empower suite

Version: Dezember 2024

Inhalt

1. TECHNISCHE HINTERGRÜNDE

1.1 Was ist die Entra ID App Registrierung und welcher Berechtigung bedarf es?

Die App Registrierung dient als Relay und ermöglicht die Anmeldung bei empower® über die Entra ID. Des Weiteren bezeichnen wir empower® auch als *Software as a Service* (SaaS) Lösung.

Grundsätzlich wird eine Administrator Zustimmung für exakt die Berechtigungen erteilt, welche eingestellt werden. empower® benötigt hier die Berechtigungen **User.Read**, **User.Read.All** und **Group.Read.All** (letztere optional).

User.Read *[Typ – Delegiert]]*	Anmelden und Benutzerprofil lesen	Ermöglicht es einer Anwendung, die Profilinformationen des angemeldeten Benutzers zu lesen. Dazu gehören Details wie der Name des Benutzers, seine E-Mail-Adresse und andere grundlegende Profilinformationen.
User.Read.All *[Typ – Anwendung]*	Liest alle vollständigen User Profile aus.	Ermöglicht es der App, im Namen des angemeldeten Benutzers alle Profileigenschaften, Berichte und Manager anderer Benutzer in Ihrer Organisation zu lesen.
Group.Read.All *[Typ – Anwendung]*	Liest alle Gruppen aus.	Ermöglicht es der App, Gruppen aufzulisten und ihre Eigenschaften und alle Gruppenmitgliedschaften im Namen des angemeldeten Benutzers zu lesen. Ermöglicht es der App auch, Kalender, Unterhaltungen, Dateien und andere Gruppeninhalte für alle Gruppen zu lesen, auf die der angemeldete Benutzer zugreifen kann.

Quelle (Microsoft): https://learn.microsoft.com/de-de/graph/permissions-reference

Benötigt werden diese Berechtigungen von empower® zur Provisionierung von Benutzern und Gruppen aus der Entra ID in empower®. Auf dem Applikationsserver läuft in regelmäßigen, konfigurierbaren Abständen ein Hintergrunddienst, der Benutzer und Gruppen aus der Entra ID abruft und in empower® bereitstellt. Auf diese Weise synchronisierte Benutzer können sich in empower® über die Entra ID als Authentifizierungsprovider anmelden und empower® verwenden.

Die synchronisierten Gruppen dienen der Berechtigungsvergabe innerhalb der empower® Bibliothek auf Gruppenebene. Die Synchronisierung der Gruppen kann optional entfallen (s.o.) Eine Berechtigungsvergabe ist nur direkt auf Benutzerebene bzw. an alle empower® bekannten Benutzer möglich. Welche Benutzer und Gruppen genau synchronisiert werden lässt sich mittels entsprechender Filter auf Basis der Gruppenzugehörigkeiten oder anderer Attribute (z.B. Präfix des Gruppennamens) konfigurieren.

Als Alternative zu diesem von empower® initiierten Synchronisierungsverfahren bieten wir auch die Benutzerbereitstellung via SCIM (System for Cross-Domain Identity Management) an (siehe **https://learn.microsoft.com/de-de/azure/active-directory/app-provisioning/how-provisioning-works**). In diesem Fall werden Benutzer und Gruppen im Push-Verfahren aus der Entra ID in empower® bereitgestellt und die o.g. Berechtigungsvergabe entfällt

1.2 Allgemeine Informationen über SCIM

SCIM steht für *System for Cross-Domain Identity Management* und ist ein offenes Standardprotokoll zur Automatisierung des Austauschs von Benutzeridentitätsinformationen zwischen Identitätsdomänen und IT-Systemen. SCIM sorgt dafür, dass Mitarbeiter, die dem Human Capital Management (HCM)-System hinzugefügt werden, automatisch Konten in Entra ID oder Windows Server Active Directory erhalten. Benutzerattribute und -profile werden synchronisiert und bei Status- oder Rollenänderungen aktualisiert oder entfernt. Im Gegensatz zum bisher verwendeten Directory Sync werden die Informationen beim SCIM nicht mehr aktiv abgefragt, sondern automatisch bereitgestellt, wenn es Änderungen an den zu übertragenden Informationen gibt.

1.1.1 Vorteile von SCIM

- empower® benötigt keine Berechtigungen zum Abruf von Benutzern oder Gruppen aus dem Benutzerverzeichnis (Entra ID). Es erfolgt lediglich eine Registrierung der App, die keinen direkten Zugriff auf die Verzeichnisdaten erfordert.
- Die Bereitstellung wird vom Kunden direkt im Verzeichnisdienst konfiguriert, was eine gezielte und bedarfsgerechte Verwaltung von Benutzerkonten ermöglicht.
- Der Verzeichnisdienst selbst wird nicht regelmäßig geladen, da sich die Ressourcen bei Microsoft befinden. Stattdessen wird das empower® Backend von einem zusätzlichen Dienst geladen, der nur aktiv wird, wenn Änderungen vorgenommen werden.

1.1.2 Funktionsweise von SCIM

SCIM funktioniert anders als der Directory Sync nach einem PUSH-Verfahren. Im Gegensatz zum Vorgang beim Directory Sync werden die Daten hierbei nicht aktiv abgefragt. Beim SCIM werden Änderungen an Benutzern oder Benutzergruppen automatisch an empower® weitergeleitet.

Entra ID App Registrierung & SCIM-Einrichtung

2. APP REGISTRIERUNG

Um die App-Registrierung durchzuführen, stellen wir Ihnen ein Paket zum Download bereit, das die Installation über ein Skript ermöglicht und den gesamten Prozess automatisiert. Das Paket enthält zwei PowerShell-Skripte: ein Skript, das zur Erstellung der App-Registrierung verwendet wird, und ein optionales Skript, das nur ausgeführt wird, wenn empower® Mails Online verwendet wird. Die dritte Datei ist eine Konfigurationsdatei, die wichtige Parameter für das Registrierungsskript im Voraus definiert, um den Prozess zu beschleunigen.

config.json, die für die Einrichtung des Skripts wichtig ist. Typischerweise hat unser Support-Team diese Datei bereits für die App, die Sie anlegen, angepasst.

