

The background of the slide is a photograph of a business meeting. Two men are seated at a white round table in a modern office with large windows. The man on the left, wearing glasses and a blue shirt under a dark jacket, is smiling. The man on the right, in a light blue shirt, is looking at a tablet. A hand is visible in the foreground pointing at the tablet screen. On the table are a remote control and a mouse.

## MAPI Permission PowerShell Modul Exchange Online RBAC for Applications (Preview)

EXUSG Meetup 2023-Q1 – Andres Bohren -23.02.2022

# About me



Cloud Engineer / Architect bei isolutions seit 2020

Seit 25 Jahren in der IT - Schwerpunkt in Messaging / Communication / Security  
(Windows Server / Active Directory / MS SQL / Exchange / Lync / Skype4B / M365 /  
Azure / PowerShell)

Hobbies: Reisen / Tauchen / Bike / Tanzen



<https://blog.icewolf.ch>



<https://twitter.com/andresbohren> / @andresbohren



<https://www.linkedin.com/in/andres-bohren-4ba45293/>



<https://github.com/BohrenAn>



<https://isolutions.ch>

isolutions'

# MAPI Permission PowerShell Modul

## Herausforderungen

- Keine Vererbung der Outlook Ordnerberechtigungen
  - Hinzufügen auf einem Ordner führt nicht dazu, dass die Berechtigung auf den Unterordnern dazukommt. Bei vielen Unterordnern wirds mühsam für den Benutzer.
- Ein neuer Ordner übernimmt die Ordnerberechtigungen des übergeordneten Ordners
- Ein Script braucht einen mix aus "Get-MailboxfolderStatistics" and "Get-MailboxfolderPermissions"
- Sonderzeichen in Ordnern
- Root Folder must have "Folder visible" to Access the Folder
  - Jedenfalls bei Additional Mailbox
- Outlook Delegates bekommen "SendOnBehalf" Rechte

# Exchange MAPI Berechtigungen

Standard Ordner	Berechtigungen
<ul style="list-style-type: none"> <li>Inbox</li> <li>Calendar</li> <li>Notes</li> <li>Tasks</li> <li>Contacts</li> </ul>	<ul style="list-style-type: none"> <li>(FolderVisible)</li> <li>Reviewer</li> <li>Contributor</li> <li>Author</li> <li>Editor</li> <li>NonEditingAuthor</li> <li>Owner</li> <li>PublishingEditor</li> <li>PublishingAuthor</li> </ul>

Posteingang Properties

General AutoArchive Policy Permissions Synchronization

Name	Permission Level
Default	None
Muster, Max	Reviewer

Add... Remove Properties...

Permissions

Permission Level: None

Read

☒ None  
☐ Full Details

Write

☐ Create items  
☐ Create subfolders  
☐ Edit own  
☐ Edit all

Delete items

☒ None  
☐ Own  
☐ All

Other

☐ Folder owner  
☐ Folder contact  
☐ Folder visible

OK Cancel Apply

isolutions'

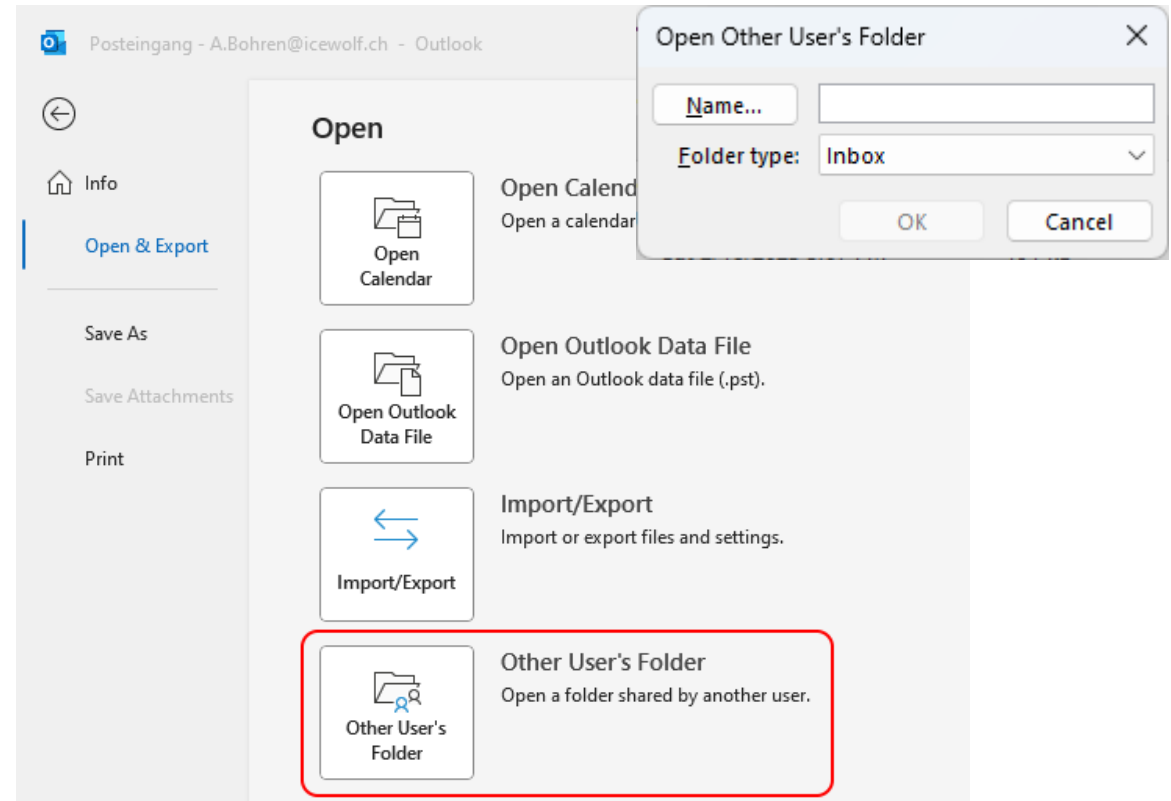
# Verschiedene Zugriffsarten

(the many ways you can mount another Mailbox...)

# Ordner eines anderen Benutzers

Ordner eines anderen Benutzers

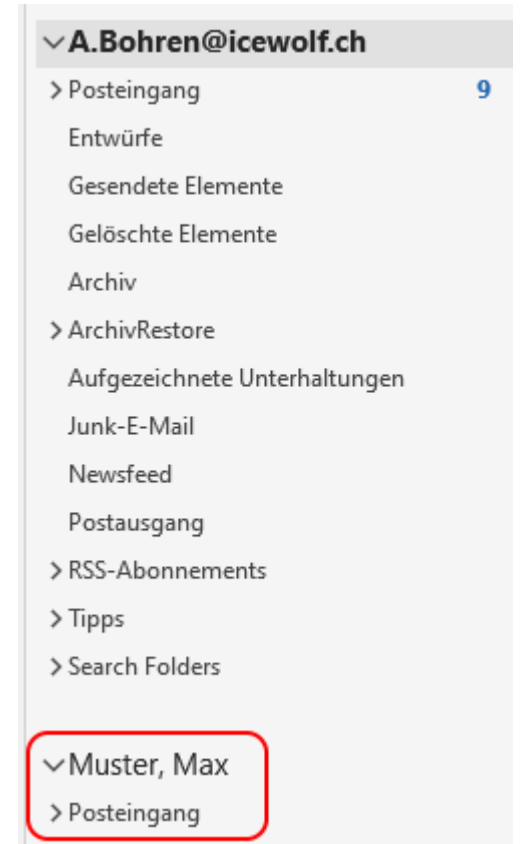
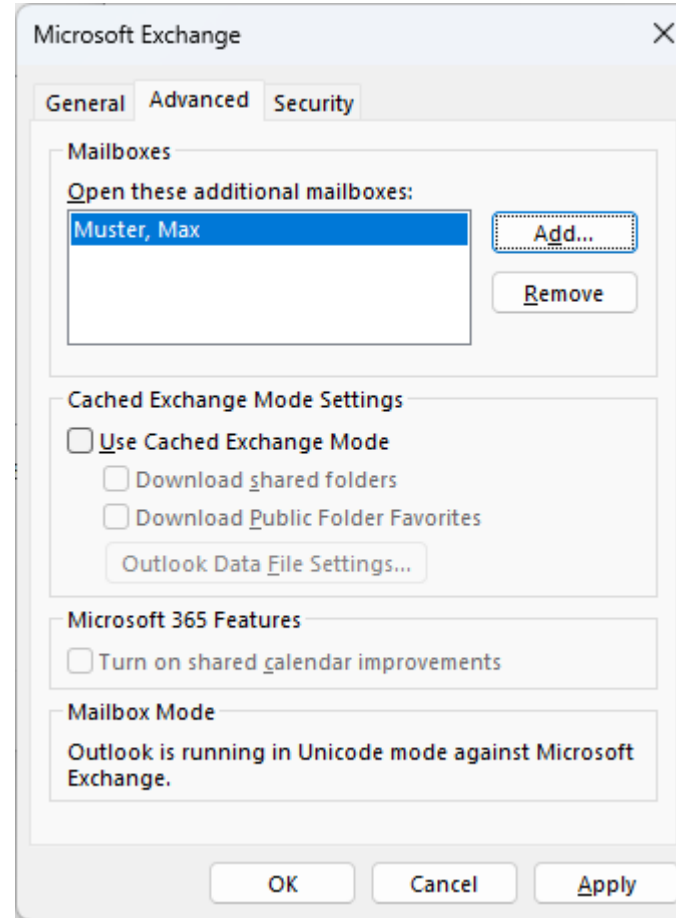
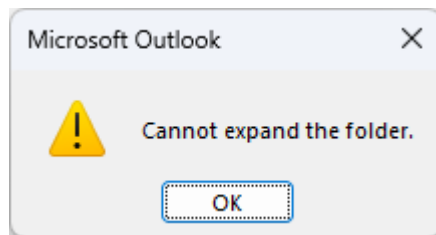
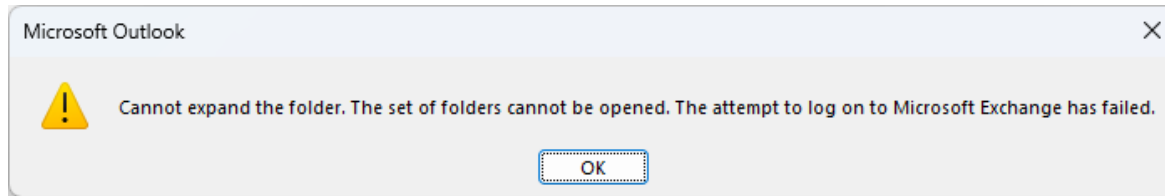
- Benötigt kein FolderVisible auf dem RootFolder



