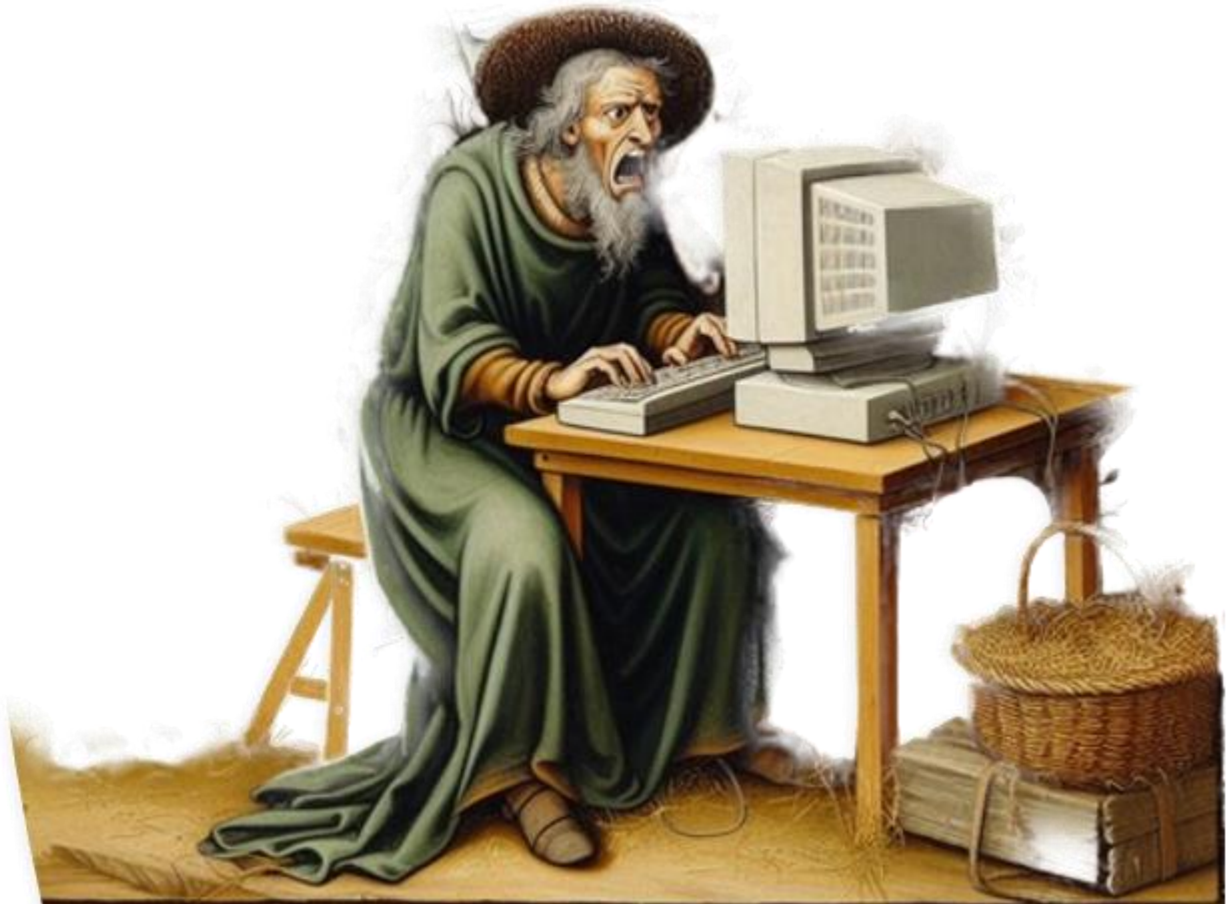
MC²

# MC2MC

## Privileged Identity Management: snowball from basic to advanced



# Louis Mastelinck

Security MVP

Microsoft Security Expert @Proximus NXT

🎙 Micromensen (oeps)

