Manage Tenants and Users

Manage a Security Cloud Control Tenant

Security Cloud Control gives you the ability to customize certain aspects of your tenant, users, and notification preferences. Review the following settings available for customized configuration:

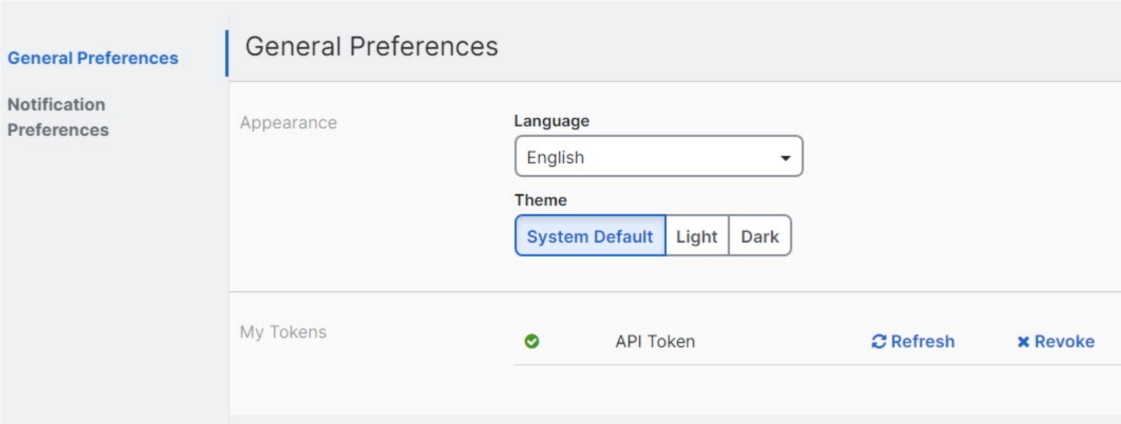
Configure User Preferences

See the following topics regarding general Security Cloud Control Settings:

- General Preferences, on page 1
- User Notification Preferences

General Preferences

Select the desired language and theme for the Security Cloud Control UI to display in. This selection only affects the user who makes this change.



General Preferences

Notification Preferences

General Preferences

Appearance

Language: English

Theme: System Default | Light | Dark

My Tokens

✓ API Token — Refresh — Revoke

Change the Security Cloud Control Web Interface Appearance

You can change the way the web interface appears.

Procedure

Step 1 From the drop-down list under your username, choose **Preferences**.

Step 2 In the **General Preferences** area, select a **Theme**:

- **Light**
- **Dark**

User Notification Preferences

Security Cloud Control generates notifications whenever a device linked to your tenant encounters a specific event. This includes actions taken by the device, expiring or expired device certificates, or the start, completion, or failure of a report generation task. By default, these notifications are enabled and visible to all users associated with the tenant, regardless of their role. You have the option to customize your personal notification preferences to display only the alerts that interest you. These preferences are unique to you and do not impact other users connected to the tenant.

Note Changes made to the notifications listed below are automatically updated in real time and do not require deployment.

View your personal preferences in the **Username ID** > **Preferences** > **Notification Preferences** page. Your Username ID is always located in the upper right corner of Security Cloud Control across all pages. From this page you can configure the following "**Notify Me in Security Cloud Control When**" alerts.

Send Alerts for Device Workflows

- **Deployments** - This action does not include integration instances for SSH or IOS devices.

- **Backups** - This action is only applicable for FDM-managed devices.
- **Upgrades** - This action is only applicable for ASA and FDM-managed devices.
- **Migrate FTD to cloud** - This action is applicable when changing the FTD

  device manager from FMC to Security Cloud Control.

Send Alerts for Device Events

- **Went offline** - This action applies to all devices associated with your tenant.
- **Back online** - This action applies to all the devices associated with your tenant.
- **Conflict detected** - This action applies to all the devices associated with your tenant.
- **HA state changed** - This action indicates the device within an HA or failover pair, the current state, and the state it changed from. This action applies to all HA and failover configurations associated with your tenant.
- **Site-to-Site session disconnected** - This action applies to all site-to-site VPN configurations configured in your tenant.

Send Alerts for Event Search Report Generation

- **Report generation started**: Receive a notification when a report generation task starts. This applies to both immediate and scheduled search reports.
- **Report generation completed**: Receive a notification when a report generation task ends. This applies to both immediate and scheduled search reports.
- **Report generation failed**: Receive a notification when a report generation task fails. This applies to both immediate and scheduled search reports. Check the parameters or the query and try again.

Opt Out of Notification Preferences

By default, all events are enabled and generate notifications. To opt out of notifications generated by the events mentioned above, you must manually **uncheck** the notification types. Note that you must click **Save** to confirm any changes.

Email Alerts

Enable the **Email Alerts** toggle to receive any of the alerts mentioned above. Check which alerts you would like to receive by email and click the **Save** button. By default, the **Use Security Cloud Control notification settings above** is checked. This means that you will receive email alerts on all of the same notifications and events as you have checked in the "Send Alerts When..." sections mentioned on this page.

If you only want **some** of the events or alerts mentioned above forwarded to your email, uncheck the **Use Security Cloud Control notification settings above"**. This action generates an additional location to modify and personalize the available alerts. This may help reduce redundancy.

View Security Cloud Control Notifications

Click the notifications icon 🔔 to view the most recent alerts that have occurred or affected the devices you have onboarded to your tenant. The selections that you make in the **Notification Settings** page impact the types of notifications displayed in Security Cloud Control. Continue reading for more information.

This drop-down page is grouped into three tabs: Overview, All, and Dismissed.

Overview Tab

The **Overview** tab displays a combination of the most recent high-priority alerts and events to which you are subscribed. High priority events are the following:

- Deployment Failed
- Backup Failed
- Upgrade Failed
- Migrate FTD to cdFMC Failed
- Device went offline
- Device HA state changed
- Device certificates expiring

You can configure which alerts you want to receive by clicking the Notification Settings in the Notifications window or by selecting **UserID** > **User Preferences** page. The User ID button in the upper right corner of the dashboard.

All Tab

The **All** tab displays all notifications regardless of their priority ranking, including email subscription notifications and all of the items listed as high priority.

Dismissed Tab

The **Dismissed** tab displays notifications you have dismissed. You can dismiss individual notifications by clicking the "**x**" of the notification.

Opting to **Dismiss** notifications from the drop-down menu dismisses notifications from **both** the "Overview" and "All" tabs. They will remain in the **Dismiss** tab for 30 days, after which they will be removed from Security Cloud Control.

Search Notifications

When viewing the notifications drop-down window, for any of the tabs mentioned above, you can use the search bar at the top of the drop-down to query for key words or alerts.

Tenant Settings

Enable Change Request Tracking

Enabling change request tracking affects all users of your tenant. To enable Change Request Tracking, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the slider under **Change Request Tracking**.

Once confirmed, you see the Change Request toolbar appear in the lower left corner of the interface and the Change Request drop-down menu in the Change Log.

Prevent Cisco Support from Viewing your Tenant

Cisco support will associate its users with your tenant to resolve support tickets or proactively fix issues that affect more than one customer. However, if you prefer, you can prevent Cisco support from accessing your tenant by changing your account settings. To do so, slide the toggle button under **Prevent Cisco support from viewing this tenant** to show a green check mark.

To prevent Cisco support from viewing your tenant, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the slider under **Prevent Cisco support from viewing this tenant**.

Enable the Option to Auto-accept Device Changes

Enabling auto-accept for device changes allows Security Cloud Control to automatically accept any changes made directly on the device. If you leave this option disabled, or disable it at a later time, you are required to review each device conflict before you can accept it.

To enable auto-accept for device changes, follow this procedure:

Procedure

Step 1 In the left pane, **Administration** > **General Settings**.

Step 2 Click the slider under **Enable the option to auto-accept device changes**.

Default Conflict Detection Interval

This interval determines how often Security Cloud Control polls onboarded devices for changes. This selection affects all devices managed with this tenant, and can be changed at any time.

Note This selection can be overridden via the **Conflict Detection** option available from the **Security Devices** page after you have selected one or multiple devices.

To configure this option and select a new interval for conflict detection, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the drop-down menu for **Default Conflict Detection Interval** and select a time value.

Enable the Option to Schedule Automatic Deployments

Enabling the option to schedule automatic deployments allows you to schedule future deployments at a date and time when it is convenient. Once enabled, you can schedule a single or a recurring automatic deployment. To schedule an automatic deployment, see Schedule an Automatic Deployment.

Note that changes made on Security Cloud Control for a device are not automatically deployed to the device if it has pending changes of its own . If a device is not in the **Synced** state, such as **Conflict Detected** or **Not Synced**, scheduled deployments are not executed. The jobs page lists any instance where a scheduled deployment fails.

If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

Important If you use Security Cloud Control to create more than one scheduled deployment for a device, the new deployment overwrites the existing deployment. If you create more than one scheduled deployment a device using API, you **must** delete the existing deployment prior to schedule the new deployment.

To enable the option to schedule automatic deployments, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the slider under **Enable the option to schedule automatic deployments**.

Web Analytics

Web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous and no sensitive data is transmitted.

Web analytics is enabled by default. To disable web analytics, or to enable in the future, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the toggle under **Web Analytics**.

Share Event Data with Cisco Talos

When you enable the **Enable event data sharing with Talos** toggle button, data about malicious events present in your device is shared with Talos, Cisco's threat intelligence organization. Sharing event data helps Talos improve its threat detection and response capabilities, allowing it to provide more targeted security updates for your network and better protection against emerging threats.

For more information about Talos, see the Cisco Talos product page.

Sharing event data with Talos is enabled by default. To opt out, follow this procedure:

Procedure

Step 1 In the left navigation bar, click **Administration** > **General Settings**.

Step 2 Click the **Enable event data sharing with Talos** toggle button to disable the setting.

Note
Sharing event data enables Talos to provide relevant security insights for your network. Disabling this setting might limit your ability to fully leverage Talos' capabilities, potentially impacting your network's defense against evolving threats.

Tenant ID

Your tenant ID identifies your tenant. This information will be helpful if you need to contact the Cisco Technical Assistance Center (TAC).

Tenant Name

Your tenant name also identifies your tenant. Note that the tenant name is not the organization name. This information will be helpful if you need to contact the Cisco Technical Assistance Center (TAC).

