PIMp Your Administration: Strengthening Zero Trust with Entra ID

Klaus Bierschenk
Director Consulting Expert, CGI

M365 Con

How many Entra ID Roles do we have today?

134

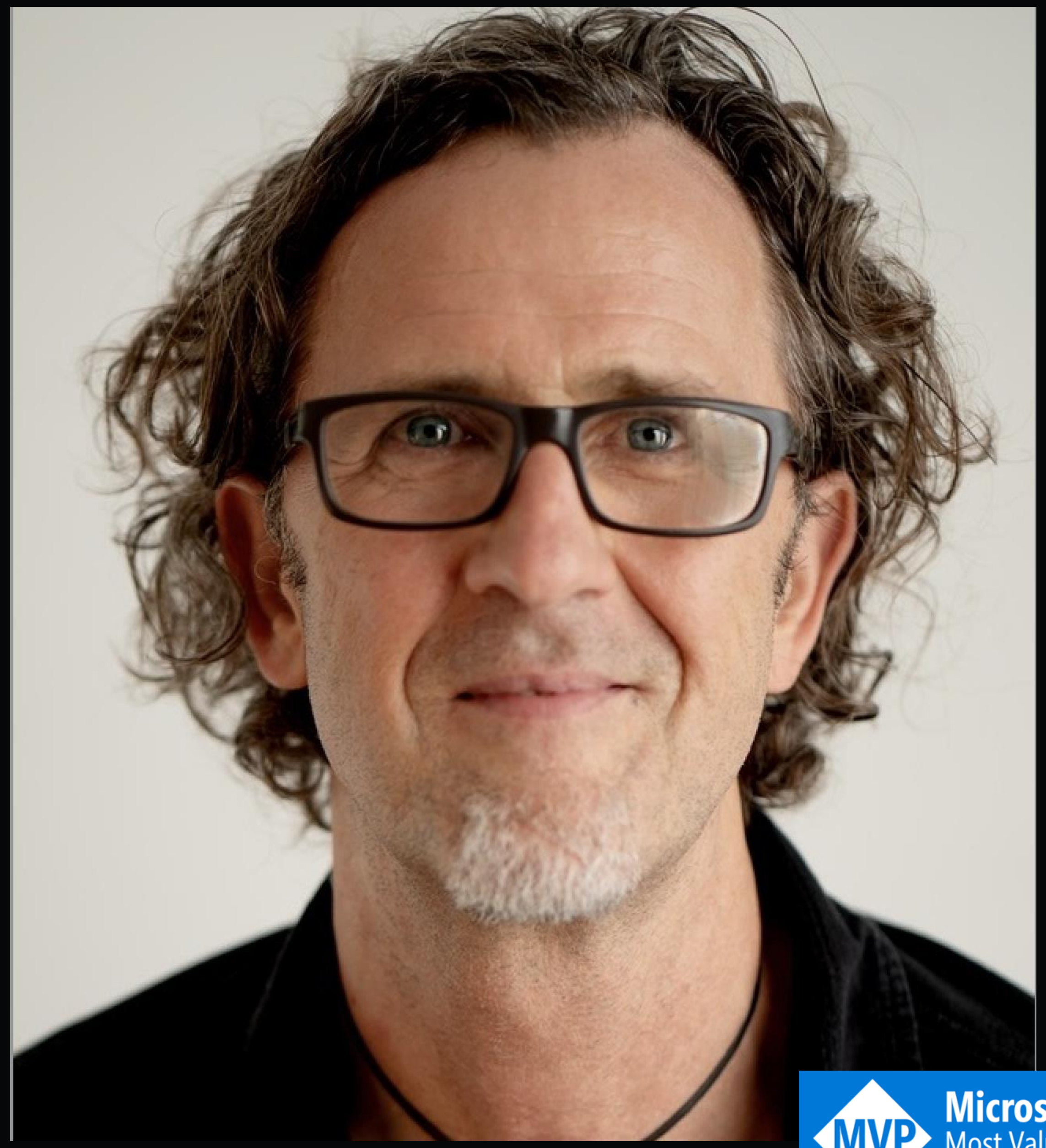
How many Azure Roles do we have today?