# Additional Mailbox

## Zusätzliche Mailbox

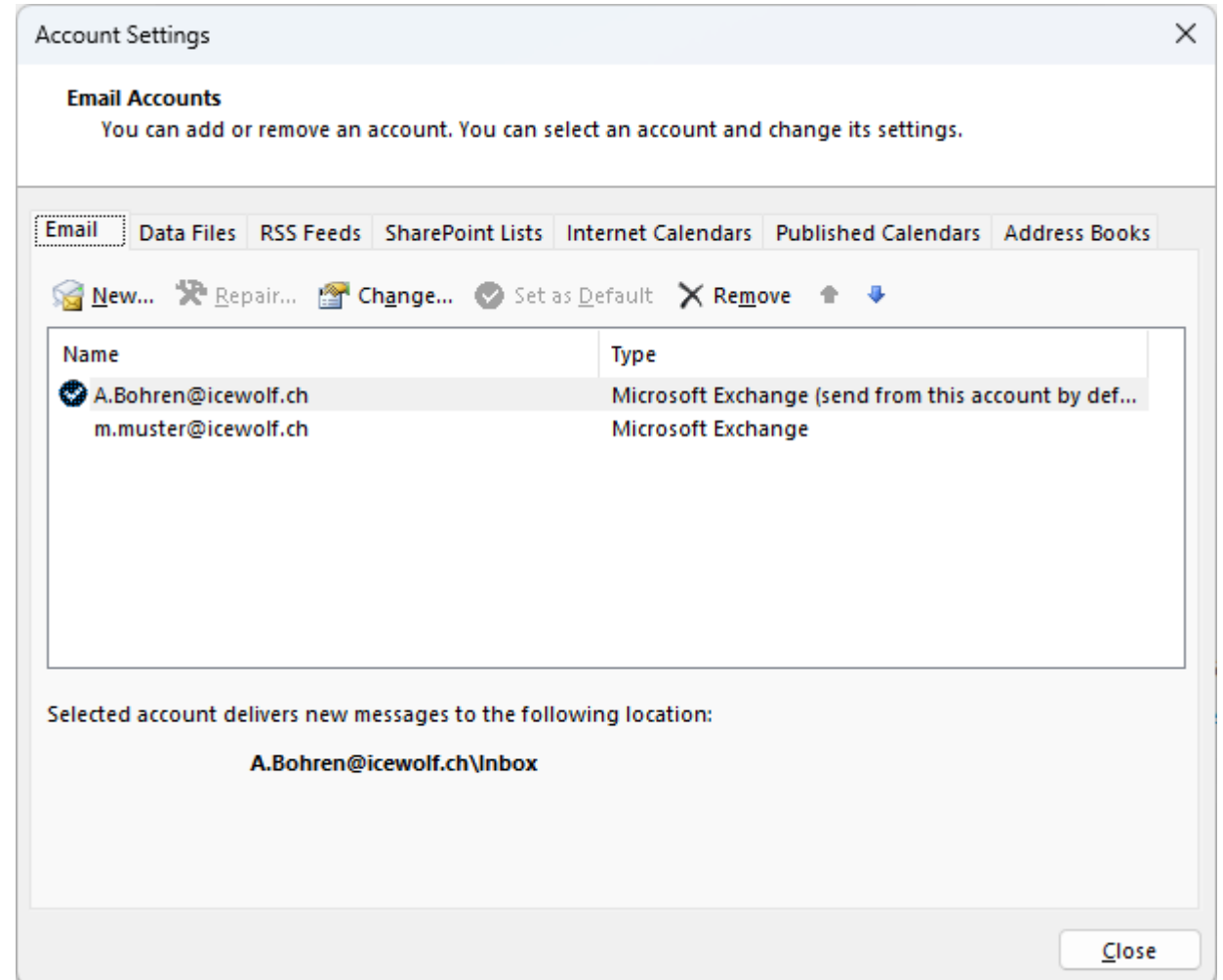
- Benötigt FolderVisible auf dem RootFolder
- Man sieht nur berechtigte Ordner





## Multi Mailbox

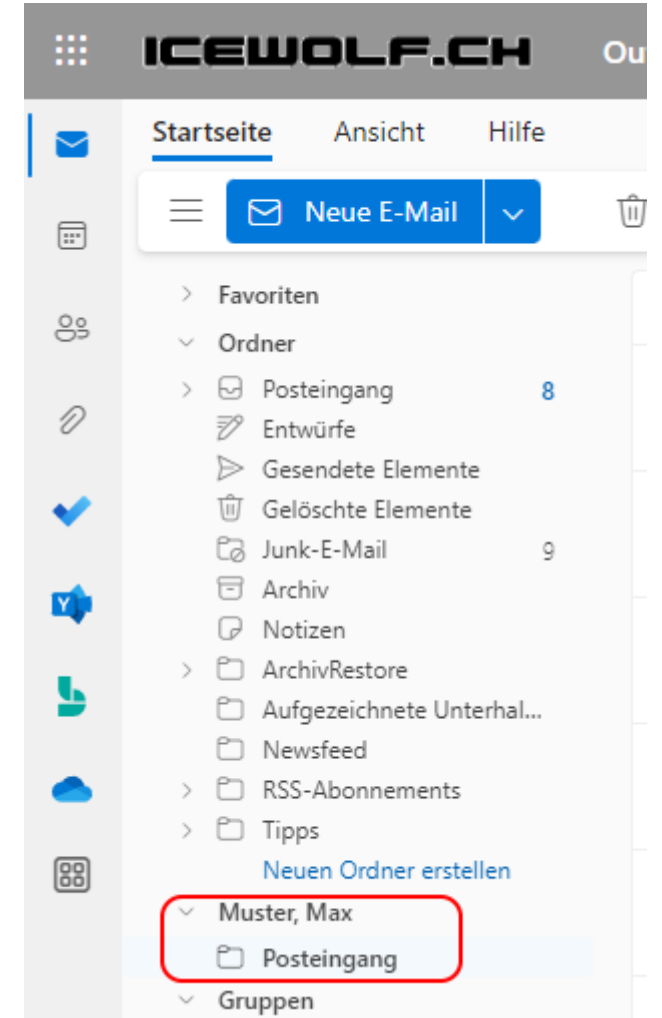
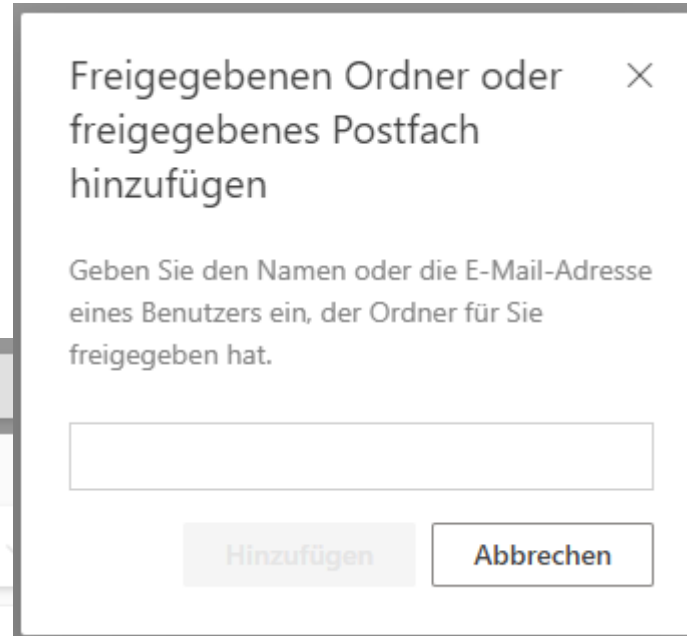
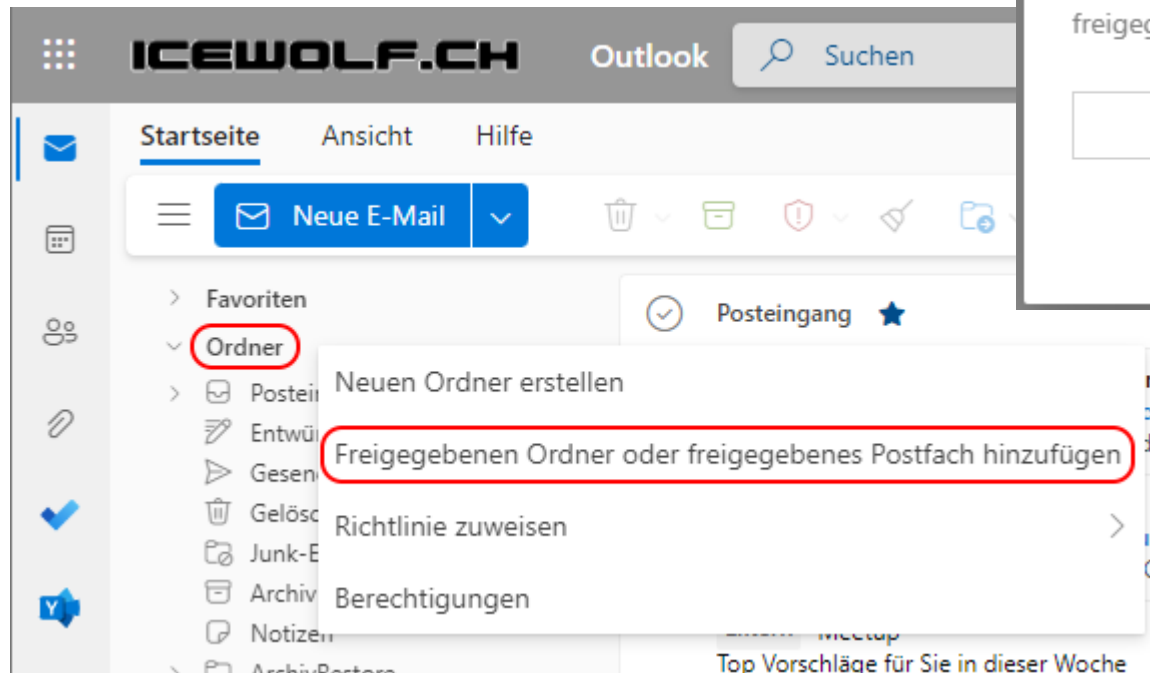
- Multi Mailbox
- Funktioniert nur mit FullAccess



