

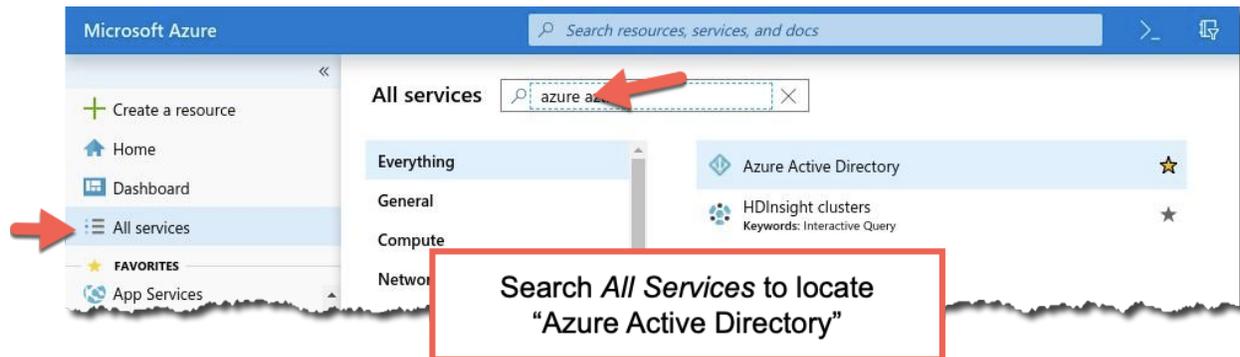
# Configuring AzureAD SAML for use with Omnilert's SAML connector

## Environment Used:

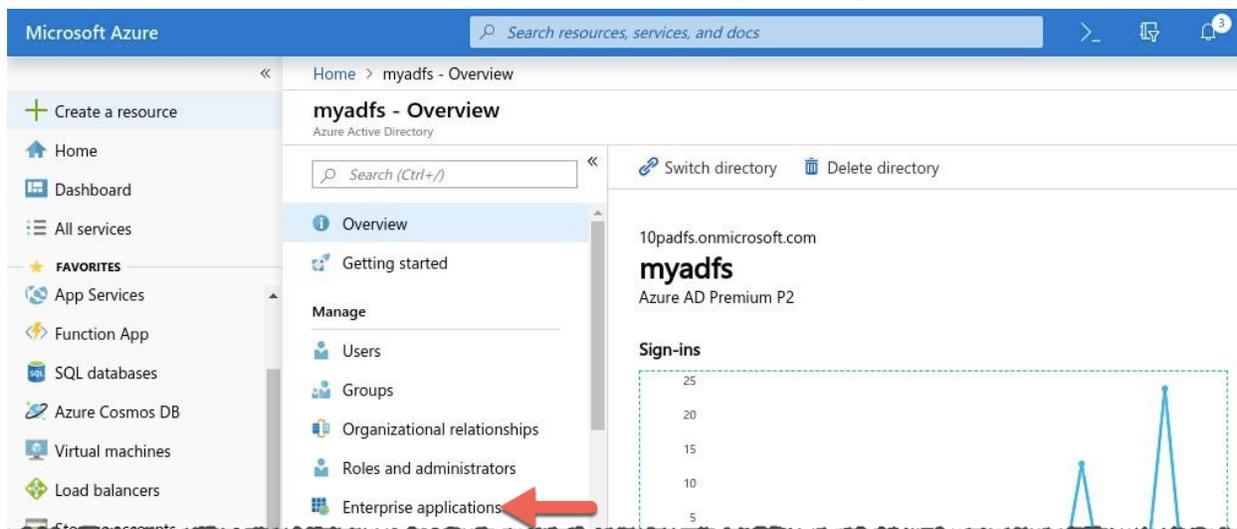
- Azure Portal
- Azure Active Directory

## Configuring SSO from Azure AD for Omnilert

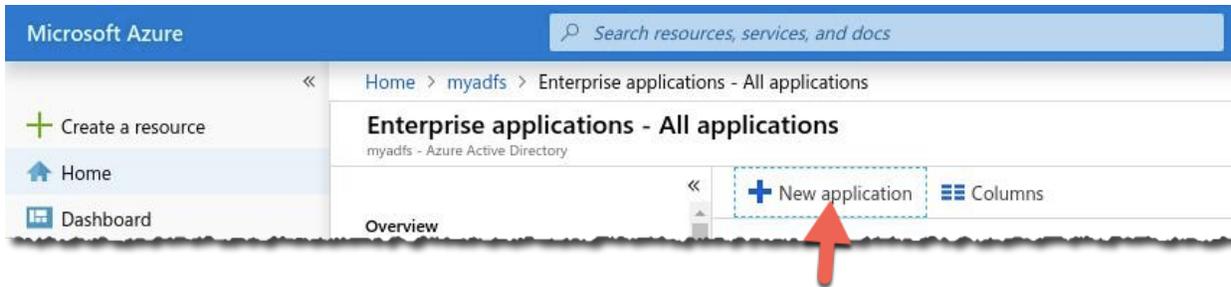
1. From your Azure Portal select **All Services** > Search for **Azure Active Directory** > Enter.



