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-Zugriffsberechtige-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.

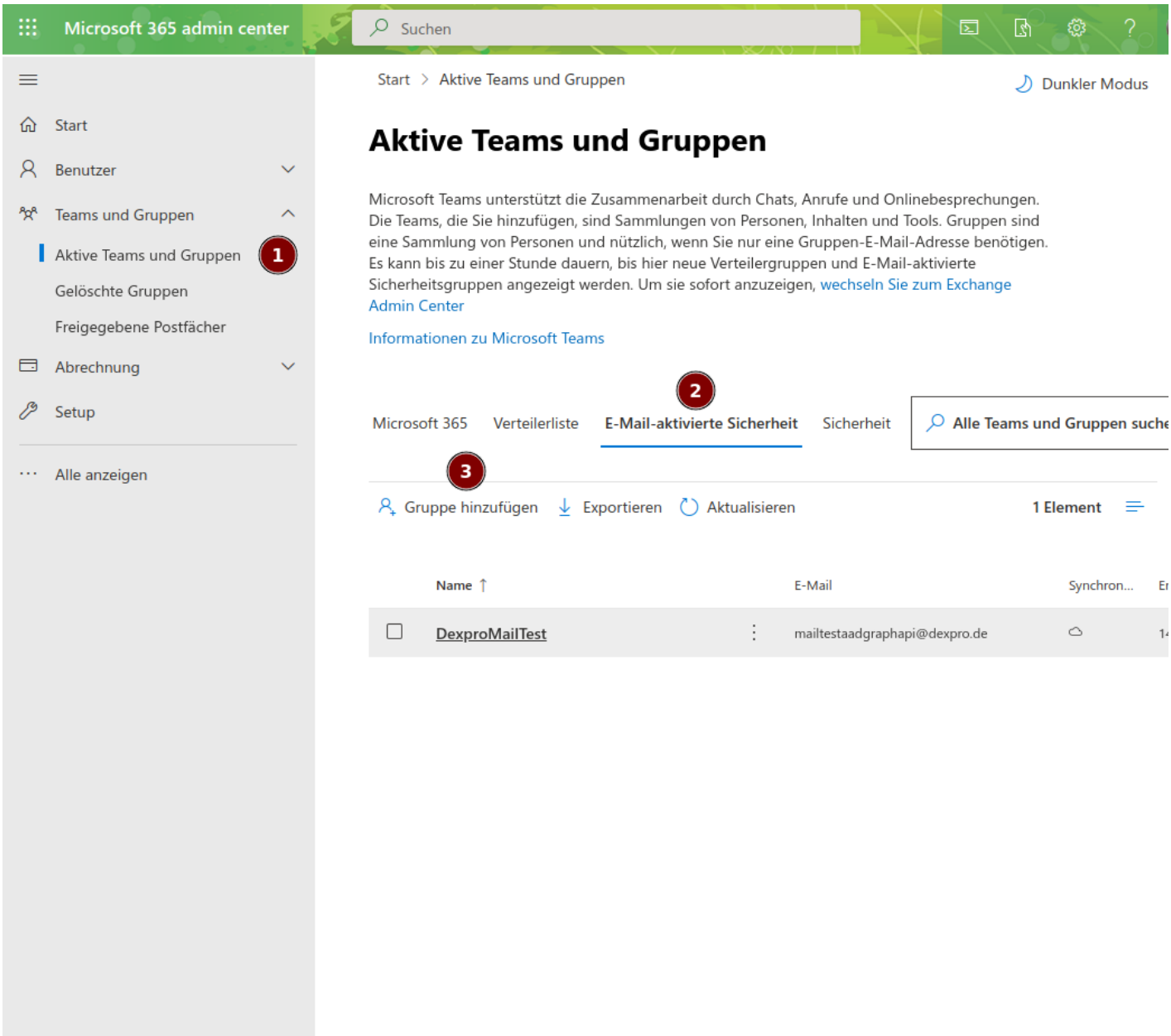
Was muss ich jetzt als nächstes tun ?

