Engage SAML Single Sign-On Set up Guide

Revision history

Rev	Date	Author	Description
1	04/03/2022	Wilson Lun	Initial Draft
2	24/06/2022	Wilson Lun	Add section to configure Azure Active Directory for SSO
3	23/03/2023	Brian Law	Remove authority claim rule Add authority_id claim rule

Disclaimer

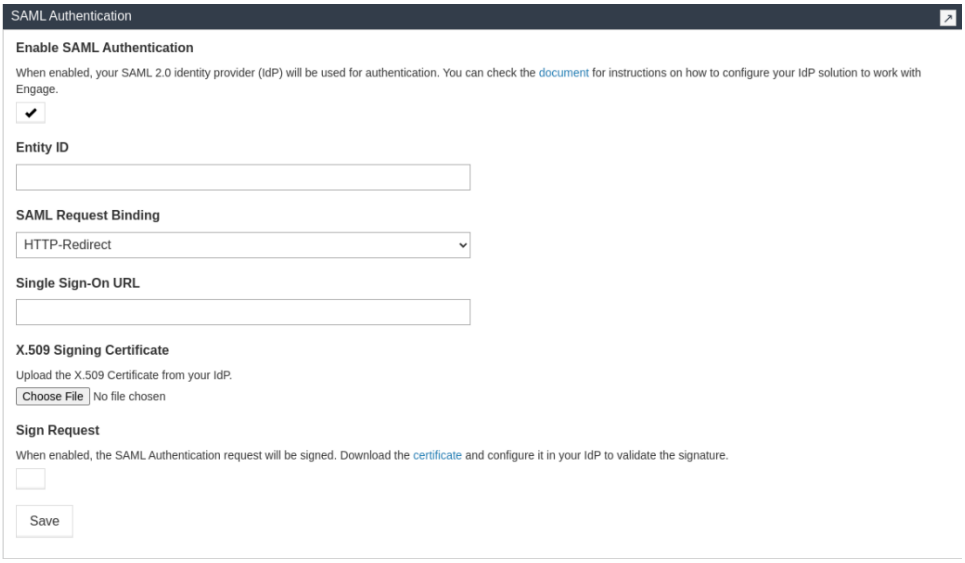
Trademarks and copyright

Contents

Configure SAML authentication in Engage

To set up SAML 2.0 based federation, it is required to configure Engage and the identity provider to trust each other. This section describes the configuration to enable this trust environment for the Engage side.

1. Sign in to Engage with an Administrator user account
2. Navigate to the **SAML Authentication** tab: **Manage Domain > Details > SAML Authentication**
3. In the **SAML Authentication** tab, toggle the checkbox under **Enable SAML Authentication**



4. In the **Entity ID** textbox, input the entity ID of the identity provider
5. In **SAML Request Binding** dropdown box, select the binding protocol for **Single Sign-On URL**
6. In **Single Sign-On URL** textbox, input the endpoint URL of single sign-on service provided by the identity provider
7. Under **X.509 signing certificate**, click **Choose File** and upload the public certificate from identify provider
8. Under **Sign request**, toggle the checkbox if expect SAML request is signed by Engage. If enable this setting, download the certificate provided by Engage and configure it in the identify provider.

Configuring Your SAML 2.0 Identity Provider solution to work with Engage

After setting up SAML authentication in the previous section, the identity provider (IdP) used for authentication will be known to Engage. The next step is to configure Engage as a service provider in your IdP.

To allow Engage to know about a user after the identity is verified by IdP, claims are required to be configured in your IdP such that the identity information is included in the authentication response. A list of the available claims used by Engage is shown below.

Name ID (Required)

This is an identifier of the user who is being authenticated.

user_loginname (Required)

This is the Engage login username of the user who is being authenticated. It must be in email address format.

authority_id (Optional)

This is a list of Engage user roles to be granted to the user who is being authenticated.

Engage manages user access control to resources through the use of user roles. User roles can be configured for users under **Mange Users** in Engage web application. After enabling Engage SAML Single Sign-On, user roles can also be granted by the authority_id attribute.

The user role authority id can be found in the **Appendix: Authority Id List**.

The following excerpt shows an example of attribute in SAML response:

```
<Attribute Name="authority_id">
  <AttributeValue>101</AttributeValue>
  <AttributeValue>103</AttributeValue>
  <AttributeValue>202</AttributeValue>
</Attribute>
```

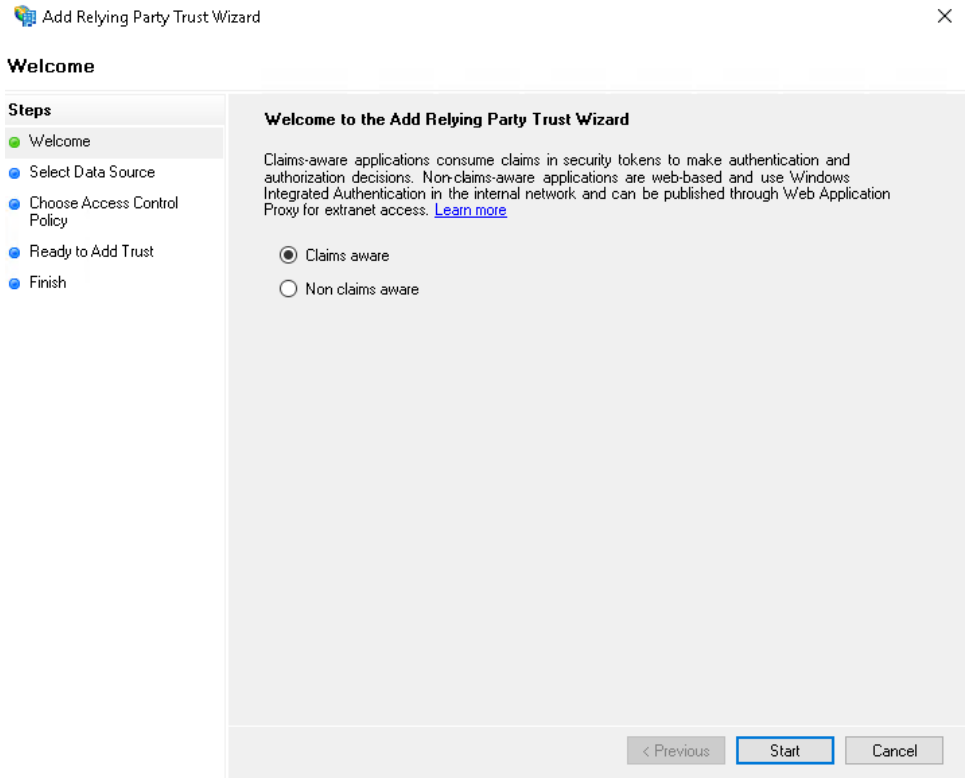
Configure ADFS as an Identity Provider for Single Sign-on

This section provided instructions on how to integrate Active Directory Federation Services (ADFS) instances with Engage using SAML-based single-sign-on (SSO).

