

# Migrere tilgangskontroll til Entra ID



[mvpdagen.no](https://mvpdagen.no)

# Takk til våre sponsorer



Se alle våre eventpartnere på skjermen i vandrehallen  
[mvpdagen.no](https://mvpdagen.no)

# Hey!

## Jeg er Marius

Jeg er her fordi jeg digger  
MVP-Dagen og kan litt av hvert  
om identitet.



# Hey!

## Jeg er Marius

CTO og Co-founder av [fortytwo.io](https://fortytwo.io)

Blogg @ [goodworkaround.com](https://goodworkaround.com)

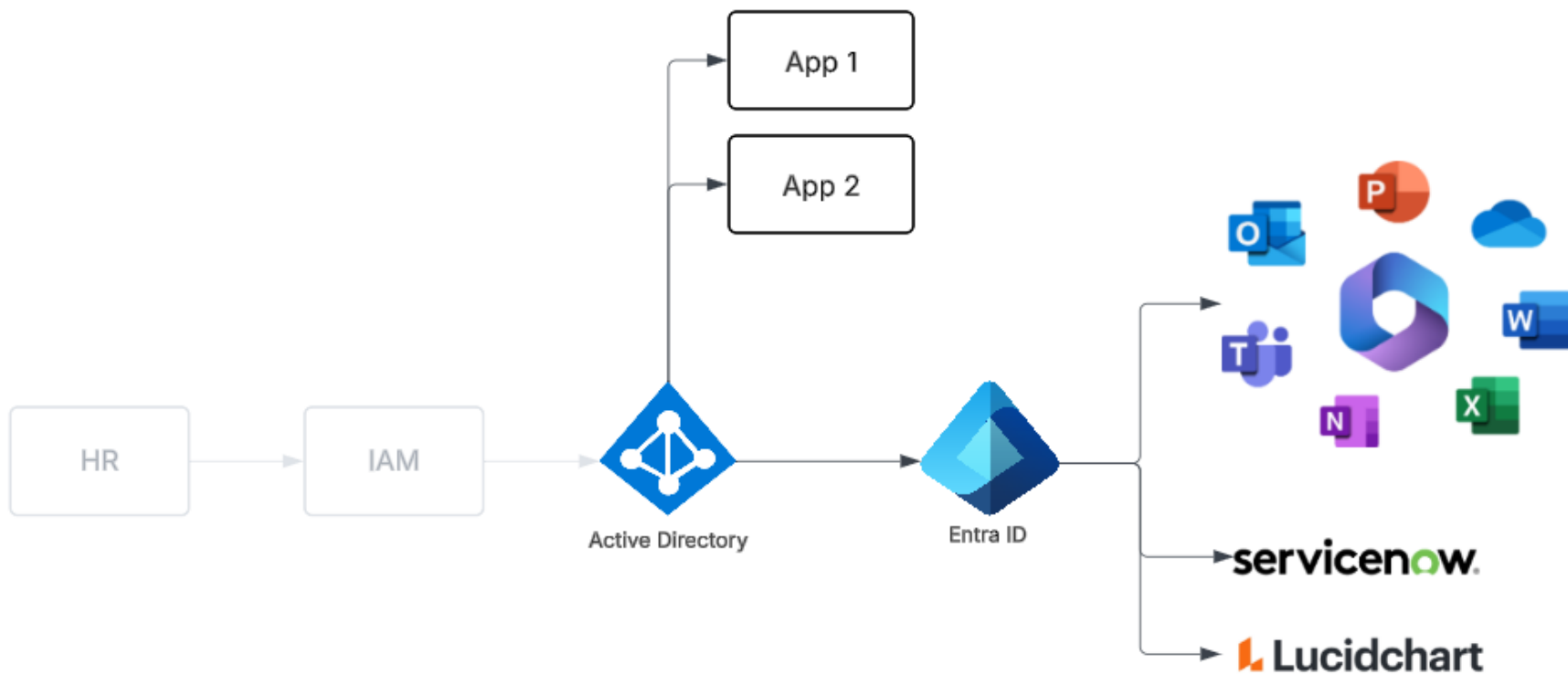


1

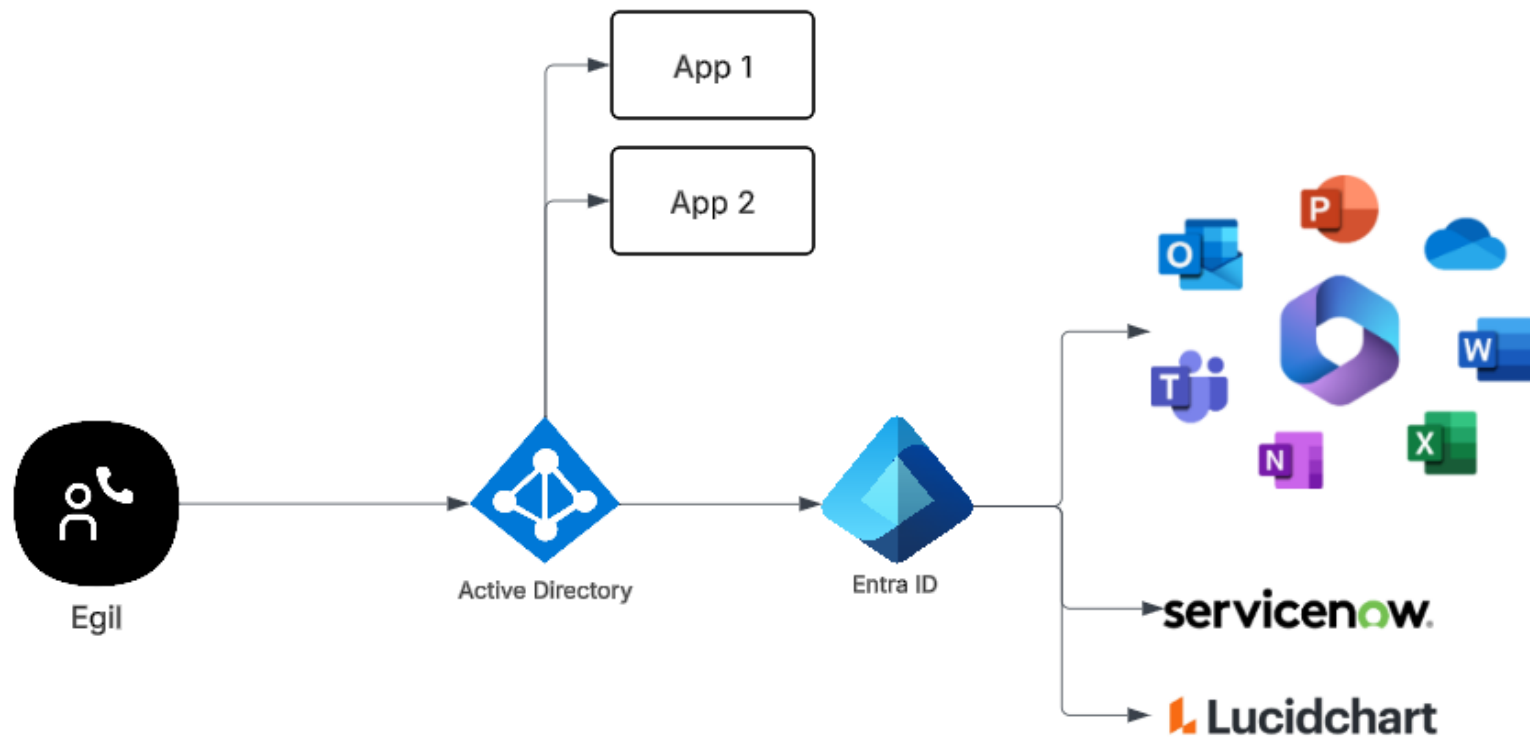
# Dagene som gikk



## Dagene som gikk



## Dagene som gikk



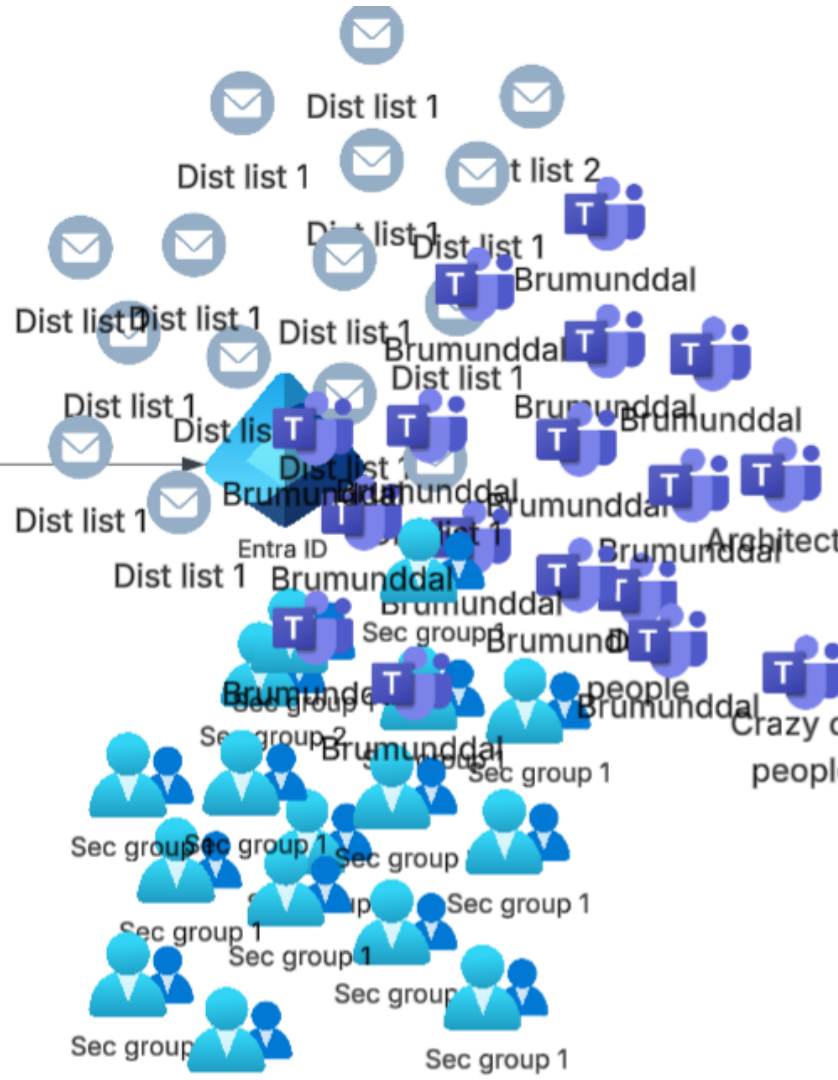
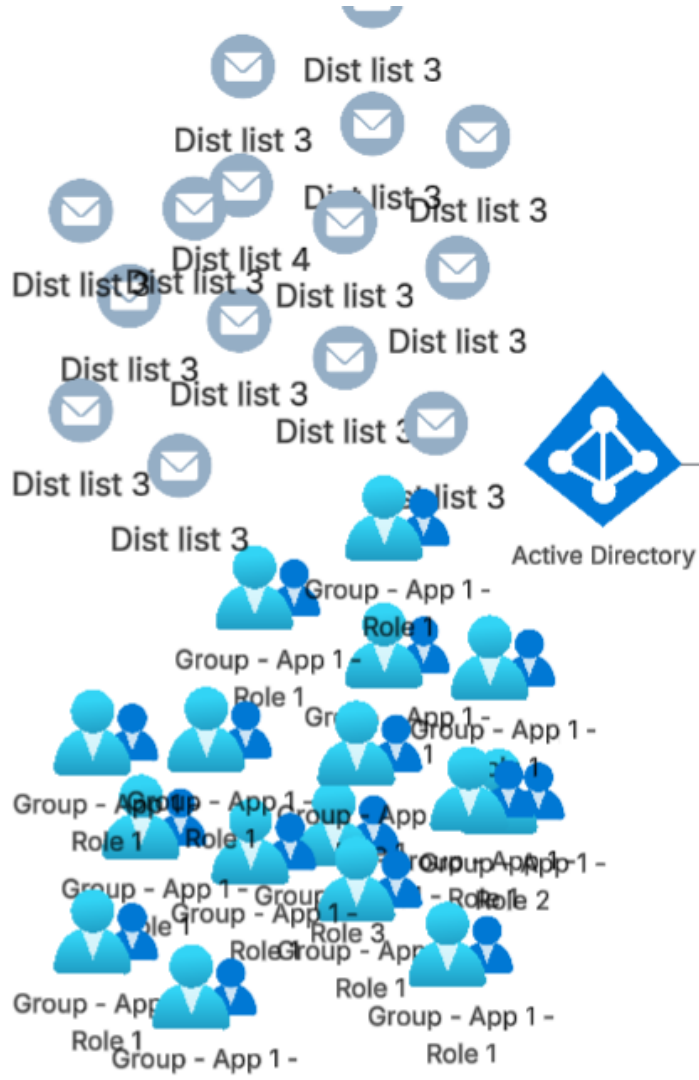


Active Directory



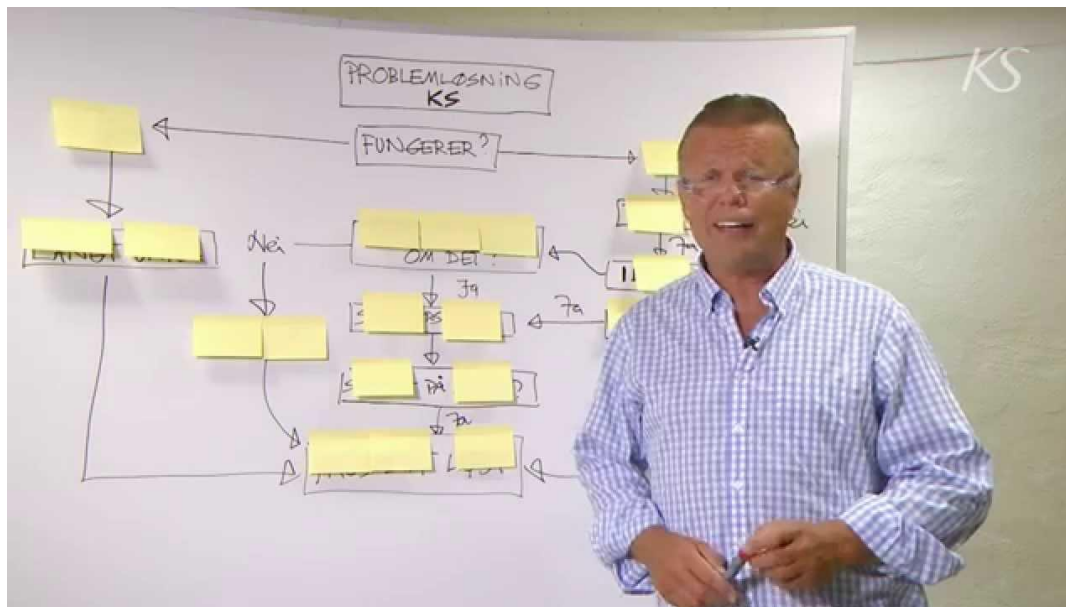
Entra ID

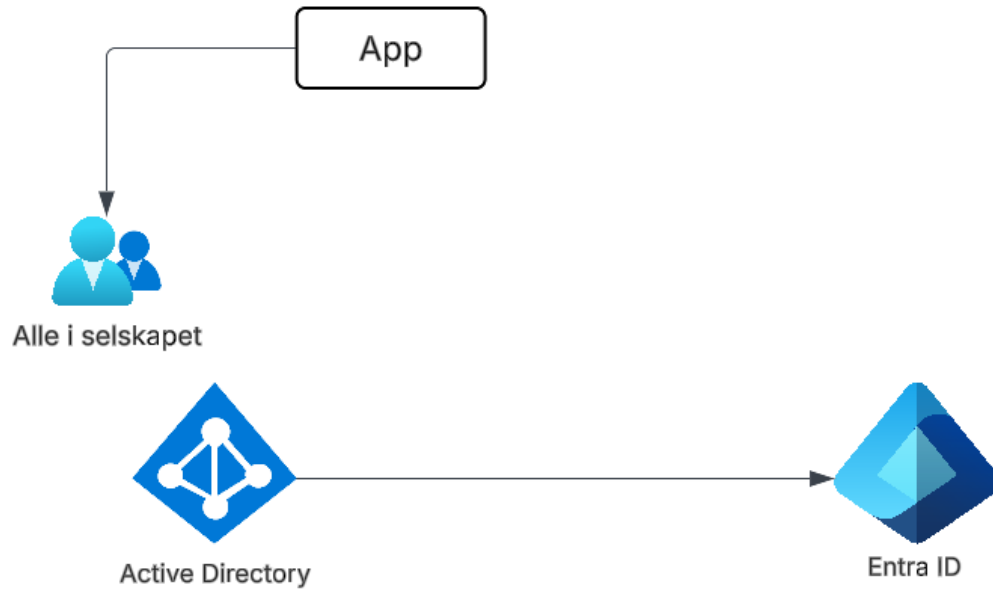






Kan du skylde på noen?









The screenshot shows a web browser window displaying a Microsoft Learn article. The browser's address bar shows the URL `learn.microsoft.com/en-us/entra/identity/users/groups-create-rule`. The page header includes the Microsoft Learn logo and navigation links for Documentation, Training, Q&A, and Topics. A secondary navigation bar lists various Microsoft Entra topics, with 'Microsoft Entra ID' selected. On the left, a sidebar menu allows filtering by title and lists various documentation topics, with 'Create a dynamic group' highlighted. The main content area features the article title 'Create or update a dynamic membership group in Microsoft Entra ID' and a sub-header 'Rule builder in the Azure portal'. The article text explains how to use rules to determine dynamic membership groups based on user or device properties in Microsoft Entra ID. A 'Note' box states that security groups can include either devices or users, while Microsoft 365 groups can include only users. A 'Was