MobileIron Access Cookbook

Access with Salesforce and SecureAuth

Revised: April 05, 2018

Contents

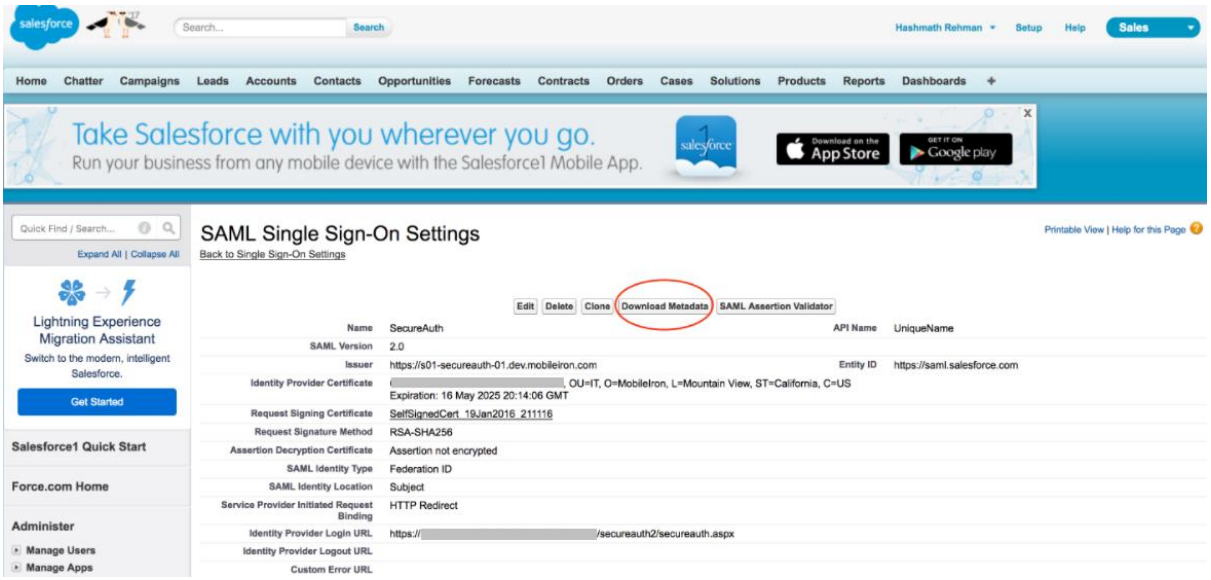
Overview

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 SecureAuth for authentication. Users authenticate to SecureAuth 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 SecureAuth as an authentication provider with Salesforce in a cloud environment.

Prerequisites

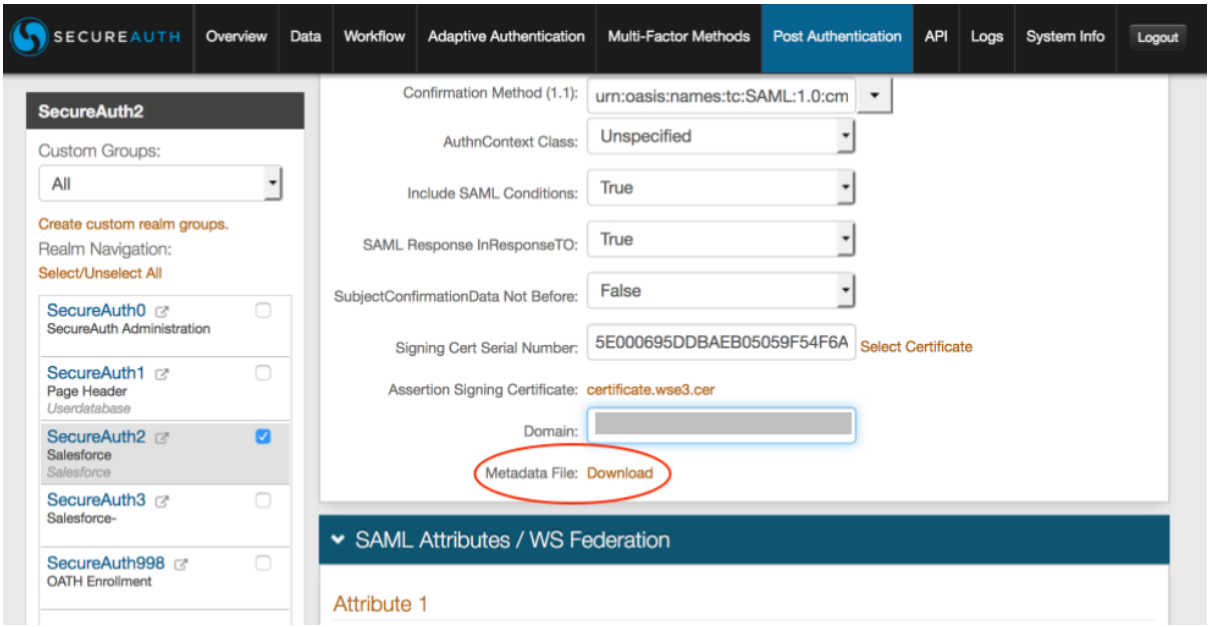
You must perform the following steps before you configure the service provider and identity provider with Access:

