



MobileIron Access Cookbook

Access with Salesforce and SecureAuth

Revised: April 05, 2018



Contents

Overview	3
Prerequisites	3
Configuring Salesforce and SecureAuth with MobileIron Access	5
Register Sentry to Access	5
Configure Access to create a Federated Pair	5
Configure the Salesforce environment with MobileIron Access	6
Configure the SecureAuth environment with MobileIron Access	7
Verification	9



Overview

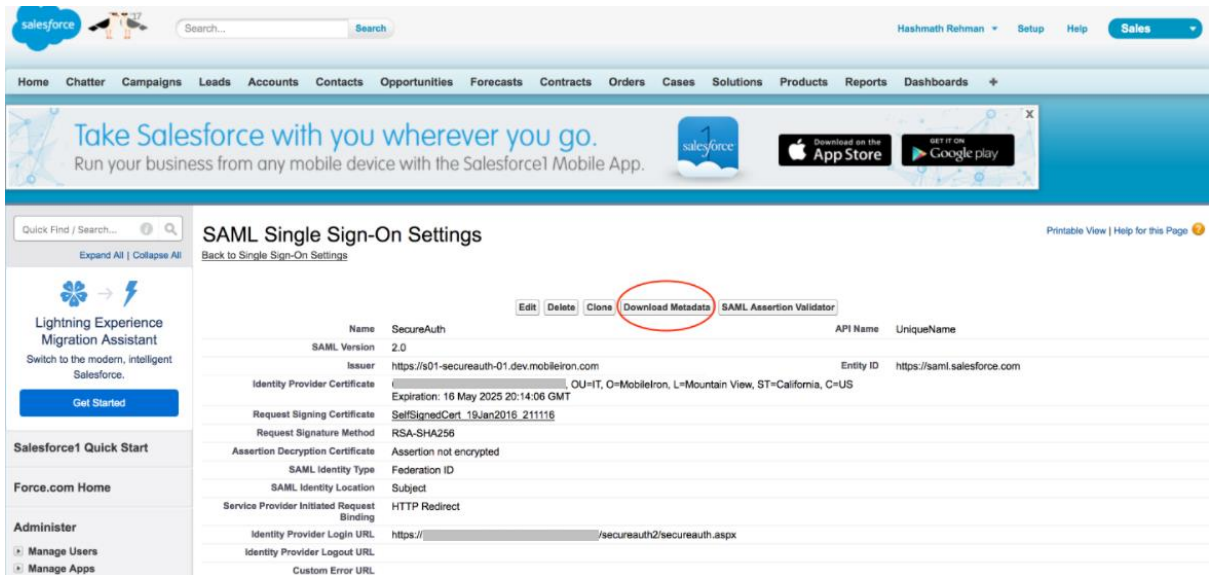
SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Salesforce is federated with an identity provider such as SecureAuth for authentication. Users authenticate to SecureAuth as an identity provider and obtain 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.

The screenshot shows the SecureAuth administration console. The top navigation bar includes tabs for Overview, Data, Workflow, Adaptive Authentication, Multi-Factor Methods, Post Authentication (selected), API, Logs, System Info, and Logout. The main content area is divided into a left sidebar and a main configuration panel.

SecureAuth2 sidebar:

- Custom Groups: All
- Create custom realm groups.
- Realm Navigation: Select/Unselect All
- SecureAuth0: SecureAuth Administration
- SecureAuth1: Page Header, Userdatabase
- SecureAuth2: Salesforce** (checked)
- SecureAuth3: Salesforce-
- SecureAuth998: OATH Enrollment

Main Configuration Panel:

- Confirmation Method (1.1): urn:oasis:names:tc:SAML:1.0:cm
- AuthnContext Class: Unspecified
- Include SAML Conditions: True
- SAML Response InResponseTO: True
- SubjectConfirmationData Not Before: False
- Signing Cert Serial Number: 5E000695DDBAEB05059F54F6A (Select Certificate)
- Assertion Signing Certificate: certificate.wse3.cer
- Domain: [Empty text box]
- Metadata File: Download** (circled in red)

SAML Attributes / WS Federation

- Attribute 1



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](#)
- [Configure Access to create a Federated Pair](#)
- [Configure the Salesforce environment with MobileIron Access](#)
- [Configure the SecureAuth environment 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**.

The screenshot shows the Salesforce 'Single Sign-On Settings' page. The page title is 'Single Sign-On Settings'. Below the title, there is a section for 'Federated Single Sign-On Using SAML' with a checkbox for 'SAML Enabled' which is checked. Below this, there is a section for 'SAML Single Sign-On Settings' with two buttons: 'New from Metadata File' and 'New from Metadata URL'. The 'New from Metadata File' button is circled in red.

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



SAML Single Sign-On Settings

Create configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't store this file.)

