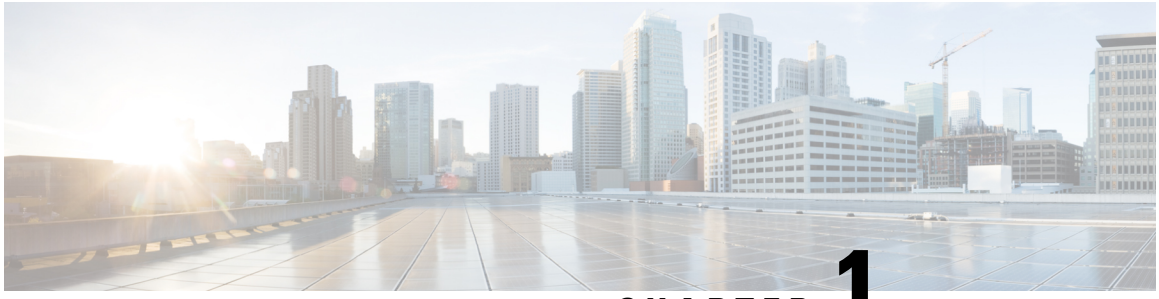
Cisco Security Cloud Sign On Identity Provider Integration Guide

First Published: 2020-09-01

Last Modified: 2022-04-19

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



CHAPTER 1

Overview

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

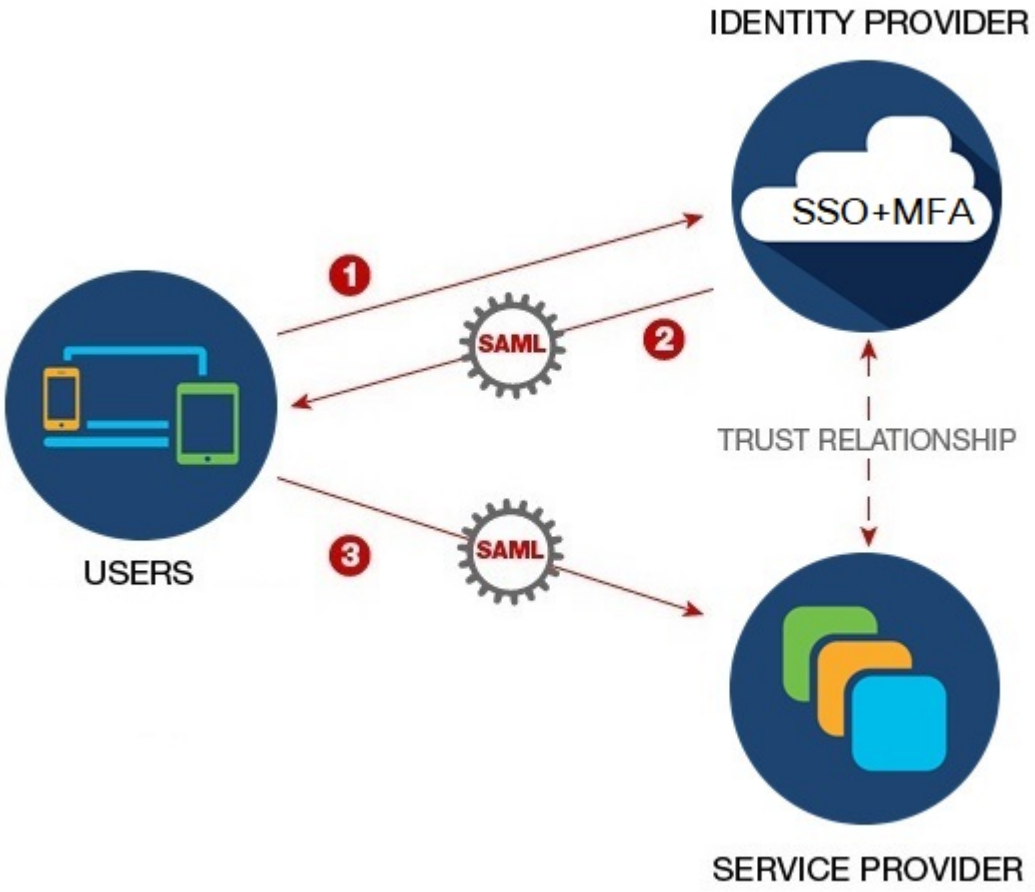
All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 1
- Multi-Factor authentication requirements, on page 2
- Customers with existing IdP integrations, on page 3

Overview

You can integrate your own or third-party identity provider (IdP) with Cisco Security Cloud Sign On using Security Assertion Markup Language (SAML). SAML is an XML-based open standard for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP). In this case, the service provider is Security Cloud Sign On. Once integrated, users can use their single sign on

credentials to sign in to Security Cloud Sign



Multi-Factor authentication requirements

Security Cloud Sign On requires Duo Multi-Factor Authentication for all accounts. Customers who Integrate your identity provider with using SAML (Security Assertion Markup Language) may opt-out of Duo MFA.

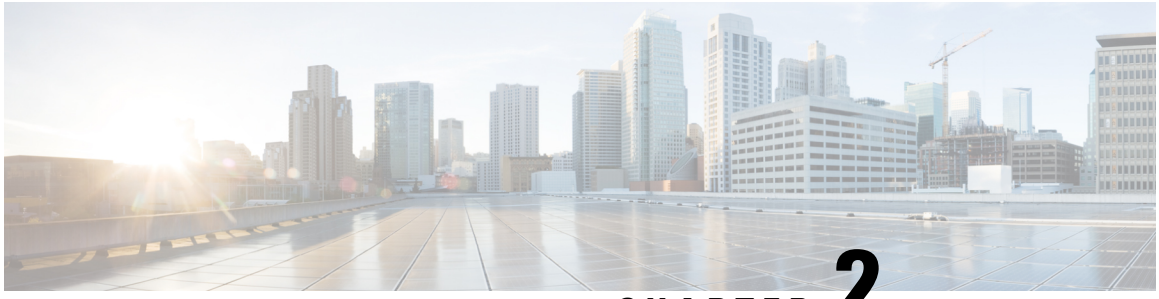
Once enrolled in Duo MFA, users can optionally enroll with Google Authenticator. Once enrolled with Google Authenticator, subsequent sign-ons will only present a Google Authenticator challenge, not a Duo MFA challenge.

This same policy is enforced if you are using federated sign-on through Cisco Customer Identity or Microsoft (under **Other login options** on the Security Cloud Sign On page).

Customers with existing IdP integrations

If you have an IdP integration with Security Cloud Sign On that was **not** created with the Enterprise settings wizard described in this guide, you cannot use the tool to update your existing configuration. You will need to open a open a case with Cisco TAC if you need to modify any of the following settings for your integration:

- SAML single sign on URL or Entity ID URI
- x.509 signing certificate
- Multi-Factor Authentication (MFA) settings



CHAPTER 2

SAML requirements for identity providers

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 5
- SAML response requirements, on page 5
- SAML metadata requirements, on page 6

Overview

The SAML response from your IdP to Security Cloud Sign On must adhere to a few rules as described in SAML response requirements, on page 5.

You will also need to obtain the SAML metadata requirements from your IdP.

SAML response requirements

SAML response signed with SHA-256

The SAML response returned by the identity provider must be signed with the SHA-256 signature algorithm. Security Cloud Sign On will reject responses that are unsigned or signed with another algorithm.

SAML response attributes

The assertion in the SAML response sent by your IdP must contain the following attribute names and must be mapped to the IdP's corresponding attributes.

SAML assertion attribute name	IdP user attribute
firstName	User's first or given name.
lastName	User's lastname or surname.

SAML assertion attribute name	IdP user attribute
email	User's email. This must match the value of the **<NameID>** element in the SAML response.

