Azure AD - App registration

Overview

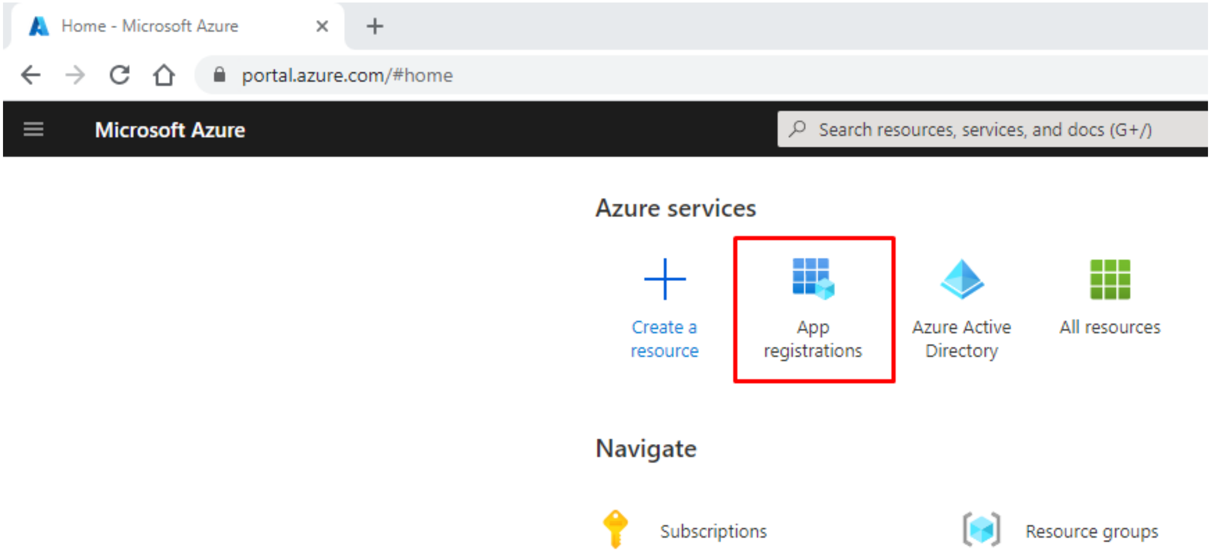
This instruction shows you how to create an app in Azure that enables you to get groups and group members from your AD into your Bosbec account.

We will use our workflows to build an integration towards the Microsoft Graph API. In order to configure the workflow we need three parameters from your Azure account.

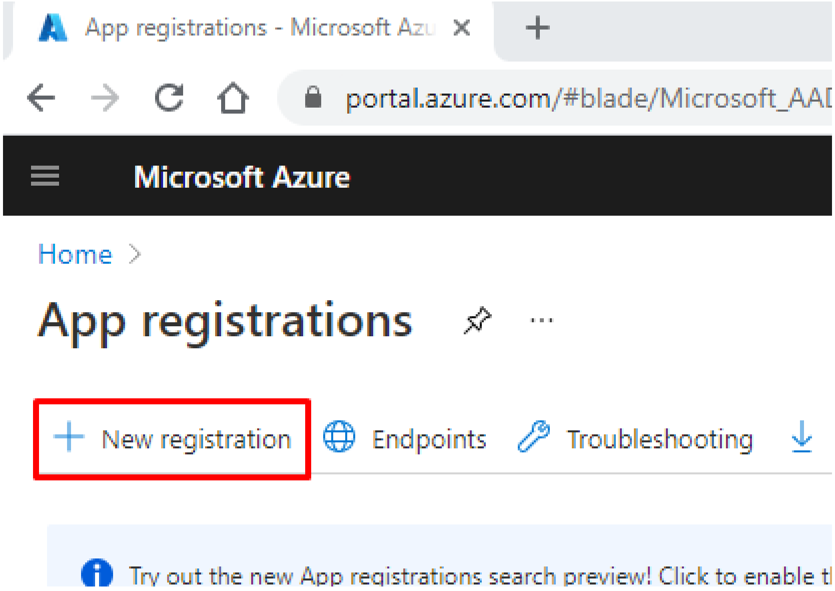
- Directory (tenant) ID
- Application (client) ID
- Client secret

