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

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.

b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, 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**.

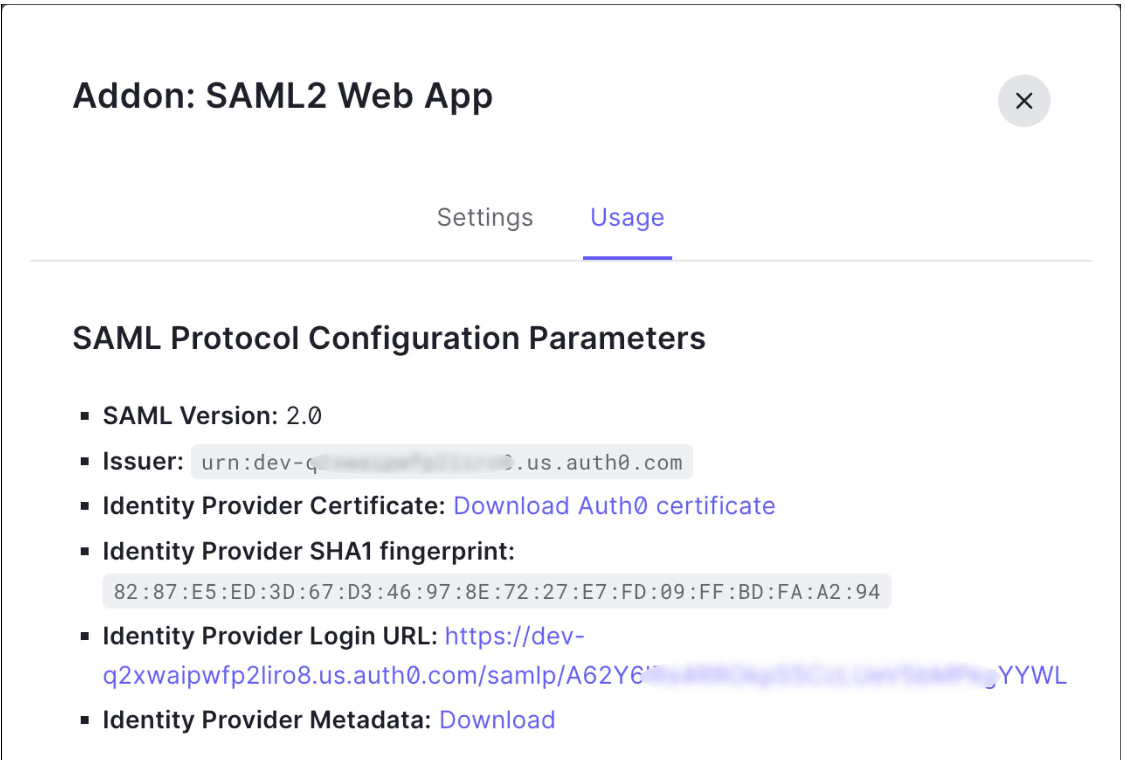
c) In the **Name** field enter **`Secure Cloud Sign On`**, or other name.

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.



Addon: SAML2 Web App

SAML Protocol Configuration Parameters

- **SAML Version:** 2.0
- **Issuer:** `urn:dev-q[redacted].us.auth0.com`
- **Identity Provider Certificate:** Download Auth0 certificate
- **Identity Provider SHA1 fingerprint:** `82:87:E5:ED:3D:67:D3:46:97:8E:72:27:E7:FD:09:FF:BD:FA:A2:94`
- **Identity Provider Login URL:** https://dev-q2xwaipwfp2liro8.us.auth0.com/samlp/A62Y6[redacted]YYWL
- **Identity Provider Metadata:** Download

