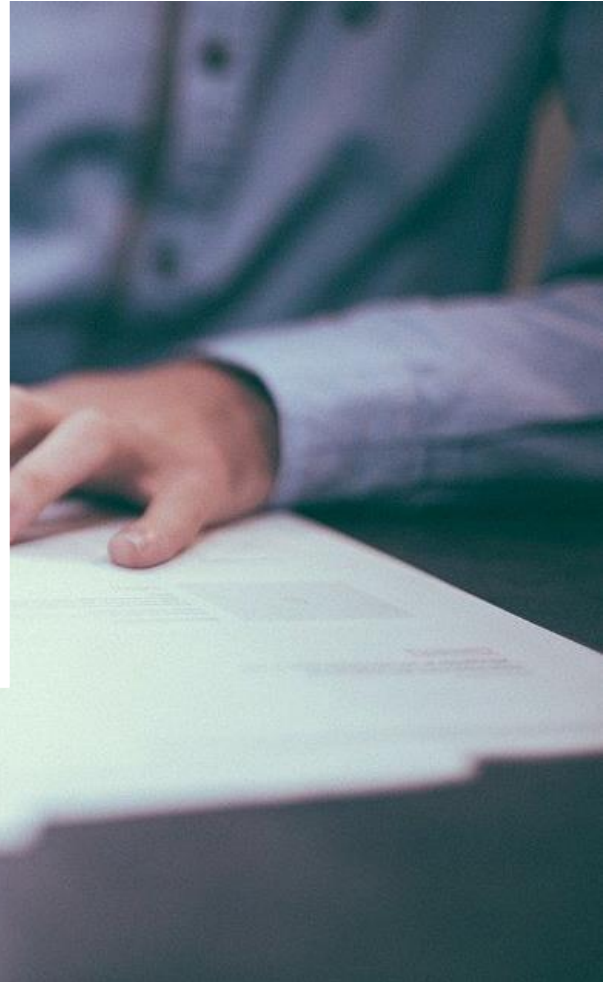


Help Center

Enterprise Service Management

Enabling Graph API Permissions

Find More- rezolve.ai/help-center



REGISTER APP IN AZURE AD

To allow the bot to perform automations for your end-user, we need to enable certain Graph API(s). We will guide you through how to do this in Azure AD.

