

MobileIron Access Cookbook

Access with ServiceNow and Microsoft ADFS

01/02/2018

Contents

Overview.....	3
Prerequisites.....	3
Configuring ServiceNow and Microsoft ADFS with MobileIron Access.....	4
Registering Sentry to Access	4
Configuring Access to create a Federated Pair	4
Configuring ServiceNow with MobileIron Access.....	5
Configuring ADFS with MobileIron Access	6
Verification	10

Overview

SAML provides single sign-on service for users accessing their services hosted in a cloud environment. Generally, a service provider such as ServiceNow 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 ServiceNow.

This guide serves as step-by-step configuration manual for users using ADFS as an authentication provider with ServiceNow in a cloud environment.

Disclaimer:

This cookbook is informational to help with the setup flow and actual screenshots. The steps might vary in your deployment scenario due to changes in SP/IdP versions.

Prerequisites

- Ensure that you have a working setup of the ServiceNow and ADFS pair without MobileIron Access.
- **Metadata files for ServiceNow**
For more information, see http://wiki.servicenow.com/index.php?title=Configuring_ADFS_3.0_to_Communicate_with_SAML_2.0#gsc.tab=0
 - Login to ServiceNow with admin credentials.
 - Navigate to **Multi Provider SSO > Identity Providers > ADFS Identity Provider**.
 - Note the following attributes:
Entity ID: <https://developer.servicenow.com>
Assertion Consumer Service URL: <https://developer.servicenow.com/navpage.do>
- **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 ServiceNow and Microsoft ADFS with MobileIron Access

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

- [Registering Sentry to Access](#)
- [Configuring Access to create a Federated Pair](#)
- [Configuring ServiceNow with MobileIron Access](#)
- [Configuring ADFS with MobileIron Access](#)

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.

Configuring Access to create a Federated Pair

You must configure Access to create a federated pair.

Prerequisites

Verify that you have configured ServiceNow and ADFS natively.

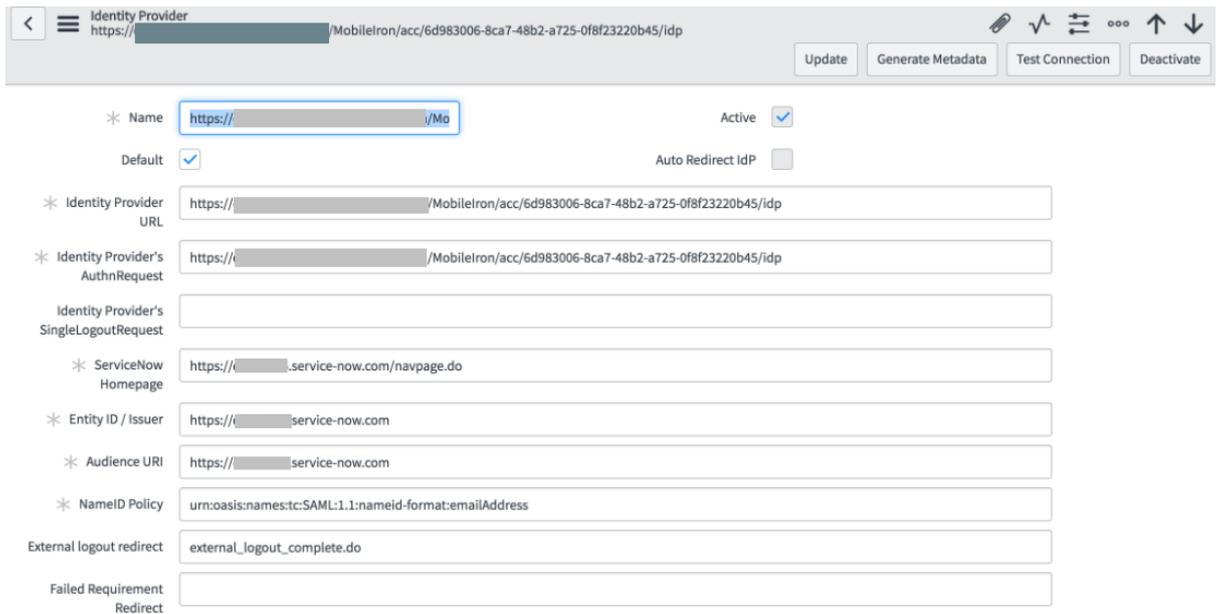
Procedure

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 **ServiceNow** 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. Add the metadata file details for the service provider
Entity ID: <https://developer.servicenow.com>
ServiceNow Homepage: <https://developer.servicenow.com/navpage.do>
 - 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 ServiceNow with MobileIron Access

You must configure the service provider with the identity provider metadata file.

1. Login to ServiceNow account with admin credentials – <https://developer.servicenow.com>.
2. Search for **Multi** in the search filter > **Identity Providers > New > SAML > Import IdP Metadata** using **ACCESS IdP Metadata (Upload to SP)** downloaded in **Step 10** of Configuring Access to create a Federated Pair.
3. Click **Test Connection** > enter the **Username and Password** > **Sign On**. Test Connection must be successful.

