



Cisco Security Provisioning and Administration User Guide

First Published: 2023-04-16

Last Modified: 2024-10-30

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Overview 1

Cisco Security Provisioning and Administration overview 1

Signing in to Security Provisioning and Administration 3

CHAPTER 2

Managing enterprises 5

Create an enterprise 5

Rename an enterprise 6

Switch enterprises 6

Support access to an enterprise 7

Enable support access 7

Disable support access 8

CHAPTER 3

Managing products and subscriptions 9

Overview 9

Claim a subscription 10

Activate a product instance 11

Attach an externally managed product instance 14

Deactivate a product instance 15

CHAPTER 4

Managing users 17

List users 17

Invite a user 17

Edit a user 18

Reset user password 18

Remove a user account 19

CHAPTER 5	Managing domains	21
	Claim and verify a domain	21

CHAPTER 6	Identity provider integration guide	23
	Prerequisites	23
	SAML response requirements	24
	Step 1: Initial setup	25
	Step 2: Provide Security Cloud SAML metadata to your identity provider	26
	Step 3: Provide SAML metadata from your IdP to Security Cloud	28
	Step 4: Test your SAML integration	29
	Step 5: Activate the integration	30
	Troubleshooting SAML errors	31

CHAPTER 7	Identity service provider instructions	33
	Integrating Auth0 with Security Cloud Sign On	33
	Integrating Microsoft Entra ID with Security Cloud Sign On	36
	Integrating Duo with Security Cloud Sign On	38
	Integrating Google Identity with Security Cloud Sign On	39
	Integrating Okta with Security Cloud Sign On	41
	Integrating Ping Identity with Security Cloud Sign On	43



CHAPTER 1

Overview

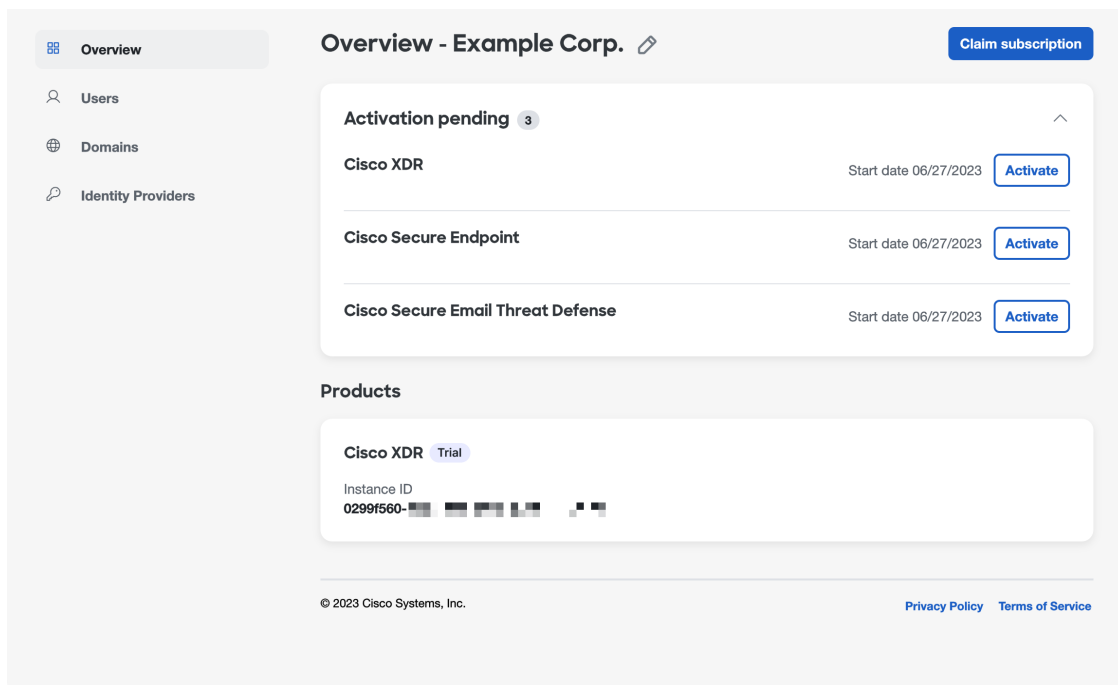
- [Cisco Security Provisioning and Administration overview, on page 1](#)
- [Signing in to Security Provisioning and Administration, on page 3](#)

Cisco Security Provisioning and Administration overview

Security Provisioning and Administration is a web application that provides centralized management of Cisco Secure product instances, user identity, and user access management across Cisco Security Cloud. Security Provisioning and Administration 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.

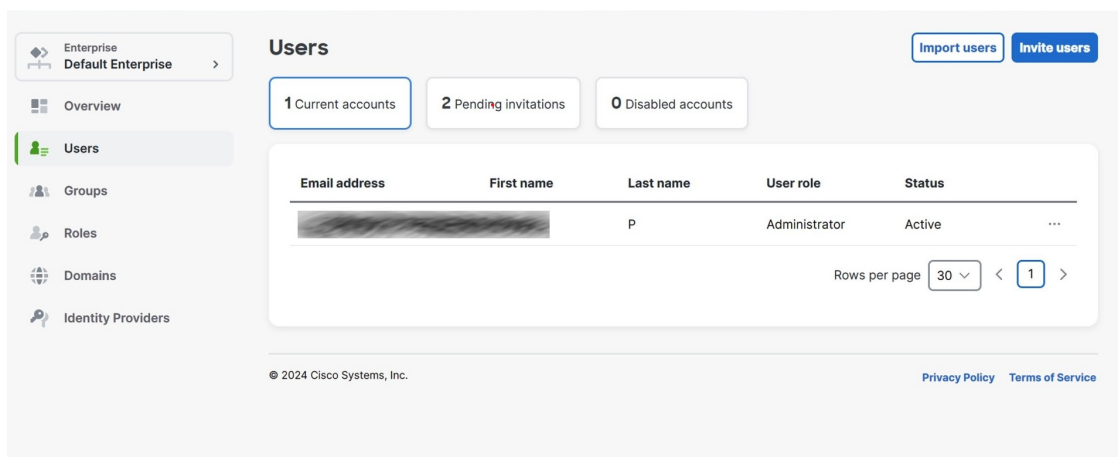
Overview tab

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 **Userstab** 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.

