Privileged Access Strategy - Best Practices and Common Mistakes when Tiering Cloud and AD

Morten Knudsen

Microsoft MVP Azure, Security & Security Copilot | Microsoft Certified Trainer

Cloud & Security Architect, freelance

How many roles do we have today in Entra ID and Azure ?

Date	6th April 2026	30th Jan 2026	9th June 2025	27th May 2024	Change in Last 10 months
Entra ID Roles	143	134	123	110	+20
Azure Roles	868	838	688	542	+180

Session Objective

- Inspiration of how to design cloud services with delegation levels & service RBACs “PIM v2” (Microsoft Enterprise Access Model & RAMP)
- Lessons learned – Pitfalls & Recommendations
- PIM for AD – using PIM for Entra ID ☺

Understanding the audience ☺

- Works with PIM design & implementation ?
- Experience with PIM Automations using IaC ?
- Use RBACs in your PIM designs already?
- Use Administrative Units in your PIM designs ?
- Knows about Microsoft Enterprise Access model with cloud tiering ?

Morten Knudsen

- Microsoft MVP Azure, Security & Security Copilot (triple-MVP)
- Freelance cloud & security architect, 2LINKIT
- Sold my 1st company (MindZet) in 2016 – 75 employees

Co-founder
Experts Live Denmark

Lead-organizer
#ELDK2025, #ELDK26

/in/knudsenmorten

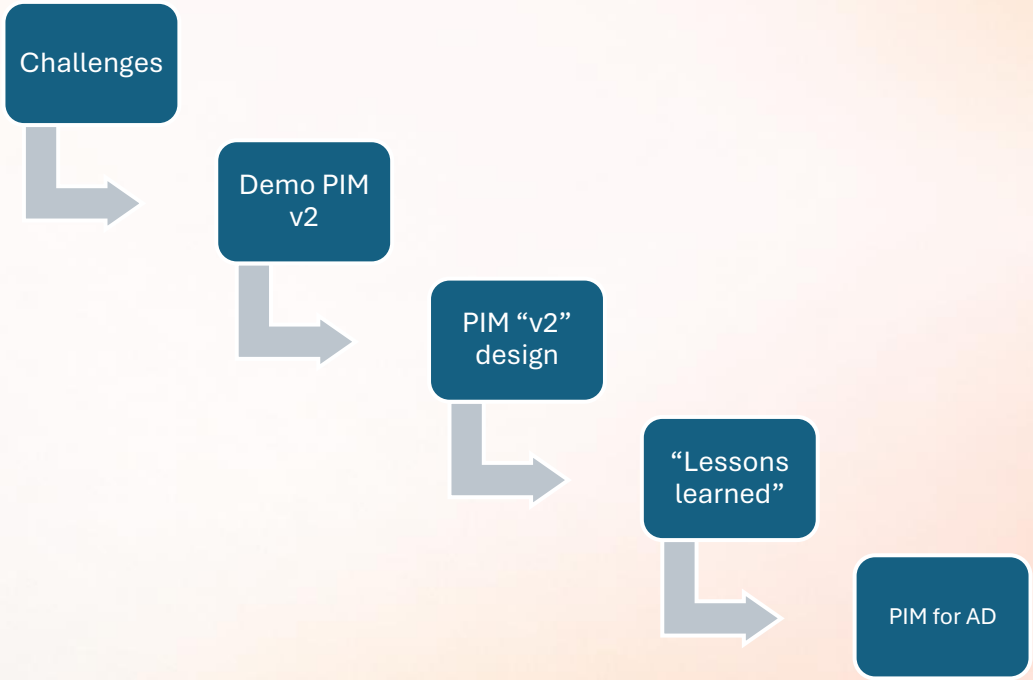
@mortenknudsen.net

@knudsenmortendk

aka.ms/morten

mok@mortenknudsen.net

Agenda


Challenges
Demo PIM v2
PIM “v2” design
“Lessons learned”
PIM for AD

RApid Modernization Plan (RAMP)

Quickly adopt Microsoft's recommended privileged access strategy

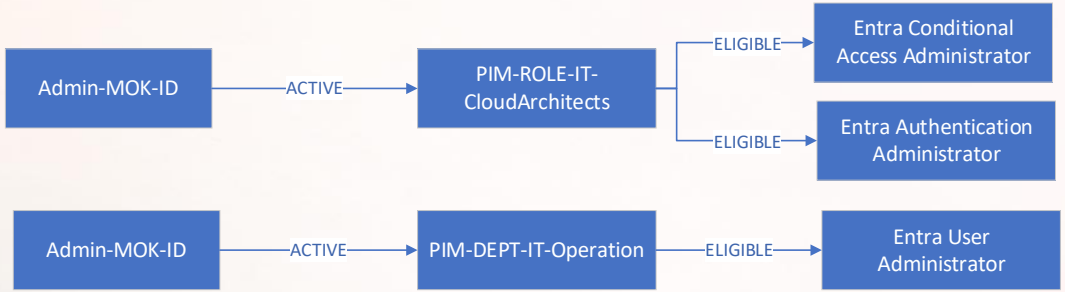
- **Separate and manage privileged accounts**
  - Emergency access accounts
  - Enable Entra ID Privileged Identity Management
  - Identify and categorize privileged accounts (Entra ID)
  - Separate accounts (On-premises AD accounts)
- **Monitoring of Active Directory**
  - Defender for Identity

- **Improve credential management experience**
  - Implement and document self-service password reset and combined security information registration
  - Protect admin accounts - Enable and require MFA / Passwordless for Entra ID privileged users
  - Block legacy authentication protocols for privileged user accounts
  - Application consent process
  - Clean up account and sign-in risks
- End-to-End Protection for Privileged Sessions
  - Admin workstations initial deployment

https://learn.microsoft.com/en-us/security/privileged-access-workstations/security-rapid-modernization-plan

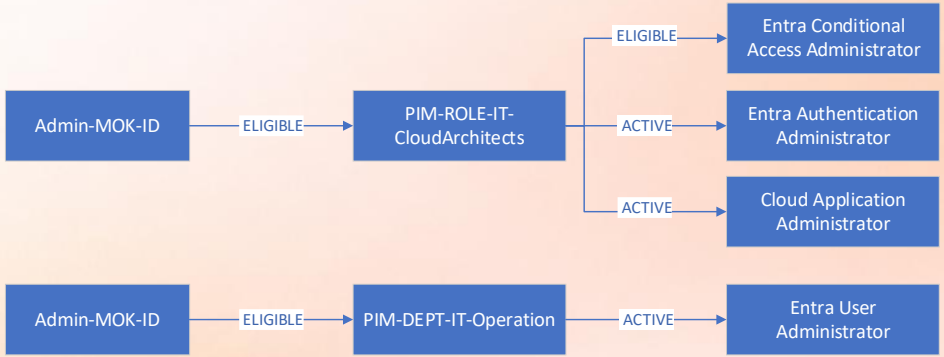
Challenges in early PIM designs

Forced to give too high/many permissions (tenantwide-permissions, project lifecycle) or had to use custom permissions



PIM v1 – "Just Enough, Just In Time" OnDemand Activation of Permission according to my Job-role

PIM v1 – Bundles / Compromise "Activate Job-role in the morning and get bundles of permissions"



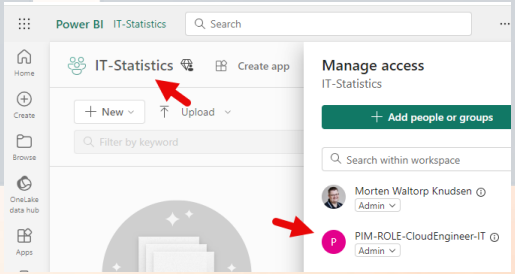
Challenges in early PIM designs

Missing RBACs

- Missing RBACs roles in individual services – or we didn't use them

Usage where ?

- Missing documentation of usage (Admin -> Role-group -> Delegation in app)



Delegation mis-configs

- Use of role groups for both internals and externals (consultants)
- Lack of Admin separation (Tier-1 Day2Day vs. Tier-0 = GA)

Challenges in early PIM designs

Scaling

- No focus on legacy system fx. AD – we focused on MS cloud – missing scale 1:N, multi-cloud
- Some systems have separate directory (no Entra integration) – “islands”

Onboarding

- Review process / no revoke – focus on assignments
- Lifecycle breaks -> Permissions expire - no license on admin account (no mail)
- Implementation completion lacked on all systems - focus on role (people) – instead of ‘per service’
- Confusions about groups (synced vs. cloud-only groups)

DEMO of PIM v2

Let’s start with lots of demos to understand concept ☺

Entra ID PIM Assignments using PIM v2 Framework

Admin:
App Registration
Role or Task

DEMO

My roles | Groups

Privileged Identity Management | My roles

Activate
- Microsoft Entra roles
- Groups
- Azure resources

Troubleshooting + Support
- Troubleshoot
- New support request

Refresh | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by role or group

Role	Group	Group type	Membership	End time
Member	PIM-Entra-ID-Bundle-GlobalRoles-L1-T0-CP-ID	Security	Direct	4/21/2026, 11:2
Member	PIM-ROLE-Management-IT-OperationSecurity	Security	Direct	5/21/2025, 5:44
Member	PIM-AD-GroupPolicyMgmt-Scoped-ClientsDevices-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41
Member	PIM-AD-GroupPolicyMgmt-Scoped-Servers-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41
Member	PIM-AD-GroupPolicyMgmt-Scoped-Users-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41
Member	PIM-AD-UserMgmt-Scoped-Users-L2-T0-CP-ID-S_AD	Security	Direct	4/5/2026, 4:31
Member	PIM-AD-DomainAdministrators-L1-T0-CP-ID-S_AD	Security	Direct	5/1/2026, 11:27
Member	PIM-AD-LocalServerAdmins-Scoped-L2-T0-CP-ID-S_AD	Security	Direct	5/10/2026, 11:2
Member	PIM-GDAP-Nunagreen-Entra-ID-GlobalAdministrator-L0-T0-CP-ID	Security	Direct	5/18/2026, 9:33
Member	PIM-GDAP-Nunagreen-Entra-ID-D365-BusinessCentralAdministrator-L1-T0-CP-ID	Security	Direct	4/26/2026, 3:57
Member	PIM-Entra-ID-SecurityAdministrator-L1-T0-CP-ID	Security	Group	4/1/2026, 8:25
Member	PIM-Entra-ID-PrivilegedAuthenticationAdministrator-L1-T0-CP-ID	Security	Group	4/1/2026, 8:25
Member	PIM-Entra-ID-AuthenticationPolicyAdministrator-L1-T0-CP-ID	Security	Group	4/1/2026, 8:25
Member	PIM-Entra-ID-LicenseAdministrator-L1-T0-CP-ID	Security	Group	4/1/2026, 8:25
Member	PIM-Entra-ID-BillingAdministrator-L1-T0-CP-ID	Security	Group	4/1/2026, 8:25
Member	PIM-Entra-ID-CloudApplicationAdministrator-L1-T0-CP-ID	Security	Group	4/1/2026, 8:25

g Ctrl+Shift+F

Use of Entra Administrative Units with PIM (Active)

Helpdesk:
Manage Corp Users

Note:
Cannot manage Admins, Guests, Service Accounts, Shared Device Users, BGAs, etc.

DEMO

My roles | Groups

Privileged Identity Management | My roles

Activate
- Microsoft Entra roles
- Groups
- Azure resources

Troubleshooting + Support

Refresh | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by role or group

Role	Group	Group type	Membership	State
Member	PIM-ROLE-Helpdesk-IT	Security	Direct	Assigned
Member	PIM-AD-ClientDevicesMgmt-Scoped-L2-T0-CP-ID-S_AD	Security	Direct	Assigned
Member	PIM-AD-GroupMgmt-Scoped-Groups-L2-T0-CP-ID-S_AD	Security	Direct	Assigned
Member	PIM-AD-GroupMembershipMgmt-Scoped-Groups-L2-T0-CP-ID-S_AD	Security	Direct	Assigned
Member	PIM-AD-UserMgmt-Scoped-Users-L2-T0-CP-ID-S_AD	Security	Direct	Assigned
Member	PIM-ORG-IT	Security	Direct	Assigned

pressing Ctrl+Shift+F

Use of Entra Administrative Units with PIM (Active)

Helpdesk:
Elevate to Tenant-wide User Mgmt (Service Accounts, Guests, Shared Device Users)

Note:
Cannot manage Admins, BGAs

DEMO

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | Admin-Helpdesk-ID@2l... 2LINKIT

Home > 2linkIT | Users > Users >

Info Screen 13 [DEMO]

User

Search

Edit properties | Delete | Refresh | Reset password | Revoke sessions | Manage view | Got feedback?