828

This is why you need PIM for JIT and JEA

M365 Con

Meet the Speaker



MVP Microsoft® Most Valuable Professional

Klaus Bierschenk

Director Consulting Expert / CGI Germany

- Based in Murnau, Bavaria
- Living with my Family, two cats, and two snakes
- Mountain lover and Ultrarunner

in linkedin.com/in/klabier/

✉ 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

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

2 Class Level Access

- Class Admins
- Manual Role Assignmnent

3 Sensitive Student Support

- Protect groups
- Monitor sensitive objects

PIM Basic

PIM for Groups

Admin Units

School (or Similar) Environment Model

1 School-wide

Mulitple GA configurations

No permanent GAs

No User Entra Admin Center access

No changes to default roles

Use PIM for Groups to manage multiple Global Administrator access

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

- Built-in Roles are not modified

- Protected Actions

PIM-GA-ConfigEngineer - Micro
Conditional Access - Microsoft
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Overview/menuId//fromNav/Identity
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
6
klaus@kbrun.de
MAIN IDENTITY LAB (KBCORP20...
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 >
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
Create new policy
Create new policy from templates
Refresh
Got feedback?
Getting started
Overview
Coverage
Tutorials

Conditional Access | Overview

Microsoft Entra ID

Manage, govern, and protect your agent identities in one place to keep your tenant secure. Learn more about Microsoft Entra Agent ID capabilities