this page helpful?' section with 'Yes' and 'No' buttons is located below the note. At the bottom, a preview of the 'Conditional Access Exceptions - Dynamic membership rules' interface is shown, including a breadcrumb trail, a title bar, and a toolbar with 'Save', 'Discard', and 'Got feedback?' options.

Migrating access control from: X shake apple adam eve - Google: X Create or Edit a Dynamic Mem: X

learn.microsoft.com/en-us/entra/identity/users/groups-create-rule

Learn Documentation Training Q&A Topics

Microsoft Entra Microsoft Entra ID External ID Global Secure Access ID Governance Microsoft Security documentation Troubleshooting

Admin center

Filter by title

Enterprise users documentation

- > Overview
- > Quickstarts
- > Tutorials
- > Concepts
  - Compare default user permissions
  - Group-based licensing basics
  - Manage access with groups
- > How-to guides
  - > Users
  - > Organization (tenant)
  - > Groups
    - Learn about groups and access rights
    - Manage access with groups
    - Manage groups PowerShell for Graph (v2)
    - Configure group settings with PowerShell
    - Search group and member lists
  - > Dynamic groups
    - Managing dynamic membership group processing
    - Create a dynamic group
    - Dynamic group rule syntax
    - Validate a membership rule
    - Create more efficient rules
    - Change group membership type
    - Group as memberOf a dynamic group

Add members in bulk

Download PDF

Learn / Microsoft Entra / Microsoft Entra ID / Users /

Ask Learn Focus mode

## Create or update a dynamic membership group in Microsoft Entra ID

05/01/2025

You can use rules to determine dynamic membership groups based on user or device properties in Microsoft Entra ID. This article describes how to set up a rule for a dynamic membership groups in the Azure portal.

