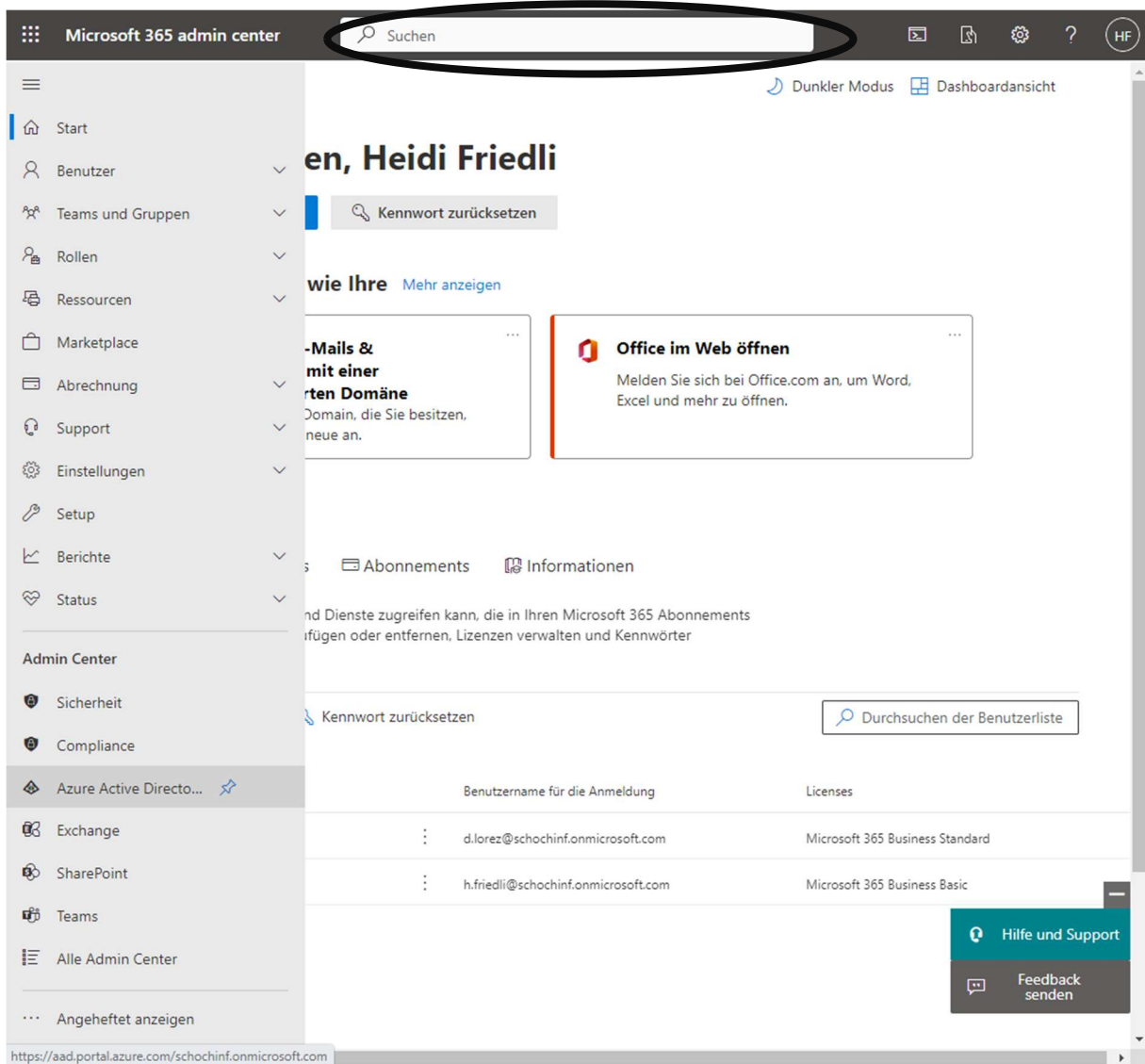
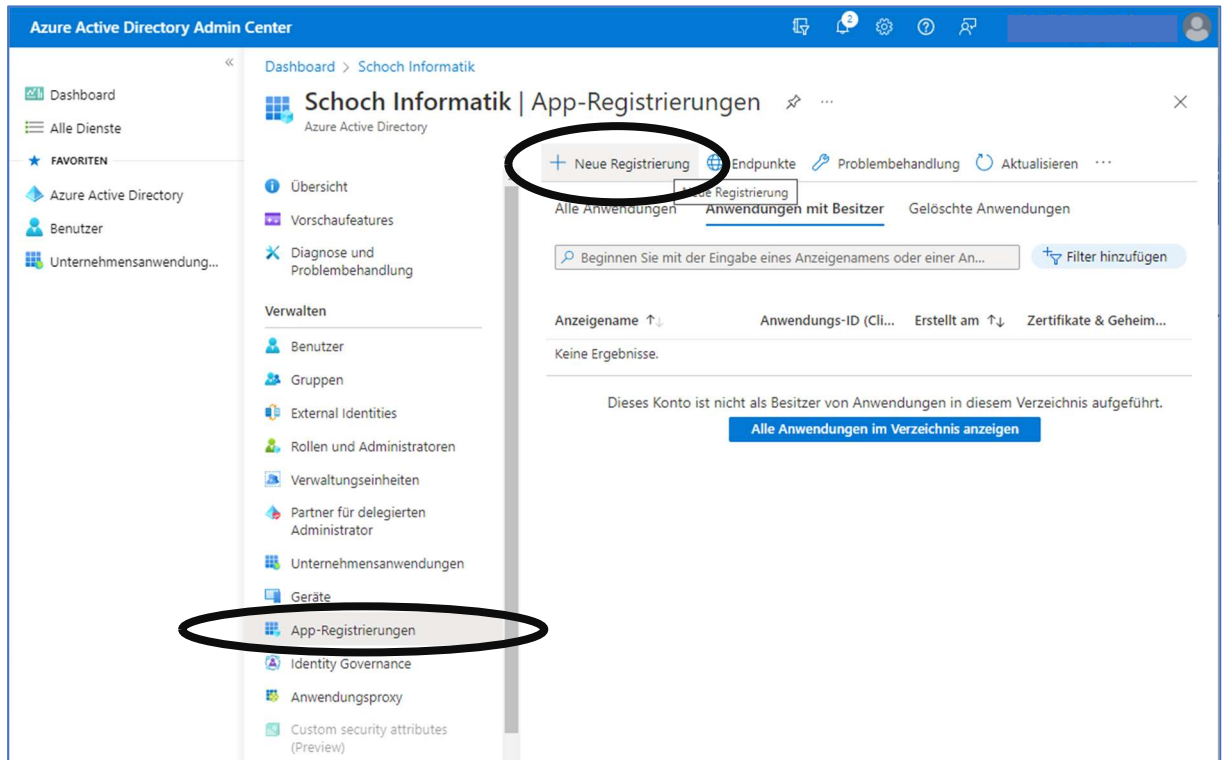


