MobileIron Access Cookbook

Access with Salesforce and Microsoft ADFS

Revised: November 02, 2017

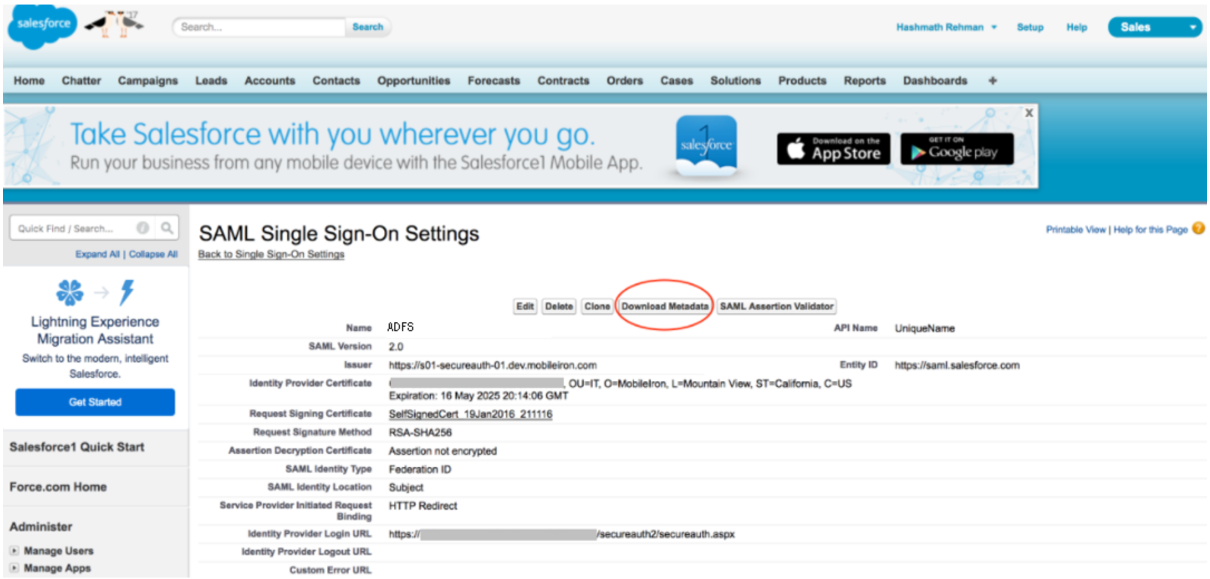
Contents

Overview

SAML provides single sign-on service 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 Microsoft ADFS for authentication. The user gets authenticated by ADFS and obtains 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 ADFS as an authentication provider with Salesforce in a cloud environment.

Prerequisites

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



SAML Single Sign-On Settings
Back to Single Sign-On Settings

Name	ADFS	API Name	UniqueName
SAML Version	2.0		
Issuer	https://s01-secureauth-01.dev.mobileiron.com	Entity ID	https://saml.salesforce.com
Identity Provider Certificate	[redacted], OU=IT, O=MobileIron, L=Mountain View, ST=California, C=US Expiration: 16 May 2025 20:14:06 GMT		
Request Signing Certificate	SelfSignedCert_19Jan2016_211116		
Request Signature Method	RSA-SHA256		
Assertion Decryption Certificate	Assertion not encrypted		
SAML Identity Type	Federation ID		
SAML Identity Location	Subject		
Service Provider Initiated Request Binding	HTTP Redirect		
Identity Provider Login URL	https://[redacted]/secureauth2/secureauth.aspx		
Identity Provider Logout URL			
Custom Error URL			

- **Metadata files for Microsoft ADFS**:
  Download your **ADFS IDP** metadata file from the following location:
  https://<ADFS Server FQDN> /FederationMetadata/2007-06/FederationMetadata.xml

Configuring Salesforce and Microsoft ADFS with MobileIron Access

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

- Configuring Access to create a Federated Pair
- Configuring Salesforce with MobileIron Access
- Configuring ADFS with MobileIron Access
- Registering Sentry to Access

Configuring Access to create a Federated Pair

You must configure Access to create a federated pair.

Prerequisites

Verify that you have configured ADFS and Salesforce natively.

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 **Salesforce** 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. Upload the metadata file of service provider 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/
6. Click **Next**.
7. Select **Microsoft ADFS** 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.