Group membership based on user or device properties is supported for security groups and Microsoft 365 groups. When you apply a rule for a dynamic membership group, user and device attributes are evaluated for matches with the membership rule. When an attribute changes for a user or device, all rules for dynamic membership groups in the organization are processed for changes. Users and devices are added or removed if they meet the conditions for a dynamic membership group. In Microsoft Entra ID, a single tenant can have a maximum of 15,000 dynamic membership groups.

**Note**

Security groups can include either devices or users, but Microsoft 365 groups can include only users.

Using dynamic membership groups requires a Microsoft Entra ID P1 license or an Intune for Education license. For more information, see [Manage rules for dynamic membership groups in Microsoft Entra ID](#).

### Rule builder in the Azure portal

Microsoft Entra ID provides a rule builder to create and update your important rules more quickly. The rule builder supports the construction of up to five expressions.

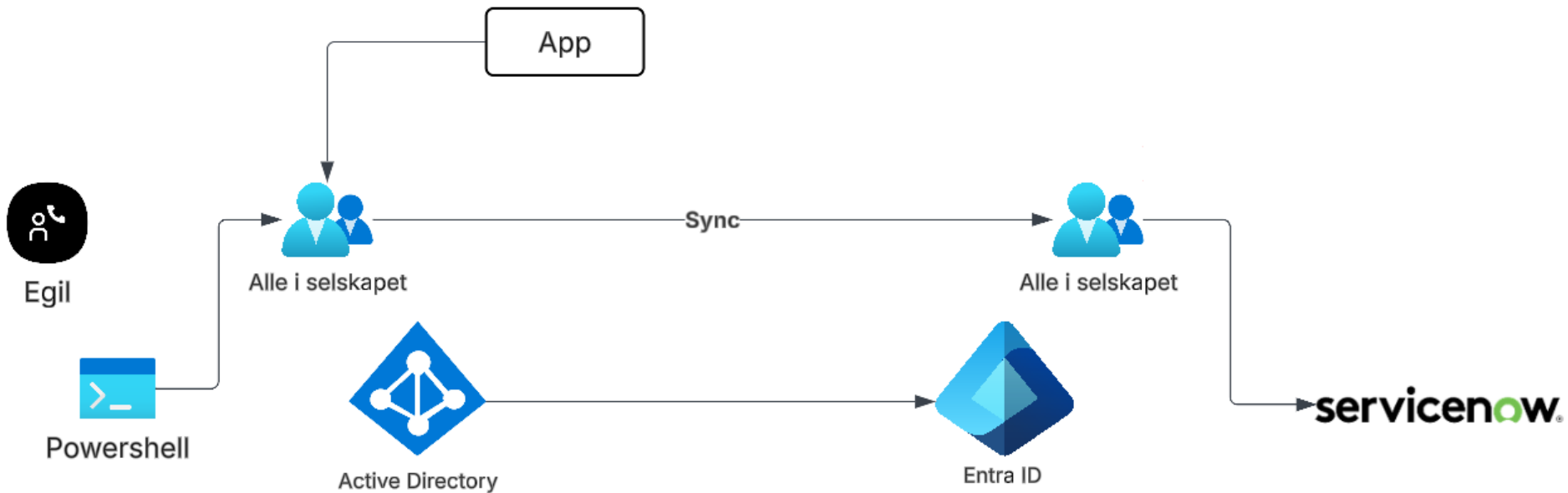
Home > Contoso > Groups - All groups > Conditional Access Exceptions - Dynamic membership rules

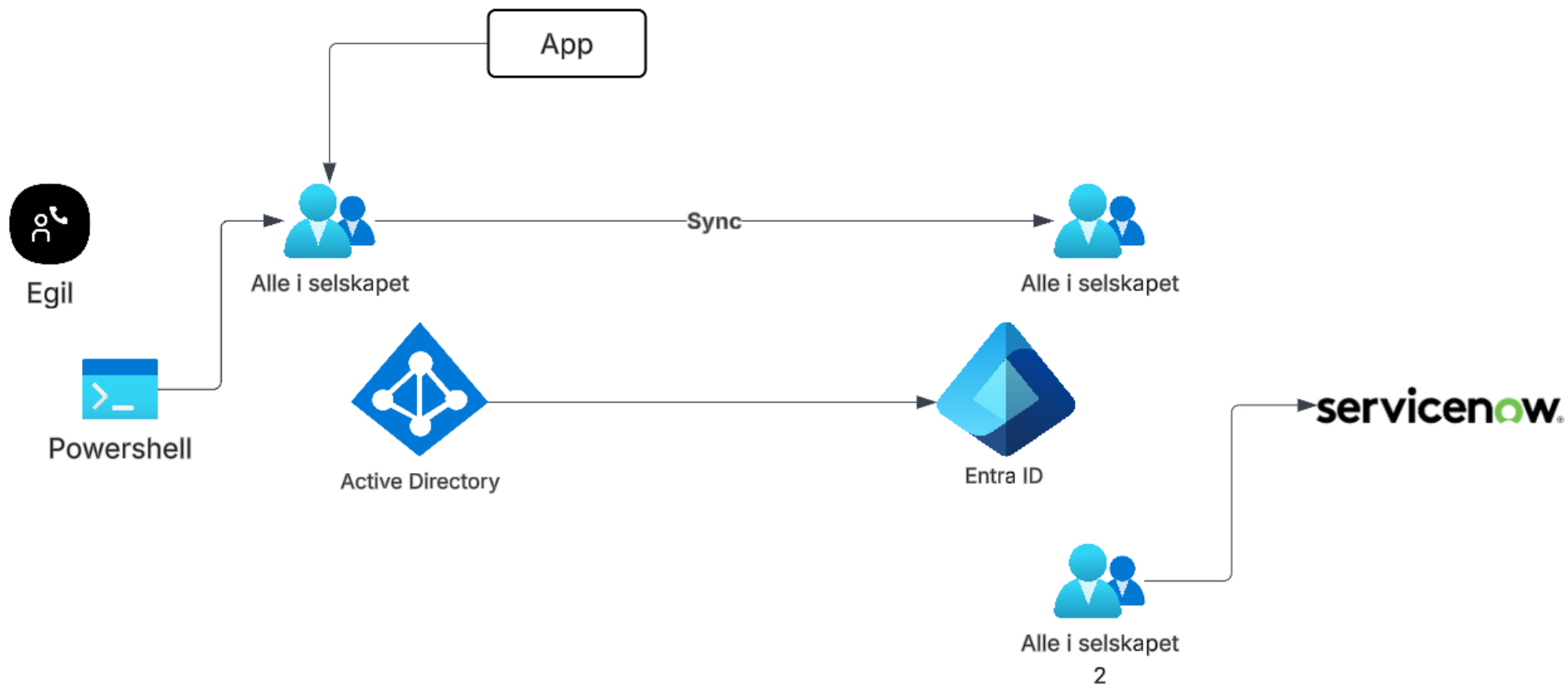
Conditional Access Exceptions - Dynamic membership rules

Group

Save Discard Got feedback?

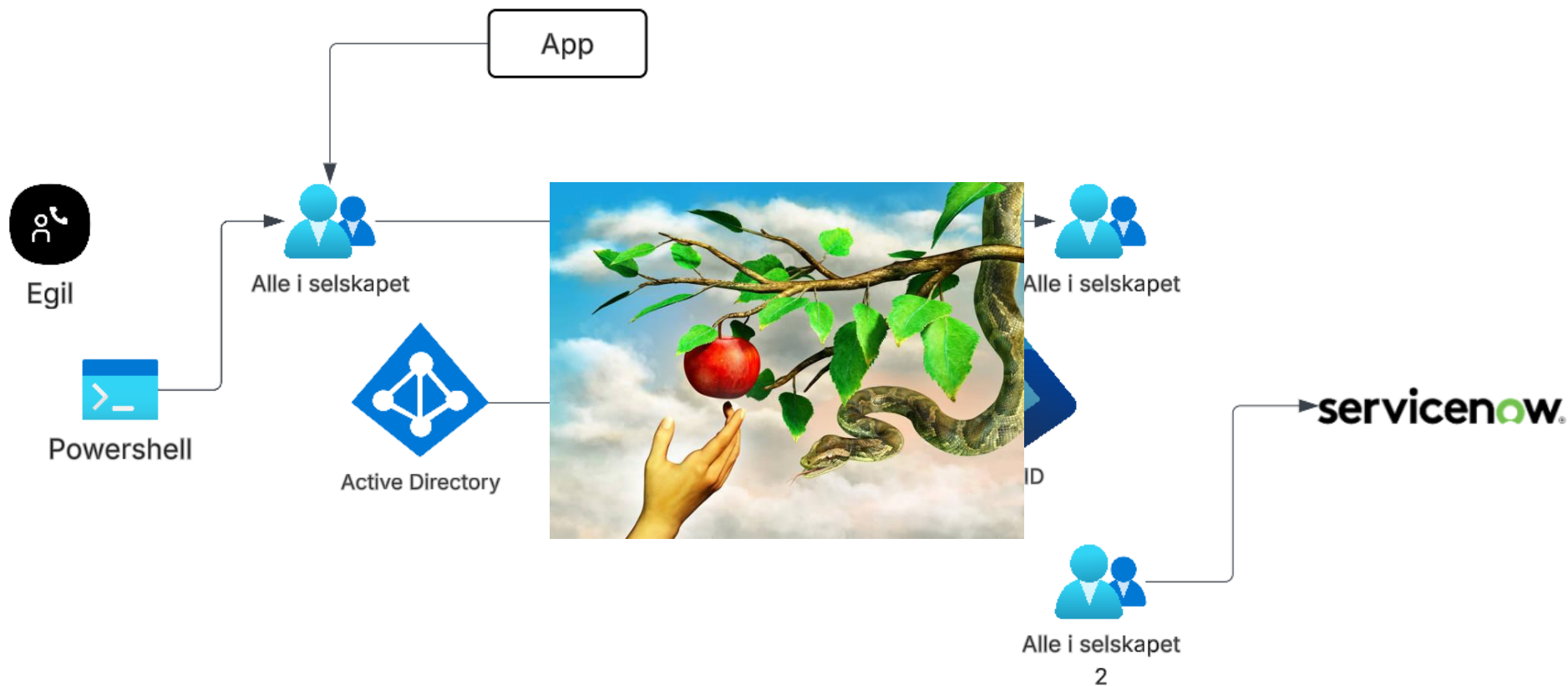
Overview Configure Rules





```
user.companyName -eq "Selskapet"
```





```
user.companyName -eq "Selskapet"
```