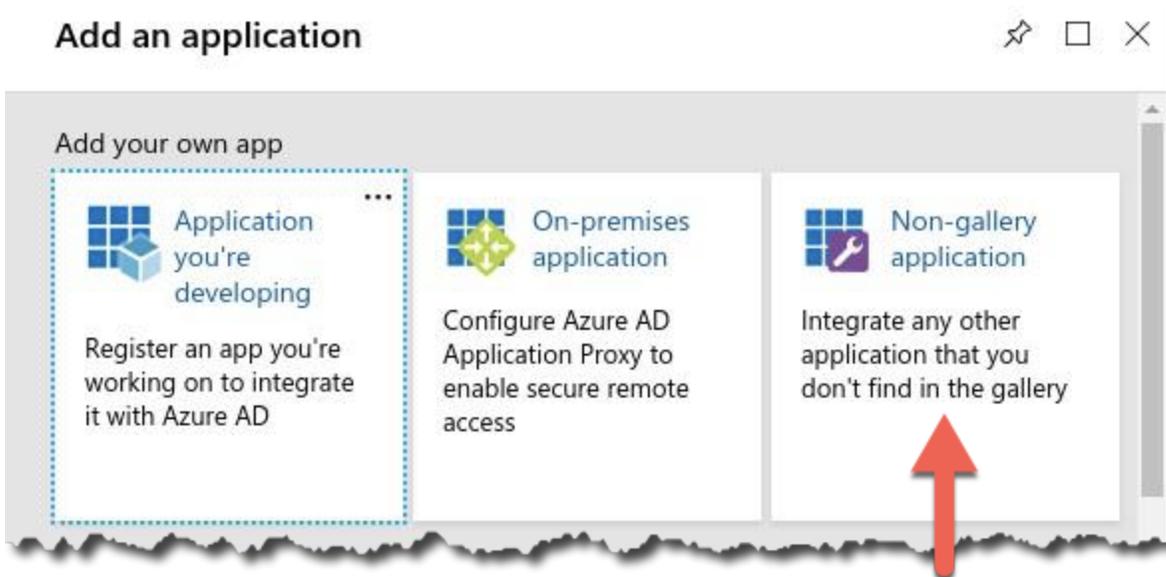
2. This will open your Azure Active Directory > Select **Enterprise Applications**



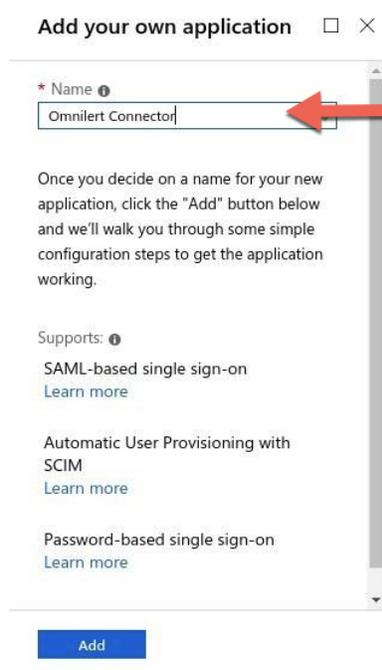
3. Once Enterprise Applications page is loaded click **New Application**



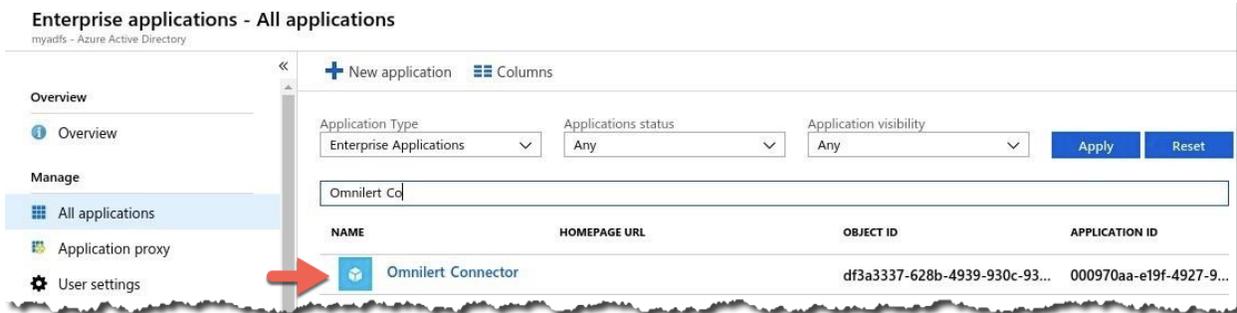
- This will open a window asking to Add your own app > select **Non-gallery application**



