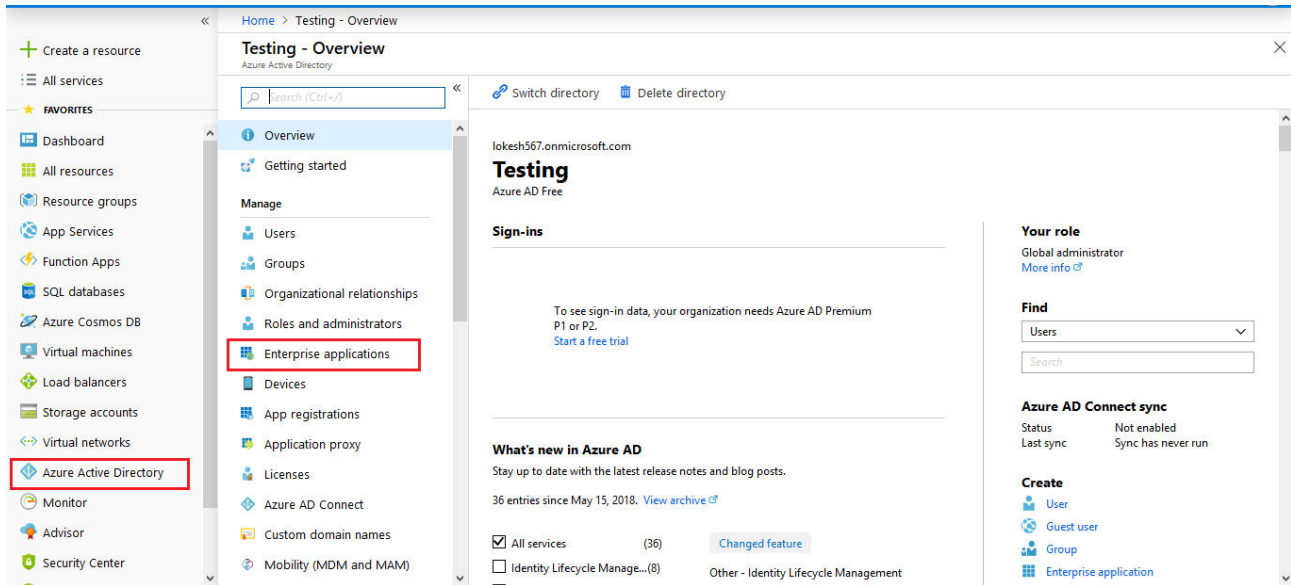
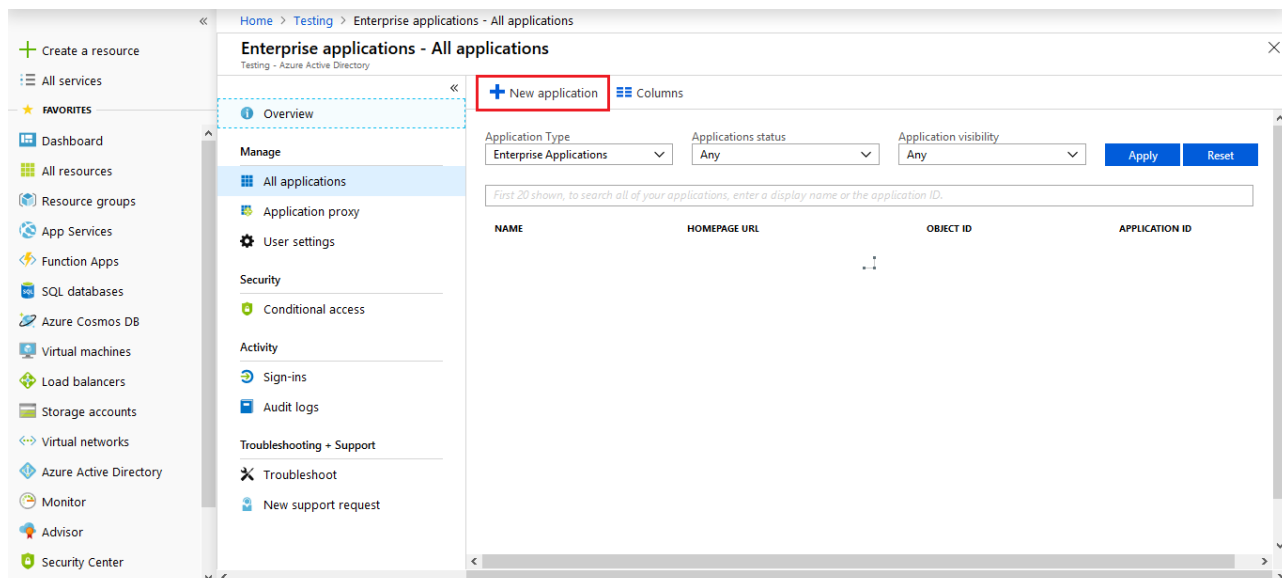