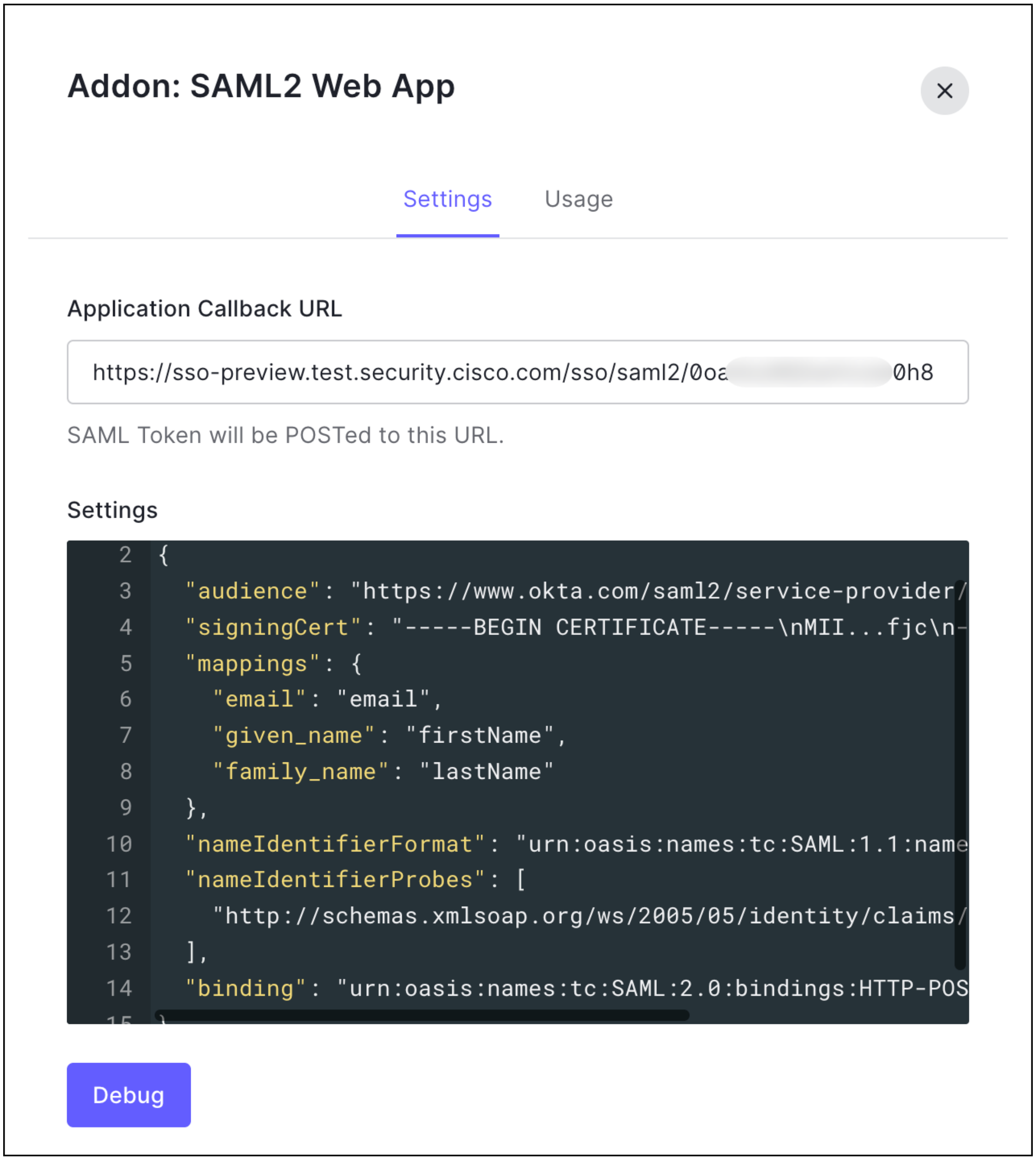
g) On the **Usage** tab, download the Auth0 **Identity Provider Certificate** and the **Identity Provider Metadata** file.

