OAuth / OpenID Connect Single Sign-On (SSO) into Joomla using Azure AD

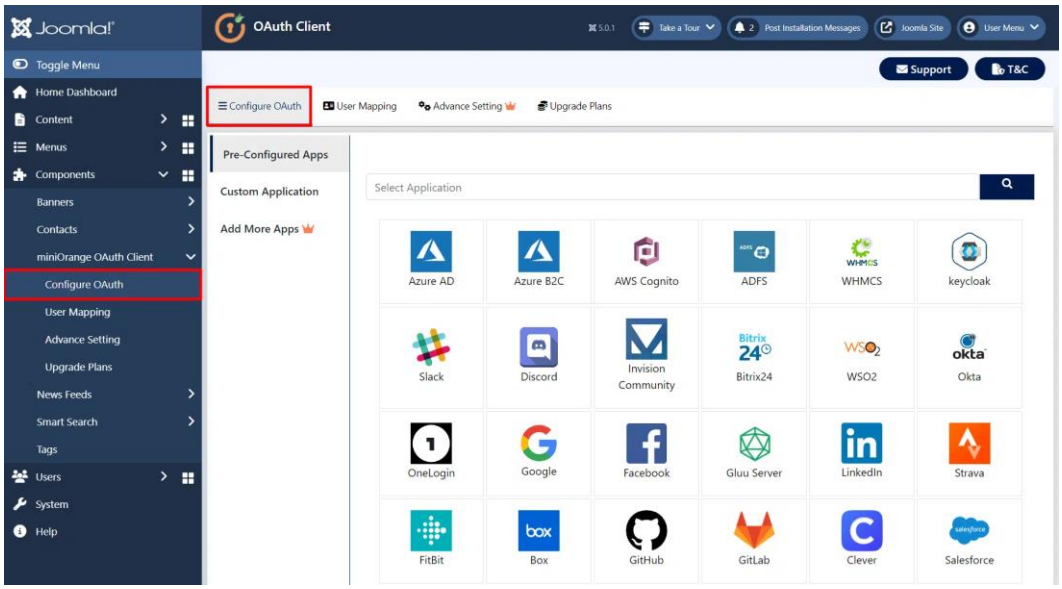
Single Sign-On (SSO) with Microsoft Entra ID (Azure AD) in Joomla uses OAuth Authorization to provide users secure access to the Joomla site. With our Joomla OAuth Single Sign-On (SSO) plugin, Microsoft Entra ID (Azure AD) acts as the OAuth provider, ensuring secure login for Joomla websites.

The integration of Joomla and Microsoft Entra ID (Azure AD) simplifies and secures the login process using OAuth protocol. This solution allows users to access their Joomla sites with Single Sign-On (SSO) using their Microsoft Entra ID (Azure AD) credentials, completely removing the need to store, remember, and reset multiple passwords.

In addition to offering OAuth Single Sign-On (SSO) using Microsoft Entra ID credentials, the plugin also provides advanced SSO features like user profile attribute mapping, role mapping, and Azure multi-tenant login and providing site access based on organization roles. For further insights into the array of features we offer within the Joomla OAuth & OpenID Connect Client plugin, kindly visit our page here. You can follow the below steps to setup Microsoft Entra ID (Azure AD) OAuth SSO with Joomla.

Steps to Install Joomla OAuth Client Plugin

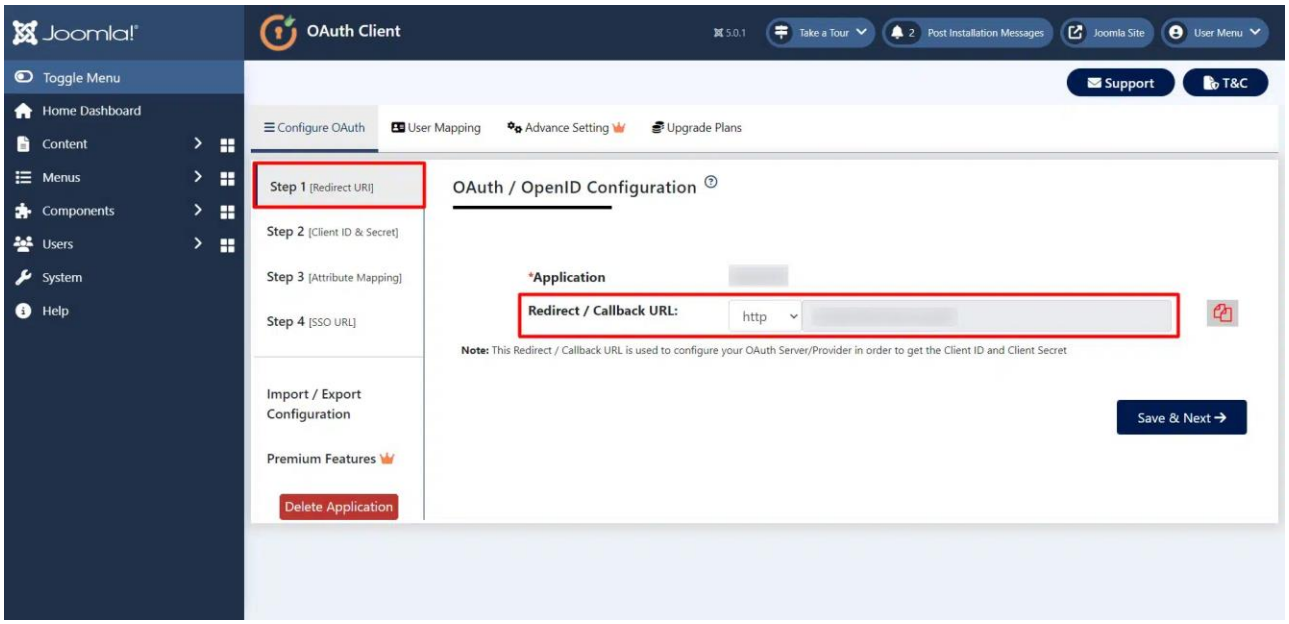
- Download the zip file for the **miniOrange OAuth Client plugin** for Joomla.
- Login into your Joomla site's **administrator console**.
- From left toggle menu, click on **System**, then under **Install** section click on **Extension**.
- Upload the downloaded zip file to install the **Joomla OAuth Client** plugin.
- Installation of the plugin is successful. Now click on **Start Using miniOrange OAuth Client plugin**.
- Under **Configure OAuth -> Pre-Configured Apps** tab, select your **OAuth Provider**. You can also search for **custom OAuth** or **custom OpenID application** in the search bar, and configure your own custom provider.



