MobileIron Access Cookbook

Access with SuccessFactors and Microsoft ADFS

Revised: 03 January 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 SuccessFactors is federated with an identity provider such as Microsoft ADFS for authentication. The user gets authenticated by ADFS and obtains a token for accessing applications in a cloud environment, such as SuccessFactors.
This guide serves as step-by-step configuration manual for users using ADFS as an authentication provider with SuccessFactors 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

Verify that you have the following components in your environment:

- ADFS version 3.0
- Ensure that you have a working setup of native federation for SuccessFactors and ADFS in your environment.
- **ADFS (IDP) Metadata Files**
  Download the ADFS metadata files for ADFS (IdP)
  - Download ADFS metadata file from https://<ADFS Server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml

- **SuccessFactors (SP) Metadata Files**
  You must get the information for metadata files for SuccessFactors (SP) from Single Sign-On Settings.
  - **Tenant ID**: https://salesdemo4.successfactors.com/login?company=<your_company>
  - **EntityID**: https://www.successfactors.com/<your_company>
  - **Assertion Consumer Service URL**: https://salesdemo4.successfactors.com/saml2/SAMLAssertionConsumer?<your_company>

Configuring SuccessFactors and Microsoft ADFS with MobileIron Access

You must perform the following tasks to accomplish the configuration between SuccessFactors and ADFS:

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. 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.

Configure Access to create a Federated Pair

You must configure Access to select your service provider and the identity provider to create a federated pair.

Prerequisites

Verify that you have the credentials for MobileIron Access.

Procedure

1. In Access, click **Profile** > **Get Started**.
2. Enter the Access host information and upload the ACCESS SSL Certificate. The other fields retain their default values. Click **Save**.
   Note: Perform **steps** 1 and 2 only if a profile is not created.
3. Click **Profile** > **Federated Pairs** > **Add New Pair.**
4. Select SuccessFactors as the service provider.
5. Enter the following details:

   - Name
   - Description
   - Select the **Access Signing Certificate** or use the **Advanced Options** to create a new Access Signing Certificate.
   - Upload or Add the service provider metadata.
     If you select Add, enter the **Entity ID** and **Assertion Consumer Service URL**. See Prerequisites.
   - (Optional): Select **Use Tunnel Certificates for SSO** for users to be authenticated automatically. This leverages the user's authentication in the MobileIron Tunnel VPN. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/curent/accs.

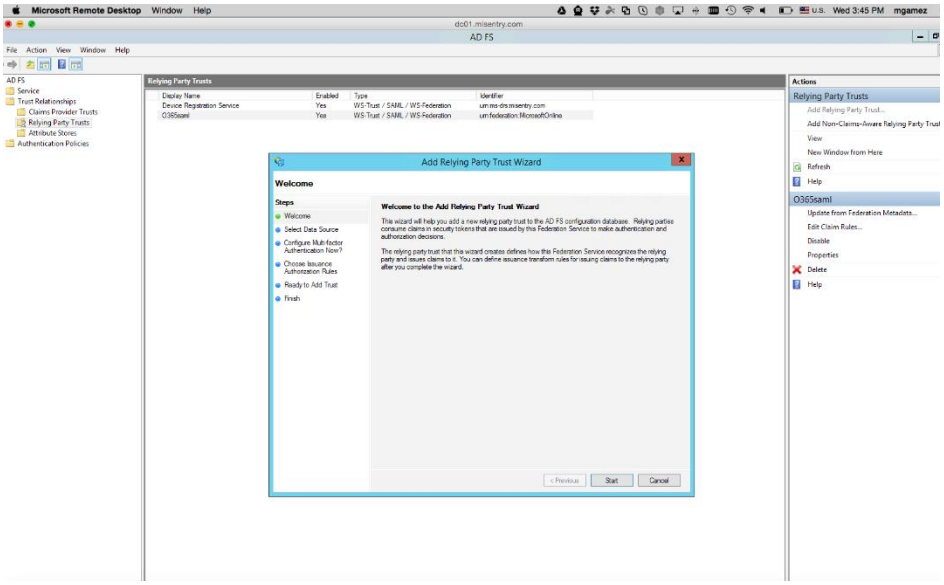
6. Click **Next** and select **Microsoft** as the identity provider.
7. Select the **Access Signing Certificate** or use the **Advanced Options** to create a new self-signed Access Signing Certificate.
8. Select Upload Metadata, Add Metadata, or Metadata URL to provide the **IdP metadata** details that you saved. See Prerequisites.
   See https://support.mobileiron.com/docs/curent/accs for more information.
   Click **Done**.
9. Download the **Access SP Metadata (Upload to IDP)** and **ACCESS IDP Metadata (Upload to SP)** metadata files.
10. Click **Publish** to publish the profile.