Security Cloud Control Platform Navigator

The platform navigator is a nine-block applications cross-launcher (⊞) that appears on the top right corner of Security Cloud Control. You can readily cross-launch to the following Cisco networking and security applications:

Networking Applications

- **Catalyst**—Cisco Catalyst products include a wide variety of network switches, wireless controllers, wireless access points, and edge platforms and routers, supporting enterprise-class business needs to heavy-duty and rugged networking environments.
- **Intersight**—Cisco Intersight is a cloud operations platform that consists of optional, modular capabilities of advanced infrastructure, workload optimization, and Kubernetes services. Cisco Intersight infrastructure services include the deployment, monitoring, management, and support of your physical and virtual infrastructure. It supports Cisco Unified Computing System (Cisco UCS) and Cisco HyperFlex hyperconverged infrastructure (HCI), and other third-party Intersight-connected targets.
- **IoT Operations Dashboard**—Cisco IoT Operations Dashboard is a cloud-based IoT services platform that empowers operations teams to securely connect, maintain, and gain insights from industrial networking devices and connected industrial assets at massive scale. With one comprehensive view of all their connected industrial assets, operation teams can uncover valuable insights that help them streamline operations and drive business continuity.
- **Meraki**—Cisco Meraki is an IT and IoT cloud-managed platform that provides a centralized management platform for Cisco Meraki devices.
- **Spaces**—Cisco Spaces is a cloud-based location services platform through which organizations can gain insights into how people and things move throughout their physical spaces. With these insights, they can deliver contextual engagements that are valuable and relevant. Besides looking at where people go, organizations can also drive operational efficiencies by monitoring the location, movement, and utilization of assets.
- **ThousandEyes**—Cisco ThousandEyes is a cloud service suite that helps monitor and measure the availability and performance of web applications, services, and networks. It provides end-to-end visibility from any user to any application over any network, enabling enterprises to swiftly get to the source of issues, resolve them faster, and manage performance effectively.
- **Workflows**—Cisco Workflows is a cloud-hosted automation application that is part of the larger Cisco Networking Cloud vision. Workflows provides an entitlement to cross-domain automation capabilities to current Cisco customers by streamlining repetitive and error-prone tasks across both Cisco and third-party applications through custom and premade automation templates and a plethora of adapter options, both provided by Cisco and build your own, to reach targets in the cloud or on-premises.

Security Applications

- **Duo Security**—Cisco Duo is a user-centric zero-trust security platform with two-factor authentication to protect access to sensitive data for all users, devices, and applications. It offers features such as adaptive policies, single sign-on (SSO), and advanced endpoint visibility, making it a comprehensive solution for securing remote access and maintaining business continuity.
- **Secure Access**—Cisco Secure Access simplifies IT operations through a single, cloud-managed console, unified client, centralized policy creation, and aggregated reporting. Extensive security capabilities converged in one solution (ZTNA, SWG, CASB, FWaaS, DNS security, RBI and more) mitigate security

risk by applying zero trust principles and enforcing granular security policies. Market leading Talos threat intelligence fuels unmatched threat blocking to mitigate risk and speed investigations.

- **Secure Endpoint**—Cisco Secure Endpoint, formerly known as Cisco AMP for Endpoints, is a cloud-managed endpoint security solution designed to prevent breaches and rapidly detect, contain, and remediate threats. It is an instant check of your files against a cloud-based scanner with advanced tracking features that enable security analysts to determine and isolate initial sources of outbreaks, and it provides a retrospective quarantine of files that are discovered to be malicious.
- **Cisco Security Provisioning and Administration**—Cisco Security Provisioning and Administration is a web application that provides centralized management of Cisco Secure product instances, user identity, and user access management across Cisco Security Cloud. Security Cloud Control administrators can create new Security Cloud enterprises, manage users in an enterprise, claim domains, and integrate their organization’s SSO identity provider, among other tasks.
- **XDR**—Cisco Extended Detection and Response (XDR) is a cloud-based solution designed to simplify security operations and empower security teams to detect, prioritize, and respond to sophisticated threats. By integrating both Cisco and third-party security solutions into a unified platform, Cisco XDR offers a comprehensive approach to threat management. Integrated with the threat intelligence provided by Talos, Cisco XDR enriches incident data with additional context and asset insights, reducing false positives and enhancing overall threat detection, response, and forensic capabilities.

Tenant Notification Settings

On the Security Cloud Control toolbar, click the notification button 🔔.

All users associated with your tenant will automatically see these alerts. In addition, some or all of these alerts can be emailed to you.

Note You must have an **Super Administrator** user role to change these settings. See User Roles for more information.

Email Subscribers

Add or modify the emails that receive alerts from your Security Cloud Control tenant. See Enable Email Subscribers, on page 9 for more information.

Service Integrations

Enable Incoming Webhooks on your messaging app and receive Security Cloud Control notifications directly to your app dashboard. See Enable Service Integrations for Security Cloud Control Notifications for more information.

Enable Email Subscribers

An email notification from Security Cloud Control denotes the type of action and the affected devices.

For further information about the current state of your devices and the content of the action, we recommend logging into Security Cloud Control and examining the Change Log of the affected devices.

Warning Be sure to enter the correct email if you are adding a mailer. Security Cloud Control does not check email addresses against known users associated with your tenant.

Add an Email Subscription

Before you begin

You must be an **Admin** to view the email subscription list, and a **SuperAdmin** to add, remove, or edit email subscriptions.

Procedure

Step 1 In the left pane, click **Administration** > **Notification Settings**.

Step 2 Click the **+** icon in the upper right corner of the page.

Step 3 Enter a valid email address in the text field.

Step 4 Check and uncheck the appropriate checkboxes for events and alerts you want the subscriber to be notified about.

Step 5 Click **Save**. At any point, click **Cancel** to create the new email subscription for the tenant.

Edit Email Subscriptions

Before you begin

You must be an **Admin** to view the email subscription list, and a **SuperAdmin** to add, remove, or edit email subscriptions.

Procedure

Step 1 In the left pane, click **Administration** > **Notification Settings**.

Step 2 Locate the email address you want to enable to edit for email subscriptions.

Step 3 Click the **Edit** icon.

Step 4 Edit the following attributes for Security Cloud Control to send alerts to the configured email address:

- **Email address**
- **Device Workflows**
- **Device Events**
- **Event Log Reports**

Step 5 Click **Ok**. At any point, click **Cancel** to negate any changes made to the email subscription.

Delete an Email Subscription

Use the following procedure to delete a mailer from the email subscription list.:

Before you begin

You must be an **Admin** to view the email subscription list, and a **SuperAdmin** to add, remove, or edit email subscriptions.

Procedure

Step 1 In the left pane, click **Administration** > **Notification Settings**.

Step 2 Locate the user you want to remove from email subscriptions for the tenant.

Step 3 Click the **Remove** icon for the user you want to remove.

Step 4 Confirm you want to remove the user from the subscription list. Note that this does not affect the user functionality in any way.

Enable Service Integrations for Security Cloud Control Notifications

Enable service integration to forward Security Cloud Control notifications through a specified messaging application or service. You need to generate a webhook URL from your messaging application and point Security Cloud Control to that webhook in Security Cloud Control's **Notification Settings** page to receive notifications.

Security Cloud Control natively supports Cisco Webex, Microsoft Teams, and Slack as service integrations. Messages sent to these services are specially formatted for channels and automated bots.

Note You must check the appropriate boxes for the notifications you want to receive per webhook.

Incoming Webhooks for Webex Teams

Before you begin

Security Cloud Control notifications appear in a designated workspace or as an automated bot in a private message. You must have the following before completing this procedure:

- A Webex account.
- A Security Cloud Control account and tenant.

Use the following procedure to allow incoming webhooks for Webex Teams:

Procedure

Step 1 Open the Webex apphub.

Step 2 Click **Connect** at the top of the page.

Step 3 Scroll to the bottom of the page and configure the following:

- **Webhook name** - Provide a name to identify the messages provided by this application.
- **Select a space** - Use the drop-down menu to choose a Webex **Space**. The Space must already exist in Webex team and you must have access to this space. If a space does not exist, you can create a new space in Webex Teams and refresh the application's configuration page to display the new space.

Note
If a Webex incoming webhook has been configured in the past and you are re-enabling it, the previous webhooks are preserved at the bottom of this page. You can delete previous webhooks if they are no longer needed or if the Webex space no longer exists.

Step 4 Select **Add**. The Webex Space you chose will receive a notification that the application is added.

Step 5 Copy the Webhook URL.

Step 6 Log into Security Cloud Control.

Step 7 In the left pane, click **Administration** > **Notification Settings**.

Step 8 Examine and confirm the notifications that are checked are correct. If they are not, we strongly recommend modifying the notification selection before you connect to a service integration.

Step 9 Scroll to **Service Integrations**.

Step 10 Click the blue plus button.

Step 11 Enter a **Name**. This name appears in Security Cloud Control as a configured service integration. It does not appear in any events forwarded to the configured service.

Step 12 Expand the drop-down menu and select **Webex** as the Service Type.

Step 13 Paste the webhook URL that you generated from the service.

Step 14 Click **OK**.

Incoming Webhooks for Microsoft Teams

Security Cloud Control can forward notifications to Microsoft Teams. These messages are displayed either in a designated channel or as an automated bot in a private chat message in Microsoft Teams. To enable this functionality, you must generate a webhook URL from Microsoft Teams and point Security Cloud Control to that webhook. For more information about adding incoming webhooks to a Microsoft Teams channel, see Create incoming webhooks with Workflows for Microsoft Teams.

Prerequisites

These are the prerequisites to allow Security Cloud Control notifications in Microsoft Teams:

- A Microsoft Teams account.
- A Security Cloud Control account and tenant.

Use this procedure to generate a webhook URL in Microsoft Teams and enable notifications from Security Cloud Control:

Procedure

Step 1 Log in to your Microsoft Teams account.

Step 2 In the **New Teams** client, click **Teams** and navigate to the channel in which you want to add an incoming webhook.

Step 3 Click **More options •••** next to the channel name.

Step 4 Click **Workflows**.

Step 5 Click **Post to a channel when a webhook request is received**.

Step 6 Provide a name for the webhook and click **Next**.

Step 7 Choose the channel where notifications must be posted.

If you use this workflow from a Microsoft Teams chat or channel, these fields get populated automatically.

Step 8 After you enter the required details, click **Add workflow**.

Step 9 Copy the unique webhook URL from the dialog box that is displayed. The URL maps to the channel. You can use it to send information to Teams.

Step 10 Log into Security Cloud Control.

Step 11 In the left pane, click **Administration** > **Notification Settings**.

Step 12 Scroll to **Service Integrations**.

Step 13 Click the blue plus button.

Step 14 Enter a **Name**.

This name is displayed in Security Cloud Control as a configured service integration. However, it does not appear in any of the events forwarded to the configured service.

Step 15 Expand the drop-down list, and select **Microsoft Teams** as the **Service Type**.

