



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 1](#)
- [Getting Started, on page 1](#)

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 Identity management console with admin 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

In your Ping Identity 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.

Add Application

SAML Configuration

Provide Application Metadata

Import Metadata
 Import From URL
 Manually Enter


[cisco-security-cloud-saml-metadata \(3\).xml](#)


ACS URLs *

<https://security.cisco.com/sso/saml2/0oa1sc3asja...>

+ Add

Entity ID *

<https://www.okta.com/saml2/service-provider/spn...>

- 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.

Attributes	PingOne Mappings	Required
saml_subject	Email Address	<input checked="" type="checkbox"/>
email	Email Address	<input checked="" type="checkbox"/>
firstName	Given Name	<input checked="" type="checkbox"/>
lastName	Family Name	<input checked="" type="checkbox"/>

- 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](#)).

- In the **Identity Provider (IdP) Name** field enter a name for the integration, such as **Ping SSO**
- In the **Single Sign-On Service URL** field enter the value of the **Issuer ID** field you copied from your Ping SAML application.
- Click **Add...** and select the Ping signing certificate you downloaded previously.
- Opt out of Duo Multi-Factor Authentication for your users at no cost, if desired.

Integrate Identity Provider

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

Set Up

Identity Provider (IdP) Name

Single Sign-On Service URL ⓘ

Entity ID (Audience URI) ⓘ

SAML Signing Certificate ⓘ

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

If your organization has integrated MFA at your IdP, you may wish to disable MFA at the SecureX Sign-On level.

- 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 Identity 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 Identity SSO page.
- b) Sign in to Ping Identity 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.

