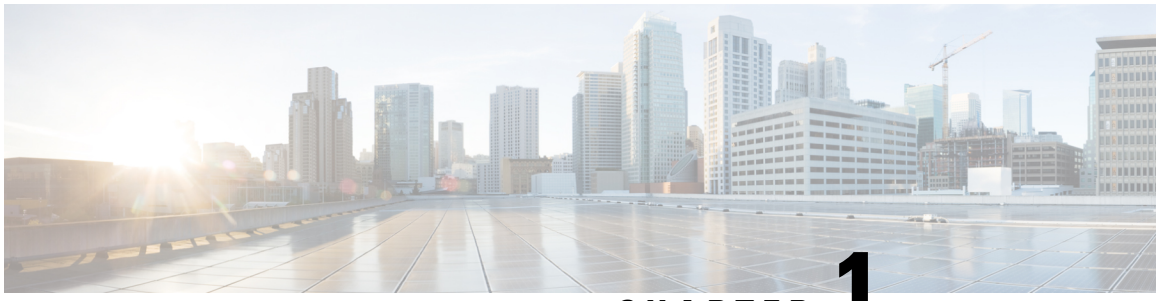
Cisco Security Cloud Control User Guide

First Published: 2023-04-16

Last Modified: 2024-08-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

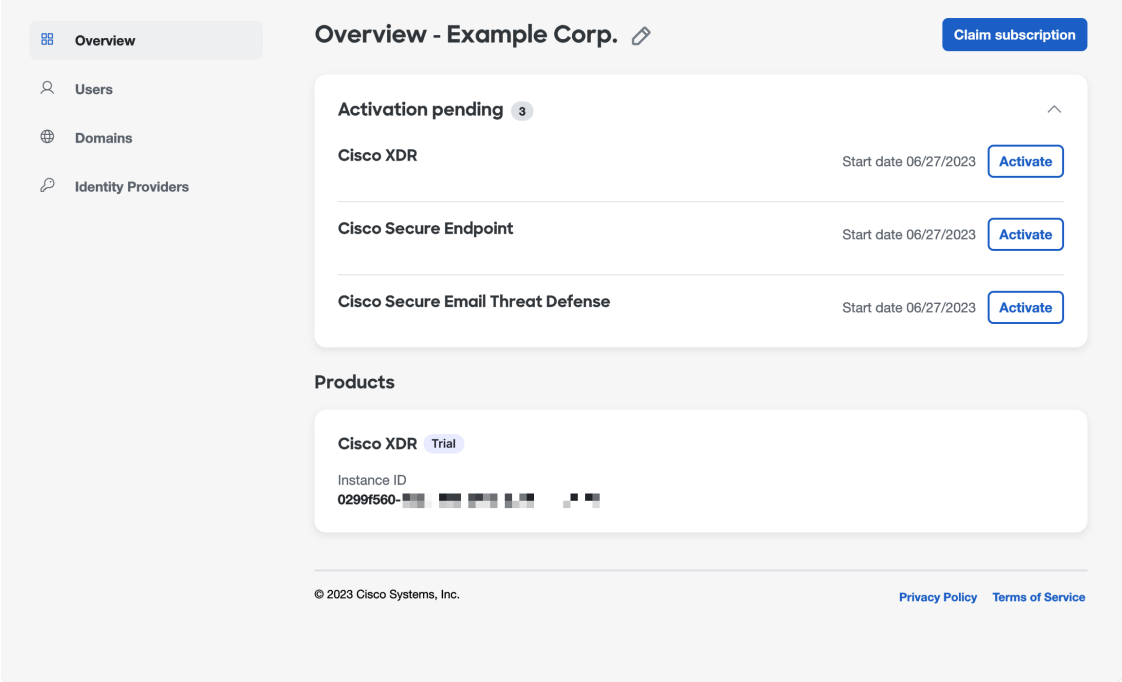
Overview

Cisco Security Cloud Control overview

Security Cloud Control 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.

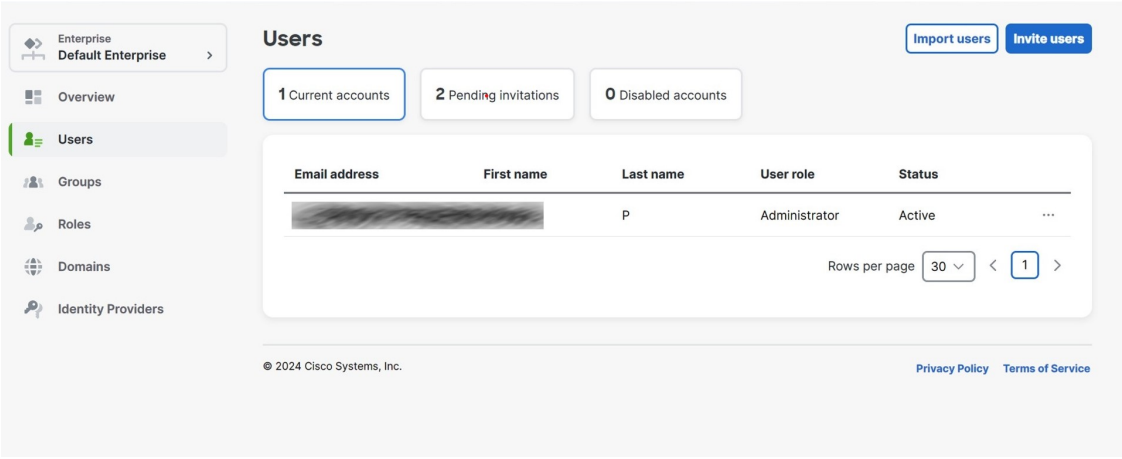
Overview tab

The **Overview** tab lists your currently activated Cisco product instances and those that are pending activation. You also can claim a subscription or attach an external product to Security Cloud from here. For details, see Managing products and subscriptions, on page 9.



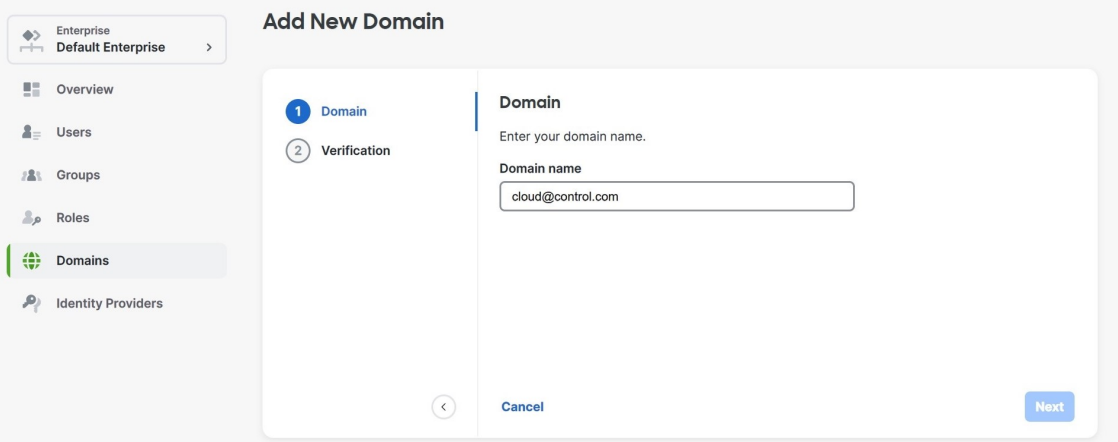
Users tab

The **Users**tab lists all users who are connected to the enterprise. The enterprise administrator can invite and add users to an enterprise. Administrator can also reset user passwords and MFA settings (for users in a Claim and verify a domain) and deactivate user accounts. See Managing users, on page 17 for more information.



Domains tab

The **Domains** tab lists email domains that have been claimed and verified for the enterprise. Verifying a domain is required to integrate an identity provider with Security Cloud Sign On. It also allows administrators to reset passwords or MFA settings of users in the claimed domain. See Managing domains, on page 21 for more information.



Identity Providers tab

The **Identity Providers** tab lists any identity providers integrated with Security Cloud Sign On using SAML (Secure Assertion Markup Language) for the current enterprise. This allows enterprise users to access their Cisco Secure products with their identity provider's SSO credentials. See Identity provider integration guide, on page 23for details.

Signing in to Security Cloud Control

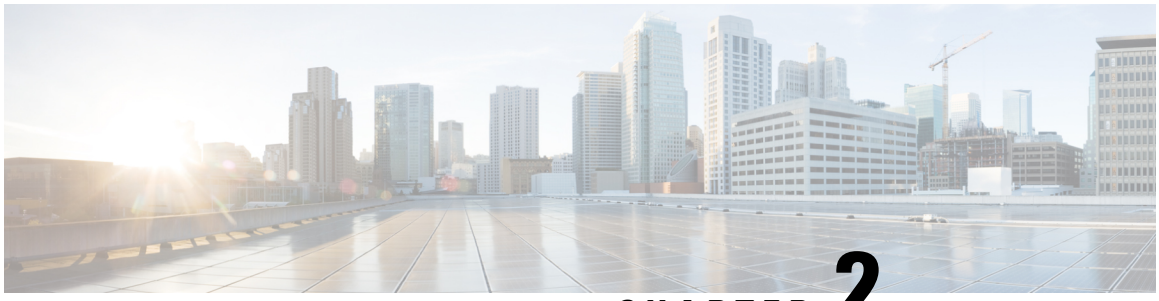
To sign in to Security Cloud Control you need a Cisco Security Cloud Sign On account. If you don't have an account, create one and configure multi-factor authentication with either Duo MFA or Google Authenticator. The first time you sign in to Security Cloud Control with your Security Cloud Sign On account, a new enterprise is created with your Security Cloud Sign On account as the sole Managing users in the enterprise.

If you only have one enterprise associated with your account, it will always be the default account when you log in. If you have multiple enterprises associated with your account, the latest one you used will be selected after you sign in.

Step 1 Open Security Cloud Control.

Step 2 Sign in with your Security Cloud Sign On credentials and MFA options you established when creating your account.

If this is the first time signing in to Security Cloud Control, account, a new enterprise is created for you with a default name. You can Rename an enterprise the enterprise by clicking the pencil icon.



CHAPTER 2

Managing enterprises

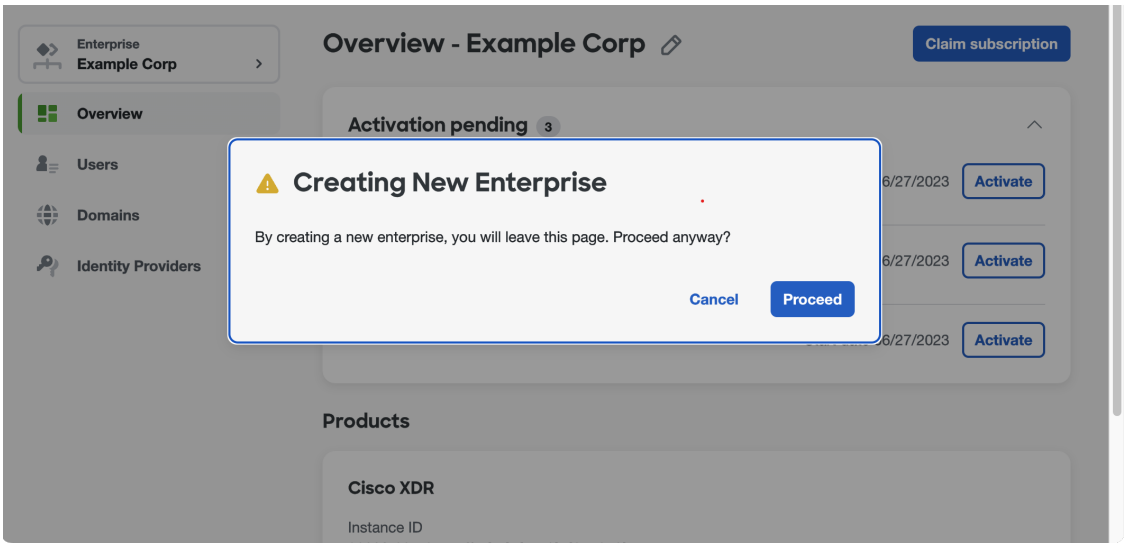
A Security Cloud enterprise is a trust boundary for Cisco products, Managing users, registered Managing domains, Identity provider integration guide, and other metadata.

Create an enterprise

You can create multiple enterprise, each with their own set of users, products, and other enterprise data.

Step 1 In Security Cloud Control, hover over the **Enterprise** menu at the top of the browser and click **Create new enterprise**.

A dialog warns you that by creating a new enterprise will you leave the current page.



Step 2 Click **Proceed**.

Security Cloud Control reloads with the new created enterprise selected. The enterprise is given a default name, which you can Rename an enterprise.

Rename an enterprise

You can rename an enterprise that you've created. enterprise names are limited to 50 characters.