Learn

Documentation

Training

Q&A

Topics

Microsoft Entra

Microsoft Entra ID

External ID

Global Secure Access

ID Governance

Microsoft Security documentation

Troubleshooting

Admin center

Filter by title

Hybrid identity

Scenarios

Cloud sync reference

What is cloud sync?

What is the provisioning agent?

Concepts

How-to guides

Installation and upgrade

Installation Prerequisites

Install the provisioning agent using CLI and PowerShell

Provision Active Directory to Entra ID

Provision Microsoft Entra ID to Active Directory

Provision Microsoft Entra ID to AD - Configuration

Scoping filter and Attribute mapping - Microsoft Entra ID to AD

Directory extensions and custom attributes - Microsoft Entra ID to AD

On-demand provisioning - Microsoft Entra ID to AD

Migration

Manage

Develop

Troubleshoot

Reference

Download PDF

Learn / Microsoft Entra / Microsoft Entra ID / Hybrid /

Ask Learn

Focus mode

# Provision Microsoft Entra ID to Active Directory - Configuration

07/17/2025

The following document will guide you through configuring Microsoft Entra Cloud Sync for provisioning from Microsoft Entra ID to Active Directory. If you are looking for information on provisioning from AD to Microsoft Entra ID, see [Configure - Provisioning Active Directory to Microsoft Entra ID using Microsoft Entra Cloud Sync](#).

## Configure provisioning

To configure provisioning, follow these steps.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [hybrid identity administrator](#).
2. Browse to **Entra ID > Entra Connect > Cloud sync**.

Home

Features

Identity

Cloud Sync

Connect Sync

Users

Groups

Devices

Applications

Risks & alerts

Billing

Settings

Protection

Identity governance

External identities

User experiences

Hybrid management

Microsoft Entra Connect

Home >

Microsoft Entra Connect | Get started

Get feedback?

Learn

Access

Manage

Get started with Microsoft Entra Connect

Microsoft Entra hybrid identity solutions span on-premise and cloud-based capabilities, creating a common user identity for authentication and authorization to all resources regardless of their location. Microsoft Entra Connect has a set of tools and features that is used for to sign your on-premise identities to Microsoft Entra ID, which you then use to access cloud applications.

What is Cloud Sync?

Microsoft Entra Connect cloud sync is a new offering from Microsoft designed to meet and accomplish your hybrid identity goals. For synchronization of users, groups and contacts to Microsoft Entra ID. It accomplishes this by using the Microsoft Entra cloud provisioning agent instead of the Microsoft Entra Connect application.

Is Cloud Sync the right solution for you?

If you are looking to start your hybrid journey, have mergers and acquisitions scenarios, and want a lightweight solution that is cost-effective, Cloud Sync is for you.

In this article

Configure provisioning

Scope provisioning to specific groups

Attribute mapping

Directory extensions and custom attribute mapping.

On-demand provisioning

Accidental deletions and email notifications

Enable your configuration

Quarantines

Restart provisioning

Show 2 more

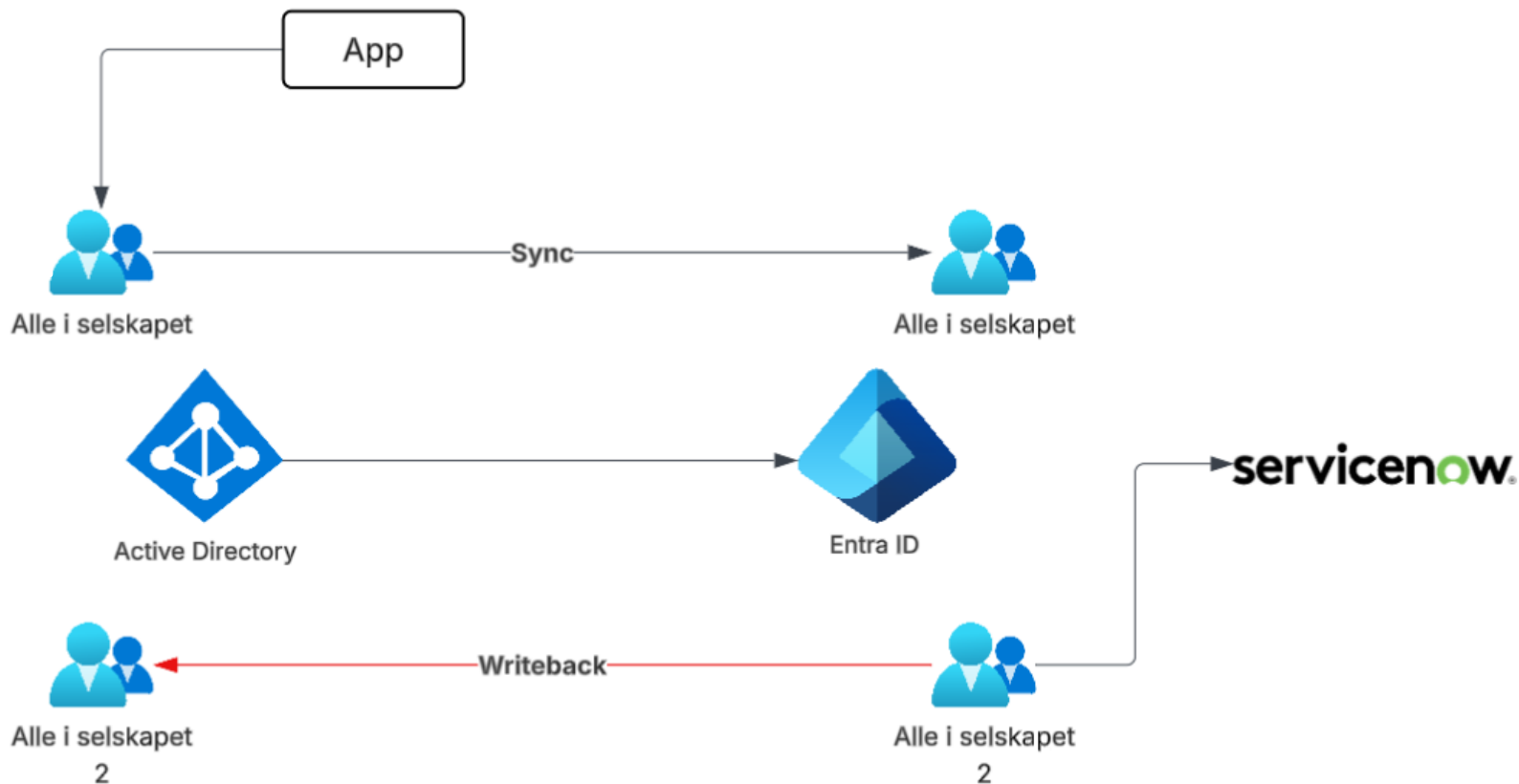
Was this page helpful?

