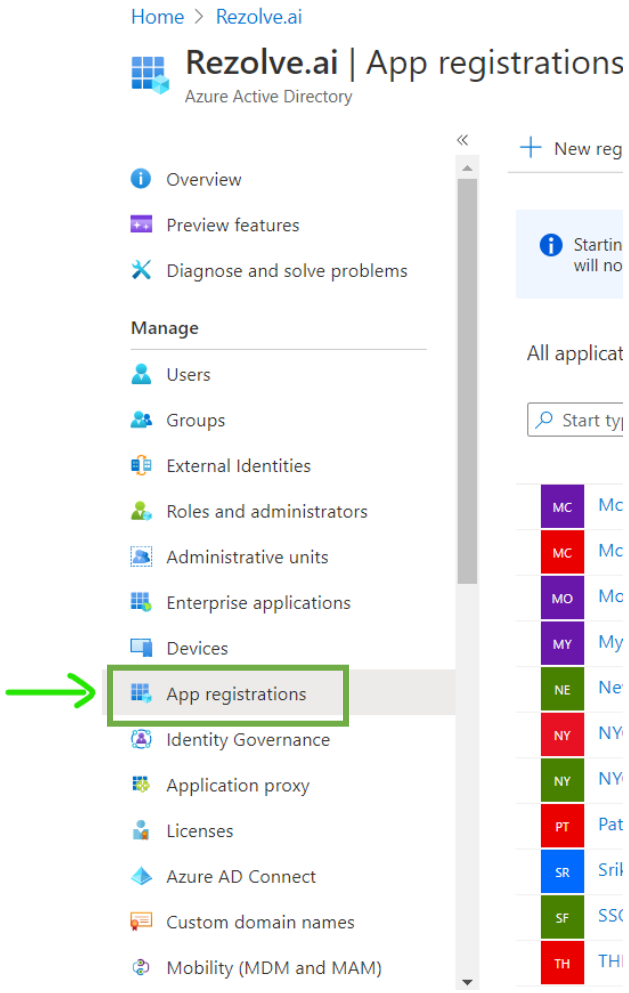
Enabling Rezolve.ai Agent in Teams App

Prerequisite

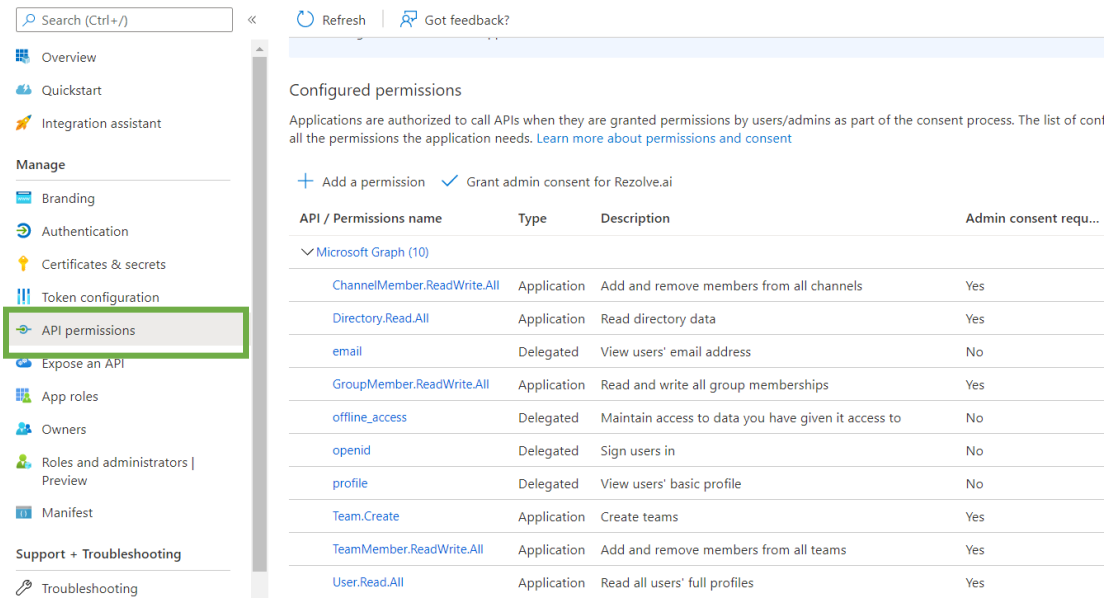
Part A: Granting API Permissions

1. Go to Azure AD Admin Portal and select *App Registration*