SETUP GUIDE FOR Azure AD AS IdP

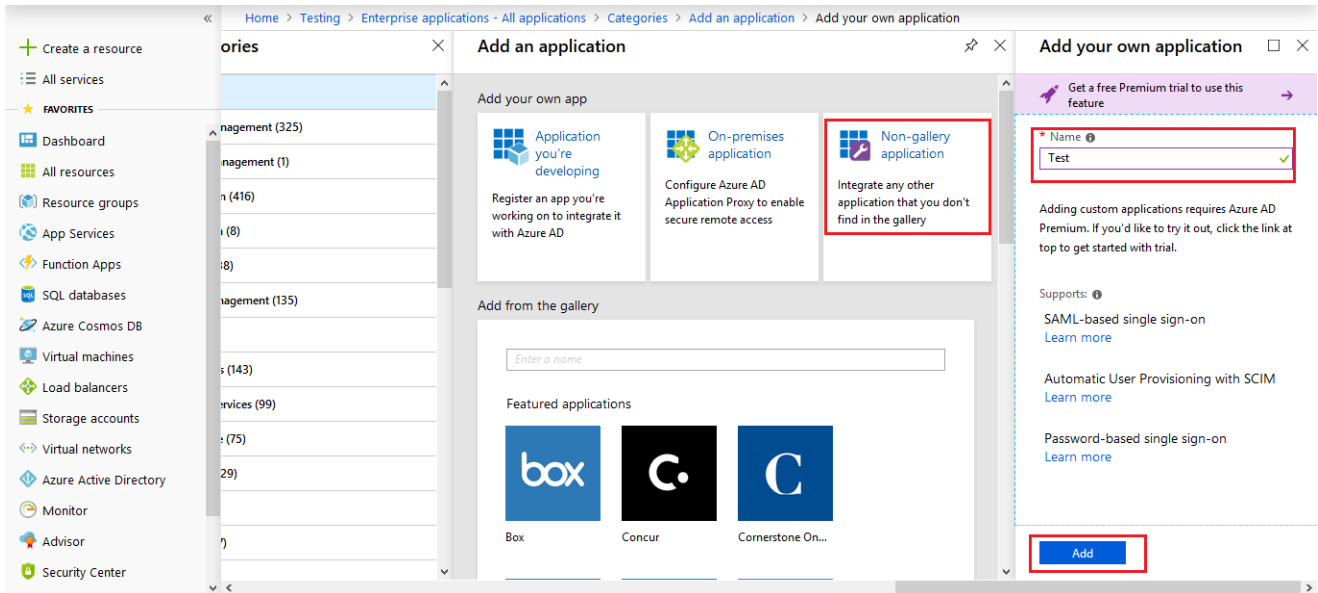
STEP 1: Navigate to Azure Management Console. Proceed to the **Azure Active Directory** tab and navigate to the **Enterprise Applications** tab.



- Click on **New Application**.