SchochTERMIN: App-Registrierung für Microsoft 365 Exchange

- Im **Microsoft365 admin center** anmelden (<https://admin.microsoft.com/>).
- Hamburger-Menü aufklappen und **Azure Active Directory Admin Center** öffnen.
- Bei neueren Versionen: Azure Active Directory Admin Center ist im Menü nicht mehr aufgeführt: Suche mittels Suchfenster nach Azure Active Directory Admin Center



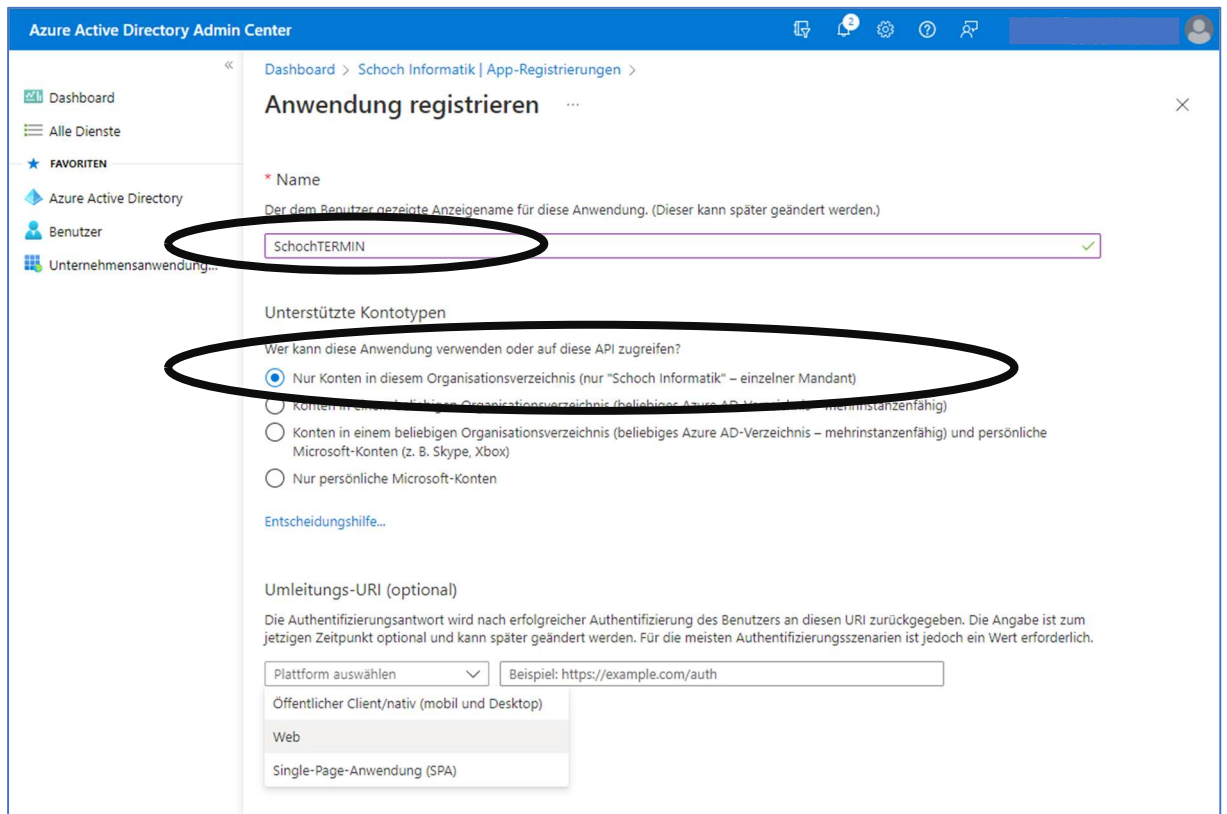
- **Azure Active Directory öffnen und App-Registrierungen auswählen**