Step 16 Paste the webhook URL generated from Microsoft Teams into **URL**.

Step 17 Under **Send Alerts When**, examine and confirm that the selected notifications are correct. If not, modify the notification selection before proceeding.

Step 18 Click **Save**.

Incoming Webhooks for Slack

Security Cloud Control notifications appear in a designated channel or as an automated bot in a private message. For more information on how Slack handles incoming webhooks, see Slack Apps for more information.

Use the following procedure to allow incoming webhooks for Slack:

Procedure

Step 1 Log into your Slack account.

Step 2 In the panel to the left, scroll to the bottom and select **Add Apps**.

Step 3 Search application directory for **Incoming Webhooks** and locate the app. Select **Add**.

Step 4 If you are not the admin of your Slack workspace, you must send a request to the admin of your org and wait for the app to be added to your account. Select **Request Configuration**. Enter an optional message and select **Submit Request**.

Step 5 Once the Incoming Webhooks app is enabled for your workspace, refresh the Slack settings page and select **Add New Webhook to Workspace**.

Step 6 Use the drop-down menu to select the Slack channel you want the Security Cloud Control notifications to appear in. Select **Authorize**. If you navigate away from this page while waiting for the request to get enabled, simply log into Slack and select the workspace name in the upper left corner. From the drop-down menu, select **Customize Workspace** and select **Configure Apps**. Navigate to **Manage** > **Custom Integrations**. Select **Incoming Webhooks** to open app's landing page and then select **Configuration** from the tabs. This lists all the users within your workspace that has this app enabled. You can only see and edit your account's configuration. Select your workspace name to edit the configuration and move forward.

Step 7 The Slack settings page redirects you to the configuration page for the app. Locate and copy the webhook URL.

Step 8 Log into Security Cloud Control.

Step 9 In the left pane, click **Administration** > **Notification Settings**.

Step 10 Examine and confirm the notifications that are checked are correct. If they are not, we strongly recommend modifying the notification selection before you connect to a service integration.

Step 11 Scroll to **Service Integrations**.

Step 12 Click the blue plus button.

Step 13 Enter a **Name**. This name appears in Security Cloud Control as a configured service integration. It does not appear in any events forwarded to the configured service.

Step 14 Expand the drop-down menu and select **Slack** as the Service Type.

Step 15 Paste the webhook URL that you generated from the service.

Step 16 Click OK.

Incoming Webhooks for a Custom Integration

Before you begin

Security Cloud Control does not format messages for custom integration. If you opt to integrate a custom service or application, Security Cloud Control sends a JSON message.

Refer to the service's documentation on how to enable incoming webhooks and generate a webhook URL. Once you have a webhook URL, use the procedure below to enable webhooks:

Procedure

Step 1 Generate and copy the webhook URL from the custom service or application of your choice.

Step 2 Log into Security Cloud Control.

Step 3 In the left pane, click **Administration** > **Notification Settings**.

Step 4 Examine and confirm the notifications that are checked are correct. If they are not, we strongly recommend modifying the notification selection before you connect to a service integration.

Step 5 Scroll to **Service Integrations**.

Step 6 Click the blue plus button.

Step 7 Enter a **Name**. This name appears in Security Cloud Control as a configured service integration. It does not appear in any events forwarded to the configured service.

Step 8 Expand the drop-down menu and select **Custom** as the Service Type.

Step 9 Paste the webhook URL that you generated from the service.

Step 10 Click OK.

Logging Settings

View your monthly event logging limit and how many days are left until the limit resets. Note that stored logging represents the compressed event data that the Cisco cloud received.

Click **View Historical Usage** to see logs your tenant has received over the past 12 months.

There are also links you can use to request additional storage.

Integrate Your SAML Single Sign-On with Security Cloud Control

Security Cloud Control uses Cisco Secure Sign-On as its SAML single sign-on identity provider (IdP) and Duo Security for multifactor authentication (MFA). This is Security Cloud Control's preferred authentication method.

If, however, customers want to integrate their own SAML single sign-on IdP solution with Security Cloud Control, they can as long as their IdP supports SAML 2.0 and identity provider-initiated workflow.

To integrate your own or third-party identity provider (IdP) with Cisco Security Cloud Sign On, see Cisco Security Cloud Sign On Identity Provider Integration Guide.

If you need more support to integrate your own SAML solution with Security Cloud Control, contact support and create a case.

Attention When you open a case, ensure that you choose **Manually Select A Technology** and select **SecureX - Sign-on and Administration** for your request to reach the right team.

Renew SSO Certificate

Your Identity Provider (IdP) is usually integrated with SecureX SSO. Open a Cisco TAC case and provide the metadata.xml file. For more information, see Cisco SecureX Sign-On Third-Party Identity Provider Integration Guide.

Attention When you open a case, ensure that you choose **Manually Select A Technology** and select **SecureX - Sign-on and Administration** for your request to reach the right team.

(legacy only) If your Identity Provider (IdP) integration is directly with Security Cloud Control, open a support ticket with Security Cloud Control TAC and provide the metadata.xml file.

My Tokens

See API Tokens for more information.

API Tokens

Developers use Security Cloud Control API tokens when making Security Cloud Control REST API calls. The API token must be inserted in the REST API authorization header for a call to succeed. API tokens are "long-lived" access tokens which do not expire; however, you can renew and revoke them.

You can generate API tokens from within Security Cloud Control. These tokens are only visible immediately after they're generated and for as long as the General Settings page is open. If you open a different page in Security Cloud Control and return to the **General Settings** page, the token is no longer visible, although it is clear that a token has been issued.

Individual users can create their own tokens for a particular tenant. One user cannot generate a token on behalf of another. Tokens are specific to an account-tenant pair and cannot be used for other user-tenant combinations.

API Token Format and Claims

The API token is a JSON Web Token (JWT). To learn more about the JWT token format, read the Introduction to JSON Web Tokens.

The Security Cloud Control API token provides the following set of claims:

- **id** - user/device uid
- **parentId** - tenant uid
- **ver** - the version of the public key (initial version is 0, for example, **cdo_jwt_sig_pub_key.0**)
- **subscriptions** - Security Services Exchange subscriptions (optional)
- **client_id** - "**api-client**"
- **jti** - token id

Token Management

Generate an API Token

Procedure

Step 1 From the drop-down list under your username, click **Preferences** > **General Preferences**.

Step 2 In My Tokens, click **Generate API Token**.

Step 3 Save the token in a secure location in accordance with your enterprise's best practices for maintaining sensitive data.

Refresh an API Token

The API token does not expire. However, you may choose to refresh your API token, which renews the existing token, if the token is lost, compromised, or to conform to your enterprise's security guidelines.

Procedure

Step 1 From the drop-down list under your username, click **Preferences**.

Step 2 In **General Preferences** > **My Tokens**, click **Refresh Token**. Security Cloud Control generates a *new* API token.

Step 3 Save the new token in a secure location in accordance with your enterprise's best practices for maintaining sensitive data.

Note

The **Revoke**, **Refresh**, **Delete**, and **Edit** options for the API-only user for the Cisco Secure Dynamic Attributes Connector service account (csdac-service@tenantname) have been disabled. This is to ensure customers don't delete, edit, or revoke the API tokens for this API account, which is required for the Cisco Secure Dynamic Attributes Connector functionality.

Revoke an API Token

Procedure

Step 1 From the drop-down list under your username, click **Preferences**.

Step 2 In **General Preferences** > **My Tokens**, click **Revoke Token**. Security Cloud Control revokes the token.

Note

The **Revoke**, **Refresh**, **Delete**, and **Edit** options for the API-only user for the Cisco Secure Dynamic Attributes Connector service account (csdac-service@tenantname) have been disabled. This is to ensure customers don't delete, edit, or revoke the API tokens for this API account, which is required for the Cisco Secure Dynamic Attributes Connector functionality.

Relationship Between the Identity Provider Accounts and Security Cloud Control User Records

To log in to Security Cloud Control, a customer needs an account with a SAML 2.0-compliant identity provider (IdP), a multi-factor authentication provider, and a user record in Security Cloud Control. The IdP account contains the user's credentials and the IdP authenticates the user based on those credentials. Multi-factor authentication provides an added layer of identity security. The Security Cloud Control user record primarily contains the username, the Security Cloud Control tenant with which they are associated, and the user's role. When a user logs in, Security Cloud Control tries to map the IdP's user ID to an existing user record on a tenant in Security Cloud Control. When Security Cloud Control finds a match, the user is logged in to that tenant.

Unless your enterprise has its own single sign-on identity provider, your identity provider is Cisco Security Cloud Sign On. Cisco Security Cloud Sign On uses Duo for mutli-factor authentication. Customers can integrate their own IdP with Security Cloud Control if they choose.

Login Workflow

This is a simplified description of how the IdP account interacts with the Security Cloud Control user record to log in a Security Cloud Control user:

Procedure

Step 1 The user requests access to Security Cloud Control by logging in to a SAML 2.0-compliant identity provider (IdP) such as Cisco Security Cloud Sign On (https://sign-on.security.cisco.com) for authentication.

Step 2 The IdP issues a SAML assertion that the user is authentic, and a portal displays the applications the user can access. One of the tiles represents Security Cloud Control.

Step 3 Security Cloud Control validates the SAML assertion, extracts the username and attempts to find a user record among its tenants that corresponding to that username.

- If the user has a user record on a single tenant on Security Cloud Control, Security Cloud Control grants the user access to the tenant and the user's role determines the actions they can take.
- If the user has a user record on more than one tenant, Security Cloud Control presents the authenticated user with a list of tenants they can choose from. The user picks a tenant and is allowed to access the tenant. The user's role on that specific tenant determines the actions they can take.
- If Security Cloud Control does not have a mapping for the authenticated user to a user record on a tenant, Security Cloud Control displays a landing page giving users the opportunity to learn more about Security Cloud Control or request a free trial.

Creating a user record in Security Cloud Control does not create an account in the IdP and creating an account in the IdP does not create a user record in Security Cloud Control.

Similarly, deleting an account on the IdP does not mean you have deleted the user record from Security Cloud Control; although, without the IdP account, there is no way to authenticate a user to Security Cloud Control. Deleting the Security Cloud Control user record does not mean you have deleted the IdP account; although, without the Security Cloud Control user record, there will be no way for an authenticated user to access a Security Cloud Control tenant.

Implications of this Architecture

Customers Who Use Cisco Security Cloud Sign On

For customers who use Security Cloud Control's Cisco Security Cloud Sign On identity provider, a Super Admin can create a user record in Security Cloud Control and a user can self-register themselves with Security Cloud Control. If the two usernames match, and the user is properly authenticated, the user can log in to Security Cloud Control.

