

Index

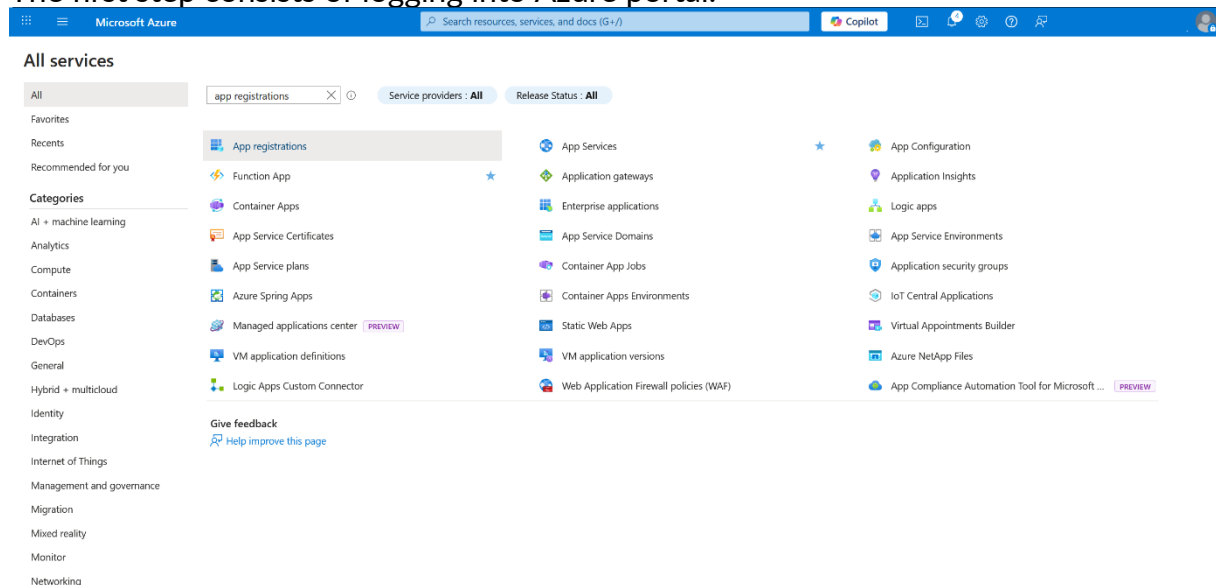
Microsoft Azure App Registration.....	1
Initial app registration	1
Configuring App registrations API permissions	3
Apply permissions for the selected site	5
Adding a client secret.....	7
Feedback to Supplydrive.....	9

Microsoft Azure App Registration for SharePoint Site Access

Please note that to complete all the steps you will need administrative rights within your Azure Active Directory tenant directory.

Initial app registration

The first step consists of logging into Azure portal.



In the Azure Portal navigate to **All Services**. Here you can find / filter on **App Registration**. Navigate to the App registration page

Microsoft Azure

Search resources, services, and docs (G+I)

Copilot

All services >

App registrations

+ New registration Endpoints Troubleshoot Refresh Download Preview features Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications Owned applications Deleted applications

Start typing a display name or application (client) ID to filter these r... Add filters

8 applications found

Display name ↑	Application (client) ID	Created on ↑	Certificates & secrets
		3/6/2025	-
		4/4/2025	Current
		3/13/2025	Current

In this case, there are already a few applications registered. We are going to register a new application by clicking on **+ New Registration**.

All services > App registrations >

Register an application

* Name

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

Supplydrive App Registration

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Supplydrive BV only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

Help me choose...

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.

Select a platform e.g. <https://example.com/auth>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

We have given the app the name, "**Supplydrive App Registration**". You can keep the supported account type to single tenant and the redirect URI is not necessary. Click **Register** to finish the initial registration.

Home > App registrations >

Supplydrive App Registration

Search Delete Endpoints Preview features

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication (Preview)
 - Certificates & secrets
 - Token configuration
 - API permissions

Essentials

Display name : Supplydrive App Registration

Application (client) ID : 430aad38-9d14-4bec-84a4-61e06ded7c3c

Object ID : cebdf320-65dd-4e3c-ab71-36338129265a

Directory (tenant) ID : bad0

Supported account types : My organization only

Client credentials : Add a certificate or secret

Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

Managed application in L : Supplydrive App Registration

State : Activated

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

Configuring App registrations API permissions

You now need to give the app registration permissions so it's able to read / write in the selected Microsoft services. Go to **API permissions** on the left-hand side.