- Provide the name of your application "**Omnilert Connector**", for example

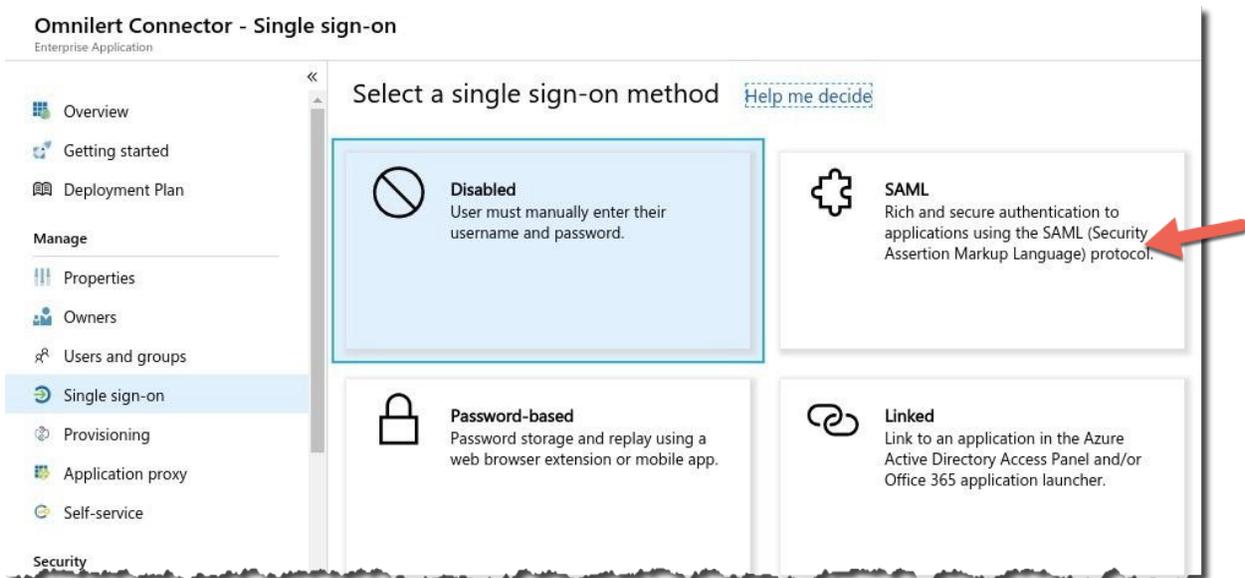


- The added application will now be available in **Enterprise Applications**. Open the application by clicking **"Omnilert Connector"**