The screenshot shows the 'Add New Domain' interface. On the left is a sidebar with a navigation menu. The main content area is titled 'Add New Domain' and contains a form with two steps: '1 Domain' and '2 Verification'. The 'Domain' step is currently active, displaying a text input field for 'Domain name' containing the text 'cloud@control.com'. Below the input field are 'Cancel' and 'Next' buttons.

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 23](#) for details.

Signing in to Security Provisioning and Administration

To sign in to Security Provisioning and Administration 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 Provisioning and Administration 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 is always the default account when you log in. If you have multiple enterprises associated with your account, the latest one you used is selected after you sign in.

Procedure

Step 1 Open [Security Provisioning and Administration](#).

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

If this is the first time signing in to Security Provisioning and Administration 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, on page 5](#)
- [Rename an enterprise, on page 6](#)
- [Switch enterprises, on page 6](#)
- [Support access to an enterprise, on page 7](#)

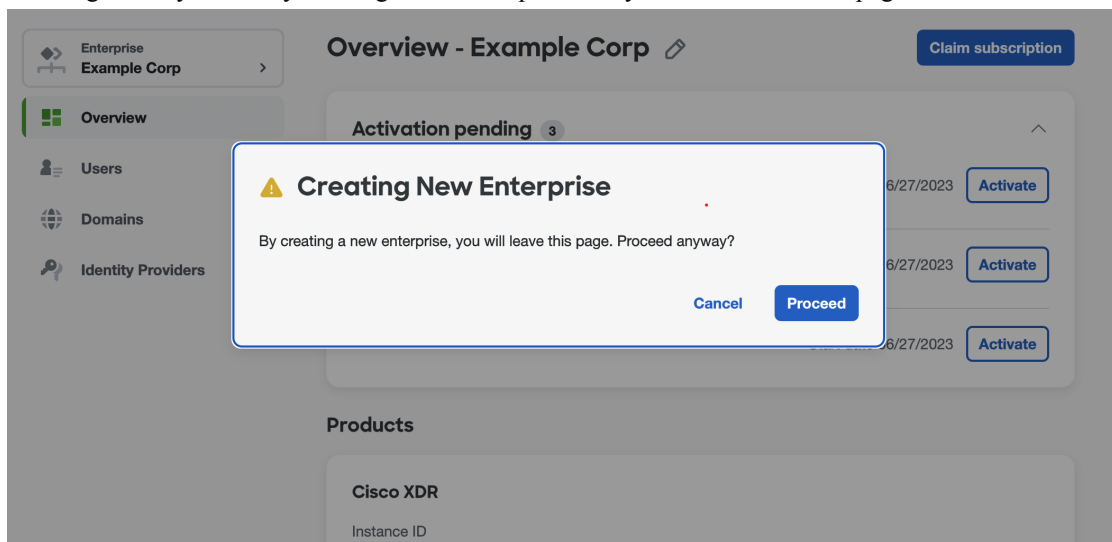
Create an enterprise

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

Procedure

Step 1 In Security Provisioning and Administration, 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 Provisioning and Administration 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.

Procedure

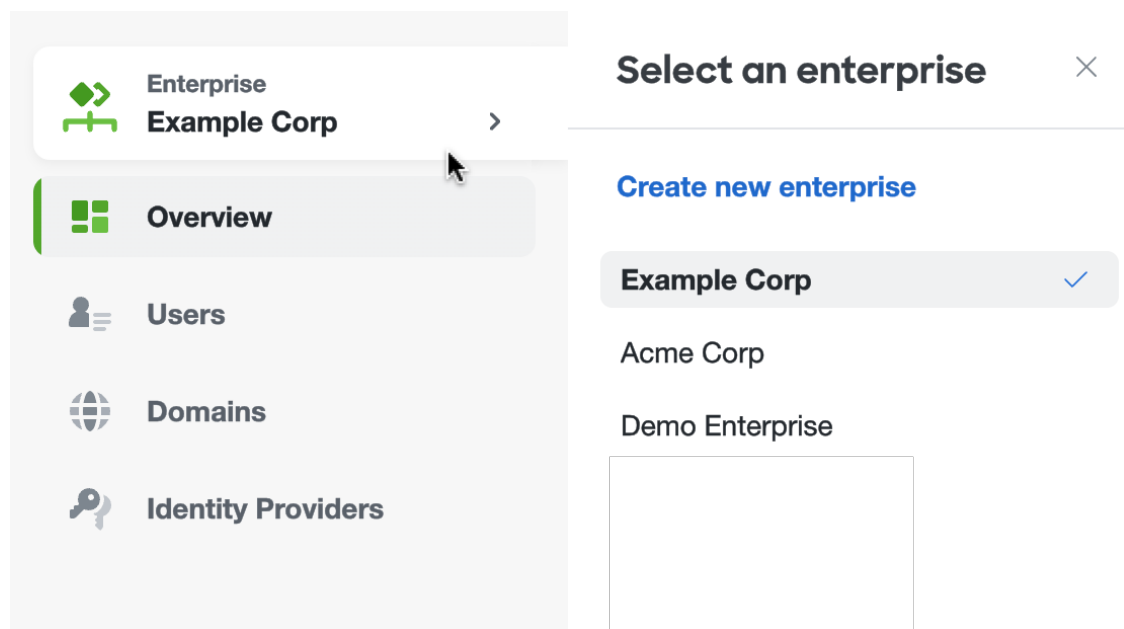
Step 1 [Switch enterprises](#) that you want to rename from the **Enterprise** menu.

