Entra ID Source of Authority Conversion

Empower IGA features and modernize your Identity Platform

Pim Jacobs

Principal Consultant @ InSpark &
Microsoft Security MVP

- Focus on the full Microsoft Entra portfolio
- One of the founders of the **Dutch Microsoft Entra Community**,
- Blog: **identity-man.eu**
- Skiing | Soccer | F1 | Time with the kids

Microsoft® Most Valuable Professional

Agenda

- Understanding Source of Authority Conversion in Entra ID
- Source of Authority Conversion for Exchange Attributes
- Source of Authority Conversion for Groups in Entra ID
- Source of Authority Conversion for Users to Entra ID
- Best Practices and Considerations for Source of Authority Transfer

Understanding Source of Authority Transfer in Entra ID

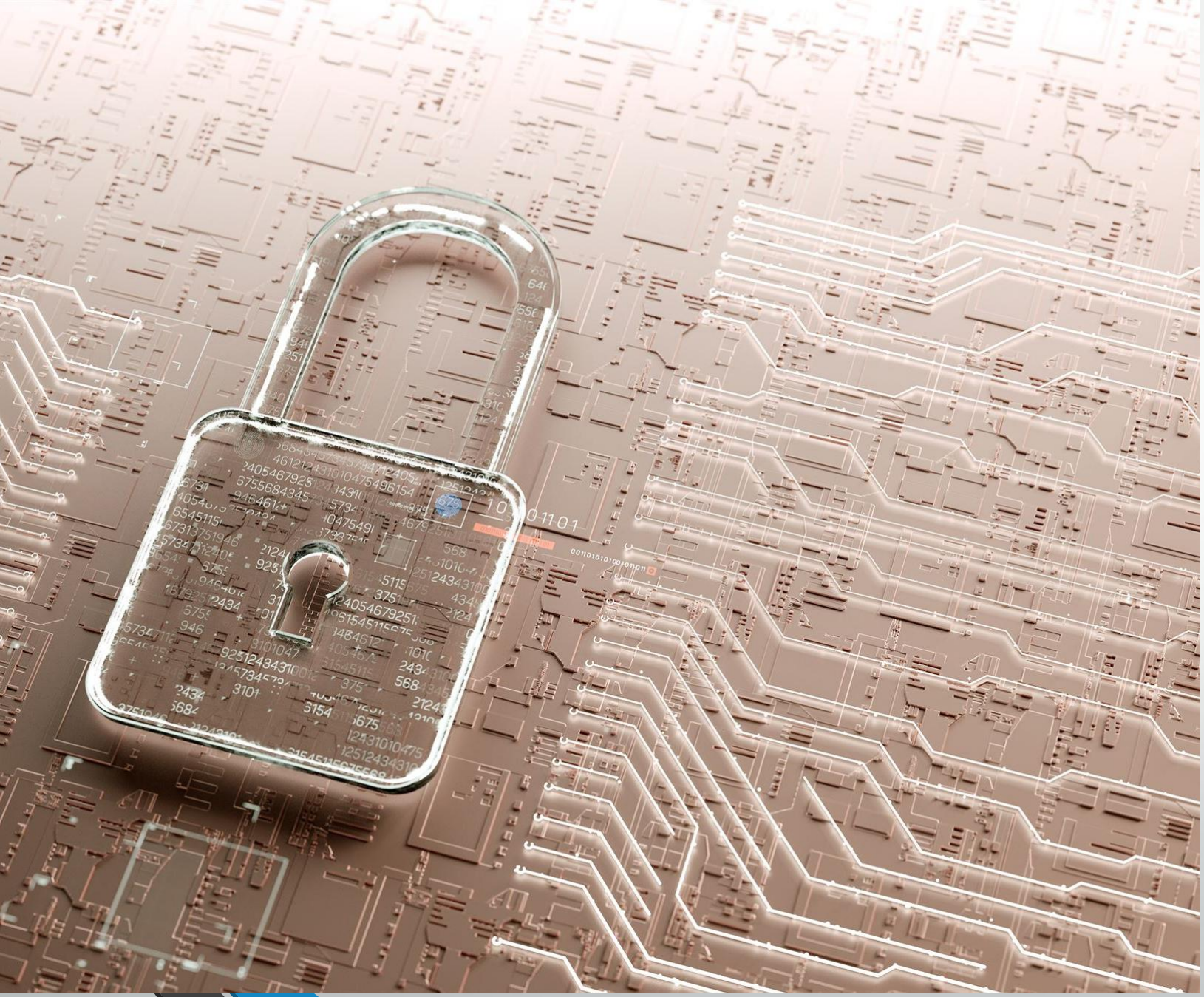
DEFINITION OF SOURCE OF AUTHORITY AND ITS SIGNIFICANCE

Source of Authority Defined

The source of authority manages identity data and attributes within a system securely and reliably, within Entra ID there is just one source of truth for synchronized values.

Importance of Transferring Source

Transferring the source for users, groups or attributes, enhances security and enables cloud functionality to be enabled on those objects.



