

Anbindung eines Exchange-Online-Postfachs an CADOSYS

Microsoft Graph und Exchange Online Application RBAC

Administrations- und Einrichtungsanleitung

Ziel dieser Anleitung

Die Einrichtung soll sicher, nachvollziehbar und reproduzierbar sein. Microsoft Entra wird über wenige, konsistente UI-Skizzen erklärt. Die Exchange-Online-Konfiguration kann anschließend vollständig über einen geführten PowerShell-Assistenten erfolgen.

Inhalt

1. Einleitung	4
2. Ablauf im Überblick	4
3. Voraussetzungen	4
4. Teil A – App Registration in Microsoft Entra	5
4.1 Microsoft Entra Admin Center öffnen	5
4.2 Neue App Registration erstellen	6
4.3 Geheimen Clientschlüssel erstellen	6
4.4 Client-ID und Tenant-ID notieren	7
4.5 Objekt-ID der Unternehmensanwendung notieren	8
4.6 Welche Werte müssen jetzt vorliegen?	8
5. Teil B – Geführter PowerShell-Assistent	8
5.1 PowerShell-Assistent herunterladen und für die Ausführung freigeben	9
5.2 Assistent starten	10
5.3 Welche Angaben fragt der Assistent ab?	10
5.4 Was prüft der Assistent vor Änderungen?	11
6. Teil C – Exchange Online manuell per PowerShell	11
6.1 ExchangeOnlineManagement prüfen und installieren	11
6.2 Verbindung herstellen	11
6.3 Variablen festlegen	11
6.4 E-Mail-aktivierte Sicherheitsgruppe erstellen	12
6.5 Service Principal in Exchange Online registrieren	12
6.6 Management Scope erstellen	12
6.7 Graph-Rolle prüfen und zuweisen	13
6.8 Erlaubtes Postfach testen	13
6.9 Verbindung trennen	13
7. Konfiguration prüfen	13
8. Einrichtung rückgängig machen	14
9. CADOSYS Buchhalter konfigurieren	14
9.1 E-Mail-Import-Postfächer öffnen	14
9.2 Neue Microsoft-Graph-Anbindung auswählen	15
9.3 Graph-Konfiguration ausfüllen	15
9.4 Ordner abrufen und auswählen	16
9.5 Verbindung testen und aktivieren	16
9.6 Bestehende Exchange-Online-Konfiguration auf Graph migrieren	17

9.7 Alte und neue Konfiguration während der Umstellung	17
10. Fehleranalyse	18
10.1 Das Skript darf nicht ausgeführt werden	18
10.2 ExchangeOnlineManagement fehlt	18
10.3 Service Principal wird nicht gefunden	18
10.4 Postfach ist InScope = False	18
11. Weiterführende Microsoft-Dokumentation	19
12. Konfigurationsblatt – Werte für die Einrichtung	20
13. Anhang – Zweck des PowerShell-Assistenten	21

1. Einleitung

In dieser Anleitung wird beschrieben, wie ein Exchange Online Postfach für den E-Mail-Abruf durch CADOSYS eingerichtet wird. CADOSYS authentifiziert sich dabei als Anwendung und greift über Microsoft Graph auf Exchange Online zu. Es ist kein interaktiv angemeldeter Benutzer für den laufenden Mailabruf erforderlich.

Die technische Identität wird als App Registration im Microsoft Entra Admin Center angelegt. Der eigentliche Zugriff auf Postfächer wird anschließend in Exchange Online über Application RBAC eingerichtet. Dadurch kann die Berechtigung Application Mail.ReadWrite auf ausdrücklich freigegebene Postfächer begrenzt werden.

Die Einrichtung ist bewusst in zwei Bereiche aufgeteilt:

- Microsoft Entra Admin Center: App Registration, geheimer Clientschlüssel und benötigte IDs.
- Exchange Online PowerShell: Sicherheitsgruppe, Service Principal, Management Scope, Application-RBAC-Rolle und Tests.
- CADOSYS: Eintragen der erzeugten Zugangsdaten und Auswahl des zu verarbeitenden Postfachs.

Warum Application RBAC?

Microsoft führt Application RBAC als aktuellen Mechanismus für granularen, ressourcenbezogenen App-Zugriff in Exchange Online. Die Rolle Application Mail.ReadWrite entspricht der Graph-Berechtigung Mail.ReadWrite, kann aber mit einem Ressourcenbereich auf bestimmte Postfächer eingeschränkt werden. Organisationsweite Entra-Berechtigungen und RBAC-Zuweisungen wirken unabhängig voneinander.

2. Ablauf im Überblick

1. App Registration im Microsoft Entra Admin Center erstellen.
2. Geheimen Clientschlüssel erzeugen und sicher zwischenspeichern.
3. Anwendungs-ID (Client), Verzeichnis-ID (Mandant) und Objekt-ID der Unternehmensanwendung notieren.
4. PowerShell-Assistent herunterladen, prüfen und starten.
5. Assistent mit Exchange Online verbinden lassen.
6. E-Mail-aktivierte Sicherheitsgruppe und erlaubte Postfächer einrichten.
7. Exchange Service Principal, Management Scope und Application Mail.ReadWrite konfigurieren.
8. Berechtigungen prüfen und ein erlaubtes Postfach testen.
9. Zugangsdaten in CADOSYS eintragen und den Mailabruf testen.

