

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

Microsoft 365 admin center

Suchen

Dunkler Modus Dashboardansicht

en, Heidi Friedli

Kennwort zurücksetzen

wie Ihre Mehr anzeigen

Office im Web öffnen

Melden Sie sich bei Office.com an, um Word, Excel und mehr zu öffnen.

Abonnements Informationen

Dienste zugreifen kann, die in Ihren Microsoft 365 Abonnements

Kennwort zurücksetzen Durchsuchen der Benutzerliste

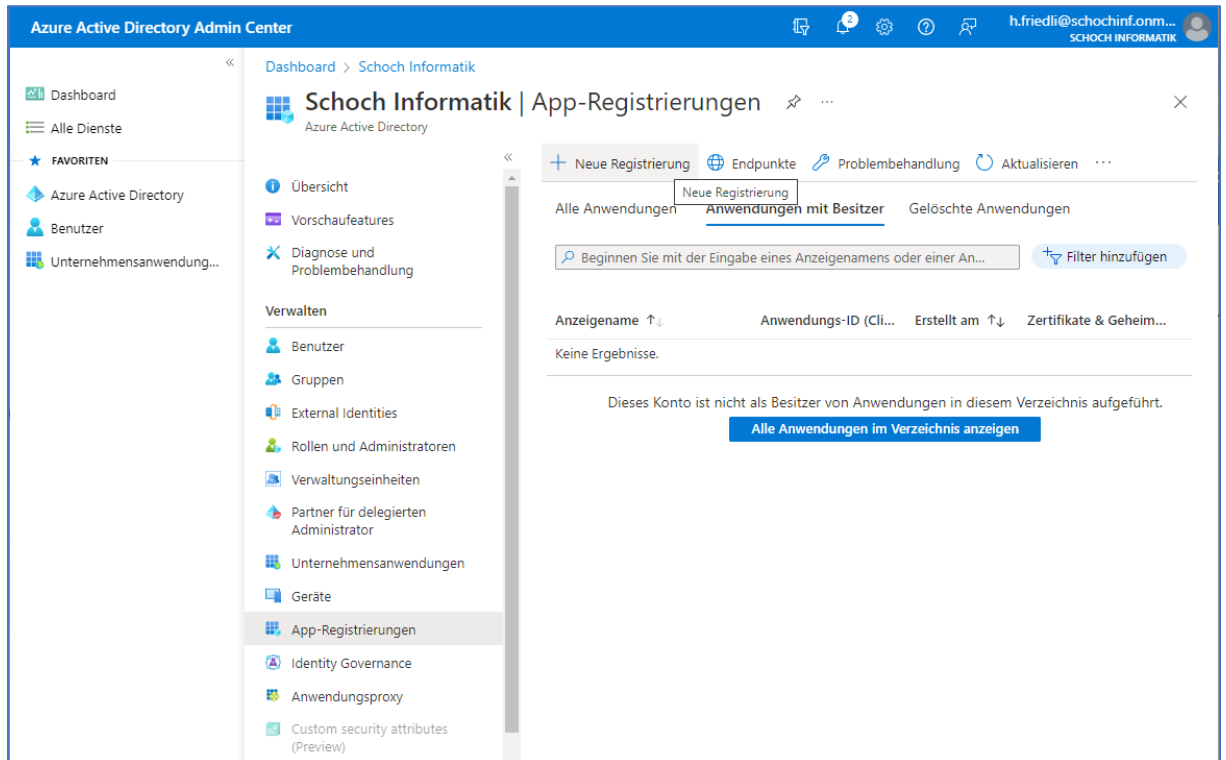
Benutzername für die Anmeldung	Licenses
d.lorez@schochinf.onmicrosoft.com	Microsoft 365 Business Standard
h.friedli@schochinf.onmicrosoft.com	Microsoft 365 Business Basic