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 Standart 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.

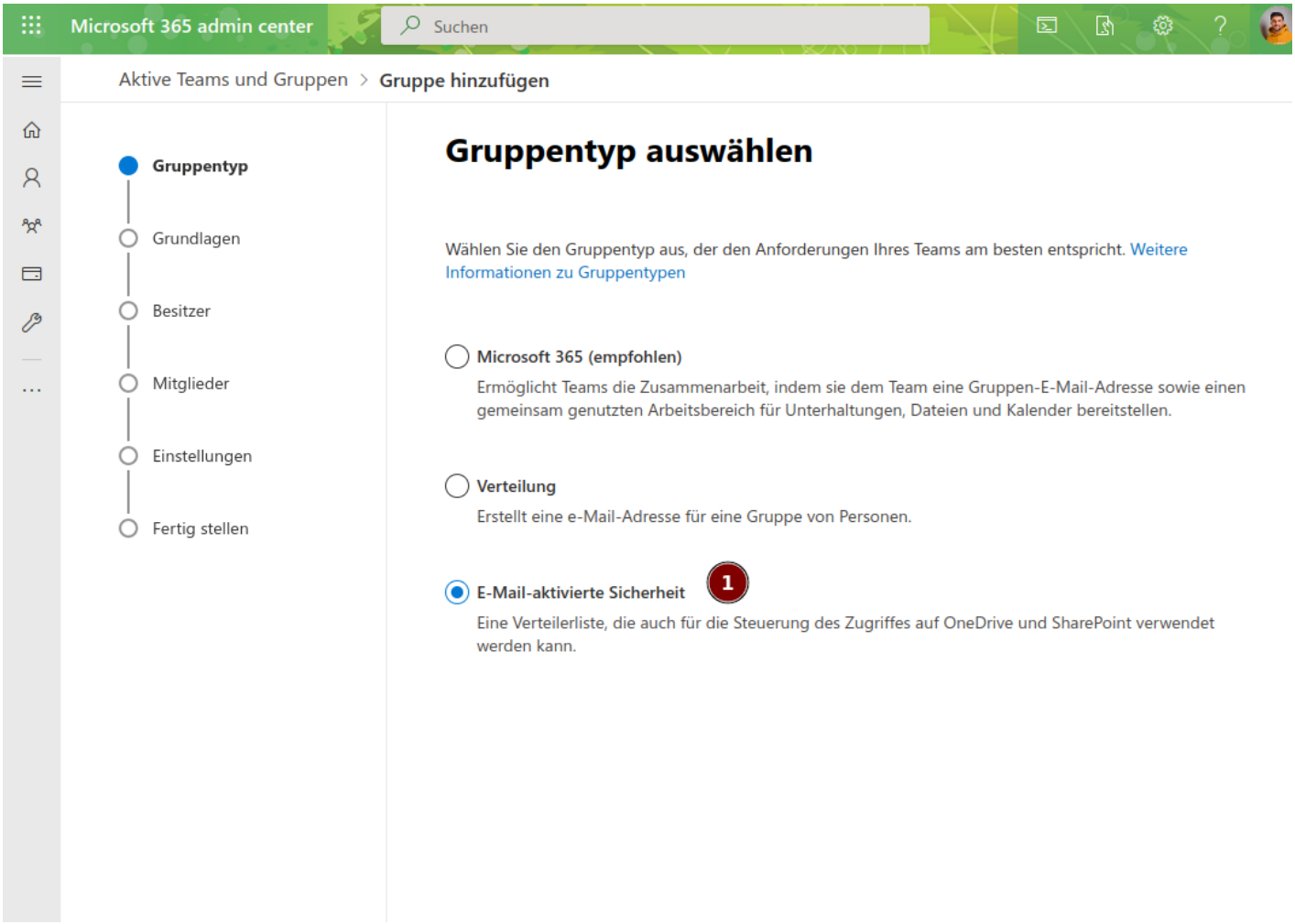
Erstellen einer E-Mail aktivierten Sicherheitsgruppe