Wichtig

Die Microsoft Graph Berechtigung Mail.ReadWrite wird in dieser Variante nicht zusätzlich als organisationsweite Application Permission im Entra Admin Center vergeben. Die Berechtigung wird über Exchange Online Application RBAC bereitgestellt und dort auf die freigegebenen Postfächer eingeschränkt.

3. Voraussetzungen

- Ein Microsoft 365 / Exchange Online Mandant.
- Ein Administratorkonto, das eine App Registration in Microsoft Entra erstellen darf.

- Für die Exchange-Konfiguration ein Konto mit Exchange Administrator und den erforderlichen Exchange-RBAC-Rechten; für die Vergabe der hier verwendeten Application-RBAC-Konfiguration ist typischerweise Organization Management erforderlich.
- Windows PowerShell 5.1 oder PowerShell 7 auf einem administrierbaren Windows-System.
- Internetverbindung zur PowerShell Gallery und zu Exchange Online.
- Die E-Mail-Adressen der Postfächer, auf die CADOSYS zugreifen soll.

4. Teil A – App Registration in Microsoft Entra

Die folgenden Abbildungen sind bewusst keine Screenshots. Sie zeigen die für diese Anleitung relevanten Bereiche in einer einheitlichen, vereinfachten Darstellung. Microsoft kann Bezeichnungen oder Positionen in der Weboberfläche ändern; die fachlichen Begriffe bleiben die Orientierung.

Konfigurationsblatt verwenden

Die in Entra ermittelten Werte können während der Einrichtung im „Konfigurationsblatt“ am Ende dieses Dokuments notiert werden. Verweisen Sie dort insbesondere auf Client-ID, Tenant-ID, Objekt-ID und die E-Mail-Adresse des freigegebenen Postfachs. Den geheimen Clientschlüssel nur temporär notieren und nach erfolgreicher Einrichtung wieder entfernen.

4.1 Microsoft Entra Admin Center öffnen

Öffnen Sie <https://entra.microsoft.com> und melden Sie sich mit einem Administratorkonto an.

Skizze 1 – App-Registrierungen öffnen

Microsoft Entra Admin Center	
Entra ID > App-Registrierungen	
Entra ID Übersicht > App-Registrierungen Unternehmensanwendungen Rollen und Administratoren	App-Registrierungen Aktion Neue Registrierung Ziel Eine technische Identität für CADOSYS anlegen.

Skizze – die Bezeichnungen entsprechen der Microsoft-Oberfläche; Darstellung und Positionen können sich ändern.

4.2 Neue App Registration erstellen

10. Wählen Sie unter Entra ID den Punkt App-Registrierungen.
11. Klicken Sie auf Neue Registrierung.
12. Vergeben Sie einen eindeutigen Namen, beispielsweise „CADOSYS-Buchhalter Firmenname“.
13. Wählen Sie „Nur Konten in diesem Organisationsverzeichnis“ (Single Tenant), sofern für Ihren Mandanten nichts anderes vorgesehen ist.
14. Registrieren Sie die Anwendung.

Skizze 2 – Anwendung registrieren

Microsoft Entra Admin Center	
Entra ID > App-Registrierungen > Neue Registrierung	
Grundlagen > App-Registrierung Authentifizierung Zertifikate & Geheimnisse	Anwendung registrieren Name CADOSYS-Buchhalter <Firmenname> Unterstützte Kontotypen Nur Konten in diesem Organisationsverzeichnis Umleitungs-URI Für die App-only Graph-Anbindung nicht erforderlich. <i>Die genaue Oberfläche kann weitere optionale Felder anzeigen.</i>

Skizze – die Bezeichnungen entsprechen der Microsoft-Oberfläche; Darstellung und Positionen können sich ändern.

4.3 Geheime Clientschlüssel erstellen

15. Öffnen Sie in der App Registration unter Verwalten den Bereich Zertifikate & Geheimnisse.
16. Wählen Sie Geheime Clientschlüssel und Neuer geheimer Clientschlüssel.
17. Vergeben Sie eine verständliche Beschreibung und eine zur eigenen Sicherheitsrichtlinie passende Gültigkeitsdauer.
18. Kopieren Sie unmittelbar nach dem Anlegen den Wert des Geheimnisses. Der Wert ist später nicht noch einmal vollständig sichtbar.

Skizze 3 – Client Secret

Microsoft Entra Admin Center	
App-Registrierung > Zertifikate & Geheimnisse	
- Übersicht - Authentifizierung - API-Berechtigungen > Zertifikate & Geheimnisse - Manifest	Geheime Clientschlüssel Beschreibung CADOSYS Exchange Online Gültigkeit Gemäß Sicherheitsrichtlinie Wert Nur direkt nach Erstellung vollständig sichtbar <i>Nicht „Geheimnis-ID“, sondern den tatsächlichen Wert für CADOSYS sichern.</i>

Skizze – die Bezeichnungen entsprechen der Microsoft-Oberfläche; Darstellung und Positionen können sich ändern.

Sicherheits-Hinweis

Der geheime Clientschlüssel ist wie ein Kennwort der Anwendung zu behandeln. Er gehört nicht in Tickets, ungeschützte Dokumentationen oder Quellcode. Nach Ablauf muss ein neuer Schlüssel erstellt und in CADOSYS hinterlegt werden.