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

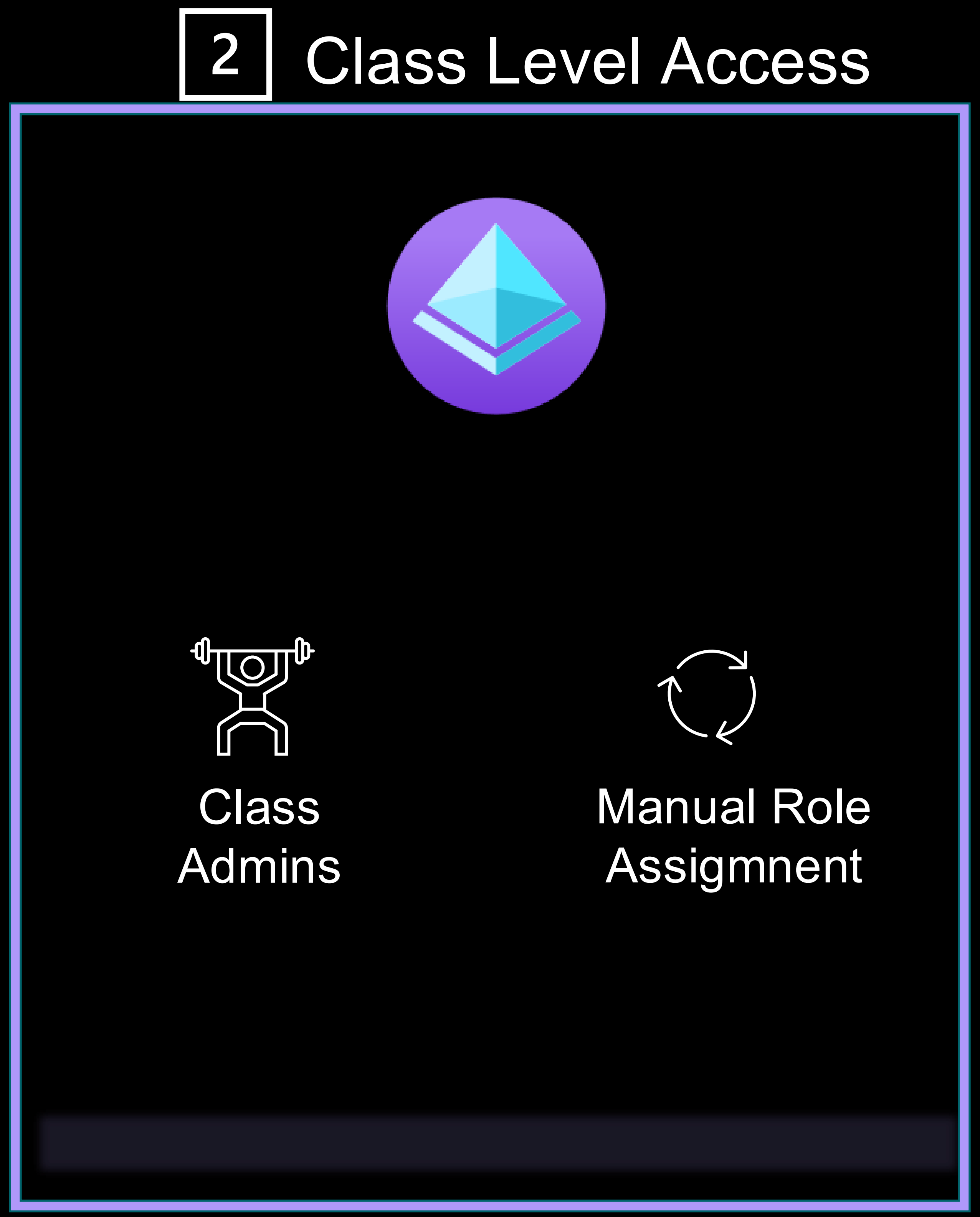
See all unmanaged devices

Applications

Browse a list of applications that are not protected by your policies.