Wenn du bereits eine Sicherheitsgruppe erstellt hast springe zu: Verbinden der App mit der E-Mail Sicherheitsgruppe

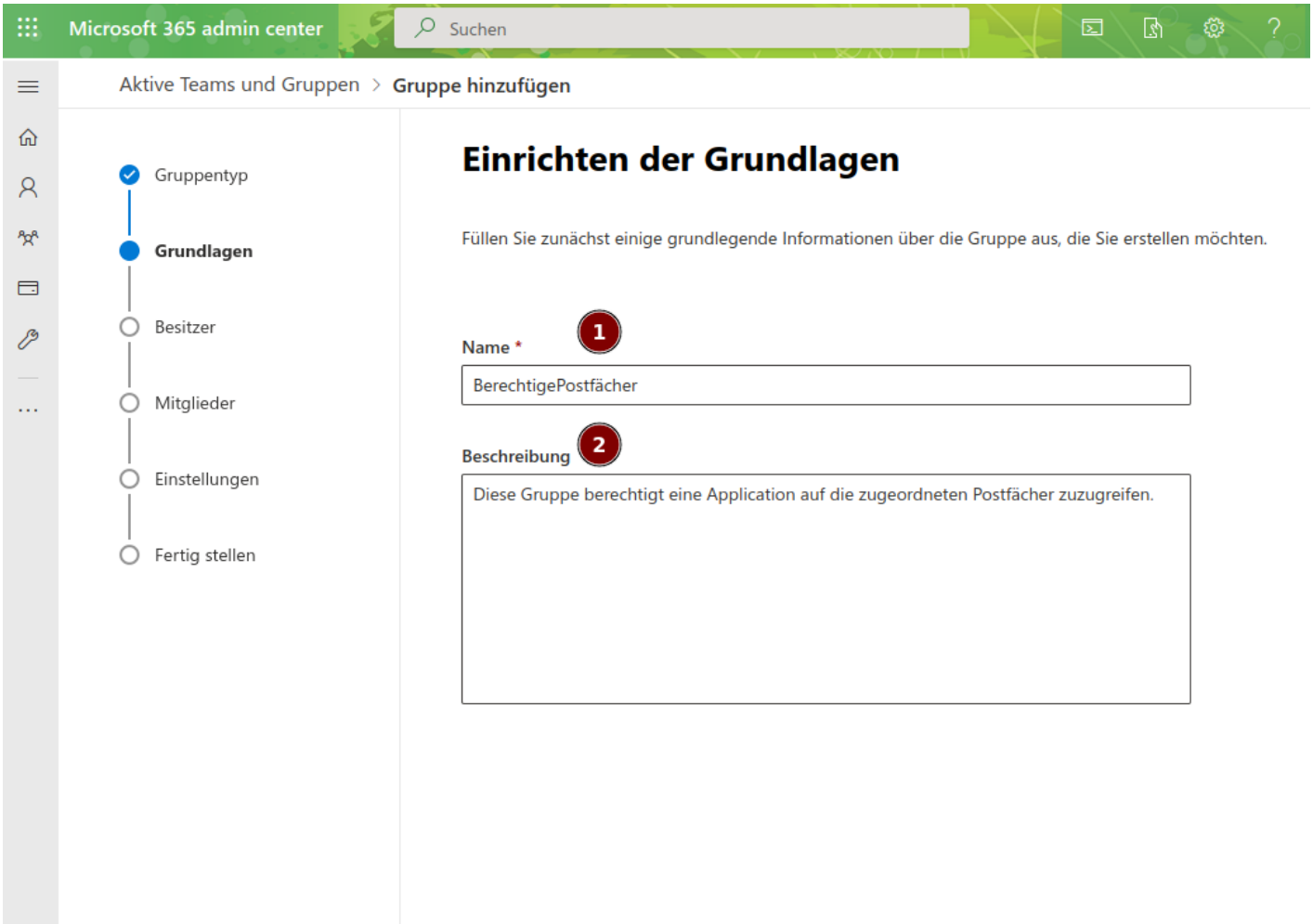
Um eine E Mail Aktivierte Sicherheitsgruppe zu erstellen wollen wir erst einmal auf die Admin-Oberfläche des AAD´s. Dort klicken wir auf die drei angegebenen Punkte (s. Screenshot) :



