MobileIron Access Cookbook

Access with Facebook Workplace and Okta

Revised: April 05, 2018

Contents

Overview 3
Prerequisites 3
Configure the Okta environment 4
Configuring Facebook Workplace and Okta with MobileIron Access 6
Configure Access to create a Federated Pair 6
Configure the Facebook Workplace environment with MobileIron Access 7
Configure the Okta environment with MobileIron Access 8
Register Sentry to Access 8
Verification 8

Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Facebook Workplace is federated with an identity provider such as Okta for authentication. The user gets authenticated by Okta and obtains a SAML token for accessing applications in a cloud environment, such as Facebook Workplace.
This guide serves as step-by-step configuration manual for users using Okta as an authentication provider with Facebook Workplace in a cloud environment.

Prerequisites

You must perform the following steps before you configure Facebook Workplace:

- Ensure that you have a working setup of native federation for Facebook Workplace and Okta in your environment

- Verify that you refer the following link before configuring Facebook Workplace and Okta.
  https://developers.facebook.com/docs/workplace/authentication/sso

- Download the metadata files for Okta.
  1. Login to Okta with admin credentials and perform the **steps 1 to 11** in the Configure the Okta environment section to download the metadata file.

- Note down the following credentials for Facebook Workplace:
  1. Login to Facebook Workplace tenant with admin credentials.
  2. Click **Dashboard** > **Settings** > **Authentication**.
  3. Scroll-down to SAML Configuration and save the settings such as:

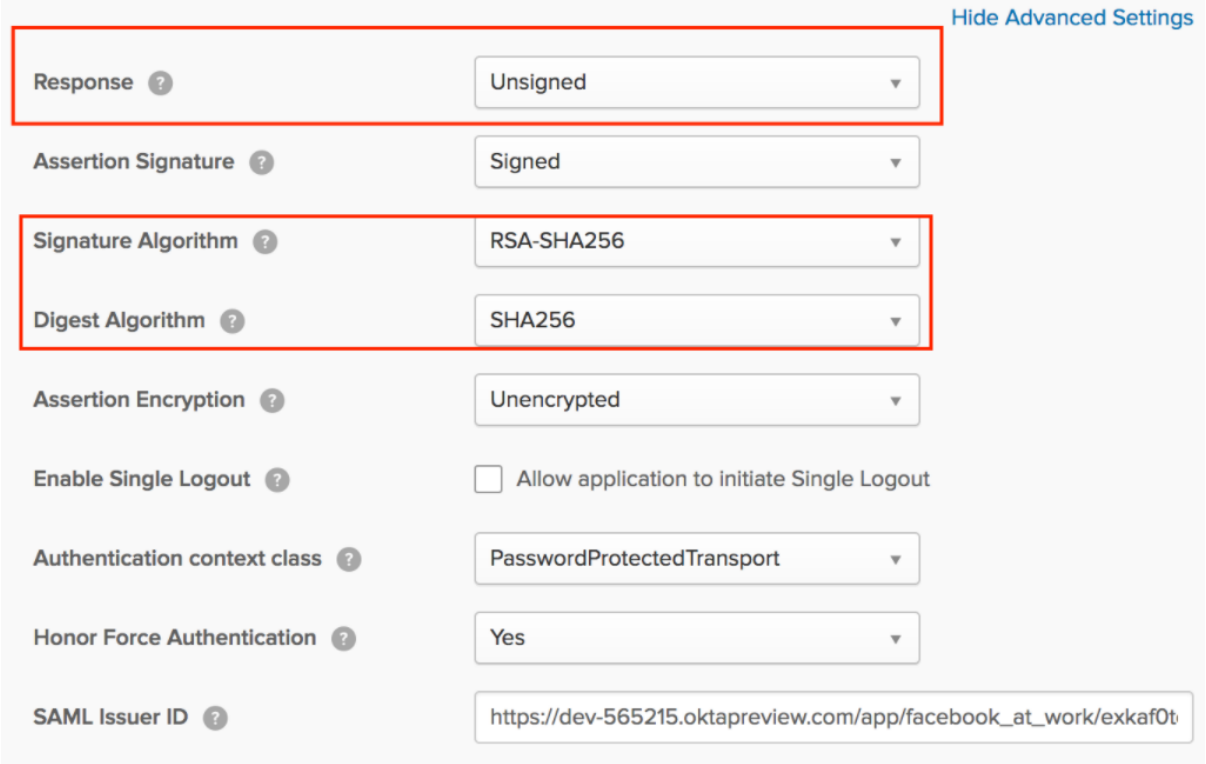
     - **Entity ID**: https://www.facebook.com/company/<ID>
     - **Assertion Consumer Service URL**: https://work-26249574.facebook.com/work/saml.php

