



# ADRIATICS TECH SUMMIT 2026

## **PIMp Your Administration**

Klaus Bierschenk  
Director Consulting Expert, CGI Germany

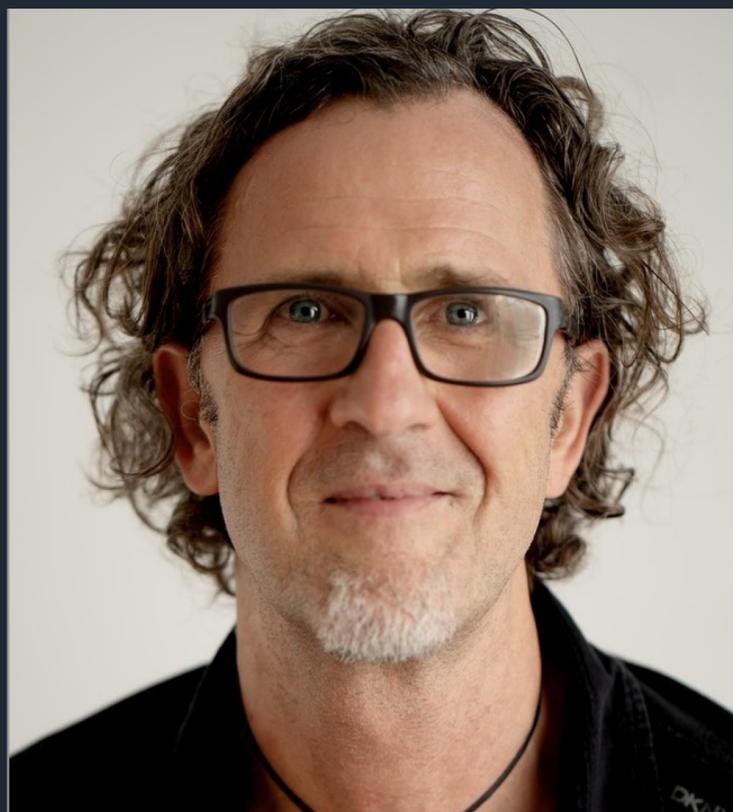


How many Entra ID Roles do we have today?

134

How many Azure Roles do we have today?

828



## Meet the Speaker

### Klaus Bierschenk

Director Consulting Expert / CGI Germany

- Based in Murnau, Bavaria
- Living with my family, two snakes, two cats – and lots of other animals my cats bring home from time to time



[linkedin.com/in/klabier/](https://www.linkedin.com/in/klabier/)



[Klaus@nothingbutcloud.net](mailto:Klaus@nothingbutcloud.net)



<https://NothingButCloud.net>



# Improve Administration – Today's Topics

- ❖ PIM Concepts Explained Using an Example Environment (School)
- ❖ Improve: PIMp Your Administration with Other Technologies
- ❖ PIM for Groups – where does eligibility belong?
- ❖ Key Things You Should Know About PIM



# School (or Similar) Environment Model

## 1 School-wide



- Multiple GA configurations
- No permanent GAs
- No User Entra Admin Center access
- No changes to default roles

