



# MobileIron Access Cookbook

## Access with Facebook Workplace and G Suite

**August 23, 2017**



## Contents

Overview.....	3
Prerequisites.....	3
Configuring Facebook Workplace and G Suite with MobileIron Access .....	4
Configure Access to create a Federated Pair .....	4
Configure the Facebook Workplace environment for Access .....	5
Configure the G Suite environment for Access .....	6
Register Sentry to Access .....	6
Verification .....	7



# 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 G Suite for authentication. Users authenticate to G Suite as an identity provider and obtain 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 G Suite as an authentication provider with Facebook Workplace 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 have the credentials for G Suite admin account.
- Ensure that you configure Facebook Workplace as a Service Provider that can work with G Suite as an Identity Provider. For more information, see [https://support.google.com/a/answer/6356973?hl=en&ref\\_topic=6304952](https://support.google.com/a/answer/6356973?hl=en&ref_topic=6304952)

Download the metadata files after the configuration. These files must be used when you configure Facebook Workplace and G Suite to flow through MobileIron Access.



# Configuring Facebook Workplace and G Suite with MobileIron Access

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

- [Configure Access to create a Federated Pair](#)
- [Configure the Facebook Workplace environment for Access](#)
- [Configure the G Suite environment for 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**. For more information on Access SSL certificates, see *Certificates* in the *MobileIron Access Guide*.
4. Click **Profiles > Federated Pairs > Add**.
5. Select **Facebook Workplace** as the service provider.
6. Enter the following details:
  - a. Enter a **Name** for the service provider.
  - b. Enter an appropriate Description.
  - c. Select *Access Self Signing Certificate* in the **Signing Certificate** drop-down list.
  - d. Select **Add Metadata** and enter the following details:
    - **Entity ID:** <https://www.facebook.com/company/your-company-id>
    - **Assertion Consumer Service URL:** <https://your-company-name.facebook.com/work/saml.php>
  - 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/>.
7. Click **Next**.
8. Select **G Suite** as the Identity provider. Click **Next** and enter the following details:
  - a. Select *Access Self Signing Certificate* in the **Signing Certificate** drop-down list.
  - b. Upload the metadata details for G Suite (see Prerequisites).
9. Click **Done**.
10. Download the **ACCESS SP Metadata** and the **ACCESS IDP Metadata** file from the Federated Pair listing page.



11. On the **Profile** tab, click **Publish** to publish the profile.

## **Task Result**

The Federated Pair is created.

## **Configure the Facebook Workplace environment for Access**

The following procedure configures a trust between Facebook Workplace Service Provider and Access so authentication flows are redirected to Access.

## **Procedure**

1. Login to Facebook Workplace tenant with Admin credentials.
2. Select **Dashboard > Settings > Authentication**.
3. Configure the Single Sign-On settings as shown below. SAML URL, Issuer URI, and Certificate must be extracted from the Access IDP Metadata (pairname-UploadTo-Facebook Workplace-SP.xml)

**SSO Settings**

**SAML Authentication**

Allow users to login via: **SSO only**

In web browsers, check SAML again after: **Never**

Require SAML in mobile apps [?]

Log people out of mobile apps after: **Never**

**Require SAML authentication for all users now**

**SAML URL** `https://app223-alt.auto.orange.com/Orange/acc/53777c2f-11ce-4e7d-887b`

**SAML Issuer URI** `https://app223-alt.auto.orange.com/Orange/acc/53777c2f-11ce-4e7d-887b`

**SAML certificate**

```
-----BEGIN CERTIFICATE-----
MIIDZCCAkwCCQCZVG/BcwYw0jANBgkqhkiG9w0BAQsFADB0MQswCQYDVQ
QGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcms5pYTEWMBQGA1UEBwwNTW91bnRhaW4g
VmldzET
MBEGA1UECgwKTW9iaWxiSXJvbjEQMA4GA1UECwwHU3VvcG9ydDERMA8GA1
UEAwI
SWRwUHJveHkwHhcNMTUxMDEzMTUyNDIwWhcNMjUxMDEwMjUyNDIwWjB0M
QswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcms5pYTEWMBQGA1UEBwwNTW9
1bnRhaW4g
VmldzETMBEGA1UECgwKTW9iaWxiSXJvbjEQMA4GA1UECwwHU3VvcG9ydDER
*****
```

**Save**

4. Add the below content in the certificate box:  
-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----
5. Click **Save**.