WHY SOURCE OF AUTHORITY TRANSFER IS ESSENTIAL FOR MODERN IDENTITY PLATFORMS

Need to port cloud capabilities to Active Directory

Applying Security Enhancements

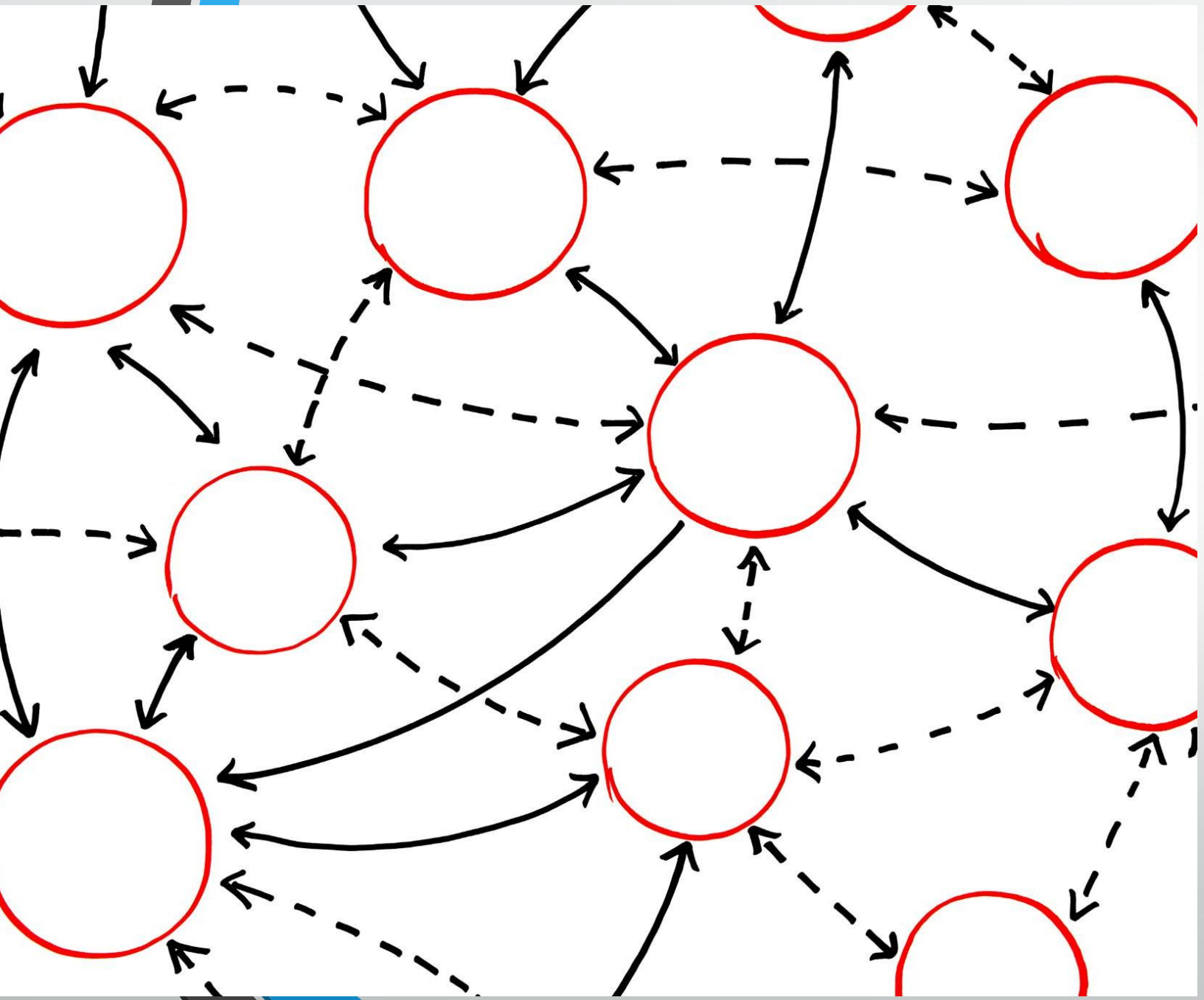
Streamlined Management

Source of Authority Conversion for Exchange Attributes

BENEFITS OF CONVERTING EXCHANGE ATTRIBUTES TO ENTRA ID AUTHORITY

Simplify & enhanced management from one single platform

Improved security posture by getting rid of Exchange on-premises and therefore vulnerabilities



