Cisco Intersight with Cisco Cloud Control Controlled Availability Onboarding Guide

Date: July 07, 2026

Controlled Availability Release

Contents

Overview

This guide describes how Cisco Intersight works with Cisco Unified Identity (CUI) as part of the Cisco Cloud Control Controlled Availability.

Cisco Cloud Control is Cisco's unified operations platform for working across supported Cisco product domains from a single experience. It provides one login, one inventory, one topology, and consistent navigation across connected Cisco products, platform services, and AI experiences such as AI Assistant and AI Canvas. Cisco Cloud Control can be accessed at https://cloud.cisco.com.

Cisco Unified Identity (CUI) provides the shared identity foundation for Cisco Cloud Control. It powers the "log in once" experience, centralizes sign-in and identity provider configuration, and supports access across integrated Cisco products while honoring product entitlements and role-based access controls.

Intersight is currently making Cisco Cloud Control and Cisco Unified Identity capabilities available to selected accounts through Controlled Availability.

When an eligible Intersight account is enabled for CUI, its identity and access capabilities use the shared Cisco identity foundation required for Cisco Cloud Control. Tenant linking connects the CUI-enabled Intersight account to Cisco Cloud Control, allowing supported Intersight data to be included in the unified Cisco Cloud Control experience, such as inventory, topology, and product navigation.

After tenant linking is complete, authorized users can access supported Intersight data in Cisco Cloud Control and navigate between Cisco Cloud Control, Intersight, and other linked Cisco products.

What this guide covers

This guide covers moving the Intersight account's identity and access management to CUI, moving an account out of Cisco Cloud Control Controlled Availability, account login from the CUI URL, sign-in behavior, Cisco Cloud Control access, identity and access changes, and known limitations for this Controlled Availability release.

What changes after an account is enabled for Cisco Unified Identity?

When an eligible Intersight account is enabled for Cisco Unified Identity, users access the account through the CUI-enabled Intersight that supports Cisco Cloud Control. This updates how users sign in, how account and role selection appears, how identity provider settings are managed, and how supported Intersight data becomes available in Cisco Cloud Control.

Key changes include:

- **Sign-In URL**: You need to sign in to Cisco Intersight through the CUI-enabled Intersight URL https://intersight.com/cui. Alternatively, you can continue to use account-specific sign-in URLs, such as `https://<account_moid>.intersight.com/cui` or `https://<account_name>.intersight.com/cui`.
- **Account Visibility:** After an account is enabled for Cisco Unified Identity, it no longer appears on the account and role selection page from the regular Intersight sign-in URL; instead, it is moved and appears only on the Cisco Unified Identity sign-in page at https://www.intersight.com/cui.
- **Default Role:** If you have more than one role in an account, Intersight signs you in with the default role for that account. You can change your default role when needed.

- **Identity Provider Configuration:** To allow SSO users to access the CUI-enabled Intersight account and Cisco Cloud Control, administrators must configure the identity provider in Cisco Unified Identity. Previously configured Intersight IdP settings are retained and can continue to be used for user sign-in to Intersight, but users authenticated only through those settings cannot access Cisco Cloud Control. To learn more about configuring identity providers in Cisco Unified Identity, see Add an identity provider.
- **Data Sharing with Cisco Cloud Control:** Supported Intersight account data is shared with Cisco Cloud Control so authorized users can access it through Cisco Cloud Control.

Limitations and restrictions

Note: Currently, these limitations and restrictions apply to Intersight enabled for CUI and Cisco Cloud Control. Note that these limitations are subject to change in future releases.

- **US-East region support only:** Only US-East region-based Intersight accounts are supported for the Controlled Availability release.
- ⚠ **CUI-specific sign-in URL required after moving to a CUI account:** After an Intersight account is moved to Cisco Unified Identity, you must access the account by using the CUI sign-in URL (https://intersight.com/cui) or the account-specific sign-in URL (`https://<account_moid>.intersight.com/cui` or `https://<account_name>.intersight.com/cui`).
- ⚠ **Moving to a CUI account signs out all active users:** When the Account Administrator completes moving to a CUI account, that administrator and all other active users are signed out immediately and must sign in again using the CUI sign-in URL or the account-specific sign-in URL.
- **IdP-based user groups are not supported:** For the Cisco Cloud Control Controlled Availability, use static user access. IdP-based user groups are not supported in the current release.
- **Self-service move-out option:** You can move an Intersight account out of Cisco Cloud Control Controlled Availability by using the self-service move-out option when the account is not linked to Cisco Cloud Control as a tenant and no routing rules remain configured in Cisco Unified Identity. If the account is linked as a tenant, contact Cisco TAC to unlink the account before you continue.
- **Appliance Support:** Only SaaS-enabled products are supported by Cisco Cloud Control. Support for on-premises appliances is not available at this time.
- **Mobile Support:** Mobile device support is not currently available for this feature within Cisco Intersight.

Requirements

Review these eligibility requirements before you use the self-service move-in option to move an Intersight account to Cisco Cloud Control Controlled Availability.

- The Intersight account must be in the **US-East region**.
- You must have **Account Administrator** privileges to use the self-service move-in option to move to a CUI account and configure identity providers.

IP Access Management

For an account with IP Access Management enabled, if you sign in using Cisco Unified Identity from an IP address outside the allowed IP range for the account, your access will be blocked because your IP address is not included in the trusted IP address ranges configured for the account.

To regain access, you must do one of the following:

- You must contact an **Account Administrator** or **User Access Administrator** to add the current IP address to the trusted IP ranges and unlock access to Intersight, or
- On the **Access Denied** dialog box, select **Switch Account** to take you to the account and role selection page so you can select another account.
  If you select another account that also blocks the current IP range, the same access-denied behaviour will occur again. Try again by switching to another account.
- If you have access to only one account, the **Switch Account** option does not apply. In this case, you must return to the homepage, wait for an administrator to update the trusted IP address range, or connect from an allowed IP address.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) in Intersight applies only to users who **sign in with Cisco Unified Identity**. It does **not** apply to users who sign in through third-party SSO providers or through an SSO configuration in Cisco Intersight. For more information, refer to Setting up Multi-Factor Authentication.

- If a user has not enabled MFA for themselves through CUI, they cannot enable MFA for their account, even if they sign in with Cisco Unified Identity.
- MFA cannot be configured from an Intersight session within Cisco Cloud Control.