# Outlook on the Web (OWA)

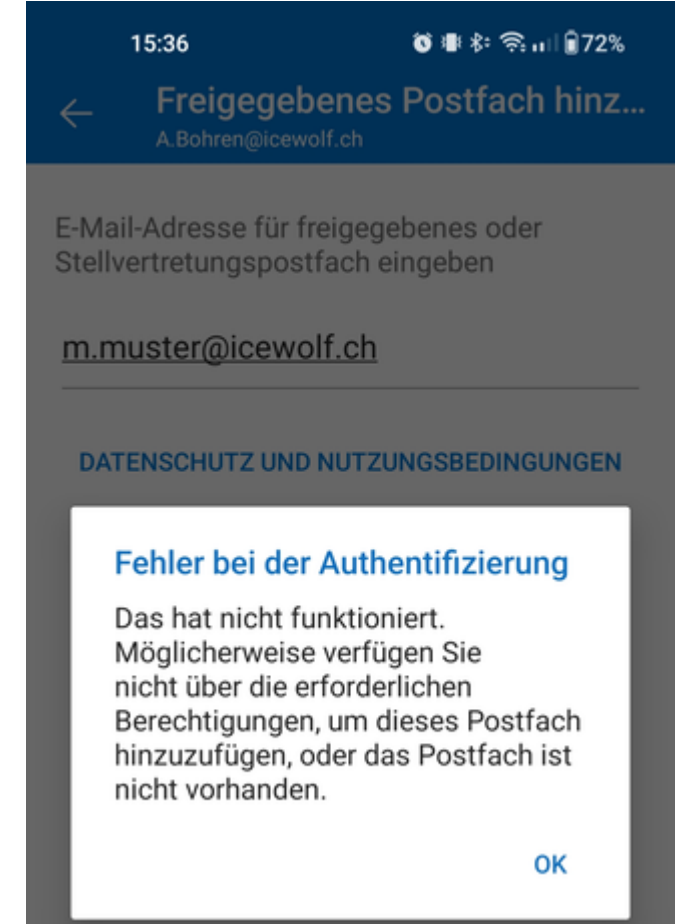
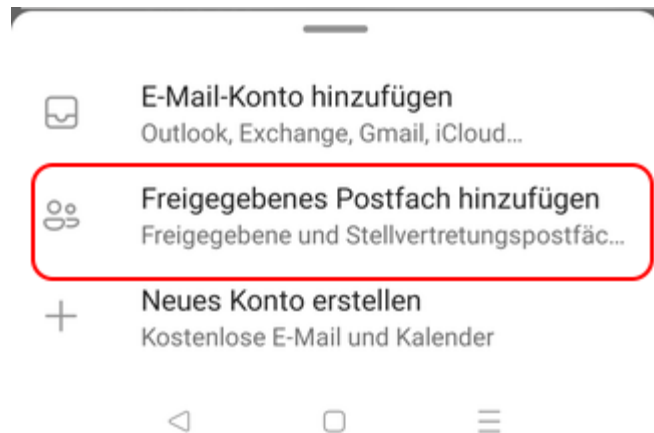
Outlook on the Web

- Benötigt kein FolderVisible auf dem RootFolder



# Outlook for Android/iOS

- Outlook for Android/iOS benötigt FullAccess



# Icewolf.Exchange.MAPI

- GitHub Code und Dokumentation  
[https://github.com/BohrenAn/GitHub\\_PowerShellScripts/tree/main/Icewolf.Exchange.MAPI](https://github.com/BohrenAn/GitHub_PowerShellScripts/tree/main/Icewolf.Exchange.MAPI)
- PSGallery <https://www.powershellgallery.com/packages/Icewolf.exchange.mapi>
- Install-Module Icewolf.Exchange.MAPI –AllowPrerelease
- Get-Command -Module Icewolf.Exchange.MAPI
- Get-Help Export-MAPIPermission
- Get-Help Add-MAPIPermission
- Get-Help Remove-MAPIPermission

# Export-MAPIPermission

- Export-MAPIPermission -Mailbox john.doe@yourdomain.com -  
FilePath C:\temp\john.doe.txt

