Ing. Walter Espejo

INVENTORY

User guide

29-11-2022

INVENTORY MICROSOFT 365

TABLE OF CONTENTS

1. INTRODUCTION

The Microsoft 365 Inventory collects data about users, groups, and licenses. In this document we describe the necessary steps to map information of your Microsoft 365 environment in Docusnap.

2. PREPARING MICROSOFT AZURE

The following chapters describe how to prepare the Microsoft Azure environment for inventorying Microsoft 365. Alternatively, a **PowerShell script can be used for setup** (this script can be downloaded from our website), as described in Chapter 3.

Before you begin, make sure that your used Azure user is authorized as a Global Administrator.

2.1 CREATING THE NEW AZURE APPLICATION

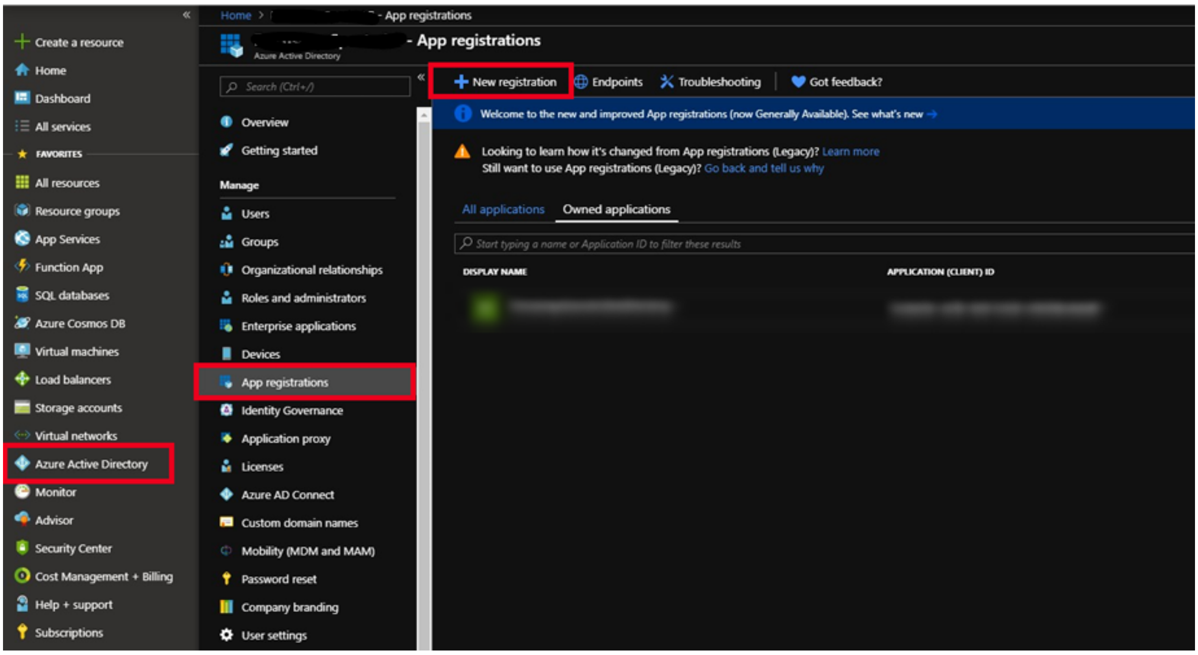
The Microsoft 365 Inventory requires mandatory a registered application, that is authorized to read and access the Microsoft 365 information. In this chapter, we describe how to create this application.

For example, the application is called **CUSTOMER_MS_365**. The name is freely selectable.

APP REGISTRATION

Create / register the app as follows:

- Select the Azure Active Directory in the resource overview or the search.
- In the Manage area, select App registrations.
- Click on the menu item New registration



Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

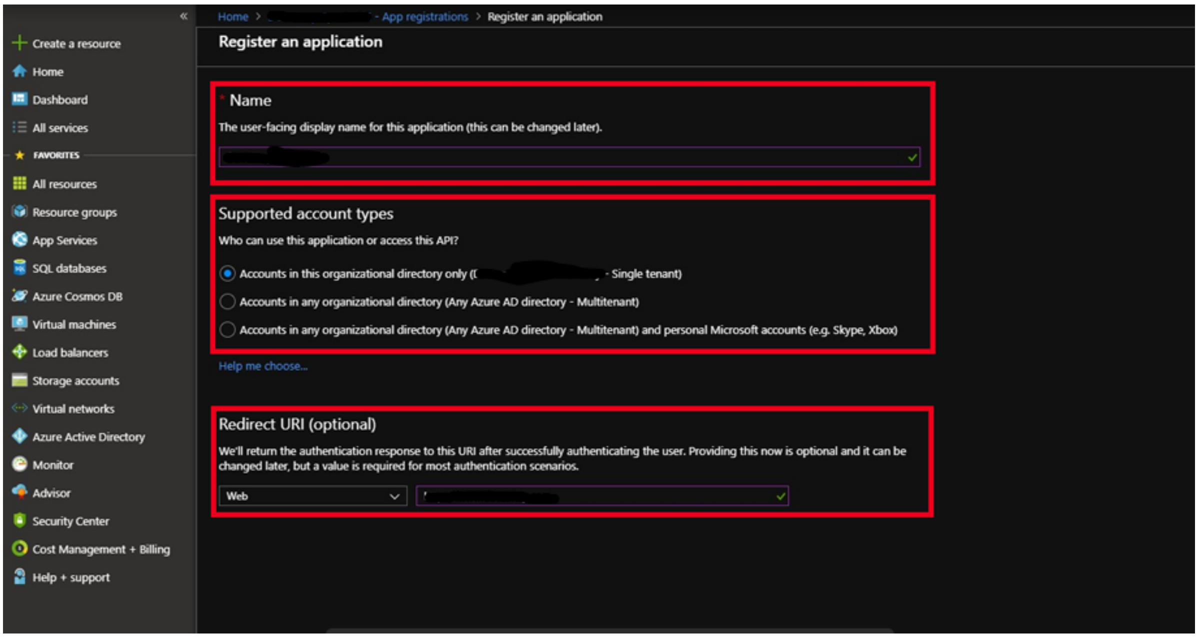
[redacted]

REGISTER THE APPLICATION

The following information is required to register the application:

- **Name:** Enter the application name **CUSTOMER_MS_365**.

- **Supported account types:** Here you can select who can use the application - select **Accounts in this organizational directory only**



Register an application

* Name

The user-facing display name for this application (this can be changed later).

[redacted] ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only ([redacted] - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

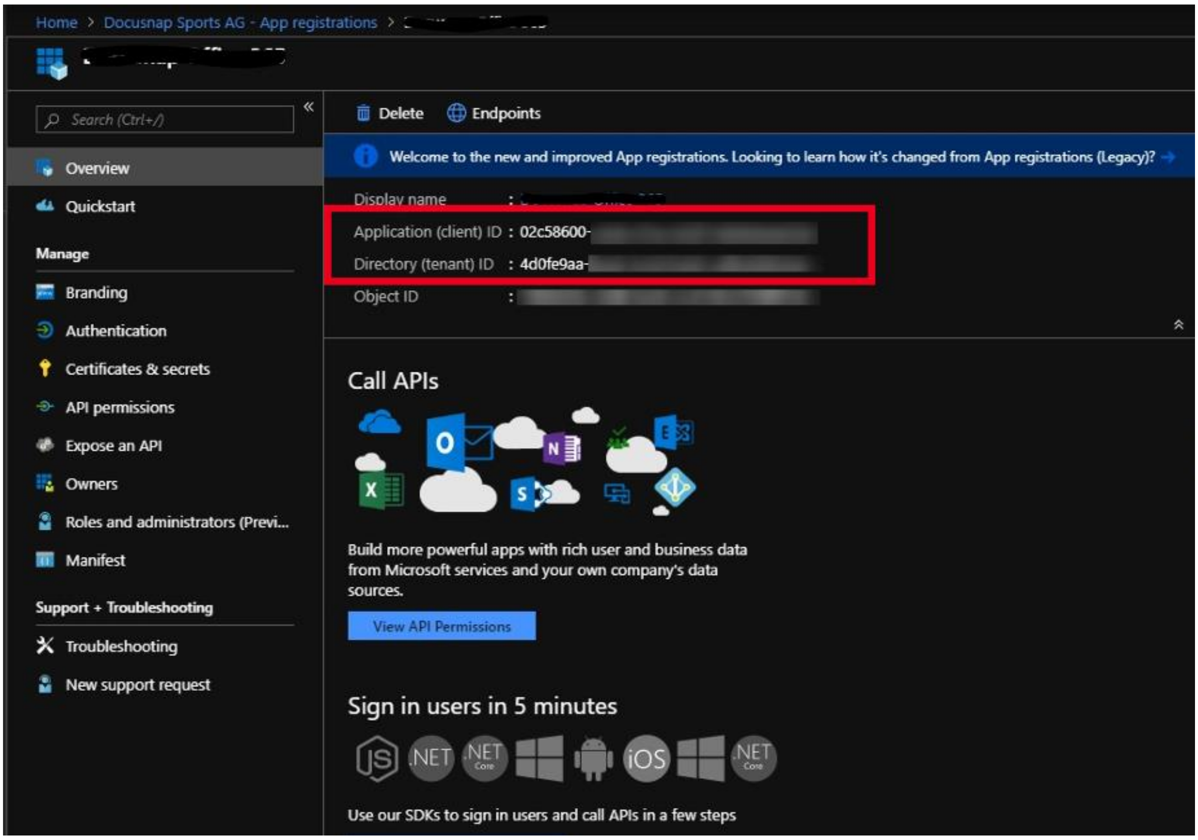
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | [redacted] ✓