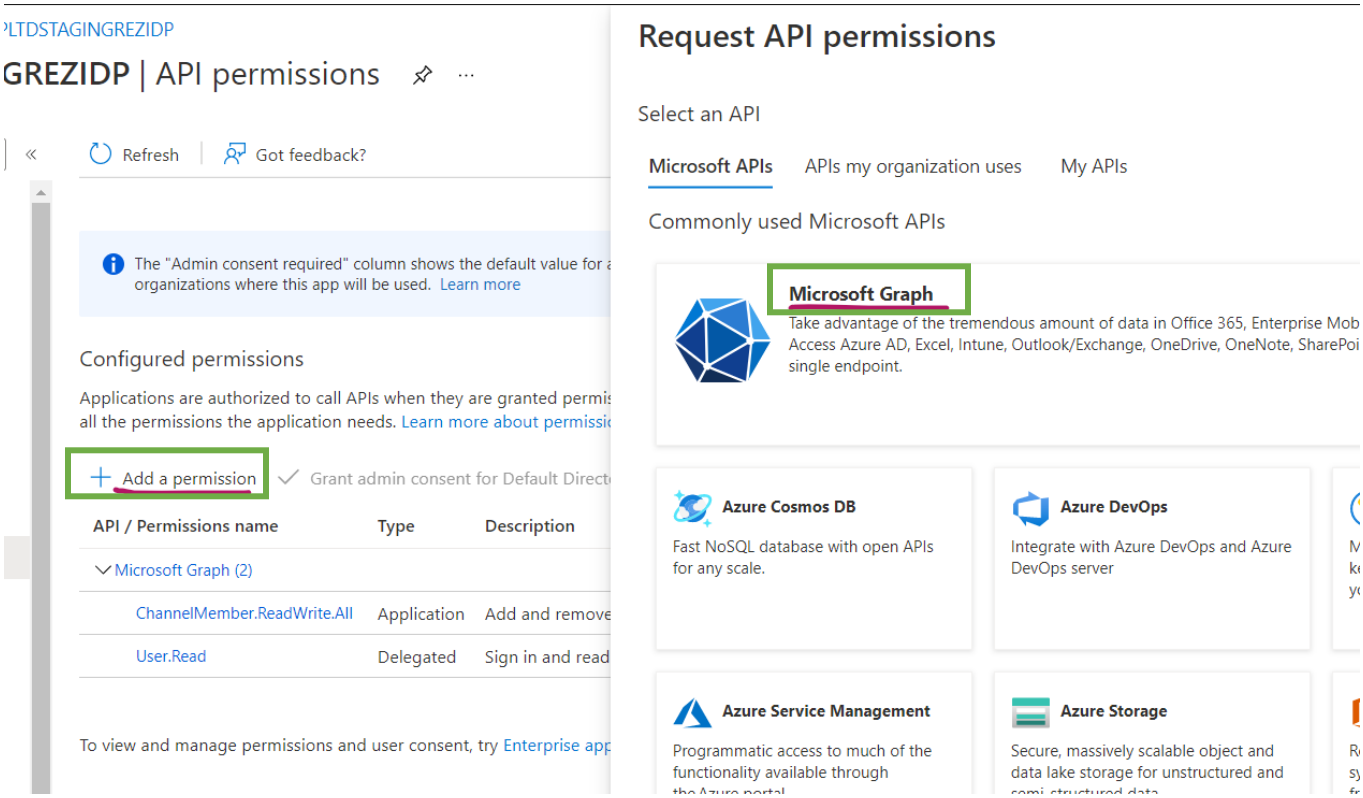


2. Select your existing Rezolve app from the list if you have one already setup. If you don't have one, create a new APP called Rezolve or the Bot name.