Die config.json-Datei sieht folgendermaßen aus:

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

tenantID: Die tenant ID, muss von Ihnen bereitgestellt werden.
appName: Der Name der Anwendung.
hostname: Die Basis-URL der Anwendung.
useMailsOnline: Boolescher Wert, um anzugeben, ob die Konfiguration von empower® Mails Online verwendet werden soll.
oneTimePasswordServiceUri: Die URI des One-Time-Passwort-Dienstes. Es besteht die Möglichkeit folgende One-Time-Password Services als Eintrag in oneTimePasswordServiceUri zu verwenden. Entweder *https://onetimepass.domaincrawler.com/* oder *https://snappass.symplasson.de/*

EntraIdAppRegistration.ps1

Dieses Skript wird für die App-Registrierung verwendet.

EntraIdAppRegistration_MailsOnline.ps1

Dieses Skript ist optional und wird nur zur Konfiguration von empower® Mails Online verwendet.

Sie können das Skript verwenden, um die für empower® erforderliche App-Registrierung zu erleichtern. Bitte laden Sie das Skript hier herunter: PowerShell Script App Registration empower®

Dieses PowerShell-Skript kann verwendet werden, um die für empower® erforderliche App-Registrierung in Entra ID automatisch zu erstellen, entweder über PowerShell oder Cloud Shell.

Bitte beachten Sie:

Das von empower® zur Vefügung gestellte PowerShell-Skript ist mit der Microsoft Graph PowerShell-Modulversion 2.19.0 kompatibel.

Bitte beachten Sie:

Bitte verwenden Sie entweder das PowerShell-Skript oder die Cloud Shell, um die App Registrierung zu erstellen.

2.1 Benutzung in PowerShell

Vorrausetzung ist das PowerShell Modul zu installieren: [PowerShell installieren]

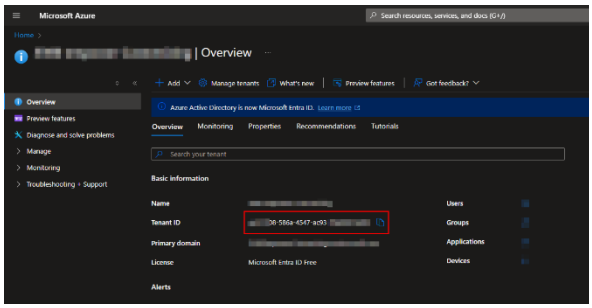
Vorbereitung

1. Stellen Sie sicher, dass das MS Graph PowerShell-Modul installiert ist.
2. Entpacken Sie den heruntergeladenen ZIP-Ordner.
3. Öffnen Sie PowerShell als Administrator im entpackten Ordner.

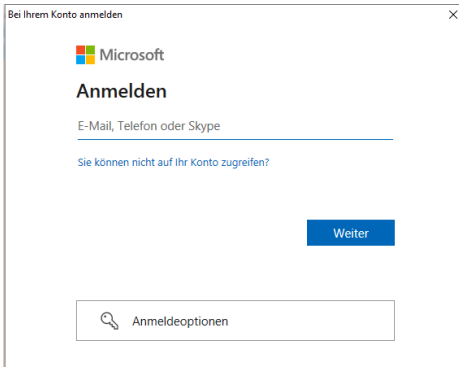
Execution

1. Führen Sie das Skript EntraIdAppRegistration.ps1 in dem Pfad aus, in dem es sich befindet. **PowerShell: .\EntraIdAppRegistration.ps1**
2. Verwenden Sie die Konfigurationswerte. Das Skript verwendet die Werte aus der *config.json*-Datei als Standardwerte.
3. Geben Sie Ihre TenantID ein oder bestätigen Sie den Standardwert aus der Konfigurationsdatei. Diese kann alternativ in ihrer Entra ID gefunden werden.

   Bitte geben Sie Ihre Microsoft Entra ID TenantID ein **[Standard: Tenant ID aus Entra ID]**
   (Via Enter können Sie den Standard aus der Konfigurationsdatei bestätigen).



4. Das Microsoft-Anmeldefenster wird ausgelöst. Melden Sie sich mit einem Benutzer an, der Zugriff auf die VM hat.



5. Geben Sie den Namen für die App-Registrierung ein oder bestätigen Sie den Standardwert aus der Konfigurationsdatei.

   Bitte geben Sie den gewünschten Namen für die App-Registrierung ein, z.B. **empower**.

6. Geben Sie die URL ein (muss mit https:// beginnen) und verwenden hierbei den von Ihrem Onboarding Specialist oder Customer Success Manager übermittelten *DNS Namen*. Bestätigen Sie Ihre Eingabe mit **Enter**.

   Bitte geben Sie den gewünschten Namen für die App-Registrierung ein, z.B.
   empower [Standard: empower]
   (Via Enter können Sie den Standard aus der Konfigurationsdatei bestätigen).

7. Als nächstes werden Sie gefragt, ob die Konfiguration von empower® Mails Online aktiviert werden soll. Drücken Sie **Enter** für den Standardwert (bereits vom Support-Team konfiguriert) oder geben Sie Ihren gewünschten Wert ein (true oder false).

8. Die App Registrierung wird nun automatisch erstellt und die erforderlichen Daten für den Backend-Installer werden angezeigt:

9. Eine *json*-Datei (*AppRegistrationInfo.json*) wird im aktuellen Ordner erstellt, der auch die Daten für den Backend-Installer enthält. Sichern Sie die Werte TenantID, ClientID und Client Secret.

> Finished

Kopieren Sie die Details von hier oder finden Sie die benötigten Details in der Datei *AppRegistrationInfo.json* im aktuellen Ordner

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

Beispiel-Link (Snappass Option):
https://snappass.symplasson.de/snappassc41ba9c2cf4e4112b67a4f44ce443441~OVNAVAoPOKhYB3hJs0UN9bYpCikKSHEqc_JforilSTI%3D

{
"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"

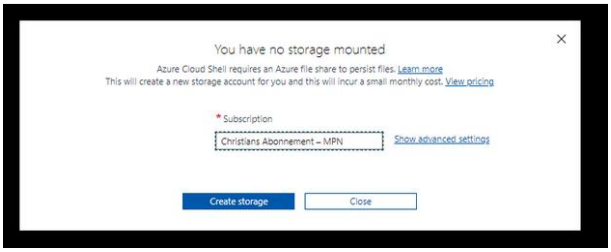
}

9. Um das Client Secret (den Secret Client Key) zu öffnen, öffnen Sie den Snappass-Link im Browser. Der Link ist einen Monat lang gültig, kann jedoch nur einmal geöffnet werden.
10. Bitte senden Sie uns zum Abschluss das Client Secret.

