empower suite

Version: December 2024

Content

1. TECHNICAL BACKGROUND

1.1 What is a Microsoft Entra ID App Registration and which permissions are required?

The App Registration serves as a relay and allows you to sign in to empower® via Entra ID. Furthermore, we also refer to empower® as a *Software as a Service* (short SaaS) solution.

In principle, an administrator consent is granted for exactly the permissions that are set. empower® requires the permissions **User.Read**, **User.Read.All** and **GroupMember.Read.All** (the latter is optional).

User.Read *[Type – Delegated]*	Sign in and read user profile	Allows an application to read the profile information of the signed-in user. This includes details like the user's name, email address, and other basic profile information.
User.Read.All *[Type – Application]*	Read all users' full profiles	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.
GroupMember.Read.All *[Type – Application]*	Read all group memberships	Allows the app to list groups and read their properties and all group memberships on behalf of the signed-in user. It also allows the app to read calendars, conversations, files, and other group content for all groups the signed-in user can access.

Source (Microsoft): https://learn.microsoft.com/en-us/graph/permissions-reference

These permissions are required by empower® to provision users and groups from the Entra ID to empower®. A background service runs on the application server at regular, configurable intervals that retrieves users and groups from Entra ID and makes them available in empower®. Users synchronized in this way can sign in to empower® through Entra ID as an authentication provider and use empower®.

The synchronized groups are used to assign permissions within the empower® library at group level. The synchronization of the groups can optionally be omitted (see above). A permission assignment is only possible directly at user level or to all empower® known users. Which users and groups are synchronized exactly can be configured using appropriate filters based on group memberships or other attributes (e.g., prefix of the group name).

As an alternative to this synchronization process initiated by empower®, we also offer user provisioning via SCIM (System for Cross-Domain Identity Management) (see https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/how-provisioning-works). In this case, users and groups are pushed from Entra ID to empower® and the above-mentioned authorization assignment is omitted.

1.2 General Information about SCIM

SCIM stands for *System for Cross-Domain Identity Management* and is an open standard protocol for automating the exchange of user identity information between identity domains and IT systems. SCIM ensures that employees added to the Human Capital Management (HCM) system automatically receive accounts in Entra ID or Windows Server Active Directory. User attributes and profiles are synchronized and updated or removed when there are status or role changes. Unlike the previously used Directory Sync, SCIM does not actively query information but automatically provides it when there are changes to the information to be transferred.

1.1.1 Advantages of SCIM

- empower® does not require any authorizations to retrieve users or groups from the user directory (Entra ID). There is only a registration of the app, which does not require direct access to the directory data.
- Provisioning is configured directly in the directory service by the customer, enabling targeted and needs-based management of user accounts.
- The directory service itself is not regularly loaded, as the resources are located at Microsoft. Instead, the empower® backend is loaded by an additional service that only becomes active when changes are made.

1.1.2 How SCIM works

Unlike Directory Sync, SCIM works according to a PUSH procedure. In contrast to the directory sync process, the data is not actively queried. With SCIM, changes to users or user groups are automatically forwarded to empower®.

Entra ID App Registration & SCIM Setup

2. APP REGISTRATION

To perform the app registration, a package is provided that enables the installation via script and automates the entire process. The package contains two PowerShell scripts, a script that is used to create the app registration and an optional script that is only executed when empower® Mails Online is used. The third file is a config file that is used to define important parameters for the registration script in advance to speed up the process.

config.json, which is important for the script’s setup. Typically, the support team has already customized this file for the app.

The config.json file looks like this:

```
{
   "tenantID": "",
   "appName": "",
   "hostname": "https://",
   "useMailsOnline": false,
   “oneTimePasswordServiceUri": "”
 }
```

tenantID: The tenant ID must be provided by you.
appName: The name of the application.
hostname: The base URL of the application.
useMailsOnline: Boolean value to indicate if the empower® Mails Online configuration is to be used
oneTimePasswordServiceUri: The URI of the One-Time-Password service. You have the option to use one of the following One-Time-Password services as an entry: https://onetimepass.domaincrawler.com/ or https://snappass.symplasson.de/

EntraIdAppRegistration.ps1	This script is used for app registration.
EntraIdAppRegistration_MailsOnline.ps1	This script is optional and only used for configuring empower® Mails Online

You can use the script to ease the App Registration that is required for empower®.

Please download the script here: PowerShell Script App Registration empower®

This PowerShell script can be used to automatically create the App Registration required for empower® in the Entra ID via PowerShell or Cloud Shell.

Please note:

The PowerShell script we provide is compatible with the Microsoft Graph PowerShell module version 2.19.0.

Please note:

Please either use the PowerShell script or Cloud Shell to create the App Registration.

2.1 Use in PowerShell

Prerequisite is to install the MS Graph PowerShell module: [Install PowerShell]()

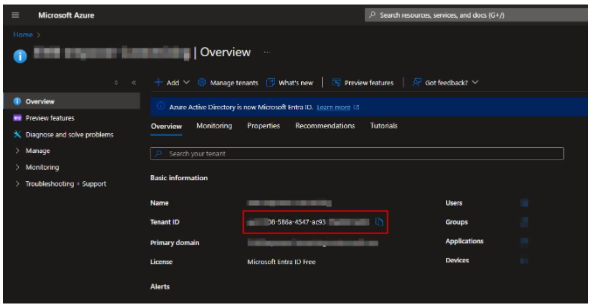
Preparation

1. Make sure MS Graph PowerShell module is installed
2. Unpack the given zip-Folder
3. Open PowerShell as Admin in the unpacked folder

Execution

1. Execute the script EntraIdAppRegistration.ps1 in the path where it is located **PowerShell: .\EntraIdAppRegistration.ps1**
2. Using the configuration values. The script will use the values from the config.json file as default values.
3. Enter the TenantID or confirm the default value from the config file. This can be found, for example, in the Entra

   Please enter your Microsoft Entra ID TenantID **[Default: Tenant Id from EntraID]** *(Use Enter for the default value):*



Azure Active Directory is now Microsoft Entra ID. Learn more

Basic information

Name [redacted]

Tenant ID [redacted]08-586a-4547-ac93 [redacted]

Primary domain [redacted]

License Microsoft Entra ID Free

Users [redacted]

