Azure Active Directory Registration and Configuration

Overview

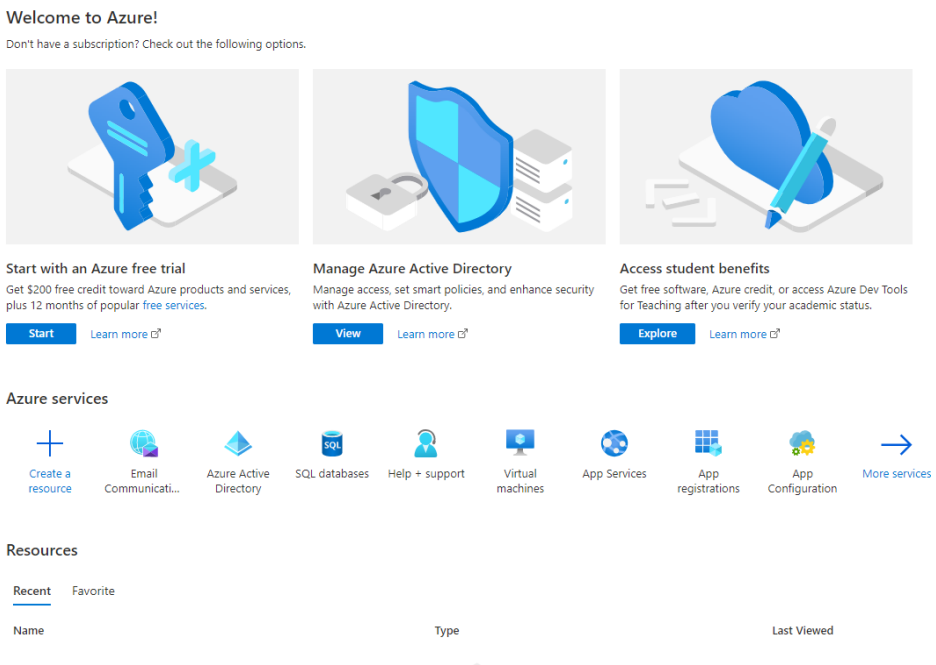
Read this guide to learn how to configure authentication for Azure App Service or Azure Functions so that your app signs in users with the Microsoft identity platform (Azure AD) as the authentication provider.

During creation of the app registration, collect the following information which you will need later when you configure Identity Service authentication in the WebUI.

- Client ID
- Tenant ID
- Client secret

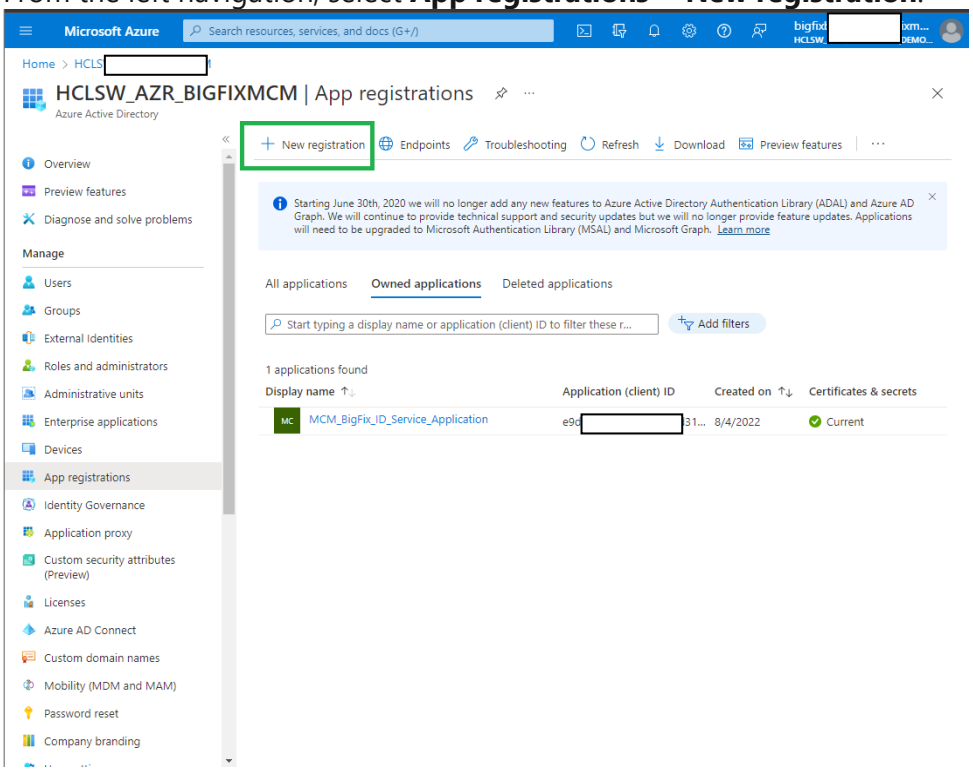
Step 1: Create an app registration in Azure AD for your App Service app