For example, the following XML snippet is an example of an **<AttributeStatement>** element included in a SAML response to the Security Cloud Sign On ACL URL:

```
<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">John
      </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">Doe
      </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">jdoe@example.com
      </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

NameID element

The **<NameID>** element in the SAML response from your IdP must have a valid email address as its value, and the email must match the value of the **email** attribute in the SAML response attributes, on page 5.

The **Format** attribute of the **<NameID>** must be set to either **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** or **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

Below is an example `<NameID>` element.

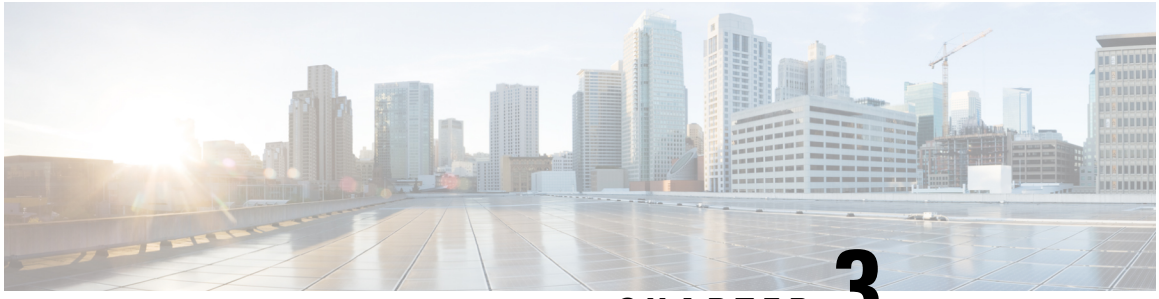
```
<saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe@example.com</saml2:NameID>
```

SAML metadata requirements

The following metadata from your IdP's SAML application is required to integrate with Security Cloud Sign On.

- **Single sign-on service initial URL** – This is sometimes referred to as "SSO URL" or "Login URL". This URL can be used to start an IdP-initiated authentication to Security Cloud Sign On.
- **Entity ID URI** – The global, unique name for your IdP. This is sometimes referred to as "Issuer".

- **X.509 signing certificate** – The public key of the public/private key pair your IdP uses to sign SAML assertions.



CHAPTER 3

Integrate your identity provider

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

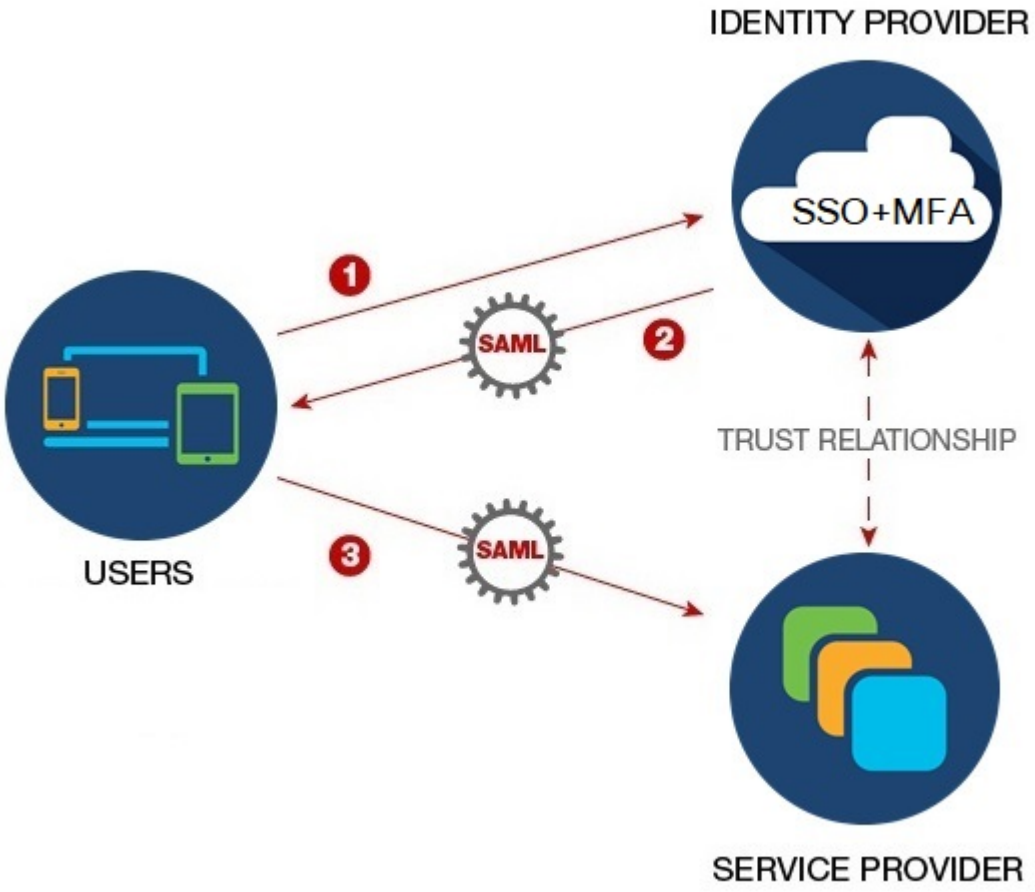
All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 9
- Enterprise settings wizard, on page 10
- Step 1: Create an enterprise, on page 11
- Step 2: Claim and verify your email domain, on page 12
- Step 3: Exchange SAML metadata, on page 13
- Step 4: Test the SSO integration, on page 15
- Step 5: Activate IdP integration, on page 16

Overview

You can integrate your own or third-party identity provider with Security Cloud Sign On using Security Assertion Markup Language (SAML). SAML is an XML-based open standard for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP), which in this case is Security Cloud Sign On. Once integrated, users can then their usual single sign on credentials to sign in to

Security Cloud Sign

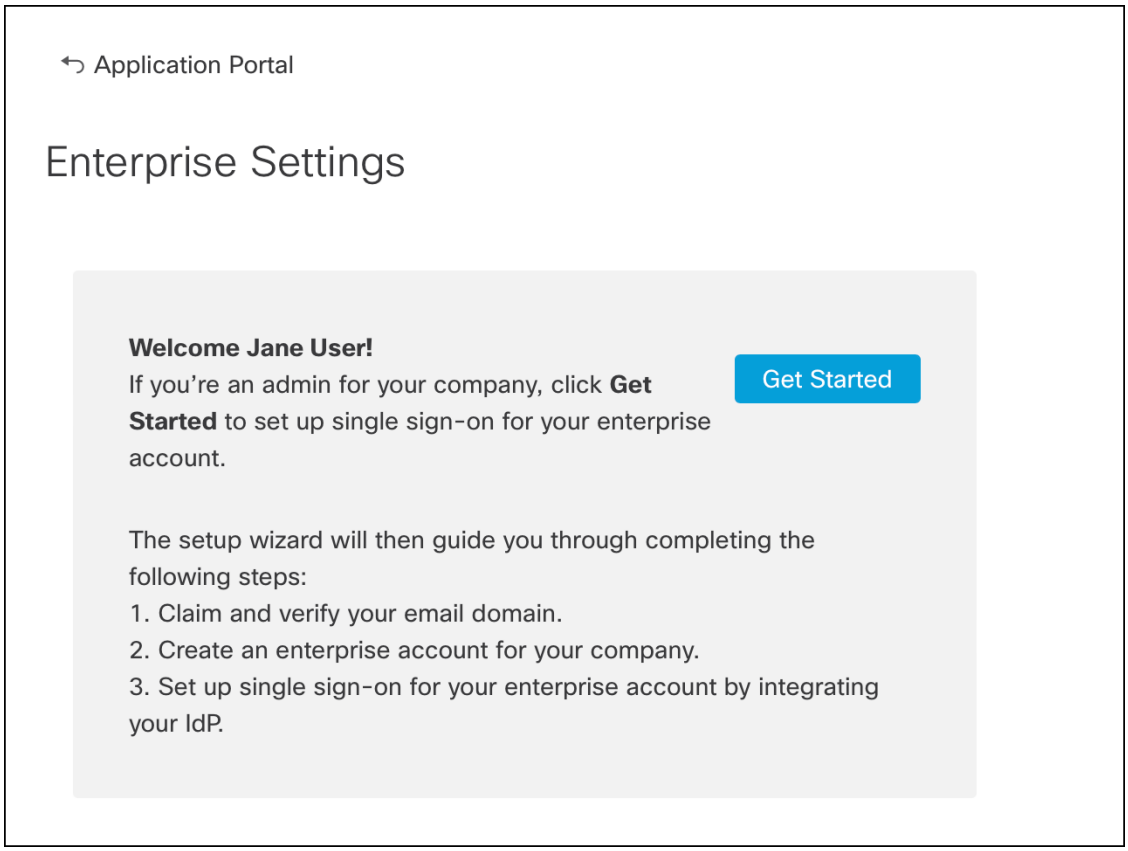


By default, Security Cloud Sign On enrolls all your IdP's users into Duo Multi-Factor Authentication (MFA) at no cost. If your organization already has MFA integrated with your IdP, you can optionally disable Duo-based MFA during the integration process.

Enterprise settings wizard

The Enterprise Settings setup wizard walks you multiple steps to integrate your own IdP with Security Cloud Sign On. The wizard saves your progress as you complete each step, so you can quit and return later to complete the process.

To open the Enterprise settings wizard, click your profile icon in the SecureX Application Portal, select **Enterprise Settings**, then click **Get Started**.



The settings wizard lets you claim one email domain and configure one identity provider. You will need to open a case with Cisco TAC in the following cases:

- You need to configure more than one identity provider
- You need to claim more than one email domain
- You want to change your organization name or email domain after Step 2: Claim and verify your email domain

Note If you have an existing IdP integration that was **not** created with the Enterprise settings wizard, you can't use the wizard to modify your integration. See Customers with existing IdP integrations, on page 3 for details.

Step 1: Create an enterprise

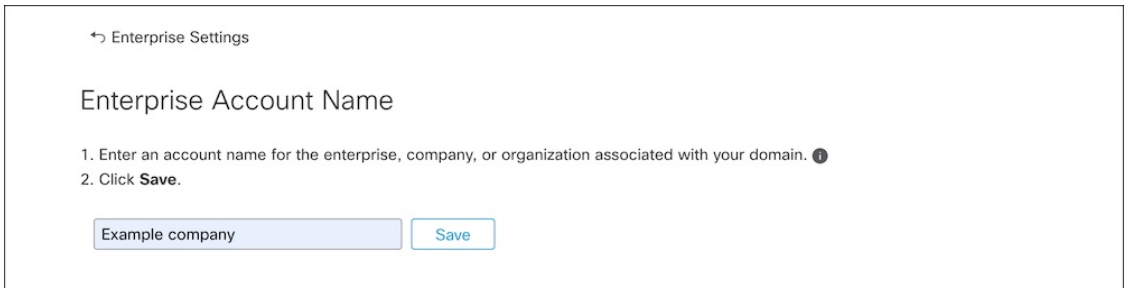
The first step is to create a named enterprise in Security Cloud Sign On. This enterprise will be associated with your claimed domain and identity provider configuration.

Step 1 Sign in to the SecureX Application Portal with a Security Cloud Sign On account.

Step 2 Click your profile icon in the upper right corner and select **Enterprise Settings**.

Step 3 Click **Get Started**.

Step 4 Enter a name for your enterprise account and click **Save**.

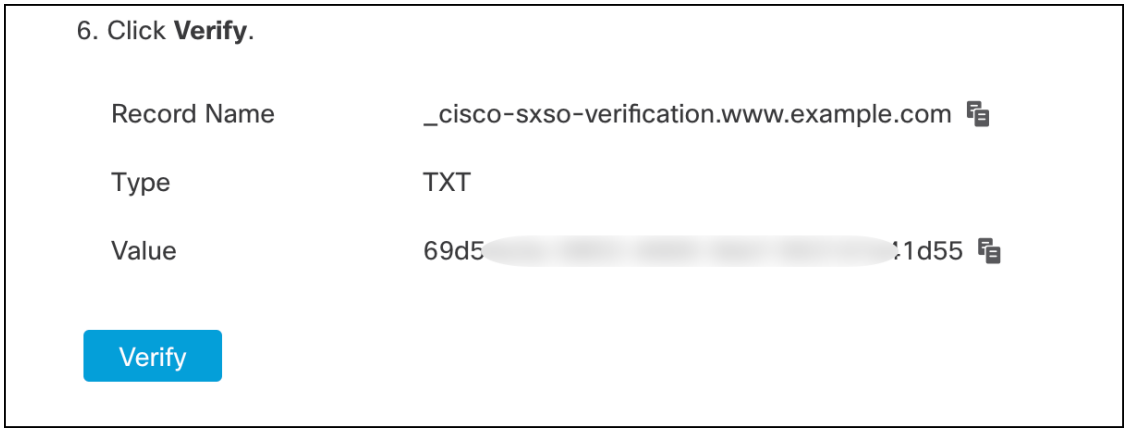


Step 2: Claim and verify your email domain

Next you'll claim and verify your enterprise's email domain. To complete this step you'll need to create a DNS record on your domain name registrar service portal. Once you've verified your domain you can delete the DNS record.

Step 1 Enter the domain you want to claim and click **Submit**.

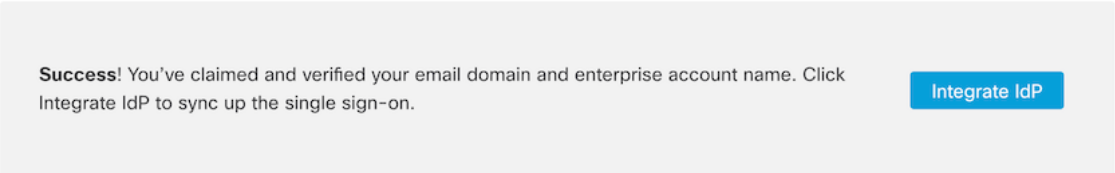
The settings wizard displays a DNS TXT record name and value.



Step 2 Sign in to your domain name registrar service and create a TXT record with the specified record name and value.

Step 3 Wait for the DNS record to propagate, then click **Verify**.

Step 4 If verification is successful, click **Integrate IdP** to begin integrating your identity provider.



Step 3: Exchange SAML metadata

