

Leitfaden: Zugriff auf Exchange Online Postfächer einschränken

Dieser Leitfaden wurde bisher mit der Azure-Active-Directory-Cloud getestet.

Dieser Leitfaden bezieht ausschließlich auf die Verwendung der Microsoft Graph-API.

Welches Problem lösen wir ?

Wir verhindern, dass die Graph API zu viele Berechtigungen auf die Azure-Active-Directory Postfächer der verschiedenen Abteilungen erhält.

Was benötigen wir ?

Um diese Anforderung zu erfüllen benötigen wir folgende softwareseitig -Komponenten:

- Eine Powershell +7.0.0
 - [Wie installiere ich die Powershell ?](#)
- Azure-Active-Directory(AAD)
- das EXO-V2 Modular Powershell 7 in der Version 2.0.4 oder höher.
 - [Wie installiere ich das EXO-V2-Module in der Powershell 7](#)
 - [Ich habe ein Problem beim ausführen von EXO-V2 !](#)
 - [Eine Email-Zugriffsberechtigte-Gruppe](#)

Vorwort

Diese Dokumentation umfasst nicht die Einrichtung der Graph API für das Abholen der Emails durch Squeeze.

Die Anleitung der Einrichtung des Email-Import findest du [hier](#).

Zudem dient dieser Artikel zur Unterstützung der Admins, die Informationen können sich im laufe der Zeit auf den referenzierten Beiträgen ändern.

Das ausführen der nachfolgenden Schritte muss **unbedingt** von einem **Admin** des AAD's durchgeführt werden.

Was muss ich jetzt als nächstes tun ?

Um eine App in seinen Berechtigungen zu beschränken, bietet die Azure-Active-Directory das Anlegen von E-Mail-aktivierten Sicherheitsgruppen. Diese Sicherheitsgruppen können je nach Verwendung zum restriktiven Zugriff auf eine App genutzt werden. Desweiteren sind diese Gruppen in der AAD-Admin-Oberfläche im Standard nicht zu einer App hinzugefügt. Diese Einstellungen kann man nur durch die Verwendung der Powershell in Verbindung mit dem EXO-V2 Modul und eines **Admin AAD Accounts** tätigen.

Erstellen einer E-Mail aktivierten Sicherheitsgruppe

Wenn du bereits eine Sicherheitsgruppe erstellt hast, springe zu: [Verbinden der App mit der E-Mail Sicherheitsgruppe](#)

Um eine E-Mail-aktivierte Sicherheitsgruppe zu erstellen, wollen wir erst einmal auf [die Admin-Oberfläche des AAD's](#). Dort klicken wir auf die drei angegebenen Punkte (s. Screenshot) :

Microsoft 365 admin center

Suchen

Start > Aktive Teams und Gruppen

Dunkler Modus

Aktive Teams und Gruppen

Microsoft Teams unterstützt die Zusammenarbeit durch Chats, Anrufe und Onlinebesprechungen. Die Teams, die Sie hinzufügen, sind Sammlungen von Personen, Inhalten und Tools. Gruppen sind eine Sammlung von Personen und nützlich, wenn Sie nur eine Gruppen-E-Mail-Adresse benötigen. Es kann bis zu einer Stunde dauern, bis hier neue Verteilergruppen und E-Mail-aktivierte Sicherheitsgruppen angezeigt werden. Um sie sofort anzuzeigen, [wechseln Sie zum Exchange Admin Center](#)

[Informationen zu Microsoft Teams](#)

Microsoft 365 Verteilerliste **E-Mail-aktivierte Sicherheit** Sicherheit

Alle Teams und Gruppen suchen

Gruppe hinzufügen Exportieren Aktualisieren

1 Element

	Name ↑	E-Mail	Synchron...	Er
<input type="checkbox"/>	DexproMailTest	mailto:taadgraphapi@dexpro.de		14

Im nachfolgenden sind diese weiteren dokumentierten Schritte auszuführen.

The screenshot shows the 'Microsoft 365 admin center' interface. The breadcrumb trail is 'Aktive Teams und Gruppen > Gruppe hinzufügen'. The left sidebar shows a progress bar with steps: Gruppentyp (selected), Grundlagen, Besitzer, Mitglieder, Einstellungen, and Fertig stellen. The main content area is titled 'Gruppentyp auswählen'. It instructs the user to choose a group type that best fits their team's needs, with a link for 'Weitere Informationen zu Gruppentypen'. Three options are listed: 'Microsoft 365 (empfohlen)' (which allows collaboration by providing a group email address and a shared workspace), 'Verteilung' (which creates an email address for a group of people), and 'E-Mail-aktivierte Sicherheit' (which is selected and marked with a red circle containing the number 1; it is described as a distribution list that can also be used for controlling access to OneDrive and SharePoint).

Name und Beschreibung festlegen:

The screenshot shows the same 'Microsoft 365 admin center' interface, but at step 2: 'Einrichten der Grundlagen'. The progress bar in the sidebar now shows 'Gruppentyp' as completed (with a checkmark) and 'Grundlagen' as the current step (selected). The main content area is titled 'Einrichten der Grundlagen' and instructs the user to fill in basic information about the group. There are two fields: 'Name' (marked with a red circle containing the number 1) and 'Beschreibung' (marked with a red circle containing the number 2). The 'Name' field contains the text 'BerechtigtePostfächer'. The 'Beschreibung' field contains the text 'Diese Gruppe berechtigt eine Application auf die zugeordneten Postfächer zuzugreifen.'