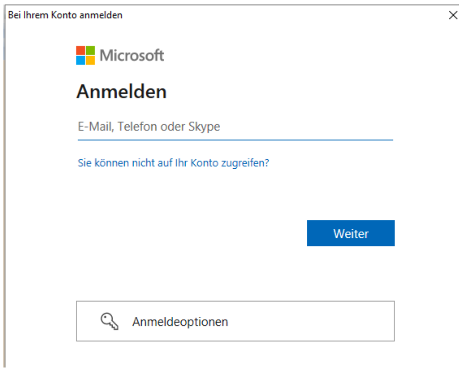
Groups [redacted]

Applications [redacted]

Devices [redacted]

Alerts

4. The Microsoft login window is triggered. Log in with a user who has access to the VM.


Bei Ihrem Konto anmelden
Microsoft
Anmelden
E-Mail, Telefon oder Skype
Sie können nicht auf Ihr Konto zugreifen?
Weiter
Anmeldeoptionen

5. Enter the name for the app registration or confirm the default value from the config file.

   Please enter the wanted name for the App Registration, e.g. **empower**.

6. Enter the URL (must start with *https://*) and use the *DNS Name* provided by your Onboarding Specialist or Customer Success Manager. Confirm with **Enter**.

   Please enter the wanted name for the App Registration, e.g.
   empower [Default: empower]
   (Use enter for the default value).

7. Next, you will be asked whether the configuration of empower® Mails Online should be activated. Press **Enter** for the default value (already configured by the support team) or type in your desired value (true or false).

8. The app registration will now be created automatically and the required data for the backend installer will be shown:

```
> Finished

Copy the details from here or find the needed details in the file AppRegistrationInfo.json, in the current folder


TenantId     : 415660fd-25c9-45a5-94de-0f632fbeb47j
clientId    : f59b7877-67bb-4ea3-8159-6ef9c7873395

Example link (Snappass optionl):
https://snappass.symplasson.de/snappassc41ba9c2cf4e4112b67a4f44ce443441~OVNAVAoPOKhYB3hJs0UN9bYpCikKSHEqc_JforilSTI%3D
```

9. A json file (*AppRegistrationInfo.json*) is written into the current folder which also contains the data for the backend installer. Save the values TenantID, ClientID, and Client Secret securely.

```
{
        "TenantId":  "415660fd-25c9-45a5-94de-0f632fbeb47j",
        "clientId":  "f59b7877-67bb-4ea3-8159-6ef9c7873395",
        "clientSecret":  "https://snappass.symplasson.de/snappassc41ba9c2cf4e4112b67a4f44ce443441~OVNAVAoPOKhYB3hJs0UN9bYpCikKSHEqc_JforilSTI%3D",
        "createDateClientSecret":  "21.06.2024",
        "expirationDateClientSecret":  "21.06.2124"
}
```

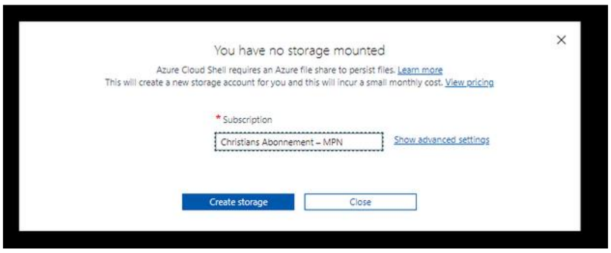
10. To open the Client Secret (the secret client key), open the Snappass link in the browser. The link is valid for one month, but can only be opened once.

11. Please send us the Client Secret afterwards.

2.2 Use in Cloud Shell

First of all, you should be connected to the tenant (portal.azure.com) in which you want to create the app registration.

In the browser, enter shell.azure.com. If you use the Cloud Shell for the first time, the following dialog appears.



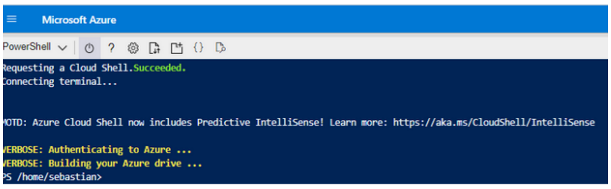
You have no storage mounted

Azure Cloud Shell requires an Azure file share to persist files. Learn more
This will create a new storage account for you and this will incur a small monthly cost. View pricing

* Subscription: Christians Abonnement – MPN

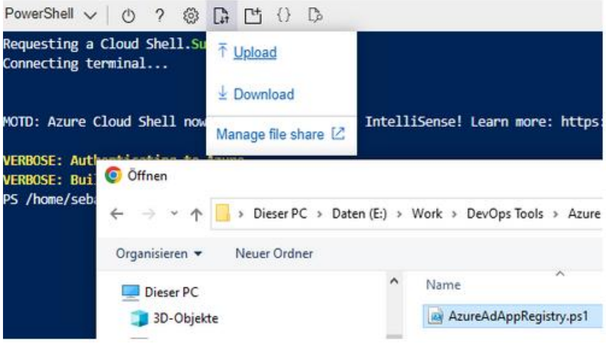
A subscription must then be selected and **Create storage** clicked. A storage account for the cloud shell is then created.

After that the cloud shell appears, please select **PowerShell** here.

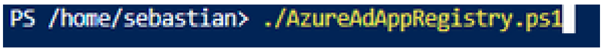


```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...


MOTD: Azure Cloud Shell now includes Predictive IntelliSense! Learn more: https://aka.ms/CloudShell/IntelliSense

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/sebastian>
```

Via the highlighted icon you can upload the script to the Cloud Shell.



Then, as in PowerShell, simply call the script.

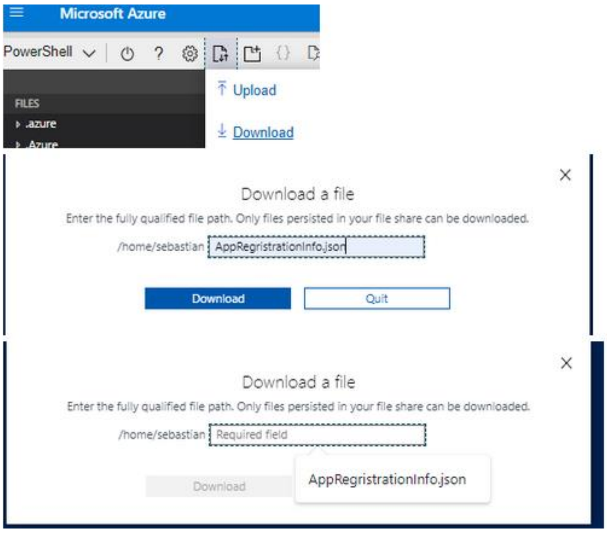


```
PS /home/sebastian> ./AzureAdAppRegistry.ps1
```

Here, the same entries are to be made as above for the PowerShell, but the TenantID is omitted and a new login is also not necessary.