1. Sign in to the Azure portal, search for and select **App Services**, and then select your app. Note your app's **URL**. You'll use it to configure your Azure Active Directory app registration.



2. From the portal menu, select **Azure Active Directory**.

3. From the left navigation, select **App registrations** > **New registration**.

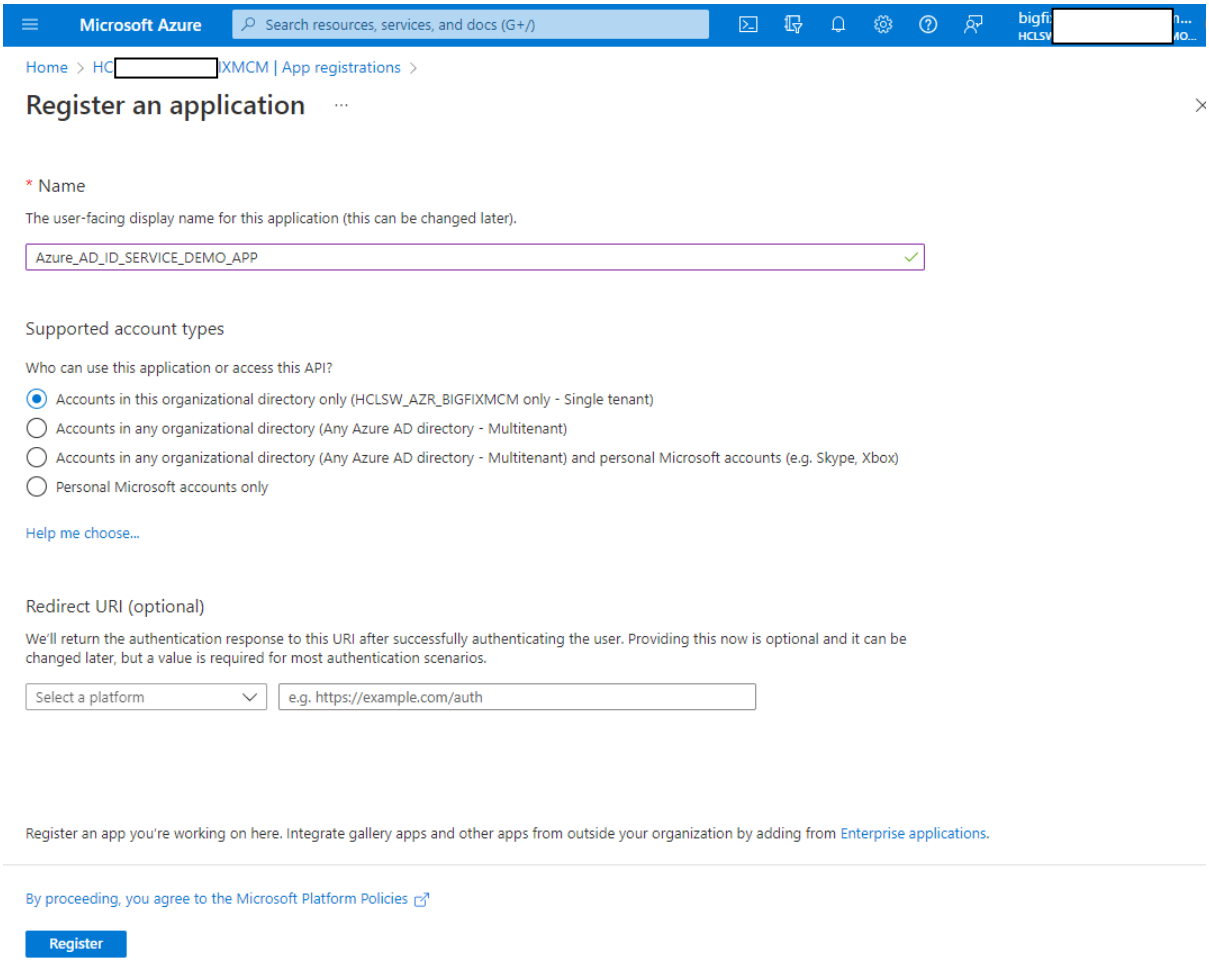


4. In the **Register an application** page, enter a **Name** for your app registration.
5. In **Supported account types**, select the account type that can access this application.
6. Select **New registration** under App registration.

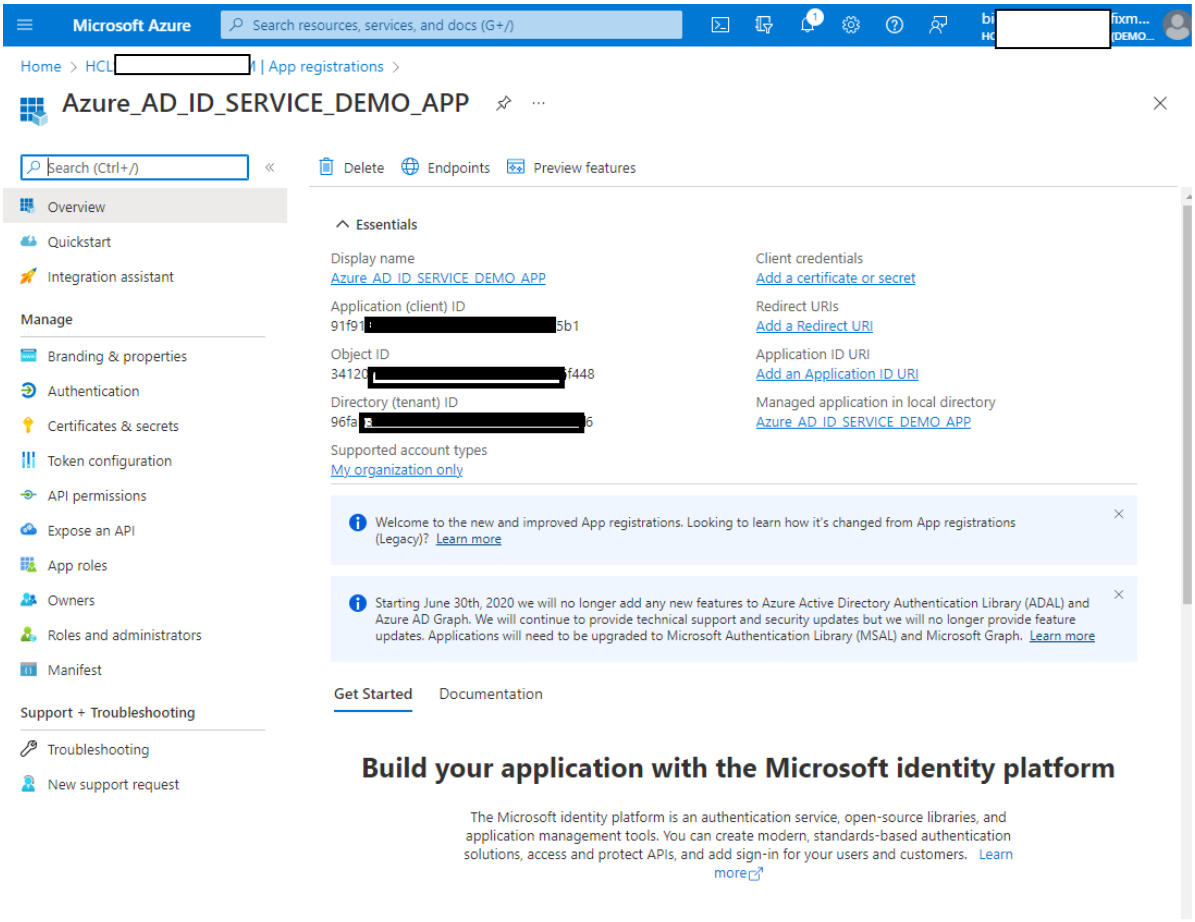
7. Set **Supported account types** as desired. The options are:

Option	Who can sign in?
Accounts in this organizational directory only	Only users in your Microsoft 365 organization
Accounts in any organizational directory	Users in any Microsoft 365 organization (work or school accounts)
Accounts in any organizational directory ... and personal Microsoft accounts	Users in any Microsoft 365 organization (work or school accounts) and personal Microsoft accounts

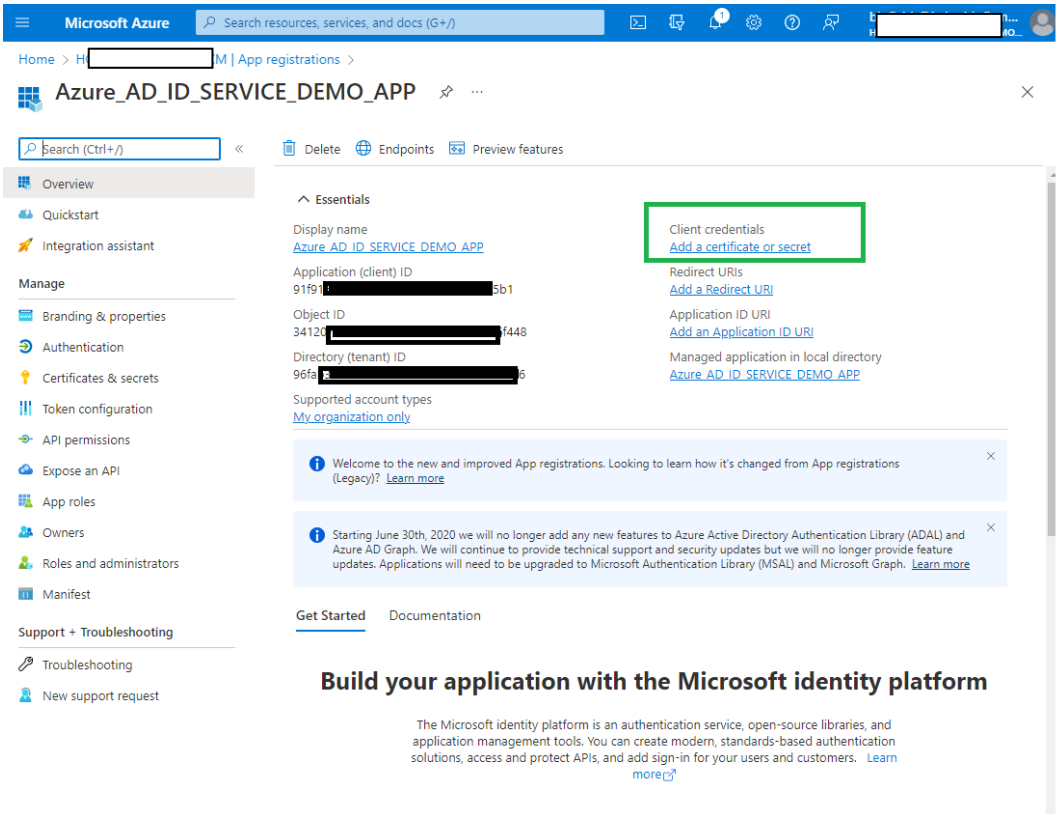
8. Redirect URI must have the information of the enrollment URL.



9. Select **Register**. On the application's **Overview** page, copy the value of the **Application (client) ID** and save it, you will need it in the next step. If you chose **Accounts in this organizational directory only** for **Supported account types**, also copy the **Directory (tenant) ID**.