- Ensure that you have a working setup of the Salesforce and SecureAuth pair without MobileIron Access.
- Verify that you have the metadata files for Salesforce.
  1. Login to Salesforce with admin credentials.
  2. Click **Security Control** > **SAML Single Sign-On Settings** > SecureAuth record.
  3. Click **Download Metadata** and save the metadata file.



- Verify that you have the metadata file for SecureAuth.
  1. Login to SecureAuth with admin credentials.
  2. Click **Salesforce** realm > **Post Authentication** and scroll down.

3. Click **Download** at the metadata file.



Configuring Salesforce and SecureAuth with MobileIron Access

You must perform the following tasks to configure Salesforce and SecureAuth 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

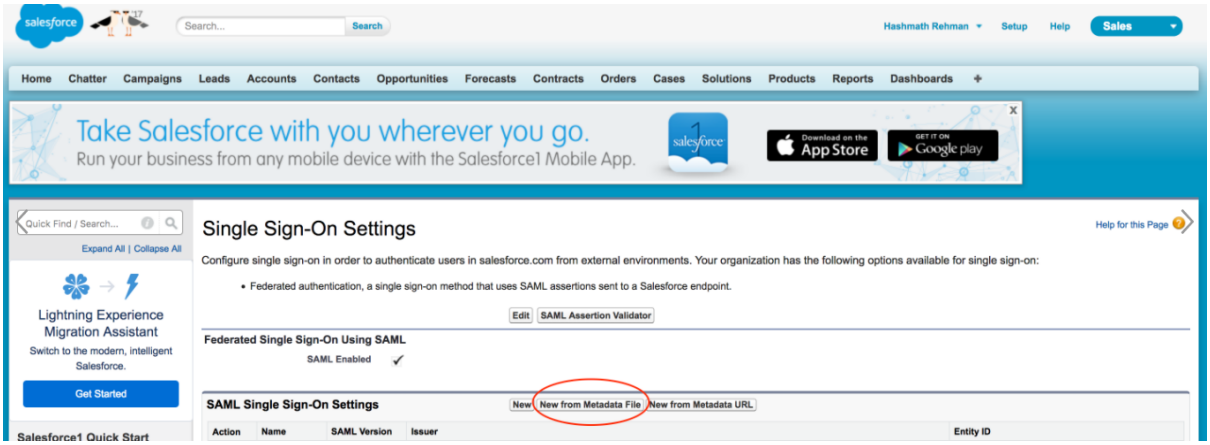
You must configure Access to select your service provider and the identity provider. You can apply the configuration settings for the service provider and the identity provider to create a federated pair.