Step 2 Click the pencil icon  next to the enterprise name at the top of Security Provisioning and Administration page.

Step 3 In the **Edit Enterprise Name** dialog box, enter the new enterprise name and click **Save**.

Switch enterprises

All operations you perform in Security Provisioning and Administration, such as creating domains or inviting users, are applied to the currently selected enterprise. The **Enterprise** menu at the top of Security Provisioning and Administration 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.



Procedure

- Step 1** Sign in to Security Provisioning and Administration.
- Step 2** Hover over the **Enterprise** menu and select the desired enterprise from the fly-out menu. Security Provisioning and Administration reloads with the selected enterprise.

Support access to an enterprise

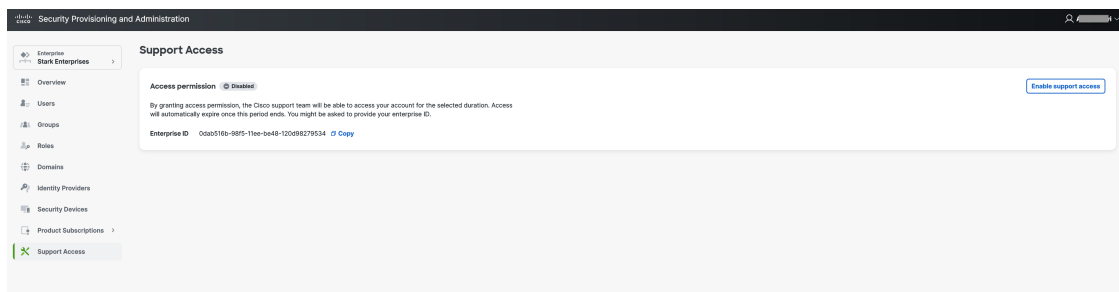
To help the support team diagnose and debug issues more effectively, you can grant the team temporary access to your enterprise. This access is automatically revoked after a specified duration, and can also be disabled anytime after it is no longer needed.

Enable support access

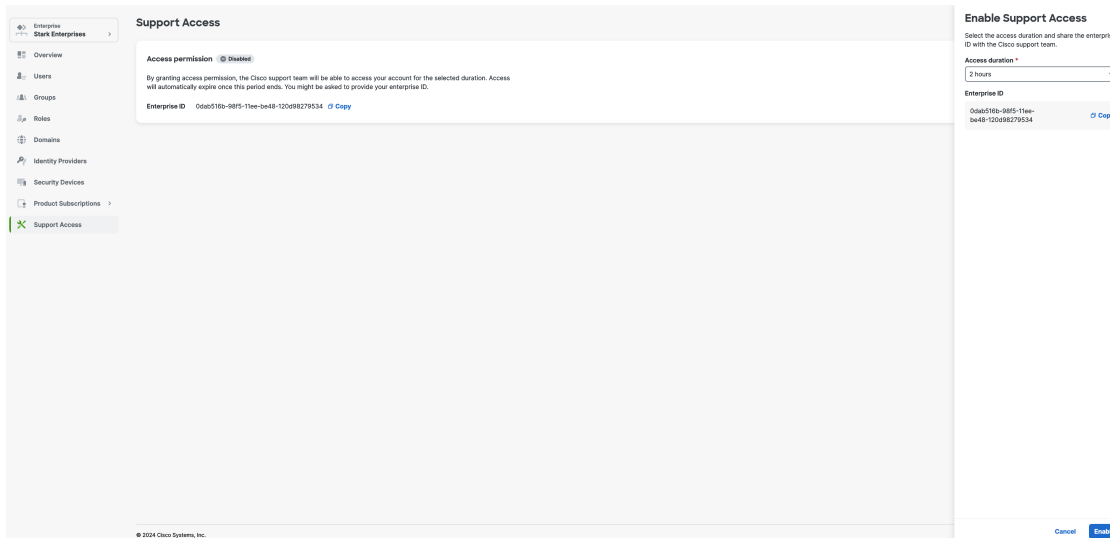
You can grant the support team access to your enterprise for better diagnosis and debugging.

Procedure

- Step 1** In the Security Provisioning and Administration window, hover over the Enterprise menu and from the slide-in pane, select the enterprise . Security Provisioning and Administration reloads with the selected enterprise.
- Step 2** Click **Support Access** in the left navigation pane.



- Step 3** In the **Support Access** page, click **Enable support access**.
- Step 4** In the **Enable Support Access** slide-in pane, select the duration from the **Access duration** drop-down list. This is the duration for which the Cisco Support team has access to your enterprise account.
- Step 5** Under **Enterprise ID**, click the clipboard icon to copy the number.
- Paste the enterprise ID into a safe text tool.
 - When asked, provide the enterprise ID to the Cisco Support team.



Step 6 Click **Enable**.

Access to your enterprise is enabled and the support team can access your enterprise for the duration that you have configured. At the end of this period, access is automatically revoked.

Disable support access

You can revoke the access that is provided to the support team, when needed. Also, after the access duration expires, the access is automatically revoked.

Procedure

- Step 1** In the Security Provisioning and Administration window, click **Support Access** in the left navigation pane.
- Step 2** Click **Disable Support Access**.
- Step 3** In the **Disable Support Access** dialog window, click **Disable access**.

External access to your enterprise is disabled.