DETERMINE APPLICATION AND DIRECTORY ID

After the creation is completed, the overview dialog of the application is displayed. Now note / copy the application and directory ID.



Home > Docusnap Sports AG - App registrations > [redacted]

[redacted]

Search (Ctrl+/)

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Expose an API

Owners

Roles and administrators (Previ...

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? →

Display name : [redacted]

Application (client) ID : 02c58600-[redacted]

Directory (tenant) ID : 4d0fe9aa-[redacted]

Object ID : [redacted]

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

View API Permissions

Sign in users in 5 minutes

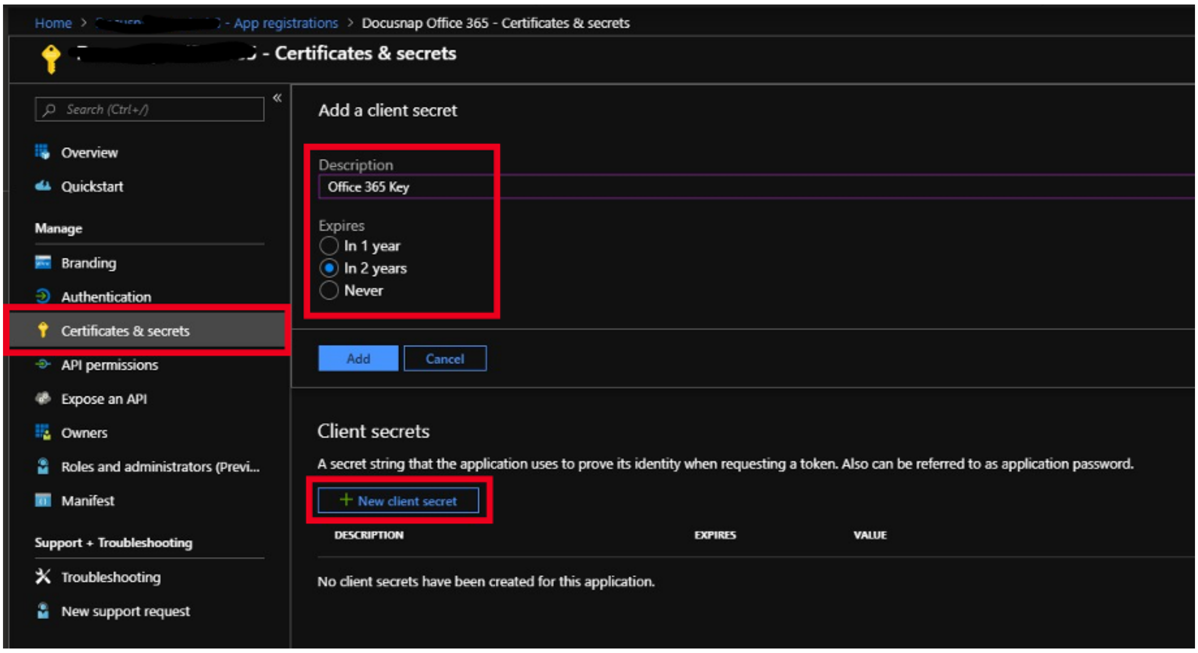
Use our SDKs to sign in users and call APIs in a few steps

CREATE A CLIENT SECRET

Now create a client secret. In the **Manage** area, select the item

- **Certificates & secrets**
- **New client secret**
- Enter a **Description** and
- the validity of the secret

Note: The key can only be viewed directly after creation. If the key is lost or becomes invalid, it must be recreated.