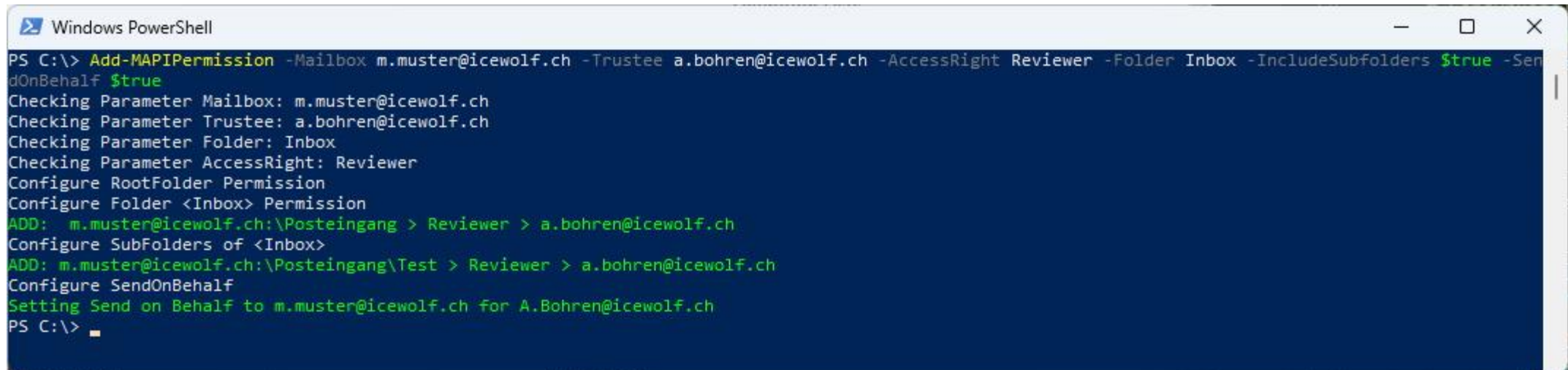
```
Windows PowerShell
PS C:\> Export-MAPIPermission -Mailbox m.muster@icewolf.ch -FilePath C:\temp\m.muster@icewolf.ch.txt
File already exists.
Do you like to overwrite the File? (y/n)[n]? y
Getting folders...
Working on Folder: m.muster@icewolf.ch:\
Working on Folder: m.muster@icewolf.ch:\Archiv
Working on Folder: m.muster@icewolf.ch:\Aufgaben
Working on Folder: m.muster@icewolf.ch:\Conversation Action Settings
Working on Folder: m.muster@icewolf.ch:\Dateien
Working on Folder: m.muster@icewolf.ch:\Einstellungen für QuickSteps
Working on Folder: m.muster@icewolf.ch:\Entwürfe
Working on Folder: m.muster@icewolf.ch:\ExternalContacts
Working on Folder: m.muster@icewolf.ch:\Gelöschte Elemente
Working on Folder: m.muster@icewolf.ch:\Gesendete Elemente
Working on Folder: m.muster@icewolf.ch:\Journal
Working on Folder: m.muster@icewolf.ch:\Junk-E-Mail
Working on Folder: m.muster@icewolf.ch:\Kalender
Working on Folder: m.muster@icewolf.ch:\Kalender\Feiertage in Deutschland
Working on Folder: m.muster@icewolf.ch:\Kalender\Feiertage in Schweiz
Working on Folder: m.muster@icewolf.ch:\Kalender\Geburtstage
Working on Folder: m.muster@icewolf.ch:\Kontakte
Working on Folder: m.muster@icewolf.ch:\Kontakte\{06967759-274D-4082-A3EB-D7F9E73727D7}
Working on Folder: m.muster@icewolf.ch:\Kontakte\{A9E2BC46-B3A0-4243-B315-60D991004455}
Working on Folder: m.muster@icewolf.ch:\Kontakte\Firmen
Working on Folder: m.muster@icewolf.ch:\Kontakte\GAL Contacts
Working on Folder: m.muster@icewolf.ch:\Kontakte\Organizational Contacts
Working on Folder: m.muster@icewolf.ch:\Kontakte\PeopleCentricConversation Buddies
Working on Folder: m.muster@icewolf.ch:\Kontakte\Recipient Cache
Working on Folder: m.muster@icewolf.ch:\Newsletter
Working on Folder: m.muster@icewolf.ch:\Notizen
Working on Folder: m.muster@icewolf.ch:\PersonMetadata
Working on Folder: m.muster@icewolf.ch:\Postausgang
Working on Folder: m.muster@icewolf.ch:\Posteingang
Working on Folder: m.muster@icewolf.ch:\Posteingang\Test
Working on Folder: m.muster@icewolf.ch:\RSS-Abonnements
Working on Folder: m.muster@icewolf.ch:\Synchronisierungsprobleme
Working on Folder: m.muster@icewolf.ch:\Synchronisierungsprobleme\Konflikte
Working on Folder: m.muster@icewolf.ch:\Synchronisierungsprobleme\Lokale Fehler
Working on Folder: m.muster@icewolf.ch:\Synchronisierungsprobleme\Serverfehler
Working on Folder: m.muster@icewolf.ch:\Test
Working on Folder: m.muster@icewolf.ch:\Verlauf der Unterhaltung
Working on Folder: m.muster@icewolf.ch:\Verlauf der Unterhaltung\Teamchat
Working on Folder: m.muster@icewolf.ch:\Yammer-Stamm
Working on Folder: m.muster@icewolf.ch:\Yammer-Stamm\Feeds
Working on Folder: m.muster@icewolf.ch:\Yammer-Stamm\Inbound
Working on Folder: m.muster@icewolf.ch:\Yammer-Stamm\Outbound
Do you like to open the exported File? (y/n)[n]? y
PS C:\>
```

```
m.muster@icewolf.ch.txt - Notepad
File Edit View

Mailbox;Trustee;AccessRights
m.muster@icewolf.ch:\;Default;None
m.muster@icewolf.ch:\;Anonymous;None
m.muster@icewolf.ch:\Archiv;Default;None
m.muster@icewolf.ch:\Archiv;Anonymous;None
m.muster@icewolf.ch:\Aufgaben;Default;None
m.muster@icewolf.ch:\Conversation Action Settings;Default;None
m.muster@icewolf.ch:\Conversation Action Settings;Anonymous;None
m.muster@icewolf.ch:\Dateien;Default;None
m.muster@icewolf.ch:\Dateien;Anonymous;None
m.muster@icewolf.ch:\Einstellungen für QuickSteps;Default;None
m.muster@icewolf.ch:\Einstellungen für QuickSteps;Anonymous;None
m.muster@icewolf.ch:\Entwürfe;Default;None
m.muster@icewolf.ch:\Entwürfe;Anonymous;None
m.muster@icewolf.ch:\ExternalContacts;Default;None
m.muster@icewolf.ch:\ExternalContacts;Anonymous;None
m.muster@icewolf.ch:\Gelöschte Elemente;Default;None
m.muster@icewolf.ch:\Gelöschte Elemente;Anonymous;None
m.muster@icewolf.ch:\Gesendete Elemente;Default;None
m.muster@icewolf.ch:\Gesendete Elemente;Anonymous;None
m.muster@icewolf.ch:\Journal;Default;None
m.muster@icewolf.ch:\Journal;Anonymous;None
m.muster@icewolf.ch:\Junk-E-Mail;Default;None
m.muster@icewolf.ch:\Junk-E-Mail;Anonymous;None
m.muster@icewolf.ch:\Kalender;Default;LimitedDetails
```

## Add-MAPIPermission

- Add-MAPIPermission -Mailbox john.doe@yourdomain.com -Trustee erika.mustermann@yourdomain.com -AccessRight Reviewer -Folder Inbox [-includeSubfolders \$true] [-SendOnBehalf \$true]

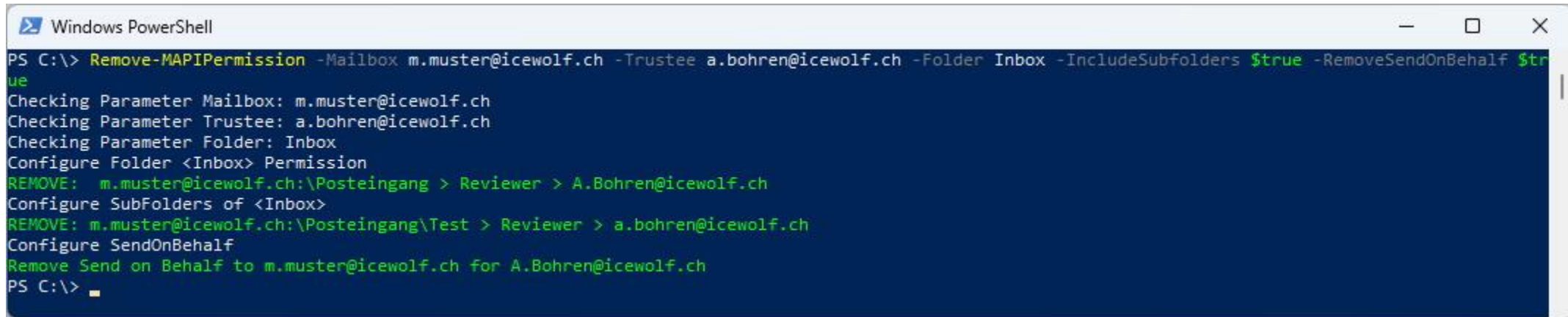


```
Windows PowerShell
PS C:\> Add-MAPIPermission -Mailbox m.muster@icewolf.ch -Trustee a.bohren@icewolf.ch -AccessRight Reviewer -Folder Inbox -IncludeSubfolders $true -SendOnBehalf $true
Checking Parameter Mailbox: m.muster@icewolf.ch
Checking Parameter Trustee: a.bohren@icewolf.ch
Checking Parameter Folder: Inbox
Checking Parameter AccessRight: Reviewer
Configure RootFolder Permission
Configure Folder <Inbox> Permission
ADD: m.muster@icewolf.ch:\Posteingang > Reviewer > a.bohren@icewolf.ch
Configure SubFolders of <Inbox>
ADD: m.muster@icewolf.ch:\Posteingang\Test > Reviewer > a.bohren@icewolf.ch
Configure SendOnBehalf
Setting Send on Behalf to m.muster@icewolf.ch for A.Bohren@icewolf.ch
PS C:\>
```



## Remove-MAPIPermission

- Remove-MAPIPermission -Mailbox john.doe@yourdomain.ch - User erika.mustermann@yourdomain.com -Folder Calendar [- IncludeSubfolders \$true] [-RemoveSendOnBehalf \$true] [- DeleteRootFolderPermission \$true]



```
Windows PowerShell
PS C:\> Remove-MAPIPermission -Mailbox m.muster@icewolf.ch -Trustee a.bohren@icewolf.ch -Folder Inbox -IncludeSubfolders $true -RemoveSendOnBehalf $true
Checking Parameter Mailbox: m.muster@icewolf.ch
Checking Parameter Trustee: a.bohren@icewolf.ch
Checking Parameter Folder: Inbox
Configure Folder <Inbox> Permission
REMOVE: m.muster@icewolf.ch:\Posteingang > Reviewer > A.Bohren@icewolf.ch
Configure SubFolders of <Inbox>
REMOVE: m.muster@icewolf.ch:\Posteingang\Test > Reviewer > a.bohren@icewolf.ch
Configure SendOnBehalf
Remove Send on Behalf to m.muster@icewolf.ch for A.Bohren@icewolf.ch
PS C:\>
```