Procedure

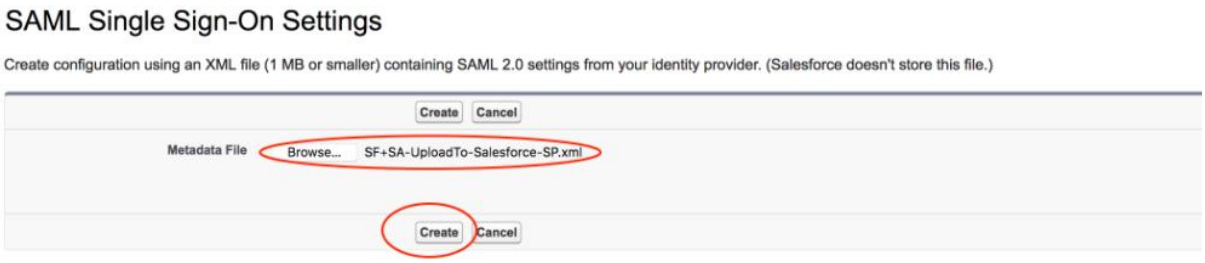
1. Log in to **Access**.
2. Click **Profiles** > **Get Started**.
3. Enter Access host information and upload the **ACCESS SSL certificate**. The other fields retain the default values. Click **Save**. For more information on Access SSL certificates, see *Certificates* in the *MobileIron Access Guide*.
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. Select the Access Signing Certificate or click **Advanced Options** to create a new certificate.
    d. Upload the metadata file for Salesforce that you downloaded. See Prerequisites.
    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 **SecureAuth** as the Identity provider. Click **Next**.
9. Select the Access signing Certificate or click **Advanced options** to create a new certificate.
10. Upload the metadata file for SecureAuth that you downloaded. See Prerequisites.
11. Download the **ACCESS SP Metadata (Upload to IDP)** and the **ACCESS IDP Metadata (Upload to SP)** files from the federated pair page.
12. On the **Profile** tab, click **Publish** to publish the profile.

Configure the Salesforce environment with MobileIron Access

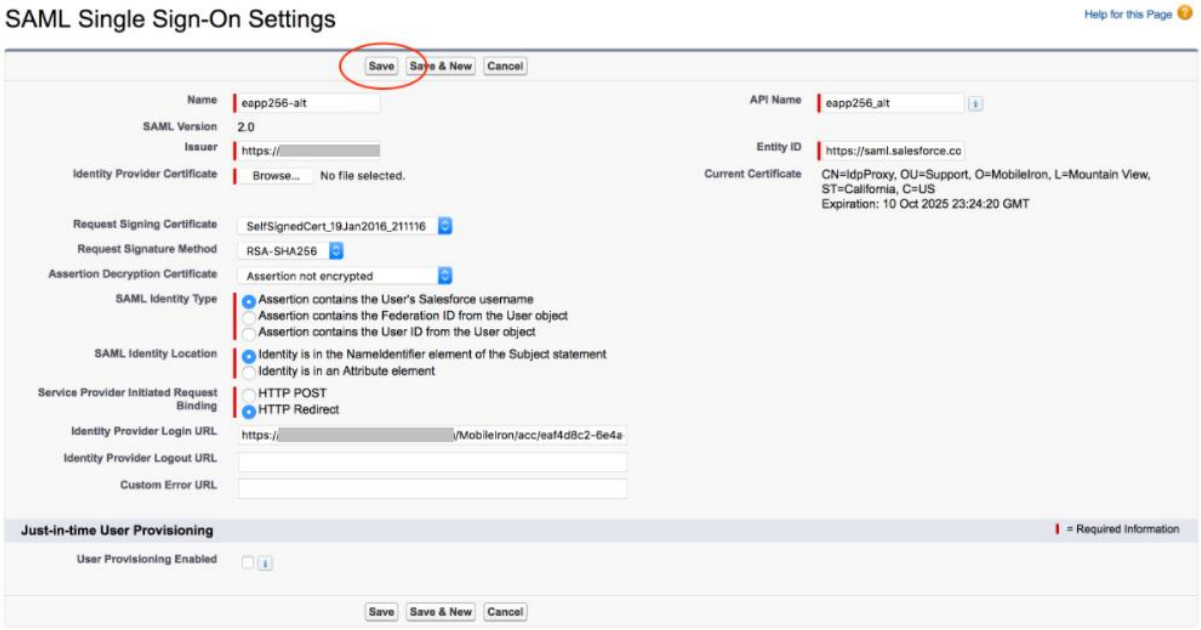
1. Login to Salesforce with admin credentials.
2. Click **Security Control** > **Single Sign-On Settings**.
3. Click **New from Metadata file**.



