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 1
- Integrating Microsoft Entra ID with Security Cloud Sign On, on page 4
- Integrating Duo with Security Cloud Sign On, on page 6
- Integrating Google Identity with Security Cloud Sign On, on page 7
- Integrating Okta with Security Cloud Sign On, on page 9
- Integrating Ping Identity with Security Cloud Sign On, on page 10

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.

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.

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 Provisioning and Administration browser tab open because you'll return to it shortly.

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

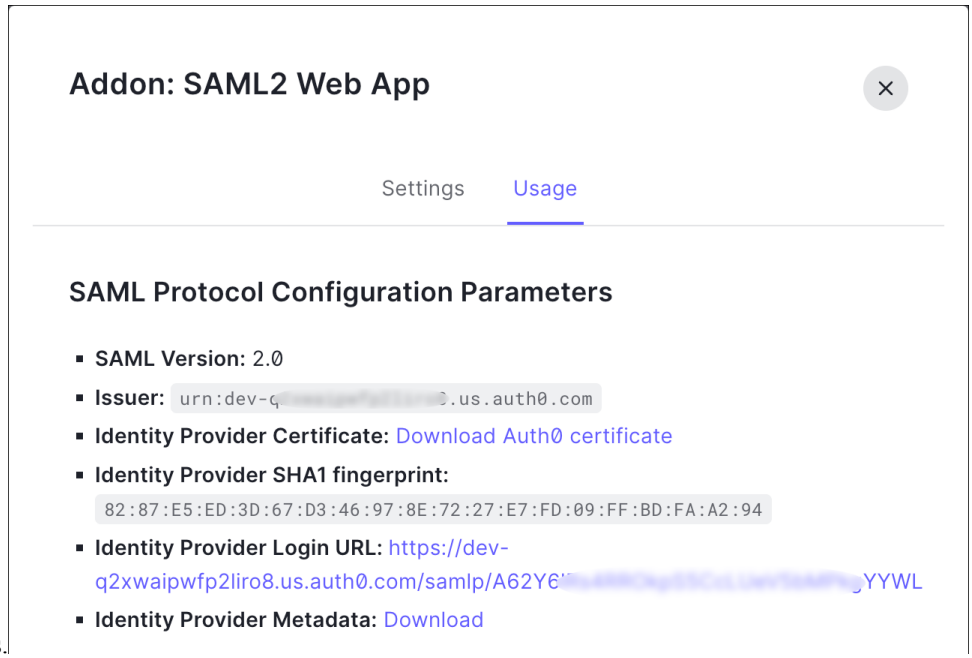
b) Click **Create Application**.

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.

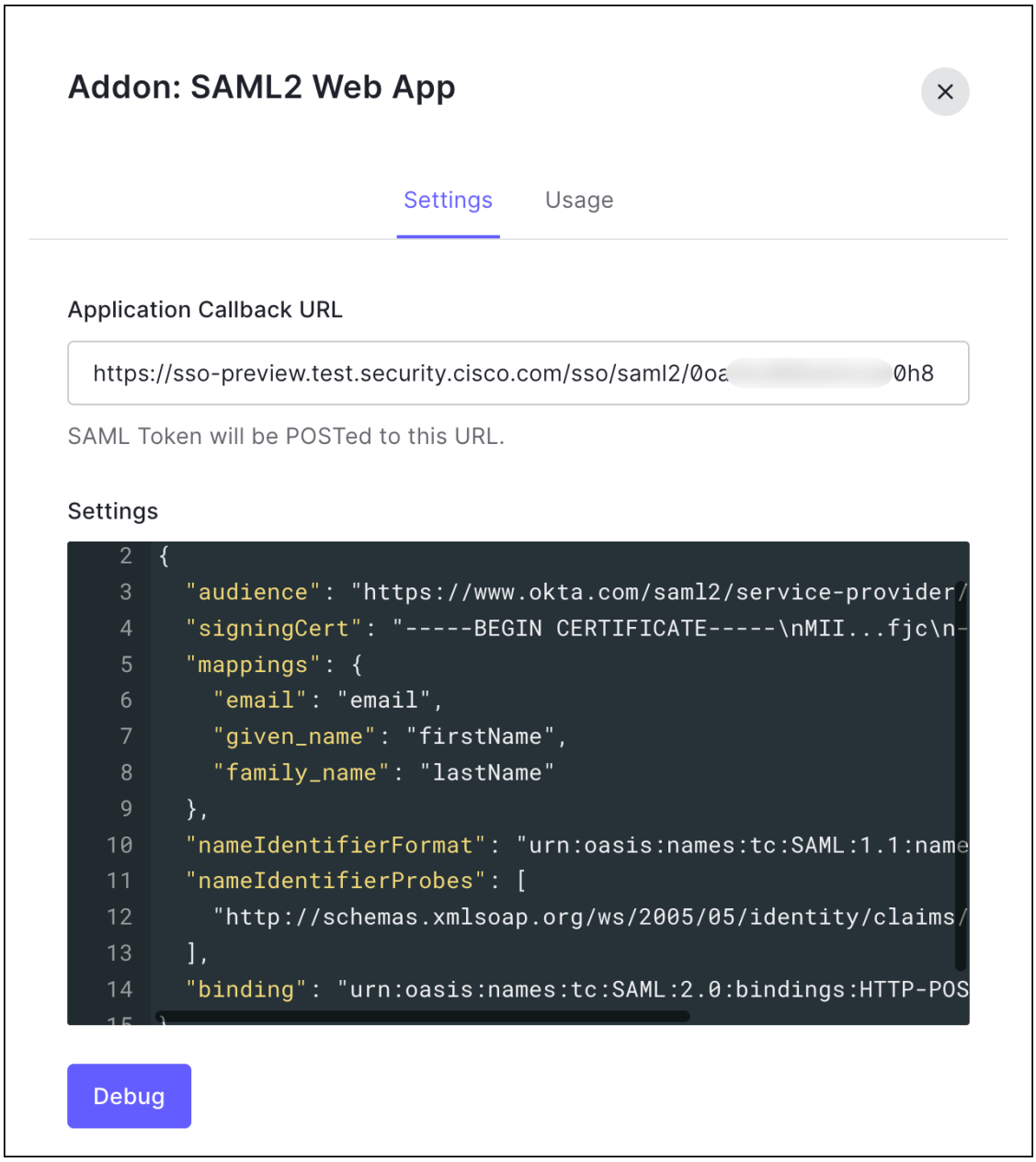
g) In the **Usage** tab, download the Auth0 **Identity Provider Certificate** and the **Identity Provider Metadata** file.