ENABLE GRAPH API

Graph API Permissions Required for basic MS Teams automation

1. Team.ReadBasic.All
2. TeamMember.ReadWrite.All
3. Directory.Read.All

TYPE OF PERMISSIONS REQUIRED

1) Application permissions

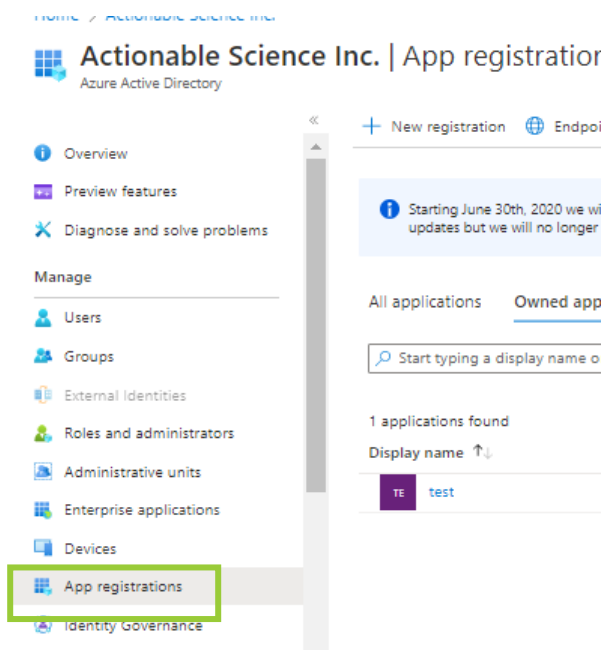
Instructions Part A

1. Open your Azure Portal
2. Click on the **View** button for *Manage Azure Active Directory*

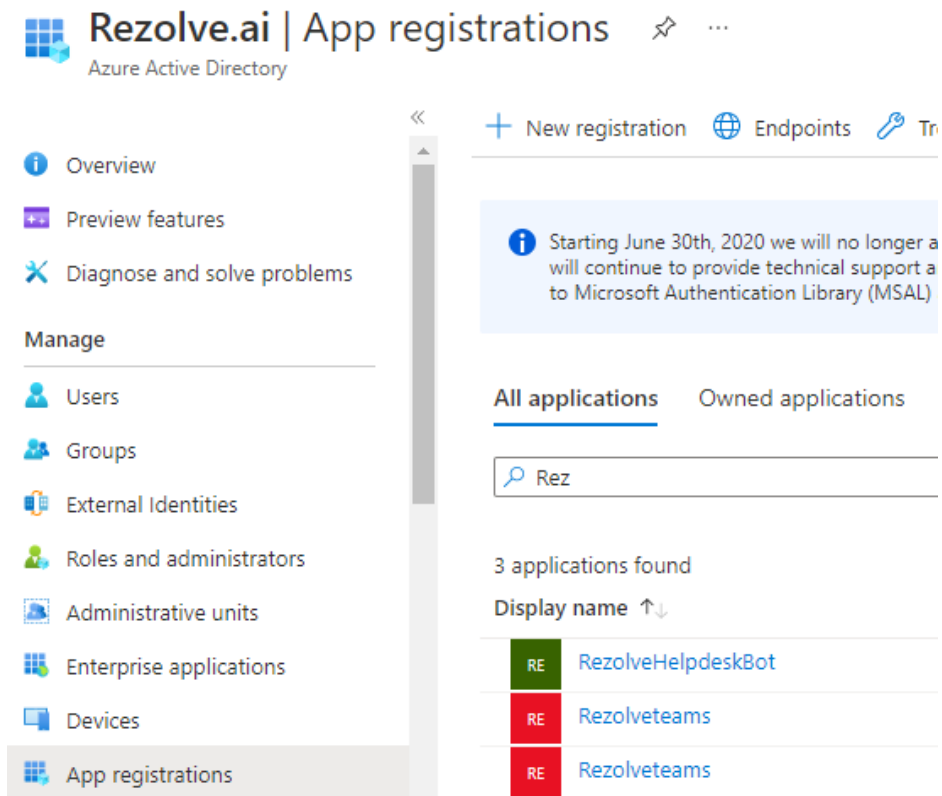
The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar with the text "Search resources, services, and docs (G+)" and several utility icons. Below the search bar, the main content area is titled "Welcome to Azure!" and includes a sub-header "Don't have a subscription? Check out the following options." There are three cards displayed:

- Start with an Azure free trial:** Includes an icon of a key and a plus sign. Text: "Get \$200 free credit toward Azure products and services, plus 12 months of popular free services." Buttons: "Start" and "Learn more".
- Manage Azure Active Directory:** Includes an icon of a shield and server racks. Text: "Manage access, set smart policies, and enhance security with Azure Active Directory." Button: "View" (highlighted with a green box) and "Learn more".
- Access student benefits:** Includes an icon of a blue graduation cap and a pencil. Text: "Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status." Buttons: "Explore" and "Learn more".

3. Click on **App Registration**



4. Search and Open the Rezolve SSO application you created



- The App Overview page will open, look for **Api Permissions** in the left hand side menu and click on it
- Select **Add a Permission** on the main part of the page

RezoiveHelpdeskBot | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API

The "Admin consent required" column shows that the application requires admin consent. This column may not reflect the actual permissions of the application.

Configured permissions

Applications are authorized to call APIs when permissions should include all the permissions listed below.

+ Add a permission Grant admin consent

API / Permissions name	Type
Microsoft Graph (2)	
Sites.Manage.All	Application

- Select **Microsoft Graph**

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

8. Click on **Application Permission** option

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

9. Type *Team* in the search box, select *Team.ReadBasic.All* and click **Add Permissions**

Select permissions

team.