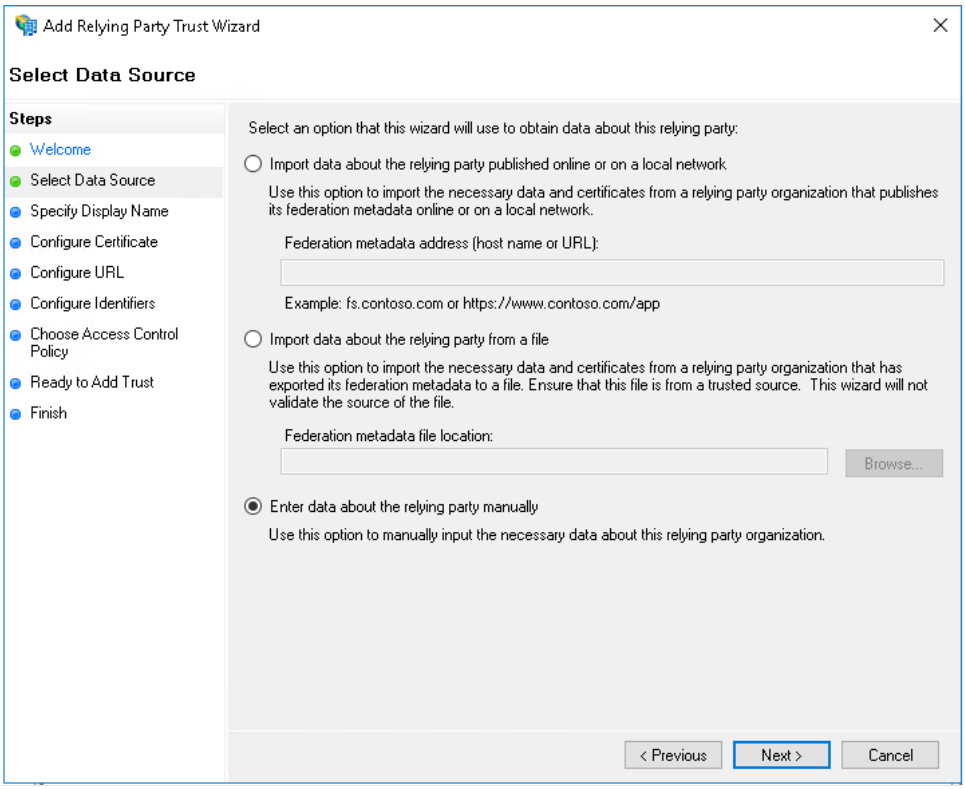
Configure Engage as a trusted relying party

To begin, we first configure the ADFS server to trust Engage as a relying party.

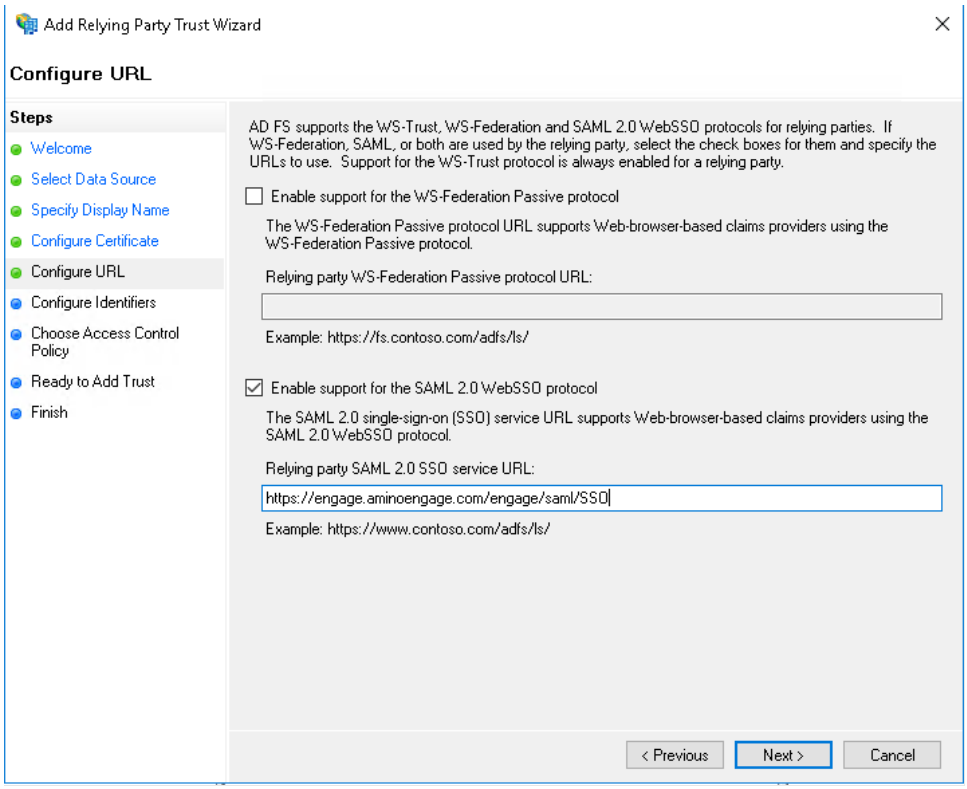
1. Sign in to the ADFS server
2. Open the Server Manager and select **AD FS Management** from Tools
3. In the left console tree, right-click **Relying Party Trusts** and then click **Add Relying Party Trust...**
4. In the **Add Relying Party Trust Wizard**, select the option **Claims aware** and click **Start**



5. In the **Select Data Source** tab, select the option **Enter data about the relying party manually**



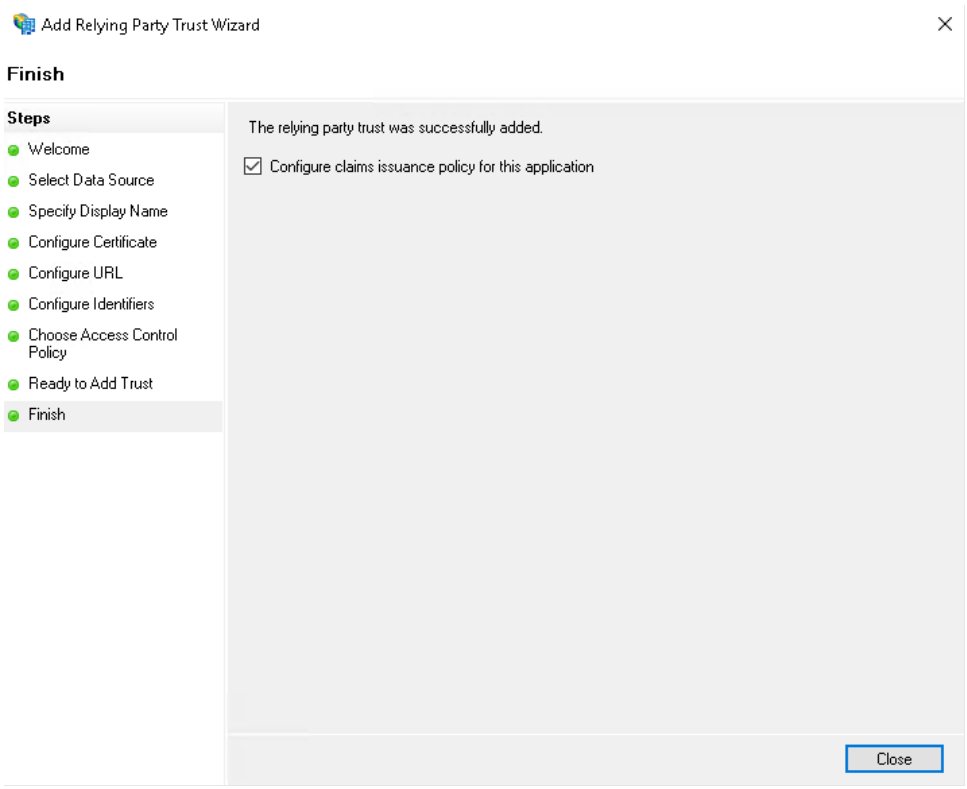
6. In the **Specify Display Name** tab, specify the display name for the application.
7. In the **Configure Certificate** tab, leave the certificate settings at their defaults.
8. In the **Configure URL** tab, select the box **Enable support for the SAML 2.0 WebSSO protocol** and enter the SAML service endpoint.
    a. For Engage: https://engage.aminoengage.com/engage/saml/SSO
    b. For Orchestrate: https://system.amino-orchestrate.com/system/saml/SSO