Hilfe und Support

Feedback senden

<https://aad.portal.azure.com/schochinf.onmicrosoft.com>

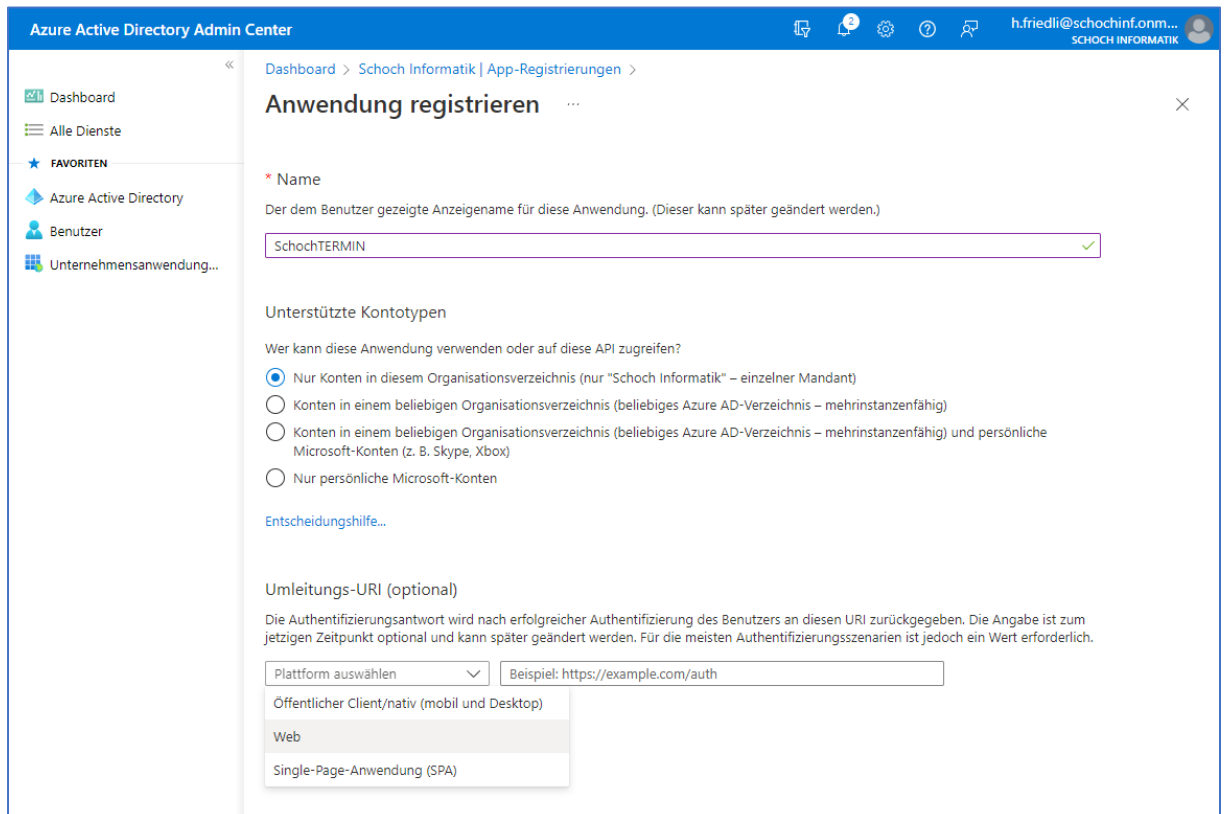
- **Azure Active Directory öffnen und App-Registrierungen auswählen**



