User Authentication with SAML and Entra ID

Last Modified on 10/20/2025 1:45 pm EDT

SAML SSO with Entra ID

SAML SSO with Entra ID needs to be created from the Enterprise Applications interface. This is different from OpenID Connect, in which applications are created from App Registrations because they require API Access.

1. Go to **Azure > Entra ID > Enterprise Applications > + New Application**.
2. Choose the Non-gallery application button.
3. Give the application a name, such as 'PoliteMail SAML2 Application', and click 'Add'.
4. Click on 'Single sign-on' from the options on the left side of the screen, and then click the SAML button. The Basic SAML Configuration screen will appear.

Basic SAML Configuration

Enter the following information in the two required fields:

Identifer (Entity ID):

```
https://yourpolitemailhostname
```

Reply URLs (Assertion Consumer Service URL):

```
https://yourpolitemailhostname/ssv/Saml2/Acs
https://yourpolitemailhostname/api/Saml2/Acs
```

User Attributes and Claims

The user may keep the default claims; however, the Role claim must also be added. The Role claim is mapped to user.assignedroles which are defined within the 'Setup the Manifest' section.

1. Under the 'User Attributes & Claims' section, click the Edit icon and click on '+ Add new claim'. The Manage Claim window will open.
2. Enter the following information:

Name: role

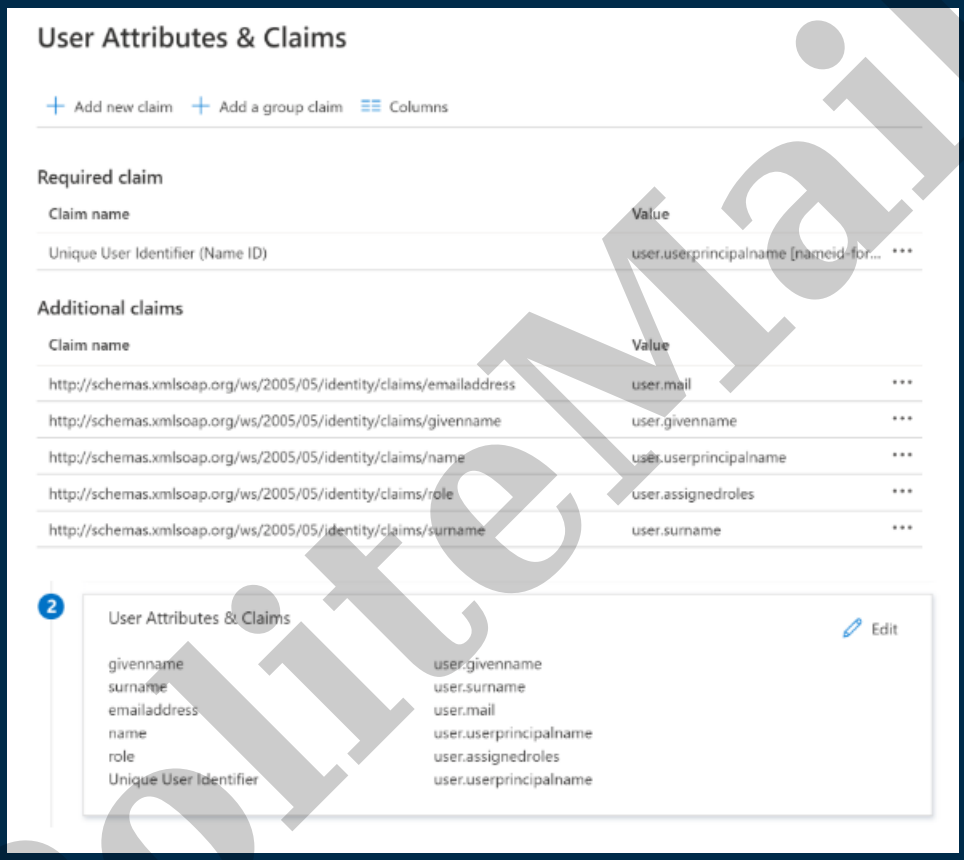
Namespace:

http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Alternatively, you can enter the line above with /role added to the end in the Name field in lieu of a name, and leave the Namespace field blank.

