

# Help Center

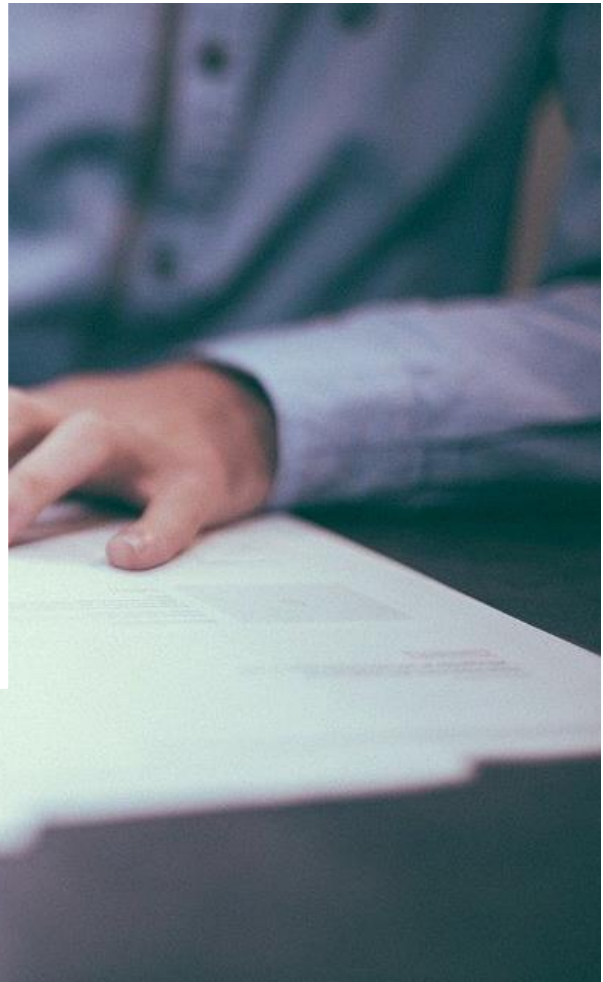
Enterprise Service Management

---

## Enabling Graph API Permissions for SharePoint List

---

Find More- [rezolve.ai/help-center](https://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. Sites.Manage.All
2. Sites.ReadWrite.All

## TYPE OF PERMISSIONS REQUIRED

### 1) Application permissions

#### Instructions Part A

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

### Welcome to Azure!

Don't have a subscription? Check out the following options.



#### Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular free services.

[Start](#)

[Learn more](#)



#### Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

[View](#)

[Learn more](#)



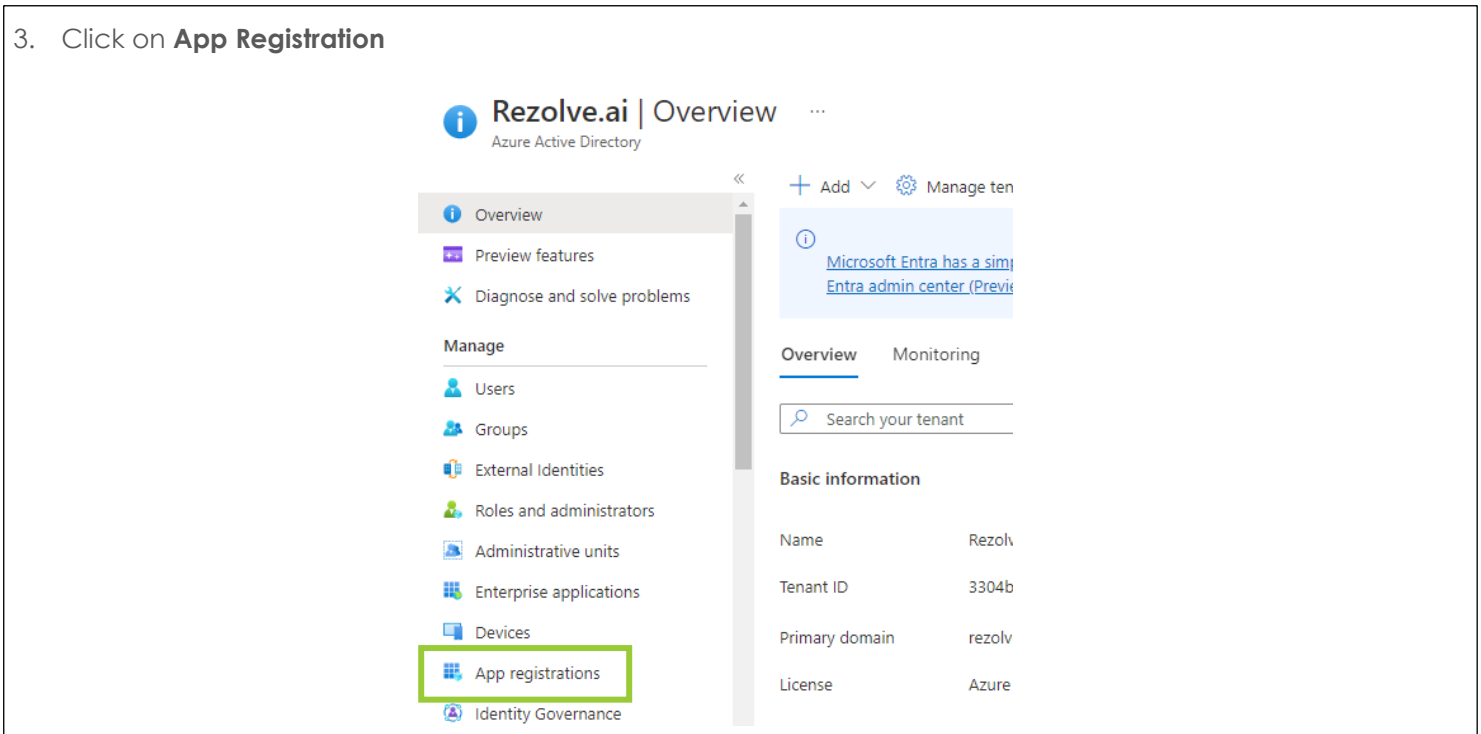
#### Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