You only have to enter the name and the URL of empower® and if you want to configure empower® Mails Online.

When the script has run through, you can download the *AppRegistration.json* file with the app registration information via **Download**.



Download a file

Enter the fully qualified file path. Only files persisted in your file share can be downloaded.

/home/sebastian AppRegristrationInfo.json

Download a file

Enter the fully qualified file path. Only files persisted in your file share can be downloaded.

/home/sebastian Required field

Alternatively, the information is displayed on the screen again.

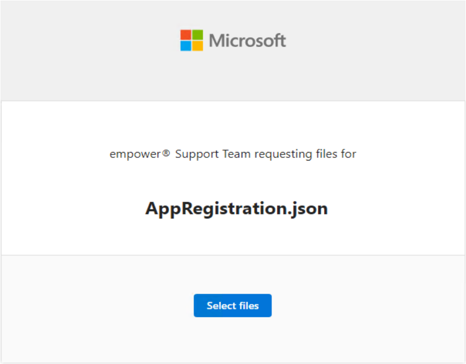
2.3 Provide empower® with the *AppRegistrationInfo.json*

Once the script is run and you have received the *AppRegistrationInfo.json*, please send over the file to your Onboarding Specialist or Customer Success Manager.

Your Onboarding Specialist or Customer Success Manager has asked for your *AppRegistrationInfo.json* via OneDrive, where you can upload your file.

Please follow the steps:

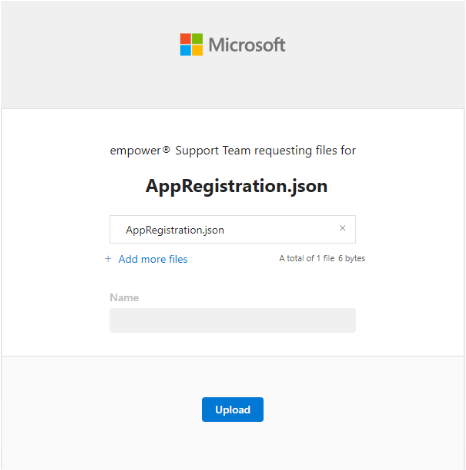
Click on **Upload files** in the e-mail you have received from your Onboarding Specialist or Customer Success Manager.


Microsoft

empower® Support Team requesting files for

AppRegistration.json

Browse through your device, select your file and click on **Upload**.

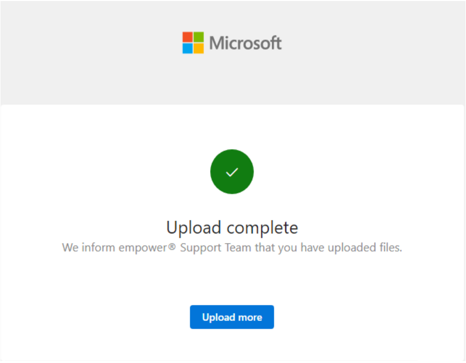

Microsoft

empower® Support Team requesting files for

AppRegistration.json

AppRegistration.json

Your upload has been completed and your Onboarding Specialist or Customer Success Manager will be informed via e-mail.


Microsoft

Upload complete

We inform empower® Support Team that you have uploaded files.

2.4 Additional Information for empower®

In addition to the *AppRegistrationInfo.json*, please provide empower® with the following information:

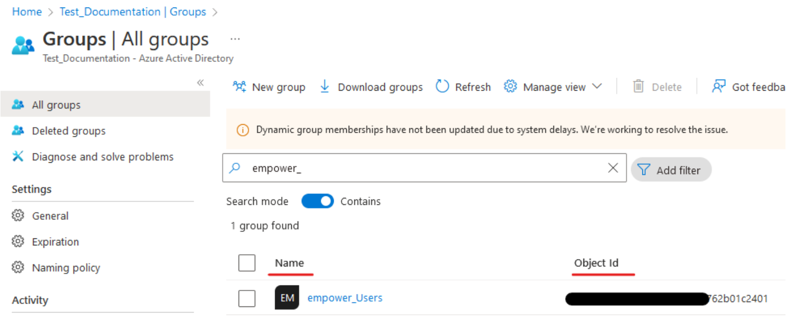
Property	Value
empower® Group Object ID	
Entra ID Group displayName	
Expiry date Client Secret*	

*You will receive a reminder from empower® before your current Client Secret expires.

empower® Group Object ID:
This ID is a globally unique identifier (GUID), more precisely, an Entra ID User Group, which is used to synchronize users to empower®. This way, we ensure that not your complete Entra ID Tenant is synchronized to empower®, but only the users that will work with empower®.

EntraGroup displayName:
In empower®, in order to grant permissions within empower®, not only users but also groups are synchronized. Therefore, it is useful to work with empower® groups or with groups that can be clustered together via name.

For example, empower® user group = **empower_users**; empower® admin group = **empower_adminusers**. This way, we can apply the permissions in empower® directly to the Entra ID groups.