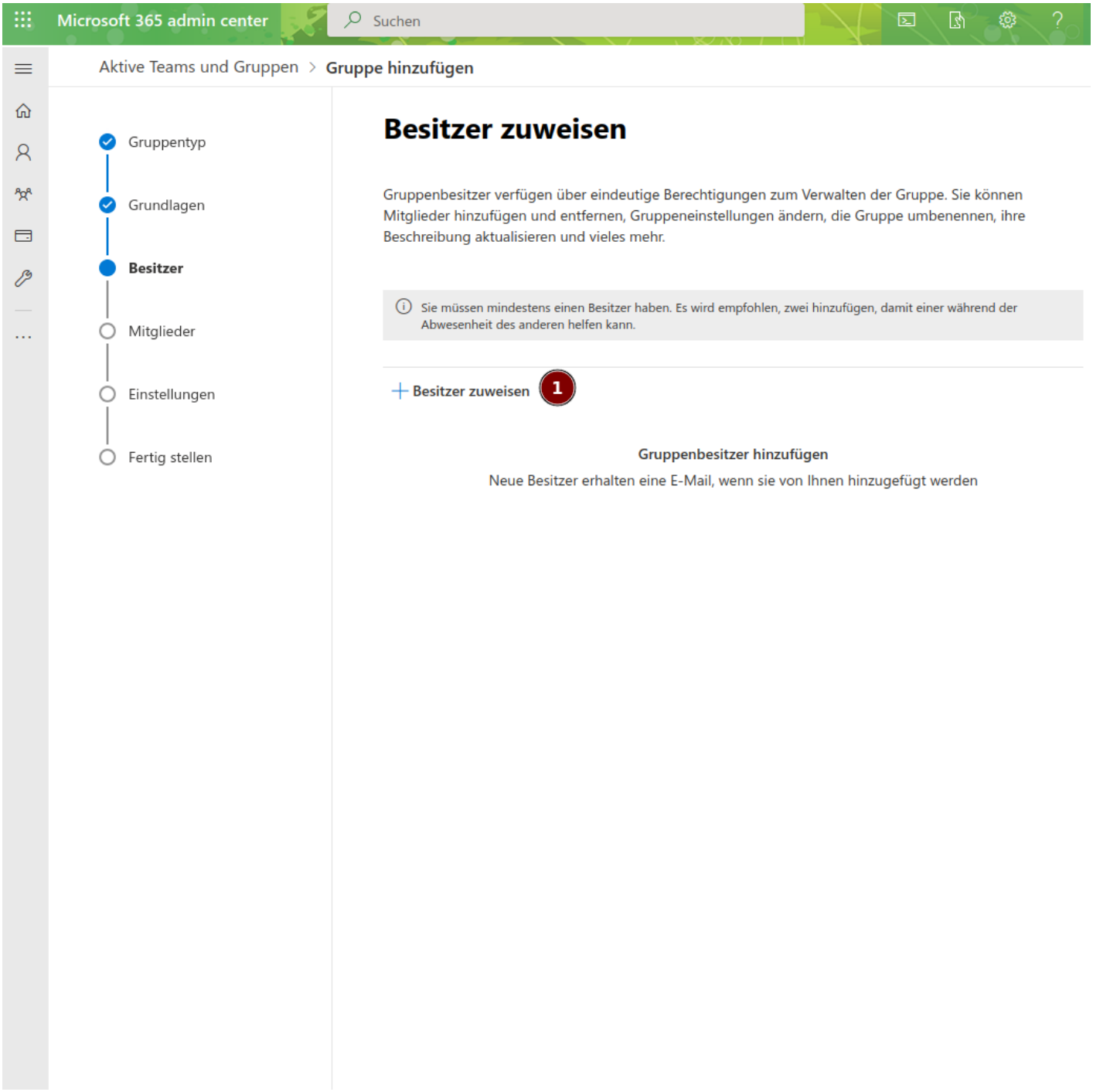
Im nachfolgenden sind diese weiteren dokumentierten Schritte auszuführen.