Onboard an Intersight account to the Cisco Cloud Control Controlled Availability

Follow one of these steps to get an account enabled for Cisco Unified Identity (CUI):

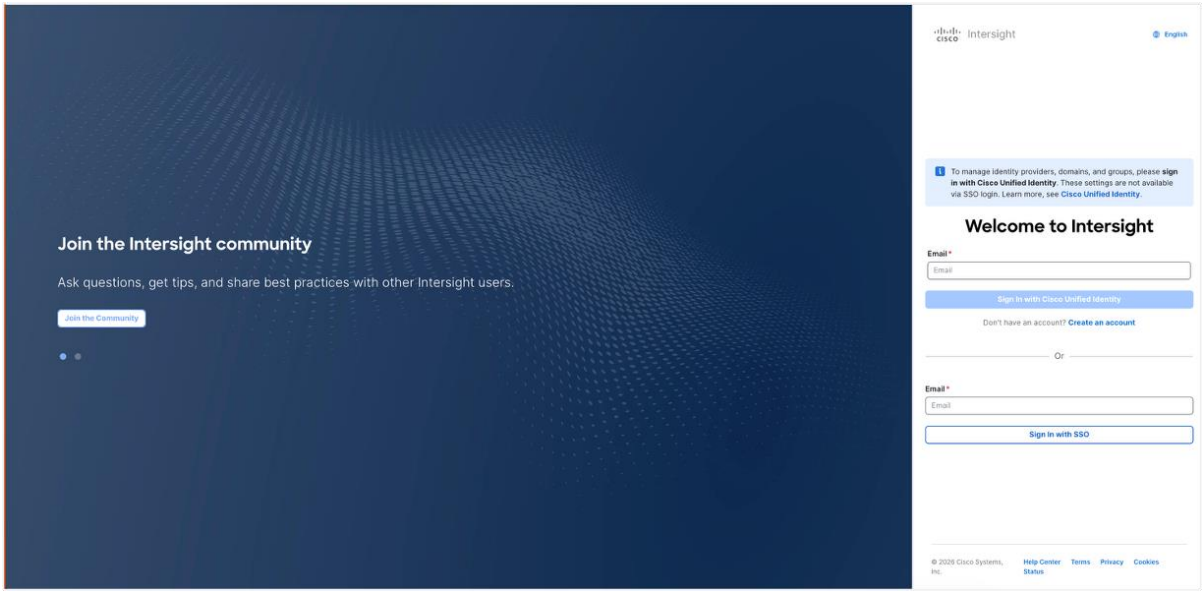
- Create a new CUI-enabled Intersight account, or
- Move an existing account to CUI by using the self-service move-in option or contacting your Cisco representative for assistance.

Create a new CUI-enabled Intersight account

Procedure

Follow these steps when you need to create a new Intersight account that is already enabled for the CUI.

1. In the address bar of a web browser, enter https://intersight.com/cui.
   The **Welcome to Intersight** page appears.



2. On the **Welcome to Intersight** page, select **Create an account**.
3. Enter a valid email address and select **Next**.
4. On the **Select region** page, select **Next**.
   The account region is not editable. The account region defaults to **US-East**; you do not need to select the account region manually. Only the **US-East** region is supported.
5. Review the **General Terms**, choose **I accept**, and select **Next**.
6. Register licensing or start a trial.
   - If you have purchased license tiers for Cisco Intersight Services, register for smart licensing to start using the services.
   - If you want to evaluate Intersight Services, register for a trial. On the **Start Trial** page, select **Infrastructure Services & Cloud Orchestrator**, and select **Start Trial**.

Move an existing Intersight account to CUI

This section describes how to use the self-service move-in option to move an existing Intersight account to CUI before it can use the CUI-enabled Controlled Availability.

Note: Initially, only select customers have access to the self-service move-in option. To enroll or submit interest in Cisco Cloud Control Controlled Availability, go to the Cisco Cloud Control sign-up page, follow the prompts, and wait to hear from Cisco.

⚠ **Caution:** Use an account where immediate sign-out of all active users is acceptable during the one-time movement of the account.

Before you begin

Review the changes that the user will experience after the account is enabled for Cisco Unified Identity.

Procedure

Follow these steps to use the self-service move-in option to move an eligible Intersight account to Cisco Cloud Control Controlled Availability.

1. Sign in to Intersight as an Account Administrator.

2. Open the **Help** menu.
3. Select **Cisco Cloud Control Controlled Availability**.
4. Review the changes described in the **Cisco Cloud Control Controlled Availability** dialog box.
5. Refer to the **Cisco Cloud Control Controlled Availability Onboarding Guide** (this guide) for additional guidance.
6. Select the acknowledgement checkbox.
   Note:
   - The Account Administrator and all active users for the account are immediately signed out upon the one-time movement of the account. You can view the currently active user sessions by navigating to **System** > **Sessions** > **Active**.
   - Starting with the next login, all users must access this account by using the CUI sign-in URL (https://intersight.com/cui) or the account-specific sign-in URL `https://<account_moid>.intersight.com/cui` or `https://<account_name>.intersight.com/cui`.
7. Select **Move to Cisco Unified Identity**.

Next Steps:

- Upon login:
  - You will be redirected to the last logged-in account.
  - If multiple roles are assigned to your CUI-enabled account, you will be signed in with one of these roles as your default role.
- Intersight data is synchronized with Cisco Cloud Control and made available to authorized users.

Move an account out of Cisco Cloud Control Controlled Availability

This section describes how to use the self-service move-out option to move an Intersight account out of Cisco Cloud Control Controlled Availability and restore the standard Intersight sign-in experience.

Note: Only eligible accounts that are not linked to Cisco Cloud Control as a tenant and do not have routing rules configured in Cisco Unified Identity can use the self-service move-out option.

Caution: Moving an account out of Cisco Cloud Control Controlled Availability signs out all active users, including your current session.

Before you begin

Review the following requirements before you move the account out:

- **Cisco Cloud Control tenant linking:** If the account is linked to Cisco Cloud Control as a tenant, the self-service move-out option is not available. Account administrators cannot unlink the account directly. Contact Cisco TAC to unlink the account before you continue.
- **Routing rules in Cisco Unified Identity:** Any routing rules configured in **Settings** > **Cisco Unified Identity** must be removed before you move the account out of Cisco Cloud Control Controlled Availability. After removing the routing rules, try the move-out action again.

Procedure

Follow these steps to use the self-service move-out option to move an eligible Intersight account out of Cisco Cloud Control Controlled Availability.

1. Sign in to Intersight as an Account Administrator.
2. Open the **Help** menu.
3. Select **Cisco Cloud Control Controlled Availability**.
4. In the **Cisco Cloud Control Controlled Availability** dialog box, select **Move out of Cisco Cloud Control**.