Configure the ADFS environment with MobileIron Access

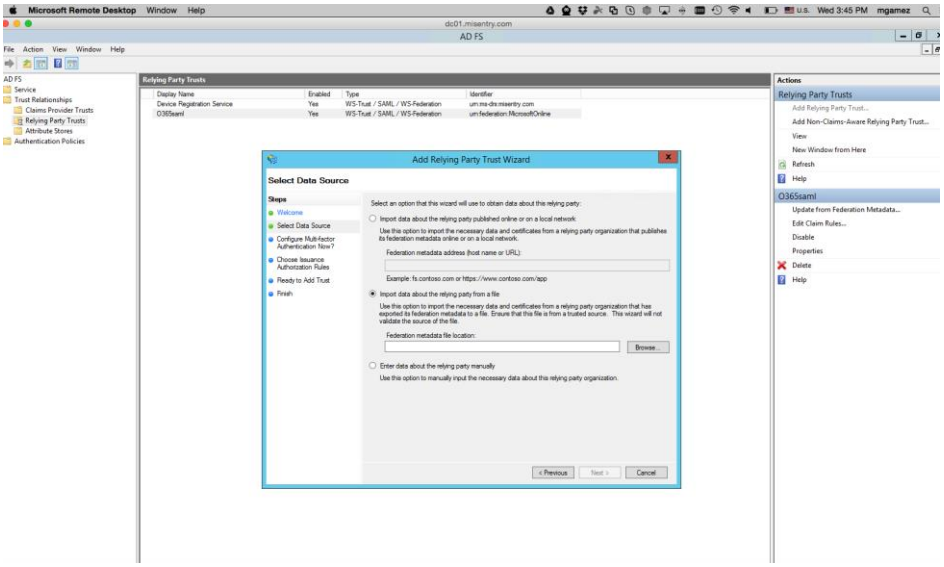
You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

Procedure

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.** Right-click and select **Add Relying Party Trust** and follow the prompts.