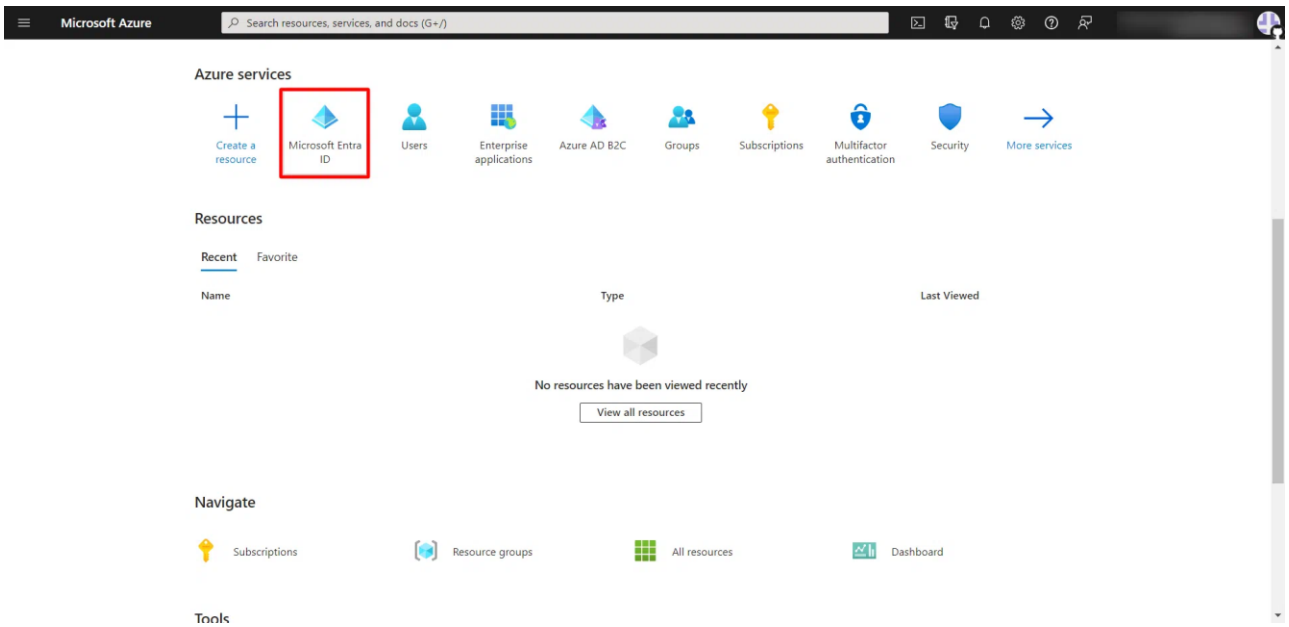
Step 1: Steps to configure Microsoft Entra ID OAuth SSO into Joomla

1. Configure Callback/Redirect URL

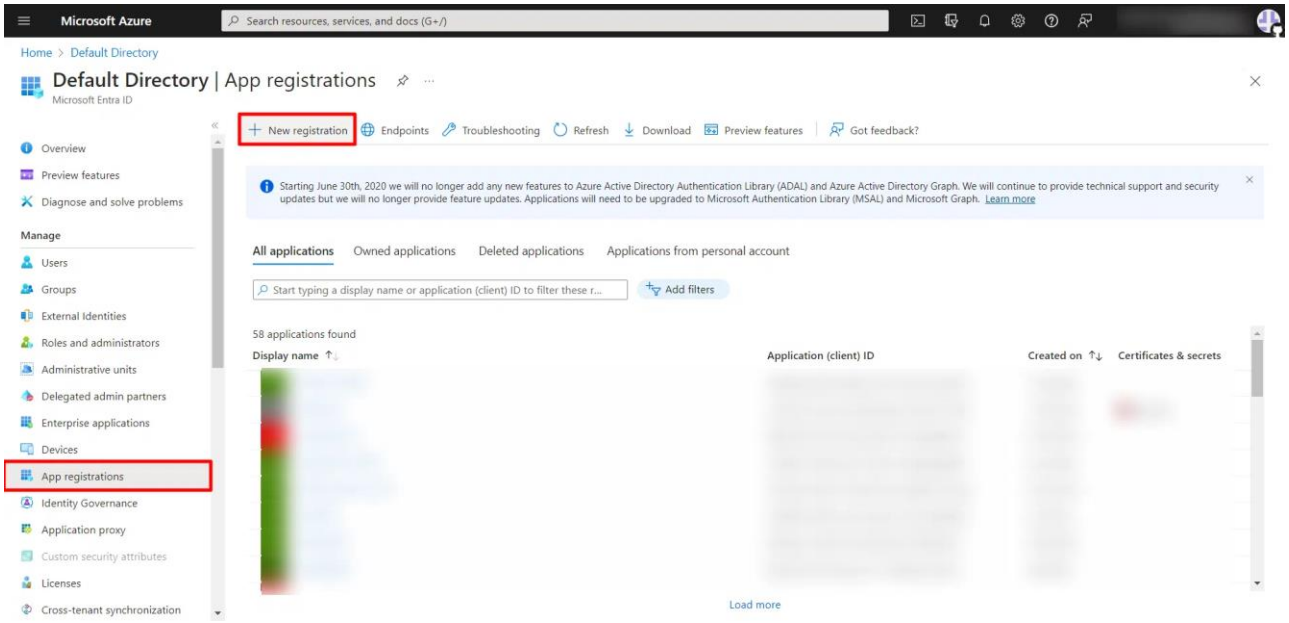
- After selecting your OAuth provider, you will be redirected to the **Step 1 [Redirect URL]** tab. Now copy the **Callback/Redirect URL** which we will use to configure Microsoft Entra ID as OAuth Server, then click on the **Save & Next** button.