Yes

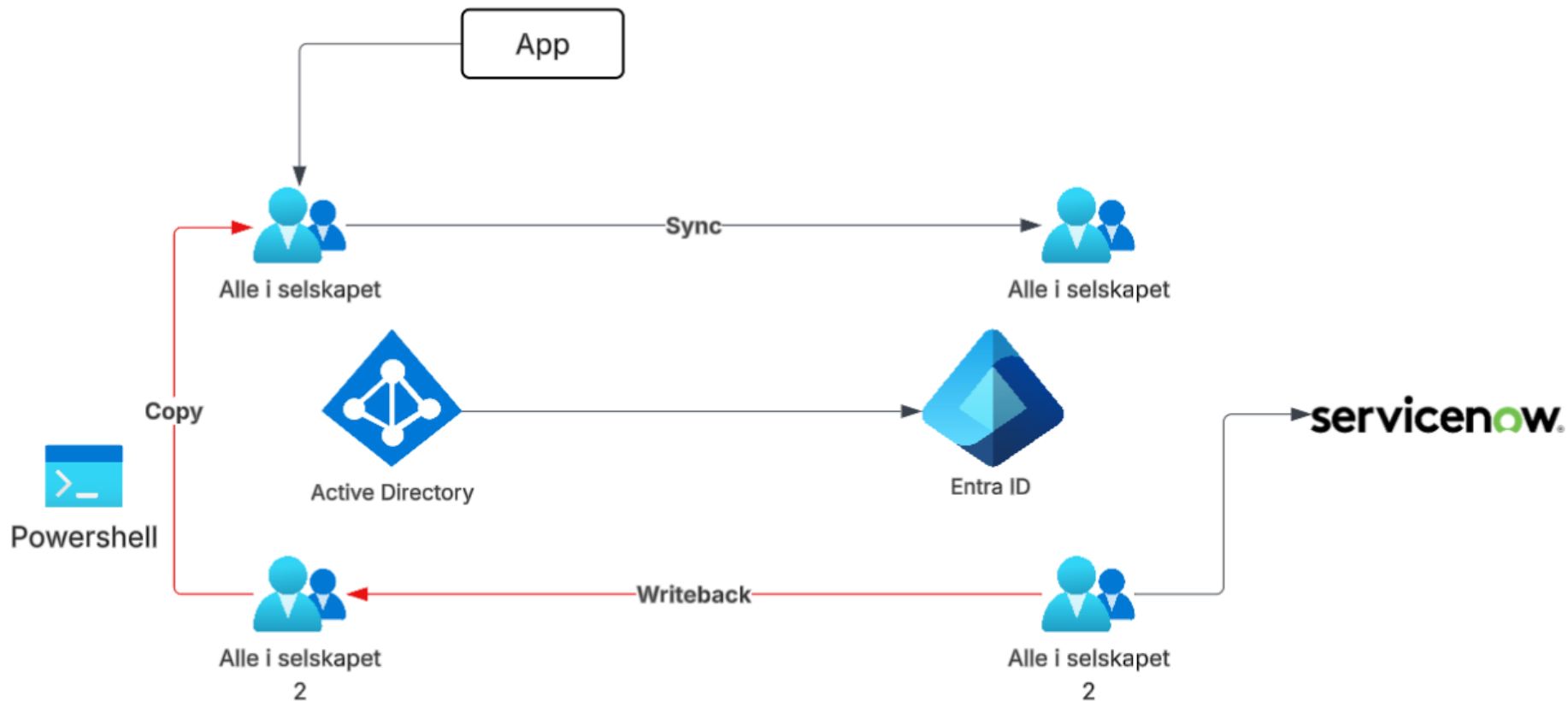
No

MVP  
Dagen

19



`user.companyName -eq "Selskapet"`



`user.companyName -eq "Selskapet"`



“Dette er en super-løsning, hadde det ikke vært for <Sett inn begrensning her> i Entra ID”

– Meg, 2025





“Dette er en super-løsning, hadde det ikke vært for <Sett inn begrensning her> i Entra ID”

– Meg, 2024





“Dette er en super-løsning, hadde det ikke vært for <Sett inn begrensning her> i Entra ID”

– Meg, 2023





“Dette er en super-løsning, hadde det ikke vært for <Sett inn begrensning her> i Azure AD”

– Meg, 2022







“Dette er en super-løsning, hadde det ikke vært for <Sett inn begrensning her> i Azure AD”

– Meg, 2021





“Dette er en super-løsning, hadde det ikke vært for <Sett inn begrensning her> i Azure AD”

– Meg, 2020





“Dette er en super-løsning, hadde det ikke vært for <Sett inn begrensning her> i Azure AD”

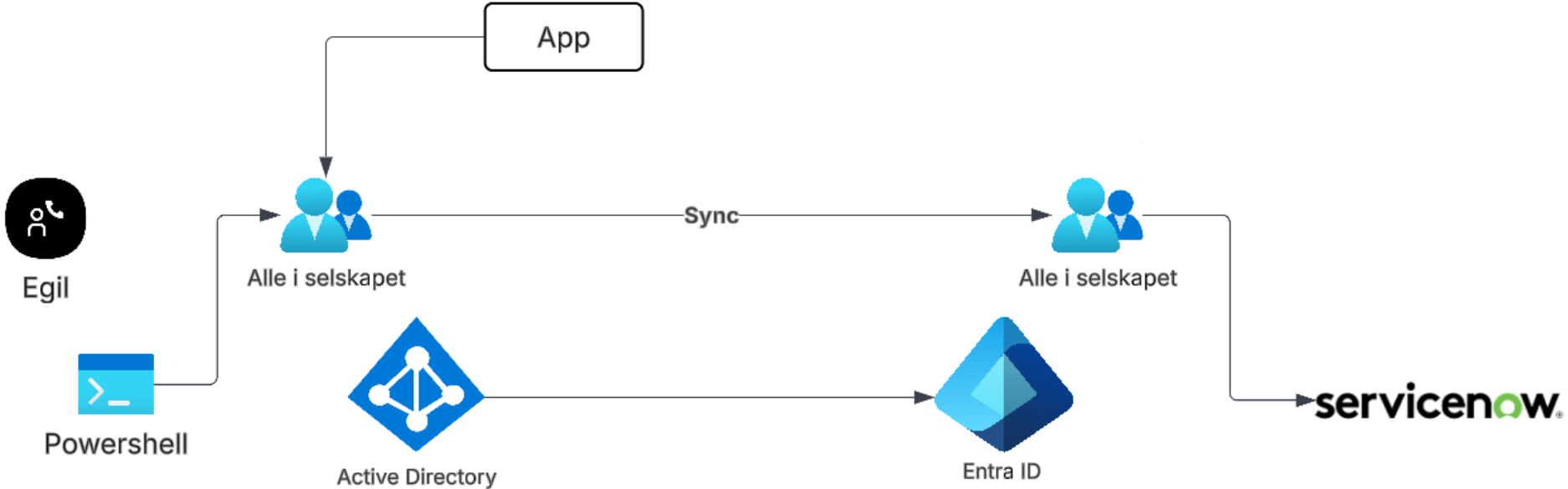
– Meg, 2019–2014





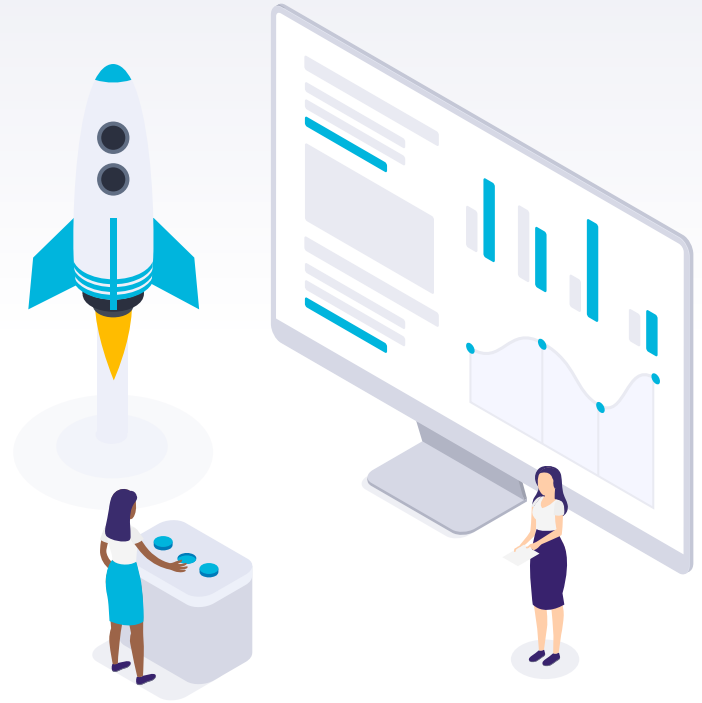
“Dette er en super-  
løsning, hadde det ikke  
vært for <Sett inn  
begrensning her> i  
Windows Azure Access  
Control Services”

