PoliteMail®

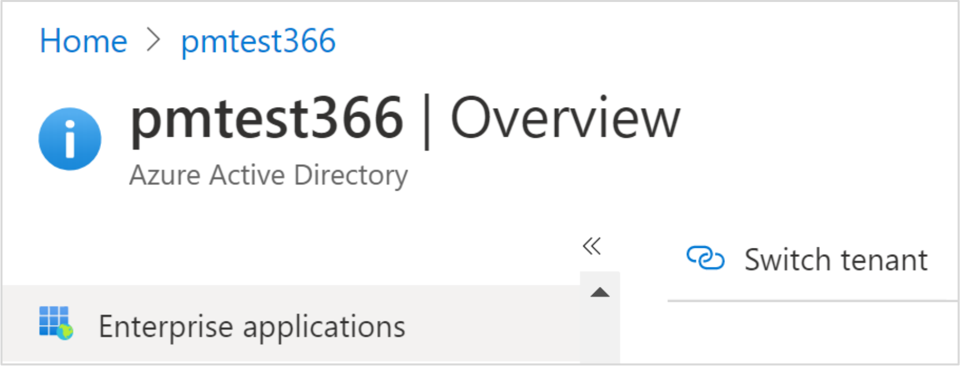
PoliteMail SAML Authentication with Azure Active Directory

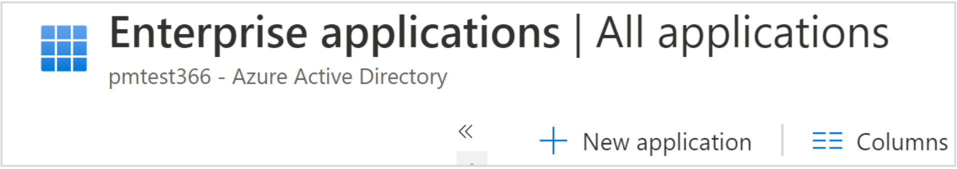
PoliteMail Cloud Environment

SAML SSO with Azure AD

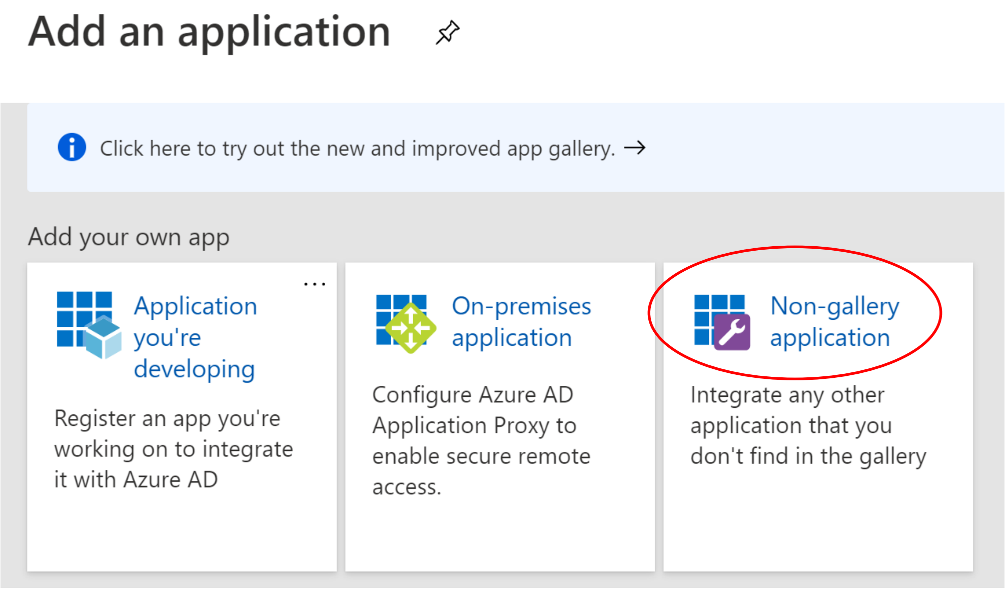
SAML SSO with AzureAD needs to be created from the Enterprise Applications interface. This is different from OpenID Connect, in which applications are created from App Registrations because they require API Access.

1. Go to **Azure** > **AzureAD** > **Enterprise Applications >** **+New Application**




Enterprise applications | All applications
pmtest366 - Azure Active Directory
+ New application
Columns

