Index

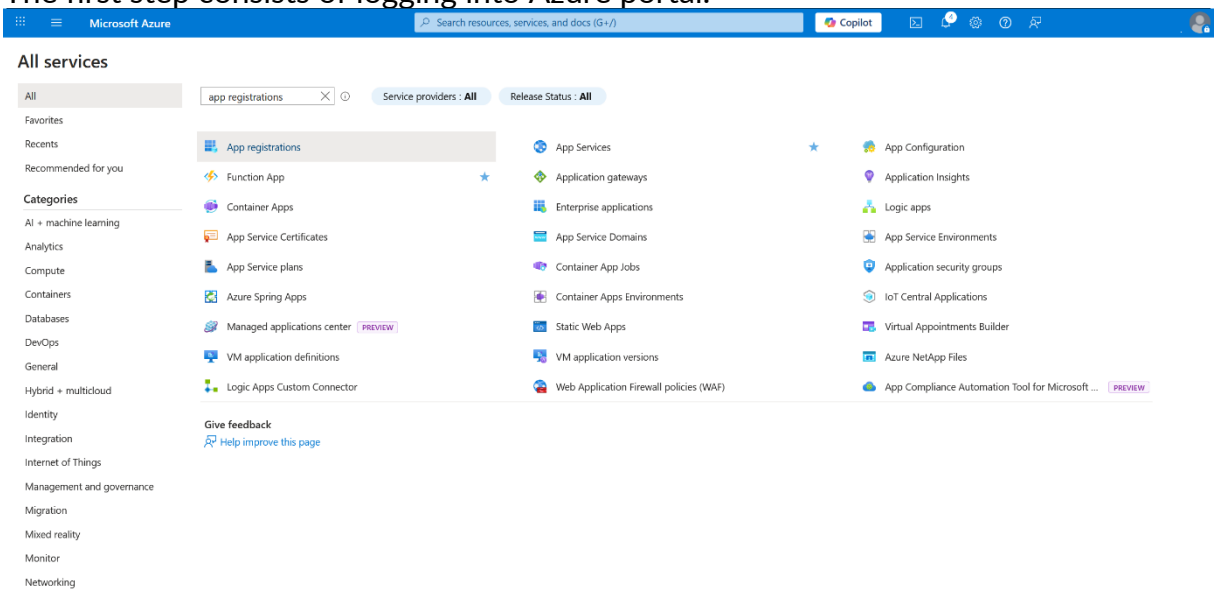
Microsoft Azure App Registration 1
Initial app registration 1
Configuring App registrations API permissions 3
Apply permissions for the selected site 5
Adding a client secret 7
Feedback to Supplydrive 9

Microsoft Azure App Registration for SharePoint Site Access

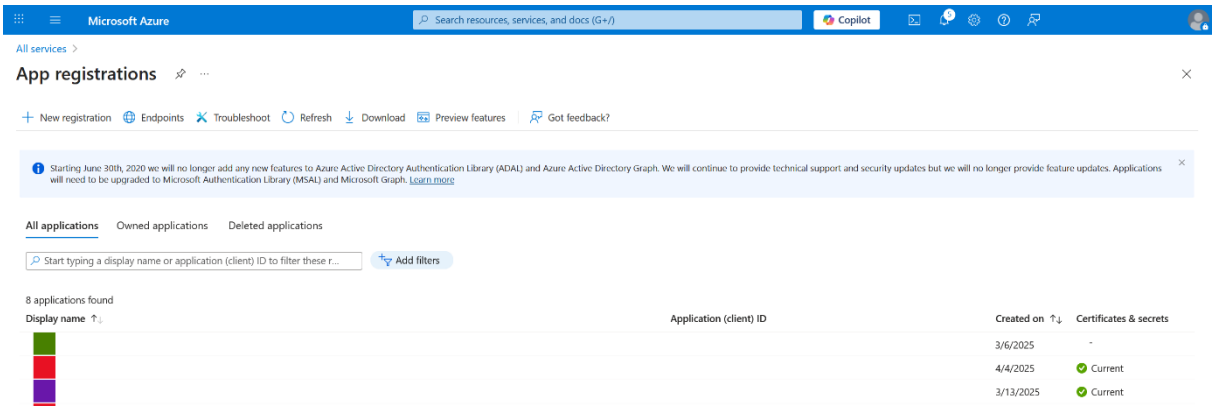
Please note that to complete all the steps you will need administrative rights within your Azure Active Directory tenant directory.

