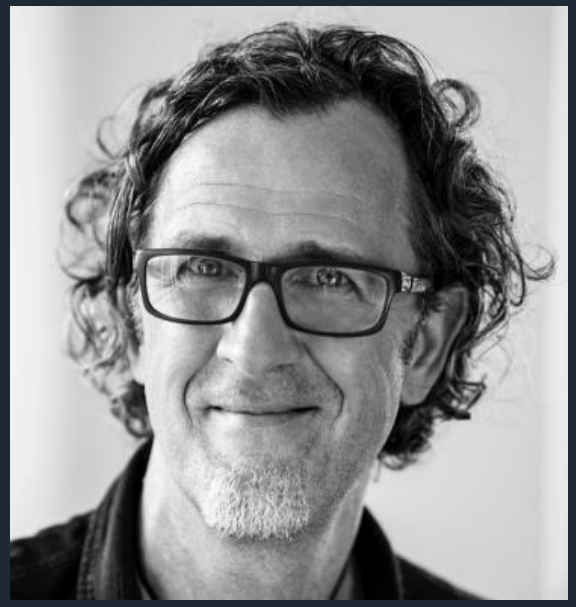
Entra ID Frühjahrsputz – Altlasten erkennen, Risiken beseitigen



Klaus Bierschenk
Director Consulting Expert @ CGI Germany

Based in Murnau am Staffelsee, Bavaria

Living with my family, two snakes, two cats – and lots of other animals my cats bring home from time to time

@klabier.bsky.social

http://www.linkedin.com/in/klabier

Klaus@NothingButCloud.net

https://nothingbutcloud.net/

Microsoft® MVP Most Valuable Professional

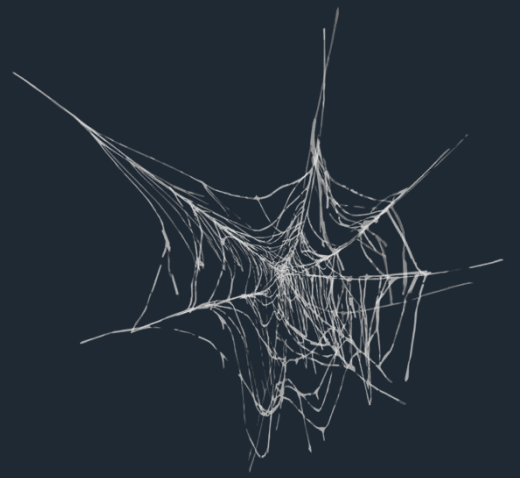
heise academy

"More than 99% of identity attacks can be prevented with basic security hygiene."
— Microsoft, Digital Defense Report 2025

https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

So why do we still have stale users, orphaned apps and unused admin roles?

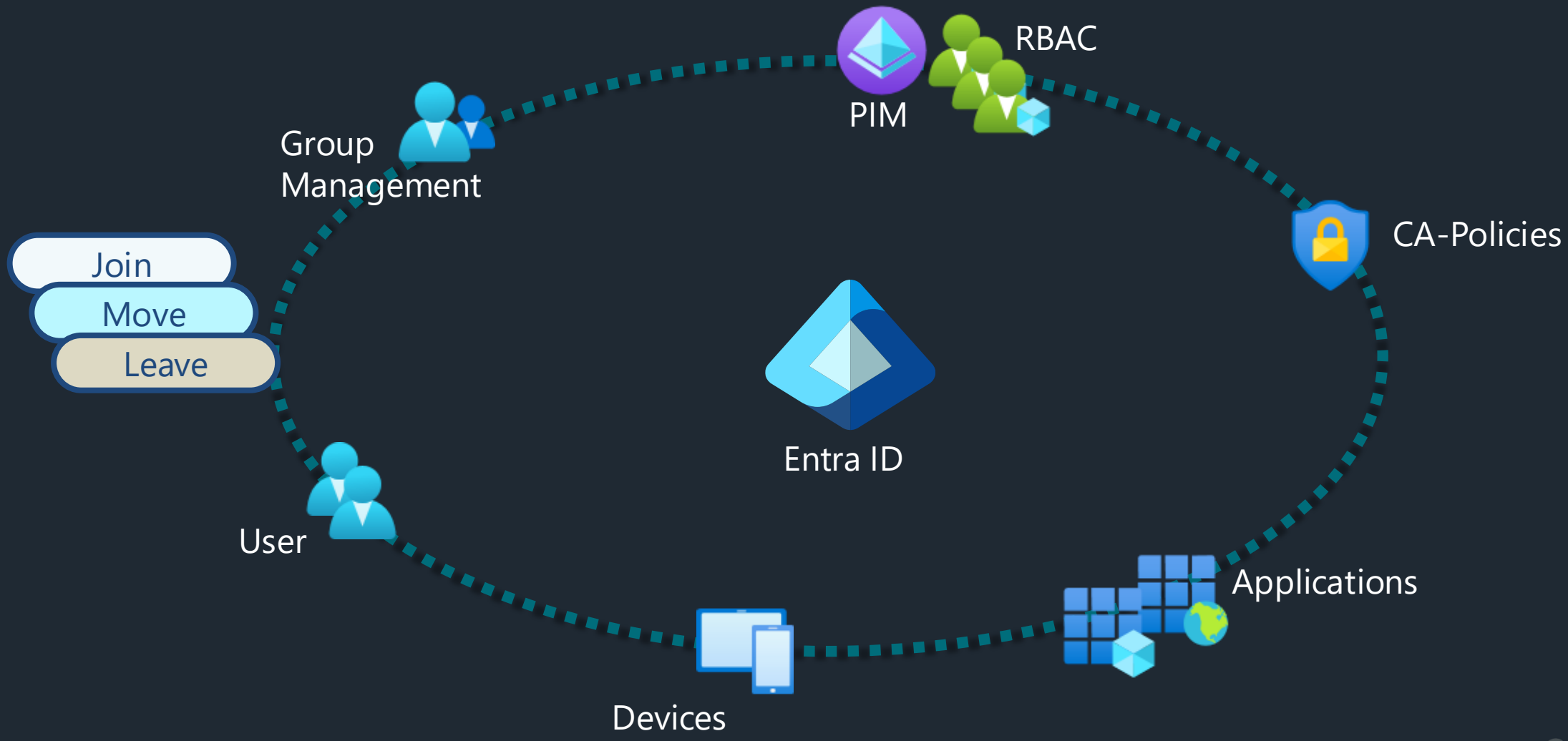
Wenn du deinen Tenant nicht aufräumst, macht es vielleicht jemand anders



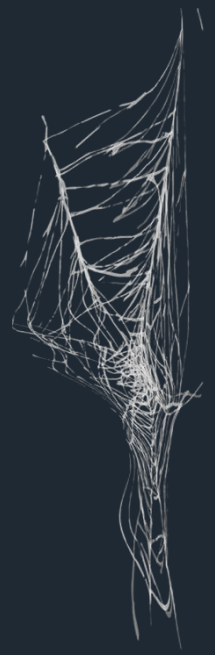
- **Die Ursachen**
  Wo und durch was entsteht Tenant Müll?
- **Werkzeuge für Housekeeping**
  Wie erkenne ich was alt ist?
- **Wo hilft uns KI?**

Blog Artikel

Die Ursachen – Wie und wo entsteht Tenant-Müll??



Security Copilot im Housekeeping?



- Embedded Experience -> eingebettet in EAC
- Standalone Edition -> securitycopilot.microsoft.com
- Agenten: Conditional Access Optimization Agent *(Blog Artikel)*
- Abrechnung über Security Compute Units (SCUs)
  Computing Units - technische Verbrauchseinheit 4$ pro Stunde
- Erstelle / entferne SCU temporär per Script *(Blog Artikel)*

Home
Agents
Promptbooks
Build Preview
History
All history
Owner
Owner settings
Plugin settings
Role assignment
Manage workspaces
Usage monitoring
Security Store

Analyze the Conditional Access policies in our tenant and point out any that appear redundant, overly broad, or not applied to any users or applications.

11 steps completed 33 seconds Private preview

Feb 14, 11:52 AM

Here's an analysis of your Conditional Access policies that are redundant, overly broad, not applied, or may clutter your policy list:

AI-generated content may be incorrect. Check it for accuracy. Export to Excel

Policy Name	Issue Type	Enabled
CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA	Overly Broad	Yes
CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA COPP	Redundant/Disabled	No
CA132-Mulder-ProtectedAction-DeletedItems	Redundant	Yes
CA132-Mulder-ProtectedAction-DeletedItemsImported COPY	Redundant	Yes

*For CA999, check if the assigned group contains any members; if not, the policy is not applied.

This table highlights 15 policies with issues, including redundancy, excessive scope, lack of application, or disabled status, based on the current configuration.