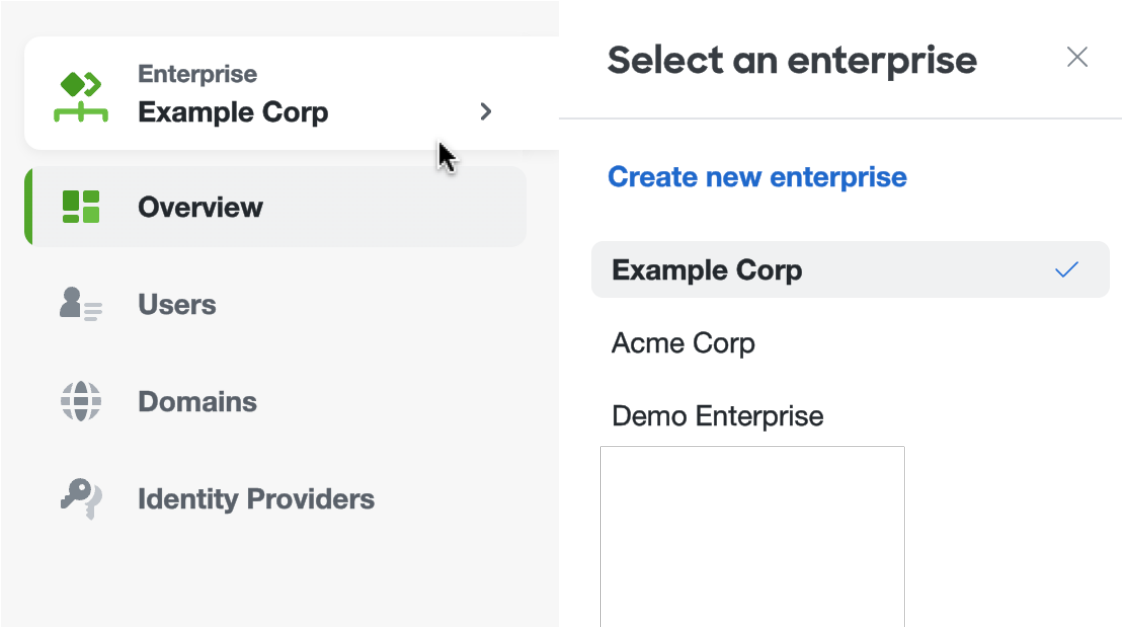
Step 1 Switch enterprises that you want to rename from the **Enterprise** menu.

Step 2 Click the pencil icon next to the enterprise name at the top of Security Cloud Control.

Step 3 Enter the new enterprise name and click **Save**.

Switch enterprises

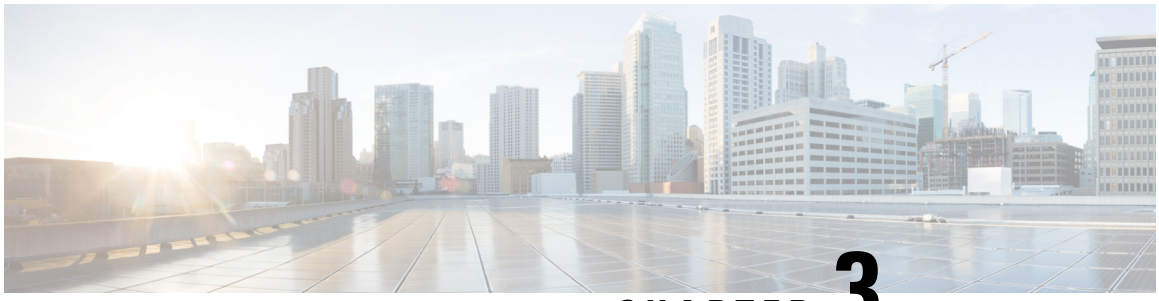
All operations you perform in Security Cloud Control, such as creating domains or inviting users, are applied to the currently selected enterprise. The **Enterprise** menu at the top of Security Cloud Control shows the currently selected enterprise. To switch to another enterprise, hover over the **Enterprise** menu and select an enterprise from the fly-out menu. You can also Switch enterprises from this menu.



Step 1 Sign in to Security Cloud Control.

Step 2 Hover over the **Enterprise** menu and select the desired enterprise from the fly-out menu.

Security Cloud Control reloads with the selected enterprise.



CHAPTER 3

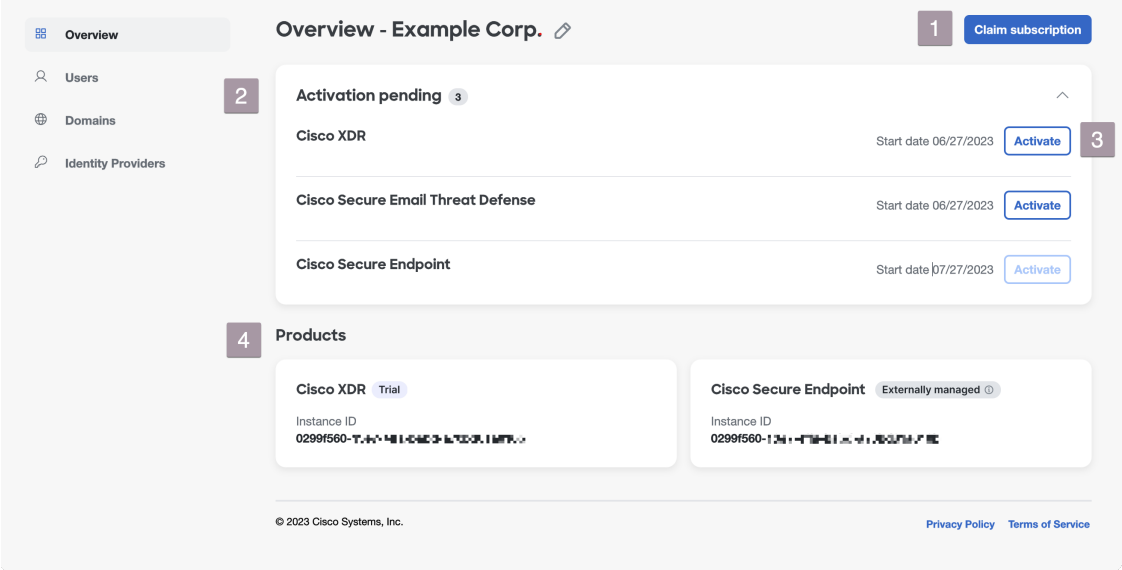
Managing products and subscriptions

Overview

When a new subscription is purchased from Cisco, a subscription claim code is emailed to the initial contact specified during the purchase process. Once a Security Cloud enterprise administrator receives the claim code, they click **Claim subscription** (**1**) to Claim a subscription for the current enterprise.

Once a subscription is claimed, its products are listed under **Activation pending** on the Overview tab with their corresponding start dates (**2**). When the start date for a product subscription has been reached, the **Activate** button (**3**) is enabled, allowing the enterprise administrator to Overview the product. Activated products are listed in the **Products** section (**4**).

Trial products are indicated by a Trial label. Externally managed product instances that have been Attach an externally managed product instance have an Externally managed label.



Claim a subscription

When a Cisco Secure product subscription is purchased, a subscription claim code is emailed to the user designated as the initial product activation contact. This contact may or may not be the Security Cloud Control administrator who will manage the subscription. A Security Cloud Control administrator uses the claim code to claim the subscription for an enterprise. Once claimed, a subscription's products are added to the **Activation pending** list and can be Activate a product instance once the subscription's start date has been reached.

Before you begin

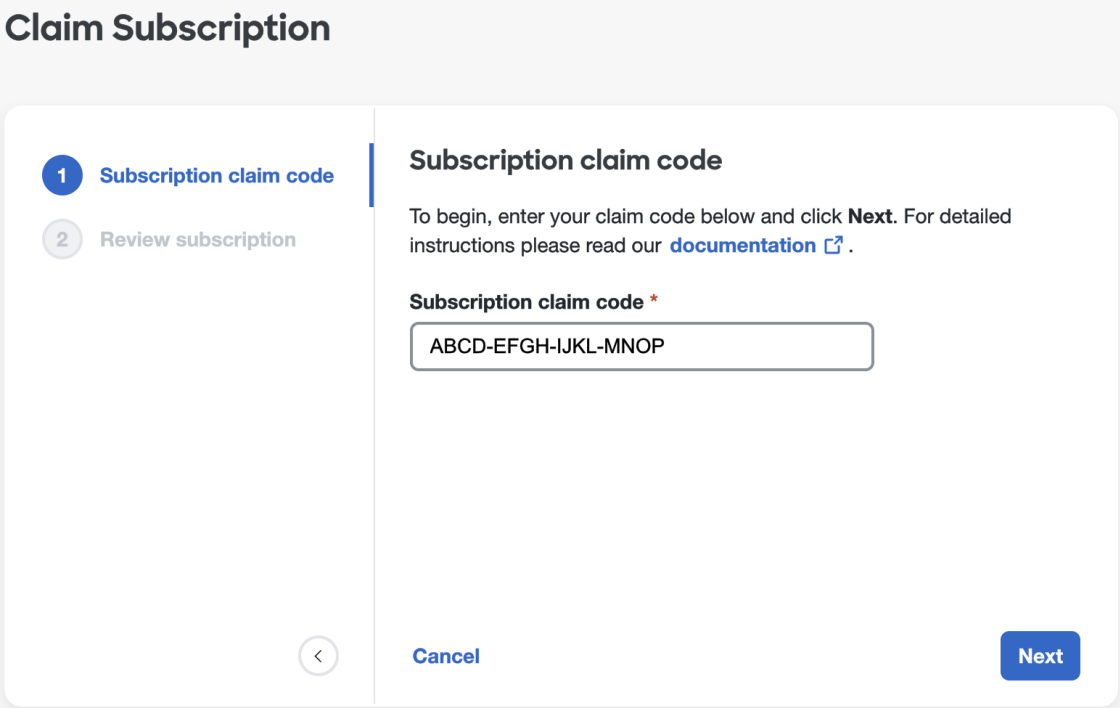
You will need a subscription claim code to complete these steps.

Step 1 Sign in to Security Cloud Control.

Step 2 When prompted, select the enterprise where you want to claim and activate the products in the subscription or create a new enterprise.

Step 3 Click **Claim subscription** in the upper-right corner.

Step 4 Enter the claim code and click **Next**.



Step 5 Review the list of products in the subscription, then click **Claim subscription**.

The products in the subscription are added to the **Activation pending** list on the **Overview** tab.

What to do next

You can start Activate a product instance whose subscription start dates have been reached.

Activate a product instance

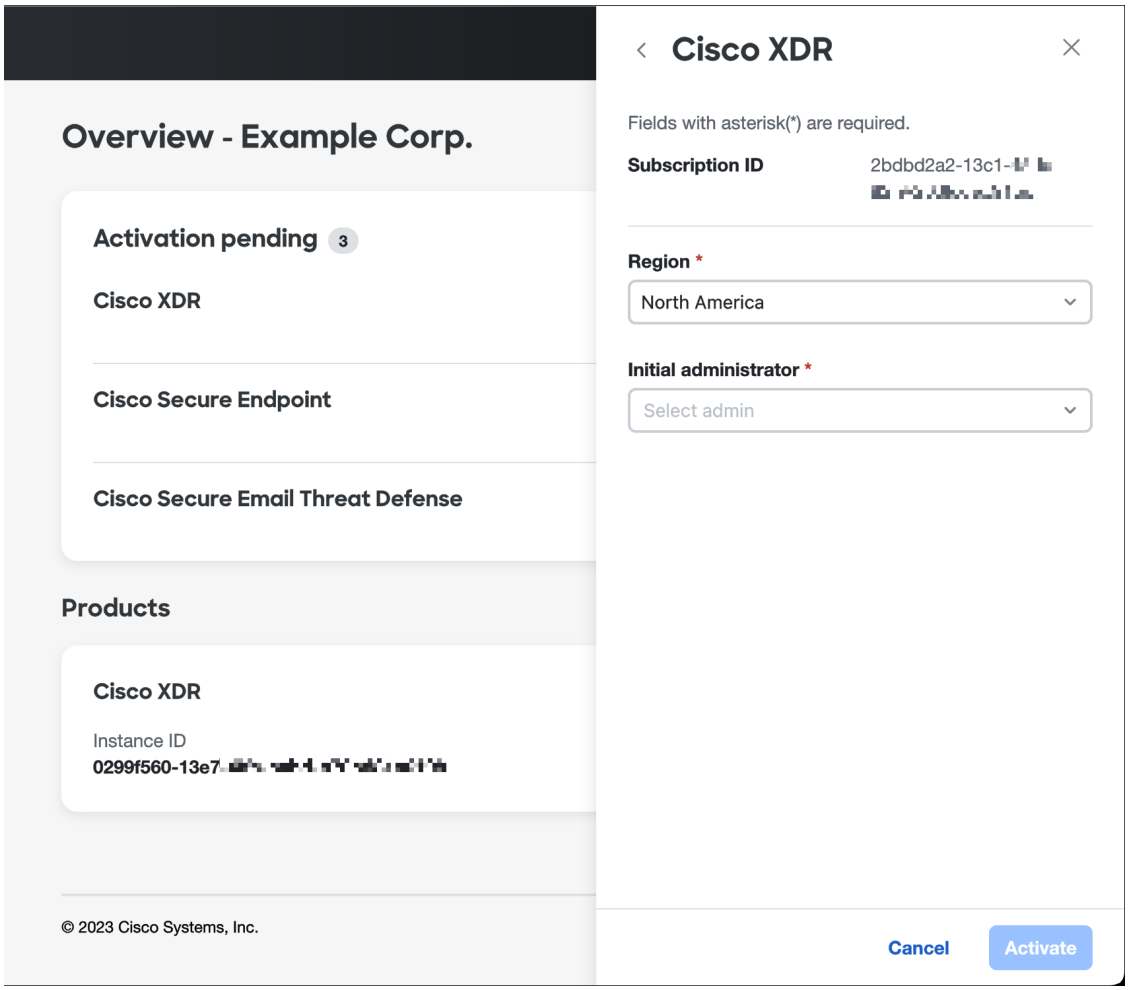
Once a subscription has been Claim a subscription and its start date has been reached, you can activate the products in the subscription. If there is an existing product instance activated in the current enterprise, you can choose to apply the new product license to an existing instance, or activate a new instance. When activating a new instance, you specify the region where it will be activated and the email of the user to be the initial administrator.