- **+ Neue Registrierung ausführen und folgende Werte eintragen:**

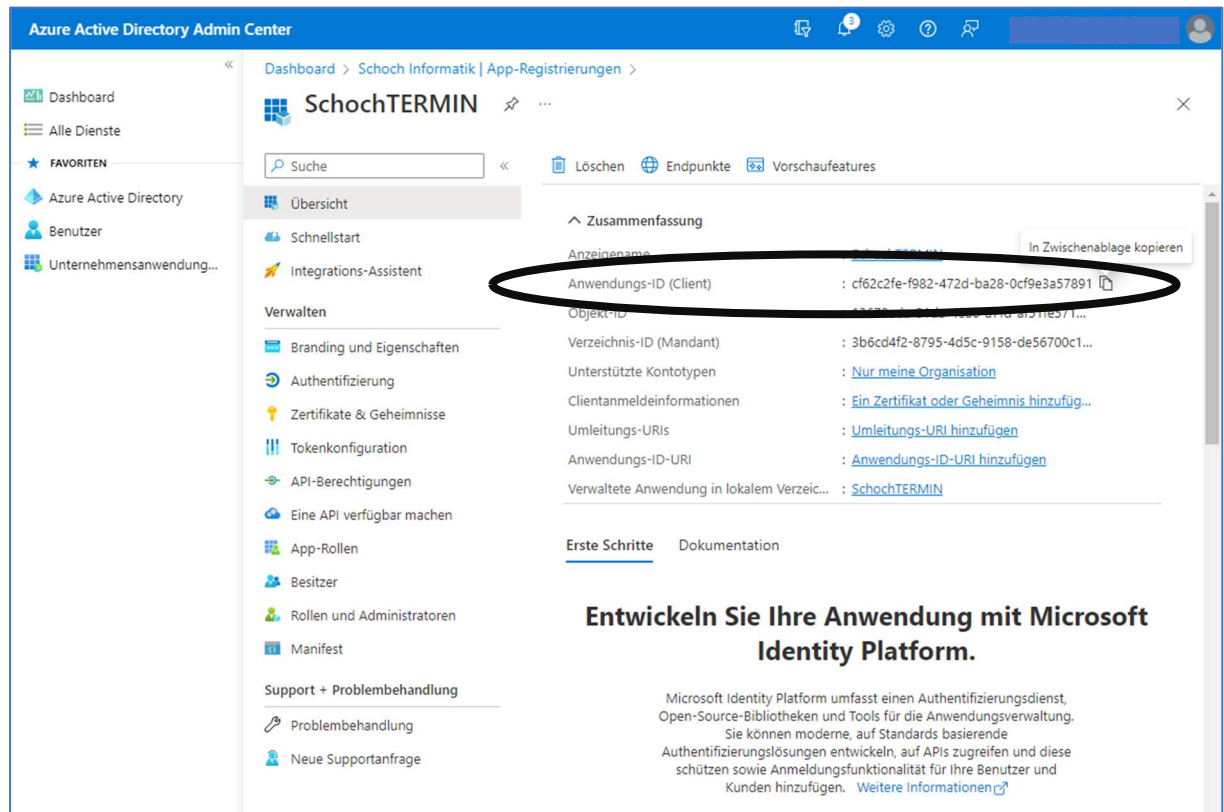
Name: SchochTERMIN

Kontentyp: Nur Konten in diesem Organisationsverzeichnis

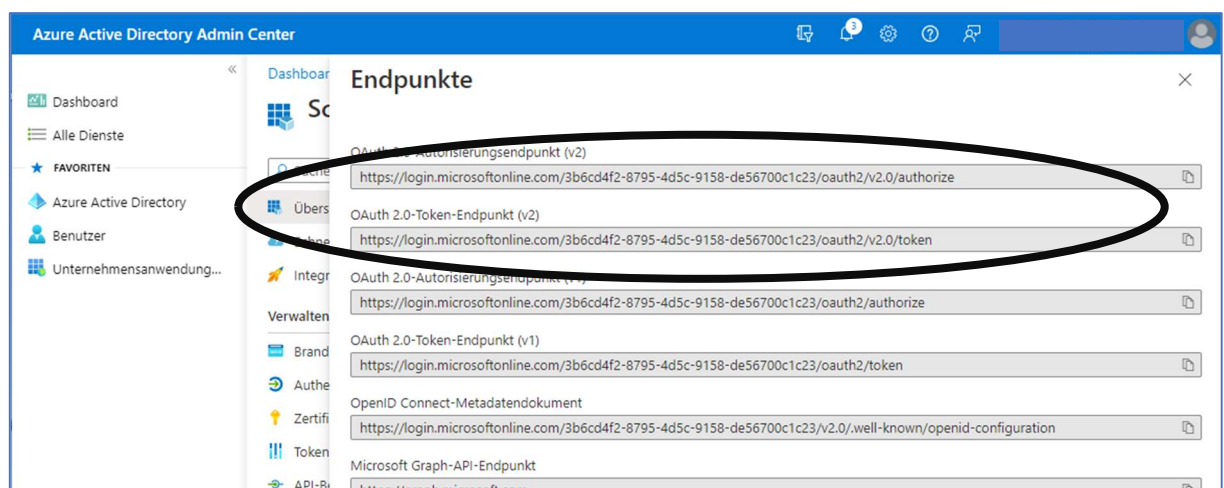
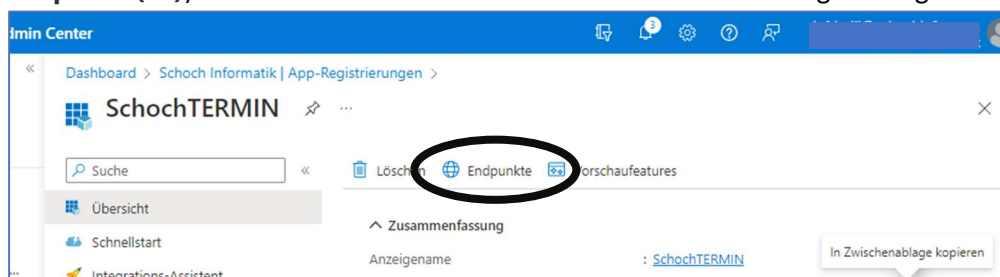


- **Den Vorgang mit Registrieren am Ende des Fensters abschliessen.**

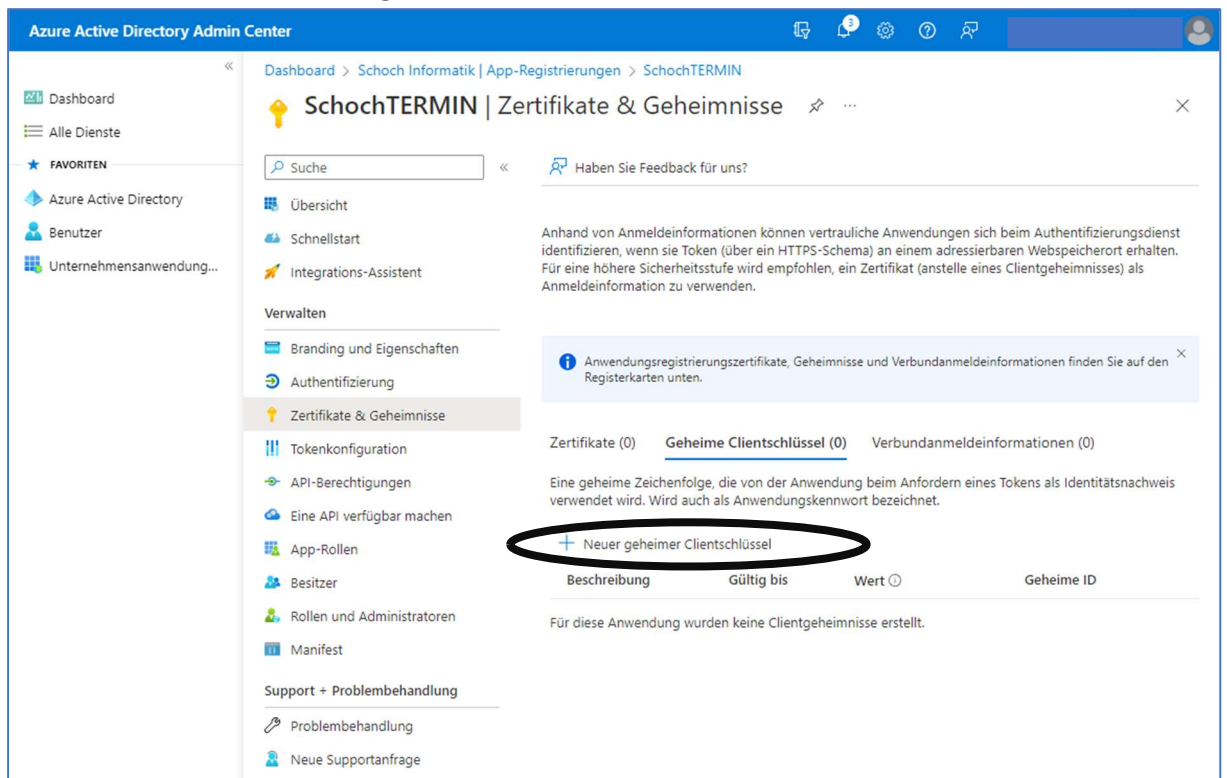
- Die App-Seite zeigt eine Übersicht über die gerade registrierte App. Der Wert des Feldes **Anwendungs-ID (Client)** wird bei der Anmeldung in der SchochTERMIN-Anwendung benötigt.