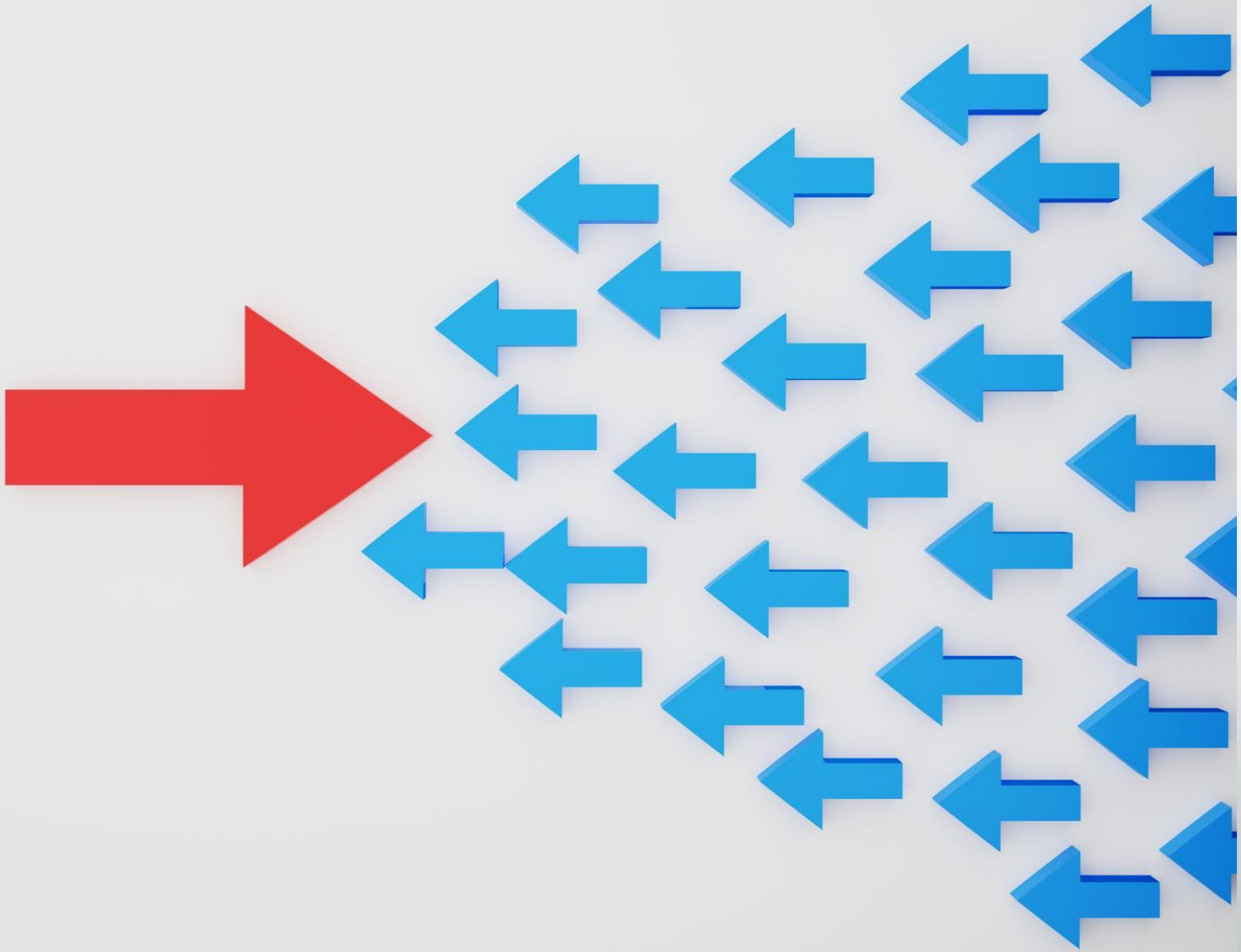
PROCESS FOR CONVERTING EXCHANGE-RELATED ATTRIBUTES

All mailboxes migrated

Convert Exchange (hybrid) only attributes on mailbox object level

Change inbound provisioning process (if any)

Inform support teams



PROCESS SEQUENCE FOR EXCHANGE ATTRIBUTE SOA CONVERSION

Convert distribution groups first

- Recreate distribution list in Exchange Online (M365 groups preferred).
- Convert distribution list to mail enabled security groups and transfer SOA.

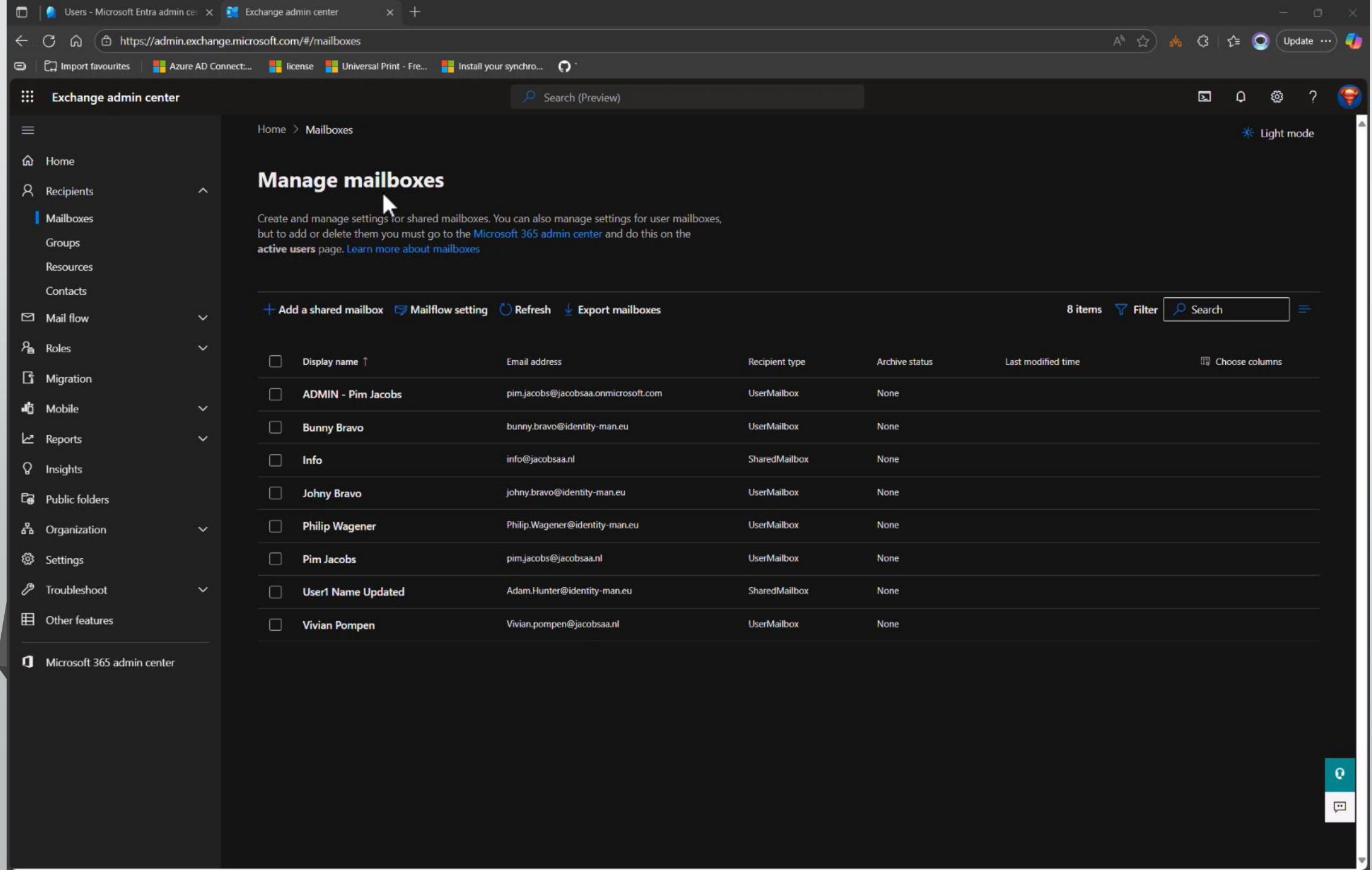
Convert SOA for mailbox exchange attributes

Decommission Exchange Hybrid

Future: Enabled write-back capabilities to update attributes in Active Directory

LIMITATIONS & CONSIDERATIONS

- Not supported with Connect Cloud Sync today
- Only for mailboxes
- Per-mailbox setting
- No write-back support yet
- Possibly requires a different relaying setup