2. Choose Non-Gallery Application.

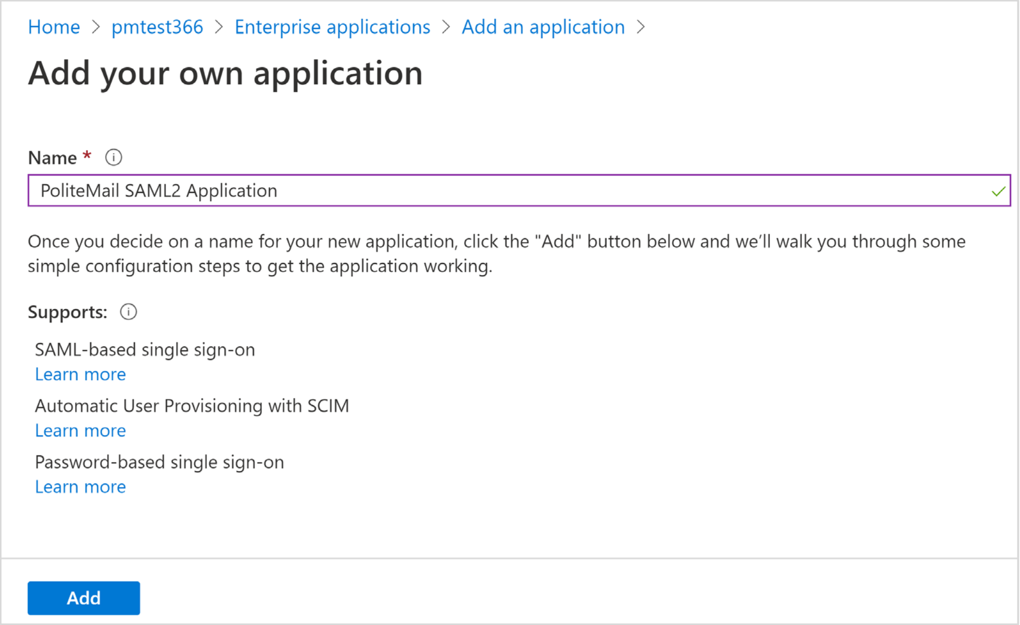

Add an application
Click here to try out the new and improved app gallery. →
Add your own app
Application you're developing
On-premises application
Non-gallery application

Register an app you're working on to integrate it with Azure AD

Configure Azure AD Application Proxy to enable secure remote access.

Integrate any other application that you don't find in the gallery

3. Give it a Name and then click the **Add** button.



Home > pmtest366 > Enterprise applications > Add an application >

Add your own application

Name * ⓘ

PoliteMail SAML2 Application ✓

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

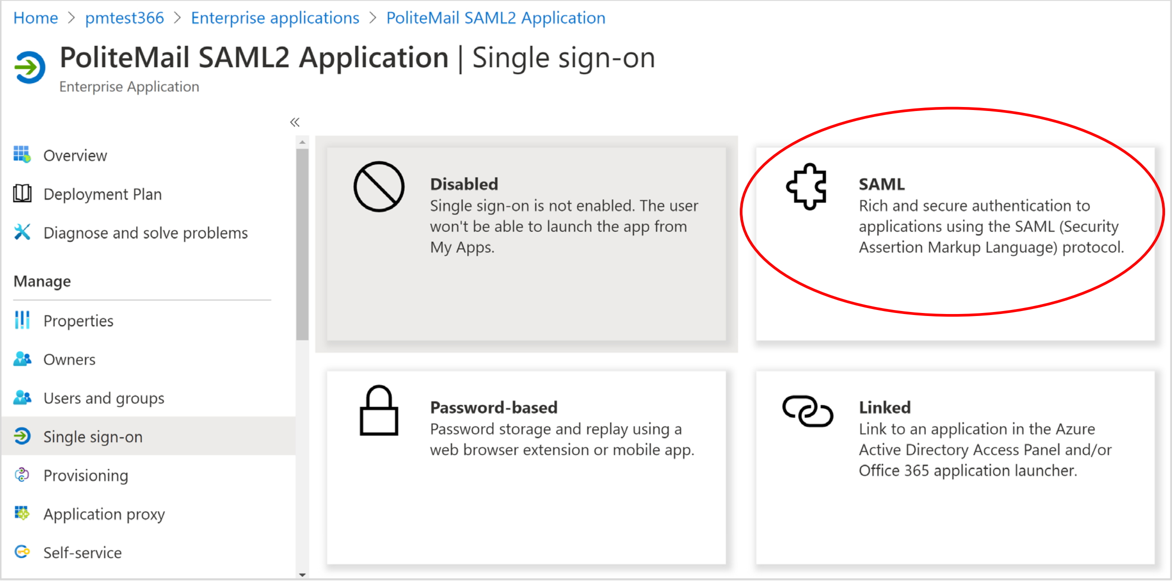
Supports: ⓘ

SAML-based single sign-on
Learn more

Automatic User Provisioning with SCIM
Learn more

Password-based single sign-on
Learn more

4. Select the Single sign-on blade then click SAML. This will display the SAML configuration page.



Home > pmtest366 > Enterprise applications > PoliteMail SAML2 Application

PoliteMail SAML2 Application | Single sign-on
Enterprise Application

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

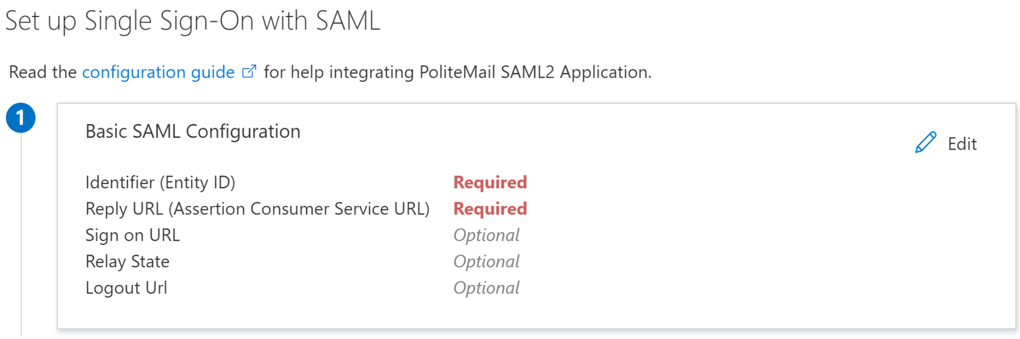
Configure Azure AD SAML to PoliteMail EntityID and Reply URL