Step 1 Sign in to Security Cloud Control.

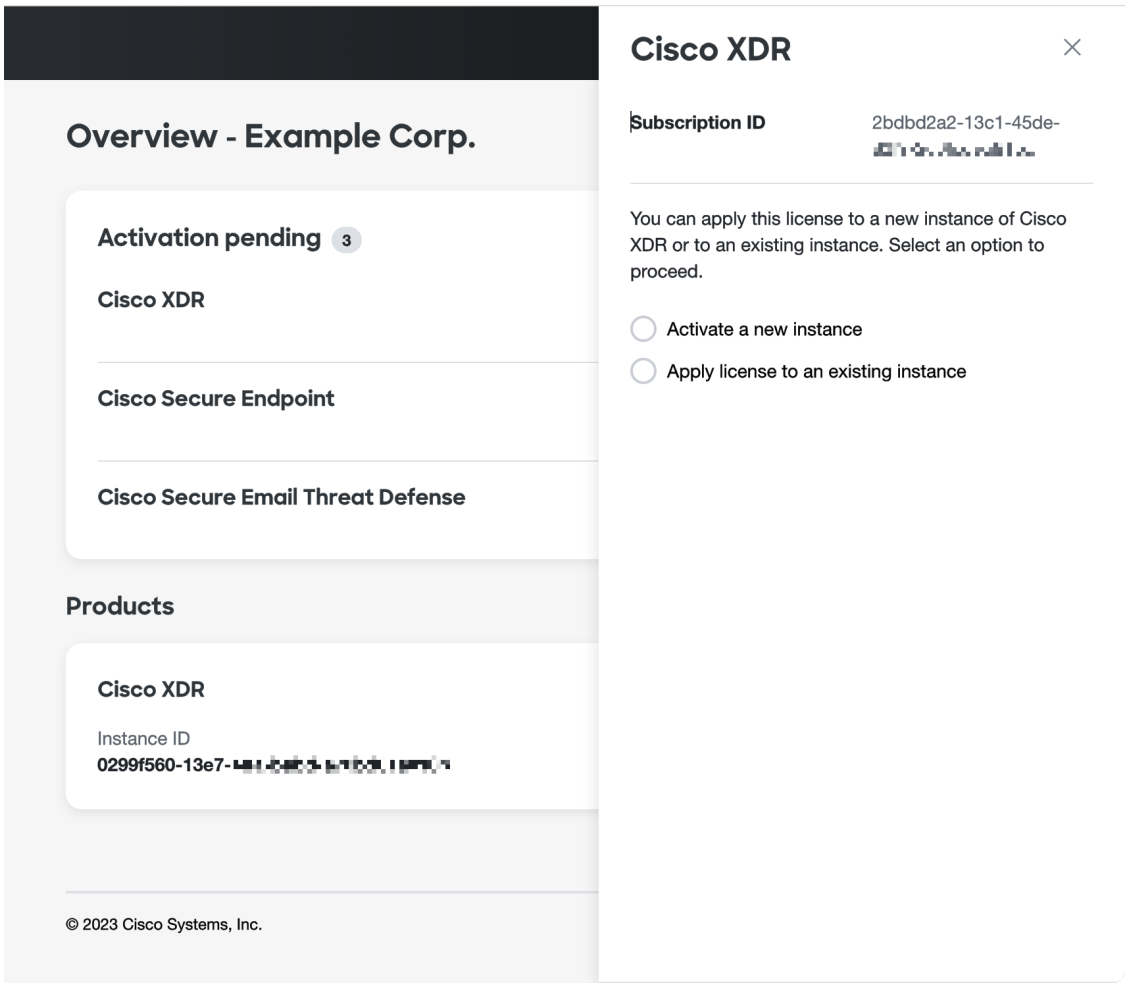
Step 2 When prompted to select an enterprise, select the same enterprise that was used to Claim a subscription the associated product subscription.

Step 3 In the **Activation pending** list, click **Activate** for the product you want to activate.

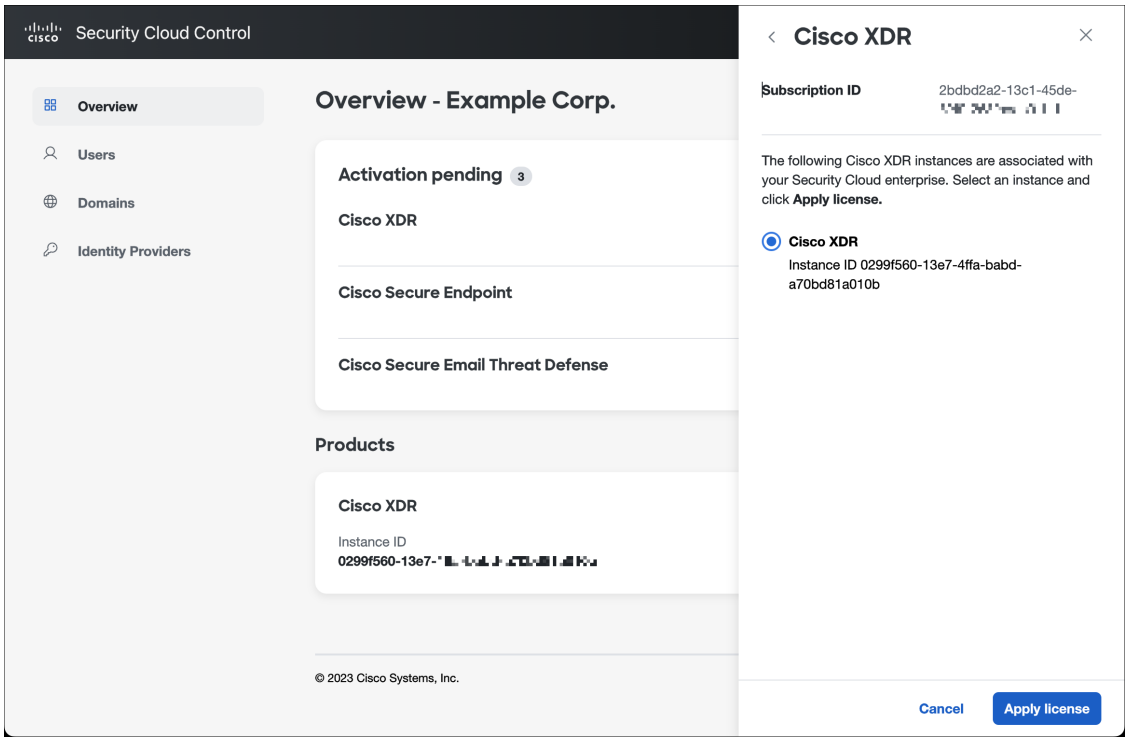
- If there are no existing activated instances of the product, select the region where you'd like to activate the product and the email of the initial administrator. Click **Activate** when ready.



- If there is an existing, activated instance of the same product, you are asked if you want to activate a new instance, or apply the license to an existing instance.



- To activate a new instance, select **Activate a new instance** and follow the same procedure as above. To apply the license to an existing instance, select **Apply license to an existing instance**, select the desired instance, and click **Apply license**.



The product is added to the **Products** table.

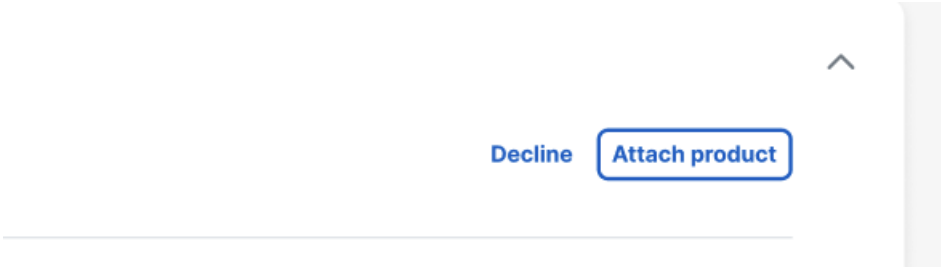
Attach an externally managed product instance

If you have a Cisco product instance that is managed outside of Security Cloud Control, you can optionally attach it to a Security Cloud enterprise. Cisco initiates this process by sending an email to a list of Security Cloud Control admins with an invitation to attach the instance to Security Cloud. An admin can sign in and attach the external instance to Security Cloud. Product instances that are attached to Security Cloud have an **Externally managed** label next to their product name.

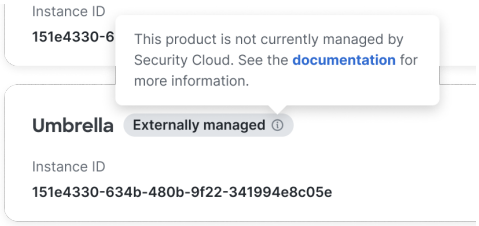
Step 1 Sign in to Security Cloud Control.

Step 2 When prompted to select an enterprise, select the enterprise to which you would like to attach the externally managed product instance.

Step 3 Click **Attach product** next to the product you wish to attach.



The attached product appears in your list of products with an **Externally managed** label.



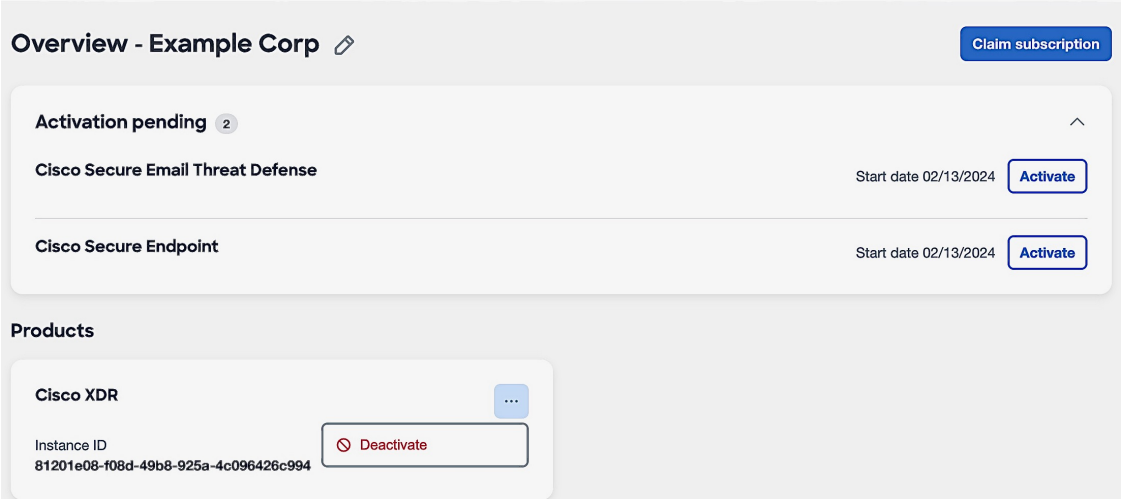
Deactivate a product instance

If you have accidentally activated a product instance or if you want to reuse the license for an existing or a new tenant, you can deactivate the product instance. After you deactivate a product instance, it reaches an inactive state. Active licenses are made available again and the enterprise administrator receives a product deactivation notification.

Step 1 Sign in to Security Cloud Control.

Step 2 When prompted to select an enterprise, select the same enterprise that was used to activate the product subscription.

Step 3 In the **Overview** page, under the **Products** table, click the three-dot menu ... next to the product to be deactivated and select **Deactivate**.



Step 4 In the deactivate confirmation dialog box, click **Deactivate**.

