

# Exchange Server Hybrid Updates

Tech Talk – 26

Dedizierte Exchange Hybrid App – Teil 2



# Exchange Server Hybrid

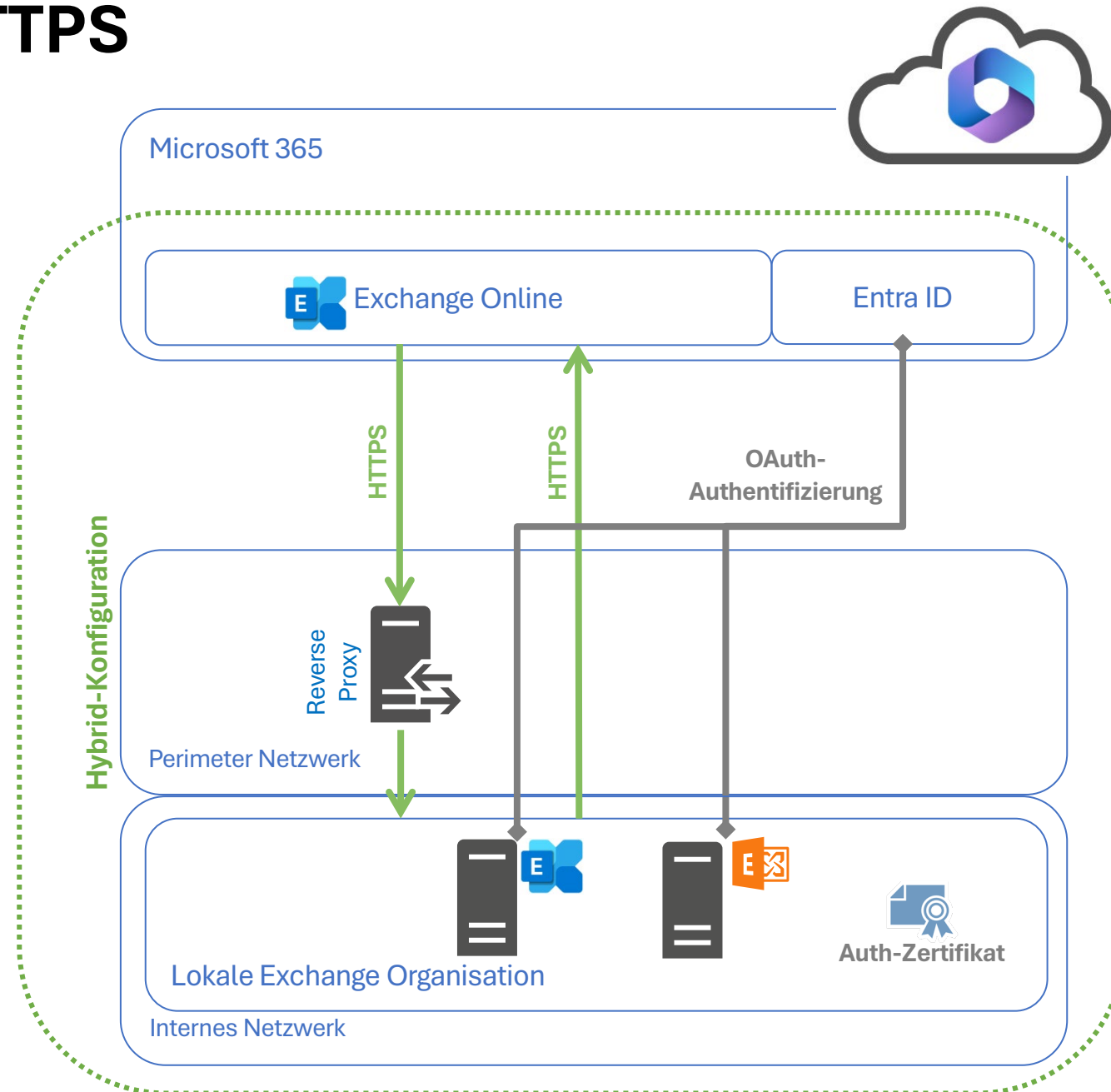
# Exchange Server April 2025 HU

## Hotfix-Update (HU)

- Das **April 2025 HU** ist **kein Sicherheitsupdate** und damit ein optionales Update
  - Das HU enthält **neue Funktionen** für den Hybrid-Betrieb von Exchange Server mit Exchange Online
  - Vorbereitung für die **Abschaltung der Exchange Web Services** in Exchange Online im **Oktober 2026**
  - **Umstellung** vom **generischen geteilten Dienstkonto** (*Shared Service Principal*) der Exchange Online Unternehmensapplikation für alle Mandanten auf eine dedizierte **Entra-Unternehmensapplikation je Mandant**
- Die Funktionen des HU sind im Mai 2025 HU und in Exchange Server SE enthalten