All services > App registrations > Supplydrive App Registration

Supplydrive App Registration | API permissions

Search Refresh Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

- Branding & properties
- Authentication (Preview)
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured 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. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Supplydrive BV

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Currently, the app registration only has one delegated permission, i.e. User.Read. you can remove the default **User.Read** delegated permission by clicking on the ... (located at the end of the row) and selecting **Remove permission**.

After that Click on **+ Add permission**.

Refresh Got feedback?

Configured 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. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Supplydrive BV

API / Permissions name	Type	Description	Admin consent requ...	Status
------------------------	------	-------------	-----------------------	--------

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

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.

Select **Microsoft Graph**. Then click on **Application permissions**.

The screenshot shows the 'Request API permissions' dialog in the Azure Portal. The dialog is titled 'Request API permissions' and has a close button (X) in the top right corner. It contains a warning message: 'Your application runs as a background service or daemon without a signed-in user.' Below this, there is a section 'Select permissions' with a search bar and a list of permissions. The permissions are grouped under 'Sites (1)'. The selected permission is 'Sites.Selected' (Access selected site collections), which has 'Yes' in the 'Admin consent required' column. Other permissions listed include 'Sites.FullControl.All', 'Sites.Manage.All', 'Sites.Read.All', and 'Sites.ReadWrite.All'. At the bottom of the dialog, there are buttons for 'Add permissions' and 'Discard'.

Navigate to Sites and select the permission Sites.Selected. Click on **Add permissions** to finish adding permissions.

Configured 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. [Learn more about permissions and consent](#)

[+ Add a permission](#) [✓ Grant admin consent for Supplydrive BV](#)

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
Sites.Selected	Application	Access selected site collections	Yes	✓ Granted for Supplydrive...

API Permissions of type application require an administrator to grant consent. Have the admin click on **Grant admin consent for ...** link (located above the table). The entries in the **Status** column of the mail permissions are now updated to **Granted**.

Apply permissions for the selected site

Important: It is highly recommended to create a dedicated site for the Supplydrive integration. **Sites.Selected** with **Write** permissions will grant the app **read + write access to the entire selected site**, not just a single folder. Using a dedicated site ensures least privilege and better security.

1. Login to the Microsoft develop graph-explorer

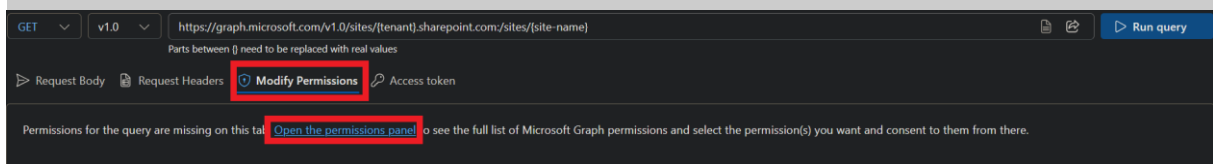
<https://developer.microsoft.com/en-us/graph/graph-explorer>

make sure you are logged in with your admin account (Sharepoint Admin / Global Admin). You can check the signed in user in the top right corner.

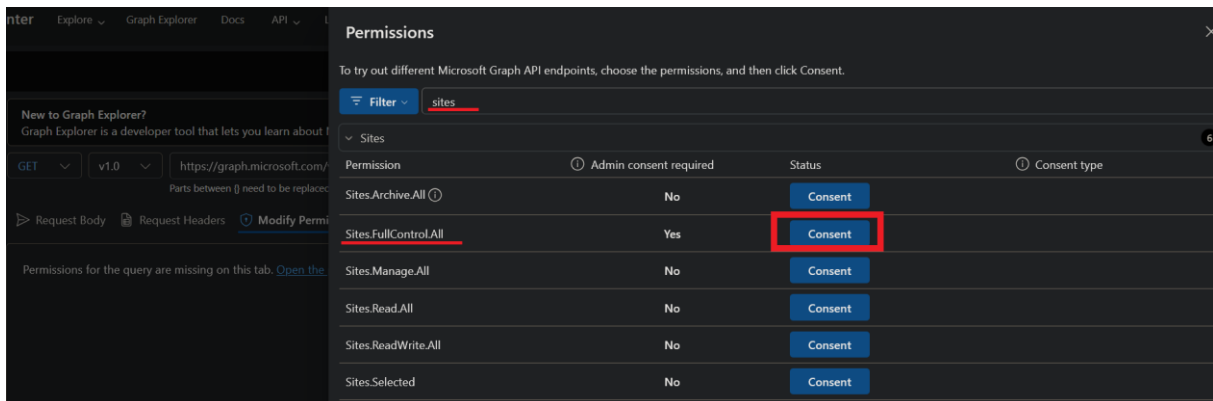
2. Apply API Consent and get the SharePoint Site ID

Enter the Graph url in from the textbox below. Make sure to replace **{tenant}** and **{site-name}** in the url. Use the http method GET.