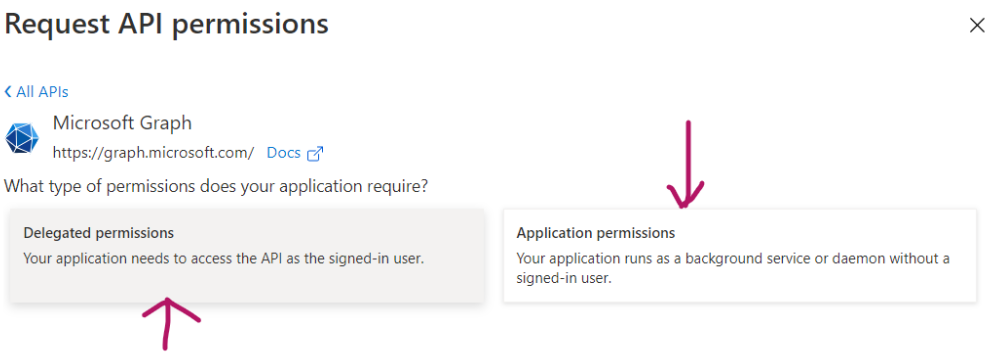
3. Once the app configuration screen opens, select *API permissions* from the menu on the left



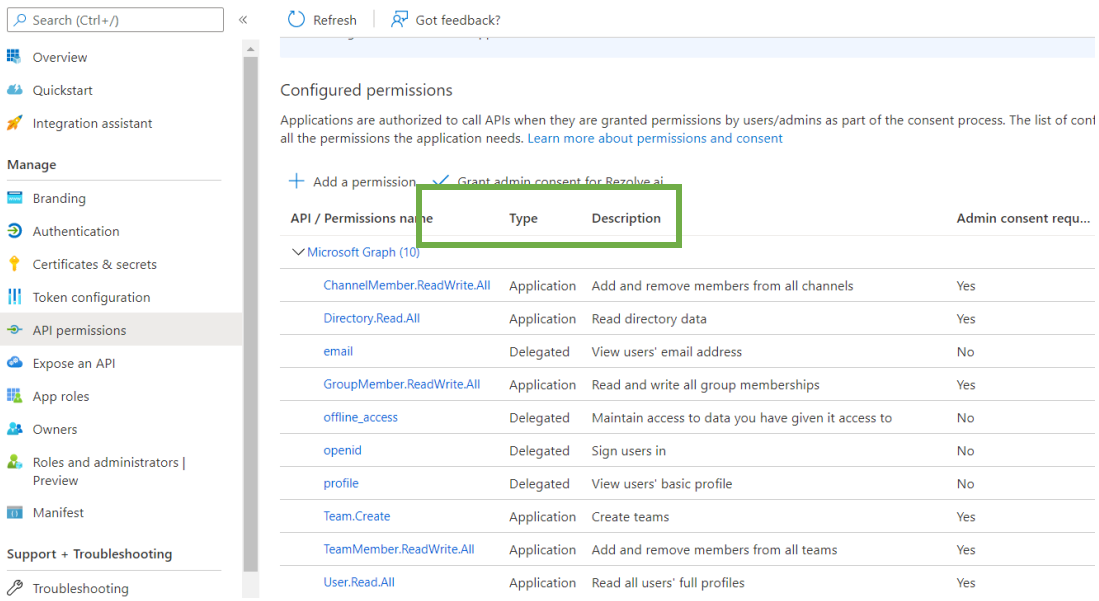
4. Click on *Add a permission* and then select *Microsoft Graph*