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"
}
```



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.

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

Procedure

Step 1 Sign in to Security Provisioning and Administration with the enterprise you want to integrate with Microsoft Entra ID.

a) Create a new identity provider and decide whether 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 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.

a) Click **Azure Active Directory**.

b) Click **Enterprise Applications** in the left sidebar.

c) Click **+ New Application** and search for `Microsoft Entra SAML Toolkit`.

d) Click **Microsoft Entra 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 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.

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

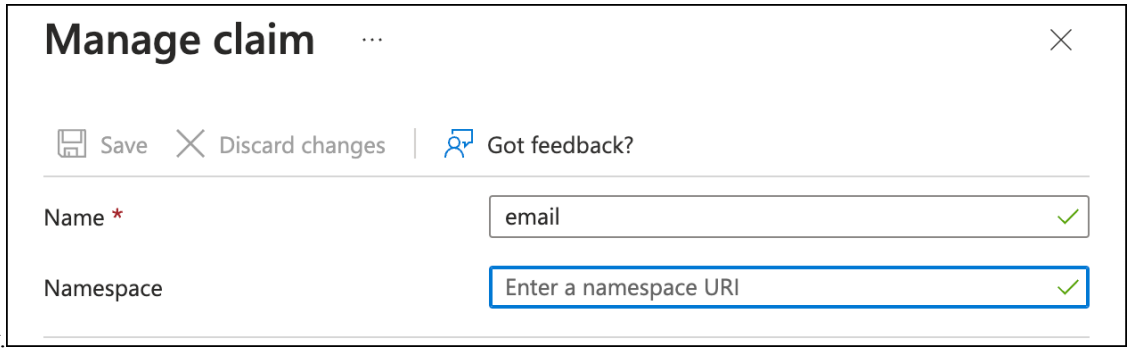
- Under **Required claim**, click the **Unique User Identifier (Name ID)** claim to edit it.

- 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 Microsoft Entra ID 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 **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.

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

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

c) In the **Entity ID (Audience URI)** field, enter the **Microsoft Entra Identifier** value that is provided by Microsoft Entra ID.

d) 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 and Step 5: Activate the integration.