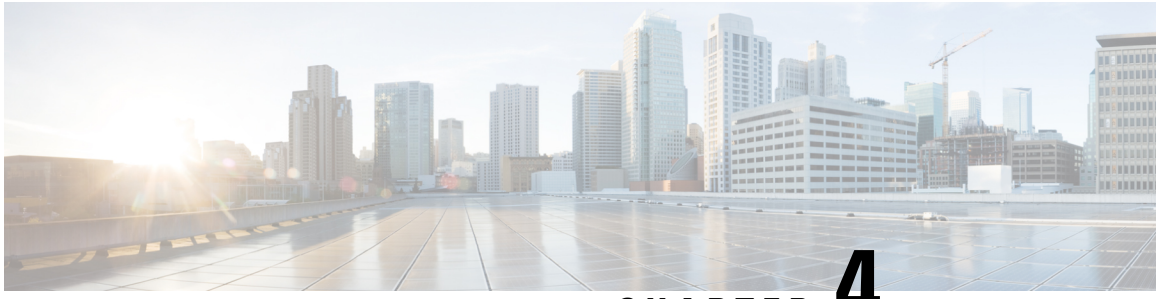
After deactivation, all services for the product instance are suspended and the product is removed from the **Products** table.

The subscription licenses for the deactivated product is returned to the **Activation pending** table.

The subscription licenses are now available to activate a new product instance or you can apply the licenses to an existing product instance. For more information, see Activate a product instance.

An email about the product deactivation is sent to the enterprise administrator.

If the deactivation process results in an error, contact the Cisco support team at Support Case Manager.



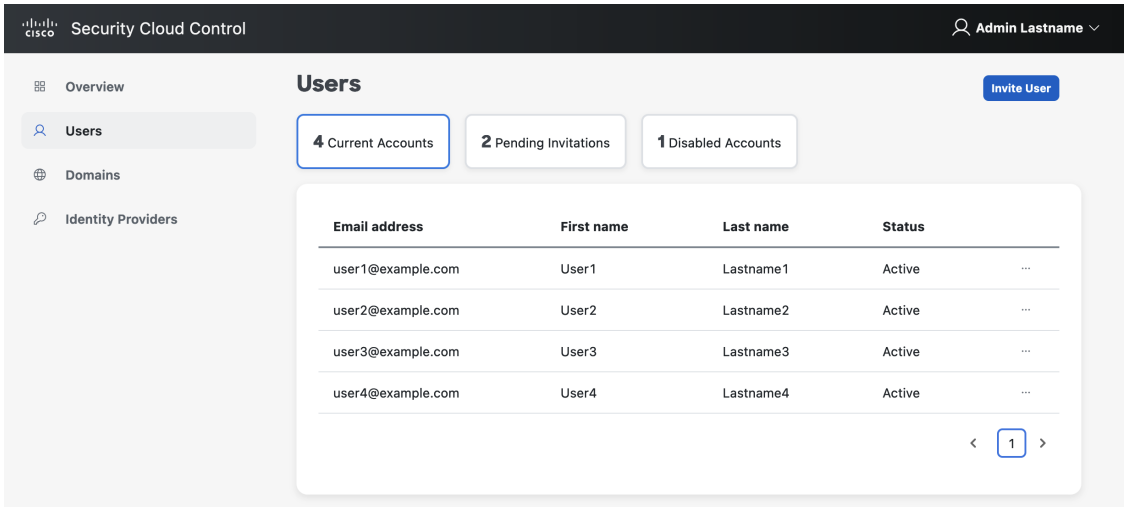
CHAPTER 4

Managing users

List users

The **Users** page provides the following views of user accounts:

- **Current Accounts** lists users in your enterprise that have been Invite a user to your enterprise.
- **Pending Invitations** lists users who have been Invite a user to join your enterprise but haven't yet activated their accounts.
- **Disabled Accounts** lists users whose accounts have been Remove a user account.



Invite a user

Enterprise administrators can invite a user to join an enterprise.

Step 1 Select the **Users** tab.

Step 2 Click **Invite User**.

Step 3 Enter the user's first name, last name, and email address.

Step 4 Click **Invite**.

Invited users are sent an email with an activation link that expires in one hour. Invitations that haven't been activated yet can be viewed under **Pending Invitations** (see List users).

Note Account activation emails are not sent to users in enterprises that have integrated an identity provider with Security Cloud Sign On.

Edit a user

An enterprise administrator can edit a user's first and last name. A user's email address can't be changed.

Step 1 Click **Users** in the left navigation, then click **Current Users**.

Step 2 Click the menu icon ... and select **Edit**.

Step 3 Edit the user's first name or last name.

Step 4 Click **Update**.

Reset user password

Enterprise administrators can reset the password for users who belong to a verified email domain.

Step 1 Click **Users** in the left navigation pane.

Step 2 Under the **Current Accounts** tab, locate the user whose password is to be reset.

Step 3 Click the three-dot menu icon ... adjacent to the user name and select **Reset password**.

On the next sign-in, that user is prompted to reset the password.

Remove a user account

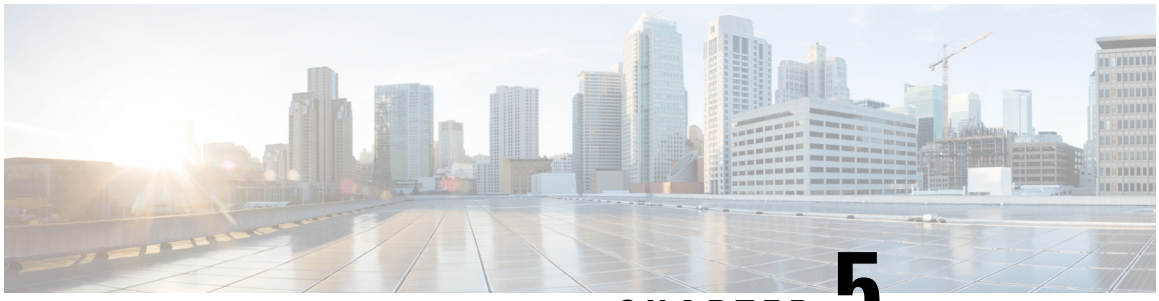
An enterprise administrator can remove a user account from the enterprise.

Step 1 Click **Users** in the left navigation pane.

Step 2 In the **Current Accounts** tab, click the three-dot menu ... adjacent to the user entry that you want to delete, and select **Remove user**.

Step 3 In the **Remove User** dialog box, click **Remove**.

The user account is removed from the enterprise and the user will no longer have access to any of the products within the enterprise.



CHAPTER 5

Managing domains

You can Claim and verify a domain for your enterprise in Security Cloud Control. This is a prerequisite to Identity provider integration guide with Security Cloud Sign On. It's also required to enable enterprise administrators to reset users' passwords or MFA settings in the claimed domain.

- Claim and verify a domain, on page 21

Claim and verify a domain

- The DNS record you create can be deleted once Security Cloud Control has verified the domain.
- You can currently verify a single domain with Security Cloud Control. If you need to verify multiple domains, please open a case with Cisco Technical Assistance Center (TAC).

Before you begin

To complete this task, you will need to be able to create a DNS record on the registrar service for your domain.

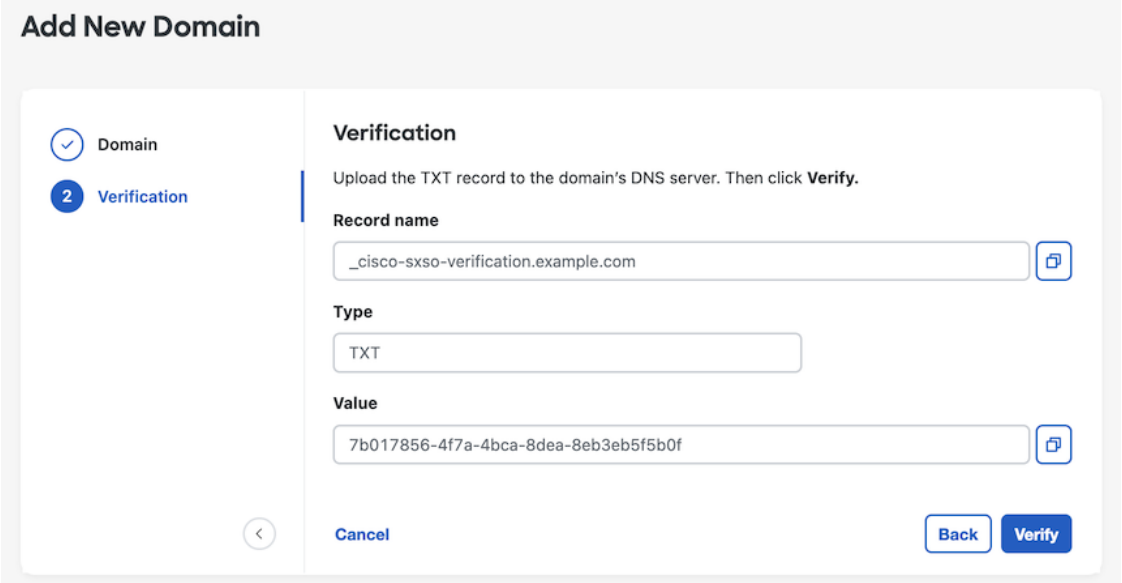
The **Domains** tab lists domains that you've Claim and verify a domain or are in the process of verifying. If you haven't claimed a domain, an **+ Add Domain** button is shown instead.

Step 1 Select the **Domains** tab.

Step 2 Click **+ Add domain**.

Step 3 In the **Add New Domain** screen, enter the domain name you want to claim and click **Next**.

The Verification page shows the **Record name** and **Value** of a TXT record you need to create on your domain registrar.



Step 4 In a new browser tab, sign in to your domain name registrar service.

Step 5 Create a new TXT record with the specified **Record name** and **Value** provided by Security Cloud Control.

Step 6 Save your changes and allow time for the DNS record to propagate.

Step 7 Return to the **Add New Domain** and click **Verify**.

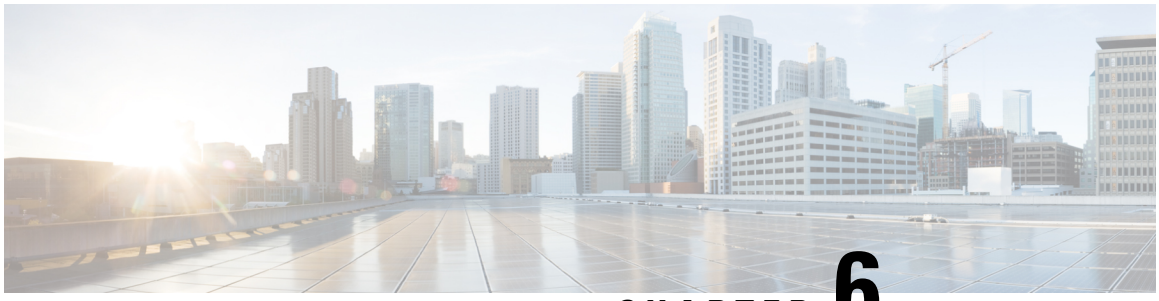
A message indicates if the verification was unsuccessful. If the verification was unsuccessful try the following

- Wait a while longer for the DNS record to propagate.
- Verify that the type, name and value of the DNS record you created on your domain registrar matches the values generated by Security Cloud Control.

What to do next

Once you've verified your email domain, you can do the following:

- Identity provider integration guide with Security Cloud Sign On
- Reset user password for users in the claimed domain.



CHAPTER 6

Identity provider integration guide

You can integrate an identity provider with Security Cloud Sign On using Security Assertion Markup Language (SAML) to provide SSO to your enterprise's users. By default, Security Cloud Sign On enrolls all users in Duo Multi-Factor Authentication (MFA) at no additional cost. If your organization already has MFA integrated with your IdP, you can optionally disable Duo-based MFA during integration.

For instructions to integrate with specific identity service providers, see the following guides:

- Auth0
- Azure AD
- Duo
- Google Identity
- Okta
- Ping

Note Once your identity provider is integrated, users in your domain must authenticate through the integrated identity provider and not through Cisco or Microsoft social log-in, for example.

Prerequisites

Integrating your identity provider with Security Cloud Sign On requires the following:

- A Claim and verify a domain

- The ability to create and configure SAML applications in your identity provider's management portal

SAML response requirements

In response to a SAML authentication request from Security Cloud Sign On, your identity provider sends a SAML response. If the user authenticated successfully, the response includes a SAML assertion that contains the `NameID` attribute and other user attributes. The SAML response must meet specific criteria, as explained below.

SHA-256-signed responses

The SAML assertion in the response from your identity provider must contain the following attribute names. These names must be mapped to the corresponding attributes of the IdP's user profile. IdP user profile attribute names vary by vendor.

SAML assertion attributes

The SAML assertion in the response from your identity provider must contain the following attribute names. These names must be mapped to the corresponding attributes of the IdP's user profile. IdP user profile attribute names vary by vendor.

