



Umbrella Multi-org Console Upgrade to Secure Access Manager Organization

Cisco Secure Access

Updated September 29, 2026

1 Before You Begin

Topics:

- [Is This Guide for You?](#)
- [Welcome to Cisco Secure Access Manager Organization](#)
- [Best Practices for the Upgrade](#)
- [Guidelines and Limitations](#)
- [Prerequisites](#)
- [Upgrade Workflow for Secure Access Manager \(Parent\) Organization](#)
- [Upgrade Workflow for Secure Access Managed \(Child\) Organization](#)

Read the entire upgrade guide before attempting to upgrade.

- Read the entire upgrade guide before attempting to upgrade. Upgrade time will vary depending on the data and number of settings, objects, and policies required to move over from Umbrella Multi-org to Secure Access Manager Organization.
- Umbrella continues to operate during this process, and your organization is always protected.
- You must have Full Admin access to start the upgrade to Secure Access.
- We recommend upgrading during non-business hours.

Is This Guide for You?

Explains the audience for this guide.

This guide is for Umbrella Multiple Organizations (Multi-org) customers upgrading to Secure Access Manager Organization.

Other package types are not eligible for this upgrade at this time, including:

- Umbrella for Managed Service Provider (MSP)
- Managed Security Services Providers (MSSPs)

These packages will be eligible for upgrade in the future. To know your current Umbrella product, navigate to your managed organization Umbrella dashboard and click **Admin > Licensing**.

Welcome to Cisco Secure Access Manager Organization

Welcome to the Cisco Secure Access manager organization, where your transition from Umbrella Multi-org empowers you with a modernized, unified security platform designed for centralized control and granular rule management.

As you upgrade from Umbrella Multi-org console to Cisco Secure Access manager organization, you are transitioning to a more advanced, flexible, and unified security platform designed to enhance your organization's protection and policy management.

Secure Access offers a modernized policy model that allows you to customize and manage rules more granularly through a manager organization and multiple managed organizations. This new structure enables centralized control with delegated management, improving operational efficiency and security posture compared to Umbrella. Unlike Umbrella's policy model, Secure Access uses distinct, unified rules for allow and block actions, providing clearer rule enforcement and better traffic handling.

Best Practices for the Upgrade

Ensure a seamless transition to a Secure Access managed organization by following these best practices.

- Upgrade during non-business hours.
- The Admin of the Multi-org console who has Full Admin access to all the child organizations needs to complete the upgrade for the Multi-org console and the child organizations.
- Use the Redirect Traffic feature to redirect a subset of identities at a time. For more information on how to Redirect Traffic for the DNS upgrade, see [Overview of Redirecting Traffic](#), and for the SIG upgrade, see [Overview of Redirecting Traffic](#). We recommend a phased upgrade approach as this allows you to:
 - Test your internet access rules with a smaller group of identities or create test identities.
 - Confirm successful integration of internet access rules.
 - Identify and address any issues early.
- Create a test organization and use that organization as a trial run to upgrade to Secure Access managed organization.

Guidelines and Limitations

The Guidelines and Limitations section outlines the essential requirements and changes necessary to ensure a stable and successful upgrade process for your environment.

Upgrade Guides

For Secure Access managed organization, see our single tenant upgrade guides.

- For Umbrella DNS upgrade guide, see [Guidelines and Limitations](#).
- For Umbrella SIG upgrade guide, see [Guidelines and Limitations](#).

Manager Organization

Delete and Add Organizations During the Upgrade

Once the upgrade process has started, you cannot delete or add any additional organizations until the upgrade is complete and all Umbrella organizations have permanently closed their accounts.

Open an Umbrella support ticket if you need to delete or add organizations during the upgrade. See, [Contact Cisco Umbrella Support](#).

Integrating Identity Providers

To learn more about Third Party IdP in Security Cloud Control, see [Identity Service Provider Instructions](#) in our Cisco Security Cloud Control Administration Guide.

Centralized Settings

Block Page is called Notification pages in Secure Access. A notification page is created and then added to a Security Profile. When creating an internet access rule, you select which Security Profile you want to apply to the rule.

Content Settings (content categories) is called Content Category Lists in Secure Access. In Secure Access manager organization, you create a content category list and add to an internet access rule in the managed organization. Then, you share the internet access rule with any of your managed organizations.