In the two required fields, please input the following:

Identifier (Entity ID): https://yourpolitemailhostname

Reply URLs (Assertion Consumer Service URL): https://yourpolitemailhostname/ssv3/Saml2/Acs

https://yourpolitemailhostname/api/Saml2/Acs

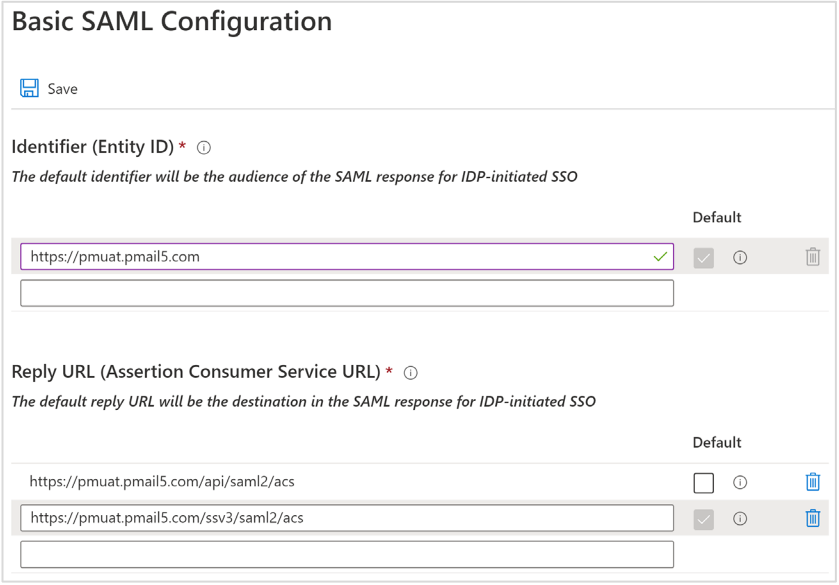


Set up Single Sign-On with SAML

Read the configuration guide for help integrating PoliteMail SAML2 Application.

1 Basic SAML Configuration

Identifier (Entity ID)	**Required**
Reply URL (Assertion Consumer Service URL)	**Required**
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*



Basic SAML Configuration

Identifier (Entity ID) *

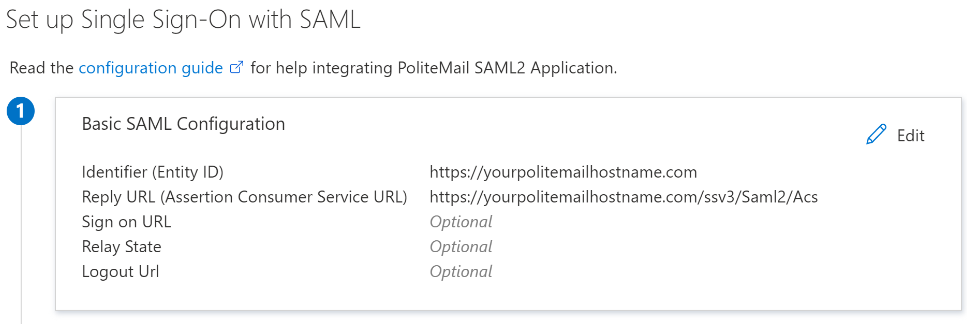
The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
https://pmuat.pmail5.com ✓	☑

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
https://pmuat.pmail5.com/api/saml2/acs	□
https://pmuat.pmail5.com/ssv3/saml2/acs	☑



Set up Single Sign-On with SAML

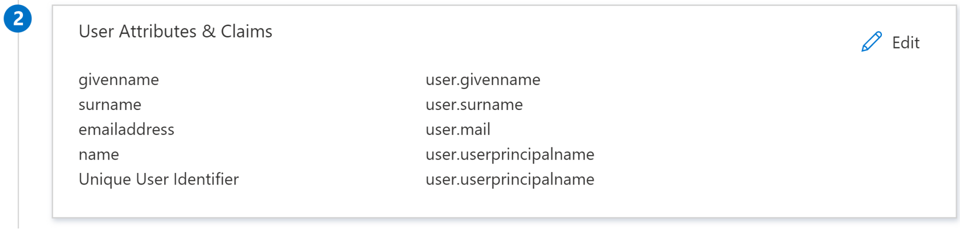
Read the configuration guide for help integrating PoliteMail SAML2 Application.