@LouisMastelinck

▶ Lousec

https://lousec.be

in Louis Mastelinck

# Permissions

Always ready

Full blown

Even for the minor changes

# Privileged Identity management

Microsoft Entra ID P2

Microsoft Entra ID Governance

# Permissions

Activate permissions when needed

Requirements

Logging, justification, ticket number

& approval

Avoid hidden administrators

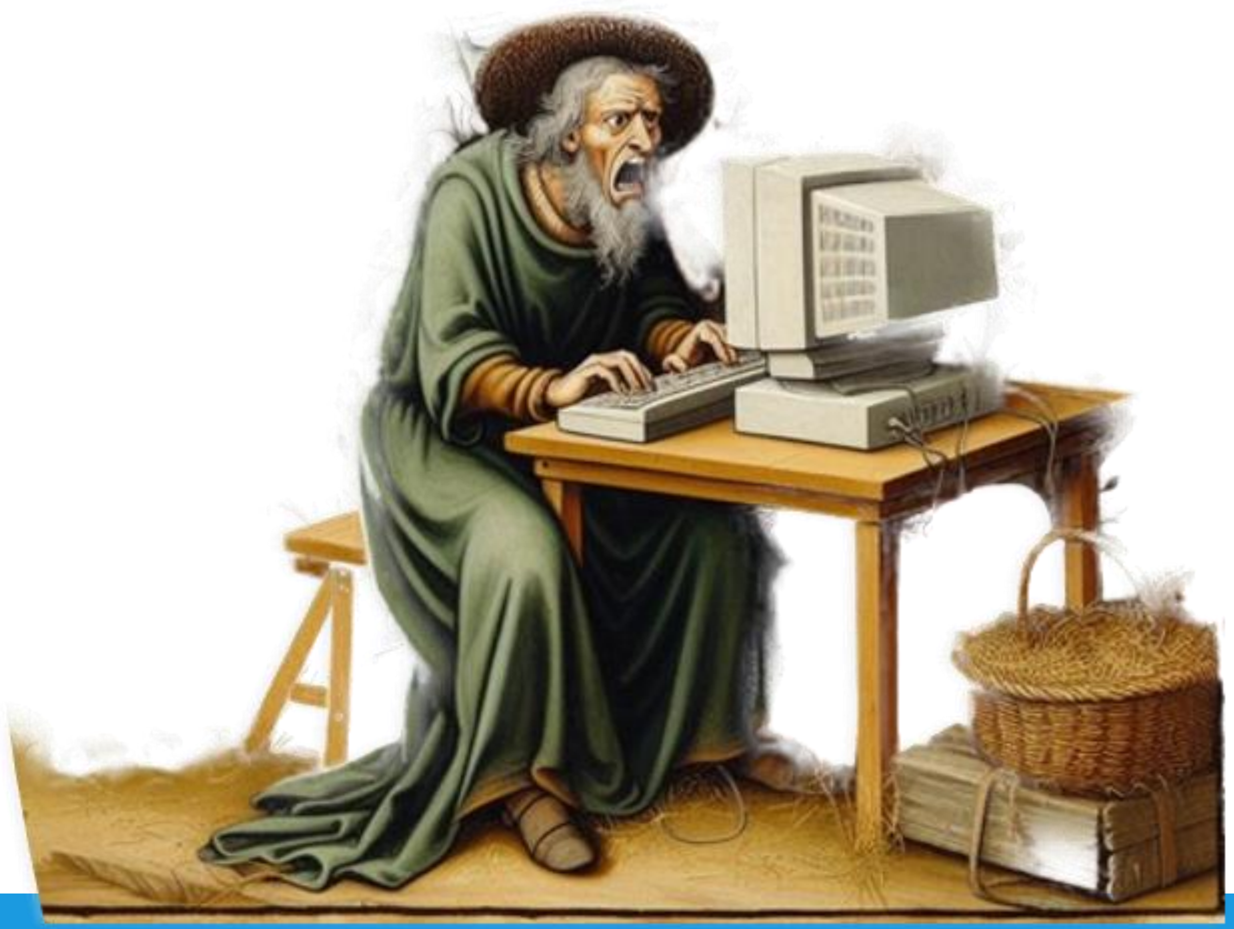
## ENTRA ID roles

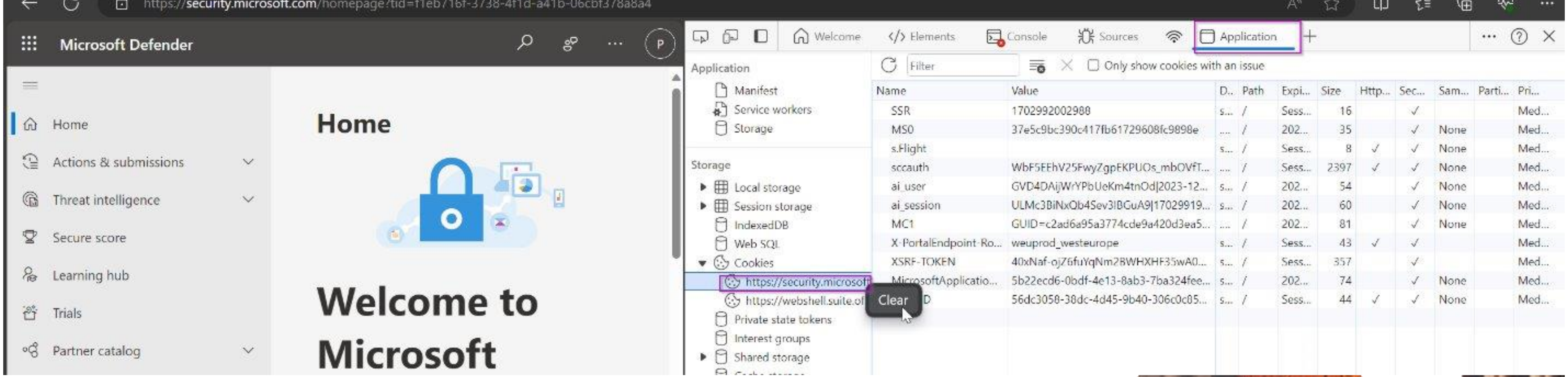
**PIM for groups**

**(Privileged access groups)**

**Azure**

# Basic demo





| Name | Value | D.. | Path | Expi... | Size | Http... | Sec... | Sam... | Parti... | Pri... |
|---|---|---|---|---|---|---|---|---|---|---|
| SSR | 1702992002988 | s... | / | Sess... | 16 | | ✓ | | | Med... |
| MS0 | 37e5c9bc390c417fb61729608fc9898e | .... | / | 202... | 35 | | ✓ | None | | Med... |
| s.Flight | | s... | / | Sess... | 8 | ✓ | ✓ | None | | Med... |
| sccauth | WbF5EEhV25FwyZgpEKPUOs_mbOVfT... | .... | / | Sess... | 2397 | ✓ | ✓ | None | | Med... |
| ai_user | GVD4DAijWrYPbUeKm4tnOd\|2023-12... | s... | / | 202... | 54 | | ✓ | None | | Med... |
| ai_session | ULMc3BiNxQb4Sev3IBGuA9\|17029919... | s... | / | 202... | 60 | | ✓ | None | | Med... |
| MC1 | GUID=c2ad6a95a3774cde9a420d3ea5... | .... | / | 202... | 81 | | ✓ | None | | Med... |
| X-PortalEndpoint-Ro... | weuprod_westeurope | s... | / | Sess... | 43 | ✓ | ✓ | | | Med... |
| XSRF-TOKEN | 40xNaf-ojZ6fuYqNm2BWHXHF35wA0... | s... | / | Sess... | 357 | | ✓ | | | Med... |
| MicrosoftApplicatio... | 5b22ecd6-0bdf-4e13-8ab3-7ba324fee... | s... | / | 202... | 74 | | ✓ | None | | Med... |
| D | 56dc3058-38dc-4d45-9b40-306c0c85... | s... | / | Sess... | 44 | ✓ | ✓ | None | | Med... |

# Common issue for beginners:
# Permissions don't load

M C 2

# The rules of PIM

Policies are per role

Having different scenario for the same role is hard:

Approval for person X yes

Approval for person Y no

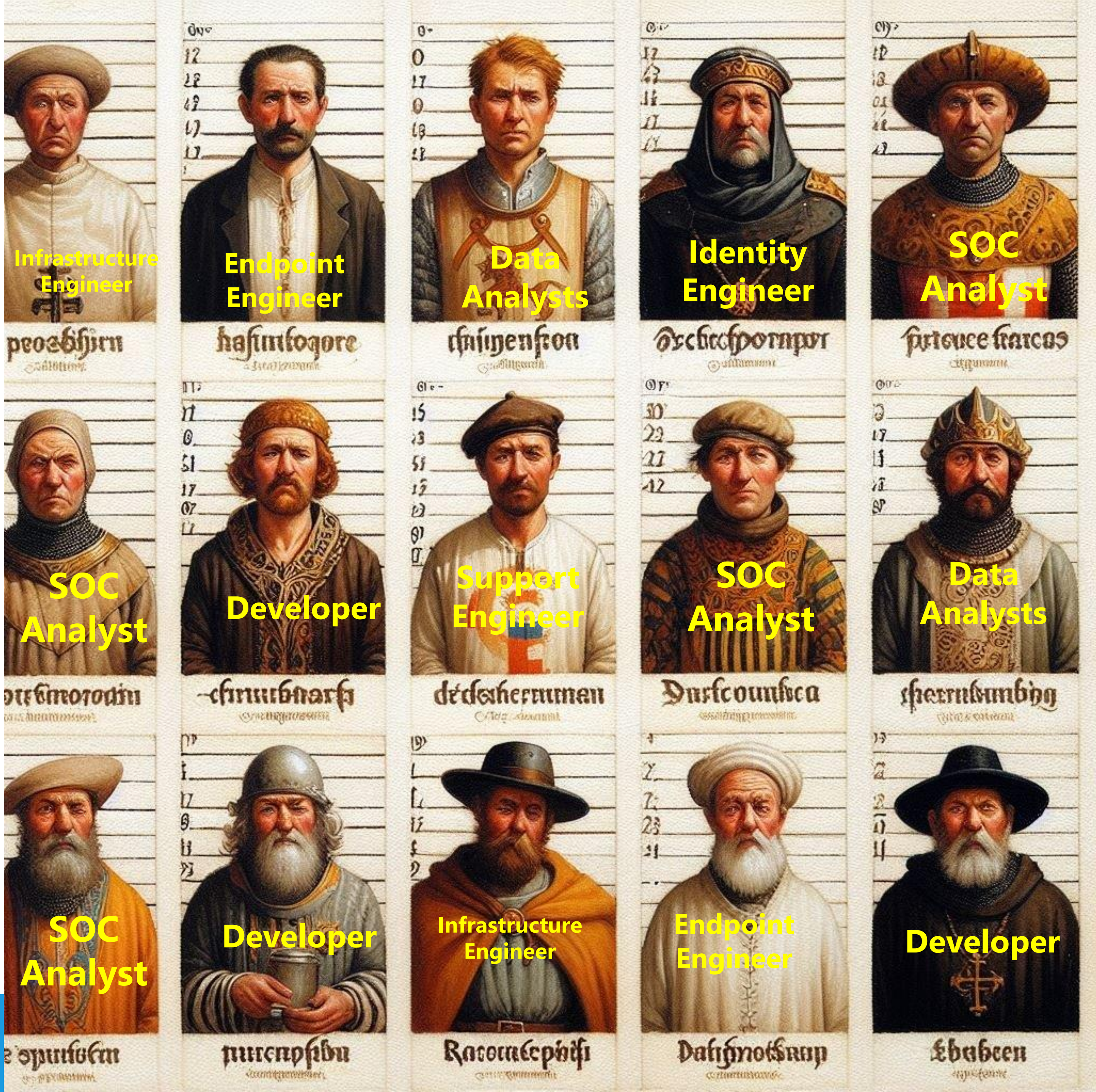
“You can be active for 8h, others for 3h”

# Magic with PIM for groups and roles

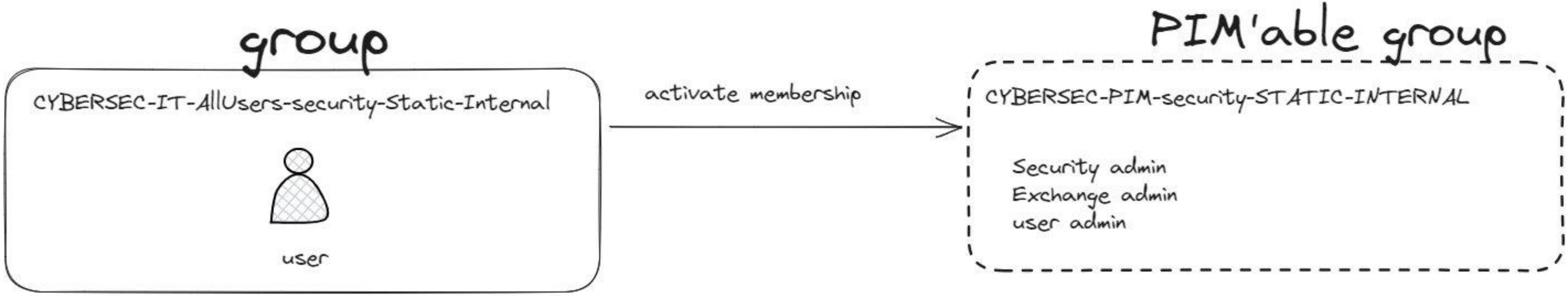
Create PIM group for each scenario

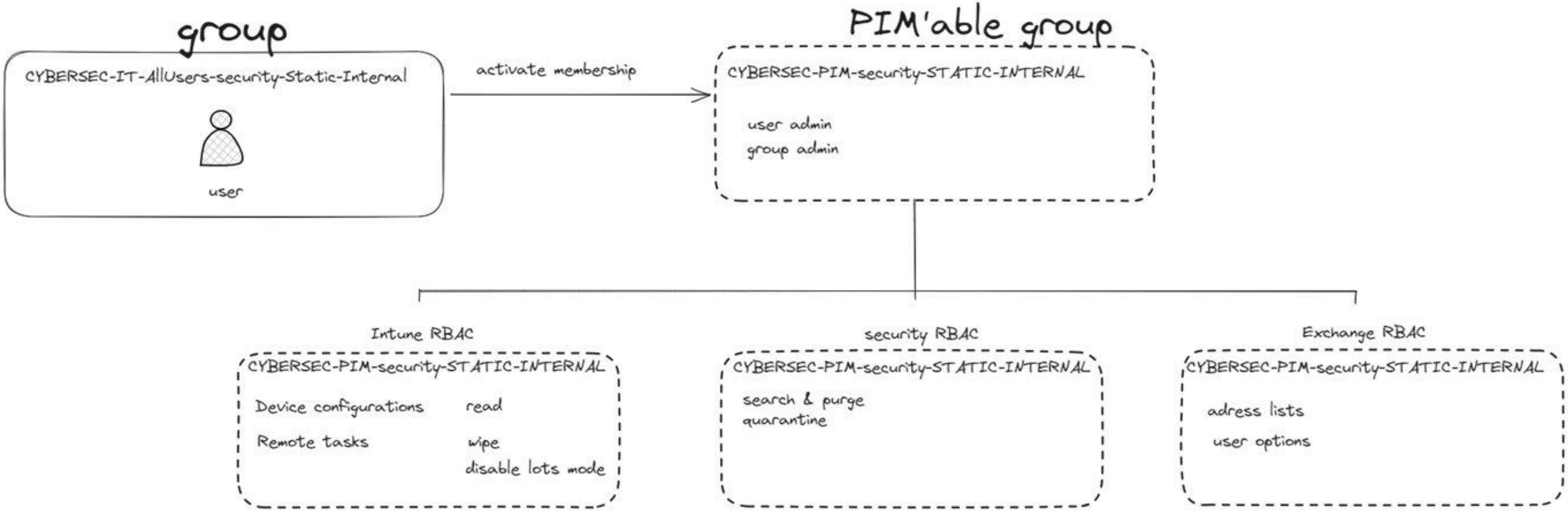
One PIM to activate them all

Duplicate a role to a custom role


Infrastructure Engineer
Endpoint Engineer
Data Analysts
Identity Engineer
SOC Analyst
SOC Analyst
Developer
Support Engineer
SOC Analyst
Data Analysts
SOC Analyst
Developer
Infrastructure Engineer
Endpoint Engineer
Developer