4. Upload the "**Access IDP Metadata (Upload to SP)**" that you downloaded in **Step 11** of Configure Access to create a Federated Pair.



5. Click **Save**.



6. Click **Domain Management** > **My Domain** > **Edit Authentication configuration** and select the new federated authentication service.

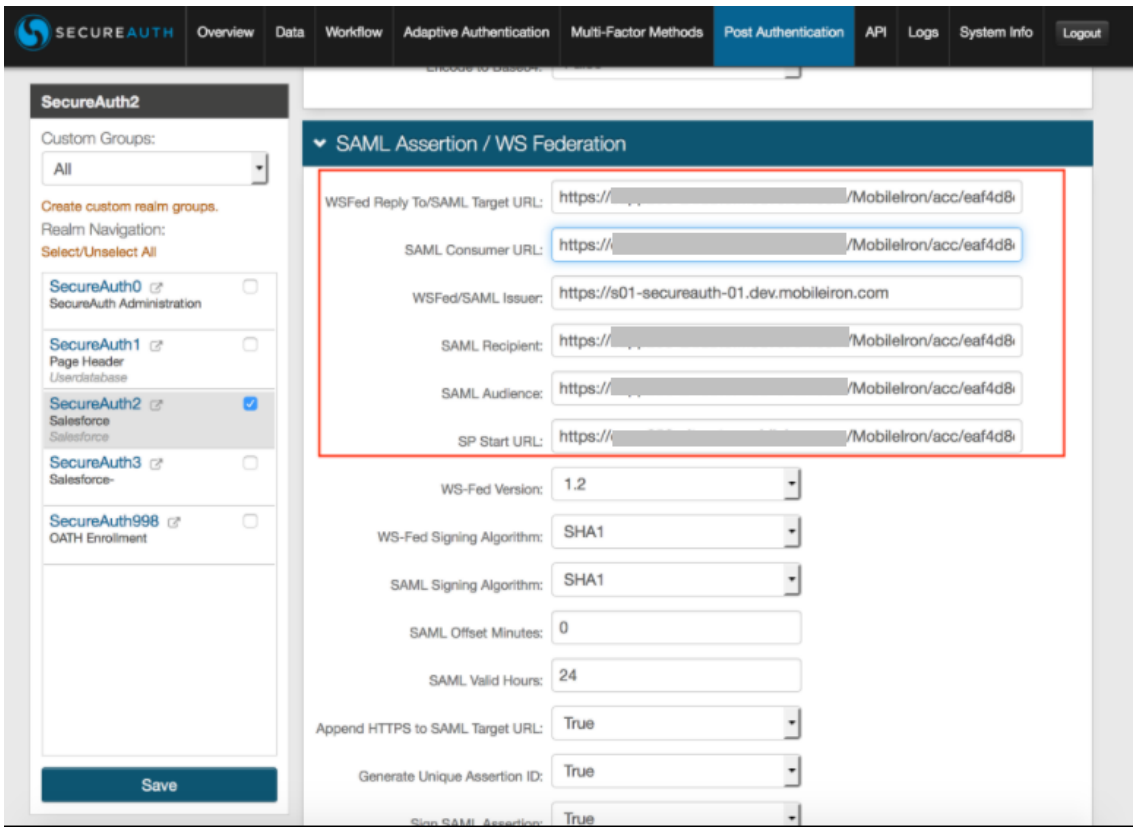
Configure the SecureAuth environment with MobileIron Access

You must configure the Identity Provider Federation settings with the values of MobileIron ACCESS SP Metadata. This builds the trust relationship between MobileIron ACCESS and SecureAuth.