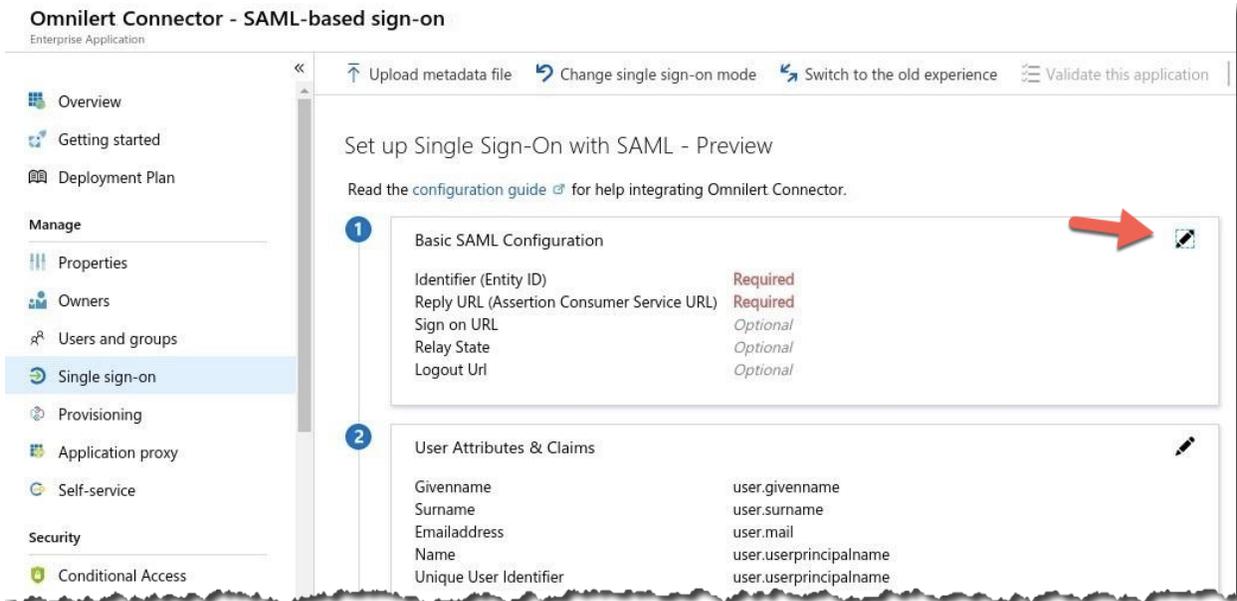


(Tip: You can search by name, just type in "Omnilert" as shown above)

- From the Overview screen click **Single sign-on**, then select **SAML**



8. Setting up **Single Sign-On with SAML - Preview** shows the configuration overview



**Omnilert Connector - SAML-based sign-on**  
Enterprise Application

Upload metadata file | Change single sign-on mode | Switch to the old experience | Validate this application

### Set up Single Sign-On with SAML - Preview

Read the [configuration guide](#) for help integrating Omnilert Connector.

- Basic SAML Configuration**

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Uri	Optional
- User Attributes & Claims**

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

9. Configure **Basic SAML Configuration** by clicking the **Edit icon** (on the right) > **Identifier** > **Reply URL** as shown below. Click **Save** then go back to the *Single Sign-On with SAML - Preview* page.

### Basic SAML Configuration

 Save

---

Identifier (Entity ID) (Required) ⓘ

ⓘ <https://www.omnilert.net/shibboleth> ...

Reply URL (Assertion Consumer Service URL) (Required) ⓘ

ⓘ <https://www.omnilert.net/Shibboleth.sso/SAML2/POST> ...

ⓘ <https://www.omnilert.net/Shibboleth.sso/SAML2/Artifact> ...

ⓘ <https://www.e2campus.net/Shibboleth.sso/SAML2/POST> ...

ⓘ <https://www.e2campus.net/Shibboleth.sso/SAML2/Artifact> ...

ⓘ <https://www.amerilert.net/Shibboleth.sso/SAML2/POST> ...

ⓘ <https://www.amerilert.net/Shibboleth.sso/SAML2/Artifact> ...

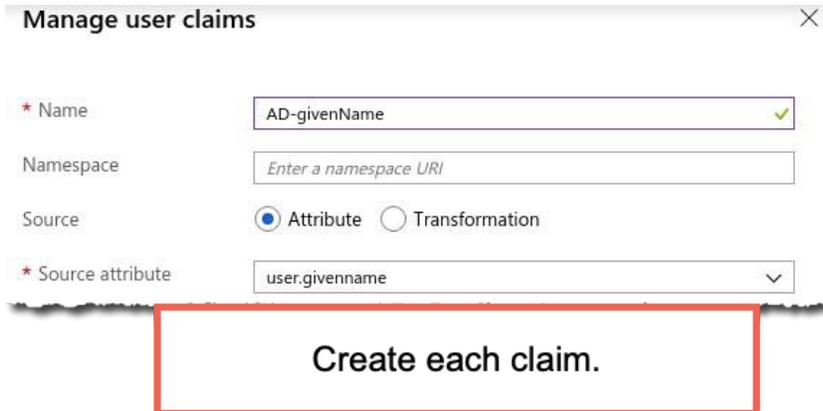
ⓘ <https://shibboleth.omnilert.net/Shibboleth.sso/SAML2/POST> ...

ⓘ <https://shibboleth.omnilert.net/Shibboleth.sso/SAML2/Artifact> ...

