










Azure AD / Office 365 Single Sign-On (SSO) login for WordPress [SAML] can be achieved by using our WordPress SAML SP Single Sign-On (SSO) plugin. Our plugin is compatible with all the SAML compliant Identity providers. Here we will go through a step-by-step guide to configure SAML SSO login between Wordpress site and Azure AD / Office 365 by considering Azure AD/Office 365 as IdP (Identity Provider) and WordPress as SP (Service Provider).

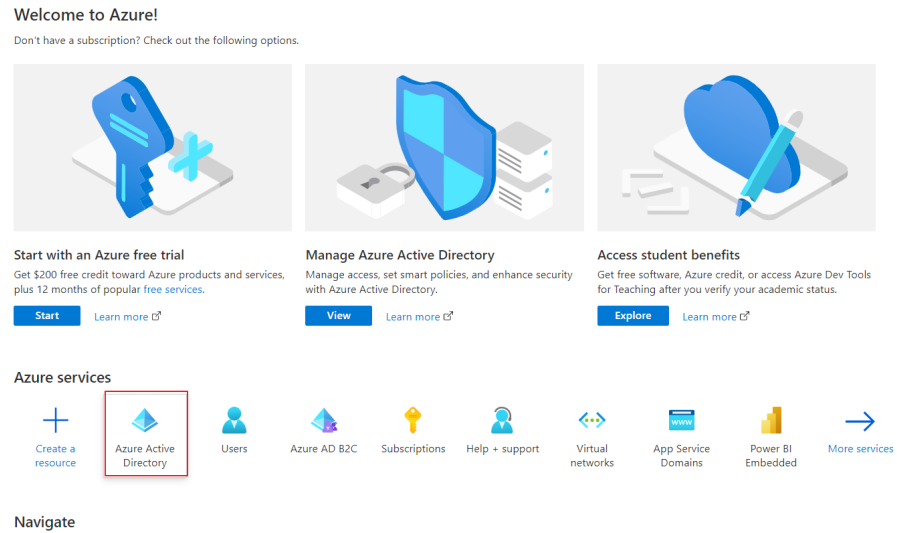
Steps to configure Azure AD Single Sign-On (SSO) into WordPress

Step 1: Setup Azure AD as IDP (Identity Provider)

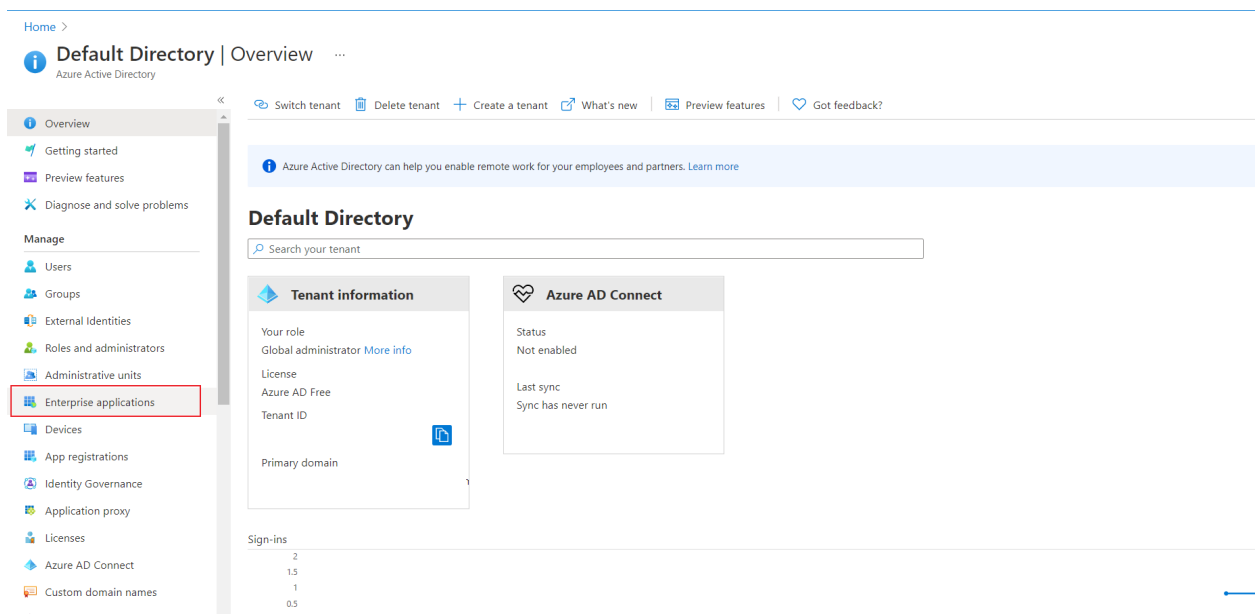
 **Configure Azure AD as IdP** : In the miniOrange SAML SP SSO plugin, navigate to **SP (Service Provider) Metadata** tab. Here, you can find the SP metadata such as SP Entity ID and ACS (AssertionConsumerService) URL which are required to configure the Azure AD as IdP (Identity Provider)