## Tipps und Fragen

- In Exchange Online braucht man eine Lizenz für MAPI Zugriff
  - Also E1 / E3 / ExchangeOnline Plan 1 oder 2
  - Allenfalls mit Get-CASMailbox -Identity <Mailbox> prüfen

### Parameter

- Parameter «-Trustee» soll der in «-User» geändert werden?



olutions

## Demo



# Exchange Online RBAC for Applications (Preview)

## Exchange Online RBAC for Applications

- Announcing Public Preview of Role Based Access Control for Applications in Exchange Online  
<https://techcommunity.microsoft.com/t5/exchange-team-blog/announcing-public-preview-of-role-based-access-control-for/ba-p/3688228>

Notes from the field: Using app-only authentication with customized RBAC roles in Exchange Online

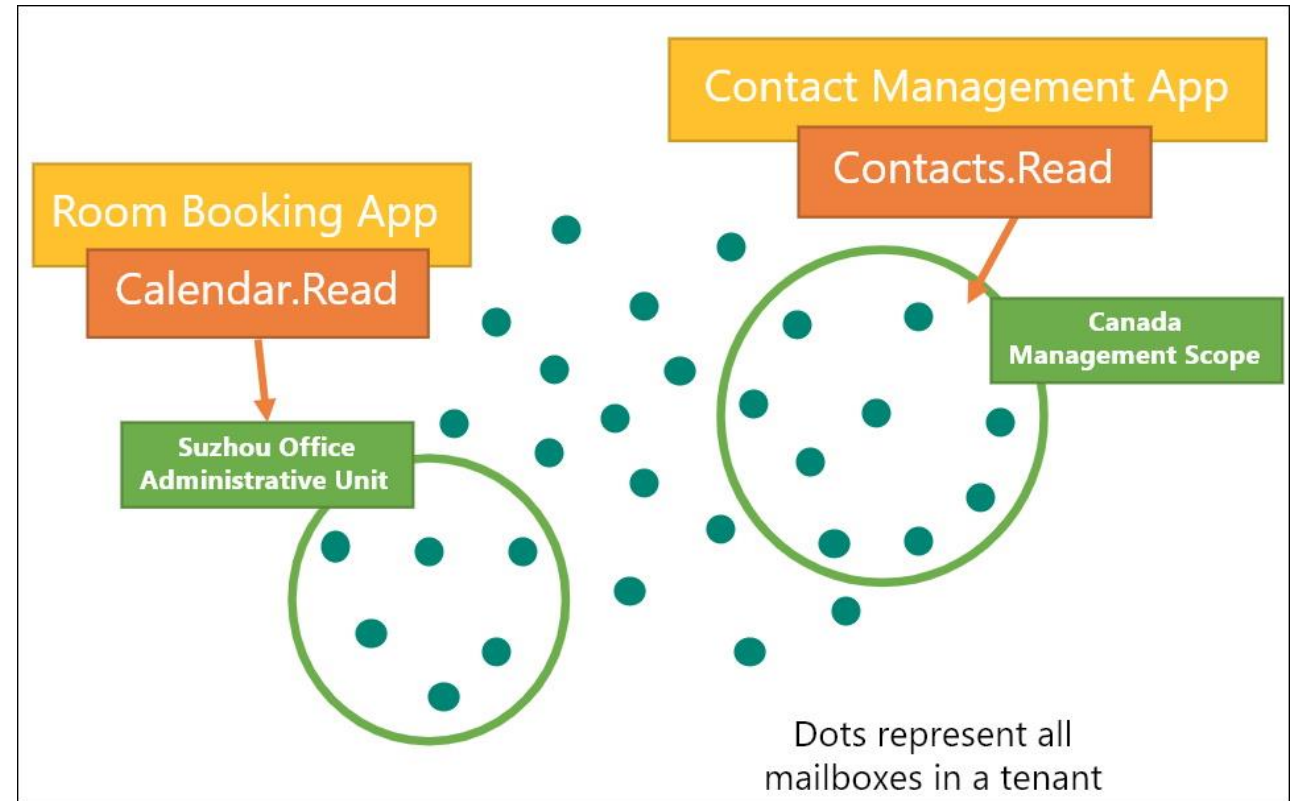
<https://techcommunity.microsoft.com/t5/exchange-team-blog/notes-from-the-field-using-app-only-authentication-with/ba-p/3690083>

## Takeaways

- Die Preview ist verfügbar für alle Kunden der Worldwide Tenants, es wird erwartet, dass "generally available" (GA) im H1 2023 erreicht wird.
- Dieses Feature erweitert das aktuelle RBAC Modell und wird das aktuelle RBAC Modell mit [Application Access Policy](#) ersetzen.
- Service Principals welche Apps repräsentieren, müssen aktuell manuell erzeugt werden. Dieser Prozess wird voraussichtlich bis zum GA automatisiert um ein effizienteres Benutzererlebnis zu bieten.
- Die Preview bietet zwei scoping Mechanismen welche von Exchange RBAC unterstützt wird: Management Scopes und Admin Units

## Scoping Mechanismen

- Entweder über Admin Unit
- Oder über Management Scope



# Evolution der Graph Application Berechtigungen

App Permission:

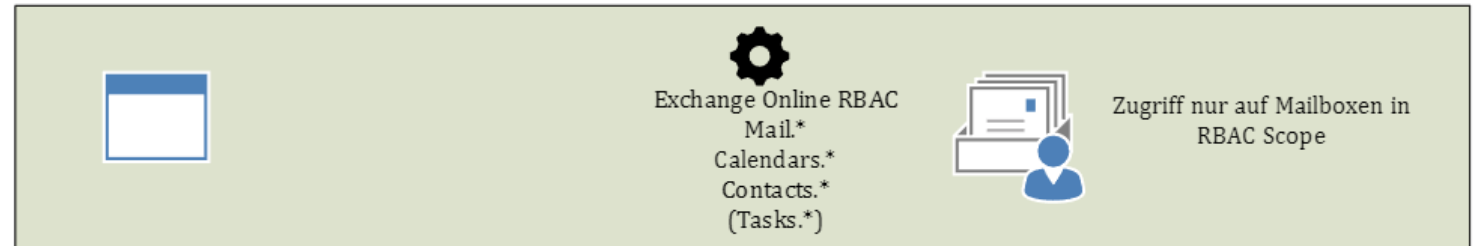
V1: Zugriff auf alle Mailboxen  
(entspricht Impersonation)



V2: Einschränkung mit  
[ApplicationAccessPolicy](#) (EXO)



V3: Exchange Online RBAC





# Azure AD App

The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains a navigation menu with options like Dashboard, All services, FAVORITES, Azure Active Directory, Groups, Users, External Identities, Administrative units, Enterprise applications, Azure AD Connect Health, Azure AD Identity Protection, Azure AD Password protection, Multifactor authentication, Azure AD Privileged Identity Management, and Azure AD Security. The main content area is titled 'Demo-EXO-RBAC' and includes a search bar, action buttons (Delete, Endpoints, Preview features), and a feedback message. The 'Overview' tab is selected, displaying essential information about the application, which is highlighted by a red box. This information includes the display name, application (client) ID, object ID, directory (tenant) ID, supported account types, client credentials, redirect URIs, application ID URI, and managed application in local directory. A bottom message states that starting June 30th, 2020, new features will not be added to ADAL and Graph, and applications will need to be upgraded to MSAL and Microsoft Graph.

**Azure Active Directory admin center**

Dashboard > Icewolf | App registrations >

## Demo-EXO-RBAC

Search

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

### Essentials

Display name <a href="#">Demo-EXO-RBAC</a>	Client credentials <a href="#">1 certificate_0 secret</a>
Application (client) ID cd32481c-6da8-47a1-b55b-742d2c3af888	Redirect URIs <a href="#">Add a Redirect URI</a>
Object ID 7079e588-c2b8-4f6b-9575-5651e28b45fa	Application ID URI <a href="#">Add an Application ID URI</a>
Directory (tenant) ID 46bbad84-29f0-4e03-8d34-f6841a5071ad	Managed application in local directory <a href="#">Demo-EXO-RBAC</a>
Supported account types <a href="#">My organization only</a>	

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

# Authentication mit Zertifikat

Azure Active Directory admin center

Dashboard > Icewolf | App registrations > Demo-EXO-RBAC

## Demo-EXO-RBAC | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

**Certificates & secrets**

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

**Certificates (1)** Client secrets (0) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Description	Start date	Expires	Certifica
07EFF3918F47995E853891848F6985C0E78622FD	O365Powershell3.cer	10/11/2022	10/11/2024	615fb458-



# Permissions

**Azure Active Directory admin center**

Dashboard > Icewolf | App registrations > Demo-EXO-RBAC

## Demo-EXO-RBAC | API permissions

Search Refresh Got feedback?

**Manage**

- Overview
- Quickstart
- Integration assistant
- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners

**Configured permissions**

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) ☒ Grant admin consent for Icewolf

API / Permissions name	Type	Description	Admin consent req...	Status
No permissions added				

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

# Service Principal / Enterprise Applications

Azure Active Directory admin center

Dashboard > Icewolf | Enterprise applications > Enterprise applications | All applications >

## Demo-EXO-RBAC | Overview

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

**Properties**

Name: Demo-EXO-RBAC

Application ID: cd32481c-6da8-47a1-b55b-...