Overview | Monitoring | Properties

Basic info

I1

Info Screen 13 [DEMO]
Infopc13@mortenknudsen.net
Member

User principal name	Infopc13@mortenknudsen.net
Object ID	f4bf70e3-c03e-4613-ad2a-cc22fe68fc26
Created date time	Mar 16, 2025, 8:45 AM
User type	Member
Identities	myfamilynetwork.onmicrosoft.com

Group memberships	12
Applications	0
Assigned roles	0
Assigned licenses	2

My Feed

Account status
Enabled
Edit

B2B invitation
Convert to external user

Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request

Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks

Add or remove favorites by pressing Ctrl+Shift+F

2linkIT | Administrative units

- Overview
- Preview features
- Diagnose and solve problems
- Manage
  - Users
  - Groups
  - External Identities
  - Roles and administrators
  - Administrative units
  - Delegated admin partners
  - Enterprise applications
  - Devices
  - App registrations
  - Identity Governance
  - Application proxy

Add or remove favorites by pressing Ctrl+Shift+F

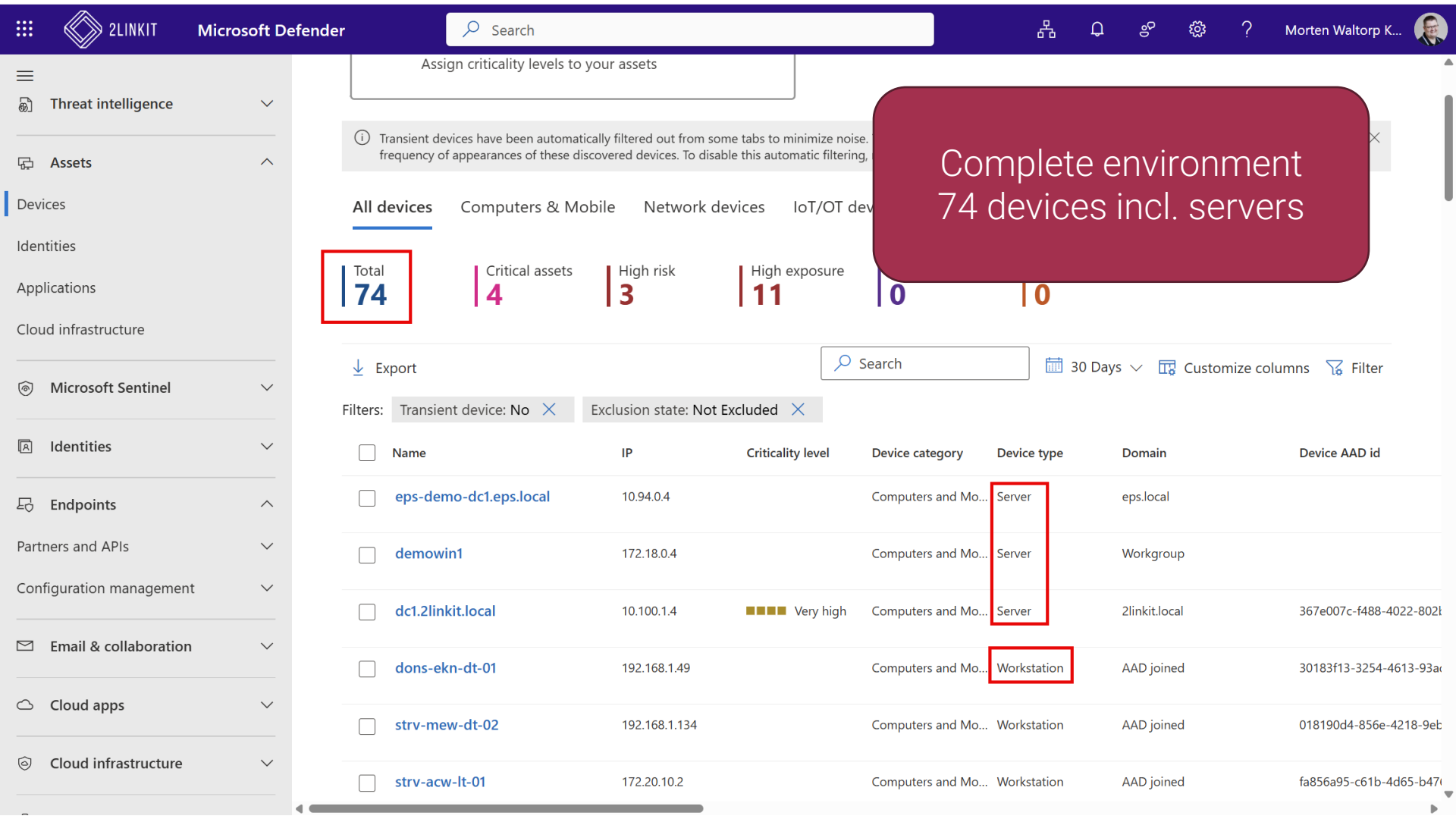
Learn more | Add | Delete | Refresh | Preview features | Got feedback?

Entra-CA-Policy-PilotGroups-HighPrivGroups	Pilot Groups for Entra CA P...	No	Assigned
Entra-CA-Policy-TargetGroups-HighPrivGroups	Target Groups for Entra CA ...	No	Assigned
Guests-Tenant-All	All guests, Tenant	No	Dynamic
PIM-Admins-L0-HighPriv	Admins-L0-HighPriv	No	Assigned
PIM-Admins-L1-L9	Admins-L1-L9	No	Assigned
PIM-Groups-L0-T0-HighPrivGlobalRoles	PIM-Groups-L0-T0-HighPriv...	No	Assigned
PIM-Groups-L1-T0-GlobalRoles	PIM-Groups-L1-T0-GlobalR...	No	Assigned
PIM-Groups-L2	PIM-Groups-L2	No	Assigned
PIM-Groups-ORGANIZATION	PIM-Groups-ORGANIZATION	No	Assigned
PIM-Groups-ROLES	PIM-Groups-ROLES	No	Assigned
PIM-Groups-T1	PIM-Groups-T1	No	Assigned
PIM-Groups-T2	PIM-Groups-T2	No	Assigned
Users-Corp-All	All users, Corp	No	Dynamic
Users-Corp-External	External users, Corp	No	Dynamic
Users-Corp-Internal	Internal users, Corp	No	Dyn
Users-Tenant-All	All users, Tenant	No	Dyn

Defender RBAC Permissions for Helpdesk

Helpdesk:
See Clients Only &
Isolate Devices Only

DEMO


2LINKIT
Microsoft Defender
Search
Morten Waltorp K...
Assign criticality levels to your assets
Threat intelligence
Assets
Devices
Identities
Applications
Cloud infrastructure
Microsoft Sentinel
Identities
Endpoints
Partners and APIs
Configuration management
Email & collaboration
Cloud apps
Cloud infrastructure
Transient devices have been automatically filtered out from some tabs to minimize noise.
frequency of appearances of these discovered devices. To disable this automatic filtering,
Complete environment
74 devices incl. servers
All devices
Computers & Mobile
Network devices
IoT/OT dev
Total
74
Critical assets
4
High risk
3
High exposure
11
0
0
Export
Search
30 Days
Customize columns
Filter
Filters:
Transient device: No
Exclusion state: Not Excluded
Name
IP
Criticality level
Device category
Device type
Domain
Device AAD id
eps-demo-dc1.eps.local
10.94.0.4
Computers and Mo...
Server
eps.local
demowin1
172.18.0.4
Computers and Mo...
Server
Workgroup
dc1.2linkit.local
10.100.1.4
Very high
Computers and Mo...
Server
2linkit.local
367e007c-f488-4022-802
dons-ekn-dt-01
192.168.1.49
Computers and Mo...
Workstation
AAD joined
30183f13-3254-4613-93a
strv-mew-dt-02
192.168.1.134
Computers and Mo...
Workstation
AAD joined
018190d4-856e-4218-9eb
strv-acw-lt-01
172.20.10.2
Computers and Mo...
Workstation
AAD joined
fa856a95-c61b-4d65-b47

Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Learning hub
Trials
Partner catalog
Assets
Devices
Endpoints
Partners and APIs

Device Inventory

Create rules for devices

Transient devices have been automatically filtered out from some tabs to minimize noise. This filtering is determined by an internal algorithm, which mainly depends on the frequency of appearances of these discovered devices. To disable this automatic filtering, navigate to the filter menu.

All devices | Computers & Mobile | Network devices | IoT/OT devices | Uncategorized devices

Total	Critical assets	High risk	High exposure	Not onboarded	Newly discovered
34	1	2	8	0	0

Export | Search | 30 Days | Customize columns | Filter

Filters: Tags: MDE_Supported | Transient device: No | Exclusion state: Not Excluded

Name	IP	Criticality level	Device category	Device type	Domain	Device AAD id	Risk le
dons-ekn-dt-01	192.168.1.49		Computers and Mo...	Workstation	AAD joined	30183f13-3254-4613-93ad-027328468bf1	
strv-mew-dt-02	192.168.1.134		Computers and Mo...	Workstation	AAD joined	018190d4-856e-4218-9eb7-c862f695cecb	
strv-acw-lt-01	172.20.10.2		Computers and Mo...	Workstation	AAD joined	fa856a95-c61b-4d65-b476-7fd1cefcefc4	
cpc-demos-hm99h	10.100.4.4		Computers and Mo...	Workstation	AAD joined	bf7dc23a-ede4-46b8-8589-14bfc6f5822f	
tomsdesktop	192.168.12.128		Computers and Mo...	Workstation	Workgroup	e066a676-a3b7-4e91-a17e-8e8df6b08747	
demo-pi6x7vfclz	10.100.7.6		Computers and Mo...	Workstation	AAD joined	e5dad30d-18db-4bd7-8151-c0b7c47fce16	

Defender RBAC with PIM – with Device Group scoping

Helpdesk:
Activate Security
Operations on Clients

DEMO

Eligible Assignment -> PIM-Defender-XDR-SecurityPosture-Operator-Scope-Clients-L3-T1-MP-ID

My roles | Groups

Privileged Identity Management | My roles

Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support

Refresh | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by role or group

Role	Group	Group type	Membership	End time
Member	PIM-ROLE-Helpdesk-TenantWide-IT	Security	Direct	6/1/2025, 12:07:49
Member	PIM-Defender-XDR-SecurityPosture-Operator-Scope-Clients-L3-T1-MP-ID	Security	Group	4/1/2026, 8:36:43 P
Member	PIM-Defender-XDR-SecurityOperations-Operator-Scope-Clients-L3-T1-MP-ID	Security	Group	4/5/2026, 10:03:22
Member	PIM-Entra-ID-LicenseAdministrator-L1-T0-CP-ID	Security	Group	4/5/2026, 2:08:46 P
Member	PIM-Entra-ID-Guests-Create-L1-T0-CP-ID	Security	Group	4/8/2026, 5:54:53 P
Member	PIM-Entra-ID-Users-CreateModifyDelete-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:01 P
Member	PIM-Entra-ID-Users-Profile-Photo-People-Update-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:03 P
Member	PIM-Entra-ID-Users-License-AssignRevoke-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:04 P
Member	PIM-Entra-ID-Users-GroupMembership-Manage-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:26 P
Member	PIM-Entra-ID-Users-Sessions-Revoke-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:38 P
Member	PIM-Entra-ID-Users-Sessions-LimitedAdmins-Revoke-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:39 P
Member	PIM-Entra-ID-Users-UPN-LimitedAdmins-Update-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:40 P
Member	PIM-Entra-ID-Users-Password-Reset-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:42 P
Member	PIM-Entra-ID-Groups-CreateModifyDelete-L1-T0-CP-ID	Security	Group	4/8/2026, 5:55:44 P
Member	PIM-Intune-ApplicationManager-L3-T1-WDP-ID	Security	Group	5/18/2026, 7:51:23
Member	PIM-Entra-ID-CA-NamedLocations-Read-L1-T0-CP-ID	Security	Group	4/8/2026, 5:56:18 P

Cloud apps
Cloud infrastructure
Cases
SOC optimization
Reports
Learning hub
Trials
More resources
System
Audit
Data management
Permissions
Health
Settings