# Live demo time!


group
CYBERSEC-IT-AllUsers-security-Static-Internal
user
activate membership
PIM'able group
CYBERSEC-PIM-security-STATIC-INTERNAL
Security admin
Exchange admin
user admin



group

CYBERSEC-IT-AllUsers-security-Static-Internal

user

activate membership

PIM'able group

CYBERSEC-PIM-security-STATIC-INTERNAL

user admin

group admin

Intune RBAC

CYBERSEC-PIM-security-STATIC-INTERNAL

Device configurations read

Remote tasks wipe

disable lots mode

security RBAC

CYBERSEC-PIM-security-STATIC-INTERNAL

search & purge

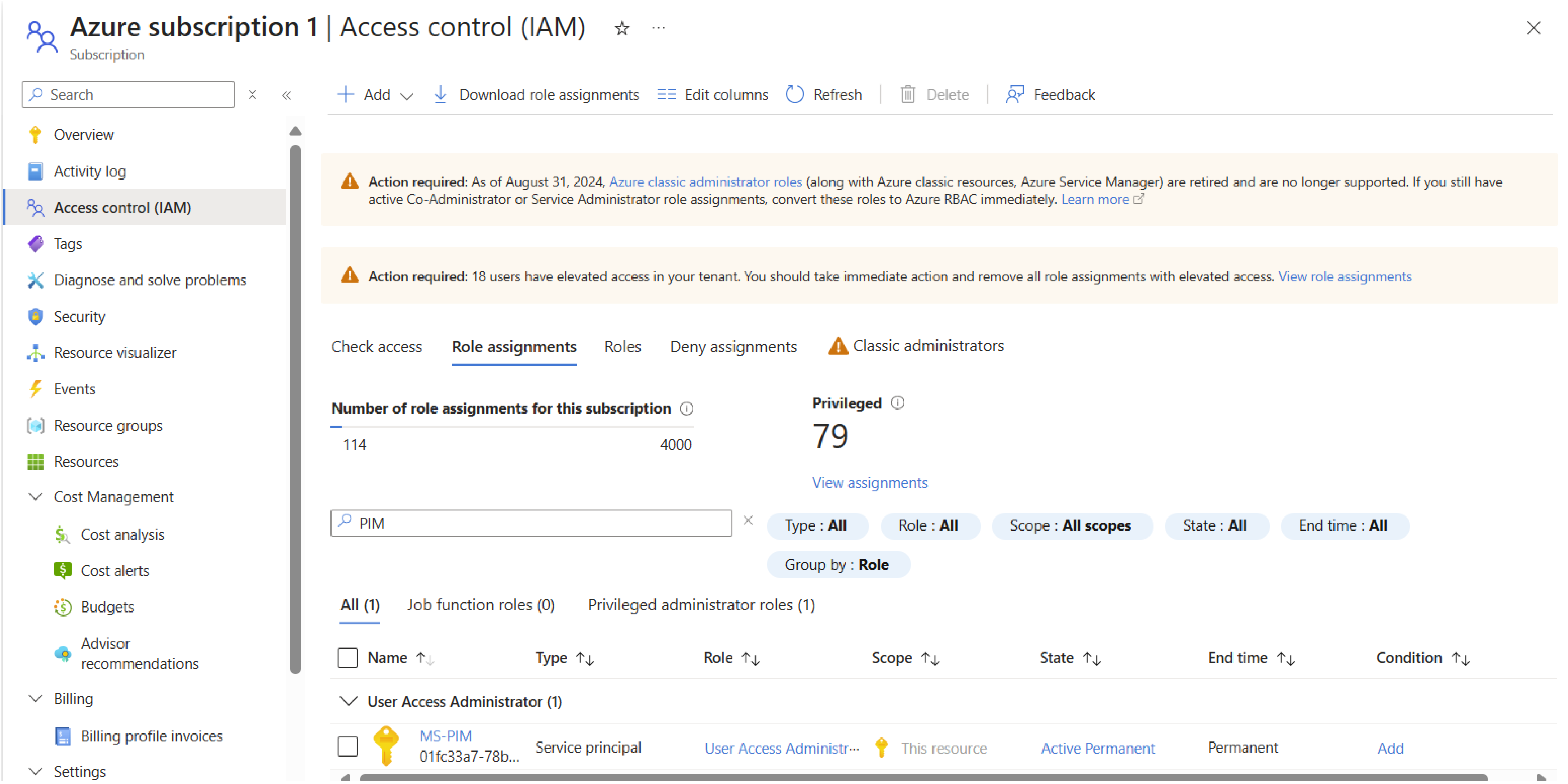
quarantine

Exchange RBAC

CYBERSEC-PIM-security-STATIC-INTERNAL

adress lists

user options



# Azure subscription 1 | Access control (IAM)

Subscription

**Action required:** As of August 31, 2024, Azure classic administrator roles (along with Azure classic resources, Azure Service Manager) are retired and are no longer supported. If you still have active Co-Administrator or Service Administrator role assignments, convert these roles to Azure RBAC immediately. Learn more

**Action required:** 18 users have elevated access in your tenant. You should take immediate action and remove all role assignments with elevated access. View role assignments

**Number of role assignments for this subscription**

114 4000

**Privileged**

79

View assignments

PIM

Type : **All** Role : **All** Scope : **All scopes** State : **All** End time : **All**

Group by : **Role**

| □ | Name | Type | Role | Scope | State | End time | Condition |
|---|---|---|---|---|---|---|---|
| | User Access Administrator (1) | | | | | | |
| □ | MS-PIM<br>01fc33a7-78b... | Service principal | User Access Administr... | This resource | Active Permanent | Permanent | Add |