References

Verify on Entra Admin Center

How's this response? AI-generated content may be incorrect. Check it for accuracy.

How can Security Copilot help?

AI-generated content may be incorrect. Check it for accuracy.

KA Klaus Admin klaus@kbrun.de

A1 | Policy Name

	A	B	C	D	E
1	**Policy Name**	**Issue Type**	**Enabled**	**Target Users/Groups/Apps**	**Details**
2	CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA	Overly Broad	Yes	All users (except 2), all apps (except 1 group)	Applies MFA to nearly all users and apps; may be too broad if more specific policies exist.
3	CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA COPP	Redundant/Disabled	No	All users (except 3), all apps (except 1 group)	Disabled duplicate/variant of above; may clutter policy list.
4	CA132-Mulder-ProtectedAction-DeletedItems	Redundant	Yes	2 specific users, authentication context c1	Nearly identical to "CA132-Mulder-ProtectedAction-DeletedItemsImported COPY"; both target same users/apps.
5	CA132-Mulder-ProtectedAction-DeletedItemsImported COPY	Redundant	Yes	2 specific users, authentication context c1	Duplicate of above; both enabled, same users/apps, same controls.
6	CA950 - Do Nothing	Not Applied	Yes	1 group, no apps	Targets a group but no applications; policy has no effect.
7	CA999-SalesForce Phishing Resistant MFA	Not Applied*	Yes	1 group, Salesforce app	If group is empty, policy is ineffective.
8	CA008-Global-IdentityProtection-UserRiskHigh-ChangePW	Overly Broad	Yes	All users (except 2), all apps (except 1 group), user risk "low"	Triggers on "low" user risk for all users/apps; typically set for "high" risk only.
9	CA004-Global-EntraTerms-AllApps-AnyPlatform-ToU xxx	Disabled/Clutter	No	Not specified	Disabled, may clutter policy list.
10	CA116-Admins-ProtectedAction-DeleteCAPolicies-Grant-OnlyGA	Disabled/Clutter	No	Not specified	Disabled, may clutter policy list.
11	CA101-Klaus-BaseProtection-AllApps-AnyPlatform-SignInFreqNonPersistent	Disabled/Clutter	No	Not specified	Disabled, may clutter policy list.
12	CA002-Global-BaseProtection-AllApps-AnyPlatform-SessionLifetime12hrs	Disabled/Clutter	No	Not specified	Disabled, may clutter policy list.
13	CA888 - Block Langley from Admin Portals	Disabled/Clutter	No	Not specified	Disabled, may clutter policy list.
14	CA132-Mulder-ProtectedAction-DeletedItemsImported COPY (disabled)	Disabled/Clutter	No	Not specified	Disabled, may clutter policy list.
15	CA116-Admins-ProtectedAction-DeleteCAPolicies-Grant-OnlyGA COPY	Disabled/Clutter	No	Not specified	Disabled, may clutter policy list.
16	CA001-Global-BaseProtection-AllApps-AnyPlatform-BlockNonPersonass	Disabled/Clutter	No	Not specified	Disabled, may clutter policy list.
17					
18					
19					
20					
21					

Microsoft Entra

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-8745-34a90b6a2a1d

Primary domain kbcorp2021.onmicrosoft.com

64 View users

59 View groups

24 View devices

35 View apps

Klaus Bierschenk
Global Administrator

03117a6e-23cb-4b06-b91f-4ec05ea55994

View user profile

My role assignments

1

High privileged role assignments
Other role assignments

Manage my roles

Users at high risk

No detections found

Copilot

Analyze the Conditional Access policies in our tenant and point out any that appear redundant, overly broad, or not applied to any users or applications.

Copilot AI-generated content may be incorrect. Check it for accuracy.

Here is an analysis of your Conditional Access (CA) policies for redundancy, overly broad scope, and lack of assignment to users or applications:

1. Redundant or Overlapping Policies

- There are several policies with very similar names and conditions, such as:
  - "CA132-Mulder-ProtectedAction-DeletedItems", "CA132-Mulder-ProtectedAction-DeletedItemsImported COPY", and "Merged CA132-Mulder-ProtectedAction-DeletedItems and CA132-Mulder-ProtectedAction-DeletedItemsImported COPY". These appear to target the same users and authentication context, with similar grant controls. Consider consolidating or removing duplicates to reduce complexity.
  - "CA116-Admins-ProtectedAction-DeleteCAPolicies-Grant-OnlyGA" and "CA116-Admins-ProtectedAction-DeleteCAPolicies-Grant-OnlyGA COPY" are both disabled and have nearly identical conditions. Keeping both is unnecessary.

2. Overly Broad Policies

- "CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA" and "CA002-Global-BaseProtection-AllApps-AnyPlatform-SessionLifetime12hrs" (disabled) both target all users and all applications, with only a few exclusions. While broad policies can be useful for baseline security, ensure that exclusions are intentional and that such policies do not conflict with more targeted controls.
- "CA008-Global-IdentityProtection-UserRiskHigh-ChangePW" targets all users and all applications for user risk level "low", which may be broader than intended for a high-risk scenario.

3. Policies Not Applied to Any Users or Applications

- "CA001-Global-BaseProtection-AllApps-AnyPlatform-BlockNonPersonass" is disabled and targets "None" for applications, meaning it is not currently applied to any app.
- "Block all high risk agents from accessing all resources" is set to "enabledForReportingButNotEnforced" and includes "None" for users, so it does not actively protect any users.
- "CA950 - Do Nothing" is enabled but targets "None" for applications, so it is not enforcing any controls.

Recommendations:

- Review and consolidate duplicate or overlapping policies to simplify management.
- Reassess broad policies to ensure they are not unintentionally impacting all users or applications, especially if more granular controls are needed.
- Remove or update policies that are not applied to any users or applications, as they do not provide any security benefit in their current state.

If you need a detailed breakdown of each policy's assignments or want to review specific policies, let me know!

Select 'open list' to see the full list with the data set. Ask any other questions by entering a prompt below.

Schließen

Ask a question, search for info, or get help with a task in Security...