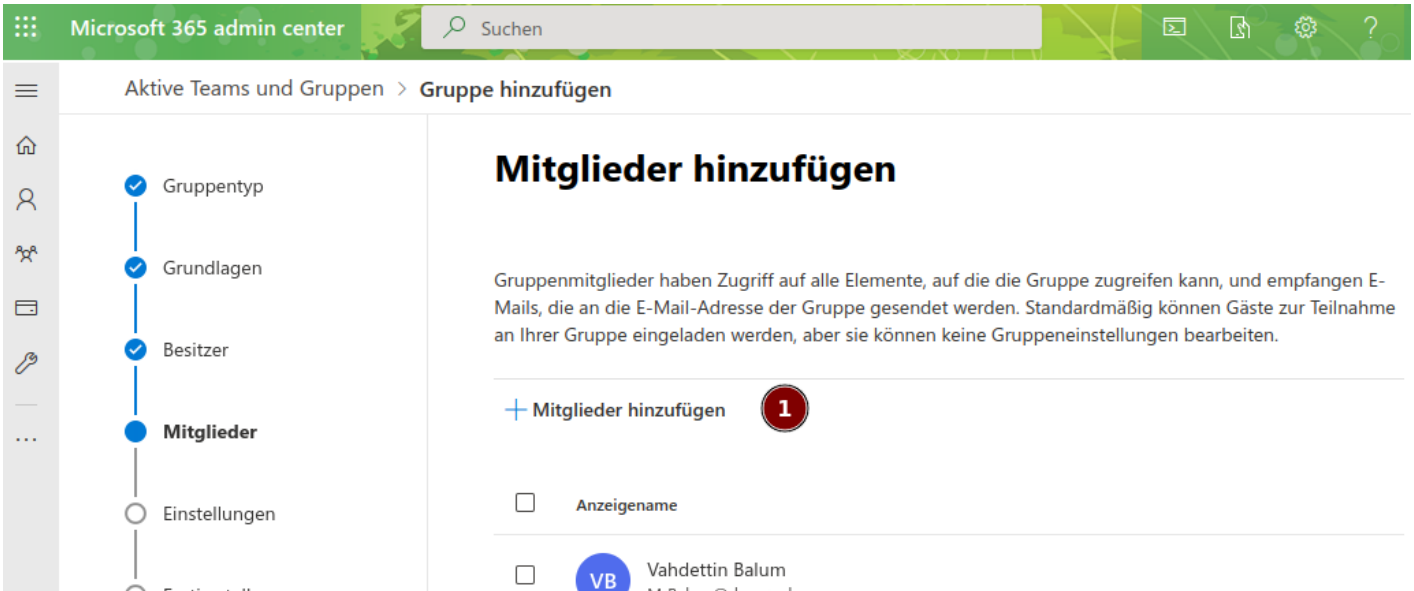
Name und Beschreibung festlegen:



Wähle den Besitzer (Admin-Account):