- Log into the Azure portal.
- Click on **Microsoft Entra ID** under **Azure services**.



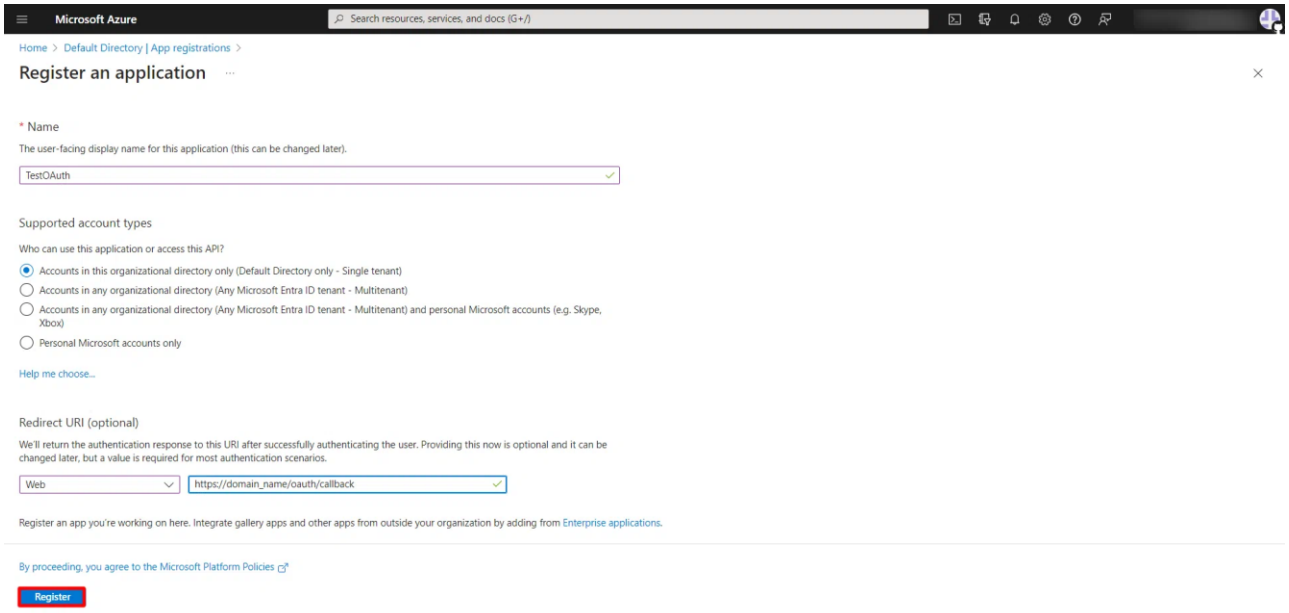
- In the left-hand navigation pane, click the **App registrations**, and click on **New registration**.



- When the Create page appears, enter your application's registration information:

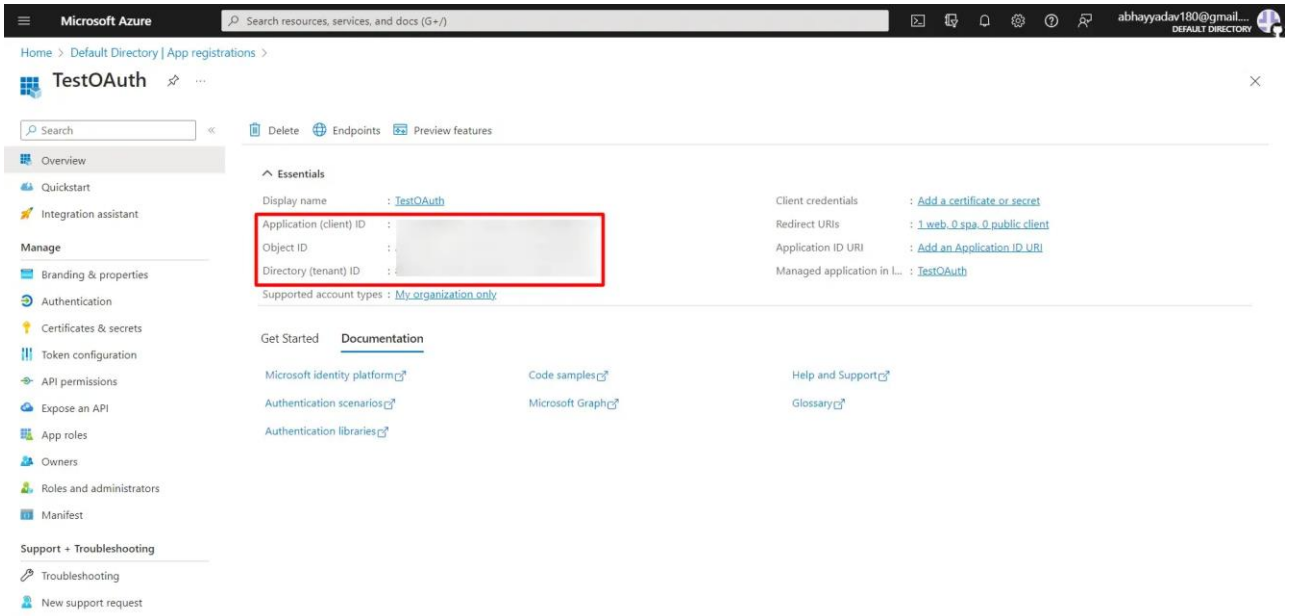
Name: Name of your application.
Application type : 1. Select *"Native"* for client applications that are installed locally on a device. This setting is used for OAuth public native clients 2. Select *"Web app / API"* for client applications and resource/API applications that are installed on a secure server. This setting is used for OAuth confidential web clients and public user-agent-based clients. The same application can also expose both a client and resource/API. **Sign-on URL :** 1. For "Web app / API" applications, provide the base URL of your app. **eg, https://<domain-name>/mo_login** might be the URL for a web app running on your local machine. Users would use this URL to sign in to a web client application. 2. For *"Native"* applications, provide the URI used by Azure AD to return token responses. Enter a value specific to your application. eg, https://localhost/joomla

- Under **Redirect URL**, select **Web** from the dropdown and enter the **Callback URL** copied earlier in the given field. Then, click on the **Register** button to register the new application.