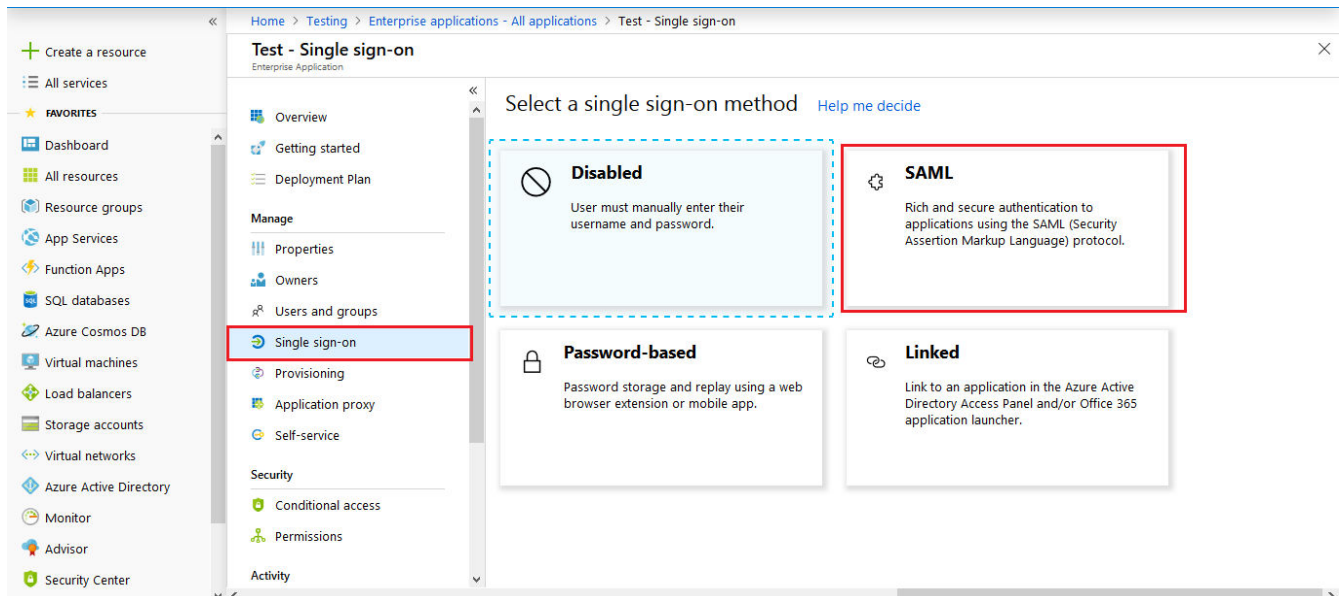
- Click on **Non-gallery application** section and enter the name for your app and click on **Add** button.



