# MobileIron Access Cookbook

## Access with G Suite and Okta

**07 February 2018**

# Contents

# Overview

SAML provides single sign-on service for users accessing their services hosted in a cloud environment. Generally, a service provider such as G Suite 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 G Suite.
This guide serves as step-by-step configuration manual for users using Okta as an authentication provider with G Suite in a cloud environment.

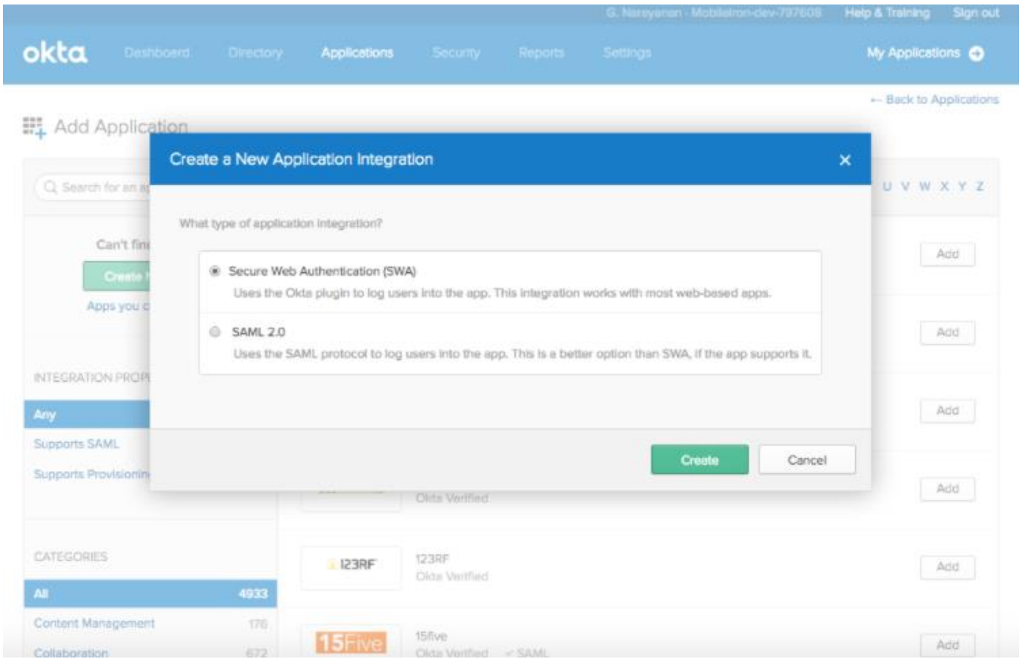
**Disclaimer**:
This cookbook is informational to help with the setup flow and actual screenshots. The steps might vary in your deployment scenario due to changes in SP/IdP versions.

# Prerequisites

- Ensure that you have a working setup of the G Suite and Okta pair without MobileIron Access.

- **Metadata files for G Suite**
  1. **Entity ID**: google.com/a/<domain name>
  2. **Assertion Consumer Service URL**: https://google.com/a/<domain name>/acs

- **Metadata files and configuration for Okta**
  1. Login to Okta with admin credentials.
  2. Click **Applications** > **Add application** > **Create New App**.
     **Create a New Application Integration** window displays.
  3. Select **SAML 2.0** as type of application integration.
  4. Click **Create**.



