Get app details and grant permissions to app registration

Provision App Registration

App Registrations are containers that allow user-independent permission assignment and are therefore ideally suited for automation. App Registrations can be created in Azure Portal \rightarrow Microsoft Entra ID \rightarrow App Registrations. App Registrations should be preferred to service accounts whenever possible.

The following variables are used to authenticate to the Graph API using application permissions. The ClientSecret must not be stored as clear text in scripts or applications under any circumstances, but must be stored in designated containers (e.g. Azure Runbook Credential Store, Azure Key Vault or Windows Credential Store).

Variables used

\$TenantID: This is the identity of the tenant, which is unique.

\$ClientID: The ClientID can be used to uniquely identify the App Registration.

\$ClientSecret: The ClientSecret expires every max. 24 months (2 years) and is like the password for the App Registration.

Read ClientID & TenantID

The ClientID & TenantID can be read out on the start page of the App Registration itself.

Home > BKW | App registrations >

🜉 AAP-RB-ALL-PERMISSION-ChangeHostnameByUPN-PROD 👒 😁

🔎 Search	« 📋 Delete 🕀 Endpoints 💀 Preview features
Reverview	∧ Essentials
📣 Quickstart	Dirplay name AAD. RE. ALL. PEDMISSION. ChangeHostnameRyl IDN. PPOD
🚀 Integration assistant	Application (client) ID
Manage	Object ID :
📰 Branding & properties	Directory (tenant) ID :
Authentication	Supported account types : <u>My organization only</u>
📍 Certificates & secrets	1 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication
Token configuration	
API permissions	Get Started Documentation
🙆 Expose an API	
15 App roles	
🚑 Owners	The Million of Identity of the sector of the
🚴 Roles and administrators	The Microsoft Identity platform is an authent
00 Manifest	
Support + Troubleshooting	
Troubleshooting	
New support request	

Create client secret

For the ClientSecret you have to switch to the "Certificates & Secrets" tab. A ClientSecret can be added via "New client secret". Then a name can be given there. **Attention:** Afterwards the ClientSecret is valid for 24 months (2 years) and expires after a certain time. In addition, the value is only displayed once. Save the ClientSecret as the first step in your password storage solution and note the expirationdate.

Manage	scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.							
Branding & properties								
Authentication	Application registration certificates, secrets and federated credentials can be found in the tabs below. X							
📍 Certificates & secrets								
Token configuration	Certificates (0) Client secrets (2) Federated credentials (0)							
→ API permissions	A serret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password							
Expose an API	reserve string that the upproxision uses to prove to harming which requesting a token rule can be retened to us upproxision passivola.							
App roles	+ New client secret							
24 Owners	Description	Expires	Value 🕕	Secret ID				
and administrators	second researcher.com	1000	Spectration and a	Series and series Office of	D 📋			
10 Manifest	Test for Screenshot	12/2/2024	tr.8Q~mNaCIPaWDirwBSy6D0gbPNdmd	e82c8ae9-60ba-4d32-9f57-0bf53b160d0f	r 🗊			
Support + Troubleshooting								
Troubleshooting								
New support request								

Grant permissions

As soon as the authentication via the app registration with the three values works, the permissions have to be assigned. This is a very tricky step, as an app could practically become a global administrator and overwrite or delete any tenant configurations.

The permissions on App Registrations for PowerShell Scripts must always be set to Application-Permissions, because the actions should be executed as App-Context.

Find the required permissions

The best way to find the required permissions is to visit the Microsoft Docs page for Graph API: Microsoft Graph REST API v1.0 endpoint reference - Microsoft Graph v1.0 | Microsoft Learn



Assign permissions

Once it has been determined which permissions need to be assigned, this can be done in Azure Portal \rightarrow Microsoft Entra ID \rightarrow App Registration \rightarrow API permissions.

First, "Add a permission" must be selected and then Microsoft Graph as an API resource.



Then it is important that "Application permissions" is selected. There you can then search for the corresponding permission from the Microsoft Docs page and add it using "Add permissions".

Request API permissions > Constructions Second Second

Consent assigned permissions

Now that the permission has been added thanks to the previous step, the last thing to do is to check it and then approve it. This can only be done with the "Global Administrator" role, as the app will then receive this permission forever and this is like assigning a role. The person who has Global Administrator must click on "Grand admin consent for <companyname>" in the app so that the permissions also become active.

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 J					
API / Permissions name	Туре	Description	Admin consent requ	Status	
✓ Microsoft Graph (3)					
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for ₩₩	•••
User.Read.All	Application	Read all users' full profiles	Yes	🛕 Not granted for 👘	
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	🛕 Not granted for 🛙 🔛	

Afterwards, the app can be used with the assigned permissions.

Revision #6 Created 2 December 2022 11:41:39 Updated 31 July 2025 07:48:53 by Luca Noah Caprez