Configure the Okta environment

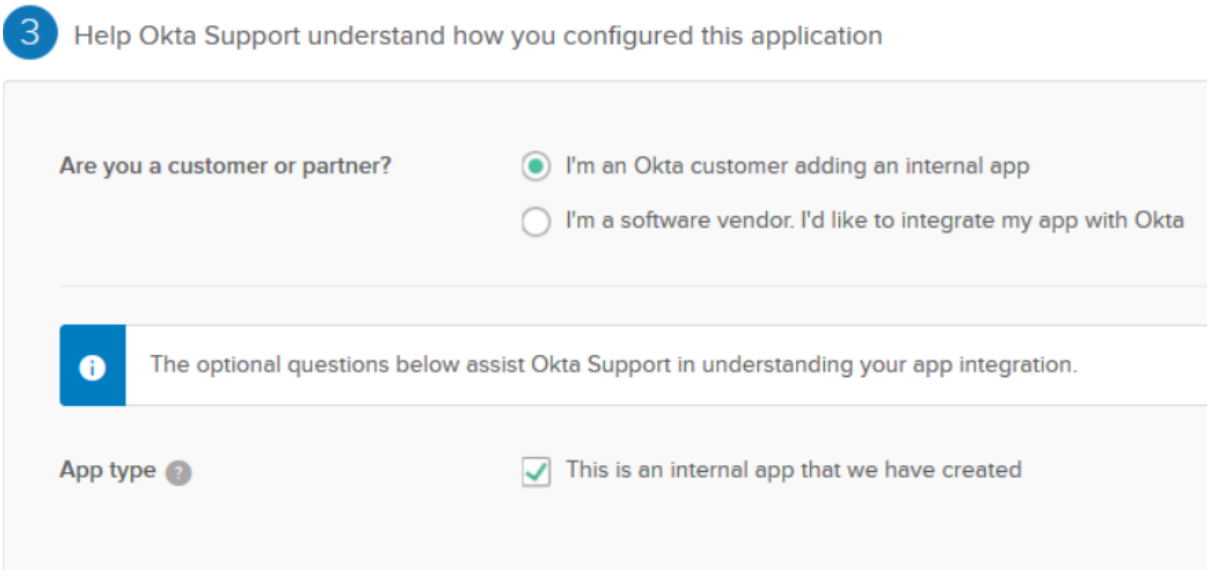
Configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

Procedure

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**.
4. **Note**: The email id should be same as that of SuccessFactors.
5. On the **Application** tab, click **Add Application**.
6. In the **Create a New Application Integration** window, select **SAML 2.0** radio button. Click **Create**.
7. Under the **General Setting** tab, enter the **Application name** and click **Next.**
8. In **SAML Settings**, enter the **Audience URL**, **Name ID** format, and Application username and click **Show Advanced Settings**.
9. Enter the configuration values as shown in the below screen and click **Next**.



10. Configure the feedback settings as below and click **Finish**.



11. Click **Applications** and select the application that you created. Click **Sign On** and download the identity provider metadata.
12. Click **Directory** > **People** > **Add Person** and **Create** a **User**.
13. On the **Applications** settings, select **Assign** to users**.**
14. Select the **User** and click **Assign**.
15. Click **Save > Done**.

Configuring Facebook Workplace and Okta with MobileIron Access

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

- Configure Access to create a Federated Pair
- Configure the Facebook Workplace environment with MobileIron Access
- Configure the Okta environment with MobileIron Access
- Register Sentry to Access

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**.
4. Click **Profiles** > **Federated Pairs** > **Add New Pair**.
5. Select **Facebook Workplace** as the service provider.
6. Enter the following details:
    a. Enter a **Name** for Facebook Workplace.
    b. Enter an appropriate Description.
    c. Select the **Access Signing Certificate** or use the **Advanced Options** to create a new Access Signing Certificate.
    d. Enter the metadata details for Facebook Workplace:
    Entity ID: https://www.facebook.com/company/<ID>
    Assertion Consumer Service URL: https://work-26249574.facebook.com/work/saml.php
    e. 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** and select Okta as the identity provider.
8. Select the **Access Signing Certificate** or use the **Advanced Options** to create and upload a new self-signed Access Signing Certificate.
9. **Add** the IdP metadata or **Upload** the IdP metadata file that you downloaded in Prerequisites.
10. Click **Done**.
11. Download the **Access SP Metadata (Upload to IDP)** and **ACCESS IDP Metadata (Upload to SP)** metadata files.
12. Click **Publish** to publish the profile.

.

Configure the Facebook Workplace environment with MobileIron Access

You must configure Facebook Workplace to use with Okta.

Procedure

1. Login to Facebook Workplace tenant with admin credentials.
2. Click **Dashboard** > **Settings** > **Authentication**.
3. Configure single sign-on settings. The information can be extracted from Access IdP metadata that downloaded when configuring Access for federated pair.

Feature	Settings
SAML Authentication	SSO only
SAML URL	https://<domain_name>/MobileIron/acc/53777c2f-11ce-4e7c-876c Extract this URL from the Entity ID of the metadata file that you downloaded.
SAML Issuer URI	https:/<domain_name>//MobileIron/acc/53777c2f-11ce-4e7c-876c Extract this URL from the Entity ID of the metadata file that you downloaded.
SAML Certificate	

4. Add the following lines in the certificate box:
   -----BEGIN CERTIFICATE-----
   -----END CERTIFICATE-----

Configure the Okta environment with MobileIron Access

1. Login to Access with admin credentials.
2. Click **Federated Pairs** > **Edit**.
3. Click **Next** and upload the metadata file that you downloaded in the Configure the Okta environment section.
4. Publish the profile.
5. Execute the following command from Sentry CLI
   (config)#accs config-fetch force-update

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. Click **OK**.
6. **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.

Verification

Single sign-on service is now configured using SAML with Facebook Workplace and Okta. This configuration lets you fetch the latest configuration from Access.
Verify that the following tests are successful:

- Open a browser and login to Facebook Workplace account. Verify in the *Access admin audit reports* that the Sentry logs for SAML request and responses are available.
- Configure Facebook Workplace on iOS device and verify in the *Access admin audit reports* that the Sentry logs for SAML request and responses are available.