Initial app registration

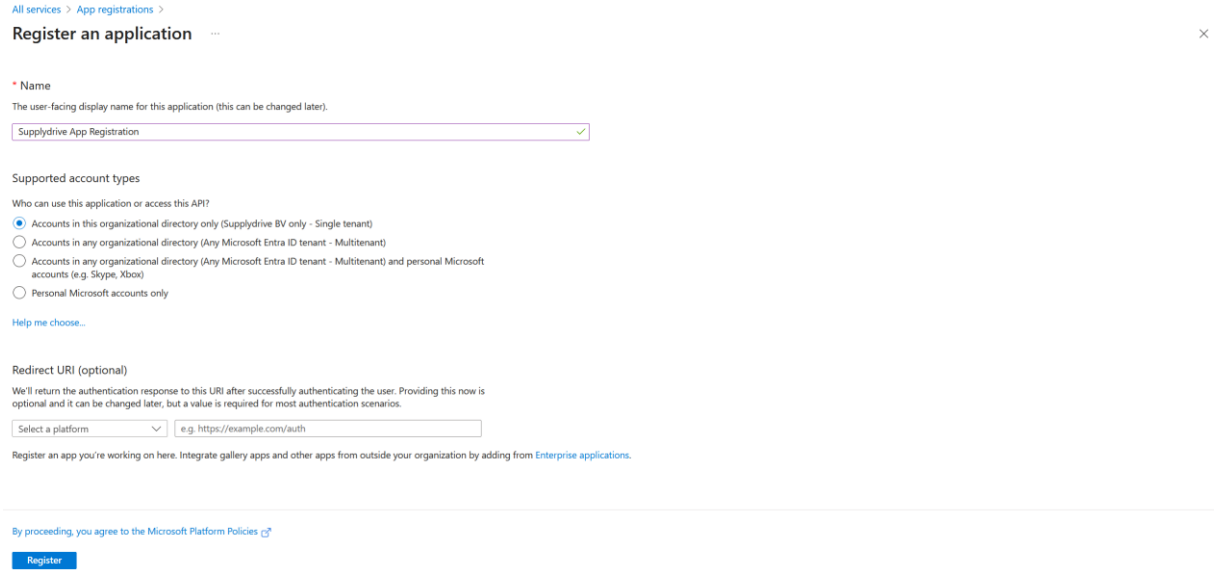
The first step consists of logging into Azure portal.



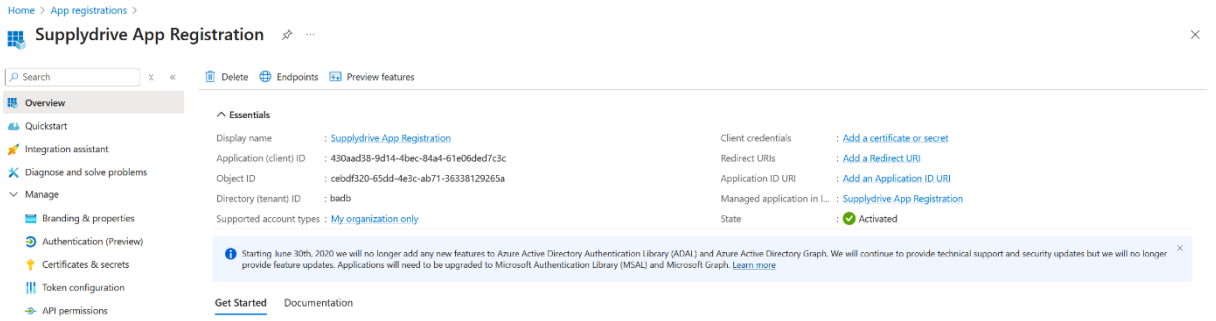
In the Azure Portal navigate to **All Services**. Here you can find / filter on **App Registration**. Navigate to the App registration page



