MobileIron Access Cookbook

Access with Salesforce and Okta

Revised: April 05, 2018

Contents

Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Salesforce is federated with an identity provider such as Okta for authentication. Users authenticate to Okta as an identity provider and obtain a SAML token for accessing applications in a cloud environment, such as Salesforce.
This guide serves as step-by-step configuration manual for users using Okta as an authentication provider with Salesforce in a cloud environment.

Prerequisites

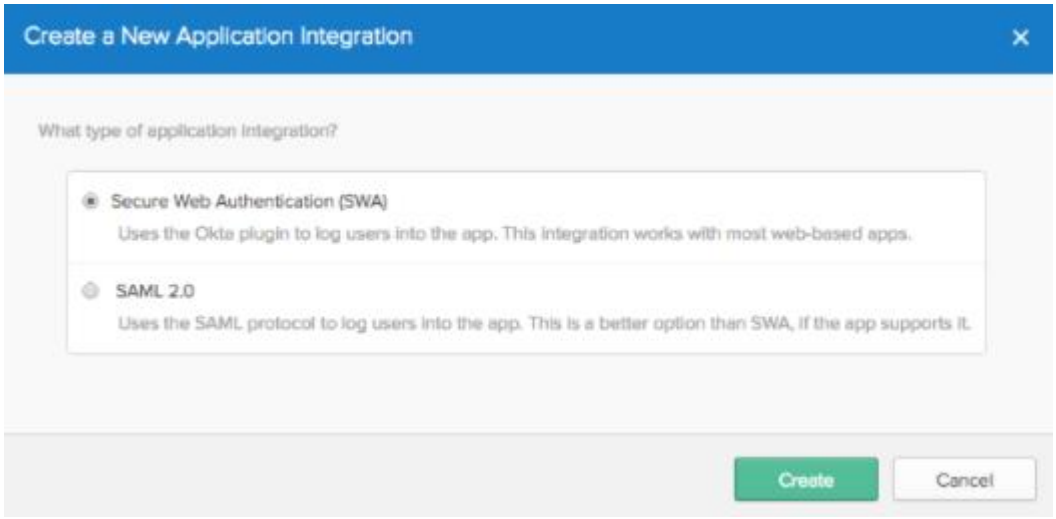
You must perform the following steps before you configure the service provider and identity provider with Access:

- Verify that you refer the following link before configuring Salesforce and Okta.
  https://developer.salesforce.com/signup
- Verify that you have the credentials for Okta admin account.
  http://developer.okta.com
  Note: After signing up, you will receive an activation link on the registered email. Save the activation URL. The URL might be similar to
  dev-931016-admin.oktapreview.com

- Verify that you have the metadata files for Okta.