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

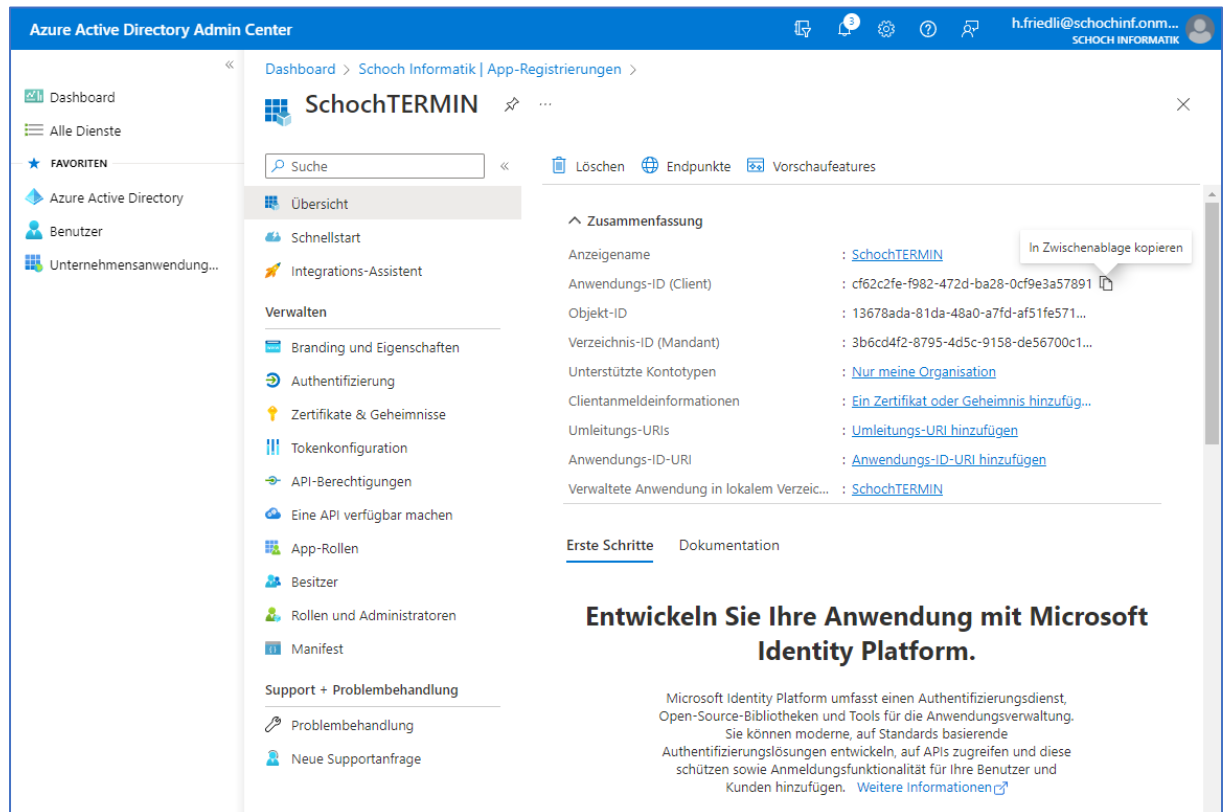
Name: SchochTERMIN

Kontentyp: Nur Konten in diesem Organisationsverzeichnis

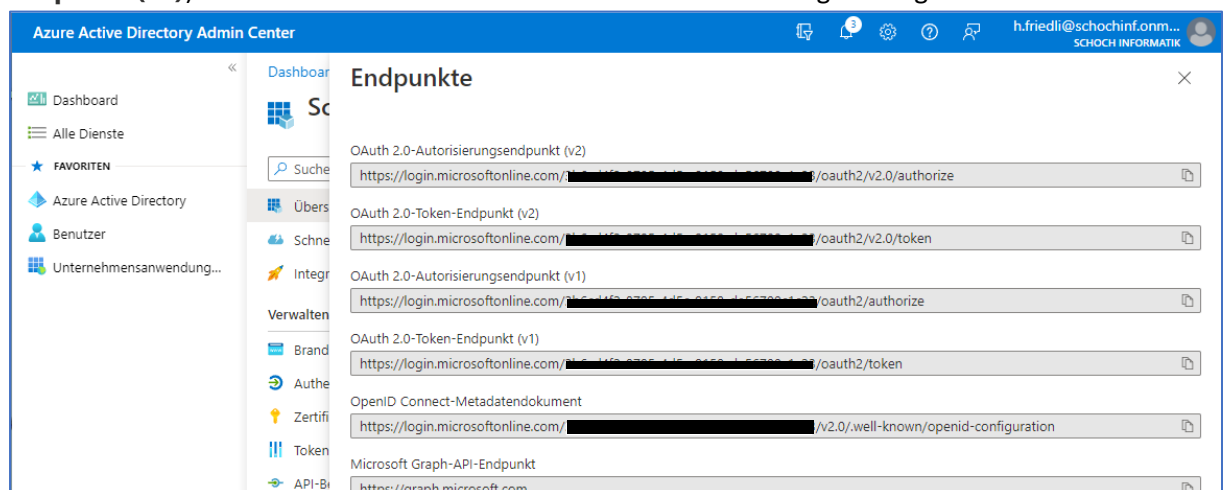


- **Den Vorgang mit Registrieren abschliessen.**

- 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 allerhand 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.