4.4 Client-ID und Tenant-ID notieren

- Öffnen Sie den Bereich Übersicht der App Registration.
- Notieren Sie die Anwendungs-ID (Client).
- Notieren Sie die Verzeichnis-ID (Mandant).

Skizze 4 – IDs der App Registration

Microsoft Entra Admin Center	
App-Registrierung > Übersicht	
> Übersicht - Authentifizierung - API-Berechtigungen - Zertifikate & Geheimnisse	Essentials Anwendungs-ID (Client) 00000000-0000-0000-0000-000000000000 Verzeichnis-ID (Mandant) 00000000-0000-0000-0000-000000000000

Skizze – die Bezeichnungen entsprechen der Microsoft-Oberfläche; Darstellung und Positionen können sich ändern.

4.5 Objekt-ID der Unternehmensanwendung notieren

Exchange Online benötigt beim Anlegen des Exchange Service Principals die Objekt-ID der zugehörigen Unternehmensanwendung. Diese ist nicht identisch mit der Objekt-ID der App Registration.

22. Öffnen Sie Entra ID > Unternehmensanwendungen > Alle Anwendungen.
23. Suchen Sie die soeben erstellte Anwendung über den Namen oder die Client-ID.
24. Öffnen Sie die Anwendung und notieren Sie deren Objekt-ID.

Skizze 5 – Unternehmensanwendung

Microsoft Entra Admin Center	
Entra ID > Unternehmensanwendungen > <CADOSYS App>	
Entra ID App-Registrierungen > Unternehmensanwendungen Alle Anwendungen	Unternehmensanwendung Anwendungs-ID entspricht der Client-ID der App Registration Objekt-ID für New-ServicePrincipal erforderlich

Skizze – die Bezeichnungen entsprechen der Microsoft-Oberfläche; Darstellung und Positionen können sich ändern.

4.6 Welche Werte müssen jetzt vorliegen?

Wert	Woher?	Wofür?
Anwendungs-ID (Client)	App Registration > Übersicht	Identifiziert die App gegenüber Microsoft Graph und Exchange Online
Verzeichnis-ID (Mandant)	App Registration > Übersicht	Identifiziert den Microsoft-365-Mandanten
Geheimer Clientschlüssel – Wert	Zertifikate & Geheimnisse	Anmeldung der Anwendung in CADOSYS
Objekt-ID der Unternehmensanwendung	Unternehmensanwendungen > Übersicht	Registrierung des Service Principals in Exchange Online

5. Teil B – Geführter PowerShell-Assistent

Der PowerShell-Assistent „Setup-CADOSYS-ExchangeOnlineGraph.ps1“ übernimmt die Exchange-Online-Konfiguration. Er fragt die erforderlichen Werte ab, prüft vorhandene Objekte und erklärt vor schreibenden bzw. löschenden Aktionen, was geändert wird.

Der Assistent bietet vier Arbeitsmodi:

- Prüfen: vorhandene Exchange-Konfiguration einer App über die Client-ID ermitteln.
- Einrichten: Sicherheitsgruppe, Mitglieder, Service Principal, Scope und Application Mail.ReadWrite konfigurieren.

- Testen: RBAC-Zuweisungen anzeigen und einzelne Postfächer mit Test-ServicePrincipalAuthorization prüfen.
- Rückgängig machen: die zur App gehörenden Exchange-Objekte ermitteln und nach Bestätigung in einer sicheren Reihenfolge entfernen.

5.1 PowerShell-Assistent herunterladen und für die Ausführung freigeben

Der CADOSYS PowerShell-Assistent wird über den CADOSYS-Downloadbereich bereitgestellt:

[Setup-CADOSYS-ExchangeOnlineGraph.zip](#)

Laden Sie die Datei „Setup-CADOSYS-ExchangeOnlineGraph.zip“ herunter und speichern Sie sie beispielsweise unter C:\CADOSYS\ExchangeGraphSetup. Entpacken Sie den Inhalt am selben Ort. In der Zip-Datei sind „Setup-CADOSYS-ExchangeOnlineGraph.ps1“ und „Setup-CADOSYS-ExchangeOnlineGraph.ps1.sha256“ enthalten. Öffnen Sie anschließend eine PowerShell und wechseln Sie in diesen Ordner:

```
Set-Location "C:\CADOSYS\ExchangeGraphSetup"
```

Bevor Sie das Skript zum ersten Mal ausführen, prüfen Sie bitte, ob die heruntergeladene Datei unverändert ist. Berechnen Sie dazu zunächst den SHA-256-Prüfwert des Skripts:

```
Get-FileHash `
  -Path ".\Setup-CADOSYS-ExchangeOnlineGraph.ps1" `
  -Algorithm SHA256
```

Die Ausgabe enthält den lokal berechneten SHA-256-Prüfwert.

Lesen Sie anschließend den von CADOSYS bereitgestellten Prüfwert aus der heruntergeladenen Prüfsummendatei:

```
Get-Content ".\Setup-CADOSYS-ExchangeOnlineGraph.ps1.sha256"
```

Vergleichen Sie beide Werte miteinander. Der lokal berechnete SHA-256-Prüfwert muss vollständig mit dem Prüfwert aus der Datei Setup-CADOSYS-ExchangeOnlineGraph.ps1.sha256 übereinstimmen.