Should the Super Admin ever need to prevent a user from accessing Security Cloud Control, they can simply delete the Security Cloud Control user's user record. The Cisco Security Cloud Sign On account will still exist and if the Super Admin ever wants to restore the user, they can by creating a new Security Cloud Control user record with the same username as the one used for Cisco Security Cloud Sign On.

Should a customer ever run into a problem with Security Cloud Control that requires a call to our Technical Assistance Center (TAC), the customer could create a user record for the TAC engineer so they could investigate the tenant and report back to the customer with information and suggestions.

Customers Who Have Their Own Identity Provider

For customers who have their own identity provider, they control both the identity provider accounts and the Security Cloud Control tenants. These customers can create and manage identity provider accounts and user records in Security Cloud Control.

Should they ever need to prevent a user from accessing Security Cloud Control, they can delete the IdP account, the Security Cloud Control user record, or both.

If they ever need help from Cisco TAC, they can create both the identity provider account and a Security Cloud Control user record, with a read-only role, for their TAC engineer. The TAC engineer would then be able to access the customer's Security Cloud Control tenant, investigate, and report back the customer with information and suggestions.

Cisco Managed Service Providers

If Cisco Managed Service Providers (MSPs) use Security Cloud Control's Cisco Security Cloud Sign On IdP, they can self-register for Cisco Security Cloud Sign On and their customers can create a user record for them in Security Cloud Control so that the MSP can manage the customer's tenant. Of course, the customer has full control to delete the MSP's record when they choose to.

Related Topics

- General Settings
- User Management
- Security Cloud Control User Roles

MSSP Portal

The MSSP portal in Security Cloud Control is a multitenant, cloud-based management platform for managed security service providers (MSSPs) to efficiently monitor and manage devices across multiple tenants.

The portal consolidates real-time information, such as **Configuration Status**, **Connectivity State**, **Software Version**, and overall network health, into a single interface, providing a seamless overview without the need to access individual tenant environments.

Before you begin

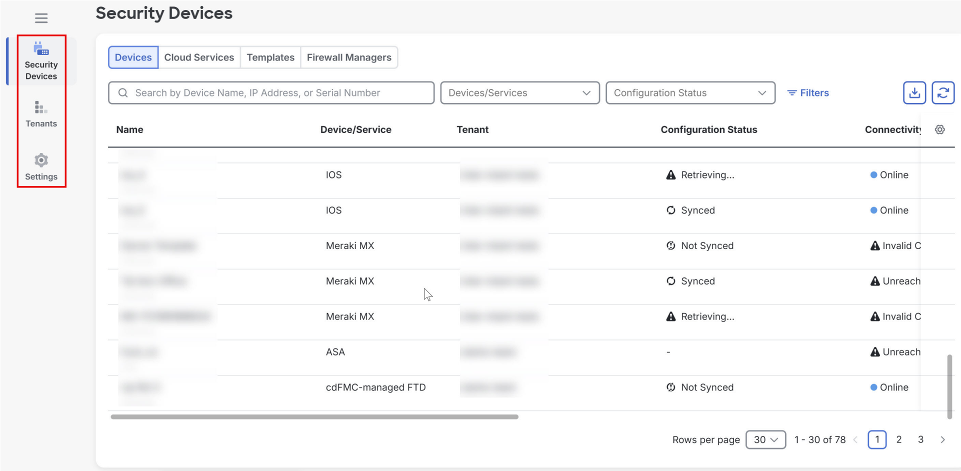
- Open a support ticket with Cisco TAC to create an MSSP portal to manage your tenants. For more information, see Open a Support Ticket with TAC.
- We recommend that you clear the cache and cookies from your web browser to avoid browser-related issues.

MSSP Portal

The options provided in the left pane of the portal enable you to view the details about security devices and tenants in the portal and configure the portal settings.

- **Security Devices**

- Provides information about all the devices, cloud services, templates, and firewall managers that are onboarded to the tenants added to the portal. For more information, see Security Devices Details, on page 20.

- 

Name	Device/Service	Tenant	Configuration Status	Connectivity
[redacted]	IOS	[redacted]	Retrieving...	Online
[redacted]	IOS	[redacted]	Synced	Online
[redacted]	Meraki MX	[redacted]	Not Synced	Invalid C
[redacted]	Meraki MX	[redacted]	Synced	Unreach
[redacted]	Meraki MX	[redacted]	Retrieving...	Invalid C
[redacted]	ASA	[redacted]	-	Unreach
[redacted]	cdFMC-managed FTD	[redacted]	Not Synced	Online

Rows per page 30 1 - 30 of 78 1 2 3

- **Tenants**
  - Provides information about all the tenants managed by the portal. You can search by tenant name and export the tenants' information to a comma-separated value (.csv) file.
  - Note that only users with **Super Admin** privileges can create new tenants or add existing tenants to the portal.

- **Settings**
  - **General Settings** provides information about **Portal Settings**.
  - **User Management** provides a list of all the **Users**, **Active Directory Groups**, and **Audit Logs**. For more information, see User Management.

Note If you are a user with Super Admin privileges, you can use API endpoints to:

- Create a Security Cloud Control tenant
- Add an existing Security Cloud Control tenant to the multitenant portal

Security Devices Details

Click **Security Devices** in the left pane to view the **Security Devices** page containing the following tabs:

Table 1: Security Devices Page Tab Descriptions

Tab name	Description
Devices	View all the devices that are onboarded to the tenants in the portal. • Click a device to view the **Device Details**, **Tenant Details**, and **Actions**. • You can manage this device in Security Cloud Control by clicking **Manage Device on Tenant** under **Actions**. This link is displayed if you have an account on that tenant and the tenant is in the same region as the portal. If you don't have permission to access the tenant, you will not see the **Manage Device on Tenant** link. Contact the Super Admin in your organization to get the required permission. • Click **Filters** to filter your devices by **Device/Services**, **Configuration Status**, **Connectivity State**, **Software Version**, **Tenant**, or **Conflict Detection**.
Cloud Services	View all the cloud services that are onboarded to the tenants in the portal. • Click a cloud service to view the **Device Details**, **Tenant Details**, and **Actions**. • Click **Filters** to filter your cloud services by **Services**, **Configuration Status**, **Connectivity State**, **Tenant**, or **Conflict Detection**.
Templates	View all the templates that are onboarded to the tenants in the portal. • Click a template to view the **Device Details**, **Tenant Details**, and **Actions**. • Click **Filters** to filter your cloud services by **Template Type**, **Configuration Status**, **Software Version**, or **Tenant**.
Firewall Managers	View all the firewall managers that are onboarded to the tenants in the portal. • Click a firewall manager to view the **Device Details**, **Tenant Details**, and **Actions**. • Click **Filters** to filter your cloud services by **Device Managers**, **Connectivity State**, **Tenant**, or **Software Version**.

- You can export the details to a comma-separated value (.csv) file to help you with analysis and compliance reporting. Every time you export data, Security Cloud Control creates a new .csv file that has the creation time stamp and the universally unique identifier of the portal in the file's name.
- The column selector allows you to select or clear the properties that you want to view in the table. Click the gear icon (⚙) at the top-right corner of the table to view the table settings.

  If you customize the table, Security Cloud Control remembers your selection the next time you view the **Security Devices** page.

Add a Tenant to the MSSP Portal

A user with **Super Admin** privileges can add tenants to the MSSP portal across multiple regions. For example, they can add a tenant from Europe to the US and vice versa.

Important We recommend that you create an API-Only user for your tenant and generate an API token for authenticating to Security Cloud Control.

Note If you want to add multiple tenants to the portal, generate API tokens from each tenant and paste them into a text file. You can then add the tenants one after another to the portal without switching to the tenant every time to generate a token.

Procedure

Step 1 In the left pane, click **Tenants**.

Step 2 Click the + icon at the top-right corner of the page.

Step 3 To add a new tenant, click **Next**.

Note

a. To import existing tenants, check the **Would you like to import existing tenant?** check box.

b. Add existing tenants from Security Cloud Control by pasting multiple API tokens separated by commas.

c. Click **Import**.

Step 4 Under **Tenant Details**, enter the **Display Name**, **Tenant Name**, and **Sales Order Number**.

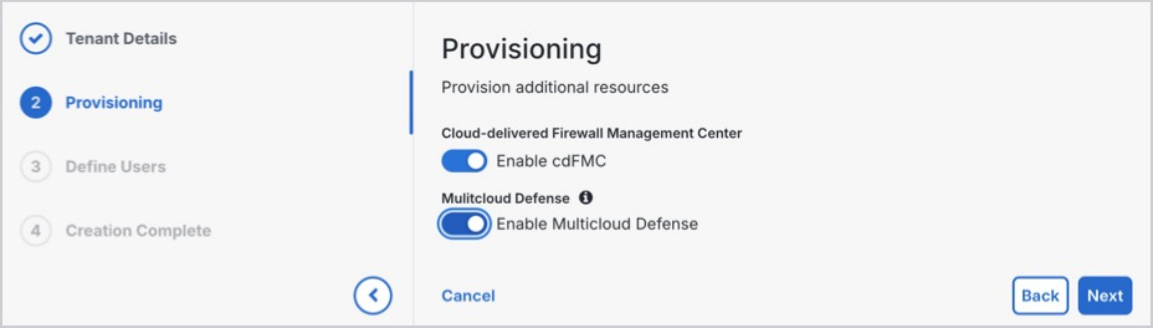
Note that tenants created without a sales order number are placed on a 30-day proof-of-value trial.

Step 5 Click **Next**.

Step 6 Under **Provisioning**,

- Click the **Enable cdFMC** toggle button to provision cloud-delivered Firewall Management Center for your tenant.
- Click the **Enable Multicloud Defense** toggle button to provision Multicloud Defense for your tenant.

- Click **Next**.



Provisioning

Provision additional resources

Cloud-delivered Firewall Management Center

Enable cdFMC

Mulitcloud Defense

Enable Multicloud Defense

Step 7 Under **Define Users**, either add users manually by entering their email address and selecting their role, or download the CSV file template, fill the necessary details, and upload the file.

The added users are displayed in the **User list** section.

Step 8 Click **Create Tenant**.

Tenant creation is complete, and provisioning may take a few minutes.

Delete a Tenant from the MSSP Portal

Procedure

Step 1 In the left pane, click **Tenants**.

Step 2 Click the corresponding delete icon on the right to remove the tenant.

Step 3 Click **Remove**.

Note that the associated devices are also removed from the portal.

Manage MSSP Portal Settings

Security Cloud Control enables you to customize certain aspects of your MSSP portal and individual user accounts on the settings page. Click **Settings** in the left pane to access the settings page.

