

[All Collections](#) > [Exchange/Office/Microsoft 365 integration](#) >

[Exchange/Office/Microsoft 365 with Add-in](#) >

[How to register the Microsoft Graph App on the Microsoft Azure portal?](#)

How to register the Microsoft Graph App on the Microsoft Azure portal?

Registering the Microsoft Graph App on the Microsoft Azure Portal.



Written by Yara | NEWOLDSTAMP

Updated over a week ago

Before you start, please check the table below about which platforms and Outlook versions support add-in:

Platform	Outlook version	Supported version and later
Windows	<ul style="list-style-type: none">- Microsoft 365 subscription- retail perpetual Outlook 2016 and later Note: Retail versions only! <i>(for now, volume-licensed versions don't include the necessary API requirements sets)</i>	from Version 2104, build 13929.20296 or above
Mac	<ul style="list-style-type: none">- new UI Note: Only the New Outlook interface is supported <i>(go to Outlook > New Outlook to enable it)</i>	from Outlook Version 16.38.506
Web browser	<ul style="list-style-type: none">- Modern Outlook UI when connected to Exchange Online: subscription, Outlook.com	-

Note: *If you have an Office 2021 LTSC or any other oldest Office with an old Outlook version, please update them to the newest version specified above.*

Additionally, you can check the [Microsoft article Outlook JavaScript API requirement sets](#) for more details.

Next, please follow these three main steps to set up Newoldstamp integration with Microsoft 365:

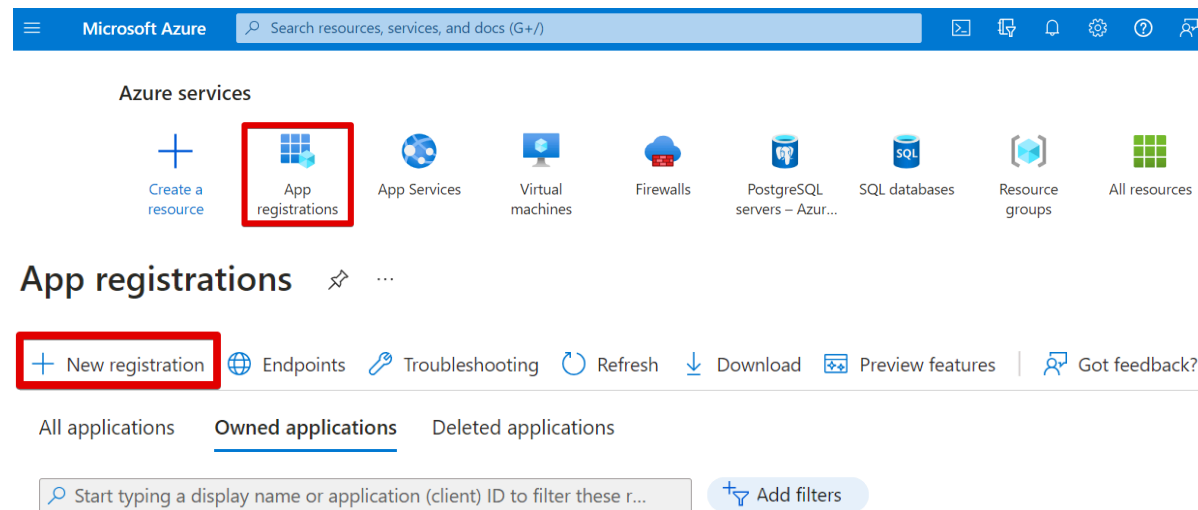
1. Register the application in the Microsoft Azure portal.
2. Create a client secret for the new application.

3. Assign permissions to access via Graph.

Step 1: Application registration on the Microsoft Azure portal.

If you have problems, please check the [required permissions](#) to verify that your account can create the identity.

1. Go to the Microsoft Azure portal at <https://portal.azure.com/> and sign in with your Microsoft Azure account.
2. Under **Azure services**, select **App registrations** and then click **New registration**.



3. In the **Register an application** page that appears, configure the following settings:

- **Name:** Enter something descriptive (e.x. newoldstamp-graph)

Note: You can change the display name anytime. Additionally, multiple app registrations can share the same name. The app registration's automatically

generated Application (client) ID, not its display name, uniquely identifies your app within the identity platform.