Prüfen Sie anschließend die für PowerShell geltenden Ausführungsrichtlinien:

```
Get-ExecutionPolicy -List
```

Windows kennzeichnet Dateien aus dem Internet häufig mit einer Sicherheitsmarkierung. Wenn Sie die Datei geprüft haben und der Quelle vertrauen, entfernen Sie diese Markierung für das Skript:

```
Unblock-File -Path ".\Setup-CADOSYS-ExchangeOnlineGraph.ps1"
```

Keine pauschale Umgehung der Ausführungsrichtlinie

Setzen Sie die Execution Policy nicht pauschal auf Bypass oder Unrestricted. Von einer Organisation per Gruppenrichtlinie vorgegebene Einstellungen dürfen nicht umgangen werden.

Falls die effektive Richtlinie für den aktuellen Benutzer Restricted ist und keine Unternehmensrichtlinie entgegensteht, kann RemoteSigned für den aktuellen Benutzer gesetzt werden:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
```

Danach kann der Assistent gestartet werden:

```
.\Setup-CADOSYS-ExchangeOnlineGraph.ps1
```

Wenn Sie die CurrentUser-Richtlinie ausschließlich für diese Einrichtung verändert haben, können Sie sie nach Abschluss wieder zurücksetzen:

```
Set-ExecutionPolicy -ExecutionPolicy Undefined -Scope CurrentUser
```

5.2 Assistent starten

```
Set-Location "C:\Pfad\zum\Download"
.\Setup-CADOSYS-ExchangeOnlineGraph.ps1
```

Der Assistent prüft zuerst, ob das Modul ExchangeOnlineManagement verfügbar ist. Fehlt es, bietet er die Installation für den aktuellen Benutzer an. Danach erscheint das Hauptmenü.

- 1 Voraussetzungen und vorhandene Konfiguration prüfen
- 2 Exchange Online für CADOSYS einrichten
- 3 Berechtigungen / Konfiguration testen
- 4 Exchange Online Konfiguration rückgängig machen
- 5 Beenden

5.3 Welche Angaben fragt der Assistent ab?

Angabe	Bedeutung
Anwendungs-ID (Client-ID) der CADOSYS App-Registrierung	Diese ID stammt aus der App-Registrierung in Microsoft Entra. Sie identifiziert die Anwendung, die CADOSYS später für den Zugriff über Microsoft Graph verwendet.
Objekt-ID der zugehörigen Unternehmensanwendung	Diese Objekt-ID stammt aus dem Bereich „Unternehmensanwendungen“ in Microsoft Entra. Sie identifiziert die konkrete Unternehmensanwendung im Tenant.
Name der CADOSYS Sicherheitsgruppe für erlaubte Postfächer	Anzeigenname der E-Mail-aktivierten Sicherheitsgruppe. Über diese Gruppe wird festgelegt, auf welche Postfächer CADOSYS zugreifen darf.
Besitzer der Sicherheitsgruppe	E-Mail-Adresse eines Administrators, der als Besitzer der Sicherheitsgruppe eingetragen wird und diese verwalten darf.
E-Mail-Adresse(n) der Postfächer, aus denen CADOSYS E-Mails abrufen darf	Ein oder mehrere Exchange-Online-Postfächer. Mehrere Adressen können kommagetrennt eingegeben werden. Der Assistent prüft, ob die Postfächer existieren, und nimmt sie in die Sicherheitsgruppe auf.
Bezeichnung der CADOSYS Anwendung in Exchange	Lesbarer Name, unter dem die CADOSYS Anwendung in Exchange Online registriert wird. Dieser Name dient nur zur Identifikation.
Name des Bereichs der für CADOSYS erlaubten Postfächer	Name des Exchange-Postfachbereichs. Dieser Bereich begrenzt den Zugriff der CADOSYS Anwendung auf die Mitglieder der Sicherheitsgruppe.
Name der Exchange-Rollenzuweisung für den CADOSYS Graph-Zugriff	Lesbarer Name der Application-RBAC-Zuweisung. Über diese Zuweisung erhält die CADOSYS Anwendung die Rolle Application Mail.ReadWrite, beschränkt auf den zuvor definierten Postfachbereich.

5.4 Was prüft der Assistent vor Änderungen?

- Ist ExchangeOnlineManagement installiert?
- Besteht bereits eine Exchange-Online-Verbindung?
- Sind die eingegebenen GUIDs formal gültig?
- Existieren die angegebenen Postfächer?
- Ist für die App bereits ein Exchange Service Principal vorhanden?
- Existieren Gruppe, Scope oder Rollenzuweisung bereits?
- Ist die Rolle Application Mail.ReadWrite verfügbar?
- Passt ein vorhandener Scope tatsächlich zur gewünschten Sicherheitsgruppe?

Sicheres Verhalten

Vor der eigentlichen Einrichtung zeigt der Assistent alle geplanten Werte gesammelt an. Ohne ausdrückliche Bestätigung werden keine Exchange-Objekte erstellt. Beim Rückbau werden die gefundenen Objekte ebenfalls zunächst angezeigt.

6. Teil C – Exchange Online manuell per PowerShell

Der Assistent vereinfacht die Einrichtung, ersetzt aber nicht die Dokumentation. Die folgenden Schritte zeigen vollständig, welche Exchange-Online-Aktionen durchgeführt werden. Sie können damit jede Änderung nachvollziehen oder die Einrichtung ohne Assistent manuell vornehmen.

6.1 ExchangeOnlineManagement prüfen und installieren

