ECS 2026

PIMp Your Administration

Klaus Bierschenk
Director Consulting Expert, CGI Germany

linkedin.com/in/klabier/

Klaus@nothingbutcloud.net

https://NothingButCloud.net

Microsoft® Most Valuable Professional

EXPERTS INSIDE

Teaming up with EasyLife 365

NER

Microsoft

TECHNOLOGY PARTNER

run events

DIAMOND

LightningTools

sitaas

ShareGate

veeam

ECS 2026

05-07 MAY | COLOGNE | GERMANY

PLATINUM

365 TRIBE

ADOPTION. CHAMPIONED

daenet

daenet – an AVI Digital company

DEKOM

dox42

automate your documents integrate your data

glueck kanja

delaware

involv

ITENOS

IT's us.

Rencore

SOLUTIONS 2SHARE

skybow

SquaredUp

Syskit

OASE

YASH Technologies

More than what you think.

Jabra GN

365 HEROES

Orchestry

Capgemini

AvePoint

infobip

SHURE

neat.

GOLD

experlogix

protiviti

Global Business Consulting

apps 365

BCC

Hive

VISIONET

Engineering. Simplified.

Yealink

Gamma

ScriptRunner

LEAP XPERT

Responsible Business Communication

mscrm-addons.com

Your company for MS-CRM ADD-ONS!

envision IT

proventeq

TD SYNNEX

SILVER

Apvee

do more with less

CROSSWARE

FLEXCOM

ichicraft

pangenda

pointfire

Multilingual SharePoint

rocketta

EasyEntra

FrontFox

u2u

tabella

all about documents

zenitech

BRONZE

Alpha Variance Solutions | GmbH

kurmi

Powell

INTELLITY

FUTURE MAKER SILVER

yasp

workplace buddy.

2501 AI

FUTURE MAKER BRONZE

ARGOS

MEDIA PARTNER

AI Tools Network

Times Of AI

AIPressRoom

Technology Record

IT-Schulungen.com

Technology & Transformation

CAPITALBAY NEWS

AI&ML events

How many Entra ID Roles do we have today?

134

How many Azure Roles do we have today?

828

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 (AU)