Add a client secret

Description: Office 365 Key

Expires
○ In 1 year
● In 2 years
○ Never

Client secrets

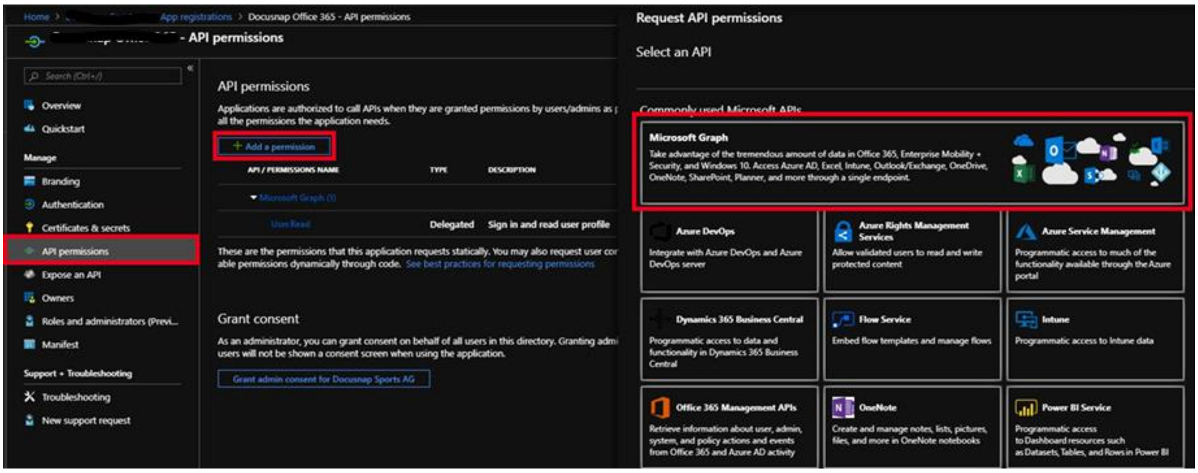
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

No client secrets have been created for this application.

AUTHORIZING THE APPLICATION – API PERMISSIONS

Now the application must be authorized for the Windows Azure Service Management API.

- In the **Manage** pane, select **API Permissions**
- **Add a permission**
- **Microsoft Graph**


Home > [redacted] App registrations > Docusnap Office 365 - API permissions
[redacted] - API permissions
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
+ Add a permission
Grant admin consent for Docusnap Sports AG
Request API permissions
Select an API
Commonly used Microsoft APIs

API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as p all the permissions the application needs.

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▾ Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

These are the permissions that this application requests statically. You may also request user co able permissions dynamically through code. See best practices for requesting permissions

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting adm users will not be shown a consent screen when using the application.

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.

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

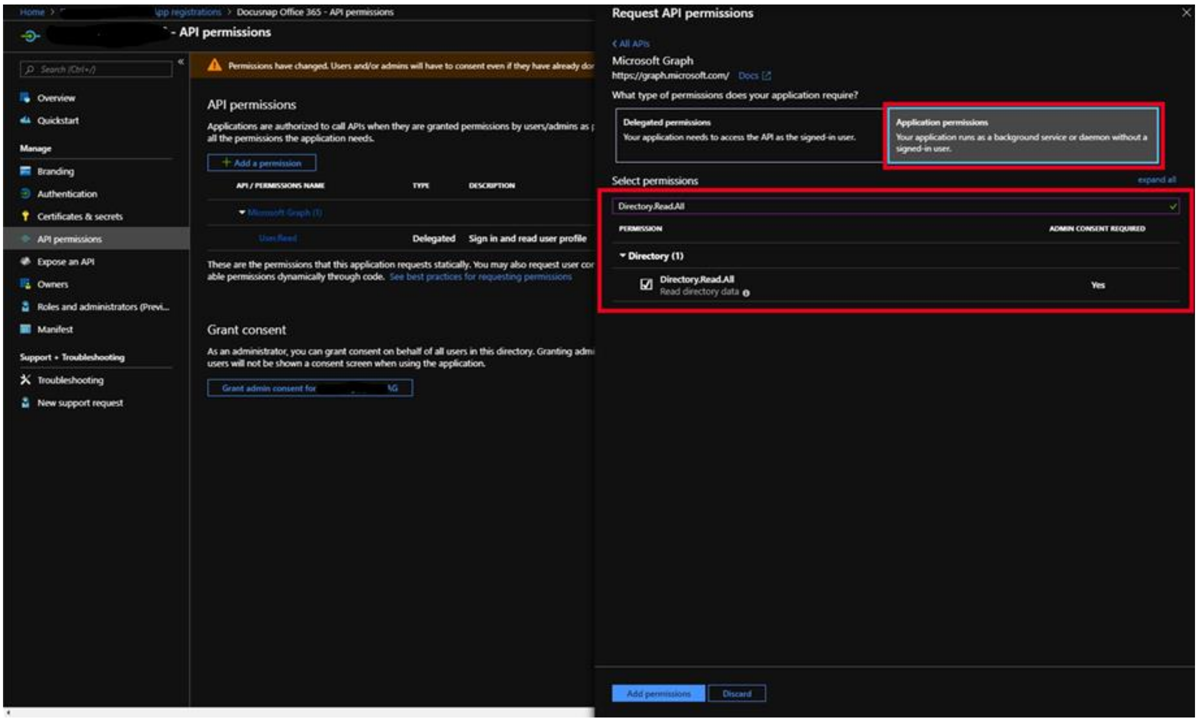
Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