Destination Lists

In Umbrella's Multi-org, you create a single destination list to share among organizations. In Secure Access manager organization, you create a destination list and add to an internet access rule. Then, you share the internet access rule with any of your managed organizations.

Security Settings in Umbrella is called Threat Categories in Secure Access. Threat categories are customized and then applied to a Security Profile. When creating an internet access rule, you select which Security Profile you want to apply to the rule.

Advanced Setting

Advanced Settings change when you are upgrading from Umbrella. Advanced settings are now located in the Security Profile in Secure Access. Security Profile contains multiple components that are reusable for internet access rules. You must create a Security Profile to use these settings in internet access rules.

Custom Integrations

Your Umbrella custom integrations do not upgrade to Secure Access. Currently, Secure Access does not have API's to update destination lists to block destinations. During the upgrade, the Umbrella destination list is copied to Secure Access as is and is no longer updated by the API.

Policy Limitations

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.

Prerequisites

Before initiating the upgrade, ensure you meet these essential prerequisites.

Before starting the upgrade, ensure the following:

- You have **Full Admin access** to your Umbrella Multi-org Console.

- Your Umbrella subscription is active and in good standing.

Upgrade Workflow for Secure Access Manager (Parent) Organization

This topic provides an overview of the centralized policy management workflow for upgrading to a Secure Access manager organization.

The upgrade workflow follows a centralized policy management approach. Complete the following steps to finalize your migration:

Procedure

1. [Setting up your Secure Access Manager Organization in Security Cloud Control.](#)
 2. [Step 1: Review Auto-Upgraded Objects.](#)
 3. [Step 2: Configure Security Profile.](#)
 4. [Step 3: Add and Share Access Rules with Managed Orgs.](#)
 5. [Step 4: Upgrade Umbrella Child Orgs.](#)
-

Upgrade Workflow for Secure Access Managed (Child) Organization

Directs administrators to the applicable single-tenant upgrade workflow for Secure Access managed child organizations, pointing to separate DNS and SIG guidance for completing the migration steps.

Navigate to our single tenant upgrade guides for these steps.

- For Umbrella DNS upgrade guide, see [Upgrade Workflow](#).
- For Umbrella SIG upgrade guide, see [Upgrade Workflow](#).

2 Upgrade from Umbrella Multi-org Console to Secure Access Manager Organization

Topics:

- [Centralized Policy Management](#)
- [Setting up your Secure Access Manager Organization in Security Cloud Control](#)
- [Overview for Umbrella Organization Upgrade to Secure Access Managed Organization](#)
- [Overview of Org Management Upgrade Status](#)

Umbrella continues to operate during this upgrade process, and your organization is always protected.

Centralized Policy Management

When you upgrade from Umbrella Multi-org to Secure Access, centralized settings move to the manager organization, which uses them to create and share internet access rules with managed organizations.

When you upgrade from Umbrella Multi-org to Secure Access managed organization, most of your existing Umbrella Centralized Settings—Destination Lists, block pages, content settings, security settings, and advanced settings—are copied to the Secure Access manager (parent) organization. These settings are then used to create internet access rules that are centrally managed at the manager organization level.

Key Points to Understand

- **Centralized Settings Transfer:** If an Umbrella (child) organization has policies containing Centralized Settings from Umbrella's Multi-org, those policies upgrade to Secure Access, but the Centralized Settings themselves do not copy over to the managed organization in Secure Access. Instead, these settings reside in the manager organization.
- **Internet Access Rules Sharing:** Once your child organizations complete their upgrade, the manager organization shares the centrally managed internet access rules with them. This ensures consistent and centralized policy enforcement across your entire organization.
- **Legacy Features:** Umbrella's Custom Integrations is a legacy feature that is not supported and does not transfer to Secure Access.
- **Managed Organization Policy Behavior:** If a child organization has policies containing Centralized Settings, those policies upgrade to Secure Access, but the Centralized Settings themselves remain in the manager organization. The manager organization uses those settings in the internet access rules and shares with managed organizations.
- **Administrator Notification:** Inform administrators of your managed organizations that after upgrading, they will not see the shared Centralized Settings directly in their internet access rules. Let them know that the manager organization shares them as needed with the managed organizations. This communication helps prevent the creation of duplicate or conflicting rules within managed organizations.
- **Post-Upgrade Customization:** After the upgrade is complete, you can create new settings and internet access rules in both manager and managed organizations to tailor policies as needed.