Object ID: bbe8724e-05fd-42af-8c9a-8...

**Getting Started**

Windows PowerShell

```
PS C:\> #####
PS C:\> # Get AzureAD Application with Microsoft.Graph PowerShell
PS C:\> #####
PS C:\> Connect-MgGraph -Scopes 'Application.Read.All'
Welcome To Microsoft Graph!
PS C:\> $ServicePrincipalDetails = Get-MgServicePrincipal -Filter "DisplayName eq 'Demo-EXO-RBAC'"
PS C:\> $ServicePrincipalDetails
```

Id	DisplayName	AppId	SignInAudience
bb8724e-05fd-42af-8c9a-8879ff974a0a	Demo-EXO-RBAC	cd32481c-6da8-47a1-b55b-742d2c3af888	AzureADMyOrg

PS C:\>

# Erstellen vom Exchange Service Principal

```
Windows PowerShell
PS C:\> Connect-ExchangeOnline

-----
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Client-Server communication. You can now run these cmdlets after turning off WinRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherently.

However, REST backed EOP and SCC cmdlets are not available yet. To use those, you will need to enable WinRM Basic Auth.

For more information check https://aka.ms/exov3-module
-----

PS C:\> New-ServicePrincipal -AppId $ServicePrincipalDetails.AppId -ServiceId $ServicePrincipalDetails.Id -DisplayName "EXO Serviceprincipal $($ServicePrincipalDetails.Displayname)"

DisplayName                ServiceId                  AppId
-----
EXO Serviceprincipal Demo-EXO-RBAC  bbe8724e-05fd-42af-8c9a-8879ff974a0a  cd32481c-6da8-47a1-b55b-742d2c3af888

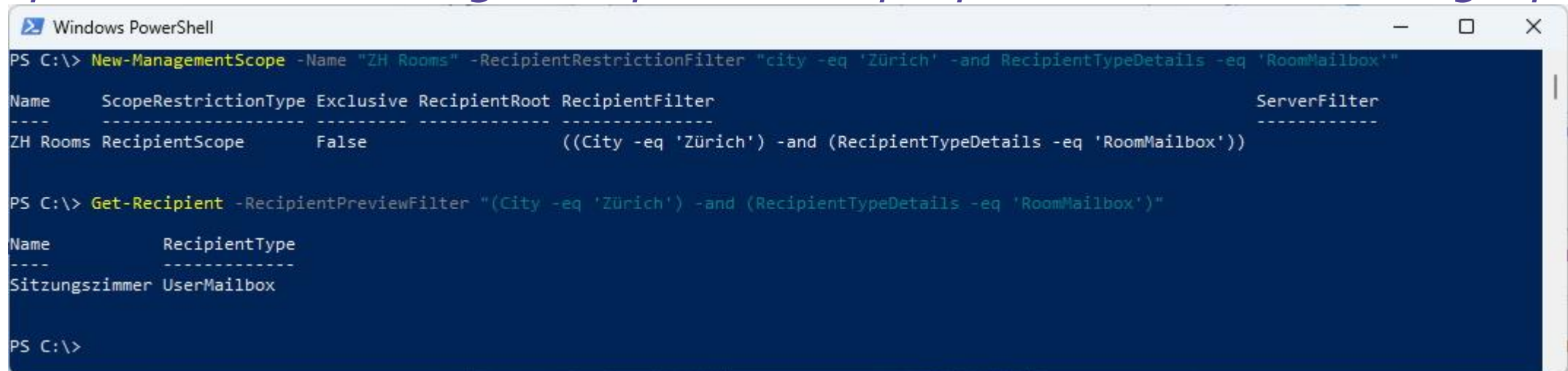
PS C:\> Get-ServicePrincipal | where {$_.AppId -eq "cd32481c-6da8-47a1-b55b-742d2c3af888"}

DisplayName                ServiceId                  AppId
-----
EXO Serviceprincipal Demo-EXO-RBAC  bbe8724e-05fd-42af-8c9a-8879ff974a0a  cd32481c-6da8-47a1-b55b-742d2c3af888

PS C:\>
```

## Management Scope

- *New-ManagementScope* <https://learn.microsoft.com/en-us/powershell/module/exchange/new-managementscope?view=exchange-ps>
- *Filterable properties for the RecipientFilter parameter on Exchange cmdlets* <https://learn.microsoft.com/en-us/powershell/exchange/recipientfilter-properties?view=exchange-ps>



```

Windows PowerShell
PS C:\> New-ManagementScope -Name "ZH Rooms" -RecipientRestrictionFilter "city -eq 'Zürich' -and RecipientTypeDetails -eq 'RoomMailbox'"

Name      ScopeRestrictionType Exclusive RecipientRoot RecipientFilter ServerFilter
----      -
ZH Rooms  RecipientScope      False      ((City -eq 'Zürich') -and (RecipientTypeDetails -eq 'RoomMailbox'))

PS C:\> Get-Recipient -RecipientPreviewFilter "(City -eq 'Zürich') -and (RecipientTypeDetails -eq 'RoomMailbox')"

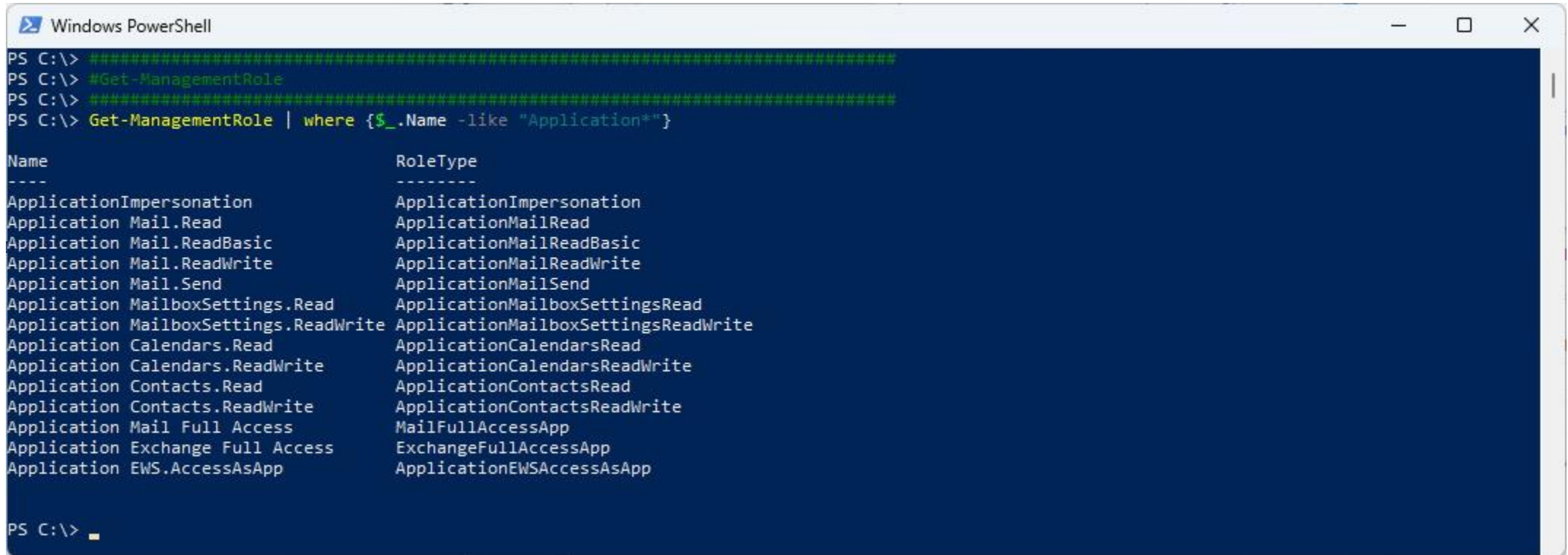
Name      RecipientType
----      -
Sitzungszimmer UserMailbox

PS C:\>
  