SP-EntityID / Issuer	http://your-wordpress-domain/wp-content/plugins/miniorange-saml-20-single-sign-on/	
ACS (AssertionConsumerService) URL	http://your-wordpress-domain/	
Single Logout URL	http://your-wordpress-domain/	
Audience URI	http://your-wordpress-domain/wp-content/plugins/miniorange-saml-20-single-sign-on/	
NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	
Recipient URL	http://your-wordpress-domain/	
Destination URL	http://your-wordpress-domain/	
Default Relay State (Optional)	http://your-wordpress-domain/	
Certificate (Optional)	Download	

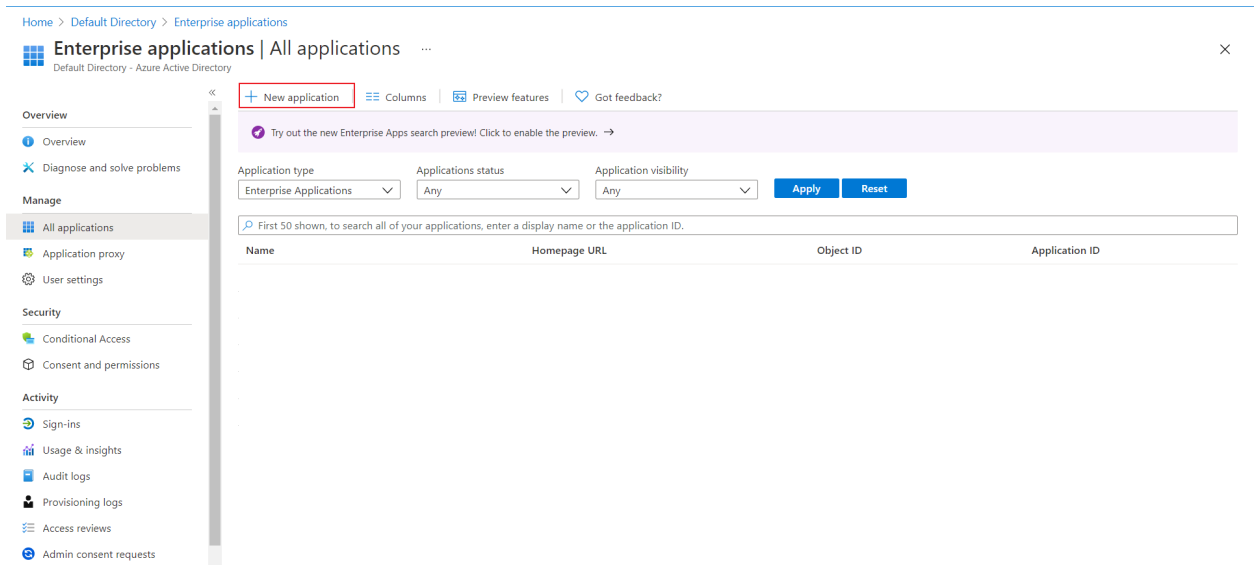
- Log in to [Azure AD Portal](#)
- Select **Azure Active Directory**.