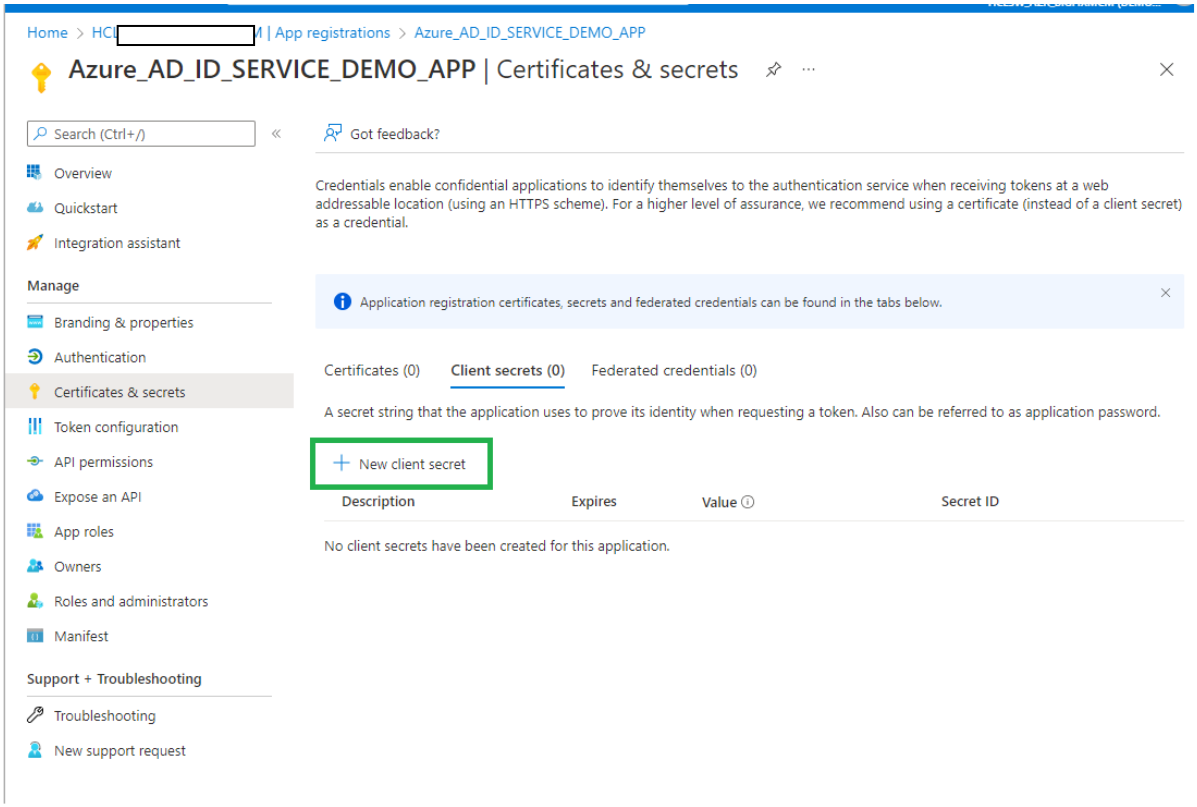


10. Click on **Client Credentials**.

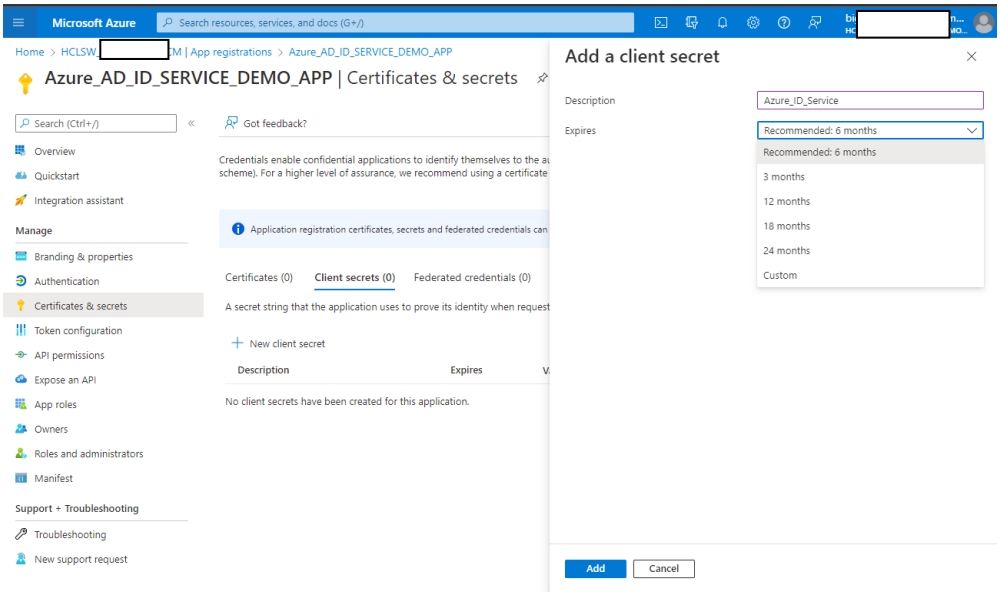


11. Generate a new client secret: To create a client secret complete the following steps:

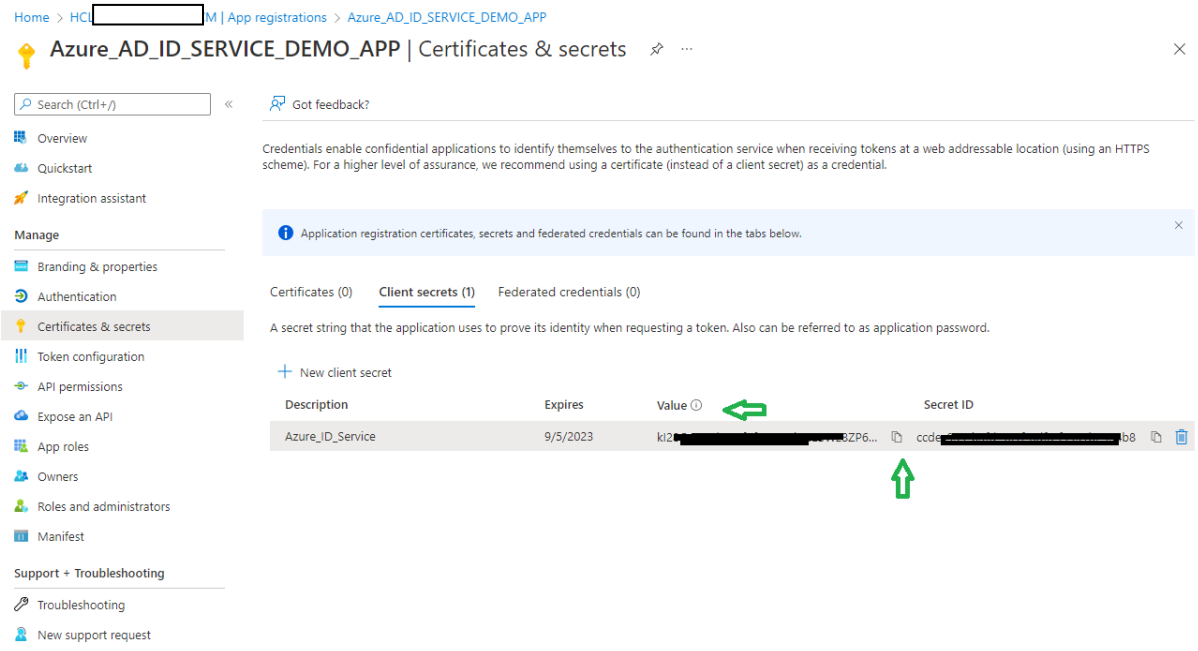
    a. From the left navigation, select **Certificates & secrets** and from the **Client secrets** tab, click **New client secret**.



