

Konfiguration Microsoft 365 für Postfach-Zugriff aus ELO

Anwendung

Für den Zugriff aus ELO muss zuerst eine Anwendung im Microsoft Entra Admin Center mit einem administrativen Benutzer der Organisation neu registriert werden.

Je nach Organisationsstruktur(en) des Kunden, kann es auch sinnvoll sein, einen mandantenfähigen Kontotypen zu wählen.

Microsoft Entra Admin Center

Nach Ressourcen, Diensten und Dokumenten suchen (G+/)

Home > Unternehmensanwendungen > Alle Anwendungen > ELO | Übersicht > App-Registrierungen >

Anwendung registrieren

* Name

Der dem Benutzer gezeigte Anzeigenname für diese Anwendung. (Dieser kann später geändert werden.)

ELO

Unterstützte Kontotypen

Wer kann diese Anwendung verwenden oder auf diese API zugreifen?

- ☒ Nur Konten in diesem Organisationsverzeichnis (nur "-----" – einzelner Mandant)
- ☐ Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig)
- ☐ Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig) und persönliche Microsoft-Konten (z. B. Skype, Xbox)
- ☐ Nur persönliche Microsoft-Konten

[Entscheidungshilfe...](#)

Umleitungs-URI (optional)

Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zurückgegeben. Die Angabe ist zum jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch ein Wert erforderlich.

Plattform auswählen Beispiel: <https://example.com/auth>

Registrieren Sie eine App, an der Sie gerade arbeiten. Integrieren Sie Katalog-Apps und andere Apps von außerhalb Ihrer Organisation, indem Sie sie aus [Unternehmensanwendungen](#) hinzufügen.

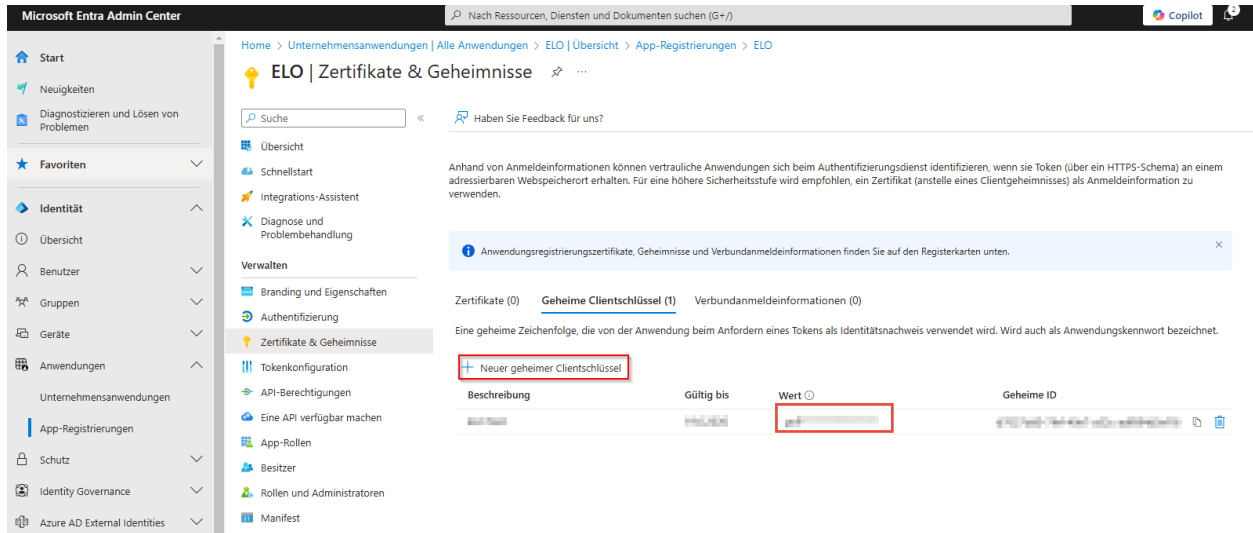
Indem Sie den Vorgang fortsetzen, stimmen Sie den [Microsoft-Plattformrichtlinien](#) zu.

Registrieren

Geheimer Clientschlüssel (Client Secret)

Für die Anwendung muss ein geheimer Clientschlüssel erstellt werden. Die maximale Gültigkeit von 2 Jahren ist zu empfehlen.

Achtung: Der Wert des geheimen Schlüssels ist nur bei der Erstellung sichtbar und muss gleich dokumentiert werden, um ihn später verwenden zu können.