## 2 Class Level Access (AU)



- Class Admins
- Manual Role Assignment

## 3 Sensitive Student Support



- Protect groups
- Monitor sensitive objects



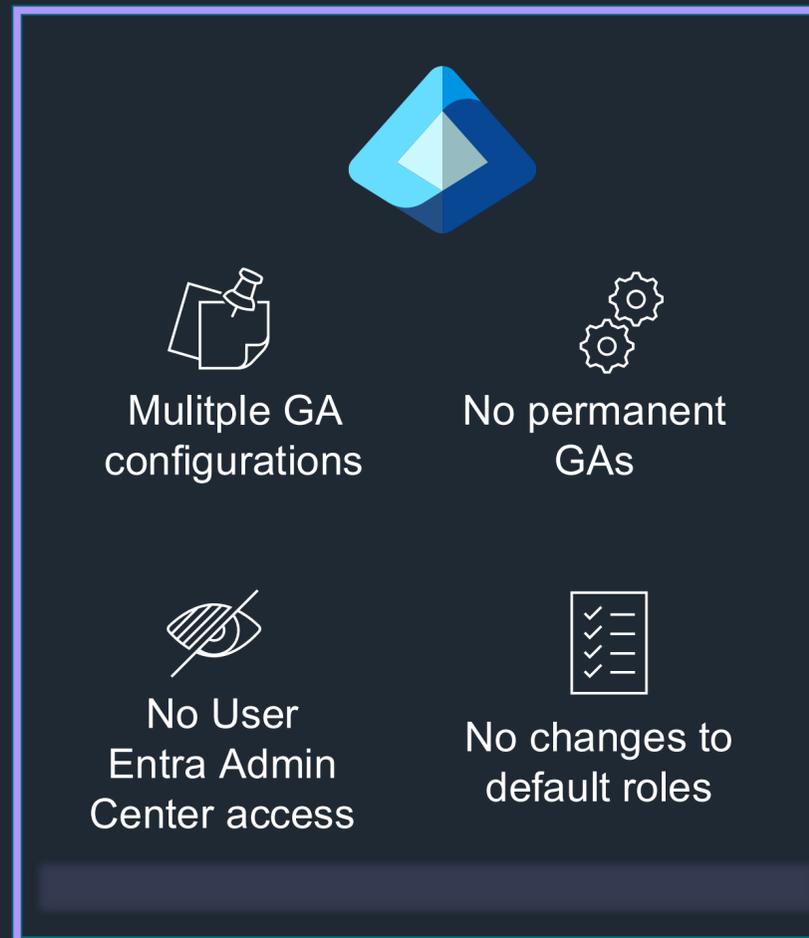
PIM Basic

PIM for Groups

Admin Units

# School (or Similar) Environment Model

## 1 School-wide



Use PIM for Groups to manage multiple Global Administrator access

Most built-in roles are not be modified

Only Break-Glass Accounts are permanently assigned

End users do not have access to the Entra Admin Center

GA activation is blocked on mobile devices (Conditional Access)



PIM Basic

PIM for Groups

Admin Units

# *Demo*

## *Tenant Settings*

- Multiple GAs via Groups*
- Conditional Access*



- Home
- Entra agents
- Favorites
- Entra ID
- Overview
- Users
- Groups
- Devices
- Agent ID (Preview)
- Enterprise apps
- App registrations
- Roles & admins
- Delegated admin partners
- Domain services
- Conditional Access
- Multifactor authentication

- Home >
- Conditional Access | Overview
- Microsoft Entra ID
- Overview
- Policies
- Deleted Policies (Preview)
- Insights and reporting
- Diagnose and solve problems
- Manage
  - Named locations
  - Custom controls (Preview)
  - Terms of use
  - VPN connectivity
  - Authentication contexts
  - Authentication strengths
  - Classic policies
- Monitoring
  - Sign-in logs
  - Audit logs
- Troubleshooting + Support
  - New support request

Get started | **Overview** | Coverage | Tutorials

Policy Summary

- Agent Identities**  
There are 5 agent identities in your tenant  
[See all unprotected sign-ins](#)  
[See all policies protecting agents](#)
- Conditional Access Optimization Agent**  
0 suggestions  
[View suggestions](#)
- Policy Snapshot**  
7 Enabled 1 Report-only 5 Off  
[View all policies](#)
- Users**  
3 users signed in during the last 7 days without any policy coverage  
[See all unprotected sign-ins](#)
- Devices**  
1% of sign-ins in the last 7 days were from unmanaged or non-compliant devices  
[See all noncompliant devices](#)  
[See all unmanaged devices](#)
- Applications**  
Browse a list of applications that are not protected by your policies.  
[View top unprotected apps](#)

# *Demo*

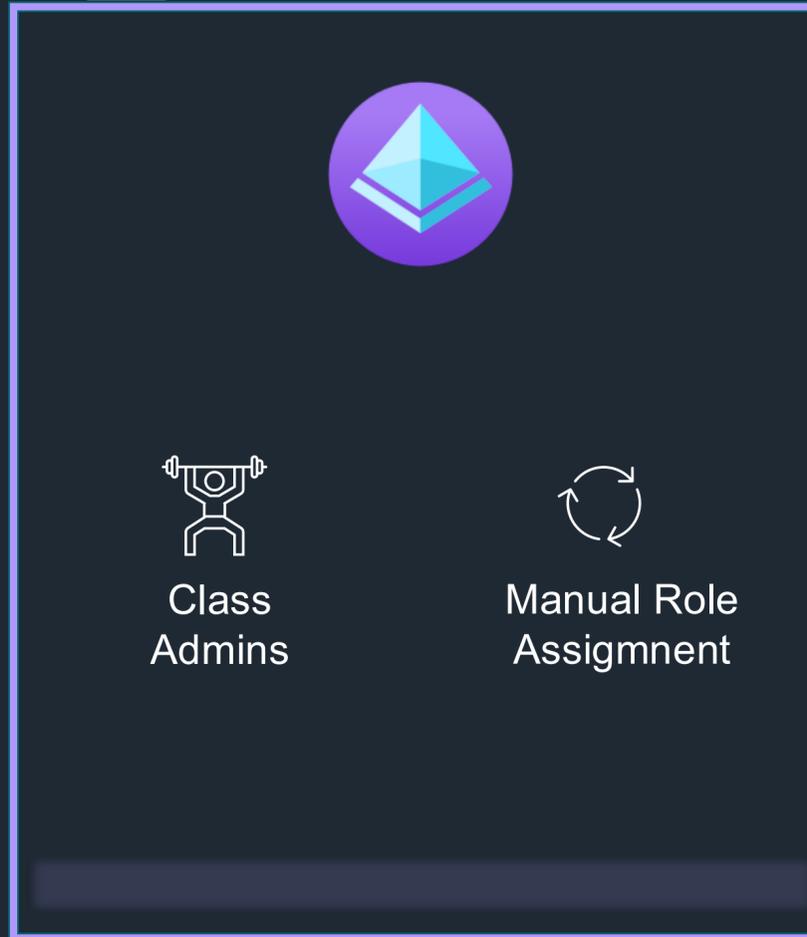
## *Tenant Settings*

- Multiple GAs via Groups*
- Conditional Access*



# School (or Similar) Environment Model

## 2 Class Level Access (AU)



Students are assigned using a dynamic membership rule

Class Admins are assigned to Administrative Units manually

Challenge:

Annual admin changes at the end of the school year

AU Admins change every year

*Do we handle this manually — or automate it?*



PIM Basic

PIM for Groups

Admin Units

# *Demo*

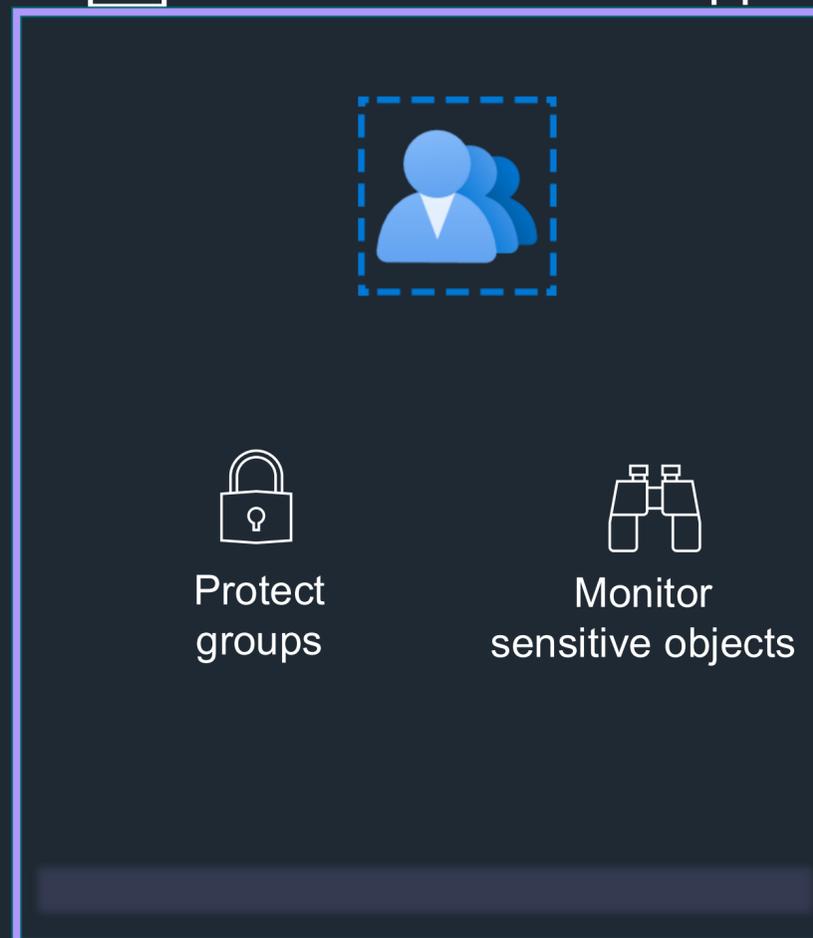
*Delegated permissions:*

- *AU administration settings*
- *Lifecycle workflows (Example)*



# School (or Similar) Environment

## 3 Sensitive Student Support



Control access to groups and objects

Only specific user should have access - no Global Admins

Alert on changes via simple Alert Rule and Action Group

Of course data still needs to be protected  
(*Purview, SPO-permissions, etc.*)