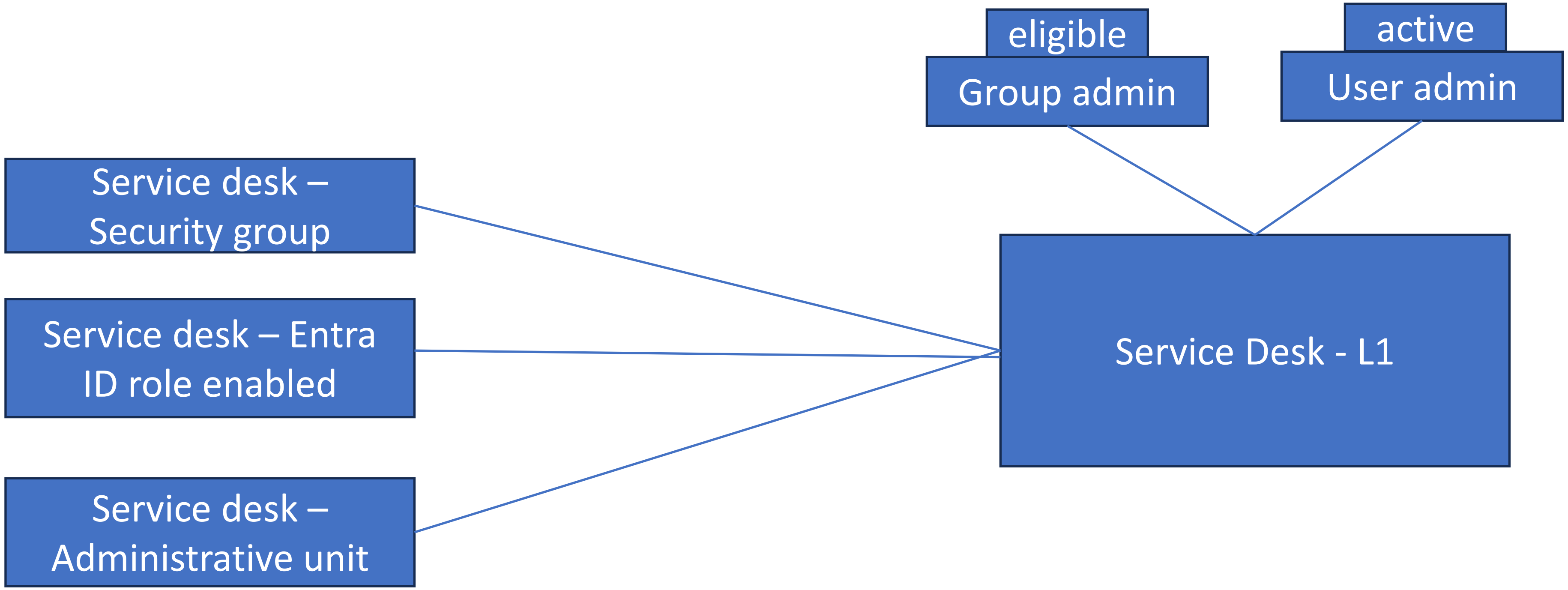
# Combine Conditional Access

PIM supports authentication context

# Making groups eligible can lead to privilege escalation

Group administrator

User administrator



eligible

Group admin

active

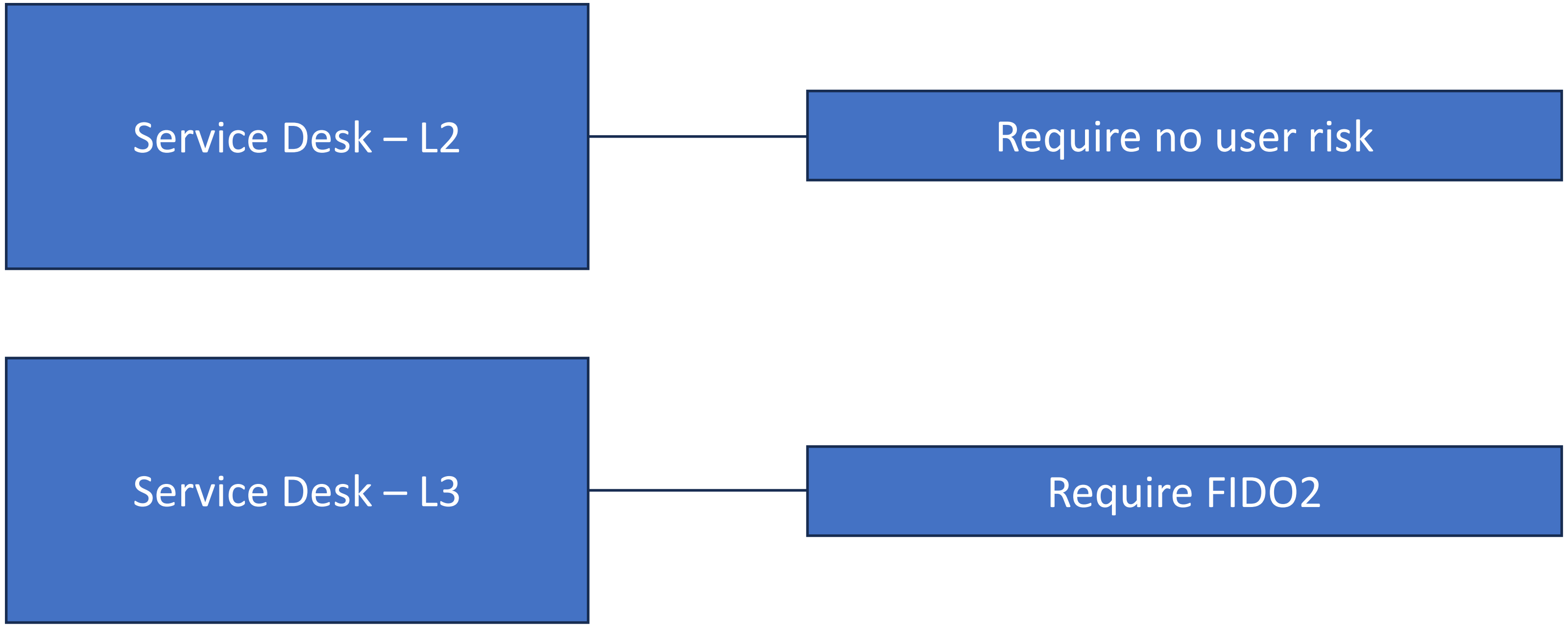
User admin

Service desk – Security group

Service desk – Entra ID role enabled

Service desk – Administrative unit

Service Desk - L1

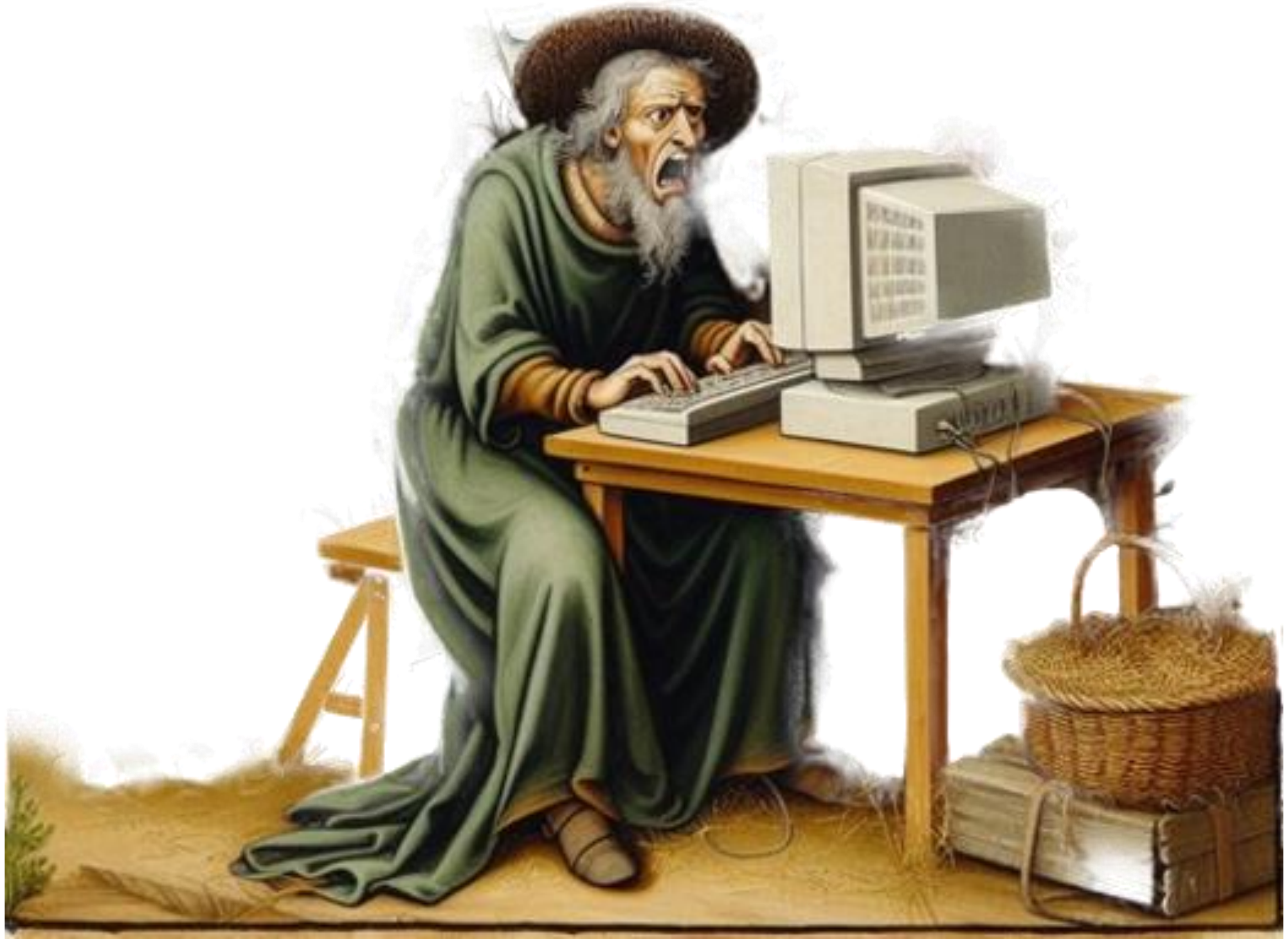


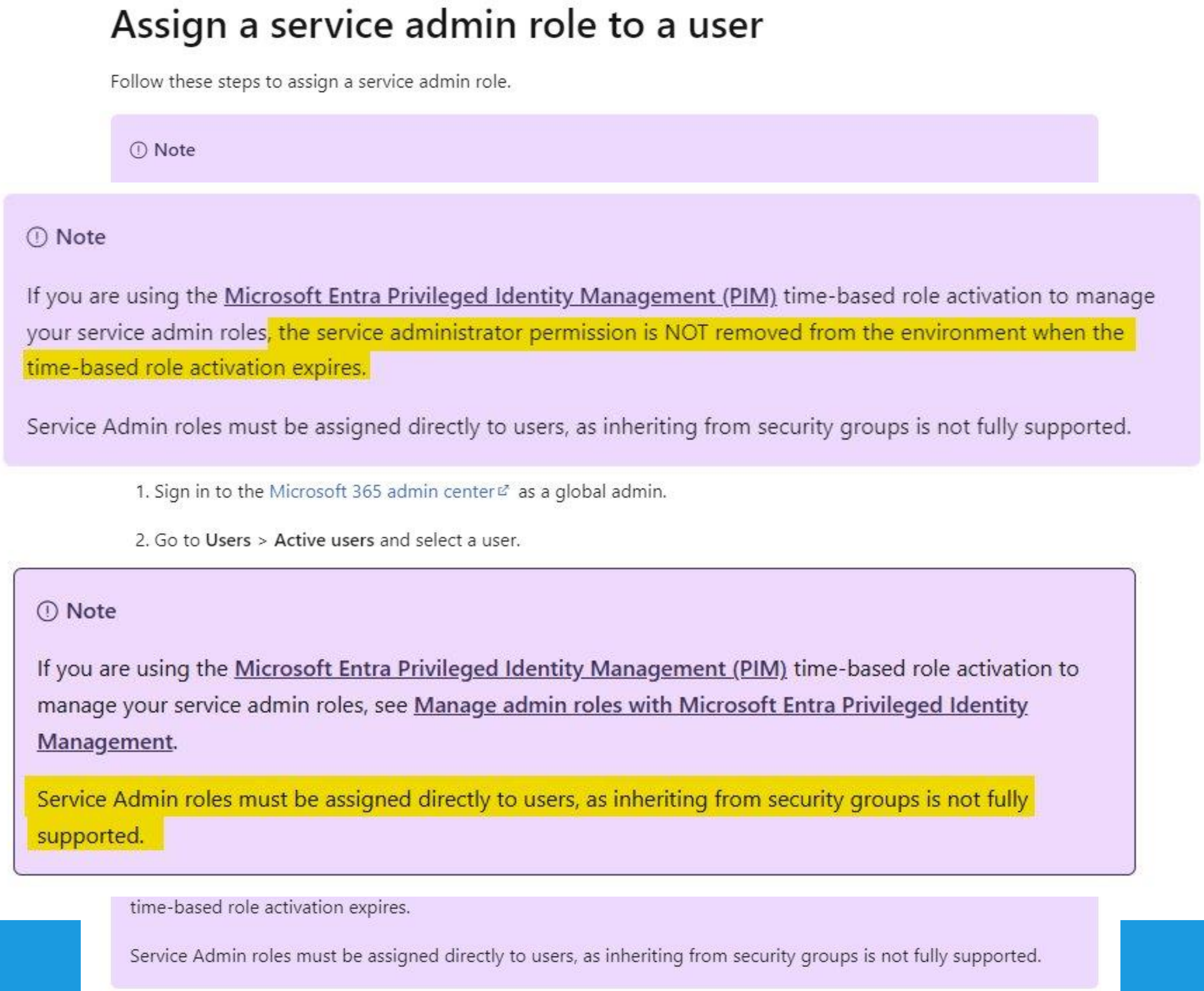
Service Desk – L2

Require no user risk

Service Desk – L3

Require FIDO2





# Assign a service admin role to a user

Follow these steps to assign a service admin role.

ⓘ Note

ⓘ Note

If you are using the Microsoft Entra Privileged Identity Management (PIM) time-based role activation to manage your service admin roles, the service administrator permission is NOT removed from the environment when the time-based role activation expires.

Service Admin roles must be assigned directly to users, as inheriting from security groups is not fully supported.

1. Sign in to the Microsoft 365 admin center as a global admin.
2. Go to **Users** > **Active users** and select a user.

ⓘ Note

If you are using the Microsoft Entra Privileged Identity Management (PIM) time-based role activation to manage your service admin roles, see Manage admin roles with Microsoft Entra Privileged Identity Management.