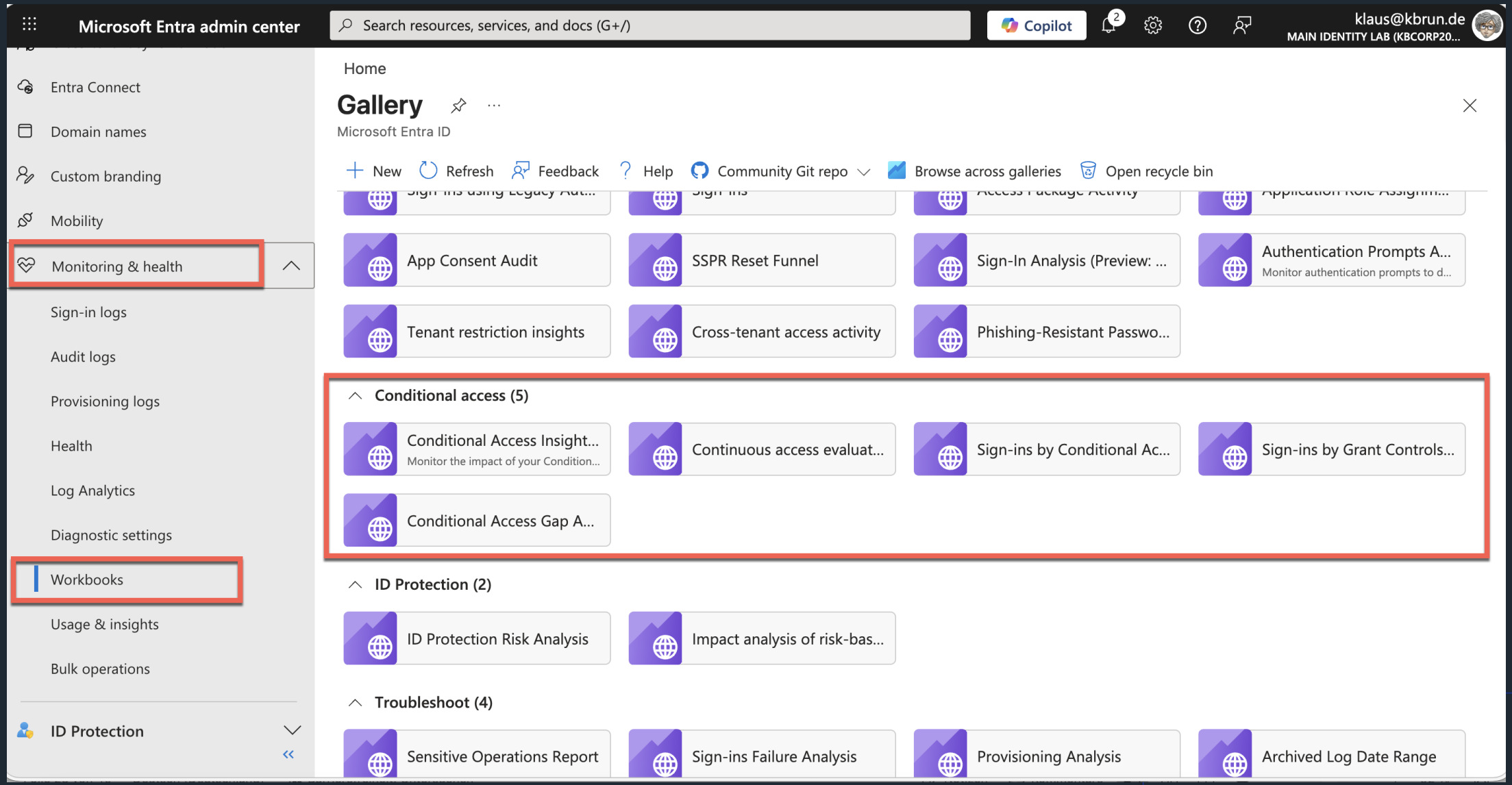
Security Copilot für M365 E5 Kunden

Berechtigte Microsoft 365 E5 Kunden erhalten
400 Security Compute Units (SCUs) pro Monat je 1.000 E5-Lizenzen
(max. 10.000 SCUs pro Monat)

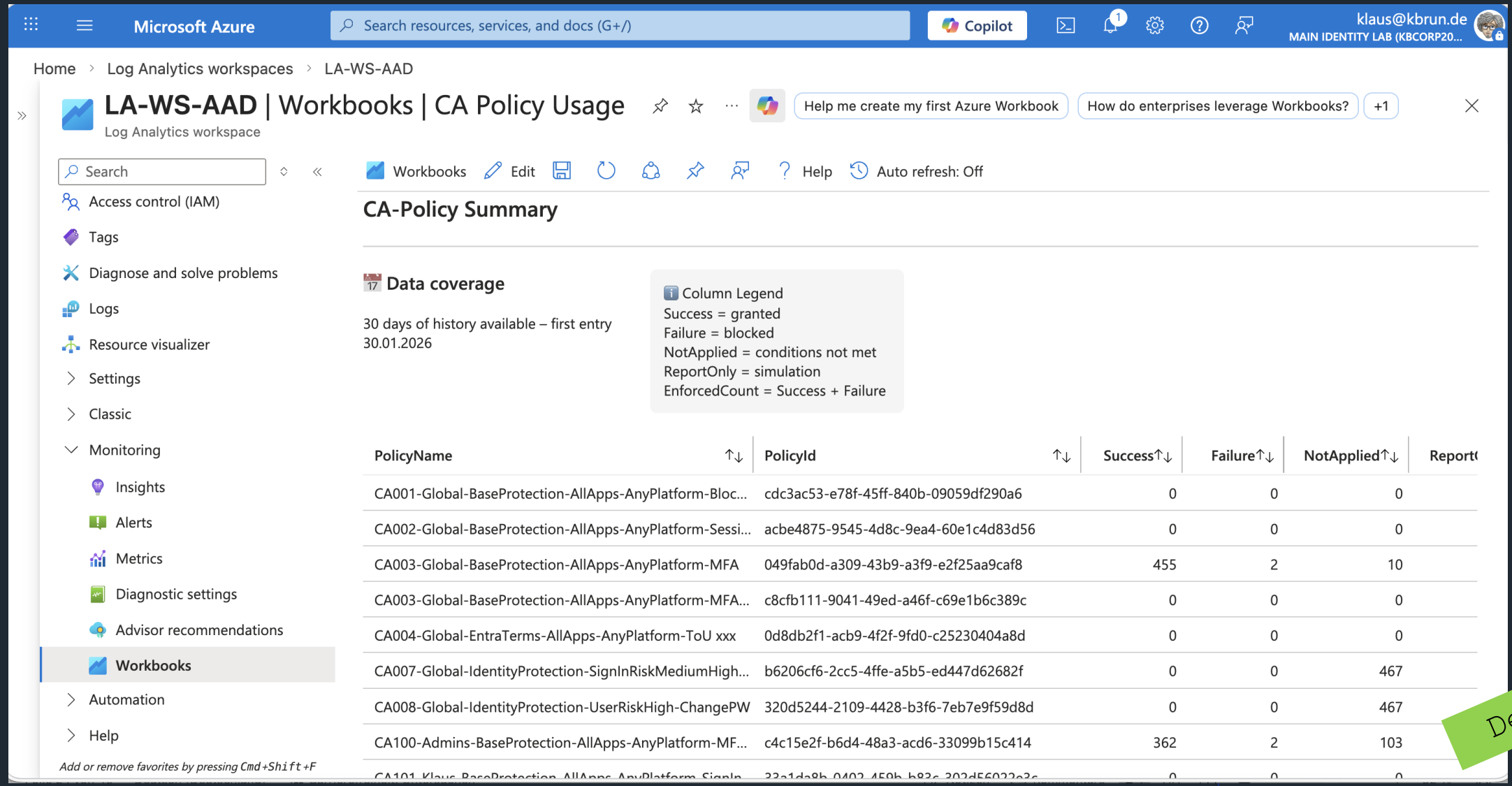
Beispiel1:
Eine Organisation mit 400 Arbeitsplätzen erhält 160 SCUs/Monat

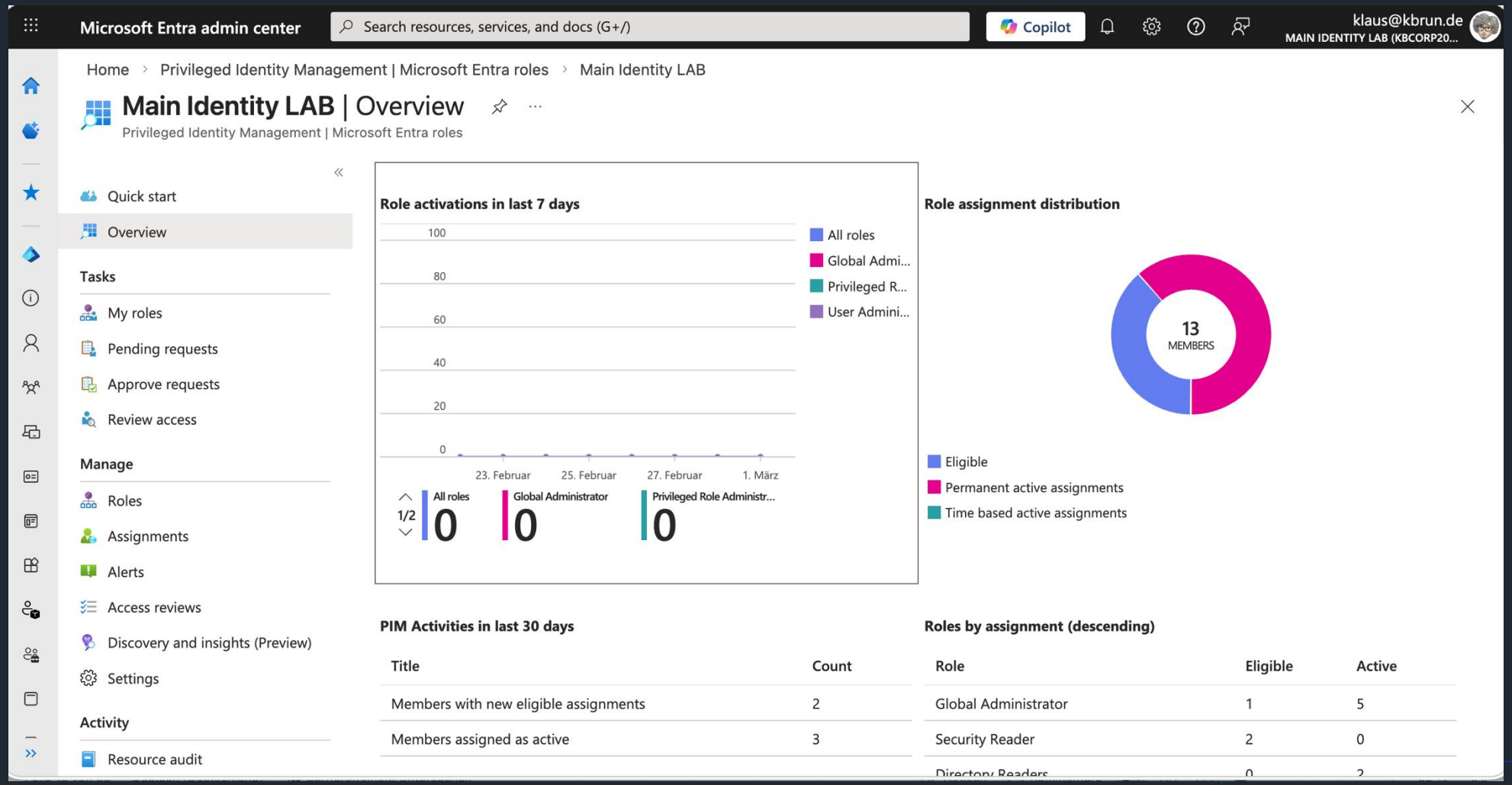
Beispiel2:
Eine Organisation mit 4.000 Arbeitsplätzen erhält 1.600 SCUs/Monat.

