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 1
- Getting started, on page 1

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 and Step 2: Claim and verify your email domain 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.

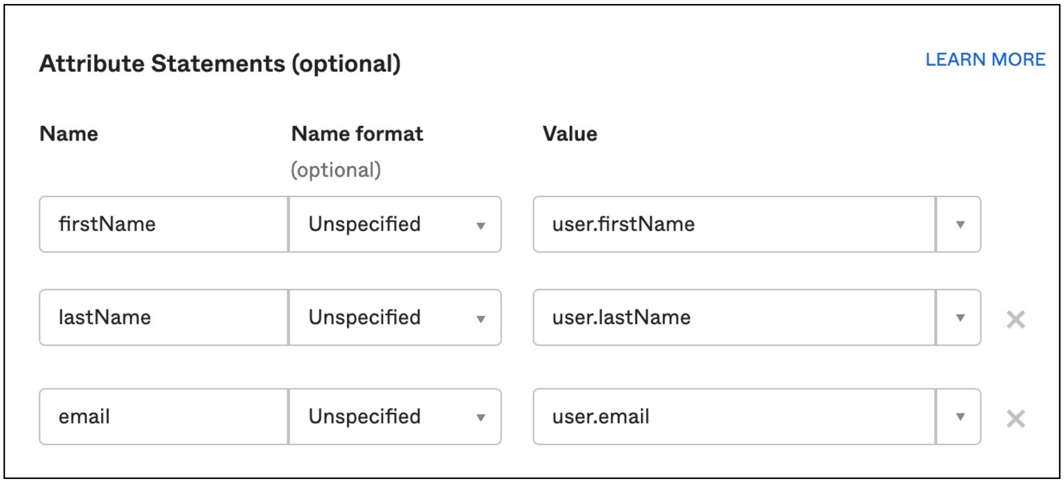
i) For **Name ID format** select either **Unspecified** or **EmailAddress**.

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



Attribute Statements (optional)

LEARN MORE

Name	Name format (optional)	Value
firstName	Unspecified ▾	user.firstName ▾
lastName	Unspecified ▾	user.lastName ▾ ✕
email	Unspecified ▾	user.email ▾ ✕

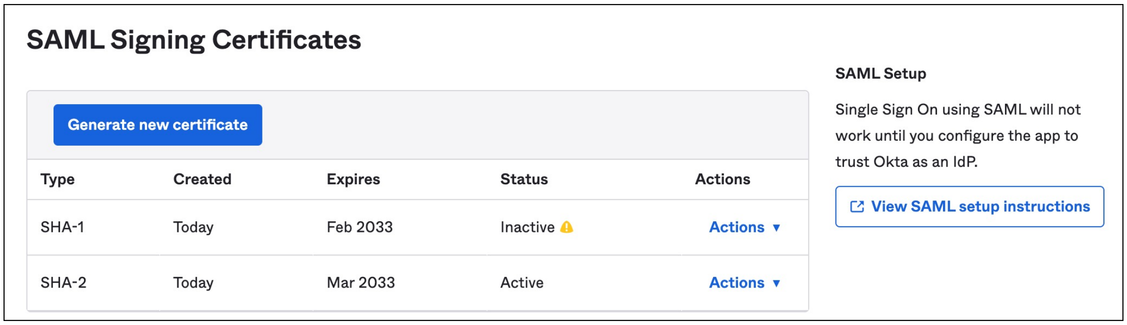
l) Click **Next**.

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**.



SAML Signing Certificates

Generate new certificate

Type	Created	Expires	Status	Actions
SHA-1	Today	Feb 2033	Inactive ⚠	Actions ▾
SHA-2	Today	Mar 2033	Active	Actions ▾

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

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.

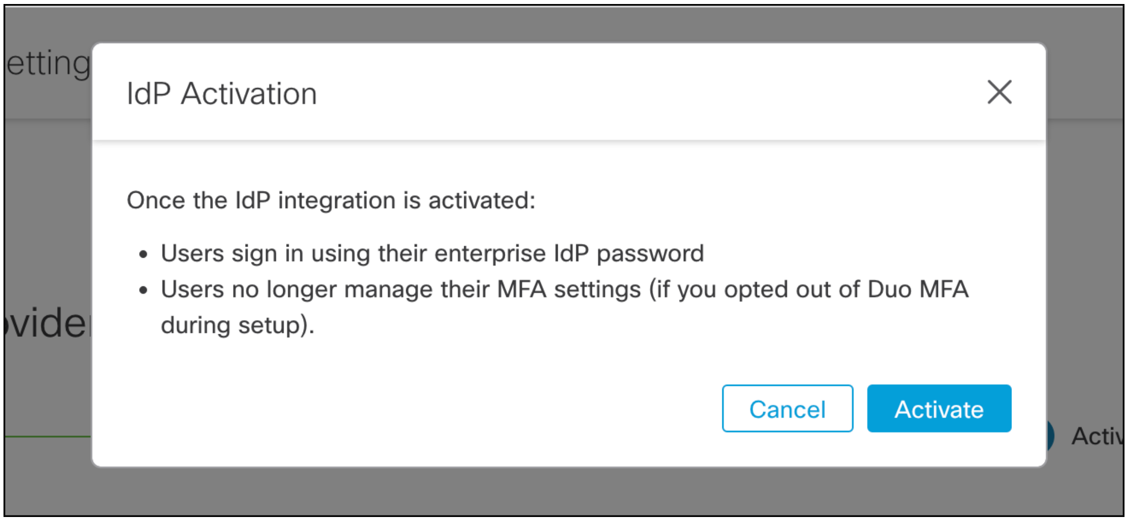
a) In the **Identity Provider Name** field enter a name for your IdP (`Okta SSO`, for example).
b) In the **Single Sign On Service URL** field enter the value of the **Identity Provider Single Sign-On URL** that you copied from Okta.
c) In the **Entity ID** field enter the value of the **Identity Provider 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 claimed 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).