Users - Microsoft Entra admin ce
Exchange admin center
https://admin.exchange.microsoft.com/#/mailboxes
Update
Import favourites
Azure AD Connect:...
license
Universal Print - Fre...
Install your synchro...
Exchange admin center
Search (Preview)
Home
Recipients
Mailboxes
Groups
Resources
Contacts
Mail flow
Roles
Migration
Mobile
Reports
Insights
Public folders
Organization
Settings
Troubleshoot
Other features
Microsoft 365 admin center
Home > Mailboxes
Light mode
Manage mailboxes
Create and manage settings for shared mailboxes. You can also manage settings for user mailboxes, but to add or delete them you must go to the Microsoft 365 admin center and do this on the active users page. Learn more about mailboxes
Add a shared mailbox
Mailflow setting
Refresh
Export mailboxes
8 items
Filter
Search
Display name
Email address
Recipient type
Archive status
Last modified time
Choose columns
ADMIN - Pim Jacobs pim.jacobs@jacobsaa.onmicrosoft.com UserMailbox None
Bunny Bravo bunny.bravo@identity-man.eu UserMailbox None
Info info@jacobsaa.nl SharedMailbox None
Johny Bravo johny.bravo@identity-man.eu UserMailbox None
Philip Wagener Philip.Wagener@identity-man.eu UserMailbox None
Pim Jacobs pim.jacobs@jacobsaa.nl UserMailbox None
User1 Name Updated Adam.Hunter@identity-man.eu SharedMailbox None
Vivian Pompen Vivian.pompen@jacobsaa.nl UserMailbox None

DEMO #1

Source of Authority Conversion for Groups in Entra ID

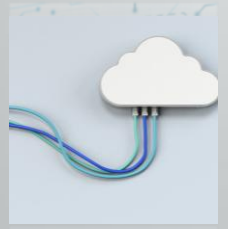
Added value of moving group authority to Entra ID

Centralised Control

Moving group authority to Entra ID enables organisations to manage access and permissions from a single platform.

Enhanced Security Policies

Transfer improves enforcement of robust security policies across user groups in Entra ID like Entitlement Management, My Groups, etc..



Empowers Active Directory with cloud services

With write-back capabilities Active Directory makes use of the intelligence from Entra ID, facilitating better and simplified resource access.

PREREQUISITES FOR GROUP SOA CONVERSION

Data Preparation

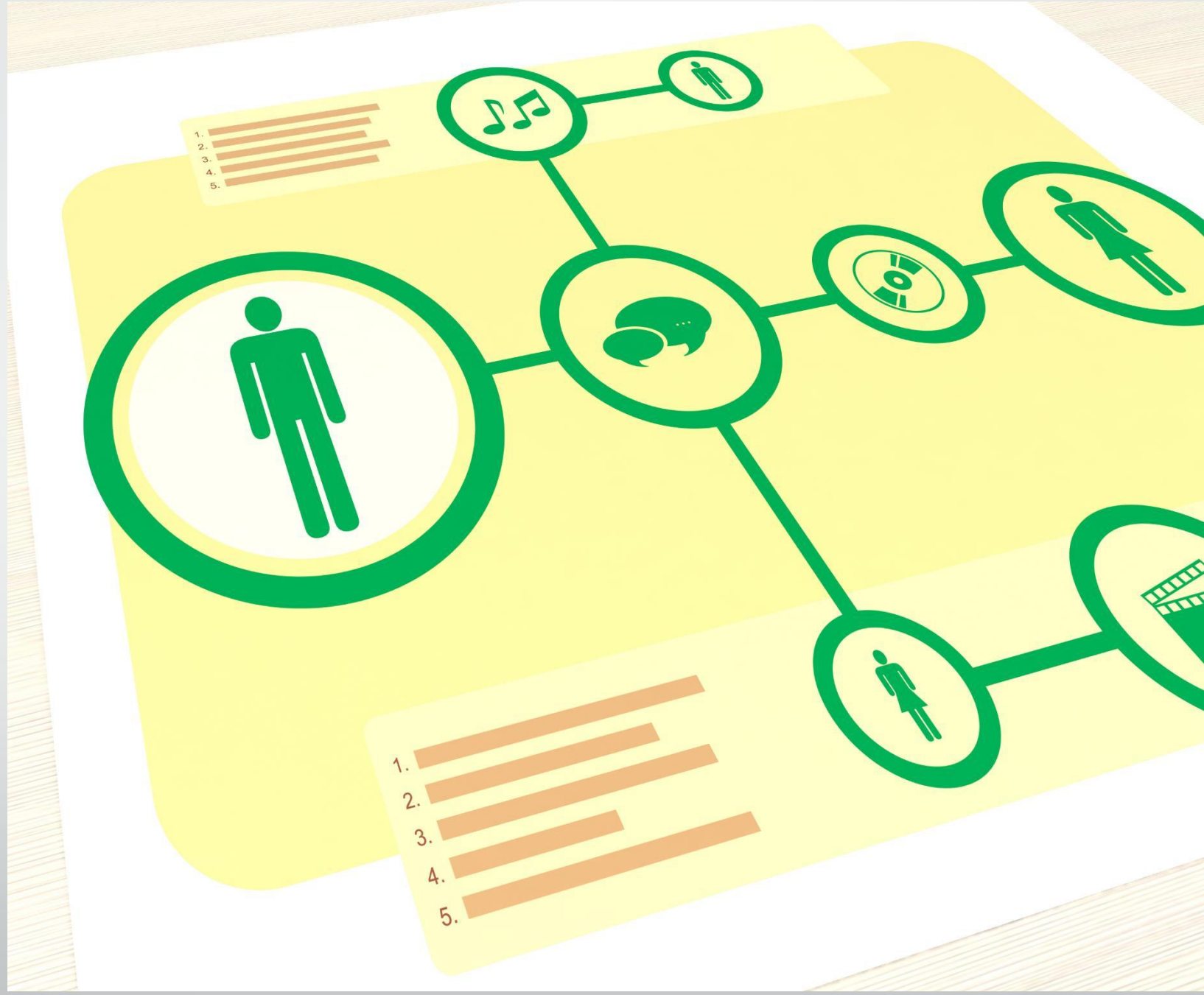
- Which groups?
- Is write-back required?