In this step you'll exchange SAML metadata and signing certificates between your IdP and Security Cloud Sign On.

Before you begin

To complete this step you'll need the following information about the Overview you've created on your identity provider:

- **Single Sign-On Service URL** – The URL where Security Cloud Sign On will send a SAML Authentication Request via HTTP POST. The URL's domain must match the domain that you previously Step 2: Claim and verify your email domain.
- **Entity ID** – Uniquely identifies your identity provider to Security Cloud Sign On. In your IdP's SAML metadata it can be found in the `entityID` attribute of the `<EntityDescriptor>` element. It is called **Identity Provider Issuer** by some IdPs.
- **SAML signing certificate** – The x.509 signing certificate used by your IdP to sign SAML assertions.

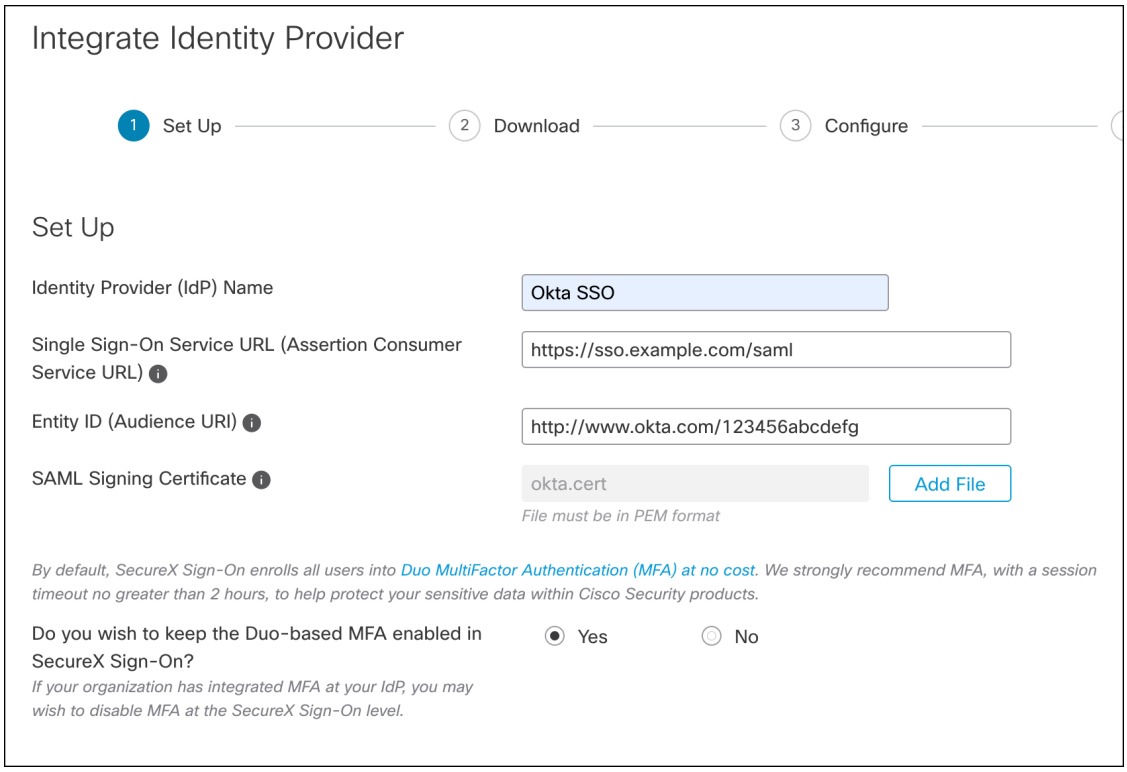
Note The certificate must be signed with the SHA-256 algorithm. Assertions signed with another algorithm are rejected with an HTTP 400 error.

Step 1 In the **Identity Provider Name** field enter a name for your IdP in the **Set Up** screen.

Step 2 Enter the values for **Single Sign-On Service URL** and **Entity ID** that you obtained from your IdP's SAML integration.

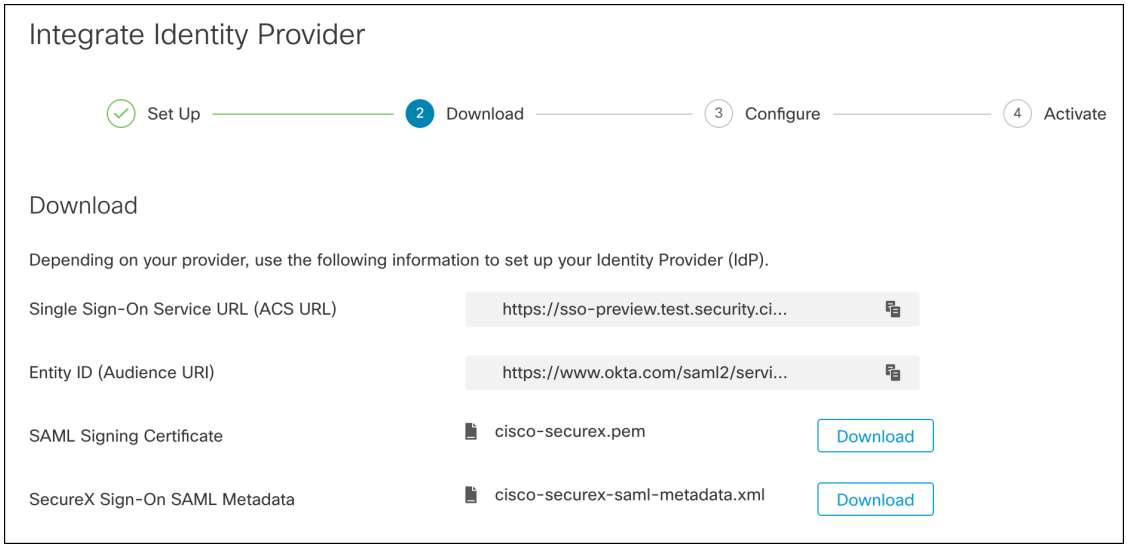
Step 3 Click **Add File** and select the SAML signing certificate you previously download from your IdP.

Step 4 If you don't want to automatically enroll your users in Duo MFA, select **No** for **Do you wish to keep the Duo-based MFA enabled in Security Cloud Sign On?**



Step 5 Click **Next** to advance to the **Download** screen.

Step 6 Copy the displayed **Single Sign-On Service (ACS URL)** and **Entity ID (Audience URL)**, and download the **SAML Signing Certificate**.



Step 7 7. Click **Next** to advance to the **Configure** screen.

Step 8 Open your the SAML application configuration page on your IdP management console and make the following changes:

a) Update the temporary values assigned to **ACS URL** and **Entity ID** with the values you obtained in the previous step.

b) Upload the SAML signing certificate provided by the settings wizard.

Note Some IdPs (Getting started, for example) require you to provide the contents of the certificate as a single-line JSON string (`-----BEGIN CERTIFICATE-----\n...\n...\n-----END CERTIFICATE-----\n`, for example).

c) Save the configuration changes to your SAML app configuration.

What to do next

Next, you'll test the IdP integration with your enterprise.

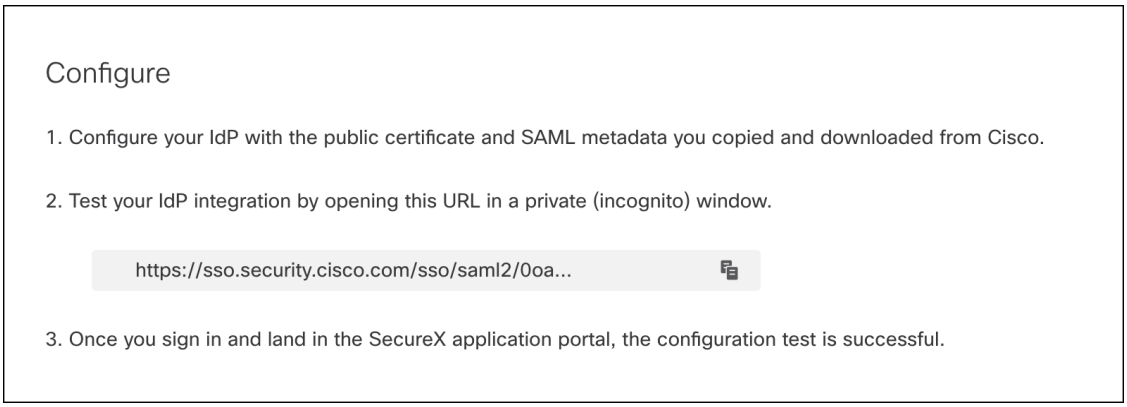
Step 4: Test the SSO integration

Next you'll test your IdP's integration by initiating an SSO request from the enterprise wizard to your IdP. If you land back in the SecureX Application Dashboard it means test was successful.

- Test the URL in a private (incognito) window.
- The email domain used to sign in must match the Step 2: Claim and verify your email domain you claimed previously.
- Test with new users (those without an existing Security Cloud Sign On account) as well as existing users.

Step 1 Return to the Enterprise settings wizard's **Configure** screen.

Step 2 Copy the SSO URL in **Step 2** to your clipboard and open it in a private (incognito) browser window.



Step 3 Sign in to your identity provider.

- The email domain used to sign in must match the Step 2: Claim and verify your email domain you claimed previously.
- Test with an account other than the one you used to initially sign up with Secure Cloud Sign On. For instance, if you used the admin@example.com account to sign up and create the IdP integration, don't use that same email to test the integration.

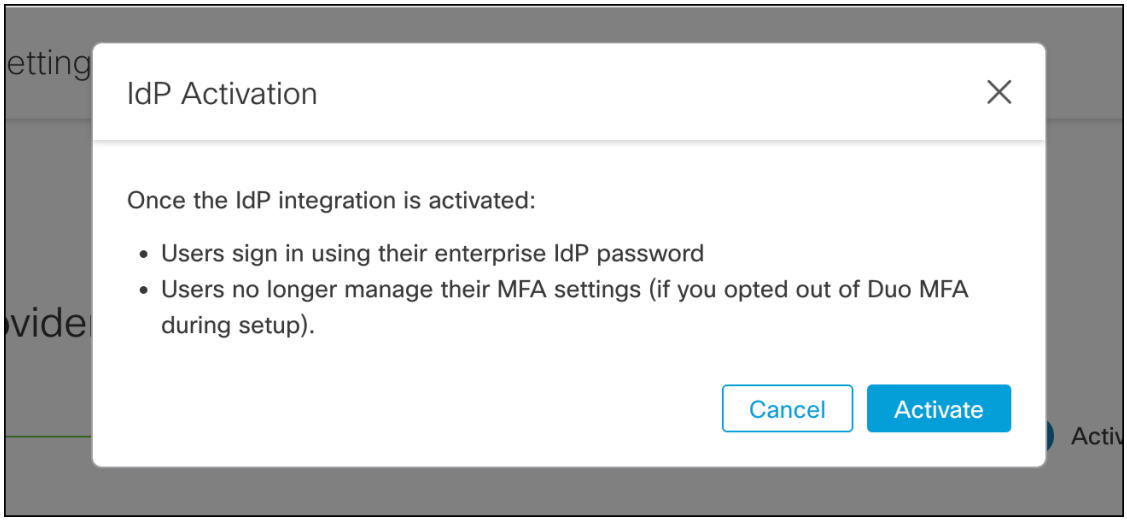
Once you land in the SecureX Application Portal, the configuration test is successful. See Troubleshooting, on page 17 if you encounter an error during the SSO process.

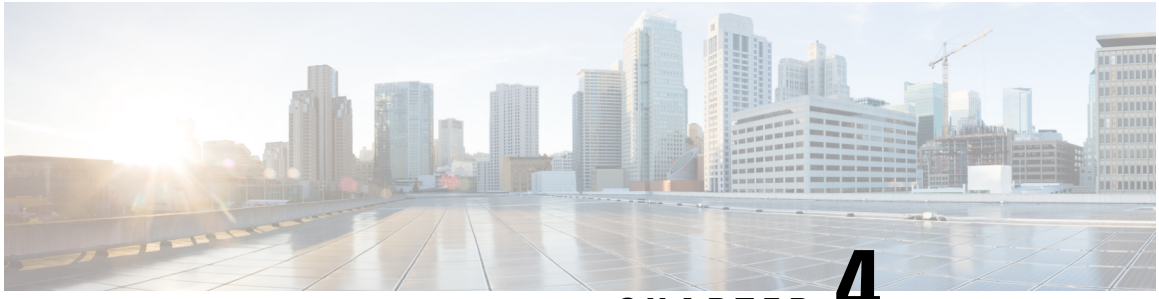
Step 4 Once you've tested the integration, click **Next** to advance to the **Activate** page.

Step 5: Activate IdP integration

Once you've Step 4: Test the SSO integration and are ready to to enable it for your organization, you can activate it. Once activated, users sign in using their enterprise (IdP) email address and password. If you opted out of free Duo MFA enrollment, your users will no longer manage their MFA settings.

To activate the integration with your IdP and Security Cloud Sign On click **Activate my IdP**, then click **Activate** in the confirmation dialog.





CHAPTER 4

Troubleshooting

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Single sign-on/SAML errors, on page 17
- Enterprise wizard errors, on page 18
- Integration with Cisco security products, on page 18

Single sign-on/SAML errors

HTTP 400 errors when testing your integration

If you get an HTTP 400 error when Step 4: Test the SSO integration in the Enterprise settings wizard, try the following troubleshooting steps.

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