Configuring Salesforce with MobileIron Access

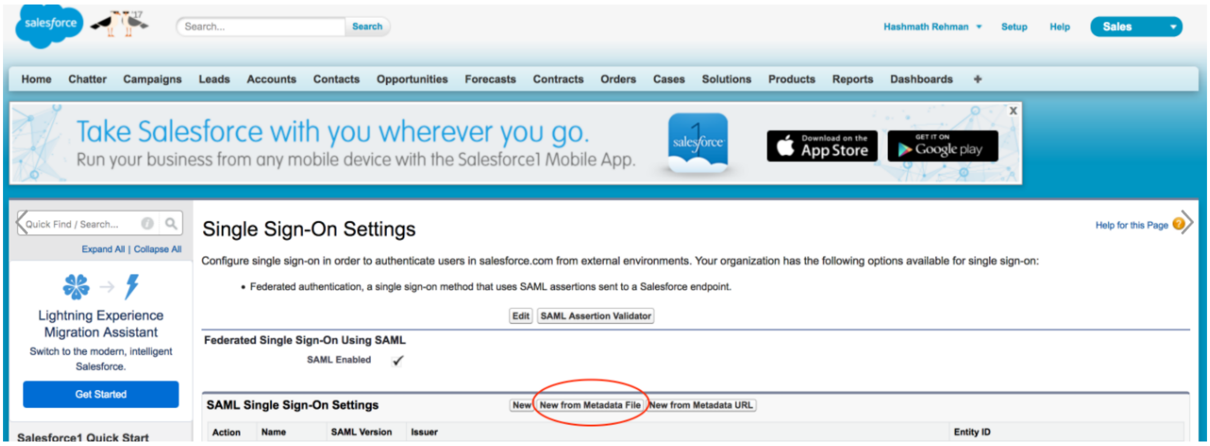
You must configure Salesforce to use with Access.

Prerequisites

- Verify that you have created a federated pair with Salesforce and ADFS.
- Verify that you have configured Salesforce and ADFS natively.

Procedure

1. Login to the Salesforce admin portal.
2. Expand **Security Controls**, and select **Single Sign-On Settings**.
3. On the **SAML Single Sign-On Settings**, click **New from Metadata file**.



Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

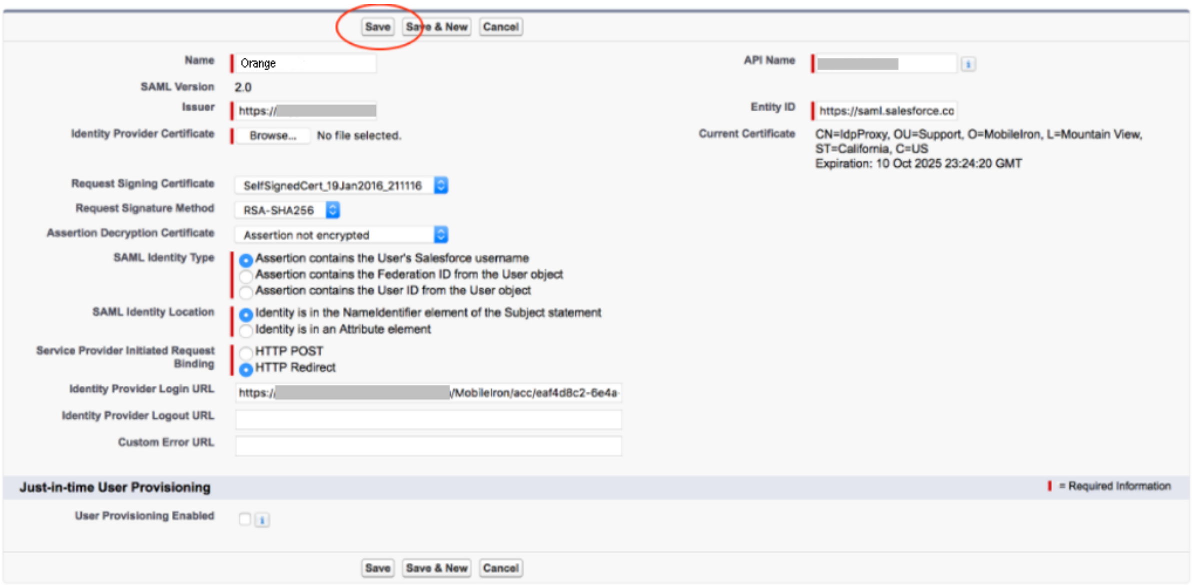
Federated Single Sign-On Using SAML

SAML Enabled ✓

SAML Single Sign-On Settings

Action	Name	SAML Version	Issuer	Entity ID

4. Upload the "**Access IDP Metadata (Upload to SP)**" that you downloaded in **Step 10** of Configuring Access to create a Federated Pair.
   Note: If certificate-based SSO is enabled, Request Signature method must be set to RSA-SHA256.
5. Click **Save**.