Service Admin roles must be assigned directly to users, as inheriting from security groups is not fully supported.

time-based role activation expires.

Service Admin roles must be assigned directly to users, as inheriting from security groups is not fully supported.

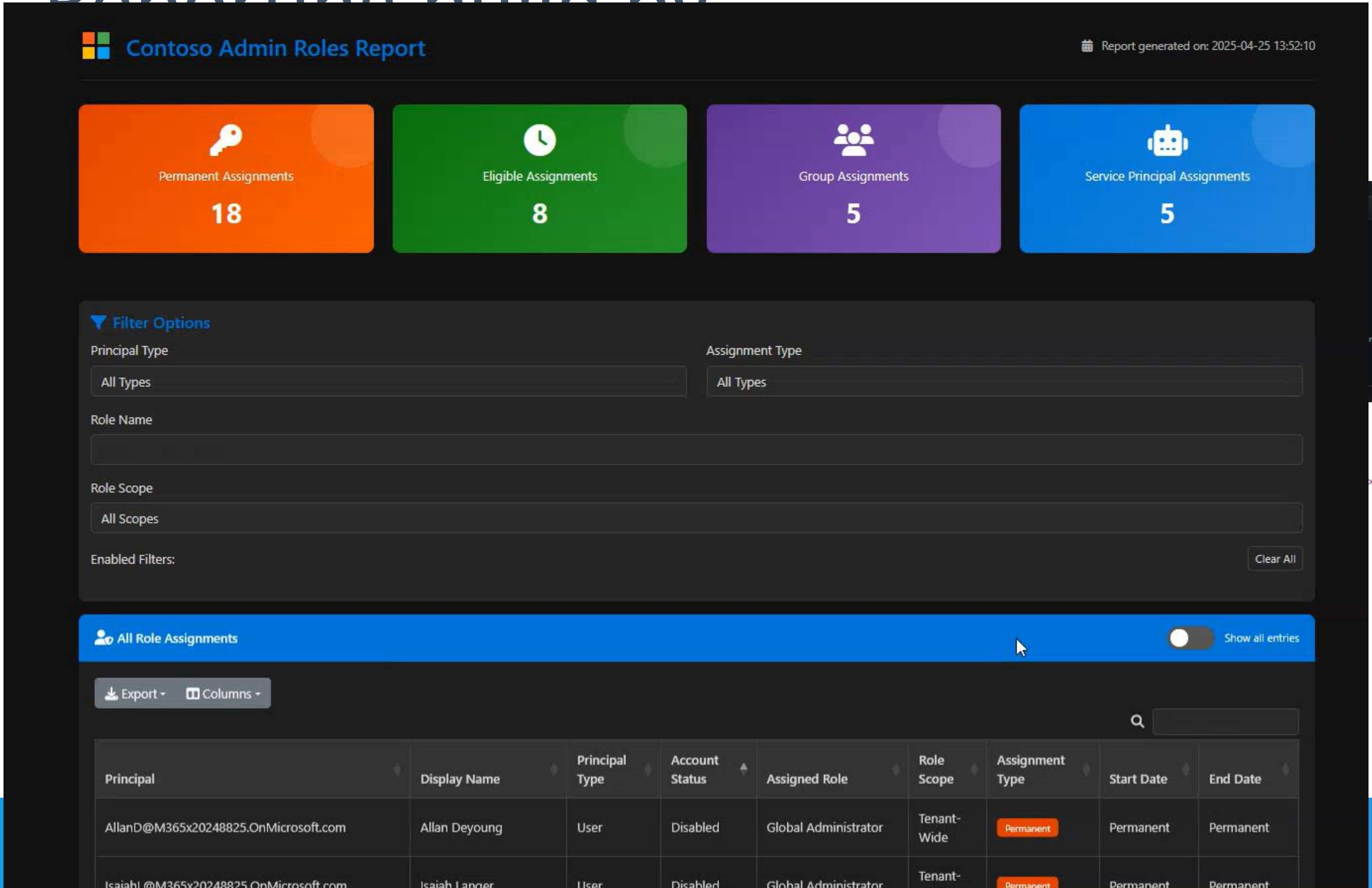
# Reporting is lacking

Reporting on individual users ✓

Reporting on the group ✓

Reporting on members of the group ✗

# Reporting build by



## Contoso Admin Roles Report

Report generated on: 2025-04-25 13:52:10

| Permanent Assignments | Eligible Assignments | Group Assignments | Service Principal Assignments |
|---|---|---|---|
| 18 | 8 | 5 | 5 |

**Filter Options**

Principal Type: All Types

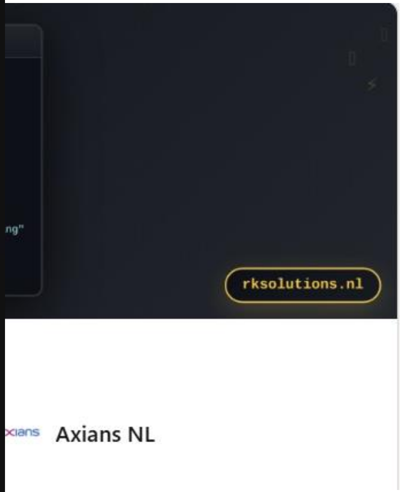
Assignment Type: All Types

Role Name:

Role Scope: All Scopes

Enabled Filters:

| Principal | Display Name | Principal Type | Account Status | Assigned Role | Role Scope | Assignment Type | Start Date | End Date |
|---|---|---|---|---|---|---|---|---|
| AllanD@M365x20248825.OnMicrosoft.com | Allan Deyoung | User | Disabled | Global Administrator | Tenant-Wide | Permanent | Permanent | Permanent |
| IsaiahL@M365x20248825.OnMicrosoft.com | Isaiah Langer | User | Disabled | Global Administrator | Tenant- | Permanent | Permanent | Permanent |



Axians NL

# Notes from field

Setting PIM up is not hard, handing it over is!