Settings

8 items

Name	Description
Microsoft Defender portal	General settings for the Microsoft Defender portal
Microsoft Defender XDR	General settings for Microsoft Defender XDR
Endpoints	General settings for endpoints
Email & collaboration	General settings for email & collaboration
Identities	General settings for identities
Device discovery	Select your device discovery mode and customize standard discovery settings
Cloud Apps	General settings for cloud apps
Microsoft Sentinel	General settings for Microsoft Sentinel

Intune RBAC Permissions for Helpdesk

Helpdesk:
Elevate to Intune
Application Manager
to Add New App

DEMO

Active Assignment -> PIM-Intune-ApplicationManager-L3-T1-WDP-ID

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Intune roles | All roles

Microsoft Intune

Search

Manage
All roles
Scope tags
Administrator Licensing
Monitor
My permissions
Roles by permission
Admin permissions
Help and support
Help and support

Create | Refresh | Export | Columns | 10 items

Search

Name	Type	Description
Policy and Profile manager	Built-in Role	Policy and Profile Managers manage compliance policy, configuration profiles, Apple enrollment, Android Enterprise enrollment profiles and corporate device identifiers.
School Administrator	Built-in Role	School Administrators can manage apps and settings for their groups. They can take remote actions on devices, including remotely locking them, restarting them, and retiring them from management.
Endpoint Privilege Reader	Built-in Role	Endpoint Privilege Readers can view Endpoint Privilege Management (EPM) policies in the Intune console.
Help Desk Operator	Built-in Role	Help Desk Operators

Azure DevOps RBAC delegation using PIM

Developer:
Elevate as Project Administrator on Azure DevOps Project

DEMO

Eligible Assignment -> PIM-AzDevOps-2linkit-Contoso-FirewallHub-Platform-Connectivity-ProjectAdministrators-L4-T1-WDP-ID

Azure DevOps

Search

MK

2 2linkit

New organization

You have been assigned Stakeholder access and will experience limited features in Azure DevOps. Learn more

2linkit

Projects | My work items | My pull requests

Filter projects

C Contoso-FirewallHub-Platform-Connec...

Power BI RBAC delegation using PIM

Data Admin:
Power BI Workspace

DEMO

Eligible Assignment -> PIM-PowerBI-WS-MyCompanyKPIs-Prod-Admins-L3-T1-WDP-ID

Power BI MyCompanyKPIs-Prod

Search

MyCompanyKPIs-Prod

Workspace settings

New item | New folder | Import | Migrate | Filter by keyword | Filter

Add

Collect data
Get data
No items
New item

Store data
Store data
No items
New item

Create visualizations
Visualize data
No items
New item

Track data
Track data
No items
New item

Basic data analytics
Task flow details
Follow these steps to obtain your batch data, store it in a warehouse, process the data, build a semantic model, and finally use the results to create quick insights through visualizations.
Edit
Tasks

Name	Type	Task	Owner	Refreshed	Next refresh	Endorsement	Sensitivity
Weekly Sales	Dashboard	—	MyCompanyKP...	—	—	—	—

Azure Resources RBAC delegation using PIM

Admin:
Azure Resources

DEMO

Eligible Assignment -> PIM-AzRes-2LINKIT-Owner-L1-T1-WDP-ID

My roles | Azure resources

Privileged Identity Management | My roles

Activate
- Microsoft Entra roles
- Groups
- Azure resources

Troubleshooting + Support
- Troubleshoot
- New support request

Refresh | Open in mobile | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by role or resource

Role	Resource	Resource type	Membership	Condition	State	End time	Action
Owner	Platform	Management group	Group	None	Assigned	7/20/2025, 11:26:35 ...	Deactiva

g Ctrl+Shift+F

Partner Center GDAP delegation with PIM

Partner:
Activate GDAP Role
Access at Customer

DEMO

Eligible Assignment -> PIM-GDAP-Nunagreen-Entra-ID-D365-BusinessCentralAdministrator-L1-T0-CP-ID

Service management
Service requests

Please enable Auto Extend using Partner Center UI or API for needed MLT GDAPs nearing their expiration to ensure uninterrupted business continuity.

Nunagreen | Service Management

Lists AOBO (Admin On Behalf Of) links to different workloads and links to Service Health.

Administer Services

If you don't see a link to administer the desired service, click here to find out why.

Microsoft Entra ID

Dynamics 365 Business Central

Microsoft Intune

Exchange

Lifecycle Services

Microsoft 365

Microsoft 365 Compliance

Microsoft 365 Defender (Use for GDAP relationships only)

Microsoft 365 Lighthouse

Microsoft Azure Management Portal

Power BI

Power Platform

Teams

Service Health

PIM for AD | Local Server Permissions

Admin:
Elevate With Local Server Admin Permissions

NOTE: No AD Domain Permissions

DEMO

Eligible Assignment -> PIM-AD-LocalServerAdmins-Scoped-L2-T0-CP-ID-S_AD

My roles - Microsoft Azure

My roles - Microsoft Azure

portal.azure.com/?feature.msaljs=true#view/Microsoft_Azure_PIMCommon/ActivationMenuBlade/~/aadgroup/provider/aadgroup

PIM | Power BI | AzDevOps | Intune

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | Admin-MOK-ID@2linkit... 2LINKIT

Home > My roles

My roles | Groups

Privileged Identity Management | My roles

Refresh | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by role or group

Role	Group	Group type	Membership	End time	Action
Member	PIM-Entra-ID-Bundle-GlobalRoles-L1-T0-CP-ID	Security	Direct	4/21/2026, 11:28:02 ...	Activate | Extend
Member	PIM-ROLE-Management-IT-OperationSecurity	Security	Direct	5/21/2025, 5:44:53 PM	Activate | Extend
Member	PIM-AD-GroupPolicyMgmt-Scoped-ClientsDevices-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41:32 AM	Activate | Extend
Member	PIM-AD-GroupPolicyMgmt-Scoped-Servers-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41:33 AM	Activate | Extend
Member	PIM-AD-GroupPolicyMgmt-Scoped-Users-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41:34 AM	Activate | Extend
Member	PIM-AD-UserMgmt-Scoped-Users-L2-T0-CP-ID-S_AD	Security	Direct	4/5/2026, 4:31:49 PM	Activate | Extend
Member	PIM-AD-DomainAdministrators-L1-T0-CP-ID-S_AD	Security	Direct	5/1/2026, 11:27:31 PM	Activate | Extend
Member	PIM-AD-LocalServerAdmins-Scoped-L2-T0-CP-ID-S_AD	Security	Direct	5/10/2026, 11:25:53 ...	Activate | Extend
Member	PIM-GDAP-Nunagreen-Entra-ID-GlobalAdministrator-L0-T0-CP-ID	Security	Direct	5/18/2026, 9:33:00 AM	Activate | Extend
Member	PIM-GDAP-Nunagreen-Entra-ID-D365-BusinessCentralAdministrator-L1-T0-CP-ID	Security	Direct	4/26/2026, 3:57:42 PM	Activate | Extend

11.41
18/05/2025

PIM for AD | Domain Admin Permissions

Admin:
Elevate With Domain Admin Permissions

DEMO

Eligible Assignment -> PIM-AD-DomainAdministrators-L1-T0-CP-ID-S_AD

My roles - Microsoft Azure

My roles - Microsoft Azure

portal.azure.com/?feature.msaljs=true#view/Microsoft_Azure_PIMCommon/ActivationMenuBlade/~/aadgroup/provider/aadgroup

PIM | Power BI | AzDevOps | Intune

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | Admin-MOK-ID@2linkit... 2LINKIT

Home > Privileged Identity Management > My roles

My roles | Groups

Privileged Identity Management | My roles

Refresh | Got feedback?

Your active assignments have changed. Click here to view your active assignments →

Eligible assignments | Active assignments | Expired assignments

Search by role or group

Role	Group	Group type	Membership	End time	Action
Member	PIM-Entra-ID-Bundle-GlobalRoles-L1-T0-CP-ID	Security	Direct	4/21/2026, 11:28:02 ...	Activate | Extend
Member	PIM-ROLE-Management-IT-OperationSecurity	Security	Direct	5/21/2025, 5:44:53 PM	Activate | Extend
Member	PIM-AD-GroupPolicyMgmt-Scoped-ClientsDevices-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41:32 AM	Activate | Extend
Member	PIM-AD-GroupPolicyMgmt-Scoped-Servers-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41:33 AM	Activate | Extend
Member	PIM-AD-GroupPolicyMgmt-Scoped-Users-L2-T0-CP-ID-S_AD	Security	Direct	6/22/2025, 2:41:34 AM	Activate | Extend
Member	PIM-AD-UserMgmt-Scoped-Users-L2-T0-CP-ID-S_AD	Security	Direct	4/5/2026, 4:31:49 PM	Activate | Extend
Member	PIM-AD-DomainAdministrators-L1-T0-CP-ID-S_AD	Security	Direct	5/1/2026, 11:27:31 PM	Activate | Extend
Member	PIM-AD-LocalServerAdmins-Scoped-L2-T0-CP-ID-S_AD	Security	Direct	5/10/2026, 11:25:53 ...	Activate | Extend
Member	PIM-GDAP-Nunagreen-Entra-ID-GlobalAdministrator-L0-T0-CP-ID	Security	Direct	5/18/2026, 9:33:00 AM	Activate | Extend
Member	PIM-GDAP-Nunagreen-Entra-ID-D365-BusinessCentralAdministrator-L1-T0-CP-ID	Security	Direct	4/26/2026, 3:57:42 PM	Activate | Extend

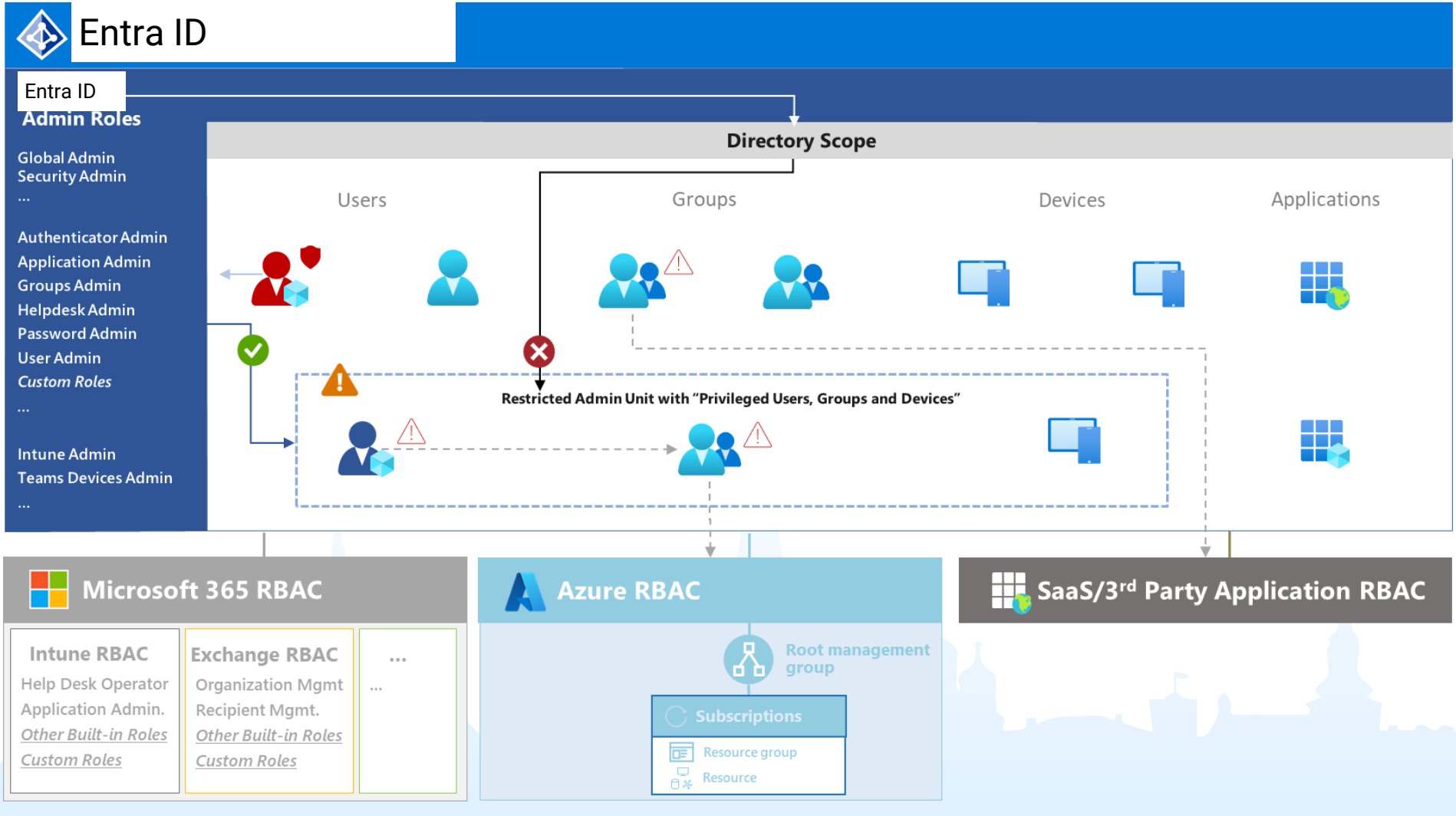
11.23
18/05/2025

Download Presentation with all demo’s

https://sharing.mortenknudsen.net/Privileged-Access-Strategy---Best-Practices-and-Common-Mistakes-when-Tiering-Cloud-and-AD-MEMSummit2026.pptx