9. In the **Configure Identifiers** tab, enter
    a. For Engage: https://engage.aminoengage.com/engage/saml/sp
    b. For Orchestrate: https://system.amino-orchestrate.com/system/saml/sp

    and click **Add**

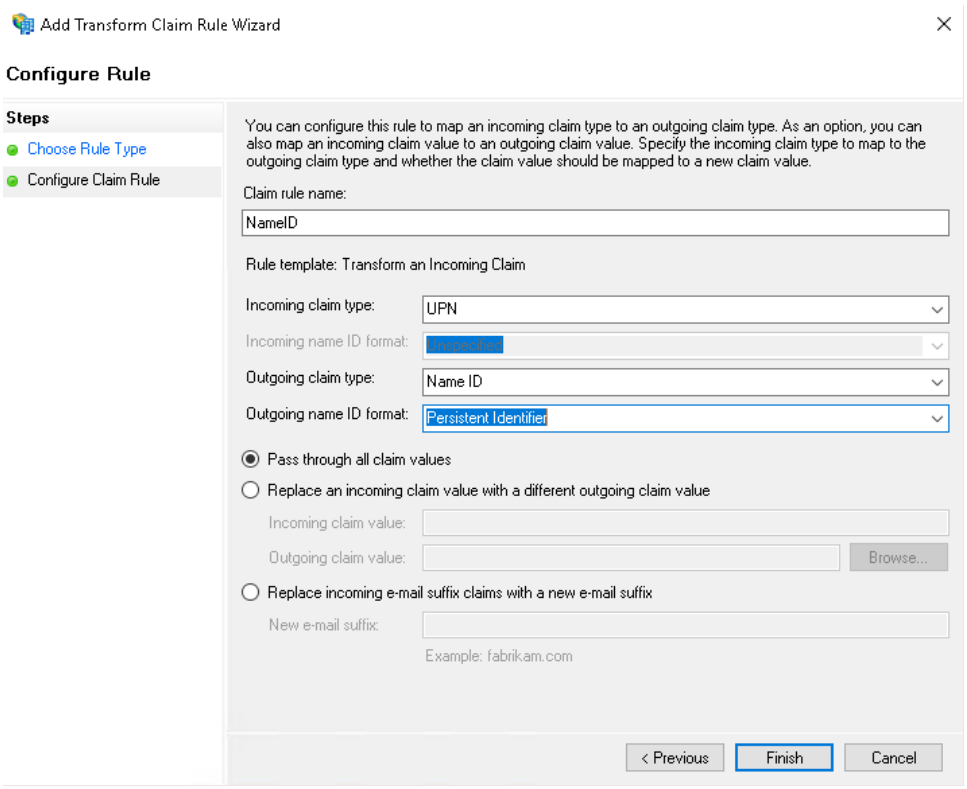
10. In the **Choose Access Control Policy** tab, select **Permit all users to access this relying party**, then click **Next** and review your setting.
11. In **Ready to Add Trust** tab, click **Next** if information is correct.
12. In **Finish** tab, toggle **Configure claims issuance policy for this application**, and click **Close** to complete.



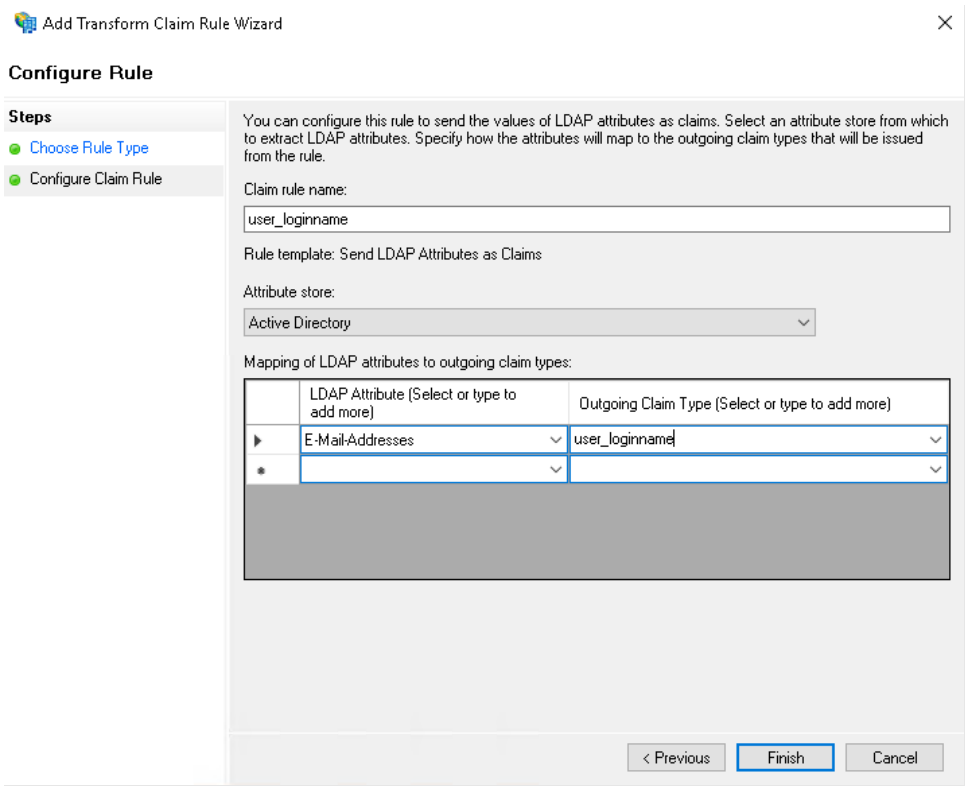
Configure claim rules for the Engage relying party

Next, add the claim rules for the relying party trust so that the attributes that Engage requires are added to the SAML authentication response. Engage requires two claims, **Name ID**, and **user_loginname**.

1. Right-click the relying party for Engage and then click **Edit Claim Issuance Policy...**
2. In the **Edit Claim Issuance Policy** dialog box, click **Add Rule...** to create a claim rule for **Name ID**
3. Select **Transform an Incoming Claim** and then click Next.
4. Configure the rule with the following settings:
    a. **Claim rule name**: NameID
    b. **Incoming claim type**: UPN
    c. **Outgoing claim type**: Name ID
    d. **Outgoing name ID format**: Persistent Identifier



5. Click **Finish**
6. Next, click **Add Rule...** to create a claim rule for **user_loginname**
7. Select **send LDAP Attributes as Claims** and then click **Next**. Create a rule with the following settings:
    a. **Claim rule name**: user_loginname
    b. **Attribute store**: Active Directory
    c. **LDAP Attribute**: E-Mail-Addresses
    d. **Outgoing Claim Type:** user_loginname