`https://graph.microsoft.com/v1.0/sites/{tenant}.sharepoint.com:/sites/{site-name}`



After putting in the url navigate to the Modify Permissions tab and search for **Sites.FullControl.All**. Click on Consent next to the permission



After you have consent Press the **Run Query** button next to the Graph url. You should get back an response with OK Code 200

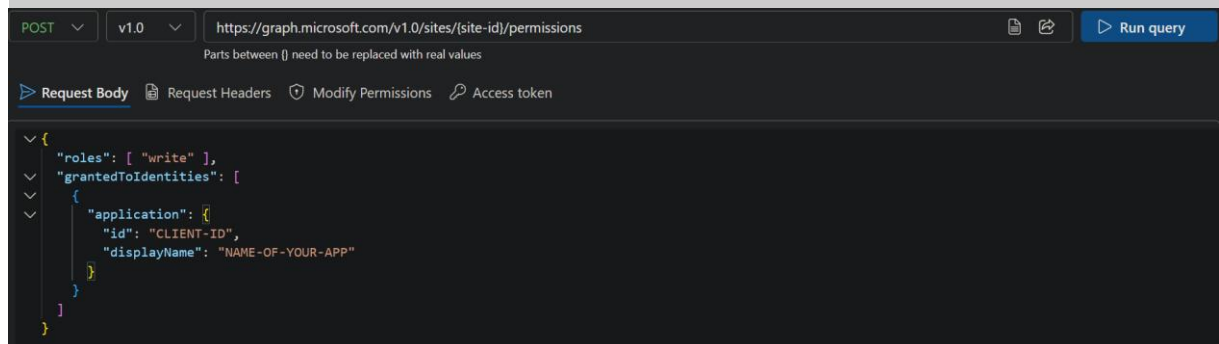
Copy the id of the site from the response

```
[Example response]
{
  ....
  "id": "tenant.sharepoint.com,12345abc-...,67890def-...",
  "name": "sitename",
  ..
}
```

2. Grant the app permission on the Sharepoint site

Make sure to replace **{site-id}** with the Site ID you got from the previous response. Select http method POST.

<https://graph.microsoft.com/v1.0/sites/{site-id}/permissions>



In the request body paste the following and replace **CLIENT-ID** with the CLIENT-ID of the app you registered earlier. You can choose your own display name

```
{
  "roles": [ "write" ],
  "grantedToIdentities": [
    {
      "application": {
        "id": "CLIENT-ID",
        "displayName": "NAME-OF-YOUR-APP"
      }
    }
  ]
}
```

Press run Query once all fields have been replaced. If everything went well you should receive a response code 201 - Created

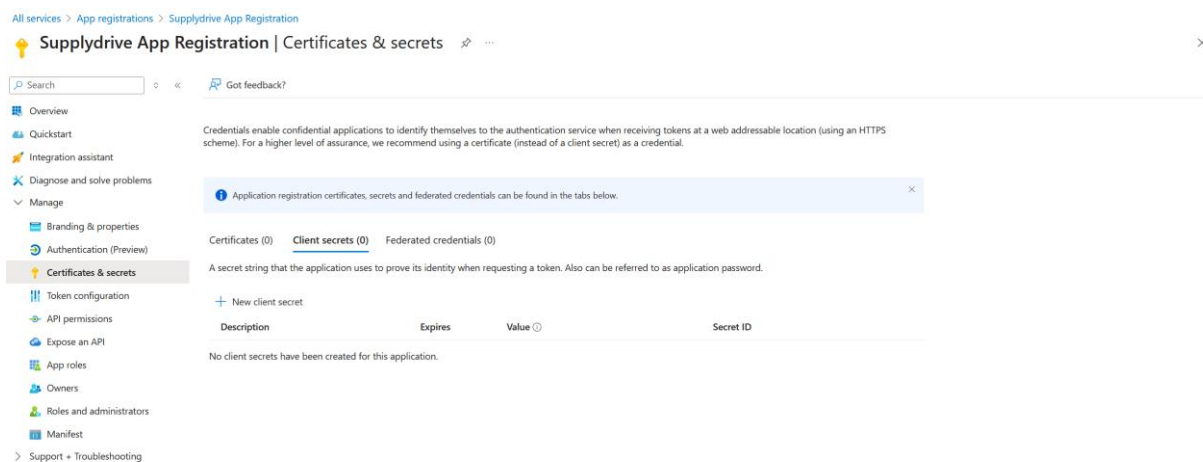
3. Verify the permission

Use the following API call to check if the permissions have been set successfully. Use the method GET.