Designing “PIM v2”

Use RBAC features, where possible


Entra ID
Entra ID
Admin Roles
Global Admin
Security Admin
...
Authenticator Admin
Application Admin
Groups Admin
Helpdesk Admin
Password Admin
User Admin
Custom Roles
...
Intune Admin
Teams Devices Admin
...
Directory Scope
Users
Groups
Devices
Applications
Restricted Admin Unit with "Privileged Users, Groups and Devices"
Microsoft 365 RBAC
Intune RBAC
Help Desk Operator
Application Admin.
Other Built-in Roles
Custom Roles
Exchange RBAC
Organization Mgmt
Recipient Mgmt.
Other Built-in Roles
Custom Roles
...
...
Azure RBAC
Root management group
Subscriptions
Resource group
Resource
SaaS/3rd Party Application RBAC

Intune RBAC

Microsoft Intune admin center

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Home > Tenant admin | Roles >

Endpoint Manager roles | All roles

Microsoft Intune

Search

Manage
All roles
Scope tags
Administrator Licensing

Monitor
My permissions

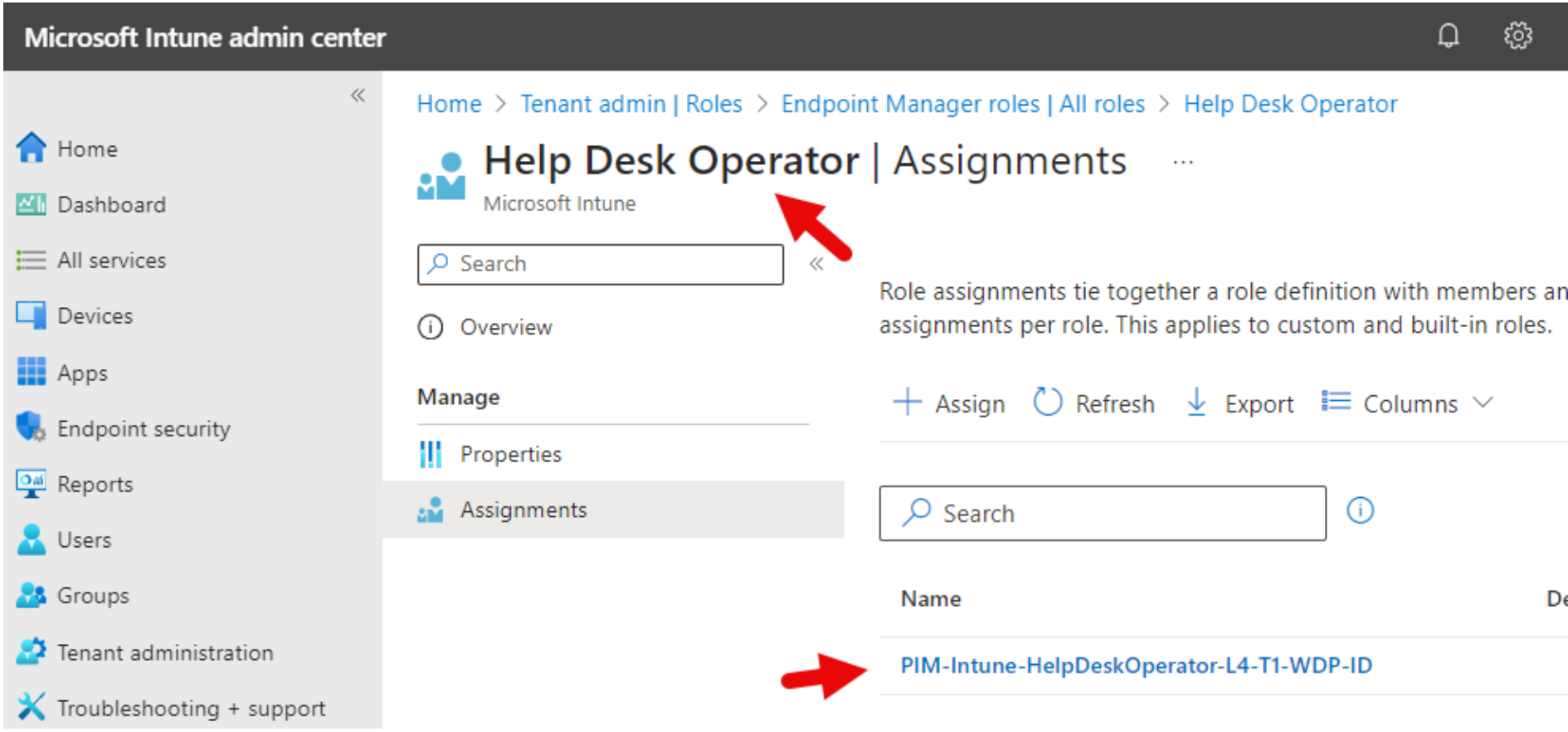
Help and support
Help and support

Create Duplicate Refresh

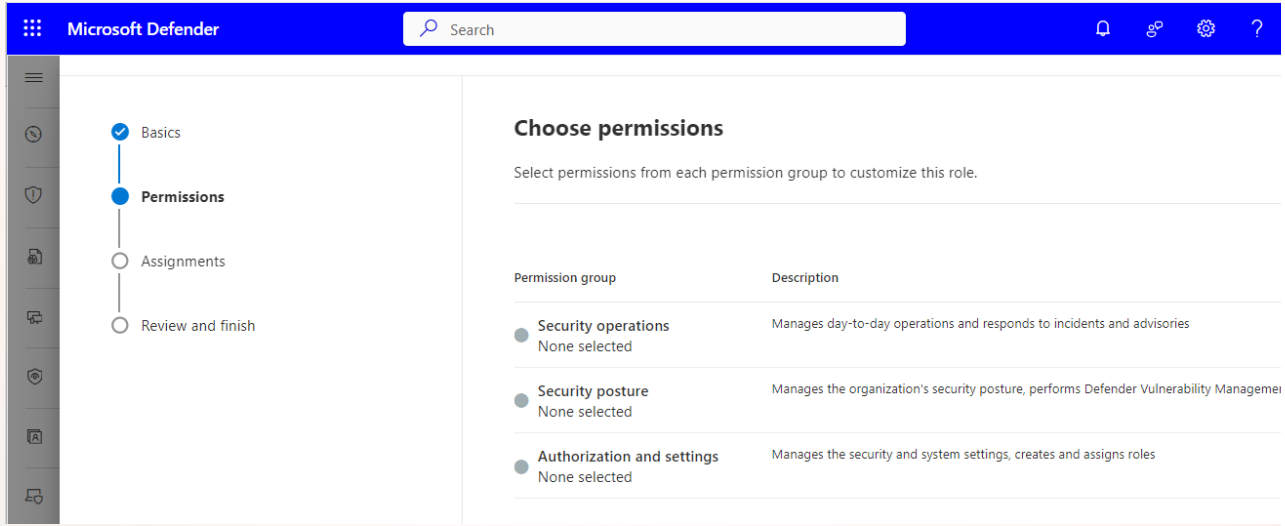
Endpoint Manager roles help you to assign permissions to administrators.

Search by name

Name	Type
Endpoint Security Manager	Built-in Role
Application Manager	Built-in Role
Endpoint Privilege Manager	Built-in Role
Read Only Operator	Built-in Role
Organizational Messages Manager	Built-in Role
School Administrator	Built-in Role
Help Desk Operator	Built-in Role
Endpoint Privilege Reader	Built-in Role
Policy and Profile manager	Built-in Role
Intune Role Administrator	Built-in Role
Modern Workplace Intune Admin	Custom Intune role


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin | Roles > Endpoint Manager roles | All roles > Help Desk Operator
Help Desk Operator | Assignments
Microsoft Intune
Search
Overview
Manage
Properties
Assignments
Role assignments tie together a role definition with members an
assignments per role. This applies to custom and built-in roles.
Assign
Refresh
Export
Columns
Search
Name
PIM-Intune-HelpDeskOperator-L4-T1-WDP-ID

Defender XDR RBAC



Security operations

Select the permissions in this group to users who perform security who respond to incidents and advisories.

Clear all permissions

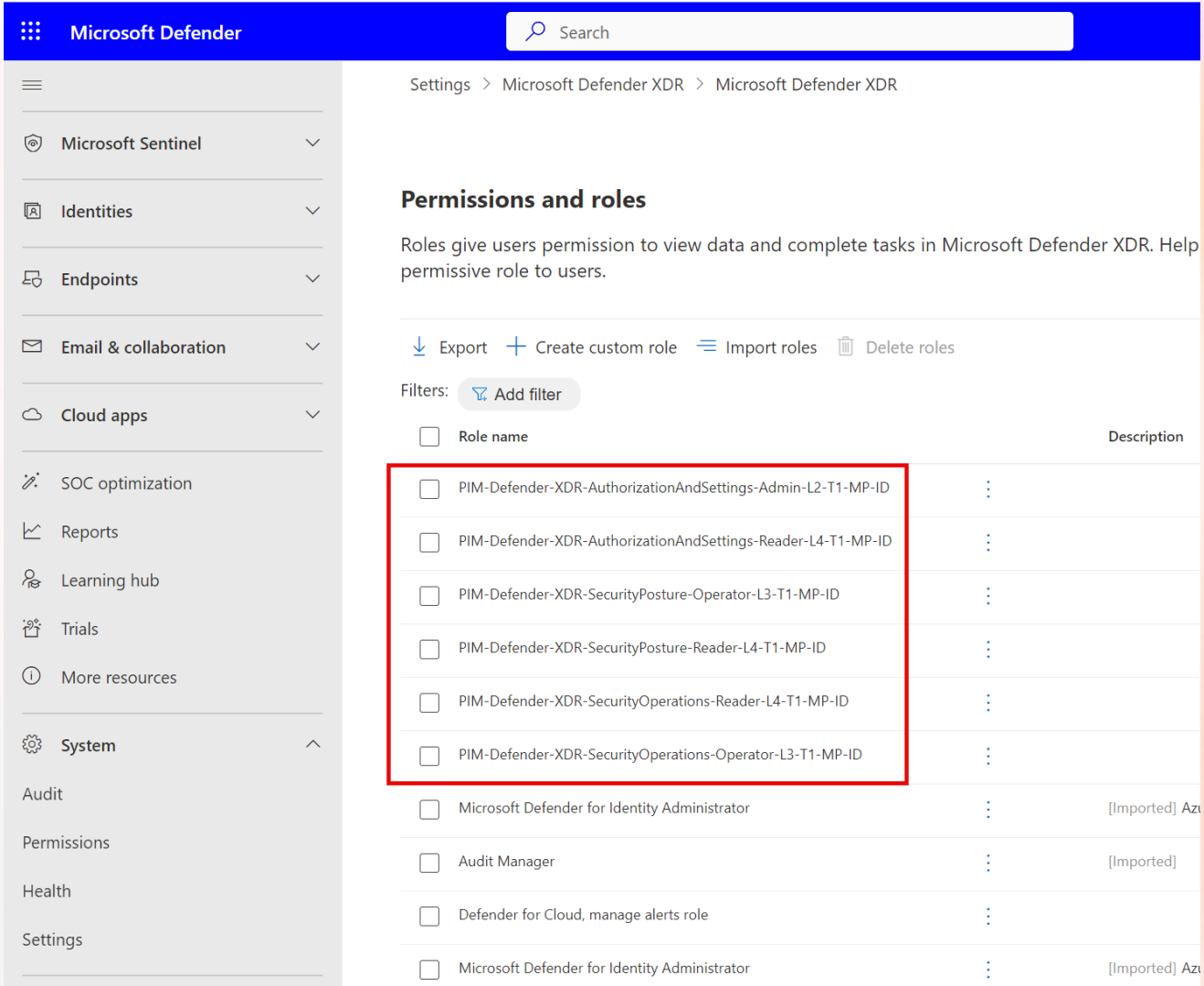
- All read-only permissions
- All read and manage permissions
- Select custom permissions