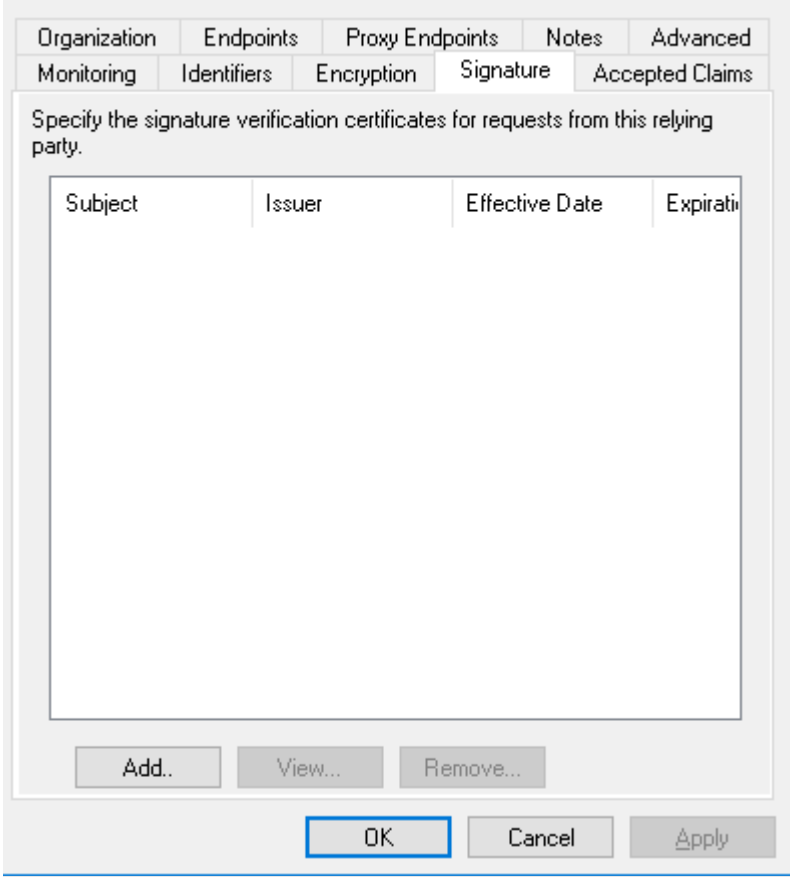


8. Click **Finish**
9. In the **Edit Claim Issuance Policy** dialog box, click **Apply** and **OK** to complete

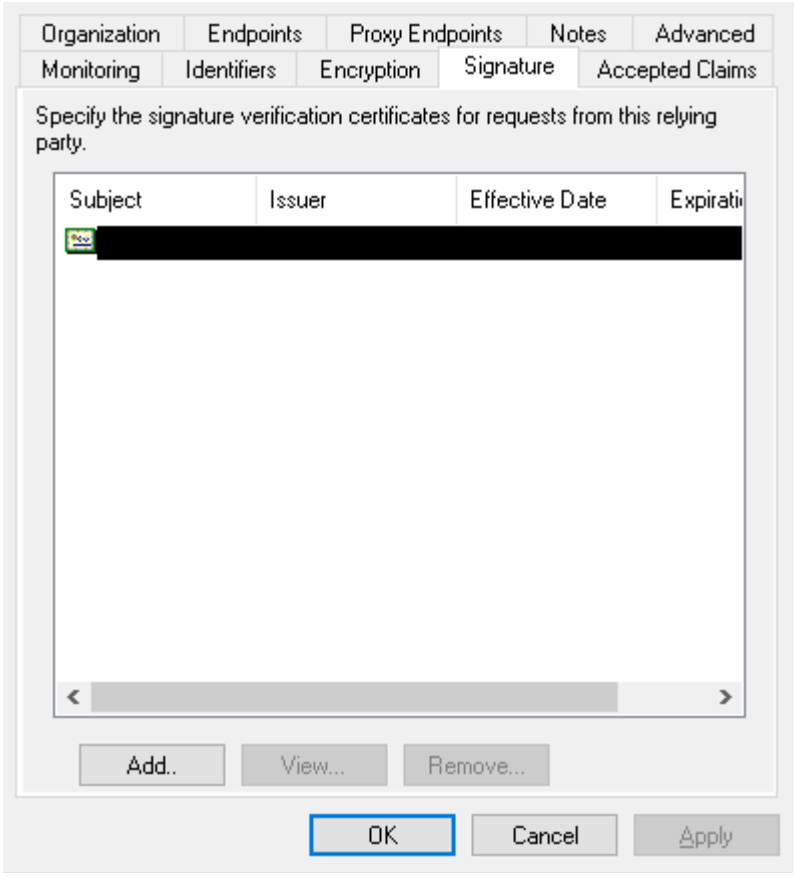
Configure signature verification for SAML requests

Next, configure the **signature verification certificate** which will allow verification of signatures in SAML requests. The certificate can be downloaded from **Manage Domain > SAML Authentication** in Engage.

1. Right-click the relying party for Engage and then click **Properties**
2. In **Signature** tab, click **Add**



3. Upload the **signature verification certificate** provided by Engage

4. 

5. Click **Apply** and **OK** to complete

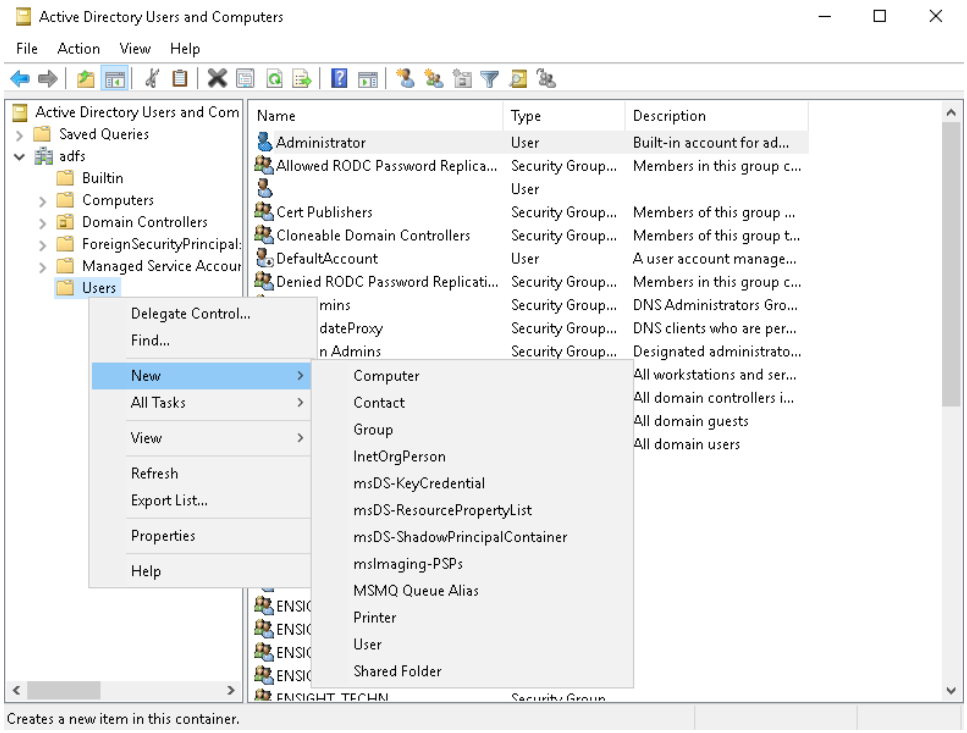
Optional: configure authority_id claim rules

After completing the above sections, SSO should now work with Engage. This section is an optional step that will allow granting Engage User roles to users through set up claims in IdP.