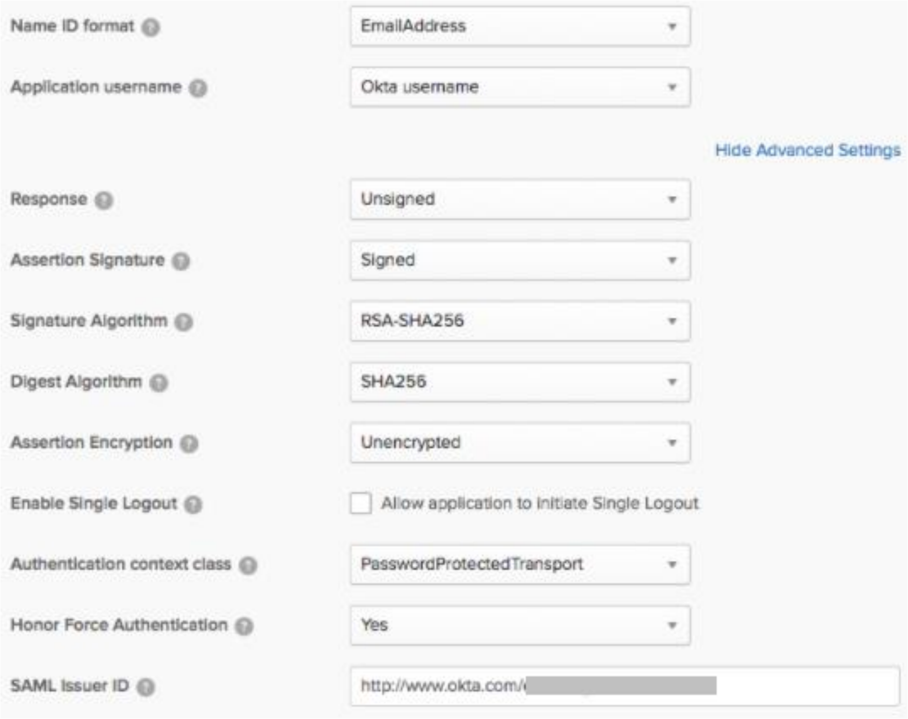
Create a New Application Integration

What type of application integration?

● Secure Web Authentication (SWA)
Uses the Okta plugin to log users into the app. This integration works with most web-based apps.

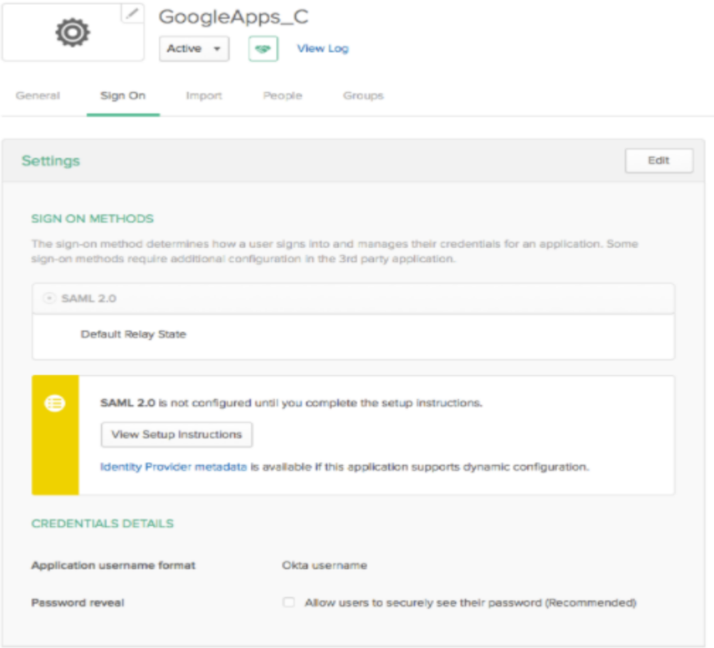
○ SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

5. On **General** settings tab, enter the application name and click **Next**.
6. In SAML settings, enter the **Single Sign On URL**, **Audience URL**, **Name ID format**, and **Application** as below and click **Next**.
    - Single Sing On URL: https://www.google.com/a/<domain_name>.com/acs
    - Audience URI (SP Entity ID): google.com/a/<domain_name>.com



| | |
|---|---|
| Name ID format | EmailAddress |
| Application username | Okta username |
| | Hide Advanced Settings |
| Response | Unsigned |
| Assertion Signature | Signed |
| Signature Algorithm | RSA-SHA256 |
| Digest Algorithm | SHA256 |
| Assertion Encryption | Unencrypted |
| Enable Single Logout | □ Allow application to initiate Single Logout |
| Authentication context class | PasswordProtectedTransport |
| Honor Force Authentication | Yes |
| SAML Issuer ID | http://www.okta.com/[redacted] |

7. Select **I'm an okta customer adding an internal app** and click **Finish**.
8. Click **Applications** and select the new application created.
9. On **Sign On** tab, download the identity provider metadata.



GoogleApps_C

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

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

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

CREDENTIALS DETAILS

| | |
|---|---|
| Application username format | Okta username |
| Password reveal | □ Allow users to securely see their password (Recommended) |

# Configuring G Suite and Okta with MobileIron Access

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

- Register Sentry to Access
- Configure Access to create a Federated Pair
- Configure G Suite with MobileIron Access
- Configure 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. 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.

## Configure Access to create a Federated Pair

You must configure Access to create a federated pair.

### Prerequisites

Verify that you have configured G Suite and Okta natively. See Prerequisites.

