

Exchange Summit 2026

Würzburg

IAM and Exchange: Frenemies in Hybrid organizations

Dave Stork



#MSEExchangeSummit

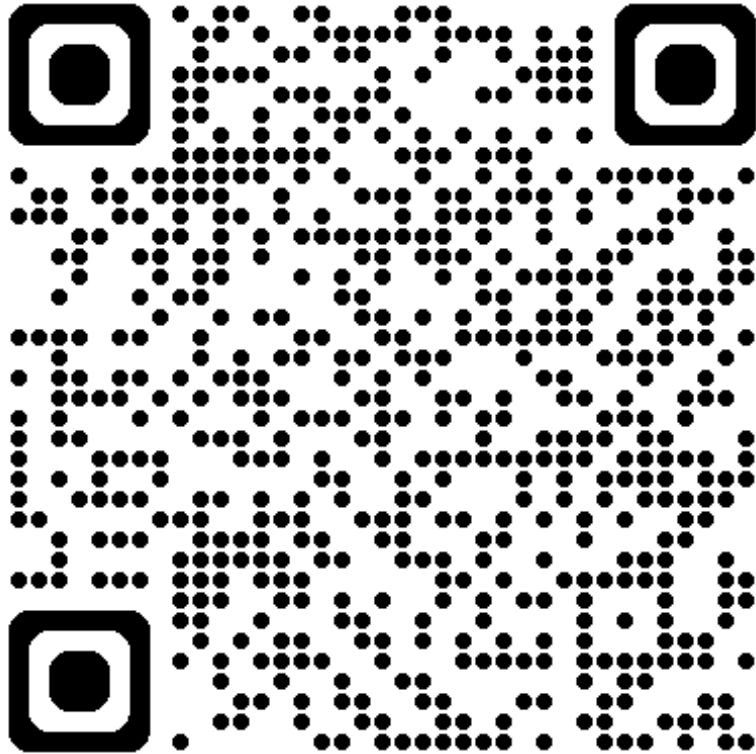
Vielen Dank unseren Eventpartnern!



**Exchange
Summit
2026**

**Exchange Server
&
Exchange Online**

#MSEExchangeSummit



Kind request: follow me on LinkedIn!



#MSEExchangeSummit

Agenda

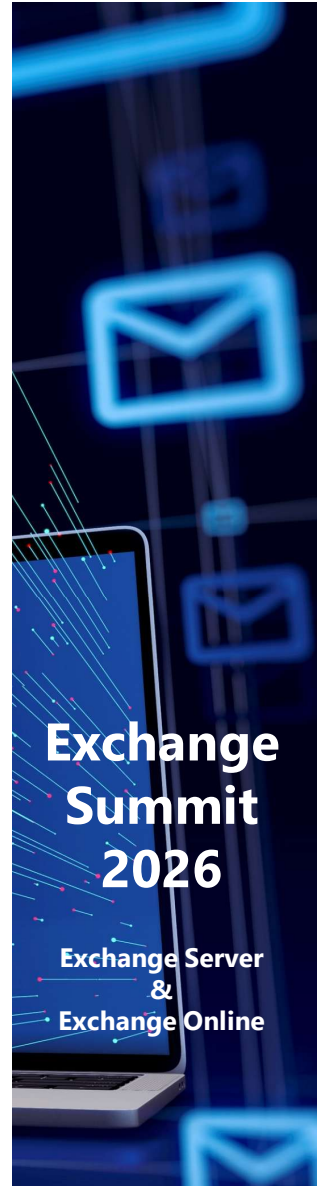
- Why this session?
- Provisioning in Entra hybrid organizations
- The impact of the MX record on IAM
- Exchange Object management
- Start-of-Authority and changing this



**Exchange
Summit
2026**

Exchange Server
&
Exchange Online

Why this session?