- https://aka.ms/securitycopilotme5
- https://aka.ms/SCP-ignite25


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
klaus@kbrun.de
MAIN IDENTITY LAB (KBCORP20...
Entra Connect
Domain names
Custom branding
Mobility
Monitoring & health
Sign-in logs
Audit logs
Provisioning logs
Health
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Bulk operations
ID Protection
Home
Gallery
Microsoft Entra ID
New
Refresh
Feedback
Help
Community Git repo
Browse across galleries
Open recycle bin
App Consent Audit
SSPR Reset Funnel
Sign-In Analysis (Preview: ...
Authentication Prompts A...
Monitor authentication prompts to d...
Tenant restriction insights
Cross-tenant access activity
Phishing-Resistant Passwo...
Conditional access (5)
Conditional Access Insight...
Monitor the impact of your Condition...
Continuous access evaluat...
Sign-ins by Conditional Ac...
Sign-ins by Grant Controls...
Conditional Access Gap A...
ID Protection (2)
ID Protection Risk Analysis
Impact analysis of risk-bas...
Troubleshoot (4)
Sensitive Operations Report
Sign-ins Failure Analysis
Provisioning Analysis
Archived Log Date Range

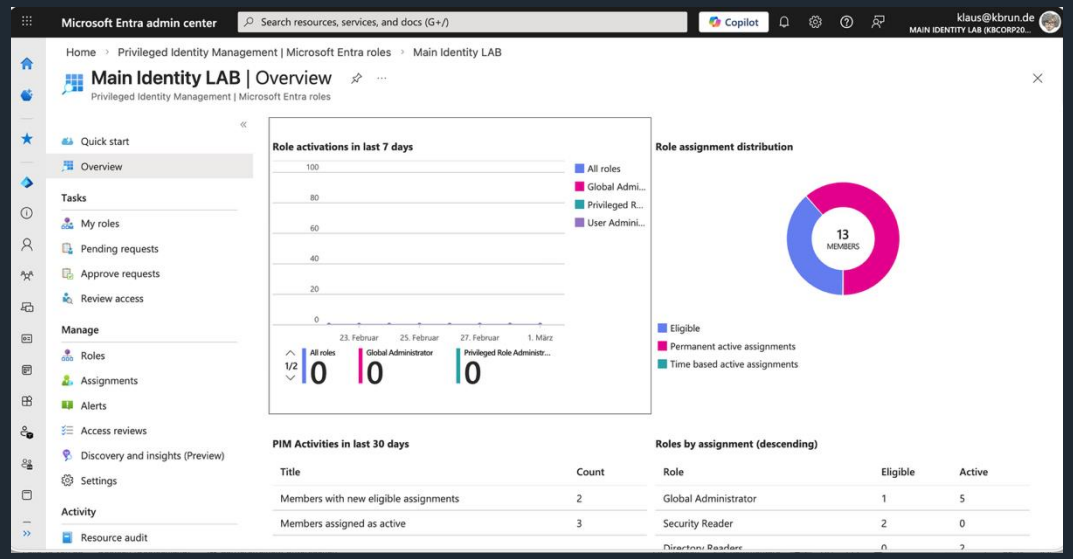
Conditional Access Policies – CA Policy Usage *(Blog Artikel)*



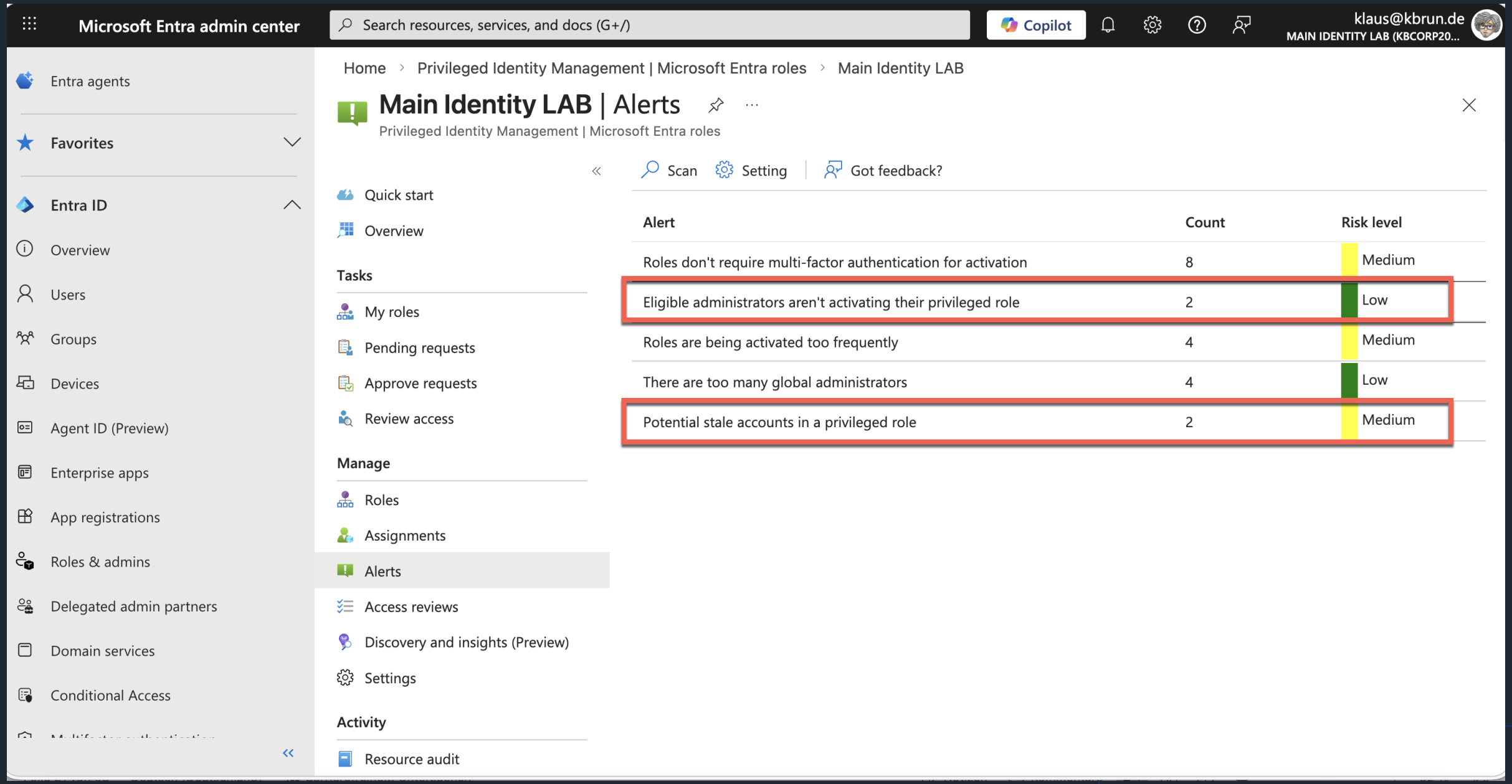

Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
klaus@kbrun.de
MAIN IDENTITY LAB (KBCORP20...
Home
Privileged Identity Management | Microsoft Entra roles
Main Identity LAB
Main Identity LAB | Overview
Privileged Identity Management | Microsoft Entra roles
Quick start
Overview
Tasks
My roles
Pending requests
Approve requests
Review access
Manage
Roles
Assignments
Alerts
Access reviews
Discovery and insights (Preview)
Settings
Activity
Resource audit
Role activations in last 7 days
100
80
60
40
20
0
23. Februar
25. Februar
27. Februar
1. März
All roles
Global Admi...
Privileged R...
User Admini...
1/2
All roles
0
Global Administrator
0
Privileged Role Administr...
0
Role assignment distribution
13
MEMBERS
Eligible
Permanent active assignments
Time based active assignments
PIM Activities in last 30 days
Title
Count
Members with new eligible assignments
2
Members assigned as active
3
Roles by assignment (descending)
Role
Eligible
Active
Global Administrator
1
5
Security Reader
2
0
Directory Readers
0
2

Privileged Access Hygiene

- PIM – Dashboards -> Overview
- PIM – Dashboards -> Alerts
- Access Reviews für Rollen
- Alles bezogen auf Rollen
  (Alerts, Access Reviews usw.)
- PIM for Groups? -> Access Reviews (Gruppen)



Demo ...



