

Okta Cookbook

This cookbook is to configure Okta for passive authentication in SAML protocol.

Note: WS-Fed for Office 365 and Okta pair is not supported.

Prerequisites

- Ensure that you download the deployment guide for Okta with Office 365:
https://support.okta.com/help/Documentation/Knowledge_Article/Office365-Deployment-Guide

Complete the following steps to configure Okta:

Step 1: Creating an application and download the metadata for Okta

Step 2: Configuring Okta in MobileIron Access

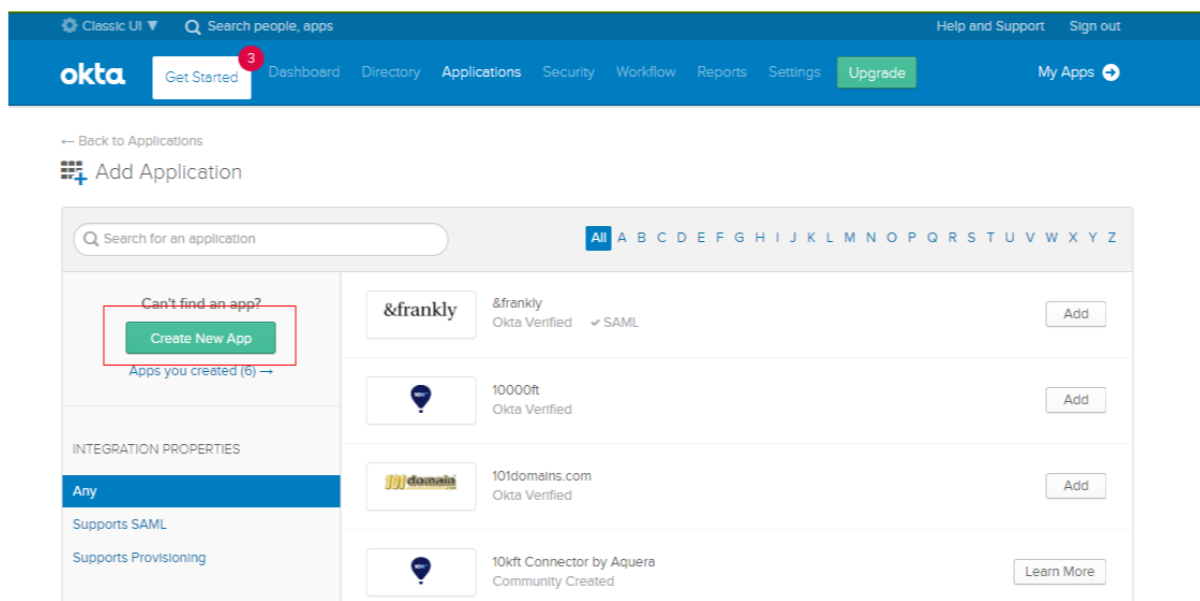
Step 3: Updating the IDP configuration

Step 1: Creating an application and downloading the metadata file for Okta

Note: If you have already created an application, skip to **Step 12** in the following procedure.

Procedure

1. Login to Okta with admin credentials.
2. Click **Applications** > **Add Application** > **Create New App**.



3. Select **SAML 2.0** and click **Create**.

Create a New Application Integration ✕

Platform

Sign on method

Secure Web Authentication (SWA)
Uses 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.


OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

4. On the **General Settings** tab, enter the **App name** for the application and click **Next**.

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name

App logo (optional) 

App visibility

Do not display application icon to users

Do not display application icon in the Okta Mobile app

5. On the **Configure SAML** tab, enter the configuration values.

A SAML Settings

GENERAL

Single sign on URL ?

Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

SAML Settings	Values
Single sign on URL	Extract the single sign on URL from the SP metadata file. Select the check box for Use this for Recipient URL and destination URL .
Audience URI (SP Entity ID)	Enter the above single sign on URL.
Default RelayState	Enter the above single sign on URL. If no value is set, a blank relay is sent.
Name ID format	Persistent
Application username	Okta username

6. Click **Show Advanced Settings**.

[Hide Advanced Settings](#)

Response ?

Assertion Signature ?

Signature Algorithm ?

Digest Algorithm ?

Assertion Encryption ?

Enable Single Logout ? Allow application to initiate Single Logout

Authentication context class ?