Class Admins

Manual Role Assigmnent

3 Sensitive Student Support

Protect groups

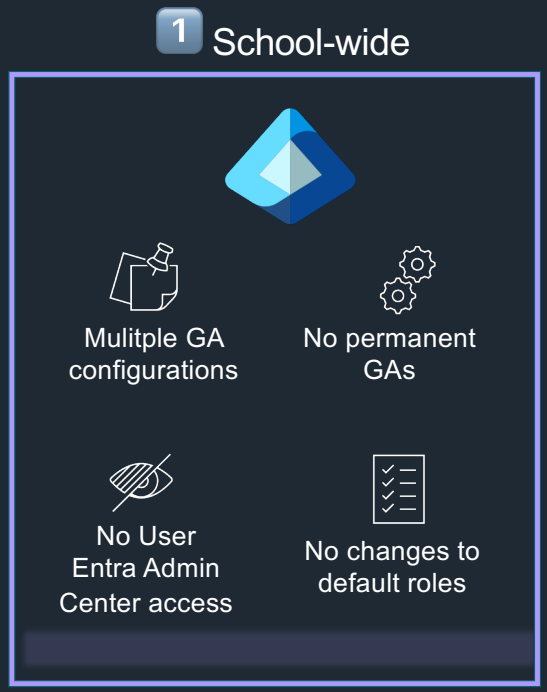
Monitor sensitive objects

PIM Basic

PIM for Groups

Admin Units

School (or Similar) Environment Model



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

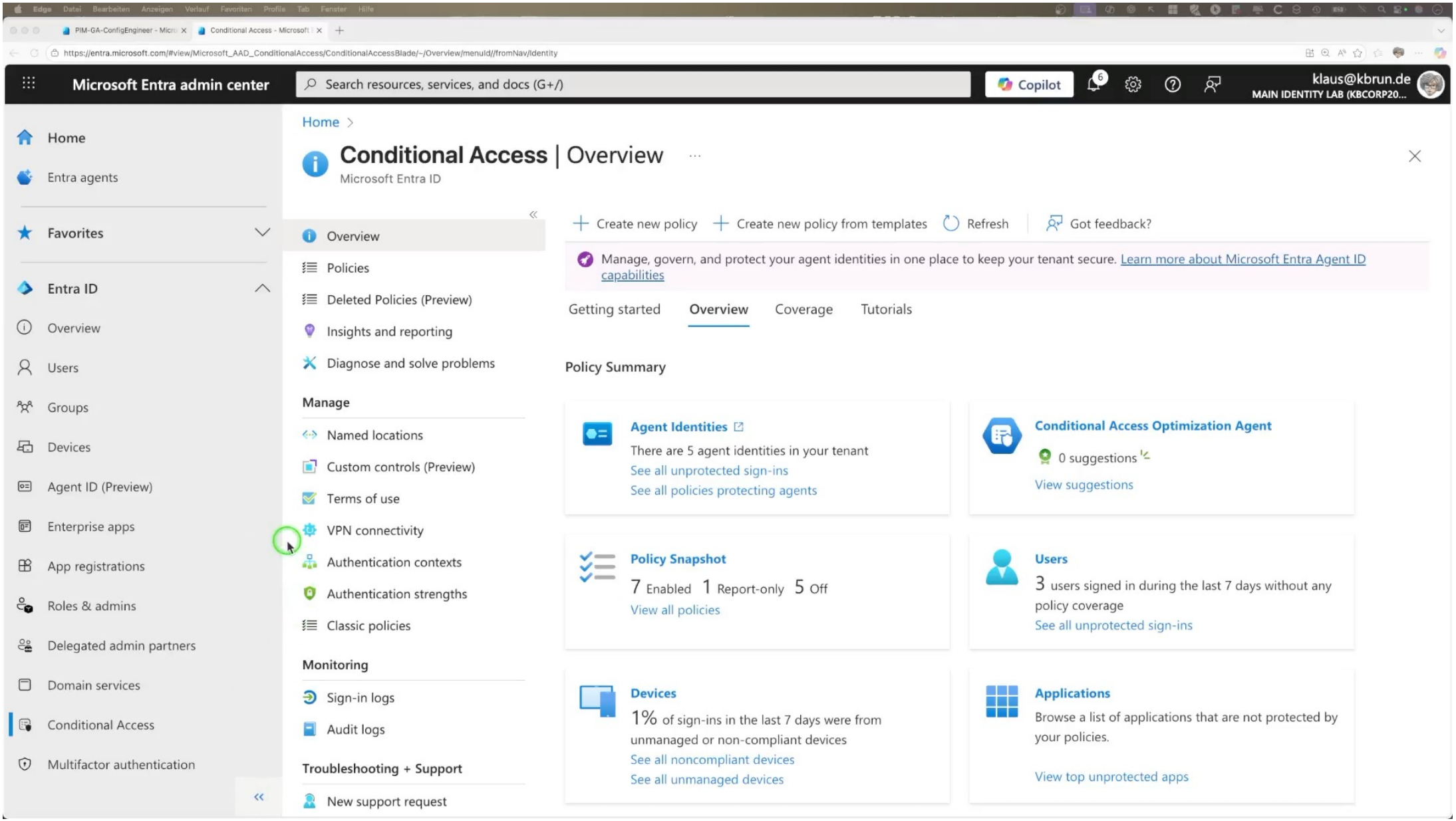
Admin Units

Demo

Tenant Settings

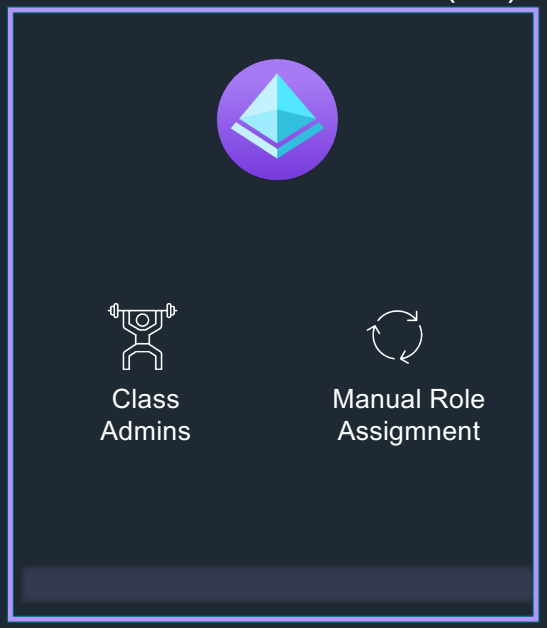
- Multiple GAs via Groups

- Conditional Access


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
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
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
Create new policy