Settings

General Settings

Web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous, and no sensitive data is transmitted.

Web analytics is enabled by default. To disable web analytics or to enable in the future, follow this procedure:

1. From the left pane, choose **Administration** > **General Settings**.
2. Click the **Web Analytics** toggle button.

User Management

You can see all the user records associated with the MSSP portal on the **User Management** screen. You can add, edit, or delete a user account. For more information, see User Management.

Switch Tenant

If you have more than one portal tenants, you can switch between different portal or tenants without signing out from Security Cloud Control.

Procedure

Step 1 On the MSSP portal, click your tenant menu at the top-right corner.

Step 2 Click **Switch Tenant**.

Step 3 Choose the portal or tenant that you want to view.

The Cisco Success Network

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the device and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism to select data of interest from the device and to transmit it in a structured format to remote management stations for the following benefits:

- To inform you of available unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that might be available for your product.
- To help Cisco improve our products.

The device establishes and maintains the secure connection at all times, and allows you to enroll in the Cisco Success Network. After you have registered the device, you can change the Cisco Success Network setting.

Note

- For Firewall Threat Defense high availability pairs, the selection of the active device overrides the Cisco Success Network setting on the standby device.
- Security Cloud Control does not manage the Cisco Success Network settings. The settings managed through, and telemetry information is provided by, the Firewall Device Manager user interface.

Enable or Disable the Cisco Success Network

During initial system setup, you are prompted to register the device with Cisco Smart Software Manager. If you instead elected to use the 90-day evaluation license, you must register the device before the end of the evaluation period. To enroll the device, either register the device with Cisco Smart Software Manager (on the Smart Licensing page) or enroll with Security Cloud Control by entering a registration key.

When you register the device, your virtual account allocates the license to the device. Registering the device also registers any optional licenses that you have enabled.

You can turn off this connection at any time by disabling Cisco Success Network, although you can only disable this option through the Firewall Device Manager UI. Disabling will disconnect the device from the cloud. Disconnection does not impact the receipt of updates or the operation of the Smart Licensing capabilities, which continue to operate normally. See the **Connecting to the Cisco Success Network** section of the System Administration chapter of the Firepower Device Manager configuration Guide, Version 6.4.0 or later for more information.

Manage Users in Security Cloud Control

Before you create or edit a user record in Security Cloud Control, read Relationship Between Identity Provider Accounts and Security Cloud Control User Records to learn how the identity provider (IdP) account and the user record interact. Security Cloud Control users need a record and a corresponding IdP account so they can be authenticated and access the Security Cloud Control tenant.

Unless your enterprise has its own IdP, Cisco Secure Sign-On is the identity provider for all Security Cloud Control tenants. The rest of this article assumes you are using Cisco Secure Sign-On as your identity provider.

You can see all the user records associated with your tenant on the **User Management** screen. This includes any Cisco support engineer who is temporarily associated with your account to resolve a support ticket.

Manage Super Admins on Your Tenant

It is a best practice to limit the number of Super Admins on your tenant. Determine which users should have Super Admin privileges, review User Management, and change the roles of other users to "Admin."

View the API User Records Associated with your Tenant

Procedure

In the left pane, **Administration** > **API User Management**.

Note
To prevent Cisco support from accessing your tenant, enable the **Prevent Cisco support from viewing this tenant** toggle in the General Settings page.

Active Directory Groups in User Management

For tenants that have a high turnover for large quantities of users, you can map Security Cloud Control to your Active Directory (AD) groups instead of adding individual users to Security Cloud Control for an easier way to manage your user lists and user roles. Any user changes, such as a new user addition or removing existing users, can now be done in Active Directory and no longer need to be done in Security Cloud Control.

You must have a **SuperAdmin** user role to add, edit, or delete an Active Directory group from the **User Management** page. See User Roles for more information.

In the left pane, choose **Settings** > **User Management**

Active Directory Groups

- In the left pane, click **Administration** > **API User Management > Active Directory Groups**.
- This page displays the role of the Active Directory group as assigned in your Active Directory manager.
- Users within an Active Directory group are not listed individually in either the **Active Directory Groups** tab or the **Users** tab.

Audit Logs

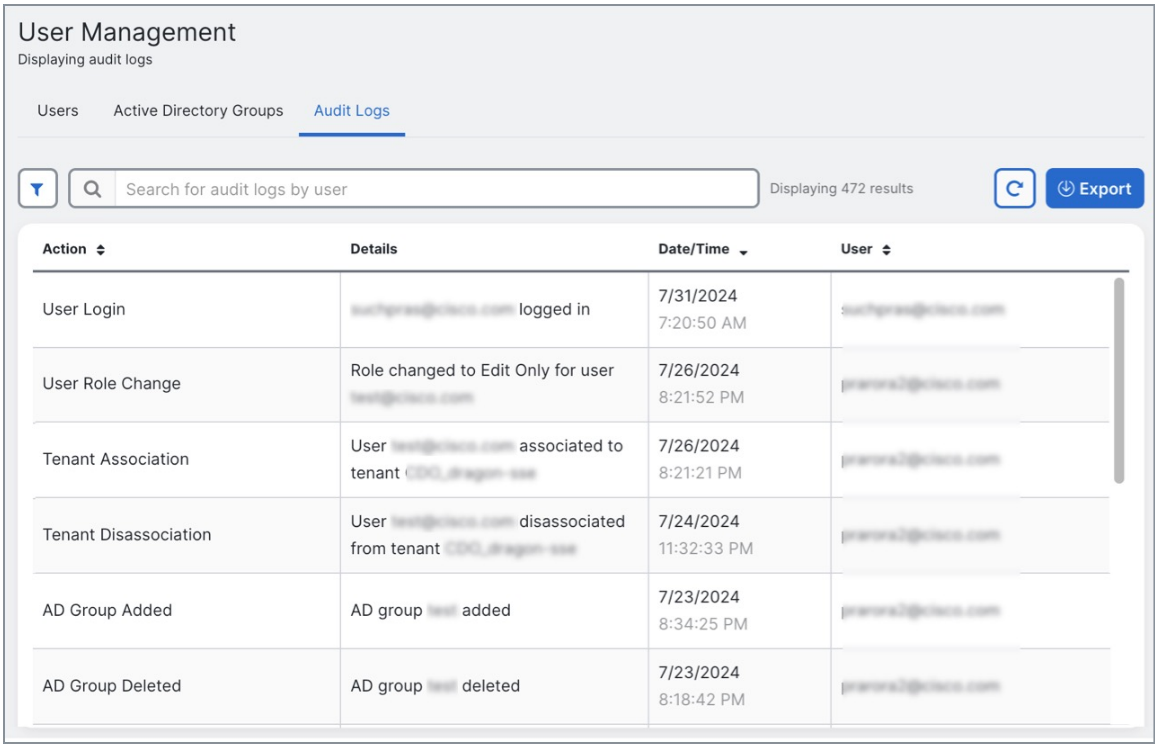
Audit Logs in Security Cloud Control record user-related and system-level actions. Key events that are captured by the **Audit Logs** include:

- **User Login:** Records every instance of user authentication.
- **Tenant Association and Disassociation:** Tracks user associations with, or disassociations from, tenants.
- **User Role Change:** Records any modifications to user roles.
- **Active Directory Groups:** Records any addition, deletion, and role changes within AD groups.

Procedure:

1. In the left pane, click **Administration** > **API User Management**.
2. Click the **Audit Logs** tab. A list of events and activities in the current tenant you are logged into is displayed.
3. Use the **Search** text box to find logs for a specific user.
4. Click the filter icon to refine your search results and view specific events. You can filter the logs based on the **Time Range** and **Event Action**.
5. Click **Export** to download the details in CSV format.

Figure 1: Audit Logs



User Management

Displaying audit logs

Action	Details	Date/Time	User
User Login	[redacted] logged in	7/31/2024 7:20:50 AM	[redacted]
User Role Change	Role changed to Edit Only for user [redacted]	7/26/2024 8:21:52 PM	[redacted]
Tenant Association	User [redacted] associated to tenant [redacted]	7/26/2024 8:21:21 PM	[redacted]
Tenant Disassociation	User [redacted] disassociated from tenant [redacted]	7/24/2024 11:32:33 PM	[redacted]
AD Group Added	AD group [redacted] added	7/23/2024 8:34:25 PM	[redacted]
AD Group Deleted	AD group [redacted] deleted	7/23/2024 8:18:42 PM	[redacted]

Multi-role Users

As an extension along the IAM capabilities in Security Cloud Control, it is now possible for a user to have multiple roles.

A user can be part of multiple groups in Active Directory, and those groups can be defined in Security Cloud Control with different Security Cloud Control roles. The final permissions that a user gets on login are a combination of the roles of all the Active Directory groups that are defined in Security Cloud Control that the user is part of. For instance, if a user is part of two Active Directory groups and both the groups are added in Security Cloud Control with two different roles such as edit-only and deploy-only, the user would have both edit-only and deploy-only permissions. This applies to any number of groups and roles.

Active Directory group mappings must only be defined one time in Security Cloud Control, and managing access and permissions for users can after be achieved exclusively in Active Directory by adding, removing, or moving users between different groups.

Note If a user is both an individual user and part of an Active Directory group on the same tenant, the user role of the individual user overrides the user role of the Active Directory group.

API Endpoints for Active Directory Groups

If you are a super admin, you can use API endpoints to do the following:

- Create an Active Directory group

- Remove an Active Directory group
- Modify an Active Directory group
- Get Active Directory groups
- Get an Active Directory group

The aforementioned links point to the corresponding sections of the Cisco DevNet website.