5. Now you will need to give the app 4 Delegate permissions and 6 Application permissions



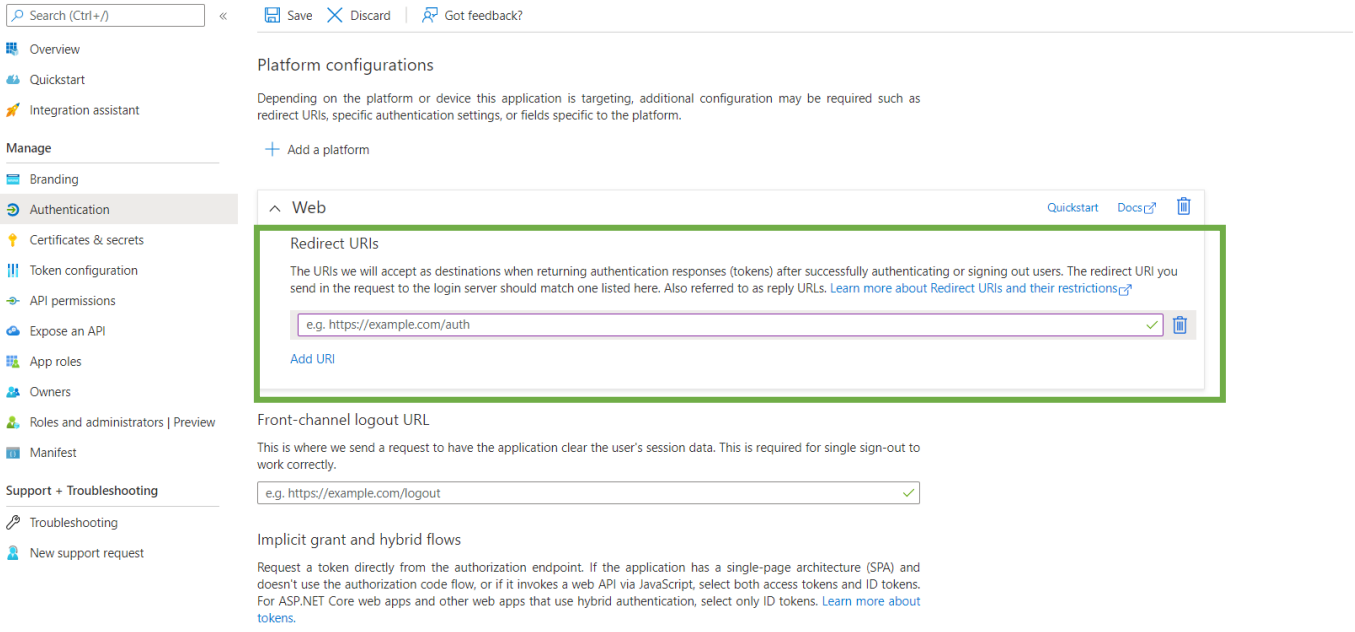
a. Select *Delegate permissions*
b. Scroll through the list, select the 4 items listed below and click Add
    - View users' email address
    - offline_access
    - openid
    - profile
c. Click *Save* (found at the top)
d. Once added, you will be taken back to the API permissions screen and will need to click *Add a permission* and then select *Microsoft Graph* again
e. This time select *Application permissions*
f. Scroll through the list, select the 6 items listed below and click Add.
    - ChannelMember. ReadWrite.All
    - Directory.Read.All
    - GroupMember.ReadWrite.All
    - Team.Create
    - TeamMember.ReadWrite.All
    - User.Read.All
g. Click *Save* (found at the top)
h. Click on the *Grant admin consent for…*