Metadata File

5. Click **Save**.

SAML Single Sign-On Settings

[Help for this Page](#)

Name API Name

SAML Version

Issuer Entity ID

Identity Provider Certificate No file selected. Current Certificate CN=IdpProxy, OU=Support, O=MobileIron, L=Mountain View, ST=California, C=US
Expiration: 10 Oct 2025 23:24:20 GMT

Request Signing Certificate

Request Signature Method

Assertion Decryption Certificate

SAML Identity Type Assertion contains the User's Salesforce username
 Assertion contains the Federation ID from the User object
 Assertion contains the User ID from the User object

SAML Identity Location Identity is in the NameIdentifier element of the Subject statement
 Identity is in an Attribute element

Service Provider Initiated Request Binding HTTP POST
 HTTP Redirect

Identity Provider Login URL

Identity Provider Logout URL

Custom Error URL

Just-in-time User Provisioning = Required Information

User Provisioning Enabled

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:



```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://[redacted]-alt.auto.mobileiron.com/MobileIron/acc/eaf4d8c2-6e4a-4f25-83eb-13144a6e3655/sp">
  <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDYjCCAKoCCQDt/
          2MBm5uwtjANBgkqhkiG9w0BAQsFADBzMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNTW91bnR
          haW4gVm1ldzETMBEGA1UECgwKTW9iaWx1SXJvbWJEQMA4GA1UECwwHU3VwcG9ydDEQMA4GA1UEAwwHU3BQcm94eTAeFw0xNTEwM
          TMyMzIxMTRaFw0yNTEwMTAyMzIxMTRaMHMxCzAJBgNVBAYTA1VTMRRMwEQYDVQQIDApDYWxpZm9ybnIhMRYwFAFDVQQA1Nb3V
          udGFpbWV3MRMwEQYDVQQKDApNb2JpbGVJcm9uMRAdDgYDVQQLDAdTDXBw3J0MRAdDgYDVQQDDAdTcFByb3h5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy9V9QoRb9r0ZsAfa/1JRT/r6RprOwrnjGQ1KdZiZwMj0x3J2hQ91oHJJd
          +LdSt1Ezc8res8XiBGHaJ73549WpoZibZUcePJJ2Z6WwKJXmWeNotshRRy/ZbGrTyulm65bD4TnAZUR0qkC0qSVtT1blchsG1
          +awAwogOHkmsHf1rEiSA3KEeDAk6DaIigrnMPd3DIAppWfYhiZmFEWLk1TPDUU8wDsC
          +fKPbpKeWmbc95zngFPkxqfNFxUyoGYRF1Y/
          t6v2ygW95jX8AuSar6wpnU08TbGwmg29qwj4ofW5MBVS3Rsvz8YIi1HlcBYU2bwA8UD
          +IAqPvaZdiUj8bwIDAQABMA0GCsGSIb3DQEBCwUA4IBAQB/Z5S6k5AJImrC24yqZGu/BHH8iuRvTyq1hxjQ/
          xdX1GzxUih61240o09iwdroDwkCh5sJRRrecrD2Z23wxC15hBcXDbjgIs/M6K1j
          +jikJIWJa9M3AMCTViAEKn1epS3vSGwaWqcT3XFjxFdujqbNgk9LxFqCgEb8KkqBimjT3rXPXuIY9XYv3qMbVfBTtSmaBjU2p
          q15ahd4TFDGzm1arMjXMQd0dCWbibXmKh6fHMTnboXT8YcOVzkDL2pmPyDa7iaPoPlGCn9JMQPKOUymtztaniqB0uXy4FDqRkR
          dtLKnEny5GoertVGuhxqP8sIimjZ6UnTvp+AVSz+B1f</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[redacted].auto.mobileiron.com/MobileIron/acc/eaf4d8c2-6e4a-4f25-83eb-13144a6e3655/sp" index="0" isDefault="true"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

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

The screenshot shows the configuration page for SecureAuth2 in the 'Post Authentication' tab. The 'SAML Assertion / WS Federation' section is expanded and highlighted with a red box. The settings are as follows:

- WSFed Reply To/SAML Target URL:
- SAML Consumer URL:
- WSFed/SAML Issuer:
- SAML Recipient:
- SAML Audience:
- SP Start URL:
- WS-Fed Version:
- WS-Fed Signing Algorithm:
- SAML Signing Algorithm:
- SAML Offset Minutes:
- SAML Valid Hours:
- Append HTTPS to SAML Target URL:
- Generate Unique Assertion ID:
- Sign SAML Assertion:



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

The screenshot shows the configuration page for SecureAuth2. On the left, a sidebar lists various realm groups, with 'SecureAuth2' (Salesforce) selected. The main area contains several configuration options: 'Sign SAML Assertion' is set to 'True', 'Sign SAML Message' is set to 'False', 'Encrypt SAML Assertion' is set to 'False', and 'SAML Data Encryption Method' and 'SAML Key Encryption Method' are both set to 'None'. The 'Encryption Cert' field is empty. The 'ACS / SAMLRequest Certificate' field contains a long alphanumeric string: MIIIDYjCCAKoCCQDlV2MBm5uwtJANBgkqhkiG9w0BAQsFADBzMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcmspYTEWMBQGA1UEBwwNTW91bnRhaW4gVmldzETMBEGA1UECgwKTW9iaWxISXJvbjEQMA4GA1UECwwHU3VwcG9ydEQMA4GA1UEAwwHU3BQcm94eTAeFw0xNTEwMTMyMzIxMTRaFw0yNTEwMTAyMzIxMTRaMHIHMxCzAJBgNVBAYTAiVTMRMwEQYDVQIDApDyYwZm9ybmlhMRYwFAYDVQQHDA1Nb3VudGFpbWV3MRMwEQYDVQQKDApNb2JpbGVJcm9uMRAwDgYDVQQLEAdTdXBwb3J0MRAwDgYDVQGDAAcTcFByb3h5MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy9V9QcRb9r0ZeAIA

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.



Copyright © 2016 - 2018 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.