Creating the app registration

Start by going to portal.azure.com and click in app registrations

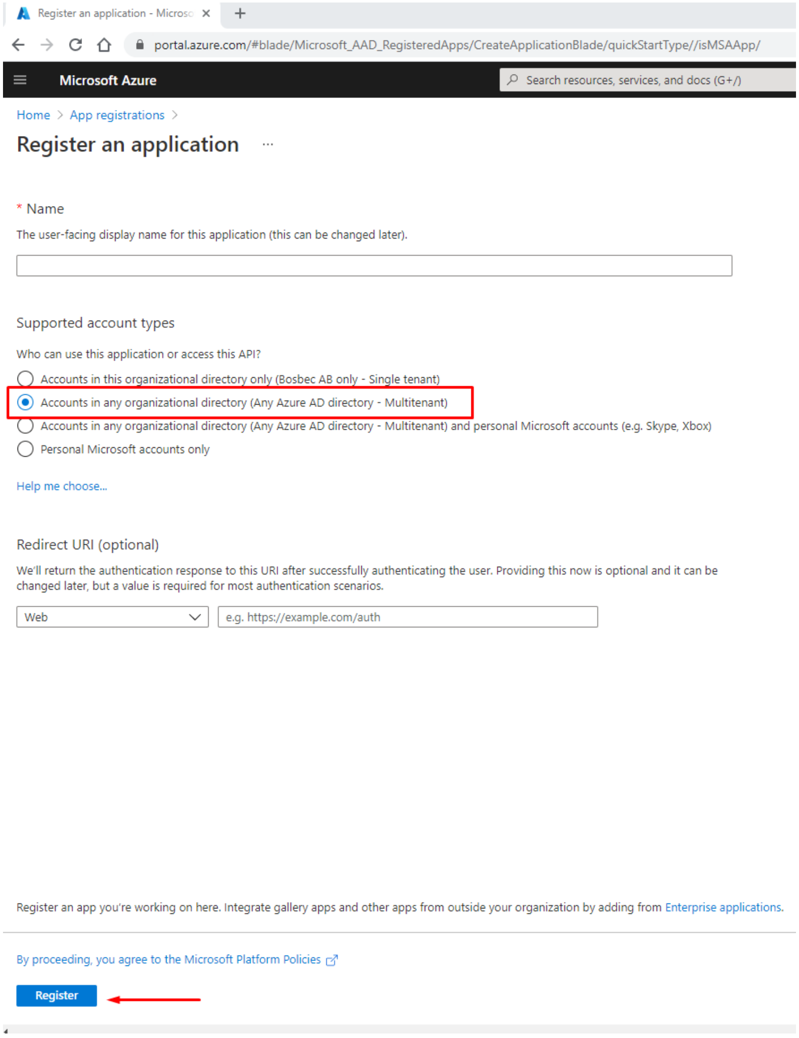


Click “New registration”



Try out the new App registrations search preview! Click to enable t

Enter a name to help you identify the app and for account type choose the second option “Any Azure Account - Multi-tenant”.


Register an application - Microso
portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/CreateApplicationBlade/quickStartType//isMSAApp/
Microsoft Azure
Search resources, services, and docs (G+/)
Home > App registrations >

Register an application

* Name

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

Supported account types

Who can use this application or access this API?