Make sure the email domain of the user account you're using to test with matches your Step 2: Claim and verify your email 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 <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 attributes, on page 5 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, namely, **firstName**, **lastName**, and **email**. See SAML response requirements, on page 5 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.

Enterprise wizard errors

Error when verifying your domain

If you encounter an error when Step 2: Claim and verify your email domain, try the following troubleshooting steps.

Wait a while and try again

Wait a while and try clicking **Verify** again. The time it takes DNS record updates to propagate to DNS servers varies by service provider.

Verify TXT DNS record name and value

Verify that the name and value of the TXT DNS record you created on your domain registrar matches the displayed by the enterprise settings wizard.

Error testing single sign-on

If you encounter an error when Step 4: Test the SSO integration it's likely a SAML configuration issue or an issue with the user account. See Single sign-on/SAML errors, on page 17 for troubleshooting steps.

Integration with Cisco security products

Sign-on errors with Cisco security products

If you are able to sign on to Security Cloud Sign On but aren't able to sign on to one or more Cisco security products, check the following.

Check if the product requires you to opt-in to Security Cloud Sign On

While some Cisco security products such as Cisco Umbrella support Security Cloud Sign On by default, others require you to opt-in. The list of supported security products identifies those Cisco security products that require opt-in.

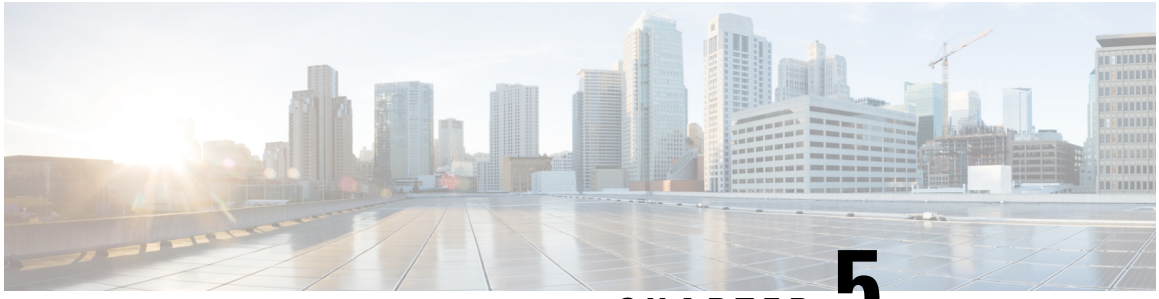
Check that your Security Cloud Sign On identity matches your product identity

Each user's Security Cloud Sign On identity (email) must match their product identity. For instance, suppose you have a Security Cloud Sign On account with the username `user@example.com`. To authenticate successfully with Umbrella using your Security Cloud Sign On account there must be an existing Umbrella account with the same email.

PART I

Identity provider integration guides

- Auth0, on page 21
- Azure AD, on page 27
- Duo, on page 31
- Google, on page 35
- Okta, on page 39
- Ping Identity, on page 43
- Generic IdP instructions, on page 47



CHAPTER 5

Auth0

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 21
- Getting started, on page 21

Overview

This guide describes how to create an Auth0 SAML application to integrate with Security Cloud Sign On.

Getting started

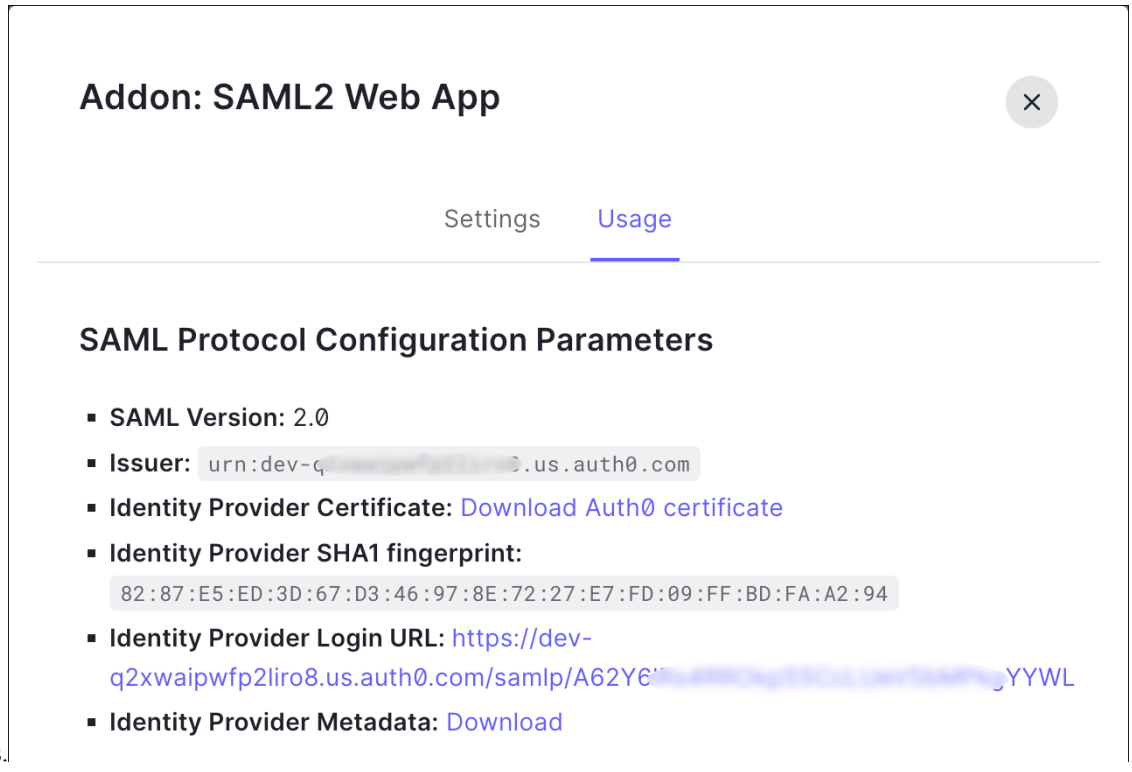
Before you begin

- You must be able to sign in to the Auth0 management console with administrator privileges.
- You need to have completed Step 1: Create an enterprise, on page 11 and Step 2: Claim and verify your email domain, on page 12.

Step 1 Sign in to your Auth0 Dashboard and do the following:

a) Select **Applications** from the **Applications** menu.
b) Click **Create Application**.
c) In the **Name** field enter `Secure Cloud Sign On`, or other name.
d) For application type, choose **Regular Web Applications** then click **Create**.
e) Click the **Addons** tab.
f) Click the **SAML2 Web App** toggle to enable the addon.

The SAML2 Web App configuration dialog



opens.

g) Copy the values for the **Issuer** and **Identity Provider Login URL** fields.

h) Click **Download Auth0 certificate** to download the **Identity Provider Certificate**.

Step 2 Open the Enterprise settings wizard's **Integrate Identity Provider** screen and do the following:

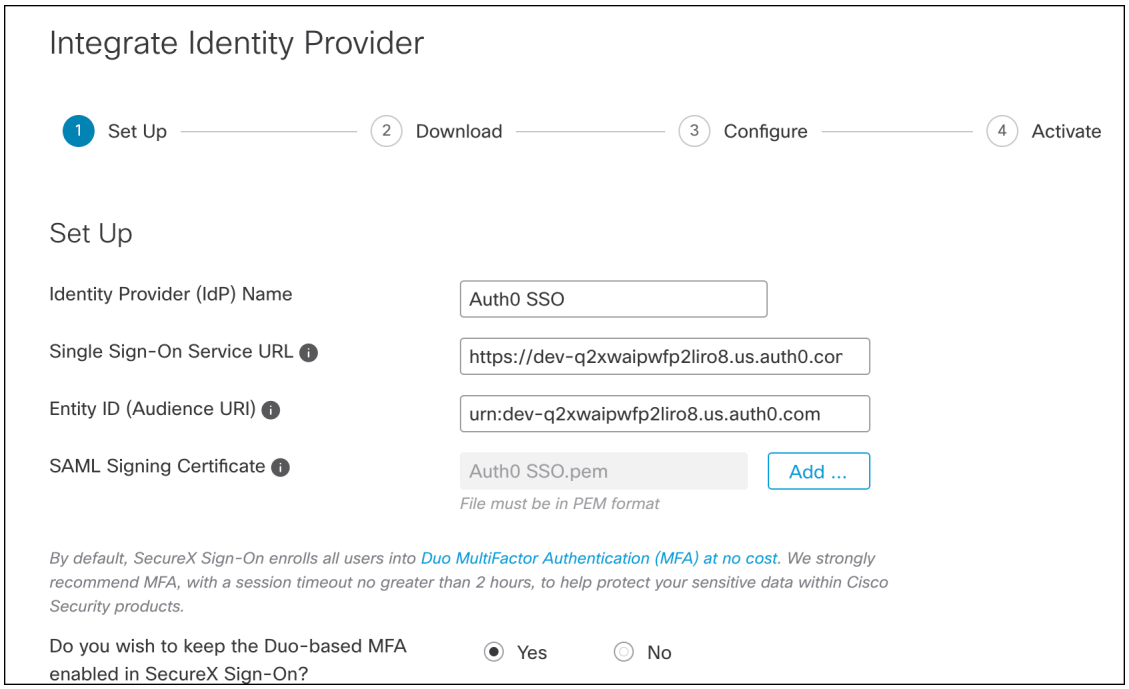
a) In the **Identity Provider Name** field enter a name for your IdP (**`Auth0 SSO`**, for example).

b) In the **Single Sign On Service URL** field enter the value of the **Identity Provider Login URL** that you copied from the SAML Addon dialog.

c) In the **Entity ID** field enter the value of the **Issuer** field you copied from the SAML Addon dialog.

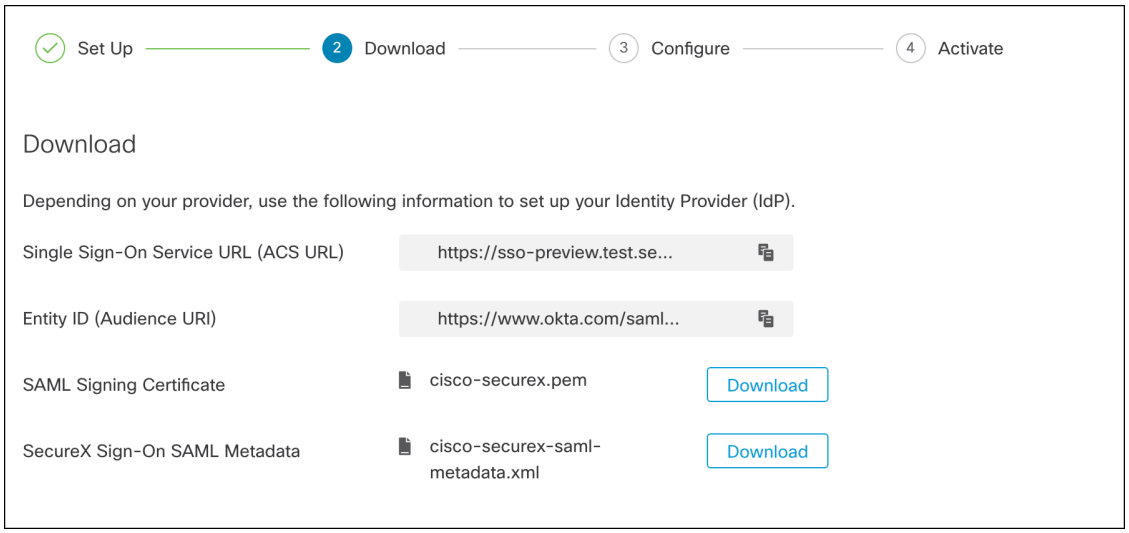
d) Click **Add File** and select the SAML signing certificate you downloaded from Auth0.

e) If desired, opt-out of free Duo-based MFA service for your users.



f) Click **Next** to advance to the **Download** settings page.

g) Copy the values of the **Single Sign-On Service URL** and **Entity ID** for later use, and download the **SAML Signing Certificate** (cisco-securex.pem).



h) Click **Next** to advance to the **Configure** screen.

Step 3 Return to the Addon configuration dialog in the Auth0 console.

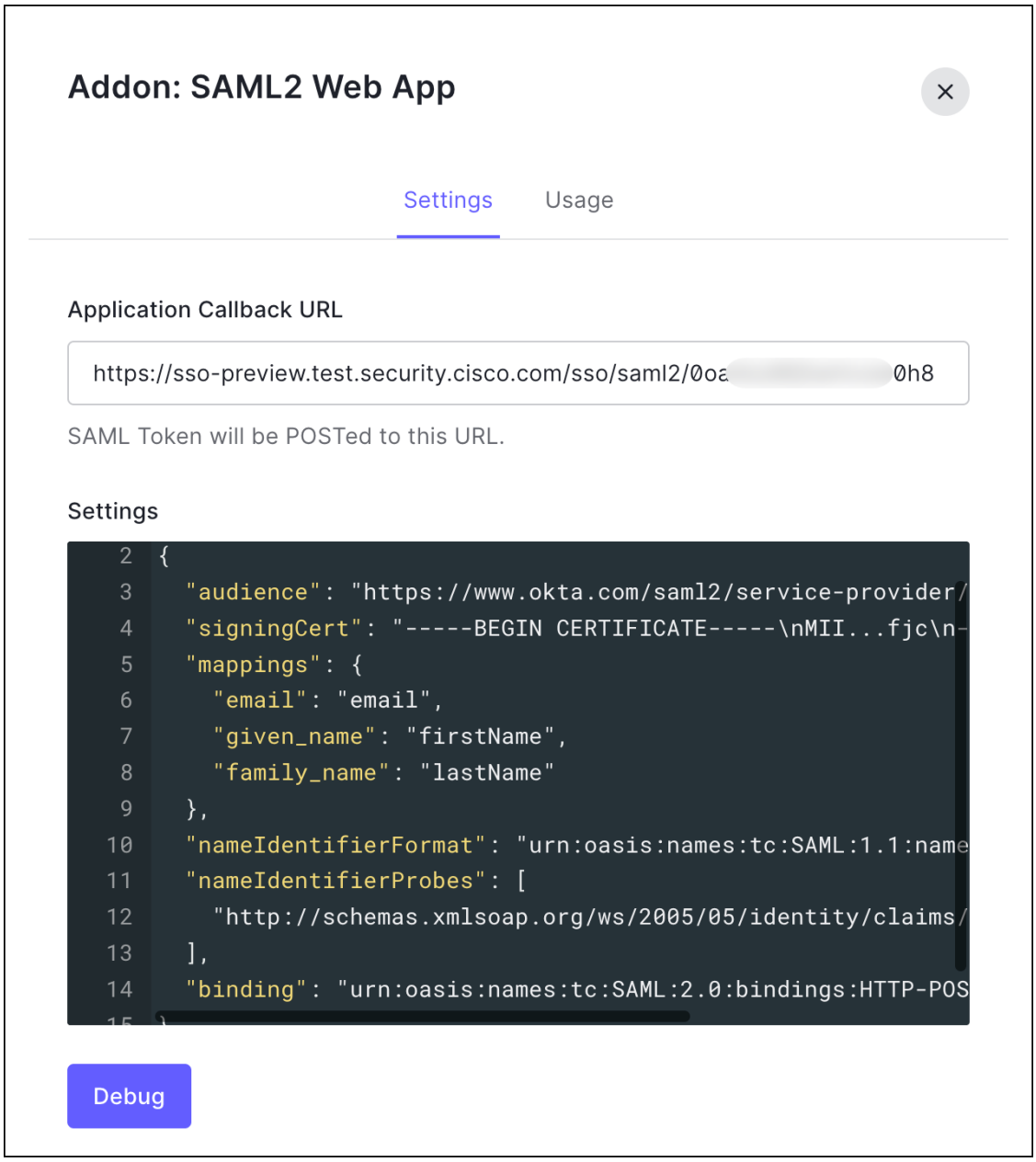
a) Click the **Settings** tab.

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

c) Optionally, click **Debug** to verify the structure and contents of a sample SAML response (your Auth0 user must be assigned to the SAML application to debug the response).

d) In the **Settings** field enter the following JSON object, replacing `<ENTITY_ID_URI>` with the value of the **Entity ID (Audience URI)** field you copied previously, and `<SIGNING_CERT>` with the contents of the SecureX Sign On signing certificate (PEM file) that you downloaded converted to a single-line string.