Prerequisites for Adding an Active Directory Group to Security Cloud Control

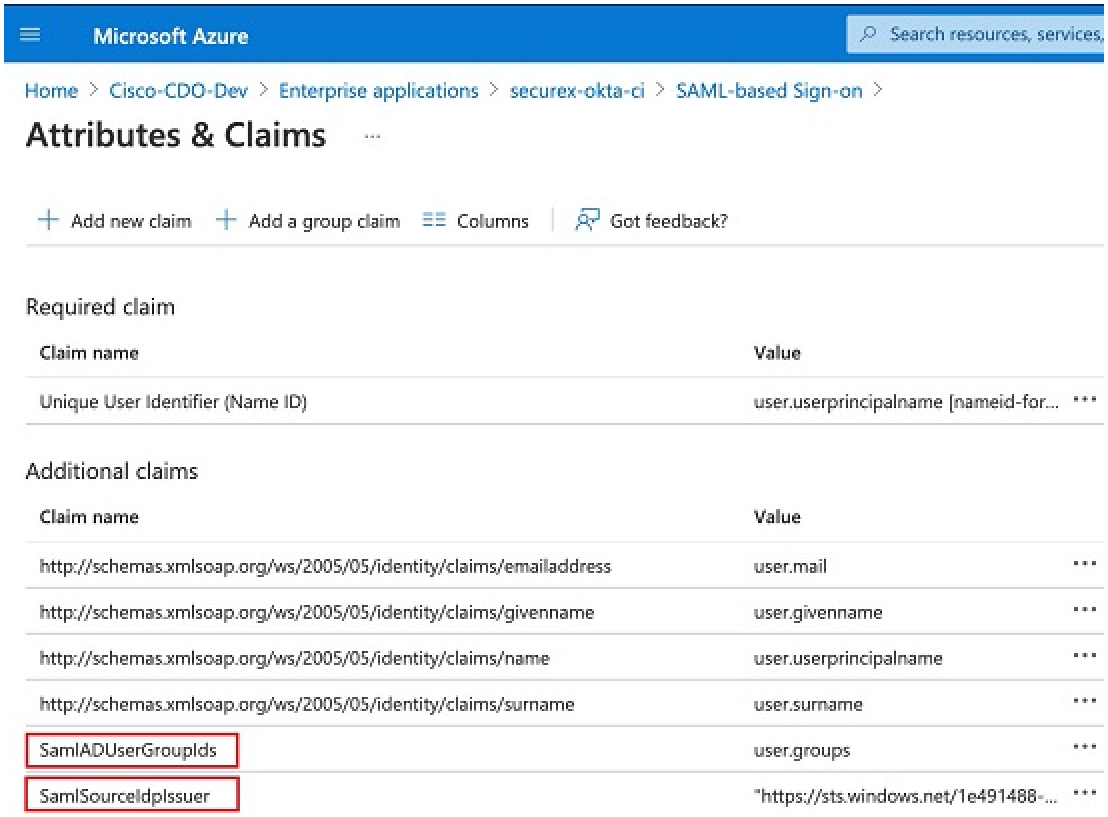
Before adding an Active Directory group mapping to Security Cloud Control as a form of user management, you must have your Active Directory that is integrated with Security Cloud Sign On. If your Active Directory Identity Provider (IdP) is not already integrated, see identity provider integration guide to integrate a custom Active Directory IdP integration with the following information:

- Your Security Cloud Control tenant name and region
- Domain to define custom routing for (for example: @cisco.com, @myenterprise.com)
- Certificate and federation metadata in the XML format

After your Active Directory integration is complete, add the following custom SAML claims in your Active Directory. The SAML claims and attributes are required, for you to be able to successfully sign-in to your Security Cloud Control tenant after your Active Directory integration is done. These values are case sensitive:

- **SamlADUserGroupIds** - This attribute describes all group associations that a user has on Active Directory. For example, in Azure select **+ Add a group claim** as seen in the screenshot below:

Figure 2: Custom Claims Defined in Active Directory


Microsoft Azure
Search resources, services,
Home > Cisco-CDO-Dev > Enterprise applications > securex-okta-ci > SAML-based Sign-on >
+ Add new claim
+ Add a group claim
Columns
Got feedback?

Attributes & Claims

Required claim

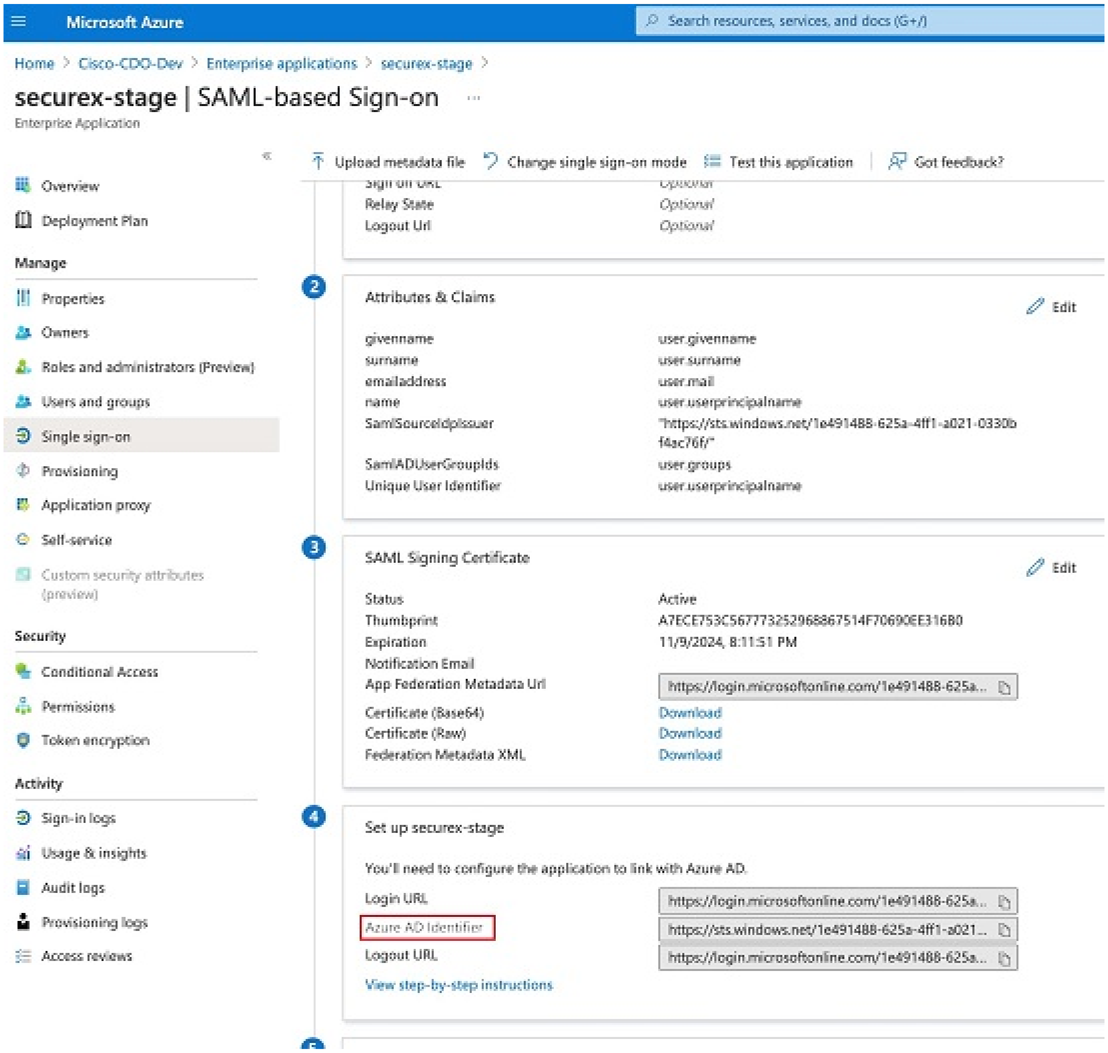
Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
SamlADUserGroupIds	user.groups
SamlSourceIdpIssuer	"https://sts.windows.net/1e491488-...

- **SamlSourceIdpIssuer** - This attribute uniquely identifies an Active Directory instance. For example, in Azure select **+ Add a group claim** and scroll to locate the Azure Active Directory Identifier as seen in the screenshot below:

Figure 3: Locate the Azure Active Directory Identifier



Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
SamlSourceIdpIssuer	"https://sts.windows.net/1e491488-625a-4ff1-a021-0330bf4ac76f/"
SamlADUserGroupIds	user.groups
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	A7ECE753C5677732529688675 14F70690EE31680
Expiration	11/9/2024, 8:11:51 PM
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/1e491488-625a...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up securex-stage

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/1e491488-625a...
Azure AD Identifier	https://sts.windows.net/1e491488-625a-4ff1-a021...
Logout URL	https://login.microsoftonline.com/1e491488-625a...

Add an Active Directory Group for User Management

You must have a **SuperAdmin** user role to add, edit, or delete an Active Directory group.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **API User Management**.

Step 3 Click the **Active Directory Groups** tab.

Step 4 Click the add Active Directory group (+) button.

Step 5 Provide the following information:

- **Group Name**: Enter a unique name. This name does not have to match the group name in your Active Directory. Security Cloud Control does not support special characters for this field.
- **Group Identifier**: Manually enter the Group Identifier from your Active Directory. The value of the group identifier should be the same as the group identifier in the custom claim definition. It could be any value that corresponds to the unique identity of the group, for example, my-favourite-group, 12345, and so forth.
- **AD Issuer**: Manually enter the Active Directory Issuer value from your Active Directory.
- **Role**: Select a user role. This determines the role for all the users included in this Active Directory group. See User Roles for more information.
- (Optional) **Notes**: Add any notes that are applicable to this Active Directory group.

Step 6 Select **OK**.

Edit an Active Directory Group for User Management

Before you begin

Note that editing an Active Directory Group's user management in Security Cloud Control only allows you to modify how Security Cloud Control limits the Active Directory group. You cannot edit the Active Directory group itself in Security Cloud Control. You must use Active Directory to edit the list of users within an Active Directory group.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **API User Management**.

Step 3 Click the **Active Directory Groups** tab.

Step 4 Identify the Active Directory Group you want to edit and click the edit icon.

Step 5 Modify the following values:

- **Group Name**: Enter a unique name. Security Cloud Control does not support special characters for this field.
- **Group Identifier**: Manually enter the Group Identifier from your Active Directory. The value of the group identifier should be the same as the group identifier in the custom claim definition. It could be any value that corresponds to the unique identity of the group, for example, my-favourite-group, 12345 and so forth.
- **AD Issuer**: Manually enter the Active Directory Issuer value from your Active Directory.
- **Role**: This determines the role for all the users included in this Active Directory group. See User Roles for more information.
- **Notes**: Add any notes that are applicable to this Active Directory group.

Step 6 Click **OK**.

Delete an Active Directory Group for User Management

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **API User Management**.

Step 3 Click the **Active Directory Groups** tab.

Step 4 Identify the Active Directory Group you want to delete.

Step 5 Click the delete icon.

Step 6 Click **OK** to confirm you want to delete the Active Directory group.

Create a New Security Cloud Control User

These two tasks are necessary for creating a new Security Cloud Control user. They do not have to be done in sequence:

- Create a Cisco Secure Sign-on Account for the New User
- Create a Security Cloud Control User Record with Your Security Cloud Control Username

After these tasks are done, then the user can open Security Cloud Control from the Cisco Secure Sign-On dashboard.

Create a Cisco Security Cloud Sign On Account for the New User

Creating a Cisco Security Cloud Sign On account can be done by the new user at any time, without needing to know the name of the assigned tenant.