Azure Active Directory Admin Center

Dashboard > Schoch Informatik | App-Registrierungen > SchochTERMIN

SchochTERMIN | Zertifikate & Geheimnisse

Suche

Haben Sie Feedback für uns?

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 (0)** 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	Geheime ID
Für diese Anwendung wurden keine Clientgeheimnisse erstellt.			

Support + Problembehandlung

Problembehandlung

Neue Supportanfrage

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

Azure Active Directory Admin Center

Dashboard > Schoch Informatik | App-Registrierungen

Geheimen Clientschlüssel hinzufügen

Beschreibung: SchochTERMIN - ClientSecret

Gültig bis: 24 Monate

Hinzufügen Abbrechen

- 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!

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 Anwendungskenntwort bezeichnet.

+ Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert	In Zwischenablage kopieren	ID
SchochTERMIN - Clie...	8.11.2024	1LI8Q~0Gdkv4u...	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

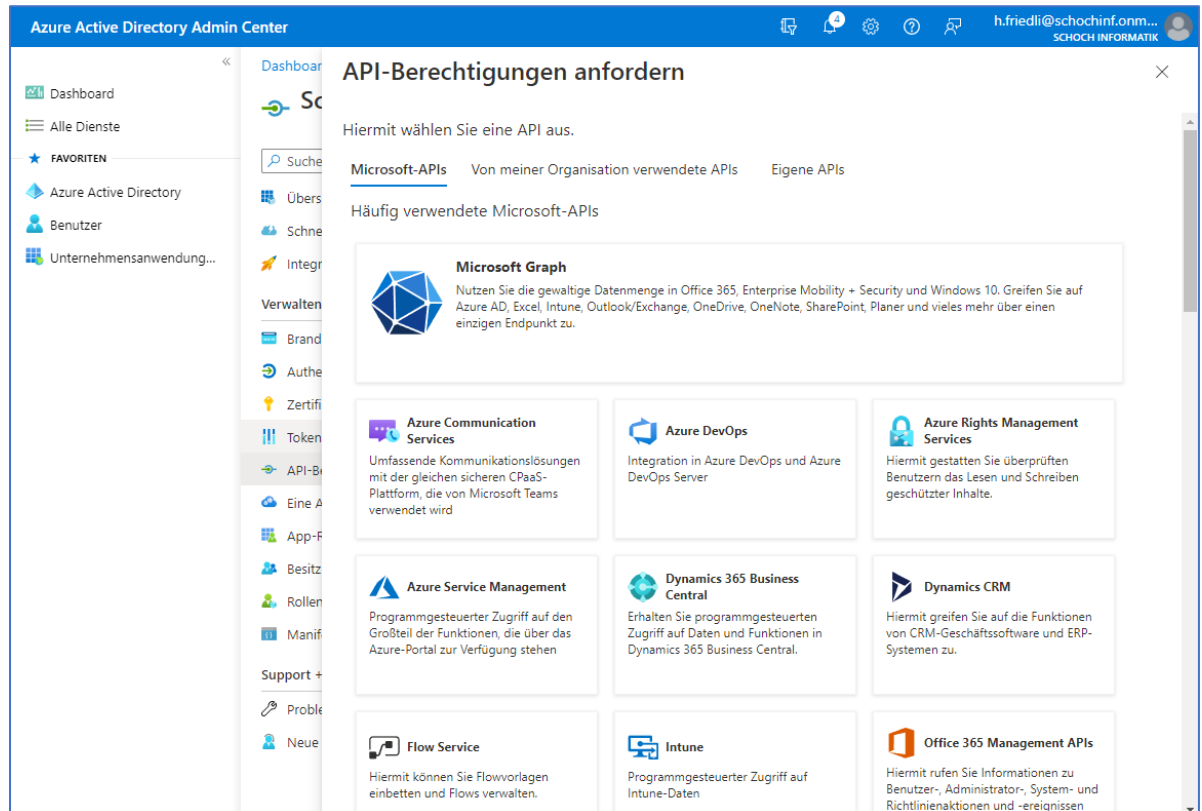
Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. [Weitere Informationen zu Berechtigungen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