Create new policy from templates
Refresh
Got feedback?
Manage, govern, and protect your agent identities in one place to keep your tenant secure. Learn more about Microsoft Entra Agent ID capabilities
Getting 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

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

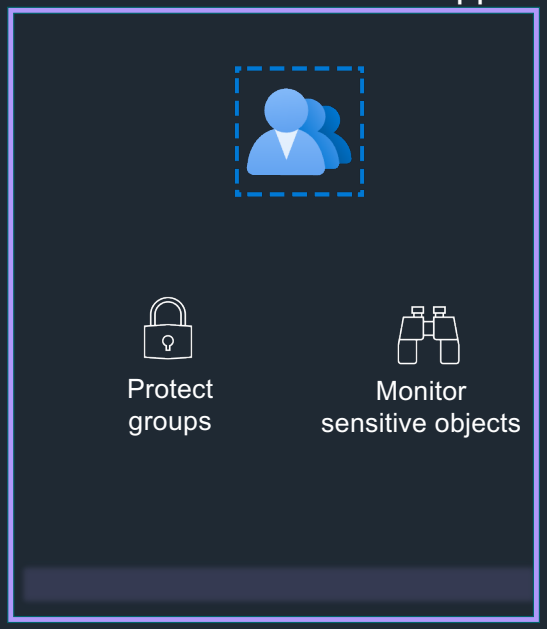
Demo

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

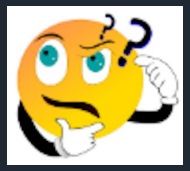
Admin Units

Demo

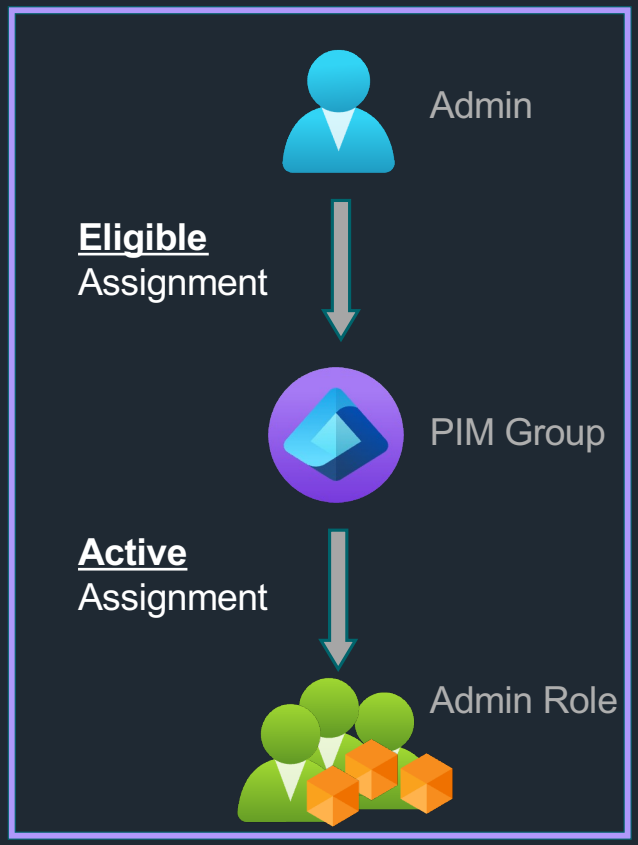
Protecting sensitive objects in Microsoft Entra ID

PIM for Groups – where does eligibility belong?