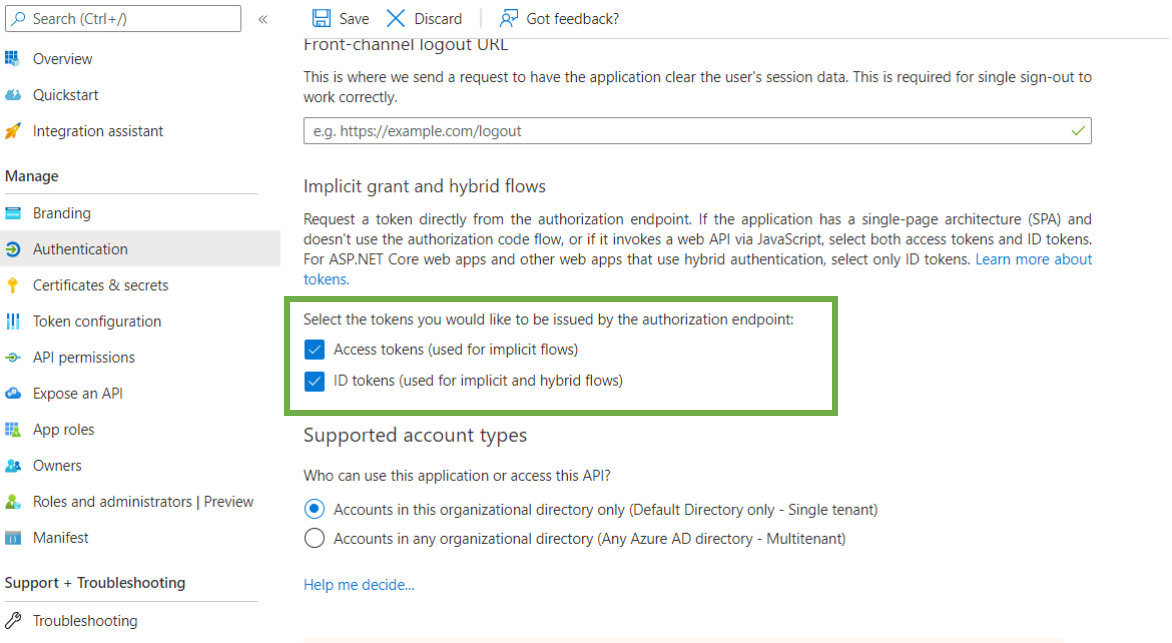
Your App Permission screen should look like this:

Part B: Configuring Authentication

1. With the app configuration screen already open, click on *Authentication* from the left-hand menu
2. On the Platform configurations page, add the 2 URLs provided by the ACS team under “Redirect URLs”



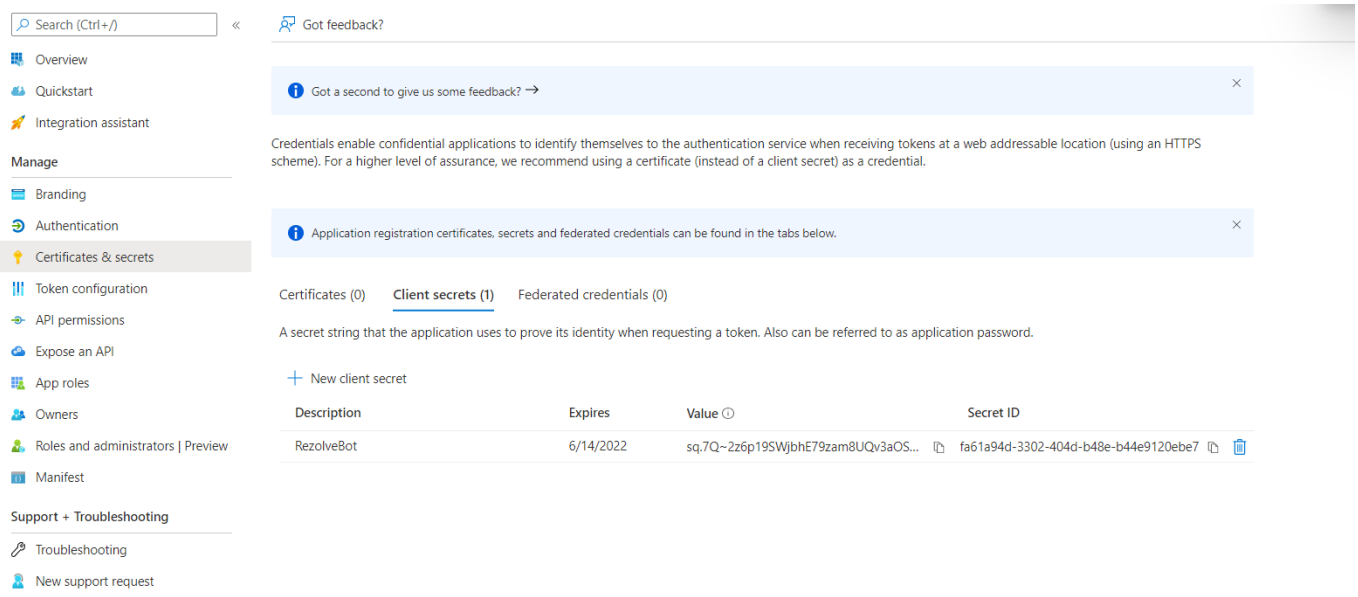
3. Check both boxes as shown under “Implicit grant and hybrid flows”