Setting up your Secure Access Manager Organization in Security Cloud Control

This topic describes how to upgrade your Umbrella multi org account to a Secure Access manager organization within Security Cloud Control.

Cisco Security Cloud Control lets you manage all your Cisco security products from one integrated platform. You can quickly set up your subscriptions and easily assign roles and permissions to users and groups. The platform features intuitive navigation, unified documentation, global search, and shared objects to streamline your workflows.

Security Cloud Control centralizes platform management for consistent access and deployment across products including Secure Access.

The Umbrella admin who receives the subscription claim code is responsible for completing the subsequent steps to activate the **upgrade feature** for the Secure Access manager organization in Security Cloud Control.

Before you begin

- Ensure that the Umbrella admin activating the upgrade tool uses the same email address that was used to create the Security Cloud Control platform. Using a different email prevents your Umbrella multi org from linking to the correct Security Cloud Control platform.

Procedure

1. Place your change order for Secure Access in Cisco Commerce Workspace (CCW).

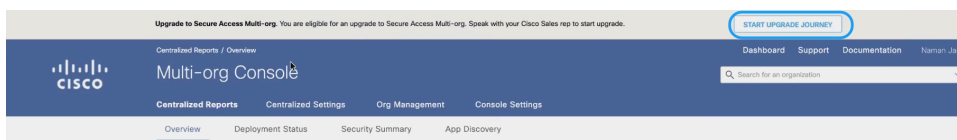
Once the order is complete, you receive a welcome email from **no-reply-security@cisco.com** that contains a claim code.



Note

Do not click on the link in the email and do not enter your subscription claim code in Security Cloud Control. This action creates a new single tenant organization that does not upgrade your existing Umbrella Multi-Org.

2. Log in to your Umbrella Multi-Org account.



3. In the banner, click **Start Upgrade Journey**, enter the claim code, and click **Start Upgrade**.

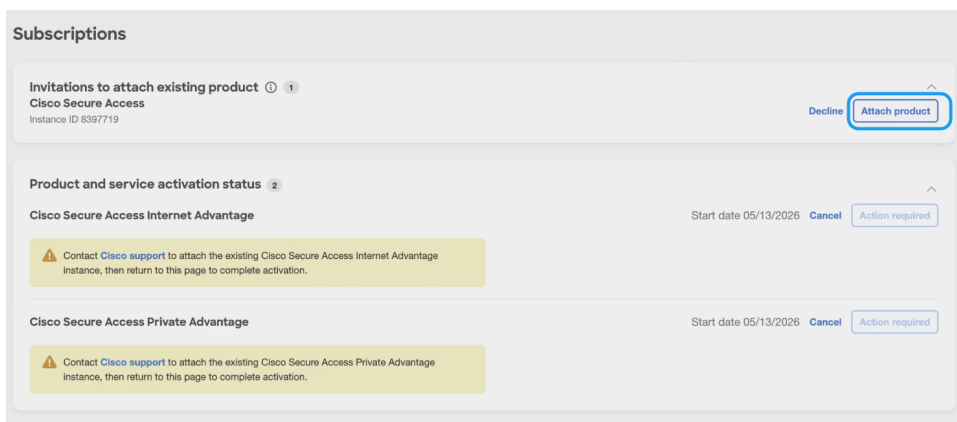
Upgrade to Secure Access Multi-org

A claim code was sent to you from no-reply-security@cisco.com with subject: 'Welcome to Cisco Security Cloud'. If you don't have the code or will like to request it again, contact your Cisco Sales representative.

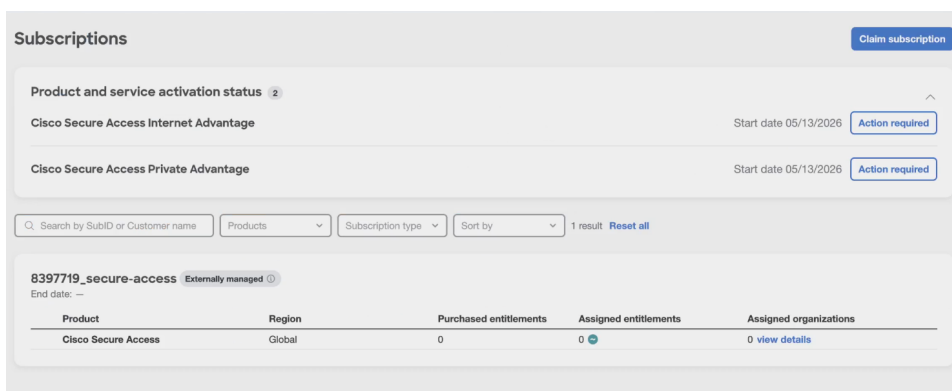
Claim code

[CANCEL](#) [START UPGRADE](#)

4. Once the claim code is validated, the Secure Access manager organization is created. Click **Secure Access Manager** to redirect to Security Cloud Control.
5. In Security Cloud Control, navigate to **Subscriptions & Services Management** and click **Attach Product**.