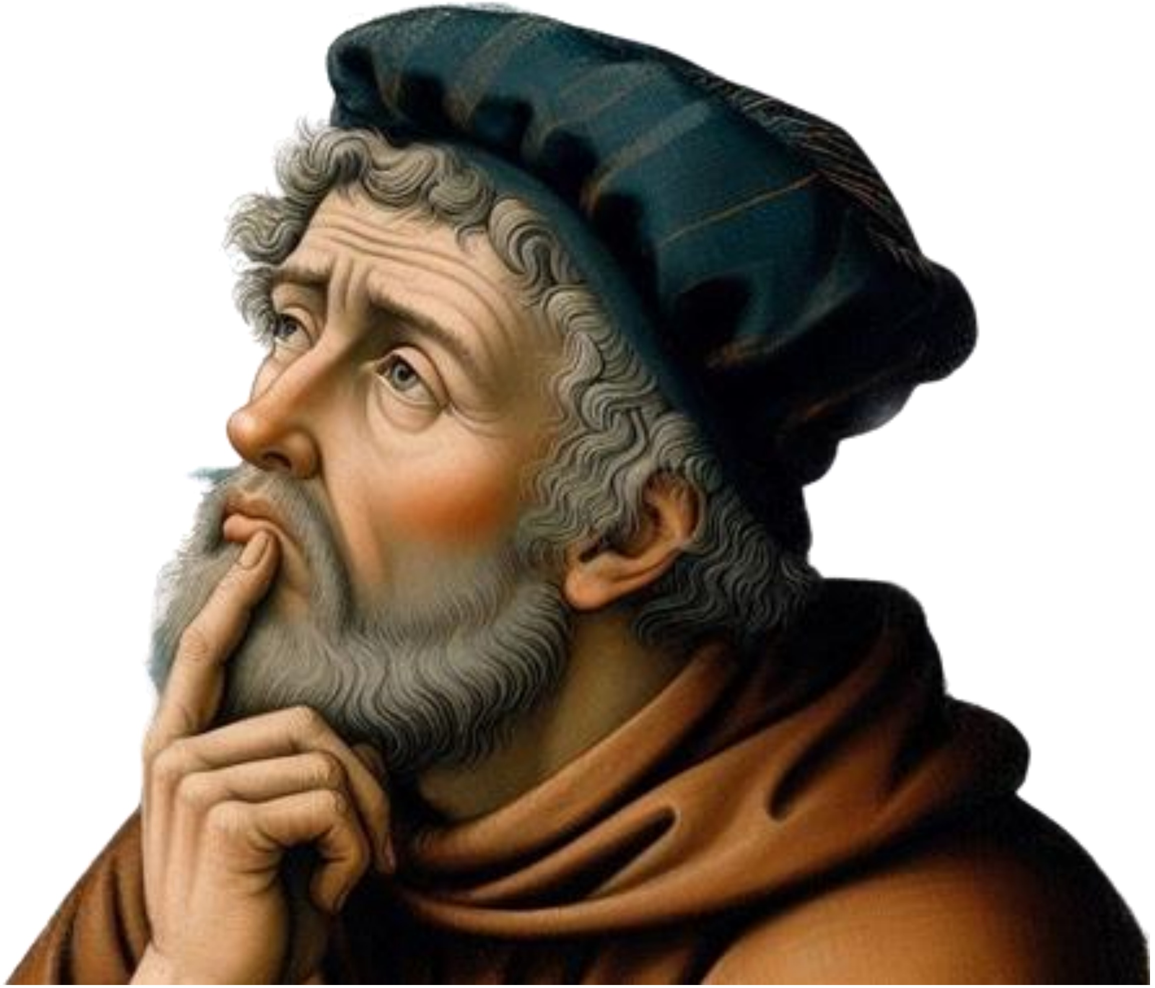
I don't use the built-in roles in RBAC portals

If needed make a copy

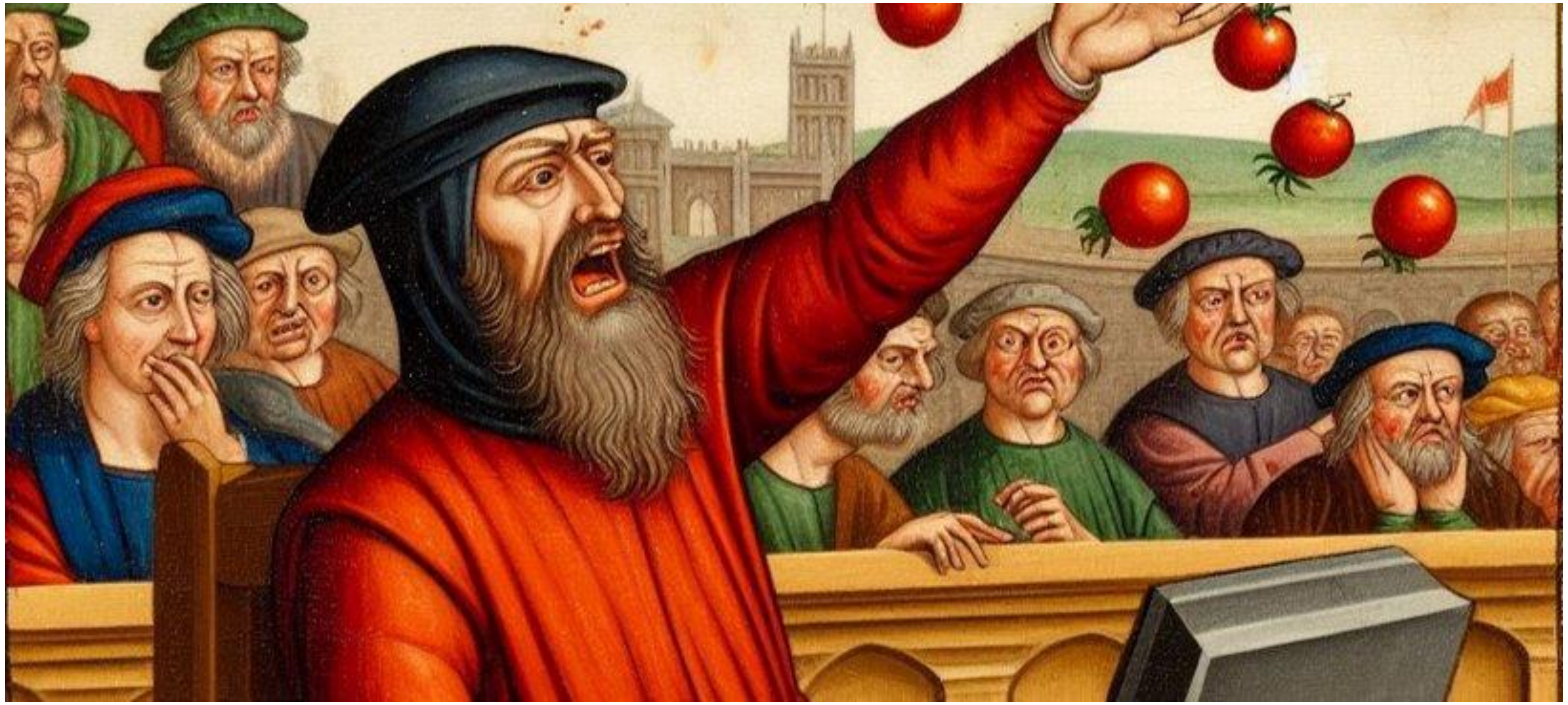
Naming convention matches with my PIM group:

Documentation reasons

Troubleshooting reasons



# Questions



# We would love to hear your feedback!

Session feedback available in home feed of the app after the session

run
events

# Thank You!

MC$^2$