About Logging in to Security Cloud Control

Security Cloud Control uses Cisco Secure Sign-On as its identity provider and Duo for multi-factor authentication (MFA). **To log into Security Cloud Control, you must first create your account in Cisco Security Cloud Sign On and configure MFA using Duo**.

Security Cloud Control requires MFA which provides an added layer of security in protecting your user identity. Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging into Security Cloud Control. The first factor is a username and password, and the second is a one-time password (OTP), which is generated on demand.

Important **If your Security Cloud Control tenant existed before October 14, 2019**, use Migrate to Cisco Security Cloud Sign On Identity Provider for log in instructions instead of this article.

Before You Log In

Install DUO Security

We recommend installing the Duo Security app in a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.

Time Synchronization

You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock set automatically or manually set it to the correct time.

Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication

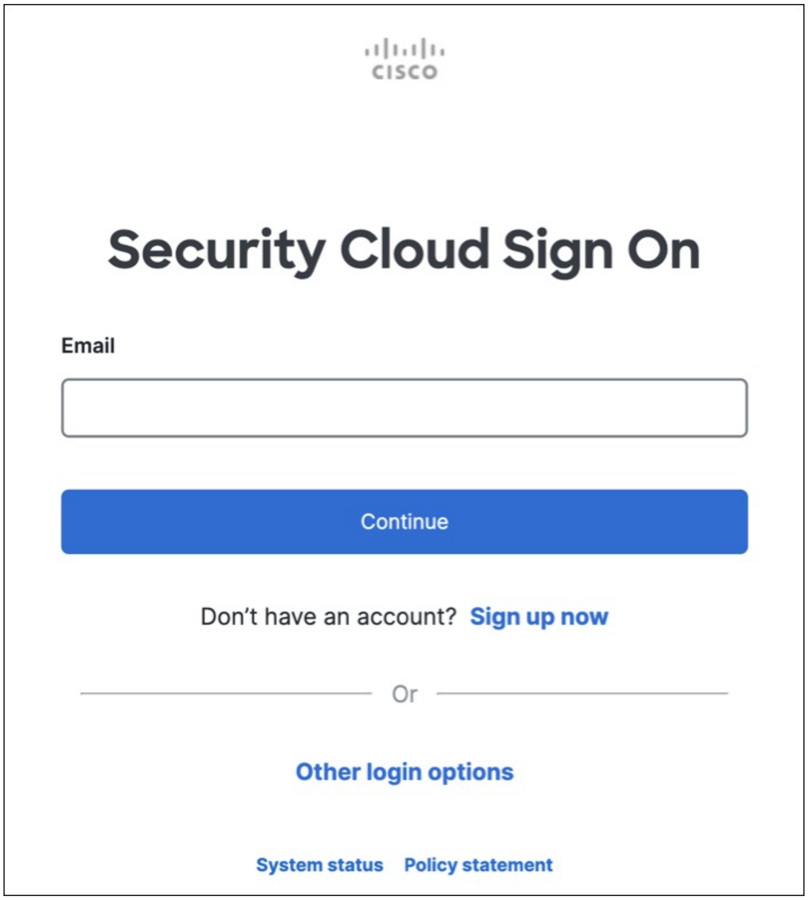
The initial sign-on workflow is a four-step process. You need to complete all four steps.

Procedure

Step 1 **Sign Up for a New Cisco Security Cloud Sign On Account**.

a. Open https://sign-on.security.cisco.com.

b. At the bottom of the sign in screen, click **Sign up now**.

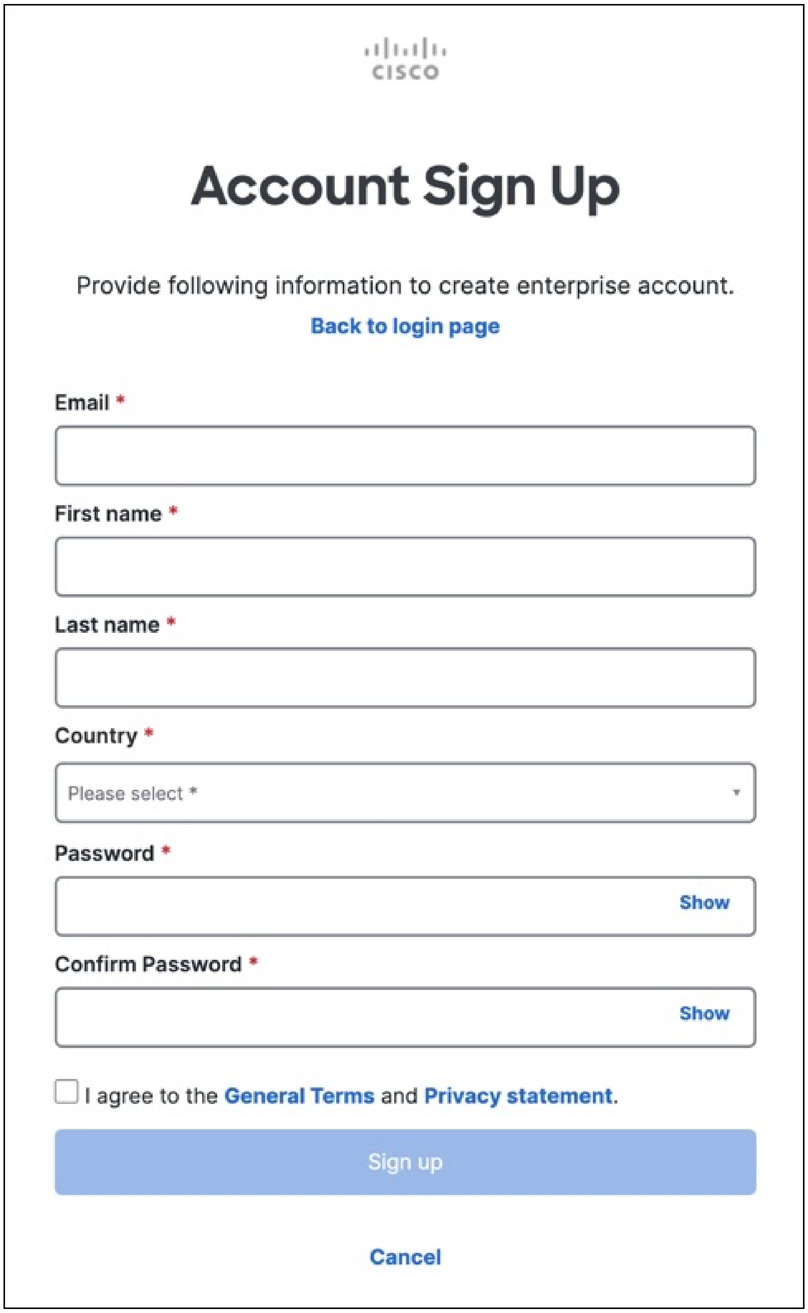


Security Cloud Sign On

Email

Don’t have an account? Sign up now

c. Provide the following information to create enterprise account.



cisco

Account Sign Up

Provide following information to create enterprise account.

Back to login page

Email *

First name *

Last name *

Country *

Please select *

Password *

Show

Confirm Password *

Show

□ I agree to the General Terms and Privacy statement.

Sign up

Cancel

Here are some tips:

- **Email**: Enter the email address that you will eventually use to log in to Security Cloud Control.
- **Password**: Enter a strong password.

d. Click **Sign up**.

Cisco sends you a verification email to the address you registered with. Open the email and click **Activate account**.

Step 2 **Set up Multi-factor Authentication Using Duo**

We recommend using a mobile device when setting up multi-factor authentication.

a. In the **Set up multi-factor authentication** screen, click **Configure factor**.

b. Click **Start setup** and follow the prompts to choose a mobile device and verify the pairing of that mobile device with your account.

For more information, see Duo Guide to Two Factor Authentication: Enrollment Guide. If you already have the Duo app on your device, you'll receive an activation code for this account. Duo supports multiple accounts on one device.

c. At the end of the wizard click **Continue to Login**.

d. Log in to Cisco Security Cloud Sign On with the two-factor authentication.

Step 3 **(Optional) Setup Google Authenticator as an additional authenticator**

a. Choose the mobile device you are pairing with Google Authenticator and click **Next**.

b. Follow the prompts in the setup wizard to setup Google Authenticator.

Step 4 **Configure Account Recovery Options for your Cisco Security Cloud Sign On**

a. Choose a recovery phone number for resetting your account using SMS.

b. Choose a security image.

c. Click **Create My Account**.

Create a User Record with Your Security Cloud Control Username

Only a Security Cloud Control user with **Super Admin** privileges can create the Security Cloud Control user record. The **Super Admin** must create the user record with the same email address that was specified in the **Create Your Security Cloud Control Username** task above.

Use the following procedure to create a user record with an appropriate user role:

Procedure

Step 1 Login to Security Cloud Control.

Step 2 In the left pane, choose **Settings** > **User Management**.

Step 3 Click + to add a new user to your tenant.

Step 4 Provide the email address of the user.

Note
The user's email address must correspond to the email address of the Cisco Secure Log-On account.

Step 5 From the **Role** drop-down list, select the user's role.

Step 6 Click **OK**.

