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

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 and Step 2: Claim and verify your email domain 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.

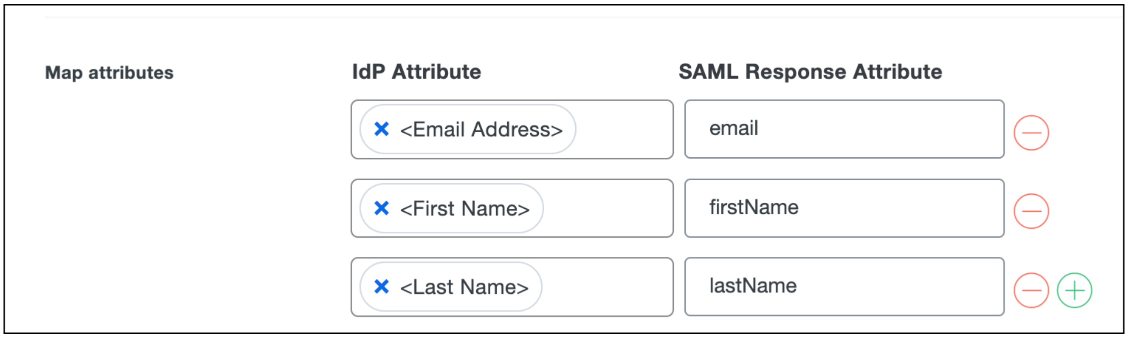
f) Copy the value of **Single Sign-On URL** and save for later use.

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



Map 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).

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.

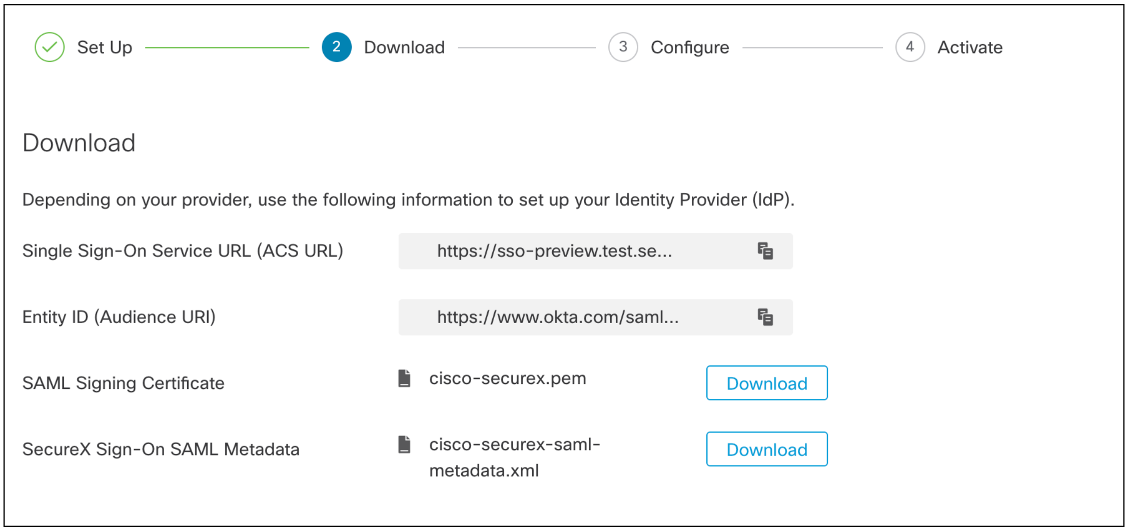
d) Click **Add File** and select the SAML signing certificate you downloaded from Duo.

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).



Download

Depending on your provider, use the following information to set up your Identity Provider (IdP).

Single Sign-On Service URL (ACS URL)	https://sso-preview.test.se...	
Entity ID (Audience URI)	https://www.okta.com/saml...	
SAML Signing Certificate	cisco-securex.pem	Download
SecureX Sign-On SAML Metadata	cisco-securex-saml-metadata.xml	Download

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.

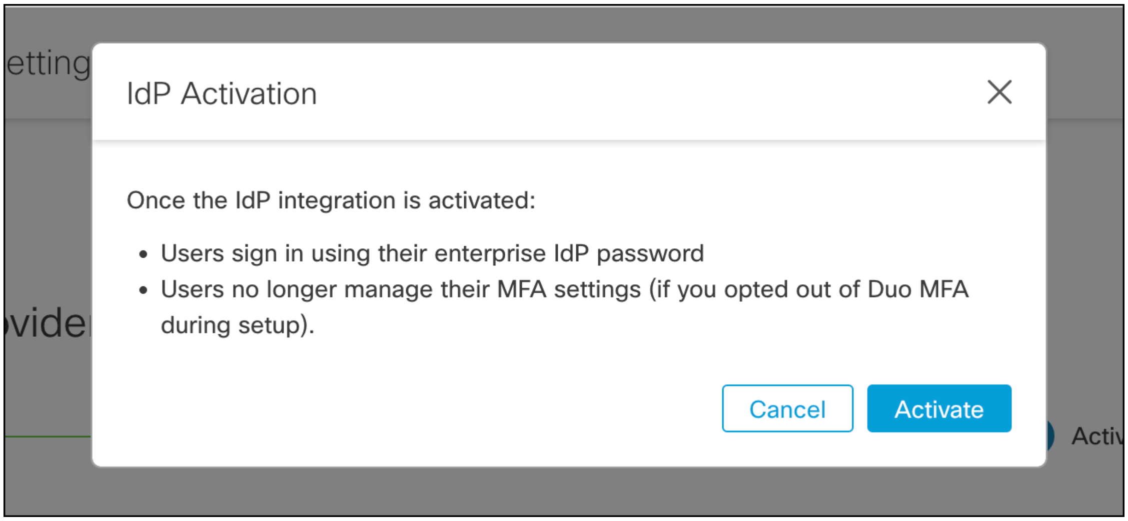
a) Copy the displayed URL and open it in a private (incognito) browser window.
The browser is redirected to the Duo SSO URL.

b) Sign in to Duo with an email address that matches your 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).