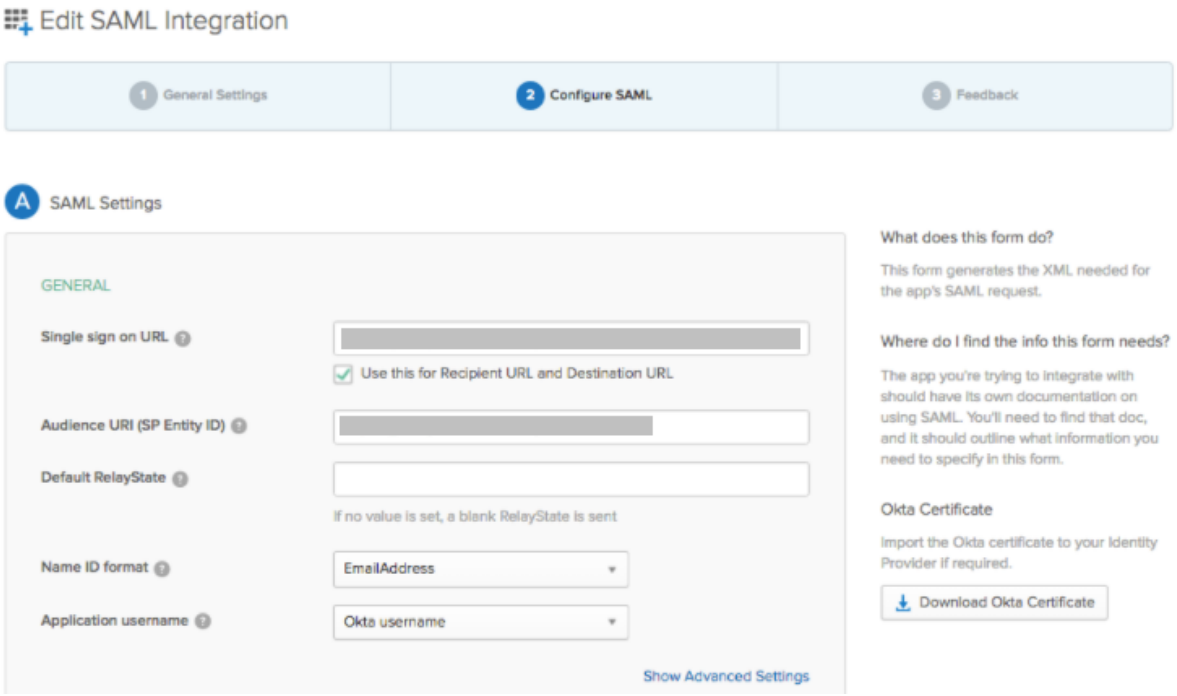
  1. Login to Okta with sign-in URL from the activation email.
  2. Click **Applications** > **Add application** > **Create New App** > Select **SAML 2.0** as type of application integration > **Create**.

Note: The following screen is available in classic mode of Okta. In Developer mode, SAML integration screen is not visible.

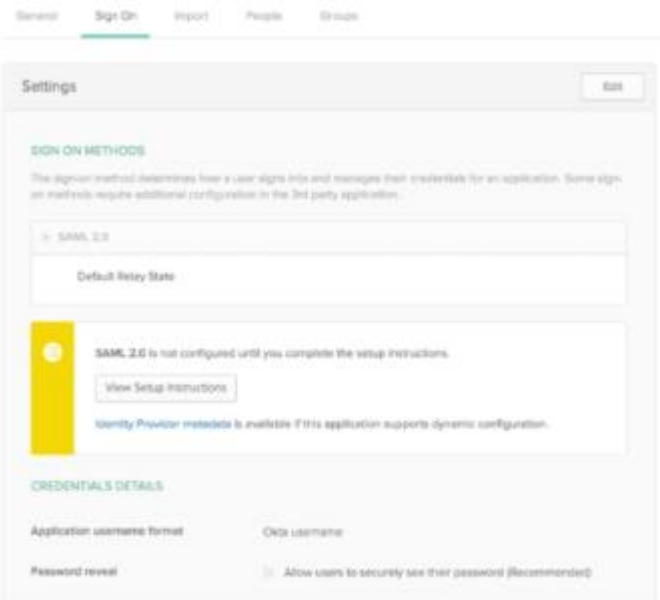


3. In **General Settings**, enter the app name and click **Next**.

4. In **SAML Settings**, enter the Salesforce custom domain URL, for example, https://<custom_domain_name>.my.salesforce.com, Audience URL, Name ID format, and Application username.



5. Click **Next**.
6. Select **I'm an octa customer adding an internal app** and click **Finish**.
7. Click **Applications** and select the application created.
8. On the **Sign on** tab, download the OKTA metadata.



- Verify that you have the metadata files for Salesforce.
  1. Login to **Salesforce** > **Security Controls** > **Single Sign on settings** > Import the OKTA metadata downloaded in the above step.
  2. Click **Save**.
  3. Download the Salesforce metadata.