Security data

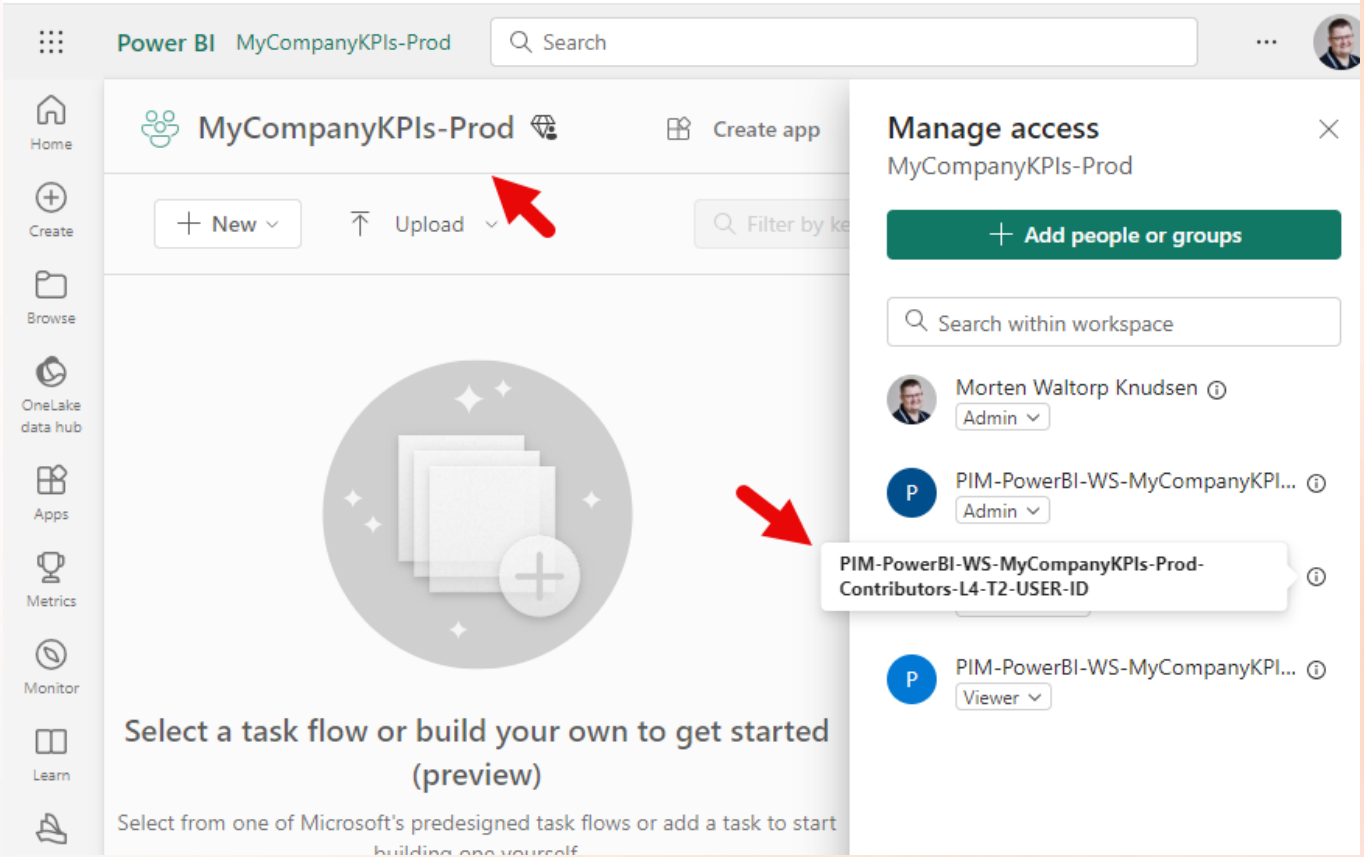
- Read-only
- Select all permissions
- Select custom permissions
  - Security data basics (read)
  - Alerts (manage)
  - Response (manage)
  - Basic live response (manage)
  - Advanced live response (manage)
  - File collection (manage)
  - Email & collaboration quarantine (manage)
  - Email & collaboration advanced actions (manage)

Raw data (Email & collaboration)

- Read-only
- Select custom permissions
  - Email & collaboration metadata (read)
  - Email & collaboration content (read)


Microsoft Defender
Search
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
SOC optimization
Reports
Learning hub
Trials
More resources
System
Audit
Permissions
Health
Settings
Settings > Microsoft Defender XDR > Microsoft Defender XDR
Permissions and roles
Roles give users permission to view data and complete tasks in Microsoft Defender XDR. Help
permissive role to users.
Export
Create custom role
Import roles
Delete roles
Filters:
Add filter
Role name
Description
PIM-Defender-XDR-AuthorizationAndSettings-Admin-L2-T1-MP-ID
PIM-Defender-XDR-AuthorizationAndSettings-Reader-L4-T1-MP-ID
PIM-Defender-XDR-SecurityPosture-Operator-L3-T1-MP-ID
PIM-Defender-XDR-SecurityPosture-Reader-L4-T1-MP-ID
PIM-Defender-XDR-SecurityOperations-Reader-L4-T1-MP-ID
PIM-Defender-XDR-SecurityOperations-Operator-L3-T1-MP-ID
Microsoft Defender for Identity Administrator
[Imported] Azu
Audit Manager
[Imported]
Defender for Cloud, manage alerts role
Microsoft Defender for Identity Administrator
[Imported] Azu

Power BI RBAC



RBAC support (samples)

- Intune
- Defender
- Power BI
- AzDevOps
- Azure
- Entra ID
- Purview
- Github Enterprise Cloud
- D365 Business Central
- D365 CRM
- Salesforce
- ServiceNow
- Dropbox Business
- Workday
- Slack
- Atlassian Jira

Designing “PIM v2”

Entra ID Groups

Entra ID PIM Assignments using PIM v2 Framework

Great Documentation using Entra ID Groups
(seen from backend)

DEMO

PIM-Entra-ID-CloudApplicationAdministrator-L1-T0-CP-ID | Assigned roles

Group

Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Administrative units
Group memberships
Assigned roles
lications
ses
e role assignments
lentity

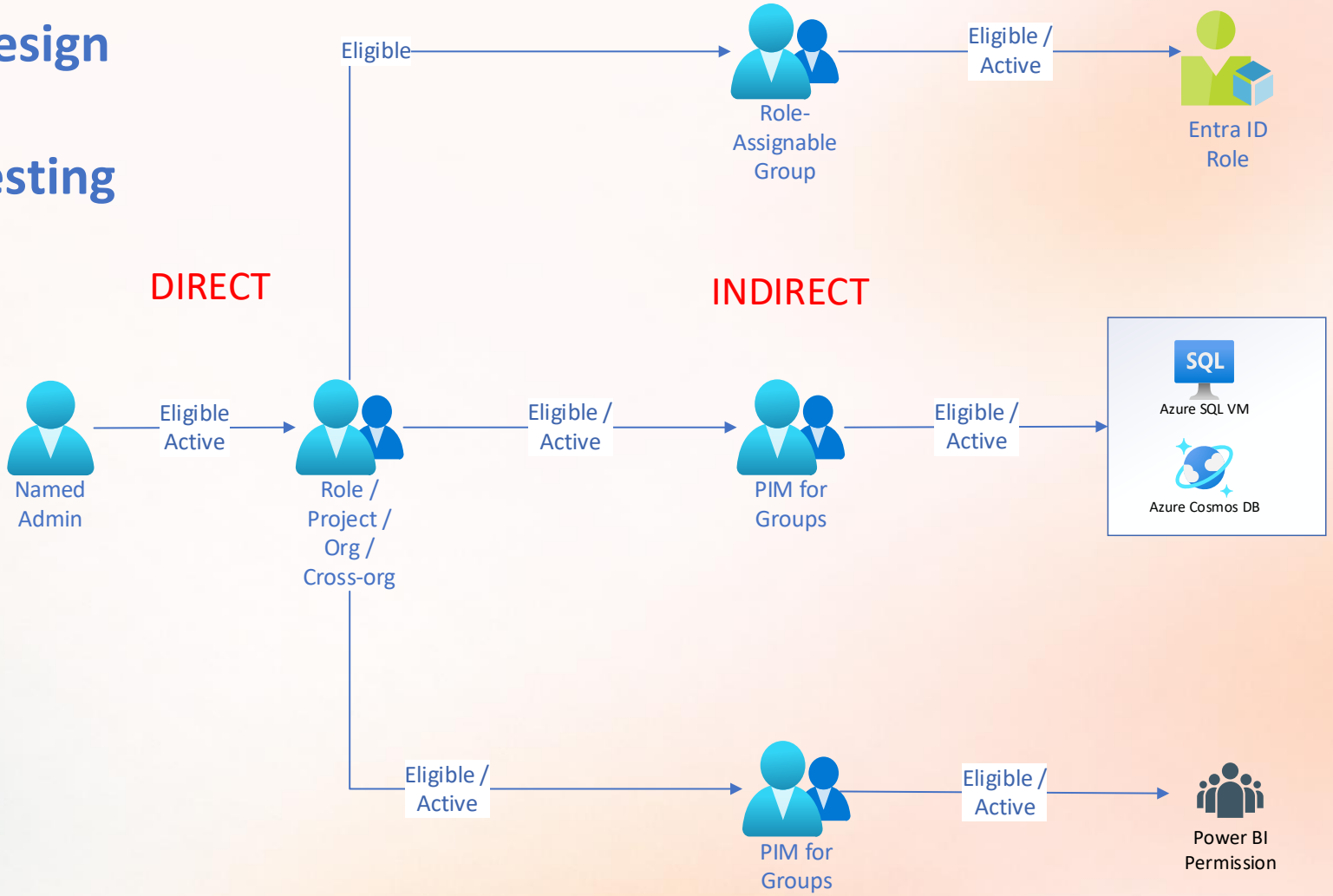
Add assignments | Refresh | Got feedback?

