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

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

Getting started

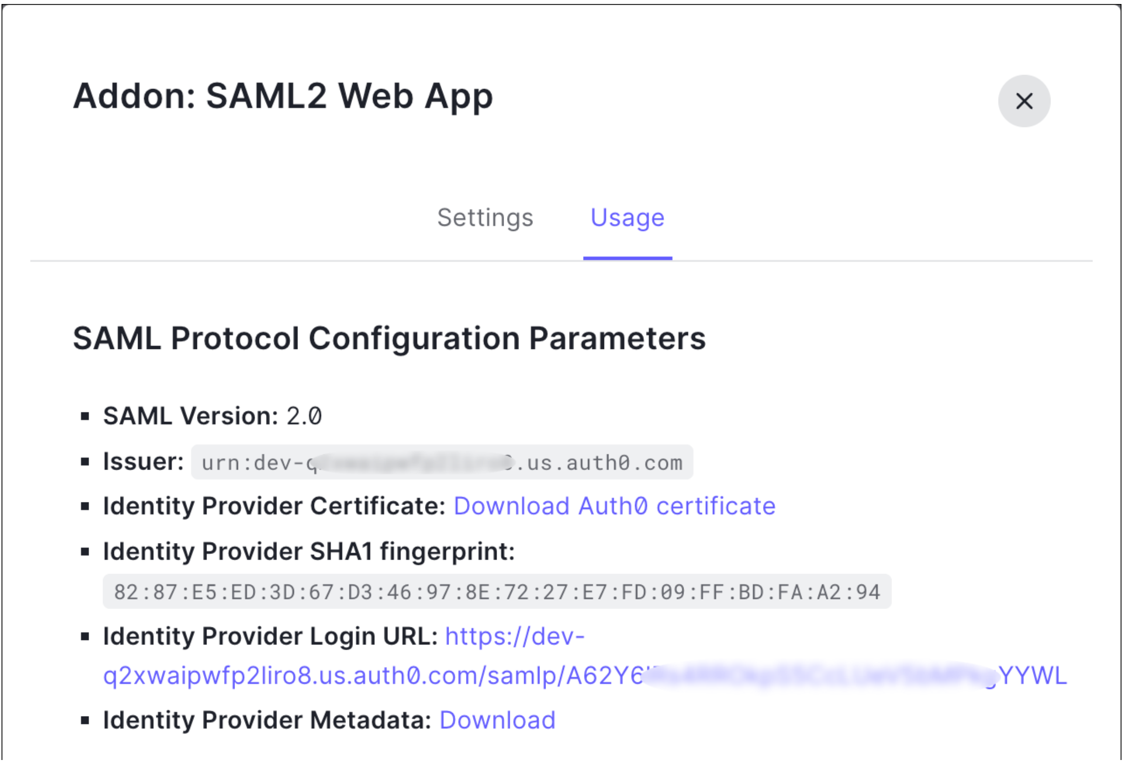
Before you begin

- 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 and Step 2: Claim and verify your email domain.

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



Addon: SAML2 Web App

SAML Protocol Configuration Parameters

- **SAML Version:** 2.0
- **Issuer:** `urn:dev-q[redacted]0.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

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:

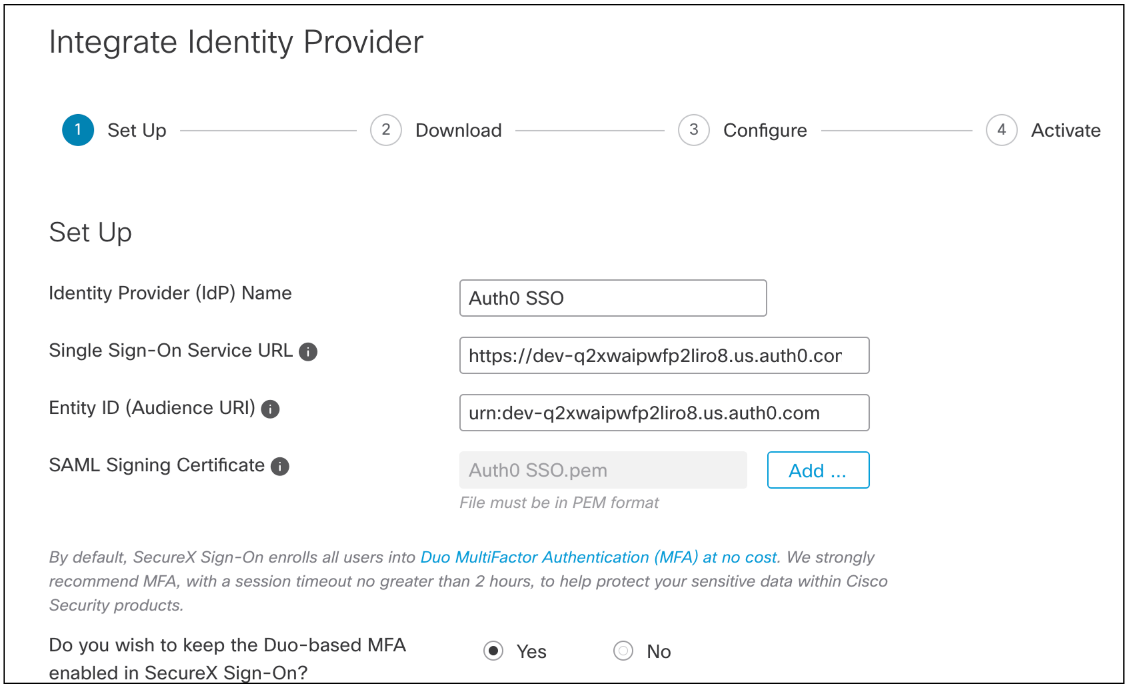
a) In the **Identity Provider Name** field enter a name for your IdP (**`Auth0 SSO`**, for example).