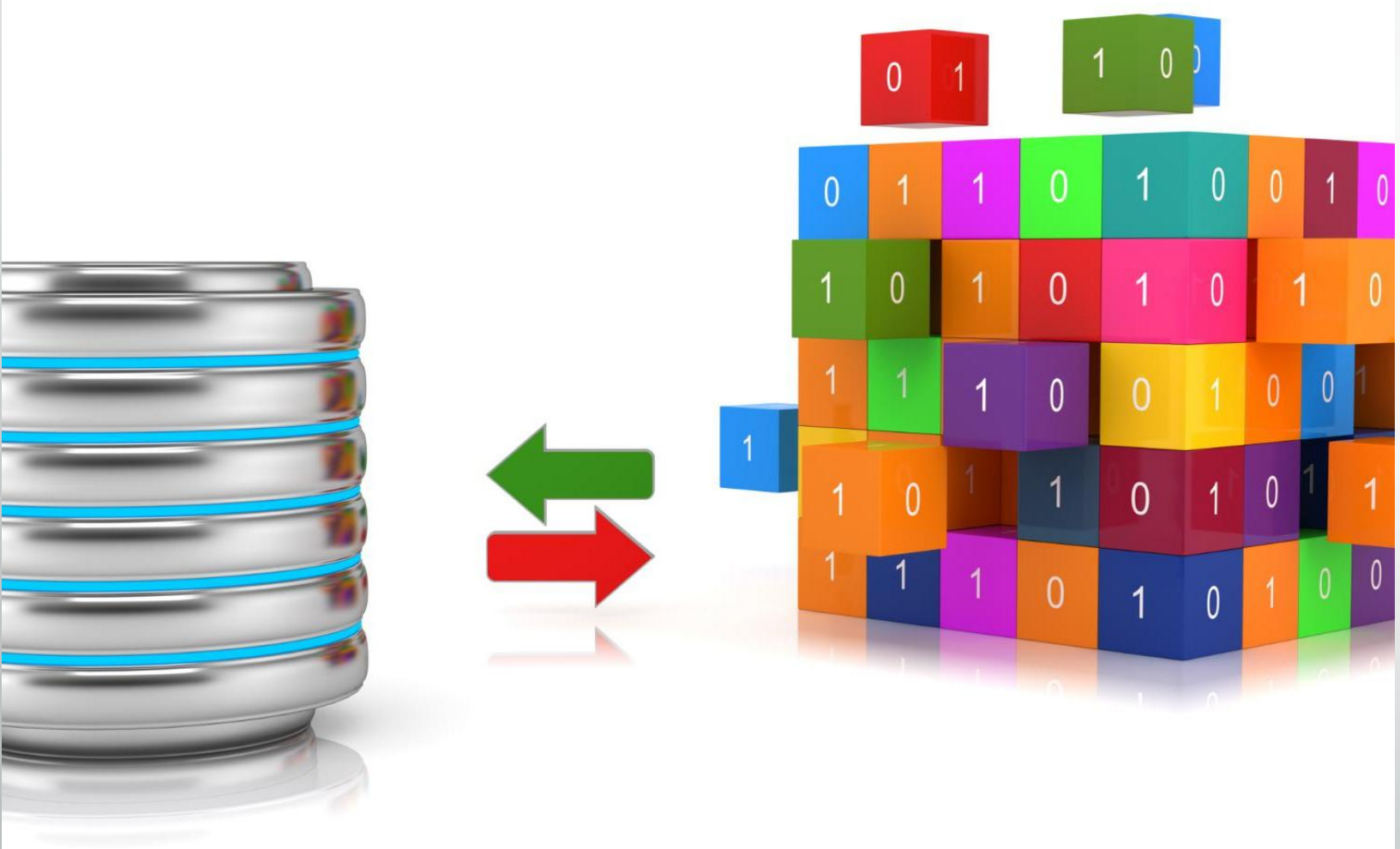
Dependency Verification

- Nested groups (yuk 😑)
- Write-back support

Execution planning

- Migrate per service
- Update Connect Cloud Sync & Connect Sync to latest version.





PROCESS SEQUENCE FOR GROUP SOA CONVERSION

Configure Group write-back if required

Change OU Path in provisioning

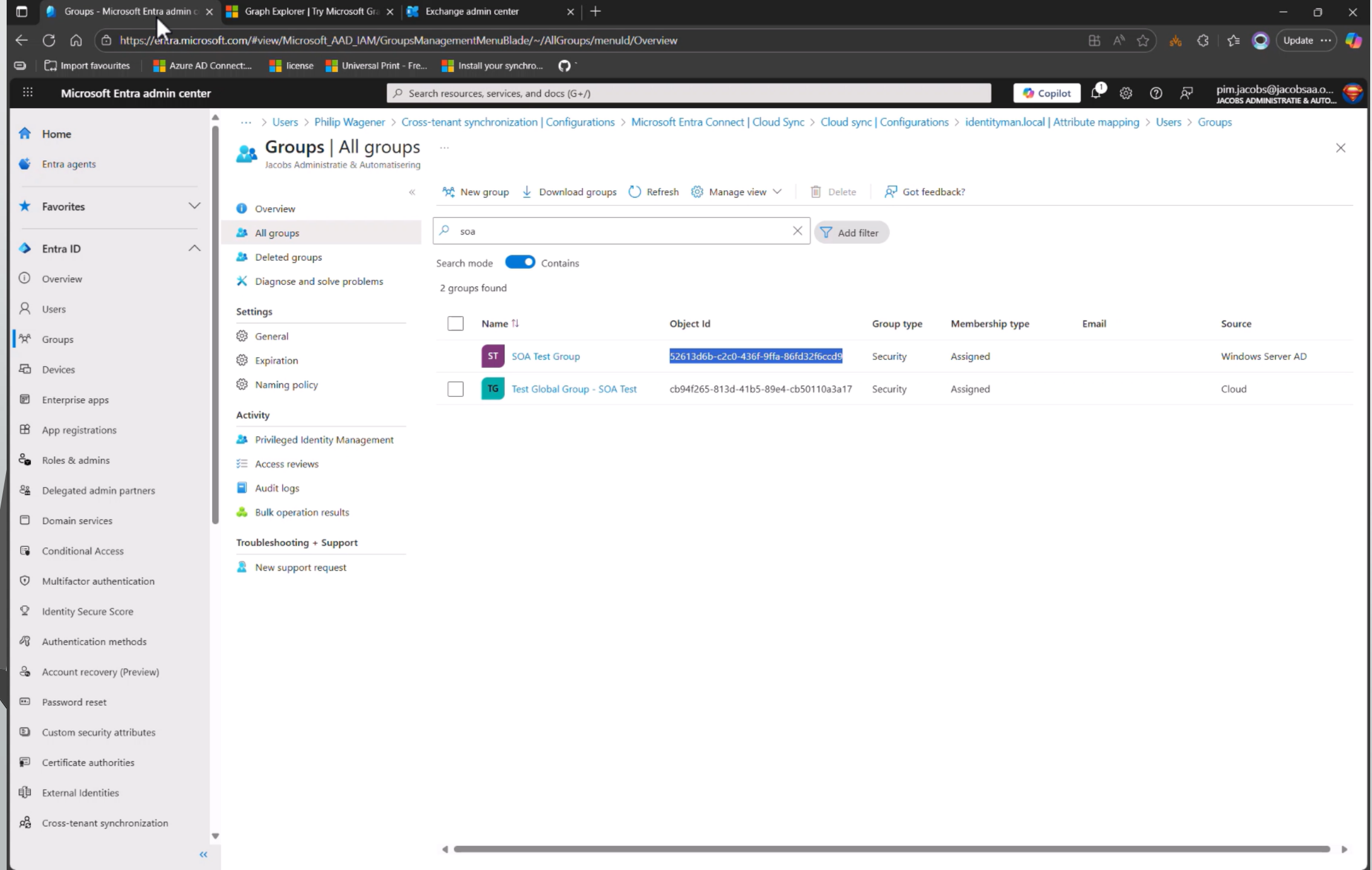
Reconfigure groups if required (group type)