Privileged Identity Management -> Roles -> Alerts

Gibt es den Benutzer noch?

Merkmale / Risiken:

- Mal eben anlegen, vorbei an Standardprozessen
- Manager- oder andere Company-Attribute leer
- Keine MFA Methode
- Ist Owner? Manager?
- Ausnahmen in CA-Policies

Maßnahmen:

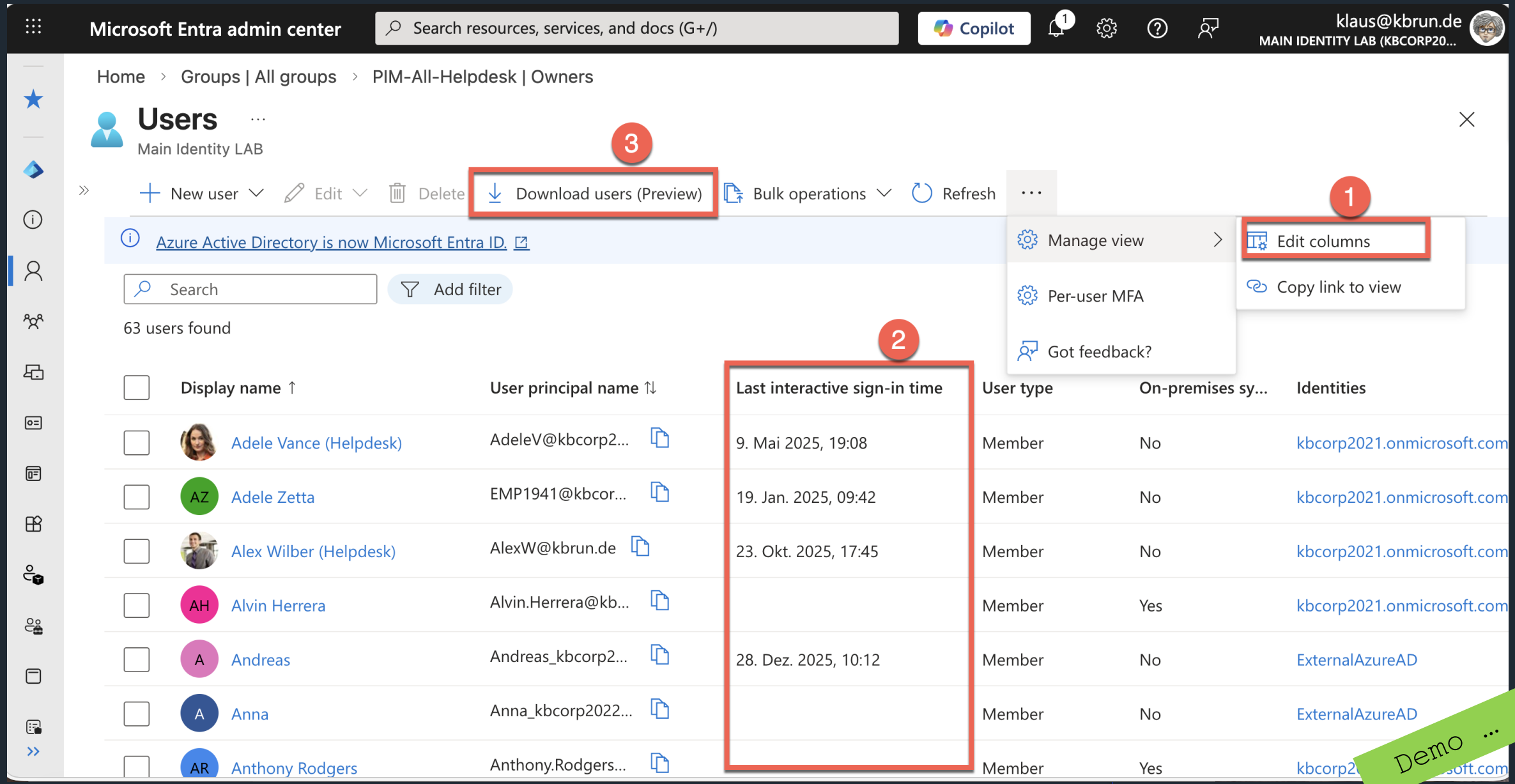
- ✓ Entra Admin Center
- ✓ lastSignInDateTime
- ✓ Registered Authentication Methods
- ✓ PowerShell / Graph
- ✓ Lifecycle Workflows
- ✗ Access Reviews (eher nicht)