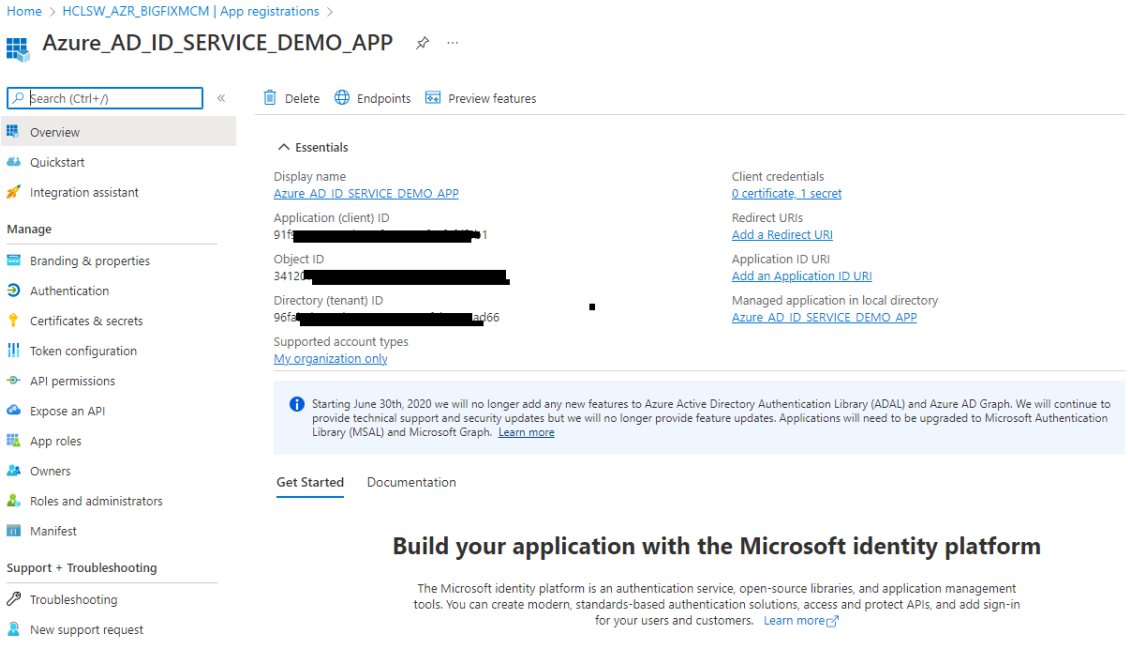
    b. Enter a description and expiration and select **Add**.



c. Copy and keep the client secret value for future use.



You can see there will be a client secret value under client credentials in overview page of application

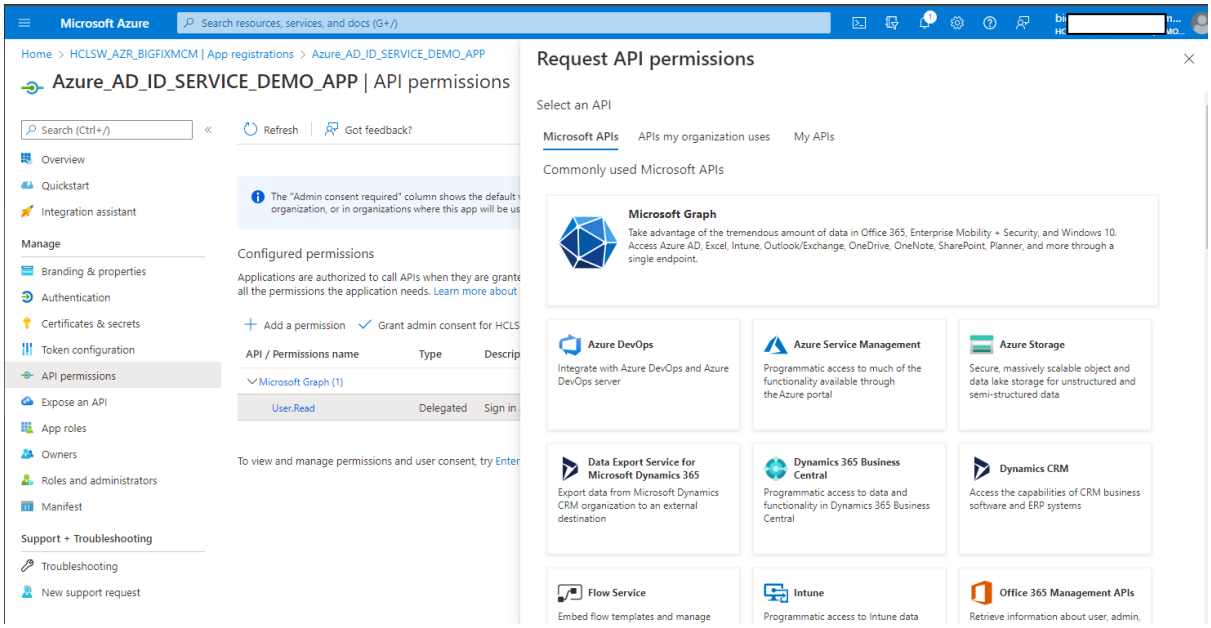


With the collected Azure AD credentials information, create a .json file in the following format to upload it to WebUI on the Manage MDM server capability page.