Choose **Application permissions** as the type of permission to be granted.

Use the keyword **Directory** to find the **Directory.Read.All** permission and add this permission.



Permissions have changed. Users and/or admins will have to consent even if they have already do

API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as p all the permissions the application needs.

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▾ Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

These are the permissions that this application requests statically. You may also request user co able permissions dynamically through code. See best practices for requesting permissions

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting adm users will not be shown a consent screen when using the application.

Microsoft Graph
https://graph.microsoft.com/

What type of permissions does your application require?

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

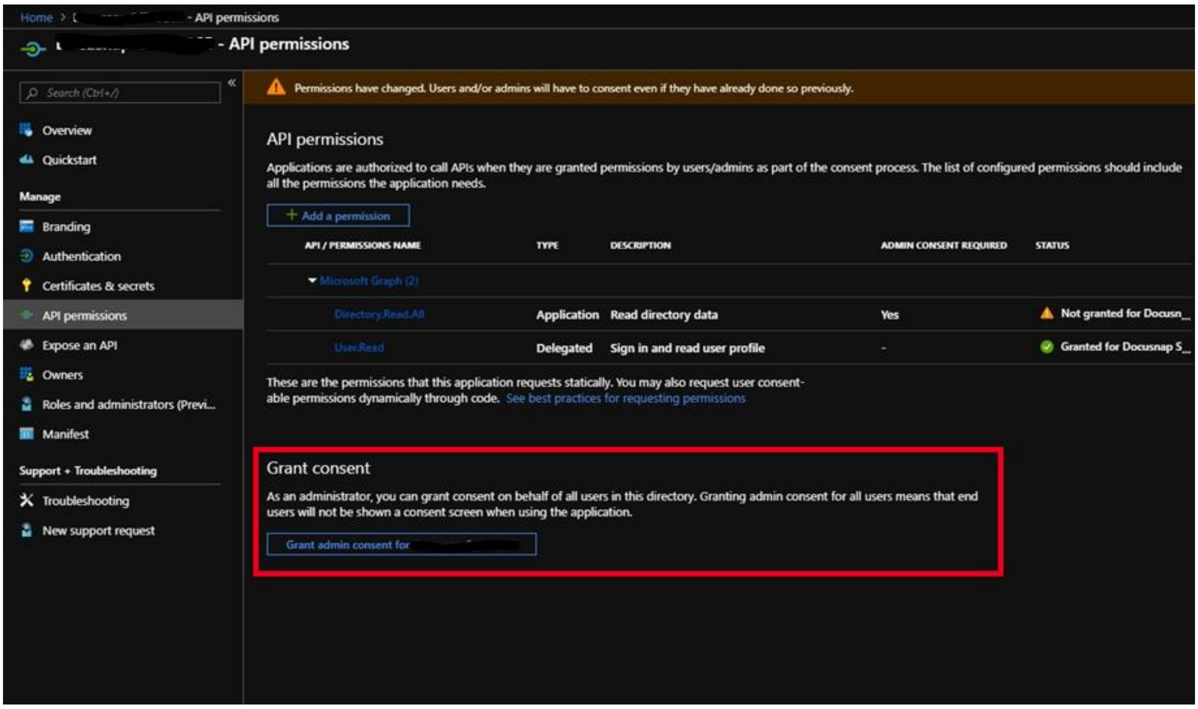
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Directory.Read.All

PERMISSION	ADMIN CONSENT REQUIRED
▾ Directory (1)	
☑ Directory.Read.All Read directory data	Yes

Now you must give your consent for the previously set permissions. To do this, select the control **Grant admin consent for "Your subscription".**



Permissions have changed. Users and/or admins will have to consent even if they have already done so previously.

API 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.

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED	STATUS
▾ Microsoft Graph (2)				
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Docusn...
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for Docusnap S...

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.