There are several ways to retrieve a user's group membership and transform the membership into a claim. The following is an example of how to set up Active Directory user groups and map them to an Engage user role using the standard ADFS attribute, **Token-Groups – Unqualified Names**, to provide all group names as Engage user roles in the **authority_id** claim.

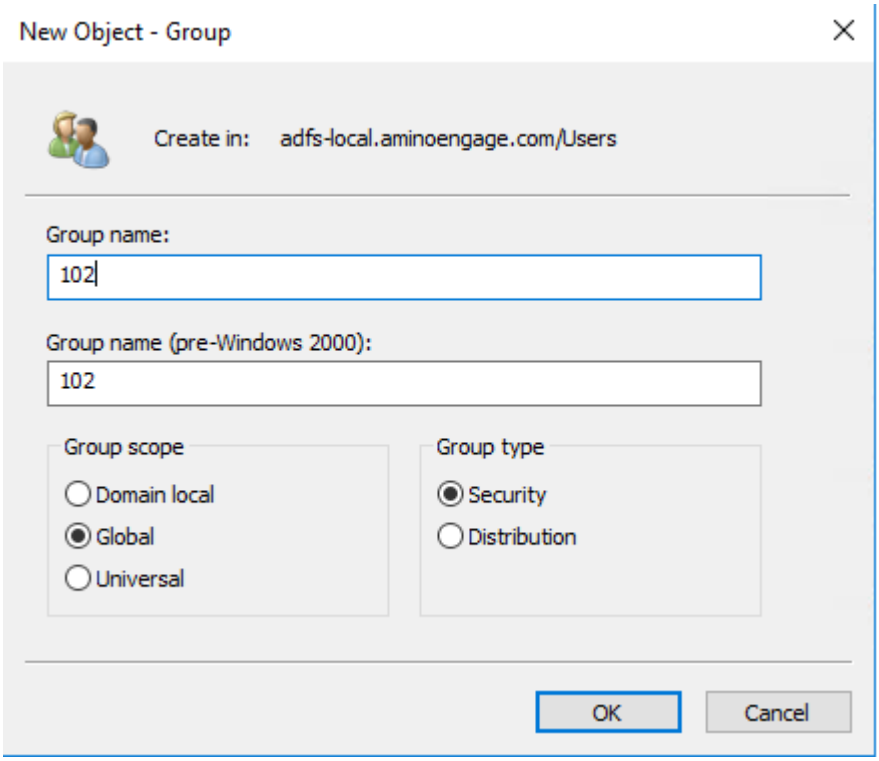
Set up an Active Directory User and map to an Engage user role.

1. In your Windows Server, open **Active Directory User and Computers**
2. Right-click **Users** and select **New > Group**



3. Create a group mapped to Engage user role with following settings:
    a. Group name: <Engage user role authority id>

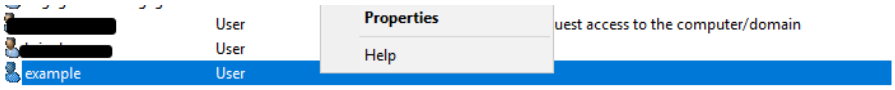
< Engage user role authority id > can be found in the **Appendix: Authority Id List**. The following is using **102(SYSTEM Operator)** as an example.



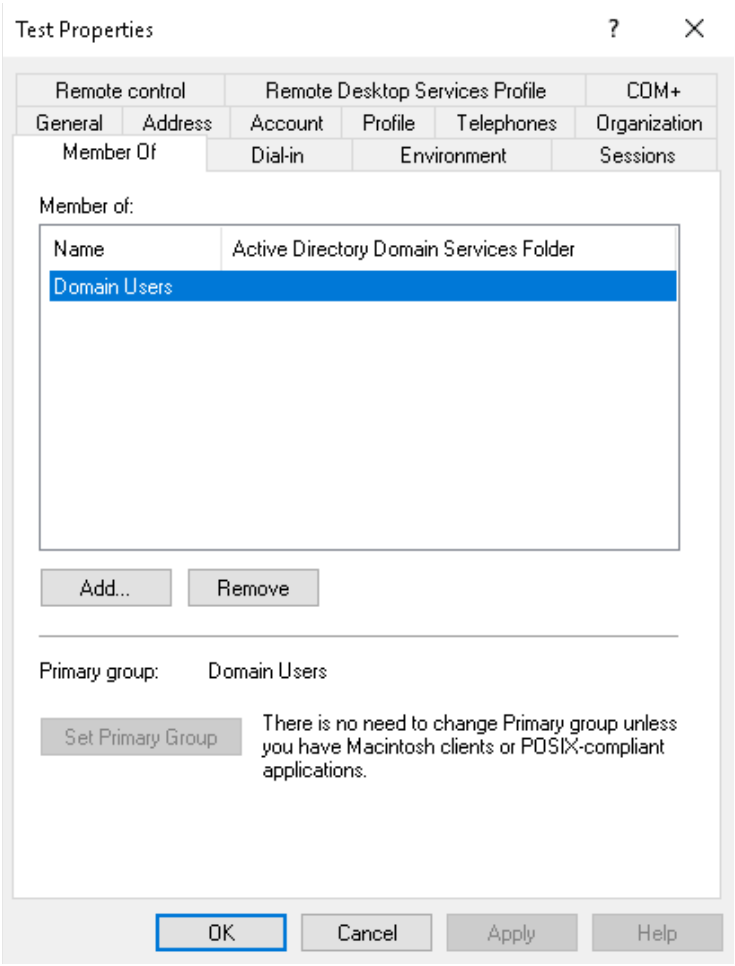
4. Click **OK** to complete

Assign the user to the Active Directory User Group

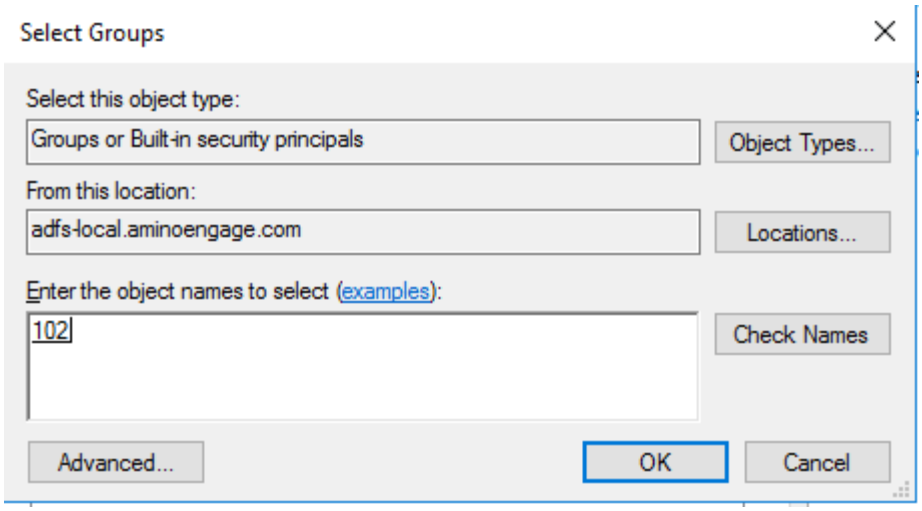
1. Open **Active Directory User and Computers**
2. Right-click a user and select **Properties**