# Exchange Server Hybrid – HTTPS

- Hybrid Configuration Wizard richtet die Hybrid-Konfiguration ein
- Logische Verknüpfung von zwei physisch getrennten Exchange Organisationen
- Besondere Vertrauensstellung für den Austausch und die Abfrage von Informationen
- OAuth-Authentifizierung mit Hilfe des Exchange Auth-Zertifikates



# Exchange Online Unternehmensanwendung

- Exchange Online ist als Unternehmensanwendung mit einer generischen AppID in jedem Mandanten vorhanden
  - Name: **Office 365 Exchange Online**
  - ID: **00000002-0000-0ff1-ce00-000000000000**

The diagram at the top shows a cloud icon with the Microsoft 365 logo. Below it, a box labeled 'Microsoft 365' contains two sub-boxes: 'Exchange Online' (with the Exchange logo) and 'Entra ID' (with a placeholder icon). A blue arrow points from the 'Entra ID' box to the screenshot below.

The screenshot shows the 'Microsoft Entra Admin Center' interface. The breadcrumb trail is: Home > Unternehmensanwendungen | Alle Anwendungen > App-Registrierungen > Unternehmensanwendungen. The page title is 'Unternehmensanwendungen | Alle Anwendungen'. The left sidebar shows the 'Verwalten' section with 'Alle Anwendungen' selected. The main content area shows a search bar with the filter 'Anwendungs... beginnt mit 00000002-0000-0ff1-ce00-00000000...' and a table with one application found.

Name	Objekt-ID	Anwendungs-ID
Office 365 Exchange Online	abdc4b6b-3e86-4952-89f1-d7d24de4e0a0	00000002-0000-0ff1-ce00-000000000000

# Exchange Online Unternehmensanwendung

- Exchange Online ist als Unternehmensanwendung mit einer generischen AppID in jedem Mandanten vorhanden
  - Name: **Office 365 Exchange Online**
  - ID: **00000002-0000-0ff1-ce00-000000000000**

The diagram at the top shows a cloud icon with the Microsoft 365 logo. Below it, a box labeled "Microsoft 365" contains two sub-boxes: "Exchange Online" (with the Exchange logo) and "Entra ID" (with the Entra ID logo). A blue arrow points from the "Entra ID" box to the screenshot below.

The screenshot shows the Microsoft Entra Admin Center interface. The breadcrumb navigation is: Home > Unternehmensanwendungen | Alle Anwendungen > App-Registrierungen > Unternehmensanwendungen. The page title is "Unternehmensanwendungen | Alle Anwendungen". The left sidebar shows the "Verwalten" section with "Alle Anwendungen" selected. The main content area shows a list of applications. One application is found: "Office 365 Exchange Online". The application details are shown in a table with columns "Name", "Objekt-ID", and "Anwendungs-ID". The "Name" is "Office 365 Exchange Online", the "Objekt-ID" is "abdc4b6b-3e86-4952-89f1-d7d24de4e0a0", and the "Anwendungs-ID" is "00000002-0000-0ff1-ce00-000000000000". A blue arrow points from the "Anwendungs-ID" in the table to the PowerShell command below.

The PowerShell command in the terminal window is:

```
PS C:\SCRIPTS> $ServiceName = "00000002-0000-0ff1-ce00-000000000000"
PS C:\SCRIPTS> $p = Get-MgServicePrincipal -Filter 'AppId eq $ServiceName'
PS C:\SCRIPTS> $p.ServicePrincipalNames
https://mail.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/mail.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/autodiscover.egxde.mail.onmicrosoft.com
00000002-0000-0ff1-ce00-000000000000/egxde.mail.onmicrosoft.com
00000002-0000-0ff1-ce00-000000000000/autodiscover.groups.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/groups.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/autodiscover.varunagroup.com
00000002-0000-0ff1-ce00-000000000000/varunagroup.com
00000002-0000-0ff1-ce00-000000000000/autodiscover.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/varunagroup.de
https://outlook.office.com
https://outlook-tdf-2.office.com/
https://ps.outlook.com
00000002-0000-0ff1-ce00-000000000000/outlook.office365.com
00000002-0000-0ff1-ce00-000000000000/mail.office365.com
00000002-0000-0ff1-ce00-000000000000/outlook.com
00000002-0000-0ff1-ce00-000000000000/*.outlook.com
```