```
Get-Module -Name ExchangeOnlineManagement -ListAvailable |
Sort-Object Version -Descending |
Select-Object Name, Version, Path
```

Wenn das Modul fehlt:

```
Install-Module -Name ExchangeOnlineManagement -Scope CurrentUser
```

```
Import-Module ExchangeOnlineManagement
```

6.2 Verbindung herstellen

```
Connect-ExchangeOnline -UserPrincipalName "administrator@ihredomain.de" -ShowBanner:$false
```

```
Get-ConnectionInformation | Format-Table State, UserPrincipalName
```

6.3 Variablen festlegen

```
$AppId = "ANWENDUNGS-ID-DER-APPREGISTRIERUNG"
$ServicePrincipalObjectId = "OBJEKT-ID-DER-UNTERNEHMENSANWENDUNG"
$ExchangeServicePrincipalName = "CADOSYS Exchange Zugriff"
$GroupName = "CADOSYS erlaubte Postfaecher"
$GroupAddress = "cadosys-postfaecher@kunde.de"
$GroupOwner = "administrator@kunde.de"
$ScopeName = "CADOSYS erlaubte Postfaecher"
$RoleAssignmentName = "CADOSYS Graph Mail Zugriff"
$AllowedMailbox = "beispiel@kunde.de"
```

6.4 E-Mail-aktivierte Sicherheitsgruppe erstellen

```
New-DistributionGroup `
  -Name $GroupName `
  -Type Security `
  -PrimarySmtpAddress $GroupAddress `
  -ManagedBy $GroupOwner
```

Erlaubtes Postfach hinzufügen:

```
Add-DistributionGroupMember `
  -Identity $GroupAddress `
  -Member $AllowedMailbox
```

Gruppe und Mitglieder prüfen:

```
Get-DistributionGroup -Identity $GroupAddress |
  Format-List Name, DisplayName, PrimarySmtpAddress, RecipientTypeDetails, DistinguishedName

Get-DistributionGroupMember -Identity $GroupAddress -ResultSize Unlimited |
  Format-Table DisplayName, PrimarySmtpAddress, RecipientType
```

Direkte Mitgliedschaft

Der verwendete Management Scope basiert auf MemberOfGroup. Die erlaubten Postfächer müssen deshalb direkte Mitglieder der E-Mail-aktivierten Sicherheitsgruppe sein.

6.5 Service Principal in Exchange Online registrieren

```
New-ServicePrincipal `
  -AppId $AppId `
  -ObjectId $ServicePrincipalObjectId `
  -DisplayName $ExchangeServicePrincipalName

Get-ServicePrincipal -Identity $AppId |
  Format-List DisplayName, AppId, ObjectId, Identity
```

6.6 Management Scope erstellen

```
$GroupDistinguishedName = (
  Get-DistributionGroup -Identity $GroupAddress
).DistinguishedName

New-ManagementScope `
  -Name $ScopeName `
  -RecipientRestrictionFilter "MemberOfGroup -eq '$GroupDistinguishedName'"

$ManagementScope = Get-ManagementScope -Identity $ScopeName

Get-Recipient `
  -RecipientPreviewFilter $ManagementScope.RecipientFilter `
  -ResultSize Unlimited |
  Format-Table DisplayName, PrimarySmtpAddress, RecipientTypeDetails
```

In dieser Ausgabe dürfen nur die Postfächer erscheinen, auf die CADOSYS zugreifen soll.

6.7 Graph-Rolle prüfen und zuweisen

```
Get-ManagementRole -Identity "Application Mail.ReadWrite" |
Format-List Name, RoleType
```

Die eigentliche Application-RBAC-Zuweisung verbindet App, Berechtigung und Ressourcenbereich:

```
New-ManagementRoleAssignment `
-Name $RoleAssignmentName `
-Role "Application Mail.ReadWrite" `
-App $ServicePrincipalObjectId `
-CustomResourceScope $ScopeName
```

```
Get-ManagementRoleAssignment -RoleAssignee $ServicePrincipalObjectId |
Format-Table Name, Role, CustomResourceScope, RoleAssigneeType, AssignmentMethod
```

6.8 Erlaubtes Postfach testen

```
Test-ServicePrincipalAuthorization `
-Identity $AppId `
-Resource $AllowedMailbox |
Format-Table RoleName, GrantedPermissions, AllowedResourceScope, ScopeType, InScope
```

Für ein erlaubtes Postfach wird für Application Mail.ReadWrite InScope = True erwartet. Ein nicht freigegebenes Postfach sollte InScope = False liefern.

Cache-Hinweis

Microsoft weist darauf hin, dass Änderungen an App-Berechtigungen in produktiven API-Aufrufen zwischengespeichert werden können. Test-ServicePrincipalAuthorization umgeht diesen Berechtigungscache und eignet sich deshalb unmittelbar nach der Einrichtung zur Prüfung.

6.9 Verbindung trennen

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

7. Konfiguration prüfen

Wenn später nicht mehr alle Namen bekannt sind, reicht die Client-ID der App als Ausgangspunkt. Der Assistent verwendet genau dieses Verfahren.