#MSExchangeSummit

Some terminology

- Hybrid user: has object in Active Directory and is synced to Microsoft 365
- Directory synchronisation: the process of syncing an object and it's attributes from one location to another
 - Entra Connect
 - Entra Cloud Sync agent
- User, groups, contacts can be hybrid
- Mailbox location: Either on-premises or Exchange Online.
- Mailbox or mail enabled: object has mailbox or has mail attributes



Provisioning user objects

#MSExchangeSummit



Provisioning in Hybrid orgs

- You need to provision in Active Directory (AD) and sync
- Provision object with mailbox
 - Enable-RemoteMailbox
- Assign license to user
- Alternative: create on-prem or cloud-only objects
- Note: Entra Provisioning API can only be used by IGA systems such as Workday



Provisioning in Cloud only orgs

- Create object directly in Entra
- Assign user Exchange License or mail-enable



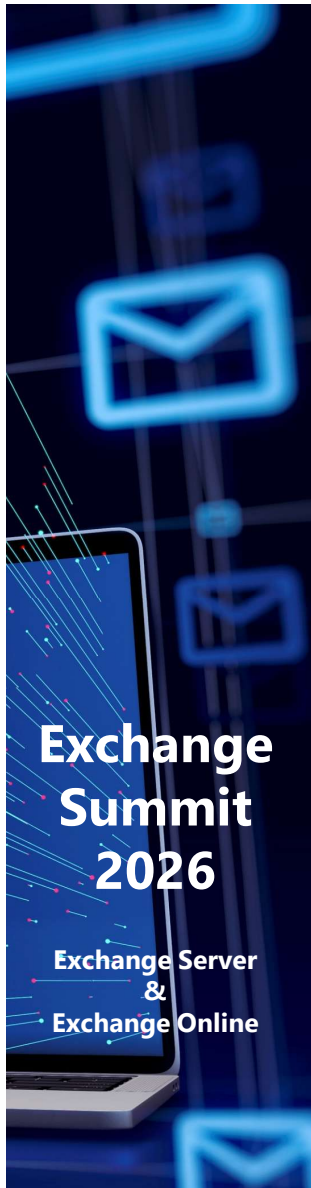
Provisioning in On-prem only

- Provision in AD with no sync required
- Mailbox or Mail enable in Exchange Server



The impact of the MX record on IAM

#MSExchangeSummit



The MX record

- Is the ingress point of mail for a specific domain
- The specific recipient(s) that is (are) addressed need to exist or be accepted
- Recipient filtering can filter unknown addresses and reject mail
- Mail might require transport to other systems
 - On-prem to Online
 - Other mail system



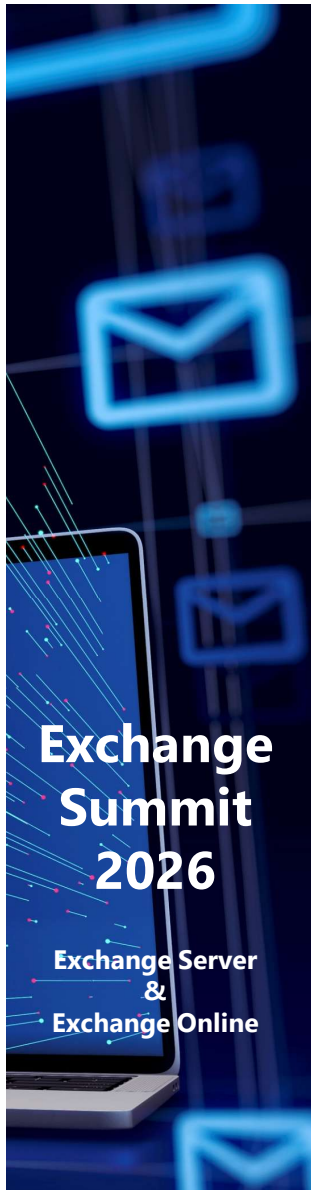
The MX record

- For hybrid objects the MX can be pointed to either on-premises or Exchange Online
 - If hybrid mailflow is setup correctly and object has correct targetaddresses
 - Requires Exchange Server when pointed to on-premises
- If you have cloud-only mail(box) enabled objects, the MX record must be pointed to Exchange Online
- On-prem only mailboxes require the MX pointed towards on-prem