# Exchange Online Unternehmensanwendung



Microsoft 365



Exchange Online



Entra ID

- Exchange Online ist als Unternehmens-anwendung mit einer generischen AppID in jedem Mandanten vorhanden
    - Name: **Office 365 Exchange Online**
    - ID: **00000002-0000-0ff1-ce00-000000000000**
  - Als Teil der OAuth-Konfiguration werden die **URLs** der virtuellen Exchange Verzeichnisse als **Service Principal Namen** hinzugefügt
  - **Exchange Server Auth-Zertifikat** wird hinzugefügt
  - Dies bestimmt, für welche Namen ein OAuth-Authentifizierungstoken gültig ist
- Eine generische Unternehmensanwendung für alle Microsoft 365 Mandanten
- Shared Service Principal

```
Administrator: C:\Program Files\PowerShell\7\pwsh.exe
PS C:\SCRIPTS> $ServiceName = "00000002-0000-0ff1-ce00-000000000000"
PS C:\SCRIPTS> $sp = Get-MgServicePrincipal -Filter "AppId eq '$ServiceName'"
PS C:\SCRIPTS> $sp.ServicePrincipalNames
https://mail.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/mail.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/autodiscover.egxde.mail.onmicrosoft.com
00000002-0000-0ff1-ce00-000000000000/egxde.mail.onmicrosoft.com
00000002-0000-0ff1-ce00-000000000000/autodiscover.groups.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/groups.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/autodiscover.varunagroup.com
00000002-0000-0ff1-ce00-000000000000/varunagroup.com
00000002-0000-0ff1-ce00-000000000000/autodiscover.varunagroup.de
00000002-0000-0ff1-ce00-000000000000/varunagroup.de
https://outlook.office.com
https://outlook-tdf-2.office.com/
https://ps.outlook.com
00000002-0000-0ff1-ce00-000000000000/outlook.office365.com
00000002-0000-0ff1-ce00-000000000000/mail.office365.com
00000002-0000-0ff1-ce00-000000000000/outlook.com
00000002-0000-0ff1-ce00-000000000000/*.outlook.com
00000002-0000-0ff1-ce00-000000000000
https://ps.compliance.protection.outlook.com
https://autodiscover-s.office365.us/
https://outlook.office365.us/
https://outlook-sdf.office.com/
https://outlook-sdf.office365.com/
https://outlook.office365.com:443/
https://outlook.office.com/
https://outlook.office365.com/
https://outlook.com/
https://outlook-dod.office365.us/
https://ps.protection.outlook.com/
https://webmail.apps.mil/
https://outlook-tdf.office.com/
PS C:\SCRIPTS>
```



Auth-Zertifikat

# Voraussetzungen

- Aktives und gültiges Exchange Auth Certificate
  - Laufzeit prüfen und ggf. vor der Einrichtung der Hybrid-App verlängern
  - PowerShell-Skript: MonitorExchangeAuthCertificate.ps1
- Berechtigungen On-Premises
  - View-Only Configuration und Organization Client Access und Organization Configuration
  - Organisation Management
- Berechtigungen Microsoft 365
  - Application Administrator
  - Globaler Administrator
- Exchange Server mit Postfach-Rolle und installiertem HU April 2025
  - Exchange Server SE RTM (15.2.2562.17)
  - Exchange Server 2019 CU15 + HU April 2025 (15.2.1748.24)
  - Exchange Server 2019 CU14 + HU April 2025 (15.2.1544.25)
  - Exchange Server 2016 CU23 + HU April 2025 (15.1.2507.55)



# PowerShell-Skript

- Automatische Prüfung auf eine neuere Version
- Ausführung in einer PowerShell-Session mit administrativer Berechtigung (Elevated Prompt)
- Rundum glücklich Aktivierung

```
# Vollautomatische Einrichtung und Aktivierung der Hybrid-Applikation  
.\ConfigureExchangeHybridApplication.ps1 -FullyConfigureExchangeHybridApplication
```

# Einrichtung mit getrennten Berechtigungen 1/2

- Einrichtung der Unternehmensapplikation durch das Entra Team
  - Manueller Export des Exchange Auth-Zertifikates und Bereitstellung der .cer-Datei → [Link](#)