```



## Management Role

- *Get-ManagementRole | where {\$\_.Name -like "Application\*"}*



```

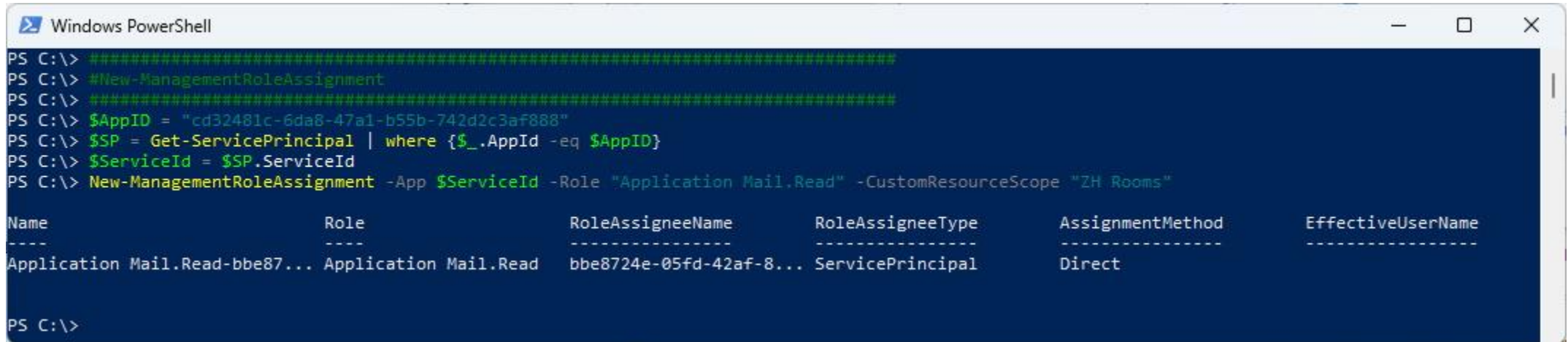
Windows PowerShell
PS C:\> #####
PS C:\> #Get-ManagementRole
PS C:\> #####
PS C:\> Get-ManagementRole | where {$_.Name -like "Application*"}

Name                                     RoleType
----
ApplicationImpersonation                ApplicationImpersonation
Application Mail.Read                   ApplicationMailRead
Application Mail.ReadBasic              ApplicationMailReadBasic
Application Mail.ReadWrite              ApplicationMailReadWrite
Application Mail.Send                   ApplicationMailSend
Application MailboxSettings.Read        ApplicationMailboxSettingsRead
Application MailboxSettings.ReadWrite   ApplicationMailboxSettingsReadWrite
Application Calendars.Read              ApplicationCalendarsRead
Application Calendars.ReadWrite         ApplicationCalendarsReadWrite
Application Contacts.Read               ApplicationContactsRead
Application Contacts.ReadWrite          ApplicationContactsReadWrite
Application Mail Full Access            MailFullAccessApp
Application Exchange Full Access        ExchangeFullAccessApp
Application EWS.AccessAsApp             ApplicationEWSAccessAsApp

PS C:\>
  
```

## Management Role Assignment

- `$AppID = "cd32481c-6da8-47a1-b55b-742d2c3af888"`  
`$SP = Get-ServicePrincipal | where {$_.AppId -eq $AppID}`  
`$ServiceId = $SP.ServiceId`  
`New-ManagementRoleAssignment -App $ServiceId -Role "Application Mail.Read" -CustomResourceScope "ZH Rooms"`



```

Windows PowerShell
PS C:\> #####
PS C:\> #New-ManagementRoleAssignment
PS C:\> #####
PS C:\> $AppID = "cd32481c-6da8-47a1-b55b-742d2c3af888"
PS C:\> $SP = Get-ServicePrincipal | where {$_.AppId -eq $AppID}
PS C:\> $ServiceId = $SP.ServiceId
PS C:\> New-ManagementRoleAssignment -App $ServiceId -Role "Application Mail.Read" -CustomResourceScope "ZH Rooms"

Name                               Role                               RoleAssigneeName                RoleAssigneeType                AssignmentMethod                EffectiveUserName
----                               -
Application Mail.Read-bbe87... Application Mail.Read            bbe8724e-05fd-42af-8... ServicePrincipal                Direct                          -----
PS C:\>
  
```

## Check der Management Role

- *Get-ManagementRoleAssignment | where {\$\_.App -eq \$ServiceId}*
- *Get-ManagementRoleAssignment | where {\$\_.App -eq \$ServiceId} | fl*

```
Windows PowerShell
PS C:\> #####
PS C:\> #Get-ManagementRoleAssignment
PS C:\> #####
PS C:\> Get-ManagementRoleAssignment | where {$_.App -eq $ServiceId}

Name                Role                RoleAssigneeName    RoleAssigneeType    AssignmentMethod    EffectiveUserName
----                -
Application Mail.Read-bbe87... Application Mail.Read bbe8724e-05fd-42af-8... ServicePrincipal    Direct              bbe8724e-05fd-42af-...

PS C:\> Get-ManagementRoleAssignment | where {$_.App -eq $ServiceId} | fl

DataObject           : Application Mail.Read-bbe8724e-05fd-42af-8c9a-8879ff974a0a
User                 :
App                   : bbe8724e-05fd-42af-8c9a-8879ff974a0a
AssignmentMethod      : Direct
Identity             : Application Mail.Read-bbe8724e-05fd-42af-8c9a-8879ff974a0a
EffectiveUserName     : bbe8724e-05fd-42af-8c9a-8879ff974a0a
AssignmentChain       :
RoleAssigneeType     : ServicePrincipal
RoleAssignee         : bbe8724e-05fd-42af-8c9a-8879ff974a0a
Role                  : Application Mail.Read
RoleAssignmentDelegationType : Regular
CustomRecipientWriteScope :
CustomResourceScope   : ZH Rooms
CustomConfigWriteScope :
RecipientReadScope    : Organization
```

# Testing – Verbinden mit MgGraph

```
Windows PowerShell
PS C:\> #####
PS C:\> #Connect-MgGraph
PS C:\> #https://github.com/microsoftgraph/msgraph-sdk-powershell
PS C:\> #####
PS C:\> #Connect with Certificate
PS C:\> $TenantId = "icewolfch.onmicrosoft.com"
PS C:\> $Scope = "https://graph.microsoft.com/.default"
PS C:\> $AppID = "cd32481c-6da8-47a1-b55b-742d2c3af888" #Demo-EXO-RBAC
PS C:\> $CertificateThumbprint = "07eff3918f47995eb53b91848f69b5c0e78622fd"
PS C:\> Connect-MgGraph -AppId $AppID -CertificateThumbprint $CertificateThumbprint -TenantId $TenantId
Welcome To Microsoft Graph!
PS C:\> Get-MgContext

ClientId           : cd32481c-6da8-47a1-b55b-742d2c3af888
TenantId           : 46bbad84-29f0-4e03-8d34-f6841a5071ad
Scopes              :
AuthType           : AppOnly
TokenCredentialType : ClientCertificate
CertificateThumbprint : 07eff3918f47995eb53b91848f69b5c0e78622fd
CertificateSubjectName :
Account            :
AppName            : Demo-EXO-RBAC
ContextScope       : Process
Certificate         :
PSHostVersion      : 5.1.22621.963
ManagedIdentityId  :
ClientSecret       :

PS C:\>
```



## Folder auflisten

- \$Mailbox = "sitzungszimmer@icewolf.ch"
- Import-Module Microsoft.Graph.Mail  
\$Result = Get-MgUserMailFolder -UserId \$Mailbox  
\$Result | Format-List DisplayName, TotalItemCount, UnreadItemCount, id

```
Windows PowerShell
PS C:\> #####
PS C:\> #Get mailFolder
PS C:\> #https://docs.microsoft.com/en-us/graph/api/mailfolder-get?view=graph-rest-1.0&tabs=http
PS C:\> #####
PS C:\> $Mailbox = "sitzungszimmer@icewolf.ch"
PS C:\> Import-Module Microsoft.Graph.Mail
PS C:\> $Result = Get-MgUserMailFolder -UserId $Mailbox
PS C:\> $Result | Format-List DisplayName, TotalItemCount, UnreadItemCount, id

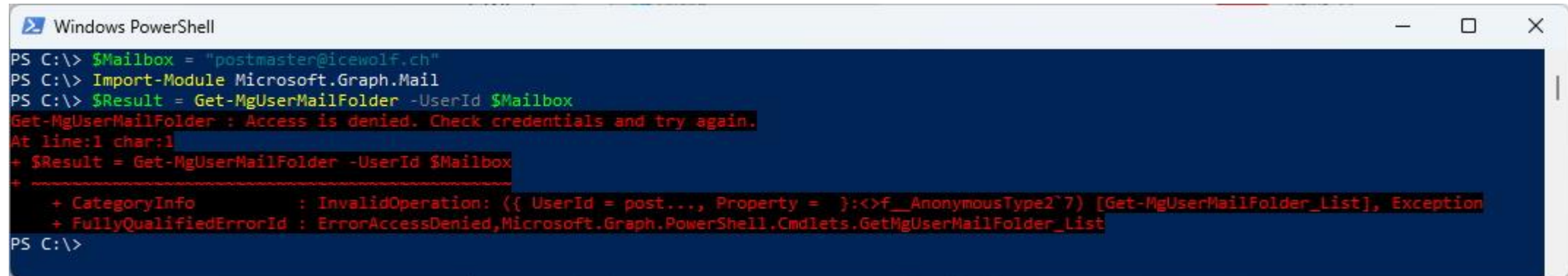
DisplayName      : Archive
TotalItemCount   : 0
UnreadItemCount  : 0
Id               : AAMkADg4ZGZmNjUyLTcxMDQtNDlmNS1hMGYyLTRkMjVjMzliOTc2MwAuAAAAADdP8zT6mLTS7DH9hjNwK7SAQCrvuM2I2dYQ5S99saA1xSoAAAAAEcAAA=

DisplayName      : Conversation History
TotalItemCount   : 0
UnreadItemCount  : 0
Id               : AAMkADg4ZGZmNjUyLTcxMDQtNDlmNS1hMGYyLTRkMjVjMzliOTc2MwAuAAAAADdP8zT6mLTS7DH9hjNwK7SAQCrvuM2I2dYQ5S99saA1xSoAAAAAEHAAA=

DisplayName      : Entwürfe
TotalItemCount   : 0
UnreadItemCount  : 0
Id               : AAMkADg4ZGZmNjUyLTcxMDQtNDlmNS1hMGYyLTRkMjVjMzliOTc2MwAuAAAAADdP8zT6mLTS7DH9hjNwK7SAQBOM8iRs jH4TpI5TTNgq29XAB61SchDAAA=
```