CHAPTER 3

Managing products and subscriptions

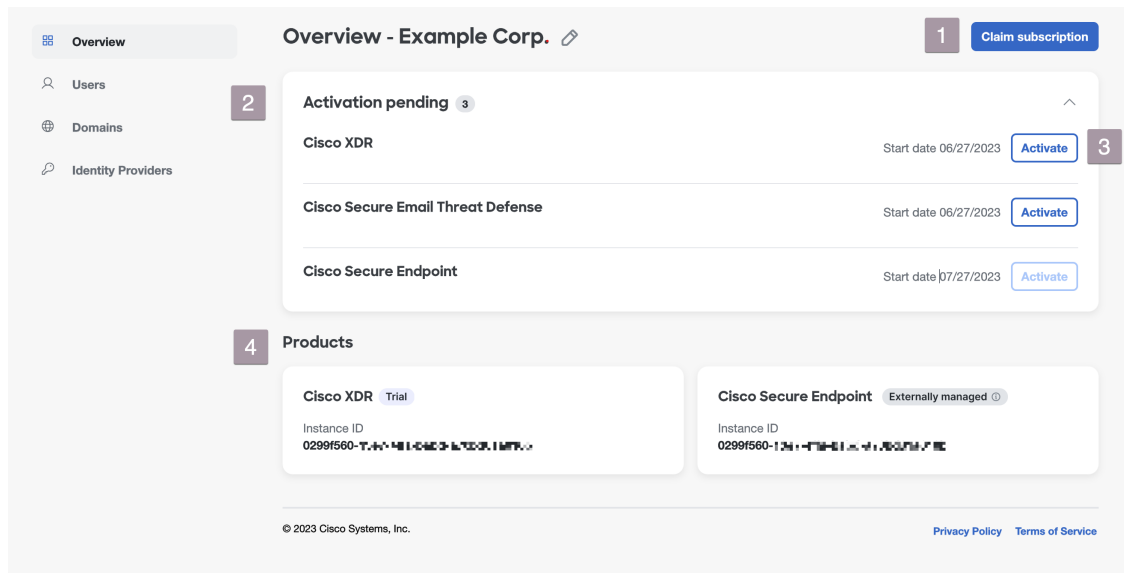
- [Overview](#), on page 9
- [Claim a subscription](#), on page 10
- [Activate a product instance](#), on page 11
- [Attach an externally managed product instance](#), on page 14
- [Deactivate a product instance](#), on page 15

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 Provisioning and Administration administrator who will manage the subscription. A Security Provisioning and Administration 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.

Procedure

-
- Step 1** Sign in to [Security Provisioning and Administration](#).
 - 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**.

Claim Subscription

- 1 **Subscription claim code**
- 2 Review subscription

Subscription claim code

To begin, enter your claim code below and click **Next**. For detailed instructions please read our [documentation](#) .

Subscription claim code *

<
Cancel
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.

Procedure

- Step 1** Sign in to [Security Provisioning and Administration](#).
- 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.

Overview - Example Corp.

Activation pending 3

Cisco XDR

Cisco Secure Endpoint

Cisco Secure Email Threat Defense

Products

Cisco XDR

Instance ID
0299f560-13e7-...

© 2023 Cisco Systems, Inc.

Cisco XDR

Fields with asterisk(*) are required.

Subscription ID 2bdbd2a2-13c1-1f...

Region *
North America

Initial administrator *
Select admin

Cancel Activate

- 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.

Overview - Example Corp.

Activation pending 3

Cisco XDR

Cisco Secure Endpoint

Cisco Secure Email Threat Defense

Products

Cisco XDR

Instance ID
0299f560-13e7-4412-8202-315152015201

© 2023 Cisco Systems, Inc.

Cisco XDR ×

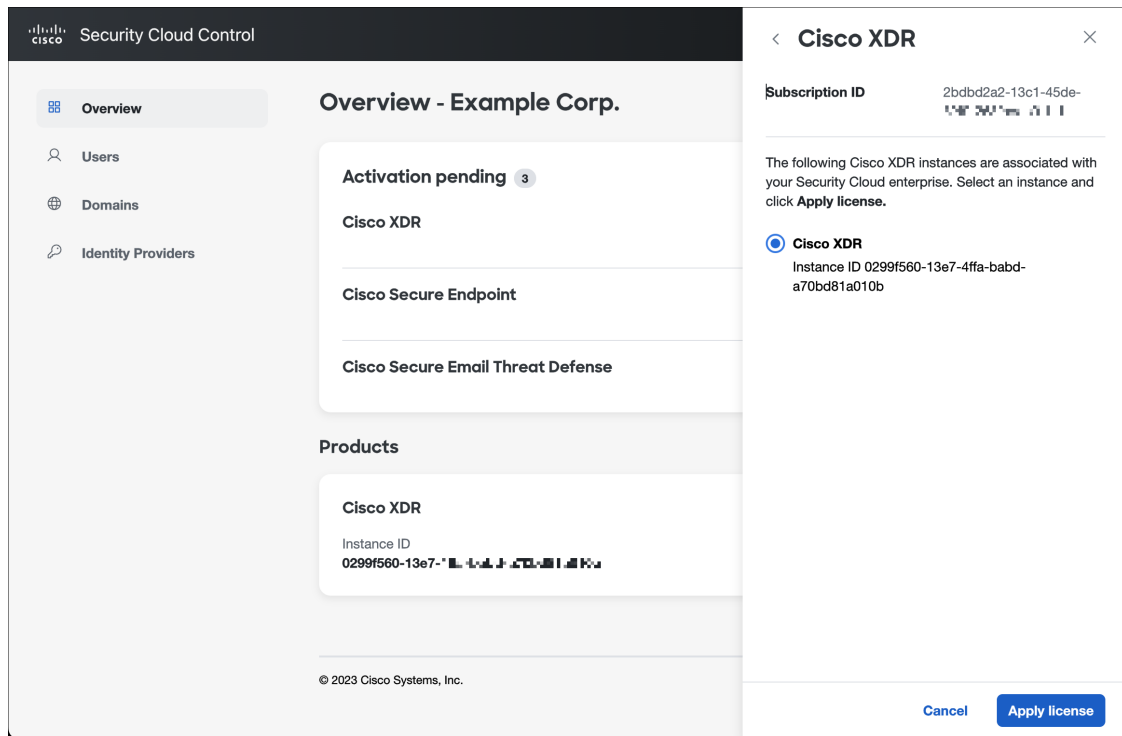
Subscription ID 2bdbd2a2-13c1-45de-
2d71-0c-3152015201

You can apply this license to a new instance of Cisco XDR or to an existing instance. Select an option to proceed.