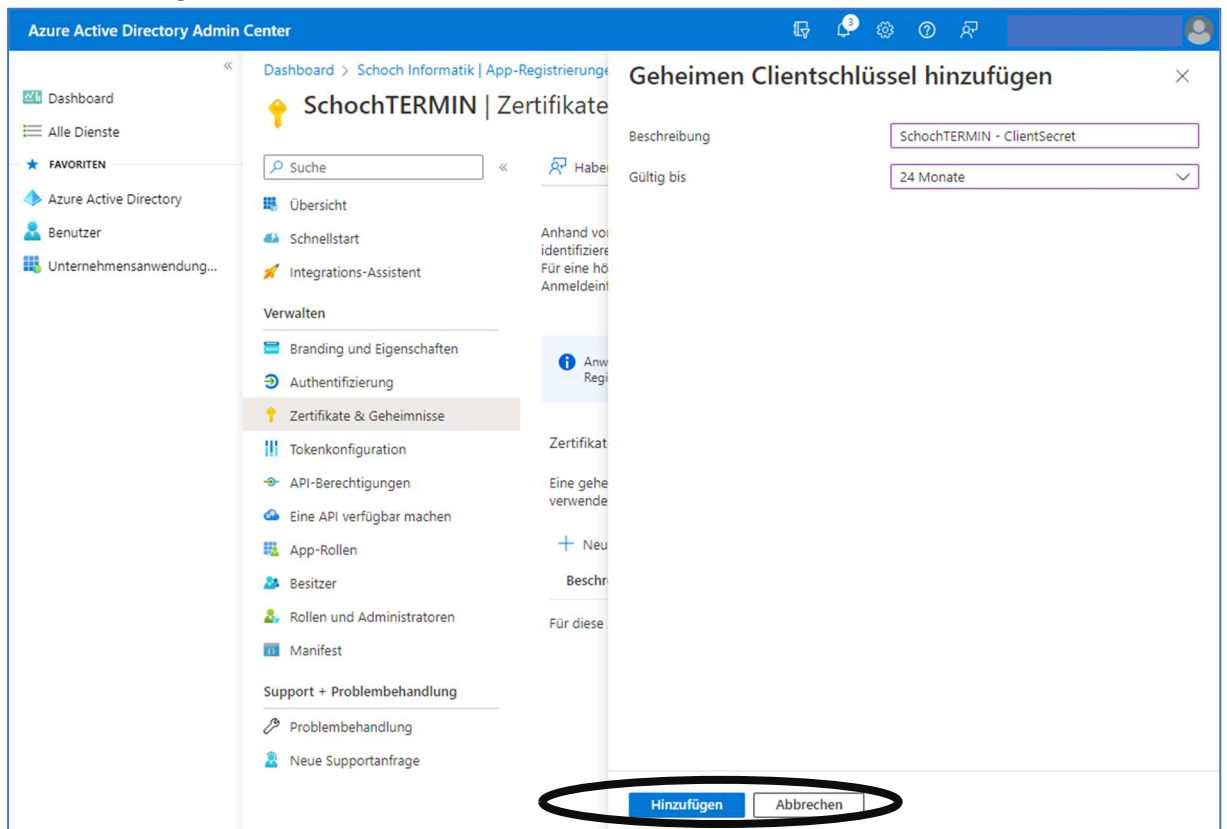
- Unter **Endpunkte** werden diverse Endpunkte für die erstellte App angezeigt. Die ersten beiden Endpunkte (**OAuth 2.0-Autorisierungsendpunkt (v2)** und **OAuth 2.0-Token-Endpunkt (v2)**) werden ebenfalls für die SchochTERMIN-Anwendung benötigt.



- Neben der Anwendungs-ID wird auch ein Passwort benötigt. Unter **Zertifikate & Geheimnisse** kann ein **+ Neuer geheimer Clientschlüssel** erstellt werden.



- Den Vorgang nach Eingabe der Beschreibung und der maximal möglichen Gültigkeitsdauer durch **Hinzufügen** abschließen



- Auch der neu generierte Clientschlüssel wird für die SchochTERMIN-Anwendung benötigt.
ACHTUNG: Der Schlüssel kann nur hier und jetzt kopiert werden. Er ist danach nicht mehr zugänglich! Unbedingt kopieren und zwischenspeichern.

Azure Active Directory Admin Center

Dashboard > Schoch Informatik | App-Registrierungen > SchochTERMIN

SchochTERMIN | Zertifikate & Geheimnisse

Suche

Haben Sie Feedback für uns?

Haben Sie einen Moment, um uns Feedback zu geben? →

Anhand von Anmeldeinformationen können vertrauliche Anwendungen sich beim Authentifizierungsdienst identifizieren, wenn sie Token (über ein HTTPS-Schema) an einem adressierbaren Webspeicherort erhalten. Für eine höhere Sicherheitsstufe wird empfohlen, ein Zertifikat (anstelle eines Clientgeheimnisses) als Anmeldeinformation zu verwenden.

Anwendungsregistrierungszertifikate, Geheimnisse und Verbundanmeldeinformationen finden Sie auf den Registerkarten unten.

Zertifikate (0) **Geheime Clientschlüssel (1)** Verbundanmeldeinformationen (0)

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

+ Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert	ID
SchochTERMIN - Clie...	8.11.2024	1LI8Q~0Gdkvbt4u...	d0ec0596-4290-49...

- Nach dem Generieren des Clientschlüssel müssen Berechtigungen gesetzt werden. Dies wird unter dem Titel **API-Berechtigungen** erledigt.

Azure Active Directory Admin Center

Dashboard > Schoch Informatik | App-Registrierungen > SchochTERMIN

SchochTERMIN | API-Berechtigungen

Suche

Aktualisieren | Haben Sie Feedback für uns?