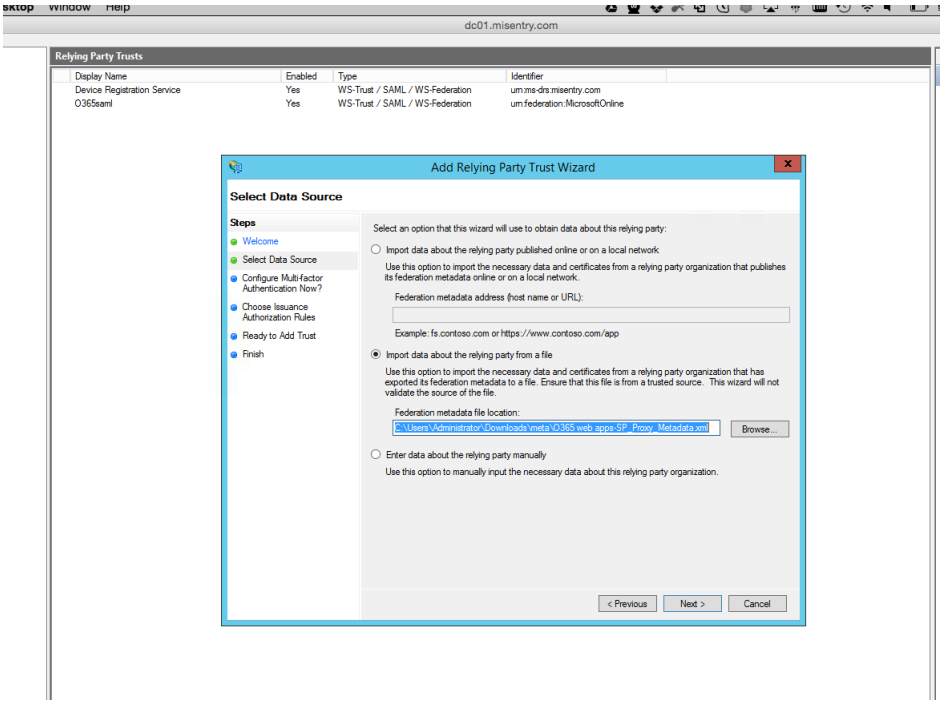


4. Click **Start** and select **Import data about the relying party from a file**. Click **Next**.

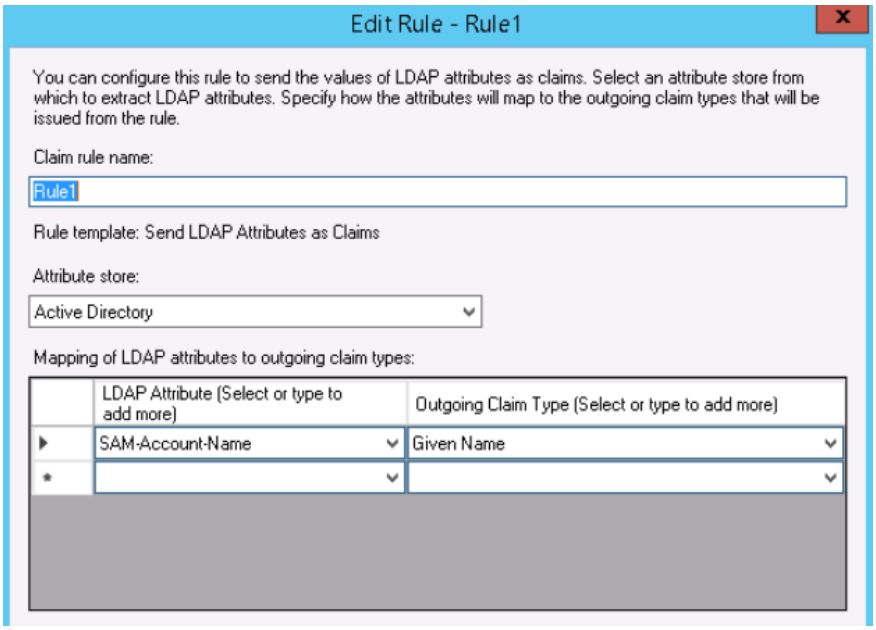


5. Click **Browse** and select the service provider proxy metadata file that you downloaded and click **Next**.

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

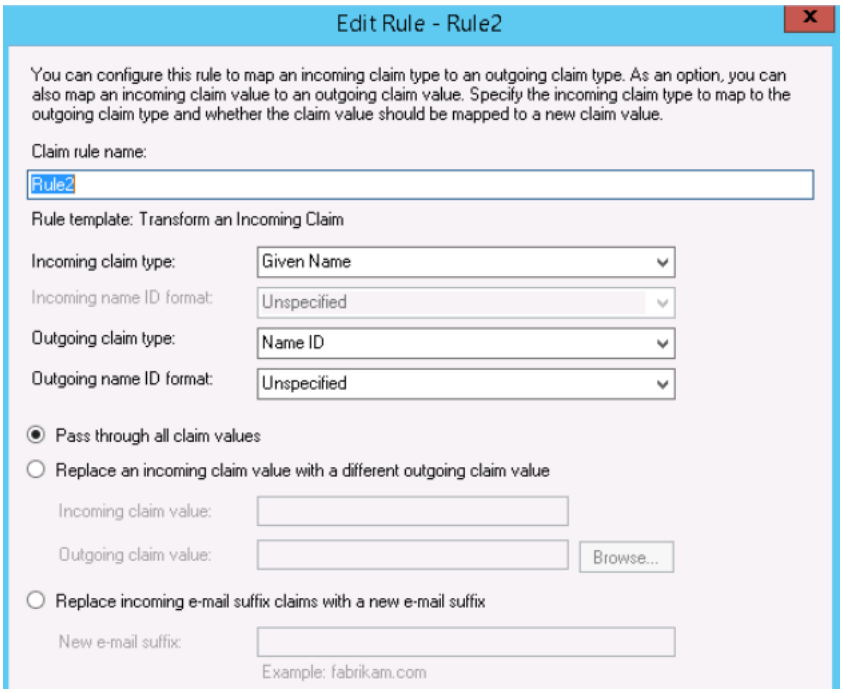


6. Enter the **Display Name** and click **Next.**
   All other fields are set to defaults. Click **Add Rule**.
7. At the end, select **Open Edit Claim rules dialog for relying party trust**.
8. Select RSA-SHA01 or RSA-SHA256 for encrypted algorithm.
9. In the **Claim Rule Template** drop-down, select **Send LDAP Attributes as Claims** and click **Next.**
10. Configure the **Claim rules** as follows:



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**.