```
$AppId = "ANWENDUNGS-ID"

$sp = Get-ServicePrincipal -Identity $AppId
$sp | Format-List DisplayName, AppId, ObjectId

Get-ManagementRoleAssignment -RoleAssignee $sp.ObjectId |
Format-Table Name, Role, CustomResourceScope
```

Aus den Rollenzuweisungen lassen sich die verwendeten Management Scopes ermitteln; aus deren RecipientFilter wiederum die betroffenen Gruppen und Postfächer.

8. Einrichtung rückgängig machen

Der Rückbau sollte immer von den abhängigen Objekten zu den Grundlagen erfolgen. Dadurch entstehen keine blockierenden Referenzen.

25. Rollenzuweisungen der App entfernen.
26. Zugehörige Management Scopes entfernen.
27. Exchange Service Principal entfernen.
28. Die für CADOSYS angelegte E-Mail-aktivierte Sicherheitsgruppe entfernen, sofern sie nicht anderweitig verwendet wird.
29. Optional anschließend die Entra App Registration manuell löschen, wenn wirklich ein vollständiger Neustart gewünscht ist.

```
Remove-ManagementRoleAssignment -Identity "<Rollenzuweisung>" -Confirm:$false
Remove-ManagementScope -Identity "<Scope>" -Confirm:$false
Remove-ServicePrincipal -Identity "<Exchange-Service-Principal-ObjectId>" -Confirm:$false
Remove-DistributionGroup -Identity "<Gruppenadresse>" -Confirm:$false
```

Warum die Entra App nicht automatisch gelöscht wird

Der PowerShell-Assistent entfernt nur die Exchange-Online-Konfiguration. Die Entra App Registration kann auch für andere Dienste verwendet werden und wird deshalb nur bewusst und manuell im Entra Admin Center gelöscht.

9. CADOSYS Buchhalter konfigurieren

Nachdem Entra und Exchange Online eingerichtet und erfolgreich geprüft wurden, wird das Postfach in CADOSYS Buchhalter konfiguriert. Die folgenden Schritte orientieren sich an der aktuellen Oberfläche für E-Mail-Import-Postfächer.

Konfigurationsblatt verwenden

Die in Entra ermittelten Werte können während der Einrichtung im „Konfigurationsblatt“ am Ende dieses Dokuments notiert werden. Verweisen Sie dort insbesondere auf Client-ID, Tenant-ID, Objekt-ID und die E-Mail-Adresse des freigegebenen Postfachs. Den geheimen Clientschlüssel nur temporär notieren und nach erfolgreicher Einrichtung wieder entfernen.

9.1 E-Mail-Import-Postfächer öffnen

30. Starten Sie CADOSYS Buchhalter und melden Sie sich mit einem Administratorkonto an.
31. Öffnen Sie den Bereich Admin und anschließend Administration.
32. Öffnen Sie Firmen und wählen Sie die Firma aus, für die der E-Mail-Import eingerichtet werden soll.
33. Öffnen Sie unter E-Mail-Import die Konfiguration der E-Mail-Postfächer.
34. Klicken Sie auf Neu, wenn ein neues Postfach angelegt werden soll.

9.2 Neue Microsoft-Graph-Anbindung auswählen

Bei einer Neuanlage wählen Sie als Postfachtyp die Graph-basierte App-Anmeldung. Diese verwendet die zuvor erstellte Entra App Registration und benötigt keine interaktive Benutzeranmeldung.

Skizze – Auswahl des Postfachtyps

Bitte geben Sie den Typ des Postfachs an
IMAP
Exchange (NTLM / On-Premises)
Exchange Online (Azure AD registrierte Anwendung)
Exchange Online (Azure AD Benutzeranmeldung)
> Microsoft Graph (Azure AD registrierte Anwendung)
POP3

Für eine neue App-only-Anbindung wählen Sie „Microsoft Graph (Azure AD registrierte Anwendung)“.

35. Wählen Sie „Microsoft Graph (Azure AD registrierte Anwendung)“.
36. Bestätigen Sie die Auswahl.
37. CADOSYS öffnet anschließend die Graph-Konfiguration für das neue Postfach.

9.3 Graph-Konfiguration ausfüllen

Tragen Sie die Werte aus der Entra-Konfiguration bzw. aus dem Konfigurationsblatt in CADOSYS ein.

Skizze – Microsoft Graph Konfiguration

E-Mail Import-Postfächer	
Neu Kopieren Speichern Test Download E-Mails (Graph) beispiel@kunde.de	Graph Konfiguration Name Frei wählbare Bezeichnung, z. B. (Graph) Rechnungseingang Aktiv Nach erfolgreichem Test aktivieren Anwendungs ID Anwendungs-ID (Client) aus Entra Verzeichnis ID Verzeichnis-ID (Mandant) aus Entra Geheimer Schlüssel Wert des Client Secrets Gültigkeitsbereich https://graph.microsoft.com/.default E-Mail Adresse Freigegebenes Exchange-Online-Postfach Geteilte E-Mail Optional, falls fachlich benötigt Clearing E-Mail Optional, falls fachlich benötigt Barcodekonfig Optional gemäß CADOSYS-Konfiguration Graph-Ordner abholen Liest die verfügbaren Mailordner des Postfachs Zu überwachender Ordner Ordner, aus dem CADOSYS E-Mails abholt Ordner für verarbeitete E-Mails Zielordner nach erfolgreicher Verarbeitung Ordner für fehlerhafte E-Mails Zielordner bei nicht verarbeitbaren E-Mails Auch gelesene E-Mails verarbeiten Nur aktivieren, wenn

	fachlich gewünscht Zusätzliche Konfiguration Nur für Experten / produktspezifische Sonderfälle
--	---

Skizze – vereinfacht nach der CADOSYS-Oberfläche. Feldbezeichnungen und Reihenfolge entsprechen der gezeigten Produktversion.

9.4 Ordner abrufen und auswählen

