Exchange Berechtigungen über AD-Gruppen vergeben

1 Grundprinzip (Empfehlung)

Best Practice: Vergib Berechtigungen in Exchange möglichst nicht direkt an einzelne Benutzer, sondern an **AD-Sicherheitsgruppen**.

Vorteile:

- Weniger Fehler (einmal korrekt setzen)
- Einfaches On-/Offboarding (nur Gruppenmitgliedschaft)
- Bessere Auditierbarkeit (wer hat Zugriff? → Gruppenmitgliedschaft)

Typische Exchange-Berechtigungen:

- **Full Access** (Mailbox öffnen, alles lesen/schreiben)
- **Send As** (als die Mailbox senden)
- **Send on Behalf** (im Auftrag von … senden)
- **Ordnerrechte** (Kalender/Inbox/Unterordner)
- (Optional) **Rollen/RBAC** (Admin-/Operator-Rechte)

2 Voraussetzung / Entscheidung: Gruppentyp

2.1 Gruppentypen

- **Security Group (Global/Universal)**: Standard für Berechtigungen im AD.
- **Mail-enabled Security Group**: Security Group, die zusätzlich eine Mailadresse besitzt (wichtig/oft hilfreich bei Exchange).
- **Distribution Group**: Nur Verteiler – i.d.R. nicht für Berechtigungen verwenden.

Empfehlung:

- Für klassische Berechtigungen (Full Access/Ordnerrechte): **Security Group** reicht häufig aus.
- Wenn Exchange/Hybrid/EXO zickt oder du konsistent bleiben willst: **Mail-enabled Security Group**.

2.2 Namensschema (Beispiel)

Nutze ein klares Schema, z.B.:

- ``SG_EX_MB_FullAccess_Info@`` (für Full Access auf Mailbox „info@“)
- ``SG_EX_MB_SendAs_Info@`` (für Send As auf „info@“)
- ``SG_EX_MB_Calendar_Info@_RW`` (für Kalenderrechte)

3 Gruppe anlegen

3.1 AD (GUI)

1. Öffne **Active Directory Users and Computers (dsa.msc)**
2. OU wählen (z.B. ``OU=Exchange,OU=Groups,DC=firma,DC=local``)
3. Rechtsklick → **New** → **Group**
4. Typ: **Security**
5. Scope: **Universal** (in Exchange-Umgebungen meist am kompatibelsten)
6. Name z.B. ``SG_EX_MB_FullAccess_Info``

3.2 Optional: Gruppe mail-enablen (on-prem Exchange)

Falls du on-prem Exchange hast, kannst du die Gruppe mail-enablen:

```
Enable-DistributionGroup -Identity "SG_EX_MB_FullAccess_Info"
```

Hinweis: Der Cmdlet-Name wirkt wie „DistributionGroup“, mail-enabled Security Groups laufen technisch darunter mit.

4 Mitglieder pflegen

1. ADUC → Gruppe öffnen → Tab **Members** → Benutzer hinzufügen
2. oder PowerShell:

```
Add-ADGroupMember -Identity "SG_EX_MB_FullAccess_Info" -Members
"max.mustermann"
```

Tipp: Verwende „Managed By“ und einen klaren Owner/Prozess.

5 Berechtigung setzen (Mailbox Full Access)

5.1 Full Access (Mailbox öffnen)

Beispiel: Gruppe bekommt Full Access auf Mailbox ``info@firma.tld``

```
Add-MailboxPermission -Identity "info" -User "SG_EX_MB_FullAccess_Info" -
AccessRights FullAccess -InheritanceType All
```

Optional (Best Practice): Auto-Mapping verhindern (damit die Mailbox nicht automatisch im Outlook auftaucht):

```
Add-MailboxPermission -Identity "info" -User "SG_EX_MB_FullAccess_Info" -
AccessRights FullAccess -InheritanceType All -AutoMapping:$false
```

5.2 Ergebnis prüfen

```
Get-MailboxPermission -Identity "info" | ? {$_.User -like
"*SG_EX_MB_FullAccess_Info*"}
```

6 Berechtigung setzen (Send As)

Beispiel: Gruppe darf als ``info@firma.tld`` senden

```
Add-ADPermission -Identity "info" -User "SG_EX_MB_SendAs_Info" -
ExtendedRights "Send As"
```

Prüfen:

```
Get-ADPermission -Identity "info" | ? { $_.User -like
"*SG_EX_MB_SendAs_Info*" -and $_.ExtendedRights -like "*Send As*" }
```

Wichtig: „Send As“ kann Replikations-/Caching-Delay haben (AD/Exchange). Plane ggf. 15–60 Minuten ein.