1 Basic SAML Configuration

Identifier (Entity ID)	https://yourpolitemailhostname.com
Reply URL (Assertion Consumer Service URL)	https://yourpolitemailhostname.com/ssv3/Saml2/Acs
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

Configure User Attributes and Claims

The user may keep the default claims, however, one claim still needs to be added and that is the role claim. This role claim is mapped to the user.assignedroles which are defined within the **Setup the Manifest** section.



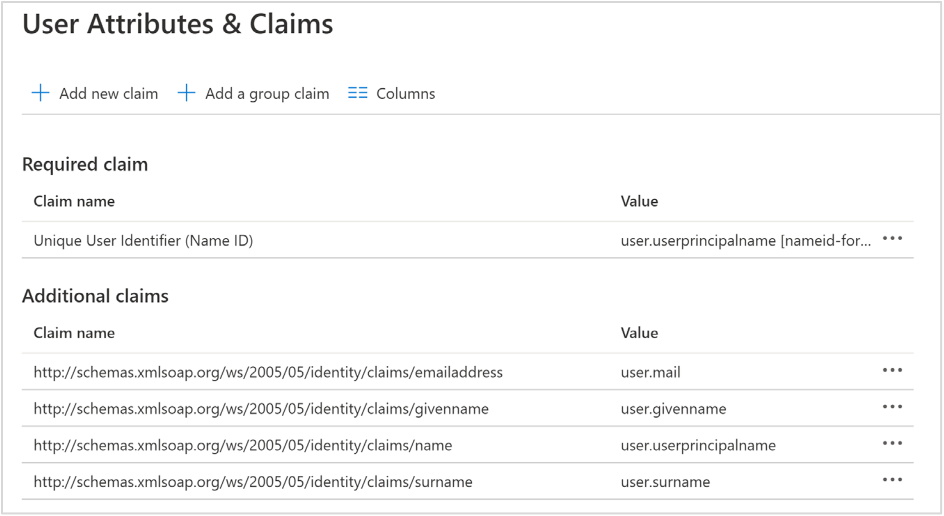
2

User Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Clicking Edit yields the following form, click **+ Add new claim**



User Attributes & Claims

Required claim

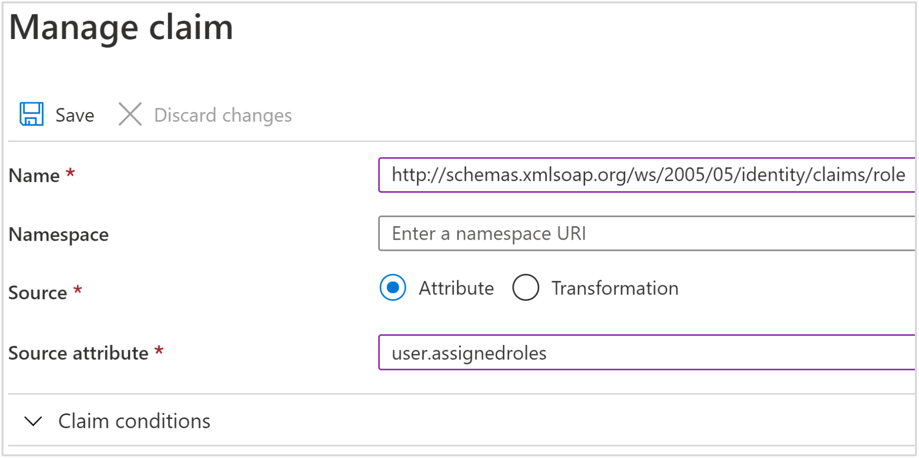
Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... •••

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname •••

This will yield the Manage Claim form. Do not give it a name, instead, just place the following URI into the name field and map it to user.assignedroles.

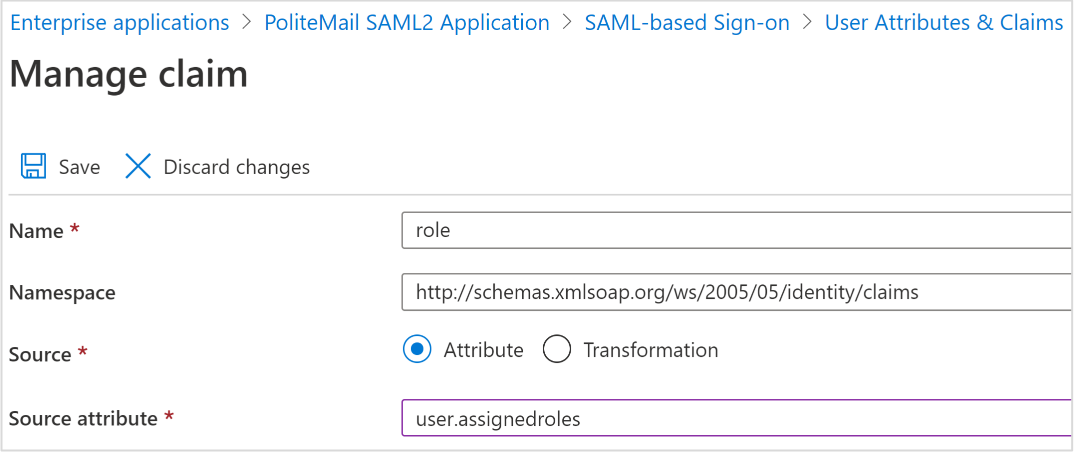
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role