   Note: If the button is unavailable, review the tooltip for the blocking condition. The account might be linked to Cisco Cloud Control as a tenant, or routing rules might still be configured in Cisco Unified Identity.

5. In the **Move out of Cisco Cloud Control Controlled Availability** dialog box, review the changes that apply after the account is moved out:
   - User authentication for this account will move from Cisco Unified Identity to the standard Intersight sign-in experience.
   - Any active sessions, including your current session, will end.
   - Users must sign in again using https://intersight.com or an account-specific sign-in URL.
   - Any routing rules configured in **Settings** > **Cisco Unified Identity** should be removed before continuing.
6. Select **I understand the required changes for this Intersight account**.
7. Select **Move out of Cisco Cloud Control**.

Result

After the account is moved out of Cisco Cloud Control Controlled Availability, you are signed out. Sign in again using https://intersight.com or an account-specific sign-in URL.

Sign in to a CUI-enabled Intersight account

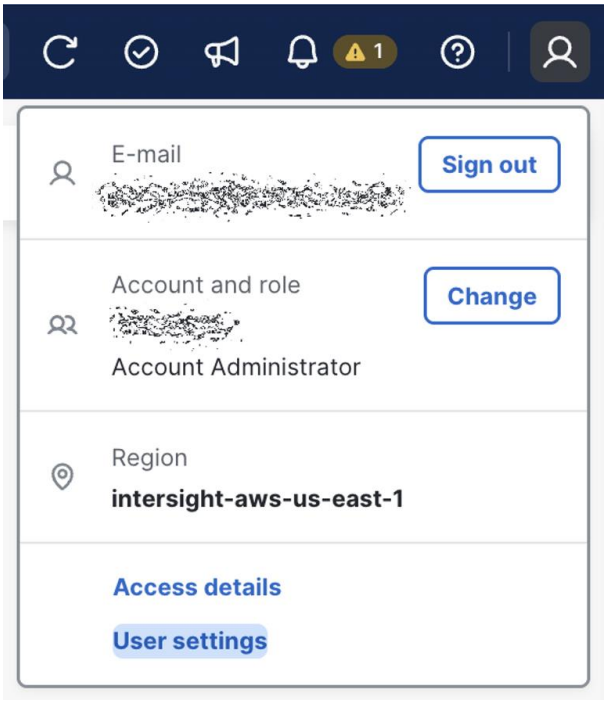
1. Enter https://intersight.com/cui in the browser.
2. On the **Welcome to Intersight** sign-in page, enter the email address associated with your account.
3. Choose one of these sign-in methods:
   - **Sign in with Cisco Unified Identity**
     Note: To manage identity providers, domains, and groups, sign in with Cisco Unified Identity. These configurations are currently not available via SSO login.
     - Enter the **Email** address associated with your account.
     - Select **Sign In with Cisco Unified Identity**.
   - **Sign in with SSO**
     Note: This is for standard access without any admin task requirements, as admin tasks are temporarily not supported through SSO.
     - Enter the **Email** address associated with your account.
     - Select **Sign in with SSO**.
4. Complete authentication.

When you sign in through Cisco Unified Identity, Intersight signs you in to the last logged-in account. If you have multiple roles configured, Intersight automatically selects a default role from the available roles. When you sign in to Intersight, a notification shows the account and role used for the session.

Change your default role

Follow these steps if you have multiple roles in a CUI-enabled account and want to change the role used during sign-in.

1. Sign in to the CUI-enabled account using https://intersight.com/cui.
2. From the **Profile** menu, select **User settings**.



3. From the **Default Role** drop-down list, select the role that you want to set as the default role for this account.
4. Select **Save**.

The selected role is used as your default role for the account on subsequent sign-ins.

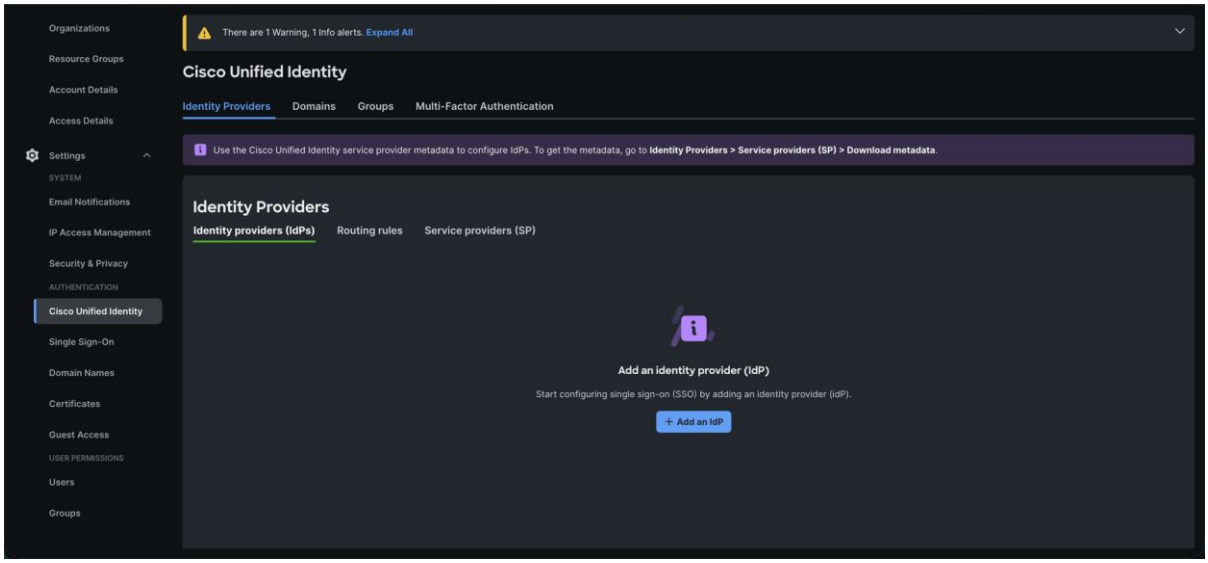
Configure Cisco Unified Identity on Intersight

Follow these steps to configure identity providers, routing rules, service providers, domains, and groups from the Cisco Unified Identity UI for the CUI-enabled Intersight account.

Procedure

To configure Cisco Unified Identity on Intersight:

1. In the address bar of a web browser, enter https://intersight.com/cui.
2. On the **Welcome to Intersight** page, **sign in with Cisco Unified Identity.**
3. Navigate to **Settings** > **AUTHENTICATION** > **Cisco Unified Identity**.
4. On the **Cisco Unified Identity** page, navigate to **Identity Providers** > **Identity providers (IdPs)**.



a. Configure either a SAML or OpenID IdP.

b. Create a routing rule.
Routing rules are applicable when setting up more than one IdP. Routing rules enable Intersight to identify which IdP to send your users to when you have configured multiple IdPs.

c. Add or renew your service provider certificate.