- By choosing **Supported account types**, specify who can use the application (sometimes called its *sign-in audience*). Select the option **Accounts in this organizational directory only**.
- **Redirect URI (optional)**: In the first box, select **Web**.

Register an application ...

newoldstamp-graph ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (newoldstamp 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.

Web ✓ 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

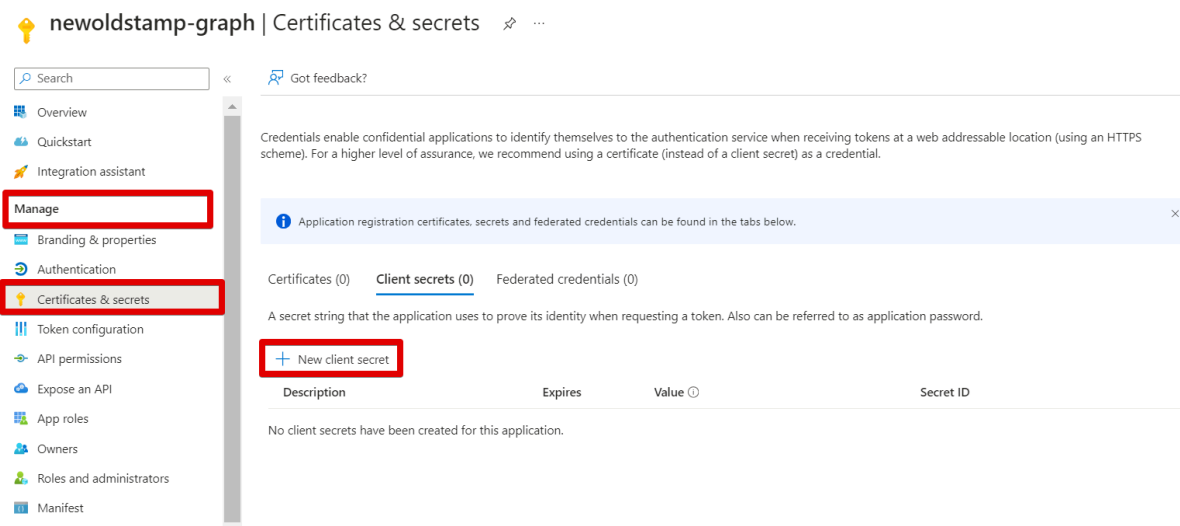
5. Once all the above is done, click **Register**.

6. Leave the page that appears open. You'll be able to use it in the next step.

Note: When registration finishes, the Microsoft Entra admin center displays the app registration's **Overview** pane. You see the **Application (client) ID**. Also called the *client ID*, this value uniquely identifies your application in the Microsoft identity platform.

Step 2: Create a client secret for the new application.

1. Under **Manage** on the left side menu, select **Certificates & secrets**.
2. On the **Certificates & secrets** page that opens, select **Client secrets**, and click **New client secret**.



3. In the dialog that appears, provide a **Description** for the new secret, select the period after which the secret expires, and then click **Add**.

Add a client secret



Description	<input type="text" value="NOSsecret"/>
Expires	<input type="text" value="365 days (12 months)"/>

Add

Cancel

4. **Copy the secret value** and **make sure to save it somewhere** to access it later because the secret will not be accessible after you proceed from here.

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.