+ Berechtigung hinzufügen ✓ Administratorzustimmung für "Schoch Informatik" erteilen

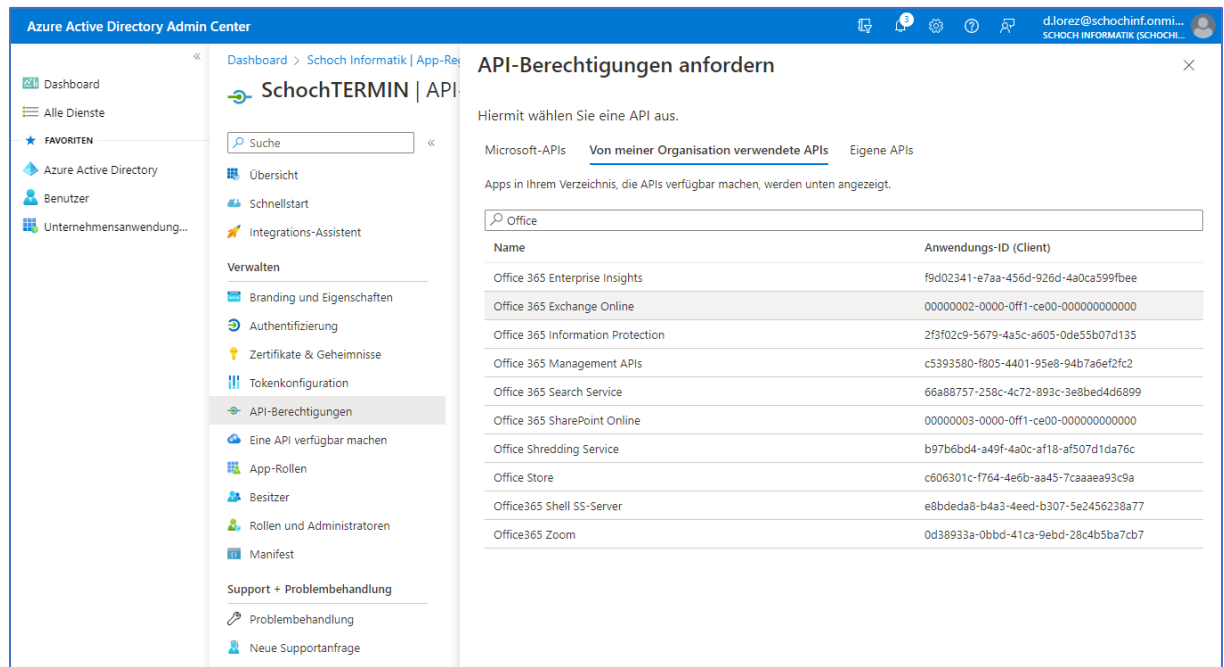
API/Berechtigungsname	Typ	Beschreibung	Administrator
Microsoft Graph (1)			
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein

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.

Azure Active Directory Admin Center

Dashboard > Schoch

API-Berechtigungen anfordern

Office 365 Exchange Online
https://ps.outlook.com

Welche Art von Berechtigungen sind für Ihre Anwendung erforderlich?

Delegierte Berechtigungen
Ihre Anwendung muss als der angemeldete Benutzer auf die API zugreifen.

Anwendungsberechtigungen
Ihre Anwendung wird als Hintergrunddienst oder Daemon ohne angemeldeten Benutzer ausgeführt.

Berechtigungen auswählen

ews

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](#)

Berechtigung	Administratoreinwilligung erforderlich...
EWS (1) <input checked="" type="checkbox"/> EWS.AccessAsUser.All ⓘ Als angemeldeter Benutzer über Exchange-Webdienste auf Postfächer zugreifen	Nein

Berechtigungen aktualisieren **Verwerfen**

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

Azure Active Directory Admin Center

Dashboard > Schoch Informatik | App-Registrierung

SchochTERMIN | API-Registrierung

API-Berechtigungen anfordern

Office 365 Exchange Online
https://ps.outlook.com

Welche Art von Berechtigungen sind für Ihre Anwendung erforderlich?

Delegierte Berechtigungen
Ihre Anwendung muss als der angemeldete Benutzer auf die API zugreifen.