5. On the **Cisco Unified Identity** page, select **Domains** to add a domain and start managing identity and access. For more information, see Set up multiple domains.

6. On the **Cisco Unified Identity** page, select **Groups** to create a group that organizes similar users for authentication management. For more information, see Set up groups.

Set up multiple IdPs

Cisco Intersight supports Single Sign-On (SSO) via Identity Providers (IdPs). While many organizations rely on a single IdP, complex environments often require more flexibility.

You might need to configure multiple IdPs if your organization:

- **Operates as a large company**: If your company is large and has centralized departments but decentralized IT organizations and identity management systems.
- **Lacks cross-federation**: If your organization cannot federate between different IdPs, Cisco Intersight provides a workaround. By configuring multiple IdPs and routing rules, you can map specific domains or user groups to the appropriate authentication source, ensuring a smooth, secure login experience for all users.

Add an identity provider

Identity providers define how users authenticate before they access the CUI-enabled Intersight account. You can add SAML or OpenID Connect identity providers.

Configure SAML

SAML provides a structured framework that allows IdPs and service providers to communicate with each other, making federated identity and single sign-on possible and efficient. You have a choice when setting up a SAML IdP. You can manually enter the IdP's metadata or directly upload the metadata to the admin portal.

Note:
When configuring the IdP for a CUI-enabled Intersight account, use Cisco Unified Identity service provider (SP) metadata, not Intersight SP metadata.
To get the CUI SP metadata, go to **Settings** > **Authentication** > **Cisco Unified Identity** > **Identity Providers** > **Service providers (SP)**, and copy the metadata values. Use the Cisco Unified Identity service provider metadata in your IdP. Do not manually modify standard Intersight SSO URLs by adding /cui. Using non-CUI Intersight SP metadata can route users back to the wrong service provider after authentication, causing SSO login failures and possible administrator lockout. Test the SSO setup before activating routing rules for the domain.

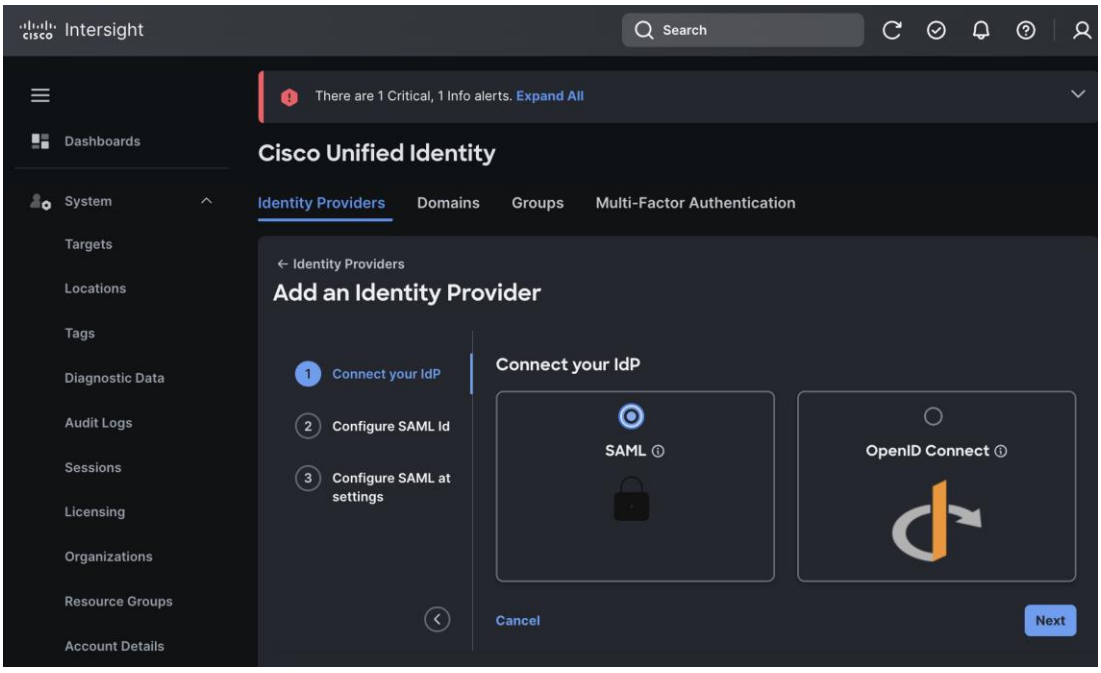
Before you begin

Ensure that you have **Account Administrator** privileges to perform this task.