## Mailbox ausserhalb von Management Scope

- *\$Mailbox = "postmaster@icewolf.ch"*
- *Import-Module Microsoft.Graph.Mail*  
*\$Result = Get-MgUserMailFolder -UserId \$Mailbox*



```

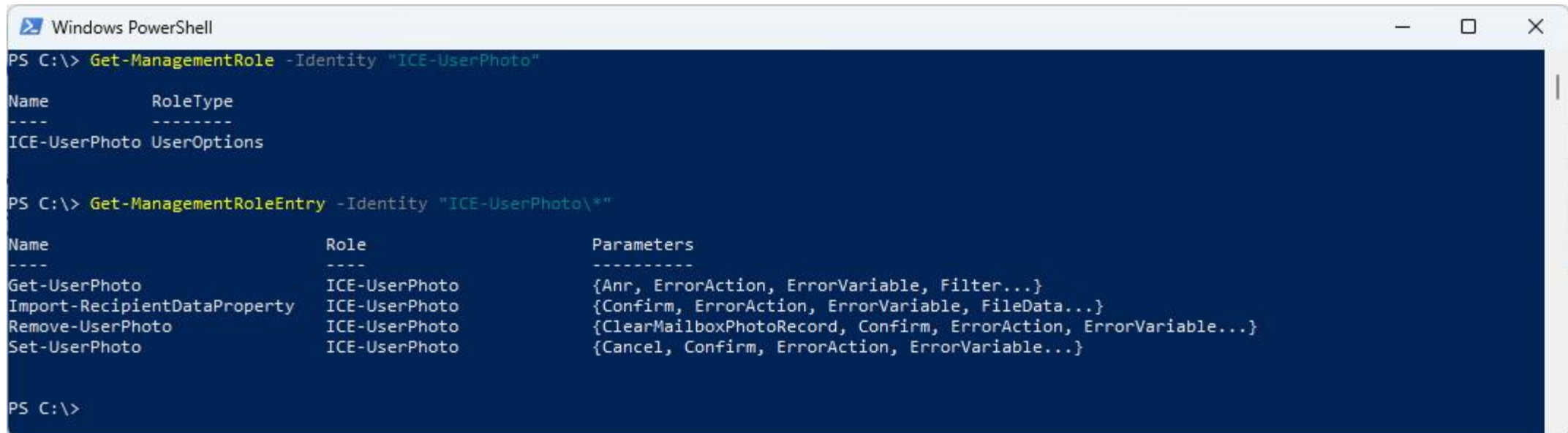
Windows PowerShell
PS C:\> $Mailbox = "postmaster@icewolf.ch"
PS C:\> Import-Module Microsoft.Graph.Mail
PS C:\> $Result = Get-MgUserMailFolder -UserId $Mailbox
Get-MgUserMailFolder : Access is denied. Check credentials and try again.
At line:1 char:1
+ $Result = Get-MgUserMailFolder -UserId $Mailbox
+ ~~~~~
+ CategoryInfo          : InvalidOperation: ({} UserId = post..., Property =  }:<>f__AnonymousType2`7) [Get-MgUserMailFolder_List], Exception
+ FullyQualifiedErrorId : ErrorAccessDenied,Microsoft.Graph.PowerShell.Cmdlets.GetMgUserMailFolder_List
PS C:\>
  
```

## Fazit

- Die Preview benötigt einen separaten Exchange Service Principal
- Mail.Task fehlt (dafür gibt es auch im Graph keine Application Permission)
- RBAC Rollen in Exchange waren schon immer komplex 😊
- Zurzeit nur mit PowerShell möglich – kein GUI
- Die Übersicht wer wo Berechtigungen hat, wird dadurch nicht einfacher

# Exchange Custom RBAC Role with App Authentication

- ExchangeOnlineManagement mit custom RBAC Role
  - Application Permission "Exchange.ManageAsApp"
  - Bisher: AzureAD Rolle "Exchange Administrator" / "Exchange Recipient Administrator"
- [Exchange Online custom RBAC Role with App Authentication \(OAuth2\)](#)



```

Windows PowerShell
PS C:\> Get-ManagementRole -Identity "ICE-UserPhoto"

Name          RoleType
----          -
ICE-UserPhoto UserOptions

PS C:\> Get-ManagementRoleEntry -Identity "ICE-UserPhoto\*"

Name          Role          Parameters
----          -
Get-UserPhoto ICE-UserPhoto {Anr, ErrorAction, ErrorVariable, Filter...}
Import-RecipientDataProperty ICE-UserPhoto {Confirm, ErrorAction, ErrorVariable, FileData...}
Remove-UserPhoto ICE-UserPhoto {ClearMailboxPhotoRecord, Confirm, ErrorAction, ErrorVariable...}
Set-UserPhoto ICE-UserPhoto {Cancel, Confirm, ErrorAction, ErrorVariable...}

PS C:\>
    
```

## New-RoleGroup

- `$AppID = "341772e9-4f7a-4444-9b2c-66620d27aec0"`  
`$SP = Get-ServicePrincipal | where {$_.AppId -eq $AppID}`  
`$ServiceId = $SP.ServiceId`  
`New-RoleGroup -Name 'Icewolf-UserPhoto' -Roles "ICE-UserPhoto" -CustomRecipientWriteScope "ZH Rooms"`  
`Add-RoleGroupMember -Identity "Icewolf-UserPhoto" -Member $ServiceId`

```

Windows PowerShell
PS C:\> $AppID = "341772e9-4f7a-4444-9b2c-66620d27aec0"
PS C:\> $SP = Get-ServicePrincipal | where {$_.AppId -eq $AppID}
PS C:\> $ServiceId = $SP.ServiceId
PS C:\> New-RoleGroup -Name 'Icewolf-UserPhoto' -Roles "ICE-UserPhoto" -CustomRecipientWriteScope "ZH Rooms"

WARNING: Parameter Id is not enabled and is ignored.
Name                AssignedRoles  RoleAssignments                                     ManagedBy
----                -
Icewolf-UserPhoto {ICE-UserPhoto} {icewolfch.onmicrosoft.com\ICE-UserPhoto-Icewolf-UserPhoto} {Organization Management, Bohren, Andres}

PS C:\> Add-RoleGroupMember -Identity "Icewolf-UserPhoto" -Member $ServiceId
PS C:\>
  
```



## Ergebnis

ExchangeOnlineManagement

CustomRecipientWriteScope

Get-Commandlet

geht für alle MBX

```
Windows PowerShell
PS C:\> $AppID = "341772e9-4f7a-4444-9b2c-66620d27aec0"
PS C:\> $CertificateThumbprint = "07eff3918f47995eb53b91848f69b5c0e78622fd"
PS C:\> $TenantId = "icewolfch.onmicrosoft.com"
PS C:\> Connect-ExchangeOnline -AppId $AppID -CertificateThumbprint $CertificateThumbprint -Organization $TenantId

-----
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Client-Server communication. You can now run these cmdlets after turning off WinRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherently.

However, REST backed EOP and SCC cmdlets are not available yet. To use those, you will need to enable WinRM Basic Auth.

For more information check https://aka.ms/exov3-module
-----

PS C:\> Get-ConnectionInformation

ConnectionId      : eac949dc-a642-4864-a45b-278145e0a479
State             : Connected
Id                : 3
Name              : ExchangeOnline_3
UserPrincipalName : OAuthUser@icewolfch.onmicrosoft.com
ConnectionUri     : https://outlook.office365.com
AzureAdAuthorizationEndpointUri : https://login.microsoftonline.com/icewolfch.onmicrosoft.com
TokenExpiryTimeUTC : 1/9/2023 10:39:53 AM +00:00
CertificateAuthentication : True
ModuleName        : C:\Users\A.Bohren\AppData\Local\Temp\tmpEXO_lieuhz5a.ozw
ModulePrefix      :
Organization      : icewolfch.onmicrosoft.com
DelegatedOrganization :
AppId             : 341772e9-4f7a-4444-9b2c-66620d27aec0
PageSize          : 1000
TenantID          : 46bbad84-29f0-4e03-8d34-f6841a5071ad
TokenStatus       : Active

PS C:\> Get-Command -Module tmpEXO_lieuhz5a.ozw

CommandType Name Version Source
-----
Function Get-UserPhoto 1.0 tmpEXO_lieuhz5a.ozw
Function Import-RecipientDataProperty 1.0 tmpEXO_lieuhz5a.ozw
Function Remove-UserPhoto 1.0 tmpEXO_lieuhz5a.ozw
Function Set-UserPhoto 1.0 tmpEXO_lieuhz5a.ozw

PS C:\>
```

isolutions'

DEMO

isolutions'

