MobileIron Access Cookbook

Access with Tableau (Cloud or ON-PREMISE) and Microsoft ADFS

Revised: November 02, 2017

Contents

Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Tableau is federated with an identity provider such as Microsoft ADFS for authentication. The user gets authentication from ADFS and obtains a SAML token for accessing applications in a cloud environment, such as Tableau.

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

Prerequisites

Verify that you have the following components in your environment:

- ADFS version 3.0

- Install Active Directory Server

- Ensure that you read about Tableau online tips at https://www.tableau.com/about/blog/2016/8/tableau-online-tips-site-admins-rejoice-adfs-authentication-using-saml-57465

- Ensure that you have a working setup of native federation for Tableau and ADFS in your environment.

- **Tableau Metadata Files**
  Cloud
  You must download the metadata files for Tableau (SP)
  1. Login to Tableau tenant with admin credentials.
  2. Click **Settings** > **Authentication** > **Export Metadata** in Configure site-specific SAML section.
  3. Save the metadata file.

  ON-PREMISE
  The metadata file for on-prem machine is available in the server configuration. The server configuration is available on your machine where you downloaded the file. For example: *C:\Program Files\Tableau\Tableau Server\SAML\*

  Note: The path for server configuration is specific to your machine.

- **ADFS (IDP) Metadata Files**
  You must download the ADFS metadata files for ADFS (IdP)
  Download ADFS metadata file from https://<ADFS Server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml

Configuring Tableau and Microsoft ADFS with MobileIron Access

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

- Configure Access to create a Federated Pair
- Configure the Tableau environment for Cloud
- Configure the Tableau environment for On-Premise
- Configure the ADFS environment
- Register Sentry to Access

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. It creates a federated pair.

Procedure

1. In Access, click **Profiles** > **Get Started**.
2. Enter the Access host information and upload the ACCESS SSL Certificate. Use the default values for the other fields. Click **Save**.
   Note: Perform the above steps if a profile is not created.
3. Click **Profiles** > **Federated Pairs** > **Add New Pair.**
4. Select **Tableau** option under the **Choose Service Provider**.
5. Enter the following details:

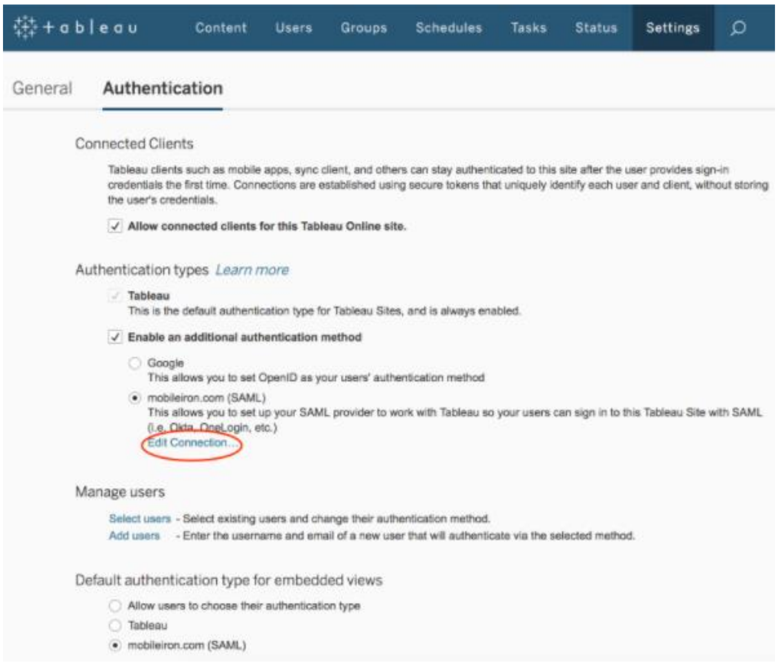
   - Name for the Federated Pair
   - Description
   - Select the **Access Signing Certificate** or use the **Advanced Options** to create a new Access Signing Certificate.
   - **Upload** or **Add Metadata**. See Prerequisites
   - (Optional): Select **Use Tunnel Certificates for SSO** for users to be 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.**
7. Select **Microsoft** as the identity provider.
8. Select the **Access Signing Certificate** or use the **Advanced Options** to create a new self-signed Access Signing Certificate.
9. 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**.