2.2 Benutzung in Cloud Shell

Als allererstes sollte man (portal.azure.com) mit dem Tenant verbunden sein, in dem man die App Registrierung anlegen möchte.

Im Browser gehen Sie auf folgende Seite: shell.azure.com

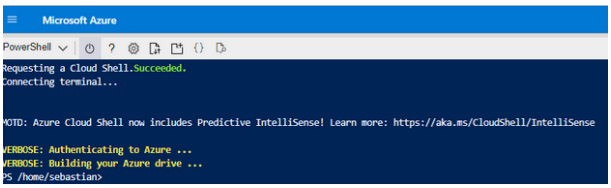


Wenn Sie die Cloud Shell zum ersten Mal verwenden, erscheint der folgende Dialog.

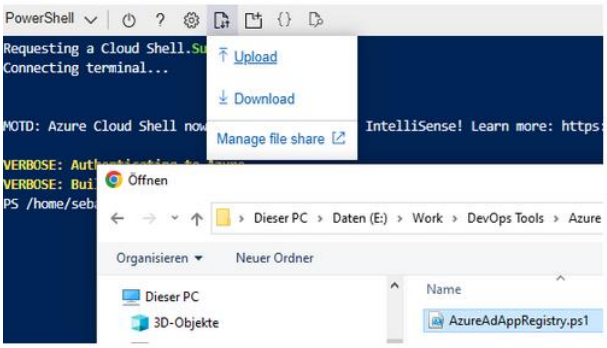
Es muss dann eine Subscription ausgewählt und auf **Create storage** geklickt werden.

Ein Storage Account für die Cloud Shell wird dann erstellt.

Danach erscheint die Cloud Shell, bitte wählen Sie hier **PowerShell** aus.



Über das hervorgehobene Symbol (siehe Screenshot) können Sie das Skript in die Cloud Shell hochladen.

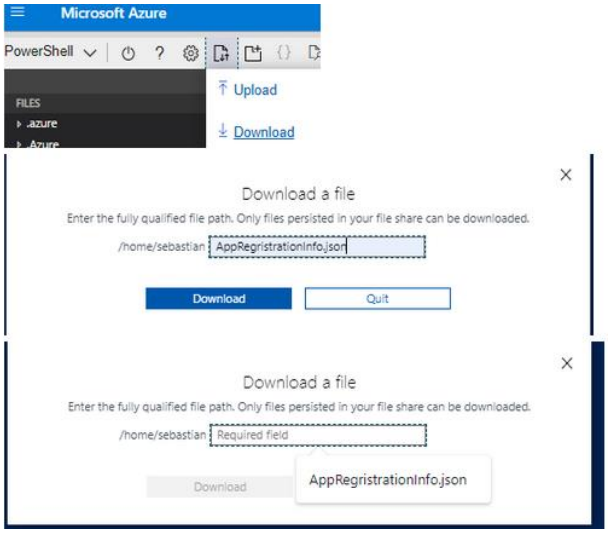


Dann rufen Sie das Skript einfach wie in PowerShell auf.

Hier sind die gleichen Eingaben wie oben für PowerShell zu machen. In diesem Szenario entfällt die TenantID und ein neuer Login ist zudem auch nicht notwendig.

Sie müssen nur den Namen und die URL von empower® eingeben und ob Sie empower® Mails Online zusätzlich konfigurieren möchten.

Wenn das Skript durchgelaufen ist, können Sie die Datei AppRegistration.json mit den benötigten App-Registrierungsinformationen über **Download** herunterladen.



Alternativ werden die Informationen erneut auf dem Bildschirm angezeigt.

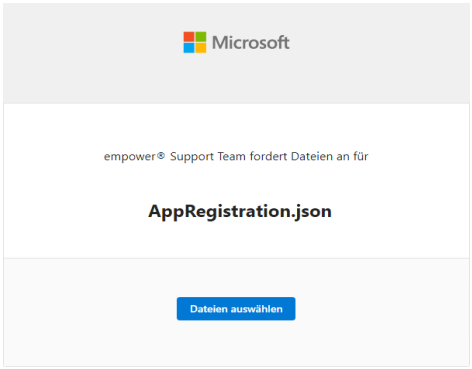
2.3 empower® die *AppRegistrationInfo.json* bereitstellen

Sobald das Skript ausgeführt wurde und Sie die *AppRegistrationInfo.json* erhalten haben, senden Sie die Datei bitte an Ihren Onboarding Specialist oder Customer Success Manager.

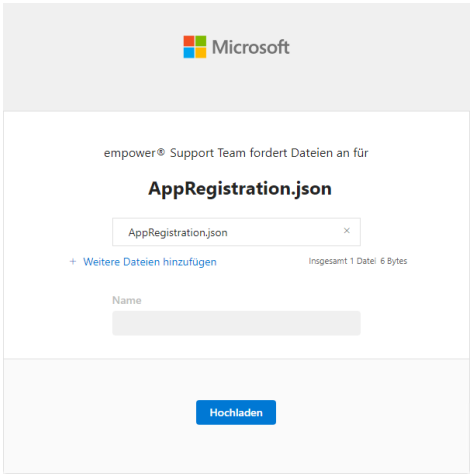
Ihr Onboarding Specialist oder Customer Success Manager hat Sie über OneDrive um Ihre *AppRegistrationInfo.json* gebeten, wo Sie Ihre Datei hochladen können.

Bitte befolgen Sie die Schritte:

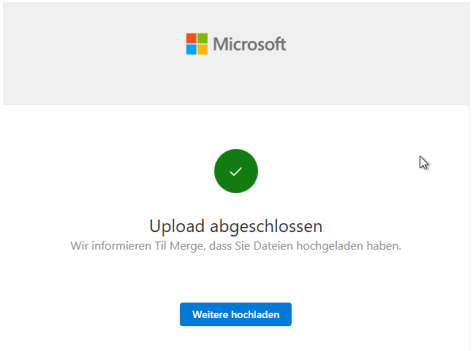
Klicken Sie in der E-Mail, die Sie von Ihrem Onboarding Specialist oder Customer Success Manager erhalten haben, auf **Dateien auswählen**.



Durchsuchen Sie Ihr Gerät, wählen Sie Ihre Datei aus und klicken Sie auf **Hochladen**.



Ihr Upload wurde abgeschlossen und Ihr Onboarding Specialist oder Customer Success Manager wird per E-Mail informiert.