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.



Integrate Identity Provider

① Set Up —— ② Download —— ③ Configure —— ④ Activate

Set Up

Identity Provider (IdP) Name: Auth0 SSO

Single Sign-On Service URL ⓘ: https://dev-q2xwaipwfp2liro8.us.auth0.cor

Entity ID (Audience URI) ⓘ: urn:dev-q2xwaipwfp2liro8.us.auth0.com

SAML Signing Certificate ⓘ: Auth0 SSO.pem Add ...

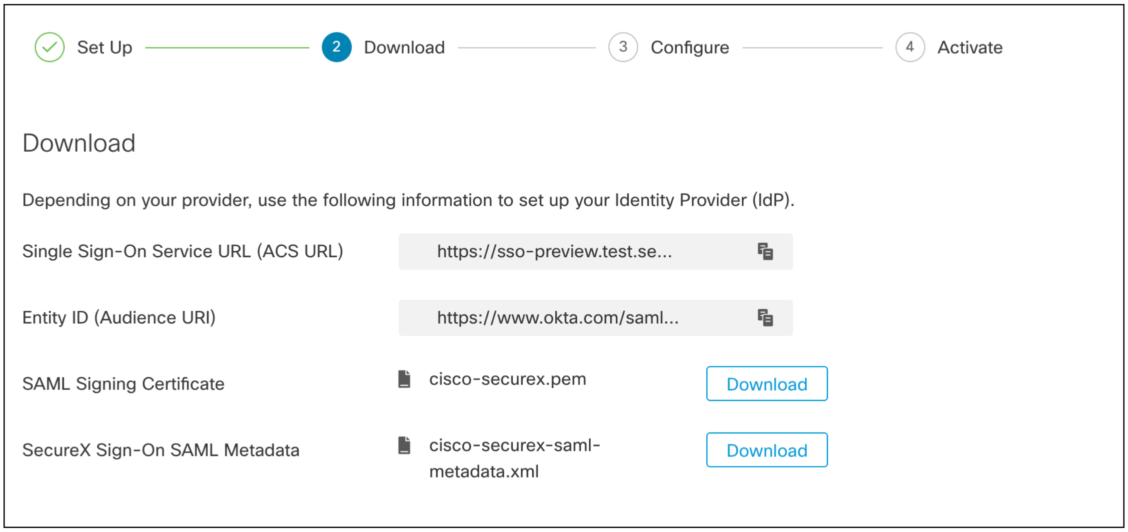
File must be in PEM format

By default, SecureX Sign-On enrolls all users into Duo MultiFactor Authentication (MFA) at no cost. We strongly recommend MFA, with a session timeout no greater than 2 hours, to help protect your sensitive data within Cisco Security products.

Do you wish to keep the Duo-based MFA enabled in SecureX Sign-On? ● Yes ○ No

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).