View top unprotected apps

School (or Similar) Environment Model



2 Class Level Access

Class Admins

Manual Role Assignment

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

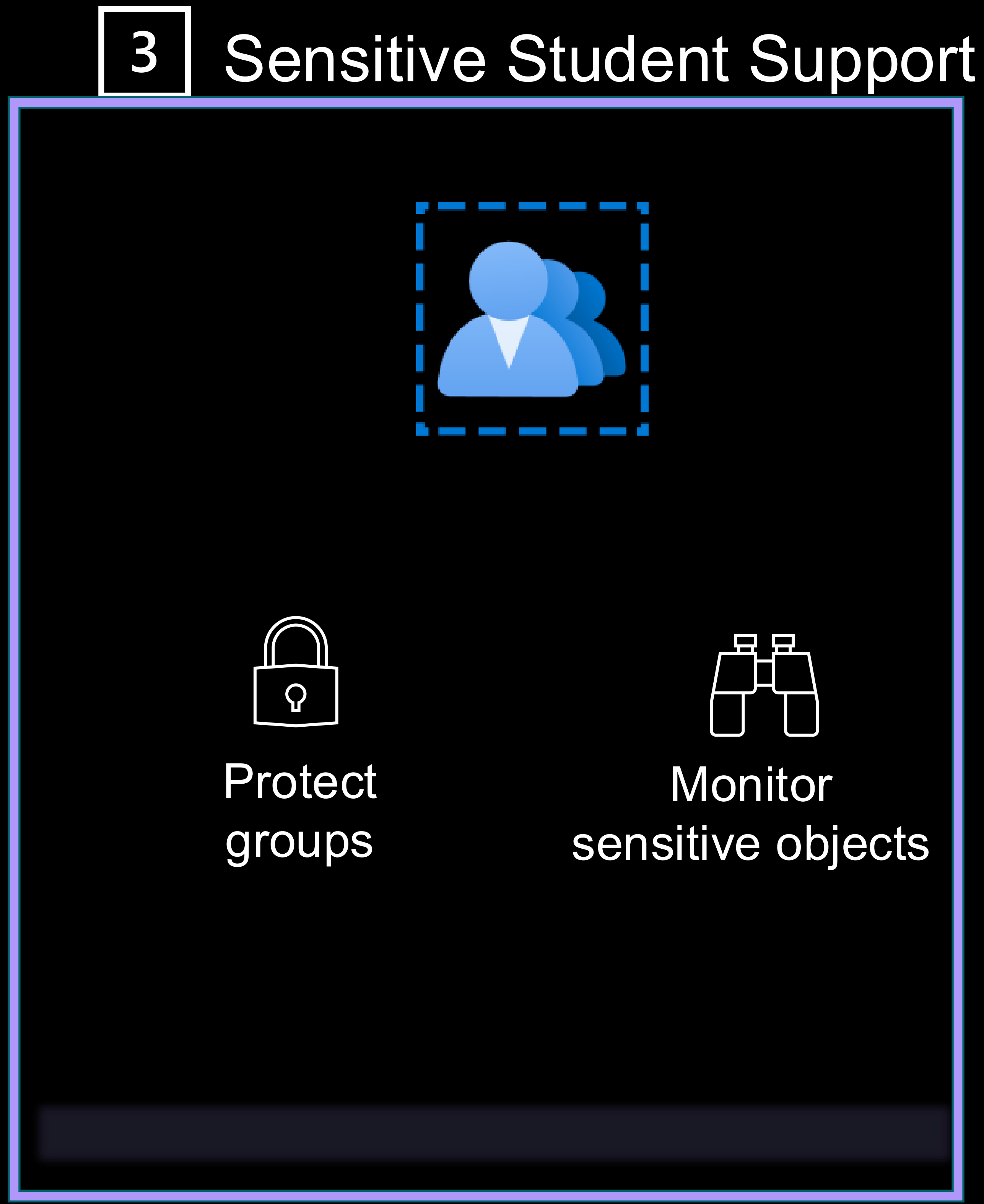
Admin Units

Demo

Delegated permissions:

- AU administration settings
- Lifecycle workflows (Example)