This way?



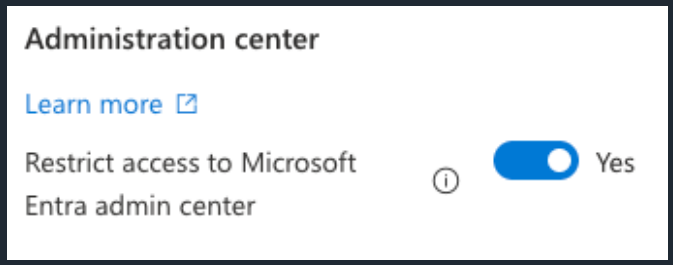
That way?



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

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

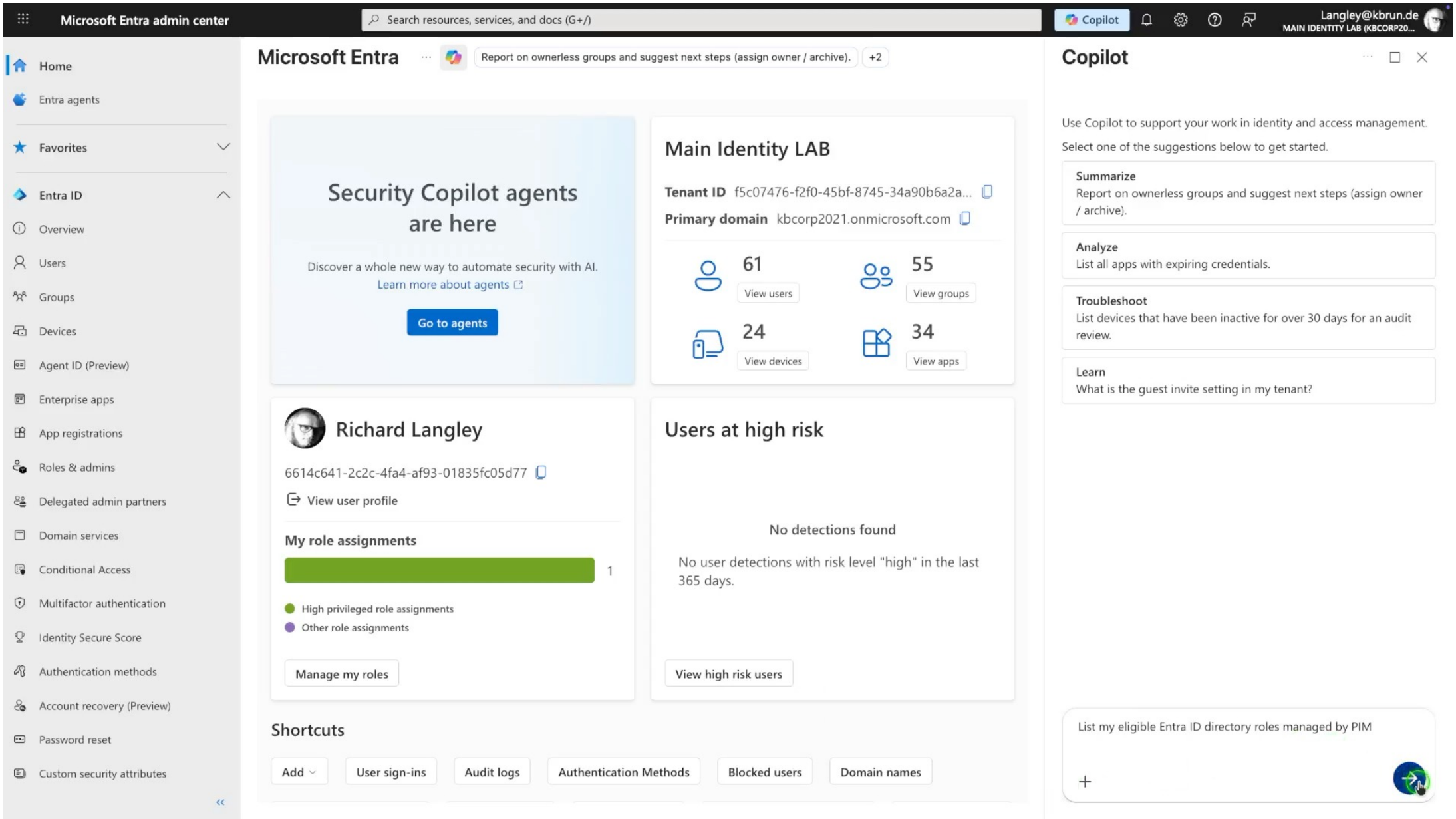


- The fastest way: aka.ms/pim

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 …


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

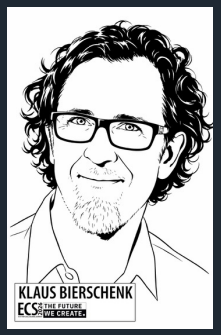
NothingButCloud Blog

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



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/
Klaus@nothingbutcloud.net
https://NothingButCloud.net