Honor Force Authentication ?

SAML Issuer ID ?

Settings	Values
Response	Unsigned
Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
Enable Single Logout	Deselect the check box for Allow application to initiate Single Logout
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/\$(org.externalKey)

(Optional) Add the screen, ATTRIBUTE STATEMENTS.

- user.email for IDPEmail
- UPN

7. Configure the **Feedback Settings** and click **Finish**.

- Are you a customer partner: Select I'm an Okta customer adding an internal app.
- Select the This is an internal app that we have created check box.

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

Why are you asking me this?
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

Previous Finish

8. Click **Directory > People > Add Person**. The **Add Person** screen displays. Create a new user.

Add Person

User type ● User

First name

Last name

Username

Primary email

Secondary email (optional)

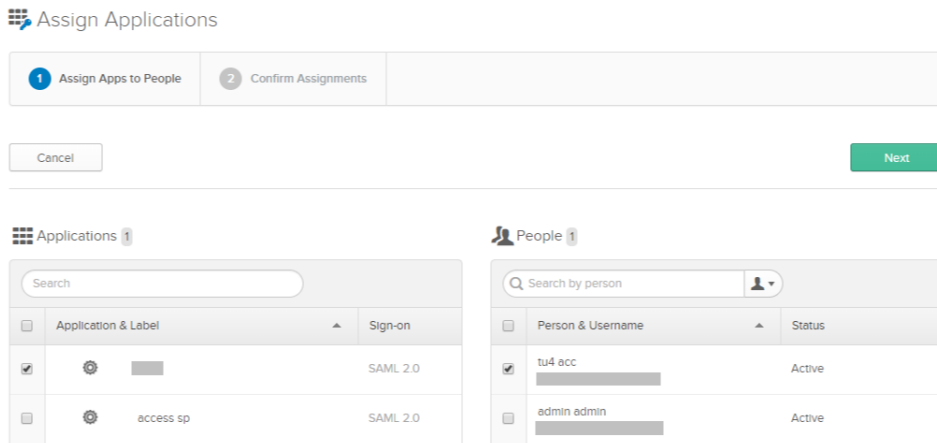
Groups (optional) You haven't added any groups

Password ● Set by user

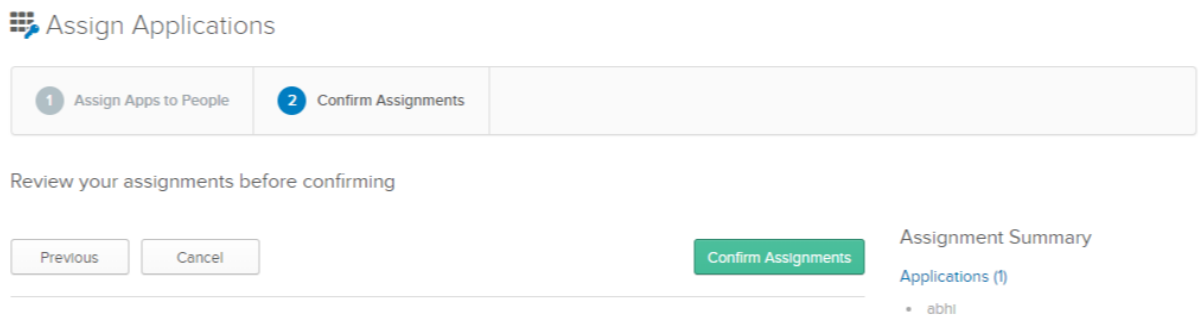
Send user activation email now ●

Save Save and Add Another Cancel

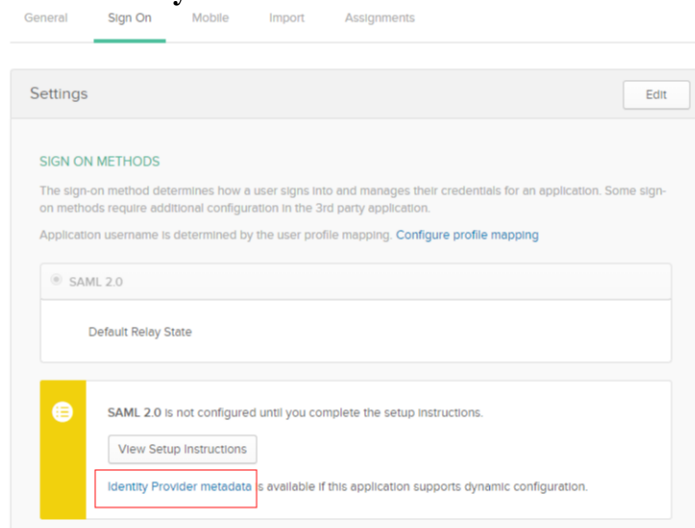
9. On the **Applications** tab, click **Assign Application**.
10. Select the Application and the User that you have created and click **Next**.