School (or Similar) Environment Model



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

Blog alert…

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

PIM Basic

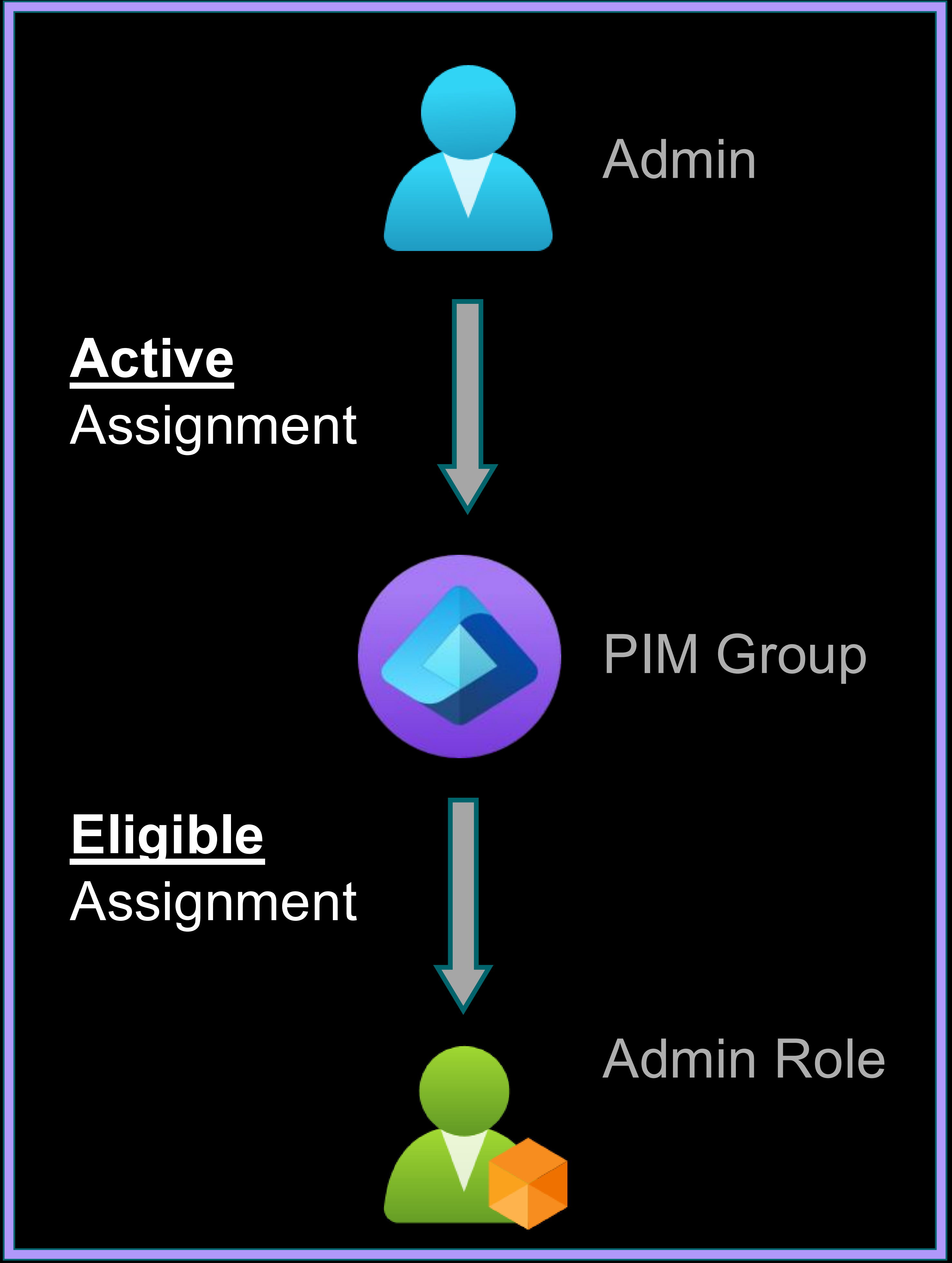
PIM for Groups

Admin Units

Demo

Protecting sensitive
objects in Microsoft Entra ID

PIM for Groups – where does eligibility belong?