SAML assertion attribute name	Identity provider user attribute
firstName	User's first or given name.
lastName	User's lastname or surname.
email	User's email. This must match the value of the **<NameID>** element in the SAML response (see below).

<NameID> element format

The value of the `<NameID>` element in the SAML response must be a valid email address and match the value of the assertion's `email` attribute. The `<NameID>` element's format attribute must be set to one of the following:

- `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`

Example SAML assertion

The following XML is an example of a SAML response from an identity provider to the Security Cloud Sign On ACL URL. Note that **jsmith@example.com** is the value of the `<NameID>` element and the `email` SAML response attribute.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id95383894959750298492624 25" IssueInstant="2023-08-02T01:13:04.861Z"
Version="2.0"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
    <saml2:Subject>
        <saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jsmith@example.com</saml2:NameID>
```

```
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData NotOnOrAfter="2023-08-02T01:18:05.160Z"
Recipient="https://sso.security.cisco.com/sso/saml2/0oa1rs8y79aeweVg80h8"/>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2023-08-02T01:08:05.160Z"
NotOnOrAfter="2023-08-02T01:18:05.160Z">
        <saml2:AudienceRestriction>

<saml2:Audience>https://www.okta.com/saml2/service-provider/12345678890</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2023-08-02T01:13:04.861Z">
        <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>

        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute Name="firstName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Joe

            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Smith
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">jsmith@example.com
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

Step 1: Initial setup

Before you begin

To begin, you need to provide a name for your Secure Cloud enterprise, and decide if you want to enroll your users in Duo Multi-Factor Authentication at no cost, or use your own MFA solution.

For all integrations, Cisco strongly recommends implementing MFA with a session timeout no greater than two hours, to help protect your sensitive data within Cisco Security products.

Step 1 Sign in to Security Cloud Control.

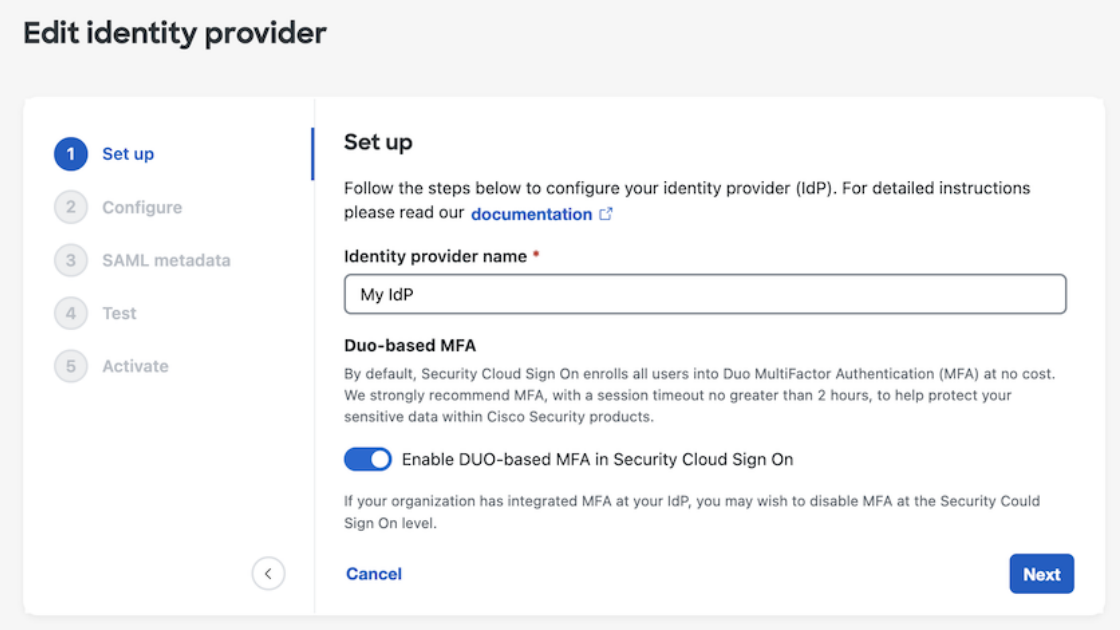
Step 2 Select **Identity Providers** from the left navigation.

Step 3 Click **+ Add Identity Provider**.

Note If you haven't claimed a domain yet you will instead see an **+ Add Domain** button. Click that button to begin Claim and verify a domain.

Step 4 On the **Set up** screen, enter a name for your identity provider.

Step 5 If desired, opt-out of Duo MFA for users in your Claim and verify a domain.



Step 6 Click **Next** to advance to the **Configure** screen.

Step 2: Provide Security Cloud SAML metadata to your identity provider

In this step you'll configure your identity provider's SAML application with the SAML metadata and signing certificate provided by Security Cloud Control. This includes the following:

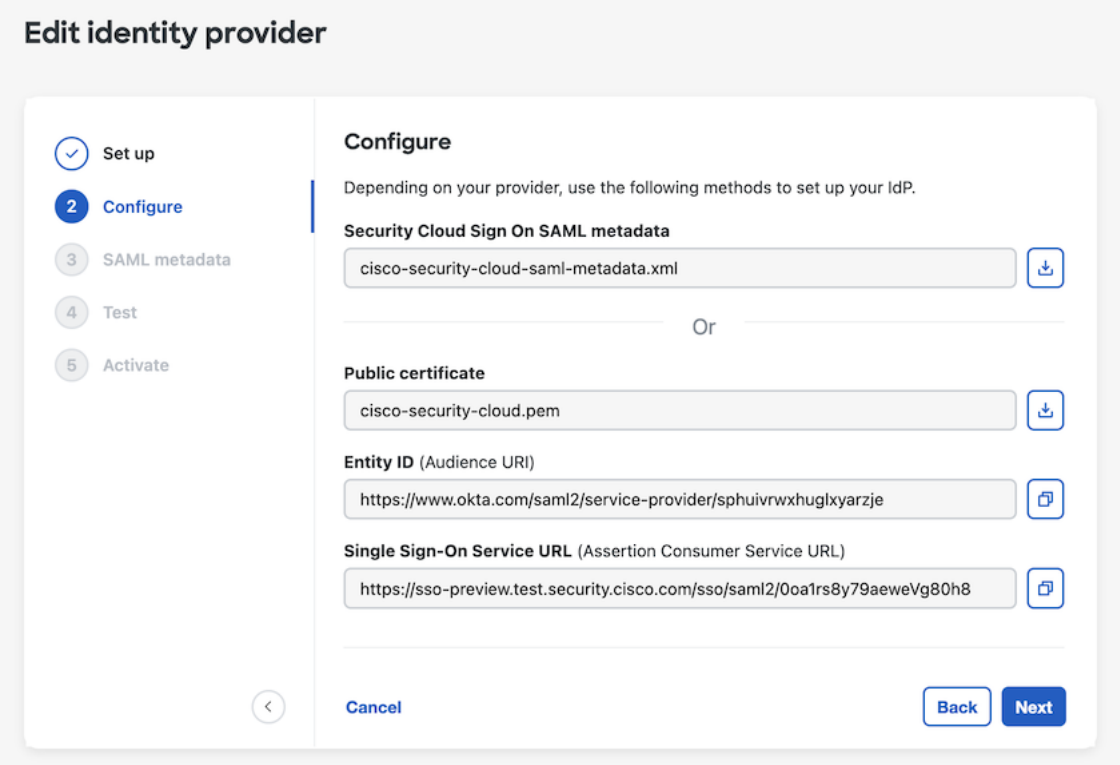
- **Single Sign-On Service URL** – Also called the Assertion Consumer Service (ACS) URL, this is the where your identity provider sends its SAML response after authenticating a user.
- **Entity ID** – Also called Audience URI, this uniquely identifies Security Cloud Sign On to your identity provider.
- **Signing certificate** – The X.509 signing certificate your identity provider uses to verify the signature sent by Security Cloud Sign On in authentication requests.

Security Cloud provides this information in a single SAML metadata file that you can upload to your identity provider (if supported), and as individual values, you can copy and paste. See Identity service provider instructions, on page 33 for steps specific to several commercially available identity service providers.

Step 1 Download the SAML metadata file on the **Configure** page if your identity provider supports it; otherwise, copy the **Single Sign-On Service** and **Entity ID** values, and download the **Public certificate**.

Step 2 On your identity provider , open your the SAML application want to integrate with Security Cloud Sign On.

Step 3 If supported by your provider, upload the SAML metadata file; otherwise, copy and paste the required Security Cloud Sign On SAML URIs into the corresponding configuration fields in your SAML application, and upload Security Cloud Sign On public signing certificate.



Step 4 Configure your SAML application with the Security Cloud Sign On SAML metadata you obtained in the previous step, either by importing the XML metadata file or manually entering the SSO Service URL and Entity ID values, and uploading the public signing certificate.

Step 5 Return to Security Cloud Control and click **Next**.

What to do next

Next you'll provide Security Cloud Control with the corresponding metadata for your identity provider's SAML application.

Step 3: Provide SAML metadata from your IdP to Security Cloud

Once you've Step 2: Provide Security Cloud SAML metadata to your identity provider with SAML metadata from Security Cloud Control, the next step is to provide the corresponding metadata from your SAML application to Security Cloud Control. See Identity service provider instructions, on page 33 for steps specific to a number of commercially available identity service providers.

Before you begin

To complete this step, you will need the following metadata for the SAML application on your identity provider:

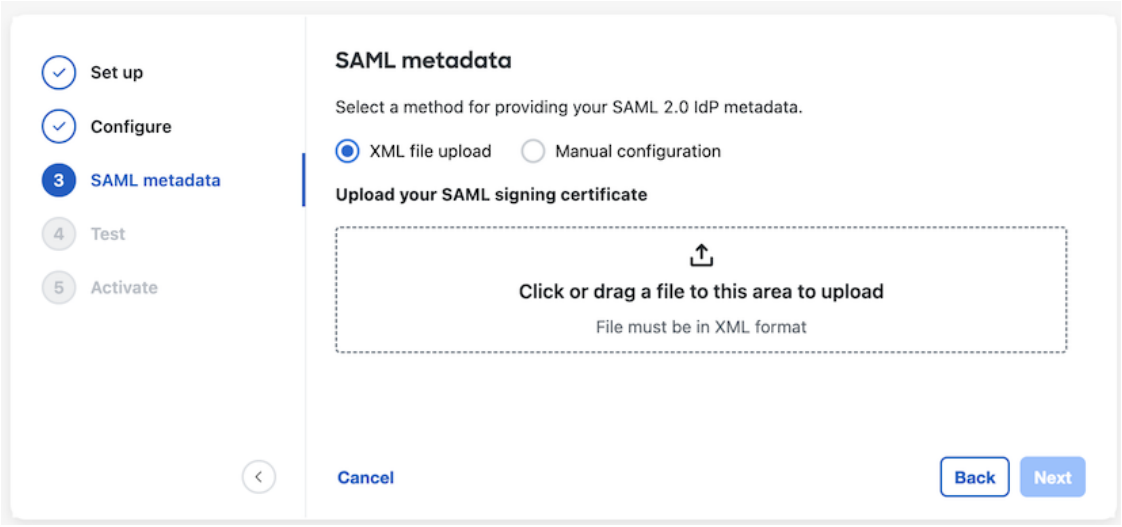
- Single Sign-on Service URL
- Entity ID (Audience URI)
- Signing certificate in PEM format

Depending on how your identity provider, you can either upload a metadata XML file that contains all of this information, or manually enter (copy/paste) the individual SAML URIs and upload the signing certificate. See Identity service provider instructions, on page 33 for steps specific to a number of commercially available identity service providers.

Step 1 Open the browser tab with Security Cloud Control.

Step 2 On the **SAML metadata** step, do one of the following:

- If you have an XML metadata file from your identity provider, select **XML file upload** and upload the XML file.
- Otherwise, click **Manual configuration** and enter the endpoints for the Single Sign-on Service URL, Entity ID, and upload the public signing certificate provided by your identity provider.



Step 3 Click **Next**.