11. Click **Confirm Assignments**.



12. Click **Applications**. Select the application you created.
13. Click **Sign On** tab.
14. Click **Identity Provider metadata** to download the metadata file for Okta.

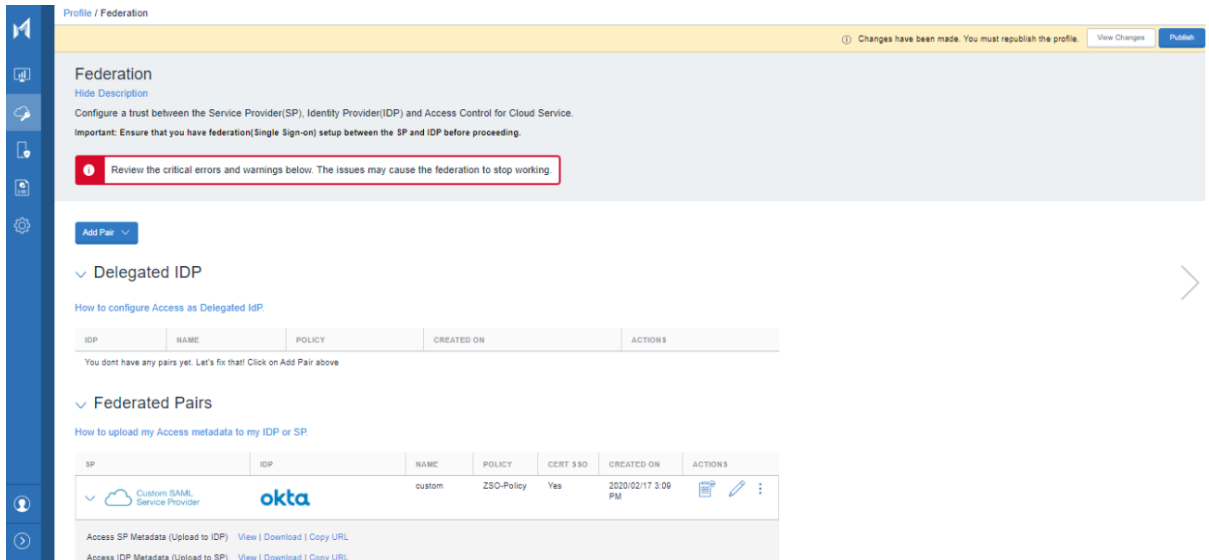


Step 2: Configuring Okta in MobileIron Access

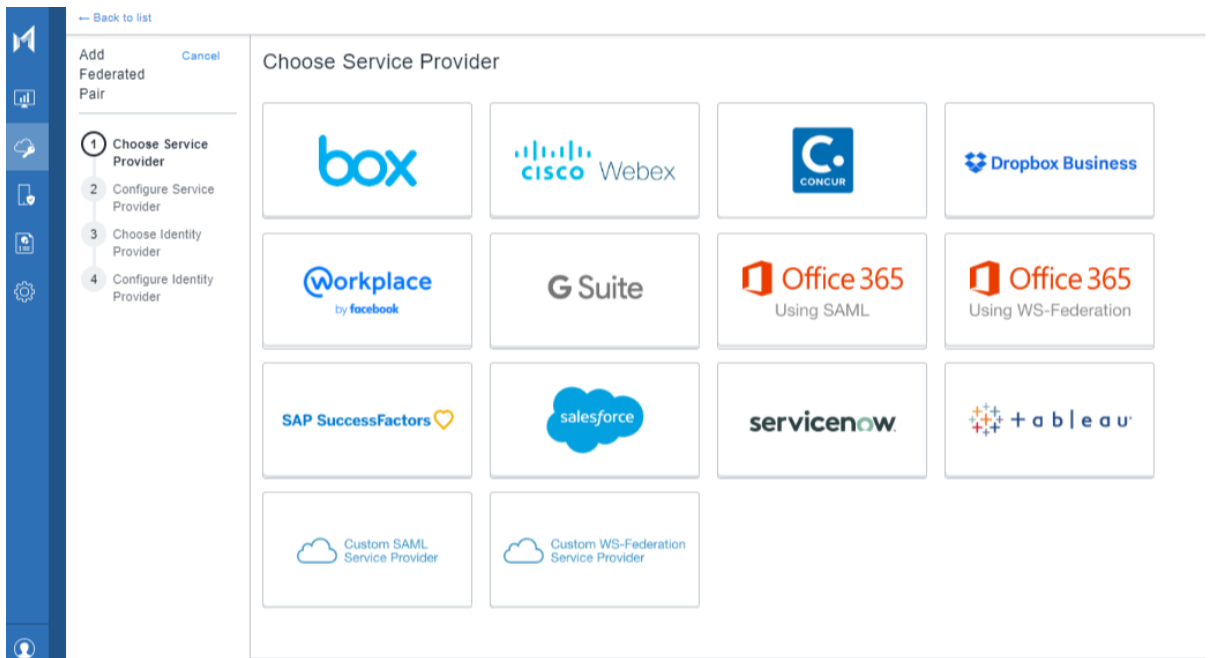
You must create the federated pair in MobileIron Access.

Procedure

1. Login to MobileIron Access administrative portal with admin credentials.
2. Click **Profile > Federation**.



3. Click **Add Pair > Federated Pair**. The Choose Service Provider window appears.



4. Select the appropriate service provider from the catalog and click **Next** to configure the desired service provider.




3. **Metadata URL:** In the Okta admin portal, on the **Applications > Sign On** tab, click **Identity Provider Metadata**. This file opens in a new tab and the URL of this page forms the Metadata URL for Okta.

For example: <https://dev-712184.oktapreview.com/app/exkpstisjbzZN6o0h7/sso/saml/metadata>

8. Enter the Identity Provider Settings.
 1. Select the **ECP backend Type** from the drop-down list.
 - WS-Trust 1.3
 - WS_Trust 2005
 - SAML 2.0
 2. Enter the **Federated Domain:** <domain_name>
9. Enter the **Active Logon Settings:** Original IDP Active Logon URL: <https://<okta>.oktapreview.com/app/office365/exkc1nvw91H9nuyFX0h7/sso/wsfed/active>
10. Click **Done**.
11. On **Profile > Federation**, download the following files:
 - **Access SP Metadata (Upload to IDP)**
 - **Access IDP Metadata (Upload to SP)**

