



AMP FOR ENDPOINTS SSO FOR PING FEDERATE

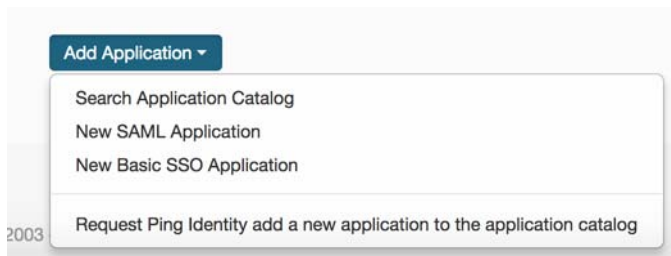
Overview

The AMP for Endpoints Single Sign-On (SSO) feature streamlines the user login process while enhancing security. This user guide will help you configure your AMP for Endpoints Console to use SSO with Ping Federate.

Set Up Ping Federate

Add an Application

1. Log in to your Ping Federate account and click on the **Applications** menu. Click **Add Application** to add a new application, and select **New SAML Application**.



Set Up Ping Federate

2. Enter an **Application Name** and the mandatory fields and click **Continue to Next Step**.

1. Application Details


Application Name

Application Description
Max 500 characters

Category

Graphics

Application Icon
For use on the dock



Max Size: 256px x 256px

NEXT: Application Configuration

Cancel

Continue to Next Step

Add Application Configuration Details

1. Enter the **Application Configuration** details. If you are unsure of some parameters, you can find them on your **SSO** page on the AMP for Endpoints Console. You will need to fill out the following fields as indicated:
 - a. For **Protocol Version**, select **SAML v2.0**.
 - b. For **Entity ID**, enter: https://auth.amp.cisco.com/auth/metadata/service_provider
 - c. For **Assertion Consumer Service (ACS)**, enter: <https://auth.amp.cisco.com/auth/acs>
 - d. Download your **Primary Verification Certificate** from the AMP for Endpoints console: <https://auth.amp.cisco.com/auth/certificate>
 - e. Under **Primary Verification Certificate**, click **upload** and upload the certificate file.

Set Up Ping Federate

f. Under **Signing Algorithm**, select **RSA_SHA256**

2. Application Configuration

[I have the SAML configuration](#)

You will need to download this SAML metadata to configure the application:

Signing Certificate [PingOne Account Origination Certificate](#)

SAML Metadata [Download](#)

Provide SAML details about the application you are connecting to:

Protocol Version ☒ SAML v 2.0 ☐ SAML v 1.1

Upload Metadata ☐ [Select File](#) [Or use URL](#)

Assertion Consumer Service (ACS) [https://auth.amp.cisco.com/auth/acs](#)

Entity ID [https://auth.amp.cisco.com/auth/meta](#)

Application URL

Single Logout Endpoint [example.com/slo.endpoint](#)

Single Logout Response Endpoint [example.com/sloresponse.endpoint](#)

Single Logout Binding Type ☐ Redirect ☐ Post

Primary Verification Certificate [sam20metadata.cer](#)
CN=iso.amp.cisco.com
Expires: 2018/11/22
[Download](#) | [Remove Certificate](#)

Secondary Verification Certificate ☐ [Choose File](#) No file chosen

Signing Algorithm [RSA_SHA256](#)

Force Re-authentication ☐

Keep the following in mind when creating your connection:

1. Both SP- and IdP-Initiated SSO are allowed
2. Map SAML_SUBJECT in your attribute contract, plus any attributes (configure them in PingOne later)
3. Allow outbound POST or redirect
4. Allow outbound POST

NEXT: SSO Attribute Mapping

[Cancel](#) [Back](#) [Continue to Next Step](#)

2. Click **Continue to Next Step**. On the next screen, click **Save & Publish**.

Review Settings and Download SAML IdP Metadata

After saving the application, review and confirm that all values are filled out correctly. You can now download the **SAML IdP metadata** that will be uploaded on the AMP for Endpoints SSO setup page in step 4 below.

Icon ⓘ □

Name ⓘ Cisco NAM (AUTH)

Description ⓘ NAM console.amp.cisco.com

Category ⓘ Engineering

Connection ID

(Optional) Click the link below to invite this SaaS Application's Administrator to register their SaaS Application with PingOne.

[Invite SAAS Admin](#)

These parameters may be needed to configure your connection

saasid

idpid

Protocol Version SAML v 2.0

ACS URL https://auth.amp.cisco.com/auth/acs

entityId https://auth.amp.cisco.com/auth/metadata/service_provider

Initiate Single Sign-On (SSO) URL ⓘ

Single Sign-On (SSO) Relay State ⓘ

Signing Certificate [Download](#)

SAML Metadata [Download](#) ←

Single Logout Endpoint

Single Logout Response Endpoint

Signing Algorithm RSA_SHA256

Force Re-authentication ⓘ false

Configure SSO on the AMP for Endpoints Console

To enable SSO for your business, do the following on your AMP for Endpoints Console:

1. Log in to your administrator account.
2. Go to **Accounts > Business**.
3. Click **Configure Single Sign-On**.

Features

Remote File Fetch	On
3rd Party API Access	Configure API Credentials View API Documentation
Single Sign-On	Disabled Configure Single Sign-On

4. Under **Identity Provider Settings** on the **Single Sign-On** page, upload the metadata file you previously downloaded from Ping Federate.

Identity Provider Settings

Metadata URL Metadata File Upload

Upload the Identity Provider metadata file.

SAML Metadata File

No file selected Browse

Save SAML Configuration

5. Click **Save SAML Configuration**
6. Click **Test** to verify the connection to the service provider. If connection is successful, a confirmation message will appear on the SSO setup page. If the test fails, verify that your settings are correct. If it continues to fail, [contact Support](#).
7. Click **Enable SAML Authentication** to complete the setup. Once SSO is enabled, you can view the settings on the SSO page.