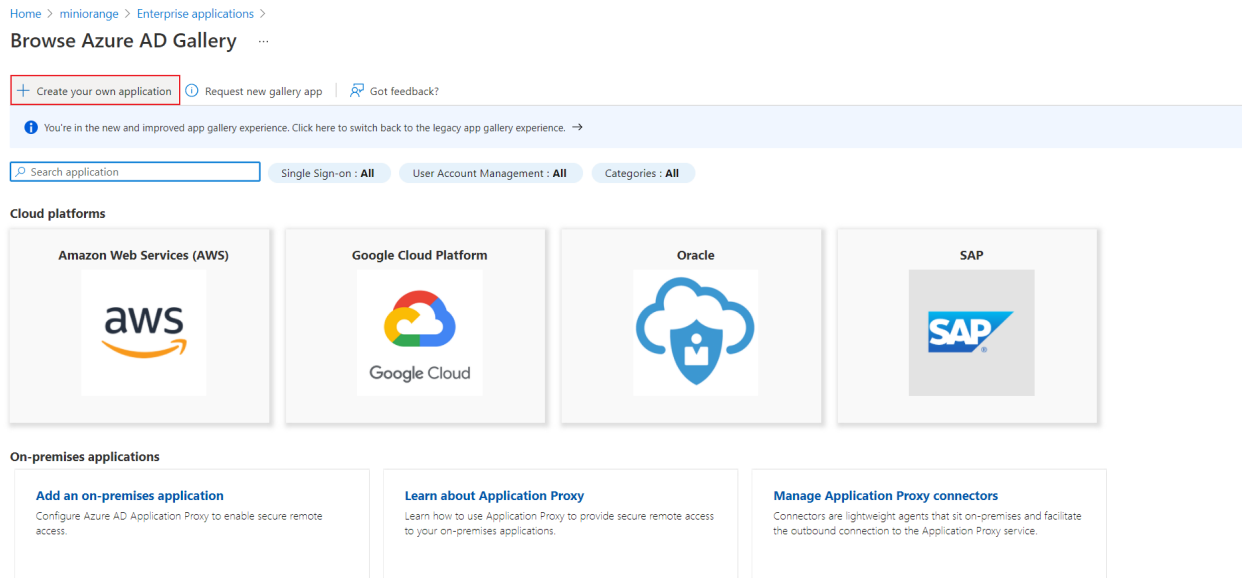
- Select **Enterprise Application**.



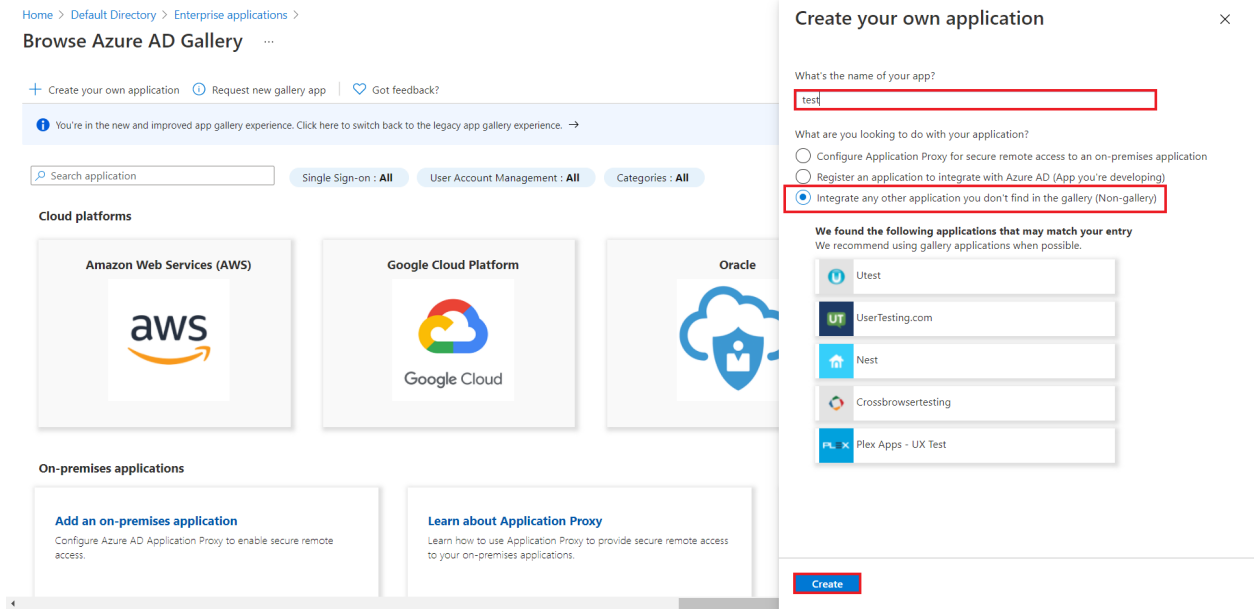
- Click on **New Application**.