## [Configure the G Suite environment for Access](#)

The following procedure configures a trust between G Suite Identity Provider and Access so authentication flows are redirected to Access.

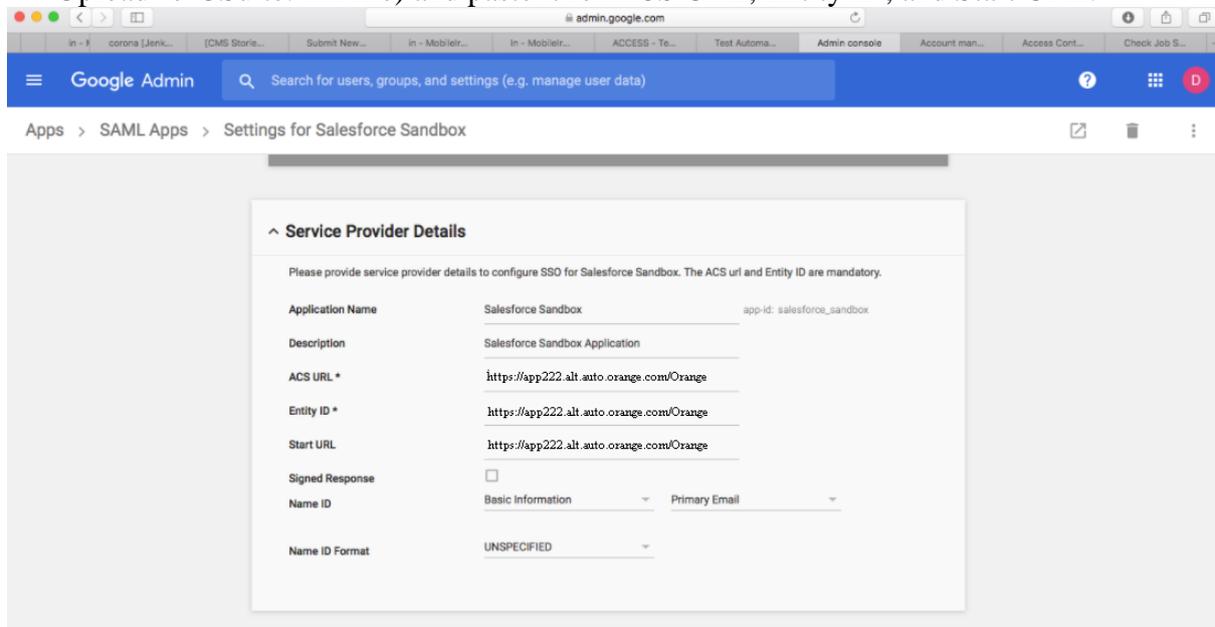
### **Procedure**

1. Login to G Suite admin console with admin credentials, (<https://admin.google.com>)
2. Navigate to Apps from the main menu and click **SAML Apps**.
3. Click **Facebook Workplace** application that was added when configuring Facebook

Workplace and G Suite without Access. If the application is not added, click  .

4. Update **ACS URL**, **Entity ID**, and **Start URL**.

Note: You can extract the Entity ID value from Access SP metadata file (pairname-UploadTo-GSuite.xml file) and paste it for ACS URL, Entity ID, and Start URL.



The screenshot shows the Google Admin console interface. The breadcrumb trail is 'Apps > SAML Apps > Settings for Salesforce Sandbox'. The main content area is titled 'Service Provider Details' and contains a form for configuring SSO for the Salesforce Sandbox application. The form includes the following fields:

Field	Value
Application Name	Salesforce Sandbox (app-id: salesforce_sandbox)
Description	Salesforce Sandbox Application
ACS URL *	https://app222.alt.auto.orange.com/Orange
Entity ID *	https://app222.alt.auto.orange.com/Orange
Start URL	https://app222.alt.auto.orange.com/Orange
Signed Response	<input type="checkbox"/>
Name ID	Basic Information (dropdown) Primary Email (dropdown)
Name ID Format	UNSPECIFIED (dropdown)

5. Configuration is complete.

## [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 **Password**.
6. Click **OK**.
7. **Click** 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 7.

### **Task Result**

Single sign-on service is now configured using SAML with Facebook Workplace and G Suite. This configuration lets you fetch the latest configuration from Access.

### **Verification**

- Log into Facebook Workplace. Redirection occurs through Access and G Suite login page displays.
- Enter valid user credentials and verify that you are redirected to Facebook Home page through Access.



Copyright © 2016 - 2017 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.