Eligible assignments | Active assignments | Expired assignments

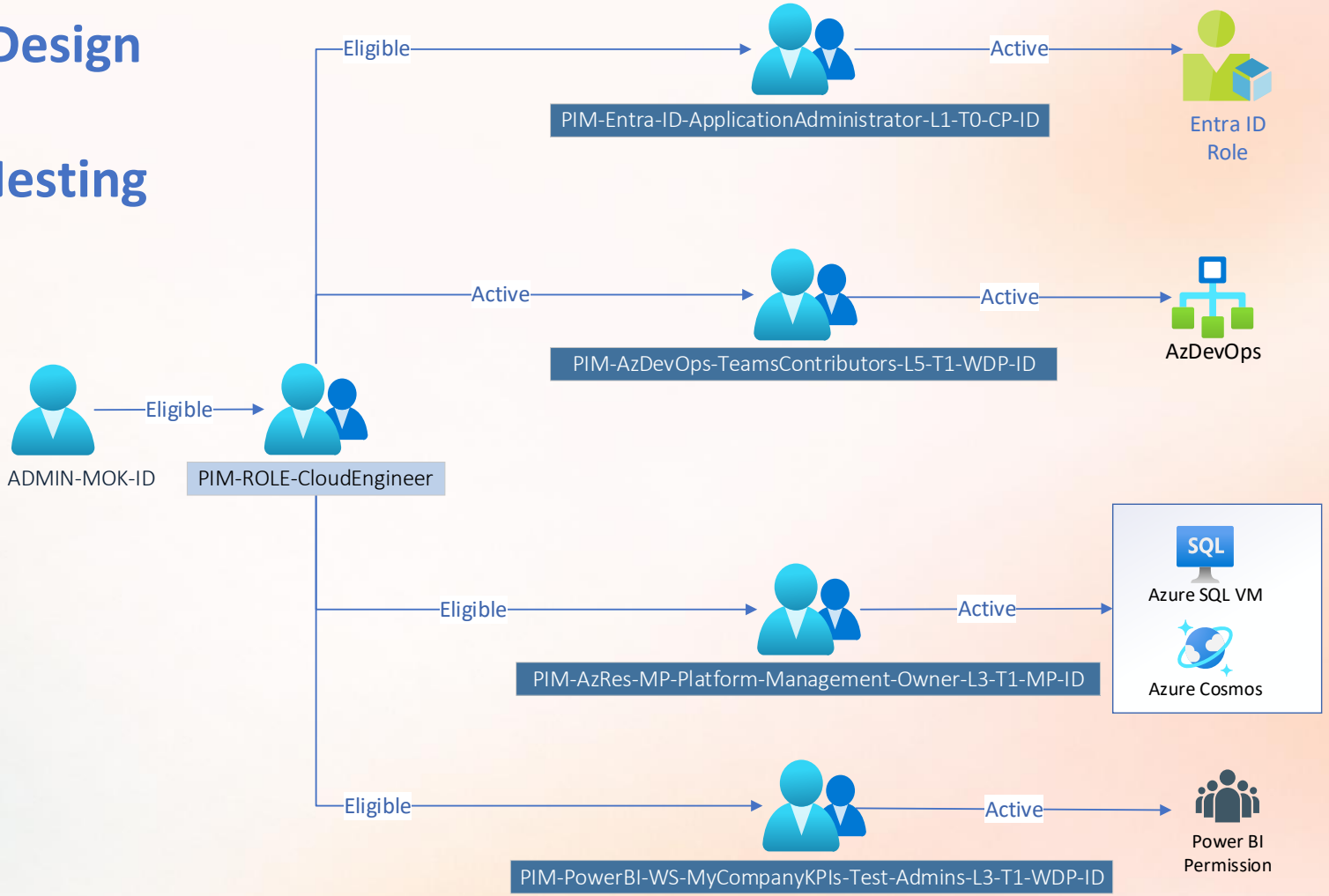
Search by role

Role	Principal name	Scope	Membership	State	St
Cloud Application Administrator		Directory	Direct	Active	5/

PIM v2 Design with Group Nesting



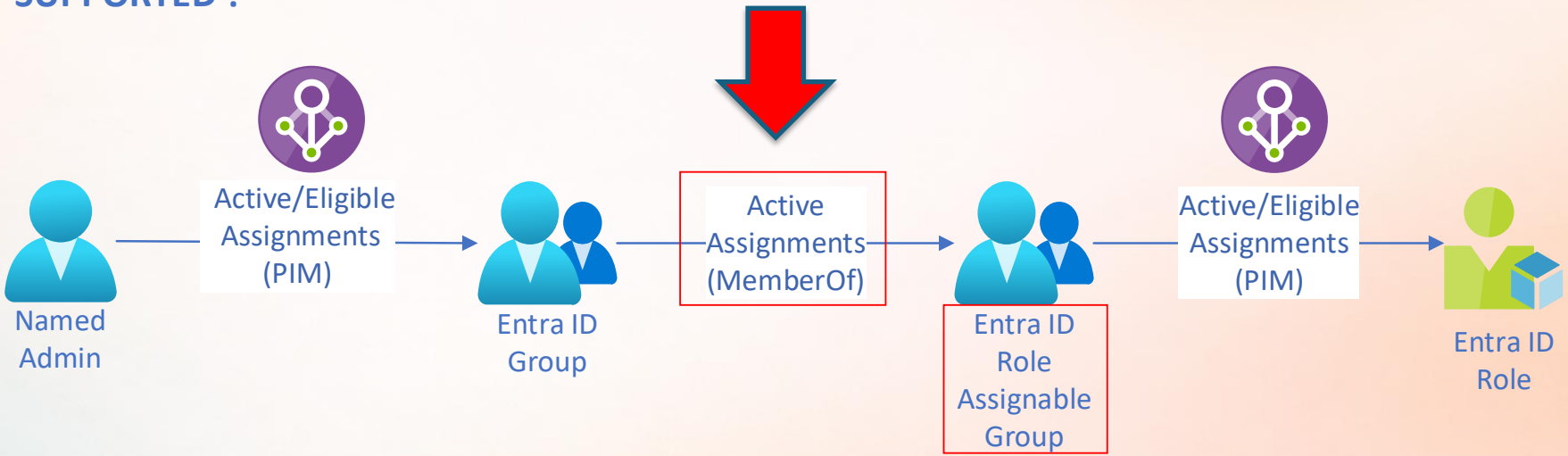
PIM v2 Design with Group Nesting



Group Nesting scenario NOT SUPPORTED

NOT SUPPORTED !

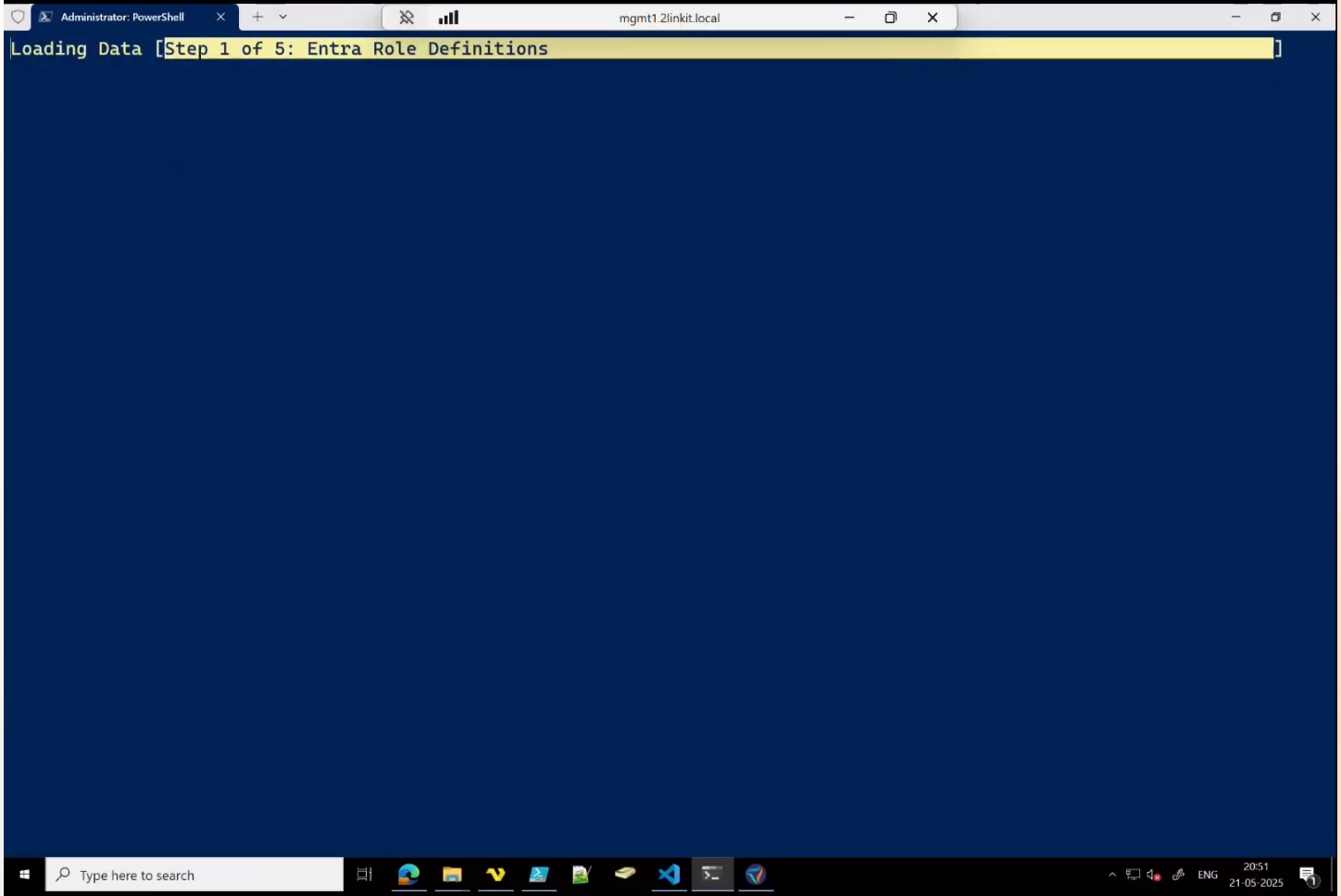
Must be Eligible for Role-assignable groups



Entra ID PIM Activation – Use AI to help

PIM Activation:
Use AI to help which role to choose ☺

DEMO


Administrator: PowerShell
mgmt1.2linkit.local
Loading Data [Step 1 of 5: Entra Role Definitions
Type here to search
ENG
20:51
21-05-2025

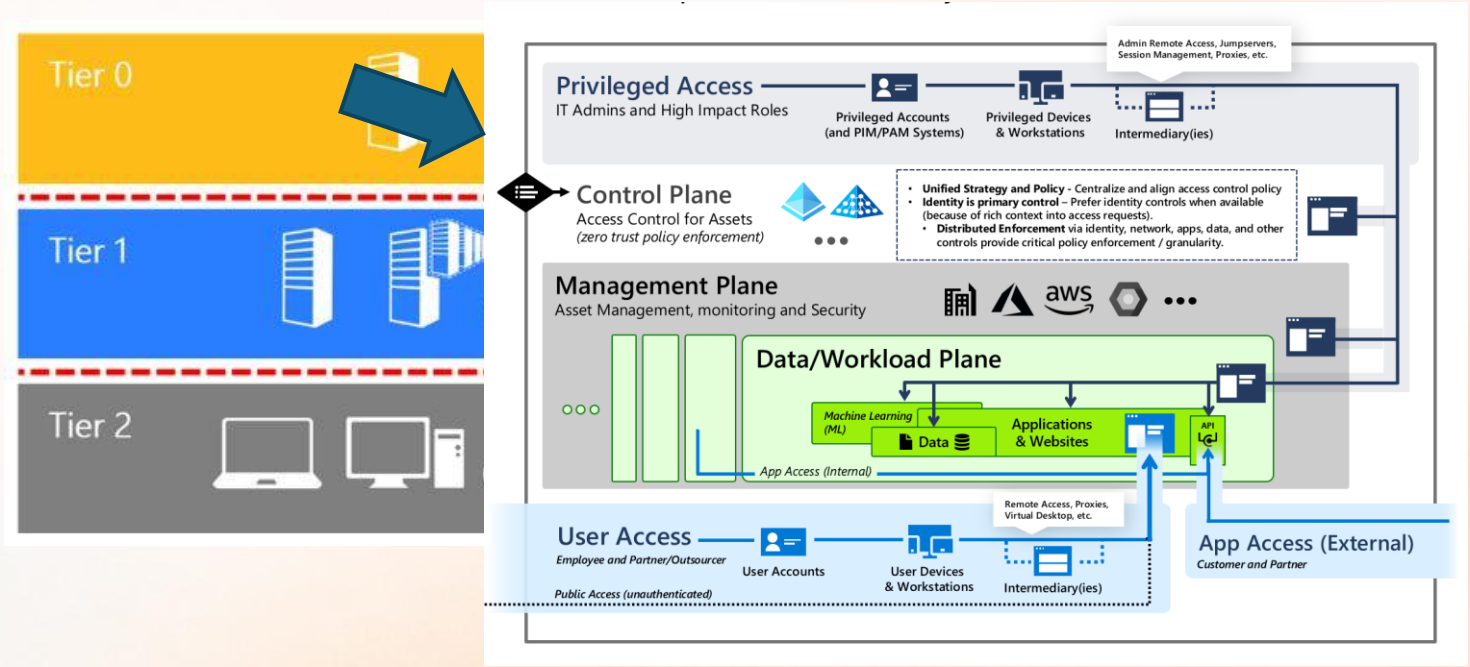
Designing “PIM v2”

Delegation Levels with Tiering

Legacy Tier-model

The enterprise access model supersedes and replaces the legacy tier model that was focused on containing unauthorized escalation of privilege in an on-premises Windows Server Active Directory environment.