- ○ Accounts in this organizational directory only (Bosbec AB only - 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)
- ○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

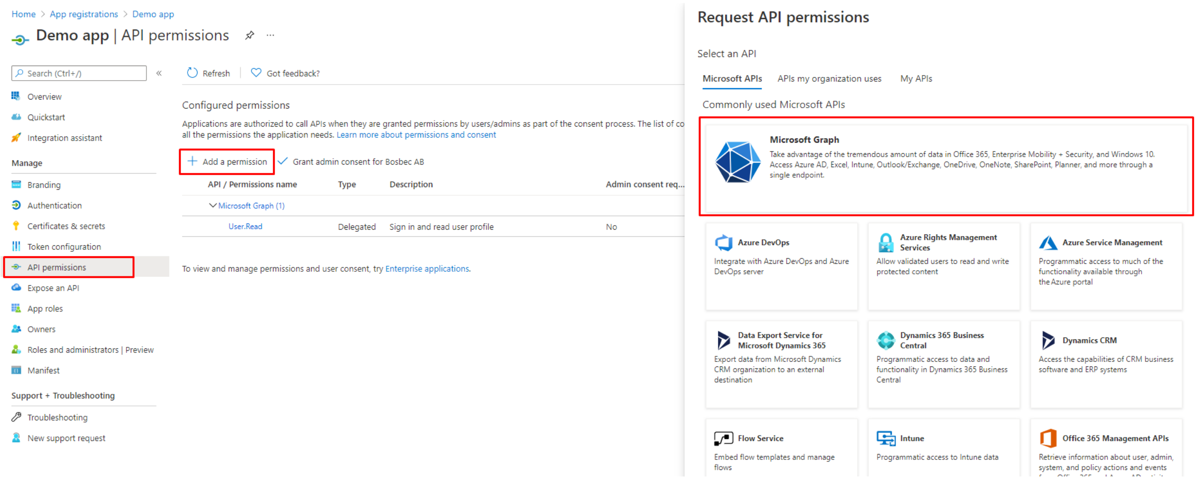
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

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

Next we will add permissions to access the groups and group members from your Azure AD. Select API permissions from the menu and then “Add a permission”. Choose Microsoft Graph as the API you want to work with.



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 co all the permissions the application needs. Learn more about permissions and consent

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

To view and manage permissions and user consent, try Enterprise applications.

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.

