more information, see Get Started With Internet Access Rules and Manage the Access Policy.

Table 1: Policy Components Mapping

Umbrella Policy Components	Secure Access Internet Access Rules
Policies	Internet Access Policy
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

Understanding Access Policy Enforcement: Secure Web Gateway Enabled

Explains the rule enforcement when SWG is enabled.

Note

Not all features described here are available to all Secure Access packages. To determine your current package, navigate to Admin > Subscription. For more information, refer to Determine Your Current Package.

If you encounter a feature described here that you do not have access to, contact your sales representative for more information. Refer to Cisco Umbrella and Cisco Secure Access packages.

Rule Enforcement Changes

When you upgrade from Cisco Umbrella to Cisco Secure Access, rule enforcement changes if Secure Web Gateway (SWG) is enabled for your organization. In Secure Access, SWG proxies perform final enforcement for rules with destinations that include URLs (example.com/login).

When a block rule matches a URL, the DNS resolver cannot evaluate the full URL path and can only identify the domain (example.com). In this case, Secure Access defers enforcement to SWG.

1. **DNS Evaluation**: A request to evaluate a destination (example.com/login). DNS resolver only sees domain (example.com) and defers to SWG for enforcement.
2. **Enforcement Deferred to SWG**: Instead of returning a block page (notification page), Secure Access returns the destination IP address and expects SWG to intercept the web traffic and enforce the block at the HTTP or HTTPS layer.
3. **SWG must be in the traffic path**: To enforce the block, user traffic must be steered through SWG by using Network Tunnel Groups, PAC Files, or Cisco Secure Client.
4. **Result without SWG**: If traffic follows a DNS-only path and does not pass through SWG, the block is not enforced and traffic is allowed.

Recommended Actions for Consistent Enforcement

To ensure consistent rule enforcement across your organization, follow these steps:

1. **Use explicit domain names**: If you want enforcement to apply to the entire domain, add the domain (example.com) to your destination lists. When you use a specific URL (example.com/login), that traffic is evaluated through SWG because URL-based enforcement requires web-layer inspection.
2. **Ensure SWG coverage**: If you require URL-based blocking, ensure that the SWG proxy is active in the data path for those specific sources or networks. To do this in Secure Access, configure Internet Security and route traffic through the Secure Access proxy by using Cisco Secure Client, PAC files, or Network Tunnel Groups.
3. **Audit your rules**: Identify any block rules that rely on specific URL paths. By aligning your rule configuration with your network architecture, you can prevent unexpected allow behavior and ensure your security rules are enforced as intended.

Refer to these topics in our Cisco Secure Access Help guidebook on different ways to configure SWG enforcement:

- Configure Cisco Secure Client Settings for roaming devices.
- Manage PAC Files.
- Configure DNS and Web Security (Enable the Web Security port 80/443 traffic only).
- Manage Network Tunnel Groups for sites, branches, or network-based traffic.

For additional resources, refer to:

- Troubleshoot Internet Access Rules.

- Control Access to Custom URLs.
- Examples.
- Manage Destination Lists.

4 Redirect Traffic

Topics:

- Overview of Redirecting Traffic

Explains how to redirect your organization's traffic through Secure Access.

Overview of Redirecting Traffic

In this step, select the Umbrella identities you want to redirect traffic to Secure Access. After the redirection, traffic from these identities will be routed exclusively through Secure Access. In Secure Access, identities are called sources.

While Upgrade Manager is active, even if you create new sources – such as Registered Networks or Roaming Devices – directly in Secure Access, you need to return to the Upgrade Manager in Umbrella to complete Step 3: Redirect Traffic.

This is necessary because the Upgrade Manager functionality keeps your new and existing sources connected to your Umbrella account until those sources are redirected.

Complete these steps to fully transition to your Secure Access dashboard:

- 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.

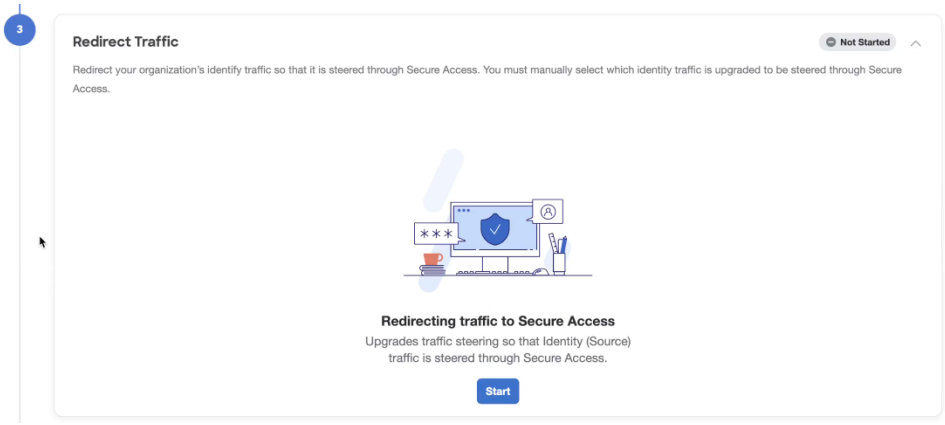
Redirect Umbrella Traffic to Secure Access Sources

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**.