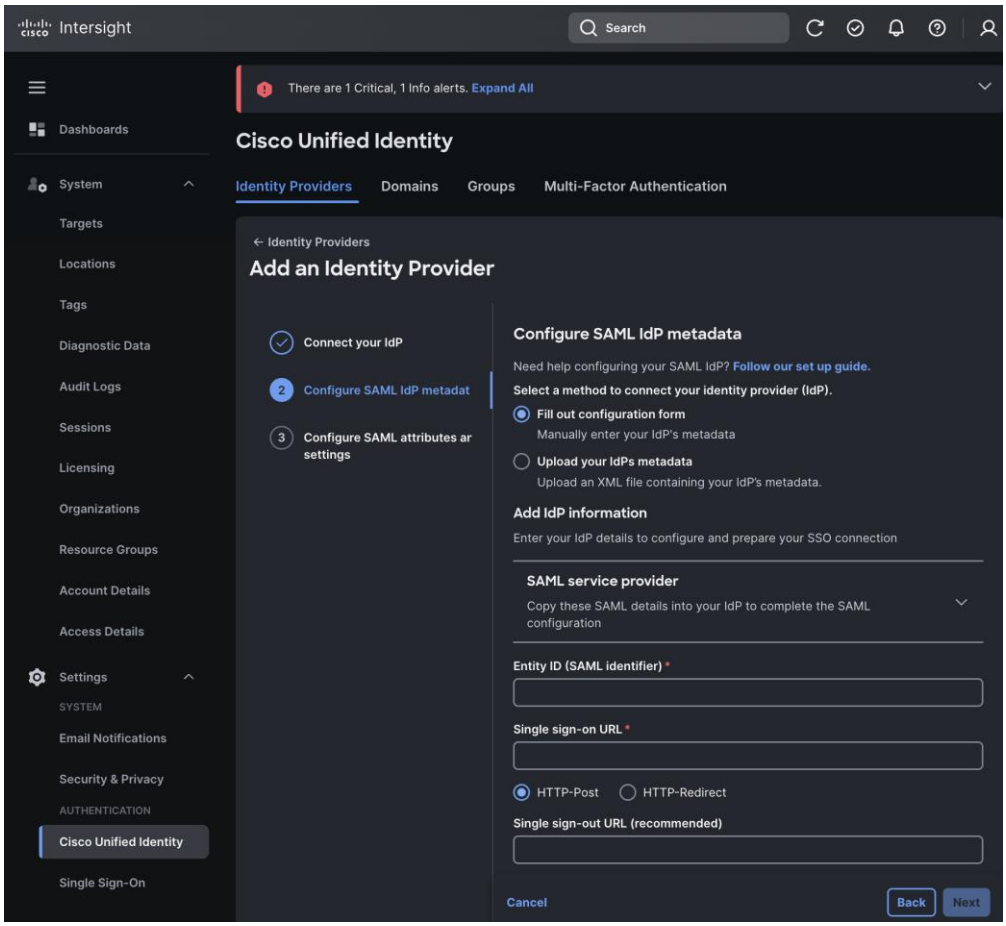
Procedure

Follow these steps to configure SAML.

1. Navigate to **Settings** > **AUTHENTICATION** > **Cisco Unified Identity**.
2. Navigate to **Identity Providers** > **Identity Providers (IdPs)**.
3. Select **Add an IdP**.
4. On the **Connect your IdP** page, select **SAML** as your IdP and select **Next**.



5. On the **Configure SAML IdP metadata** page, select one of these methods to connect your IdP:
   - **Fill out the configuration form:** Manually enter your IdP's metadata
   - **Upload your IdP's metadata:** Upload an XML file containing your IdP's metadata



6. If you select **Fill out configuration form**, follow these substeps:
   a. Enter your **Entity ID (SAML Identifier)**.
   b. Enter your **Single sign-on URL**.
   c. Select a binding method: **HTTP-Post** or **HTTP-Redirect**.
   d. (Optional) Enter your **Single sign-out URL**.
   e. (Optional) Select a binding method: **HTTP-Post** or **HTTP-Redirect**.
   f. Select the checkbox to enable **Sign SAML request**.

      Select this checkbox if your IdP requires authentication requests from Intersight to be signed.
   g. Select a **NameID format**.

      You can select from these options:

      - `urn:oasis:names:tc:SAML1.1:nameid-format:emailAddress` (default): This format uses your email address as your NameID.
      - `urn:oasis:names:tc:SAML2.0:nameid-format:transient`: This format generates a temporary, one-time NameID for each authentication.
      - `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`: This format indicates that no specific NameID format is requested, leaving it to your IdP to determine or default to an appropriate format.

h. Upload your **IdP certificate files**.

   If your IdP uses multiple signing certificates, upload up to two IdP certificate files in `.pem` or `.cer` format.

i. Select **Next**.

j. If you select **Upload your IdP's metadata**, follow these substeps:

   i. Upload an XML file containing your IdP's metadata.

      When uploading the metadata file, there are two ways to validate the metadata from the customer IdP:

      - Not signed, self-signed, or private CA-signed IdP metadata file. Your IdP provides a self-signed private CA or does not provide a signature for its metadata. This option is less secure.
      - Signed by a public certificate authority: Your IdP provides a signature in the metadata that is signed by a public root CA.

   ii. Select **Next**.

7. [Optional] On the **Configure SAML attributes and settings** page, configure the name of the SAML attribute for Intersight Username or Primary email address from uid to the value agreed upon with the IdP manager, such as email or User Principal Name (UPN).
8. Select **Add IdP**.
   If this is the first IdP you have configured, the IdP is saved as your default IdP, and a default routing rule is created.

Configure OpenID Connect

OpenID Connect (OIDC) configuration uses the OAuth 2.0 framework. It uses built-in certificates and encryption to streamline the SSO setup.

Note: When you set up OIDC with **Entra ID** or an IdP where the email is not a permanent identifier, we recommend you use the **externalId** linking attribute to map to a Unique Identifier. For Entra ID, we suggest mapping OIDC to externalId. If the entered email does not match the linking attribute, the user is prompted to verify their identity or create a new user with the correct email address.

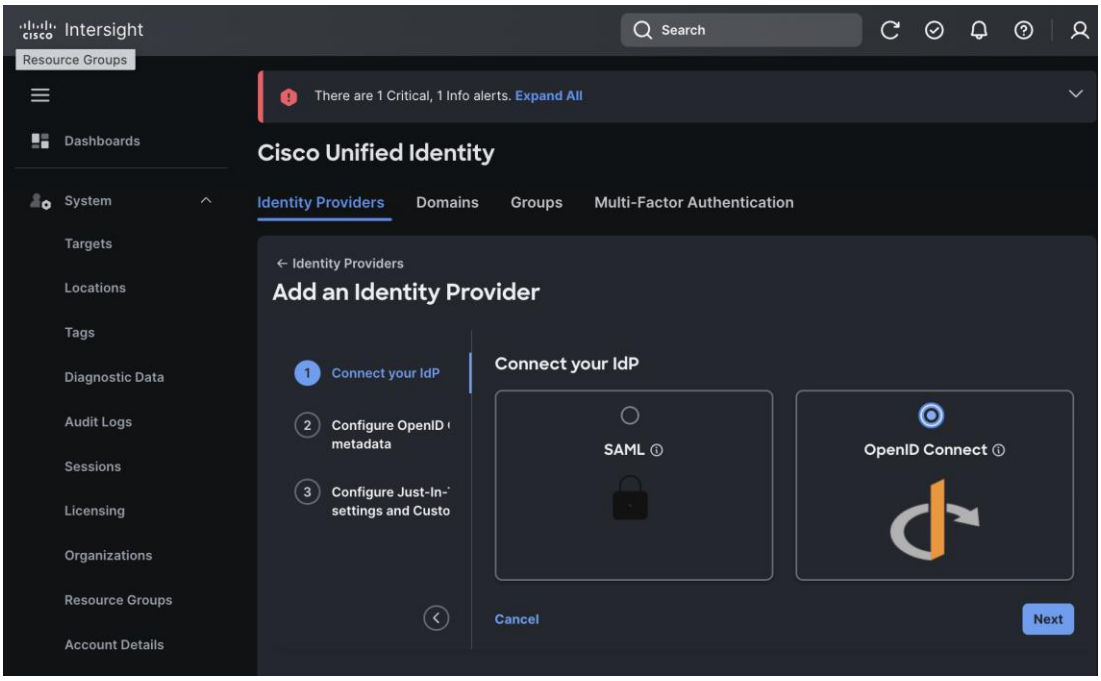
Before you begin

Ensure that you have **Account Administrator** privileges to perform this task.