```
{
  "audience": "https://www.okta.com/saml2/...",
  "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"
}
```



e) Click **Enable** at the bottom of the dialog to enable the SAML application.

Step 4 Return to the Enterprise settings wizard's **Configure** screen.

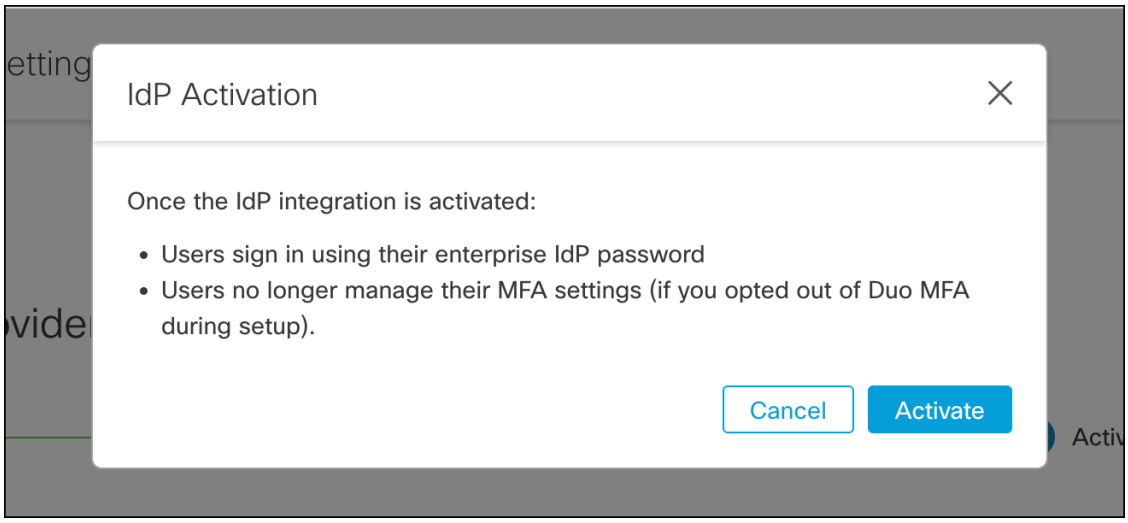
a) Copy the displayed URL and open it in a private (incognito) browser window.
The browser is redirected to the Auth0 SSO page.

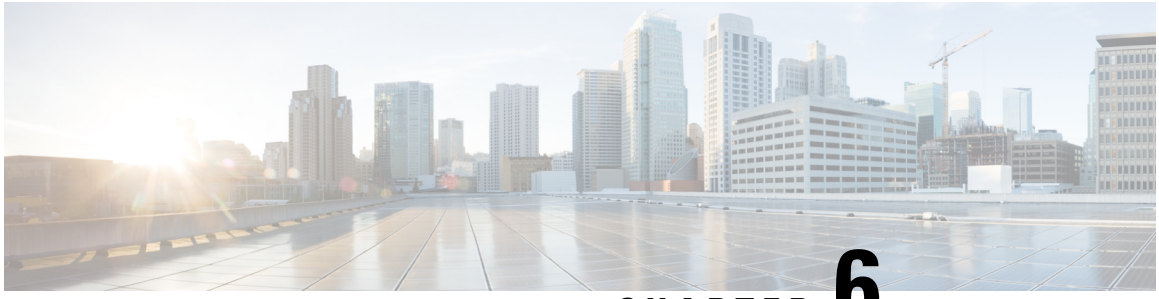
b) Sign in to Auth0 with an email address that matches your Step 2: Claim and verify your email domain.
The test is successful if you land back in the SecureX Application Portal.

c) Click **Next** in the settings wizard to advance to the **Activate** screen.

d) To activate the integration for your users, click **Activate my IdP**.

e) Confirm your decision in the dialog.


IdP Activation
Once the IdP integration is activated:
• Users sign in using their enterprise IdP password
• Users no longer manage their MFA settings (if you opted out of Duo MFA during setup).
Cancel
Activate



CHAPTER 6

Azure AD

Important

Enterprise Manager has been discontinued. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 27
- Getting started, on page 27

Overview

This guide shows how to create an Azure AD SAML application and integrate with it with Security Cloud Sign On .

Note

- Keep in mind that the user principal name (UPN) of an Azure AD user is not always the same as the user's email address.
- The `<NameID>` element and the `email` user attribute in the SAML response **must** contain the user's email address. See SAML response requirements, on page 5 for details.
- The specified email address should match the one used in existing product access controls. If they do not match you will need to update your product access controls.

Getting started

Before you begin

- You must be able to sign in to the Azure portal with admin privileges.
- You need to have completed Step 1: Create an enterprise, on page 11 and Step 2: Claim and verify your email domain, on page 12 of the enterprise settings wizard.

Step 1 Sign in to https://portal.azure.com.

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 **`SecureX 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**.

- Under **Identifier (Entity ID)** click **Add Identifier** and enter a temporary value of **`https://example.com`** or other valid URL. You'll replace this temporary value later.
- Under **Reply URL (Assertion Consumer Service URL)** click **Add reply URL** and enter a temporary value of **`https://example.com`** or other valid URL. You'll replace this temporary value later.
- In the **Sign on URL** field enter **`https://sign-on.security.cisco.com/`**.
- Click **Save** and close the **Basic SAML Configuration** panel.

i) Under **Required claim**, click the **Unique User Identifier (Name ID)** claim to edit it.
j) Set the **Source** attribute field to `user.userprincipalname`.

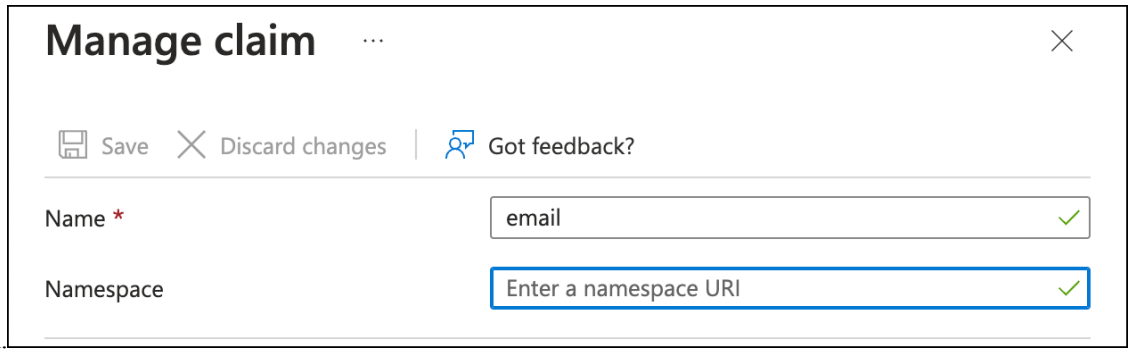
This assumes that the value of **user.userprincipalname** represents a valid email address. Otherwise, set **Source** to use **user.primaryauthoritativeemail**.

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

This assumes that the value of **user.userprincipalname** represents a valid email address. Otherwise, set **Source attribute** for the **email** claim to use **user.primaryauthoritativeemail**.

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.



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

m) 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 2 In a new browser tab, open the Enterprise settings wizard. You should be on the **Integrate Identity Provider** > **Set Up** screen (Step 3: Exchange SAML metadata, on page 13).

a) In the **Identity Provider (IdP) Name** field enter `Azure SSO` or other name for the integration.

b) In the **Single Sign-On Service URL** field enter the value of the **Login URL** field you copied from Azure.

c) In the **Entity ID (Audience URI)** field enter the value of the **Azure AD Identifier** you copied from Azure.

d) Click **Add File** and upload the SAML signing certificate you downloaded from the Azure portal.

e) Opt out of free Duo MFA for your users, if desired.

f) On the **Download** screen click **Next**.

g) Copy the values of **Single Sign-On Service URL (ACS URL)** and **Entity ID (Audience URI)** for use later in this procedure.

h) Click **Next**.

Step 3 Return to the Azure console browser tab.

a) In the **Basic SAML Configuration** section click **Edit**.

b) In the **Identifier (Entity ID)** field replace the temporary identity provider you entered with the value of the **Entity ID (Audience URI)** field you copied from the Enterprise settings wizard.

c) In the **Reply URL (Assertion Consumer Service URL)** field replace the temporary identity provider you entered with the value of the **Single Sign-On Service URL (ACS URL)** field you copied from the Enterprise settings wizard.

d) Click **Save** and close the **Basic SAML Configuration** panel.

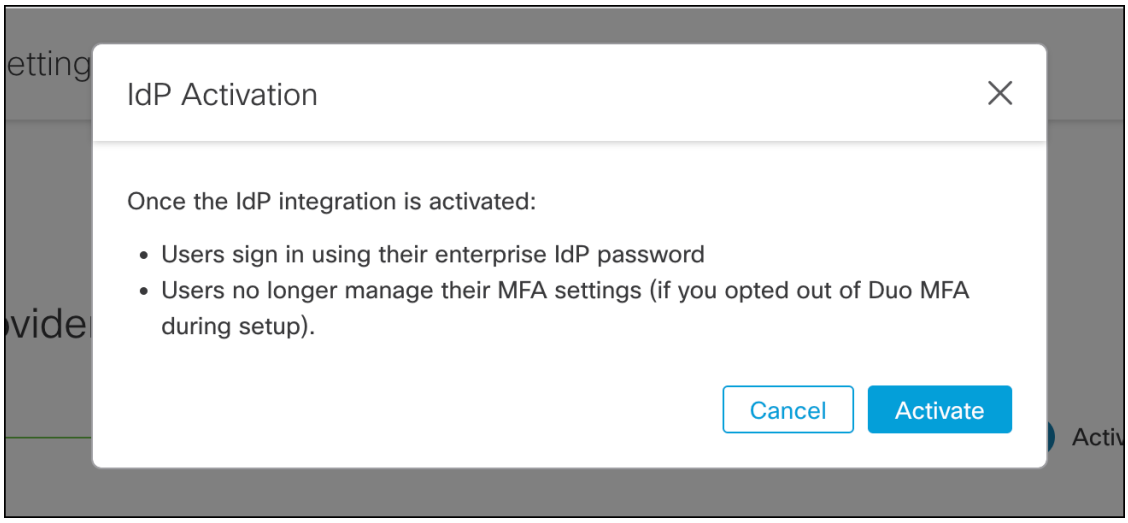
Step 4 Return to the Enterprise settings wizard to test the integration. You should be on the **Configure** screen (Step 4: Test the SSO integration, on page 15) and do the following:

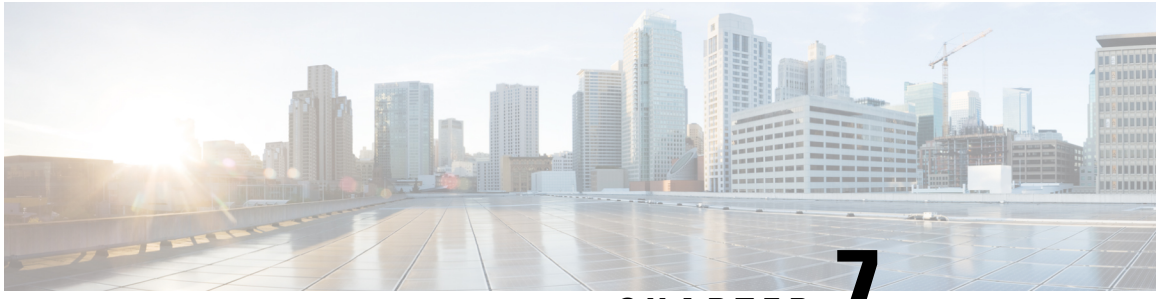
a) Copy the provided URL and open it a private (incognito) window.

b) Sign in with an Azure AD account associated with the SAML application.
If you land back in the SecureX Application Portal then the test was successful. If you encounter an error see Troubleshooting, on page 17.

c) Click **Next** to advance to the **Activate** screen.

d) When you're ready click **Activate my IdP** and then confirm your choice in the dialog box.