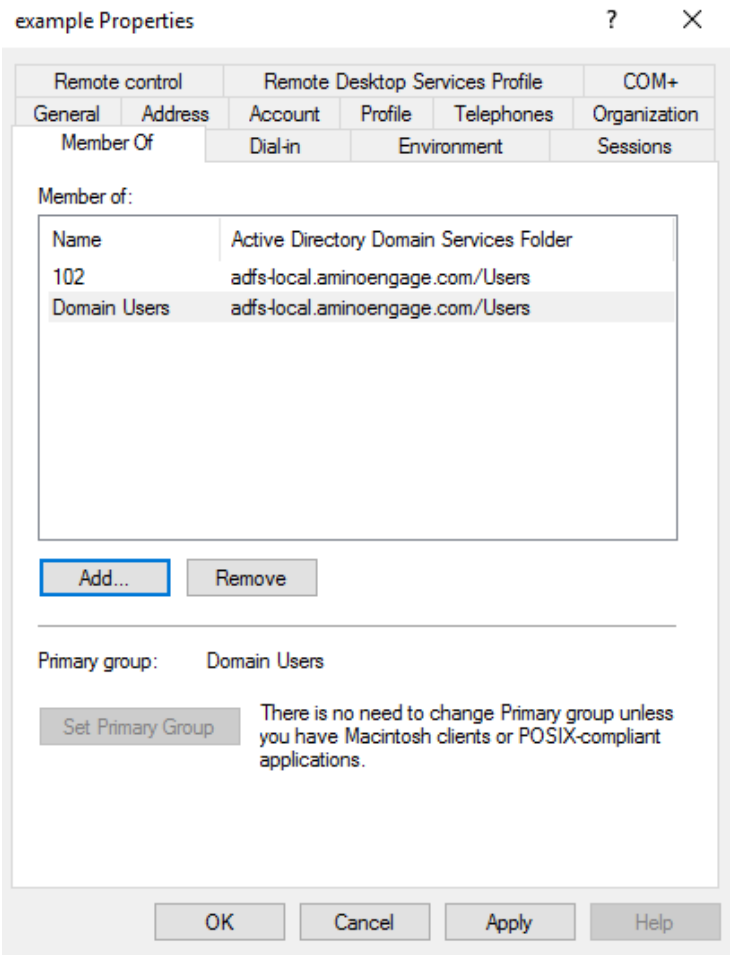
3. In **Member Of** tab, then click **Add...**



4. In **Enter the object name to select** textbox, input the name of the Group mapped to Engage user role. Click **Check Names** to verify, and the group name will be underlined. Click **OK** to confirm.



5. In **Member Of** tab, a new group name will be added.

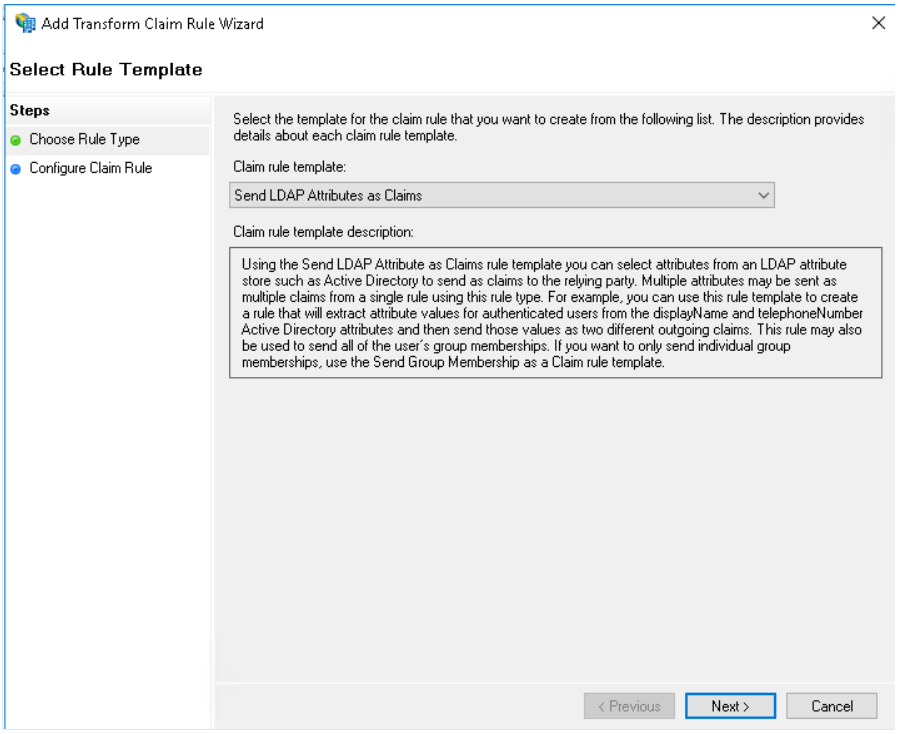


6. Click **Apply** and **OK** to complete.

Configure authority_id claim rule with Token-Groups – Unqualified Names attribute

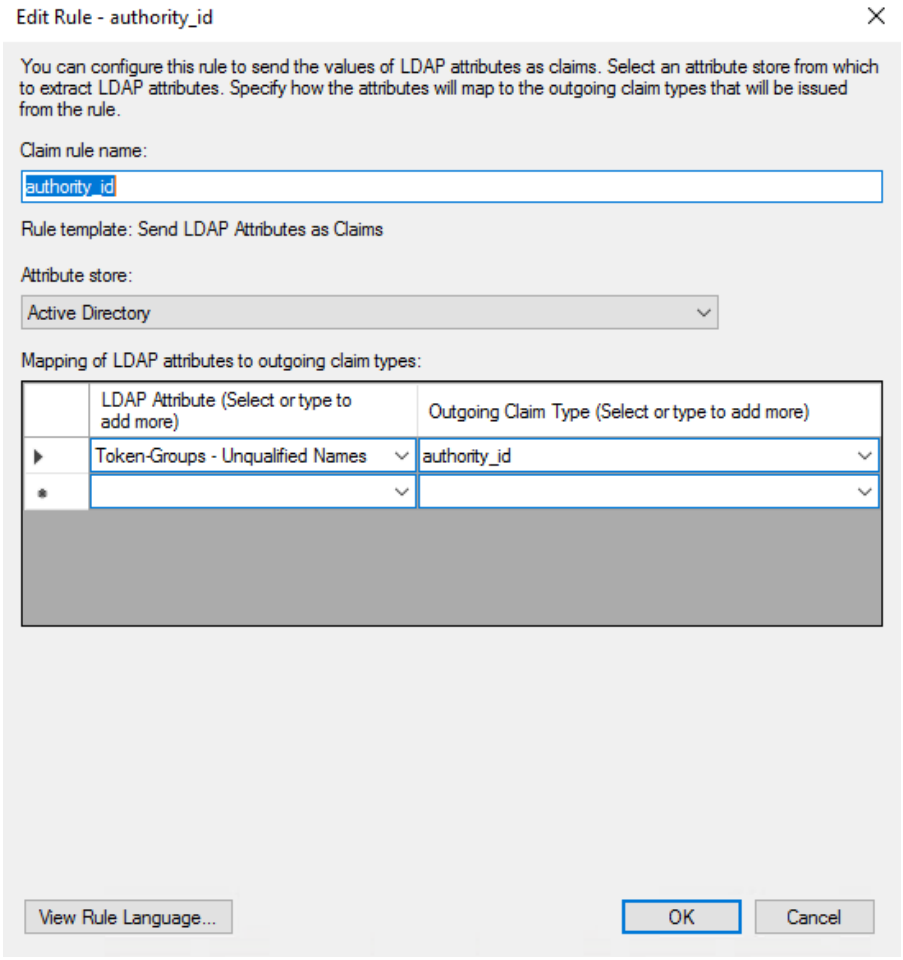
1. Right-click the relying party for Engage and then click **Edit Claim Issuance Policy...**

2. In the **Edit Claim Issuance Policy** dialog box, click **Add Rule...** to create a claim rule for **authority**
3. Select S**end LDAP Attributes as Claims** and then click Next.