In der Spalte "Administratoreinwilligung erforderlich," wird der Standardwert für eine Organisation angezeigt. Die Benutzereinwilligung kann jedoch pro Berechtigung, Benutzer oder App angepasst werden. Diese Spalte zeigt möglicherweise nicht den Wert für Ihre Organisation oder für Organisationen, in denen diese App verwendet wird. [Weitere Informationen](#)

Konfigurierte Berechtigungen

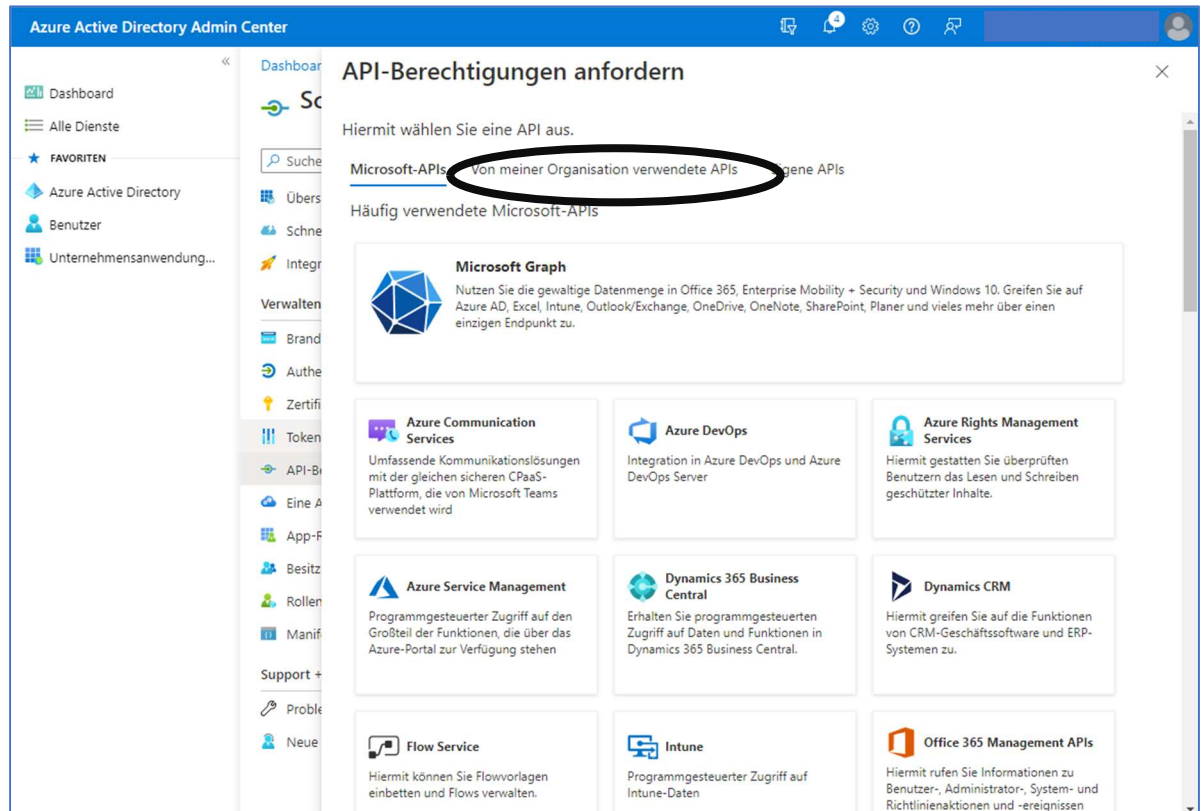
Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. [Weitere Informationen zu Berechtigungen und Zustimmung](#)

+ Berechtigung hinzufügen

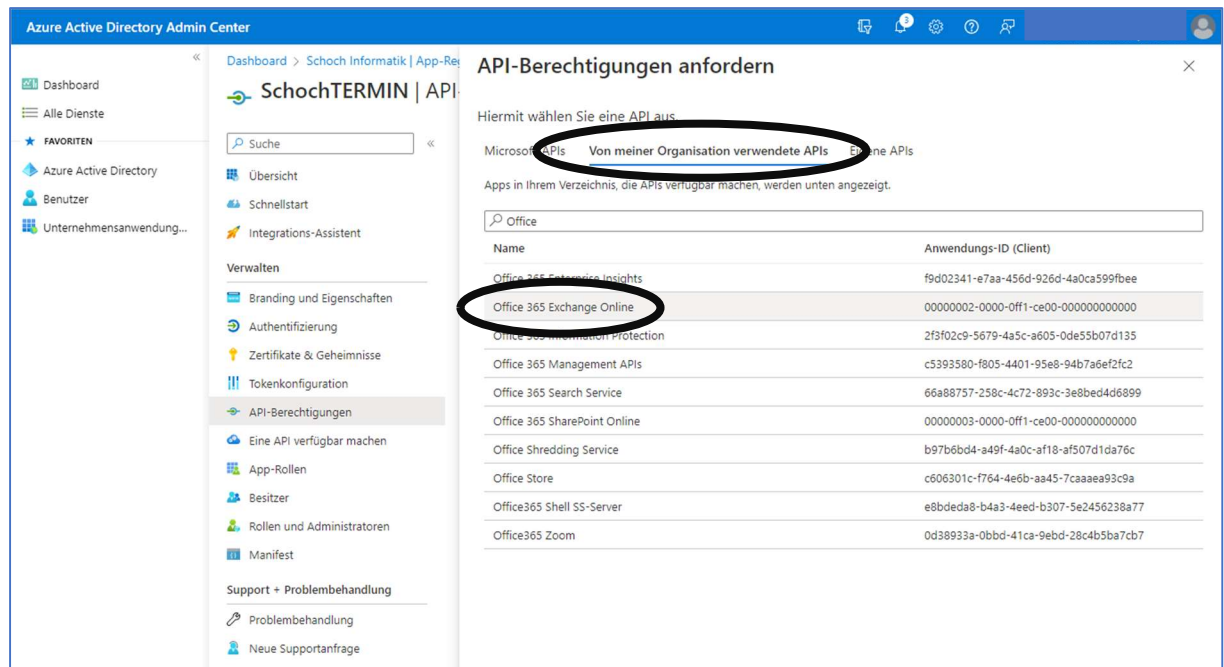
API/Berechtigungsnamen	Typ	Beschreibung	Administratoren
Microsoft Graph (1)			
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein

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

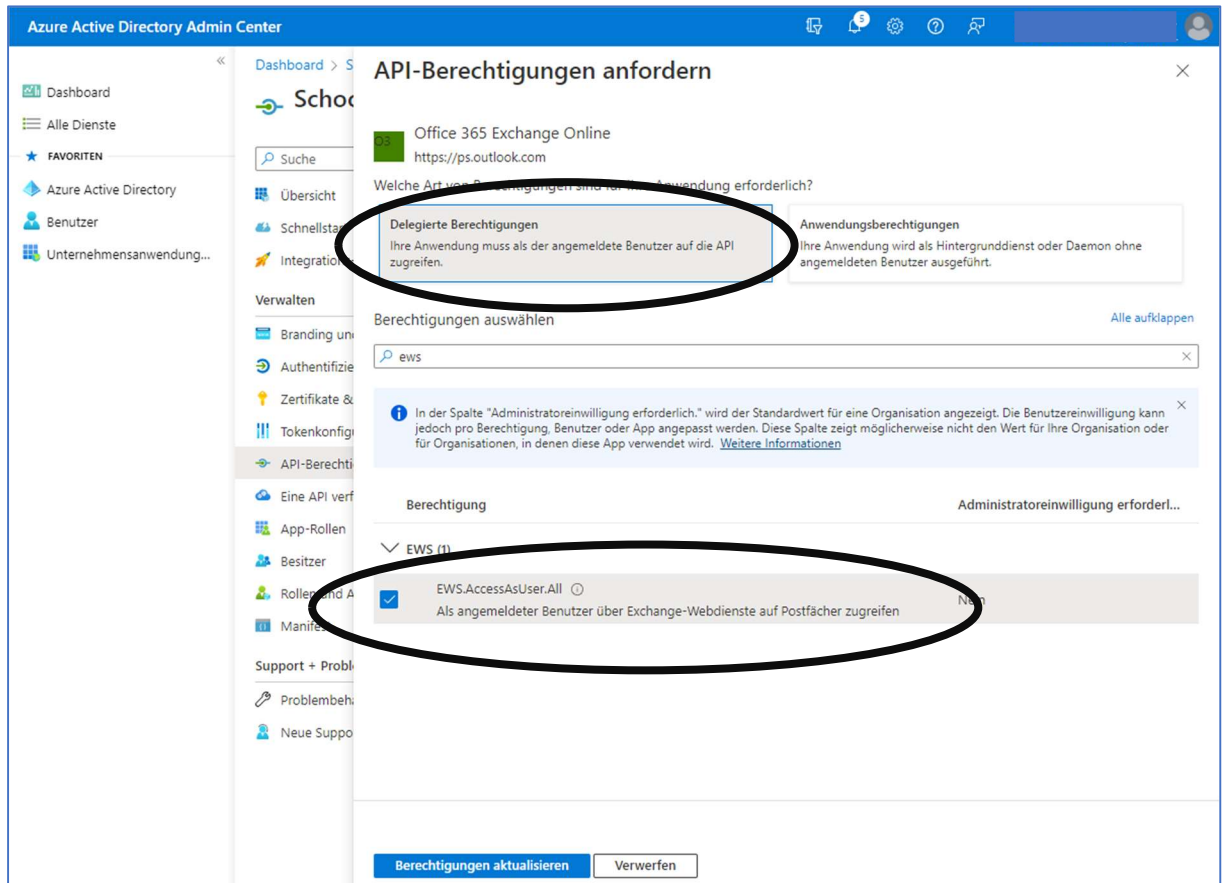
- Mit **+ Berechtigung hinzufügen** wird das Auswahlfenster geöffnet.



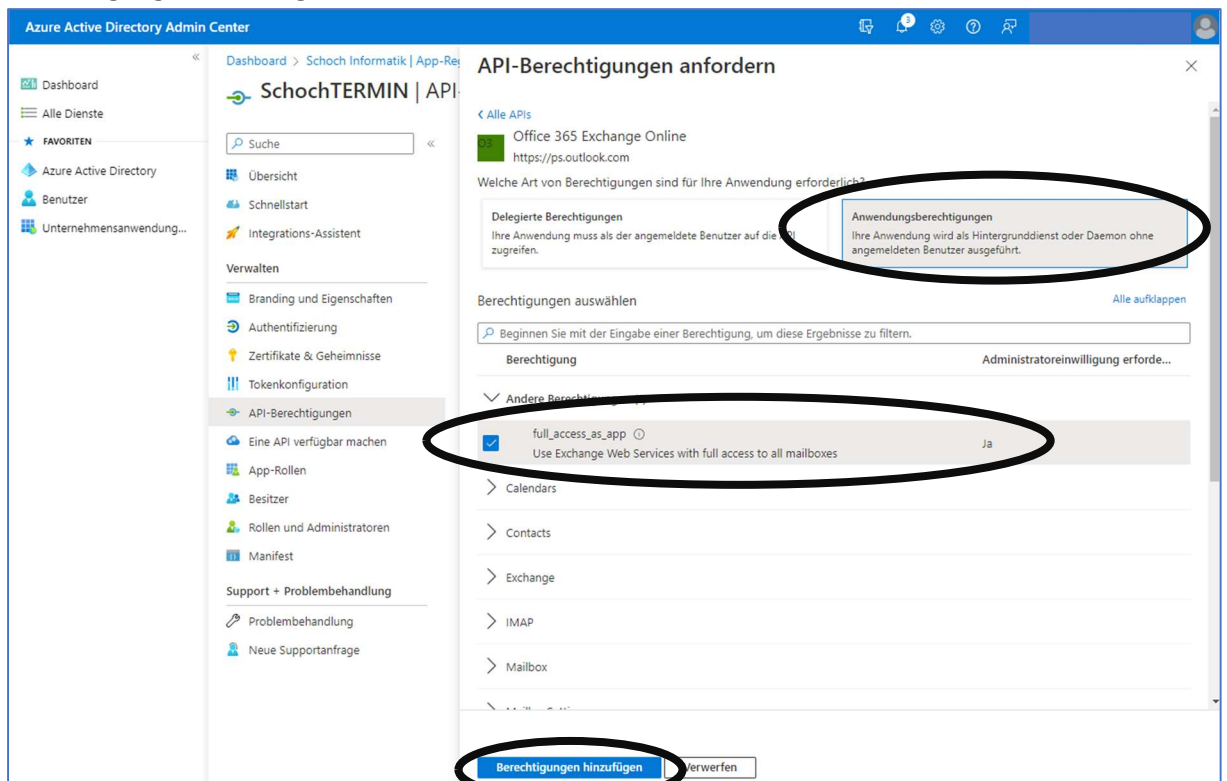
- Die benötigten Berechtigungen liegen im Register **Von meiner Organisation verwendete APIs** und heisst: **Office 365 Exchange Online**.