IdP Activation
Once the IdP integration is activated:
• Users sign in using their enterprise IdP password
• Users no longer manage their MFA settings (if you opted out of Duo MFA during setup).
Cancel
Activate



CHAPTER 7

Duo

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 31
- Getting started, on page 31

Overview

This guide describes how to create a Duo SAML application and integrate it with Security Cloud Sign On.

Getting started

Before you begin

- You must be a Duo admin with the Owner role.
- Have at least one authentication source already configured in Duo under **Duo Admin** > **Single Sign-On** > **Configured Authentication Sources**.
- You need to have completed Step 1: Create an enterprise, on page 11 and Step 2: Claim and verify your email domain, on page 12 of the enterprise settings wizard.

Step 1 Sign in to the Duo Admin Panel.

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.

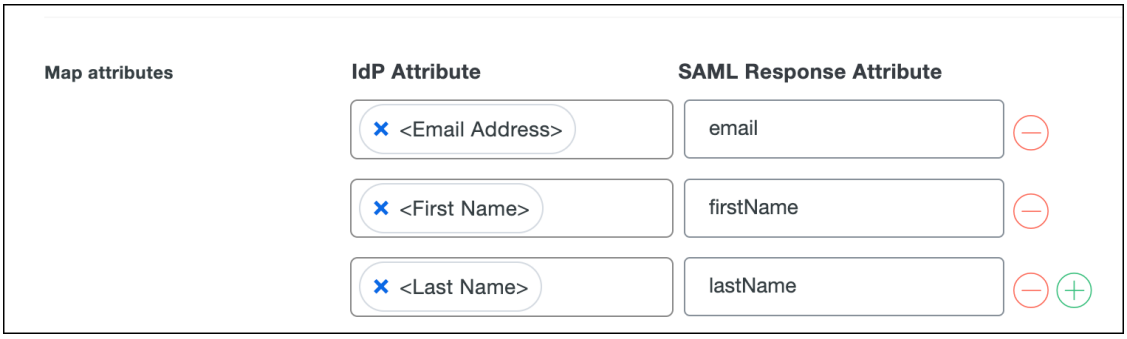
d) In the **Metadata** section:

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.
h) In the SAML Response section do the following:

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

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

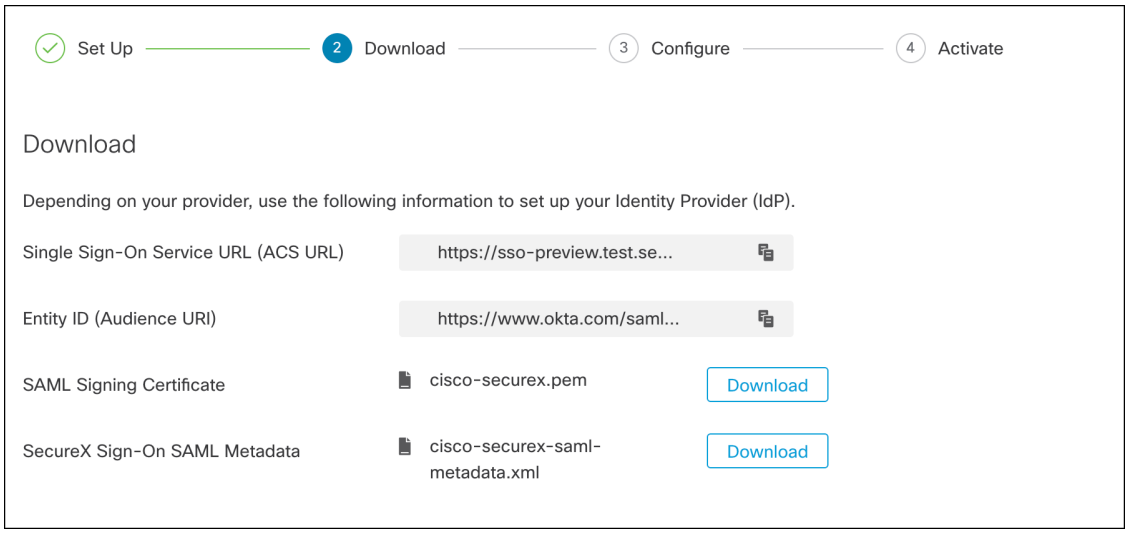


i) In the **Settings** section enter **Secure Cloud Sign On** or other value in the **Name** field.

Leave the Duo SAML settings browser window open.

Step 2 Open the Enterprise settings wizard in a new browser tab. You should be on the **Set Up** step of the **Integrate identity provider** screen (see Step 3: Exchange SAML metadata, on page 13).

a) In the **Identity Provider Name** field enter a name for your IdP (`Duo SSO`, for example).
b) In the **Single Sign On Service URL** field enter the value of the **Single Sign-On URL** that you copied from Duo.
c) In the **Entity ID** field enter the value of the **Entity ID** field you copied from Duo.
d) Click **Add File** and select the SAML signing certificate you downloaded from Duo.
e) If desired, opt-out of free Duo-based MFA service for your users.
f) Click **Next** to advance to the **Download** screen.
g) Copy and save the values of the **Single Sign-On Service URL (ACS URL)** and **Entity ID (Audience URI)** fields for later use.
h) Download the **SAML Signing Certificate** (cisco-securex.pem).



i) Click **Next** to advance to the **Configure** screen.

Step 3 Return to the Duo SAML application configuration and do the following:

a) In **Entity ID** field in the **Service Provider** section, enter the value of the **Entity ID (Audience URI)** field provided by the settings wizard in the previous step.

b) In the **Assertion Consumer Service (ACS) URL** enter the value of the **Single Sign-On Service URL (ACS URL)** field provided by the settings wizard in the previous step.

c) At the bottom of the configuration page, click **Save**.

Step 4 Return to the Enterprise settings wizard's **Configure** screen.

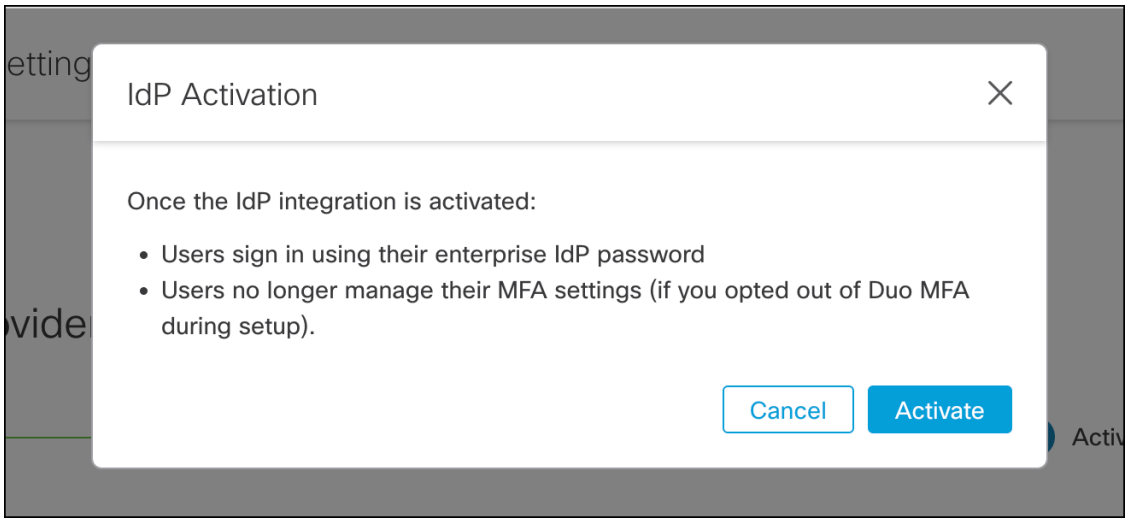
a) Copy the displayed URL and open it in a private (incognito) browser window.
The browser is redirected to the Duo SSO URL.

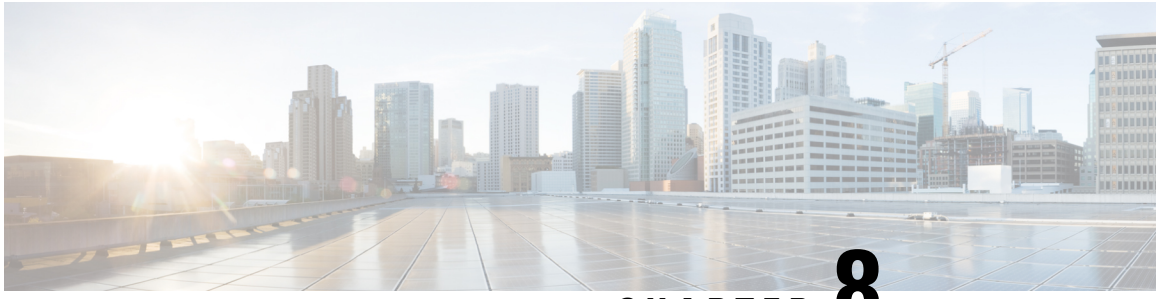
b) Sign in to Duo with an email address that matches your Step 2: Claim and verify your email domain.
The test is successful if you land back in the SecureX Application Portal.

c) Click **Next** in the settings wizard to advance to the **Activate** screen.

d) To activate the integration for your users, click **Activate my IdP**.

e) Confirm your decision in the dialog.


IdP Activation
Once the IdP integration is activated:
• Users sign in using their enterprise IdP password
• Users no longer manage their MFA settings (if you opted out of Duo MFA during setup).
Cancel
Activate



CHAPTER 8

Google

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 35
- Getting Started, on page 35

Overview

This guide explains how to create and integrate a Google Workplace SAML application and integrate it with Security Cloud Sign On.

Getting Started

Before you begin

- You must have a Google Workspace account with super administrator privileges.
- You need to have completed Step 1: Create an enterprise, on page 11 and Step 2: Claim and verify your email domain, on page 12 of the enterprise settings wizard.

Step 1 Sign in to your Google Admin console using an account with super administrator privileges.

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**.
e) Copy the **SSO URL** and **Entity ID** and download the **Certificate**.

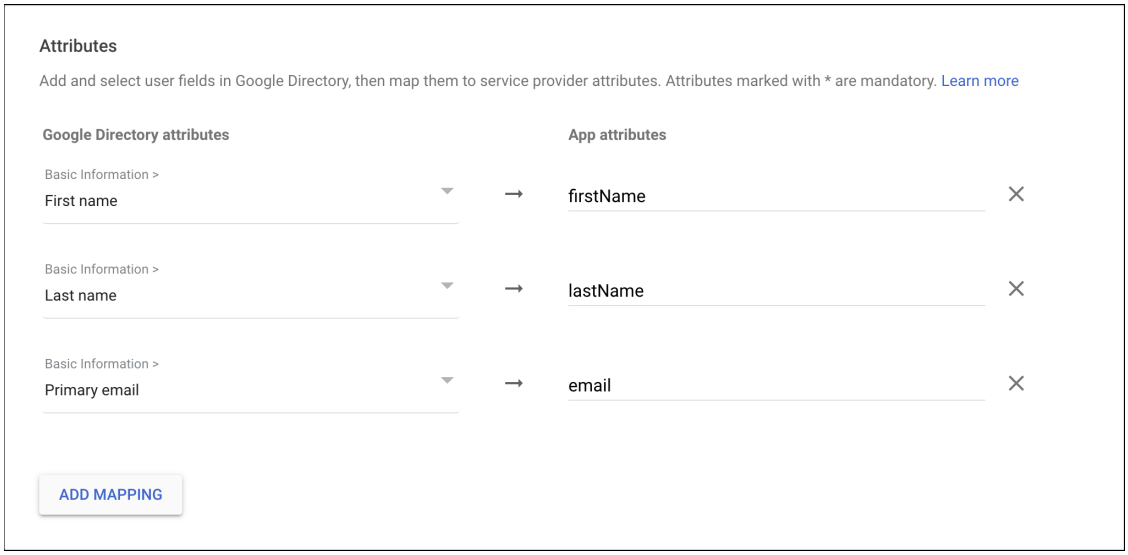
Step 2 In a new browser tab, open the Enterprise settings wizard. You should be on Step 3: Exchange SAML metadata, on page 13.

a) Enter `Google SSO` or other value for **Identity Provider (IdP) Name**.
b) In the **Single Sign-On Service URL** field enter the "SSO URL" you copied from the Google admin console.
c) In the **Entity ID (Audience URI)** field enter the "Entity ID" you copied from the Google admin console.
d) Click **Add File...** and select the certificate you downloaded from the Google admin console.
e) If desired, opt out of free Duo Multi-Factor Authentication for your users.
f) Click **Next**.
g) Copy the **Single Sign-On Service URL (ACS URL)** and **Entity ID (Audience URI)** and download the **SAML Signing Certificate**.

Step 3 Return to the Google admin console.

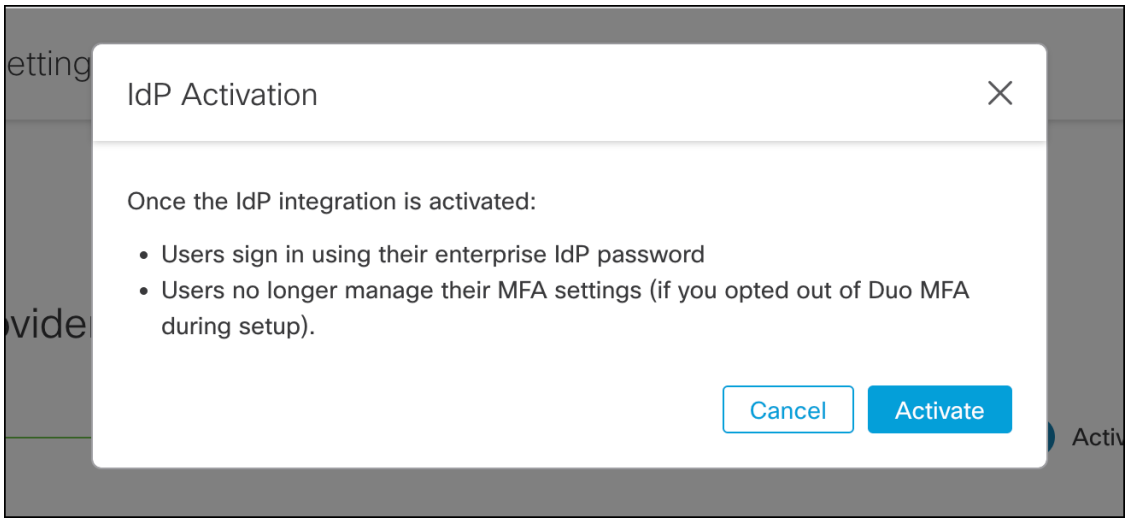
a) Click **Continue** on the **Add custom SAML app** page.
b) In the **ACS URL** field enter the "Single Sign-On Service URL (ACS URL)" you previously copied from the enterprise settings wizard.
c) For **Name ID** format select either `UNSPECIFIED` or `EMAIL`.
d) For Name ID select **Basic Information > Primary email**.
e) Click **Continue**.