Activate a new instance

Apply 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**.



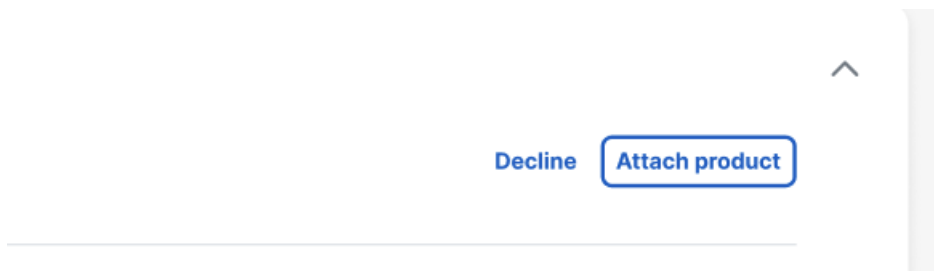
The product is added to the **Products** table.

Attach an externally managed product instance

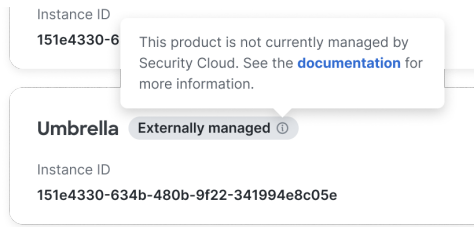
If you have a Cisco product instance that is managed outside of Security Provisioning and Administration, you can optionally attach it to a Security Cloud enterprise. Cisco initiates this process by sending an email to a list of Security Provisioning and Administration admins with an invitation to attach 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.

Procedure

- Step 1** Sign in to [Security Provisioning and Administration](#).
- 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.



Note You can't deactivate an unlicensed or externally managed product instance. If you have incorrectly associated a product instance with your enterprise, contact the [Cisco support team](#).

Procedure

- Step 1** Sign in to [Security Provisioning and Administration](#).
- 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**.

The screenshot shows a user interface for managing products and subscriptions. At the top, there is a header 'Overview - Example Corp' with an edit icon and a 'Claim subscription' button. Below this, there is a section titled 'Activation pending' with a notification icon '2'. This section contains two rows of product instances:

Product Name	Start date	Action
Cisco Secure Email Threat Defense	02/13/2024	Activate
Cisco Secure Endpoint	02/13/2024	Activate

Below the 'Activation pending' section is a 'Products' section. It contains a card for 'Cisco XDR' with an instance ID of '81201e08-f08d-49b8-925a-4c096426c994'. A 'Deactivate' button with a red circle icon is visible next to the instance ID.

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](#).

The Deactivate option doesn't remove an unlicensed or externally managed product instance.



CHAPTER 4

Managing users

- [List users, on page 17](#)
- [Invite a user, on page 17](#)
- [Edit a user, on page 18](#)
- [Reset user password, on page 18](#)
- [Remove a user account, on page 19](#)

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](#).

Email address	First name	Last name	Status
user1@example.com	User1	Lastname1	Active
user2@example.com	User2	Lastname2	Active
user3@example.com	User3	Lastname3	Active
user4@example.com	User4	Lastname4	Active

Invite a user

Enterprise administrators can invite a user to join an enterprise.

Procedure

- 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.


Procedure

- 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.

Procedure

- 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.

Procedure

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 Provisioning and Administration. 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 that you create can be deleted after Security Provisioning and Administration has verified the domain.
- You can currently verify a single domain with Security Provisioning and Administration. If you must verify multiple domains, open a case with [Cisco Technical Assistance Center](#) (Cisco TAC).

Before you begin

To complete this task, you should 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, a + **Add Domain** button is shown instead.

Procedure

Step 1 Select the **Domains** tab.

Step 2 Click + **Add domain**.

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

The **Verification** page shows the name under **Record Name**, and the value under **Value** of a text record that you must create on your domain registrar.

The screenshot shows a web interface titled "Add New Domain". On the left, there is a sidebar with two steps: "Domain" (marked with a checkmark) and "Verification" (marked with a "2"). The main content area is titled "Verification" and contains the following instructions and fields:

- Instruction: "Upload the TXT record to the domain's DNS server. Then click **Verify**."
- Field: "Record name" with the value "_cisco-sxso-verification.example.com" and a copy icon.
- Field: "Type" with the value "TXT".
- Field: "Value" with the value "7b017856-4f7a-4bca-8dea-8eb3eb5f5b0f" and a copy icon.
- Buttons: "Cancel", "Back", and "Verify".

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 Provisioning and Administration.

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

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

If the verification is 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 that are generated by Security Provisioning and Administration.