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

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

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

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

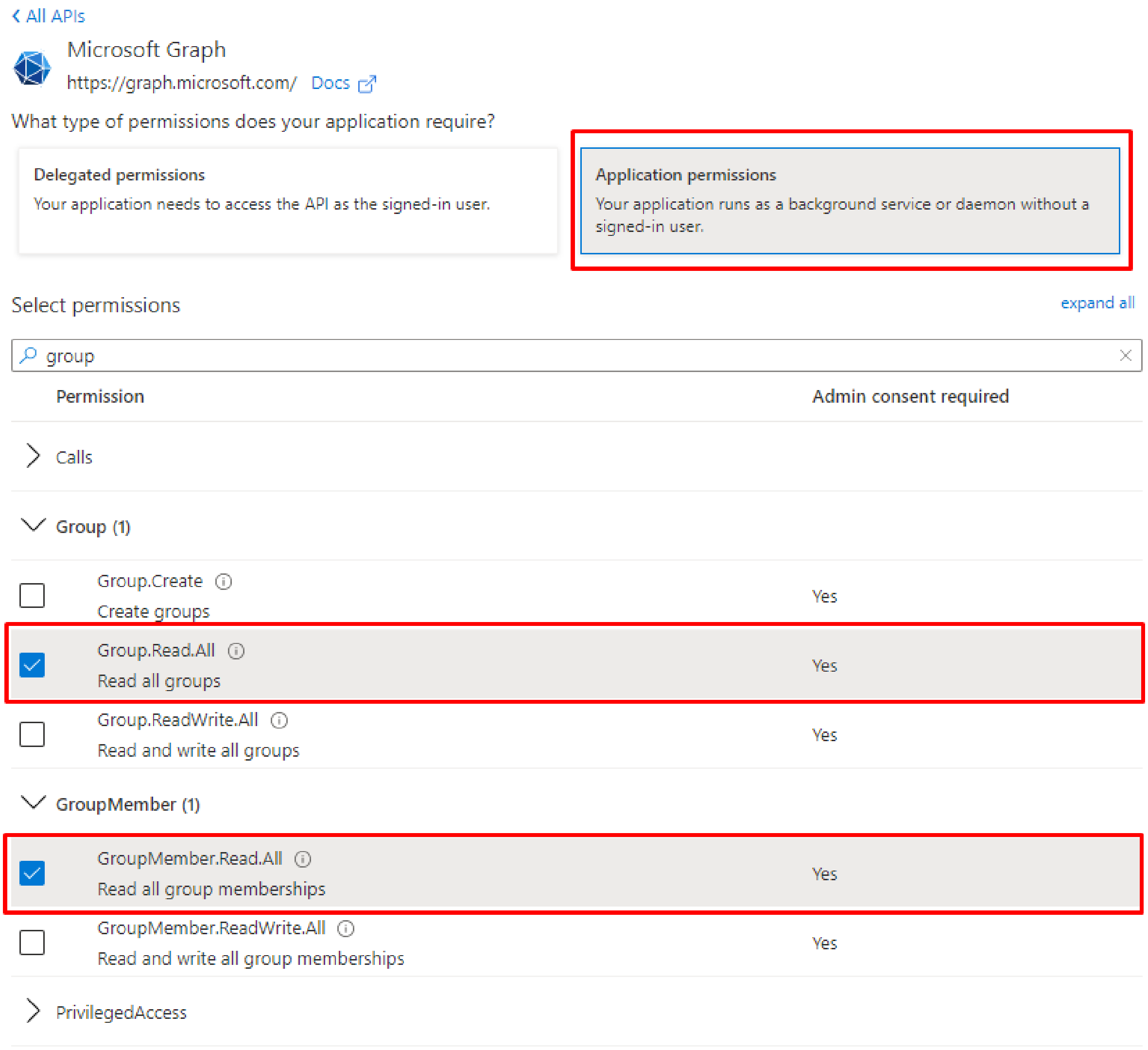
Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events

Next choose “application permissions” as type and the search and add the following permissions (you can select multiple permissions at the same time).

- Application.ReadAll
- Directory.ReadAll
- Domain.ReadAll
- Group.ReadAll
- GroupMember.ReadAll
- User.ReadAll



< 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.

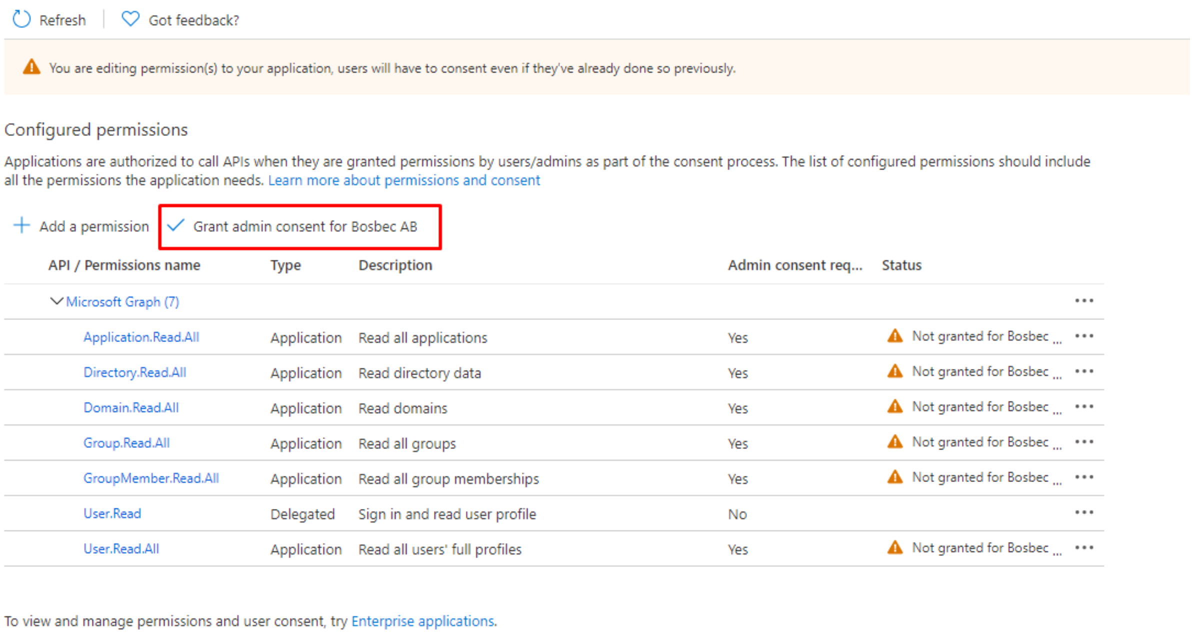
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions — expand all