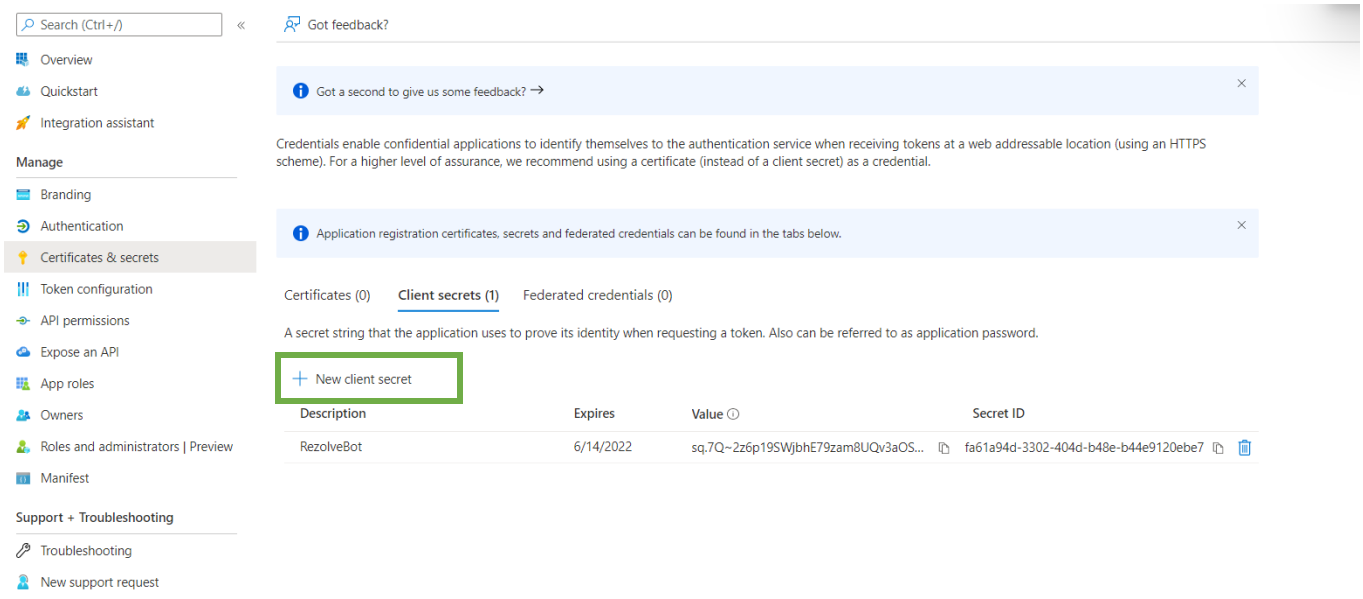
4. Click Save

Part C: Generate New Client Secret.