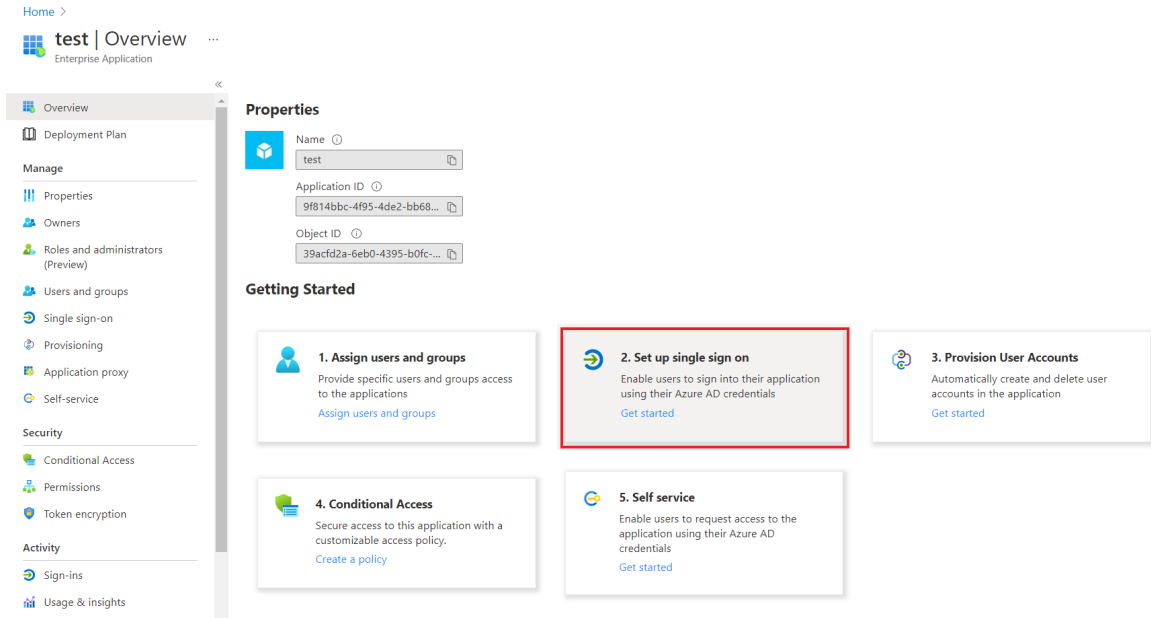
- Click on **Create your own Application**.



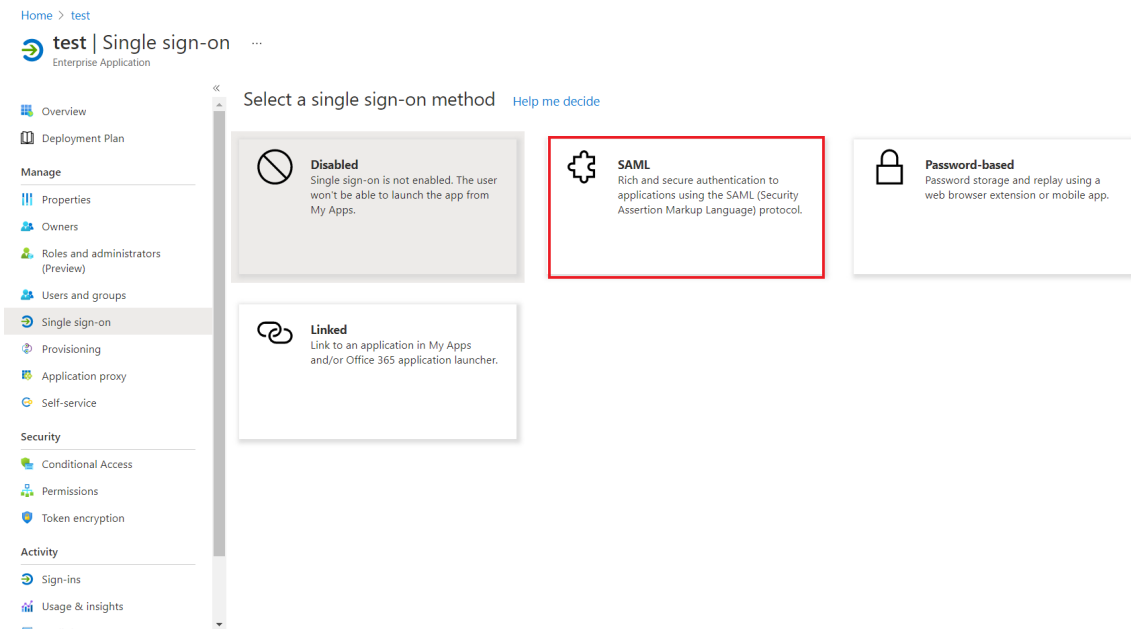
- Enter the name for your app then select the Non-gallery **application** section and click on **Create** button.