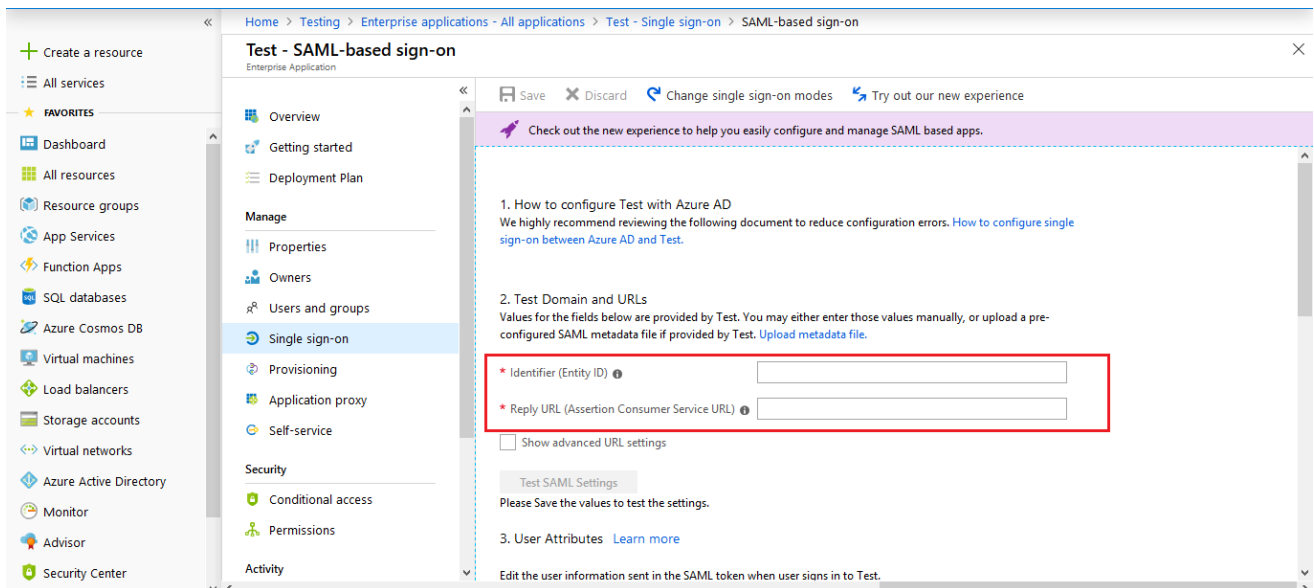
STEP 2: Configure Application

➤ Single Sign On Configuration

- Click on **Single sign-on** from the application's left hand navigation menu. The next screen presents the options for configuring single sign-on. Click on **SAML**.



- Enter the **SP Entity ID** for **Identifier** and the **ACS URL** for **Reply URL** from Identity Provider tab of the plugin.



Home > Testing > Enterprise applications - All applications > Test - Single sign-on > SAML-based sign-on

Test - SAML-based sign-on

Enterprise Application

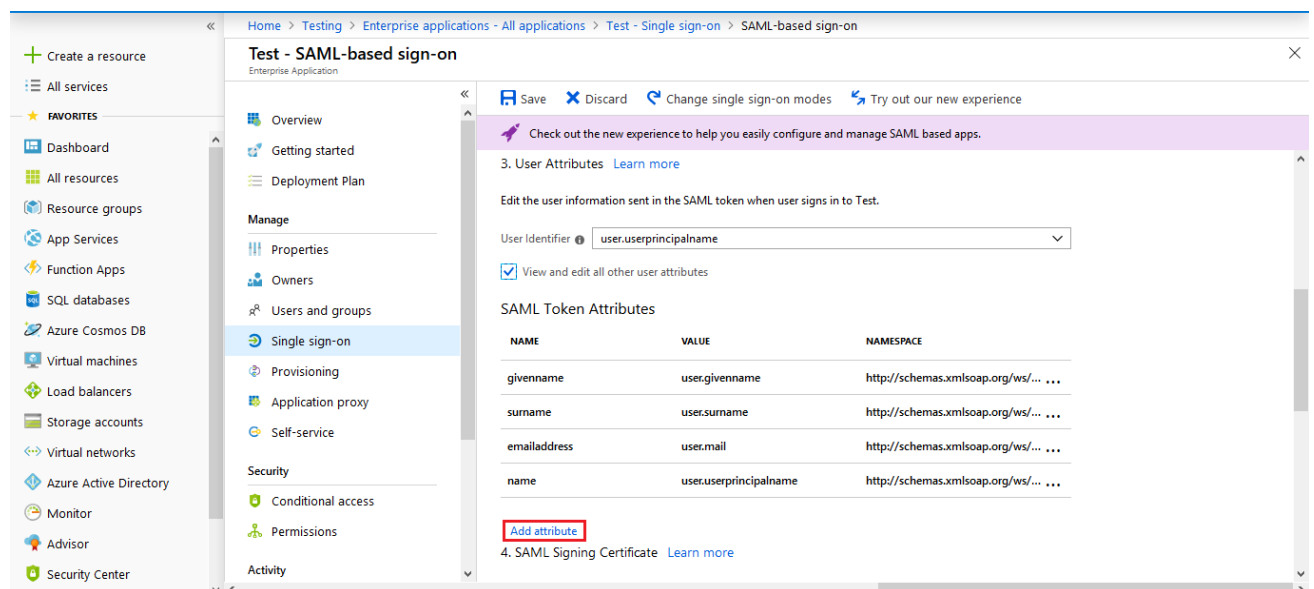
Save Discard Change single sign-on modes Try out our new experience

Check out the new experience to help you easily configure and manage SAML based apps.

- How to configure Test with Azure AD
We highly recommend reviewing the following document to reduce configuration errors. [How to configure single sign-on between Azure AD and Test.](#)
- Test Domain and URLs
Values for the fields below are provided by Test. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by Test. [Upload metadata file.](#)
 - * Identifier (Entity ID)
 - * Reply URL (Assertion Consumer Service URL)☐ Show advanced URL settings
- User Attributes [Learn more](#)
Edit the user information sent in the SAML token when user signs in to Test.