Dynamic group memberships have not been updated due to system delays. We're working to resolve the issue.

empower_

Search mode ● Contains

1 group found

□	Name	Object Id
□	EM empower_Users	[redacted]62b01c2401

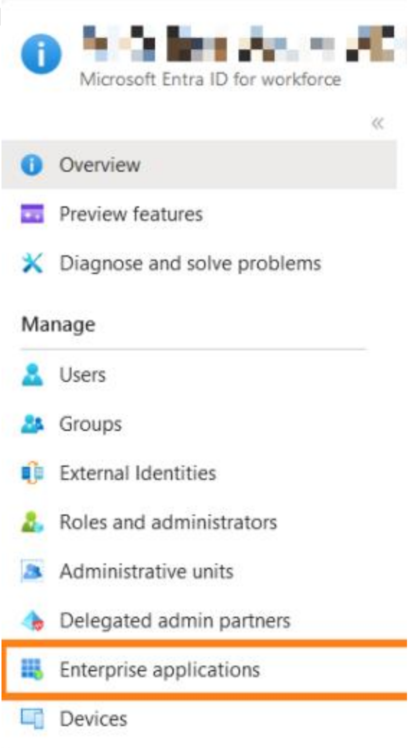
3. SET UP SCIM IN AZURE

3.1 Setting up the SCIM API

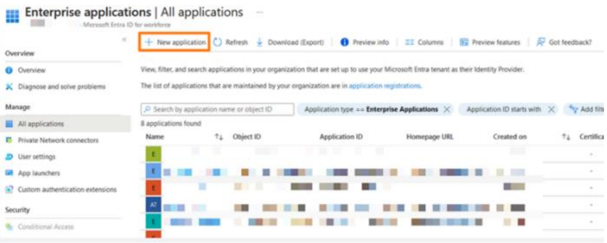
An app registration must first be made in the Azure portal. The creation of this app registration is described below.

> **Please note:**
>
> These steps must be carried out **before** using the empower® backend setup Installer.

1. Search for Microsoft Entra ID in the Azure portal and select the service.



2. Select the **Enterprise applications** tab in the bar on the left.
3. Click on the **New application** button.


Enterprise applications | All applications
Microsoft Entra ID for workforce
+ New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
Overview
Overview
Diagnose and solve problems
Manage
All applications
Private Network connectors
User settings
App launchers
Custom authentication extensions
Security
Conditional Access
Search by application name or object ID
Application type == Enterprise Applications
Application ID starts with
Add filt

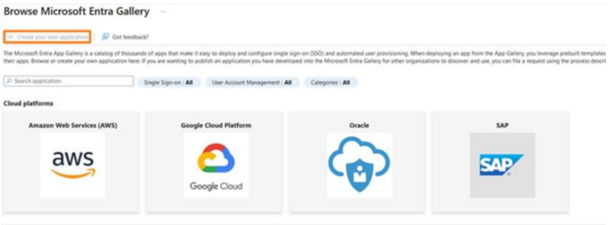
View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

8 applications found

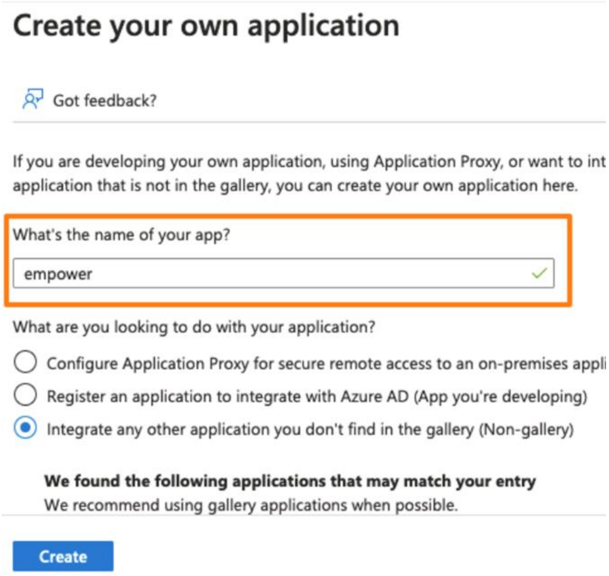
Name	Object ID	Application ID	Homepage URL	Created on	Certifica
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	-
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	-
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	-
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	-
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	-

4. Click on the **Create your own application** button.



The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process descri

5. Enter a name for the application.
6. Click on the **Create** button.



Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to int application that is not in the gallery, you can create your own application here.

What's the name of your app?

empower

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises appli
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

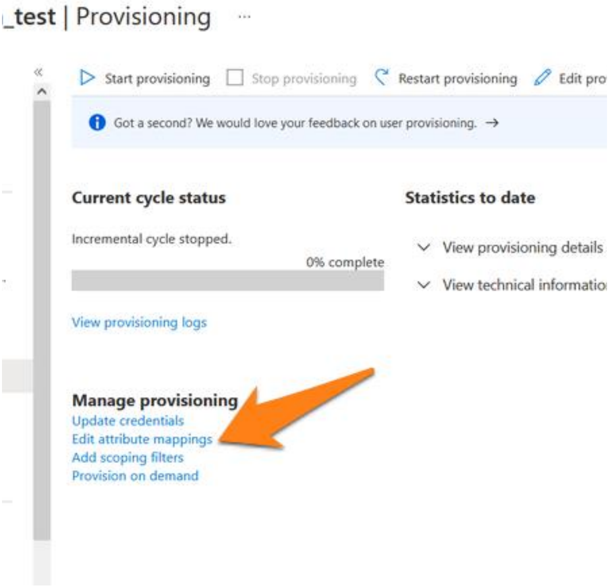
We found the following applications that may match your entry
We recommend using gallery applications when possible.

3.2 Editing the attribute mappings

To set up SCIM, it is also necessary to adjust the attribute mappings. This is not necessary for the Directory Sync. There are two attribute mappings in the Mappings section: one for users and one for groups.

The standard attribute mappings must be adapted for empower®. To do this, proceed as follows:

1. Also under Provisioning in the Manage Provisioning section, click **Edit Mappings**.



_test | Provisioning

Got a second? We would love your feedback on user provisioning. →

Current cycle status

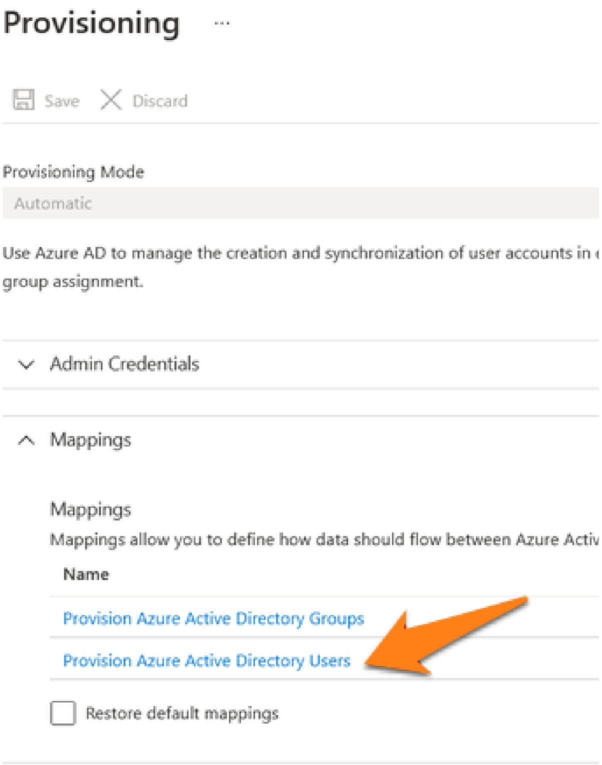
Incremental cycle stopped.