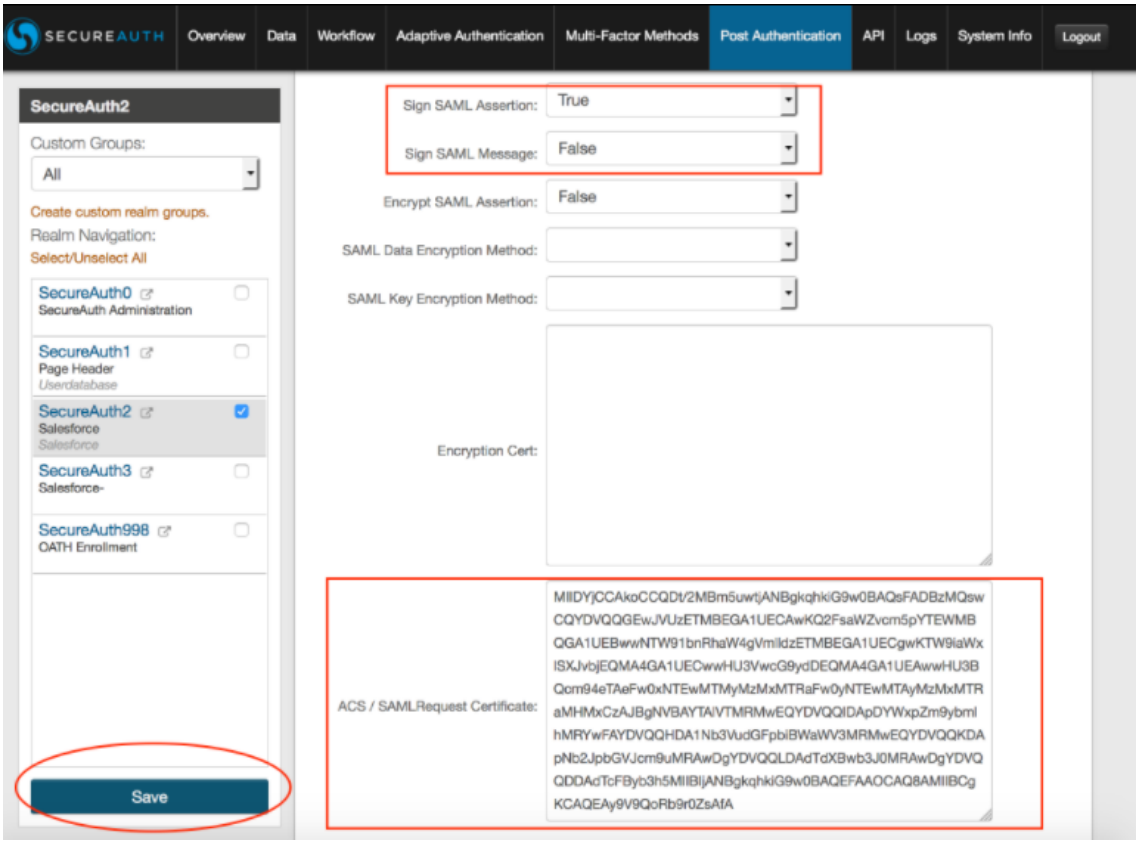
Procedure

1. Login to the SecureAuth portal with admin credentials.
2. Click the **Salesforce** realm and select **Post Authentication** tab.
3. Open the **Access SP Metadata (Upload to IDP)** that you downloaded in **Step 11** of Configure Access to create a Federated Pair. Extract the Entity ID and certificate as shown below:

4. Edit the SAML Assertion or WS Federation settings as shown below.



5. Select the SAML values as below and click **Save**.



Verification

1. Register a device to Core.
2. Download the Salesforce app from App store.
3. Open the application that triggers per-app-vpn.
4. Verify that the SAML SSO is working.