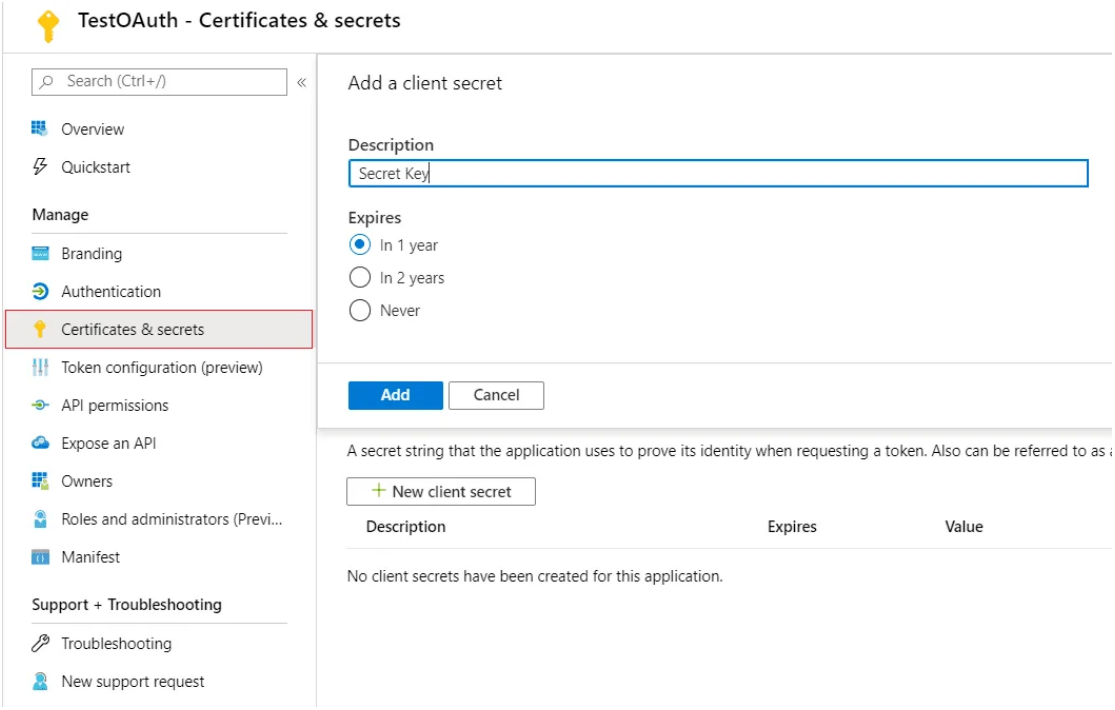


2. Configure Client ID and Secret

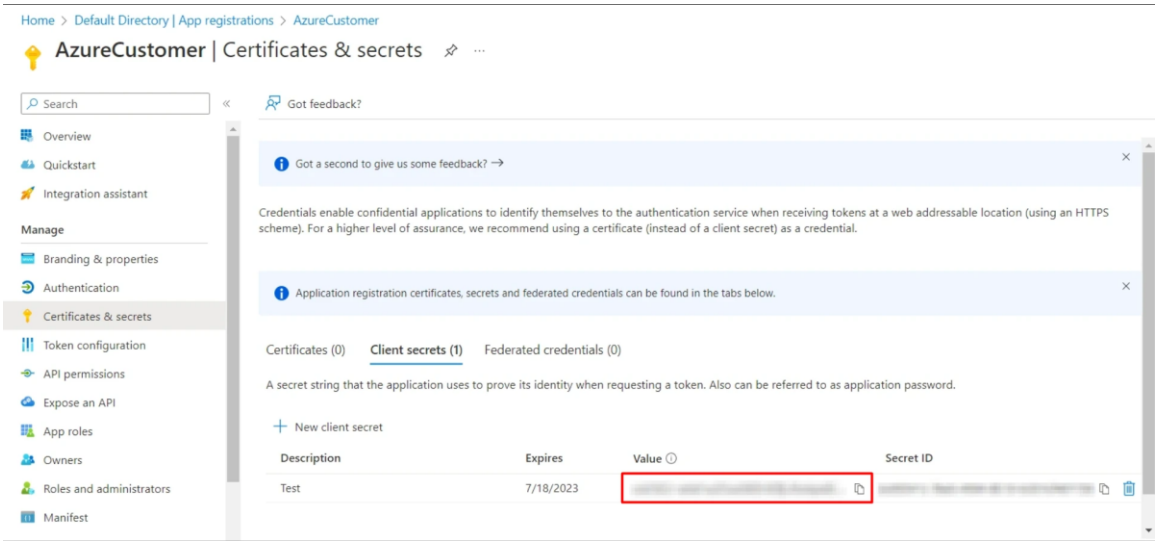
- Now go to the **Overview** tab of your **registered application**. Here, copy the **Application ID** and the **Directory ID**, this will be your **Client ID** and **Tenant ID** respectively.