Manage claim

Name *	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role
Namespace	Enter a namespace URI
Source *	● Attribute ○ Transformation
Source attribute *	user.assignedroles

Optionally, the Name can be **role** and the namespace can be http://schemas.xmlsoap.org/ws/2005/05/identity/claims

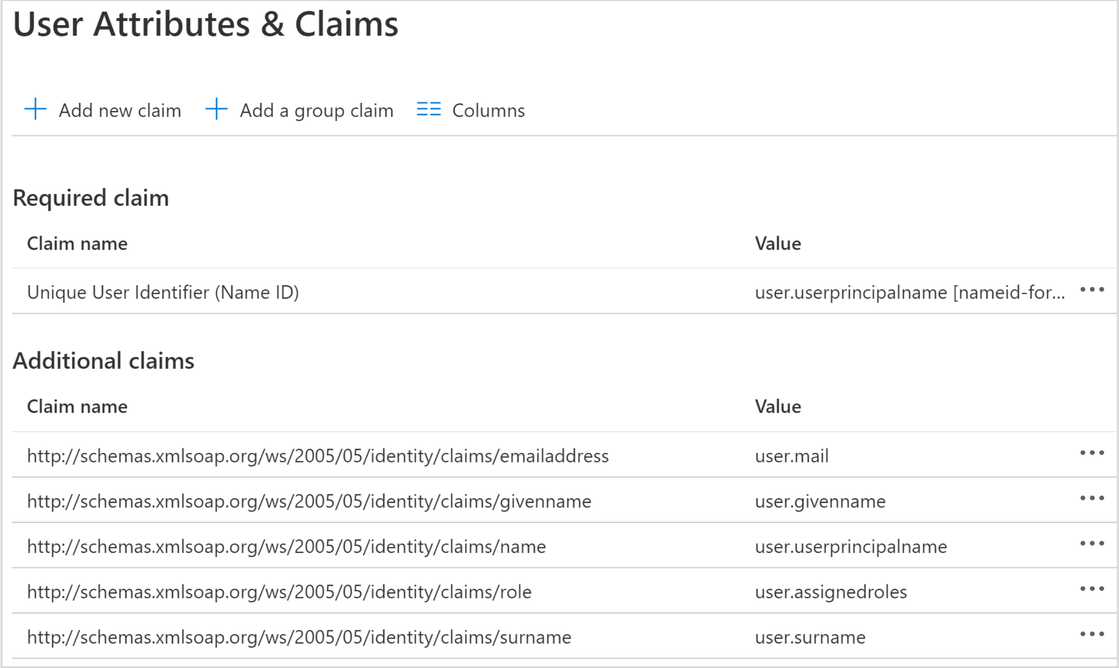


Enterprise applications > PoliteMail SAML2 Application > SAML-based Sign-on > User Attributes & Claims

Manage claim

Name *	role
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
Source *	● Attribute ○ Transformation
Source attribute *	user.assignedroles

Result



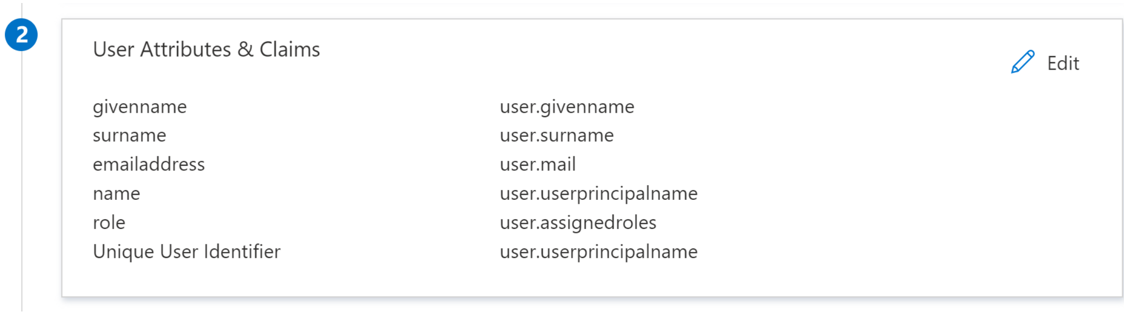
User Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role	user.assignedroles
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