2.4 Zusätzliche Informationen für empower®

Zusätzlich zur *AppRegristrationInfo.json* stellen Sie empower® bitte die folgenden Informationen zur Verfügung:

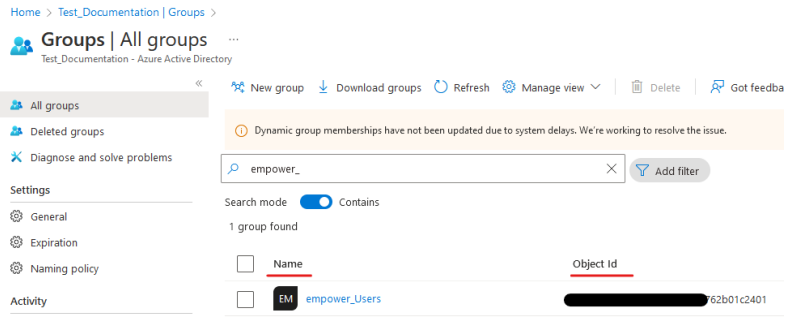
Eigenschaft	Wert
empower® Group Object ID	
Entra ID Group displayName	
Ablaufdatum Client Secret*	

*Sie erhalten von empower® vor Ablaufen Ihres aktuellen Client Secret eine Erinnerung.

empower® Group Object ID:
Diese ID ist ein globally unique identifier (GUID). Gemeint ist eine Entra ID Benutzer Gruppe, aus der empower® dann alle Nutzer synchronisiert. Mithilfe dieser Entra ID Benutzer Gruppe wird verhindert, dass Ihr komplettes Entra ID Tenant in empower® synchronisiert wird und ausschließlich die Nutzer synchronisieren, die empower® nutzen sollen.

Entra ID Group displayName:
In empower® werden für die Vergabe von Berechtigungen innerhalb von empower® neben den Benutzern auch Gruppen synchronisiert. Hierbei ist es hilfreich, mit dedizierten empower® Gruppen zu arbeiten oder mit Gruppen, die sich über den Namen zusammenfassen lassen.

Bspw. empower® Benutzer-Grruppe = **empower_users**; empower® Admingruppe = **empower_adminusers**. So können die Berechtigungen in empower® direkt auf die Entra ID Gruppen angewendet werden.



3. SCIM IN AZURE EINRICHTUNG

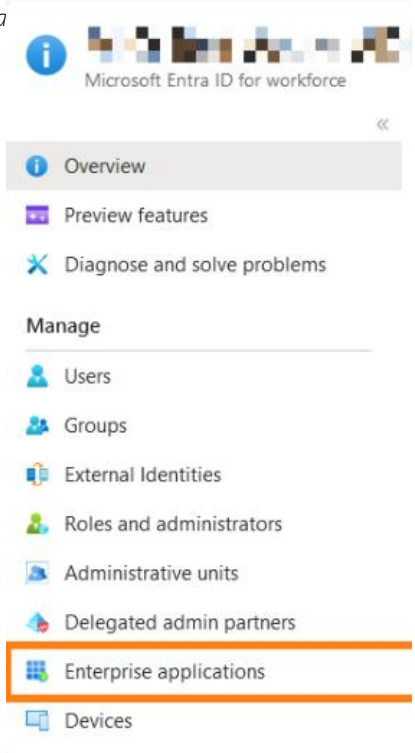
3.1 Einrichten der SCIM API

Im Azure-Portal muss zunächst eine App-Registrierung vorgenommen werden. Nachfolgend wird das Anlegen dieser App-Registrierung beschrieben.

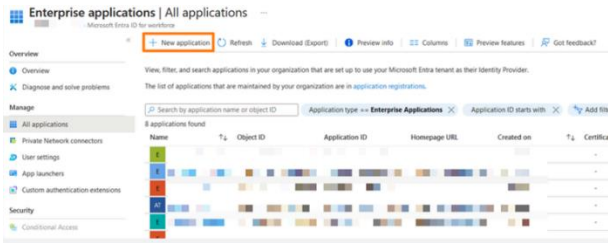
Bitte beachten Sie:

Diese Schritte müssen ausgeführt werden, **bevor** der empower® Backend Setup Installer verwendet wurde.

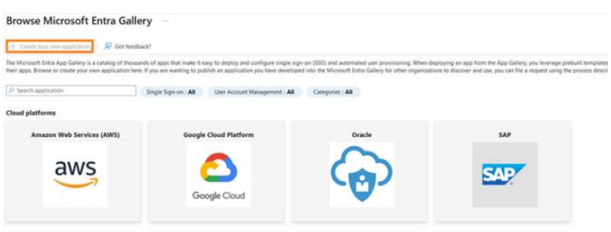
1. Suchen Sie im Azure-Portal nach *Microsoft Entra ID* und wählen Sie den Dienst aus.



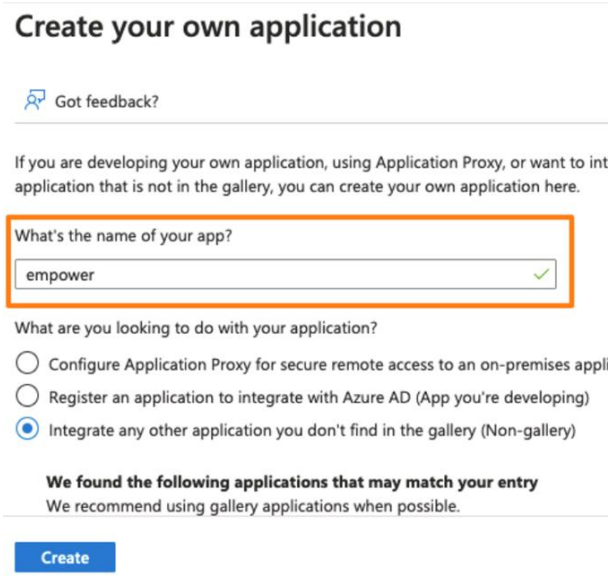
2. Wählen Sie links in der Leiste den Tab **Enterprise applications (Unternehmensanwendungen)** aus.
3. Klicken Sie auf den Button **New application (Neue Anwendung).**