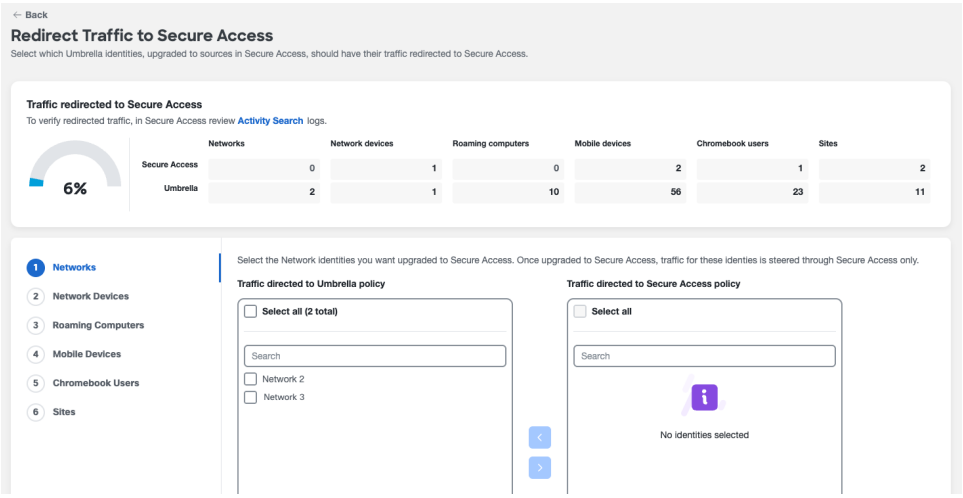


The **Redirect Traffic to Secure Access** page displays the following identity types with traffic that you can redirect to Secure Access.

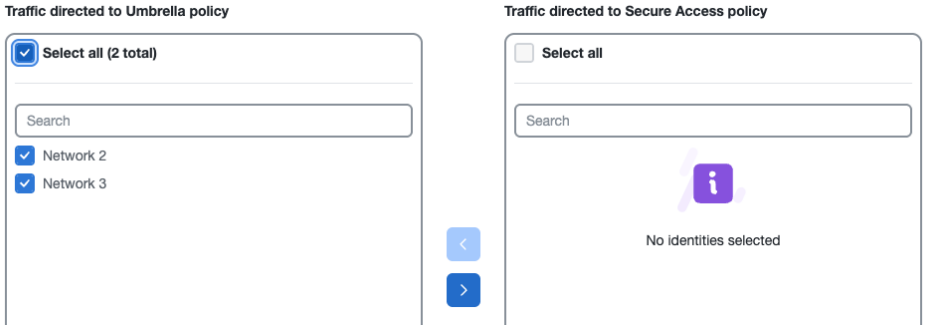
- Networks
- Network Devices
- Roaming Computers
- Mobile Devices
- Chromebook Users
- Sites

2. Click an identity type.

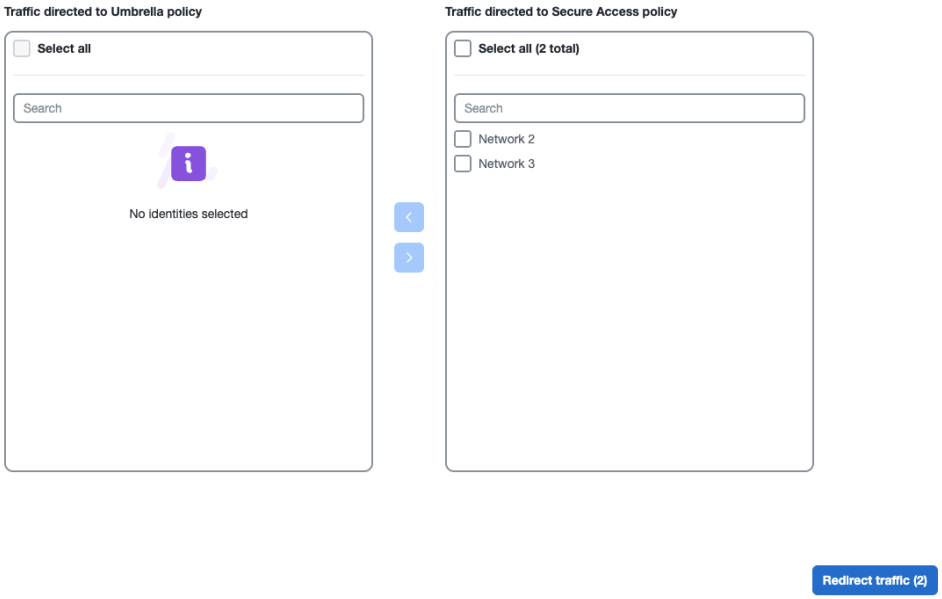
A list of the available identities of that identity type will appear in **Traffic directed to Umbrella policy**.