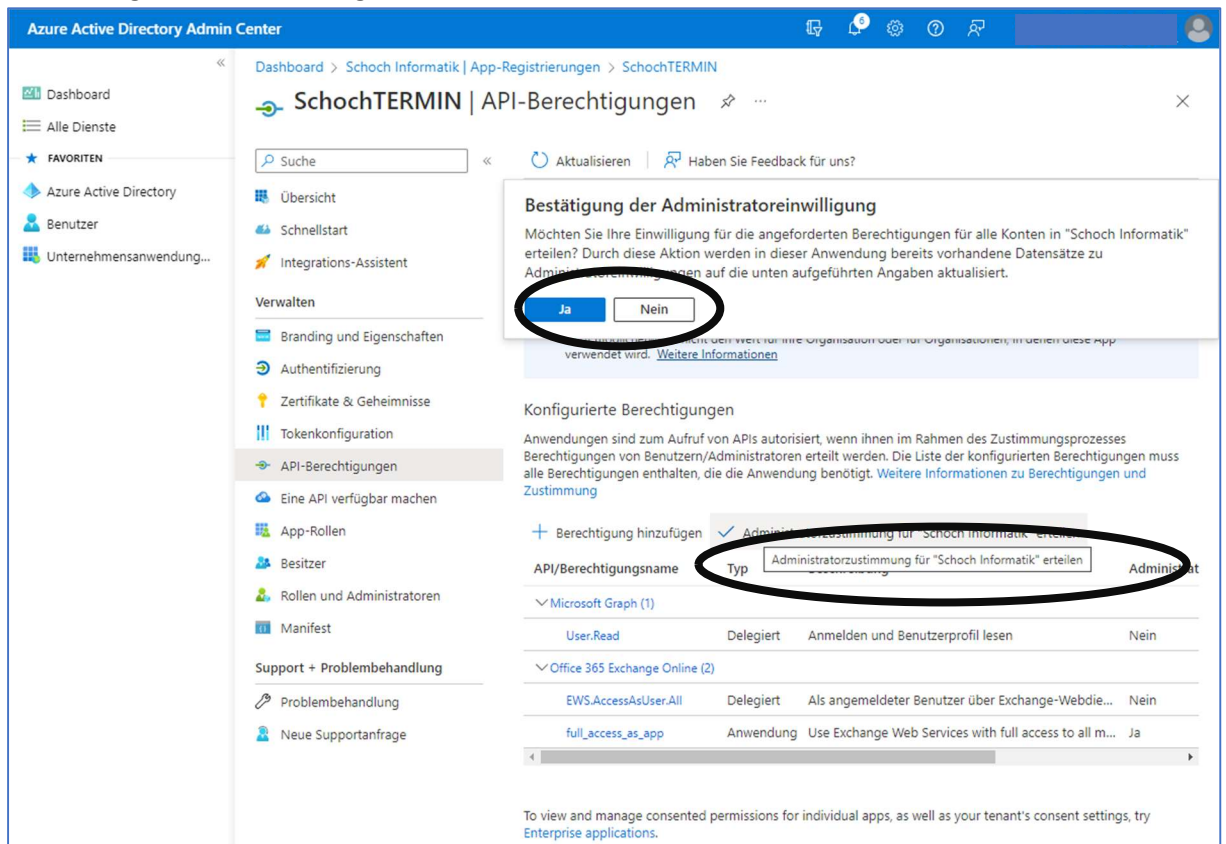
- Unter **Delegierte Berechtigungen** die Berechtigung **EWS.AccessAsUser.All** auswählen.



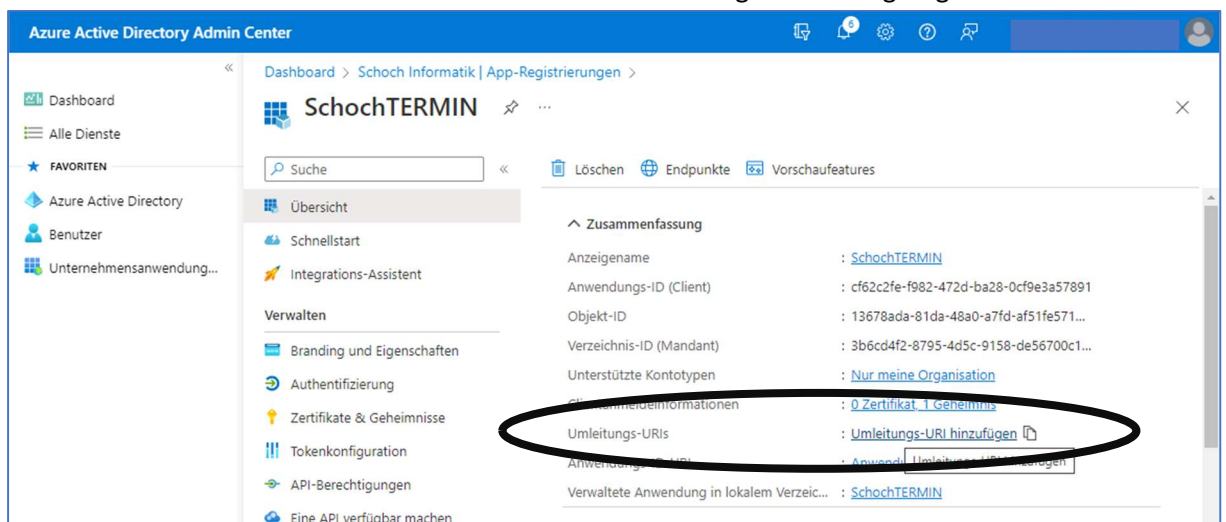
- Unter **Anwendungsberechtigungen** die Berechtigung **full_access_as_app** auswählen und mit **Berechtigungen hinzufügen** erstellen.



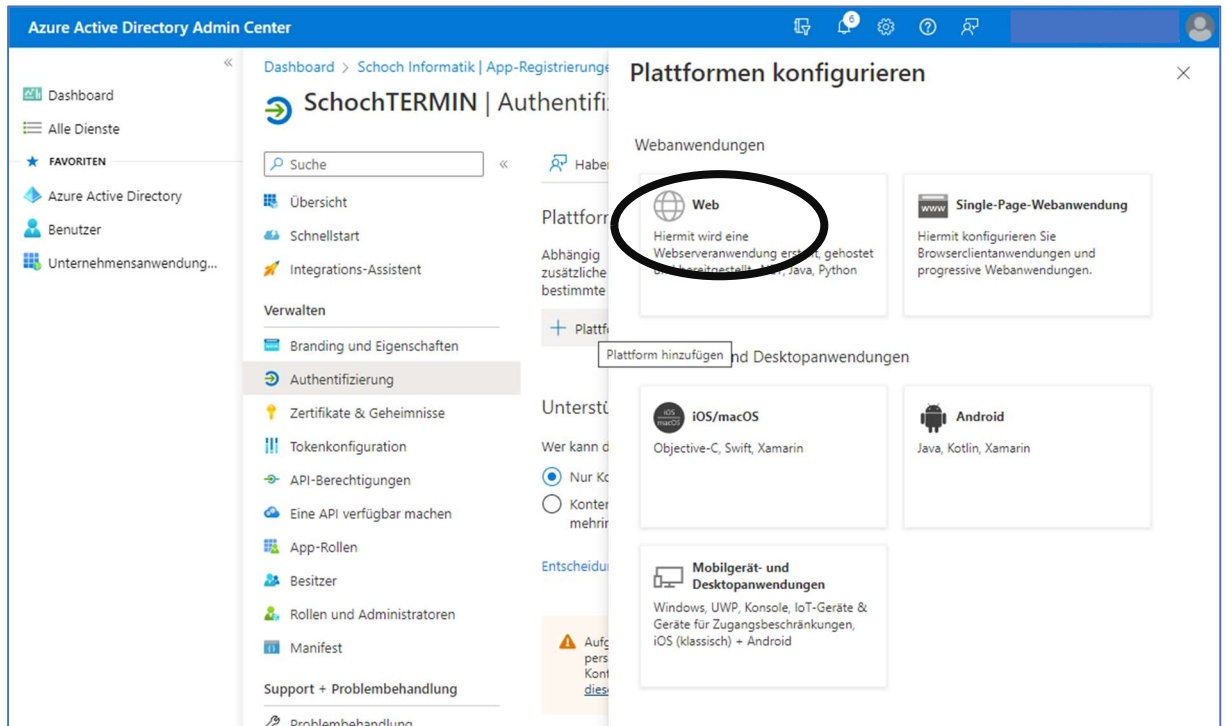
- Nachdem die Berechtigung hinzugefügt wurde, kann die Zustimmung zu SchochTERMIN-Anwendung mittels **Administratorenzustimmung für «Schoch Informatik» erteilen** für alle Benutzer auf einmal erteilt werden. Wenn dies hier nicht getan wird, wird bei der ersten Anmeldung um die Erlaubnis gebeten.