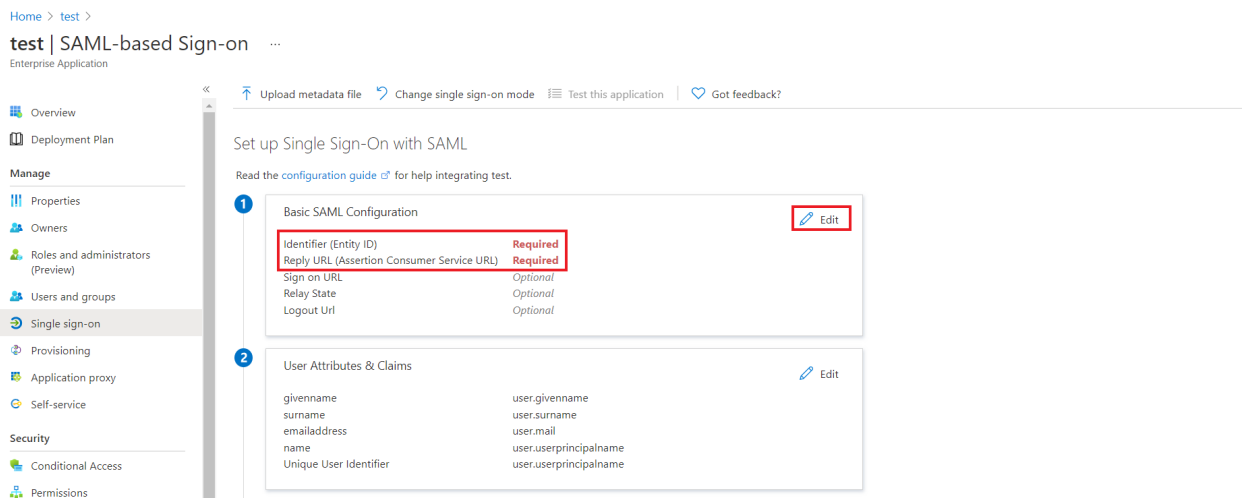
- Click on **Setup Single sign-on**.



- Select the **SAML** tab.



- After clicking on **Edit**, enter the **SP Entity ID** for **Identifier** and the **ACS URL** for **Reply URL** from the Service **Provider Metadata** tab of the plugin.



Home > test > test | SAML-based Sign-on ...
Enterprise Application

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-ins
Usage & insights

Set up Single Sign-On with SAML
Read the [configuration guide](#) for help integrating test.

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*

2 User Attributes & Claims

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

3 SAML Signing Certificate

Status	Active
Thumbprint	9CEA37643
Expiration	12/21/2025
Notification Email	demosecur
App Federation Metadata Url	https://lo

Basic SAML Configuration

Save

Identifier (Entity ID) * **Required**
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default
http://adapplicationregistry.onmicrosoft.com/customappssso/primary

Reply URL (Assertion Consumer Service URL) * **Required**
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Sign on URL **Optional**
Enter a sign on URL

Relay State **Optional**
Enter a relay state

Logout Url **Optional**
Enter a logout url

- By default, the 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 > test > test | SAML-based Sign-on ...
Enterprise Application