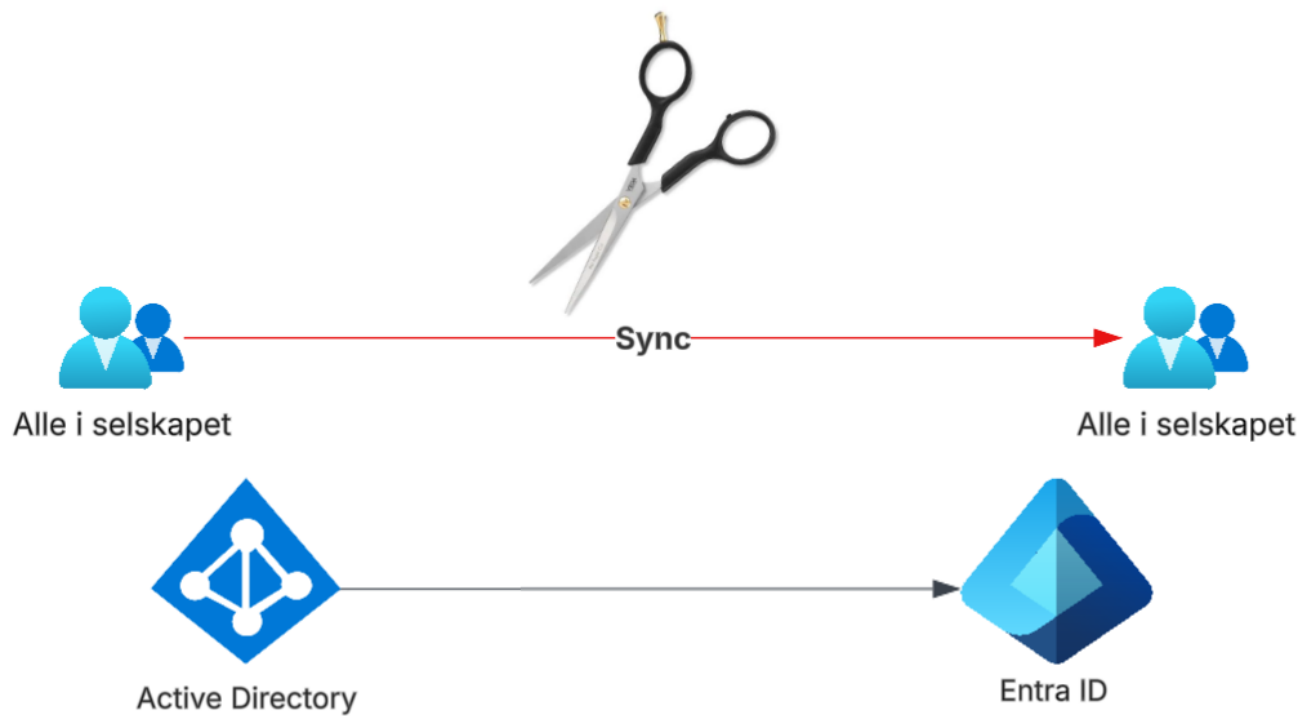




# DEMO 1

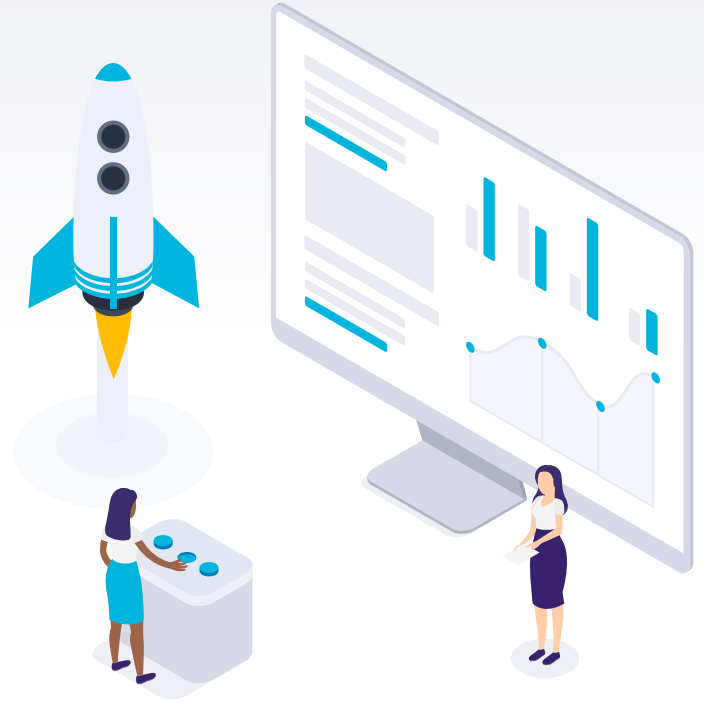
Scissors please





# DEMO 2

Not in sync







Active Directory

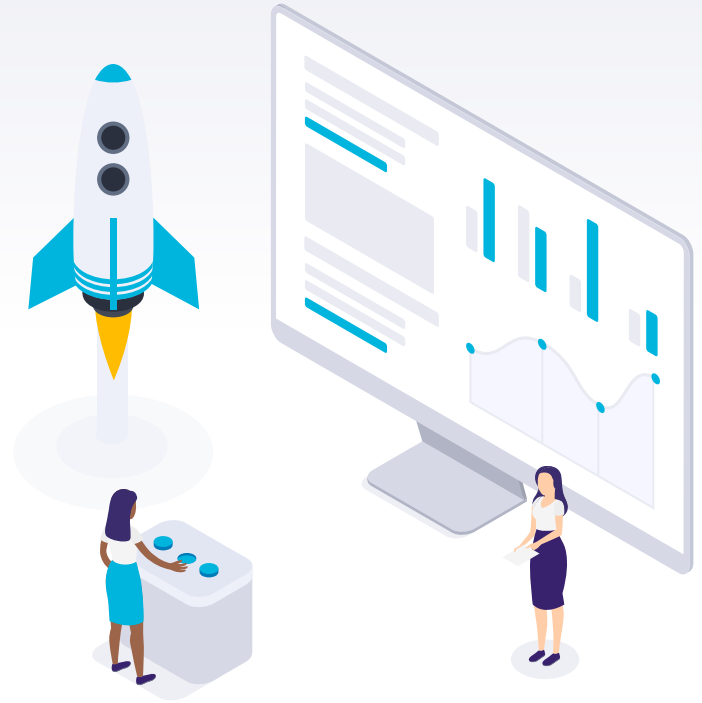


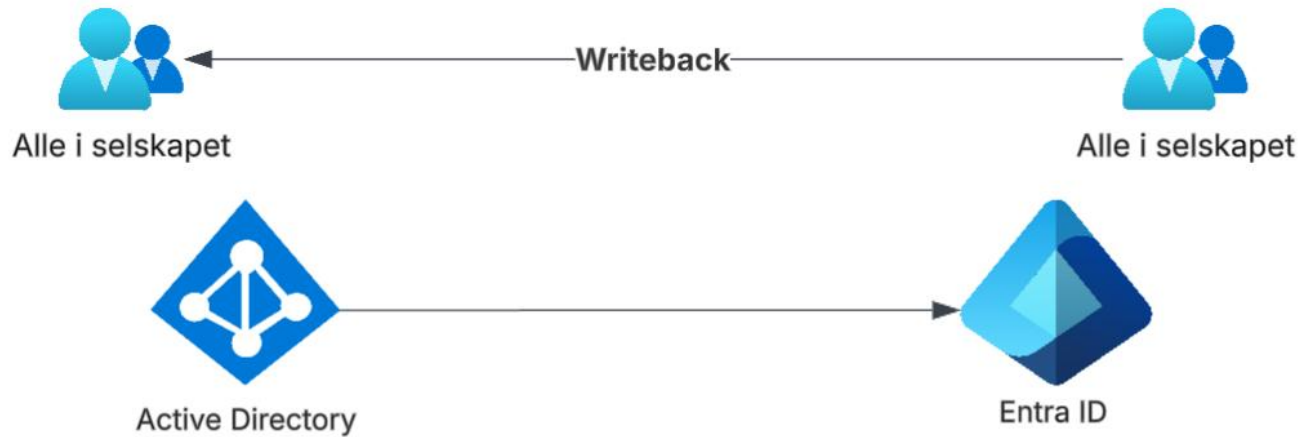
Entra ID



# DEMO 3

Back to the future





2

Hva med  
brukerkontoer  
da?



Filter by title

- Hybrid identity
- Scenarios
  - Getting started with Active Directory
  - Managing your deployment
  - Managing users and groups
  - Managing passwords
  - Managing single sign-on
  - Managing attributes
  - Provision Active Directory to Microsoft Entra ID
- Cloud-first approach with Source of Authority
  - IT architect guide for transferring Source of Authority (SOA)
  - Group Source of Authority (SOA)
- User Source of Authority (SOA)
  - Concepts
  - How to guides
    - Configure User SOA**
    - Audit and monitor User SOA

Download PDF

Microsoft Entra ID / Hybrid /

Ask Learn

Focus mode

# Configure user Source of Authority (SOA) (Preview)

10/06/2025

This article explains the prerequisites, and steps, to configure User Source of Authority (SOA). This article also explains how to revert changes, and current feature limitations. For a full overview for User SOA, see [Embrace cloud-first posture: Transfer User Source of Authority to the cloud \(Preview\)](#).

## Prerequisites

Expand table

Requirement	Description
Roles	<a href="#">Hybrid Administrator</a> is required to call the Microsoft Graph APIs to read and update SOA of users. <a href="#">Application Administrator</a> or <a href="#">Cloud Application Administrator</a> is required to grant user consent to the required permissions to Microsoft Graph Explorer or the app used to call the Microsoft Graph APIs.
Permissions	For apps calling into the <code>onPremisesSyncBehavior</code> Microsoft Graph API, the <code>User-OnPremisesSyncBehavior.ReadWrite.All</code> permission scope needs to be granted. For more information, see <a href="#">how to consent to this permission</a> using the Microsoft