Exchange Object management

#MSExchangeSummit

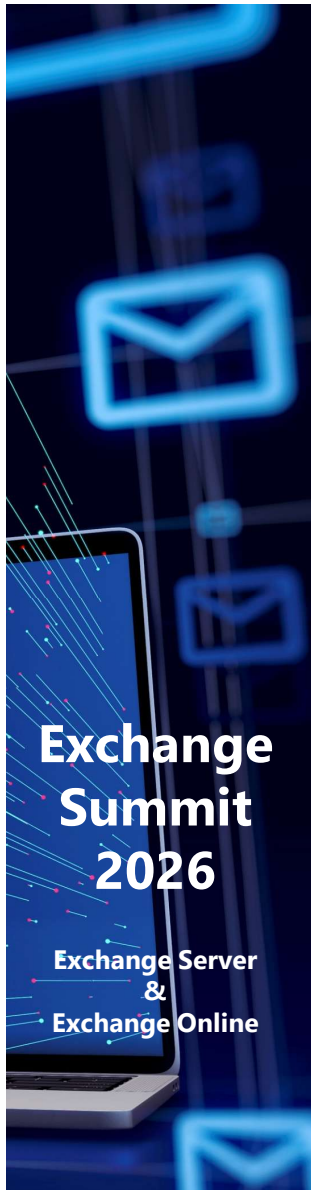


Exchange Object Management

- An Exchange Server was traditionally a requirement in Hybrid
 - LES = Last Exchange Server
- The Serverless Management option
 - No Exchange Server required (delete, NOT remove via Setup)
 - PowerShell, but not Remote PowerShell
 - No audit logging or RBAC
 - Scott says NO!
- The new SOA options
 - Start of Authority of Exchange attributes, Groups, Contacts and User objects



Start-of-Authority and changing this



**Exchange
Summit
2026**

Exchange Server
&
Exchange Online

#MSExchangeSummit

Start of Authority

- What is the Start-of-Authority
- Why is it important
- Now you can change it, what are your options?
- Hybrid user => isExchangeCloudManaged
- Groups \ Contacts \ User => isCloudManaged
- Both possible with Entra Connect and Entra Cloud Sync



**Exchange
Summit
2026**

Exchange Server
&
Exchange Online

Start of Authority Exchange Attributes

- ONLY Exchange Attributes become writeable in Exchange Online
 - Microsoft listed which attributes are affected
- In Exchange Online PowerShell
 - Set-Mailbox -isExchangeCloudManaged \$True
- Exchange Online mailbox has to be provisioned
- Currently no write-back
 - This will be Phase 2
 - only with Cloud Sync, not Entra Connect
 - Important depending on your MX record!



Start of Authority Exchange Attributes

Adding a mailaddress in Exchange Online:

Before:

✗ Email address type update failed

Error:

Error executing request. The operation on mailbox "Test_a985e4351c" failed because it's out of the current user's write scope. The action 'Set-Mailbox', 'EmailAddresses', can't be performed on the object 'Test_a985e4351c' because the object is being synchronized from your on-premises organization. This action should be performed on the object in your on-premises organization.

After:

✓ Email addresses have been updated

**Exchange
Summit
2026**

Exchange Server
&
Exchange Online

Start of Authority Groups

Similar principle for users and contacts

- Via MS Graph: isCloudManaged
- Basically decouples on-premises and cloud object
 - Remove the on-prem object to prevent confusion
 - Connect-MgGraph -Scopes 'Group.ReadWrite.All', 'Group-OnPremisesSyncBehavior.ReadWrite.All'
 - Get-MgGroup -> \$groupId
 - \$body = @{ isCloudManaged = \$true }
 - \$uri =
"https://graph.microsoft.com/v1.0/groups/\$groupId/onPremisesSyncBehavior"
 - Invoke-MgGraphRequest -Uri \$uri -Method PATCH -Body (\$body | ConvertTo-Json) -ContentType "application/json"



Start of Authority Groups

Before:

DatabaseBeheerders	:	DatabaseBeheerders@		📧
Functioneel behee	:	Functioneelbeheer		📧
ictbeheer	:	ictbeheer@		☁
incidentbeheer	:	incidentbeheer@		📧
Indexeerteam MBT Deelnemers	:	IndexeerteamMBTDeelnemers@		📧