4. Klicken Sie auf den Button **Create your own application (Eigene Anwendung erstellen).**



5. Geben Sie einen Namen für die Anwendung ein.
6. Klicken Sie auf den Button **Create (Erstellen)**.

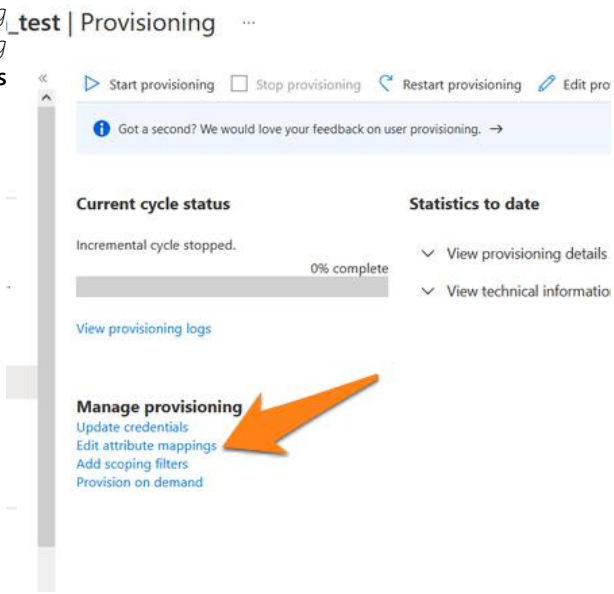


3.2 Bearbeiten der Attributzuordnungen (Mappings)

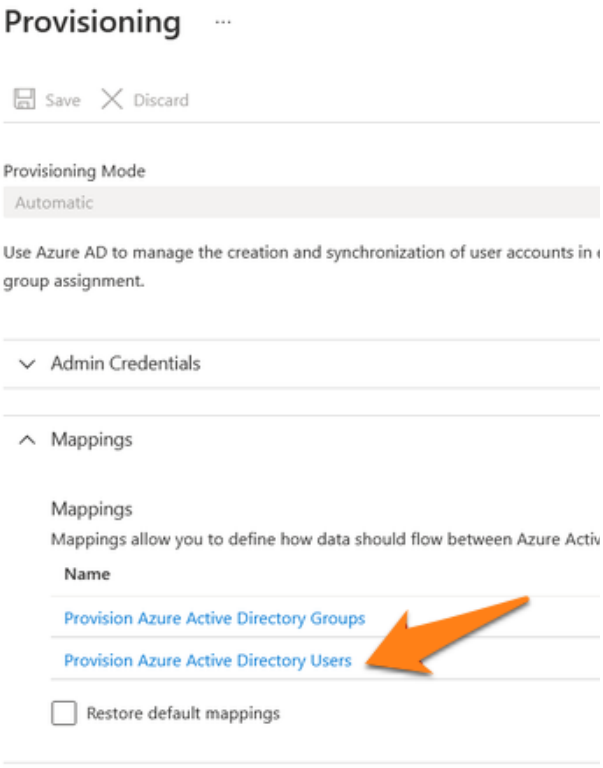
Für die Einrichtung von SCIM ist außerdem eine Anpassung der Attributzuordnungen notwendig. Dies ist für den Directory Sync nicht notwendig.

Im Abschnitt Mappings gibt es zwei Attribut-Zuordnungen: eins für Benutzer und eins für Gruppen. Für empower® müssen die Standard-Attributzuordnungen angepasst werden. Gehen Sie dazu wie folgt vor:

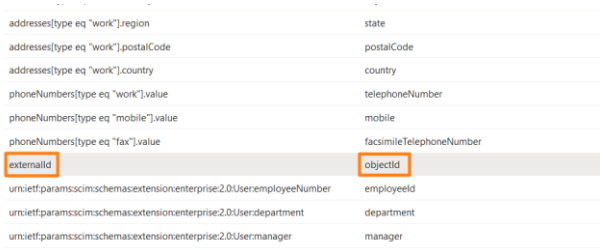
1. Klicken Sie ebenfalls unter *Provisioning (Bereitstellung)* im Abschnitt *Manage Provisioning (Bereitstellung verwalten)* auf **Edit Mappings (Zuordnungen bearbeiten).**



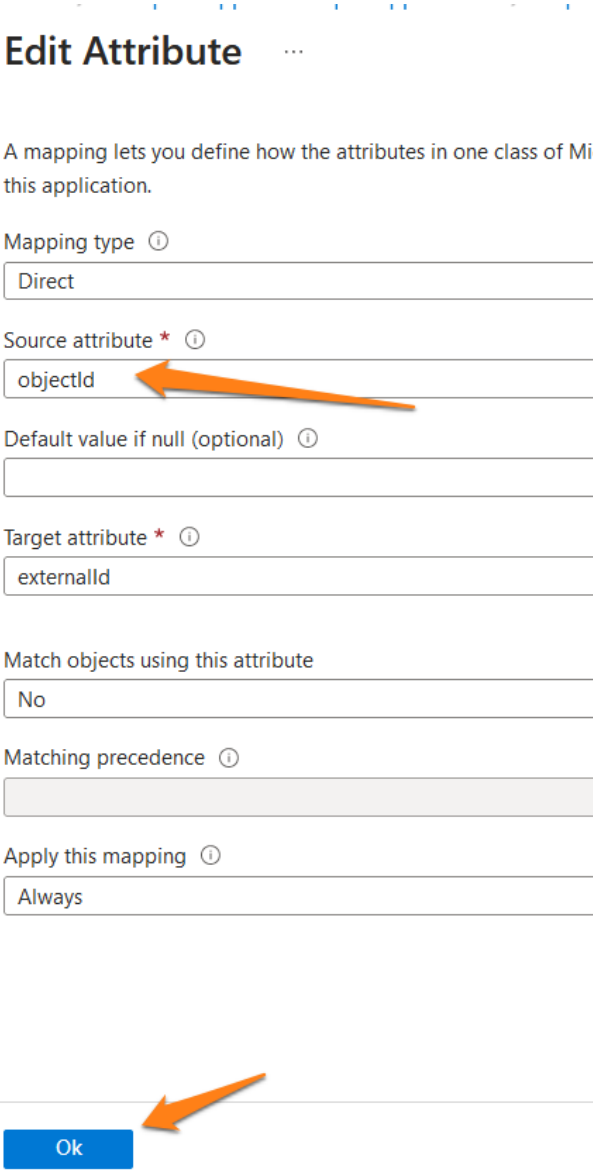
2. Klicken Sie dann im Abschnitt *Mappings (Zuordnungen)* auf den Link **Provision Azure Directory Users.**



3. Ändern Sie das Mapping für *externalId* zu *objectId*. Standardmäßig wird hier meist der E-Mail-Nickname verwendet.