38. Klicken Sie auf Graph-Ordner abholen. CADOSYS fragt damit über Microsoft Graph die verfügbaren Ordner des angegebenen Postfachs ab.
39. Wählen Sie unter „Zu überwachender Ordner“ den Ordner aus, aus dem CADOSYS neue E-Mails verarbeiten soll.
40. Wählen Sie den Ordner für erfolgreich verarbeitete E-Mails.
41. Wählen Sie den Ordner für fehlerhafte bzw. nicht verarbeitbare E-Mails.
42. Speichern Sie die Konfiguration.

Berechtigung erforderlich

Wenn „Graph-Ordner abholen“ fehlschlägt, prüfen Sie zuerst die Exchange Application-RBAC-Konfiguration und insbesondere, ob Test-ServicePrincipalAuthorization für dieses Postfach Application Mail.ReadWrite mit InScope = True ausgibt.

9.5 Verbindung testen und aktivieren

43. Klicken Sie auf Test.
44. Prüfen Sie, ob CADOSYS erfolgreich eine Verbindung zum Postfach herstellen und Mailinformationen abrufen kann.
45. Korrigieren Sie bei einem Fehler zunächst Client-ID, Tenant-ID, Client Secret, Gültigkeitsbereich und E-Mail-Adresse.
46. Aktivieren Sie die Konfiguration erst, wenn der Verbindungstest erfolgreich war.
47. Speichern Sie die Konfiguration.

Gültigkeitsbereich für Graph

Für die Graph-Anbindung ist in der gezeigten CADOSYS-Version der Gültigkeitsbereich <https://graph.microsoft.com/.default> vorgesehen. Die EWS-Werte <https://outlook.office365.com/ews/exchange.asmx> und <https://outlook.office365.com/.default> gehören zur bisherigen Exchange-Online-/EWS-Anbindung und werden für die neue Graph-Konfiguration nicht verwendet.

9.6 Bestehende Exchange-Online-Konfiguration auf Graph migrieren

Ist bereits ein Postfach über „Exchange Online (Azure AD registrierte Anwendung)“ eingerichtet, muss die Konfiguration nicht vollständig neu angelegt werden. In der bestehenden Exchange-Konfiguration steht dafür die Schaltfläche „Nach Graph migrieren“ zur Verfügung.

Skizze – bestehende Exchange-Konfiguration mit Migration

E-Mail Import-Postfächer	
Neu Kopieren Speichern Test Nach Graph migrieren Download E-Mails beispiel@kunde.de (Graph) beispiel@kunde.de	Exchange Konfiguration Url https://outlook.office365.com/ews/exchange.asmx Version Exchange2013_SP1 / produktspezifische Auswahl Gültigkeitsbereich https://outlook.office365.com/.default Anwendungs ID bestehende Client-ID Verzeichnis ID bestehende Tenant-ID Geheimer Schlüssel bestehender Client-Secret-Wert E-Mail Adresse bestehendes Postfach Nach Graph migrieren übernimmt die bestehende Konfiguration in eine neue Graph-Variante <i>Die alte Exchange-Konfiguration bleibt zunächst sichtbar; die neue Graph-Konfiguration wird separat angelegt.</i>

Skizze – vereinfacht nach der CADOSYS-Oberfläche. Feldbezeichnungen und Reihenfolge entsprechen der gezeigten Produktversion.

48. Wählen Sie links die bestehende Exchange-Online-Konfiguration aus.
49. Klicken Sie auf „Nach Graph migrieren“.
50. CADOSYS legt aus der bestehenden Anmeldung eine Graph-Variante an. In der Postfachliste ist diese als neue Graph-Konfiguration erkennbar.
51. Öffnen Sie die neue Graph-Konfiguration und prüfen Sie insbesondere Anwendungs-ID, Verzeichnis-ID, geheimen Schlüssel, E-Mail-Adresse und den Graph-Gültigkeitsbereich.
52. Rufen Sie die Graph-Ordner ab und kontrollieren Sie die drei Ordnerzuordnungen.
53. Führen Sie den Test aus.
54. Aktivieren Sie die Graph-Konfiguration erst nach erfolgreichem Test.

Migration ersetzt nicht die Microsoft-365-Berechtigung

Der Migrationsbutton überträgt die CADOSYS-Konfiguration. Die Microsoft-365-Seite muss trotzdem für Microsoft Graph eingerichtet sein: Exchange Service Principal, Application Mail.ReadWrite und der Management Scope für das Postfach müssen vorhanden und erfolgreich getestet sein.

9.7 Alte und neue Konfiguration während der Umstellung

Nach der Migration können alte Exchange- und neue Graph-Konfiguration zunächst parallel in der Liste sichtbar sein. Dadurch lässt sich die neue Variante kontrollieren, bevor die bisherige Konfiguration außer Betrieb genommen wird.

Skizze – alte und migrierte Graph-Konfiguration

E-Mail Import-Postfächer	
Speichern Test Download E-Mails beispiel@kunde.de (Graph) beispiel@kunde.de	Graph Konfiguration Name (Graph) beispiel@kunde.de Gültigkeitsbereich https://graph.microsoft.com/.default E-Mail Adresse beispiel@kunde.de Status Graph-Konfiguration testen und anschließend aktivieren

Skizze – vereinfacht nach der CADOSYS-Oberfläche. Feldbezeichnungen und Reihenfolge entsprechen der gezeigten Produktversion.

Empfohlene Umstellung

Lassen Sie die bisherige Konfiguration während der Prüfung unverändert. Sobald die Graph-Konfiguration erfolgreich getestet wurde und die gewünschten Ordner korrekt zugeordnet sind, kann die bisherige EWS-Konfiguration deaktiviert bzw. nach den betrieblichen Vorgaben entfernt werden.

10. Fehleranalyse

10.1 Das Skript darf nicht ausgeführt werden