After:

DatabaseBeheerders	:	DatabaseBeheerders@		☁
Functioneel behee	:	Functioneelbeheer		☁
ictbeheer	:	ictbeheer@		☁
incidentbeheer	:	incidentbeheer@		☁
Indexeerteam MBT Deelnemers	:	IndexeerteamMBTDeelnemers@		☁

Exchange
Summit
2026

Exchange Server
&
Exchange Online

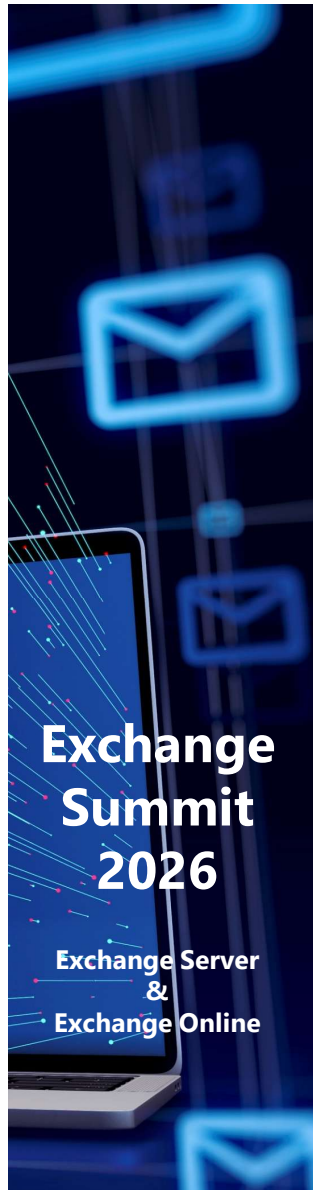
The impact of SoA changes

- IMHO Feasible option for Exchange Object Management
 - Better option than Serverless
 - Auditing
 - Automation Exchange properties
- Granular phase-out of on-prem AD
 - Previously all or nothing
- Changes IAM possibilities
 - Take note of the status of write-back for attributes!
- Reduced attack surface
 - Only user accounts that really need AD authentication are hybrid



In conclusion

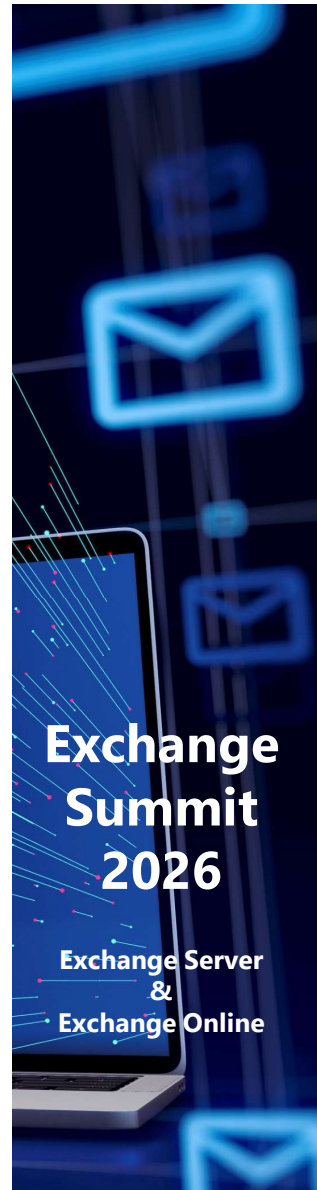
#MSEExchangeSummit



What is important?



- ... who wins: IAM or Exchange? Or you?



Resources

Download-Links

- [Cloud-based management of Exchange attributes for Remote Mailboxes in hybrid environments](#)
- [Cloud-First identity management: Guidance for IT architects](#)
- [Configure user Source of Authority \(SOA\)](#)
- [Configure Group Source of Authority \(SOA\)](#)
- [Migrate from Microsoft Entra Connect to Cloud Sync: Decision Guide](#)



Exchange Summit 2026

Würzburg



#MSEExchangeSummit