Convert group SOA of identified groups

Bring groups in scope of write-back

LIMITATIONS & CONSIDERATIONS

- SOA is applied on object level and only supports (mail-enabled) security groups.
- For write-back only security groups (not mail enabled security groups) are supported.
- For write-back the group type in AD must and always will be of type universal
- Users in scope of write-back are part of the same forest.
- Write-back only available in Connect Cloud Sync.
- Separate consent permission required **'Group-OnPremisesSyncBehavior.ReadWrite.All'**
- Runs with an interval of 20 minutes


Groups - Microsoft Entra admin c
Graph Explorer | Try Microsoft Gra
Exchange admin center
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/GroupsManagementMenuBlade/~/AllGroups/menuId/Overview
Import favourites
Azure AD Connect:...
license
Universal Print - Fre...
Install your synchro...
Update
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
pim.jacobs@jacobsaa.o...
JACOBS ADMINISTRATIE & AUTO...
Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Enterprise apps
App registrations
Roles & admins
Delegated admin partners
Domain services
Conditional Access
Multifactor authentication
Identity Secure Score
Authentication methods
Account recovery (Preview)
Password reset
Custom security attributes
Certificate authorities
External Identities
Cross-tenant synchronization
Users > Philip Wagener > Cross-tenant synchronization | Configurations > Microsoft Entra Connect | Cloud Sync > Cloud sync | Configurations > identityman.local | Attribute mapping > Users > Groups
Groups | All groups
Jacobs Administratie & Automatisering
Overview
All groups
Deleted groups
Diagnose and solve problems
Settings
General
Expiration
Naming policy
Activity
Privileged Identity Management
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
New group
Download groups
Refresh
Manage view
Delete
Got feedback?
soa
Add filter
Search mode
Contains
2 groups found
Name
Object Id
Group type
Membership type
Email
Source
ST
SOA Test Group
52613d6b-c2c0-436f-9ffa-86fd32f6ccd9
Security
Assigned
Windows Server AD
TG
Test Global Group - SOA Test
cb94f265-813d-41b5-89e4-cb50110a3a17
Security
Assigned
Cloud