Admin

Active
Assignment

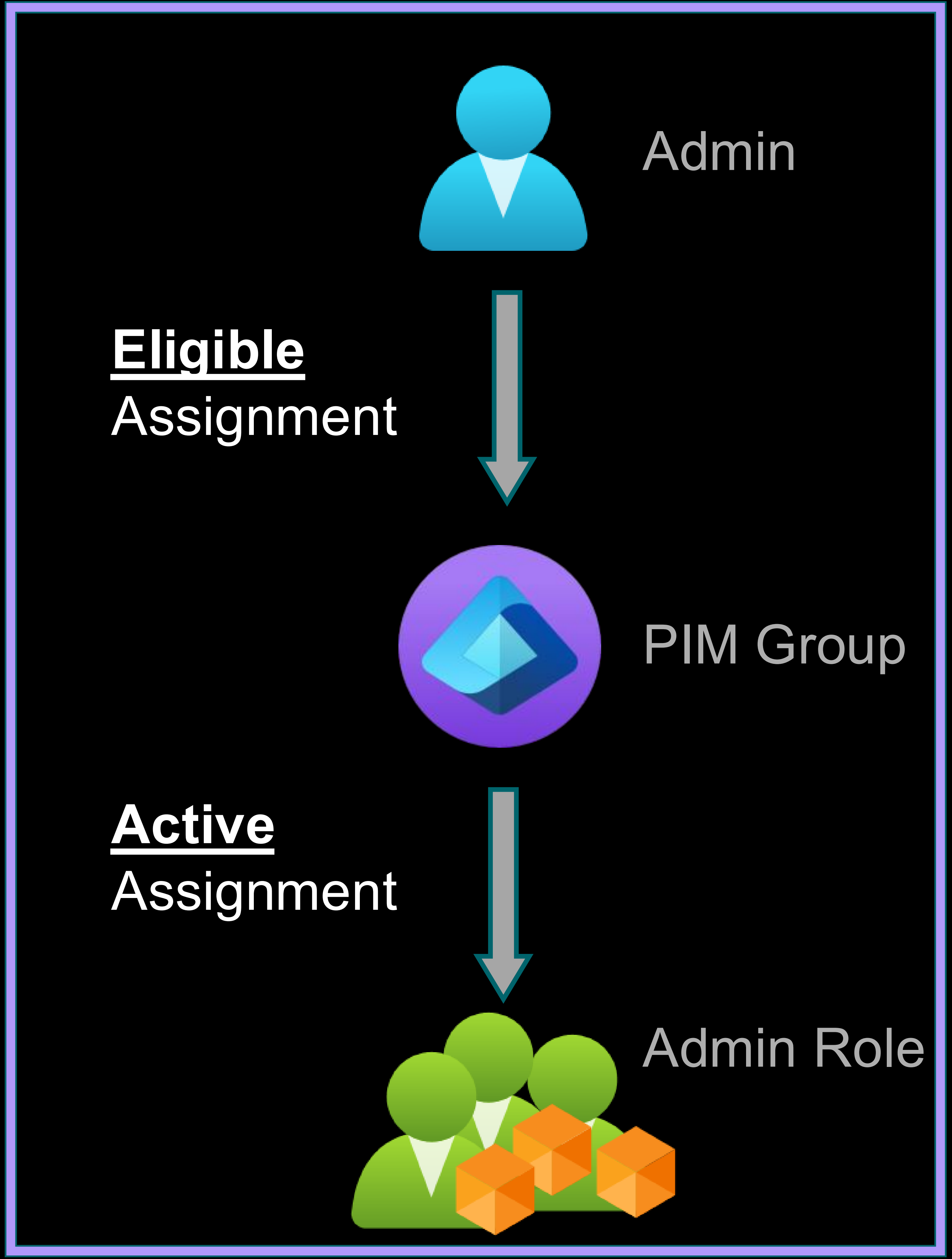
PIM Group

Eligible
Assignment

Admin Role

This way?

That way?



Admin

Eligible
Assignment

PIM Group

Active
Assignment

Admin Role

Blog alert…

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept

Demo

PIM for Groups …

Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
5
klaus@kbrun.de
MAIN IDENTITY LAB (KBCORP20...