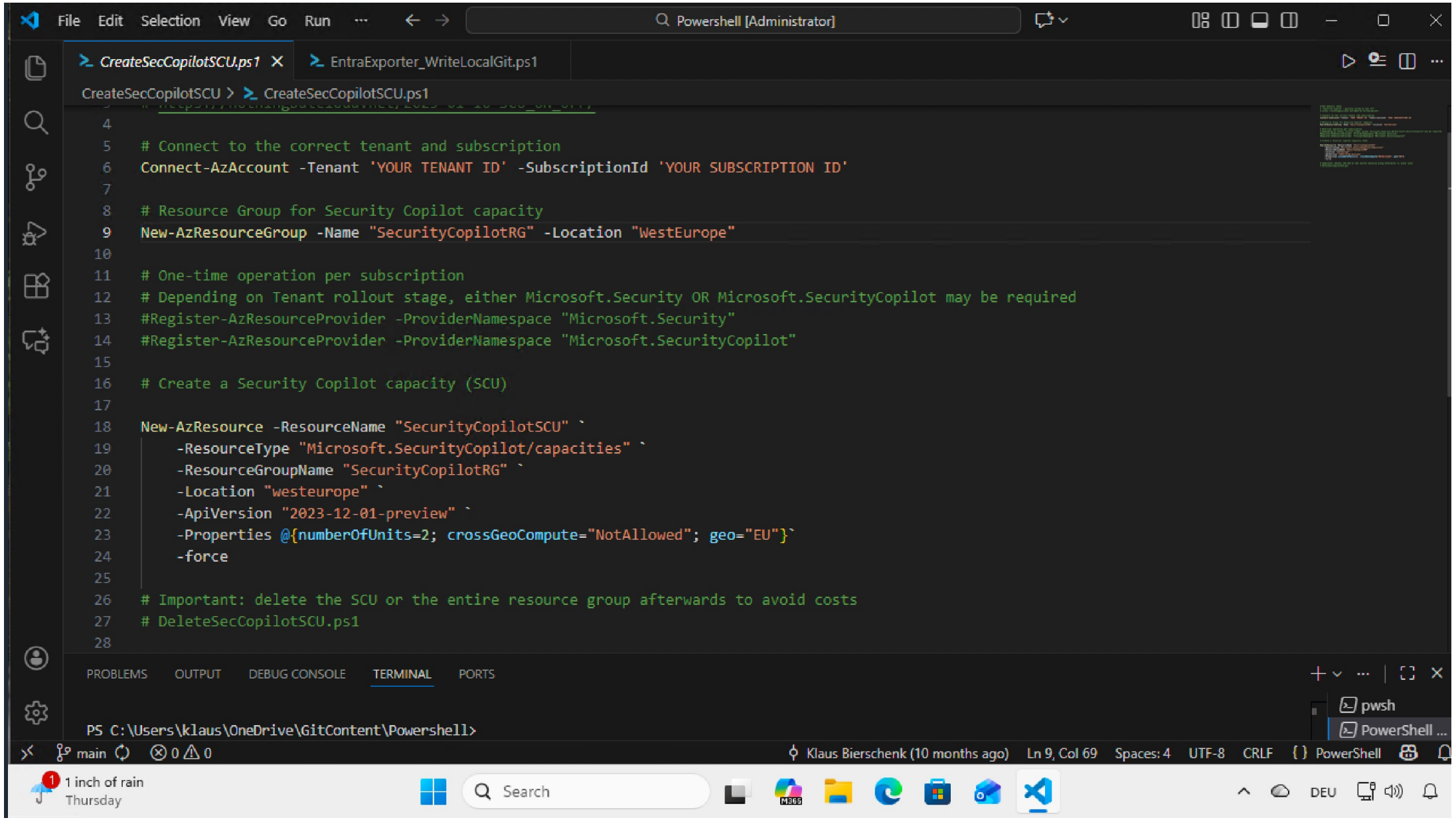
Microsoft® Most Valuable Professional