DEMO #2

Source of Authority Conversion for Users to Entra ID

VALUE ADD BY MIGRATING USER SOA TO ENTRA ID

Centralised Identity Management

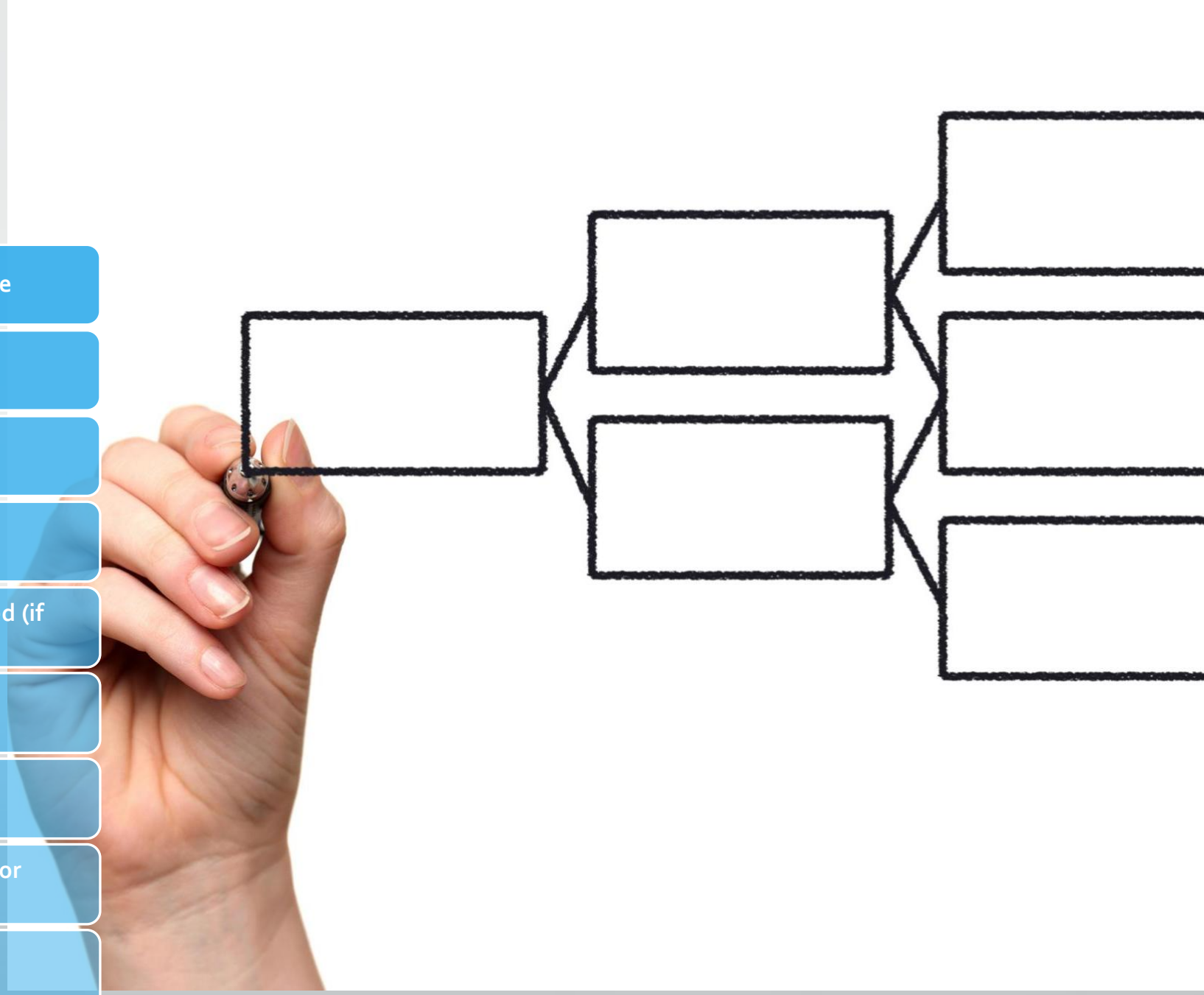
Reducing on-premises footprint

Improved Security

Use of modern Authentication Protocols (no passwords 🥳)

PREREQUISITES FOR USER SOA CONVERSION

- Entra Connect Sync and Cloud Sync fully up-to-date
- SOA for groups executed
- Exchange hybrid fully decommissioned
- Device migrated to Entra Joined (no hybrid)
- Inbound provisioning preparation changes prepared (if any)
- Dynamic group changes prepared
- MIM Changes prepared
- Use of passwordless methods like Windows Hello for Business or Passkeys
- No password expiry



PROCESS SEQUENCE FOR USER SOA CONVERSION

Execute inbound provisioning changes(if applicable)

Execute dynamic group rule property changes

Execute MIM changes (if applicable)