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 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.

Procedure

Step 1 Sign in to Security Provisioning and Administration with the enterprise that you want to integrate with Duo.

a) Create a new identity provider and decide whether 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 Provisioning and Administration tab open, because you'll return to it shortly.

a) From the left navigation 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 and choose **2FA with SSO hosted by Duo** for **Protection Type**.

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.

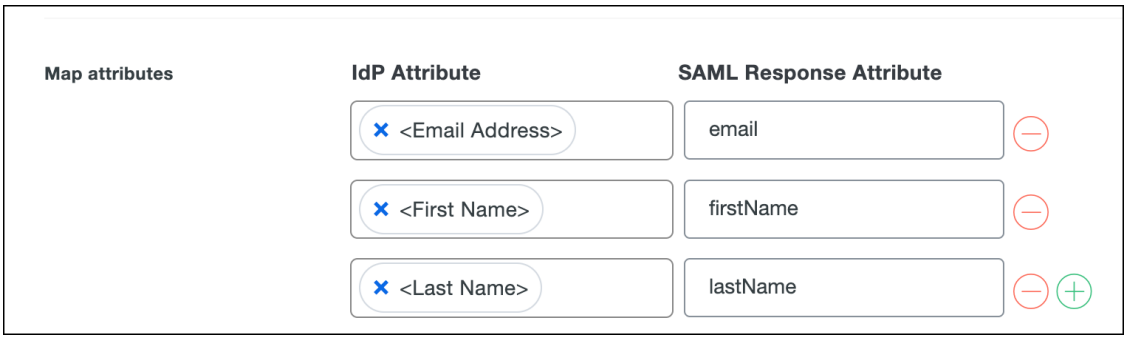
f) Copy the value of **Single Sign-On URL** and save for later use.

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) 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.

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 that is provided by Duo.
c) In the **Entity ID (Audience URI)** field, enter the **Entity ID** value provided by Duo.
d) Upload the **Signing Certificate** that 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.

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.
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.

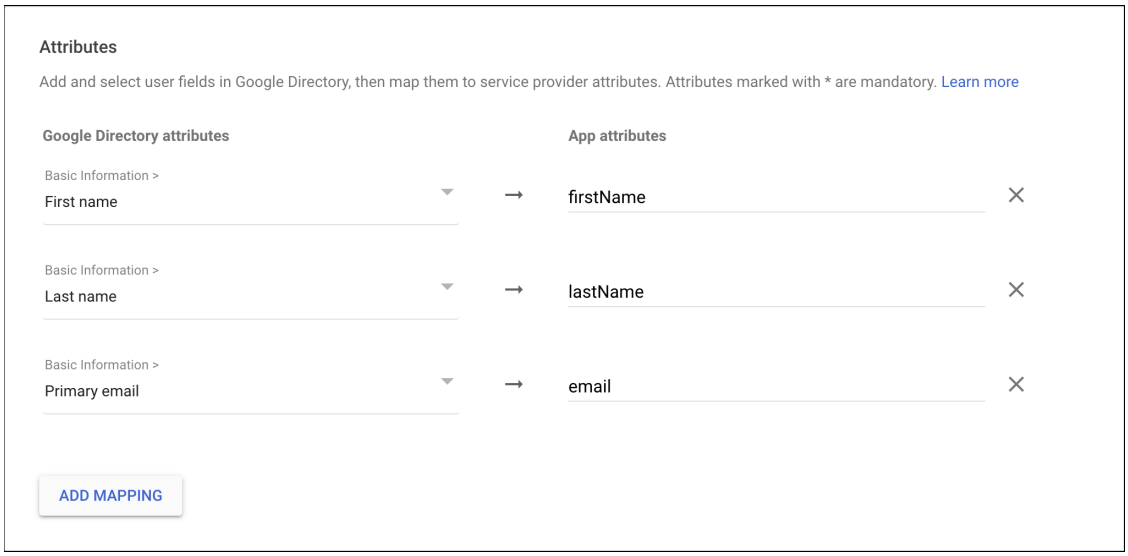
Step 2 In a new browser tab, sign in to your Google Admin console using an account with super administrator privileges. Keep the Security Provisioning and Administration tab open.

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 IDURL** 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