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service

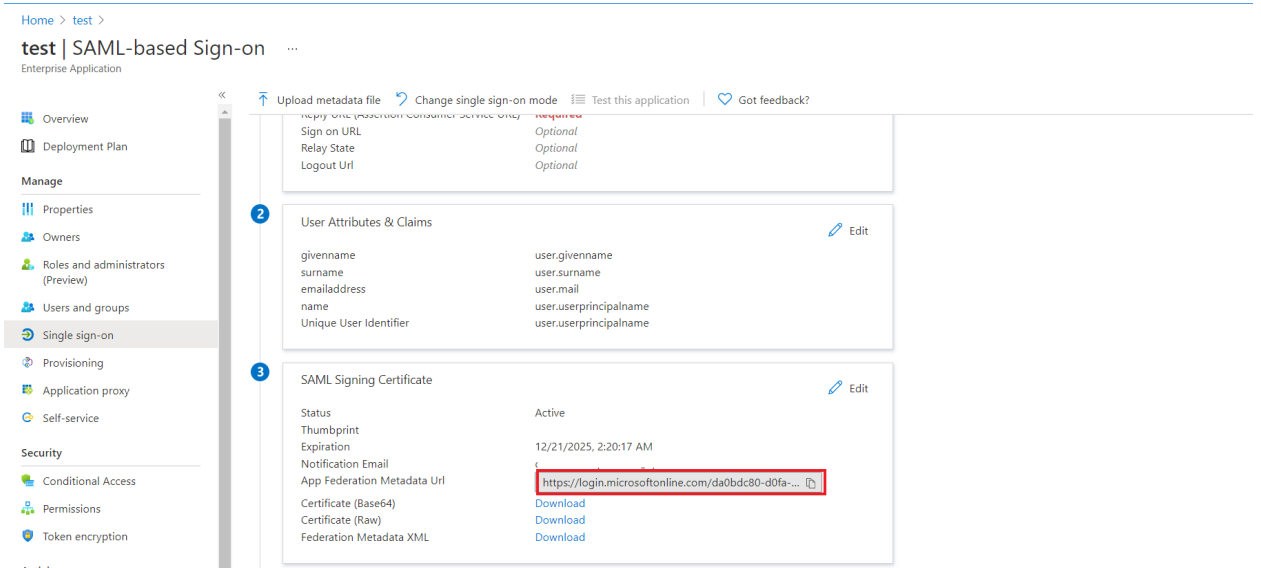
1 Basic SAML Configuration

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

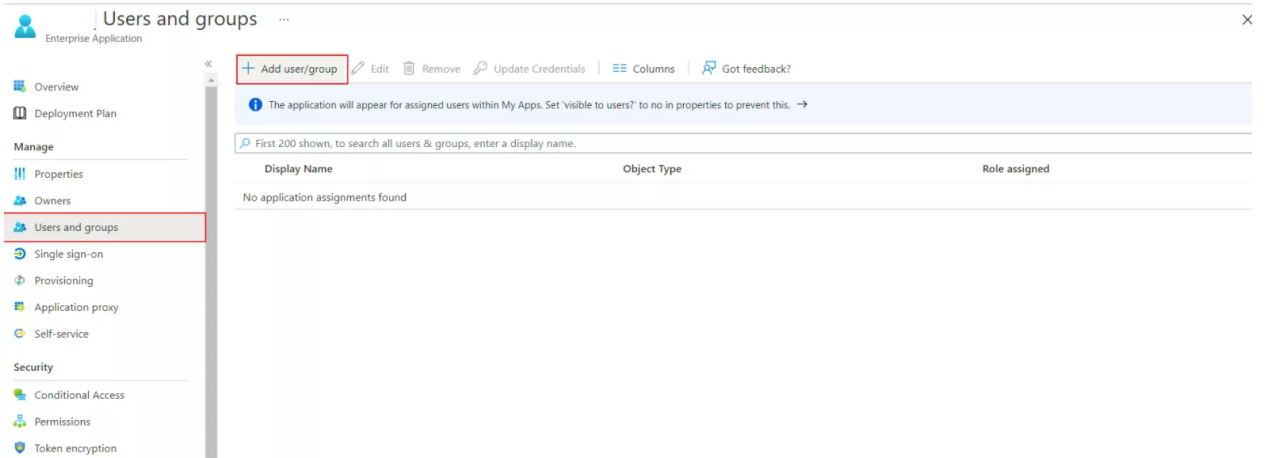
2 User Attributes & Claims

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

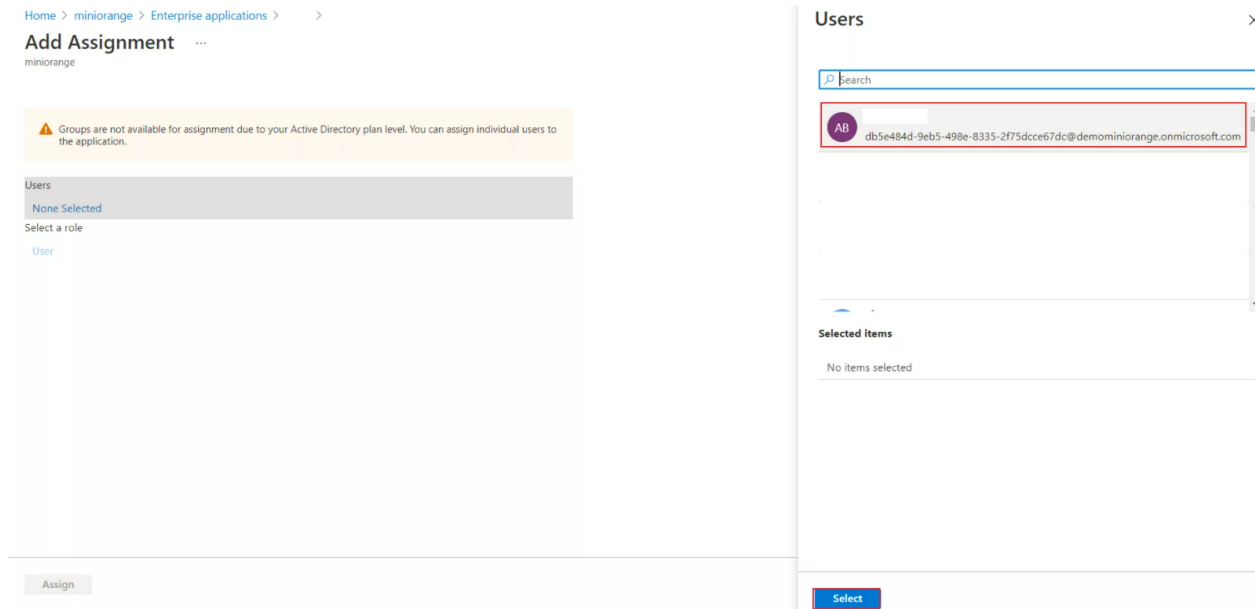
Copy **App Federation Metadata Url** to get the **Endpoints** required for configuring your **Service Provider**.