f) On the **Attributes mapping** page, add the following attribute mappings:

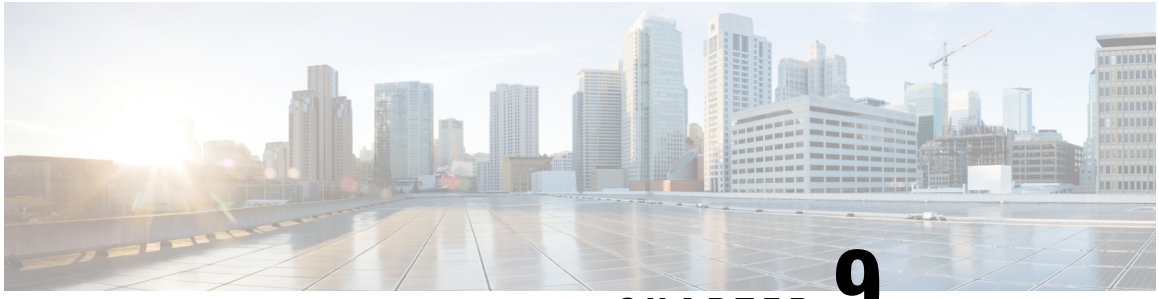
Google Directory attributes	App attributes
First name	firstName
Last name	lastName
Primary email	email



Step 4 Return to the Enterprise settings wizard's **Configure** screen.

a) Copy the displayed URL and open it in a private (incognito) browser window.
The browser is redirected to yourGoogle SSO URL.
b) Sign in to Google with an email address that matches your Step 2: Claim and verify your email domain.
The test is successful if you land back in the SecureX Application Portal.
c) Click **Next** in the settings wizard to advance to the **Activate** screen.
d) To activate the integration for your users, click **Activate my IdP**.
e) Confirm your decision in the dialog.





CHAPTER 9

Okta

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 39
- Getting started, on page 39

Overview

This guide describes how to create an Okta SAML application and integrate with Security Cloud Sign On.

Getting started

Before you begin

- You must be able to sign in to your Okta dashboard with administrator privileges.
- You need to have completed Step 1: Create an enterprise, on page 11 and Step 2: Claim and verify your email domain, on page 12 of the enterprise settings wizard.

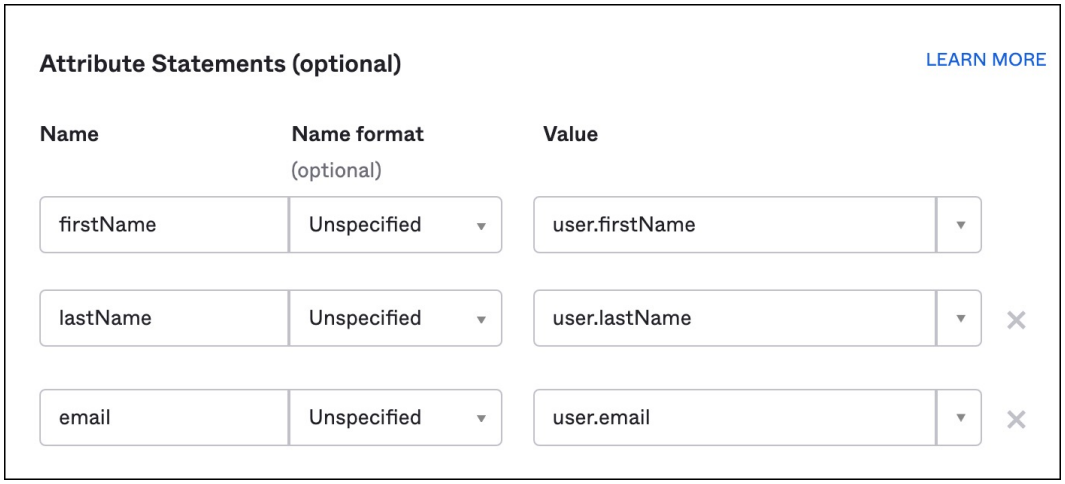
Step 1 Sign in to the Okta Admin Console and do the following:

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**.
f) On the **Configure SAML** tab.
g) In the **Single sign on URL** field enter a temporary value, such as `https://example.com/sso`. You'll replace this with the actual Security Cloud Sign On ACS URL later.

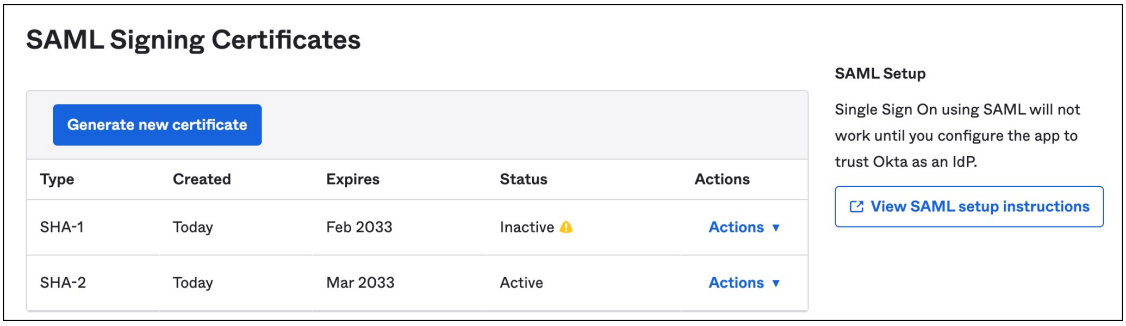
h) In the **Audience URI** field enter a temporary value, such as `https://example.com/audience`. You'll replace this with the actual Security Cloud Sign On Audience ID URI later.
i) For **Name ID format** select either **Unspecified** or **EmailAddress**.
j) For **Application username** select **Okta username**.
k) In the **Attribute Statements (optional)** section add the following attribute mappings:

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

Figure 1: Example of adding attributes



l) Click **Next**.
m) Provide feedback to Okta and click **Finish**.
n) Assign the application to a group of users.
o) On the **Sign On** tab.
p) Scroll down and click **View SAML Setup Instructions**.



q) In the page that opens copy the **Identity Provider Single Sign-On URL** and **Identity Provider Issuer** and download the **X.509 Certificate**.

Next you'll start integrating your SAML application with Security Cloud Sign On in the Enterprise settings wizard.

Step 2 Open the Enterprise settings wizard in a new browser tab. You should be at Step 3: Exchange SAML metadata, on page 13.

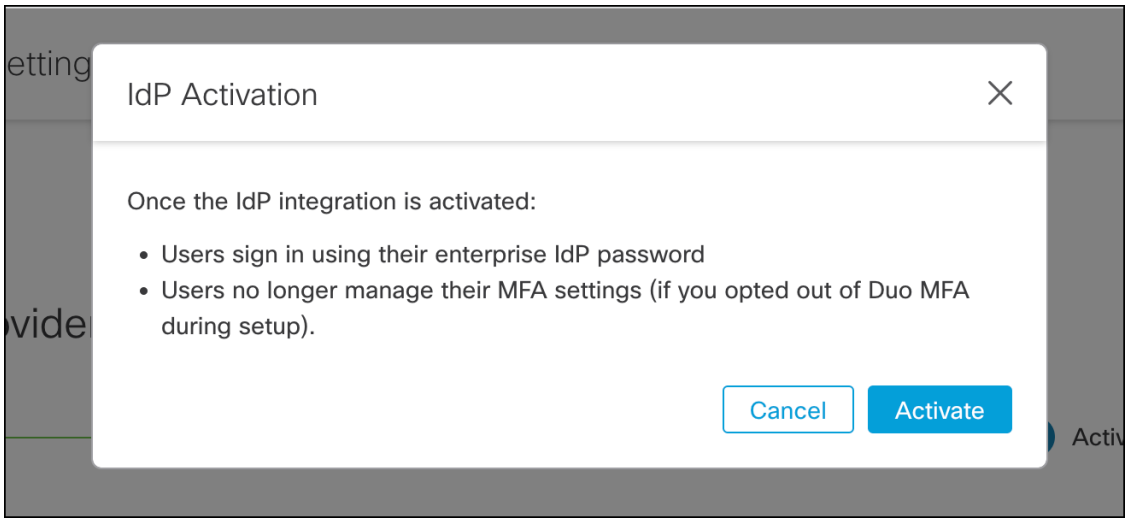
a) In the **Identity Provider Name** field enter a name for your IdP (`Okta SSO`, for example).
b) In the **Single Sign On Service URL** field enter the value of the **Identity Provider Single Sign-On URL** that you copied from Okta.
c) In the **Entity ID** field enter the value of the **Identity Provider Issuer** field you copied from Okta.
d) Click **Add File** and select the SAML signing certificate you downloaded from Okta.
e) If desired, opt-out of free Duo-based MFA service for your users.
f) Click **Next** to advance to the **Download** screen.
g) Copy and save the values of the **Single Sign-On Service URL (ACS URL)** and **Entity ID (Audience URI)** fields for use in the next step.
h) Download the **SAML Signing Certificate** (cisco-securex.pem) for use in the next step.

Step 3 Return to the SAML application settings in Okta:

a) Click the **General** tab.
b) Click **Edit** in the **SAML Settings** section.
c) Click **Next**.
d) Replace the value of **Single sign-on URL** with the value of the "Single Sign-On Service URL (ACS URL)" field provided by the enterprise settings wizard.
e) Replace the value of **Audience URI (SP Entity ID)** with the value of the "Entity ID (Audience URI)" field provided by the enterprise settings wizard.
f) Click **Show Advanced Settings** and locate the **Signature Certificate** field.
g) Click **Browse files...** and locate the Cisco SAML signing certificate you downloaded previously.
h) Click **Next**.
i) Click **Finish** to save your changes.

Step 4 Return to the Enterprise settings wizard's **Configure** screen.

a) Copy the displayed URL and open it in a private (incognito) browser window.
The browser is redirected to the Okta SSO URL.
b) Sign in to Duo with an email address that matches your Step 2: Claim and verify your email domain.
The test is successful if you land back in the SecureX Application Portal.
c) Click **Next** in the settings wizard to advance to the **Activate** screen.
d) To activate the integration for your users, click **Activate my IdP**.
e) Confirm your decision in the dialog.


IdP Activation
Once the IdP integration is activated:
• Users sign in using their enterprise IdP password
• Users no longer manage their MFA settings (if you opted out of Duo MFA during setup).
Cancel
Activate

CHAPTER 10

Ping Identity

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Overview, on page 43
- Getting Started, on page 43

Overview

This guide explains how to create a SAML application on Ping Identity and integrate it with Security Cloud Sign On.

Getting Started

Before you begin

- You must be able to sign in to the Ping Idendity management console with admin privileges.
- You need to have completed Step 1: Create an enterprise, on page 11 and Step 2: Claim and verify your email domain, on page 12 of the enterprise settings wizard.

Step 1 In your Ping Idendity console:

a) Go to **Connections** > **Applications**.