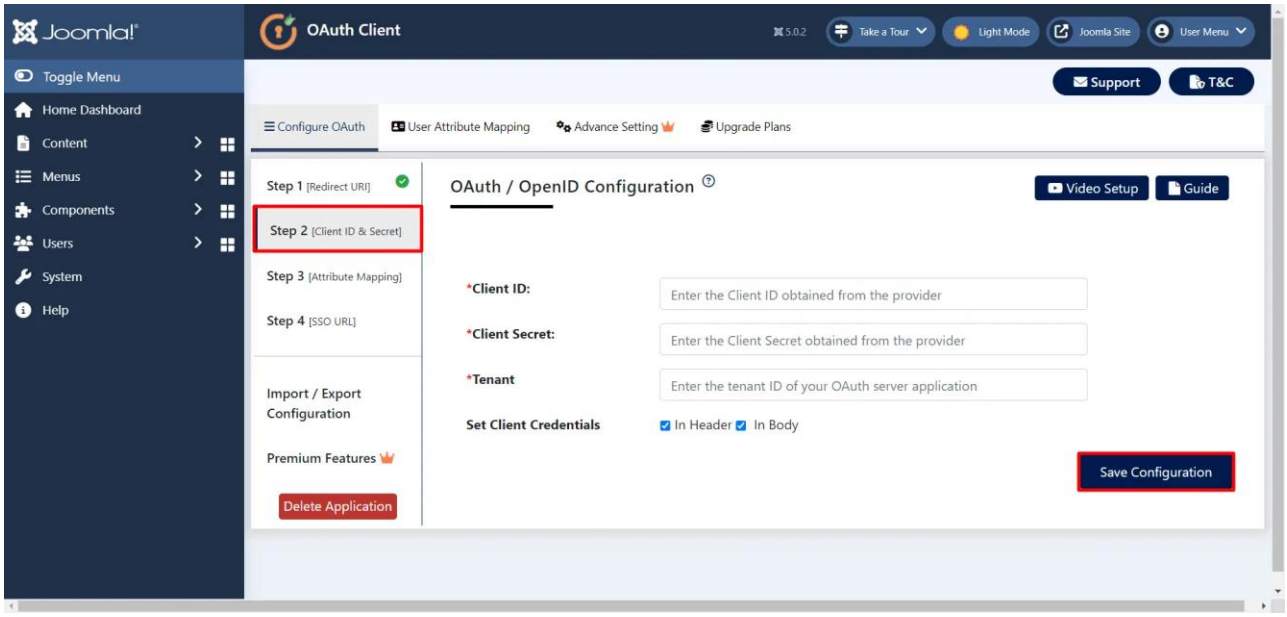
- Go to **Certificates and Secrets** from the left navigation pane and click on **New Client Secret**. Enter description and expiration time and click on **Add** option.



- Copy **value**. This will be your **Client Secret**.

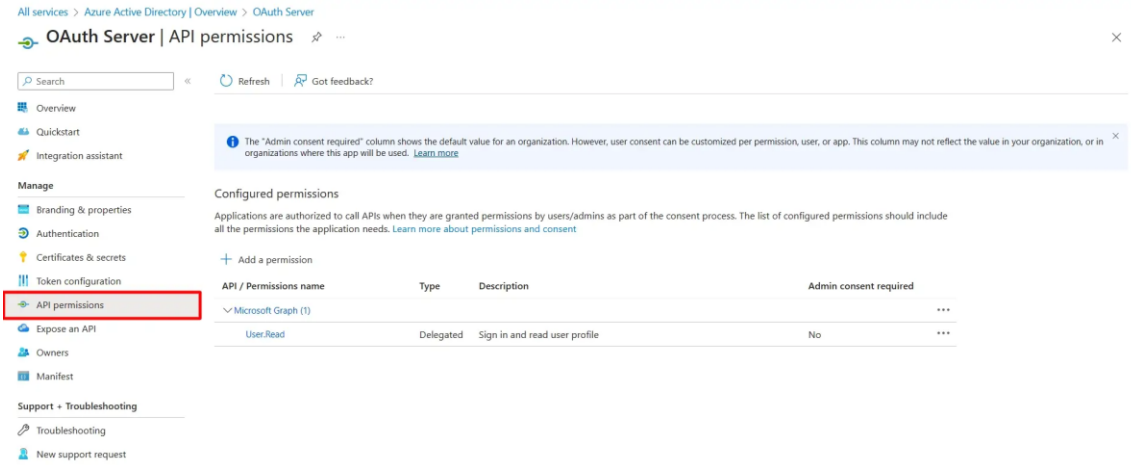


- Go to the **Step 2 [Client ID & Secret]** tab of the Joomla OAuth Client plugin, here paste the **Client ID**, **Client Secret** and **Tenant**. Click on the **Save Configuration** button.