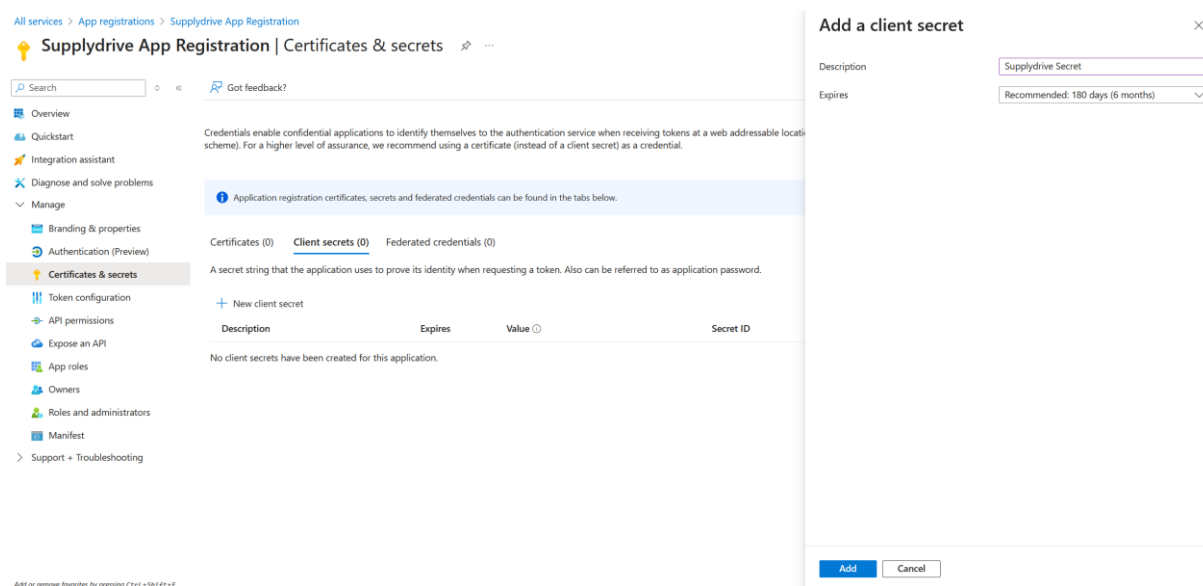
<https://graph.microsoft.com/v1.0/sites/{site-id}/permissions>

Adding a client secret

To allow us to use the app registration, you'll need to generate a client secret. Click on either **Certificates & Secrets** on the left-hand side or **Add a certificate or secret** link (next to Client credentials).



We currently have no client secrets. Click on the **+ New client secret**.



Give your secret a name and select an expiration date. Click on **add**.

Expires: At Supplydrive, we are notified when a secret is expired, but not when it will expire. The organization is responsible for renewing the secret. Once expired, we will notify the client, but it's best to renew it before expiration. Choose an expiration period that fits your security policies and processes.

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 ⓘ	Copy to clipboard	ID
Supplydrive Secret	1/21/2026	KBJ8Q~wE52a3M4KGvJlt1UVpwarq0SoS ...		1de7c214-b120-4f8d-88fe-185be6f60d2f

You have now generated a secret. Please note that the value of the secret is only available right after generation and is no longer available for copying after moving to a different screen. Copy the value and store it somewhere safe. You will need it later to send all necessary information to Supplydrive.

Please send the following information back to Supplydrive:

- Application (client) ID
- Directory (tenant) ID
- Client Secret Value
- SharePoint Site ID

Please send the information securely by using either <https://onetimesecret.com/> (Self destructing links), Encrypted e-mail or another similar secure method.

Information send in plain text over email will not be accepted!

Suppydrive App Registration

Search [] << [] Delete [] Endpoints [] Preview features []

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : [Suppydrive App Registration](#)

Application (client) ID : 430aad38-9d14-4bec-84a4-61e06ded7c3c

Object ID : cebdf320-65dd-4e3c-ab71-36338129265a

Directory (tenant) ID : badb

Supported account types : [My organization only](#)

Client credentials

0 certificate, 1 secret

Redirect URIs : [Add a Redirect URI](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in L... : [Suppydrive App Registration](#)

State : Activated

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	Copy to clipboard	at ID
Suppydrive Secret	1/21/2026	KBJ8Q~-wE52a3M4KGvlt1UVpwarq0SoS ...		1de7c214-b120-4f8d-88fe-185be6f60d2f

Credentials submitted without using a secure method will be rejected!
If credentials are shared in plain text, we ask you to create a new secret.