0% complete

Statistics to date

Manage provisioning

2. Then click on the **Provision Azure Directory Users** link in the Mappings section.



Provisioning ...

Save Discard

Provisioning Mode

Automatic

Use Azure AD to manage the creation and synchronization of user accounts in group assignment.

Admin Credentials

Mappings

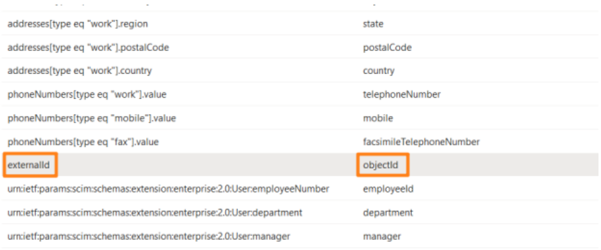
Mappings

Mappings allow you to define how data should flow between Azure Activ

Name
Provision Azure Active Directory Groups
Provision Azure Active Directory Users

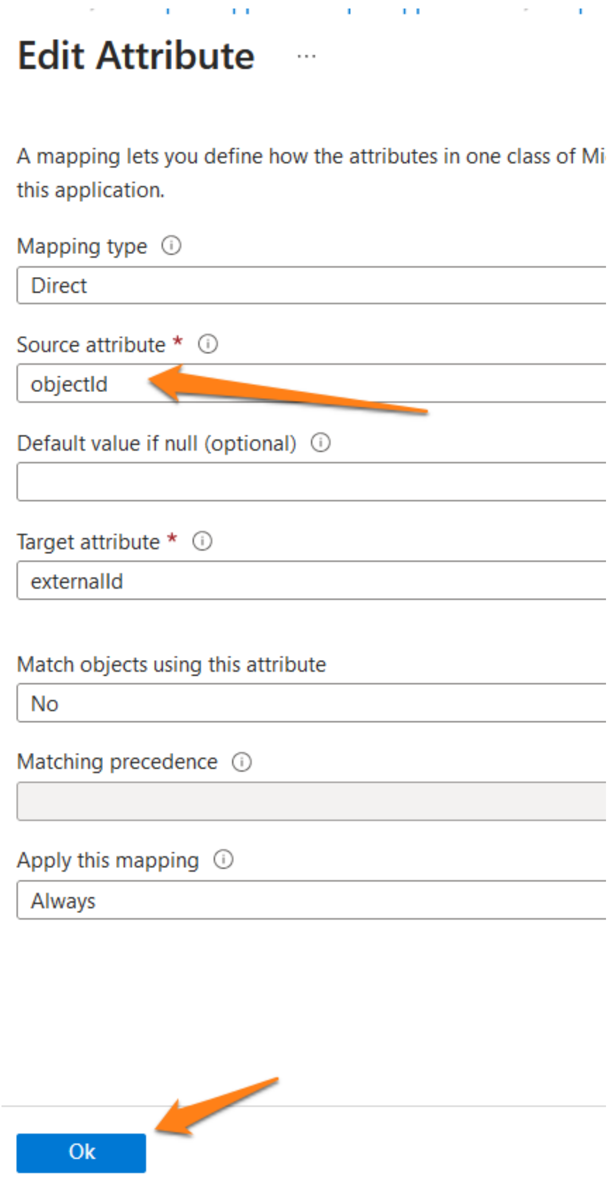
□ Restore default mappings

3. Change the mapping to externalId to objectId. By default, the email nickname is usually used here.



addresses[type eq "work"].region	state
addresses[type eq "work"].postalCode	postalCode
addresses[type eq "work"].country	country
phoneNumbers[type eq "work"].value	telephoneNumber
phoneNumbers[type eq "mobile"].value	mobile
phoneNumbers[type eq "fax"].value	facsimileTelephoneNumber
externalId	objectId
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber	employeeId
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department	department
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager	manager

4. Click on **Ok**.



Edit Attribute

A mapping lets you define how the attributes in one class of Mi
this application.

Mapping type: Direct

Source attribute *: objectId

Default value if null (optional):

Target attribute *: externalId

Match objects using this attribute: No

Matching precedence:

Apply this mapping: Always

5. When you have completed the configuration, set the Provisioning Status to **On**.

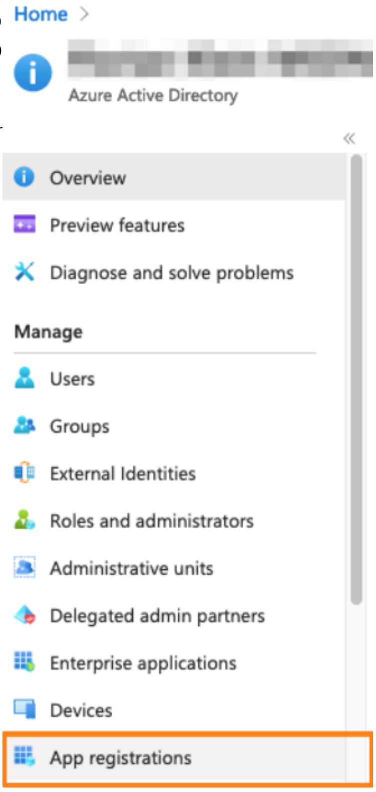
6. To activate the Entra ID provisioning service, click **Save**.

3.3 Saving the values for the Enterprise Application

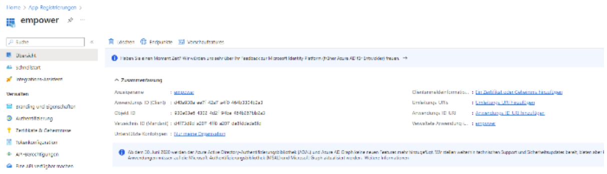
For the installation of the empower® backend, the values Application ID and Directory ID are required in the backend installer. It therefore makes sense to save these values when creating the Enterprise Application. To do this, proceed as follows:

1. After creating the Enterprise Application, switch to the general overview of the Microsoft Entra ID directory.
2. Then select the **App registrations** tab in the bar on the left.