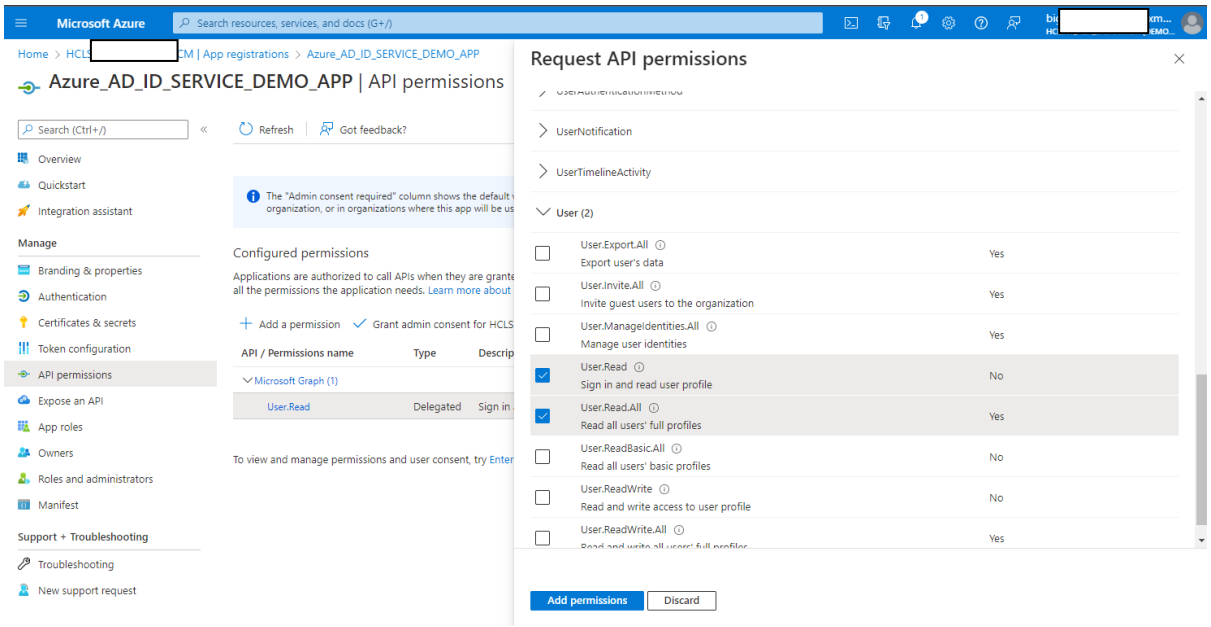
```
{ "client_id": "06b6d920-xxxx-xxxx-xxxx-73792306xxxx",
  "tenant_id": "31ac2431-xxxx-xxxx-xxxx-6215b1c2xxxx",
  "client_secret": "d7bc6b2e-xxxx-xxxx-xxxx-b5c681e5xxxx"
 }
```

Step 2: Add permissions for Microsoft graph API to fetch user and group details

1. Under the application, click on the **API permissions** section.



2. Request user and group permissions



3. Once you add permission and the same is approved by the Admin, you can view list of avaialble persmission as below.

Azure_AD_ID_SERVICE_DEMO_APP | API permissions

Search (Ctrl+/)

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Refresh | Got feedback?

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in y

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

Add a permission | Grant admin consent for HCLSW_AZR_BIGFIXMCM

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Group.Read.All	Application	Read all groups	Yes	Granted for HCLSW_AZ...
GroupMember.Read.All	Application	Read all group memberships	Yes	Granted for HCLSW_AZ...
User.Read	Delegated	Sign in and read user profile	No	Granted for HCLSW_AZ...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for HCLSW_AZ...

To view and manage permissions and user consent, try Enterprise applications.