Configuring Salesforce and Okta with MobileIron Access

You must perform the following tasks to configure Salesforce and Okta with MobileIron Access:

Register Sentry to Access

You must register Sentry to Access to fetch the latest configuration from Access.

Prerequisite

Verify that you have registered Sentry earlier. If so, then do not perform this step.

Procedure

1. **Clish** Sentry. In the configuration mode, execute the following command for registration.
   (config)#accs registration https:/<FQDN of Access server><Admin Username of Access Server>
2. Enter the **Tenant password** and complete the registration.
3. In **Access**, click the **Sentry** tab.
4. Select the appropriate Sentry instance, then click **Action** > **Assign**.
5. Enter the tenant password.
6. Click **OK**.
7. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

   (config)# accs config-fetch update

   Note: All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

Configure Access to create a Federated Pair

You must configure Access to select your service provider and the identity provider. You can apply the configuration settings for the service provider and the identity provider to create a federated pair.

Procedure

1. Log in to **Access**.
2. Click **Profiles** > **Get Started**.
3. Enter Access host information and upload the **ACCESS SSL certificate**. The other fields retain the default values. Click **Save**. For more information on Access SSL certificates, see *Certificates* in the *MobileIron Access Guide*.
4. Click **Profiles** > **Federated Pairs** > **Add New Pair**.
5. Select **Salesforce** as the service provider.
6. Enter the following details:
    a. Enter a **Name** for the
    b. Enter an appropriate **Description**.
    c. Upload the metadata details for Salesforce.
    d. (Optional) Select *Use Tunnel Certificates for SSO* to configure Cert SSO on MobileIron Core. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/current/accs/ .
7. Click **Next**.
8. Select **Okta** as the Identity provider. Click **Next**.
9. Upload the **IdP certificate** and the **IdP metadata file**. Click **Done**.
10. Download the **ACCESS SP Proxy** and the **ACCESS IDP Proxy** metadata file from the federated pair page.
11. On the **Profile** tab, click **Publish** to publish the profile.

Task Result

The Federated Pair is created.

Configure the Okta environment

1. Login to Okta with admin credentials using the sign-in URL received in the activation mail.
2. Select **Admin >Directory > People**.
3. Select **Add Person > Fill details > Save details**.
   Note: The email id should be same as that of Salesforce.
4. On the **Application** tab, click **Add Application**.
5. In the **Create a New Application Integration** window, select **SAML 2.0** radio button. Click **Create**.
6. Edit SAML integration settings:
    - Under the **General Setting** tab, enter the **Application name** and click **Next.**
    - Select **Configure SAML> SAML Settings**, enter the Salesforce custom domain URL, such as https://name-dev-ed.my.salesforce.com, Audience URL, Name ID format, and Application username.
    - Click **Next**.
7. Select **I'm an Okta customer adding and internal app** and click **Finish**.
8. On the **Applications** tab, select **Created Application > Sign-on and download identity provider metadata**.
9. Click **Sign On** tab.
10. Click **Identity Provider metadata** and download the metadata file.

Verification

1. Login to **Salesforce > Go to Security Controls > Single-sign on setting > Import identity provider metadata** to Salesforce and click **Save**.
2. Download the Salesforce Metadata (SP metadata).
3. Extract **Salesforce Login URL** from respective SSO Salesforce settings.
4. Select **Domain Management > My Domains > Edit the authentication configuration**, and select Okta entry.
5. Select Applications general settings **of Okta > Edit SAML Settings > Next >** Replace Single Sign on URL with **Salesforce Login URL > Next** and **Finish**.
6. Download the Okta Metadata (IDP metadata).
7. Select Applications general settings of **Okta > People > Assign to people.**
8. Access Salesforce from web browser.

Configure the Salesforce environment

You must configure the service provider with the identity provider. This builds the trust relationship with the identity provider.