## In this article

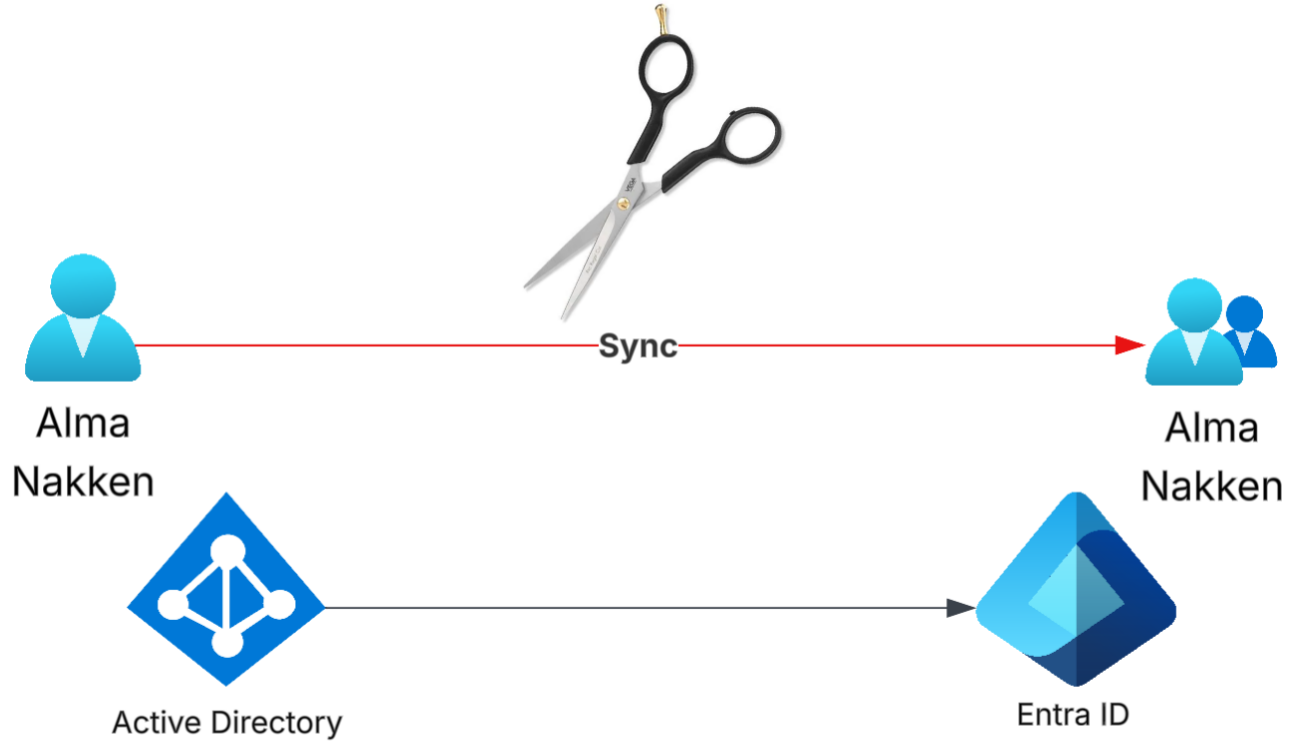
### Prerequisites

- Setup
- Consent permission to apps
- Transfer SOA for a test user
- Connect Sync client
- Roll back SOA update
- Validate in Connect Sync client
- Clear on-premises attributes for SOA transferred users
- Related content

## Was this page helpful?

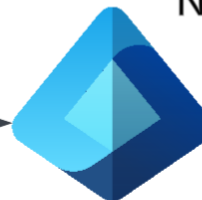
Yes

No





Active Directory



Entra ID



Alma  
Nakken



## Search PowerShell packages:

Az, etc...

[View full stats](#)

10/20/2025

Last Published

Info

[Contact Owners](#)[Report](#)

## Fortytwo.IAM.UserWriteback 1.2.0

A module for synchronizing users from Entra ID into Active Directory, and writing onpremises\* attributes back to Entra ID. Useful when certain users still require on-premises AD users, while all users have their SOA convert to Entra ID.

See the project page for more information on usage: <https://github.com/fortytwoservices/powershell-module-entraiduserwriteback>

Minimum PowerShell version  
7.2

## Installation Options

Install Module

Install PSResource

Azure Automation

Manual Download

Copy and Paste the following command to install this package using PowerShellGet [More Info](#)

```
PS> Install-Module -Name Fortytwo.IAM.UserWriteback
```



## Owners

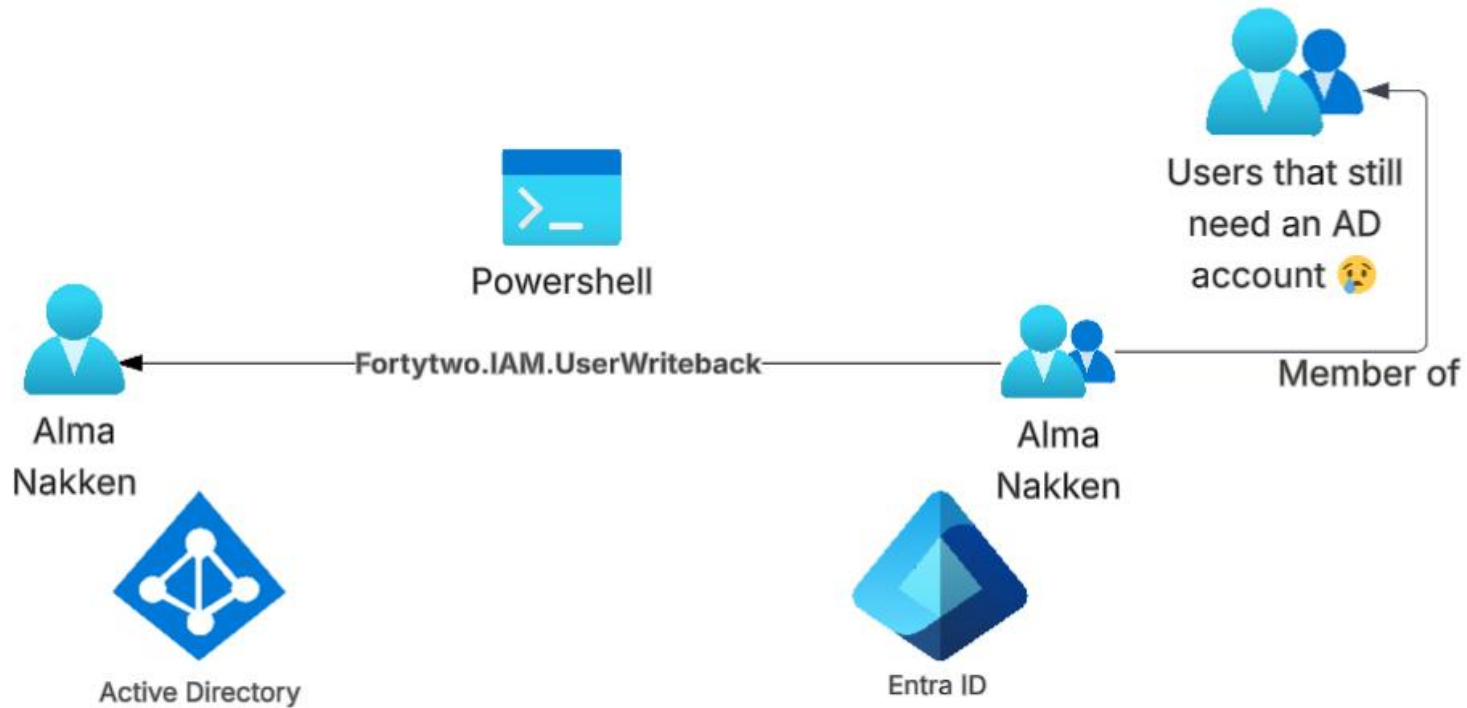
[fortytwo](#)

## Copyright

(c) Fortytwo Technologies AS

[Package Details](#)[FileList](#)