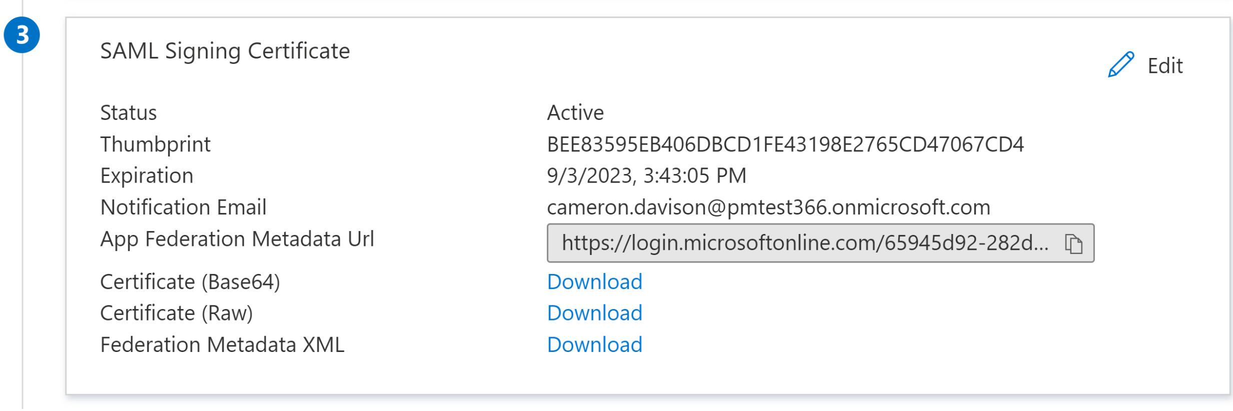


2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
role	user.assignedroles
Unique User Identifier	user.userprincipalname

Download the SAML Signing Certificate

This certificate is unique generated each time, however, clicking **Edit** allows the certificate to be changed out or regenerated. No action necessarily needs to occur, however be sure to download the Base64 certificate and place it onto the PoliteMail Server.

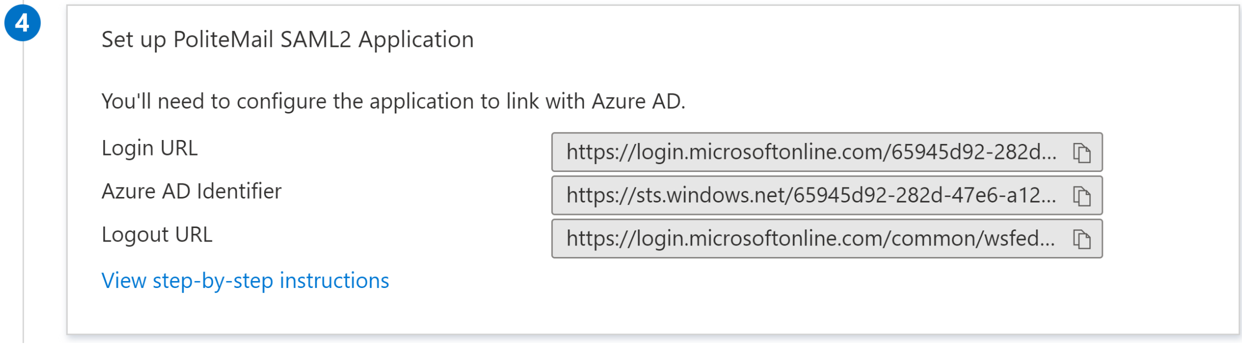


3 SAML Signing Certificate

Status	Active
Thumbprint	BEE83595EB406DBCD1FE43198E2765CD47067CD4
Expiration	9/3/2023, 3:43:05 PM
Notification Email	cameron.davison@pmtest366.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/65945d92-282d...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Save the Setup Information for PoliteMail Setup

This information needs to be saved and copied over to the PoliteMail Server, as it will be needed for setting up the SAML2 Application within PoliteMail



4 Set up PoliteMail SAML2 Application

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/65945d92-282d...
Azure AD Identifier	https://sts.windows.net/65945d92-282d-47e6-a12...
Logout URL	https://login.microsoftonline.com/common/wsfed...

View step-by-step instructions

Information to Provide to PoliteMail

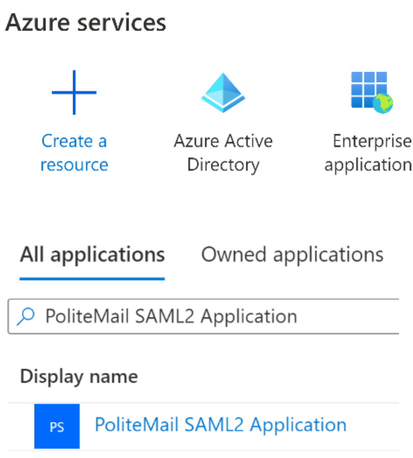
1.) App Federation Metadata Url
2.) Certificate (Base64)
3.) Login URL
4.) AzureAD Identifier
5.) Logout URL

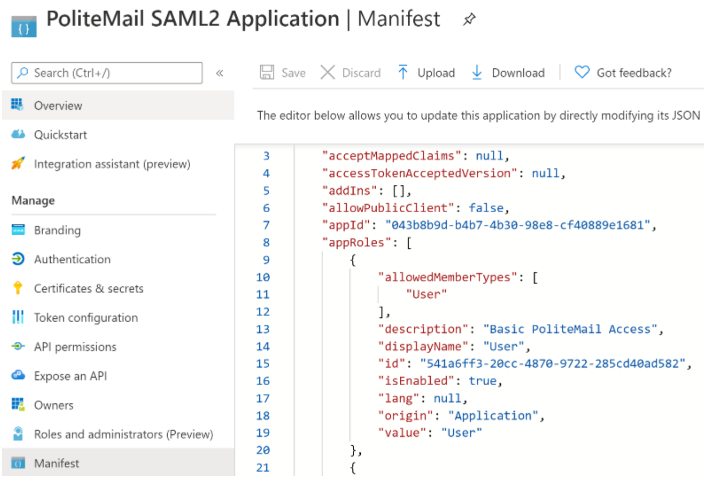
Setup the Manifest

The below JSON will need to be added to the manifest, this sets up the general roles 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: Administrators, Manager, or User.