4. Klicken Sie auf den Button **OK.**



5. Wenn Sie die Konfiguration abgeschlossen haben, setzen Sie den *Provisioning Status (Bereitstellungsstatus)* auf **On (An)**.

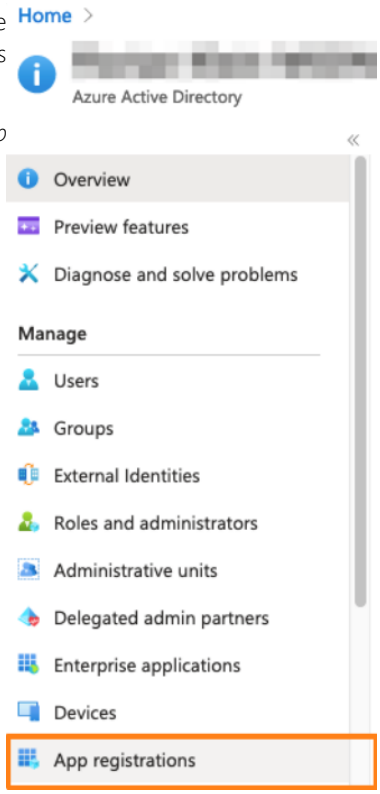
6. Um den Entra-ID-Bereitstellungsdienst zu aktivieren, klicken Sie auf den Button **Save (Speichern).**

3.3 Abspeichern der Werte zur Enterprise Application

Für die Installation des empower® Backends werden im Backend Installer die Werte *Application ID* und *Directory ID* benötigt. Daher ist es sinnvoll, diese Werte bereits bei Erstellung der Enterprise Application abzuspeichern. Gehen Sie dazu wie folgt vor:

1. Wechseln Sie nach Erstellung der Enterprise Application zur allgemeinen Übersicht des Microsoft-Entra-ID-Verzeichnisses.
2. Wählen Sie dann links in der Leiste den Tab *App registrations (App-Registrierungen)* aus.

Die neu erstellte Enterprise Application wird nun angezeigt.



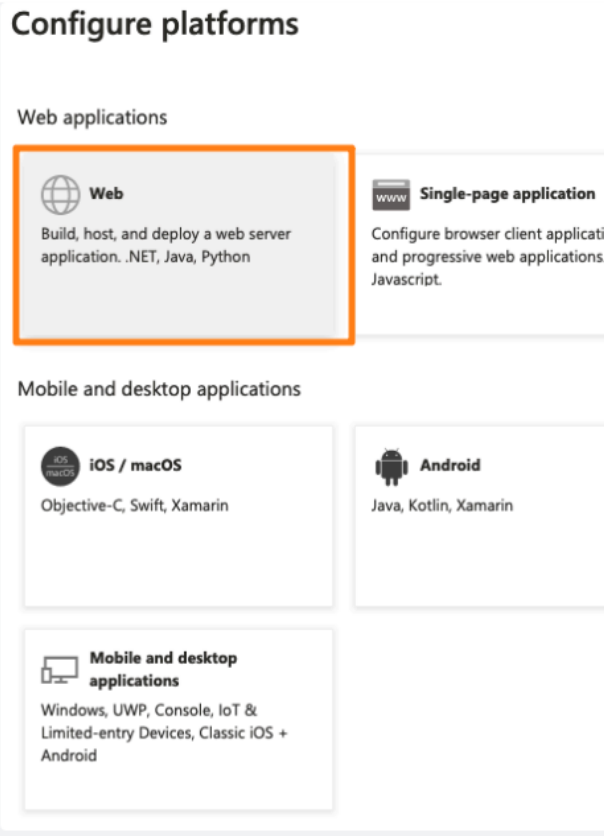
3. Wählen Sie die soeben erstellte Enterprise Application aus. Sie werden zur anwendungsspezifischen Übersicht weitergeleitet.

4. Speichern Sie sich die **Application (Client) ID (Anwendungs-ID)** und die **Directory (Tenant) ID (Verzeichnis-ID)** ab.

3.4 Umleitungs-URIs

Umleitungs-URIs sind notwendig, damit Azure nach erfolgreicher Authentifizierung weiß, wohin der oder die Nutzende weitergeleitet werden soll. Damit die URIs bekannt sind, müssen sie vorher definiert werden. Gehen Sie hierzu wie folgt vor:

1. Wählen Sie links in der Leiste der anwendungsspezifischen Übersicht den Tab **Authentication (Authentifizierung)** aus.
2. Klicken Sie auf den Button **Add a platform (Plattform hinzufügen).**
3. Wählen Sie unter *Web applications (Webanwendungen)* die Option **Web** aus.



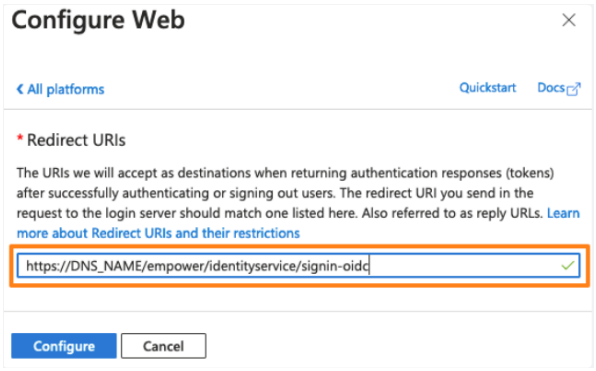
4. Geben Sie auf der Seite **Redirect URIs (Umleitungs-URIs)** die erste der drei folgenden Umleitungs-URIs Ihrer empower® Umgebung an:

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

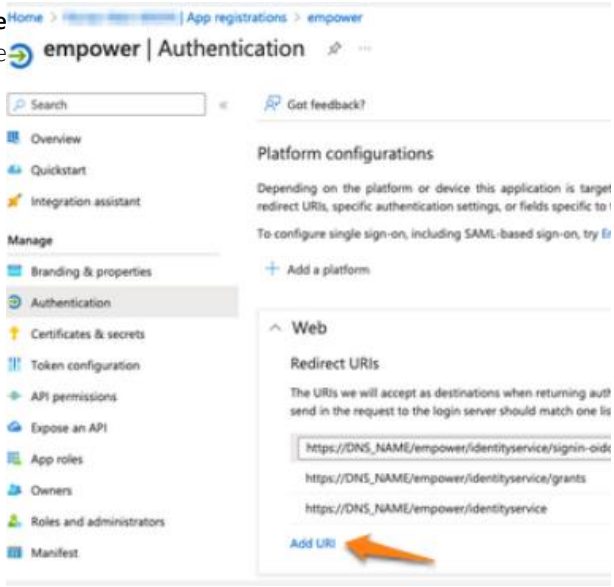
`https://[DNS_Name]/empower/identityservice/grants`

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

[DNS_NAME] entspricht dem DNS Namen Ihrer empower® Umgebung. Die restlichen beiden URIs werden in den folgenden Schritten nachgetragen.