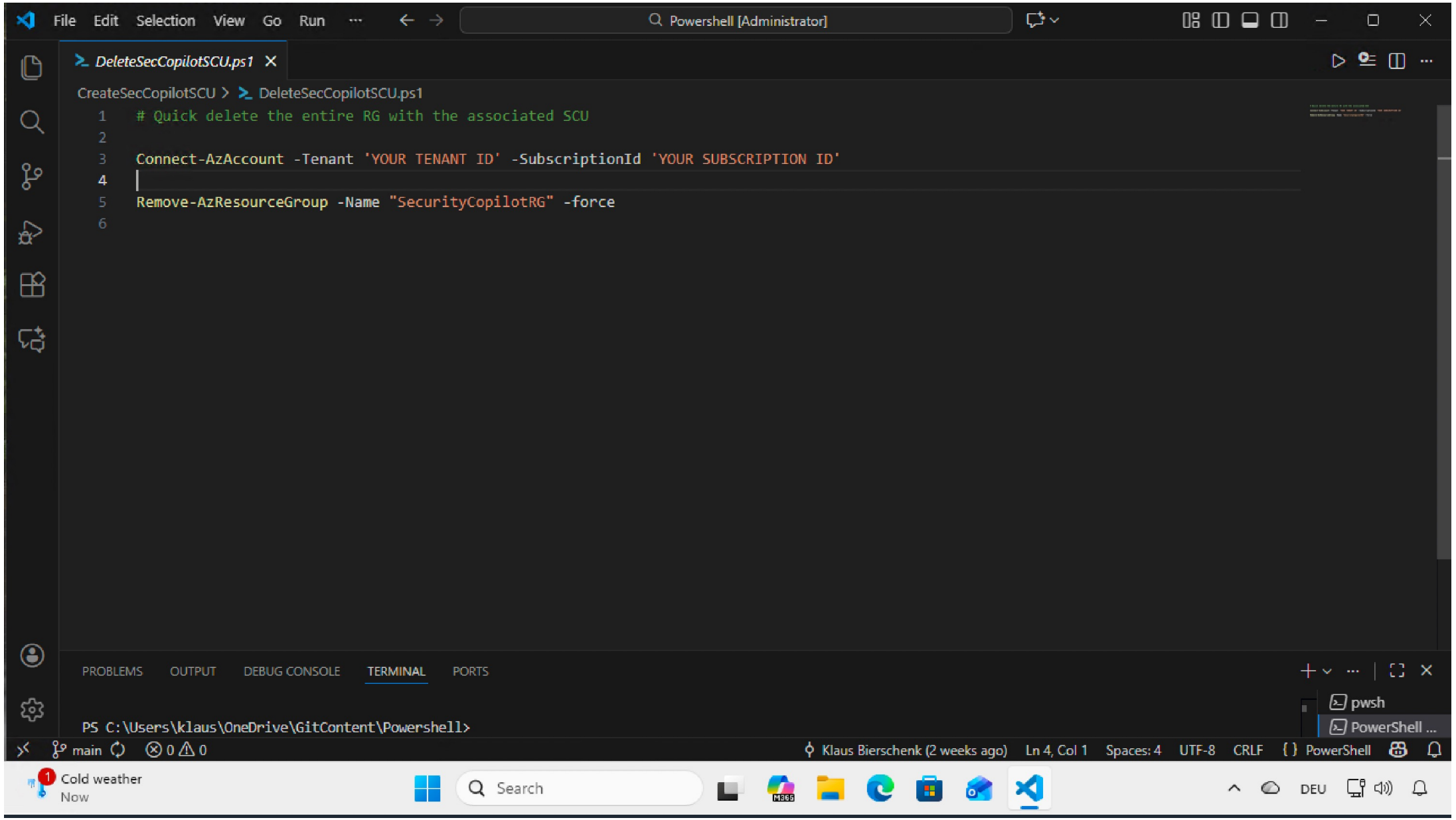
Slides and resources
nothingbutcloud.net