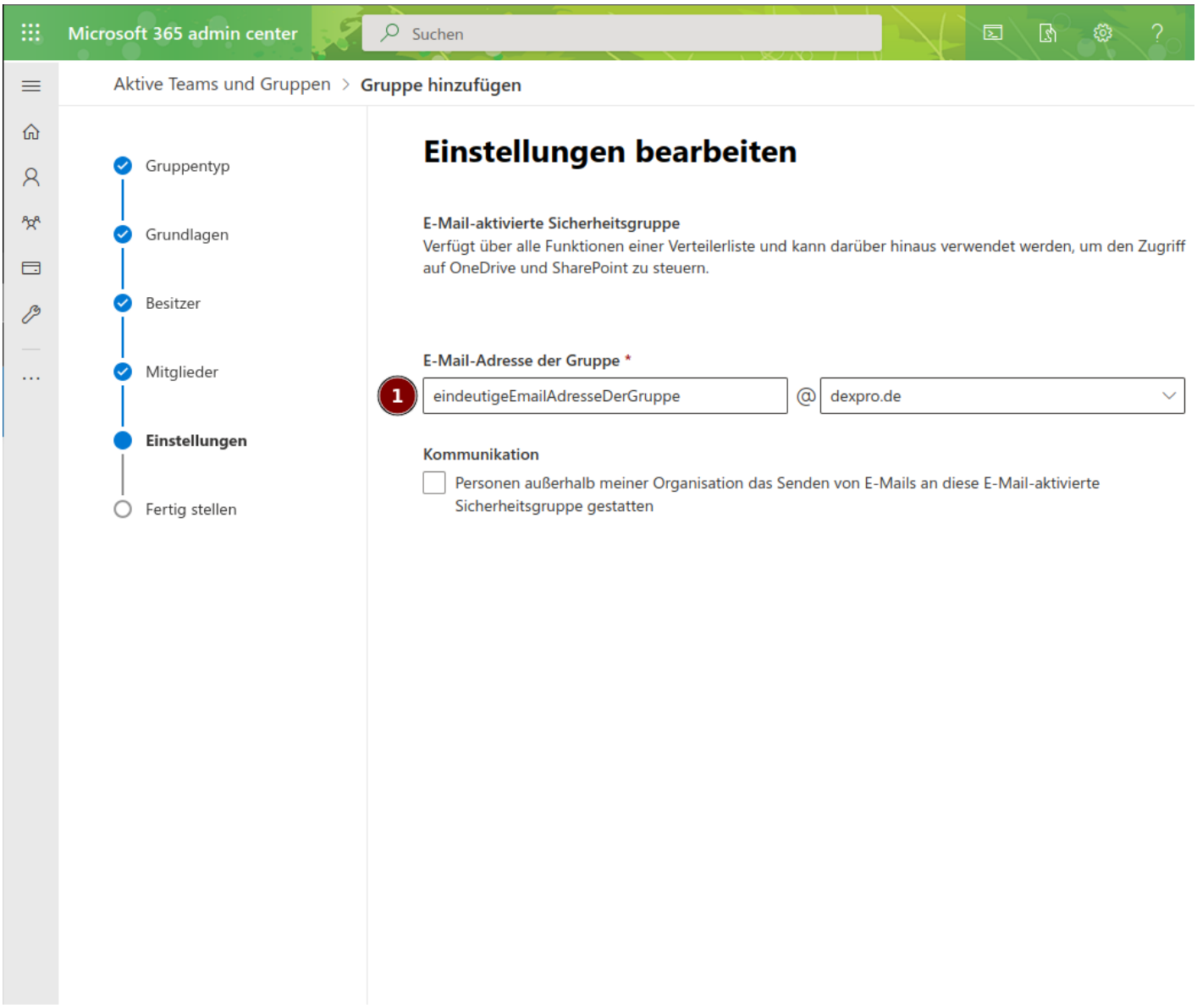


Wähle nun Mitglieder/Email-Accounts die auf die App durch diese Gruppe berechtigt werden soll:



Nun vergeben wir der Gruppe eine eigene Email-Address:

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



Im letzen 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:

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