The newly created Enterprise Application is now displayed.



3. Select the Enterprise Application you have just created. You will be redirected to the application-specific overview.



Haben Sie einen Moment Zeit? Wir würden uns sehr über Ihr Feedback zur Microsoft Identity Platform (früher Azure AD für Entwickler) freuen. →

Anzeigename : empower
Anwendungs-ID (Client) : [illegible]
Objekt-ID : [illegible]
Verzeichnis-ID (Mandant) : [illegible]
Unterstützte Kontotypen : Nur meine Organisation
Clientanmeldeinformatio... : Ein Zertifikat oder Geheimnis hinzufügen
Umleitungs-URIs : Umleitungs-URI hinzufügen
Anwendungs-ID-URI : Anwendungs-ID-URI hinzufügen
Verwaltete Anwendung i... : empower

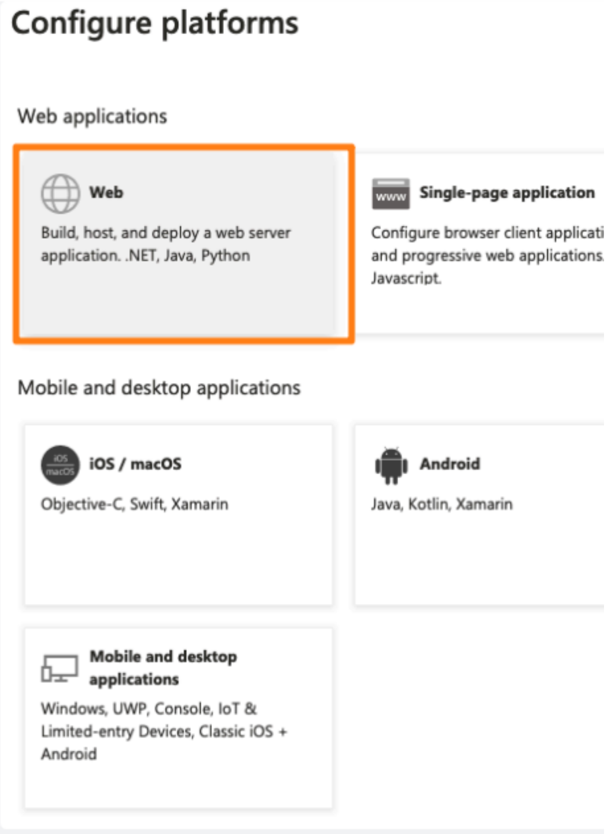
Ab dem 30. Juni 2020 werden der Azure Active Directory-Authentifizierungsbibliothek (ADAL) und Azure AD Graph keine neuen Features mehr hinzugefügt. Wir stellen weiterhin technischen Support und Sicherheitsupdates bereit, bieten aber [illegible] Anwendungen müssen auf die Microsoft-Authentifizierungsbibliothek (MSAL) und Microsoft Graph aktualisiert werden. Weitere Informationen

4. Save the **Application (client) ID (application ID)** and the **Directory (tenant) ID (directory ID)**.

3.4 Redirection URIs

Redirection URIs are necessary so that Azure knows where the user should be redirected after successful authentication. To ensure that the URIs are known, they must be defined beforehand. To do this, proceed as follows:

1. Select the Authentication tab in the bar on the left of the application-specific overview.
2. Click on the **Add a platform button**.
3. Under **Web applications**, select the Web option.



Configure platforms

Web applications

Web
Build, host, and deploy a web server application. .NET, Java, Python
Single-page application
Configure browser client applicati and progressive web applications. Javascript.
Mobile and desktop applications
iOS / macOS
Objective-C, Swift, Xamarin
Android
Java, Kotlin, Xamarin
Mobile and desktop applications
Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

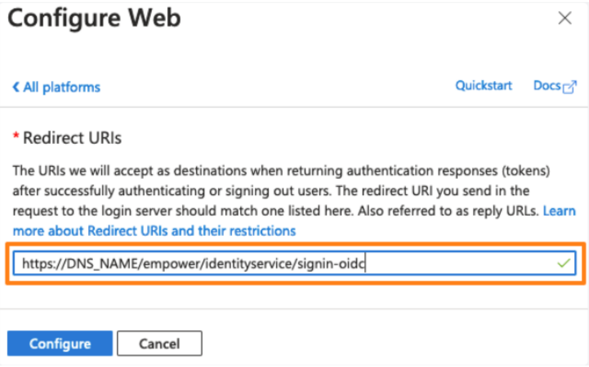
4. On the **Redirect URIs page**, enter the first of the following three redirect URIs for your empower® environment:

https://[DNS_Name]/empower/identityservice/signin-oidc

https://[DNS_Name]/empower/identityservice/grants

https://[DNS_Name]/empower/identityservice

[DNS_NAME] corresponds to the DNS name of your empower® environment. The remaining two URIs are added in the following steps.

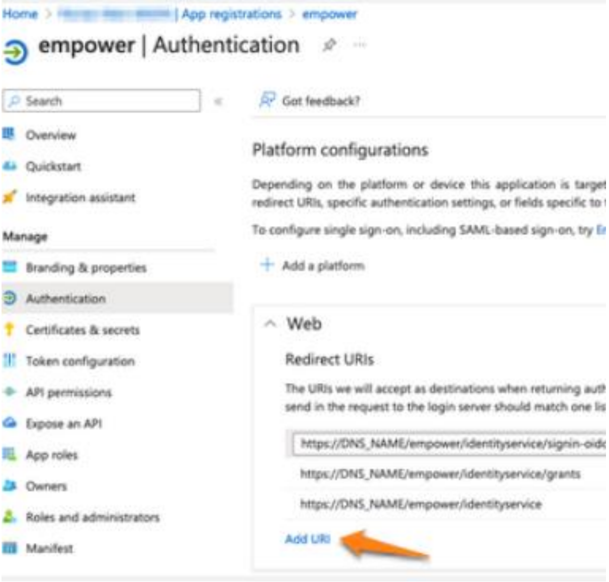


* Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://DNS_NAME/empower/identityservice/signin-oidc

5. Click on the **Configure button**. Further redirection URIs can now be added under **Web**.



Depending on the platform or device this application is target redirect URIs, specific authentication settings, or fields specific to