Upload today evening

Thank you very much

Happy to take your questions


File Edit Selection View Go Run ···
Powershell [Administrator]
CreateSecCopilotSCU.ps1
EntraExporter_WriteLocalGit.ps1
CreateSecCopilotSCU > CreateSecCopilotSCU.ps1
Connect to the correct tenant and subscription
Connect-AzAccount -Tenant 'YOUR TENANT ID' -SubscriptionId 'YOUR SUBSCRIPTION ID'
Resource Group for Security Copilot capacity
New-AzResourceGroup -Name "SecurityCopilotRG" -Location "WestEurope"
One-time operation per subscription
Depending on Tenant rollout stage, either Microsoft.Security OR Microsoft.SecurityCopilot may be required
#Register-AzResourceProvider -ProviderNamespace "Microsoft.Security"
#Register-AzResourceProvider -ProviderNamespace "Microsoft.SecurityCopilot"
Create a Security Copilot capacity (SCU)
New-AzResource -ResourceName "SecurityCopilotSCU" `
-ResourceType "Microsoft.SecurityCopilot/capacities" `
-ResourceGroupName "SecurityCopilotRG" `
-Location "westeurope" `
-ApiVersion "2023-12-01-preview" `
-Properties @{numberOfUnits=2; crossGeoCompute="NotAllowed"; geo="EU"}`
-force
Important: delete the SCU or the entire resource group afterwards to avoid costs
DeleteSecCopilotSCU.ps1
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS C:\Users\klaus\OneDrive\GitContent\Powershell>
pwsh
PowerShell ...
main 0 0
Klaus Bierschenk (10 months ago) Ln 9, Col 69 Spaces: 4 UTF-8 CRLF PowerShell
1 inch of rain
Thursday
Search
DEU


File Edit Selection View Go Run ···
Powershell [Administrator]
DeleteSecCopilotSCU.ps1
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
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS C:\Users\klaus\OneDrive\GitContent\Powershell>
pwsh
PowerShell ...
main 0 0
Klaus Bierschenk (2 weeks ago) Ln 4, Col 1 Spaces: 4 UTF-8 CRLF PowerShell
Cold weather
Now
Search
DEU