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

Configure the SuccessFactors environment with MobileIron Access

Procedure

1. Login to SAP SuccessFactors instance and click **Single Sign-On (SSO)** settings.
2. Extract the **SAML Issuer**, **Certificate**, **Global Logout Service URL (Logout Request destination)**, **Single Sign On** redirect service location from the metadata file that you downloaded in the Step 10 of.Configure Access to create a Federated Pair.

3. Configure **SSO settings** as shown below on the **Success Factors portal**.

SAML v2 : SP-initiated logout

Support SP-initiated Global Logout	Yes
SP sign LogoutRequest	No
SP validate LogoutResponse	No
Global Logout Service URL (LogoutRequest destination)	https://[redacted]-alt.auto.mobileiron.com/[redacted]/acc/dad0e42

SAML V2 : IDP-initiated Global Logout

SP validate LogoutRequest signature	Yes
SP sign LogoutResponse	Yes
Global Logout Service URL (LogoutResponse destination)	https://[redacted]-alt.auto.mobileiron.com/[redacted]/acc/dad0e42

SAML v2: Login Response with Http artifact binding

Artifact Resolution Service Location (supplied by idp):	
Require ArtifactResolve Signature (sp to idp)	No
Require ArtifactResponse Signature (idp to sp)	No

SAML v2: NameID Setting

Require sp must encrypt all NameID elements	No
NameID Format	unspecified

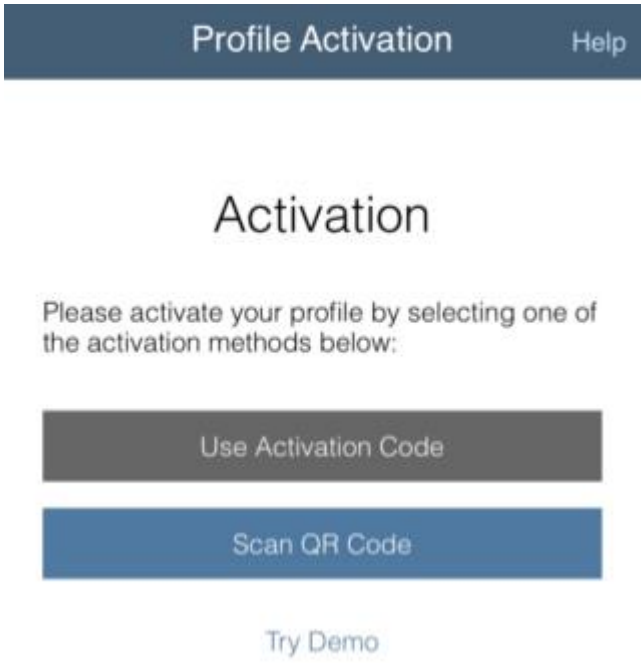
SAML v2 : SP-initiated login

Enable sp initiated login (AuthnRequest)	Yes
Default issuer	☑
single sign on redirect service location (to be provided by idp)	https://[redacted]-alt.auto.mobileiron.com/[redacted]/acc/dad0e42
Send request as Company-Wide issuer	No

Verification

SuccessFactors Mobile App follows Activation process for the user to activate the profile. There are three kinds of Activation models. The following models do not support SAML SSO flow.

1. Activation Code
2. QR Code



3. Email based Activation: This model must be used to use Access with the SuccessFactors mobile application.

    - Download the SuccessFactors mobile application on the device.
    - From safari on iOS and chrome on Android, Access the URL mentioned in step 2 in the email.
      Note: The Access Sentry URL must be added in the Safari domain configuration for Tunnel profile.
      It prompts to open the link in Mobile App on iOS.Click Ok.
      On Android, everything is seamless. This starts the SAML SSO flow.