Note: Some roles will exist by default, those need to be set to `"isEnabled": false`, before they can be removed.

AzureAD > App Registrations > PoliteMail SAML2 Application > Manifest





The editor below allows you to update this application by directly modifying its JSON

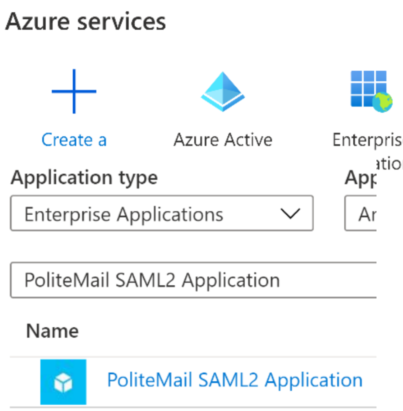
```
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": false,
    "appId": "043b8b9d-b4b7-4b30-98e8-cf40889e1681",
    "appRoles": [
        {
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Basic PoliteMail Access",
            "displayName": "User",
            "id": "541a6ff3-20cc-4870-9722-285cd40ad582",
            "isEnabled": true,
            "lang": null,
            "origin": "Application",
            "value": "User"
        },
        {
```

```
"appRoles": [
    {
    "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

AzureAD > Enterprise Applications > PoliteMail OpenID Application > Users and groups > + Add user

*Note: In Azure, groups are not available for role assignment in development tenants but are available in production tenants

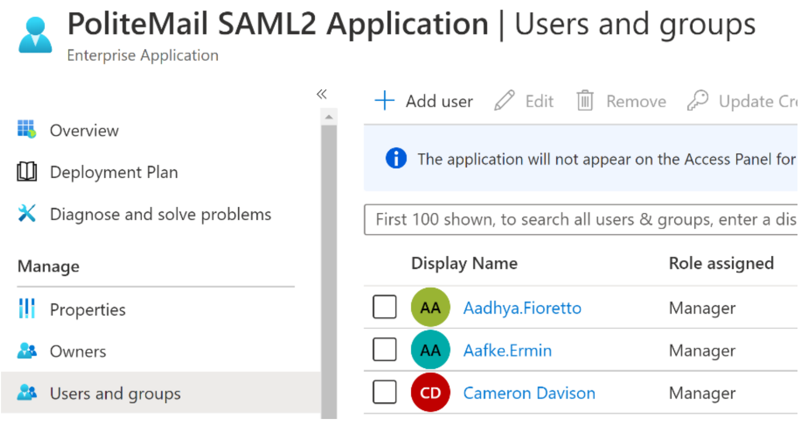

Azure services

Application type: Enterprise Applications

App: Ar

PoliteMail SAML2 Application

Name
PoliteMail SAML2 Application

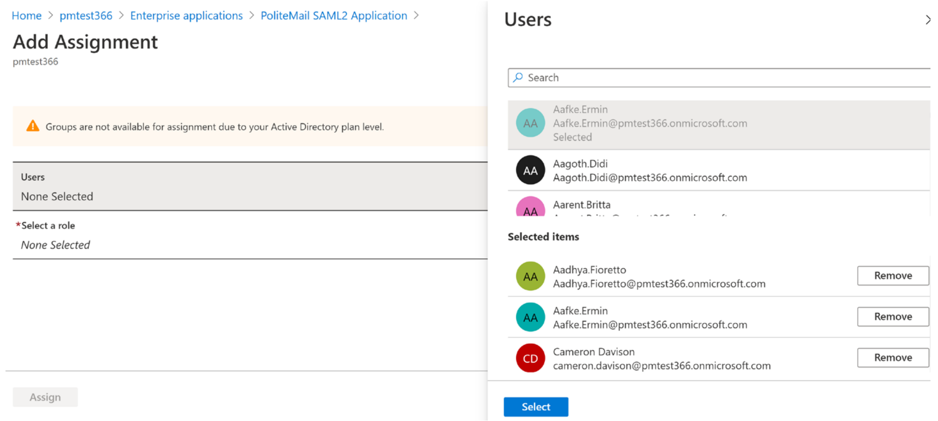

PoliteMail SAML2 Application | Users and groups

Enterprise Application

The application will not appear on the Access Panel for

First 100 shown, to search all users & groups, enter a dis

Display Name	Role assigned
□ AA Aadhya.Fioretto	Manager
□ AA Aafke.Ermin	Manager
□ CD Cameron Davison	Manager


Home > pmtest366 > Enterprise applications > PoliteMail SAML2 Application >

Add Assignment

pmtest366

Groups are not available for assignment due to your Active Directory plan level.

Users: None Selected

*Select a role: None Selected

Users

AA Aafke.Ermin
Aafke.Ermin@pmtest366.onmicrosoft.com
Selected

AA Aagoth.Didi