Search: group

	Permission	Admin consent required
	> Calls	
	∨ Group (1)	
☐	Group.Create ⓘ Create groups	Yes
☑	Group.Read.All ⓘ Read all groups	Yes
☐	Group.ReadWrite.All ⓘ Read and write all groups	Yes
	∨ GroupMember (1)	
☑	GroupMember.Read.All ⓘ Read all group memberships	Yes
☐	GroupMember.ReadWrite.All ⓘ Read and write all group memberships	Yes
	> PrivilegedAccess	

After you have added the permissions you need to grant admin consent to use them.



Refresh | Got feedback?

⚠ You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

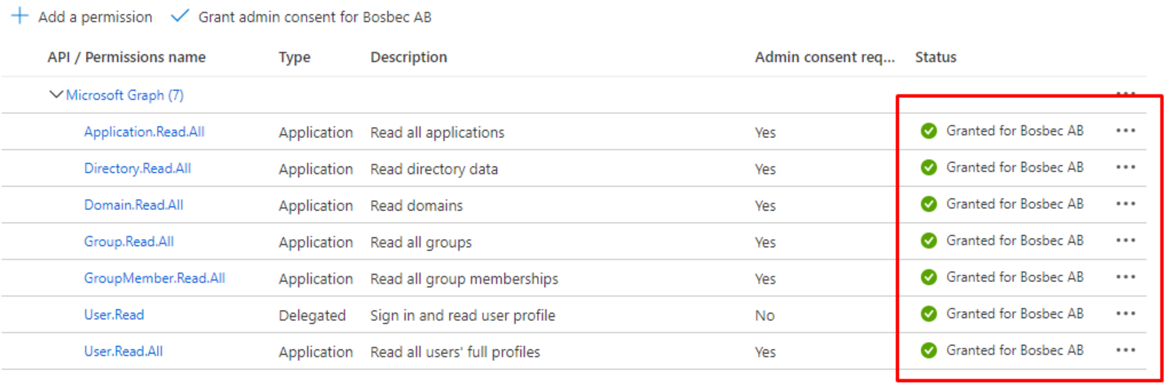
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for Bosbec AB

API / Permissions name	Type	Description	Admin consent req...	Status	
∨ Microsoft Graph (7)					•••
Application.Read.All	Application	Read all applications	Yes	⚠ Not granted for Bosbec ...	•••
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Bosbec ...	•••
Domain.Read.All	Application	Read domains	Yes	⚠ Not granted for Bosbec ...	•••
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Bosbec ...	•••
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for Bosbec ...	•••
User.Read	Delegated	Sign in and read user profile	No		•••
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Bosbec ...	•••

To view and manage permissions and user consent, try Enterprise applications.