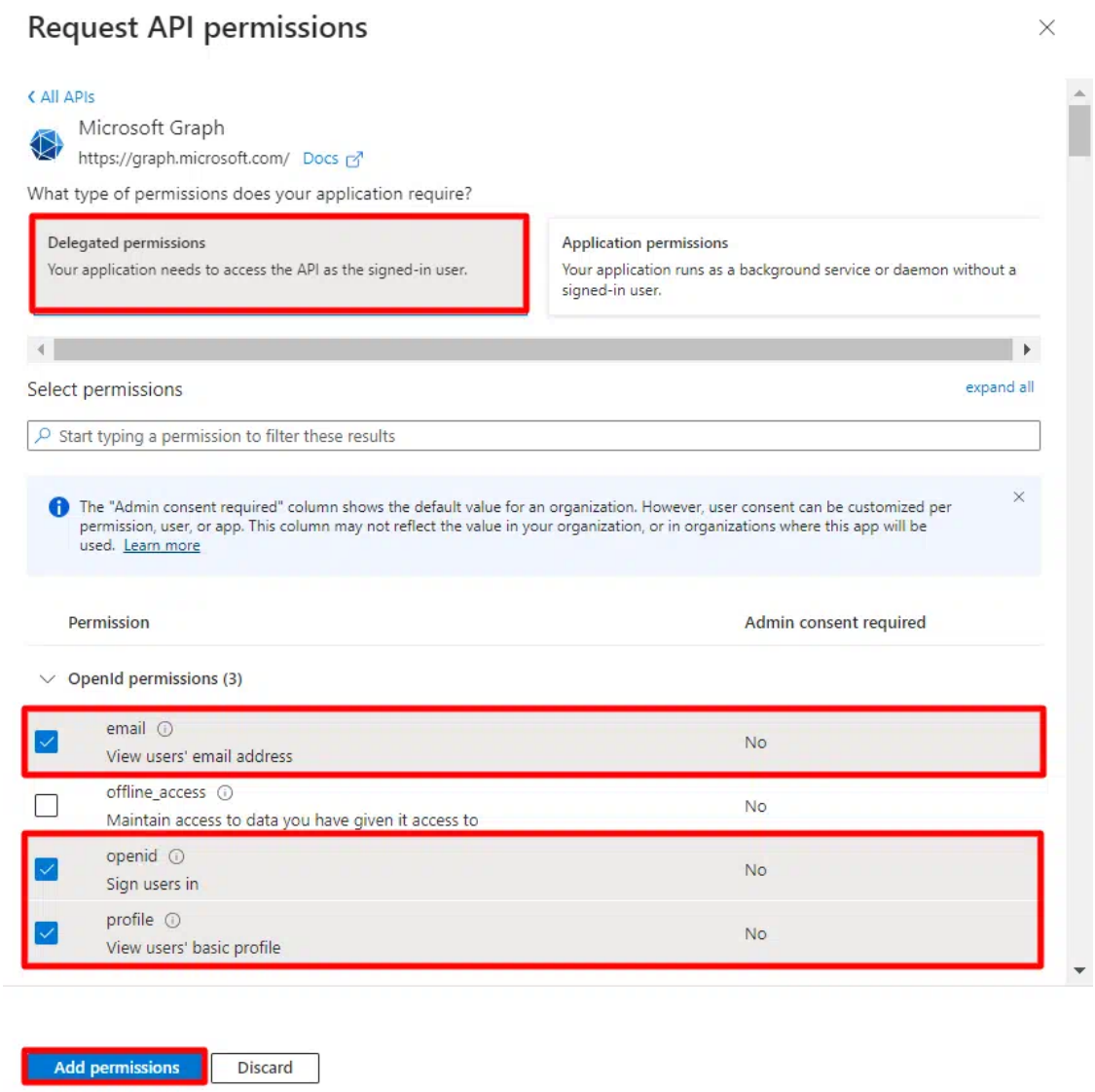


2.1. Scope & Endpoints

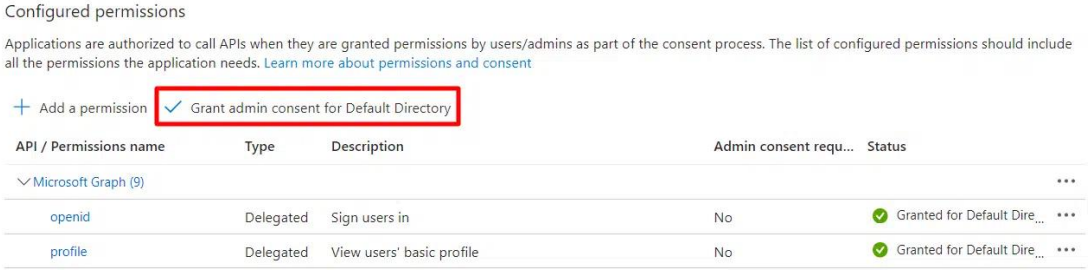
- If you want to enable scopes, you can follow the following steps:
- Go to **Application** -> Select the application where you want to enable scopes. Now, Go to the **API Permissions** tab.



- Click on the **Add permission** button, and then **Microsoft Graph API -> Delegated Permissions** and select **openid, Profile scope** and click on the **Add Permissions** button.



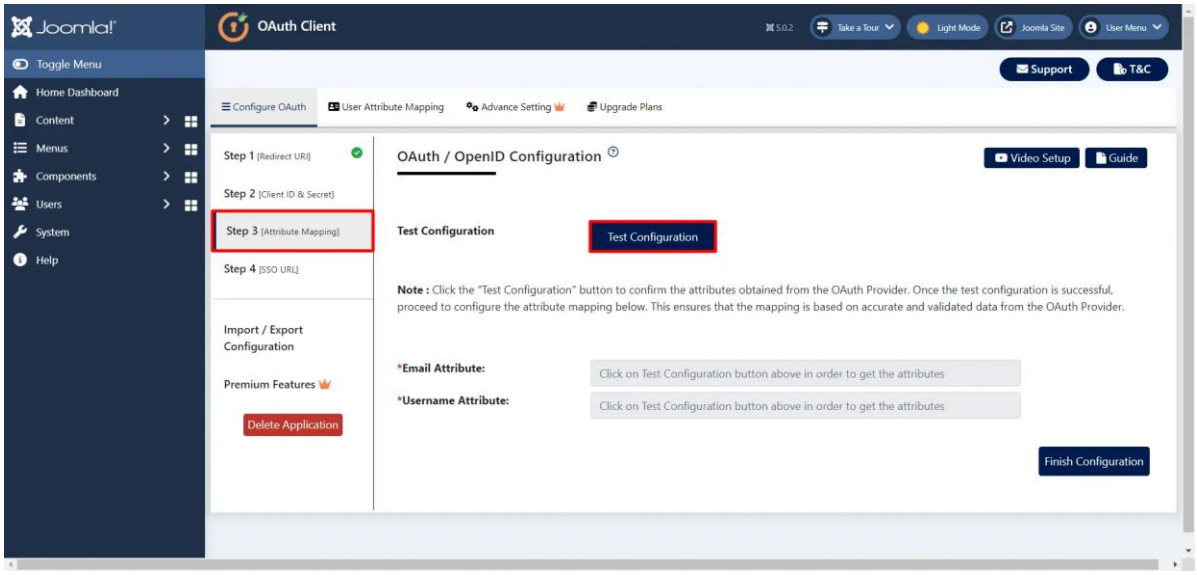
- Click on the **Grant admin consent for default directory** for Demo button.