Anwendungsberechtigungen
Ihre Anwendung wird als Hintergrunddienst oder Daemon ohne angemeldeten Benutzer ausgeführt.

Berechtigungen auswählen

Beginnen Sie mit der Eingabe einer Berechtigung, um diese Ergebnisse zu filtern.

Berechtigung	Administratoreinwilligung erforderlich...
Andere Berechtigungen (1) <input checked="" type="checkbox"/> full_access_as_app ⓘ Use Exchange Web Services with full access to all mailboxes	Ja

Berechtigungen hinzufügen **Verwerfen**

- 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.

Bestätigung der Administratoreinwilligung

Möchten Sie Ihre Einwilligung für die angeforderten Berechtigungen für alle Konten in "Schoch Informatik" erteilen? Durch diese Aktion werden in dieser Anwendung bereits vorhandene Datensätze zu Administratoreinwilligungen auf die unten aufgeführten Angaben aktualisiert.

[Ja](#) [Nein](#)

Zeige 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](#) ☒ Administratorenzustimmung für "Schoch Informatik" erteilen

API/Berechtigungsname	Typ	Administratorenzustimmung für "Schoch Informatik" erteilen	Administrator
Microsoft Graph (1)			
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein
Office 365 Exchange Online (2)			
EWS.AccessAsUser.All	Delegiert	Als angemeldeter Benutzer über Exchange-Webdie...	Nein
full_access_as_app	Anwendung	Use Exchange Web Services with full access to all m...	Ja

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

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

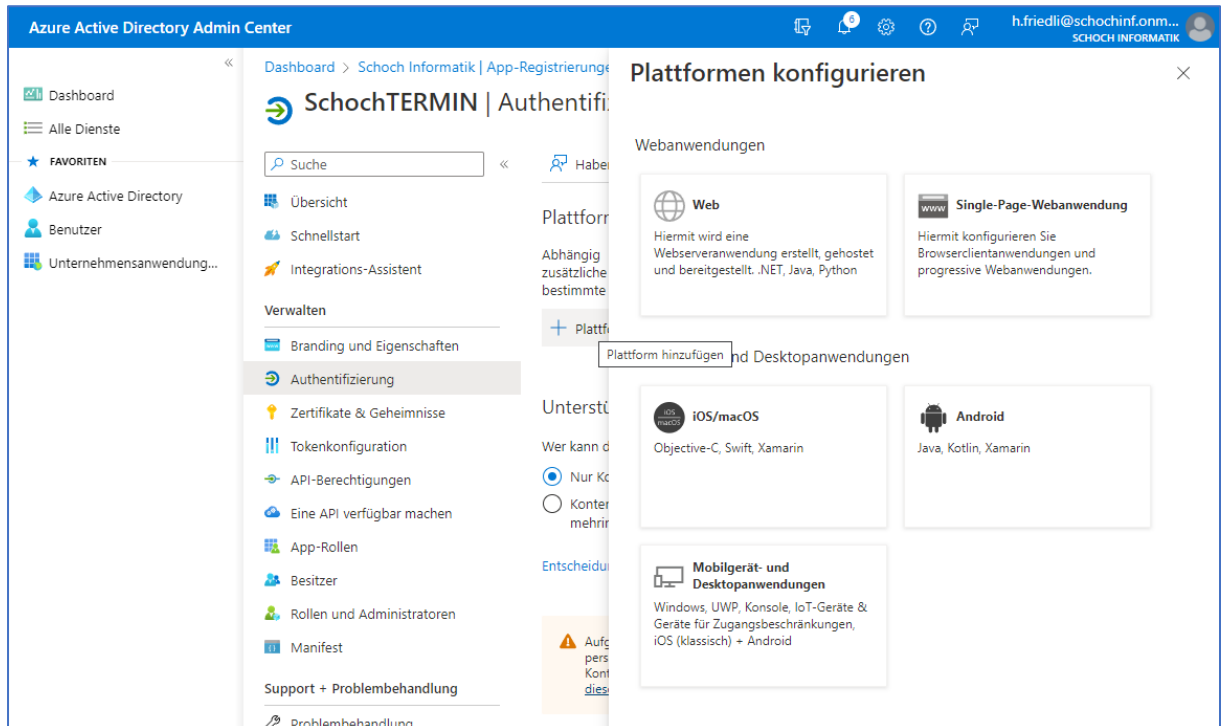
SchochTERMIN

[Löschen](#) [Endpunkte](#) [Vorschaufeatures](#)