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"
}
```



Application Callback URL

https://sso-preview.test.security.cisco.com/sso/saml2/0oa[redacted]0h8

SAML Token will be POSTed to this URL.

Settings

```
{
  "audience": "https://www.okta.com/saml2/service-provider/
  "signingCert": "-----BEGIN CERTIFICATE-----\nMII...fjc\n-
  "mappings": {
    "email": "email",
    "given_name": "firstName",
    "family_name": "lastName"
  },
  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:name
  "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
  ],
  "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POS
}
```

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.

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 and Step 5: Activate the integration 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 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 and Step 3: Provide SAML metadata from your IdP to Security Cloud.

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.

b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, 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.

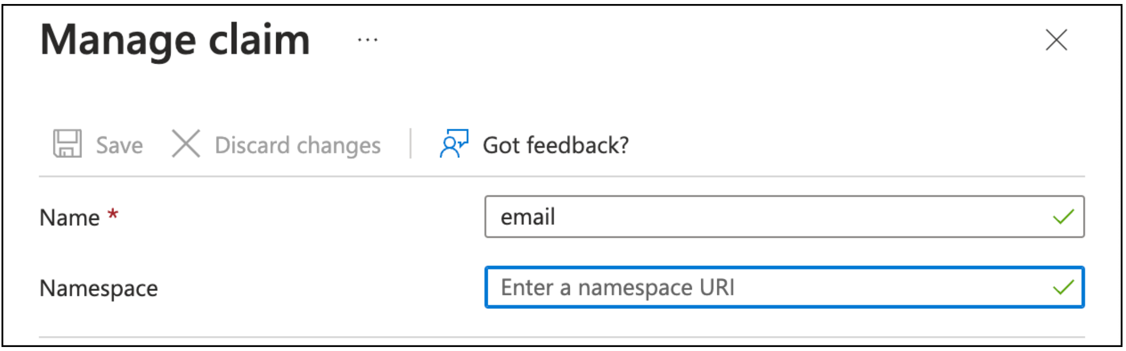
i) In the **Attributes & Claims** panel click **Edit**.

- 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.



Name * email

Namespace Enter a namespace URI

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.

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 and Step 5: Activate the integration.

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

