

INFOTECH

[IT & Communication]

Automatisierung von Abläufen mit Microsoft Power Platform (u.a. Microsoft Power Apps) und MIP

Günter Krausgruber



- Power BI -> [Geschäfts]daten visualisieren
- Power Apps -> [Geschäfts]anwendungen (Low-code apps) entwickeln
- Power Pages -> [Geschäfts]websites erstellen
- Power Automate -> [Geschäfts]prozesse automatisieren
- Power Virtual Agents -> Chatbots entwickeln



- Power Apps (Apps = Applikationen) sind grundsätzlich für die Nutzung auf Smartphones und Tablets gedacht, sie funktionieren natürlich aber auch im Browser
- Mit Microsoft Power Apps können Applikationen entwickelt und geteilt werden
 - Lizenz: Power Apps per user plan
 - create, customize, share, run/use
 - unbegrenzte Anzahl von Power Apps
 - Lizenz: Power Apps per app plan
 - use
 - eine ganz bestimmte „shared“ Power App
- Entwickeln soll schnell, einfach und mit wenig Code erfolgen
- Low-code: JA, für aufwendigere und „coole“ Sachen: NEIN



- Microsoft Graph [RESTful Web API]
 - Standardisierte Schnittstelle für Microsoft Cloud Dienste, wie



Bildquelle: <https://learn.microsoft.com/en-us/graph/overview>

- Abfragen und Zugriffe sind schnell (wirklich schnell)



- Was ist erforderlich, um die Microsoft Graph API mit Power Apps (oder Power Automate) nutzen zu können
 - Applikation (Service Principal) in Azure Active Directory registrieren
 - Custom Connector erstellen



Power Apps Microsoft Graph Applikation in Azure AD registrieren

- Application/Client ID, Directory/Tenant ID

PowerApp MFA external Users

Search << Delete Endpoints Preview features

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest

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

Essentials

Display name : [PowerApp MFA external Users](#)

1 Application (client) ID [Redacted]

Object ID [Redacted]

Directory (tenant) ID [Redacted]

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

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL)

[Get Started](#) [Documentation](#)

The Microsoft identity platform is an authentication service



Power Apps Microsoft Graph Applikation in Azure AD registrieren

- Client secret (Zugangspasswort)

PowerApp MFA external Users | Certificates & secrets

Search

Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets 2
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

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.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

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
PowerPlatform	4/28/2024	[REDACTED]	[REDACTED]



Power Apps Microsoft Graph Applikation in Azure AD registrieren

- API permissions

PowerApp MFA external Users | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions 3
Expose an API
App roles
Owners
Roles and administrators
Manifest

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This d

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 shows all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for [REDACTED]

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for
UserAuthenticationMethod.ReadWrite.All	Delegated	Read and write all users' authentication methods.	Yes	✓ Granted for

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



Power Apps Microsoft Graph Custom Connector in Power Apps erstellen

- Authentifizierung festlegen

OAuth 2.0

Identity Provider
Azure Active Directory

Client id *
Client id 1

Client secret *
***** 2

Login URL
https://login.windows.net

Tenant ID
common

Resource URL *
Resource URL

Enable on-behalf-of login
false

Scope
User.Read.All, UserAuthenticationMethod.ReadWrite.All 3

Redirect URL
https://global.consent.azure-apim.net/redirect

Edit



Power Apps

Microsoft Graph

Custom Connector in Power Apps erstellen

- Microsoft Graph API-Zugriffe definieren

The screenshot shows the Microsoft Graph API Explorer interface for the connector 'MSGraphMFAForExternalUsers'. The base URL is 'graph.microsoft.com/'. The 'Schemes' dropdown is set to 'HTTPS'. An 'Authorize' button is visible. The 'default' environment is selected. The API endpoints are listed as follows:

Method	Endpoint	Description	Lock
GET	/v1.0/users	Get All External Users	Yes
GET	/beta/users/{userPrincipalName}/authentication/phoneMethods/3179e48a-750b-4051-897c-87b9720928f7	Get Phone Authentication Method	Yes
PUT	/beta/users/{userPrincipalName}/authentication/phoneMethods/3179e48a-750b-4051-897c-87b9720928f7	Update Phone Authentication Method	Yes
POST	/beta/users/{userPrincipalName}/authentication/phoneMethods	Add new Phone Authentication Method	Yes



- Ziel: Externe Benutzer sollen das MFA-Einrichtungssetup nicht durchlaufen müssen, Standard MFA-Methode sowie Telefonnummer werden bereits bei der Benutzeranlage festgelegt

The screenshot shows the 'Authentication methods' page for a user named 'Test Extern'. The left sidebar contains navigation options: Overview, Audit logs, Sign-in logs, Diagnose and solve problems, and a 'Manage' section with Custom security attributes (preview), Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, and Authentication methods (highlighted). The main content area has a search bar and action buttons: '+ Add authentication method', 'Reset password', 'Require re-register multifactor authentication', and 'Revoke multifactor authentication sessions'. A blue information banner asks: 'Want to switch back to the old user authentication methods experience? Click here to go back. →'. Below this, a text block states: 'Authentication methods are the ways your users sign into Azure AD and perform SSPR.' A section titled 'Usable authentication methods' contains a table with two columns: 'Authentication method' and 'Detail'. One row is highlighted in yellow, showing 'Phone number' and '+43 12345688'.

Authentication method	Detail
Phone number	+43 12345688



- Beispiel: MFA (Multi-Faktor-Authentifizierung) für externe Benutzer festlegen
 - Standard MFA-Methode für Benutzer festlegen
 - Im konkreten Fall: „Telefonnummer“ als Standard-Authentifizierungsmethode
 - Umsetzung mit Power Automate und Power Automate Desktop
 - PhoneAuthenticationMethod, d.h. die eigentliche Telefonnummer setzen oder updaten
 - Beispiel: +43 67612345678
 - Umsetzung mit Microsoft Graph



- Beispiel: Automatisierte Benutzeranlage
 - Benutzerdaten aus ERP-System des Kunden via REST/JSON entgegennehmen
 - Benutzer mit den erhaltenen Attributen im lokalen Active Directory (AD) anlegen oder updaten
 - Office 365 Mailbox für bestehenden On-premises AD Benutzer anlegen
 - Benutzerdatenblatt befüllen (Vor-/Nachname, E-Mail-Adresse, Benutzererstpasswort, Vorgesetzte/r etc.) und das erzeugte Word-Dokument der HR-Abteilung zur Verfügung stellen
 - Aus verschiedenen Word-Vorlagen wird dabei je nach Anstellungsverhältnis (fixer Mitarbeiter, Leasing, Lehrling etc.) das entsprechende Dokument ausgewählt und befüllt
 - Fertiges Dokument wird in MS Teams und SharePoint der HR-Abteilung bereitgestellt



- Beispiel 1: Dokumente in SharePoint-Site (Dokumentenbibliothek) schützen
 - Dokumente, die in eine bestimmte SharePoint-Dokumentenbibliothek hochgeladen werden, mittels MIP Sensitivity Label automatisiert schützen
 - Innerhalb vom Label können unterschiedliche Verwendungsrechte festgelegt werden z.B.
 - Benutzer 1 darf das Dokument nur ansehen, jedoch nicht drucken oder ändern
 - Benutzer 2 erhält Vollzugriffsrechte, d.h. Dokument ansehen, ändern etc.
- Beispiel 2: MFA bei Zugriff auf bestimmte SharePoint Site aktivieren