What to do next

After 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:

- [Integrating Auth0 with Security Cloud Sign On](#)
- [Integrating Microsoft Entra ID with Security Cloud Sign On](#)
- [Integrating Duo with Security Cloud Sign On](#)
- [Integrating Google Identity with Security Cloud Sign On](#)
- [Integrating Okta with Security Cloud Sign On](#)
- [Integrating Ping Identity with Security Cloud Sign On](#)



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, on page 23](#)
- [SAML response requirements, on page 24](#)
- [Step 1: Initial setup, on page 25](#)
- [Step 2: Provide Security Cloud SAML metadata to your identity provider, on page 26](#)
- [Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28](#)
- [Step 4: Test your SAML integration, on page 29](#)
- [Step 5: Activate the integration, on page 30](#)
- [Troubleshooting SAML errors, on page 31](#)

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
<code>firstName</code>	User's first or given name.
<code>lastName</code>	User's lastname or surname.
<code>email</code>	User's email. This must match the value of the <code><NameID></code> 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="id9538389495975029849262425" 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/saml2/0a1rs8y79aewevg80h8"/>
        </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.

Procedure

Step 1 Sign in to [Security Provisioning and Administration](#).

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 Provisioning and Administration. 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.

Procedure

- 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.

Edit identity provider

✓ Set up

2 Configure

3 SAML metadata

4 Test

5 Activate

Configure

Depending on your provider, use the following methods to set up your IDP.

Security Cloud Sign On SAML metadata

cisco-security-cloud-saml-metadata.xml

Or

Public certificate

cisco-security-cloud.pem

Entity ID (Audience URI)

https://www.okta.com/saml2/service-provider/sphuivrxhuglxyarzje

Single Sign-On Service URL (Assertion Consumer Service URL)

https://sso-preview.test.security.cisco.com/sso/saml2/0oa1rs8y79aeweVg80h8

Cancel **Back** **Next**

- 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 Provisioning and Administration and click **Next**.

What to do next

Next you'll provide Security Provisioning and Administration with the corresponding metadata for your identity provider's SAML application.

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

After you've [Step 2: Provide Security Cloud SAML metadata to your identity provider](#) with SAML metadata from Security Provisioning and Administration, the next step is to provide the corresponding metadata from your SAML application to Security Provisioning and Administration. See [Identity service provider instructions, on page 33](#) for steps specific to several commercially available identity service providers.

Before you begin

To complete this step, you 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 provides data, you can either upload a metadata XML file that contains all this information, or manually enter (copy and paste) the individual SAML URIs and upload the signing certificate. See [Identity service provider instructions, on page 33](#) for steps specific to several commercially available identity service providers.

Procedure

Step 1 Open the browser tab with Security Provisioning and Administration.

Step 2 In the **SAML metadata** page, 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.

SAML metadata

Select a method for providing your SAML 2.0 IdP metadata.

XML file upload Manual configuration

Upload your SAML signing certificate

Click or drag a file to this area to upload

File must be in XML format

Cancel Back Next

Step 3 Click **Next**.

What to do next

Next you'll [Step 4: Test your SAML integration](#) by initiating an SSO from Security Provisioning and Administration to your identity provider.

Step 4: Test your SAML integration

After 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 [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 Provisioning and Administration. For instance, if you used `admin@example.com` to create the integration then test with another SSO user (`jsmith@example.com`, for instance).

Procedure

Step 1 In Security Provisioning and Administration, from the **Edit identity provider** > **Test** page, copy the sign in URL to your clipboard and open it in a private (incognito) browser window.

Test

1. Configure your IdP with the public certificate and SAML metadata you copied and downloaded from Cisco.
2. Test your IdP integration by opening this URL in a private(Incognito) window.

https://s[redacted]cisco.com/sso/saml2/0oa1sc3asjayJkNM0[redacted]
3. Once you sign in and land in the Security Cloud Control portal, the configuration test is successful.

[Cancel](#)

Step 2 Sign in to your identity provider.

The test is successful if, after authenticating with your identity provider, you are signed in to the [Application Portal](#). If you receive an error, see [Troubleshooting SAML errors, on page 31](#).

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.

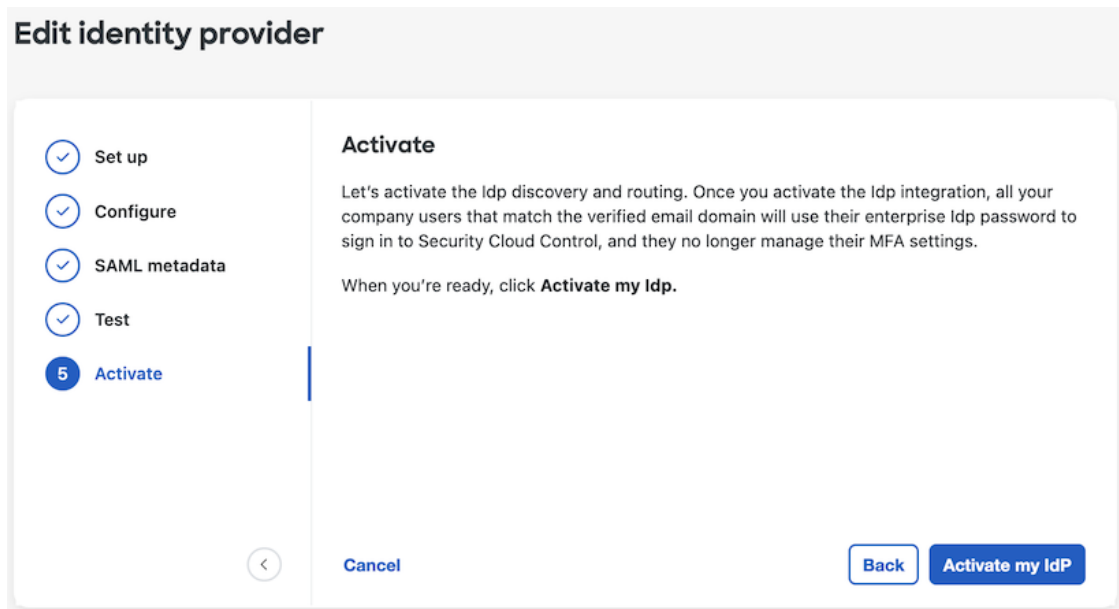


Caution Be sure to [Step 4: Test your SAML integration](#) before activating it.

