AMP FOR ENDPOINTS SSO FOR OKTA

Overview

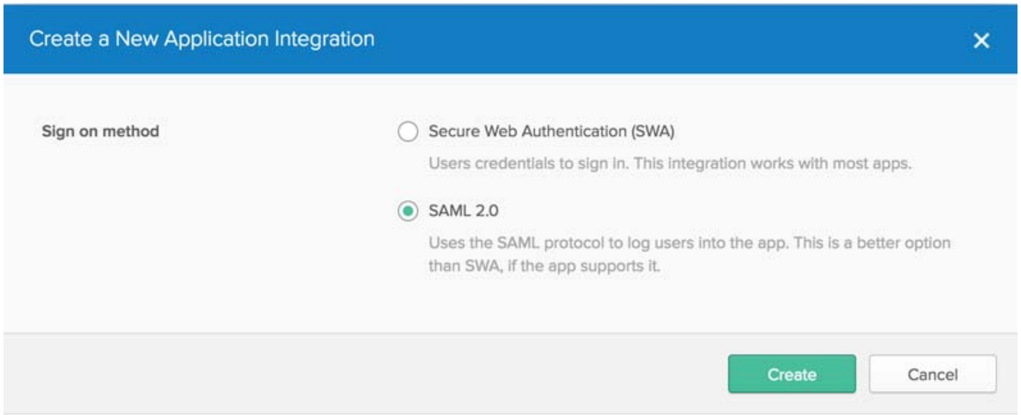
The AMP for Endpoints Single Sign-On (SSO) feature streamlines the user login process while enhancing security. This user guide will help you configure your AMP for Endpoints Console to use SSO with Okta.

Set Up Okta

The first step in configuring an application to support SAML-based SSO from Okta is to set up an application in Okta. This requires configuring Okta with the details of your application (the SAML service provider).

To set up a SAML application in Okta, do the following:

1. Log in to your Okta organization as a user with administrative privileges.
2. Click the **Admin** button.
3. Click the **Add Applications** shortcut.
4. Click the **Create New App** button.
5. In the dialog, select **SAML 2.0** then click the **Create** button.



Create a New Application Integration

Sign on method

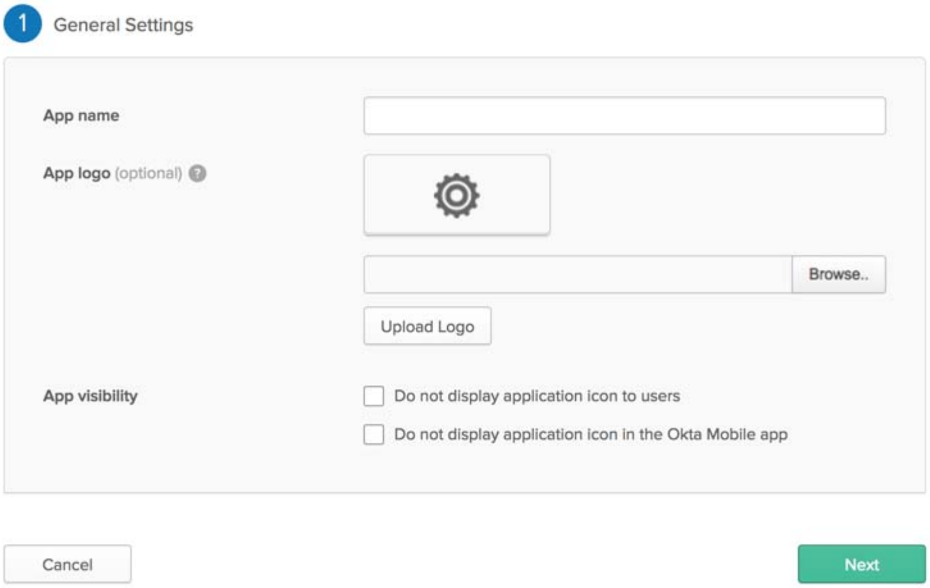
○ Secure Web Authentication (SWA)

Users credentials to sign in. This integration works with most apps.