▼ Federated Pairs

How to upload my Access metadata to my IDP or SP.

SP	IDP	NAME	POLICY	CERT BBO	CREATED ON	ACTIONS
▼ Custom SAML Service Provider	okta	custom	ZSO-Policy	Yes	2020/02/17 3:09 PM	  
Access SP Metadata (Upload to IDP) View Download Copy URL						
Access IDP Metadata (Upload to SP) View Download Copy URL						

Step 3: Updating the IDP configuration

You must configure the IDP settings with the SP proxy settings to build a trust relationship.

Prerequisites

Extract the Entity ID from the **Access SP Metadata (Upload to IDP)** downloaded after creating the federated pair.

Procedure

1. Login to Okta administrative portal with admin credentials.
2. On the **Application** tab, select the application that you created.
3. On the **General tab > SAML Settings**. Click **Edit**.
4. On **General Settings** tab, click **Next**.
5. Enter the following details extracted from the **Access SP Metadata (Upload to IDP)**:

- **Single sign on URL:** Entity ID of the **Access SP Metadata (Upload to IDP)**
- **Audience URI:** Same as Single sign on URL
- **Name ID Format:** Persistent
- **Application username:** Okta username

6. Click **Next > Finish**.

Related Topics

The following topics are available in the MobileIron Access Guide. See [Access Product Documentation](#).

- See "Zero Sign-on with MobileIron Access" in the *MobileIron Access Guide*.
- See "Configuring LDAP in MobileIron Cloud for session revocation" and "Configuring LDAP in MobileIron Core for session revocation" in the *MobileIron Access Guide*.