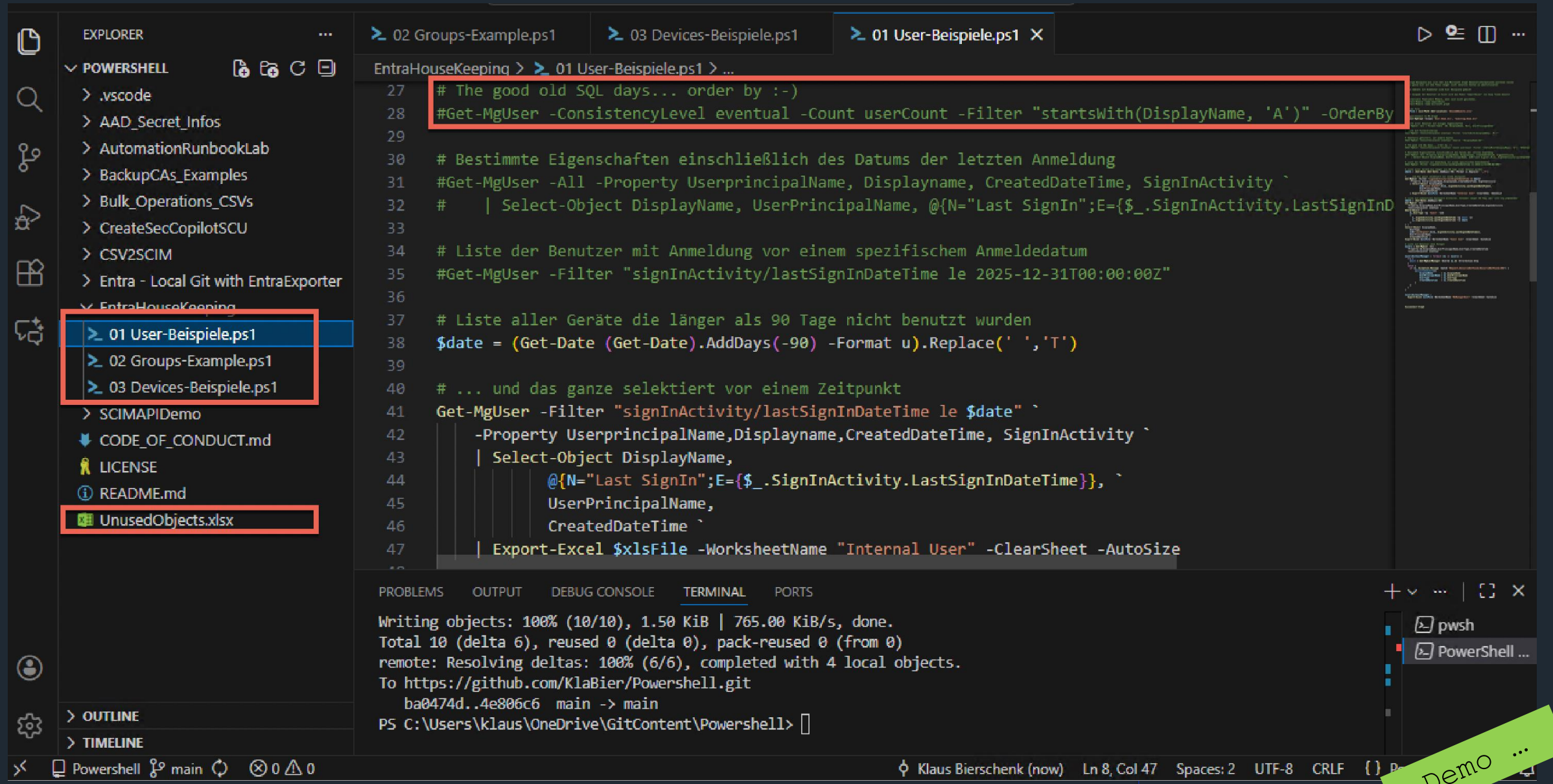
Demo

→ *Entra Admin Center*
User Filter

→ *PowerShell is your friend*

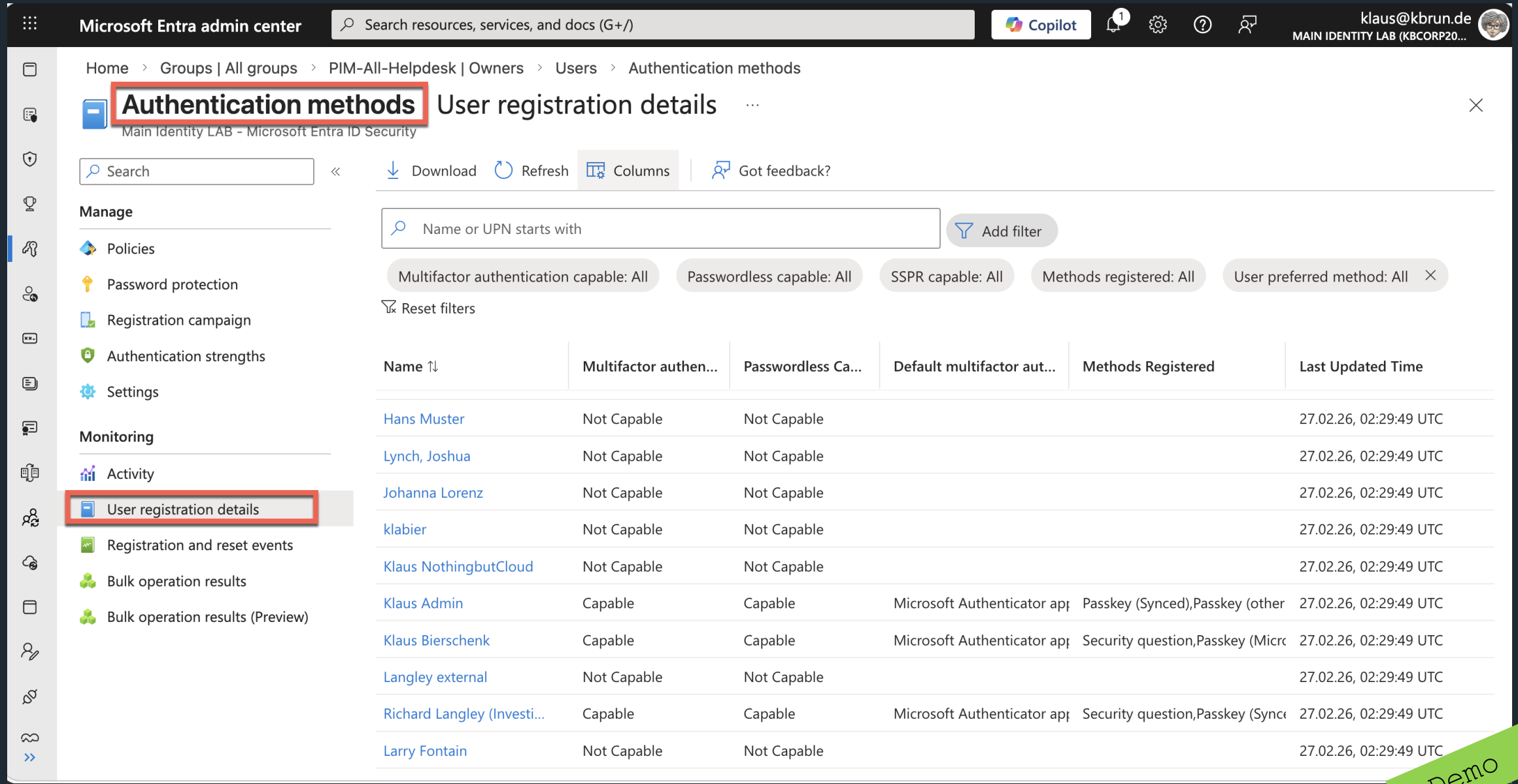
→ *Authentication Methods*


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
klaus@kbrun.de
MAIN IDENTITY LAB (KBCORP20...
Home
Groups | All groups
PIM-All-Helpdesk | Owners
Users
Main Identity LAB
3
New user
Edit
Delete
Download users (Preview)
Bulk operations
Refresh
1
Manage view
Edit columns
Per-user MFA
Copy link to view
Got feedback?
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter
63 users found
2
Display name
User principal name
Last interactive sign-in time
User type
On-premises sy...
Identities
Adele Vance (Helpdesk)
AdeleV@kbcorp2...
9. Mai 2025, 19:08
Member
No
kbcorp2021.onmicrosoft.com
Adele Zetta
EMP1941@kbcor...
19. Jan. 2025, 09:42
Member
No
kbcorp2021.onmicrosoft.com
Alex Wilber (Helpdesk)
AlexW@kbrun.de
23. Okt. 2025, 17:45
Member
No
kbcorp2021.onmicrosoft.com
Alvin Herrera
Alvin.Herrera@kb...
Member
Yes
kbcorp2021.onmicrosoft.com
Andreas
Andreas_kbcorp2...
28. Dez. 2025, 10:12
Member
No
ExternalAzureAD
Anna
Anna_kbcorp2022...
Member
No
ExternalAzureAD
Anthony Rodgers
Anthony.Rodgers...
Member
Yes
Demo



Demo ...

https://github.com/KlaBier/Powershell/tree/main/EntraHouseKeeping


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
klaus@kbrun.de
MAIN IDENTITY LAB (KBCORP20...
Home
Groups | All groups
PIM-All-Helpdesk | Owners
Users
Authentication methods
Authentication methods
User registration details
Main Identity LAB - Microsoft Entra ID Security
Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
Bulk operation results (Preview)
Download
Refresh
Columns
Got feedback?
Name or UPN starts with
Add filter
Multifactor authentication capable: All
Passwordless capable: All
SSPR capable: All
Methods registered: All
User preferred method: All
Reset filters
Name
Multifactor authen...
Passwordless Ca...
Default multifactor aut...
Methods Registered
Last Updated Time
Hans Muster Not Capable Not Capable 27.02.26, 02:29:49 UTC
Lynch, Joshua Not Capable Not Capable 27.02.26, 02:29:49 UTC
Johanna Lorenz Not Capable Not Capable 27.02.26, 02:29:49 UTC
klabier Not Capable Not Capable 27.02.26, 02:29:49 UTC
Klaus NothingbutCloud Not Capable Not Capable 27.02.26, 02:29:49 UTC
Klaus Admin Capable Capable Microsoft Authenticator ap Passkey (Synced),Passkey (other 27.02.26, 02:29:49 UTC
Klaus Bierschenk Capable Capable Microsoft Authenticator ap Security question,Passkey (Micr 27.02.26, 02:29:49 UTC
Langley external Not Capable Not Capable 27.02.26, 02:29:49 UTC
Richard Langley (Investi... Capable Capable Microsoft Authenticator ap Security question,Passkey (Sync 27.02.26, 02:29:49 UTC
Larry Fontain Not Capable Not Capable 27.02.26, 02:29:49 UTC
Demo

I WANT YOU
To take care of your
Guest Accounts

Wird das Gastkonto noch benötigt?

Merkmale / Risiken:

- Einladung ist vielfältig möglich
- Ohne Lifecycle Prozess unsterblich
- Source of truth (Management) in fremden Tenant
- Admin Rollen vorhanden
- CA-Policies auf Guests angewendet?
- Sponsor Attribut

Maßnahmen:

- ✓ Check Guest (Tenant) Settings
- ✓ Wer darf einladen?
- ✓ Governance – View Inactive Guests
- ✓ Lifecycle Workflows
- ✓ Access Reviews!

Demo

→ *Umgang mit Gast Konten*

https://entra.microsoft.com/#view/Microsoft_Azure_IdentityGovernance/InactiveGuestsReport.ReactView

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

Home > Main Identity LAB

Insights and reporting | Inactive guest accounts

Microsoft - Entra ID

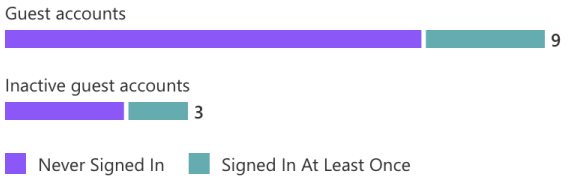
Last updated: 20. Februar 2026 um 02:11 MEZ

Monitor the inactive guest accounts in your organization. Customize the inactivity threshold depending on your organization's needs, narrow down the scope of guests you want to monitor and identify the guest accounts that may be inactive.