Name	Orange	API Name	[redacted]
SAML Version	2.0		
Issuer	https://[redacted]	Entity ID	https://saml.salesforce.co
Identity Provider Certificate	Browse... 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	SelfSignedCert_19Jan2016_211116		
Request Signature Method	RSA-SHA256		
Assertion Decryption Certificate	Assertion not encrypted		
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	https://[redacted]/MobileIron/acc/eaf4d8c2-6e4a		
Identity Provider Logout URL			
Custom Error URL			

Just-in-time User Provisioning

❙ = Required Information

User Provisioning Enabled □

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

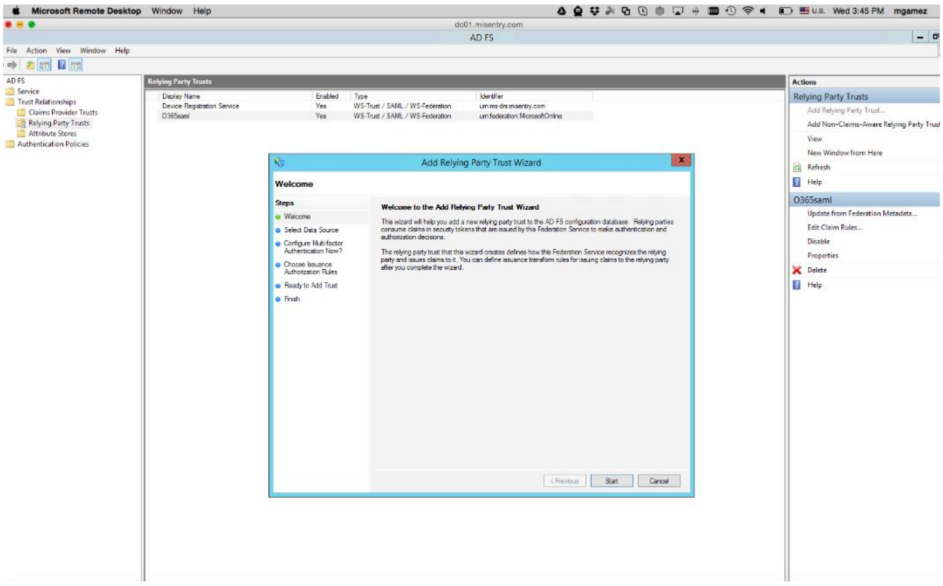
Task Result

Salesforce is configured with Access.

Configuring ADFS with MobileIron Access

You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

1. Use Remote Desktop services to log into an ADFS machine with Admin credentials.
2. Click **Start** > **Administrative tools** > **ADFS Management** > Expand **Trust Relationships.**
3. Click **Relying Party Trust.** In the right-hand pane, click **Add Relying Party Trust** and follow the prompts.



Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	urn:ms-drs:misentry.com
O365saml	Yes	WS-Trust / SAML / WS-Federation	urn:federation:MicrosoftOnline

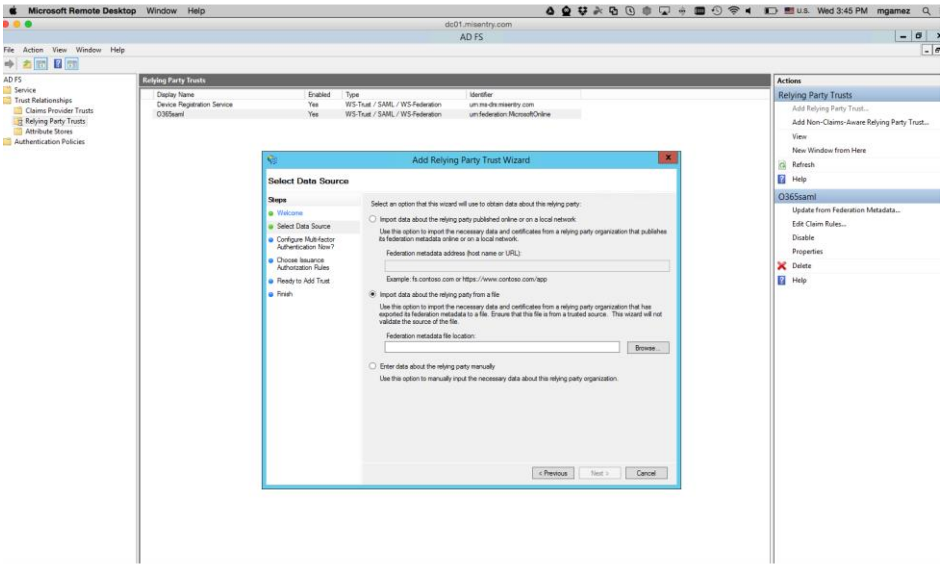
Welcome

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

4. Click **Start** and select **Import data about the relying party from a file**. Click **Next**.



Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	urn:ms-drs:misentry.com
O365saml	Yes	WS-Trust / SAML / WS-Federation	urn:federation:MicrosoftOnline