6. Click **Attach** in the banner to link the manager organization to this instance.
A success notification appears when the Secure Access managed organization is attached.
7. Click **Action required** for the product, such as Cisco Secure Access DNS or SIG.



8. Click **Apply license**. A success notification appears confirming that the Cisco Secure Access manager organization is linked to the Security Cloud Control platform.
Your Secure Access manager organization now appears under **Product > Secure Access** in the Security Cloud Control navigation menu.

What to do next

After successfully setting up your Secure Access manager organization, navigate to **Product > Secure Access > Overview** to complete the following migration steps:

1. Review auto upgraded objects: Verify the objects transitioning to Secure Access. See [Step 1: Review Auto-Upgraded Objects](#).
2. Configure security profile: Set up the security profiles required for your internet access rules. See [Step 2: Configure Security Profile](#).
3. Add and share access rules with managed organizations: Define and distribute access rules across your organization. See [Step 3: Add and Share Access Rules with Managed Orgs](#).
4. Upgrade Umbrella child organizations: Perform the final migration steps for your child organizations. See [Step 4: Upgrade Umbrella Child Orgs](#).

Step 1: Review Auto-Upgraded Objects

This topic describes how to review objects transitioning to Secure Access during the upgrade process.

The upgrade process requires a review of objects transitioning to Secure Access. Note that Umbrella advanced settings change in Secure Access and are now located in the security profile. You must create a security profile to use these settings in internet access rules.

Procedure

1. Navigate to **Product > Secure Access > Overview**.
2. Click Continue upgrade to open the upgrade stepper interface.
3. **Auto-upgraded:** Click **Review** to review the information regarding objects that are automatically upgraded from the Umbrella multi organization to the managed organizations.
These objects, such as content category lists, threat categories, destination lists, and block pages, remain consistent in Secure Access.
4. **Not upgraded:** Click **Review** to review the objects that will change when you upgrade to Secure Access.
5. Click **Mark as Done**.

What to do next

Continue to Step 2: Configure Security Profile.

Step 2: Configure Security Profile

This topic describes how to review and configure security profiles to manage reusable components for access rules.

In Umbrella's Multi-org console, you use the Centralized Settings to configure individual settings (Destination Lists, Block Pages, Content Settings, and Security Settings) to share with each organization. Each organization would use these settings in their policies.

In Secure Access, you can configure majority of these settings also known as components in the Security Profile. A Security Profile is a reusable component that you include in access policy rules. Review and configure the Security profiles before creating any rules.

For a list of the components in Secure Access DNS, see [Functionality Included in a Security Profile for Internet Access](#) in our Cisco Secure Access DNS–Defense Help.

For a list of the components in Secure Access, see [Functionality Included in a Security Profile for Internet Access](#) in our Cisco Secure Access Help.

**Note**

Destination Lists and Content settings (content categories) are configured in the **Internet and SaaS Resources** section in Secure Access. You can then add these destinations to an internet access rule.

Procedure

1. Click **Security Profiles**.
2. Click to expand the **System Provided – Internet Access**.
3. Review the settings and components .

What to do next

Step 3: Add and Share Access Rules with Managed Orgs.

Step 3: Add and Share Access Rules with Managed Orgs

This topic describes how to create and share internet access rules from a manager organization to managed organizations.

Managed rules are created by the manager organization and shared with managed organizations. Managed rules appear at the top of the managed organization's Access policy list, ensuring they take precedence over local rules. Managed rules are generally broad rules that are shared across organizations. Managed organizations can view these managed rules, they cannot edit or remove them.

Rule Processing

Traffic is evaluated against the rule list in order. Since managed rules are positioned at the top, they are processed first; any traffic matching a managed rule is handled accordingly, and subsequent rules lower in the list are not applied.