Permission

> TeamsAppInstallation

> TeamsTab

✓ Team (1)

Team.Create ⓘ
Create teams

Team.ReadBasic.All ⓘ
Get a list of all teams

Add permissions

Discard



- Click **Add a Permission > Microsoft Graph > Application permissions** again
- Type *Team* in the search box, this time select *TeamMember.ReadWrite.All* and click **Add Permissions**

Select permissions

Permission

TeamMember (1)

- TeamMember.Read.All ⓘ
Read the members of all teams
- TeamMember.ReadWrite.All ⓘ
Add and remove members from all teams
- TeamMember.ReadWriteNonOwnerRole.All
Add and remove members with non-owner



- Click **Add a Permission > Microsoft Graph > Application permissions** again
- Type *direct* in the search box, this time select *Directory.Read.All* and click **Add Permissions**

Select permissions

Permission

Directory (1)

- Directory.Read.All ⓘ
Read directory data
- Directory.ReadWrite.All ⓘ
Read and write directory data

> RoleManagement



- Close the *Request API Permissions* box so you are back at the *Configure permissions* screen
- Select **Grant admin consent for ...**

+ Add a permission Grant admin consent for Resolve.ai

API / Permissions name	Type	Description
Microsoft Graph (2)		
Sites.Manage.All	Application	Create, edit, and delete items and lists in all site collections
Sites.ReadWrite.All	Application	Read and write items in all site collections

16. Click **Yes** to Grant admin consent confirmation

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Rezolve.ai? This will update any existing admin consent records this application already has to match what is listed below.

15. Confirm that the screen looks similar to below with your listed permissions, Admin Consent Req set to Yes and Granted for has a green check

+ Add a permission ✓ Grant admin consent for Rezolve.ai

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (2) ***				
Sites.Manage.All	Application	Create, edit, and delete items and lists in all site collections	Yes	<input checked="" type="checkbox"/> Granted for Rezolve.ai ***
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	<input checked="" type="checkbox"/> Granted for Rezolve.ai ***

Instructions Part B

1. Look for **Certificates & secrets** in the left hand side menu and select it
2. Then select **New client secret** on the main part of the page

RezolveHelpdeskBot | Certificates & secrets

Search (Ctrl+/) << Got feedback?

Overview
Quickstart
Integration assistant

Manage

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

Credentials enable confidential applications to identify themselves to the authenticator (instead of using a username and password). For a higher level of assurance, we recommend using a certificate (instead of a secret string).

Application registration certificates, secrets and federated credentials can be found in the **Application registration** blade.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token.

+ New client secret

Description	Expires	Value
No client secrets have been created for this application.		

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

Add a client secret

Description

Expires

5. Copy the *Value* and *Secret ID* and save them somewhere

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
ResolveBot	2/2/2023	wBC8Q~qnf9pitH.RkUqZV~1DB...	fe0fdc78-1fb3-4e47-9067-1304...

6. Select **Overview** in the left hand side menu

Copy the *Application (client) ID* and save with Client Secret ID

ResolveHelpdeskBot

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

^ Essentials

Display name
ResolveHelodeskBot

Application (client) ID
fed26789-73b3-4752-8007-5217eae47e65

Object ID
349c3a5b-52cf-4270-9d33-a5861e4e8533

Directory (tenant) ID
3304b368-9baa-47ee-9b9e-0be7ecab9a53

Supported account types
[My organization only](#)

Starting June 30th, 2020 we will no longer add any new features to Azur provide technical support and security updates but we will no longer pr Library (MSAL) and Microsoft Graph. [Learn more](#)

[Get Started](#) [Documentation](#)

8. Select **Manifest** in the left hand side menu
9. Click on **Download**

The screenshot shows the Azure portal interface for configuring an application manifest. The left-hand navigation pane is open to the 'Manifest' section. The main area displays a code editor with the application manifest JSON. The 'Download' button in the top right toolbar is highlighted with a green box. The manifest JSON includes the following details:

```

1  {
2    "id": "349c3a5b-52cf-4270-9d33-a58",
3    "acceptMappedClaims": null,
4    "accessTokenAcceptedVersion": null,
5    "addIns": [],
6    "allowPublicClient": false,
7    "appId": "fed26789-73b3-4752-8007-",
8    "appRoles": [
9      {
10       "allowedMemberTypes": [
11         "User"
12       ],
13       "description": "User",
14       "displayName": "User",
15       "id": "18d14569-c3bd-439b-",
16       "isEnabled": true,
17       "lang": null,
18       "origin": "Application",
19       "value": null
20     }
21   ],
22   "allowedMemberTypes": [
23     "User"
  
```

10. Send the *Application (client) ID*, *Client Secret ID* and the downloaded *Manifest* to Rezolve