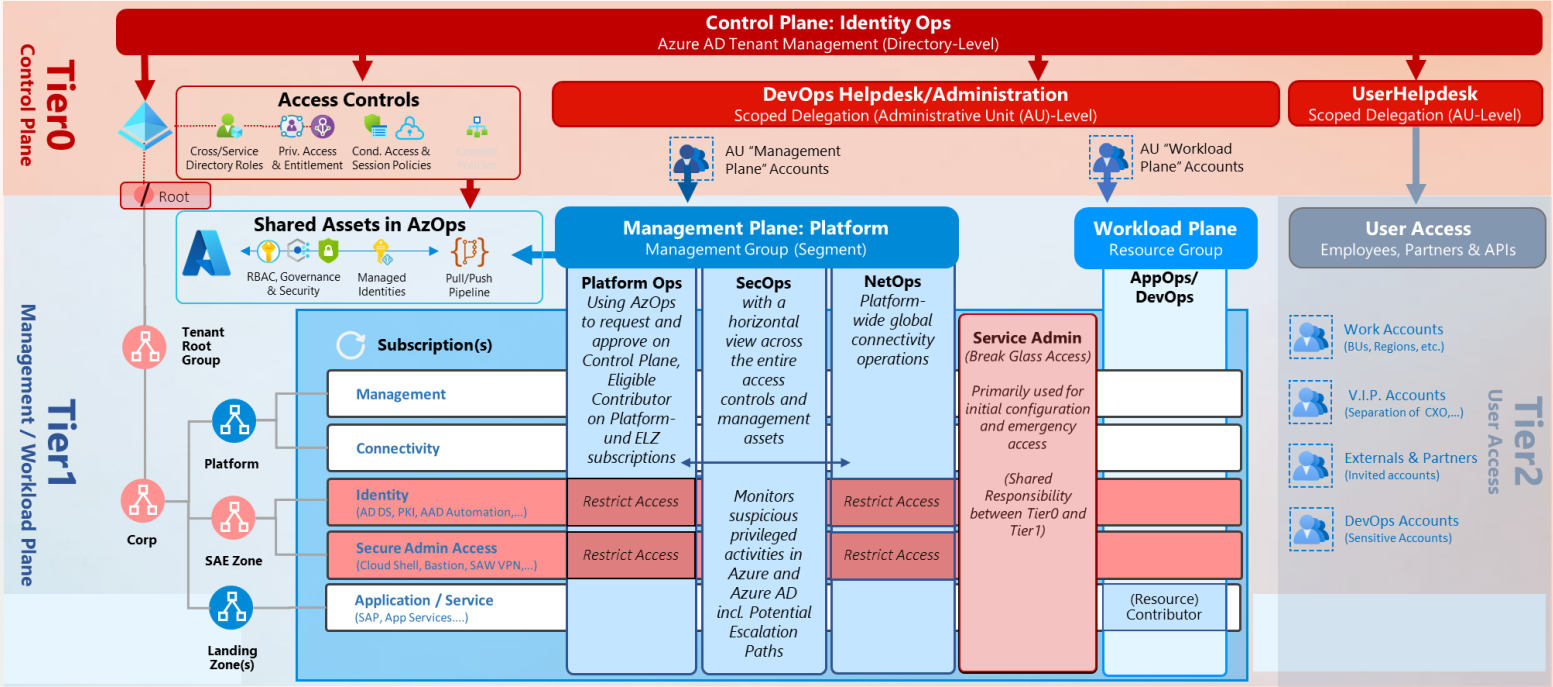
The enterprise access model incorporates these elements as well as full access management requirements of a modern enterprise that spans on-premises, multiple clouds, internal or external user access, and more.



https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

Enterprise Access and Tiered Administration Model

Holistic overview with tiering



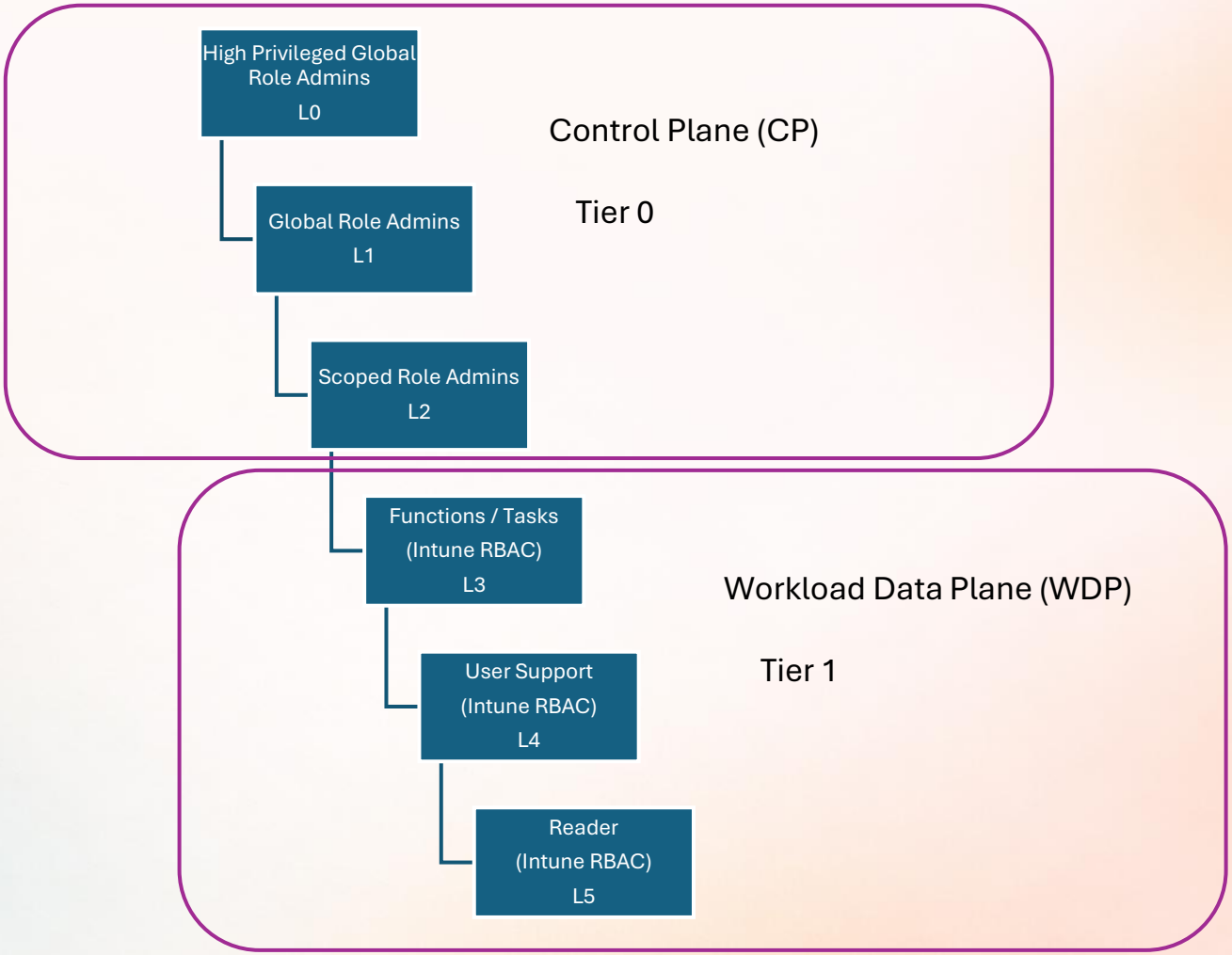
Credit drawing: Thomas Naunheim

Tiering Levels

Tiering	Tiering Acronym	Permission Plane	Purpose
T0	T0-CP	Control Plane	Global roles and services like conditional access
T1	T1-WDP	Workload / Data Plane	Business data or application
T1	T1-MP	Management Plane	Management platform (logging, security, identity, connectity). Cross-platform
T2	T2-App	App Access	Read/Write specific data – for example for integration with partner
T2	T2-User	User Access	User access to service fx. Power BI platform

Delegation Levels

Level	Tier	Level	Samples
L0	T0	**High Privileged Global Role**	**Entra ID** • Global Administrator **Active Directory** • Forest Administrator
L1	T0	**Global Role Admins**	**Entra ID** • All 100+ Tenant Roles except for Global Administrator **Active Directory** • Domain Administrator
L2	T0	**Scoped Role Admins**	**Entra ID** • Specific Tenant Roles delegated to Administrative Unit (AU) targeted for specific set of users/devices/groups **Active Directory** • Specific permissions delegated to Organizational Unit (OU) targeted for specific set of users/devices/groups
L3-L9	T1	**Service Admins**	Service/Workload/Data



Example

Intune

Services

Service Name	Service Acronym	Delegations			
		TOTAL	Tier 0	Tier 1	Tier 2
Active Directory	AD	3	3 (L0-L2)		
Entra ID	Entra-ID	3	3 (L0-L2)		
Conditional Access	Entra-CA	3	3 (L0-L2)		
Privileged Identity Management	Entra-PIM	2	2 (L0-L1)		
Entra Private/Internet Access	Entra-GSA	2	2 (L0-L1)		
Intune	Intune	6	3 (L0-L2)	3 (L3-L5)	
Exchange	Exchange	3	3 (L0-L2)	4 (*)	
Teams	Teams	3	3 (L0-L2)		
Sharepoint	Sharepoint	7	3 (L0-L2)	1 (*)	3
PowerBI (master data)	PowerBI-MasterData	6	2 (L0-L1)	2 (L2-L3)	2
Power BI (Business data)	PowerBI-WS	5	2 (L0-L1)	3 (L2-L4)	1
Azure Resources	Azure	10	1 (L0)	9 (L1-L9)	(2)
Azure DevOps	AzDevOps	6	2 (L0-L1)	4 (L2-L5)	
Defender XDR	Defender	6	2 (L0-L1)	4 (L2-L5)	

(*) T1 RBAC doesn't support PIM as they require mail-enabled security group type, only T0 roles

DELEGATION GROUPS

Level	Tier	Group Name	Role assignable
L0	T0	PIM-Entra-ID-GlobalAdministrator-L0-T0-CP-ID	Yes
L1	T0	PIM-Entra-ID-IntuneAdministrator-L1-T0-CP-ID	Yes
L1	T0	PIM-Entra-ID-CloudDeviceAdministrator-L1-T0-CP-ID	Yes
L1	T0	PIM-Entra-ID-WindowsUpdateAdministrator-L1-T0-CP-ID	Yes
L1	T0	PIM-Entra-ID-AzureADJoinedDeviceLocalAdministrator-L1-T0-CP-ID	Yes
L1	T0	PIM-Entra-ID-MicrosoftHardwareWarrantyAdministrator-L1-T0-CP-ID	Yes
L3	T1	PIM-Intune-IntuneRoleAdministrator-L3-T1-WDP-ID	No
L3	T1	PIM-Intune-OrganizationalMessagesManager-L3-T1-WDP-ID	No
L3	T1	PIM-Intune-PolicyAndProfileManager-L3-T1-WDP-ID	No
L3	T1	PIM-Intune-SchoolAdministrator-L3-T1-WDP-ID	No
L3	T1	PIM-Intune-ApplicationManager-L3-T1-WDP-ID	No
L3	T1	PIM-Intune-EndpointPrivilegeManager-L3-T1-WDP-ID	No
L3	T1	PIM-Intune-EndpointSecurityManager-L3-T1-WDP-ID	No
L3	T1	PIM-Intune-CloudPCAdministrator-L3-T1-WDP-ID	No
L4	T1	PIM-Intune-HelpDeskOperator-L4-T1-WDP-ID	No
L5	T1	PIM-Intune-EndpointPrivilegeReader-L5-T1-WDP-ID	No
L5	T1	PIM-Intune-ReadOnlyOperator-L5-T1-WDP-ID	No
L5	T1	PIM-Intune-CloudPCReader-L5-T1-WDP-ID	No