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

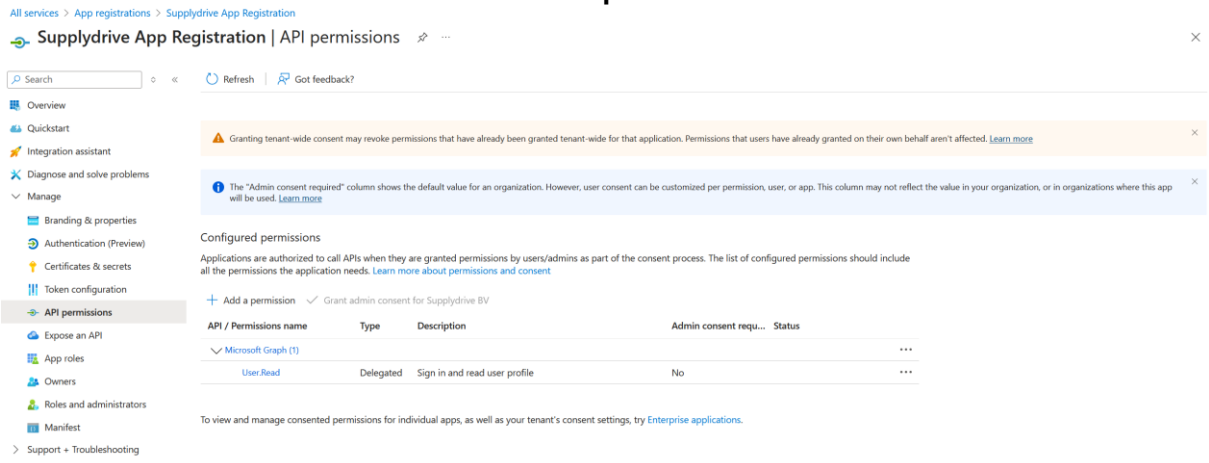


We have given the app the name, "**Supplydrive App Registration**". You can keep the supported account type to single tenant and the redirect URI is not necessary.
Click **Register** to finish the initial registration.



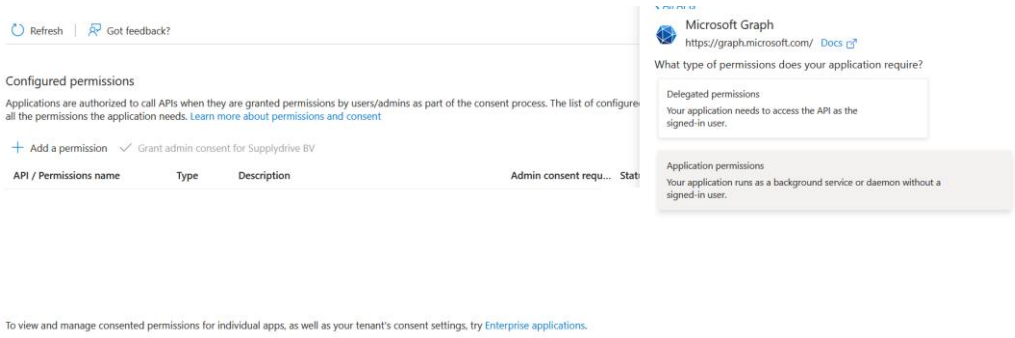
Configuring App registrations API permissions

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.