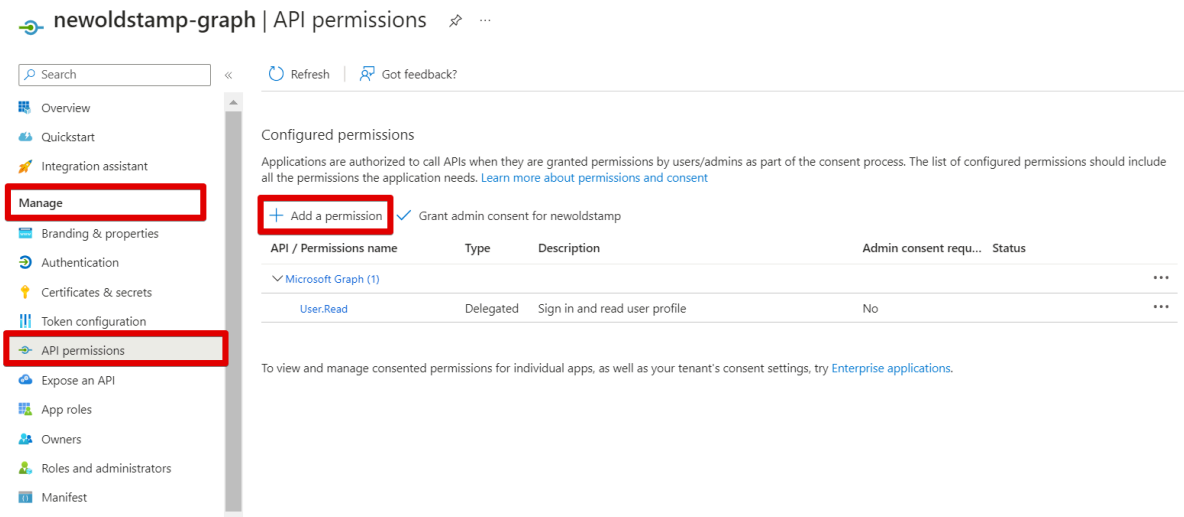
[+ New client secret](#)

Description	Expires	Value ⓘ	Secret ID
NOSsecret	3/5/2024	Etf8Q~8BOWTccGC5d.fjvIDIC1VI9EVSm~...	954c0d28-54e5-4082-9a8c-534786ddd03a ⓘ 🗑️

Note: Copy the secret value on that step because it will not be accessible after you proceed from here.

Step 3: Assign permissions to access via Graph.

1. Under **Manage**, on the left side menu, select **API permissions**.
2. On the **API permissions** page that opens, click **Add permission**.



3. On the **Request API permissions** window that appears, click **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 Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Communication Services

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams



Azure DevOps

Integrate with Azure DevOps and Azure DevOps server



Azure Rights Management Services

Allow validated users to read and write protected content

4. Click **Application permissions**.

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.

5. Then, the **Permission tree** appears below:

- Expand the **Group** node and select **Group.Read.All**

- Expand the **User** node and select **User.Read.All**

Request API permissions



Group (1)

<input type="checkbox"/>	Group.Create ⓘ Create groups	Yes
<input checked="" type="checkbox"/>	Group.Read.All ⓘ Read all groups	Yes
<input type="checkbox"/>	Group.ReadWrite.All ⓘ Read and write all groups	Yes

User (1)

<input type="checkbox"/>	User.EnableDisableAccount.All ⓘ Enable and disable user accounts	Yes
<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage all users' identities	Yes
<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

- Click **Add permissions** to confirm the selection.

8. On the **API permissions** page that opens, do the following steps:

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 newoldstamp

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (3) ***				
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for newo... ***
User.Read	Delegated	Sign in and read user profile	No	***
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for newo... ***

Select **Grant admin consent for <Organization>**, read the confirmation dialog that opens, and then click **Yes**.

Grant admin consent confirmation.

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

The **Status** value should now be **Granted for <Organization>**.

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 newoldstamp

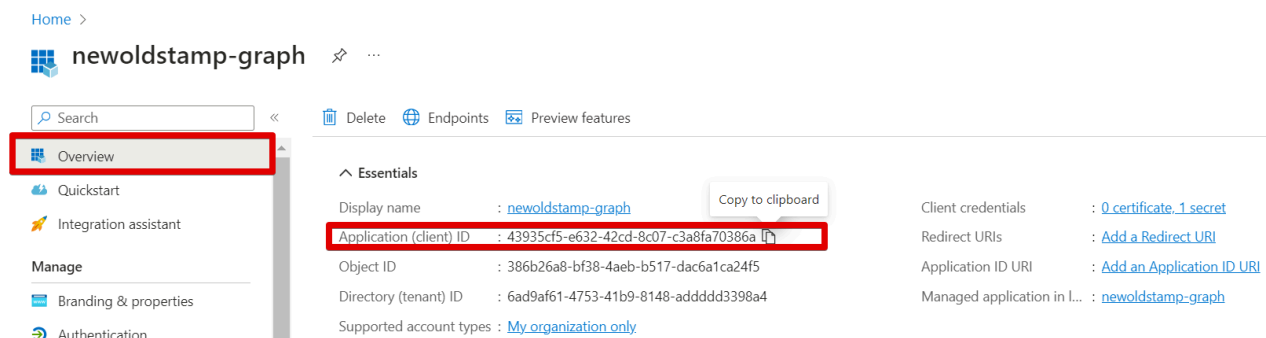
API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (3) ***				
Group.Read.All	Application	Read all groups	Yes	✅ Granted for newoldst... ***
User.Read	Delegated	Sign in and read user profile	No	✅ Granted for newoldst... ***
User.Read.All	Application	Read all users' full profiles	Yes	✅ Granted for newoldst... ***