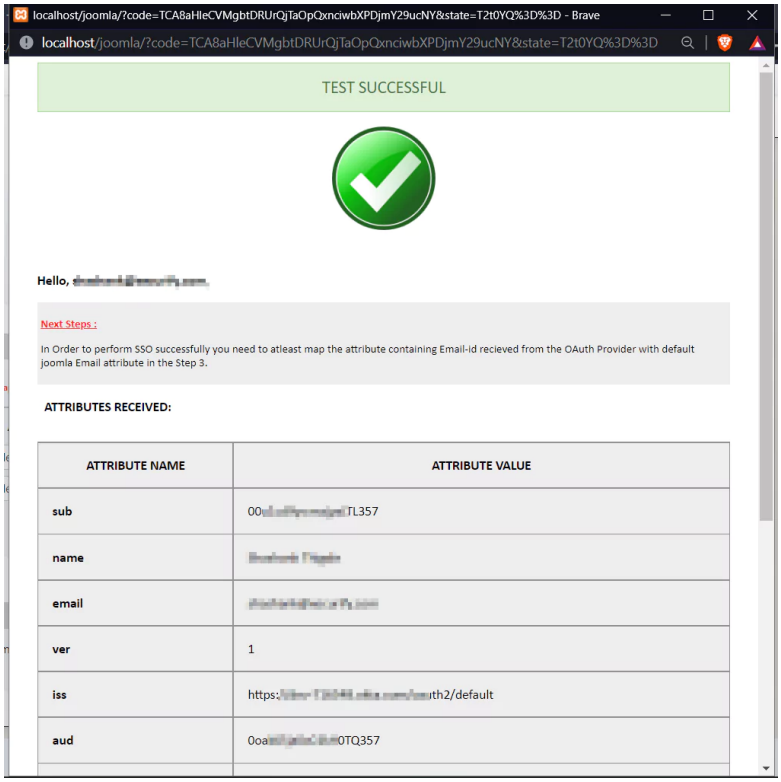
3. Configure Attribute Mapping

- User Attribute Mapping is mandatory for enabling users to successfully login into Joomla. We will be setting up user profile attributes for Joomla using below settings.

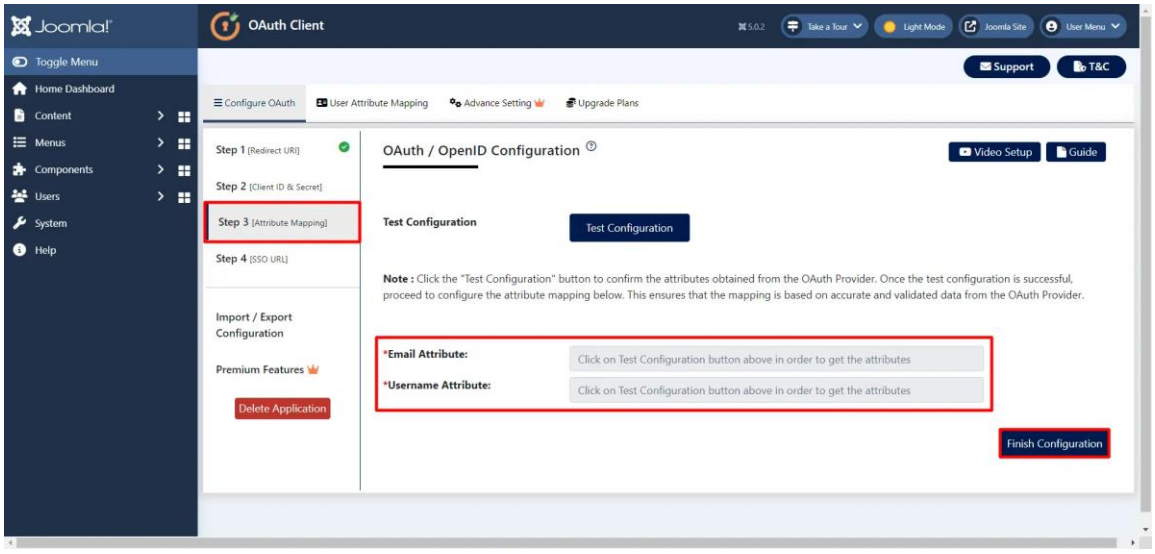
- Go to **Step 3 [Attribute Mapping]** tab and click on **Test Configuration** button.



- You will be able to see the attributes in the Test Configuration output as follows.

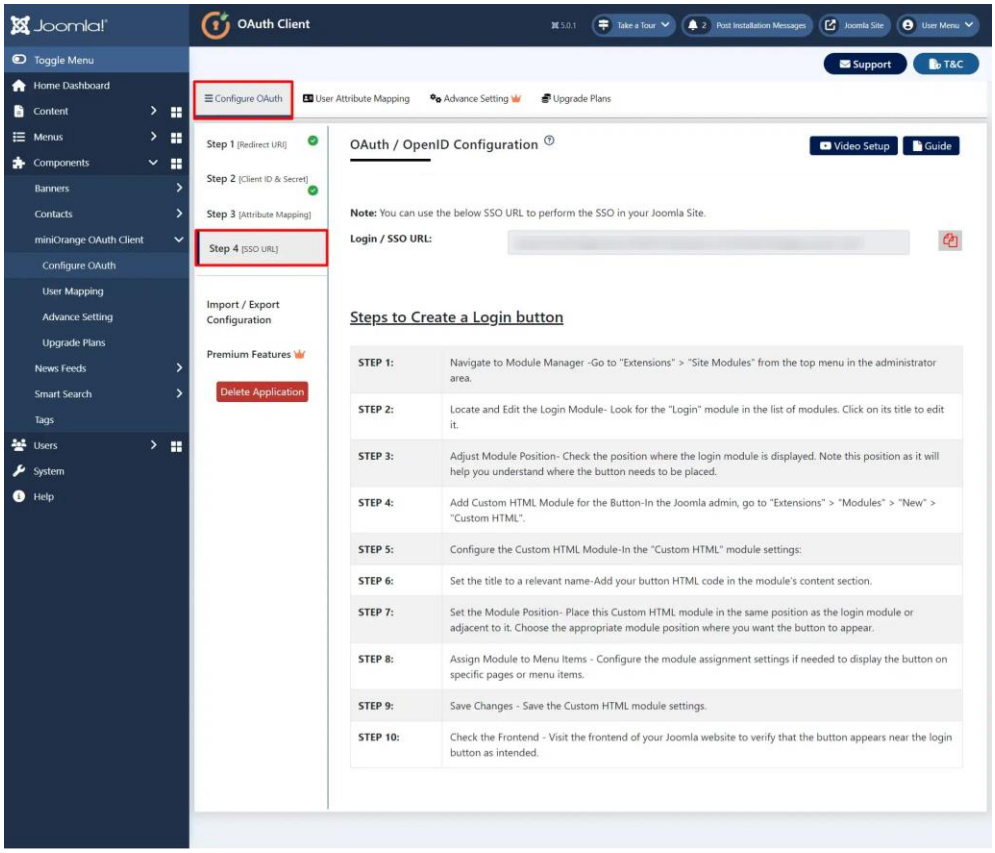


- Now go to the **Step 3 [Attribute Mapping]** tab and Select the attribute name for **Email and Username** from dropdown. Then click on **Finish Configuration** button.