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.

b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, 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.

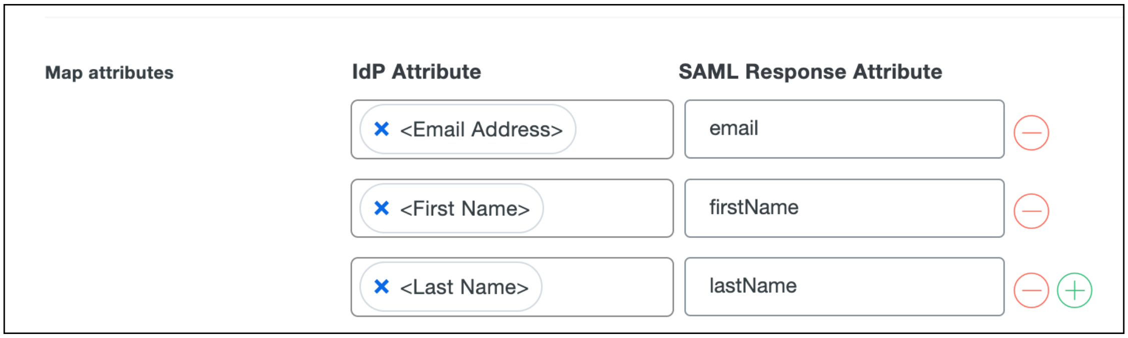
f) Copy the value of **Single Sign-On URL** and save for later use.

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



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.

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 and Step 5: Activate the integration 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 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 and Step 3: Provide SAML metadata from your IdP to Security Cloud.

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.

b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, 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.

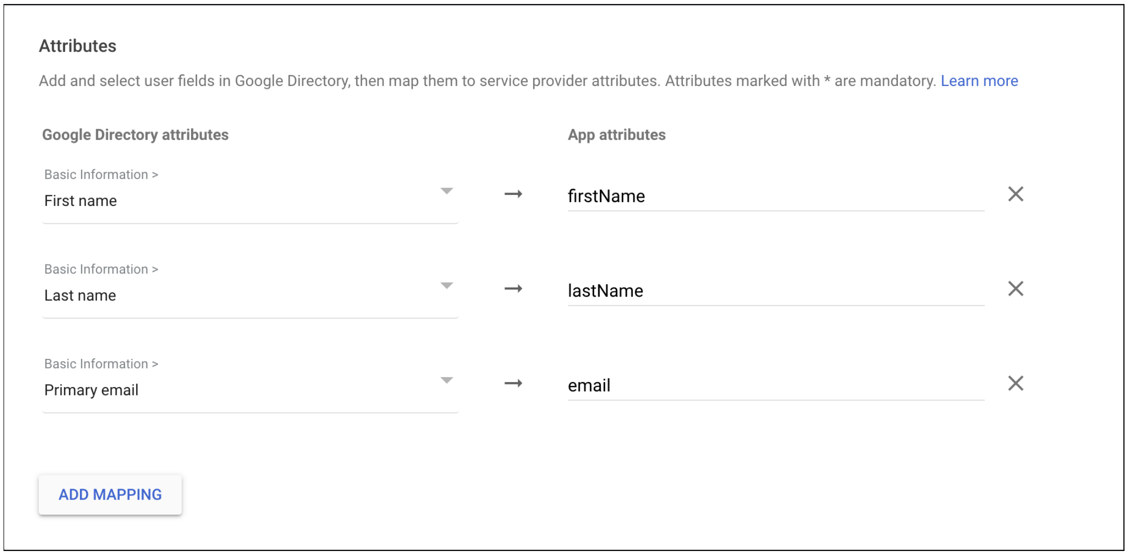
j) For **Name ID Format**, select either `UNSPECIFIED` or `EMAIL`.

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



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

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.

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 and Step 5: Activate the integration 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 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 and Step 3: Provide SAML metadata from your IdP to Security Cloud.

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.

b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, 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.