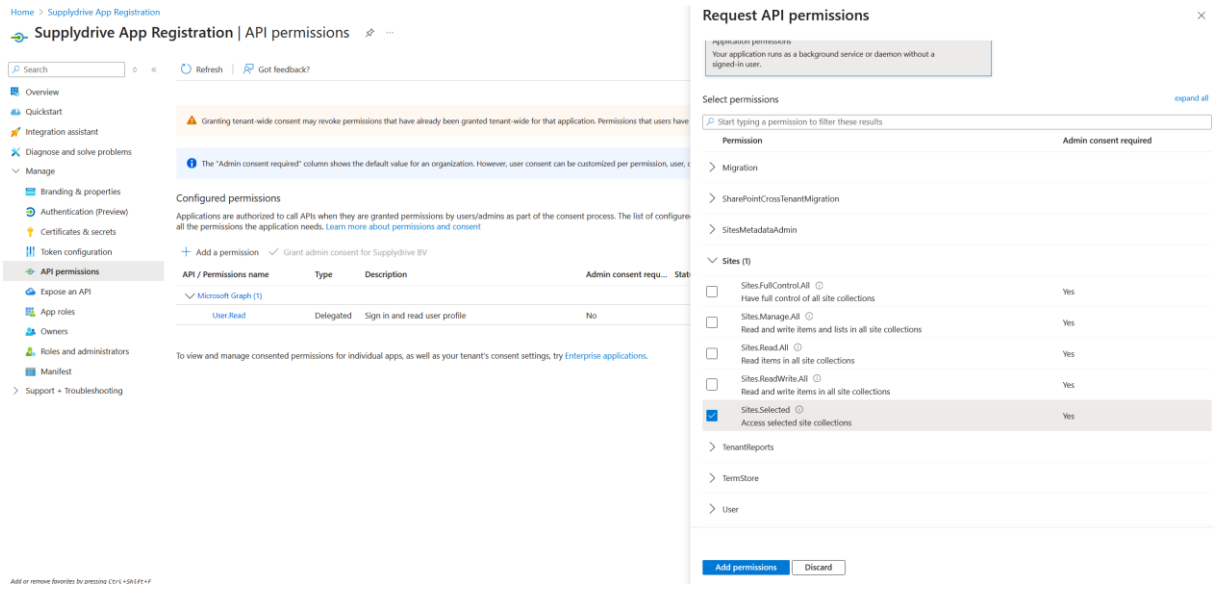


Currently, the app registration only has one delegated permission, i.e. User.Read. you can remove the default **User.Read** delegated permission by clicking on the **...** (located at the end of the row) and selecting **Remove permission**.

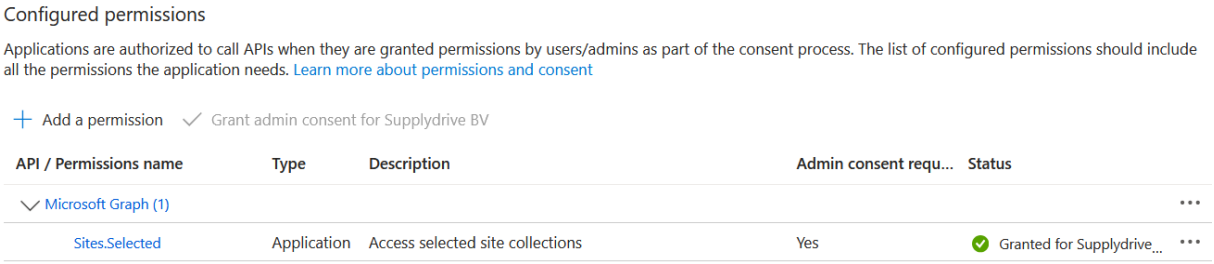
After that Click on **+ Add permission**.



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



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



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

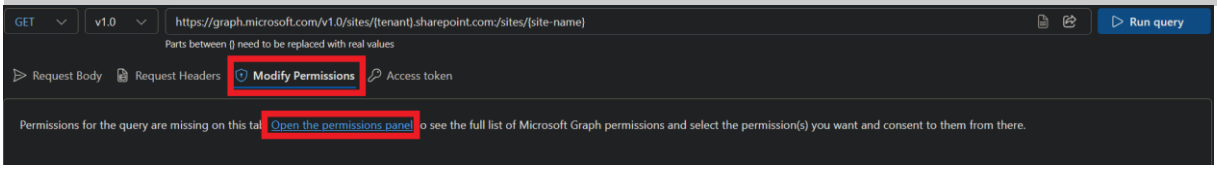
https://developer.microsoft.com/en-us/graph/graph-explorer

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.

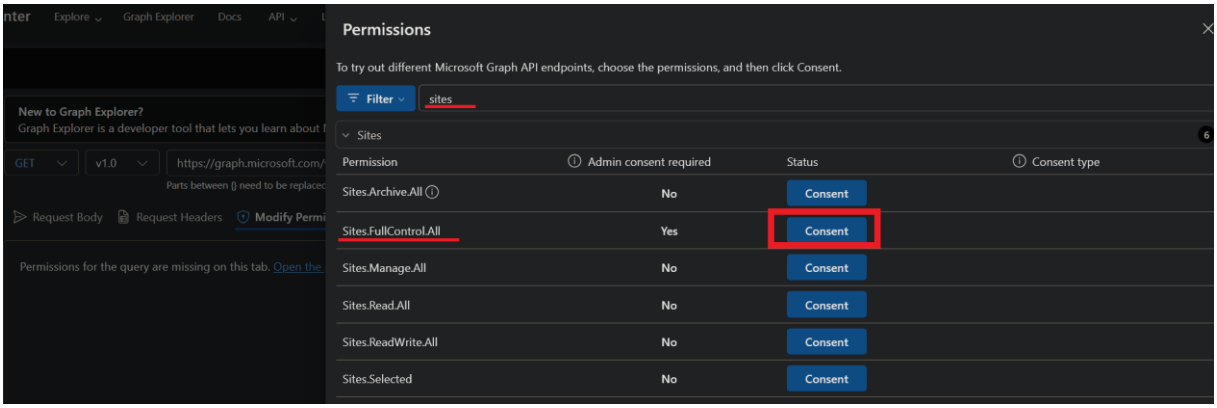
2. Apply API Consent and get the SharePoint Site ID