# Einrichtung der Hybrid-Applikation in Entra

```
.\ConfigureExchangeHybridApplication.ps1 '  
    -CreateApplication '  
    -UpdateCertificate '  
    -CertificateMethod "File" '  
    -CertificateInformation "C:\AuthCertExport\certificate.cer"
```

- Nach der Einrichtung der Applikation benötigt das Exchange Team für die spätere Aktivierung der Hybrid-App folgende Informationen
  - App-ID
  - Tenant-ID
  - Remote Routing Domäne

# Einrichtung mit getrennten Berechtigungen 2/2

- Konfiguration Einrichtung der Nutzung der dedizierten Hybrid-App On-Premises
  - Keine Prüfung der eingerichteten Entra-Unternehmensapplikation


# Einrichtung der Hybrid-Applikation in Entra

```
.\ConfigureExchangeHybridApplication.ps1 '  
-ConfigureAuthServer '  
-EnableExchangeHybridApplicationOverride '  
-CustomAppId bdc1c8e0-4b34-40a4-8555-061c14e46349 '  
-TenantId f3a1d24b-d8e4-4efd-8df1-6483535b9c63 '  
-RemoteRoutingDomain varunagroup.mail.onmicrosoft.com
```



**Demo**

# Zugriffsprüfung

 **ExchangeServerApp-** Unternehmensanwendung | **Anmeldeprotokolle** ...

» [Herunterladen](#) ▾ [Dateneinstellungen exportieren](#) [Problembehandlung](#) [Aktualisieren](#) | [Haben Sie Feedback?](#)

[Filter hinzufügen](#) [Datumswerte anzeigen als: UTC](#) [Datumsbereich: Letzte 24 Stunden](#) [Zeitaggregat: 24 Stunden](#) ["Anwendung" enthält](#) [Filter zurücksetzen](#)

[Benutzeranmeldungen \(interaktiv\)](#) [Benutzeranmeldungen \(nicht interaktiv\)](#) [Dienstprinzipalanmeldungen](#) [Anmeldungen für verwaltete Identitäten](#)

ID	Dienstprinzipalname	Status	Mandantenüberg...	Basismandanten-...	Ressourcenmand...	IP-Adresse	Ressource	Ressourcen-ID	Bedingter Zugriff	Anzahl von Anmeldungen
·46c9-8ea...	ExchangeServerApp-...	Erfolg	Keine				Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000	Nicht angewendet	4
·46c9-8ea...	ExchangeServerApp-...	Erfolg	Keine				Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000	Nicht angewendet	1
·46c9-8ea...	ExchangeServerApp-...	Erfolg	Keine				Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000	Nicht angewendet	1
·46c9-8ea...	ExchangeServerApp-...	Erfolg	Keine				Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000	Nicht angewendet	1
·46c9-8ea...	ExchangeServerApp-...	Erfolg	Keine				Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000	Nicht angewendet	1
·46c9-8ea...	ExchangeServerApp-...	Erfolg	Keine				Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000	Nicht angewendet	84

# Zusammenfassung

- Die Einrichtung der dedizierten Unternehmensanwendung ist einfach
- Im Regelfall treten keine Probleme auf
  - Selbst in einer komplexen Umgebung mit ausgehenden https-Verbindungen via Proxy-Server gab es keine Probleme
- Die Dokumentation des PowerShell-Skriptes auf der Microsoft Exchange Server Support Scripts-Seite enthält bereits Kommandos für die kommende MS Graph Integration

# Optional oder nicht?

## Umstellung

- Die Umstellung ist, für eine **vollwertige Hybridstellung**, sog. *Rich Coexistence*, **verpflichtend**
  - **Frei-/Gebuchzeiten, Mail-Tipps, Profilbilder**, etc.
- **Ohne vollwertige Hybridstellung** sollte die "alte" Exchange-Unternehmensapplikation bereinigt werden
  - `ConfigureExchangeHybridApplication.ps1` → Service Principal Clean-Up Mode

# Bereinigung des 1st-Party Service Principals

```
.\ConfigureExchangeHybridApplication.ps1 '  
-ResetFirstPartyServicePrincipalKeyCredentials
```





# Thomas Stensitzki

Experte

Granikos GmbH & Co. KG

MVP | M365 + Exchange

MCT Community Lead

<https://linktr.ee/stensitzki>



Thomas' Tech Talk wird produziert mit [Camtasia](#)