```
Get-ExecutionPolicy -List
Get-Item ".\Setup-CADOSYS-ExchangeOnlineGraph.ps1" -Stream *
```

Wenn die Datei geprüft wurde und als Internetdownload blockiert ist:

```
Unblock-File -Path ".\Setup-CADOSYS-ExchangeOnlineGraph.ps1"
```

10.2 ExchangeOnlineManagement fehlt

```
Install-Module -Name ExchangeOnlineManagement -Scope CurrentUser
```

10.3 Service Principal wird nicht gefunden

```
Get-ServicePrincipal -Identity $AppId
```

Prüfen Sie, ob die Client-ID korrekt ist und ob New-ServicePrincipal bereits erfolgreich ausgeführt wurde.

10.4 Postfach ist InScope = False

- Ist das Postfach direktes Mitglied der Sicherheitsgruppe?
- Verweist der Management Scope auf den Distinguished Name der richtigen Gruppe?
- Wurde der Scope in der Rollenzuweisung über CustomResourceScope verwendet?
- Ist Application Mail.ReadWrite der erwarteten App zugewiesen?

11. Weiterführende Microsoft-Dokumentation

- [Microsoft Entra Admin Center](#)
- [Role Based Access Control for Applications in Exchange Online](#)
- [Microsoft Graph permissions reference](#)
- [Exchange Online PowerShell module](#)
- [Connect to Exchange Online PowerShell](#)
- [PowerShell execution policies](#)
- [PowerShell script signing / Unblock-File](#)

12. Konfigurationsblatt – Werte für die Einrichtung

Diese Tabelle kann während der Einrichtung als Arbeitsblatt verwendet werden. Die Werte werden an mehreren Stellen benötigt. Bewahren Sie das Dokument entsprechend Ihrer internen Sicherheitsvorgaben auf.

Client Secret nur temporär

Tragen Sie den Wert des geheimen Clientschlüssels nur ein, wenn dies für die Einrichtung erforderlich ist. Entfernen Sie ihn nach erfolgreicher Konfiguration wieder aus diesem Dokument oder bewahren Sie ihn ausschließlich in einem dafür vorgesehenen sicheren Secret- bzw. Passwortspeicher auf.

Information	Wert / Notiz	Quelle / Verwendung
Name der Entra App Registration		Entra App-Registrierungen
Anwendungs-ID (Client)		Entra App Registration / CADOSYS
Verzeichnis-ID (Mandant)		Entra App Registration / CADOSYS
Objekt-ID der Unternehmensanwendung		Entra Unternehmensanwendungen / PowerShell-Assistent
Client Secret – Beschreibung / Ablaufdatum		Entra Zertifikate & Geheimnisse
Client Secret – Wert (nur temporär!)		CADOSYS Graph Konfiguration
Exchange Sicherheitsgruppe – Name		PowerShell / Application RBAC
Exchange Sicherheitsgruppe – Adresse		PowerShell / Application RBAC
Freigegebene Postfächer		Mitglieder der Sicherheitsgruppe
Exchange Service Principal – Anzeigename		PowerShell
Management Scope – Name		PowerShell
Role Assignment – Name		PowerShell
CADOSYS Konfigurationsname		E-Mail Import-Postfächer
CADOSYS E-Mail-Adresse		Graph Konfiguration
Zu überwachender Ordner		CADOSYS
Ordner für verarbeitete E-Mails		CADOSYS
Ordner für fehlerhafte E-Mails		CADOSYS
Datum / Administrator		Dokumentation der Einrichtung

13. Anhang – Zweck des PowerShell-Assistenten

Der PowerShell-Assistent ist kein Blackbox-Installer. Er führt dieselben Schritte aus, die in Kapitel 6 einzeln dokumentiert sind. Sein Zweck ist, Tippfehler zu reduzieren, Abhängigkeiten in der richtigen Reihenfolge zu behandeln und dem Administrator vor jeder wesentlichen Änderung eine verständliche Zusammenfassung zu zeigen.

Für produktive Bereitstellung über einen CADOSYS-Downloadserver empfiehlt sich zusätzlich eine Authenticode-Signatur des Skripts mit einem vertrauenswürdigen Code-Signing-Zertifikat. Dadurch lässt sich die Herkunft des Skripts besser prüfen und Umgebungen mit AllSigned unterstützen.