- **Assign users and groups to your SAML application**
 - Navigate to **Users and groups** tab and click on **Add user/group**.



- Click on **Users** to assign the required user and then click on **select**.



- You can also assign a role to your application under the Select **Role** section.

Step 2: Configuring WordPress as SP (Service Provider)

We will go through the steps to set up WordPress as a Service Provider. Here, we will be adding the IdP metadata to configure the plugin.

In the miniOrange SAML plugin, go to the Service Provider Setup tab of the plugin. There are two ways to configure the plugin:

A. By uploading IDP metadata:

- Click on **Upload IDP metadata** button.
- Enter the **Identity Provider Name**
- You can either **upload a metadata file** and click on **Upload** button or use a **metadata URL** and click on **Fetch Metadata**.
- In the **Premium plugin**, you can **enable auto-sync** for the **metadata URL** which will auto-update the plugin configuration as per the IDP metadata after a set interval of time

Upload IDP Metadata

Cancel

Identity Provider Name*:

Upload Metadata: No file chosen

OR

Enter metadata URL:

Update IdP settings by pinging metadata URL ? (We will store the metadata URL)

Select how often you want to ping the IdP :

B.Manual Configuration:

- Provide the required settings (i.e. Identity Provider Name, IdP Entity ID or Issuer, SAML Login URL, X.509 Certificate) as provided by your **Identity Provider** and click on the **Save** button.
- In the Premium Plugin, you can provide the SAML Logout URL to achieve Single Logout on your WordPress site.

Step 3: Attribute Mapping

- **Attribute Mapping** feature allows you to map the **user attributes** sent by the IDP during SSO to the user attributes at WordPress.
- In the WordPress SAML plugin, go to **Attribute/Role Mapping** tab and fill up the following fields in **Attribute Mapping** section.

Attribute Mapping

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

Username *:	<input type="text" value="NameID"/>
Email *:	<input type="text" value="NameID"/>
First Name:	<input type="text" value="--Select an Attribute--"/>
Last Name:	<input type="text" value="--Select an Attribute--"/>
Group/Role:	<input type="text" value="--Select an Attribute--"/>
Display Name:	<input type="text" value="Username"/>

- **Custom Attribute Mapping:** This feature allows you to map any attribute sent by the IDP to the **usermeta** table of WordPress.

Map Custom Attributes

Map extra IDP attributes which you wish to be included in the user profile.

NOTE: Customized Attribute Mapping means you can map any attribute of the IDP to the attributes of **user-meta** table of your database.

Enable the **Display Attribute** option for an attribute if you want to display it in the Wordpress [Users](#) menu.

Attribute Name	Attribute Value	Display Attribute
<input type="text" value="Custom attribute name"/>	<input type="text" value="--Select an Attribute--"/>	<input type="checkbox"/>

Step 4: Role Mapping

- This feature allows you to assign and manage roles of the users when they perform SSO. Along with the default WordPress roles, this is compatible with any custom roles as well. From the **Attribute Mapping** section of the plugin, provide a mapping for the field named **Group/Role**. This attribute will contain the role related information sent by the IDP and will be used for Role Mapping.
- Navigate to the role mapping section and provide the mappings for the highlighted roles.

Role Mapping (Optional)

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

NOTE: Role will be assigned only to non-admin users (user that do NOT have Administrator privileges). You will have to manually change the role of Administrator users.

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

Do not assign role to unlisted users.

Do not update existing user's roles.