10. Configure **User Attributes & Claims** by clicking the **Edit icon** (on the right) > **Delete All Unnecessary Claims** > **Add new Claim** three times for the following attributes:

- **Name** : AD-omnilertUsername, **Source Attribute** : user.userprincipalname
- **Name** : AD-givenName, **Source Attribute** : user.givenname
- **Name** : AD-sn, **Source Attribute** : user.surname

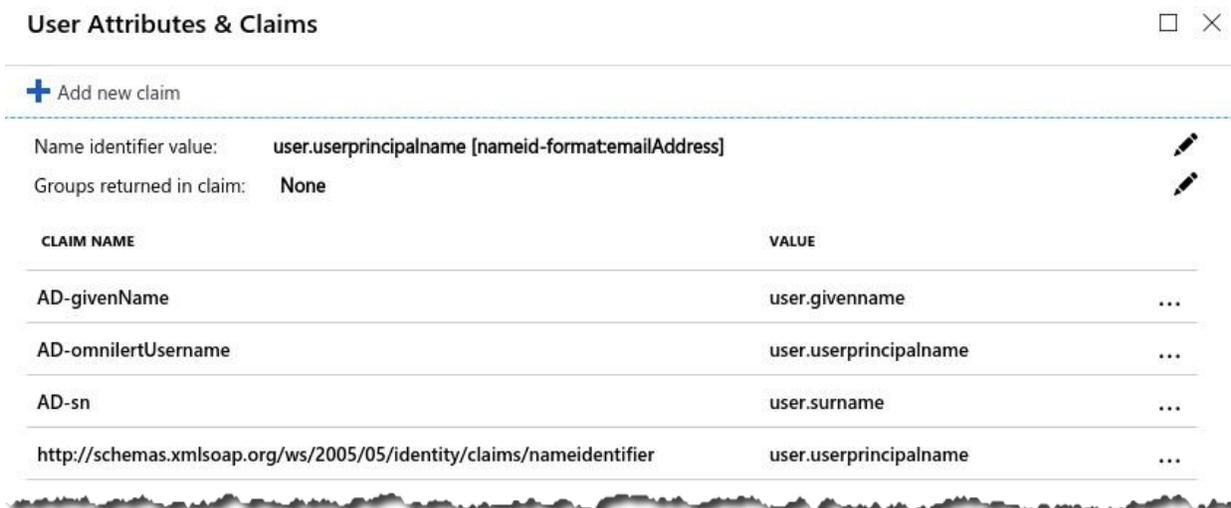
Example:



The screenshot shows a 'Manage user claims' dialog box with the following fields:

- Name**: AD-givenName (with a green checkmark)
- Namespace**: Enter a namespace URI
- Source**: Attribute (selected), Transformation
- Source attribute**: user.givenname

A red box highlights the text: **Create each claim.**



The screenshot shows the 'User Attributes & Claims' interface with a table of claims:

CLAIM NAME	VALUE	
AD-givenName	user.givenname	...
AD-omnilertUsername	user.userprincipalname	...
AD-sn	user.surname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname	...

Additional details from the interface:

- Name identifier value: user.userprincipalname [nameid-formatemailAddress]
- Groups returned in claim: None

11. On the *Single Sign-On with SAML - Preview Overview* page you can verify > Basic SAML Configuration, User Attributes, and Claims, are now configured. Provide **App Federation Metadata Url** to Omnilert from **SAML Signing Certificate** in Step 3.

3

SAML Signing Certificate	
Status	Active
Thumbprint	13465CC7D7AC82A47FB60D338F4D41BDD877682C
Expiration	5/1/2022, 7:19:23 PM
Notification Email	Missing
App Federation Metadata Url	<a href="https://login.microsoftonline.com/809f0c9b-a8cc-4...">https://login.microsoftonline.com/809f0c9b-a8cc-4...</a> 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download



Provide the “App Federation Metadata Url” to Omnilert Support

12. Note that you must configure your **Identifier** and **Logout Url** on the Omnilert system’s Shibboleth / SAML Single Configuration page.

4

Set up Omnilerts

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

Login URL	<a href="https://login.microsoftonline.com/809f0c9b-a8cc-4...">https://login.microsoftonline.com/809f0c9b-a8cc-4...</a> 
Azure AD Identifier	<a href="https://sts.windows.net/809f0c9b-a8cc-4cdb-9de4-...">https://sts.windows.net/809f0c9b-a8cc-4cdb-9de4-...</a> 
Logout URL	<a href="https://login.microsoftonline.com/common/wsfede...">https://login.microsoftonline.com/common/wsfede...</a> 

[View step-by-step instructions](#)



The Omnilert Shibboleth / SAML configuration will use the “Azure AD Identifier” as the “Identity Providers Entity ID” and the “Logout URL” as the “Logout redirect URL”

See <https://support.omnilert.com/hc/en-us/articles/115008509908-Single-Sign-On-Shibboleth-SAML-Settings> for the settings in Omnilert’s administrator portal.

**NOTE:** This document is provided as a general guide for informational purposes only. Please consult with your Azure administrators/vendor for specific guidance for your Azure system.