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. C**lick 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

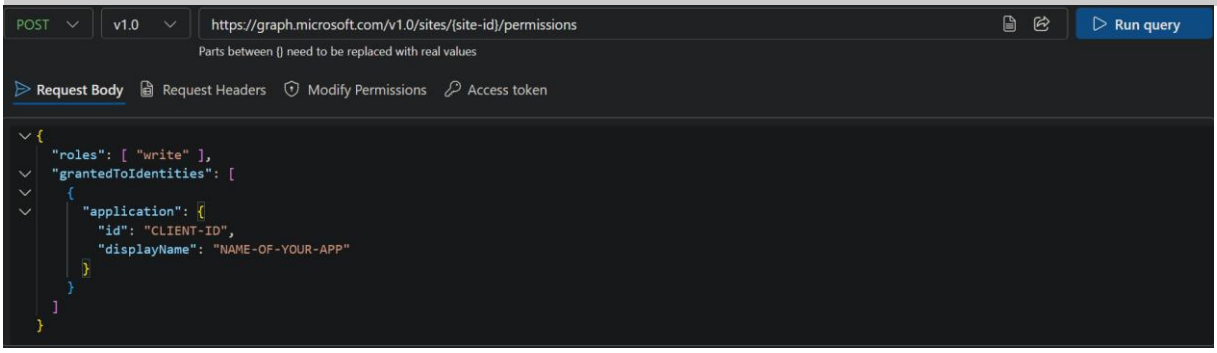
Copy the id of the site from the response

```
[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

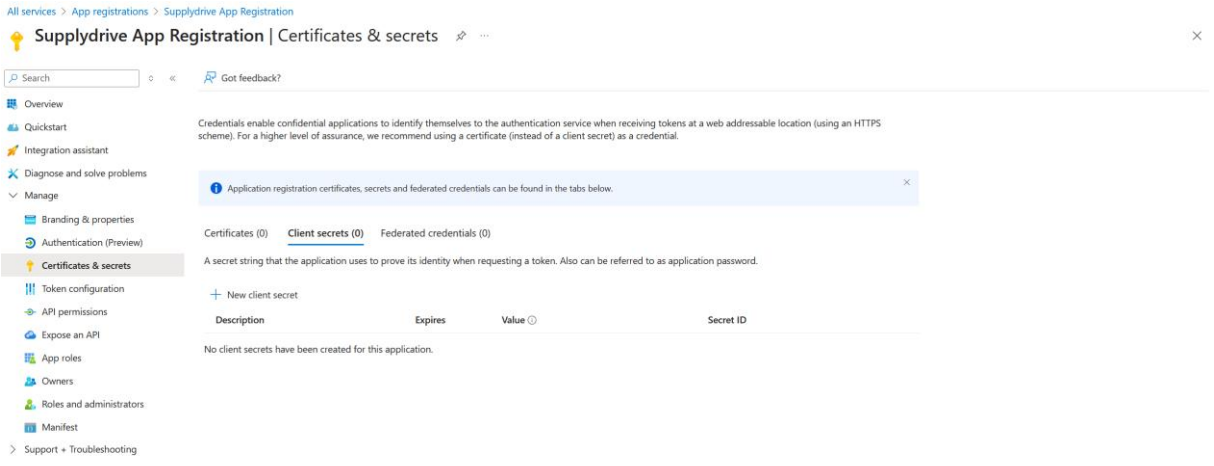
3. Verify the permission

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

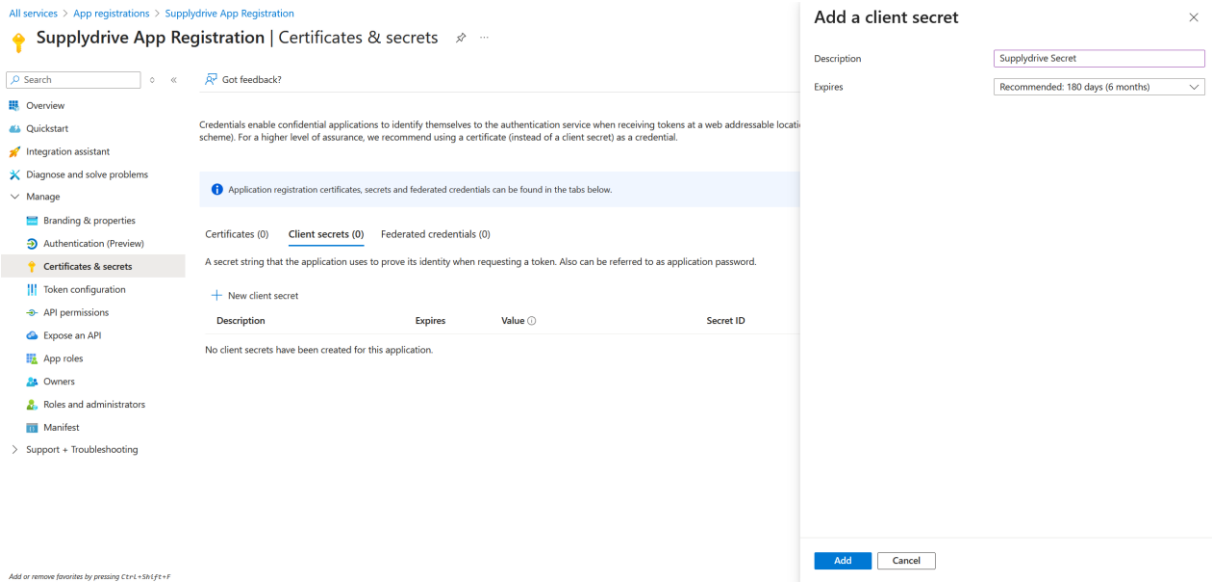
```
https://graph.microsoft.com/v1.0/sites/{site-id}/permissions
