Configuring SSO for Workplace in Active Directory Federation Services (ADFS)

Overview

Active Directory Federation Services is a component that allows organizations to use Single Sign On (SSO) access with other applications. In this guide, we will detail the setup required within ADFS to successfully integrate your SSO with Workplace.

PREREQUISITES

- Your enterprise SSO system uses Windows Server version 2016 or 2012 R2, Active Directory Domain Services (AD DS), and Active Directory Federation Services (AD FS) v3 or v2
- You have Admin privileges on your Workplace instance
- Your Workplace admin user has the exact same email address as your corresponding Active Directory user. If the email addresses are not a case-sensitive match, you will not be able to complete this procedure successfully

To finish this configuration and have AD FS produce a valid SAML Assertion, you MUST be able to authenticate to AD FS as the user that has the exact same email address as your Workplace admin (case sensitive)

These instructions are also applicable to the configuration of Windows Server version 2008 R2 with AD FS v2, but be aware there are some minor differences in the configuration flow.

HIGH-LEVEL STEPS

1. Gather from Workplace the parameters needed to configure AD FS
2. Configure AD FS to enable SAML SSO for Workplace
3. Gather the AD FS parameters needed to configure Workplace
4. Configure Workplace to authenticate users via AD FS
5. Test and Deploy the SSO Configuration within Workplace

Implementation

GATHER THE PARAMETERS NEEDED TO CONFIGURE AD FS

2. Go to the Authentication tab, choose Single Sign-On and find your Audience URL and Recipient URL, which you will need during the AD FS configuration step
Before AD FS will allow federated authentication (i.e., SSO) for an external system, you must set up a Relying Party Trust. This configuration identifies the external system along with the specific technology that is used for SSO. This procedure will create a Relying Party Trust that produces SAML 2.0 Assertions for Workplace.

**CREATE THE RELYING PARTY TRUST**

1. Open the **AD FS Management** snap-in.
2. Under **AD FS > Trust Relationships**, right click on **Relying Party Trusts** and choose **Add Relying Party Trust**....
3. Click **Start** to begin the configuration wizard.

4. Choose the radio button **Enter data about the relying party manually** and click **Next**.

5. Set the **Display Name** as “Workplace” and set the **Notes** as “Configures relying party trust for SSO via SAML to Workplace”. Click **Next**.

6. For the **Profile**, accept the default selection AD FS profile.
7. Click **Next** to skip the optional step of selecting a token signing certificate.

8. Click the checkbox **Enable support for the SAML 2.0 WebSSO protocol**. Enter your Workplace **Recipient URL** into the text box **Relying party SAML 2.0 SSO service URL** and click **Next**.

9. Enter your Workplace **Audience URL** in the text box **Relying Party Trust Identifier**, click **Add** and then click **Next**.
10. Click **Next** to configure the multi-factor authentication setup, if required by your organization (not available in AD FS v2).

11. Click **Next** to accept the default issuance authorization rules.

12. Review your settings and click **Next** to add the relying party trust.

13. Leave the checkbox selected to open the Edit Claim Rules dialog when the wizard closes and click **Close**.

CREATE THE CLAIM RULES

After a user is authenticated, AD FS claim rules specify the data attributes (and those attributes’ format) that will be sent to Workplace in the SAML Response. Since Workplace requires a Name ID element that contains the user’s email address, this example shows a configuration with two rules:

- The first rule extracts the user’s User Principal Name from Active Directory (i.e., the user’s Windows Account Name)
- The second rule transforms the User Principal Name into a Name ID with Email format

**Note:** Depending on the data within your Active Directory, your Claim Rules may differ from this example

To create your claim rules:

1. The window **Edit Claim Rules for Workplace** should open automatically. If not, you can edit claim rules from the AD FS Management snap-in by selecting the **Workplace relying party trust** and in the right-hand window choose **Edit Claim Rules**.

2. Within the **Issuance Transform Rules** tab, click **Add Rule...** to start a new rule.

3. For the **Claim rule** template, select **Send LDAP Attributes as Claims** and click **Next** to continue.
4. Set the **Claim Rule Name** to **Get LDAP Attributes**.

5. Set the **Attribute store** to **Active Directory**.

6. In the first row, set the **LDAP Attribute** to **E-Mail-Addresses** and set the **Outgoing Claim Type** to **E-Mail-Addresses**.

7. Click **Finish** to add the rule.

8. Click **Create Rule...** to start a second new rule.

9. For the **Claim rule template**, select **Transform an Incoming Claim**.
10. For **Claim Rule Name**, enter **Transform Email Address**.
11. For **Incoming claim type**, select **E-Mail Address**.
12. For **Outcoming claim type**, select **Name ID**.
13. For **Outgoing name ID format**, select **Email**.
14. Accept the default radio button selection **Pass through all claim values**.

15. Click **Finish** to add the rule.
16. Click **Apply** to enact the claim rules.
GATHER THE AD FS PARAMETERS NEEDED TO CONFIGURE WORKPLACE

1. Open the **AD FS Management** snap-in.
2. Navigate to **AD FS > Service > Endpoints**
3. Confirm the URL of your AD FS metadata under the heading **Metadata**.
4. From a web browser, open your AD FS metadata file. This location will be something like:
5. Make a note of your **SAML Issuer URL**, which is contained in the **entityID** attribute of the **EntityDescriptor** element.
6. You will also need to make a note of your **SAML URL**, which is contained in the **Location** attribute of the **AssertionConsumerService** element that has **Binding** type urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.

   <!-- The entityId value is your Workplace SAML Issuer URL -->
   <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="_f20fe059-194a-45aa"
   <!-- The Location value is your Workplace SAML URL -->
   <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

CONVERT YOUR TOKEN-SIGNING CERTIFICATE INTO X509 FORMAT

1. From the AD FS management console, choose **AD FS > Service > Certificates**. Right click on your Token-signing certificate and click **View Certificate**...

2. Choose the **Details** tab and click the button **Copy to File**...
3. Click **Next** to start the wizard.

4. Choose **Base-64 encoded X.509 (.CER)**.

5. Choose a location on the file system to save the exported certificate file.

6. Click **Finish** to complete the export.
Configuring Workplace

In order to configure Workplace to delegate to your SSO provider please follow the setup guide [here](#).

**Note:** Depending on your browser settings, the SSO test pop-up may be blocked. Please allow all pop-ups from Facebook in order for the test to run.