Source: Attribute

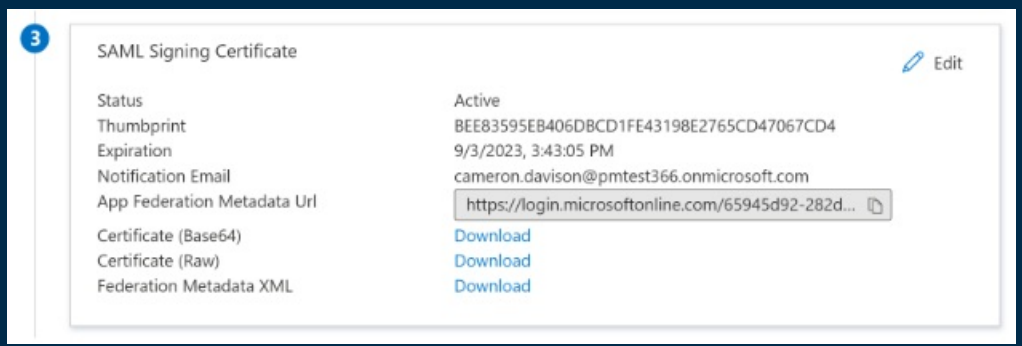
Source Attribute: user.assignedroles



SAML Signing Certificate

This certificate is unique generated each time; clicking Edit allows the certificate to be changed out or regenerated.

Download the Base64 certificate and place it onto the PoliteMail Server.



Set up PoliteMail SAML2 Application

The information in this section contains the Login URL, Entra ID Identifier, and Logout URL.

1. Send the App Federation Metadata URL (from the SAML Signing Certificate section above), the Base64 Certificate you downloaded, and the three items shown here (Login URL, Entra ID Identifier, Logout URL) to PoliteMail Support.

Setting Up the Manifest

Some JSON will need to be added to the manifest. This sets up the general rules that can be applied to a user or group.

- The 'value' field is the static default and should not be changed from the PoliteMail Roles.
- Some roles will exist be default. Before they can be removed, "isEnabled" will need to be set to false.

Go to **Entra ID > App Registrations > PoliteMail SAML2 Application > Manifest** and follow the steps below:

1. Add the JSON code below to the manifest:

```
"appRoles": [
 {
 "allowedMemberTypes": [
 "User"
 ],
 "displayName": "SystemAdministrator",
 "id": "98464916-35bb-4f71-a320-8e1d1c34c51a",
 "isEnabled": true,
 "description": "SystemAdministrator on PoliteMail Server",
 "value": "SystemAdministrator"
 },
 {
 "allowedMemberTypes": [
 "User"
 ],
 "displayName": "Administrators",
 "id": "98464916-35bb-4f71-a320-8e1d1c34c51a",
 "isEnabled": true,
 "description": "Administrator on PoliteMail Server",
 "value": "Administrators"
 },
 {
 "allowedMemberTypes": [
 "User"
 ],
 "displayName": "Manager",
 "id": "c062df2a-7e65-42f7-bf2d-1600dfbf5afe",
 "isEnabled": true,
 "description": "Manager on PoliteMail Server",
 "value": "Manager"
 },
 {
 "allowedMemberTypes": [
 "User"
 ],
 "displayName": "User",
 "id": "541a6ff3-20cc-4870-9722-285cd40ad582",
 "isEnabled": true,
 "description": "Basic PoliteMail Access",
 "value": "User"
 }
 ]
```


Adding Users/Groups and Assigning a Role

Go to Entra ID and select Enterprise Applications under the available services. Click on the 'Application Type' drop-down and select 'Enterprise Applications', and select 'PoliteMail OpenID Application from the list. Select 'Users and Groups' and click the '+ Add user' button.

You can now select a User from the list, and select a Role from 4 options: System Administrator, Administrator, Manager, or User.

Note that in Entra ID, groups are available for production tenants but not development tenants.

About PoliteMail Roles

In the general implementation for SAML2 with Entra ID and PoliteMail, its recommended to use the manifest, but in reality, any Azure value can be mapped to role. Should there beneed for a more custom role-based implementation to match the structure of the customer, that can be implemented.

For example, the User.Department field could be used, and the Entra ID values could be Development, Marketing, or Support. That value will be passed to the PoliteMail Server. On the PoliteMail Server that field then needs to be mapped to a role (System Administrator, Administrators, Manager, or User). This also allows multiple Azure values to bemapped to a PoliteMail role.

Entra ID Key	Entra ID Value	PoliteMail Key	PoliteMail Value
User.department	Development	Development	Administrators
User.department	IT	IT	System Administrator
User.department	Support	Support	Manager
User.department	Marketing	Marketing	User