4. Configure the rule with the following settings:
    a. **Claim rule name**: authority_id
    b. **Attribute store**: Active Directory
    c. **LDAP Attribute**: Token-Groups – Unqualified Names

d. **Outgoing Claim Type**: authority_id



5. Click **Finish**
6. In the **Edit Claim Issuance Policy** dialog box, click **Apply** and **OK** to complete

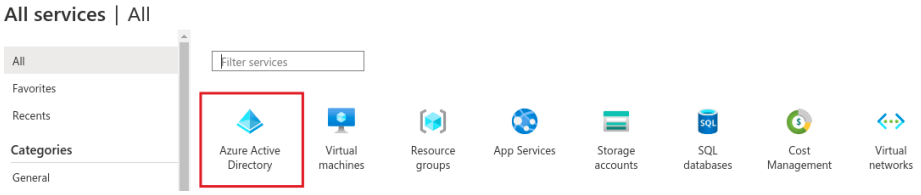
Configure Azure Active Directory as an Identity Provider for Single Sign-on

This section provided instructions on how to integrate Azure Active Directory (Azure AD) with Engage using SAML-based single-sign-on (SSO).

Configure Engage as a trusted relying party

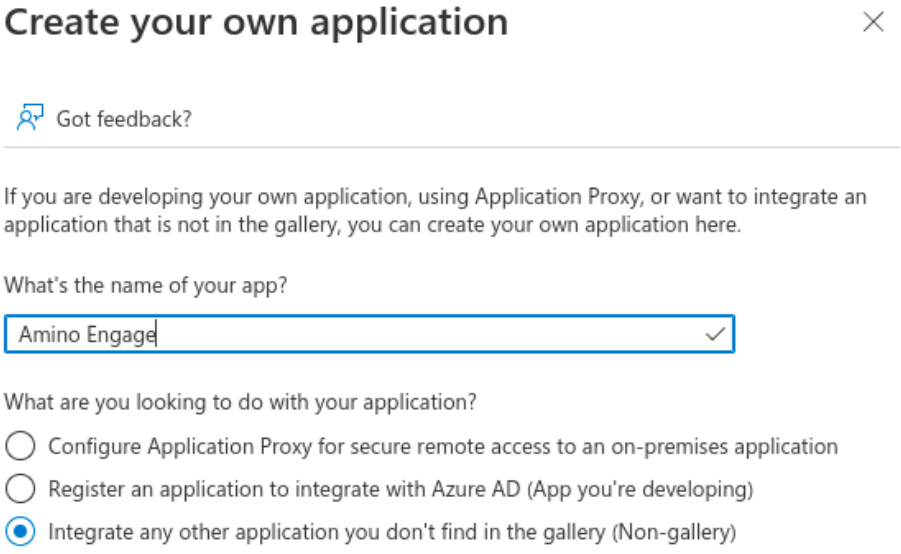
To begin, we first configure the ADFS server to trust Engage as a relying party.

1. Sign in to the Azure portal by using a Microsoft account
2. Select **Azure Active Directory** service



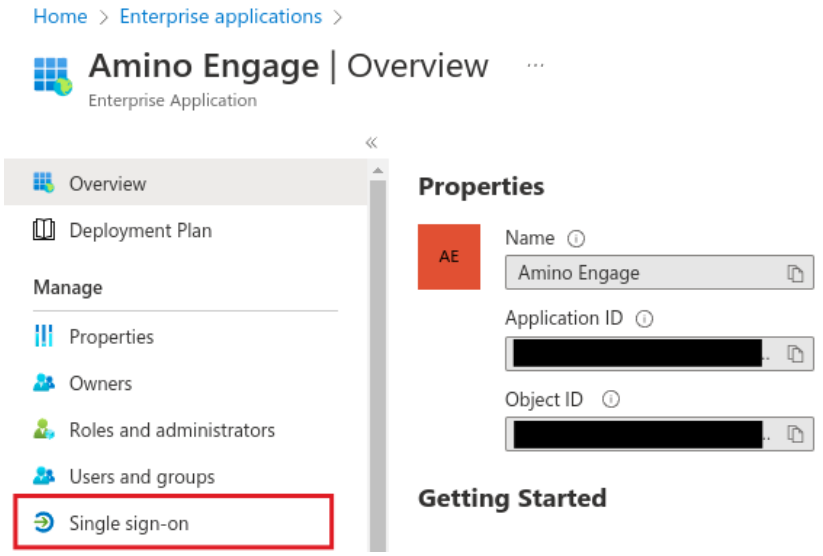
3. On the left panel, select **Enterprise Applications**
4. To add an application, select **New Application**
5. In the **Browse Azure AD Gallery** page, select **Create your own application**

6. The **Create your own application** pane opens. Input a name and select **Integrate any other application you don't find in the gallery (Non-gallery)**

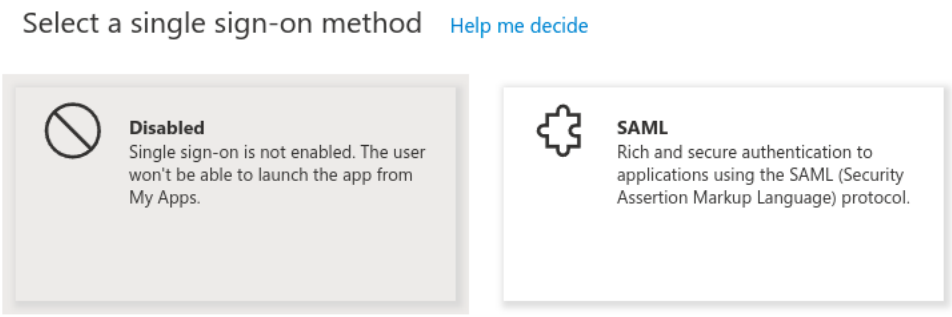


7. Click **Create**.

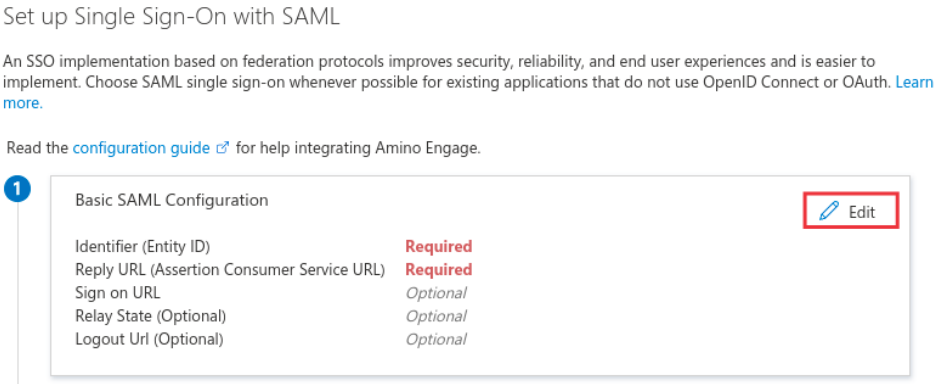
8. Once the app is created, the Enterprise Application page shows. On the left panel, select **Single sign-On**