PIM Basic

PIM for Groups

Admin Units

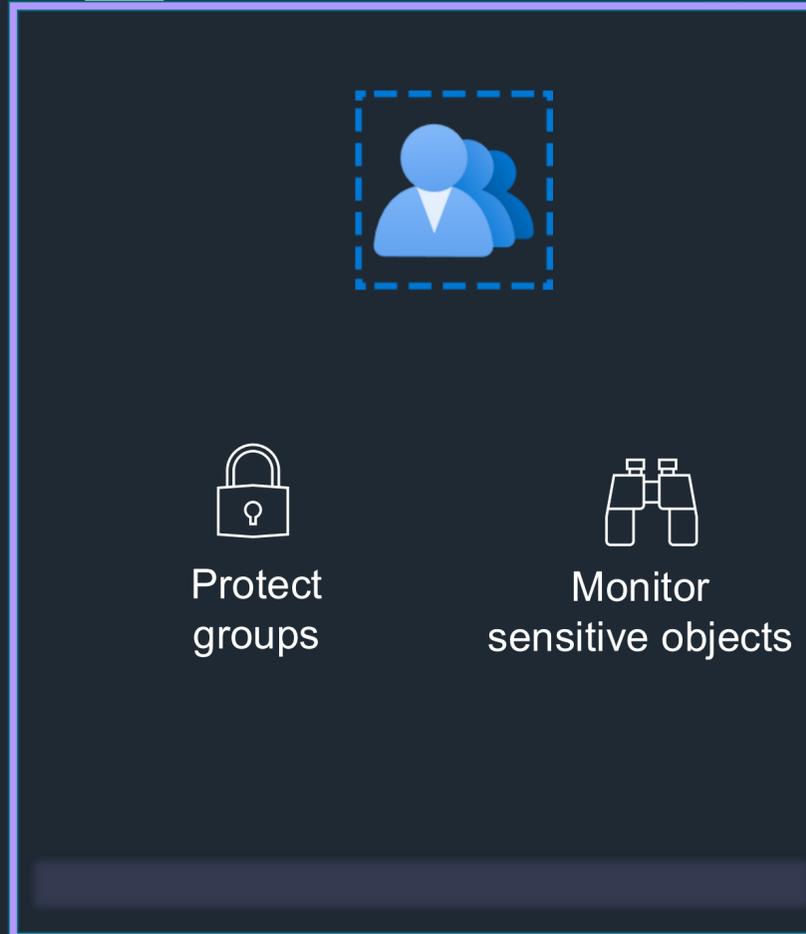
# *Demo*

*Protecting sensitive  
objects in Microsoft Entra ID*



# School (or Similar) Environment Model

## 3 Sensitive Student Support



Control access to groups and objects

Only specific user should have access - no Global Admins

Alert on changes via simple Alert Rule and Action Group