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

https://entra.microsoft.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/menuId/Overview

What else? Things You Should Know!

- Role activation not visible? Takes too long?
  https://aka.ms/pim/tokenrefresh
  (not officially documented)

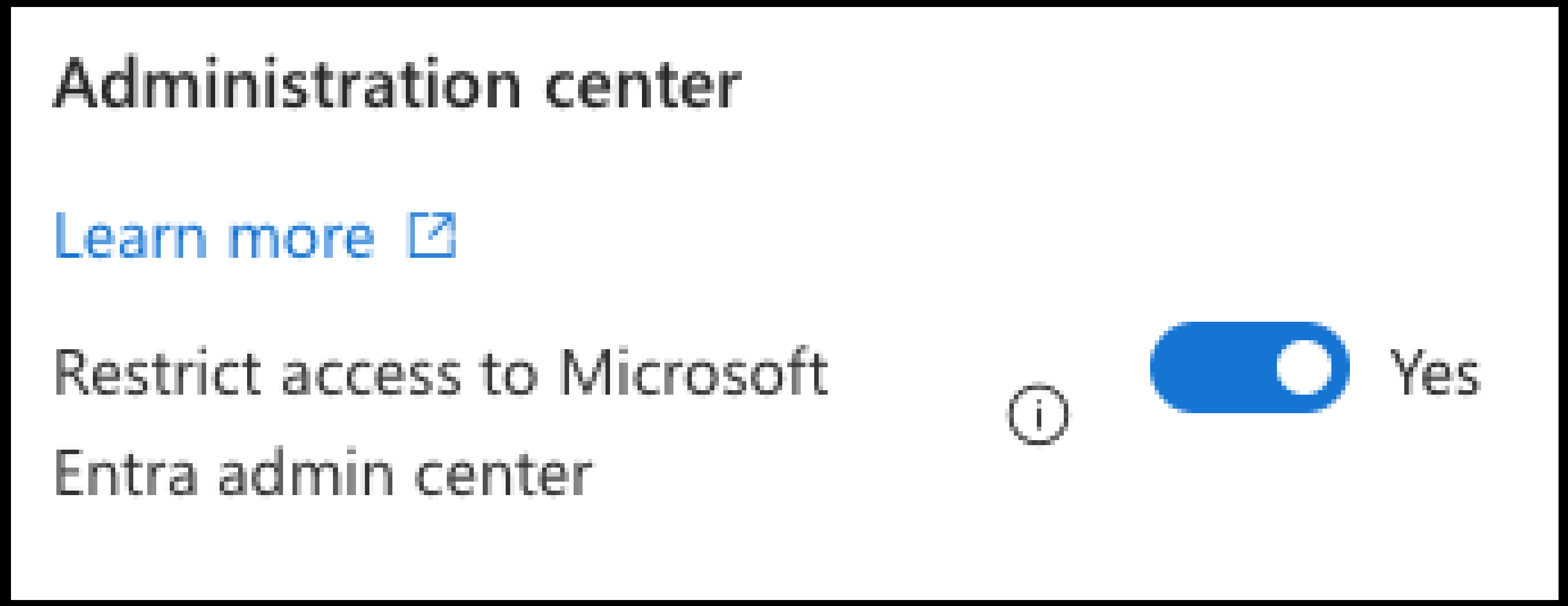
- Entra Admin Center Access restricted?