Wähle den Besitzer (Admin-Account):

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes the 'Microsoft 365 admin center' logo and a search bar. The left sidebar shows a navigation menu with icons for home, users, groups, and settings. The main content area is titled 'Aktive Teams und Gruppen > Gruppe hinzufügen'. On the left, a vertical progress bar shows the steps: Gruppentyp (checked), Grundlagen (checked), **Besitzer** (selected), Mitglieder, Einstellungen, and Fertig stellen. The main content area is titled 'Besitzer zuweisen'. It contains a paragraph explaining that group owners have unique permissions to manage the group, including adding and removing members, changing group settings, renaming the group, and updating the description. Below this, a warning message states: 'Sie müssen mindestens einen Besitzer haben. Es wird empfohlen, zwei hinzufügen, damit einer während der Abwesenheit des anderen helfen kann.' (You must have at least one owner. It is recommended to add two so that one can help during the absence of the other.) At the bottom, there is a button '+ Besitzer zuweisen' with a red circle containing the number '1', and a section titled 'Gruppenbesitzer hinzufügen' with the text 'Neue Besitzer erhalten eine E-Mail, wenn sie von Ihnen hinzugefügt werden'.

Wähle nun Mitglieder/Email-Accounts die auf die App durch diese Gruppe berechtigt werden soll:

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes the 'Microsoft 365 admin center' logo and a search bar. The left sidebar shows a navigation menu with icons for home, users, groups, and settings. The main content area is titled 'Aktive Teams und Gruppen > Gruppe hinzufügen'. On the left, a vertical progress bar shows the steps: Gruppentyp (checked), Grundlagen (checked), Besitzer (checked), **Mitglieder** (selected), Einstellungen, and Fertig stellen. The main content area is titled 'Mitglieder hinzufügen'. It contains a paragraph explaining that group members have access to all elements that the group can access, and they receive emails sent to the group's email address. Standardly, guests can be invited to participate in the group, but they cannot edit group settings. Below this, there is a button '+ Mitglieder hinzufügen' with a red circle containing the number '1'. At the bottom, there is a section titled 'Anzeigenamen' with a checkbox and a list of users, including 'Vahdettin Balum' with a blue circle containing the letters 'VB'.

Nun vergeben wir der Gruppe eine eigene Email-Address:

Die Gruppen-Email Adresse wird für später verwendet, daher sollte man sich diese Email ablegen.

Microsoft 365 admin center

Aktive Teams und Gruppen > Gruppe hinzufügen

Einstellungen bearbeiten

E-Mail-aktivierte Sicherheitsgruppe
Verfügt über alle Funktionen einer Verteilerliste und kann darüber hinaus verwendet werden, um den Zugriff auf OneDrive und SharePoint zu steuern.

E-Mail-Adresse der Gruppe *

1 eindeutigeEmailAdresseDerGruppe @ dexpro.de

Kommunikation

☐ Personen außerhalb meiner Organisation das Senden von E-Mails an diese E-Mail-aktivierte Sicherheitsgruppe gestatten

Im letzten Fenster bestätigt ihr eure Einstellung und erstellt die Gruppe.

Verbinde Sicherheitsgruppe mit Application durch Powershell

Da wir nun eine E-Mail aktivierte Sicherheitsgruppe besitzen, müssen wir diese Gruppe der Application (die [zuvor erstellt wurde](#)) zuordnen. Aktuell haben wir nur die Möglichkeit über die Powershell in Verbindung mit EXO-V2 eine Gruppe, einer App hinzu zufügen.

Im ersten Schritt verbinden wir uns mit unserem AAD-Remote Cmdlet, dafür öffnen wir unsere Powershell als Administrator und geben folgenden Befehl ein. [Für weitere Information...](#)

```
Connect-ExchangeOnline -UserPrincipalName <admin@company.com>
```

Nun sollte sich ein Pop-Up öffnen, dass einen durch die Authentifizierung bei Microsoft führt.

Unter manchen Linux oder MacOS Distributionen wird kein Pop-Up geöffnet.
Um das Problem zu lösen muss über den Device-Code Flow die Authentifizierung durchgeführt werden.
Der folgende Befehl muss für den Device-Code Flow ausgeführt werden:

```
Connect-ExchangeOnline -device
```

Nach der erfolgreichen Authentifizierung, erhält man alle Remote-Cmdlets des Exchange-Servers auf die man Berechtigungen hat. Um nun eine App-Berechtigungsgruppe einer App zu zuordnen muss folgender Befehl ausgeführt werden.

```
New-ApplicationAccessPolicy -AppId <Deine Application ID / Client ID> -PolicyScopeGroupId  
deineGruppenEmail@deineFirma.com -AccessRight RestrictAccess -Description "Restrict this app  
to members of distribution group ...."
```

Ist der Befehl erfolgreich ausgeführt worden, dann kann mann seine Anpassungen mit diesem Befehl testen:

```
Test-ApplicationAccessPolicy -Identity deineGruppenEmail@deineFirma.com -AppId <deine  
Application ID / Client ID>
```

Das Ergebnis des Befehls sollte so aussehen:

```
PS /home/vahdettinbalum/SQUEEZE> Test-ApplicationAccessPolicy -Identity mailtestaadgraphapi@dexpro.de -AppId ec8b6e4f-b3ae-4b
4c-

RunspaceId      : 9d3b0f04-
AppId           : ec8b6e4f-
Mailbox         : DexproMai
MailboxId       : 4eea1556-
MailboxSid      : S-1-5-21-
AccessCheckResult : Gewährt

PS /home/vahdettinbalum/SQUEEZE>
```

Nun solltest du die App auf die ausgewählten Nutzer der E-Mail aktivierten Sicherheitsgruppe beschränkt haben.

Bis die Änderungen im AAD greifen, kann es bis zu einer Stunde laut Microsoft dauern.

Revision #10

Created 14 September 2022 13:25:25 by Vahdettin Balum

Updated 3 November 2022 13:10:23 by Fabian Terstegen