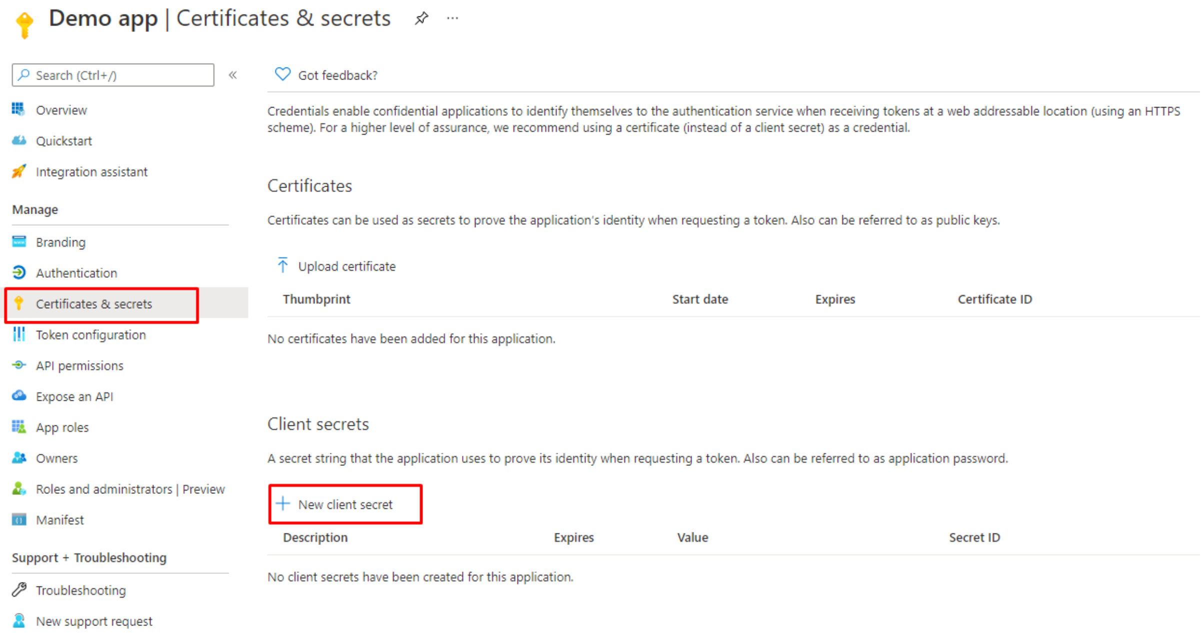
This is how it looks after giving admin consent



+ Add a permission ✓ Grant admin consent for Bosbec AB

API / Permissions name	Type	Description	Admin consent req...	Status	
∨ Microsoft Graph (7)					•••
Application.Read.All	Application	Read all applications	Yes	✓ Granted for Bosbec AB	•••
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Bosbec AB	•••
Domain.Read.All	Application	Read domains	Yes	✓ Granted for Bosbec AB	•••
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Bosbec AB	•••
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for Bosbec AB	•••
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Bosbec AB	•••
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Bosbec AB	•••

Last step is to create a client secret. Click “Certificates & secrets” in the left menu and choose “New client secret”.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

No certificates have been added for this application.

