MobileIron Access Cookbook

Access with Salesforce and G Suite

August 23, 2017

Contents

Overview 3

Prerequisites 3

Configuring Salesforce and G Suite with MobileIron Access 4

- Configure Access to create a Federated Pair 4
- Configure the Salesforce environment for Access 5
- Configure the G Suite environment for Access 5
- 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 Salesforce 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 Salesforce.

This guide serves as step-by-step configuration manual for users using G Suite 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 have the credentials for G Suite admin account.
- Verify that you refer the following link before configuring Salesforce and G Suite. https://developers.Salesforce.com/signup.
- Ensure that you configure Salesforce as a Service Provider that can work with G Suite as an Identity Provider. For more information, see https://support.google.com/a/answer/6194938?hl=en

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

Configuring Salesforce and G Suite with MobileIron Access

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

- Configure Access to create a Federated Pair
- Configure the Salesforce 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 **Salesforce** 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. Upload the metadata details for Salesforce (see Prerequisites) and click **Next**.
   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**.
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 Salesforce environment for Access

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

Procedure

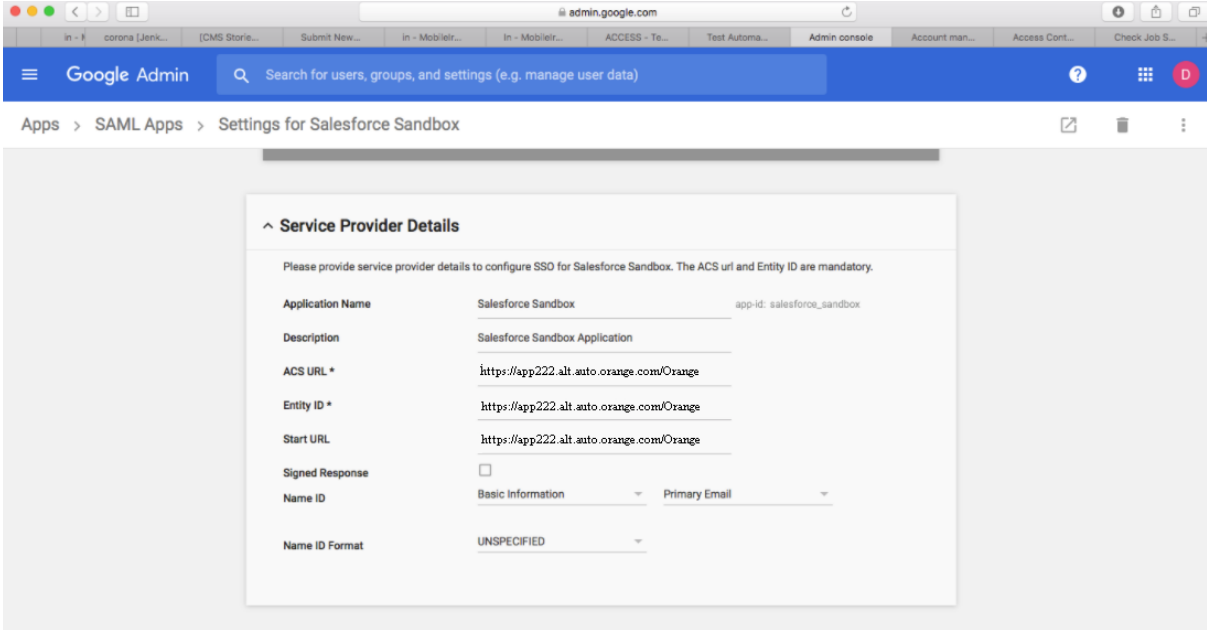
1. Login to Salesforce with Admin credentials.
2. Select **Security Controls** > **Single Sign On** > **New from Metadata File**.
3. Click **Browse** and upload the **Access IDP Metadata** (Pairname-UploadTO-Salesforce-SP.xml) File downloaded when configuring Access to create a Federated Pair. See Step 10 in **Configure Access to create a Federated Pair.**
4. Click **Create > Save**.
5. Select **Domain Management** > **My Domain** > **Authentication Configuration settings.**
6. Click **Edit** and select the Authentication service that was created in **Step 4**.
7. 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 **Salesforce** application that was added when configuring Salesforce 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.



Apps > SAML Apps > Settings for Salesforce Sandbox

Service Provider Details

Please provide service provider details to configure SSO for Salesforce Sandbox. The ACS url and Entity ID are mandatory.

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	□	
Name ID	Basic Information	Primary Email
Name ID Format	UNSPECIFIED	

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. **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 7.

Task Result

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

Verification

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