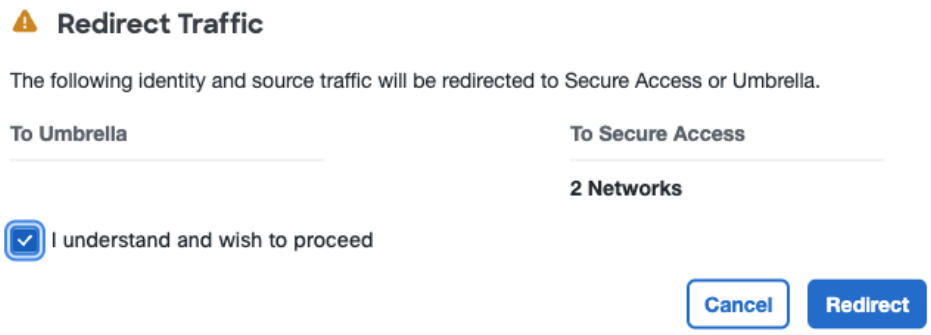
3. Select the identities to redirect traffic to Secure Access.



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

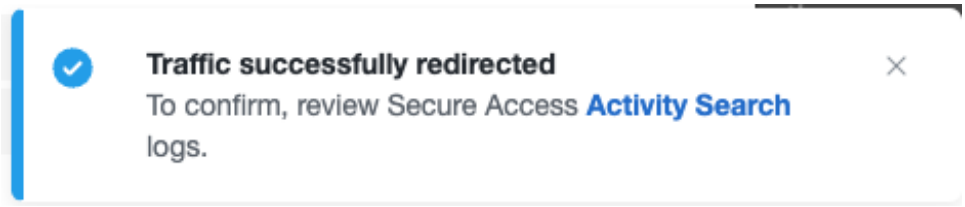


5. Click **Redirect Traffic**.
6. A pop-up message states, **The following identity and source traffic will be redirected to Secure Access or Umbrella.**



7. Check **I understand and wish to proceed**.
8. Click **Redirect**.

   After 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, refer to View and Customize the Activity Search Report.

5 Reports

Topics:

- Reports in Cisco Secure Access - DNS Defense

Describes the reports during the upgrade transition to Cisco Secure Access - DNS Defense.

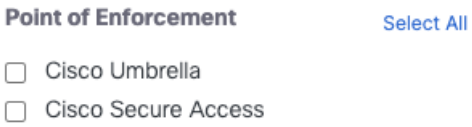
Reports in Cisco Secure Access - DNS Defense

All Umbrella reports are available in Secure Access - DNS Defense.

You can generate reports for a specific time period, with a maximum range of the last 90 days.

For more information, refer to Monitor Secure Access with Reports.

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, refer to 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 after you have completed the prerequisites, upgraded all policy rules, and directed all traffic to Secure Access.

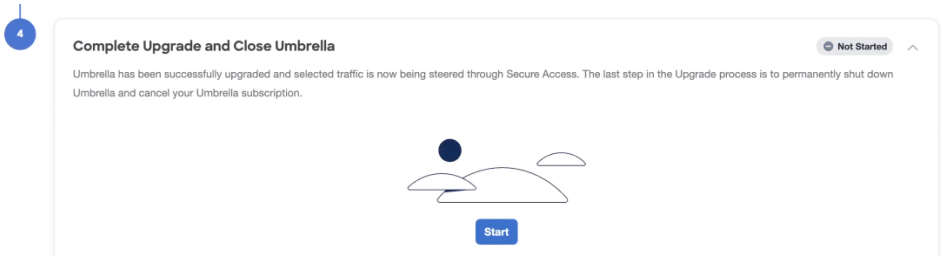
Close Umbrella

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

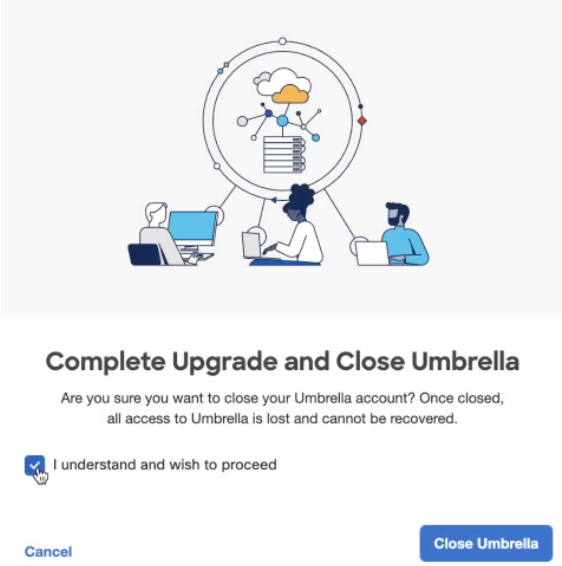
Umbrella is successfully upgraded and selected traffic are now steered through Secure Access. The last step in the Upgrade Manager is to permanently shut down Umbrella and cancel your Umbrella subscription.

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 - DNS Defense.

7 Troubleshoot Overview

Topics:

- Troubleshoot Upgrade Manager

Troubleshooting tips when upgrading from Cisco Umbrella DNS to Cisco Secure Access - DNS Defense.

The following topic discusses possible scenarios 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