Of course data still needs to be protected  
*(Purview, SPO-permissions, etc.)*

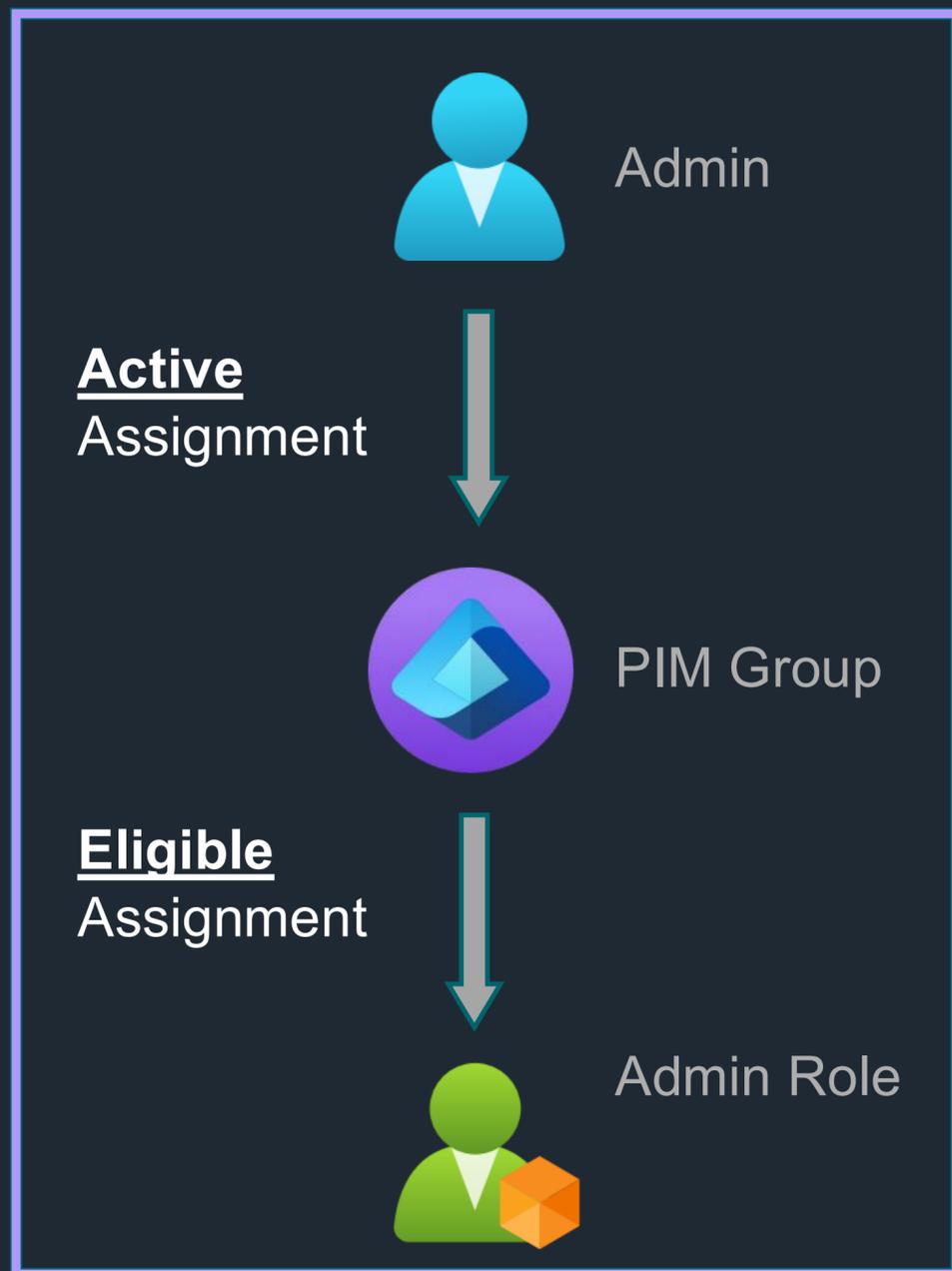


PIM Basic

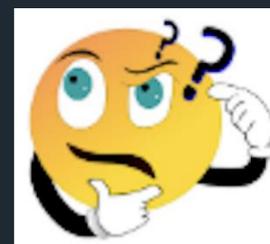
PIM for Groups

Admin Units

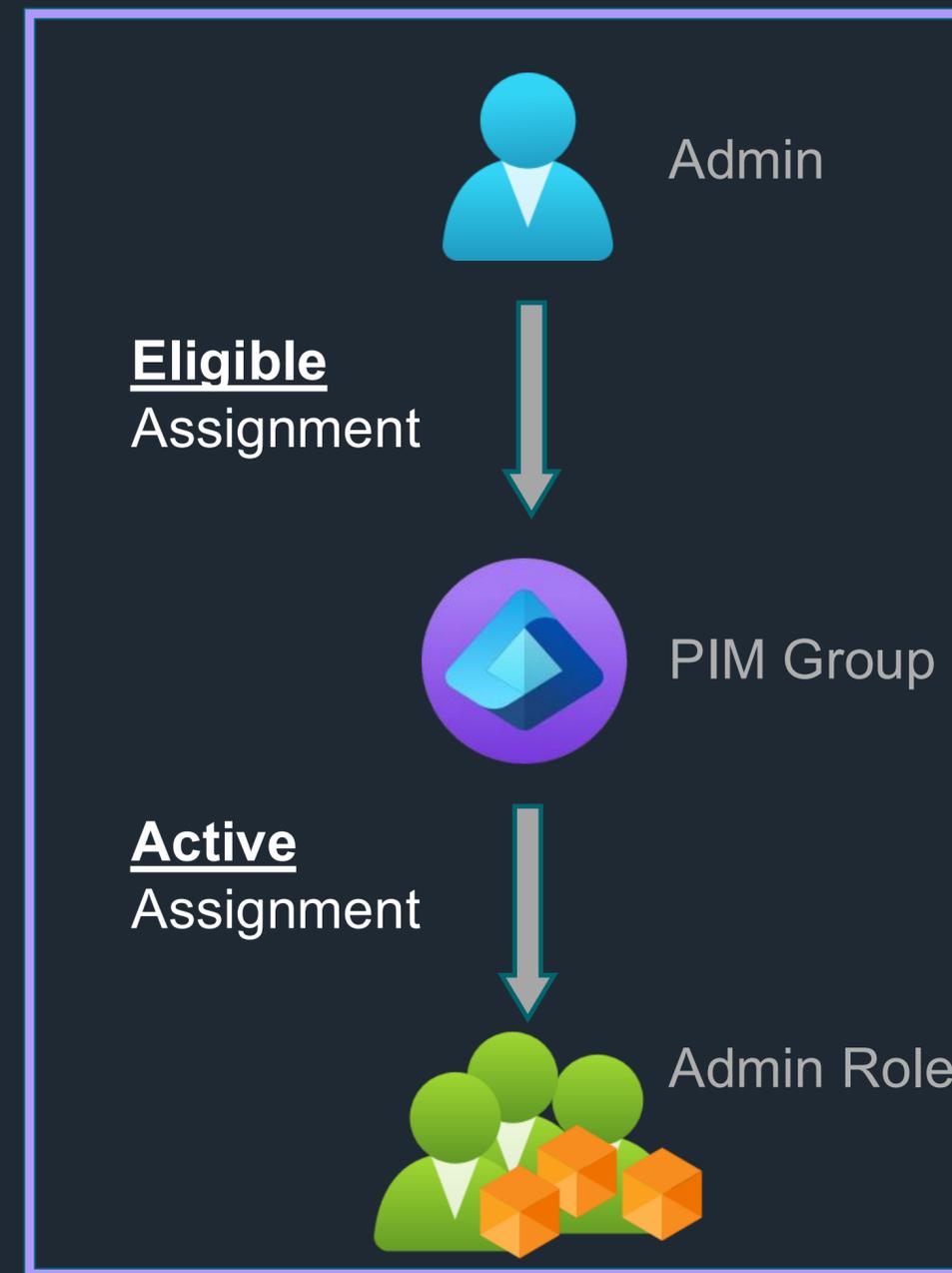
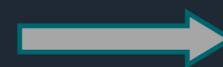
# PIM for Groups – where does eligibility belong?



This way?



That way?