The New User Opens Security Cloud Control from the Cisco Secure Sign-On Dashboard

Procedure

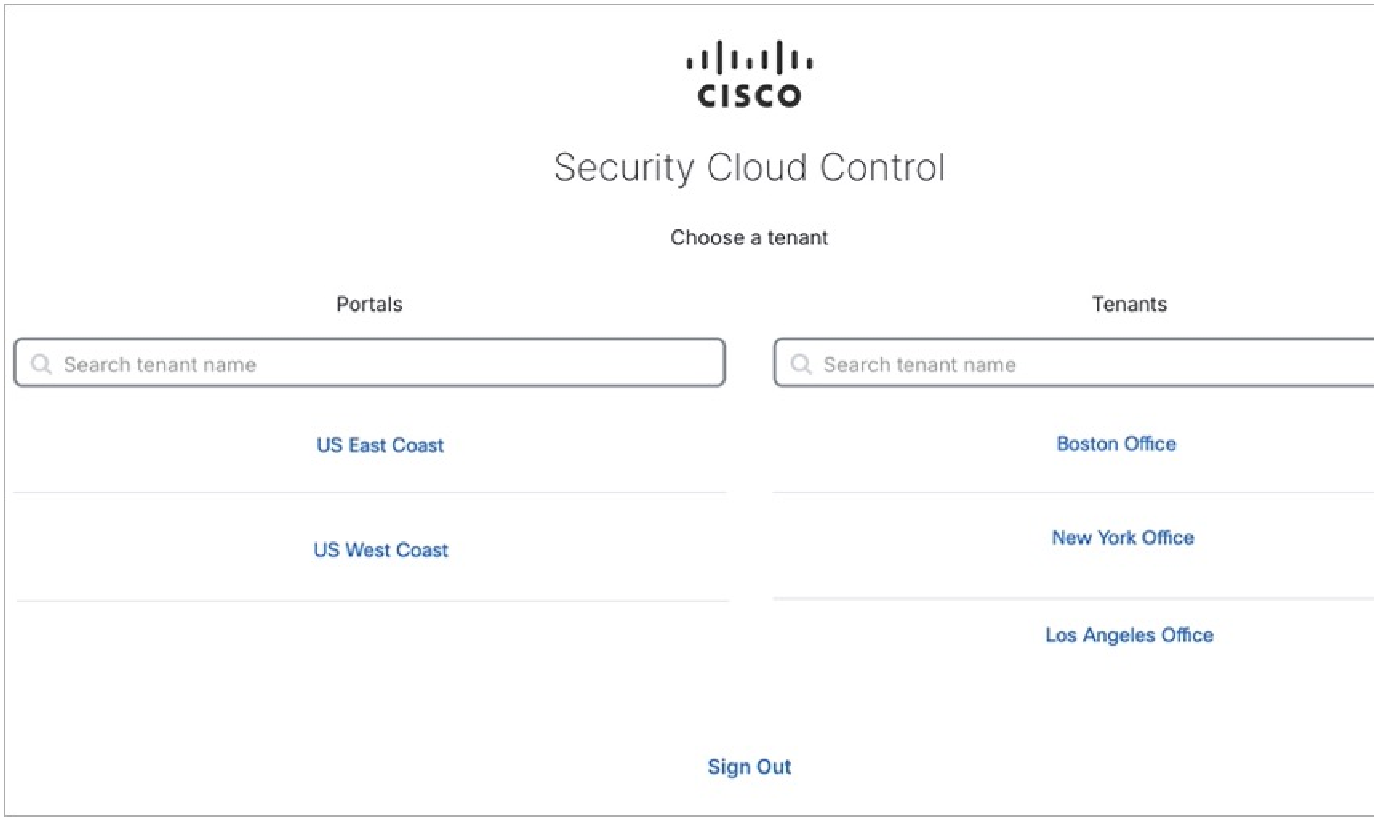
Step 1 Click the appropriate **Security Cloud Control** tile on the Cisco Secure Sign-on dashboard for your tenant's region.

Step 2 Click the authenticator logo to choose Duo Security or Google Authenticator if you have set up both authenticators.

- If you already have a user record on an existing tenant, you are logged into that tenant.
- If you already have a user record on several portals, you will be able to choose which portal to connect to.
- If you already have a user record on several tenants, you will be able to choose which Security Cloud Control tenant to connect to.
- If you do not already have a user record on an existing tenant, you will be able to learn more about Security Cloud Control or request a trial tenant.

The **Portals** view retrieves and displays consolidated information from multiple tenants. See Manage Multiple Security Cloud Control Tenants for more information.

The **Tenant** view shows several tenants on which you have a user record.

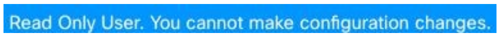


User Roles in Security Cloud Control

There are a variety of user roles in Security Cloud Control: Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a Security Cloud Control user has access to more than one tenant, they may have the same user ID but different roles on different tenants. A user may have a read-only role on one tenant and a Super Admin role on another. When the interface or the documentation refers to a Read-only user, an Admin user, or a Super Admin user we are describing that user's permission level on a particular tenant.

Read-only Role

A user assigned the Read-Only role sees this blue banner on every page:



Read Only User. You cannot make configuration changes.

Users with the Read-Only role can do the following:

- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a read-only user revokes their own token, they cannot recreate it.
- Contact support through our interface and can export a change log.

Read-Only users **cannot** do the following:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

Edit-Only Role

Users with the Edit-Only role can do the following:

- Edit and save device configurations, including but not limited to objects, policies, rulesets, interfaces, VPN, etc.
- Allow configuration changes that are made through the **Read Configuration** action.
- Utilize the Change Request Management action.

Edit-Only users **cannot** do the following:

- Deploy changes to a device or to multiple devices.
- Discard staged changes or changes that are detected through OOB.
- Upload AnyConnect Packages, or configure these settings.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create Security Cloud Control user records.
- Change user role.

Deploy-Only Role

Users with the Deploy-Only role can do the following:

- Deploy staged changes to a device, or to multiple devices.
- Revert or restore configuration changes for ASA devices.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Utilize the Change Request Management action.

Deploy-Only users **cannot** do the following:

- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create, update, configure, or delete anything on any page.

- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

VPN Sessions Manager Role

The VPN Sessions Manager role is designed for administrators monitoring remote access VPN connections, not site to site VPN connections.

Users with the VPN Sessions Manager role can do the following:

- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see RA VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a VPN Sessions Manager user revokes their own token, they cannot recreate it.
- Contact support through our interface and export a change log.
- Terminate existing RA VPN sessions.

VPN Sessions Manager users **cannot** do the following:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

Admin Role

Admin users have complete access to most aspects of Security Cloud Control. Admin users can do the following:

- Create, read, update, and delete any object or policy in Security Cloud Control and configure any setting.
- Onboard devices.
- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.

- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can contact support through our interface and can export a change log.

Admin users **cannot** do the following:

- Create Security Cloud Control user records.
- Change user role.

Super Admin Role

Super Admin users have complete access to all aspects of Security Cloud Control. Super Admins can do the following:

- Change a user role.
- Create user records.

Note Though Super Admins can create a Security Cloud Control user record, that user record is not all that is needed for a user to log in to your tenant. The user also needs an account with the identity provider used by your tenant. Unless your enterprise has its own single sign-on identity provider, your identity provider is Cisco Security Cloud Sign On. Users can self-register for their Cisco Security Cloud Sign On account; see Initial Login to Your New Security Cloud Control Tenant for more information.

- Create, read, update, and delete any object or policy in Security Cloud Control and configure any setting.
- Onboard devices.
- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can
- Contact support through our interface and can export a change log.

Change The Record of the User Role

The user record is the currently recorded role of a user. By looking at the users associated with your tenant, you can determine what role each use has by their record. By changing a user role, you change the user record. User's roles are identified by their role in the User Management table. See User Management for more information.

You must be a Super Admin to change the user record. If your tenant has no Super Admins, contact Security Cloud Control support.

Add a User Account to Security Cloud Control

Security Cloud Control users need a Security Cloud Control record and a corresponding IdP account so they can be authenticated and access your Security Cloud Control tenant. This procedure creates the user's Security Cloud Control user record, not the user's account in Cisco Security Cloud Sign On. If the user does not have an account in Cisco Security Cloud Sign On, they can self-enroll by navigating to https://sign-on.security.cisco.com and clicking **Sign up** at the bottom of the Sign in screen.

Note You will need to have the role of Super Admin on Security Cloud Control to perform this task.

Create a User Record

Use the following procedure to create a user record with an appropriate user role:

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **API User Management**.

Step 3 Click the blue plus button (+) to add a new user to your tenant.

Step 4 Provide the email address of the user.

Note
The user's email address must correspond to the email address of the Cisco Secure Log-On account.

Step 5 Select the user's role from the drop-down menu.

Step 6 Click **Save**.

Note
Though Super Admins can create a Security Cloud Control user record, that user record is not all that is needed for a user to log in to your tenant. The user also needs an account with the identity provider used by your tenant. Unless your enterprise has its own single sign-on identity provider, your identity provider is Cisco Secure Sign-on. Users can self-register for their Cisco Secure Sign-On account; see Initial Login to Your New Security Cloud Control Tenant for more information.

Create API Only Users

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **API User Management**.

Step 3 Click the blue plus button (+) to add a new user to your tenant.

Step 4 Select the **API Only User** checkbox.

Step 5 In the **Username** field, enter a name for the user and click **OK**.

Important
The user name can't be an email address or contain the '@' character as the '@yourtenant' suffix will be automatically appended to the user name.

Step 6 Select the user's role from the drop-down menu.

Step 7 Click **OK**.

Step 8 Click the **User Management** tab.

Step 9 In the **Token** column for the new API Only user, click **Generate API Token** to obtain an API token.

Edit a User Record for a User Role

You will need to have the role of Super Admin to perform this task. If the Super Admin changes the role of a Security Cloud Control user that is logged in, once their role has been changed, the user is automatically logged out of their session. Once the user logs back in, they assume their new role.

Note You will need to have the role of Super Admin on Security Cloud Control to perform this task.

Caution Changing the role of a user record will delete an API token associated with the user record if there is one. The user must generate a new API token once the user role changes.

Edit a User Role

Note If a Security Cloud Control user is logged in, and a Super Admin changes their role, the user must log out and log back in again for the change to take effect.

To edit the role defined in the user record, follow this procedure:

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **API User Management**.

Step 3 Click the edit icon in the user's row.

Step 4 Select the user's new role from the Role drop-down menu.

Step 5 If the user record shows that there is an API token associated with the user, you will need to confirm that you want to change the user's role and delete the API token as a result.

Step 6 Click **v**.

Step 7 If Security Cloud Control deleted the API token, contact the user so that they may create a new API Token.

Note
The **Revoke**, **Refresh**, **Delete**, and **Edit** options for the API-only user for the Cisco Secure Dynamic Attributes Connector service account (csdac-service@tenantname) have been disabled. This is to ensure customers don’t delete, edit, or revoke the API tokens for this API account, which is required for the Cisco Secure Dynamic Attributes Connector functionality.

Delete a User Record for a User Role

Deleting a user record in Security Cloud Control prevents the associated user from logging in to Security Cloud Control by breaking the mapping of the user record with the Cisco Security Cloud Sign On account. When you delete a user record, you are also deleting the API token associated with that user record should there be one. Deleting a user record in Security Cloud Control does not delete the user's IdP account in Cisco Security Cloud Sign On.

Note You will need to have the role of Super Admin on Security Cloud Control to perform this task.

Delete a User Record

To delete the role defined in the user record, see the following procedure:

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **API User Management**.

Step 3 Click the trash can icon 🗑 in the row of the user you want to delete.

Step 4 Click **OK**.

Step 5 Confirm that you want to remove the account from the tenant by clicking OK.

Note

The **Revoke**, **Refresh**, **Delete**, and **Edit** options for the API-only user for the Cisco Secure Dynamic Attributes Connector service account (csdac-service@tenantname) have been disabled. This is to ensure customers don’t delete, edit, or revoke the API tokens for this API account, which is required for the Cisco Secure Dynamic Attributes Connector functionality.