To configure single sign-on, including SAML-based sign-on, try En

The URIs we will accept as destinations when returning auth send in the request to the login server should match one lis

https://DNS_NAME/empower/identityservice/signin-oidc

https://DNS_NAME/empower/identityservice/grants

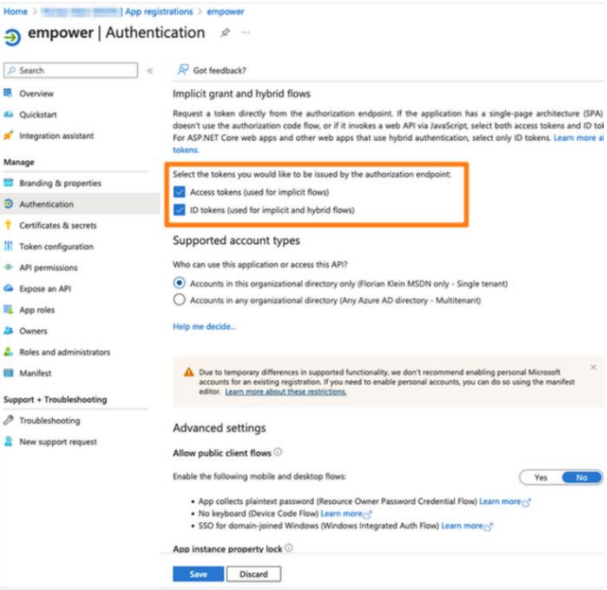
https://DNS_NAME/empower/identityservice

6. To add the two missing URIs, click on **Add URIs**.

3.5 Activate Implicit Flow

Implicit Flow is used as the login method for empower® **up to and including version 9.2**. Implicit Flow must therefore be activated in the Azure portal.

1. Also activate the *Implicit Flow* in the *Authentication* tab by activating the **Access tokens** and **ID tokens** option.



Home > [redacted] | App registrations > empower

empower | Authentication

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tok For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more a tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Florian Klein MSDN only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: Yes [✓ No]

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

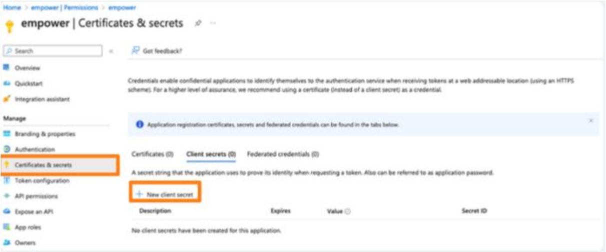
App instance property lock

2. Click on the **Save** button.

3.6 Client Secret

empower® also requires a valid client secret (secret client key) to be able to perform the user login. Set up a client secret in the following step.

1. Select the **Certificates and Secrets** tab in the bar on the left of the application-specific overview.



Home > empower | Permissions > empower

empower | Certificates & secrets

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.

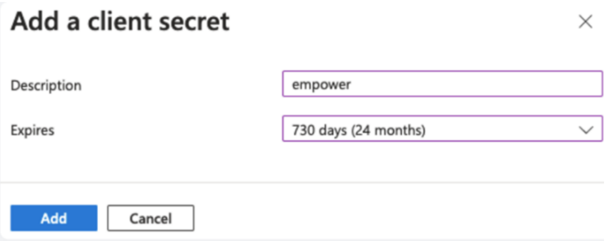
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

2. Click on the **News client secret** button.

3. Enter a description for the new client secret.



Add a client secret

Description: empower

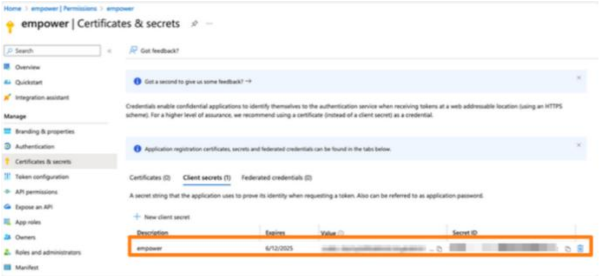
Expires: 730 days (24 months)

4. Determine the validity of the client secret according to the guidelines of the client company.

5. Click on the **Add** button.

6. Copy the Client Secret and save it.

> **Please note:**
>
> The client secret is only visible once!



Home > empower | Permissions > empower

empower | Certificates & secrets

Got a second to give us some feedback? →

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
empower	6/12/2025	[redacted]	[redacted]

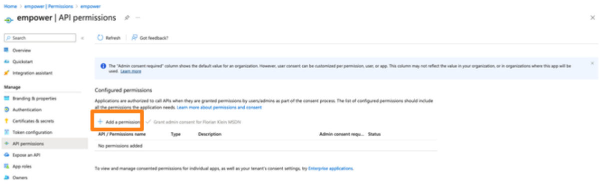
3.7 Necessary API authorization

Then adjust the permissions for the application. Adjusting the permissions allows empower® to read the user and user groups from the directory. The following describes how to set the User.Read to successfully set up the user login.

The following permission is always required for the user login:

- *User.Read*

1. Select the API permissions tab in the bar on the left of the application-specific overview.
2. Click on the **Add a permission** button.



Home > empower | Permissions > empower

empower | API permissions

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

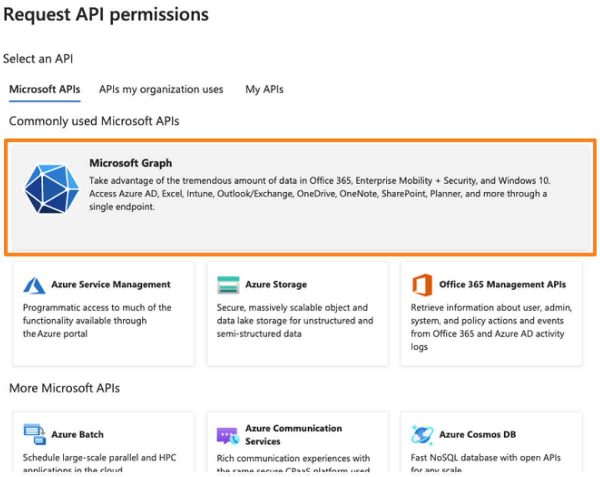
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for Florian Klein MSDN