What to do next

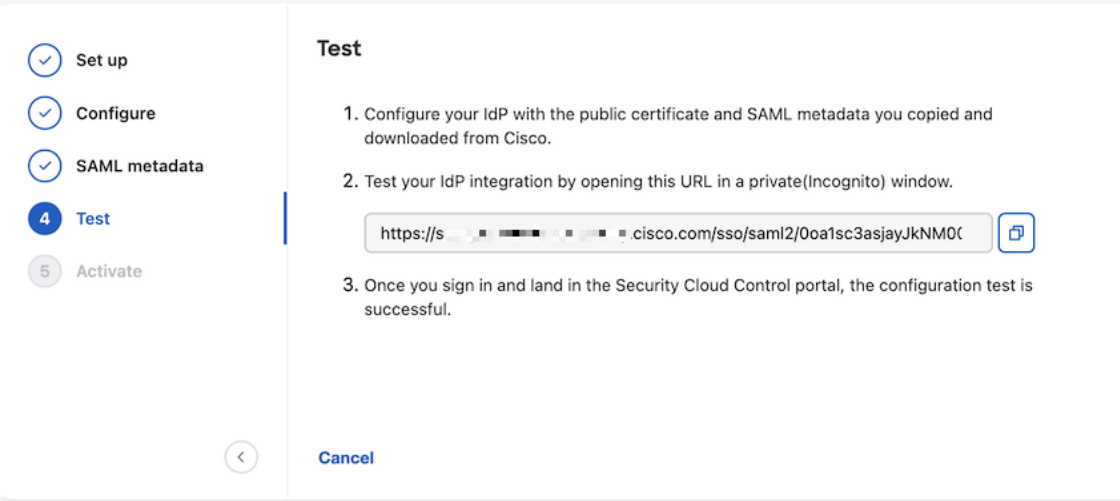
Next you'll Step 4: Test your SAML integration by initiating a SSO from Security Cloud Control to your identity provider.

Step 4: Test your SAML integration

Once you've exchanged SAML metadata between your SAML application and Security Cloud Sign On, you can test the integration. Security Cloud Sign On sends a SAML request to your identity provider's SSO URL. If your identity provider successfully authenticates the user, they are redirected and automatically signed in to the SecureX Application Portal.

Important: Be sure to test with an SSO user account other than the one you used to create the SAML integration in Security Cloud Control. For instance, if you used admin@example.com to create the integration then test with another SSO user (jsmith@example.com, for instance).

Step 1 In Security Cloud Control, copy the sign in URL displayed on the Test page to your clipboard and open it in a private (incognito) browser window.



Step 2 Sign in to your identity provider.

The test is successful if, after authenticating with your IdP, you are signed in to the SecureX Application Portal. If you receive an error, see Troubleshooting SAML errors, on page 30.

Click **Next** to advance to the **Activate** step.

Step 5: Activate the integration

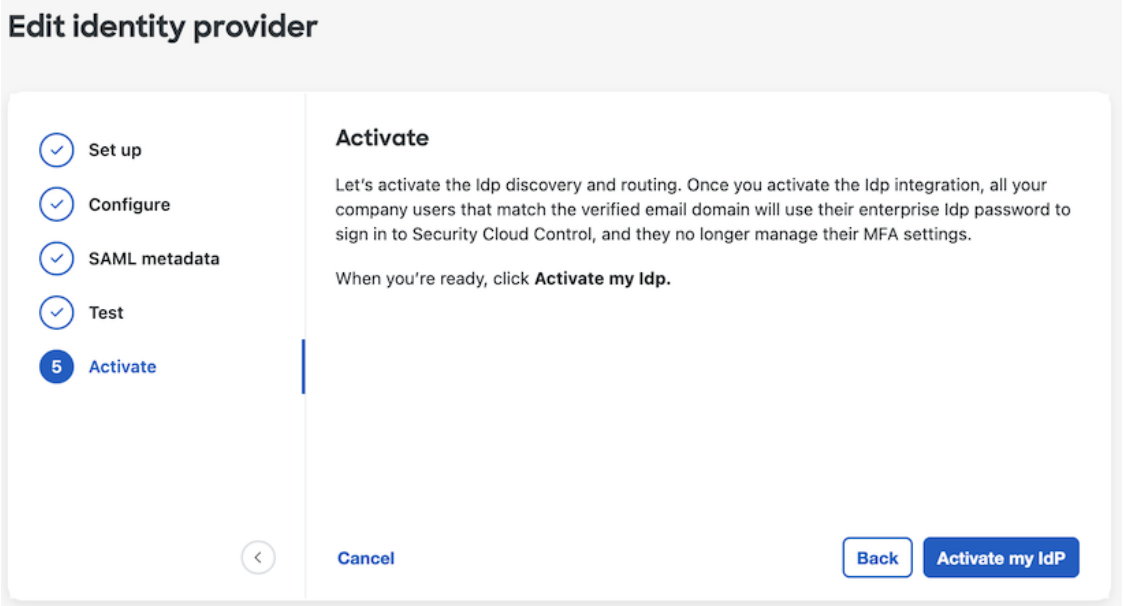
Once you've Step 4: Test your SAML integration you can activate it. Activating an integration has the following effects:

- Users in the verified domain **must** authenticate using the integrated identity provider. If a user tries to sign on using the Cisco or Microsoft social sign-on options, a 400 error will result.
- Users that sign in to Security Cloud Sign On with an email domain that matches your Claim and verify a domain will be redirected to your identity provider to authenticate.
- If you opted in to Duo MFA, users in your claimed domain will no longer manage their MFA settings.

Caution Be sure to Step 4: Test your SAML integration before activating it.

Activating an integration has the following effects:

Step 1 On the Activate step, click **Activate my IdP**.



Step 2 Click **Activate** in the dialog to confirm the action.

Troubleshooting SAML errors

If you get an HTTP 400 error when Step 4: Test your SAML integration, try the following troubleshooting steps.

Check that the user's sign-on email domain matches the claimed domain

Ensure the email domain of the user account you're using to test matches your Claim and verify a domain. For instance, if you claimed a top-level domain, such as `example.com`, then users must sign in with `<username>@example.com` and not `<username>@signon.example.com`.

Check that the user is signing in through their identity provider

Users must authenticate through the integrated identity provider. An HTTP 400 error is returned if a user signs in using the Cisco or Microsoft social sign-in options or attempts to sign in directly through Okta.

Check that the <NameID> element in the SAML response is an email address

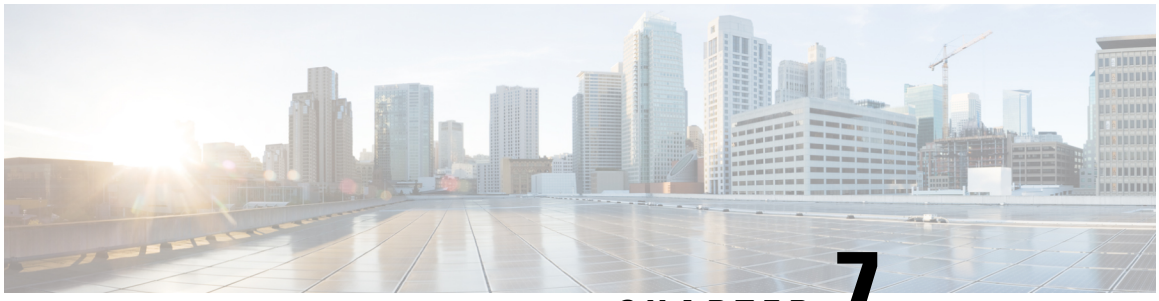
The value of the `<NameId>` element in the SAML response must be an email address. The email address must match the **email** specified in the user's SAML attributes. See SAML response requirements, on page 24 for details.

Check that the SAML response contains the correct attribute claims

The SAML response from your IdP to Security Cloud Sign On includes the required user attributes: **firstName**, **lastName**, and **email**. See SAML response requirements, on page 24 for details.

Check that the SAML response from your IdP is signed with SHA-256

SAML response from your identity provider must be signed with the SHA-256 signature algorithm. Security Cloud Sign On rejects assertions that are unsigned or signed with another algorithm.



CHAPTER 7

Identity service provider instructions

This guide provides instructions for integrating Security Cloud Sign On with various identity service providers.

Integrating Auth0 with Security Cloud Sign On

This guide explains how to integrate an Auth0 SAML Addon with Security Cloud Sign On.

Before you begin

Before you begin, read the Identity provider integration guide, on page 23 to understand the overall process. These instructions supplement that guide with details specific to Auth0 SAML integrations, specifically Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26 and Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

Step 1 Sign in to Security Cloud Control with the enterprise you want to integrate with Auth0.

a) Create a new identity provider and decide whether or not to opt out of Duo MFA, as explained in Step 1: Initial setup, on page 25.

b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26, download the **Public certificate**, and copy the values for **Entity ID** and **Single Sign-On Service URL** for use in the next steps.

Step 2 In a new browser tab, sign in to your Auth0 organization as an administrator. Keep the Security Cloud Control browser tab open as you'll return to it shortly.

a) Select **Applications** from the **Applications** menu.

b) Click **Create Application**.

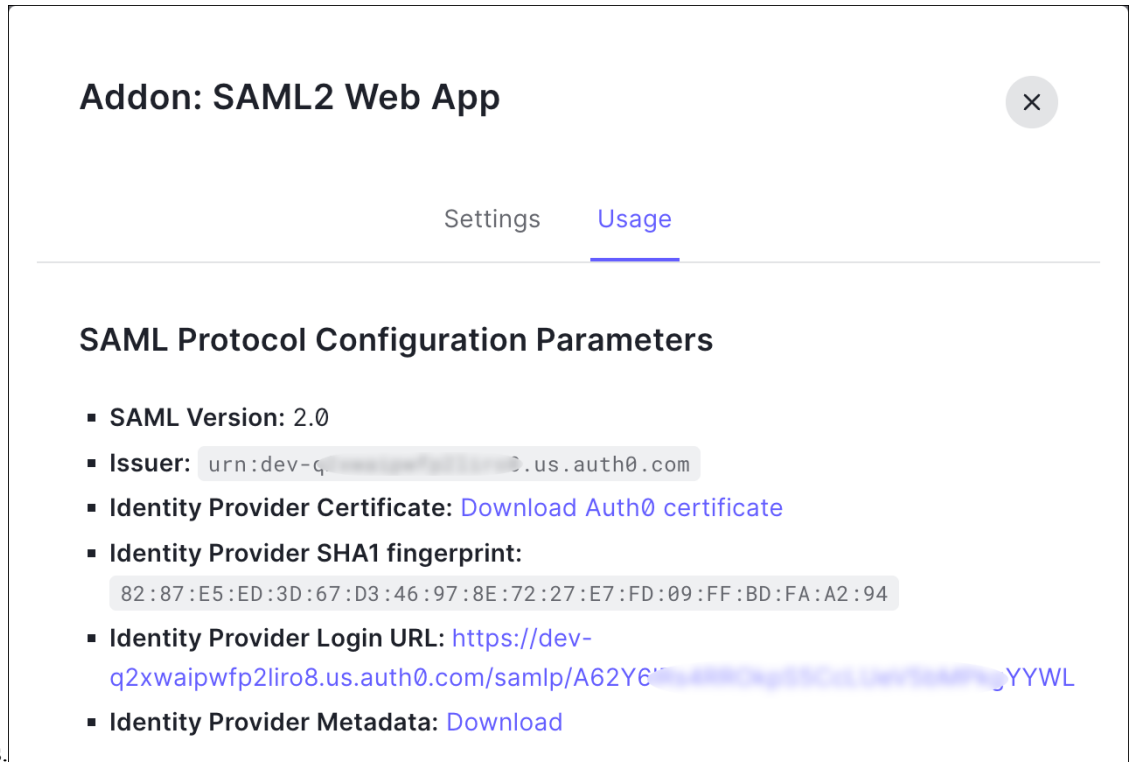
c) In the **Name** field enter `Secure Cloud Sign On`, or other name.

d) For application type, choose **Regular Web Applications** then click **Create**.

e) Click the **Addons** tab.

f) Click the **SAML2 Web App** toggle to enable the addon.

The SAML2 Web App configuration dialog



opens.