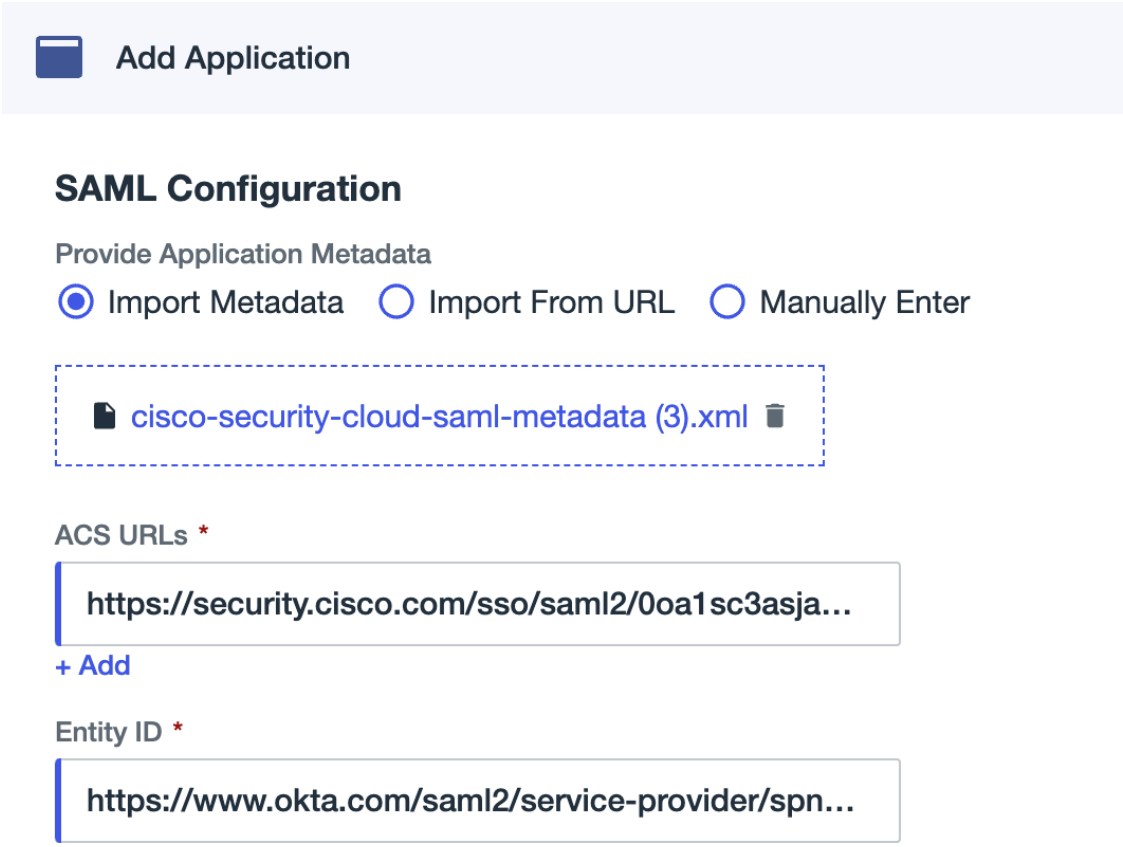
b) Click the **+** button to open the **Add Application** dialog.

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**.

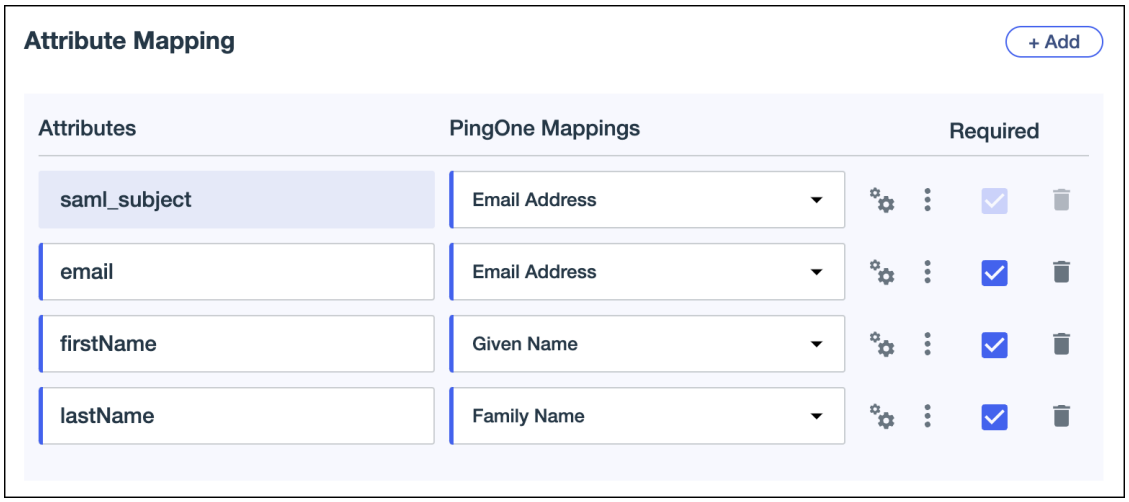
f) In the **SAML Configuration** dialog select the option to **Manually Enter** SAML metadata and enter temporary URLs for **ACS URL** and **Entity ID**. You'll replace these later with the real URLs.



g) Click **Save**.
h) Click the **Configuration** tab.
i) Click **Download Signing Certificate**.
j) Copy the values of the **Issuer ID** and **Single Signon Service** properties for use in the next step.
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.

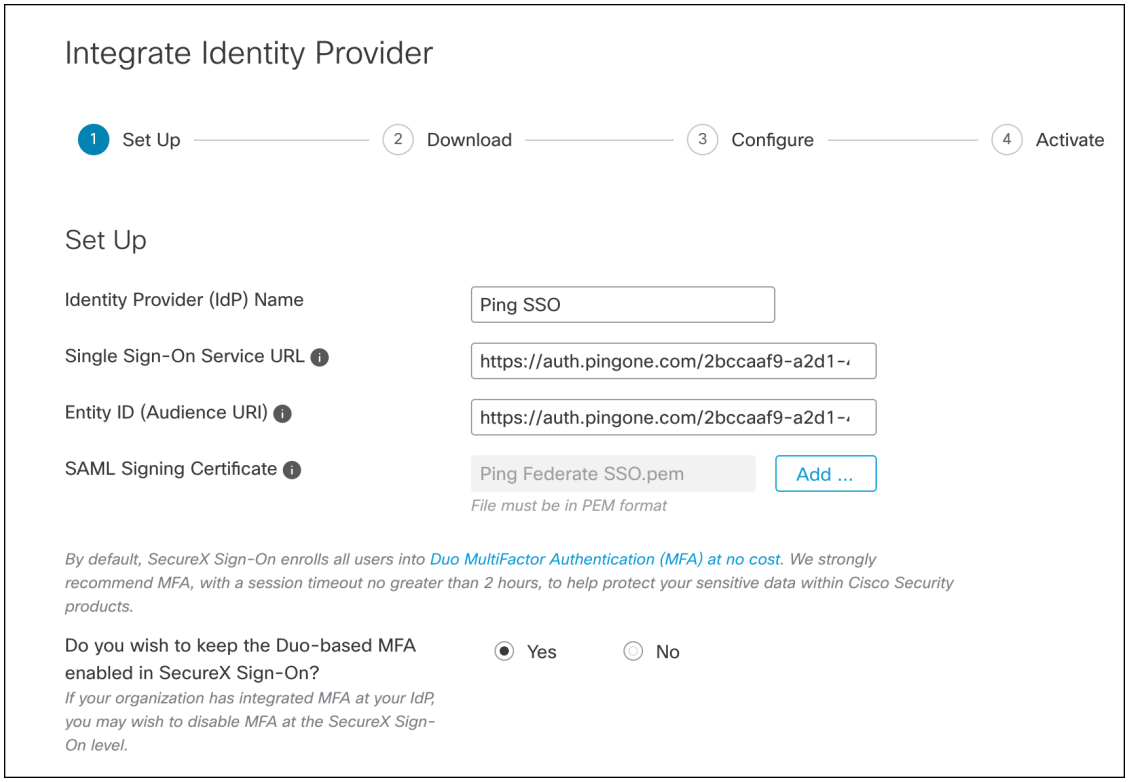
Step 2 In a new browser tab open the Enterprise settings wizard. You should be on the **Set Up** step of the **Integrate Identity Provider** screen (Step 3: Exchange SAML metadata, on page 13).

a) In the **Identity Provider (IdP) Name** field enter a name for the integration, such as `Ping SSO`

b) In the **Single Sign-On Service URL** field enter the value of the **Issuer ID** field you copied from your Ping SAML application.

c) Click **Add...** and select the Ping signing certificate you downloaded previously.

d) Opt out of Duo Multi-Factor Authentication for your users at no cost, if desired.



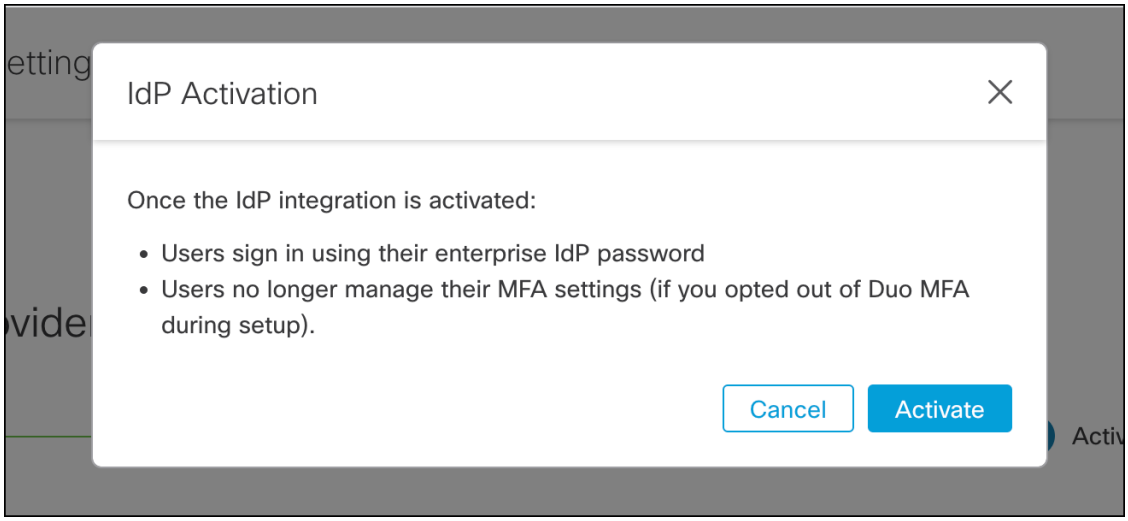
e) Click **Next** to advance to the **Download** screen.
f) On the **Download** screen, copy the values of the **Single Sign-On Service URL (ACS URL)** and **Entity ID (Audience URI)** properties, and click **Download** to download the signing certificate.

Step 3 Return to the Ping Idendity console and do the following:

a) On the **Configuration** tab click the edit (pencil) icon.
b) In the **ACS URLs** field replace the temporary URL with the "Single Sign-On Service URL (ACS URL)" you copied in the previous step.
c) In the **Entity ID** field replace the temporary URL with the "Entity ID (Audience URI)" you copied in the previous step.
d) For the **Verification Certificate** field, select the **Import** option and click **Choose File**.
e) Select the Security Cloud Sign On signing certificate you downloaded in the previous step.
f) Click **Save**.
g) Enable user access to the application by clicking the toggle at the top of the application configuration panel.

Step 4 Return to the Enterprise settings wizard's **Configure** screen.

a) Copy the displayed URL and open it in a private (incognito) browser window.
The browser is redirected to the Ping Idendity SSO page.
b) Sign in to Ping Idendity with an email address that matches your Step 2: Claim and verify your email domain.
The test is successful if you land back in the SecureX Application Portal.
c) Click **Next** in the settings wizard to advance to the **Activate** screen.
d) To activate the integration for your users, click **Activate my IdP**.
e) Confirm your decision in the dialog.



CHAPTER 11

Generic IdP instructions

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- Generic IdP instructions, on page 47
- SAML response requirements, on page 47
- SAML metadata requirements, on page 48

Generic IdP instructions

If instructions for creating a SAML application for your specific identity provider are not provided here, follow the instructions provided by your IdP. The SAML response must be configured with the proper <NameID> value and attribute name mappings. You also need to provide Security Cloud Sign On with your SAML app's Single Sign On URL and entity ID.

SAML response requirements

SAML response signed with SHA-256

The SAML response returned by the identity provider must be signed with the SHA-256 signature algorithm. Security Cloud Sign On will reject responses that are unsigned or signed with another algorithm.

SAML response attributes

The assertion in the SAML response sent by your IdP must contain the following attribute names and must be mapped to the IdP's corresponding attributes.

SAML assertion attribute name	IdP user attribute
firstName	User's first or given name.
lastName	User's lastname or surname.

SAML assertion attribute name	IdP user attribute
email	User's email. This must match the value of the **<NameID>** element in the SAML response.

For example, the following XML snippet is an example of an **<AttributeStatement>** element included in a SAML response to the Security Cloud Sign On ACL URL:

```
<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">John
      </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">Doe
      </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">jdoe@example.com
      </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

NameID element

The **<NameID>** element in the SAML response from your IdP must have a valid email address as its value, and the email must match the value of the **email** attribute in the SAML response attributes, on page 47.

The **Format** attribute of the **<NameID>** must be set to either **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** or **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

Below is an example `<NameID>` element.

```
<saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe@example.com</saml2:NameID>
```

SAML metadata requirements

The following metadata from your IdP's SAML application is required to integrate with Security Cloud Sign On.

- **Single sign-on service initial URL** – This is sometimes referred to as "SSO URL" or "Login URL". This URL can be used to start an IdP-initiated authentication to Security Cloud Sign On.
- **Entity ID URI** – The global, unique name for your IdP. This is sometimes referred to as "Issuer".

- **X.509 signing certificate** – The public key of the public/private key pair your IdP uses to sign SAML assertions.