Activating an integration has the following effects:

Procedure

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, on page 33](#)
- [Integrating Microsoft Entra ID with Security Cloud Sign On, on page 36](#)
- [Integrating Duo with Security Cloud Sign On, on page 38](#)
- [Integrating Google Identity with Security Cloud Sign On, on page 39](#)
- [Integrating Okta with Security Cloud Sign On, on page 41](#)
- [Integrating Ping Identity with Security Cloud Sign On, on page 43](#)

Integrating Auth0 with Security Cloud Sign On

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

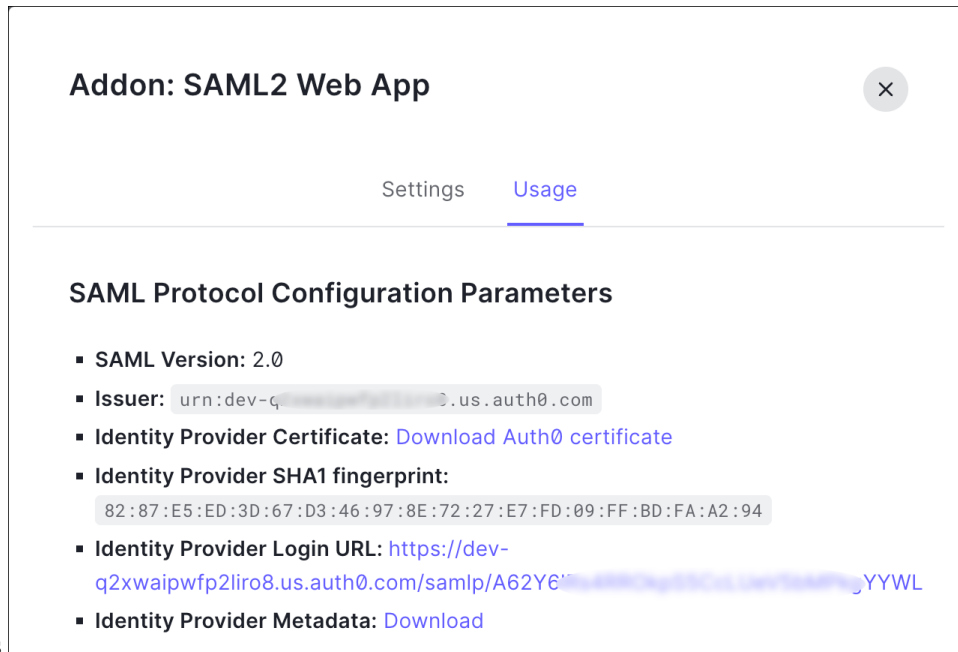
Before you begin

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](#).

Procedure

- Step 1** Sign in to [Security Provisioning and Administration](#) with the enterprise that you want to integrate with Auth0.
- a) Create a new identity provider and decide whether 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 Provisioning and Administration browser tab open because 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 the 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) In 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** that 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 Provisioning and Administration 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"
}
```

Addon: SAML2 Web App ✕

[Settings](#) [Usage](#)

Application Callback URL

SAML Token will be POSTed to this URL.

Settings