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

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

3. Select **Microsoft Graph**.



Request API permissions

Select an API

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 Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

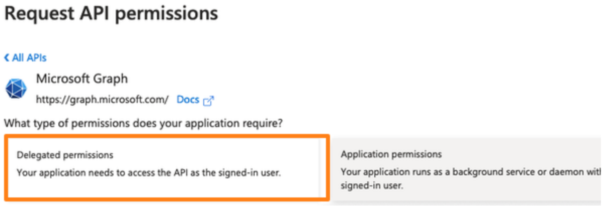
More Microsoft APIs

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Communication Services
Rich communication experiences with the same secure CPaaS platform used

Azure Cosmos DB
Fast NoSQL database with open APIs for any scale

4. Repeat the process and now select **Delegated permissions**.



Request API permissions

‹ All APIs

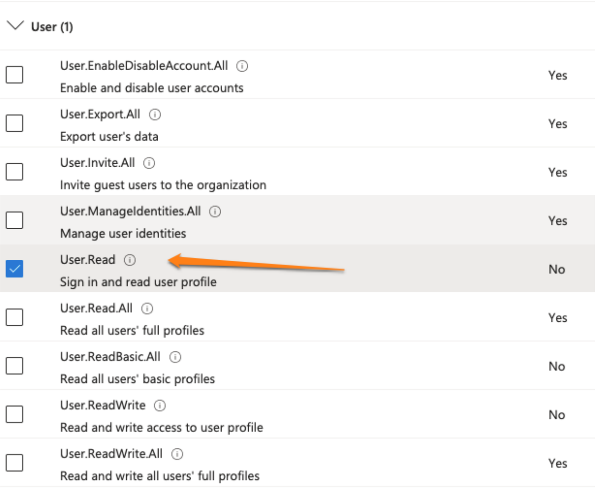
Microsoft Graph
https://graph.microsoft.com/ Docs

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 wit
signed-in user.

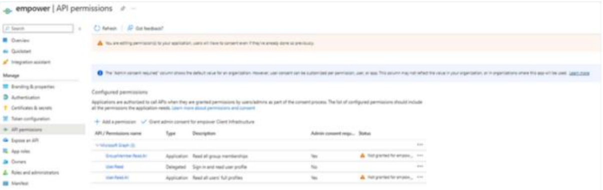
5. In the following list, activate *User.Read*.



User (1)

□	User.EnableDisableAccount.All Enable and disable user accounts	Yes
□	User.Export.All Export user's data	Yes
□	User.Invite.All Invite guest users to the organization	Yes
□	User.ManageIdentities.All Manage user identities	Yes
☑	User.Read Sign in and read user profile	No
□	User.Read.All Read all users' full profiles	Yes
□	User.ReadBasic.All Read all users' basic profiles	No
□	User.ReadWrite Read and write access to user profile	No
□	User.ReadWrite.All Read and write all users' full profiles	Yes

6. Click on the **Add permissions** button. You will return to the overview page.



API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
GroupMember.Read.All	Application	Read all group memberships	Yes	Not granted for empow...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for empow...

3.8 Endpoint setting for SCIM

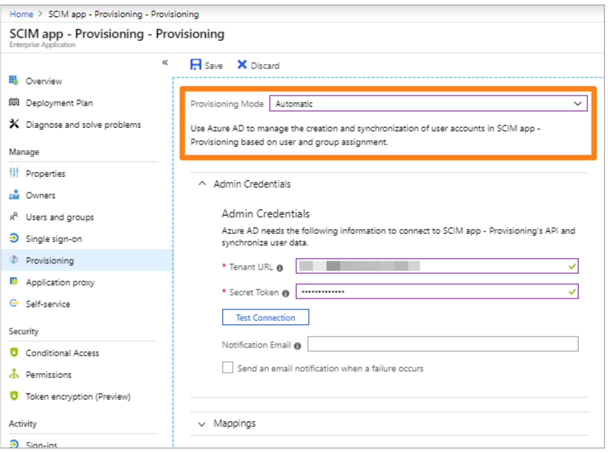
This section explains how to set the endpoint for SCIM provisioning to which the user elements are to be synchronized.

Please note:

These settings can only be made after the empower® backend setup Installer has been unsed and SCIM has been set up.

If you want to use SCIM as provisioning method, proceed as follows:

1. Switch to the application-specific overview.
2. Select the Provisioning tab in the bar on the left on the application-specific overview.
3. For Provisioning Mode, select **Automatic** from the drop-down menu.



Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in SCIM app - Provisioning based on user and group assignment.

Admin Credentials

Azure AD needs the following information to connect to SCIM app - Provisioning's API and synchronize user data.

* Tenant URL: [redacted]

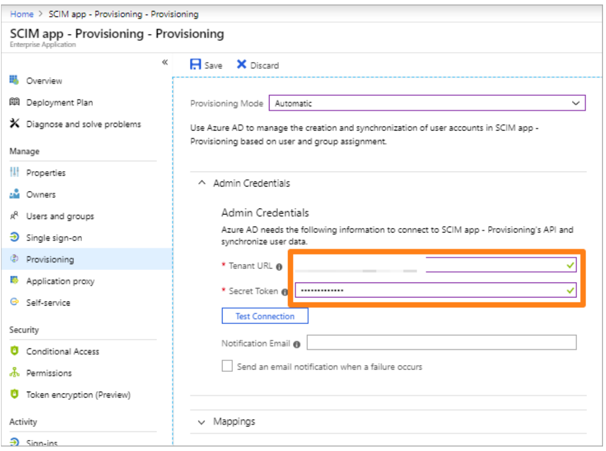
* Secret Token: ••••••••••••••

Notification Email:

□ Send an email notification when a failure occurs

4. In the Tenant URL field, enter the URL of the SCIM endpoint which was generated during the empower® Installer for the application in the following format:

```
<https://<dns_name>/empower/scimapi/scim>
```



Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in SCIM app - Provisioning based on user and group assignment.

Admin Credentials

Azure AD needs the following information to connect to SCIM app - Provisioning's API and synchronize user data.

* Tenant URL

* Secret Token: ••••••••••••••

Notification Email

□ Send an email notification when a failure occurs

5. In the Secret Token field, enter the token that was generated during the empower® Installer.

6. To test the connection, click on **Test Connection**.
   If the attempt fails, an error message is displayed

7. If the attempt is successful, click **Save**.