# *Demo*

## *PIM for Groups ...*



Home >

# Privileged Identity Management | Quick start

Privileged Identity Management

<< What's new Get started

Quick start

## Tasks

- My roles
- My requests
- Approve requests
- Review access

## Manage

- Microsoft Entra roles
- Groups
- Azure resources

## Activity

- My audit history

## Troubleshooting + Support

- Troubleshoot
- New support request

# Manage your privileged access

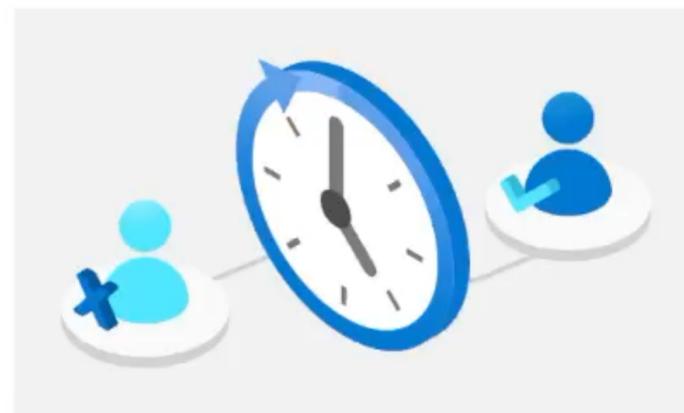
Use Privileged Identity Management to manage the lifecycle of role assignments, enforce just-in-time access policy, and discover who has what roles. [Learn more](#)



### Manage access

Users with excessive access are vulnerable in the event of account compromise. Ensure your organization manages to least privilege by periodically reviewing, renewing, or extending access to resources.

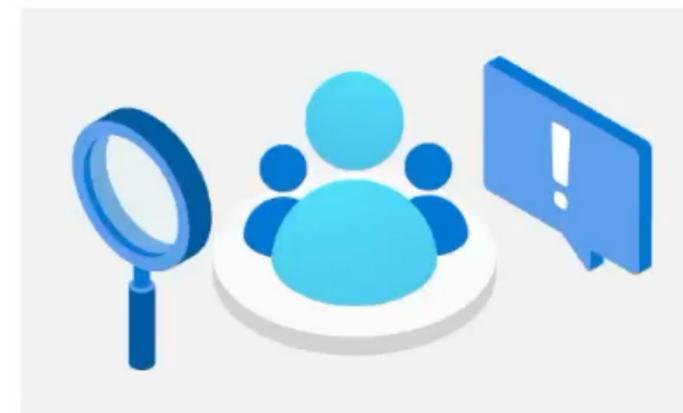
Manage



### Activate just in time

Reduce the potential for lateral movement in the event of account compromise by eliminating persistent access to privileged roles and resources. Enforce just in time access to critical roles with PIM.

Activate



### Discover and monitor

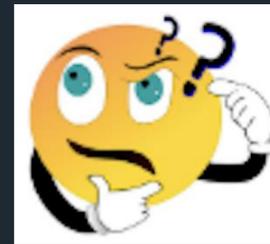
It is common for access to critical resources to go undetected. Ensure you know who has access to what, and receive notifications when new assignments are granted to accounts in your organization.

Discover

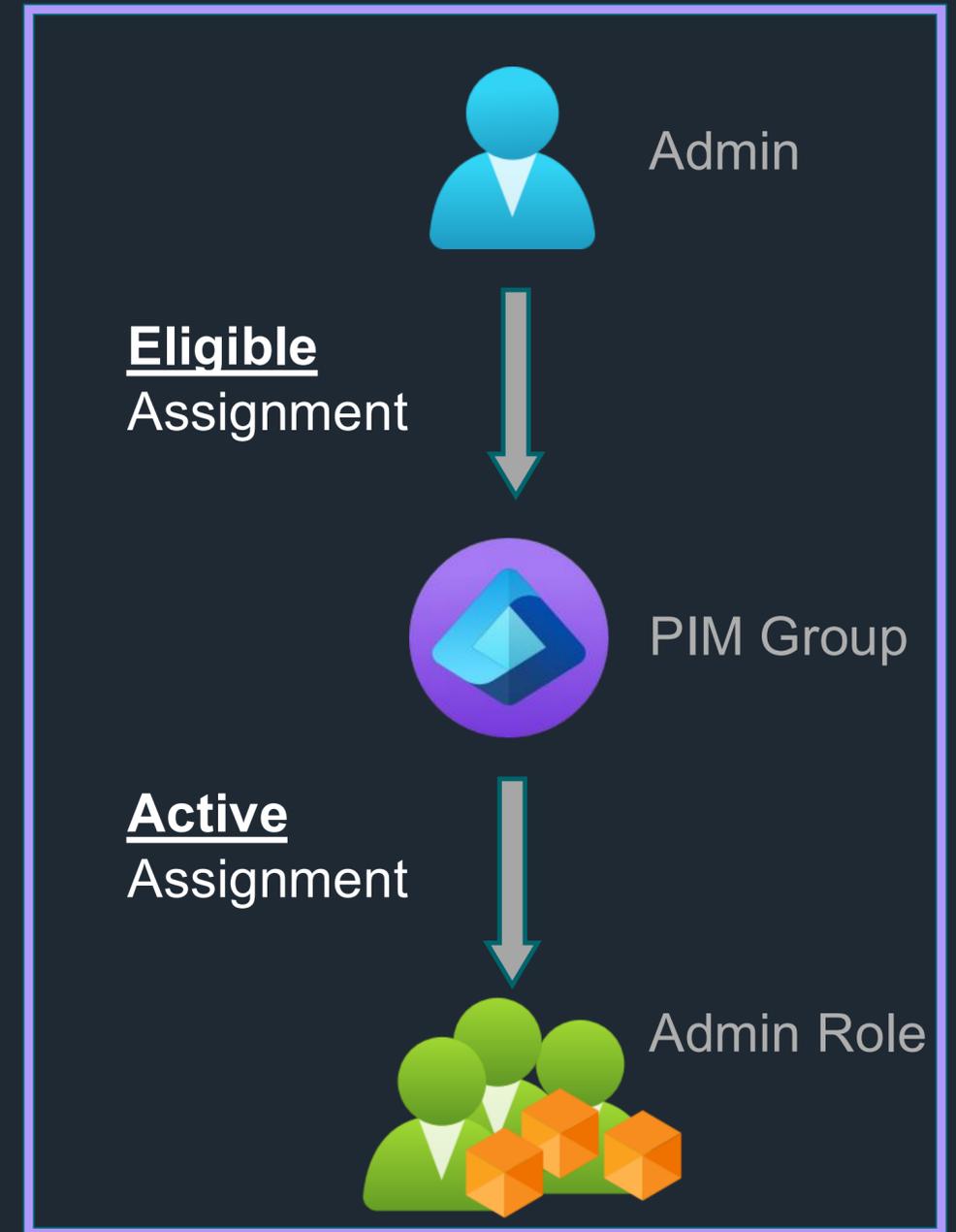
# PIM for Groups – where does eligibility belong?