```
2 {
3   "audience": "https://www.okta.com/saml2/service-provider/
4   "signingCert": "-----BEGIN CERTIFICATE-----\nMII...fjc\n-
5   "mappings": {
6     "email": "email",
7     "given_name": "firstName",
8     "family_name": "lastName"
9   },
10  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:name
11  "nameIdentifierProbes": [
12    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
13  ],
14  "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POS
15 }
```

[Debug](#)

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

Step 3

Return to Security Provisioning and Administration and click **Next**. You should be on [Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28](#).

- Select the **XML file upload** option.
- 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 30](#) to test and activate your integration.

Integrating Microsoft Entra ID with Security Cloud Sign On

This guide explains how to integrate a Microsoft Entra ID with Security Provisioning and Administration.

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 Microsoft Entra ID 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](#).

Procedure

-
- Step 1** Sign in to [Security Provisioning and Administration](#) with the enterprise you want to integrate with Microsoft Entra ID.
- Create a new identity provider and decide whether to opt out of Duo MFA, as explained in [Step 1: Initial setup, on page 25](#).
 - 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 Provisioning and Administration 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 Microsoft Entra ID tenant that you want.
- Click **Azure Active Directory**.
 - Click **Enterprise Applications** in the left sidebar.
 - Click **+ New Application** and search for **Microsoft Entra SAML Toolkit**.
 - Click **Microsoft Entra SAML Toolkit**.
 - In the **Name** field, enter **Security Cloud Sign On** or other value, then click **Create**.
 - On the **Overview** page, click **Single Sign On** under **Manage** in the left sidebar.
 - Select **SAML** for the select single sign on method.
 - 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 Provisioning and Administration.
 - Under **Reply URL (Assertion Consumer Service URL)**, click **Add reply URL** and enter the **Single Sign-On Service URL** from Security Provisioning and Administration.
 - In the **Sign on URL** field, enter `https://sign-on.security.cisco.com/`.
 - Click **Save** and close the **Basic SAML Configuration** panel.
 - 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 Microsoft Entra ID user properties and SAML attributes.

Name	Namespace	Source attribute
email	No value	<code>user.userprincipalname</code>
firstName	No value	<code>user.givenname</code>
lastName	No value	<code>user.surname</code>

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 **Microsoft Entra Identifier** for use later in this procedure.

Step 3

Return to Security Provisioning and Administration and click **Next**. You should be on [Step 3: Provide SAML metadata from your IdP to Security Cloud, on page 28](#).

- Select the **Manual Configuration** option.
- In the **Single Sign-on Service URL (Assertion Consumer Service URL)** field, enter the **Login URL** value that is provided by Azure.
- In the **Entity ID (Audience URI)** field, enter the **Microsoft Entra Identifier** value that is provided by Microsoft Entra ID.
- Upload the **Signing Certificate** provided by Azure.

Note The signing certificate file that is provided by Azure has a **.cer** extension. However, for Security Provisioning and Administration to accept the certificate, change the file extension to **.cert** and then upload it.

Step 4

Click **Next** in Security Provisioning and Administration.

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 30](#).

Integrating Duo with Security Cloud Sign On

This guide explains how to integrate a 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](#).

Procedure

-
- Step 1** Sign in to [Security Provisioning and Administration](#) with the enterprise that you want to integrate with Duo.
- Create a new identity provider and decide whether to opt out of Duo MFA, as explained in [Step 1: Initial setup, on page 25](#).
 - 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 Provisioning and Administration tab open, because you'll return to it shortly.
- From the left navigation menu, click **Applications** and then click **Protect an Application**.
 - Search for **Generic SAML Service Provider**.
 - Click **Protect** next to the **Generic Service Provider** application and choose **2FA with SSO hosted by Duo** for **Protection Type**.

The configuration page for the Generic SAML Service Provider opens.

- In the **Metadata** section:
- Copy the value of **Entity ID** and save for later use.
- Copy the value of **Single Sign-On URL** and save for later use.
- Click **Download certificate** in the Downloads section for later use.
- 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

IdP Attribute	SAML Response Attribute
<First Name>	firstName
<Last Name>	lastName

Map attributes	IdP Attribute	SAML Response Attribute
	<input type="text" value="x <Email Address>"/>	<input type="text" value="email"/> <input type="button" value="−"/>
	<input type="text" value="x <First Name>"/>	<input type="text" value="firstName"/> <input type="button" value="−"/>
	<input type="text" value="x <Last Name>"/>	<input type="text" value="lastName"/> <input type="button" value="−"/> <input style="color: green;" type="button" value="+"/>

i) Under **Settings**, for the **Name** field, enter **Security Cloud Sign On** or other value.

Step 3

Return to Security Provisioning and Administration and click **Next**. You should be on [Step 3: Provide SAML metadata from your IdP to Security Cloud](#), on page 28.

- Select the **Manual Configuration** option.
- In the **Single Sign-on Service URL (Assertion Consumer Service URL)** field, enter the **Single Sign-On URL** value that is provided by Duo.
- In the **Entity ID (Audience URI)** field, enter the **Entity ID** value provided by Duo.
- Upload the **Signing Certificate** that 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 30 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.


Procedure

Step 1 Sign in to [Security Provisioning and Administration](#) with the enterprise you want to integrate with Google.

- a) Create a new identity provider and decide whether 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 Provisioning and Administration 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 Provisioning and Administration.
- h) In the **Entity ID** field, enter the **Entity ID URL** provided by Security Provisioning and Administration.
- 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

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

Google Directory attributes		App attributes	
Basic Information > First name	→	firstName	×
Basic Information > Last name	→	lastName	×
Basic Information > Primary email	→	email	×

[ADD MAPPING](#)

n) Click **Finish**.

Step 3 Return to Security Provisioning and Administration 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 30](#) 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 Provisioning and Administration.

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](#).

Procedure

- Step 1** Sign in to [Security Provisioning and Administration](#) with the enterprise that you want to integrate with Okta.
- a) Create a new identity provider and decide whether 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 Provisioning and Administration 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) In 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** page.
- f) In the **Single sign-on URL** field, enter the **Single Sign-On Service URL** provided by Security Provisioning and Administration.
- g) In the **Audience URI** field, enter the **Entity ID** provided by Security Provisioning and Administration.
- 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 in 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 that you previously downloaded from Security Provisioning and Administration.

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 Provisioning and Administration next.

Step 3

Return to Security Provisioning and Administration 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 30](#) 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](#).

Procedure

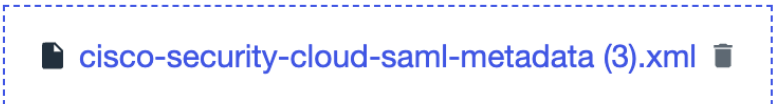
-
- Step 1** Sign in to [Security Provisioning and Administration](#) with the enterprise that you want to integrate with Ping.
- Create a new identity provider and decide whether to opt out of Duo MFA, as explained in [Step 1: Initial setup, on page 25](#).
 - On [Step 2: Provide Security Cloud SAML 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 Provisioning and Administration browser tab open.
- Go to **Connections > Applications**.
 - Click the + button to open the **Add Application** dialog.
 - In the **Application Name** field enter **Secure Cloud Sign On**, or other name.
 - Optionally, add a description and upload an icon.
 - For **Application Type**, select **SAML application** and then click **Configure**.
 - In the **SAML Configuration** dialog select the option to **Import Metadata** and click **Select a file**.
 - Locate **Security Cloud Sign On SAML metadata** file you downloaded from Security Provisioning and Administration.

Add Application

SAML Configuration

Provide Application Metadata

- Import Metadata
- Import From URL
- Manually Enter



ACS URLs *

+ Add

Entity ID *

- h) Click **Save**.
- i) Click the **Configuration** tab.
- j) Click **Download Metadata** to download a SAML metadata file to provide to Security Provisioning and Administration.
- 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.

Attributes	PingOne Mappings	Required
saml_subject	Email Address	<input checked="" type="checkbox"/>
email	Email Address	<input checked="" type="checkbox"/>
firstName	Given Name	<input checked="" type="checkbox"/>
lastName	Family Name	<input checked="" type="checkbox"/>

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

Step 3

Return to Security Provisioning and Administration 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 30](#) to test and activate your integration.