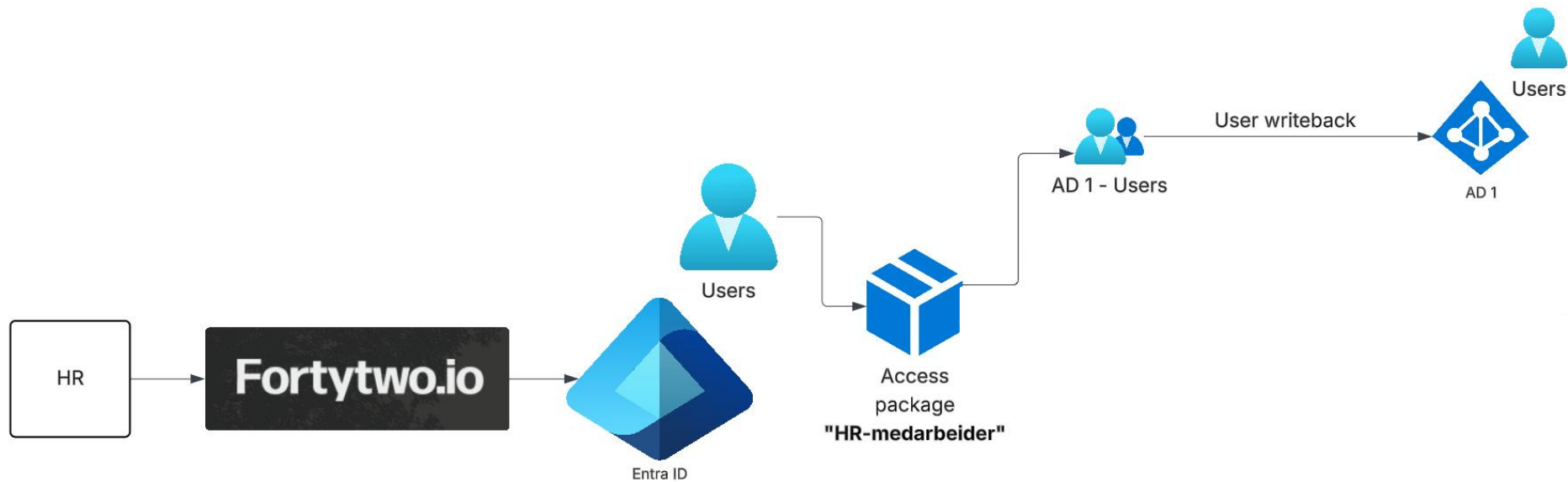


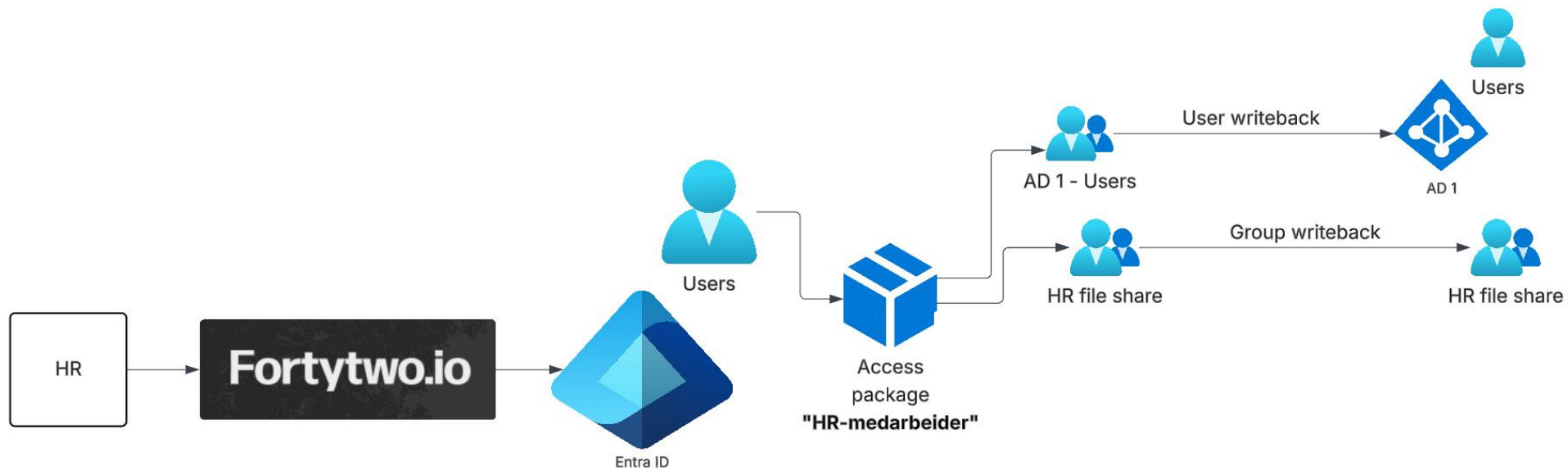


## Ett viktig spørsmål – Hvorfor?

- Alle brukere trenger skya, færre trenger AD
- Følge Microsoft sine anbefalinger om “AD minimization”
- Forvaltning av brukerkontoer skjer i Entra ID
  - inkludert provisjonering fra HR









## Noe som ikke funker?

- Passord

3

Håndtere hvem  
som faktisk er  
medlem av  
disse gruppene





# ► Manuelt

- Helpdesk
- Delegert til en eier
- Delegert til en administrator av en AU



# Criteria based

- ▶ `user.companyName -eq 'Fortytwo'`
- ▶ `(user.proxyAddresses -any(_ -endsWith "@fortytwo.io"))`
- ▶ `user.memberOf -any (group.objectId -in [`
- ▶     `'group-object-id',`
- ▶     `'group-object-id'`
- ▶ `])`



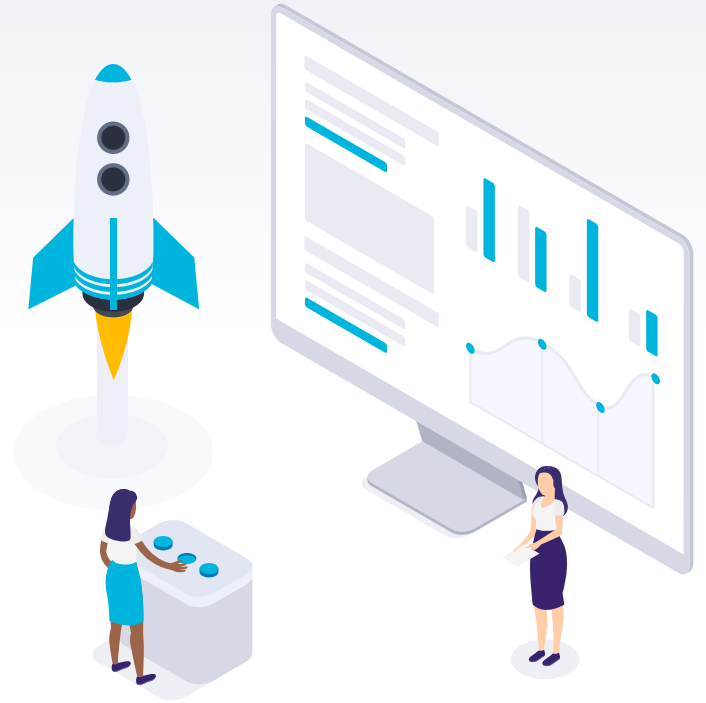
# ► Access packages

- Request access
- Request access on behalf of direct reports
- Auto assignment



# DEMO 4

Access packages



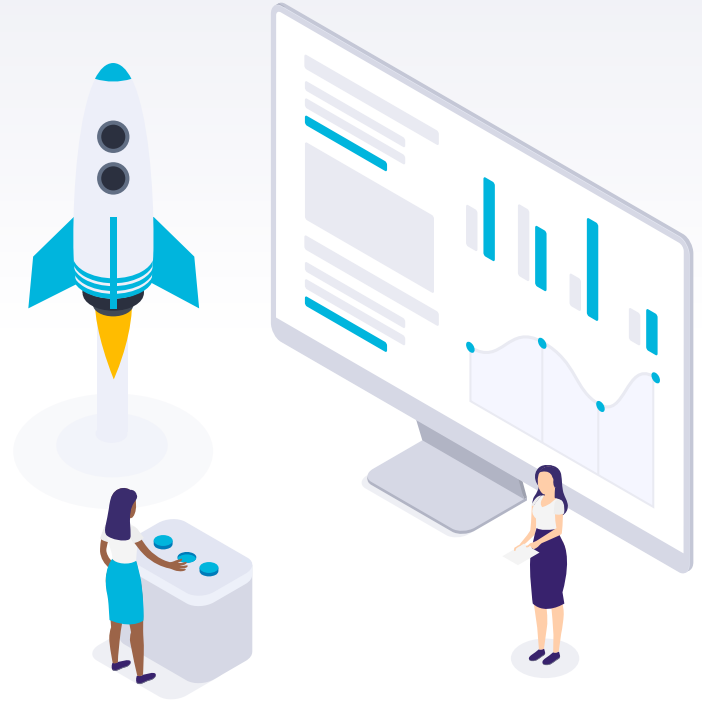
# Life cycle workflows

- ▶ Add to a group
- ▶ Remove from a group
- ▶ Add to an access package
- ▶ Remove from an access package
- ▶ Remove from all groups
- ▶ Remove from all access packages



# DEMO 5

Life cycle workflows

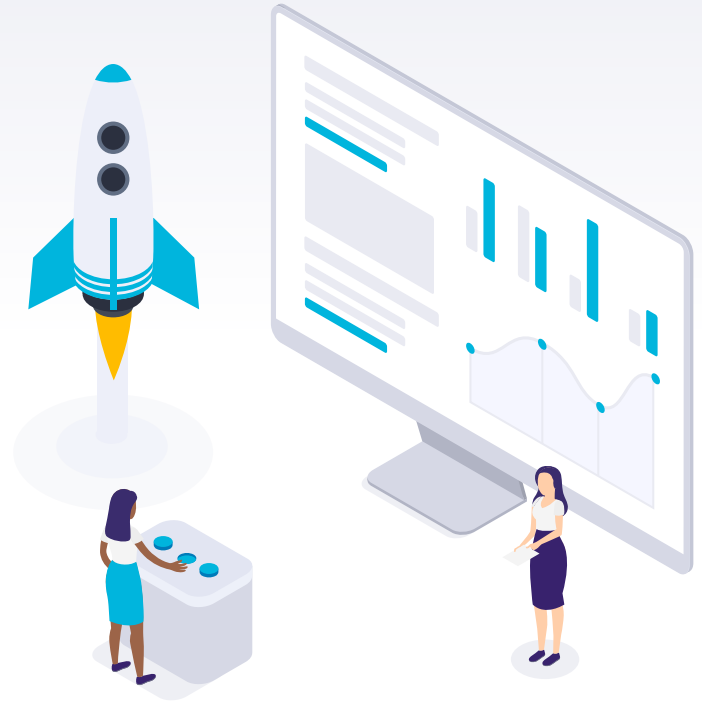


# ► PIM for Groups



# DEMO 6

PIM for groups



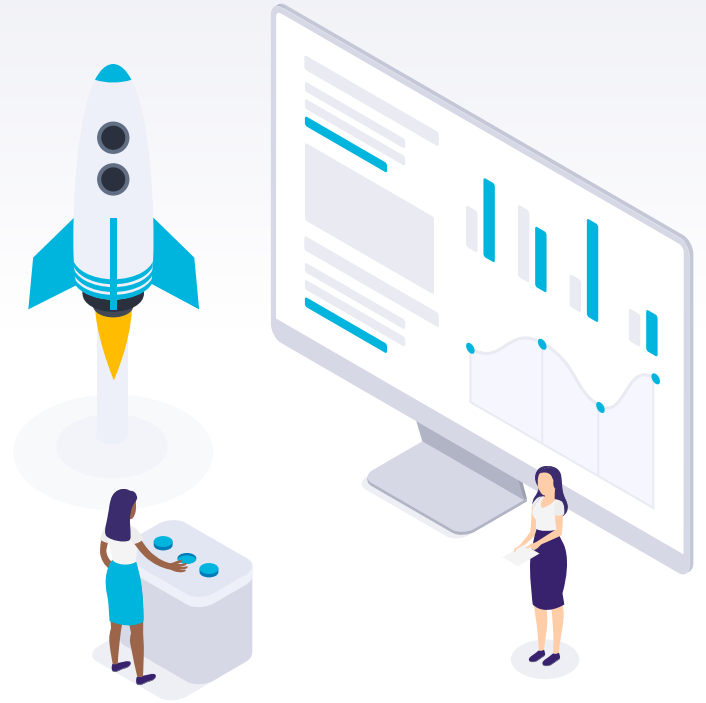


# ► Access reviews



# DEMO 7

## Access reviews



# Takk!

## Spørsmål?

Du finner meg her:

- Fortytwo.io
- goodworkaround.com
- [linkedin.com/in/mariusm/](https://www.linkedin.com/in/mariusm/)