9. On the **Select a single sign-on method** pane, select **SAML**



10. In the **Set up Single Sign-On with SAML** page, select the **Edit** button for **Basic SAML Configuration**

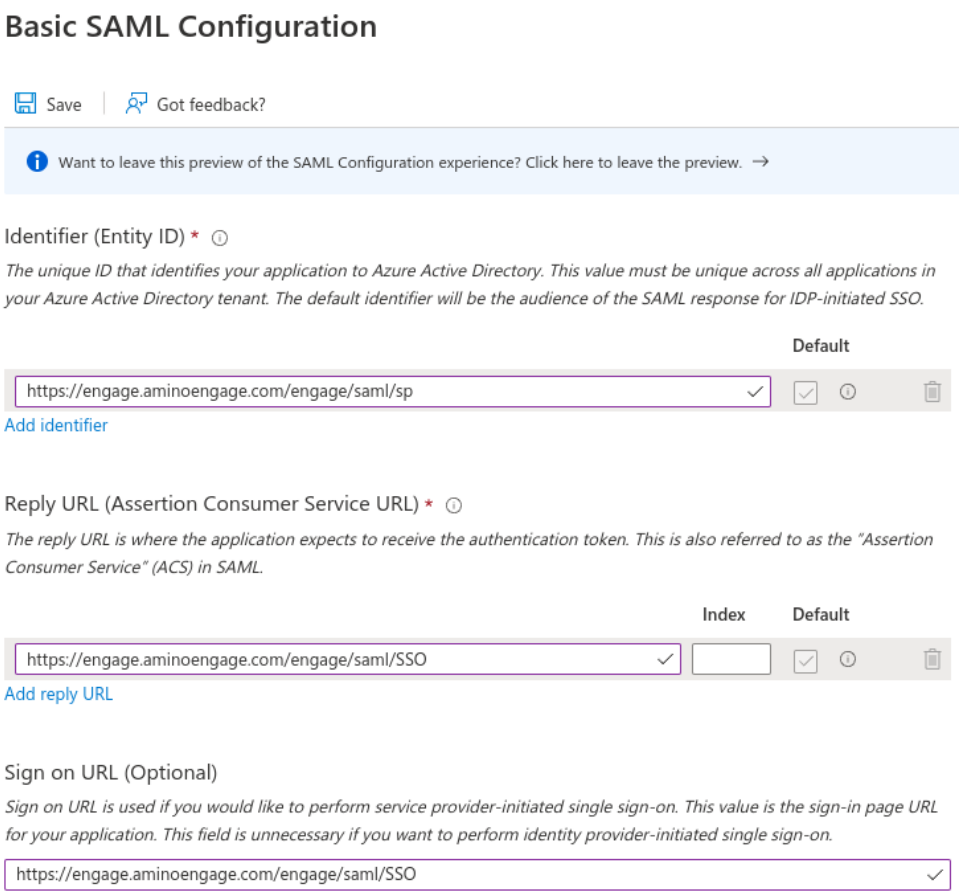


11. The **Basic SAML Configuration** pane opens.
    a. Under **Identifier (Entity ID)** section, select **Add identifier** and input
        i. For Engage: https://engage.aminoengage.com/engage/saml/sp

ii. For Orchestrate: https://system.amino-orchestrate.com/system/saml/sp

b. Under **Reply URL (Assertion Consumer Service URL)** section, select **Add identifier** and input
   i. For Engage: https://engage.aminoengage.com/engage/saml/SSO
   ii. For Orchestrate: https://system.amino-orchestrate.com/system/saml/SSO

c. Under Sign on URL (Optional) section, input
   i. For Engage: https://engage.aminoengage.com/engage/saml/SSO
   ii. For Orchestrate: https://system.amino-orchestrate.com/system/saml/SSO

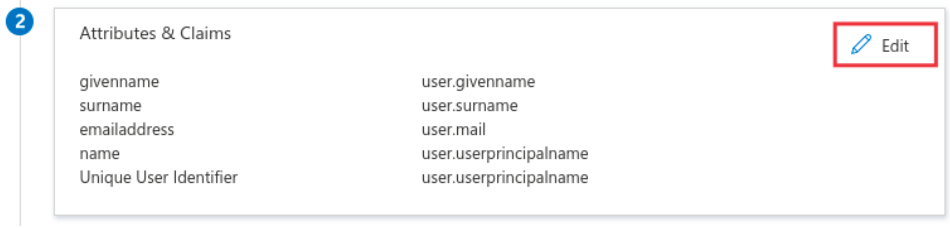


12. Click **Save** button at the top of the pane

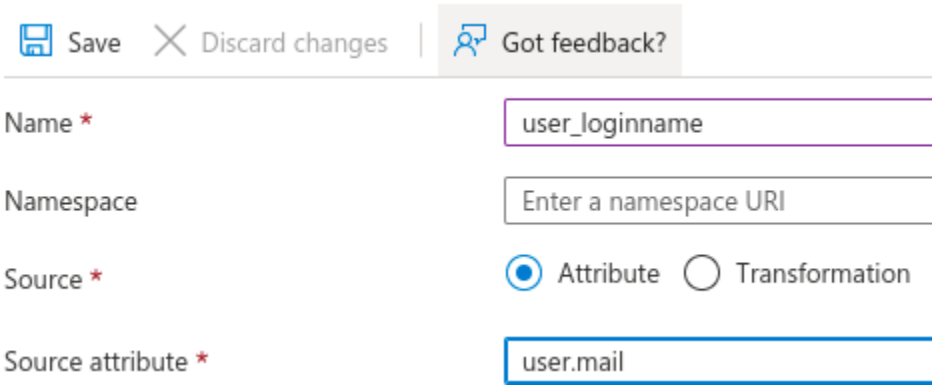
Configure claim rules for the Engage relying party

Next, add the claim rules for the relying party trust so that the attributes that Engage requires are added to the SAML authentication response. Engage requires two claims, **Name ID**, and **user_loginname**.

1. On the **Set up Single Sign-On with SAML** page, select the **Edit** button for **Attributes & Claims**



2. Skip configure the claim **Name ID**, because it is added as **Unique User Identifier** by Azure AD automatically
3. On **Attributes & Claims** page, select **Add new claim** button
4. On Manage Claim pane, create a cliam for **user_loginname** with the following settings:
    a. **Name**: user_loginname
    b. **Source**: Attribute
    c. **Source attribute:** user.mail



5. Click **Save** button

Grant user to access Engage

Next, enable users to use Azure Single Sign On by granting access to Engage

1. In the Azure portal, select **Enterprise Applications**, and then select **All applications**.
2. In the applications list, select **Amino Engage**
3. On the left panel, select **Users and groups**
4. Select **Add user/group** button
5. In **Add Assignment** page, select user in **Users** list. Click **Select** button at the bottom of the pane.
6. Click **Assign** button

Signature verification for SAML requests

Azure AD does not validate signed authentication requests if a signature is present. There is no effect to enable **Sign Request** in Engage **SAML Authentication** page.

Appendix: Authority Id List

Module	Authority Role Name	Authority Id
System	Administrator	101
System	Operator	102
System	INI Signer	104
System	Server Monitor	105
Manage	Administrator	201
Manage	Operator	202
Manage	RMA User	204
Resolve	Domain Administrator	302
Resolve	Operator	303
Resolve	Technician	304
Resolve	Viewer	305
Optimize	Administrator	501
Optimize	Viewer	502