Axure Share Enterprise Single Sign-On with Microsoft's Active Directory Federation Service

This document will walk you through setting up Single Sign-On (SSO) for your Axure Share Enterprise (ASE) server with Microsoft's Active Directory Federation Service (ADFS).

**Note:** This document assumes you have some prior knowledge of server setups.

**Prerequisites**

- You must already have an Active Directory domain controller, DNS, DHCP, ASE, database, and Certificate Authority servers in working order.

- The ASE server requires an SSL certificate, and you must install it before beginning the steps below.

- You should already have installed the ASE software. Make sure to check the box for **Force HTTPS (SSL) connections** on the Axure Share Enterprise Settings screen of the Axure Share Server Manager.

You can find the ASE installation guide at the link below: [https://docs.axure.com/axure-cloud/business/install-on-premises/](https://docs.axure.com/axure-cloud/business/install-on-premises/)

- You must have admin permissions for both ASE and ADFS.

- The ADFS server must already be joined to the same domain as the Active Directory (AD) before it can be configured.

- Domain account attributes must be configured before you start [Section 1.b](#).

**Setup Overview**

1. Configure ADFS for ASE
   a. Add a relying party trust for ASE
   b. Map email to domain account
   c. Export the ADFS security certificate

2. Enable Single Sign-On in the ASE Admin Settings
1 – Configure ADFS for ASE

1.a – Add Relying Party Trust for ASE

1. Open the Server Manager Dashboard and go to Tools > AD FS Management.

2. In the AD FS window, right-click Relying Party Trust in the left column and select Add Relying Party Trust.

3. In the wizard that appears, make sure Claims aware is selected on the Welcome screen and click Start.

4. On the Select Data Source screen, select Enter data about the relying party manually.

5. On the Specify Display Name screen, enter a descriptive display name for the relying party. Click Next and then click Next again on the Configure Certificate screen.
6. On the **Configure URL** screen, check the box for **Enable support for the SAML 2.0 WebSSO protocol**. Then, enter your service URL in the text field. The service URL is case sensitive and must be in the following format:

https://**hostname.domain**/identity/consume/

- **hostname**: hostname of the ASE server
- **domain**: the local domain the ASE server is located on

For example: https://ASETest.classyharbor.local/identity/consume/
7. On the **Configure Identifiers** screen, enter your ASE server's URL in FQDN format: `https://hostname.domain`. For example: `https://ASETest.classyharbor.local`

Then click **Add** to move it into the list of relying party trust identifiers.

8. On the **Choose Access Control Policy** screen, select **Permit everyone** for now. You can fine tune permissions later once you have everything set up and working.

9. Click **Next** on the **Ready to Add Trust** screen. On the **Finish** screen, make sure the box for **Configure claims issuance policy for this application** is checked and click **Close**.
1.b – Map Email to Domain Account

1. Back in the AD FS window, go to the Actions panel on the right and click Edit Claim Issuance Policy under the name of the relying party trust you just created in Section 1.a.

2. In the window that appears, click Add Rule.

3. On the Choose Rule Type screen of the wizard that appears, select Send LDAP Attributes as Claims in the Claim rule template dropdown.
4. On the **Configure Claim Rule** screen, enter a descriptive name for the rule and select **Active Directory** in the **Attribute store** dropdown.

The table at the bottom of the screen is where you'll map your LDAP attributes to the outgoing claim types. Add a new row and select **E-Mail-Addresses** in the left dropdown and **Name ID** in the right.

![Configure Rule](image)

**Configure Rule**

- **Steps**
  - Choose Rule Type
  - Configure Claim Rule

**Claim rule name:**
- [email to domain account]

**Rule template:** Send LDAP Attributes as Claims

**Attribute store:**
- Active Directory

**Mapping of LDAP attributes to outgoing claim types:**

<table>
<thead>
<tr>
<th>LDAP Attribute (Select or type to add more)</th>
<th>Outgoing Claim Type (Select or type to add more)</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail-Addresses</td>
<td>Name ID</td>
</tr>
</tbody>
</table>

**Note:** If the dropdowns in the table are empty, that means your domain account attributes haven't yet been configured. Configure them now, and then return to this step to continue.

5. Click **Finish** to close the wizard, and then click **Apply** in the **Edit Claim Issuance Policy** window to complete the mapping.
1.c – Export the ADFS security certificate

1. Back in the AD FS window, expand the Service item in the left column and select Certificates. Then double-click the certificate listed under Token-signing in the center of the window.

2. In the window that appears, select the Details tab and click Copy to File.
3. In the wizard that appears, click **Next**, and then select **Base-64 X.509 (.CER)** on the following screen.

4. On the following screen, enter a descriptive name for the exported .CER file and select a save location. You'll need to access the file from your ASE server in **Section 2** of this guide, so make sure to save it in a shared location or copy it to a removable storage device.

5. On the next screen, click **Finish** to export the security certificate to your chosen location.
2 – Enable Single Sign-On in the ASE Admin Settings

**Note:** If you haven't yet installed the ASE software, do so now before continuing. See the Prerequisites section on the first page of this document for all requirements.

1. Log in to the ASE web interface with an admin account and go to the Admin page.

2. On the Single Sign On (SAML) tab, fill in the form as follows:

   - **Sign On URL:** The ASE server's full URL followed by /adfs/ls/. For example: https://ASETest.classyharbor.local/adfs/ls/
   
   - **Logout URL:** The URL end users will be directed to after logging out. This can be any URL you want. If you'd like users to be directed back to the login screen, use the sign-on URL.
   
   - **Security Certificate:** The exported .CER file from Section 1.c of this guide

3. Click **Save** to commit the changes and get your SSO URL. You can now enable SAML on your end users' accounts by following the steps at the link below:

   https://docs.axure.com/axure-cloud/business/accounts-permissions-workspaces/#adding-and-removing-saml-from-user-accounts