### Procedure

1. Log in to **Access**.
2. Click **Profile** > **Get Started**.
3. Enter the Access host information, and upload the **ACCESS SSL certificate** in p12 format. All the other fields are set to default. Click **Save**.
4. On the **Federated Pairs** tab, click **Add New Pair** and select **G Suite** as the service provider.
5. Enter the following details:
   a. Name
   b. Description
   c. Upload the Access Signing Certificate or click **Advanced Options** to create a new certificate.
   d. Click **Add Metadata** and enter the **Entity ID** and **Assertion Consumer Service URL**. See Prerequisites.
      **Entity ID**: https://docs.google.com/a/<domain_name>
      **Assertion Consumer Service URL**:
      https://www.google.com/a/domain_name/acs
   e. (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/
6. Click **Next**.
7. Select **Okta** as the Identity provider. Click **Next**.
8. Select the **Access Signing Certificate** or click **Advanced options** to create a new certificate.
9. Upload the IdP metadata file that you downloaded. See Prerequisites. Click **Done**.
10. Download the **ACCESS SP Metadata (Upload to IDP)** and the **ACCESS IDP Metadata (Upload to SP)** files from the federated pair page.
11. On the **Profile** tab, click **Publish** to publish the profile.

## Configure G Suite with MobileIron Access

You must configure G Suite to use with Access.

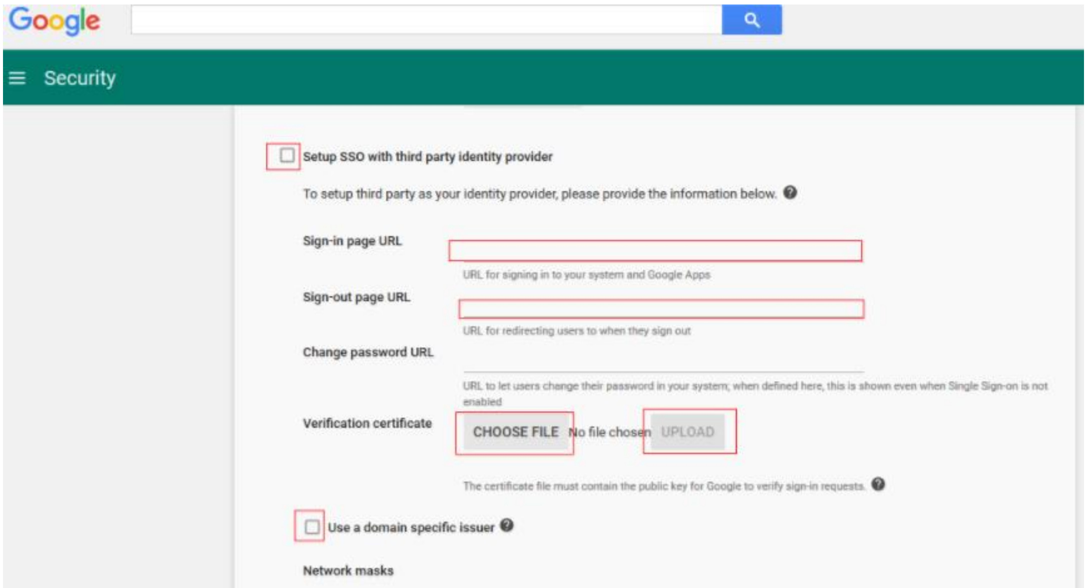
### Prerequisites

- Verify that you have created a federated pair with Google Suite and Okta.
- Verify that you have configured G Suite and Okta natively.

### Procedure

1. Login to the G Suite domain with admin credentials.
2. Click **Security**, and select **Single Sign-On Settings**.
3. Enter the following information from the **Access IDP Metadata (Upload to SP).** See **Step 10** in Configure Access to create a Federated Pair:
   a. **Sign-in page URL**: <Entity ID >
   b. **Sign-out page URL**: <Entity ID >
   c. **Change password URL**

d. **Verification certificate**



□ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below.

Sign-in page URL

URL for signing in to your system and Google Apps

Sign-out page URL

URL for redirecting users to when they sign out

Change password URL

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate CHOOSE FILE No file chosen UPLOAD

The certificate file must contain the public key for Google to verify sign-in requests.

□ Use a domain specific issuer

Network masks

4. Click **Save**.

## Configure Okta with MobileIron Access

You must 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.
2. Click **My Applications** and select the SAML application created for G Suite.
3. On the **General** tab, scroll-down to SAML settings and click **Edit.**
4. Click **Next**.
5. Replace the **Single Sign on URL** and **Audience URI** (SP Entity ID), with the Entity ID extracted from the file **Access SP Metadata (Upload to IDP).** See **Step 10** in Configure Access to create a Federated Pair.
6. Click **Next**.
7. Select **I'm an Okta customer adding an internal app** and click **Finish**.

# Verification

1. Register a device to Core.
2. Download G Suite application from App Store.
3. Opening this application triggers the per-app-vpn.
4. Verify that SAML SSO is working.