This way?



That way?



# What else? Things You Should Know!

## ❖ Entra Admin Center Access restricted?

→ direct URL through Azure Portal

→ or via Entra Admin Center

*both links are in the appendix slide*

→ Does not work with *Admin Portal Target in Conditional Access Policy*

## ❖ The fastest way: [aka.ms/pim](https://aka.ms/pim)

Administration center

[Learn more](#) 

Restrict access to Microsoft



Yes

Entra admin center

# A Few More Things You Should Know!

- ❖ **No integration with MyAccess.microsoft.com**  
*(not an Admin Portal Target)*
- ❖ **Don't forget licensing**  
*Users benefiting from PIM must be licensed*
- ❖ **Delayed cleanup with PIM groups – cosmetic only**
- ❖ **Auditing**  
Role activation: Resource audit  
Group activation: Audit logs (**Service**=PIM, **Category**=Group Management)
- ❖ **Ask Security Copilot ...**

Demo ...



- Home
- Entra agents
- Favorites
- Entra ID
- Overview
- Users
- Groups
- Devices
- Agent ID (Preview)
- 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

Microsoft Entra Report on ownerless groups and suggest next steps (assign owner / archive). +2

### Security Copilot agents are here

Discover a whole new way to automate security with AI.  
[Learn more about agents](#)

[Go to agents](#)

### Main Identity LAB

**Tenant ID** f5c07476-f2f0-45bf-8745-34a90b6a2a... [Copy](#)  
**Primary domain** kbcorp2021.onmicrosoft.com [Copy](#)

<b>61</b> <a href="#">View users</a>	<b>55</b> <a href="#">View groups</a>
<b>24</b> <a href="#">View devices</a>	<b>34</b> <a href="#">View apps</a>

**Richard Langley**  
 6614c641-2c2c-4fa4-af93-01835fc05d77 [Copy](#)  
[View user profile](#)

#### My role assignments

1

- High privileged role assignments
- Other role assignments

[Manage my roles](#)

### Users at high risk

No detections found

No user detections with risk level "high" in the last 365 days.

[View high risk users](#)

- ### Shortcuts
- Add
  - User sign-ins
  - Audit logs
  - Authentication Methods
  - Blocked users
  - Domain names

### Copilot

Use Copilot to support your work in identity and access management. Select one of the suggestions below to get started.

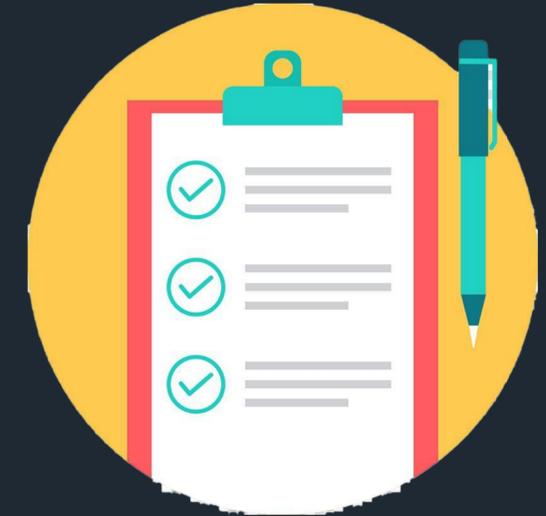
- Summarize**  
Report on ownerless groups and suggest next steps (assign owner / archive).
- Analyze**  
List all apps with expiring credentials.
- Troubleshoot**  
List devices that have been inactive for over 30 days for an audit review.
- Learn**  
What is the guest invite setting in my tenant?