Test SAML Settings
Please Save the values to test the settings.

- By default following attributes will be sent in the SAML token. You can view or edit the claims sent in the SAML token to the application under the **Attributes** tab.



Home > Testing > Enterprise applications - All applications > Test - Single sign-on > SAML-based sign-on

Test - SAML-based sign-on

Enterprise Application

Save Discard Change single sign-on modes Try out our new experience

Check out the new experience to help you easily configure and manage SAML based apps.

3. User Attributes [Learn more](#)
Edit the user information sent in the SAML token when user signs in to Test.
User Identifier
- ☒ View and edit all other user attributes

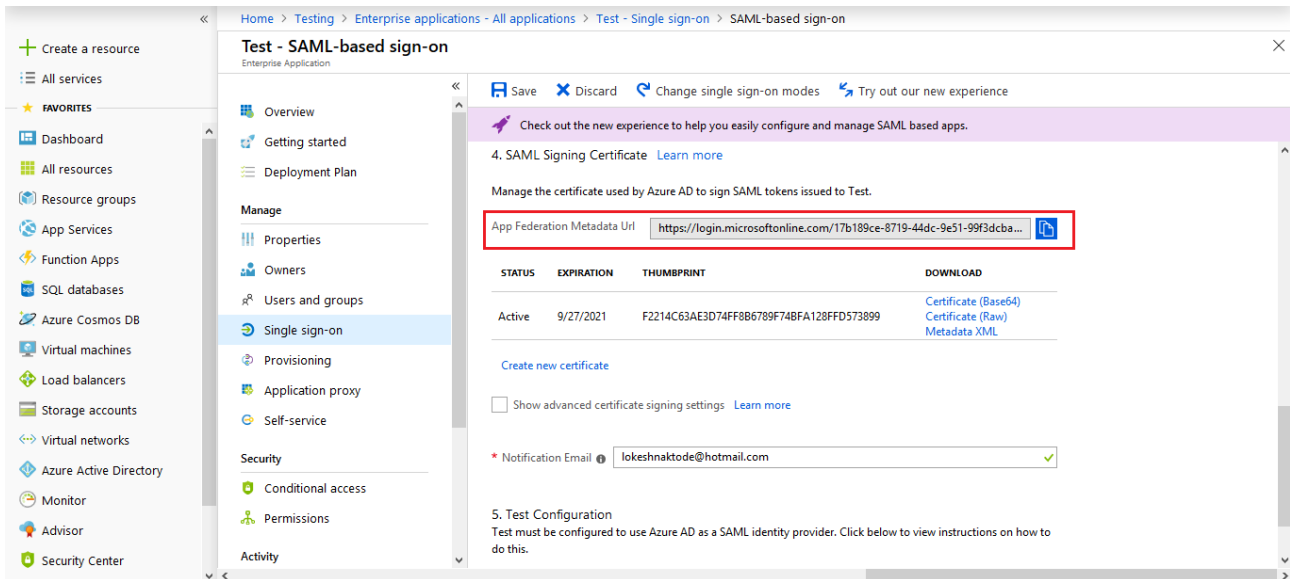
SAML Token Attributes

NAME	VALUE	NAMESPACE
givenname	user.givenname	http://schemas.xmlsoap.org/ws/... ..
surname	user.surname	http://schemas.xmlsoap.org/ws/... ..
emailaddress	user.mail	http://schemas.xmlsoap.org/ws/... ..
name	user.userprincipalname	http://schemas.xmlsoap.org/ws/... ..

[Add attribute](#)

4. SAML Signing Certificate [Learn more](#)

- Copy **App Federation Metadata Url**(will be used in Step 3).



Home > Testing > Enterprise applications - All applications > Test - Single sign-on > SAML-based sign-on

Test - SAML-based sign-on

Enterprise Application

Save Discard Change single sign-on modes Try out our new experience

Check out the new experience to help you easily configure and manage SAML based apps.

4. SAML Signing Certificate [Learn more](#)

Manage the certificate used by Azure AD to sign SAML tokens issued to Test.