DELEGATION GROUPS

Level	Tier	Group Name	Role Assignable
L0	T0	PIM-Entra-ID-GlobalAdministrator-L0-T0-CP-ID	Yes
L1	T0	PIM-Entra-ID-PowerPlatformAdministrator-L1-T0-CP-ID	Yes
L1	T0	PIM-Entra-ID-PowerBIAdministrator-L1-T0-CP-ID	Yes
L1	T0	PIM-Entra-ID-FabricAdministrator-L1-T0-CP-ID	Yes
L2	T1	PIM-PowerBI-MasterData-OrgAdmins-L2-T1-WDP-ID	No
L3	T1	PIM-PowerBI-MasterData-DataSet-Admins-L3-T1-WDP-ID	No
L3	T1	PIM-PowerBI-WS-ASSETMANAGEMENT-Prod-Admins-L3-T1-WDP-ID	No
L3	T1	PIM-PowerBI-WS-ASSETMANAGEMENT-Test-Admins-L3-T1-WDP-ID	No
L3	T1	PIM-PowerBI-WS-HR-Prod-Admins-L3-T1-WDP-ID	No
L3	T1	PIM-PowerBI-WS-HR-Test-Admins-L3-T1-WDP-ID	No
		… (more workspaces here)	No
L4	T2	PIM-PowerBI-MasterData-Build-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-MasterData-Read-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-MasterData-Share-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-BIDATAMODEL-Prod-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-BIDATAMODEL-Test-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-BUSINESSINTELLIGENCE-Prod-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-BUSINESSINTELLIGENCE-Test-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-DRIFT-Prod-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-DRIFT-Test-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-FJERNVARMEFYNKPI-Prod-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-FJERNVARMEFYNKPI-Test-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-FJERNVARMEFYNPUBLIC-Prod-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-FJERNVARMEFYNPUBLIC-Test-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-GUIDELINESPOWERBI-Prod-Contributors-L4-T2-USER-ID	No
L4	T2	PIM-PowerBI-WS-GUIDELINESPOWERBI-Test-Contributors-L4-T2-USER-ID	No

Be Prepared for Discussions

- Everyone needs to understand the WHY
- Admin vs. User Account (when to use) - examples
  - PowerBI Contributor Workspace
  - Developers need User Account access to AzDevOps
  - User account must have access to Storage Account

Level	Entra ID	Entra-CA	Entra-PIM	Entra-GSA	Intune	Exchange	Teams	Sharepoint	Power BI (master data)	Power BI (ws data)	Azure	Azure DevOps	Defender XDR
L0	High	High	High	High	High	High	High	High	High	High	Tenant Root	High	High
L1	Global	Global	Global	Global	Global	Global	Global	Global	Global	Global	Corp	Global	Global
L2	Scoped	Scoped			Scoped	Scoped	Scoped	Scoped	Org	Org	WDP: Regions MP: Platform	Org Collection Admins	Org settings
L3					Function	Org		Site Admin	Data Set Admins	Workspace Admins	WDP: Environm. MP: Platform Type	Project Admins	Org Admins
L4					Support	Function		Site Owner	User Std Roles	User Workspace Contributor	WDP: Corp/Online MP: Platform Type	Teams Admins	Function Admins
L5					Reader	Support		Site Member	User Custom Roles		MP: Platform Type	Teams Contributors	Reader
L6						Reader		Site Viewer			LZ Workload (MG)		
L7											Subscription		
L8											RG		
L9											Resource		

Usage of Account
L0 Admin Account (High Priv
Admin Account (day2day)
Discussions admin vs. user
User Account

PIM for Active Directory

Using PIM for Entra ID as Session Initiator to legacy AD

Groups & Members are created in AD (separate)

```
Validating PIM members for group PIM-AD-AccountOperators-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-ClientDevicesMgmt-Scoped-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-ComputerMgmt-Domain-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-DHCPAdministrators-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-DNSAdministrators-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-DomainAdministrators-L1-T0-CP-ID-S_AD
  PIM for AD: Adding user x-Admin-MOK-AD with group membership for 144 min (PIM for AD)

Validating PIM members for group PIM-AD-EnterpriseAdministrators-L0-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupMembershipMgmt-Domain-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupMembershipMgmt-Scoped-Groups-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupMgmt-Domain-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupMgmt-Scoped-Groups-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupPolicyMgmt-Domain-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupPolicyMgmt-Scoped-ClientsDevices-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupPolicyMgmt-Scoped-Servers-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupPolicyMgmt-Scoped-Users-L2-T0-CP-ID-S_AD
```

Auto-remove, if user manually deactivates PIM-session or session TTL runs out (auto-deactivated)

```
Validating PIM members for group PIM-AD-EnterpriseAdministrators-L0-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupMembershipMgmt-Domain-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupMembershipMgmt-Scoped-Groups-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupMgmt-Domain-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupMgmt-Scoped-Groups-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupPolicyMgmt-Domain-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupPolicyMgmt-Scoped-ClientsDevices-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupPolicyMgmt-Scoped-Servers-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-GroupPolicyMgmt-Scoped-Users-L2-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-LocalServerAdmins-Scoped-L2-T0-CP-ID-S_AD
  PIM for AD: Removing User x-Admin-MOK-AD from group PIM-AD-LocalServerAdmins-Scoped-L2-T0-CP-ID-S_AD

Validating PIM members for group PIM-AD-PrintOperators-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-SchemaAdministrators-L0-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-UserMgmt-Domain-L1-T0-CP-ID-S_AD
Validating PIM members for group PIM-AD-UserMgmt-Scoped-Users-L2-T0-CP-ID-S_AD
```

```
Validating PIM members for group PIM-AD-SRV-Mgmt1-ID-S_AD
  PIM for AD: Removing User x-Admin-MOK-AD from group PIM-AD-SRV-Mgmt1-ID-S_AD
```

TTL check each cycle

```
Validating PIM members for group PIM-AD-SRV-Mgmt1-ID-S_AD

  Current TTL in AD is 26096 for user x-Admin-MOK-AD
  Expected TTL from ID PIM-session is 26112
  Deviation of seconds is -16
  Deviation of seconds is acceptable

  PIM for AD: User x-Admin-MOK-AD is already member of PIM-AD-SRV-Mgmt1-ID-S_AD
```

```
Validating PIM members for group PIM-AD-LocalServerAdmins-Scoped-L2-T0-CP-ID-S_AD

  Current TTL in AD is 24779 for user x-Admin-MOK-AD
  Expected TTL from ID PIM-session is 24765
  Deviation of seconds is 14
  Deviation of seconds is acceptable

  PIM for AD: User x-Admin-MOK-AD is already member of PIM-AD-LocalServerAdmins-Scoped-L2-T0-CP-ID-S_AD
```

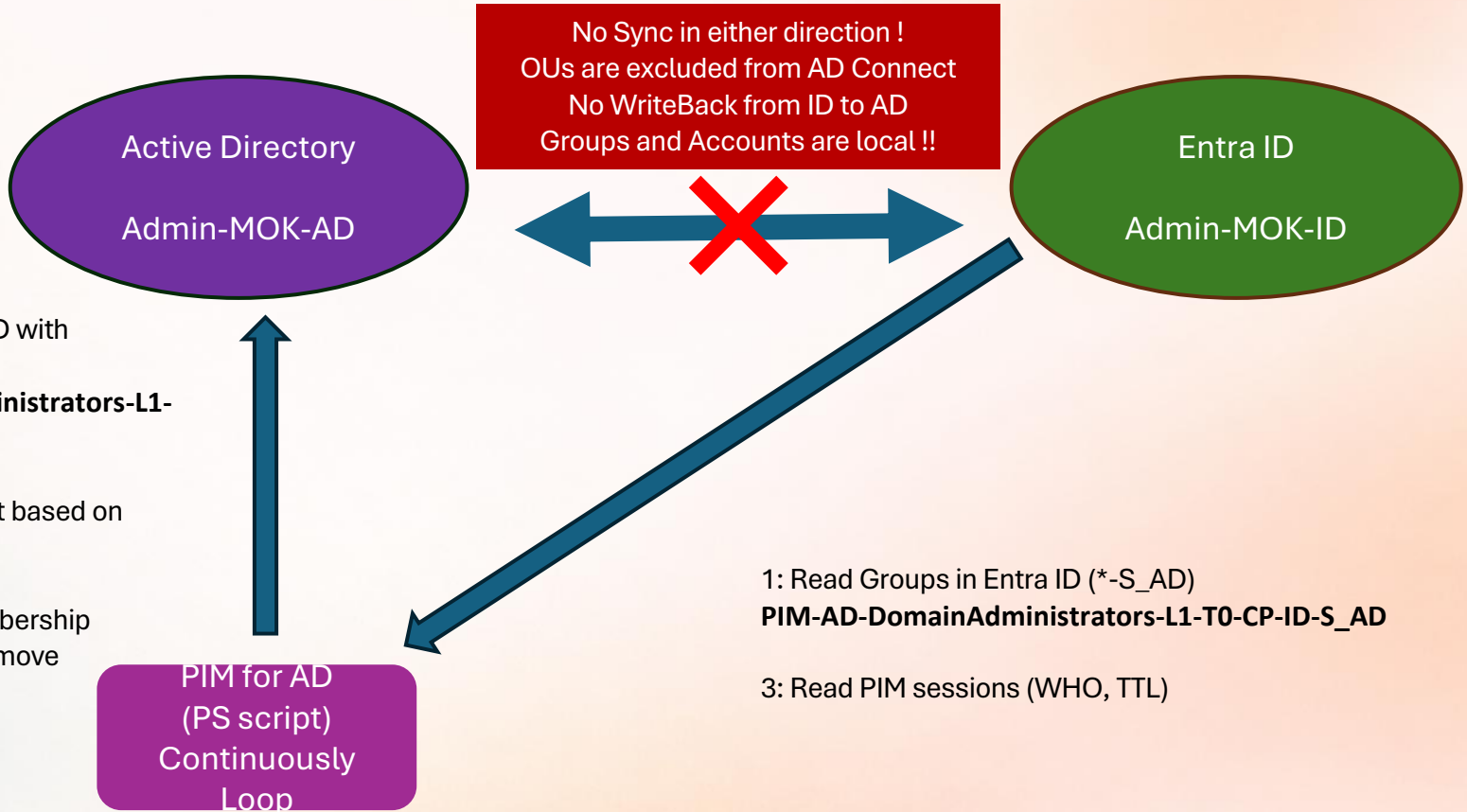
Auto-correct TTL if deviations more than +/- 2 min


```
Validating PIM members for group PIM-AD-SRV-Mgmt1-ID-S_AD

  Current TTL in AD is 8021 for user x-Admin-MOK-AD
  Expected TTL from ID PIM-session is 7114
  Deviation of seconds is 907
  Deviation of seconds is NOT acceptable (+/-2 min)

  PIM for AD: Adding user x-Admin-MOK-AD with group membership for 119 min (PIM for AD)
```

PIM for legacy AD Flow



TTL feature group membership
Windows Server 2016 forest functional level features

- Privileged Access Management

```
Add-ADGroupMember -Identity $AD_GroupName
                  -Members $AD_UserName
                  -MemberTimeToLive $AD_TimeSpanTotalMinutesGroupMemberShip
                  -Credential $AD_Credentials
```

Supported domain controller operating systems:

Windows Server 2022
Windows Server 2019
Windows Server 2016

The minimum requirement to add one a domain controller of one of these versions of Windows Server is a Windows Server 2008 functional level.

The domain also has to use DFS-R as the engine to replicate SYSVOL.

Check PAM-support:
Get-ADOptionalFeature -filter "name -eq 'privileged access management feature'"

Enable PAM-support:
Enable-ADOptionalFeature 'Privileged Access Management Feature' -Scope ForestOrConfigurationSet -Target 2linkit.local

Automation

- **Automation of Entra PIM – full & delta – CSV, SQL, cmdlets** (private right now, public soon)
  - PIM Assignment Wizard, PIM Revoker, PIM Exporter

- **https://github.com/KnudsenMorten/PIM4ActiveDirectoryPS** (private right now, public soon)
  - Automation of PIM for AD

- **https://github.com/KnudsenMorten/EntraPolicySuite**
  - Command line management of Entra Conditional Access Policies, Named Locations, Authentication Strengths and more
  - +120 Conditional Access policies with full documents

- **https://github.com/KnudsenMorten/PIM-Role-Advisor**
  - Show PIM role to solve a task - and group to activate the needed permission

Download Presentation with all demo’s

https://sharing.mortenknudsen.net/Privileged-Access-Strategy---Best-Practices-and-Common-Mistakes-when-Tiering-Cloud-and-AD-MEMSummit2026.pptx

Please rate this session!

Your feedback will help with

- speaker evaluation
- content relevance
- decision making for future events
- quality improvement

Love to connect with you ☺
Morten Knudsen

/in/knudsenmorten

@mortenknudsen.net

@knudsenmortendk

aka.ms/morten

mok@mortenknudsen.net