● SAML 2.0

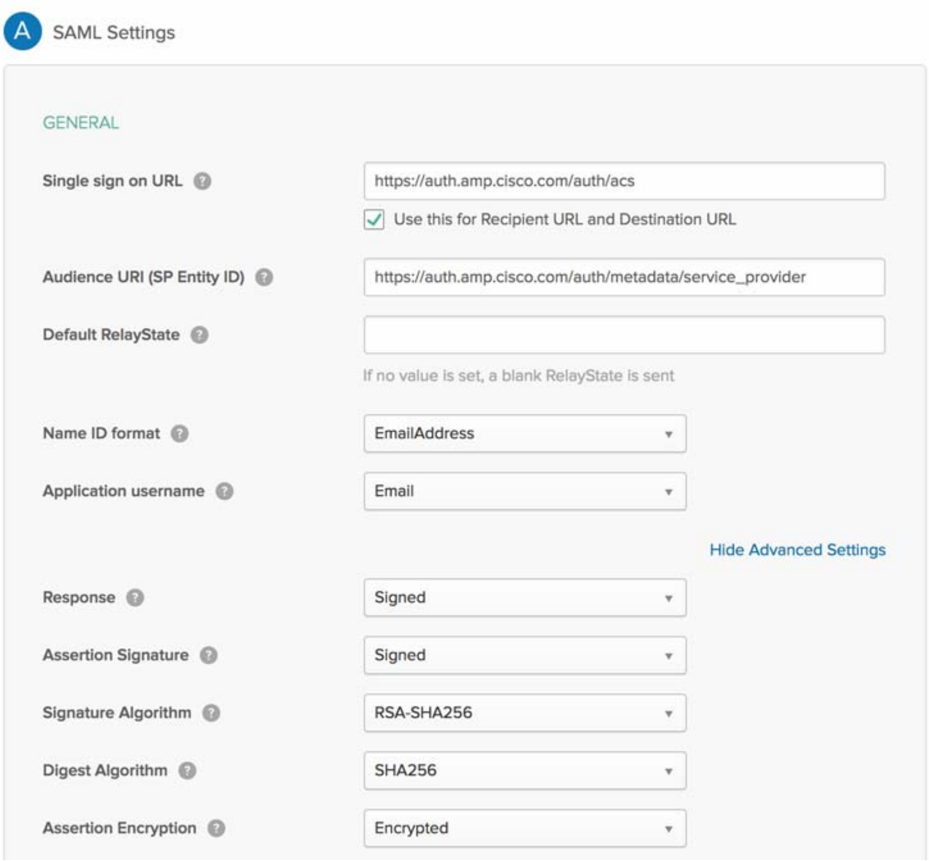
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

6. In **General Settings** under **App name** enter a name like “AMP for Endpoints” or whatever you want to assign as the name then click **Next**.


1
General Settings
App name
App logo (optional)
Browse..
Upload Logo
App visibility
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile app
Cancel
Next

7. In **Configure SAML**, do the following:

a. Paste the following URL into the **Single sign on URL** and **Audience URI (SP Entity ID)** fields: https://auth.amp.cisco.com/auth/metadata/service_provider



A SAML Settings

GENERAL

Single sign on URL: https://auth.amp.cisco.com/auth/acs

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): https://auth.amp.cisco.com/auth/metadata/service_provider