Aagoth.Didi@pmtest366.onmicrosoft.com

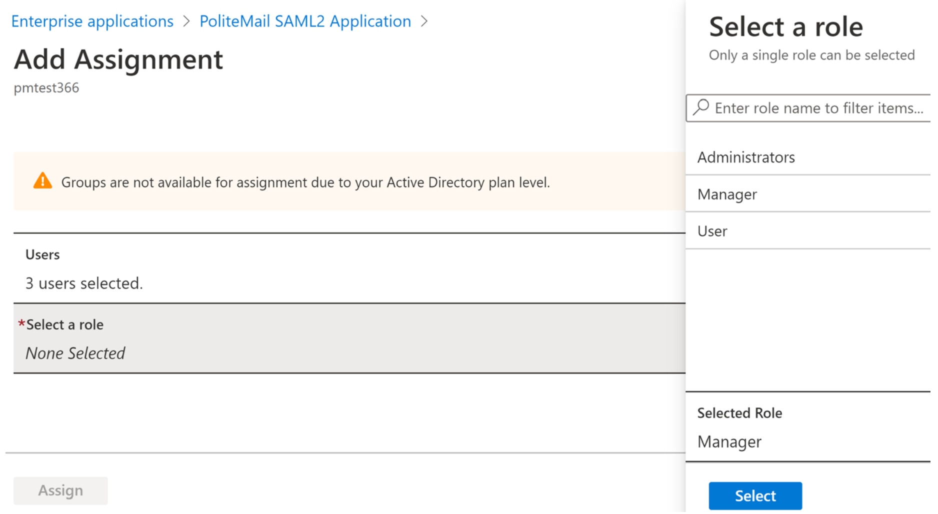
AA Aarent.Britta

Selected items

AA Aadhya.Fioretto
Aadhya.Fioretto@pmtest366.onmicrosoft.com — Remove

AA Aafke.Ermin
Aafke.Ermin@pmtest366.onmicrosoft.com — Remove

CD Cameron Davison
cameron.davison@pmtest366.onmicrosoft.com — Remove


Enterprise applications > PoliteMail SAML2 Application >

Add Assignment

pmtest366

Groups are not available for assignment due to your Active Directory plan level.

Users: 3 users selected.

*Select a role: None Selected

Select a role

Only a single role can be selected

Administrators

Manager

User

Selected Role: Manager

More About PoliteMail Roles

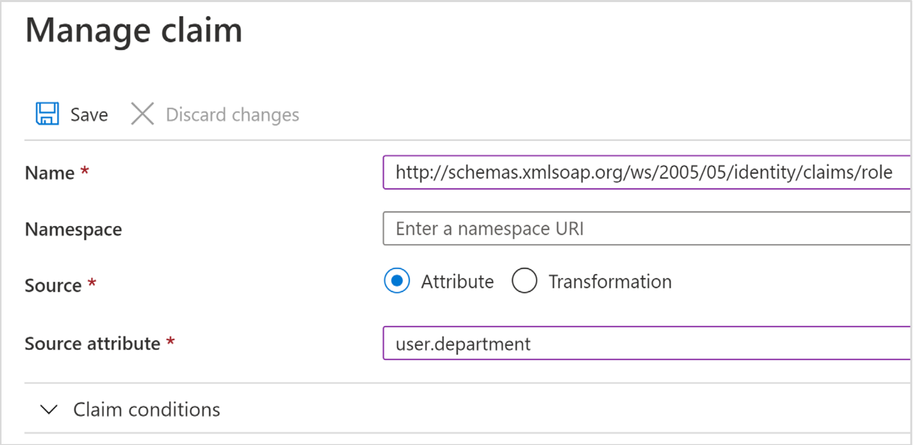
In the general implementation for SAML2 with AzureAD and PoliteMail, its recommended to use the manifest, but in reality, any Azure value can be mapped to role. Should there be need for a more custom role-based implementation to match the structure of the customer, that can be implemented.

For example, the **User.Department** field could be used, and the values could be Development, Marketing, or Support, for example. That value will be passed to the PoliteMail Server. On the PoliteMail Server that field then needs to be mapped to a role. The mapping on the PoliteMail Server is covered in the PoliteMail Server portion of this document. This also allows multiple Azure values to be used say IT/Manager could be mapped to administrators.

Static PoliteMail Roles

Administrators
Manager
User

Azure Key	Azure Value	PoliteMail Key	PoliteMail Value
User.department	Development	Development	Administrators
User.department	IT	IT	Administrators
User.department	Support	Support	Manager
User.department	Marketing	Marketing	User



Manage claim

Name *	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role
Namespace	Enter a namespace URI
Source *	● Attribute ○ Transformation
Source attribute *	user.department