5. Klicken Sie auf den Button **Configure (Konfigurieren).** Unter **Web** können nun weitere Umleitungs-URIs hinzugefügt werden.

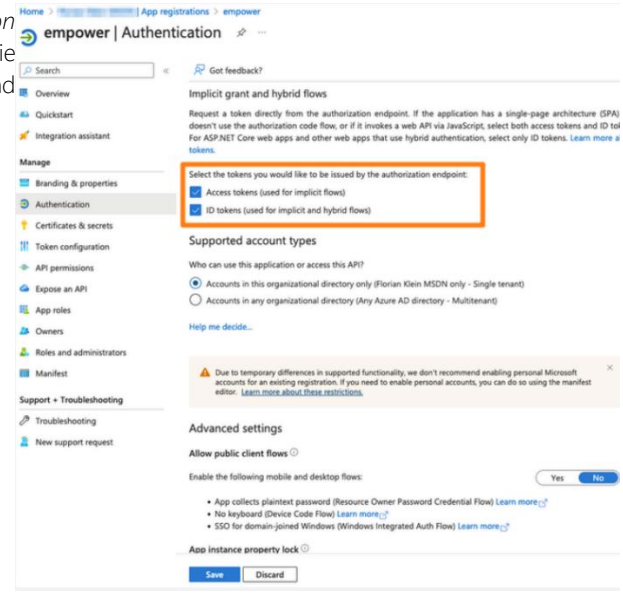


6. Um die beiden fehlenden URIs hinzuzufügen, klicken Sie auf **Add URIs (URIs hinzufügen).**

3.5 Implicit Flow aktivieren

Für empower® wird bis einschließlich Version 9.2 *Implicit Flow* als Anmeldeverfahren verwendet. Daher muss im Azure-Portal für diese Versionen der *Implicit Flow* aktiviert werden.

1. Aktivieren Sie ebenfalls im Tab *Authentication (Authentifizierung)* den *Implicit Flow*, indem Sie die Optionen **Access tokens (Zugriffs-Tokens)** und **ID tokens (ID-Tokens)** aktivieren.

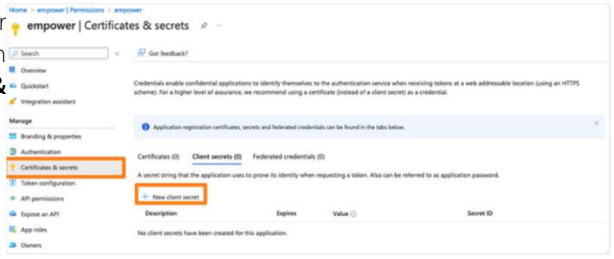


2. Klicken Sie auf den Button **Save (Speichern)**.

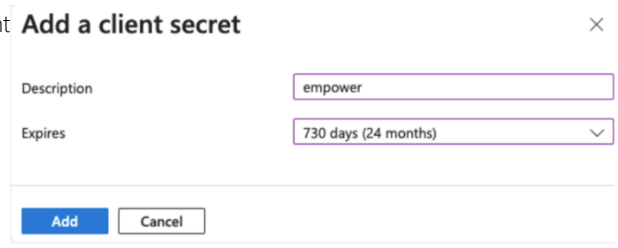
3.6 Client Secret

Um die Benutzeranmeldung durchführen zu können, benötigt empower® ebenfalls ein gültiges Client Secret (geheimer Clientschlüssel). Richten Sie im folgenden Schritt ein Client Secret ein.

1. Wählen Sie links in der Leiste der anwendungsspezifischen Übersicht den Tab **Certificates and Secrets (Zertifikate & Geheimnisse)** aus.



2. Klicken Sie auf den Button **New client secret (Neuer geheimer Clientschlüssel)**.
3. Geben Sie eine Beschreibung für das neue Client Secret ein.

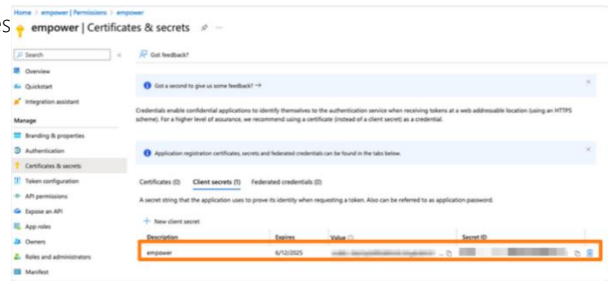


4. Bestimmen Sie für die Gültigkeit des Client Secrets nach den Richtlinien des Kundenunternehmens.

5. Klicken Sie auf den Button **Add (Hinzufügen)**.
6. Kopieren Sie das Client Secret und speichern Sie es ab.

Bitte beachten Sie:

Das Client Secret ist nur einmal sichtbar.



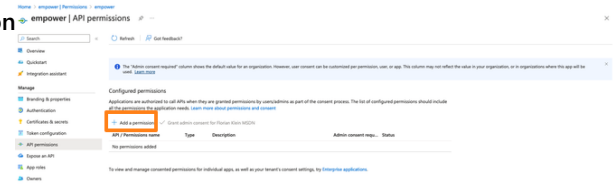
3.7 Erforderliche API-Autorisierung

Passen Sie dann die Berechtigungen für die Anwendung an. Die Anpassung der Berechtigungen erlaubt es empower®, die Benutzer- und Benutzergruppen aus dem Verzeichnis zu lesen. Im Folgenden wird beschrieben, wie Sie die User.Read einstellen, um die Benutzeranmeldung erfolgreich einzurichten.