[Explore](#)

[Learn more](#)

3. Click on **App Registration**



**Rezolve.ai | Overview**  
Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems
- Manage**
  - Users
  - Groups
  - External Identities
  - Roles and administrators
  - Administrative units
  - Enterprise applications
  - Devices
  - App registrations**
  - Identity Governance

Microsoft Entra has a similar admin center (Previous version)

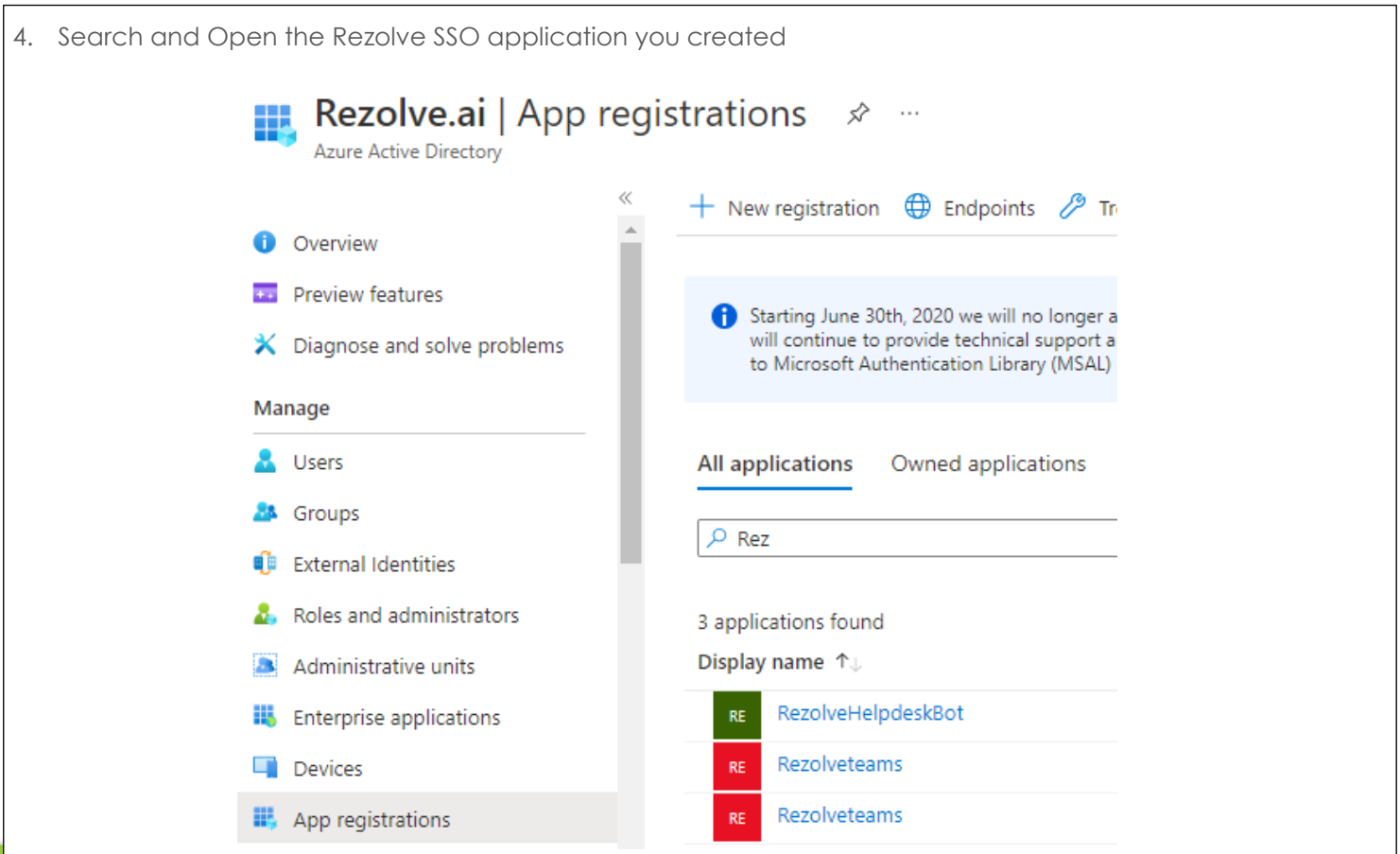
Overview Monitoring

Search your tenant

**Basic information**

Name	Rezolv
Tenant ID	3304b
Primary domain	rezolv
License	Azure

4. Search and Open the Rezolve SSO application you created



**Rezolve.ai | App registrations**  
Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems
- Manage**
  - Users
  - Groups
  - External Identities
  - Roles and administrators
  - Administrative units
  - Enterprise applications
  - Devices
  - App registrations**

New registration Endpoints Tr

Starting June 30th, 2020 we will no longer be able to provide technical support for applications that use the Microsoft Authentication Library (MSAL)

All applications Owned applications

Rez

3 applications found

Display name ↑↓

RE	RezolveHelpdeskBot
RE	RezolveTeams
RE	RezolveTeams

- 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

RezoHelpdeskBot | 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 should be set to true for this app. This column may not reflect the value for all permissions.

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 *sites* in the search box, select *Sites.Manage.All* and click **Add Permissions**

10. Click **Add a Permission > Microsoft Graph > Application permissions** again

11. Type *sites* in the search box, this time select *Sites.ReadWrite.All* and click **Add Permissions**

Here is an example:

Select permissions

Permission

▼ Sites (1)

- Sites.FullControl.All ⓘ  
 Have full control of all site collections
- Sites.Manage.All ⓘ  
 Create, edit, and delete items and lists in all site collections
- Sites.Read.All ⓘ  
 Read items in all site collections
- Sites.ReadWrite.All ⓘ  
 Read and write items in all site collections
- Sites.Selected ⓘ  
 Access selected site collections

Add permissions

Discard

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

10.

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

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

- 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 Resolve.ai? This will update any existing admin consent records this application already has to match what is listed below.

- 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 Resolve.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	✓ Granted for Resolve.ai ...
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	✓ Granted for Resolve.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

ResolveHelpdeskBot | 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 authenticating authority. For a higher level of assurance, we recommend using a certificate (instead of a client secret).

Application registration certificates, secrets and federated credentials can be found in the [Application Registration](#) page.

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

ResolveAIBot

Expires

Recommended: 6 months

Add

Cancel



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

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

**ResolveHelpdeskBot** ✨ ...

Search (Ctrl+/) << 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  
[ResolveHelpdeskBot](#)

**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 Azure AD. We will continue to provide technical support and security updates but we will no longer provide new features to the Azure AD Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

8. Select **Manifest** in the left hand side menu

9. Click on **Download**

RezolveHelpdeskBot | Manifest

Search (Ctrl+/) Save Discard Upload Download

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

The editor below allows you to update this application by application manifest.

```

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