Berechtigungen

Berechtigungen müssen an zwei Stellen vergeben werden. Die erste Stelle sind die API-Berechtigungen der registrierten Anwendung. Zusätzliche müssen im Exchange Berechtigungen für die Anwendung auf die abzuholenden Postfächer gewährt werden.

API-Berechtigungen der registrierten Anwendung

Es werden folgende Berechtigungen der API „Office 365 Exchange Online“ benötigt:

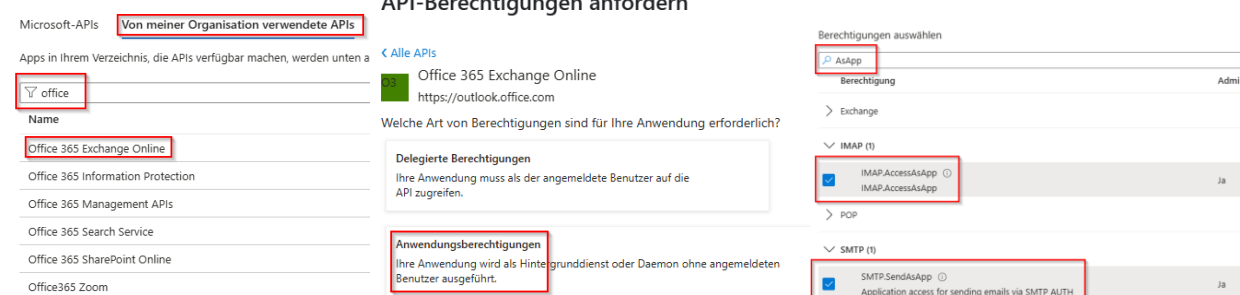
- **IMAP.AccessAsApp** (Allow application to access user's mailbox via IMAP protocol)
- **SMTP.SendAsApp** (Allows the app to have send access to all mailboxes)

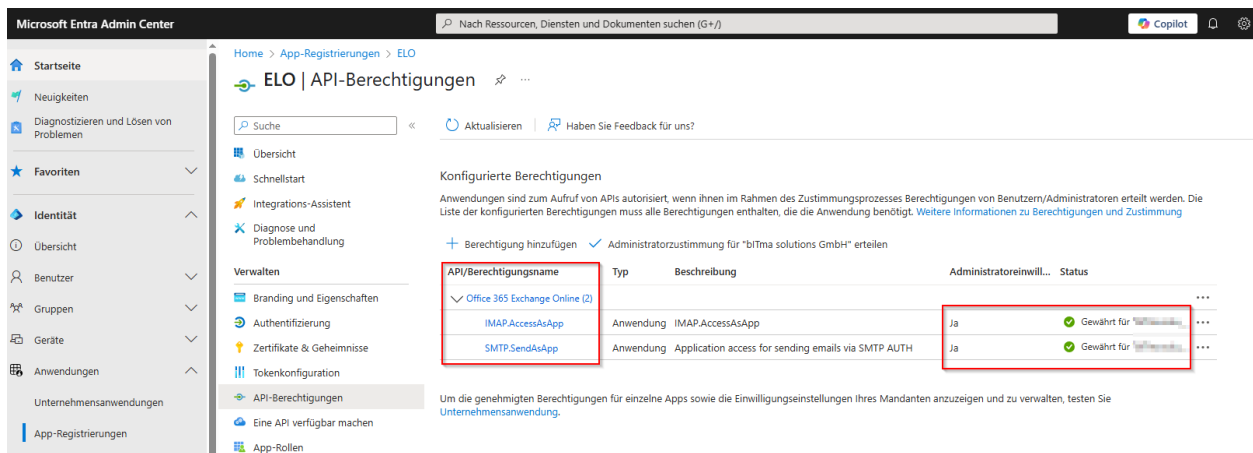
Diese Berechtigungen erlauben sowohl ein Abrufen als auch Versenden von E-Mails. Ist nur der Abruf gewünscht, kann *SMTP.SendAsApp* entfallen. Ist nur der Versand gewünscht kann *IMAP.AccessAsApp* entfallen.

Für die gesetzten Berechtigungen muss jeweils auch die **Administratoreinwilligung** gewährt werden.

API-Berechtigungen anfordern

Hiermit wählen Sie eine API aus.





Berechtigungen im Exchange auf Postfächer

Für die Anwendung wird im Exchange ein entsprechender Dienstprinzipal angelegt. Diesem Dienstprinzipal werden dann jeweils Berechtigungen auf die abzurufenden Postfächer gewährt.