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: EmailAddress

Application username: Email

Hide Advanced Settings

Response: Signed

Assertion Signature: Signed

Signature Algorithm: RSA-SHA256

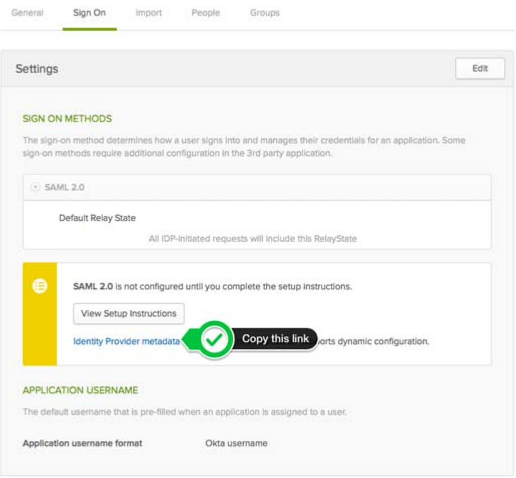
Digest Algorithm: SHA256

Assertion Encryption: Encrypted

b. Click **Next**

8. Under **Feedback** enter the appropriate information, then click **Finish**.

9. You will now see the **Sign On** section of your newly created application. Click the **Identity Provider metadata** link to download the metadata file.You will need to upload this file to the AMP for Endpoints Console later



Settings

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

○ SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

SAML 2.0 is not configured until you complete the setup instructions.

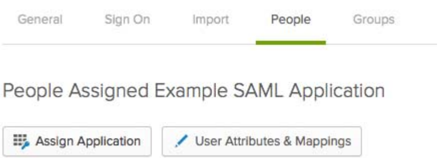
Identity Provider metadata ...orts dynamic configuration.

APPLICATION USERNAME

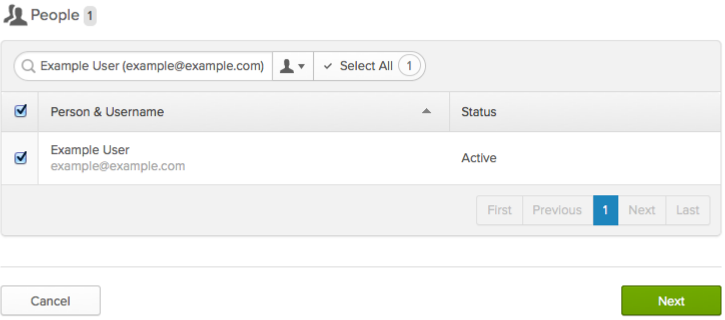
The default username that is pre-filled when an application is assigned to a user.

Application username format: Okta username

10. Right-click on the **People** section of the application and select **Open Link In New Tab** (so you can come back to the **Sign On** section later). In the new tab, click on **Assign Application**.


General
Sign On
Import
People
Groups
People Assigned Example SAML Application
Assign Application
User Attributes & Mappings

11. A dialog named **Assign Application** will open. Type your username into the search box. Select the checkbox next to your username, then click **Next.** Please note the email address should be a valid email that has an AMP for Endpoints account or is mapped correctly to an AMP for Endpoints account email address. Once users are assigned, save and click **Done**.



Example User (example@example.com)

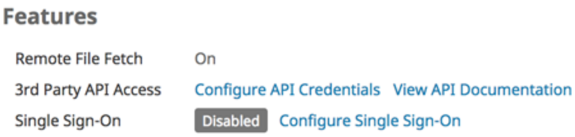
☑	Person & Username	Status
☑	Example User example@example.com	Active

You are now ready to configure SAML in your application. The information in the tab you opened in **step #10** contains the information that you'll need to configure SAML in your application. On AMP for Endpoints console, enter the SSO metadata URL or upload the metadata file, save and then enable **SAML Authentication**.

Configure SSO on the AMP for Endpoints Console

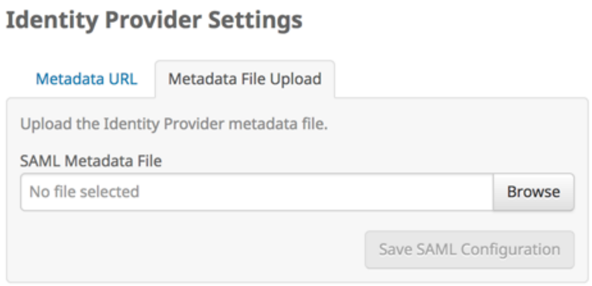
To enable SSO for your business, do the following:

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



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 Okta.



Identity Provider Settings

Upload the Identity Provider metadata file.

SAML Metadata File: No file selected

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 setup. Once SSO is enabled, you can view the settings on the SSO page.