Execute last sync

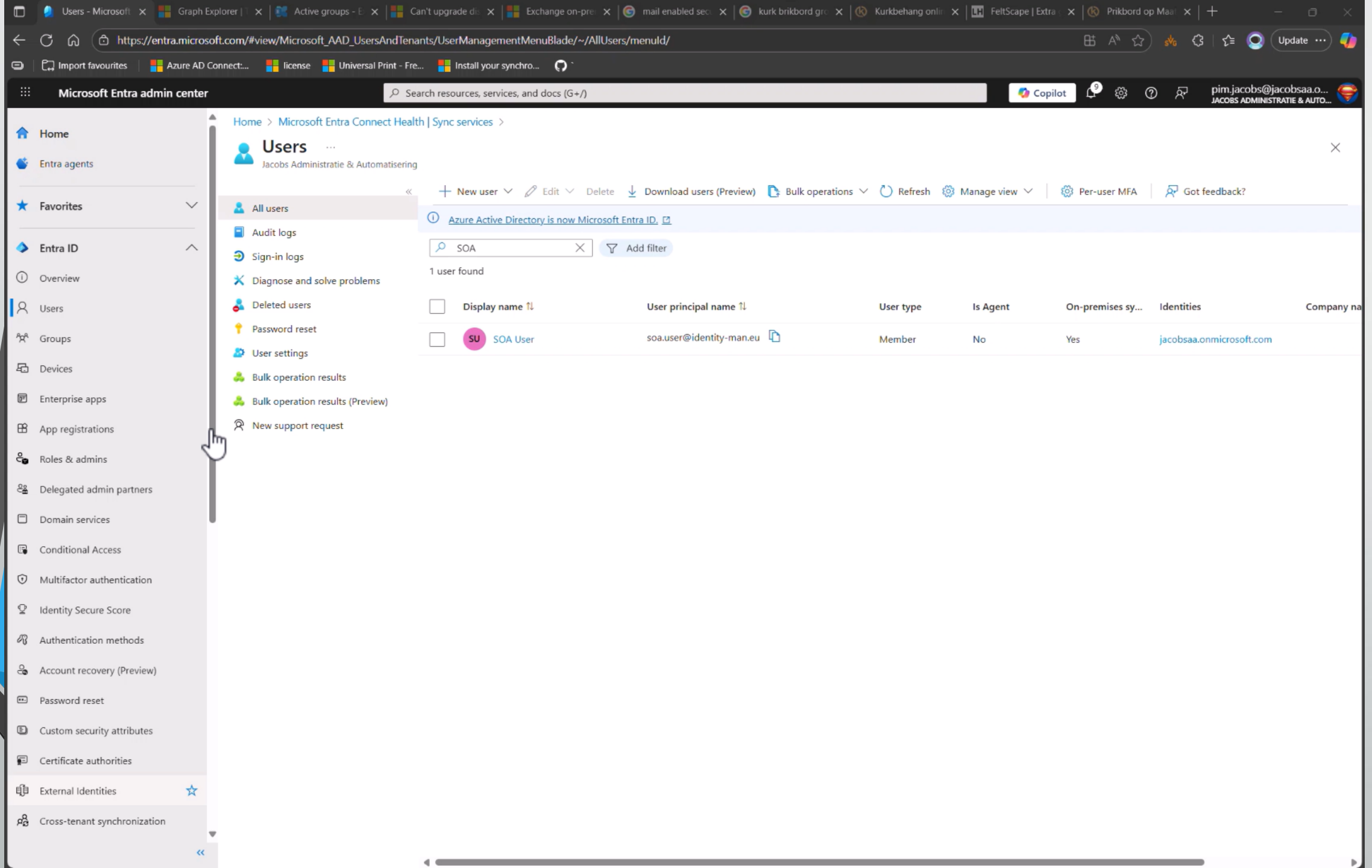
Stop making changes in AD

Transfer SOA of user(s) to the cloud

Validate and test SSO to on-premises resources with passwordless authentication

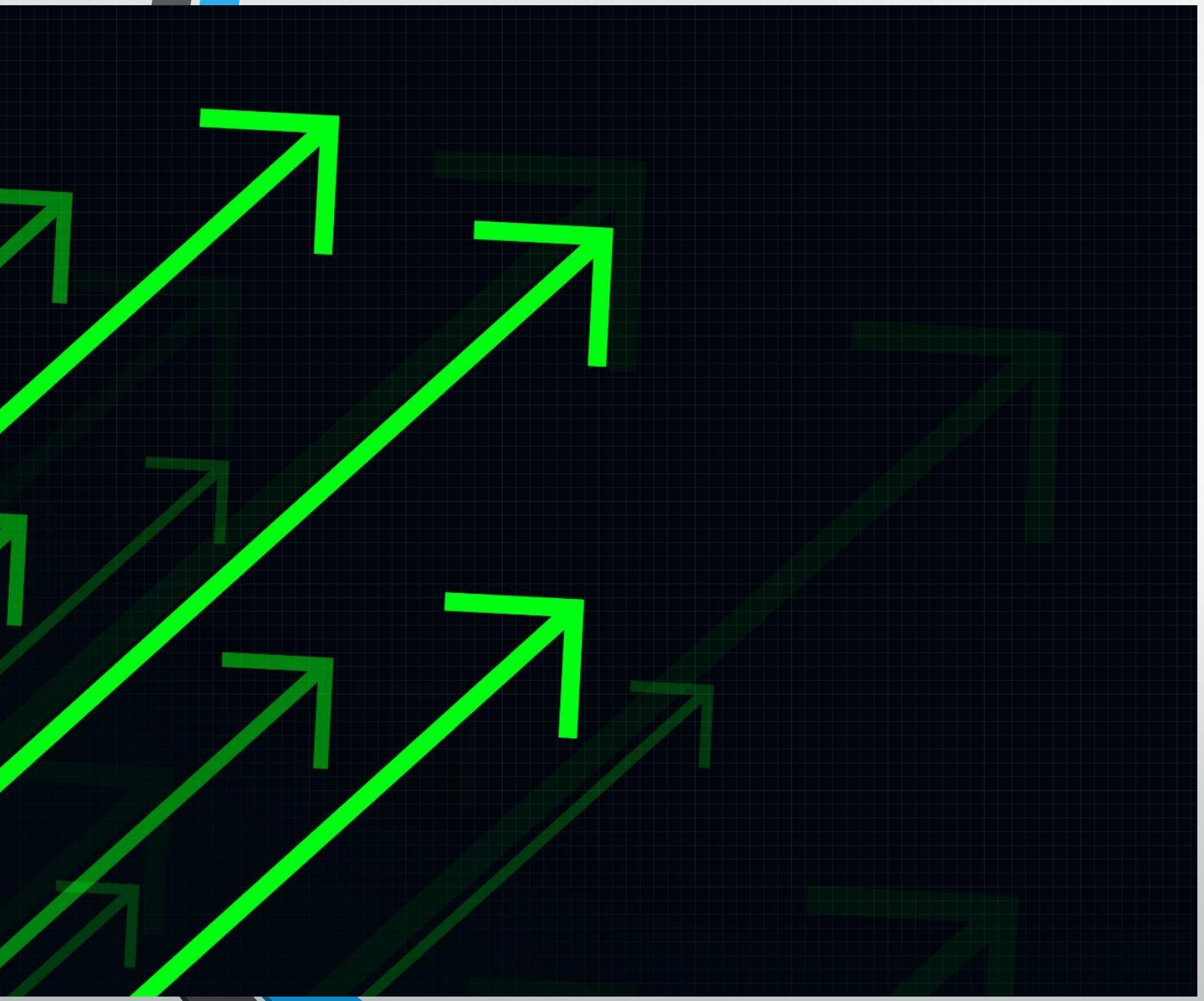
LIMITATIONS & CONSIDERATIONS

- No write-back capabilities yet
- No support for LDAP applications for authentication, Kerberos based is supported
- No federated setup, cloud native authentication is required.
- Migration can only be executed on object level
- Separate consent permission required **'User-OnPremisesSyncBehavior.ReadWrite.All'**


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Enterprise apps
App registrations
Roles & admins
Delegated admin partners
Domain services
Conditional Access
Multifactor authentication
Identity Secure Score
Authentication methods
Account recovery (Preview)
Password reset
Custom security attributes
Certificate authorities
External Identities
Cross-tenant synchronization
Home > Microsoft Entra Connect Health | Sync services >
Users
Jacobs Administratie & Automatisering
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Deleted users
Password reset
User settings
Bulk operation results
Bulk operation results (Preview)
New support request
New user
Edit
Delete
Download users (Preview)
Bulk operations
Refresh
Manage view
Per-user MFA
Got feedback?
Azure Active Directory is now Microsoft Entra ID.
SOA
Add filter
1 user found
Display name
User principal name
User type
Is Agent
On-premises sy...
Identities
SU
SOA User
soa.user@identity-man.eu
Member
No
Yes
jacobsaa.onmicrosoft.com

DEMO #3

Best Practices and Considerations for Source of Authority Transfer



BEST PRACTICES FOR SOA CONVERSIONS

Create a plan for SOA switches including roll-back

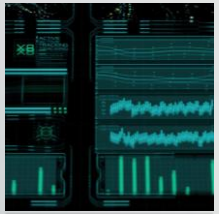
Make sure the pre-requisites are in place

Switch SOA for Exchange Mailboxes and mail-enabled groups

Switch SOA for Security groups per workload/service

Switch user SOA as a last step

SOA Conversion is not a goal, it’s part of the transition to the a modern identity infrastructure!



Single platform

Execute management activities from one single control panel

Modernize identity platform

Use modern techniques for managing your modern identities at scale

Brings Advanced Security Features

Use modern security techniques to protect user identities.

Questions?