```

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).

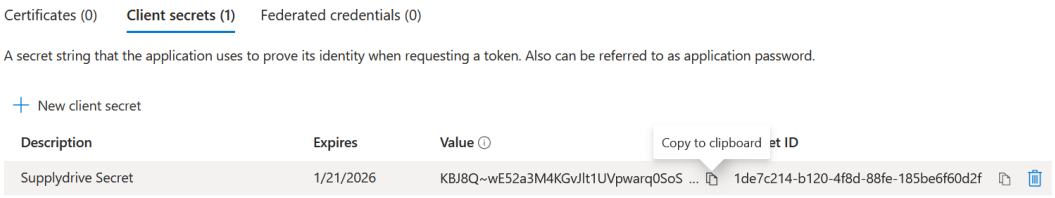


We currently have no client secrets. Click on the **+ New client secret**.



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.



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.

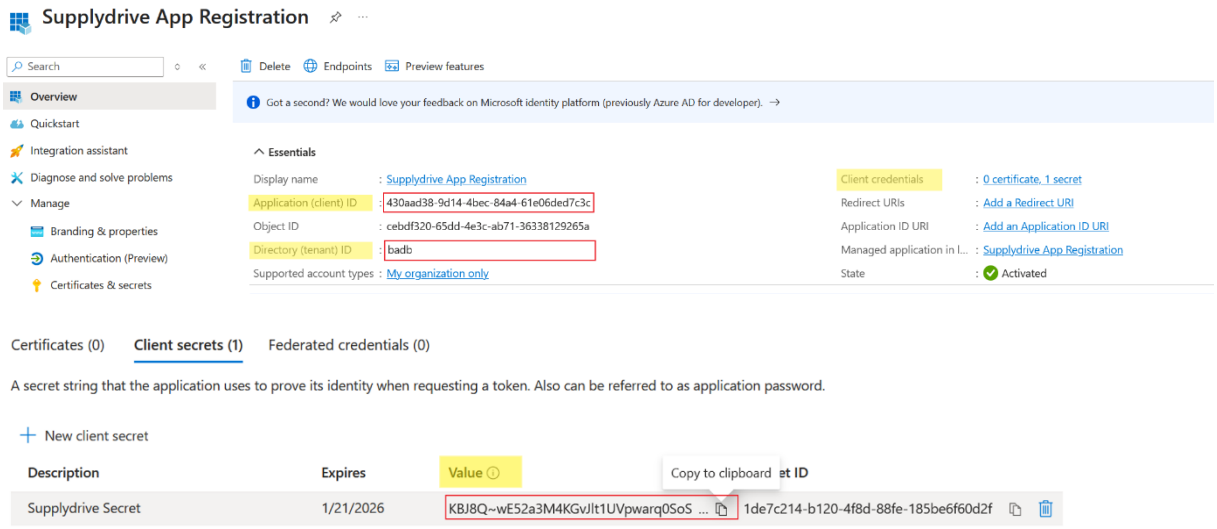
Feedback to Supplydrive

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!



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.