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

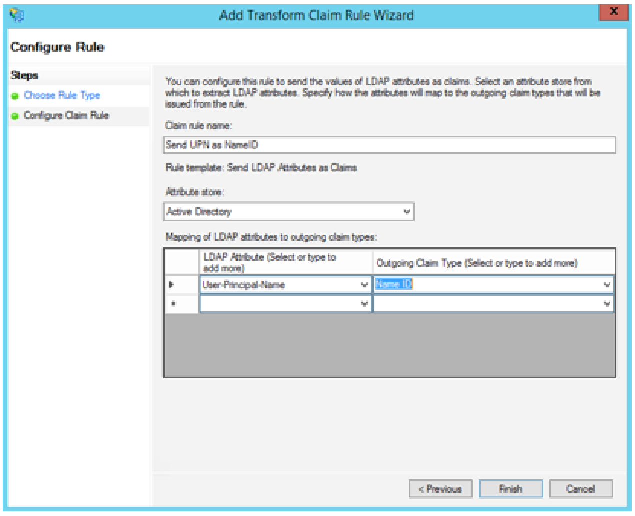
Use this option to manually input the necessary data about this relying party organization.

5. Click **Browse** and select the service provider proxy metadata file that you downloaded and click **Next**.

   Note: The filename for the proxy metadata file name ends with *UploadTo-Microsoft ADFS-IdP.xml*.

6. Enter the **Display Name** and click **Next.**
   All other fields are set to defaults. Click **Add Rule**.
7. At the end, select **Open Edit Claim rules dialog for relying party trust**.
8. Select SHA01 for encrypted algorithm.
9. In the **Claim Rule Template** drop-down, select **Send LDAP Attributes as Claims.**
10. Click **Next.**

a) On the **Configure Claim Rule** step, enter the following details and click **Finish**.



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Send UPN as NameID

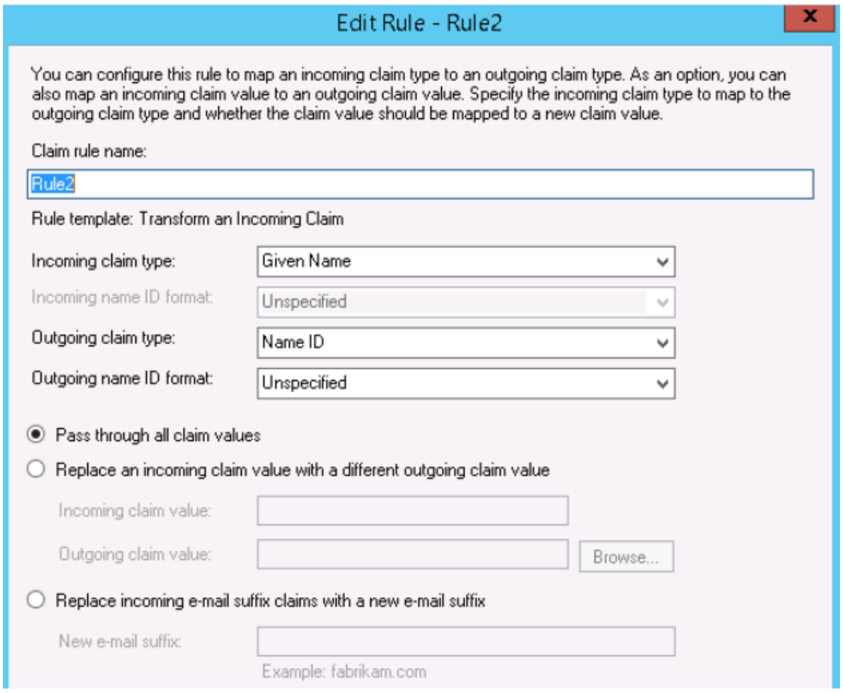
Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▸	User-Principal-Name	Name ID
*		

11. Add another rule and select the option **Transform an Incoming Claim**. Click **Next**.
12. Enter a name for the rule. The incoming type is Given Name and Outgoing Type is Name ID. The outgoing name ID format must be **Unspecified**.



You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Rule2

Rule template: Transform an Incoming Claim

Incoming claim type: Given Name

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Unspecified

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

13. Click **Apply** and **OK.**

Registering 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.

Verification

Salesforce and Microsoft ADFS is now configured with MobileIron Access. You must validate the new federation settings.

- Login to Salesforce domain with a test user and observe the SAML flow in Sentry logs.
- SAML SSO traffic should be redirected to Access instead of going directly to ADFS. Note: This works only if this option is chosen while adding the Federated Pair.