

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 Moduler 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 durch die 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) :

The screenshot shows the Microsoft 365 Admin Center interface. The left navigation pane has a red circle '1' next to 'Aktive Teams und Gruppen'. The main content area has a red circle '2' above the 'E-Mail-aktivierte Sicherheit' tab. Below the tabs, there is a red circle '3' above the 'Gruppe hinzufügen' button. A table below shows one group: 'DexproMailTest' with email 'mailto:exchapi@dexpro.de'.

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

Im nachfolgenden sind diese weiteren dokumentierten Schritte auszuführen.

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes the Microsoft 365 logo, a search bar with the text 'Suchen', and several utility icons. The main header reads 'Aktive Teams und Gruppen > Gruppe hinzufügen'. On the left, a vertical navigation pane lists steps: 'Gruppentyp' (selected with a blue dot), 'Grundlagen', 'Besitzer', 'Mitglieder', 'Einstellungen', and 'Fertig stellen'. The main content area is titled 'Gruppentyp auswählen'. It contains the instruction: 'Wählen Sie den Gruppentyp aus, der den Anforderungen Ihres Teams am besten entspricht. [Weitere Informationen zu Gruppentypen](#)'. Three options are listed: 'Microsoft 365 (empfohlen)' (radio button), 'Verteilung' (radio button), and 'E-Mail-aktivierte Sicherheit' (radio button, selected with a blue dot and marked with a red circle containing the number '1'). The description for 'E-Mail-aktivierte Sicherheit' reads: 'Eine Verteilerliste, die auch für die Steuerung des Zugriffs auf OneDrive und SharePoint verwendet werden kann.'

Name und Beschreibung festlegen:

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar is identical to the previous screenshot. The main header reads 'Aktive Teams und Gruppen > Gruppe hinzufügen'. The left navigation pane shows 'Gruppentyp' with a checkmark and 'Grundlagen' selected with a blue dot. The main content area is titled 'Einrichten der Grundlagen'. It contains the instruction: 'Füllen Sie zunächst einige grundlegende Informationen über die Gruppe aus, die Sie erstellen möchten.' There are two input fields: 'Name *' (marked with a red circle containing the number '1') with the value 'BerechtigtePostfächer' entered, and 'Beschreibung' (marked with a red circle containing the number '2') with the value 'Diese Gruppe berechtigt eine Application auf die zugeordneten Postfächer zuzugreifen.' entered.

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, a search bar with the text 'Suchen', and several utility icons. The main content area is titled 'Aktive Teams und Gruppen > Gruppe hinzufügen'. On the left, a vertical navigation pane shows a progress indicator with steps: Gruppentyp (checked), Grundlagen (checked), **Besitzer** (selected), Mitglieder, Einstellungen, and Fertig stellen. The main content area is titled 'Besitzer zuweisen'. It contains a descriptive paragraph: 'Gruppenbesitzer verfügen über eindeutige Berechtigungen zum Verwalten der Gruppe. Sie können Mitglieder hinzufügen und entfernen, Gruppeneinstellungen ändern, die Gruppe umbenennen, ihre Beschreibung aktualisieren und vieles mehr.' Below this is an information box with a red 'i' icon: 'Sie müssen mindestens einen Besitzer haben. Es wird empfohlen, zwei hinzuzufügen, damit einer während der Abwesenheit des anderen helfen kann.' At the bottom, there is a '+ Besitzer zuweisen' button 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 is identical to the previous screenshot. The main content area is titled 'Aktive Teams und Gruppen > Gruppe hinzufügen'. The left navigation pane shows the progress indicator with steps: Gruppentyp (checked), Grundlagen (checked), Besitzer (checked), **Mitglieder** (selected), Einstellungen, and Fertig stellen. The main content area is titled 'Mitglieder hinzufügen'. It contains a descriptive paragraph: 'Gruppenmitglieder haben Zugriff auf alle Elemente, auf die die Gruppe zugreifen kann, und empfangen E-Mails, die an die E-Mail-Adresse der Gruppe gesendet werden. Standardmäßig können Gäste zur Teilnahme an Ihrer Gruppe eingeladen werden, aber sie können keine Gruppeneinstellungen bearbeiten.' Below this is a '+ Mitglieder hinzufügen' button with a red circle containing the number '1'. At the bottom, there is a list of members with checkboxes: 'Anzeigename' (unchecked) and 'VB Vahdettin Balum' (unchecked).

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

Gruppentyp
Grundlagen
Besitzer
Mitglieder
Einstellungen
Fertig stellen

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 man 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