# AZURE AD SETUP

**Context:** How to setup Azure AD in Microsoft Azure Portal to get Azure token for accessing the Microsoft Graph API. Graph API are simple API that can be accessed without any coding. You can use the user endpoint which given the user profile info for the user for which the client id and client secret is generated. This document shows step by step guide to set up application and then get azure token to access the graph Apis.

**Step 1: Register an Application in Azure AD**

1. **Log in to Azure Portal**:
   * Navigate to [Azure Portal](https://portal.azure.com/).
2. **Go to Azure Active Directory**:
   * From the left-hand menu, select **Azure Active Directory**.
3. **App Registrations**:
   * Click on **App Registrations** under the "Manage" section.
   * Click **New Registration**.
4. **Create the App**:
   * Enter a name for your application (e.g., "TestGraphAPI").
   * Set the **Supported Account Types** (e.g., "Accounts in this organizational directory only").
   * Leave the **Redirect URI** blank for now.
   * Click **Register**.
5. **Copy Important Details**:
   * After registration, note down:
     + **Application (Client) ID**
     + **Directory (Tenant) ID**

**Step 2: Add Permissions to the Application**

1. **Navigate to API Permissions**:
   * In your app's settings, go to **API Permissions** → **Add a Permission**.
2. **Select Microsoft Graph**:
   * Choose **Microsoft Graph** → Select **Delegated permissions** or **Application permissions** (depending on your use case).
3. **Choose Permissions**:
   * For basic testing, select User.Read (Delegated) or User.Read.All (Application).
4. **Grant Admin Consent**:
   * If you're using Application permissions, click **Grant Admin Consent** for your app.

**Step 3: Create a Client Secret**

1. **Go to Certificates & Secrets**:
   * In your app's settings, click **Certificates & Secrets**.
2. **Create a New Secret**:
   * Click **New Client Secret**, provide a description, and set an expiration period.
   * Click **Add** and **copy the secret value** (you won’t be able to view it again).

**Step 4: Get an Access Token**

1. **Use Postman or cURL**: You’ll use the Azure AD token endpoint to get a token: POST [https://login.microsoftonline.com/{tenant\_id}/oauth2/v2.0/token](https://login.microsoftonline.com/%7btenant_id%7d/oauth2/v2.0/token)
2. **Request Body**: Use the following parameters:

client\_id: <your-client-id>

client\_secret: <your-client-secret>

scope: https://graph.microsoft.com/.default

grant\_type: client\_credentials

**Step 5: Test Microsoft Graph API**

Choose an Endpoint: Use any Microsoft Graph API endpoint. For example: GET <https://graph.microsoft.com/v1.0/users>

**Authorization Header**: Include the token in your request header as Bearer token

That’s all. You will get the user profile info