Do not allow the users to login with the following roles.

Semi-colon(;) separated Group/Role value

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

Administrator	<input type="text" value="Semi-colon(;) separated Group/Role value for Administrator"/>
Editor	<input type="text" value="wp-editor"/>
Author	<input type="text" value="Semi-colon(;) separated Group/Role value for Author"/>
Contributor	<input type="text" value="Semi-colon(;) separated Group/Role value for Contributor"/>
Subscriber	<input type="text" value="Semi-colon(;) separated Group/Role value for Subscriber"/>

Save

- For example, If you want a user whose **Group/Role** attribute value is wp-editor to be assigned as an Editor in WordPress, just provide the mapping as wp-editor in the **Editor** field of Role Mapping section.

Step 5: SSO settings

- In the Premium plugin you can enable SP-initiated SSO using the following options.**Auto-Redirection from site:** If this option is enabled, any unauthenticated user trying to access your site will get redirected to the IDP login page and after successful authentication they will be redirected back to the same page on your site which they were trying to access.

- **Steps:**

1. Go to the Redirection and SSO Links tab of the plugin and navigate to **Option 1 : Auto-Redirection from site.**
2. Enable **Redirect to IdP if the user is not logged in [PROTECT COMPLETE SITE]** option.

Option 1: Auto-Redirection from site

1. Enable this option if you want to restrict your site to only logged in users. The users will be redirected to your IdP if logged in session is not found.

Redirect to IdP if user not logged in [PROTECT COMPLETE SITE]

HOW DO I PROTECT SPECIFIC PAGES OF MY SITE?

You can use our [Page Restriction](#) add-on to restrict users from accessing specific pages of your site.

Auto-Redirection from WordPress Login: If this option is enabled, any unauthenticated user trying to access the default WordPress login page will get redirected to the IDP login page for authentication. After successful authentication, they will be redirected back to the WordPress site.

- **Steps:**

- 1. Go to the Redirection and SSO Links tab of the plugin and navigate to **Option 2: Auto-Redirection from WordPress Login**.
- 2. Enable **Redirect to IdP from WordPress Login Page** option.

Option 2: Auto-Redirection from WordPress Login

1. Enable this option if you want the users visiting any of the following URLs to get redirected to your configured IdP for authentication:

Redirect to IdP from WordPress Login Page

2. Enable this option to create a backdoor, using which you can login to your website using WordPress credentials, incase you get locked out of your IDP.

Enable backdoor login

Backdoor URL:
(Please note it down)

Update

WARNING: Enabling the above option will open 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.

NOTE: Please enable the Backdoor login and note down the backdoor URL. This will allow you to access the WordPress login page in case you get locked out of the IDP login.

Login Button: You can add a customized login button anywhere on your site or WordPress login page by navigating to **Option 3: Login Button** section of Redirection and SSO Links tab.

Option 3: Login button

Enable this option to redirect your users to WordPress Login Page if they are not already logged in.

- Redirect to WP Login page
- Add a Single Sign on button on the Wordpress login page
- Use button as ShortCode
- Use button as Widget

Customize Login Button:

Shape

- Round
- Rounded Edges
- Square
- Long Button with Text

Theme

- Button Color:
- Button Text:
- Font Color:
- Font Size:

Size of Icons

- Width:
- Height:
- Curve:

Position of Login Button on WordPress Login Page :

- Above WP Login Form
- Below WP Login Form

Preview:



- **SSO Links:** You can add SSO links anywhere on your site using the Shortcode and Widget provided in **Option 4: SSO Links** section of Redirection and SSO Links tab.

Option 4: SSO Links

Login text:	<input type="text" value="Login with miniOrange"/>
Greeting text:	<input type="text" value="Hello,"/> <input type="text" value="Username"/>
Logout text:	<input type="text" value="Logout"/>

The above custom texts will be applied to the SSO links, which you can add on your site using the following ways:

Widget:

1. Go to [Widgets](#)
2. Select "Login with miniOrange", drag and drop to your favourite location and save.

Shortcode:

1. For PHP page:

2. For HTML page:

OR

You have successfully configured **WordPress as SAML SP** for achieving **Azure AD SSO**. **Login into your WordPress (WP) Site using Azure AD as IdP**.

In this Guide, you have successfully configured Azure AD SAML Single Sign-On (Azure AD SSO Login) choosing Azure AD as IdP and WordPress as SP using miniOrange SAML Single Sign On – SSO Login plugin. This solution ensures that you are ready to roll out secure access to your WordPress(WP) site using Azure AD login credentials within minutes.