4. Setup Login/SSO URL

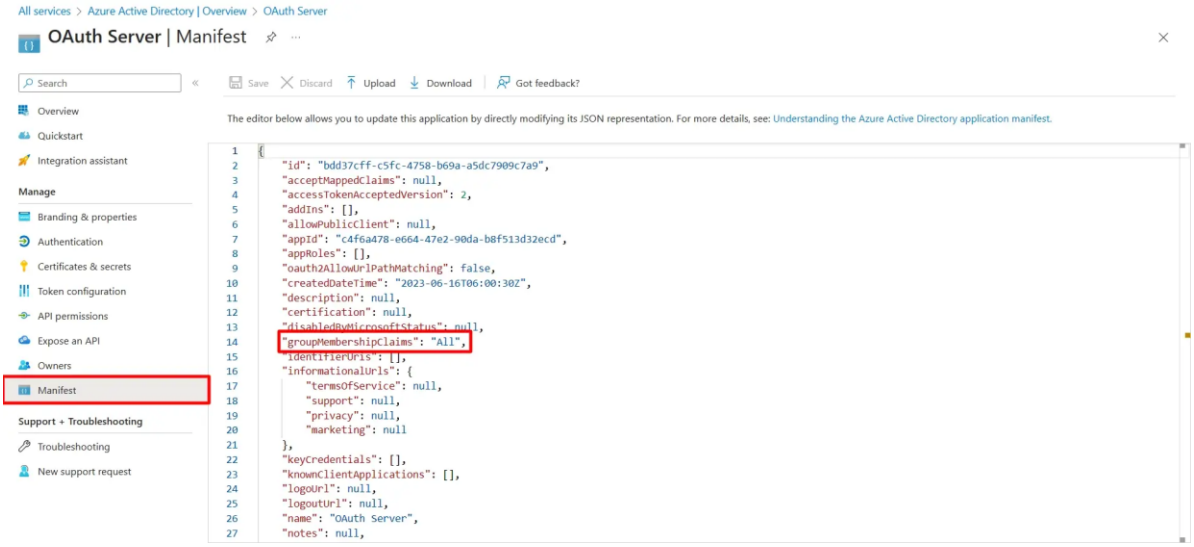
- Now go to **Step 4 [SSO URL]** tab, here copy the **Login/SSO URL** and add it to your Site by following the given steps.



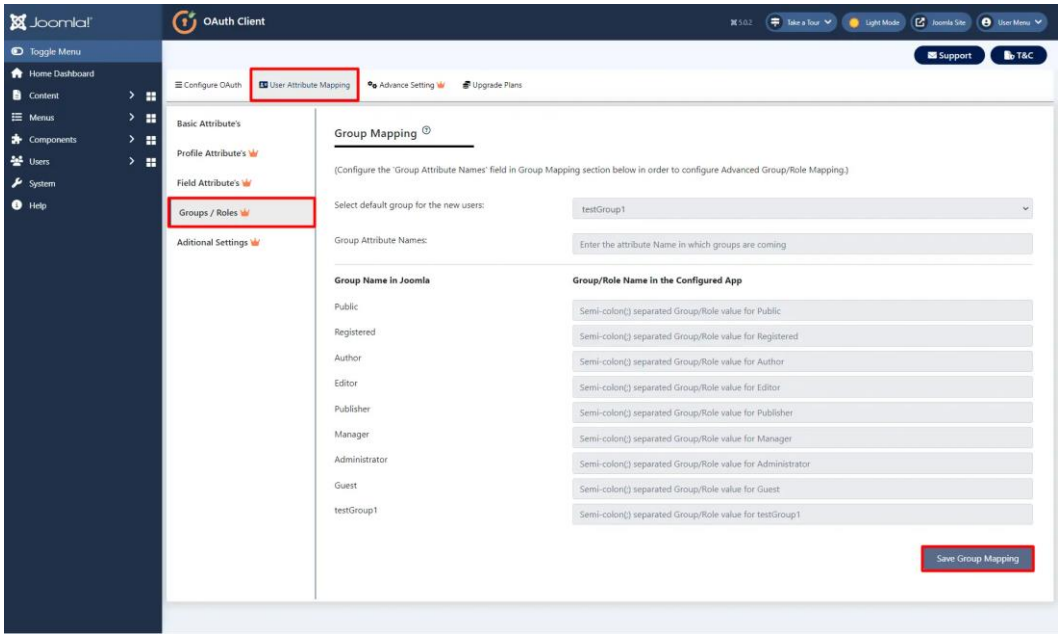
- Now logout and go to your Joomla site's pages where you have added this link. You will see a login link where you placed that button. Click on this button to perform SSO.

5. Configure Group/Role Mapping

- Go to **Manifest** tab and find **groupMembershipClaims** and changes it’s value to "All" and click on the **save** button.



- Now go to the **User Attribute Mapping** tab in **Joomla OAuth CLient plugin**, and click on **Group/Roles** tab from the left hand bar. Here, you can configure the **'Group Attribute Names'** field in order to configure Advanced Group/Role Mapping. Then click on the **Save Group Mapping** button.



In this guide, you have successfully configured Joomla Azure AD Single Sign-On (SSO) by configuring Azure AD as OAuth Provider and Joomla as OAuth Client using our Joomla OAuth Client plugin.This solution ensures that you are ready to roll out secure access to your Joomla site using Azure AD login credentials within minutes.