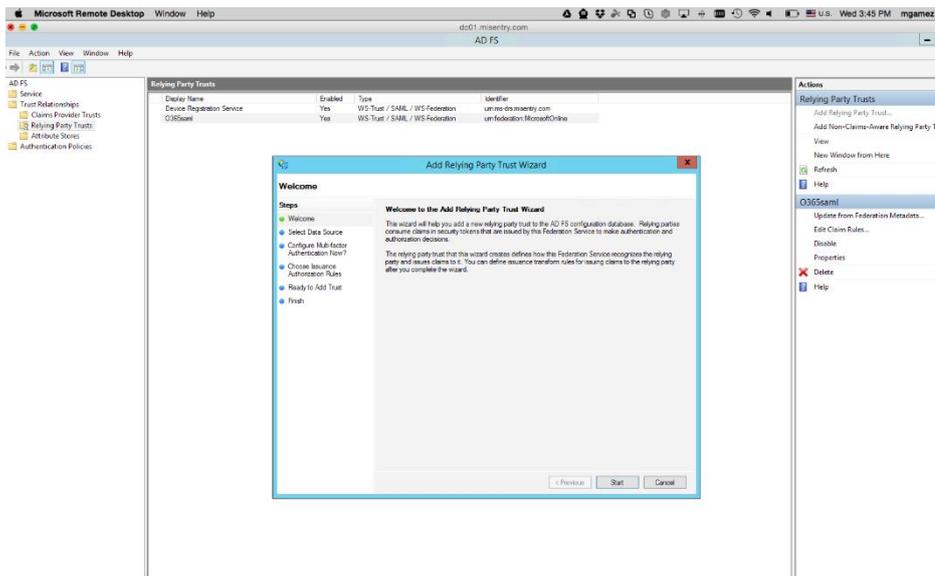


4. Click **Activate** to activate the rule. The Activate button is available after the connection is tested.
5. Click **Set as Auto Redirect IdP** to enable Auto Redirect IdP.

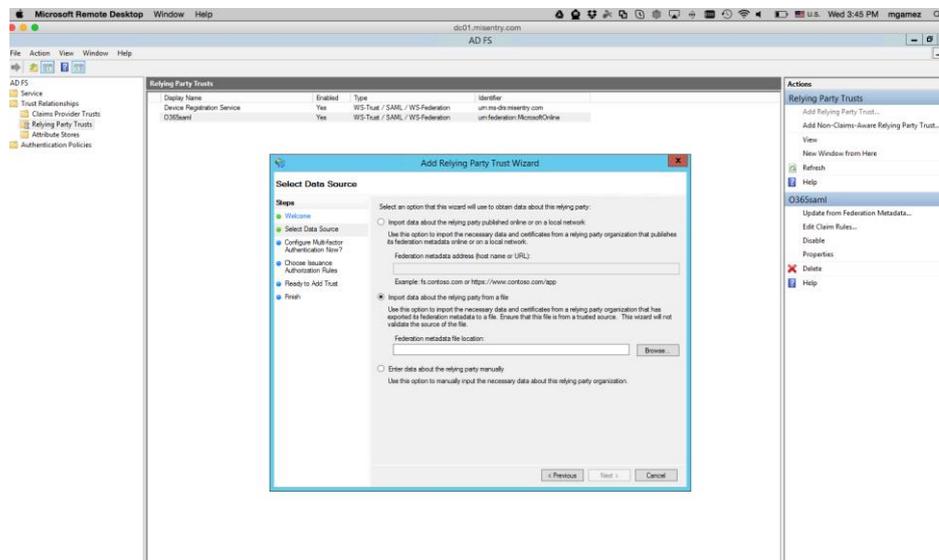
Configuring ADFS with MobileIron Access

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.



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



- Click **Browse** and select the service provider proxy metadata file that you downloaded in **Step 10** of [Configuring Access to create a Federated Pair](#) and click **Next**.
- Clear the Open the Claims when this finishes checkbox and close the page.
- Right-click the relying party trust and select **Properties**.
- Click **Advanced** and select **SHA-1** for secure hash algorithm.
- Browse to the Endpoints tab and add a SAML Assertion Consumer with a Post binding and a URL of <https://developer.servicenow.com/navpage.do>.
- Right-click on relying party trust and select **Edit Claim Rules**.
- On the Issuance Transform Rules tab, select **Add Rules**.
- In the **Claim Rule Template** drop-down, select **Send LDAP Attributes as Claims**.
- Click **Next**.
 - On the **Configure Claim Rule** step, enter the following details and click **Finish**.

Edit Rule - Get Attribute

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:

Rule template: Send LDAP Attributes as Claims

Attribute store:

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)
▶	E-MailAddresses	E-Mail Address
*		

14. Add another rule and select the option **Transform an Incoming Claim**. Click **Next**.
15. 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**.

Edit Rule - Rule2 ✕

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:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

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

16. Click **Apply** and **OK**.

Verification

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

- Login to ServiceNow domain with a test user:
<https://developer.servicenow.com/navpage.do>
- Click **Use External Login** > Enter **Username** and **Password** > follow the prompts.
- Register the mobile device with Core. Launch the ServiceNow application and proceed with logon.
- 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.

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.