Procedure

1. Login to Salesforce with Admin credentials.
2. Select **Security Controls** > **Single Sign On** > **New from Metadata File**.
3. Upload the IDP-PROXY metadata file downloaded when configuring Access to create a Federated Pair.
4. Click **Save**.
5. Select **Domain Management** > **My Domain** > **Edit Authentication Configuration settings** > **IDP-Proxy (Sentry)**.

Configure Okta for Salesforce through Access

You have configured Okta for Salesforce. You can configure Okta to work with Salesforce through Access.

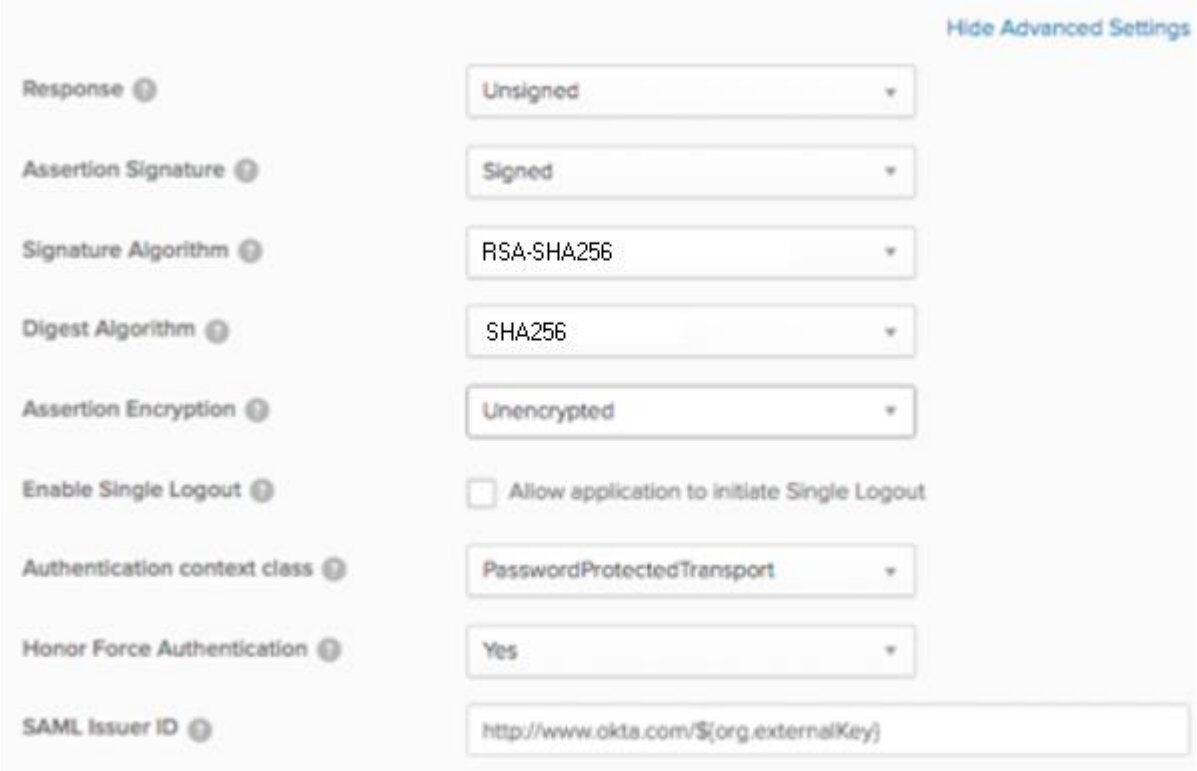
Prerequisites

Verify that you extract the entity ID from SP_PROXY_Metadata.

Procedure

1. Login to Okta with admin credentials.
2. Click **Applications** > **General** > Edit **SAML settings** and click **Next**.
3. Add the EntityID value to **Single Sign On URL** and **Audience URL**.

4. Click **Show Advanced settings** and enter the following values:



Verification

When salesforce is accessed, enter the custom domain details. You are redirected to Okta login page for authentication.