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.

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 Provisioning and Administration.

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.

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.
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 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

Name (in SAML assertion)	Value (in Okta profile)
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.

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.

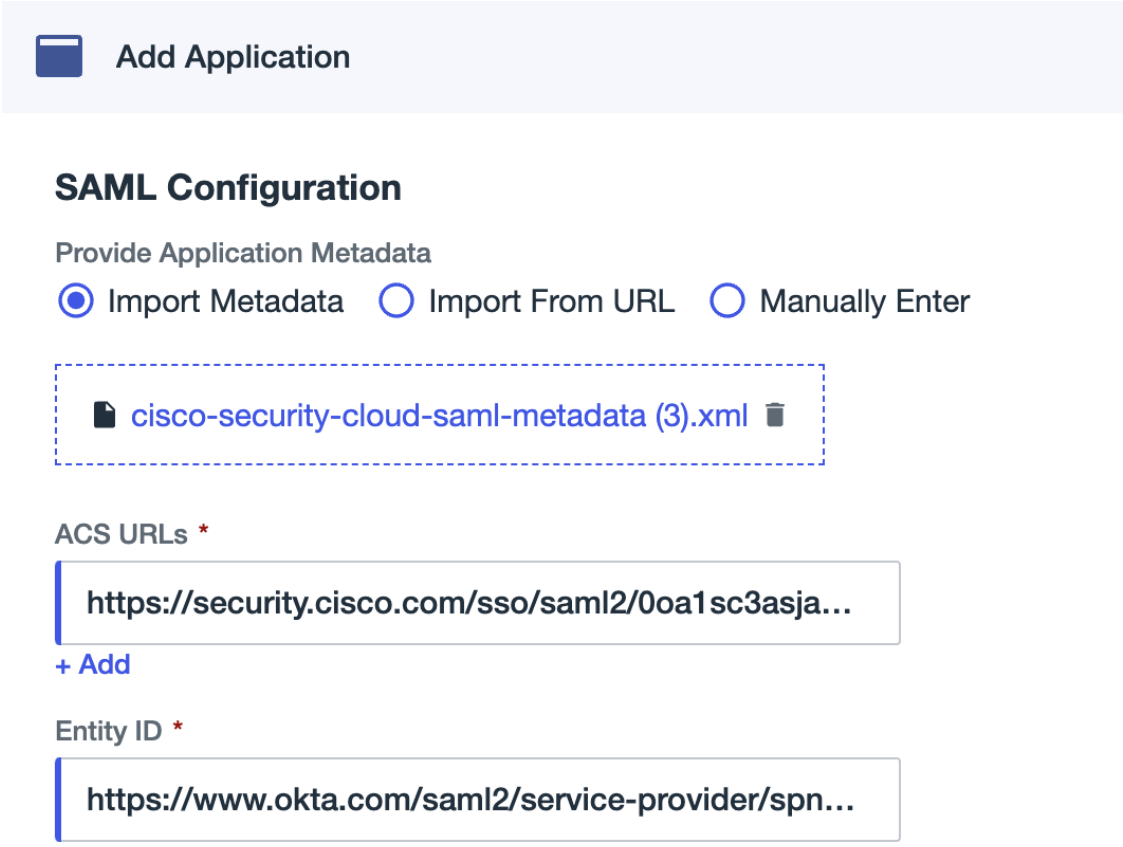
Procedure

Step 1 Sign in to Security Provisioning and Administration with the enterprise that you want to integrate with Ping.

a) Create a new identity provider and decide whether 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 Provisioning and Administration browser tab open.

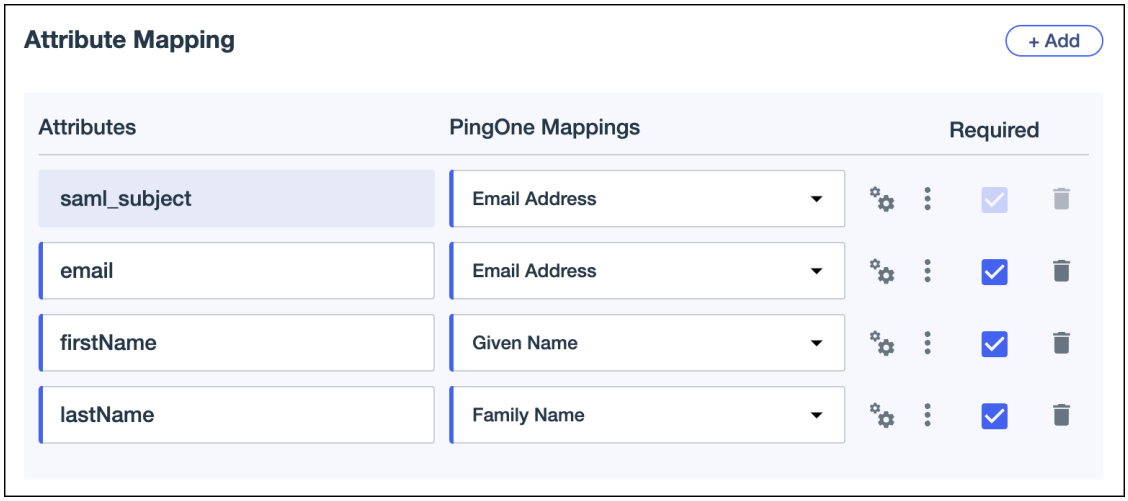
a) Go to **Connections** > **Applications**.
b) Click the **+** button to open the **Add Application** dialog.
c) In the **Application Name** field enter `Secure Cloud Sign On`, or other name.
d) Optionally, add a description and upload an icon.
e) For **Application Type**, select **SAML application** 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 Provisioning and Administration.



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.



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.

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.