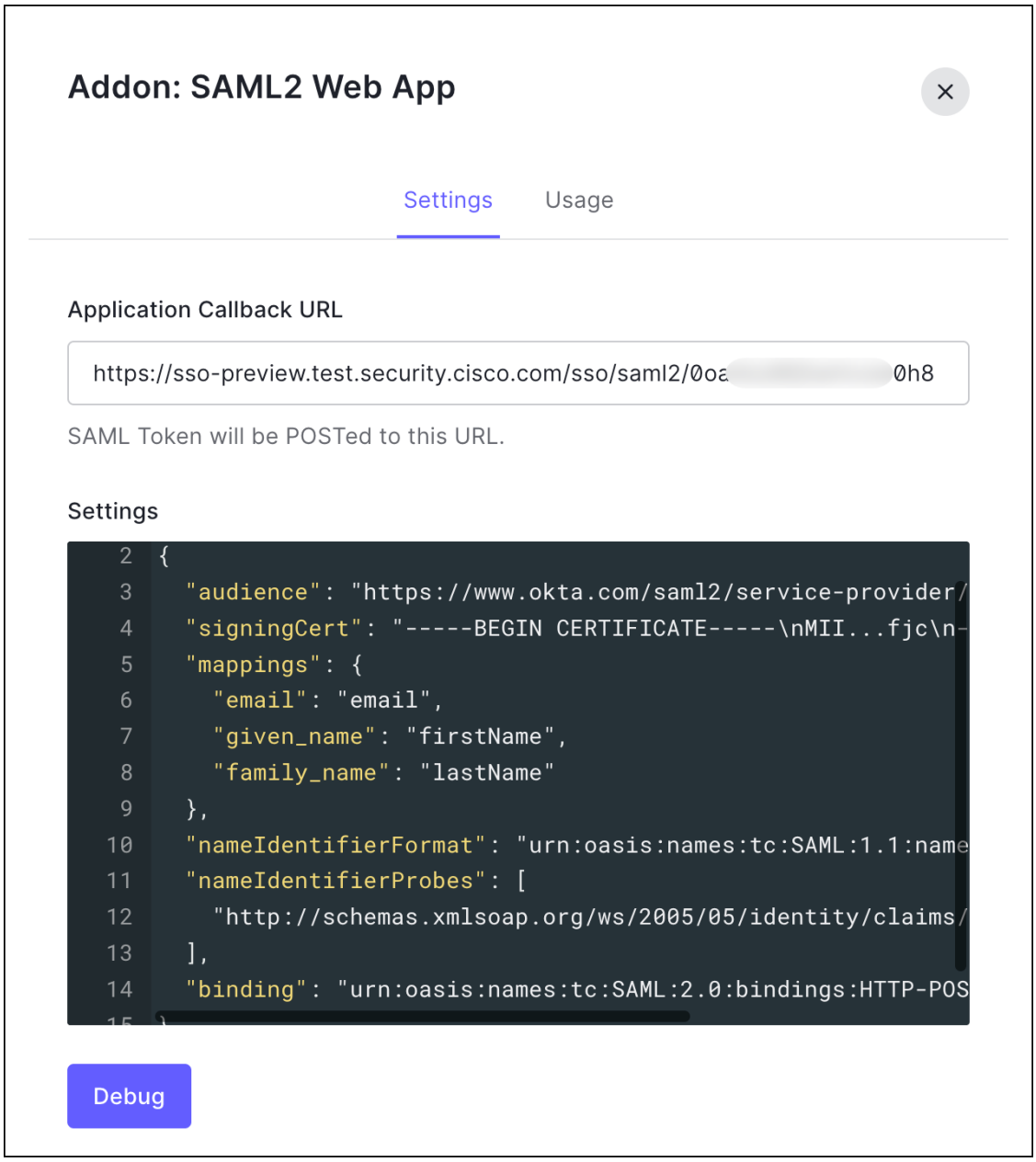
g) On the **Usage** tab, download the Auth0 **Identity Provider Certificate** and the **Identity Provider Metadata** file.

h) Click the **Settings** tab.

i) In the **Application Callback URL** field enter the value of the **Single Sign-On Service URL** you copied from the enterprise settings wizard.

j) In the **Settings** field enter the following JSON object, replacing the value for `audience` with the value of **Entity ID (Audience URI)** provided , and `signingCert` with the contents of the signing certificate provided by Security Cloud Control converted to a single line of text.

```
{
  "audience": "...",
  "signingCert": "-----BEGIN CERTIFICATE-----\n...-----END CERTIFICATE-----\n",
  "mappings": {
    "email": "email",
    "given_name": "firstName",
    "family_name": "lastName"
  },
  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
  "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  ],
  "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
}
```



k) Click **Enable** at the bottom of the **Addon** dialog to enable the application.

Step 3 Return to Security Cloud Control and click **Next**. You should be on Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

a) Select the **XML file upload** option.

b) Upload the **Identity Provider Metadata** file provided by Auth0.

What to do next

Next, follow the instructions in Step 4: Test your SAML integration, on page 29 and Step 5: Activate the integration, on page 29 to test and activate your integration.

Integrating Azure AD with Security Cloud Sign On

This guide explains how to integrate an Azure AD with Security Cloud Control.

Before you begin

Before you begin, read the Identity provider integration guide, on page 23 to understand the overall process. These instructions supplement that guide with details specific to Azure AD SAML integrations, specifically Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26 and Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

Step 1 Sign in to Security Cloud Control with the enterprise you want to integrate with Azure AD.

a) Create a new identity provider and decide whether or not to opt out of Duo MFA, as explained in Step 1: Initial setup, on page 25.
b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26, download the **Public certificate**, and copy the values for **Entity ID** and **Single Sign-On Service URL** for use in the next steps.

Step 2 In a new browser tab, sign in to https://portal.azure.com as an administrator. Keep the Security Cloud Control tab open as you'll return to it shortly.

If your account gives you access to more than one tenant, select your account in the upper right corner. Set your portal session to the Azure AD tenant that you want.

a) Click **Azure Active Directory**.
b) Click **Enterprise Applications** in the left sidebar.
c) Click **+ New Application** and search for **`Azure AD SAML Toolkit`**.
d) Click **Azure AD SAML Toolkit**.
e) In the **Name** field, enter **`Security Cloud Sign On`** or other value, then click **Create**.
f) On the Overview page, click **Single Sign On** under **Manage** in the left sidebar.
g) Select **SAML** for the select single sign on method.
h) In the **Basic SAML Configuration** panel, click **Edit**, and do the following:

- Under **Identifier (Entity ID)**, click **Add Identifier** and enter the **Entity ID** URL provided by Security Cloud Control.
- Under **Reply URL (Assertion Consumer Service URL)**, click **Add reply URL** and enter the **Single Sign-On Service URL** from Security Cloud Control.
- In the **Sign on URL** field, enter **`https://sign-on.security.cisco.com/`**.
- Click **Save** and close the **Basic SAML Configuration** panel.

i) In the **Attributes & Claims** panel click **Edit**.

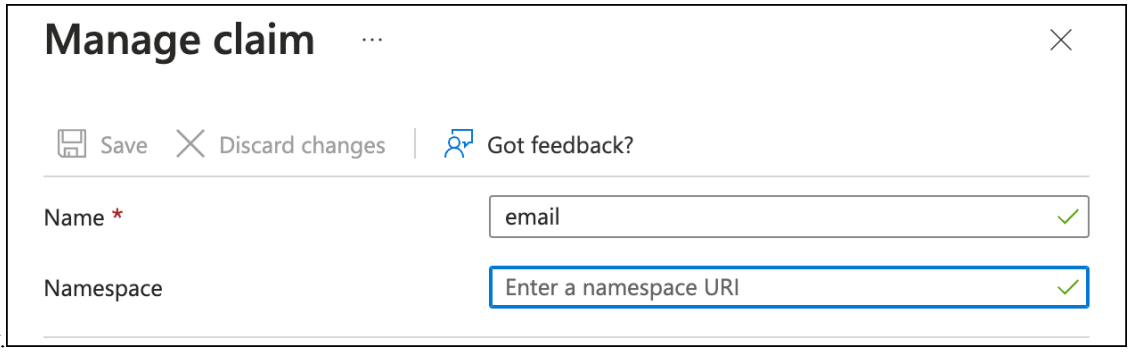
- Under **Required claim**, click the **Unique User Identifier (Name ID)** claim to edit it.

- Set the **Source** attribute field to `user.userprincipalname`. This assumes that the value of **user.userprincipalname** represents a valid email address. If not, set **Source** to **user.primaryauthoritativeemail**.

j) Under **Additional Claims** panel, click **Edit** and create the following mappings between Azure AD user properties and SAML attributes.

Name	Namespace	Source attribute
`email`	No value	`user.userprincipalname`
`firstName`	No value	`user.givenname`
`lastName`	No value	`user.surname`

Be sure to clear the **Namespace** field for each claim, as shown below.



k) In the **SAML Certificates** panel, click **Download** for the **Certificate (Base64)** certificate.

l) In the **Set up Single Sign-On with SAML** section, copy the value of **Login URL** and **Azure AD Identifier** for use later in this procedure.

Step 3 Return to Security Cloud Control and click **Next**. You should be on Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

a) Select the **Manual Configuration** option.

b) In the **Single Sign-on Service URL (Assertion Consumer Service URL)** field, enter the **Login URL** value provided by Azure.

c) In the **Entity ID (Audience URI)** field, enter the **Azure AD Identifier** value provided by Azure AD.

d) Upload the **Signing Certificate** provided by Azure.

Step 4 Click **Next** in **Security Cloud Control**.

What to do next

Test and activate your integration by following Step 4: Test your SAML integration, on page 29 and Step 5: Activate the integration, on page 29.

Integrating Duo with Security Cloud Sign On

This guide explains how to integrate an Duo SAML application with Security Cloud Sign On.

Before you begin

Before you begin, read the Identity provider integration guide, on page 23 to understand the overall process. These instructions supplement that guide with details specific to Duo SAML integrations, specifically Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26 and Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

Step 1 Sign in to Security Cloud Control with the enterprise you want to integrate with Duo.

a) Create a new identity provider and decide whether or not to opt out of Duo MFA, as explained in Step 1: Initial setup, on page 25.

b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26, download the **Public certificate**, and copy the values for **Entity ID** and **Single Sign-On Service URL** for use in the next steps.

Step 2 Sign in to your Duo organization as an administrator in a new browser tab. Keep the Security Cloud Control tab open, as you'll return to it shortly.

a) From the left menu, click **Applications** and then click **Protect an Application**.

b) Search for **Generic SAML Service Provider**.

c) Click **Protect** next to the **Generic Service Provider** application with a **Protection Type** of **2FA with SSO hosted by Duo**. The configuration page for the Generic SAML Service Provider opens.

d) In the **Metadata** section:

e) Copy the value of **Entity ID** and save for later use.

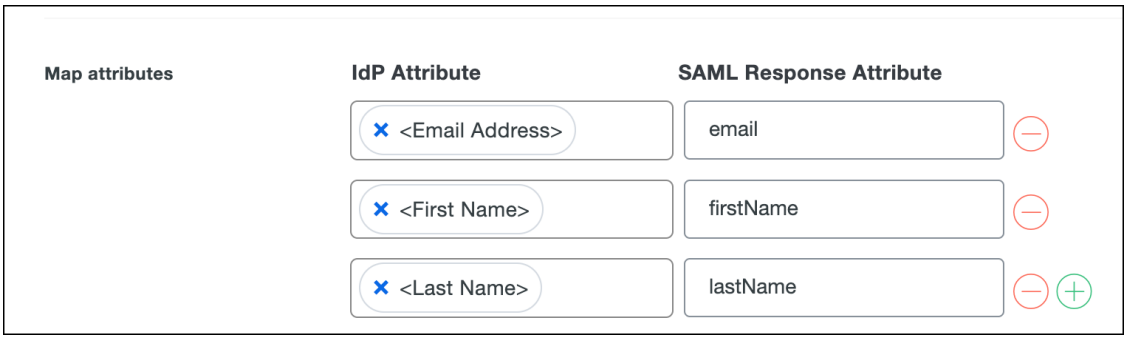
f) Copy the value of **Single Sign-On URL** and save for later use.

g) Click **Download certificate** in the Downloads section for later use.

h) In the **SAML Response** section, do the following:

- For **NameID format** select either **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** or **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
- For **NameID attribute** select **<Email Address>**.
- In the **Map Attributes** section, enter the following mappings of Duo IdP user attributes to SAML response attributes:

IdP Attribute	SAML Response Attribute
<Email Address>	**email**
<First Name>	**firstName**
<Last Name>	**lastName**



i) In the **Settings** section enter **Security Cloud Sign On** or other value in the **Name** field.

Step 3 Return to Security Cloud Control and click **Next**. You should be on Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

a) Select the **Manual Configuration** option.
b) In the **Single Sign-on Service URL (Assertion Consumer Service URL)** field, enter the **Single Sign-On URL** value provided by Duo.
c) In the **Entity ID (Audience URI)** field, enter the **Entity ID** value provided by Duo.
d) Upload the **Signing Certificate** you downloaded from Duo.

What to do next

Next, follow the instructions in Step 4: Test your SAML integration, on page 29 and Step 5: Activate the integration, on page 29 to test and activate your integration.

Integrating Google Identity with Security Cloud Sign On

This guide explains how to integrate a Google Identity SAML application with Security Cloud Sign On.

Before you begin

Before you begin, read the Identity provider integration guide, on page 23 to understand the overall process. These instructions supplement that guide with details specific to Google Identity integrations, specifically Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26 and Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

Step 1 Sign in to Security Cloud Control with the enterprise you want to integrate with Google.