Es wird ein Zugriff auf den Exchange-Online über die Powershell benötigt. Hierfür muss das Powershell-Modul *ExchangeOnlineManagement* installiert und in der aktuellen Powershell-Sitzung verfügbar sein.

Dies kann mit folgenden zwei Powershell-Befehlen durchgeführt werden:

```
Install-Module -Name ExchangeOnlineManagement  
Import-Module -Name ExchangeOnlineManagement
```

1. Herstellen einer Verbindung zum Exchange-Online

```
Connect-ExchangeOnline -Organization Organisationsname
```

Jetzt anmelden mit administrativem Benutzer im grafischen Dialog

Organisationsname ist hier normalerweise der Teil der E-Mail-Adresse nach dem @.

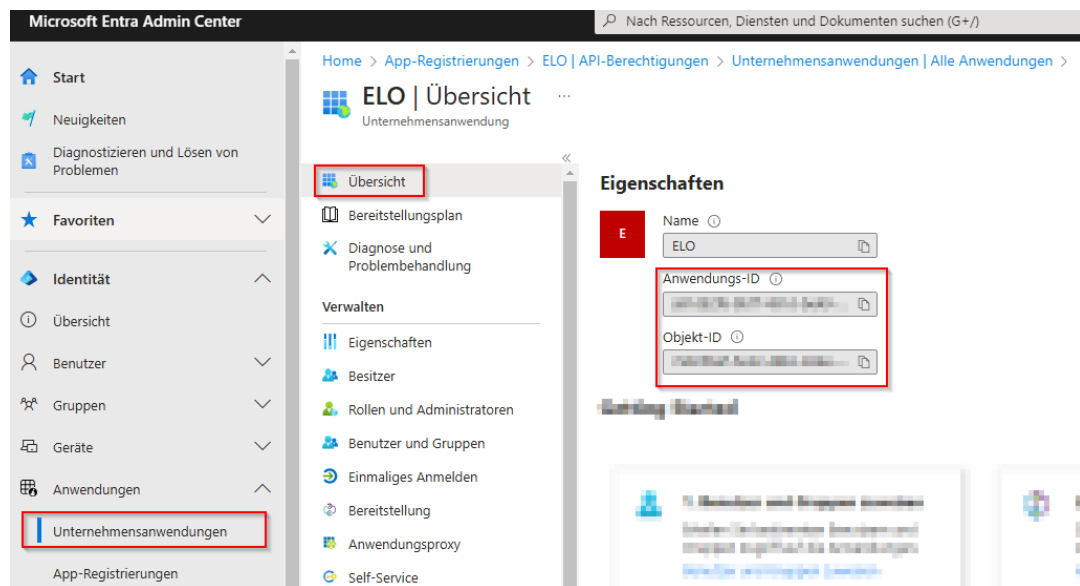
2. Anlegen eines Dienstprinzipals für die registrierte Anwendung

```
New-ServicePrincipal -AppId AppId -ObjectId ObjectId -DisplayName  
DisplayName
```

Die *AppId* und *ObjectId* sind der Übersicht im Bereich „Unternehmensanwendungen“ zu entnehmen.

Achtung: Die *ObjectId* im Bereich „App-Registrierungen“ unterscheidet sich von der im Bereich „Unternehmensanwendungen“ und darf deshalb NICHT verwendet werden!!!

Als *DisplayName* sollte ein eindeutiger, sprechender Name (z.B. „ELO“) gewählt werden, mit dem dieser Dienstprinzipal gut von anderen unterschieden werden kann.



3. Auslesen der Id des gerade angelegten Dienstprinzips

```
Get-ServicePrincipal -Identity Identity | fl DisplayName, Id
```

- *Identity*: vergebener DisplayName aus Punkt 2

Die Id des Dienstprinzips wird in Schritt 4 benötigt

4. Vergeben der Berechtigungen für den Dienstprinzipal auf ein Postfach

```
Add-MailboxPermission -Identity Identity -User User -AccessRights  
AccessRights
```

- *Identity*: Postfach auf das Berechtigungen gewährt werden sollen (am einfachsten ist hier die Angabe der primären E-Mail-Adresse)
- *User*: Id des Dienstprinzips
- *AccessRights*: FullAccess

5. Trennung der Verbindung zum Exchange-Online

```
Disconnect-ExchangeOnline
```

Trennen ohne Bestätigungsaufforderung:

```
Disconnect-ExchangeOnline -Confirm:$false
```