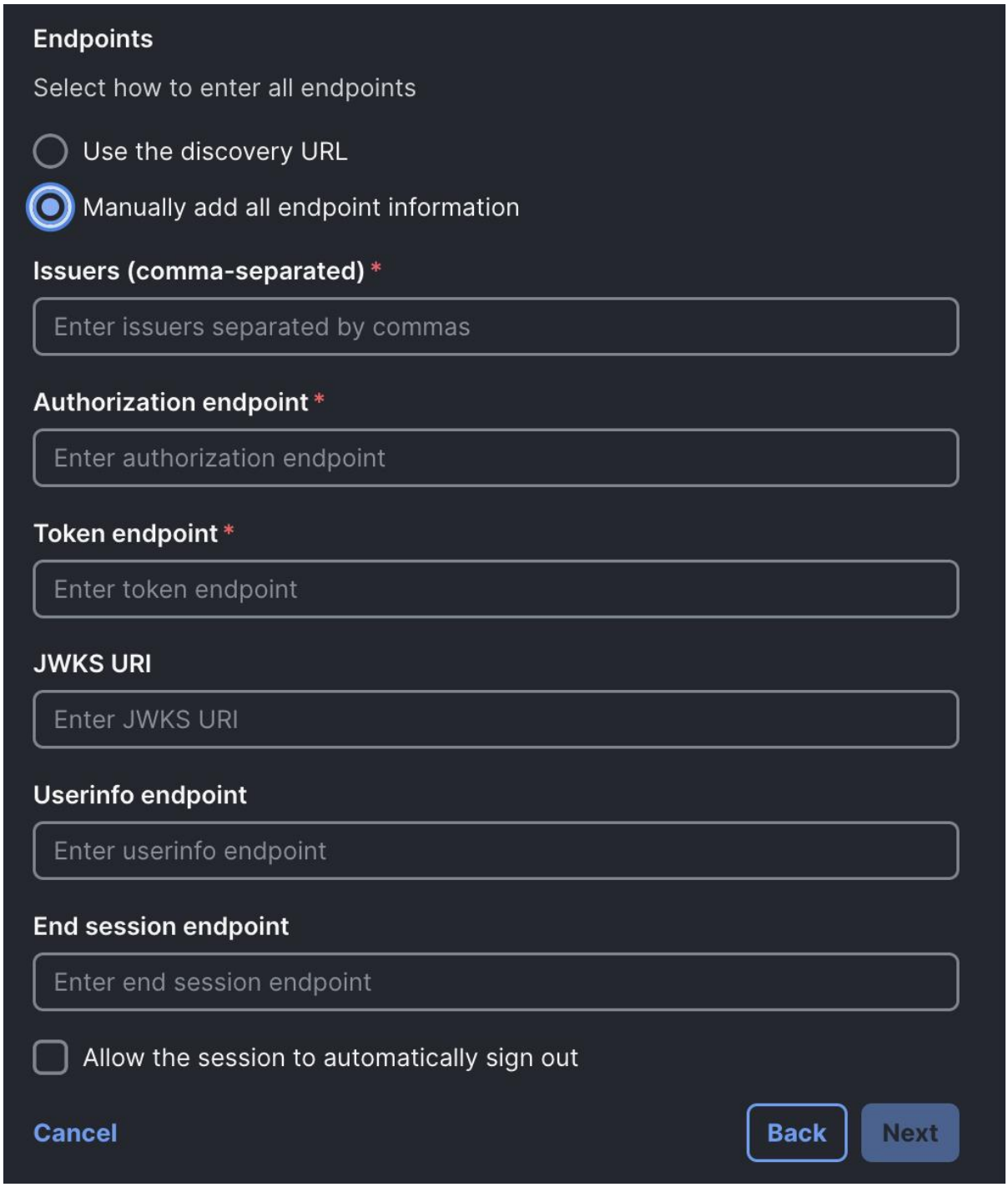
Procedure

Follow these steps to configure OpenID Connect:

1. Navigate to **Settings** > **AUTHENTICATION** > **Cisco Unified Identity**.
2. Navigate to **Identity Providers** > **Identity Providers (IdPs)**.
3. Select **Add an IdP**.
4. On the **Connect your IdP** page, choose **OpenID Connect** as your IdP, and select **Next**.



5. Enter the IdP information.
   - **Name**: The name to identify your IdP.
   - **Client ID**: The unique ID to identify you and your IdP.
   - **Client Secret**: The password that you and your IdP know.
   - **Scopes**: The scopes you want to associate with your IdP.
6. Select a method to add endpoints.
   a. **Use the discovery URL**
      i. Enter the discovery URL for the IdP. This URL automatically populates the endpoints for OIDC single logout (SLO).
      ii. Enable **Allow the session to automatically sign out** to ensure users are signed out across all connected applications and services when they log out of Intersight.
   b. **Manually add all endpoint information**
      Select this method if the IdP does not support discovery URLs. Follow these substeps:
      - **Issuers (comma-separated)**: Enter the issuer URL as specified by your IdP.
      - **Authorization endpoint**: Enter the authorization endpoint URL.
      - **Token endpoint**: Enter the token endpoint URL.
      - **JWKS URI**: (Optional) Enter the JSON Web Key Set (JWKS) URL.
      - **Userinfo endpoint**: (Optional) Enter the user information endpoint URL.
      - **End session endpoint**: (Optional) Enter the session signout endpoint URL. You must provide a URL to enable **Allow the session to automatically sign out** and single logout (SLO) across all connected applications.



c. Select **Add IdP**.
If this is the first IdP you have configured, the IdP is saved as the default IdP and a default routing rule is created.

Actions available for IdPs

In the table view, select ellipsis (**...**) next to an IdP configuration to view the available actions.

This table describes the actions available for IdP configurations.

Action	Description
Edit IdP	To edit an IdP configuration
Delete IdP	To delete an IdP configuration

Configure routing rules

Routing rules are applicable when setting up more than one IdP. Routing rules enable Intersight to identify which IdP to send your users to when you have configured multiple IdPs.

Add a routing rule

Before you begin

Ensure that you have **Account Administrator** privileges to perform this task.