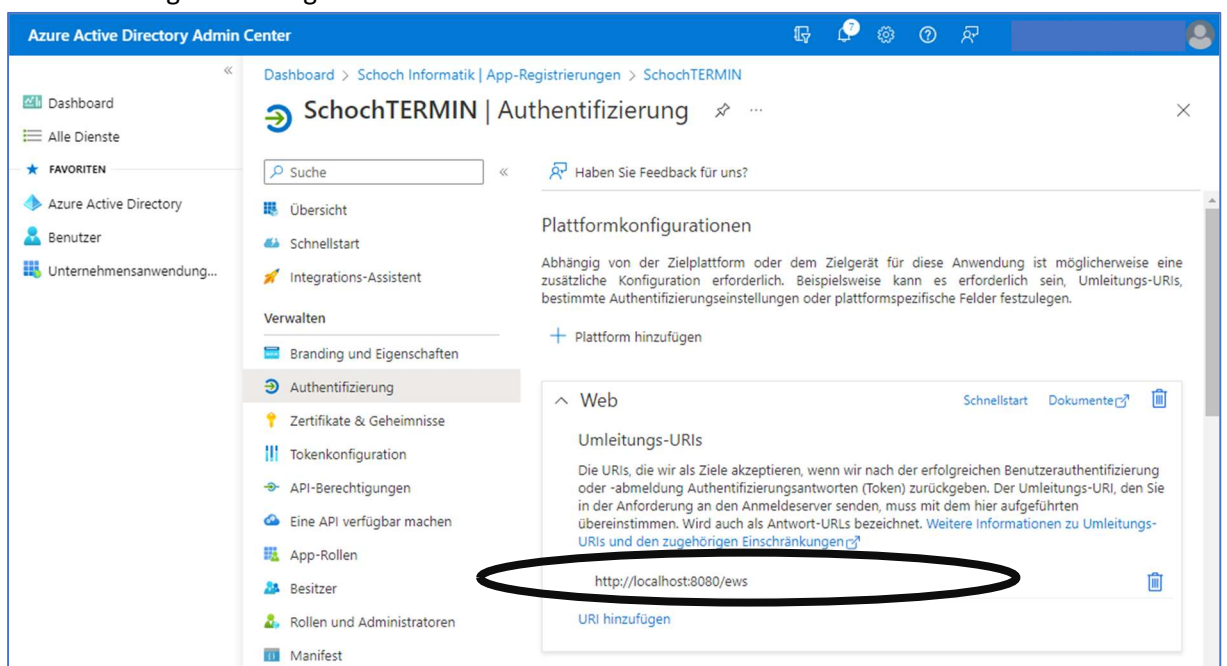
- Zurück auf der Übersicht wird zum Schluss noch die Umleitungs-URI hinzugefügt.



- Unter **+ Plattform hinzufügen** wird Web ausgewählt



- Als Umleitungs-URI wird **http://localhost:8080/ews** (oder <http://localhost/ews>) angegeben und mit Konfigurieren abgeschlossen.



SchochTERMIN: Anmeldung

Dies muss an jedem Arbeitsplatz ausgefüllt werden, der eine eigene Termin Installation besitzt.

EWS Profile

Specify the logon parameters.

Connection

Server

Use Autodiscover or use Exchange Web Service URL directly:

☐ Autodiscover E-Mail: Example: someone@somewhere.com

☒ Service URL: https://outlook.office365.com/EWS/Exchange.asmx

OAuth Authentication

☒ Use OAuth2 (Registration must have been completed first)

Grant Type: ClientCredentials (NT-Service Applications, uses impersonation)

Client App ID: cf62c2fe-f982-472d-ba28-0cf9e3a57891

Client Secret:

Redirect URI: http://localhost:8080/ews

Scope: https://outlook.office365.com/.default

Auth. Endpoint (V2): https://login.microsoftonline.com/3b6cd4f2-8795-4d5c-9158-de56700c1c23/oauth2/v2.0/au

Token Endpoint (V2): https://login.microsoftonline.com/3b6cd4f2-8795-4d5c-9158-de56700c1c23/oauth2/v2.0/to

Basic Authentication

☐ Use the following credentials

Username:

Password:

Domain:

Suggestion: Use UPN/SMTP address as username and leave domain empty for Outlook 365

☒ Store the credentials with the profile (encrypted)

Impersonation

☒ Use impersonation to open the messagestore

Id Type: SmtpAddress

Id: schoch@schochinf.onmicrosoft.com

Test OK Cancel

Wenn die Anmeldung erfolgreich war, können Sie die Mitarbeiter hinzufügen:

Klicken Sie dazu auf «Neu» und wählen Sie den Mitarbeiter aus dem Drop Down Feld «Mitarbeiter:» aus. Im Feld «Bezeichnung» wird die Emailadresse des Mitarbeiters erfasst. Mit dem Klick auf «Speichern» wird die Kalender ID ausgefüllt. Um die erste Synchronisation auszuführen, kann man anschliessend noch die Termine aus Schoch Termin ins Outlook und umgekehrt ausführen. Als Einstellung für die Synchronisationszeit haben sich 15 min bewährt.

Führen Sie diese Schritte für alle Mitarbeiter aus, die die Termine sehen sollen.