List my eligible Entra ID directory roles managed by PIM

[+](#)

## Wrap up - takeaway

- ❖ JIT and JEA on a group-to-role basis (1:1 or 1:n relationships)
- ❖ Administrative Units + PIM for Groups enable real-world delegation models
- ❖ Full automation of admin roles is intentionally limited – but governance fills the gap



# Further Resources ...



## Microsoft Learn Licensing Infos

Use Microsoft Entra groups to manage role assignments

Restricted management administrative units in Microsoft Entra ID



## Best Practices & Community

Restricted management administrative units in Microsoft Entra ID

custom activation is not working in PIM -> Tokenrefresh

Direkt URL thru Azure Portal

Direct URL thru Entra Portal



## NothingButCloud Blog

Zero Trust in Entra ID: Monitoring Break-Glass Accounts and Other Sensitive Operations (sensitive student demo)

Demystifying Assignment Strategies with 'PIM for Groups'

When Static Roles Are Not Enough: Dynamic Admin Assignment for Entra AUs (class admin demo)

<https://github.com/KlaBier/Powershell/tree/main/CreateSecCopilotSCU>

PREMIUM SPONSOR



# ADRIATICS TECH SUMMIT 2026

DIAMOND SPONSOR



PARTNER



GOLD SPONSOR



SILVER SPONSOR



GENERAL MEDIA PARTNER



BUSINESS MEDIA PARTNER



# ADRIATICS TECH SUMMIT 2026

30.3.-1.4. / SARAJEVO / BIH





## Meet the Speaker

### Klaus Bierschenk

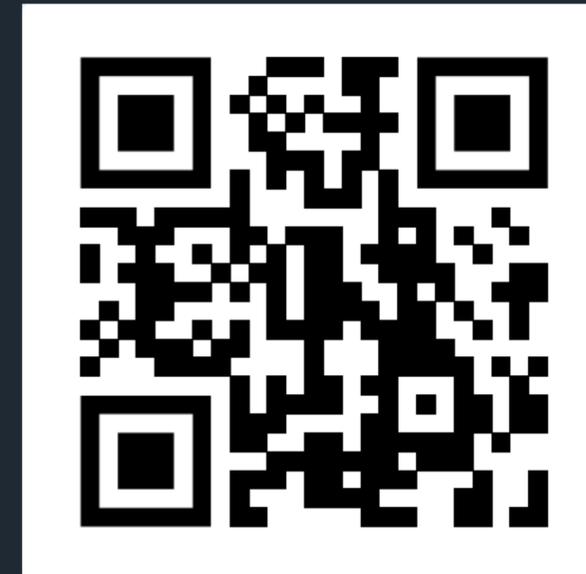
Director Consulting Expert / CGI Germany

- Based in Murnau, Bavaria
- Living with my family, two snakes, two cats – and lots of other animals my cats bring home from time to time

 [linkedin.com/in/klabier/](https://www.linkedin.com/in/klabier/)

 [Klaus@nothingbutcloud.net](mailto:Klaus@nothingbutcloud.net)

 <https://NothingButCloud.net>



Slides and resources  
[nothingbutcloud.net](https://nothingbutcloud.net)

*Thank you very much*

*Happy to take  
your questions*

```

4
5 # Connect to the correct tenant and subscription
6 Connect-AzAccount -Tenant 'YOUR TENANT ID' -SubscriptionId 'YOUR SUBSCRIPTION ID'
7
8 # Resource Group for Security Copilot capacity
9 New-AzResourceGroup -Name "SecurityCopilotRG" -Location "WestEurope"
10
11 # One-time operation per subscription
12 # Depending on Tenant rollout stage, either Microsoft.Security OR Microsoft.SecurityCopilot may be required
13 #Register-AzResourceProvider -ProviderNamespace "Microsoft.Security"
14 #Register-AzResourceProvider -ProviderNamespace "Microsoft.SecurityCopilot"
15
16 # Create a Security Copilot capacity (SCU)
17
18 New-AzResource -ResourceName "SecurityCopilotSCU" `
19     -ResourceType "Microsoft.SecurityCopilot/capacities" `
20     -ResourceGroupName "SecurityCopilotRG" `
21     -Location "westeurope" `
22     -ApiVersion "2023-12-01-preview" `
23     -Properties @{numberOfUnits=2; crossGeoCompute="NotAllowed"; geo="EU"} `
24     -force
25
26 # Important: delete the SCU or the entire resource group afterwards to avoid costs
27 # DeleteSecCopilotSCU.ps1
28

```



CreateSecCopilotSCU > DeleteSecCopilotSCU.ps1

```

1 # Quick delete the entire RG with the associated SCU
2
3 Connect-AzAccount -Tenant 'YOUR TENANT ID' -SubscriptionId 'YOUR SUBSCRIPTION ID'
4 |
5 Remove-AzResourceGroup -Name "SecurityCopilotRG" -force
6

```

PS C:\Users\klaus\OneDrive\GitContent\Powershell>