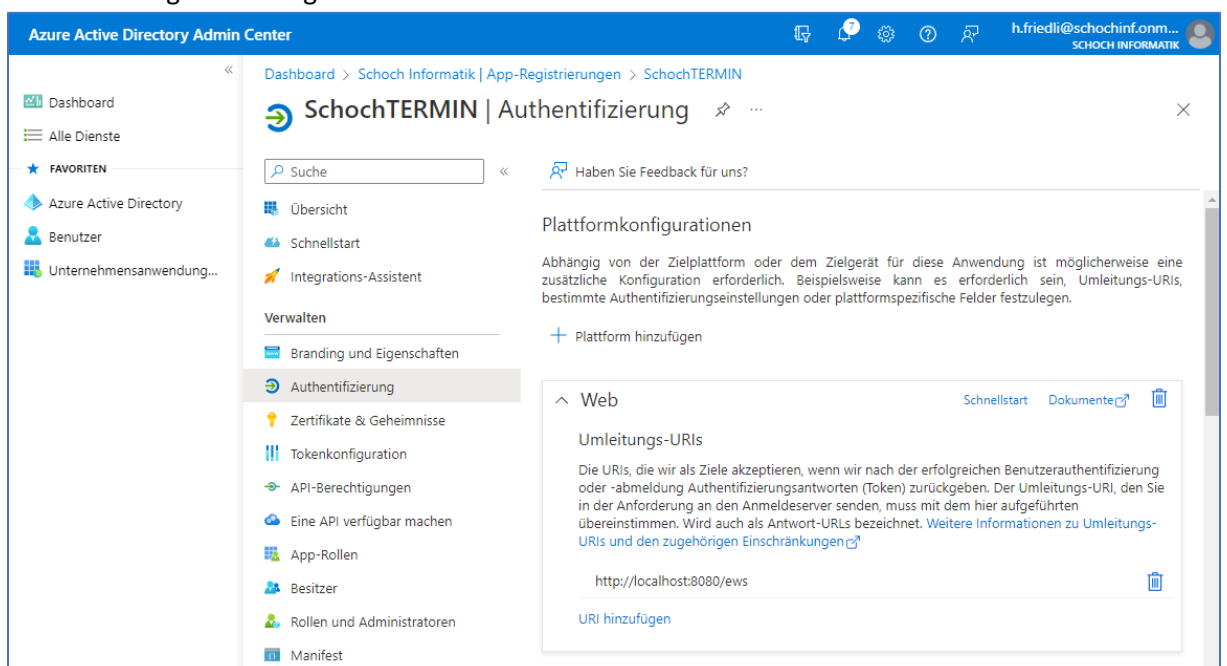
Zusammenfassung

Anzeigenname	: SchochTERMIN
Anwendungs-ID (Client)	: cf62c2fe-f982-472d-ba28-0cf9e3a57891
Objekt-ID	: 13678ada-81da-48a0-a7fd-af51fe571...
Verzeichnis-ID (Mandant)	: 3b6cd4f2-8795-4d5c-9158-de56700c1...
Unterstützte Kontotypen	: Nur meine Organisation
Clientanmeldeinformationen	: 0 Zertifikat_1 Geheimnis
Umleitungs-URIs	: Umleitungs-URI hinzufügen
Anwendungs-ID-URI	: Anwendungs-ID-URI hinzufügen
Verwaltete Anwendung in lokalem Verzeic...	: SchochTERMIN

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



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



Fertig 😊

SchochTERMIN: Anmeldung

EWS Profile

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: [REDACTED]

Client Secret: [REDACTED]

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

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

Auth. Endpoint (V2): https://login.microsoftonline.com/[REDACTED]/oauth2/v2.0/au

Token Endpoint (V2): https://login.microsoftonline.com/[REDACTED]/oauth2/v2.0/to

Basic Authentication

☐ Use the following credentials

Username: [REDACTED]

Password: [REDACTED]

Domain: [REDACTED]

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: [REDACTED]@[REDACTED].onmicrosoft.com

Test

OK

Cancel