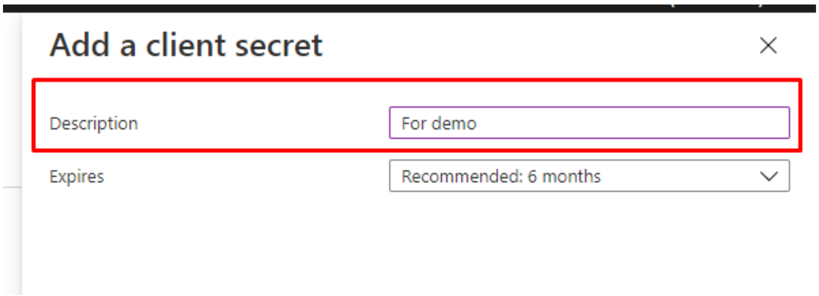
Client secrets

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

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

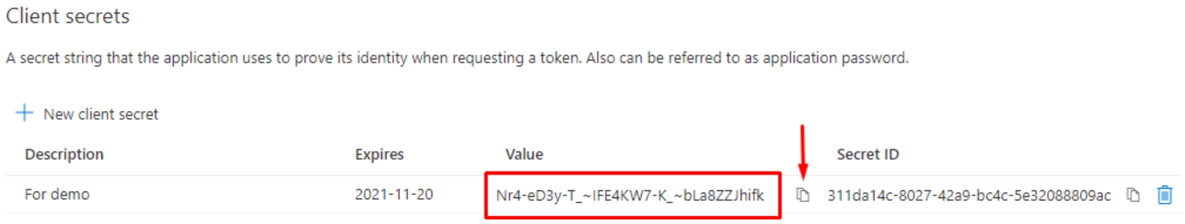
Enter a description and assign how long the secret should be valid. For security reasons it is good practice to change the secret once every 1-2 years. It is easy to change the secret in the workflow to a new one when it has expired and you can have more than one valid at the same time to avoid any downtime.


Add a client secret

Description: For demo

Expires: Recommended: 6 months

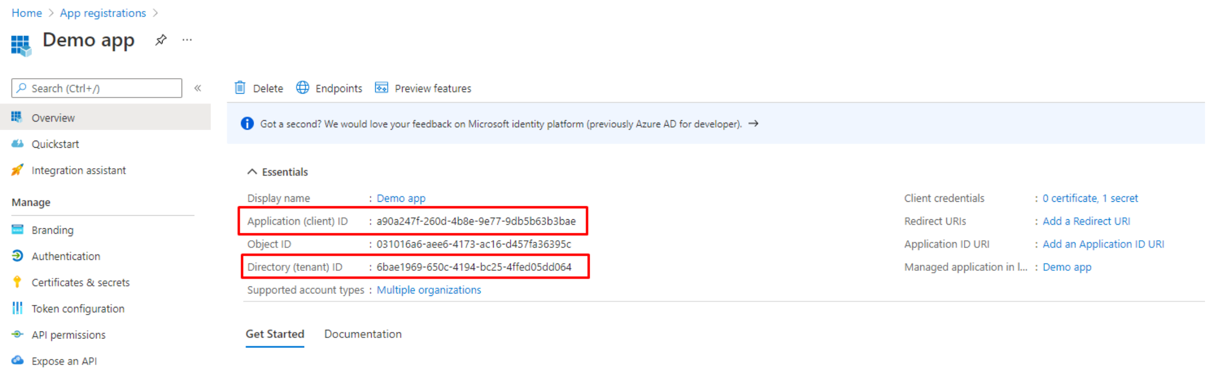
Remember that the secret is only available when it is created so make a copy of it before you move on.


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.

Description	Expires	Value	Secret ID
For demo	2021-11-20	Nr4-eD3y-T_~IFE4KW7-K_~bLa8ZZJhifk	311da14c-8027-42a9-bc4c-5e32088809ac

Now you have everything you need to start configuring your workflow. You can find the application (client) id and directory (tenant) id on the overview page.



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

Display name	: Demo app
Application (client) ID	: a90a247f-260d-4b8e-9e77-9db5b63b3bae
Object ID	: 031016a6-aee6-4173-ac16-d457fa36395c
Directory (tenant) ID	: 6bae1969-650c-4194-bc25-4ffed05dd064
Supported account types	: Multiple organizations
Client credentials	: 0 certificate, 1 secret
Redirect URIs	: Add a Redirect URI
Application ID URI	: Add an Application ID URI
Managed application in l...	: Demo app

Quick guide - Azure app registration

1) App registrations: New registration
    a) Any Azure AD - Multi tenant
2) Api permissions:
    a) Microsoft Graph
        i) Application.ReadAll
        ii) Directory.ReadAll
        iii) Domain.ReadAll
        iv) Group.ReadAll
        v) GroupMember.ReadAll
        vi) User.ReadAll
    b) Grant admin consent
3) Certificates & secrets: New client secret
    a) Value = secret
4) Overview
    a) Application (client) ID
    b) Directory (tenant) ID