1. With the app configuration screen already open, select *Certificates and Secrets* from the left-hand menu

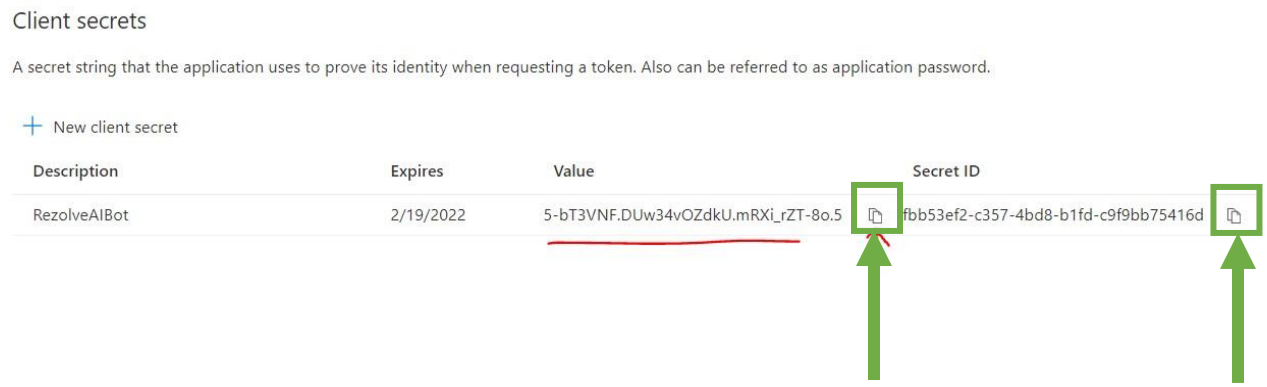


2. Click *+ New client secret*

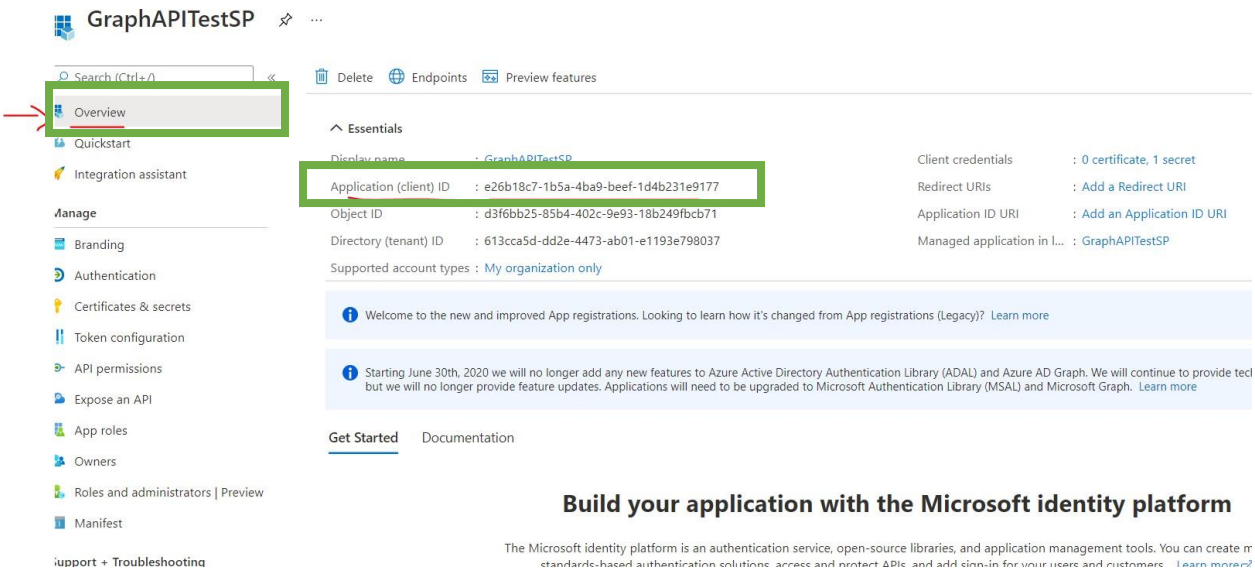


3. Enter a description i.e. *RezolveAIBot* and click Add

4. Copy the *Value* and *Secret ID,* then paste it somewhere safe



5. Select Overview in the left hand side menu
6. Copy the *Application (client) ID*



Share the Value, Client Secret and Client ID, and SAML-P sign-on endpoint (Directory (tenant) ID) with ACS.