7 Berechtigung setzen (Send on Behalf)

Beispiel: Gruppe darf „im Auftrag von“ senden

```
Set-Mailbox -Identity "info" -GrantSendOnBehalfTo @{Add="SG_EX_MB_SOB_Info"}
```

Prüfen:

```
Get-Mailbox -Identity "info" | select -Expand GrantSendOnBehalfTo
```

8 Ordnerrechte per Gruppe (z.B. Kalender)

Beispiel: Gruppe erhält Editor-Rechte auf den Kalender der Mailbox „info“.

8.1 Kalenderrechte setzen

Deutscher Client kann Ordnernamen anders anzeigen. Technisch heißt der Kalender meistens ``Calendar`` oder sprachabhängig ``Kalender``. Prüfe zuerst den korrekten Pfad:

```
Get-MailboxFolderStatistics -Identity "info" | ? {$_.FolderType -eq
"Calendar"} | select Name,FolderPath
```

Dann Rechte vergeben (Beispiel mit FolderPath):

```
Add-MailboxFolderPermission -Identity "info:\Kalender" -User
"SG_EX_MB_Calendar_Info_RW" -AccessRights Editor
```

Prüfen:

```
Get-MailboxFolderPermission -Identity "info:\Kalender" | ? {$_.User -like
"*SG_EX_MB_Calendar_Info_RW*"}
```

9 Entfernen / Rollback

9.1 Full Access entfernen

```
Remove-MailboxPermission -Identity "info" -User "SG_EX_MB_FullAccess_Info" -
AccessRights FullAccess -InheritanceType All
```

9.2 Send As entfernen

```
Remove-ADPermission -Identity "info" -User "SG_EX_MB_SendAs_Info" -
ExtendedRights "Send As"
```

9.3 Ordnerrecht entfernen

```
Remove-MailboxFolderPermission -Identity "info:\Kalender" -User
"SG_EX_MB_Calendar_Info_RW"
```

10 Troubleshooting / typische Stolpersteine

- **AutoMapping:** FullAccess setzt oft AutoMapping → Mailbox taucht automatisch in Outlook auf. Nutze ``-AutoMapping:$false``.
- **Delays:** „Send As“ wirkt manchmal zeitverzögert (AD/Exchange Cache).
- **Gruppenscope:** In manchen Setups sind **Universal Security Groups** am kompatibelsten.
- **Hybrid/EXO:** Wenn du Exchange Online nutzt, können cmdlets abweichen (EXO v3). Verwende die passenden EXO-Cmdlets und prüfe, ob Gruppen sauber synchronisiert sind.
- **Nested Groups:** Verschachtelte Gruppen funktionieren nicht überall gleich zuverlässig (je nach Berechtigungstyp). Wenn es klemmt: direkte Mitgliedschaft bevorzugen.

11 Komplettbeispiel (End-to-End)

Ziel: Max und Erika sollen die Mailbox ``info@firma.tld`` öffnen und als ``info@`` senden können.

1. Gruppen:
    - ``SG_EX_MB_FullAccess_Info``

- ``SG_EX_MB_SendAs_Info``

1. Mitglieder:
   - ``max.mustermann``
   - ``erika.mustermann``

Commands:

```
Add-ADGroupMember -Identity "SG_EX_MB_FullAccess_Info" -Members
"max.mustermann","erika.mustermann"
Add-ADGroupMember -Identity "SG_EX_MB_SendAs_Info" -Members
"max.mustermann","erika.mustermann"

Add-MailboxPermission -Identity "info" -User "SG_EX_MB_FullAccess_Info" -
AccessRights FullAccess -InheritanceType All -AutoMapping:$false
Add-ADPermission -Identity "info" -User "SG_EX_MB_SendAs_Info" -
ExtendedRights "Send As"
```

Prüfen:

```
Get-MailboxPermission -Identity "info" | ? {$_.User -like
"*SG_EX_MB_FullAccess_Info*"}
Get-ADPermission -Identity "info" | ? { $_.User -like
"*SG_EX_MB_SendAs_Info*" -and $_.ExtendedRights -like "*Send As*" }
```

Kurze Rückfrage (damit ich es 100% passend mache)

Arbeitest du mit Exchange on-prem, Exchange Online, oder Hybrid? Dann kann ich dir die Anleitung auf deine Variante zuschneiden (z. B. EXO-Cmdlets, AAD-Sync, RBAC, Besonderheiten bei „Send As“).