✓ Set Up —— ② Download —— ③ Configure —— ④ Activate

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

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

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

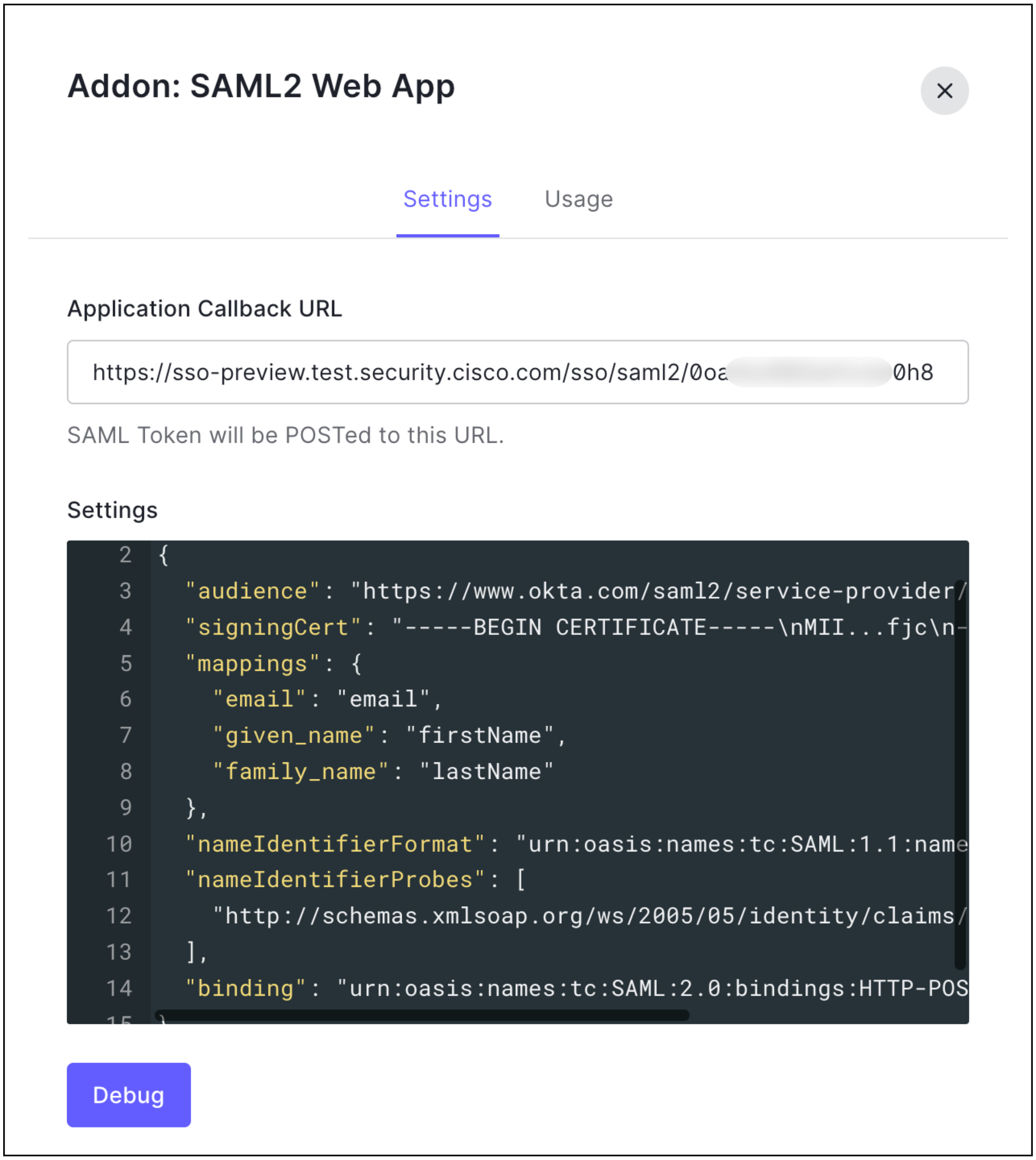
a) Click the **Settings** tab.

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"
}
```



Addon: SAML2 Web App

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
```

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.

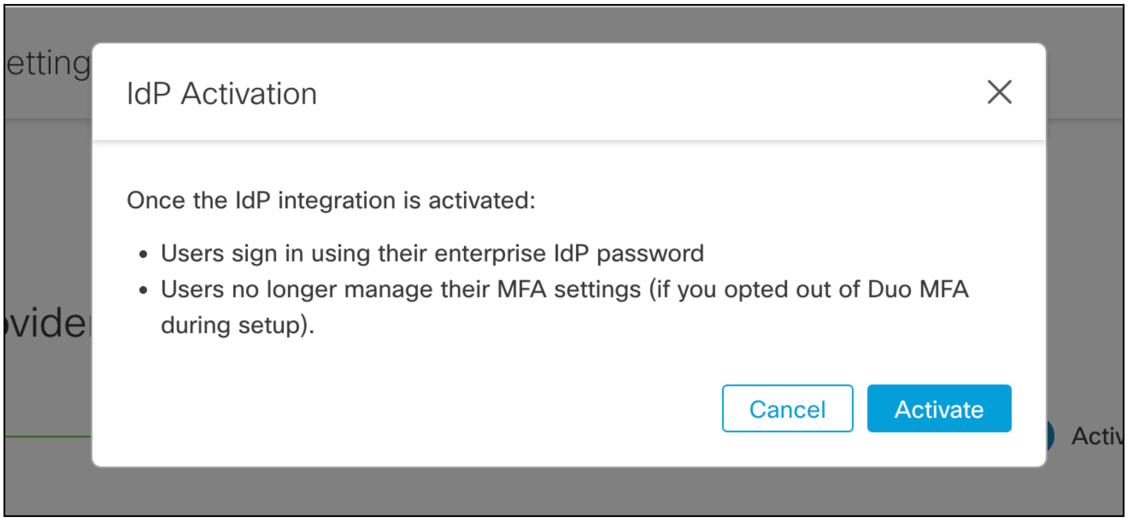
a) Copy the displayed URL and open it in a private (incognito) browser window.
The browser is redirected to the Auth0 SSO page.

b) Sign in to Auth0 with an email address that matches your 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).