Manager Organization Responsibilities

- **Create and Configure:** Define internet access rules, security profiles, and associated settings.
- **Share:** Distribute these rules to managed organizations to ensure consistent policy enforcement.

**Note**

The managed organization must complete the upgrade process (**Step 2: Start Upgrade**) before you can share any internet access rules.

- For Umbrella DNS managed organizations, see [Start Upgrade](#).
- For Umbrella SIG managed organizations, see [Overview to Start Upgrade](#).

Add an Internet Access Rule in Manager Organization

Provides instructions for creating an internet access rule in a Secure Access Manager Organization, sharing it with managed organizations, and verifying that the shared rule appears in the managed organization's policy list.

The steps to add an internet access rule for a Secure Access manager organization is the same as a single tenant organization. The only difference is at the last step when you share the rule with the managed organizations.

Procedure

1. Log in to your Secure Access manager organization through [Security Cloud Control](#).
2. Configure Security Profile.
 - a) For DNS navigate to our Cisco Secure Access – DNS Defense Help, [Security Profiles for Internet Access](#).
 - b) For SIG navigate to our Cisco Secure Access Help, [Security Profiles for Internet Access](#).
3. Navigate to **Secure Access > Access Policy > Add Rule > Internet Access**.
4. Follow the detailed steps on how to create an internet access rule by navigating to:
 - a) Cisco Secure Access – DNS Defense Help, [Get Started With Internet Access](#).
 - b) Cisco Secure Access Help, [Get Started With Internet Access](#).
5. Select the managed organizations to share the internet access rule with. Click **Save**.
If a managed organization is not visible in the list, the Umbrella child organization must first complete Step 2: Start Upgrade in their dashboard to successfully link to their Secure Access organization in Security Cloud Control.

What to do next

Navigate to the managed organization to see the Secure Access manager organization's internet access rule added to the list of Managed Rules.

Step 4: Upgrade Umbrella Child Orgs

This topic describes how to migrate Umbrella child organizations to Secure Access managed organizations.

Before you begin

Ensure that the parent organization migration is complete.

Procedure

1. Create a Secure Access managed organization that is attached in Security Cloud Control. For instructions, refer to [Manually Add Umbrella's Child Org as a Secure Access Managed Organization](#).
 - a) (Optional) Add the admins after you create the Secure Access managed organization.

2. You begin the process of upgrading the settings and policies from the Umbrella child organization to Secure Access managed organization.
 - For Umbrella DNS follow the steps in [Cisco Umbrella DNS to Cisco Secure Access - DNS Defense Upgrade Guide](#).
 - For Umbrella SIG follow the steps in [Cisco Umbrella SIG Upgrade Guide to Cisco Secure Access](#).
3. Repeat these steps for all child organizations.
4. Click **Close Umbrella parent console** once all the Umbrella child organizations have completed all the steps to upgrade to Secure Access managed organization and closed their Umbrella account.
This step permanently closes your Umbrella Multi-org console. This action cannot be reversed.

What to do next

Your traffic is now steered through Secure Access. To learn more about Security Cloud Control and Secure Access, see our [additional documentation](#).

Overview for Umbrella Organization Upgrade to Secure Access Managed Organization

Guides administrators through planning and completing the Umbrella Multi-org migration to a Secure Access Manager Organization. It explains centralized policy management, manager organization setup, review of upgraded objects, security profile configuration, internet access rule creation and sharing, child organization migration, and upgrade status tracking.

Before you begin upgrading the Umbrella child organization, ensure that the admin of the manager organization has completed the initial steps to add your Umbrella child organization to Security Cloud Control.

For more information, see [Manually Add Umbrella's Child Org as a Secure Access Managed Organization](#).

The steps to upgrade the Umbrella child organization is similar to the process of a single tenant upgrading from Umbrella to Secure Access.

Navigate to Upgrade Workflow for Secure Access Managed Organization to see the steps.

Manually Add Umbrella's Child Org as a Secure Access Managed Organization

Guides administrators through creating a Secure Access managed organization in Security Cloud Control, attaching the existing Umbrella child organization, assigning seats and optional admin groups, and linking the product subscription before completing the managed organization upgrade.

Create the Secure Access managed organizations in Security Cloud Control's platform.