App Federation Metadata Url <https://login.microsoftonline.com/17b189ce-8719-44dc-9e51-99f3dcba...>

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	9/27/2021	F2214C63AE3D74FF8B6789F74BFA128FD573899	Certificate (Base64) Certificate (Raw) Metadata XML

[Create new certificate](#)

☐ Show advanced certificate signing settings [Learn more](#)

* Notification Email

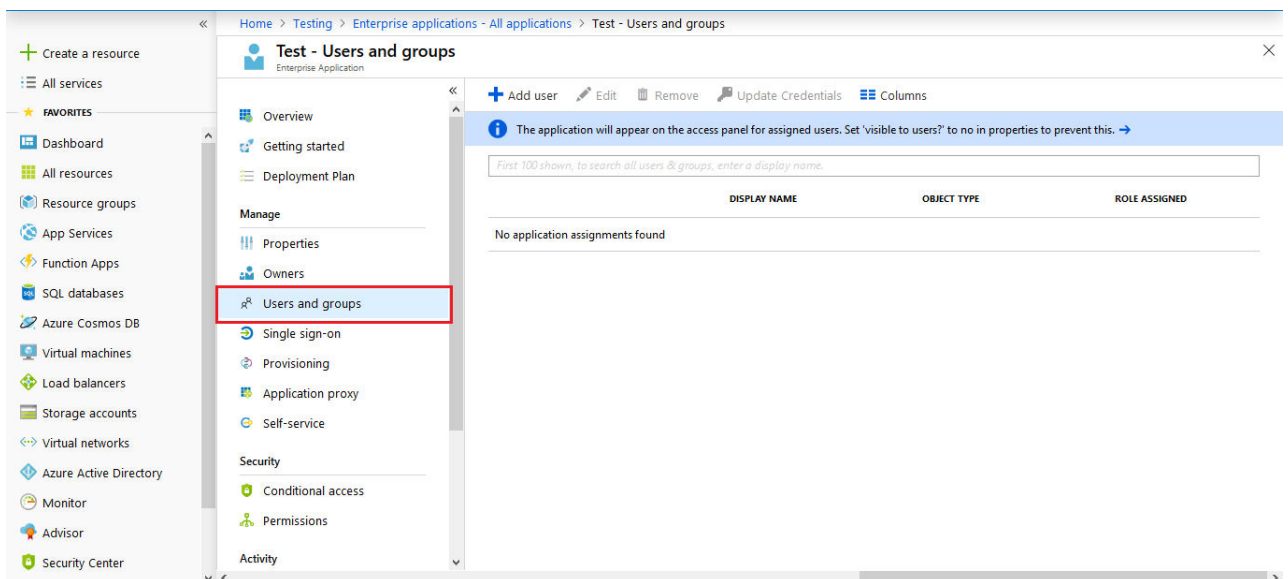
5. Test Configuration

Test must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.

- You can also save the metadata document by going to this endpoint.
- Information in this metadata document is required to configure your Wordpress website.

➤ Assign users and groups to your SAML application

- As a security control, Azure AD will not issue a token allowing a user to sign into the application unless Azure AD has granted access to the user. Users may be granted access directly, or through a group membership.
- Click on **User and groups** from the applications left hand navigation menu. The next screen appears the options for assigning the users/groups to the application.



Home > Testing > Enterprise applications - All applications > Test - Users and groups