10. Download the **Access SP Metadata (Upload to IDP)** and **ACCESS IDP Metadata (Upload to SP)** metadata files.
11. Click **Publish** to publish the profile.

Configure the Tableau environment for Cloud

Procedure

1. Login to Tableau with admin credentials.
2. Click **Settings** > **Authentication** > **Edit Connection**.



Connected Clients

Tableau clients such as mobile apps, sync client, and others can stay authenticated to this site after the user provides sign-in credentials the first time. Connections are established using secure tokens that uniquely identify each user and client, without storing the user's credentials.

☑ Allow connected clients for this Tableau Online site.

Authentication types *Learn more*

☑ Tableau
This is the default authentication type for Tableau Sites, and is always enabled.

☑ Enable an additional authentication method

○ Google
This allows you to set OpenID as your users' authentication method

● mobileiron.com (SAML)
This allows you to set up your SAML provider to work with Tableau so your users can sign in to this Tableau Site with SAML (i.e. Okta, OneLogin, etc.)
Edit Connection...

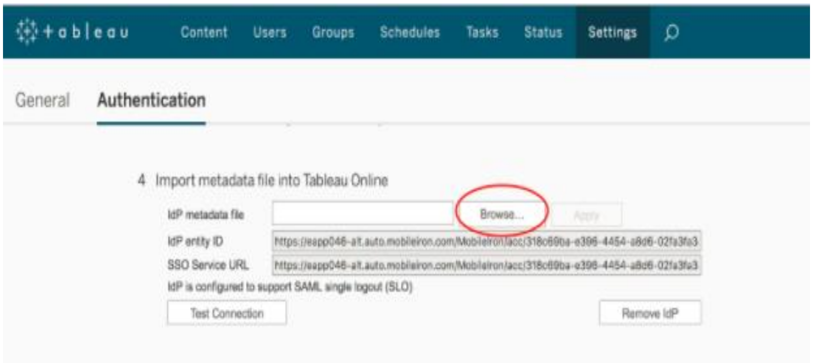
Manage users

Select users - Select existing users and change their authentication method.
Add users - Enter the username and email of a new user that will authenticate via the selected method.

Default authentication type for embedded views

○ Allow users to choose their authentication type
○ Tableau
● mobileiron.com (SAML)

3. Click **Browse** to upload IdP proxy metadata file that you downloaded in the prerequisites section:



4 Import metadata file into Tableau Online

IdP metadata file
IdP entity ID https://eapp046-alt.auto.mobileiron.com/MobileIron/acc/318c69ba-e396-4454-a8d6-02fa3fa3
SSO Service URL https://eapp046-alt.auto.mobileiron.com/MobileIron/acc/318c69ba-e396-4454-a8d6-02fa3fa3
IdP is configured to support SAML single logout (SLO)

Note: The IdP entity ID and SSO Service URL are populated by default when you upload the metadata file.

Configure the Tableau environment for On-Premise

Procedure:

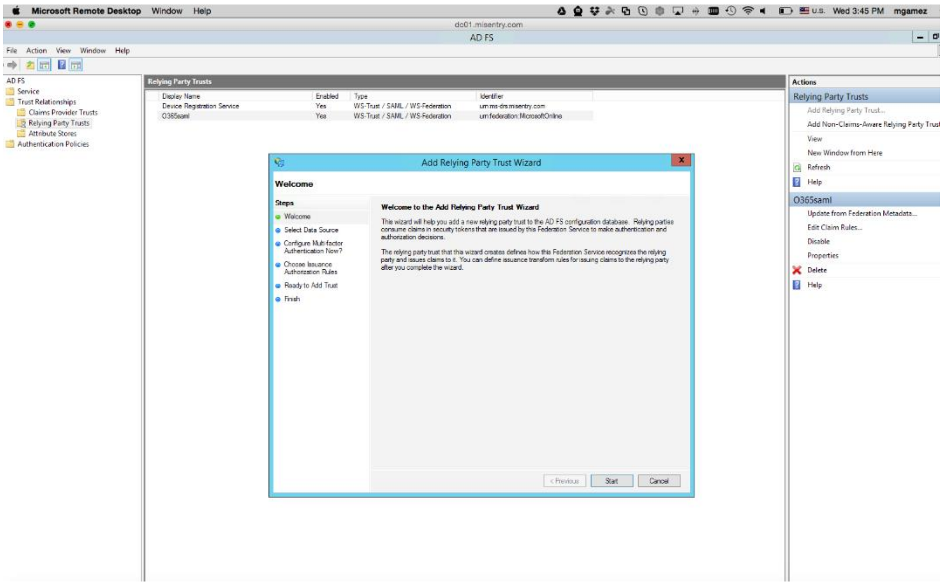
1. Use Remote Desktop Services to log into a Tableau machine with admin credentials.
2. Stop the Tableau service.
3. Verify that the idp-proxy metadata file is available in C:\program Files\Tableau\Tableau Server\SAML\
4. Open the Tableau server configuration and upload the IdP proxy metadata file.
5. Start the Tableau service.

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.** In the right-hand pane, under the **Actions** section 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

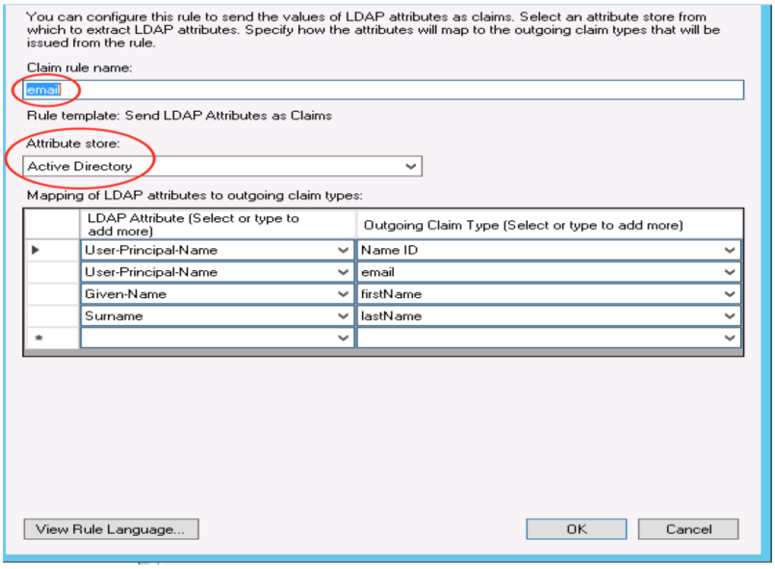
Welcome to the Add Relying Party Trust Wizard

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**.
5. Click **Browse** and select the service provider proxy metadata file that you downloaded when configuring Access and click **Next**.
6. Enter the **Display Name** such as tableau-access and click **Next.**
7. All other fields are set to defaults. Follow the prompts.

8. At the end, select **Open Edit Claim rules dialog for relying party trust**.
9. In the **Claim Rule Template,** drop-down, select **Send LDAP Attributes as Claim** and click **Next.**
10. Configure **Claim rules** as follows:



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: email

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
	User-Principal-Name	email
	Given-Name	firstName
	Surname	lastName
*		

11. Click **OK.**
12. Click **Properties** > **Advanced** tab, select **SHA-1** as **Secure hash algorithm**.
13. Click **Apply** and **OK.**

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 for the profile.
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.

Verification

Single-sign-on service is now configured using SAML with Tableau as the service provider and Microsoft ADFS as the identity provider. This configuration lets you fetch the latest configuration from Access.

1. Register your device with core.
2. Open the Tableau application.
3. Observe the SAML SSO logs in sentry log file.
4. You must be able to login to Tableau server or tenant successfully.