Procedure

1. In Security Cloud Control navigate to **Managed Organizations > + Add organization > Existing organization**.
2. Enter your Umbrella's organization name as it appears in the Multi-org console.
3. Do not enter a subscription claim code. Click **Save** or **Skip** to go to the next step.
The subscription claim code was already claimed at the initial request when creating a Security Cloud Control for the Secure Access manager organization.
4. Enter the number of seats to assign to this managed organization.
This should match the number of seats for your Umbrella organization.
5. Select **Attach existing instance** from the Select instance type drop-down list. Click **Save**.
Do not select New Instance - this creates a new organization that will not map your existing Umbrella account.

6. (Optional) In the drop-down list select any admin groups from the manager organization that need to be added to this managed organization. Click **Save** or **Skip**.
After the upgrade, you can add admins by following the steps in our Cisco Security Cloud Control Administration Guide on how to [Invite a User](#).
7. In the left-hand navigation, click on **Manager Organization** > In the **All organizations** list, click on the managed organization's name.
8. Click **Switch to this organization**. Click **Proceed**.
You have created a new Secure Access managed organization in Security Cloud Control, but you need to attach the existing Umbrella child organization to start upgrading the settings and policies over.
9. Navigate to the Umbrella child organization's dashboard > **Admin** > **Licensing**>**Request Invitation**.
 - a) The admin with access to Security Cloud Control can initiate the request, and that same admin needs to complete the upgrade process for the managed organization.
 - b) The admin receives an invitation email to **Attach Your Product to Cisco Security Cloud**.
 - c) Click the link in your email to login to your Security Cloud Control. The admin that activated the Upgrade Manager must use the same email address to create the Security Cloud Control.
10. Click **Platform Management** > **Subscriptions** > **Attach product**.
11. Click **Attach**.
12. Click **Action required**.
13. Click **Apply license**.
A success notification appears that Cisco Secure Access managed organization is linked to the Security Cloud Control.

What to do next

Your Secure Access managed organization now appears Security Cloud Control's left-hand navigation, under Managed Organizations.

You or another admin must complete the steps to complete the upgrade for the managed organization to Secure Access.

- For DNS Upgrade follow steps 2 - 6 in the [Upgrade Workflow](#).
- For SIG Upgrade follow steps 2 - 6 in the [Upgrade Workflow](#).

Overview of Org Management Upgrade Status

Org Management page shows the managed organizations upgrade status.

Org Management page shows the managed organizations upgrade status.

- **Not started:** Indicates that the upgrade process for the managed organization has not yet begun. This means that no traffic has been redirected to Secure Access, and the organization continues to operate entirely within Cisco Umbrella.
- **In progress:** The managed organization has started the upgrade process.
- **Complete:** All traffic for the organization is redirected from Umbrella to Secure Access and the Umbrella organization is permanently closed.

A Appendix

Topics:

- [Frequently Asked Questions](#)
- [Additional Documentation and Support](#)

Includes frequently asked questions and links for additional information and support.

Frequently Asked Questions

Frequently asked questions about the Umbrella Multi-org upgrade.

1. For General FAQs for Security Cloud Control navigate to [General FAQs](#).
2. What if I claimed the subscription code in Security Cloud Control instead of opening a TAC case?
 - This creates a new single tenant Secure Access organization that is not linked to your Umbrella Multi-org console.
 - You need to [open a TAC case](#) and ask Cisco Support to create and link a Secure Access manager organization with your Umbrella Multi-org.
3. What if my policies and rules did not copy over correctly?
 - Review the Umbrella DNS Upgrade guide to see how policies are structured in Secure Access. Navigate to [Getting Started with Internet Access Rules](#).
 - Review the Umbrella SIG Upgrade guide to see how policies are structured in Secure Access. Navigate to [Getting Started with Internet Access Rules](#).

Additional Documentation and Support

Additional documentation and support for Security Cloud Control and Secure Access.

Additional Documentation

[Security Help Center](#)

[Security Cloud Control Getting Started Guide for Existing Customers](#)

[Cisco Security Cloud Control Administration Guide](#)

[Browsers Supported by Security Cloud Control](#)

[Getting Started with Security Cloud Control Multi-Organizations](#)

[Security Cloud Control Multi-Organizations](#)

[Secure Access Multi-Organization Guide](#)

[Cisco Secure Access DNS Defense Help](#)

[Cisco Secure Access Help](#)

Contact Support

Navigate to [Cisco Worldwide Support Contacts](#) and open a TAC case.