Test - Users and groups

Enterprise Application

+ Add user Edit Remove Update Credentials Columns

The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

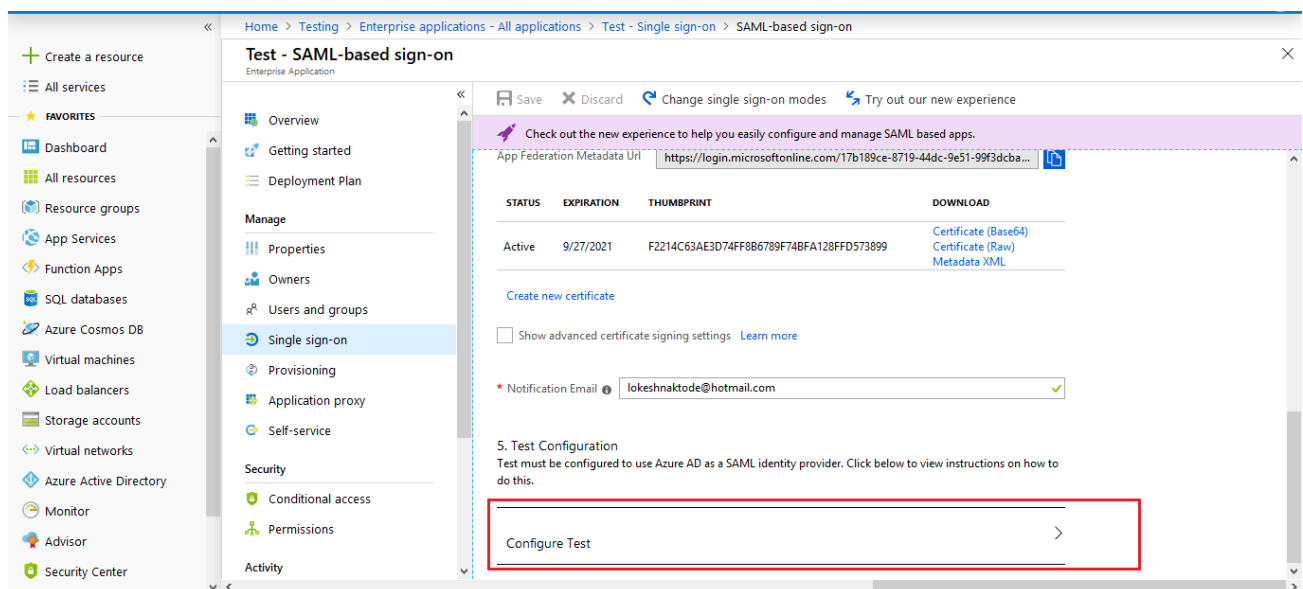
First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
No application assignments found		

STEP 3: Configuring Wordpress as SP

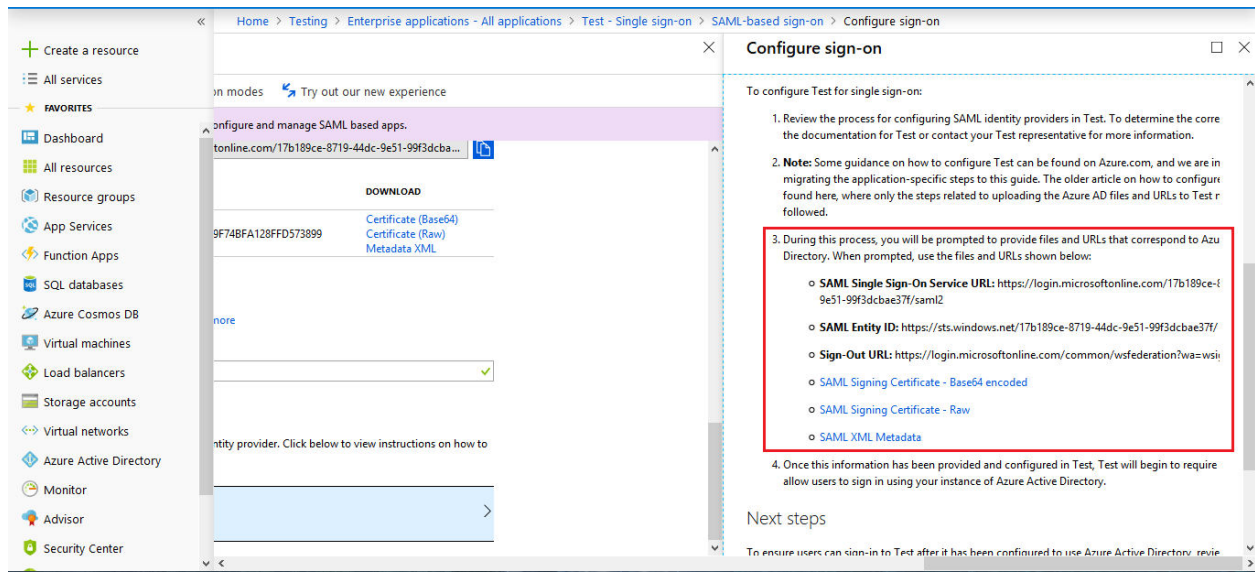
In miniOrange SAML plugin, go to **Service Provider** tab. There are three ways to configure the plugin:

- **By Azure AD Metadata URL**
 1. Click on Upload IDP Metadata.
 2. Enter Identity provider Name.
 3. Enter Metadata URL (**copied in step 2**) and click on Fetch Metadata.
- **By Uploading Azure AD Metadata**
 1. Click on Upload IDP Metadata.
 2. Enter Identity Provider Name.
 3. Upload metadata file and click on Upload.
- **Manual Configuration**
 1. Click on **Configure Test** to see the application's SAML documentation.



2. Enter the following values in the **Service Provider** tab in the plugin configuration.

- **Identity Provider Name:** Azure AD
- **SAML Login URL:** The SAML Single-Sign-On Endpoint URL (See Image)
- **SAML Logout URL:** The SAML Sign-Out Endpoint URL (See Image)
- **IdP Entity ID:** SAML Entity ID in the Federation Metadata document.
- **X.509 Certificate:** SAML Signing Certificate.
- **Response Signed:** Unchecked
- **Assertion Signed:** Checked



STEP 4: Attribute Mapping

In miniOrange SAML plugin, go to **Attribute/RoleMapping** tab. Enter the following values:

- **Username:** Name of the username attribute from IdP (Keep NameID by default)
- **Email:** Name of the email attribute from IdP (Keep NameID by default)
- **FirstName:** Name of the firstname attribute from IdP
- **LastName:** Name of the lastname attribute from IdP
- **Group/Role:** Name of the Role attribute from IdP

Service Provider
Identity Provider
Attribute/Role Mapping
Configuration Settings
Sign in Settings

Attribute Mapping (Optional)

[[Click Here](#) to know how this is useful.]

NOTE: Use attribute name **NameID** if Identity is in the *NameIdentifier* element of the subject statement in SAML Response.

Username *:

Email *:

First Name:

Last Name:

Group/Role:

Save

You can check the **Test Configuration Results** to get a better idea as to which values to map here.

STEP 5: Role mapping (It is Optional to fill this)

- WordPress uses a concept of Roles, designed to give the site owner the ability to control what users can and cannot do within the site.
- WordPress has six pre-defined roles: Super Admin, Administrator, Editor, Author, Contributor and Subscriber.
- Role mapping helps you to assign specific roles to users of a certain group in your IdP.
- While auto registering, the users are assigned roles based on the group they are mapped to.

Role Mapping (Optional)

[[Click Here](#) to know how this is useful.]

NOTE: Role will be assigned only to new users. Existing Wordpress users' role remains same.

☐ *Do not auto create users if roles are not mapped here.

☐ Do not assign role to unlisted users.

Default Role: Select the default role to assign to Users.

Administrator

Editor

Author

Contributor

Subscriber

STEP 6: SSO Settings

- Go to **Sign In Settings** tab. Enable auto-redirect to IDP using **Redirect to IdP if user not logged in** option.

Service Provider

Identity Provider

Attribute/Role Mapping

Configuration Settings

Sign in Settings

Sign in options

☐ *Redirect to IdP if user not logged in. [\[What does this mean?\]](#)

☐ Force authentication with your IdP on each login attempt. [\[What does this mean?\]](#)

Choose how you want users to log into your WordPress website. You can choose any or all of the three options below.

Option 1: Use Default WordPress Login

☐ Check this option if you want to auto redirect the user to IdP. [\[What does this mean?\]](#)

☐ Checking this option creates a backdoor to login to your Website using WordPress credentials incase you get locked out of your IdP. (Note down this URL: `https://localhost/wordpress_single_site1/wp-login.php?saml_sso=false`)

WARNING: Checking the above option will enable a security hole. Anybody knowing the above URL will be able to login to your website using WordPress Credentials. Please do not share this URL.

Option 2: Use a Widget

☐ Check this option if you want to add a Widget to your page.

Option 3: Use a ShortCode

☐ Check this option if you want to add a shortcode to your page.