  → direct URL through Azure Portal

  → or via Entra Admin Center
  both links are in the appendix slide

  → *Does <u>not work</u> with Admin Portal Target in Conditional Access Policy*

- The fastest way: aka.ms/pim



Administration center

Learn more

Restrict access to Microsoft Entra admin center ⓘ ● Yes

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

Security Copilot and PIM …

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

Langley@kbrun.de
MAIN IDENTITY LAB (KBCORP20...

- 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...

Primary domain kbcorp2021.onmicrosoft.com

61 View users	55 View groups
24 View devices	34 View apps

Richard Langley

6614c641-2c2c-4fa4-af93-01835fc05d77

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

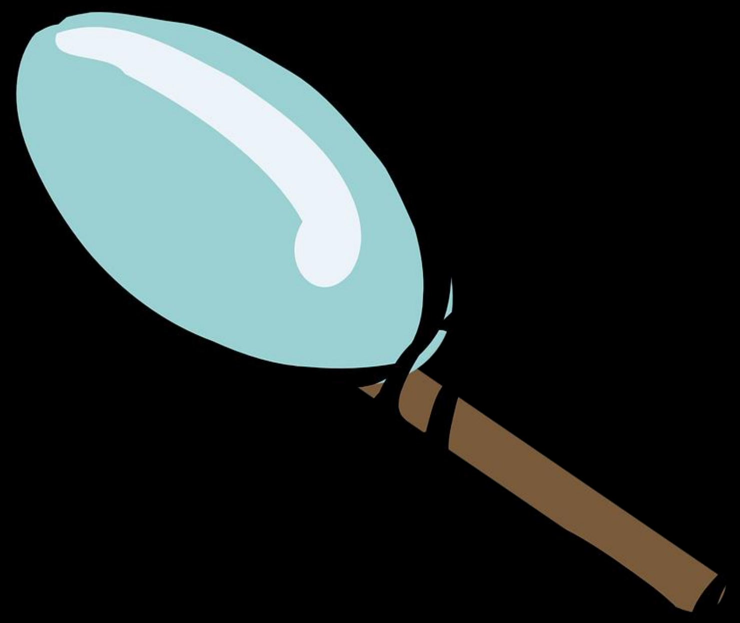
Wrap up - takeway

- 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

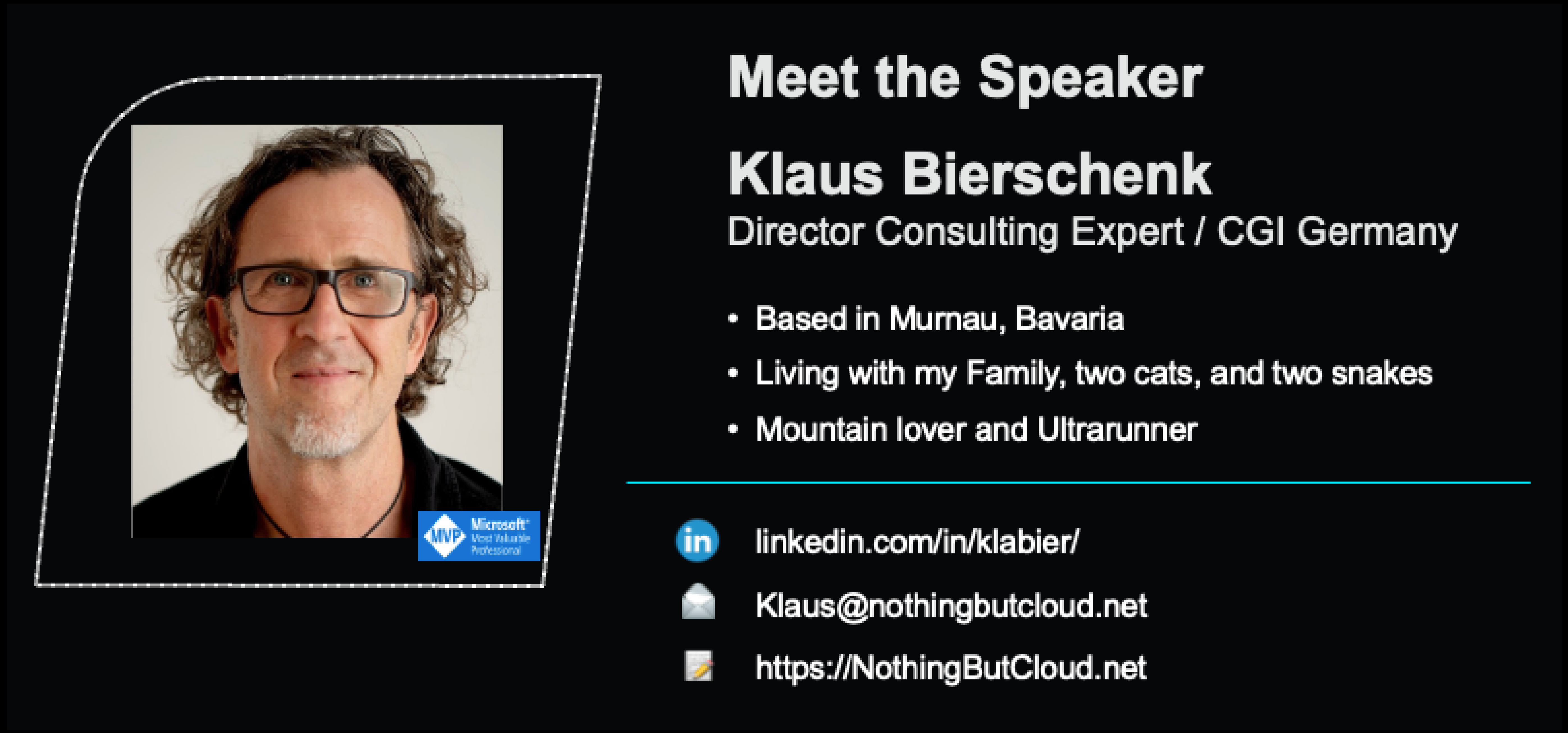
NothingButCloud Blog

Zero Trust in Entra ID: Monitoring Break-Glass Accounts and Other Sensitive Operations

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



Meet the Speaker

Klaus Bierschenk

Director Consulting Expert / CGI Germany

- Based in Murnau, Bavaria
- Living with my Family, two cats, and two snakes
- Mountain lover and Ultrarunner

in linkedin.com/in/klabier/

Klaus@nothingbutcloud.net

https://NothingButCloud.net

Thank you 👍

Questions?