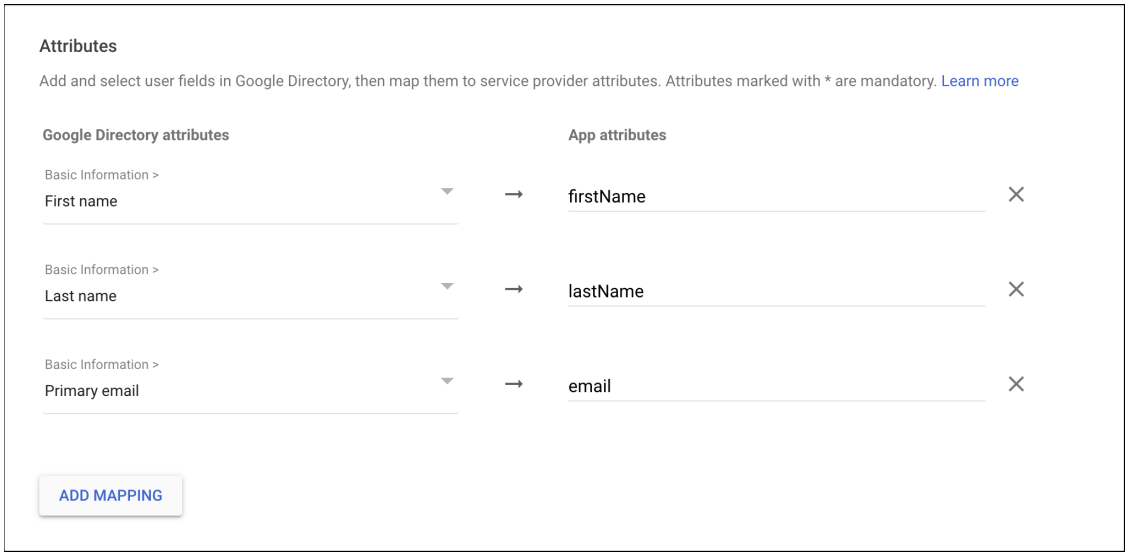
a) Create a new identity provider and decide whether or not to opt out of Duo MFA, as explained in Step 1: Initial setup, on page 25.
b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26, download the **Public certificate**, and copy the values for **Entity ID** and **Single Sign-On Service URL** for use in the next steps.

Step 2 In a new browser tab, sign in to your Google Admin console using an account with super administrator privileges. Keep the Security Cloud Control tab open.

a) In the Admin console, go to Menu > **Apps** > **Web and mobile apps**.
b) Click **Add App** > **Add custom SAML app**.
c) On the **App Details** page:
   - Enter `Secure Cloud Sign On` or other value for the application name.
   - Optionally, upload an icon to associate with the application.
d) Click **Continue** to go to the **Google Identity Provider** details page.
e) Click **Download Metadata** to download the Google SAML metadata file for later use.
f) Click **Continue** to go to the **Service provider details** page.
g) In the **ACS URL** field, enter the **Single Sign-On Service URL** provided by Security Cloud Control.
h) In the **Entity ID** field, enter the **Entity ID**URL provided by Security Cloud Control.

i) Check the **Signed Response** option.
j) For **Name ID Format**, select either `UNSPECIFIED` or `EMAIL`.
k) For **Name ID**, select **Basic Information > Primary Email**.
l) Click **Continue** to advance to the **Attribute mapping** page.
m) Add the following mappings of Google Directory attributes to App attribute:

Google Directory attributes	App attributes
First name	firstName
Last name	lastName
Primary email	email



n) Click **Finish**.

Step 3 Return to Security Cloud Control and click **Next**. You should be on Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

a) Select the **XML file upload** option.
b) Upload the SAML metadata file you previously downloaded from Google.
c) Click Next to advance to the **Testing** page.

What to do next

Next, follow the instructions in Step 4: Test your SAML integration, on page 29 and Step 5: Activate the integration, on page 29 to test and activate your integration.

Integrating Okta with Security Cloud Sign On

This guide explains how to integrate an Okta SAML application in Security Cloud Control.

Before you begin

Before you begin, read the Identity provider integration guide, on page 23 to understand the overall process. These instructions supplement that guide with details specific to Okta SAML integrations, specifically Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26 and Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

Step 1 Sign in to Security Cloud Control with the enterprise you want to integrate with Okta.

a) Create a new identity provider and decide whether or not to opt out of Duo MFA, as explained in Step 1: Initial setup, on page 25.

b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26, download the **Public certificate**, and copy the values for **Entity ID** and **Single Sign-On Service URL** for use in the next steps.

Step 2 In a new browser tab, sign in to your Okta organization as an administrator. Keep the Security Cloud Control tab open as you'll return to it shortly.

a) From the **Applications** menu, choose **Applications**.

b) Click **Create App Integration**.

c) Select **SAML 2.0** and click **Next**.

d) On the **General Settings** tab, enter a name for your integration (**Security Cloud Sign On**, for example) and optionally upload a logo.

e) Click **Next** to go to the **Configure SAML** screen.

f) In the **Single sign-on URL** field, enter the **Single Sign-On Service URL** provided by Security Cloud Control.

g) In the **Audience URI** field, enter the **Entity ID** provided by Security Cloud Control.

h) For **Name ID format**, select either **Unspecified** or **EmailAddress**.

i) For **Application username**, select **Okta username**.

j) In the **Attribute Statements (optional)** section, add the following mappings of names SAML attributes to Okta user profile values:

Name (in SAML assertion)	Value (in Okta profile)
email	user.email
firstName	user.firstName
lastName	user.lastName

k) Click **Show Advanced Settings**.

l) Click **Next**.

m) For **Signature Certificate**, click **Browse files...** and upload the public signing certificate you previously downloaded from Security Cloud Control.

Note The response and assertion must be signed with the RSA-SHA256 algorithm.

n) Under **Sign On > Settings > Sign on method**, click **Show details**.

o) Click **Next** and provide feedback to Okta, then click **Finish**.

p) Copy the values of **Sign on URL** and **Issuer** and download the **Signing Certificate** to provide to Security Cloud Control next.

Step 3 Return to Security Cloud Control and click **Next**. You should be on Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

a) Select the **Manual Configuration** option.
b) In the **Single Sign-on Service URL (Assertion Consumer Service URL)** field, enter the **Sign on URL** value provided by Okta.
c) In the **Entity ID (Audience URI)** field, enter the **Issuer** value provided by Okta
d) Upload the **Signing Certificate** provided by Okta.

What to do next

Next, follow the instructions in Step 4: Test your SAML integration, on page 29 and Step 5: Activate the integration, on page 29 to test and activate your integration.

Integrating Ping Identity with Security Cloud Sign On

This guide explains how to integrate a Ping SAML application with Security Cloud Sign On.

Before you begin

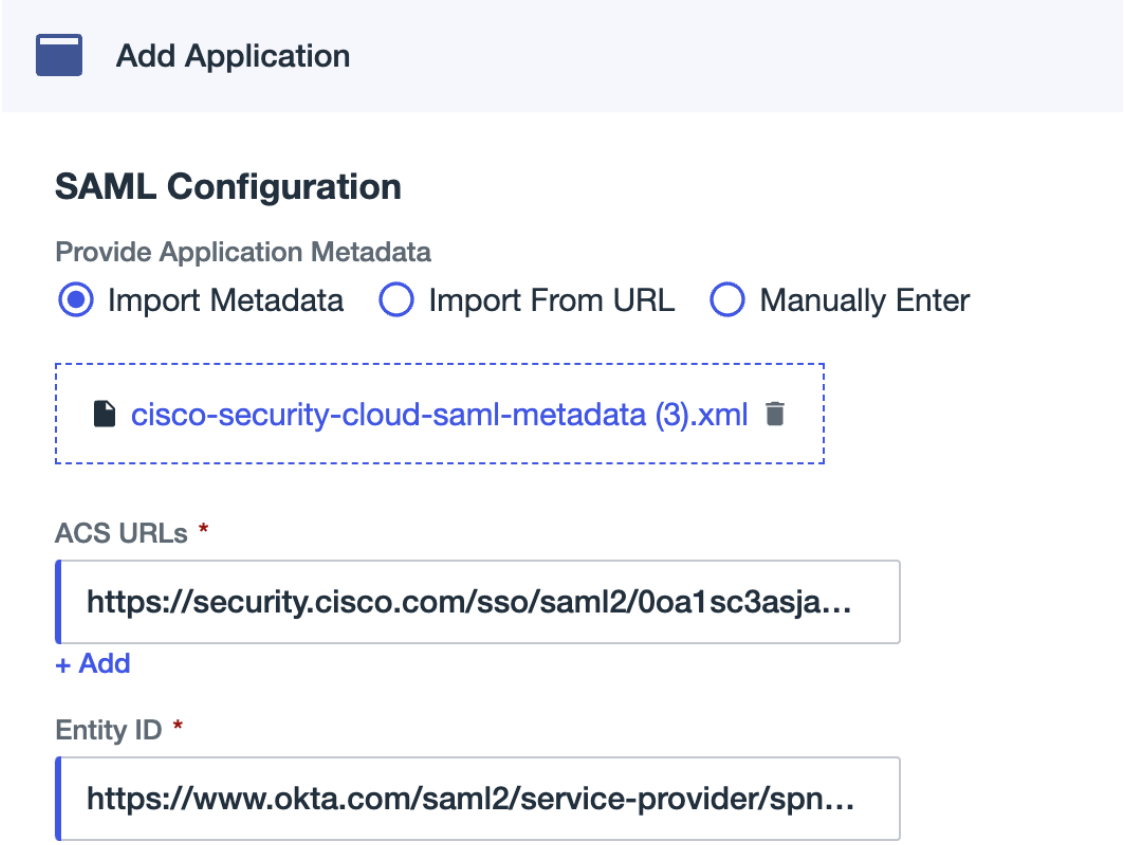
Before you begin, read the Identity provider integration guide, on page 23 to understand the overall process. These instructions supplement that guide with details specific to Ping integrations, specifically Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26 and Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

Step 1 Sign in to Security Cloud Control with the enterprise you want to integrate with Ping.

a) Create a new identity provider and decide whether or not to opt out of Duo MFA, as explained in Step 1: Initial setup, on page 25.
b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26, download the **Security Cloud Sign On SAML metadata** file for later use.

Step 2 In a new browser tab, sign in to your Ping admin console. Keep the Security Cloud Control browser tab open.

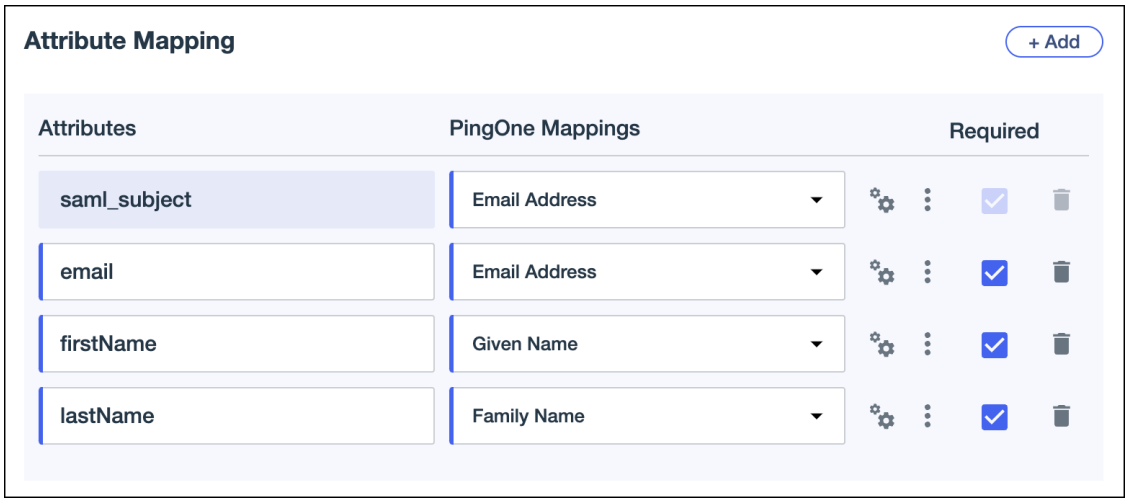
a) Go to **Connections** > **Applications**.
b) Click the + button to open the **Add Application** dialog.
c) In the **Application Name** field enter `Secure Cloud Sign On`, or other name.
d) Optionally, add a description and upload an icon.
e) For **Application Type** select **SAML application** and then click **Configure**.
f) In the **SAML Configuration** dialog select the option to **Import Metadata** and click **Select a file**.
g) Locate **Security Cloud Sign On SAML metadata** file you downloaded from Security Cloud Control.



h) Click **Save**.
i) Click the **Configuration** tab.
j) Click **Download Metadata** to download a SAML metadata file to provide to Security Cloud Control.
k) Click the **Attribute Mappings** tab.
l) Click the Edit (pencil) icon.
m) For the required **saml_subject** attribute, select **Email Address**.
n) Click **+Add** and add the following mappings of SAML attributes to PingOne user identity attributes, enabling the **Required** option for each mapping.

Attributes	PingOne Mappings
firstName	Email Address
lastName	Given Name
email	Family Name

The Attribute Mapping panel should look like the following.



o) Click **Save** to save your mappings.

Step 3 Return to Security Cloud Control and click **Next**. You should be on Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28.

a) Select the **XML file upload** option.
b) Upload the SAML metadata file you previously downloaded from Ping.
c) Click Next to advance to the **Testing** page.

What to do next

Next, follow the instructions in Step 4: Test your SAML integration, on page 29 and Step 5: Activate the integration, on page 29 to test and activate your integration.