Note: If you use **Key Vaults**, please ensure you configure access policies on resources by

checking [this Microsoft guide](#).

Step 4. Finally, go to the Newoldstamp application and provide the following:

- **Application (client) ID** (as shown below):



Home > newoldstamp-graph

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Delete Endpoints Preview features

Essentials

Display name : newoldstamp-graph

Application (client) ID : 43935cf5-e632-42cd-8c07-c3a8fa70386a

Object ID : 386b26a8-bf38-4aeb-b517-dac6a1ca24f5

Directory (tenant) ID : 6ad9af61-4753-41b9-8148-addddd3398a4

Supported account types : My organization only

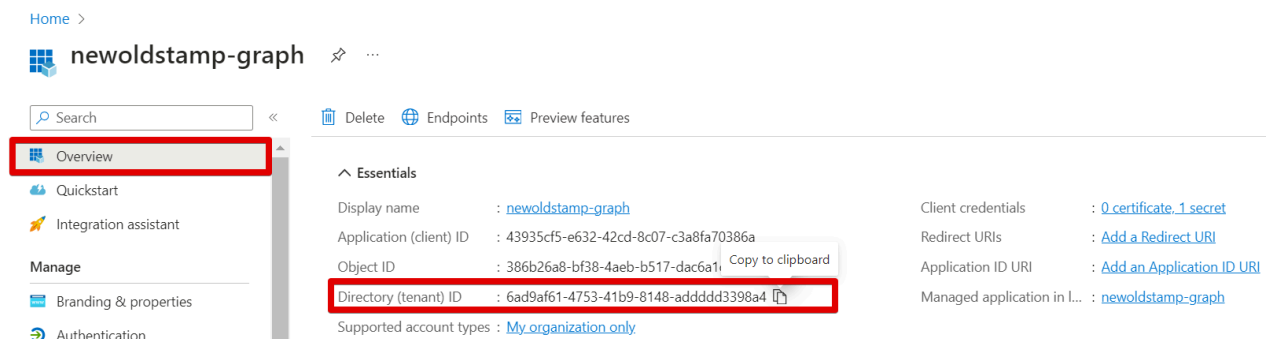
Client credentials : 0 certificate_1 secret

Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

Managed application in L... : newoldstamp-graph

- **Client secret** (saved on Step 2)
- **Directory (tenant) ID** (as shown below)



Home > newoldstamp-graph

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Delete Endpoints Preview features

Essentials

Display name : newoldstamp-graph

Application (client) ID : 43935cf5-e632-42cd-8c07-c3a8fa70386a

Object ID : 386b26a8-bf38-4aeb-b517-dac6a1ca24f5

Directory (tenant) ID : 6ad9af61-4753-41b9-8148-addddd3398a4

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... : newoldstamp-graph

Choose if you would like to turn on or off an automatic sync with Active Directory every 24 hours and click Continue:

 Azure AD Application Credentials

1 Step

2 Step

3 Step

Please, provide the following information after you have set the AD application:

Application ID

Application secret

Application Tenant ID

Automatic Signature Update with Active Directory

Newoldstamp can automatically update signatures if any information imported to the signature is changed in Google Directory. Automatic sync will occur every 24 hours. Manual signature updates can still be done at any point of time.

Continue

Done! The add-in has been registered. Now, please [follow the steps in this guide](#) to centrally install the add-in to the users in your organization.

Did this answer your question?



DASHBOARD

 We run on Intercom