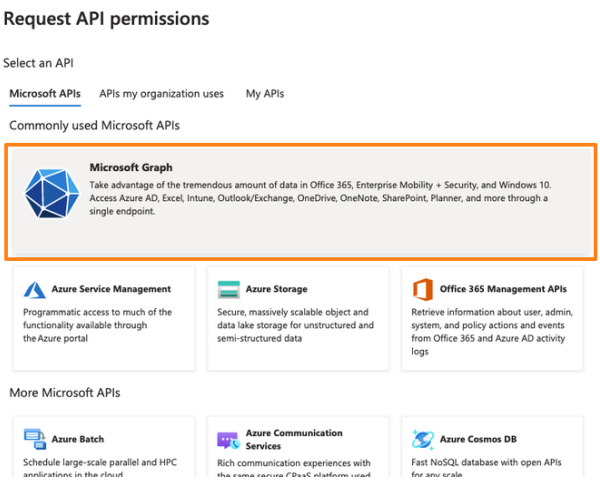
Die folgende Berechtigung ist für die Benutzeranmeldung immer erforderlich:

- *User.Read*

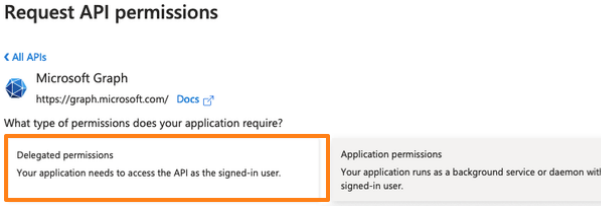
1. Wählen Sie links in der Leiste der anwendungsspezifischen Übersicht den Tab *API permissions (API-Berechtigungen)* aus.
2. Klicken Sie auf den Button **Add a permission (Berechtigung hinzufügen).**



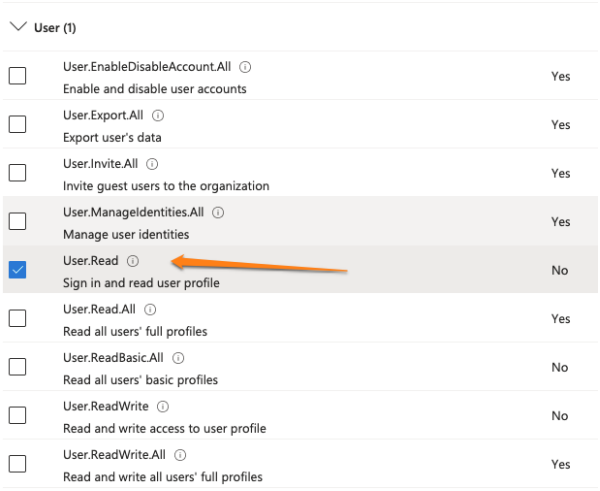
3. Wählen Sie **Microsoft Graph** aus.



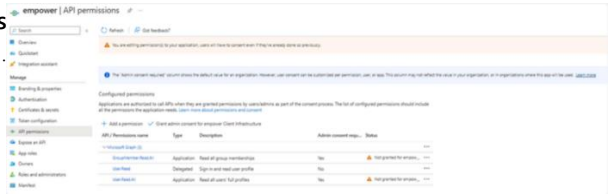
4. Wählen Sie nun **Delegated permissions (Delegierte Berechtigungen)** aus.



5. Aktivieren Sie in der folgenden Liste *User.Read*.



6. Klicken Sie auf den Button **Add permissions (Berechtigungen hinzufügen)**. Sie gelangen zurück zur Übersichtsseite.



3.8 Endpunkteinstellung für SCIM

In diesem Abschnitt wird erläutert, wie Sie den Endpunkt für die SCIM-Bereitstellung festlegen, mit dem die Benutzerelemente synchronisiert werden sollen.

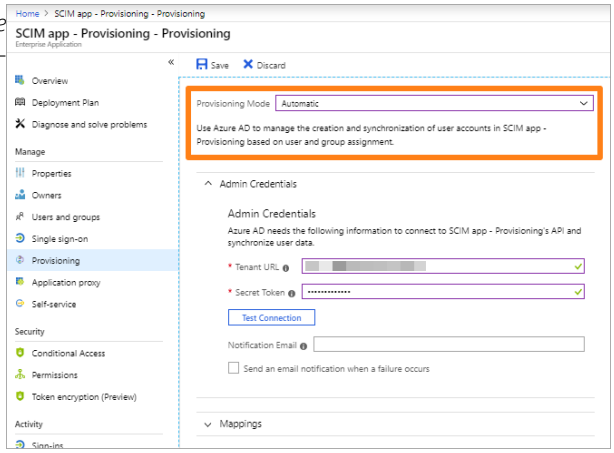
Bitte beachten Sie:

Diese Einstellungen können erst getroffen werden, **nachdem** der empower® Backend Setup Installer verwendet wurde und SCIM damit eingerichtet wurde.

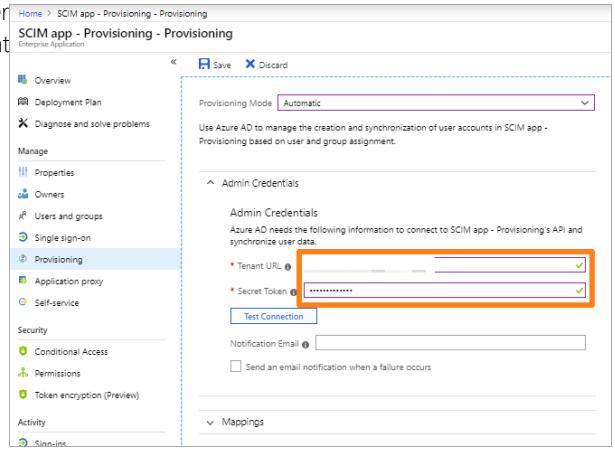
Wenn Sie SCIM als Bereitstellungsverfahren nutzen möchten, gehen Sie wie folgt vor:

1. Wechseln Sie zur anwendungsspezifischen Übersicht.
2. Wählen Sie links in der Leiste der anwendungsspezifischen Übersicht den Tab Provisioning (Bereitstellung) aus.

3. Wählen Sie für *Provisioning Mode (Bereitstellungsmodus)* aus dem Dropdown-Menü **Automatic (Automatisch)** aus.



4. Geben Sie im Feld **Tenant URL** die URL des SCIM-Endpoint, welche beim empower® Installer generiert wurde für die Anwendung in dem Format an: `<https://<DNS_Name>/empower/scimapi/scim>`



5. Geben Sie im Feld *Secret Token (Geheimes Token)* den Token ein, der beim empower® Installer generiert wurde.
6. Um die Verbindung zu testen, klicken Sie auf **Test Connection (Verbindung testen).**
7. Wenn der Versuch erfolgreich ist, klicken Sie auf den Button **Save (Speichern)**.