Procedure

Follow these steps to add a routing rule:

1. Navigate to **Settings** > **AUTHENTICATION** > **Cisco Unified Identity**.
2. Navigate to **Identity Providers** > **Routing rules**.
   Note: When configuring your first IdP, the routing rule is automatically added and is set as the default rule. You can choose another IdP to set as the default rule later.
3. Select **Add a new routing rule**.
4. Enter the details for a routing rule:
   - **Rule name**: Enter the name for the routing rule.
   - **Select a routing type**: Select domain or group.
   - **If these are your domains**: Enter the domains or groups within your organization.
   - **Then use this identity provider**: Select the IdP.
5. Select the multi-factor authentication (MFA) method:
   - **Duo MFA**: Select Duo MFA as your MFA method of choice.
   - **Bring your own TOTP MFA Authenticator**: Use a time-based one-time password authenticator app such as Cisco Secure Authenticator as your preferred MFA method.
   - **I attest this IdP enforces MFA for users, so Cisco MFA is not required**: Select this option if your IdP provides its own MFA option for users.

     For more information on configuring MFA for your organization, see Enable multi-factor authentication integration in Control Hub.
6. (Optional) Select **Test SSO Setup** to test your SSO before you activate your routing rule.
   The SSO test opens in a new browser window. You can also select **Copy URL to clipboard** to test your SSO configuration in a browser window of your choice.

   Note: We recommend testing your SSO setup to ensure that you've configured your organization's SSO correctly.
7. Select **Add**.
8. Select the new routing rule and select **Activate**.
   Note: You can change the routing rule priority order if you have routing rules for multiple IdPs.

Actions available for routing rules

In the table view, select ellipsis (**...**) next to a rule to view the available actions.
This table describes the actions available for routing rules.

Action	Description	Note
Edit routing rule	To edit a routing rule	—
Deactivate	To deactivate a routing rule	The Default rule can't be deactivated or deleted, but you can modify the routed IdP. The routing rule's configuration is preserved for future use.
Delete	To permanently remove the selected rule from the list of routing rules	Make sure you have another active routing rule for the IdP. Otherwise, you may run into problems with your SSO login.

Configure service provider certificates

Occasionally, you may receive an email or see an alert indicating that the IdP certificate is about to expire. Because each IdP vendor has its own process for certificate renewal, this guide explains what's required in Intersight. It also provides general steps to retrieve updated IdP metadata and upload it to Intersight to complete the renewal.

Before you begin

Ensure to update all IdPs in your organization when renewing your service provider (SP) certificate.

Add or Renew SP Certificate

Procedure

1. Log in to Intersight.
2. Navigate to **Settings** > **AUTHENTICATION** > **Cisco Unified Identity**.
3. Navigate to **Identity Providers** > **Service providers (SP)**.
4. Select **Add or renew certificate**.
5. On the **Add or renew certificate** page:
   a. Select a certificate to add or renew. Choose one of these:
      - **Self-signed by Cisco**: We recommend this choice. Let Cisco sign the certificate so you only need to renew it once every five years.
      - **Signed by a public certificate authority**: The customer IdP provides a signature in the metadata that is signed by a Public Root CA. This option is more secure but you'll need to frequently update the metadata (unless your IdP vendor supports trust anchors).
   b. Select **Save**.

The SP Certificate is listed in the table view.

Actions available for SP certificates

In the table view, select ellipsis (**...**) next to an SP certificate to view the available actions.

This table describes the actions available for SP certificates:

Action	Description
Download metadata	To download the service provider certificate metadata. The service provider certificate metadata is used to configure and establish trust between the IdP and

	service providers. It contains the public certificate, the IdP entity ID, SSO URLs, and other relevant information, all packaged in a comprehensive XML file.
Download certificate	To download the public key certificate. If you do not want to download the entire certificate metadata, you can download the public key certificate to verify the authenticity of the IdP.

Set up multiple domains

You can use domains to ensure the security and integrity of your organization. You can also use domains to help with user management.

Add a domain

Before you begin

- You must own the domains you want to verify and claim.
- You must add domains in a specific order to prevent admin lockout. For example, you must add the administrator domain first, followed by all other domains.

Procedure

1. Log in to Intersight.
2. Navigate to **Settings** > **AUTHENTICATION** > **Cisco Unified Identity** > **Domains**.
3. Select **Add domain**.
4. On the **Add a Domain** page:
   a. Enter your domain or subdomain name and select **Add Domain**.
   b. Copy and add this DNS verification token to the TXT record section to prove that you own the domain.
   c. Select **Done**.
      - Your domain appears in your list of domains with the status **Pending**. Once verified, the status changes to **Verified**.

        After the domain is verified, the TXT record is no longer required, and you can remove the verification token from your DNS server.
      - If the verification fails, the error is cached by your DNS server. Your DNS server clears the cache after the specified length of time in the Time To Live (TTL) setting. You must wait to try again after the DNS server clears the cache. You can add the verification token again and request the verification for the domain.

The domain is listed in the table view.

Actions available for domains

In the table view, select ellipsis (**...**) next to a domain to view the available actions.

This table describes the actions available for domains:

Action	Description
Remove domain	You can remove a domain from your organization at any time. For example, if you sell a domain or no longer need a test domain used in a trial, you may want to remove it.

Set up groups

Groups are useful when you want to assign a specific IdP to a group of users.

Create a group

Before you begin

Ensure that you create the domain name in Cisco Single Sign-On, add the domain name, and finally navigate to the Single Sign-On section to add the IdP.

Procedure

1. Log in to Intersight.
2. Navigate to **Settings** > **AUTHENTICATION** > **Cisco Unified Identity** > **Groups**.
3. Select **Create a Group**.
4. On the **Create a new group** page:
    a. In the **Name** field, enter the group name.
    b. (Optional) In the **Description** field, enter a description for the group.
    c. Select **Next**.
5. In **Add group members (optional)**:
    a. Search and select members for the group. You can add up to 500 group members at a time.
    b. Select **Create group**.

The group is listed in the table view.

Actions available for groups

In the table view, select ellipsis (**...**) next to a group to view the available actions.

This table describes the actions available for groups:

Action	Description
Add member	To add a member.
View group details	To view group details.
Delete group	To delete the group.