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 and Step 5: Activate the integration 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

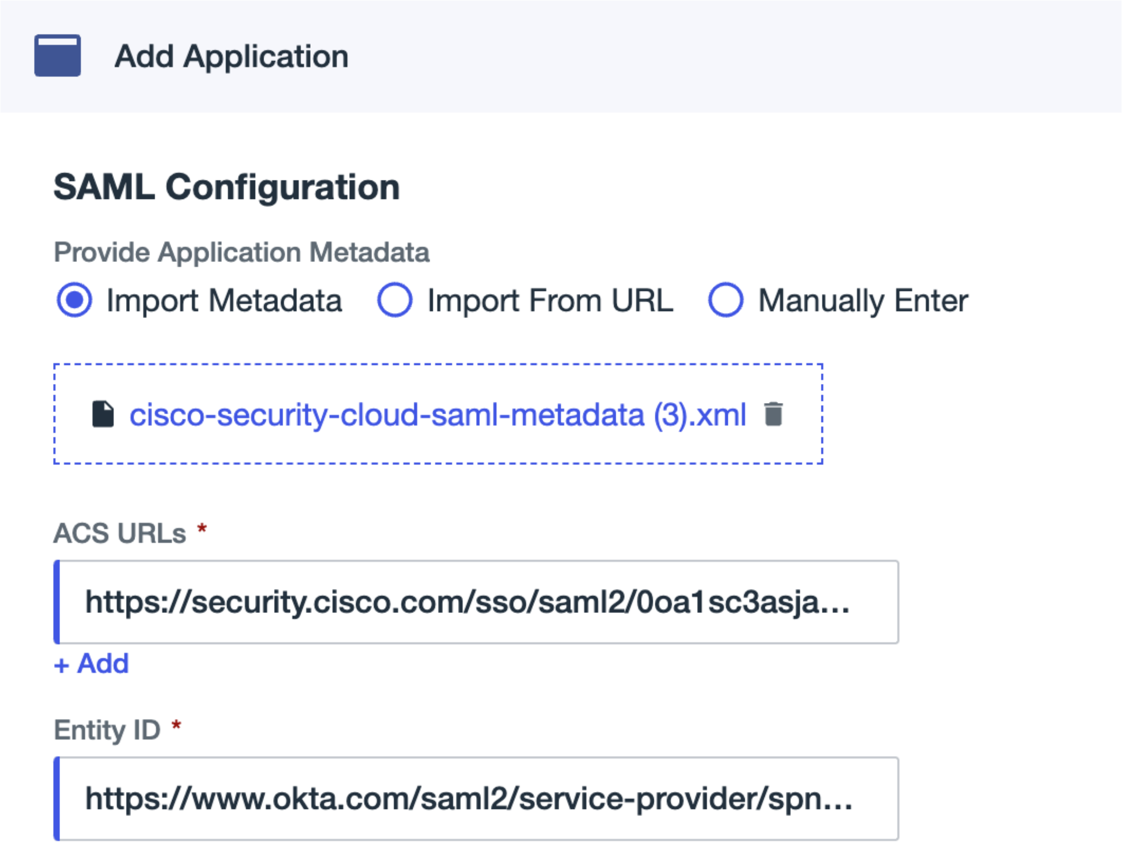
Before you begin, read the Identity provider integration guide to understand the overall process. These instructions supplement that guide with details specific to Ping integrations, specifically Step 2: Provide Security Cloud SAML metadata to your identity provider and Step 3: Provide SAML metadata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

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.
b) On Step 2: Provide Security Cloud SAML metadata to your identity provider, 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.



Add Application

SAML Configuration

Provide Application Metadata

● Import Metadata ○ Import From URL ○ Manually Enter

cisco-security-cloud-saml-metadata (3).xml

ACS URLs *

https://security.cisco.com/sso/saml2/0oa1sc3asja...

+ Add

Entity ID *

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

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.

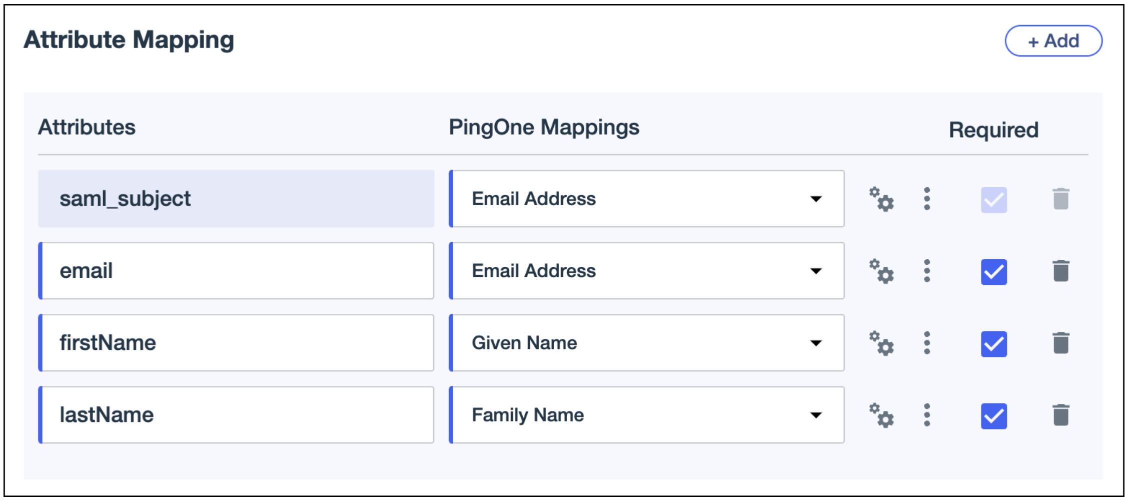
l) Click the Edit (pencil) icon.

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.



Attribute Mapping

Attributes	PingOne Mappings	Required
saml_subject	Email Address	☑
email	Email Address	☑
firstName	Given Name	☑
lastName	Family Name	☑

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.

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 and Step 5: Activate the integration to test and activate your integration.