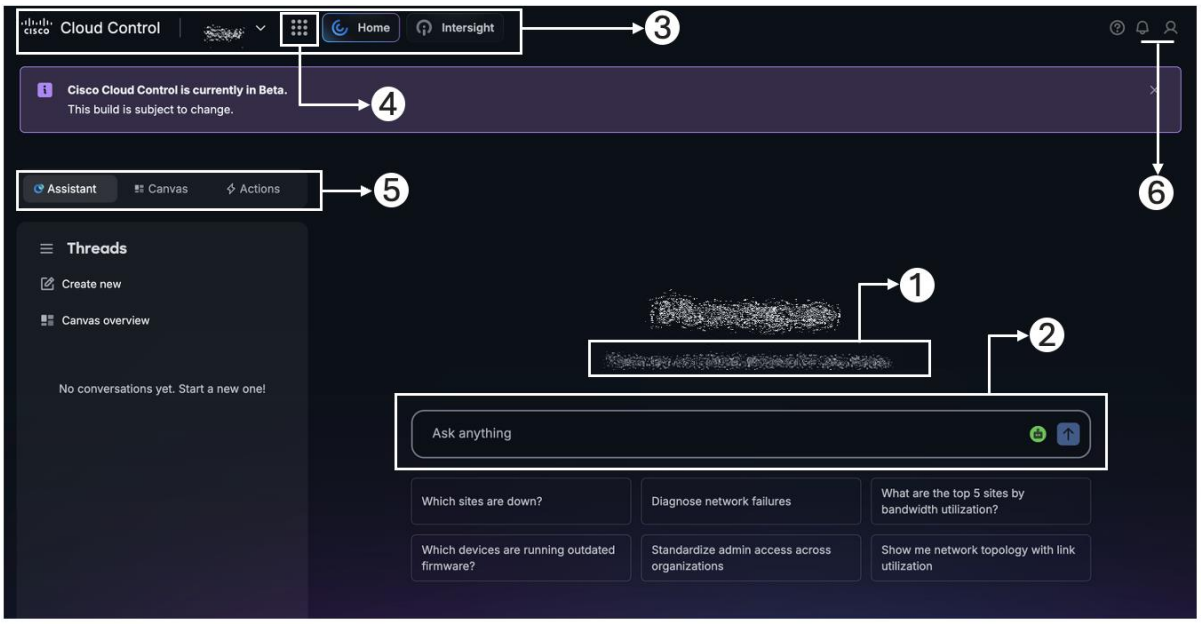
Associate Intersight with Cisco Cloud Control

Follow these steps to associate Intersight with Cisco Cloud Control:

1. Go to https://cloud.cisco.com
2. Complete the Intersight account linking and onboarding steps. For more information, refer to Cisco Cloud Control Getting Started.

Cisco Cloud Control Home page

The Cisco Cloud Control Home page is the main entry point for working across your Cisco environment. From here, you can review actions that need attention, use AI Assistant or AI Canvas to investigate, and open platform apps and integrated products.



1. **Action summary:** The **Home** page displays a greeting, a status message, and the number of actions that require review. When actions are available, select **Review actions** to view issues that need attention.
2. **AI Assistant:** AI Assistant is the natural language entry point in Cisco Cloud Control. Use it to ask questions, get quick answers, and continue investigations.
3. **Top navigation bar:** Use the navigation bar at the top of the window to quickly access the integrated products and platform apps you use most often. It remains consistent across integrated products, giving you the ability to move between Cisco Cloud Control and onboarded products without losing context.

   From the top navigation bar, you can change the currently selected tenant using the tenant switcher, access app launcher, return to **Home,** cross-launch onboarded products, access pinned items, or access admin settings and integrations.
4. **App launcher:** The app launcher opens additional navigation options.

   From the app launcher, you can search for products and favorites, access platform apps such as inventory, topology, and workflows, access onboarded products that are not pinned to the top navigation bar, or access your favorites.
5. **Homepage tabs:** Switch between **Assistant**, **Canvas**, and **Actions** to ask questions, investigate issues in a shared workspace, and review issues that need attention. By default, **Assistant** is selected.

6. **Notifications and user settings:** Access notifications and user settings, including options to log out or change the display theme.

Launch Intersight from within Cisco Cloud Control

You can access the onboarded Intersight account from Cisco Cloud Control by using the top navigation bar or the app launcher. If Intersight is launched from within Canvas, the Intersight header provides quick access to **AI Assistant** and **Canvas**. Pinned products appear in the navigation bar for quicker access.

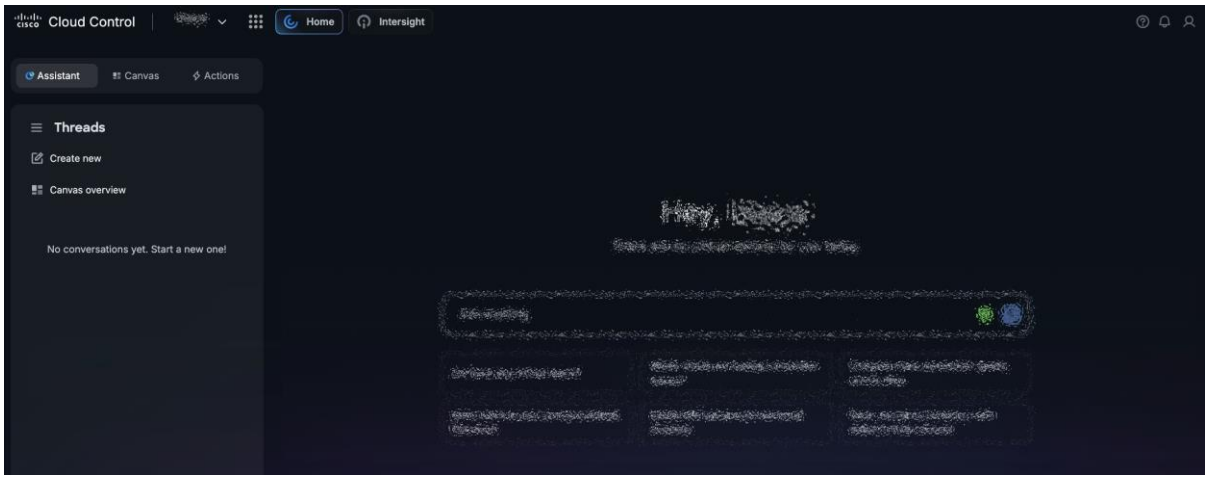
Before you begin

Ensure that you have created a CUI-enabled account in Intersight. For more information, refer to Create a CUI account in Intersight.

Procedure

To cross-launch **Intersight** from the **Cisco Cloud Control:**

1. Go to https://cloud.cisco.com
2. Log in to Cisco Cloud Control using the Intersight login credentials.
3. Open the app launcher .
4. Select **Intersight**.



To pin or unpin Intersight:

1. Select .
2. Select the pin next to the item to add it to or remove it from the navigation bar.

Note: If you log out from a CUI-enabled native Intersight session, you are also logged out from Intersight in Cisco Cloud Control. If you log out from Intersight in Cisco Cloud Control, you are also logged out from the same account in the native Intersight session. Logging out from another Cisco Cloud Control-enabled product does not log you out from Intersight.

Additional resources

- Cisco Cloud Control Getting Started
- Intersight Help Center

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA **Cxx-xxxxxx-xx** **06/26**