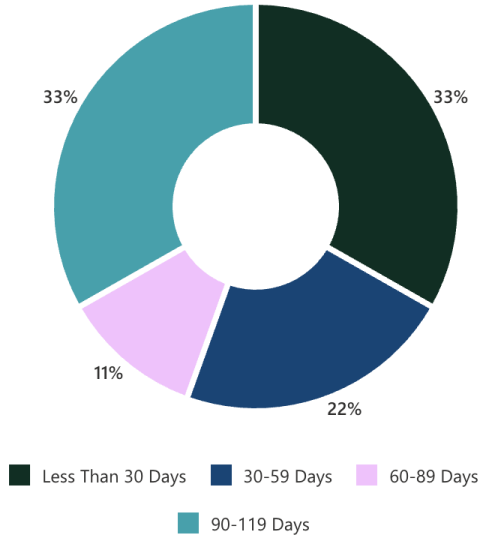
Inactivity threshold

90 days without sign in

Guest account overview

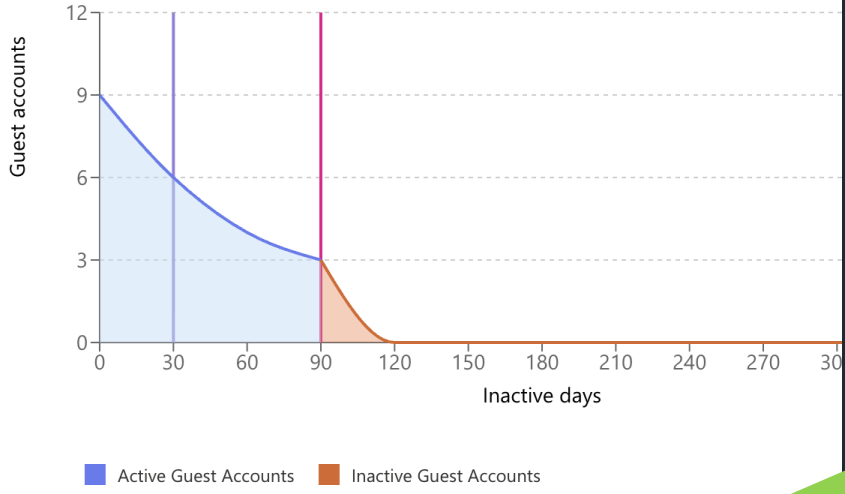


Guests inactivity distribution



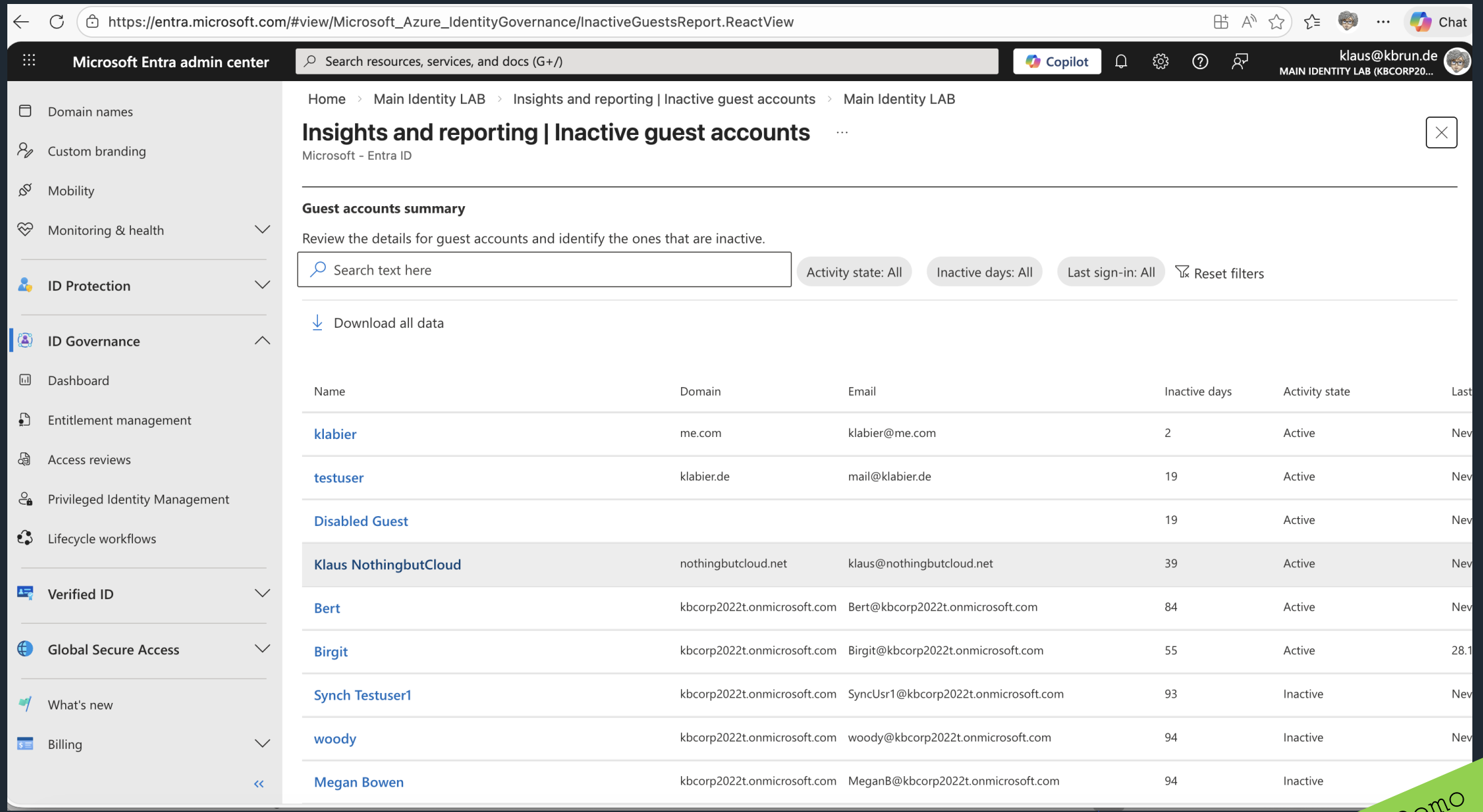
Guest inactivity overview

50th percentile	90th percentile	95th percentile	Inactivity thresh...
30 days	90 days	90 days	90 days



Demo ...

EAC -> ID Governance -> Dashboard -> View inactive Guests



Demo ...

EAC -> ID Governance -> Dashboard -> View inactive Guests

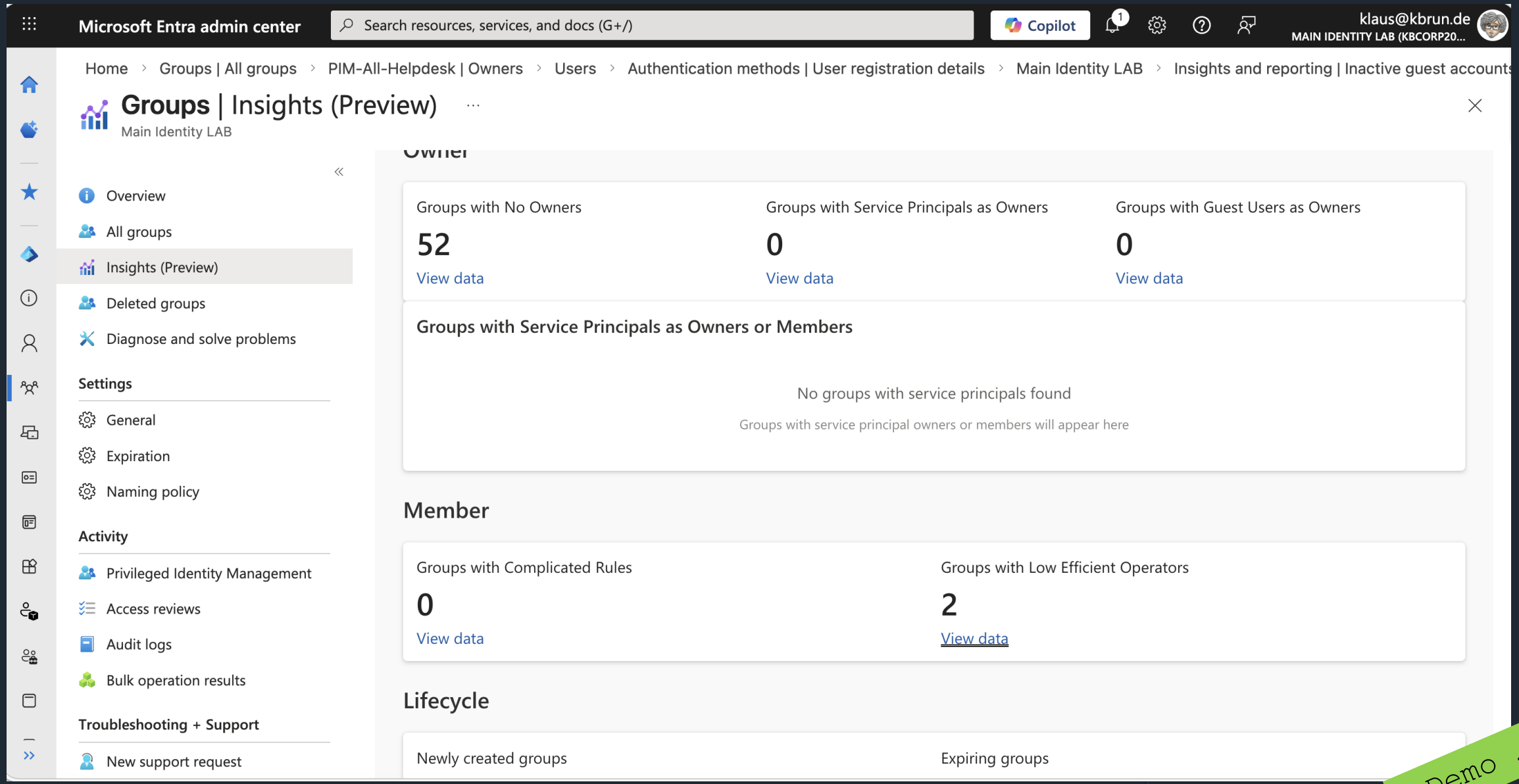
Alte Gruppen ausmisten

Merkmale / Risiken:

- Gruppen ohne Mitglieder
- Gruppen ohne Owner
- Owner inaktiv

Maßnahmen:

- ✓ Groups Insights (Preview)
- ✓ Powershell / Graph
- ✓ Source of truth?
- ✓ Managed by vs. Owner

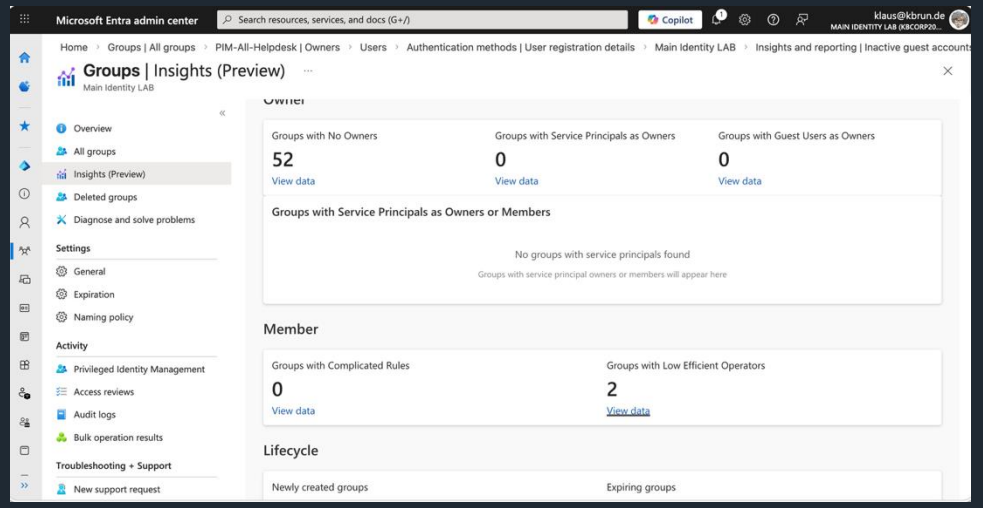


Demo ...

EAC -> Groups -> Groups Insight (Preview)

Group Insights Feature

- Aktuell in Preview
- Infos auf 2 Ebenen:



1. Portal UI
   -> Visuelle Übersicht über Gruppenunordnung

2. API Endpoint
   -> Datenquelle für eigene Reports (eigene Parameter)

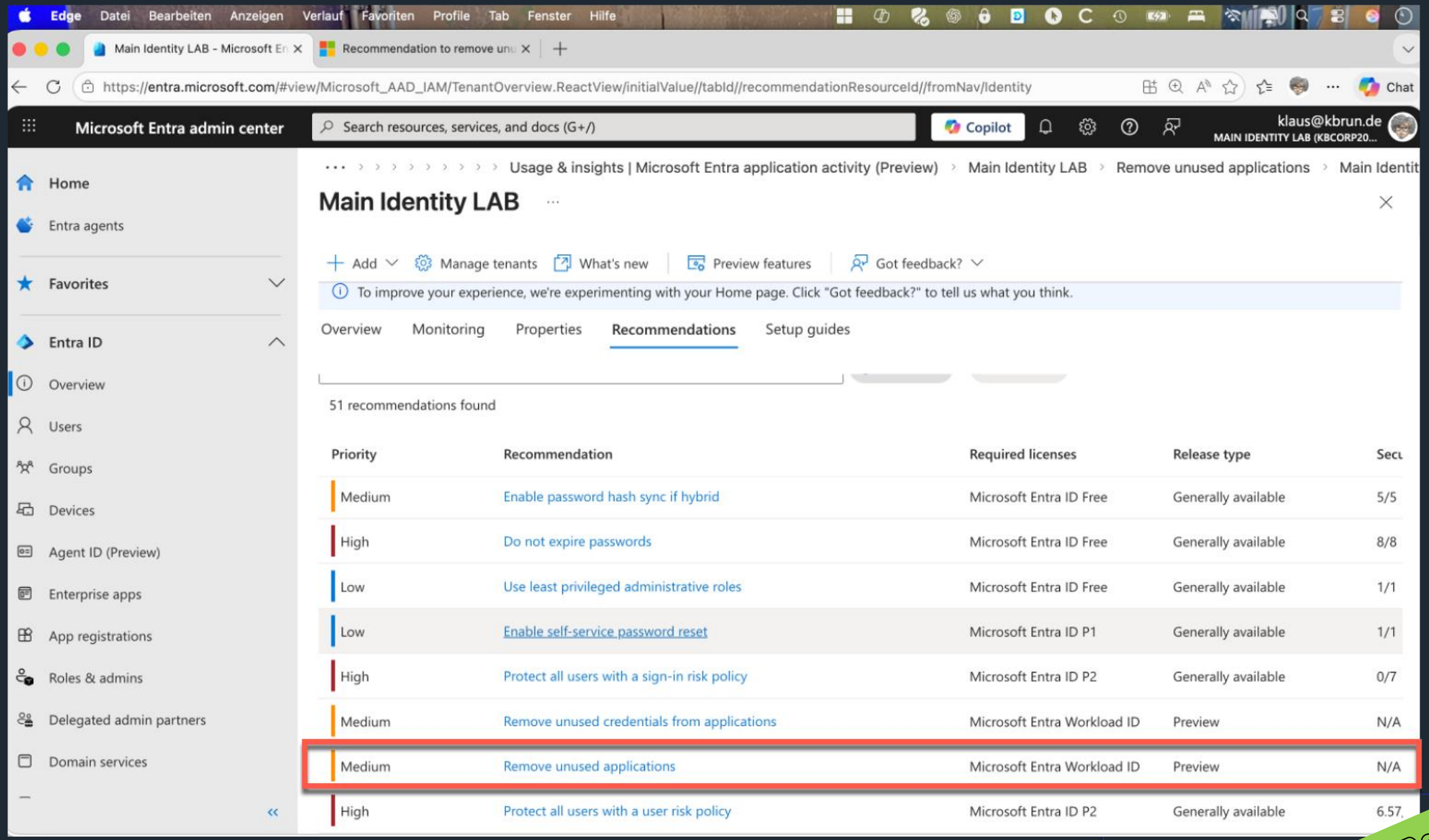
Quelle: *Jan Bakker – What admins can learn from the new Entra ID Groups Insights blade* (Feb 18, 2026)

Enterprise Applikationen / App Registrations

Wer hat das eigentlich angelegt?

- Kein Owner
- Keine Sign-ins
- AssignmentRequired = Yes
  aber 0 Assignments
- Secret Hygiene? (App Registrations)
- Powershell / EAC

Demo ...



Demo ...

EAC -> Overview -> Recommendations -> Remove unused applications

Takeaways

- ✓ Verwaiste Identitäten konsequent eliminieren
  - Benutzer, Gruppen, Applikationen
  - Powershell und Automatisierung nutzen (Blog Artikel)
  - Dokumentation

- ✓ Governance etablieren- Access Review Strategie finden / LCW Strategie
  - Access Review
  - Lifecycle Workflows

- ✓ Housekeeping ist kein Projekt – es ist ein Prozess

Microsoft Learn

Embrace cloud-first posture: Convert Group Source of Authority to the cloud Infos

Use Microsoft Entra groups to manage role assignments

Manage guest access with access reviews

Create an access review of Azure resource and Microsoft Entra roles in PIM

Best Practices & Community

Jan Bakker – What admins can learn from the new Entra ID Groups Insights blade (Feb 18, 2026)

NothingButCloud Blog

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

KlaBier Github: CreateSecCopilotSCU PowerShell

KlaBier Github: Powershell Housekeeping Beispiele ← secIT Beispiele

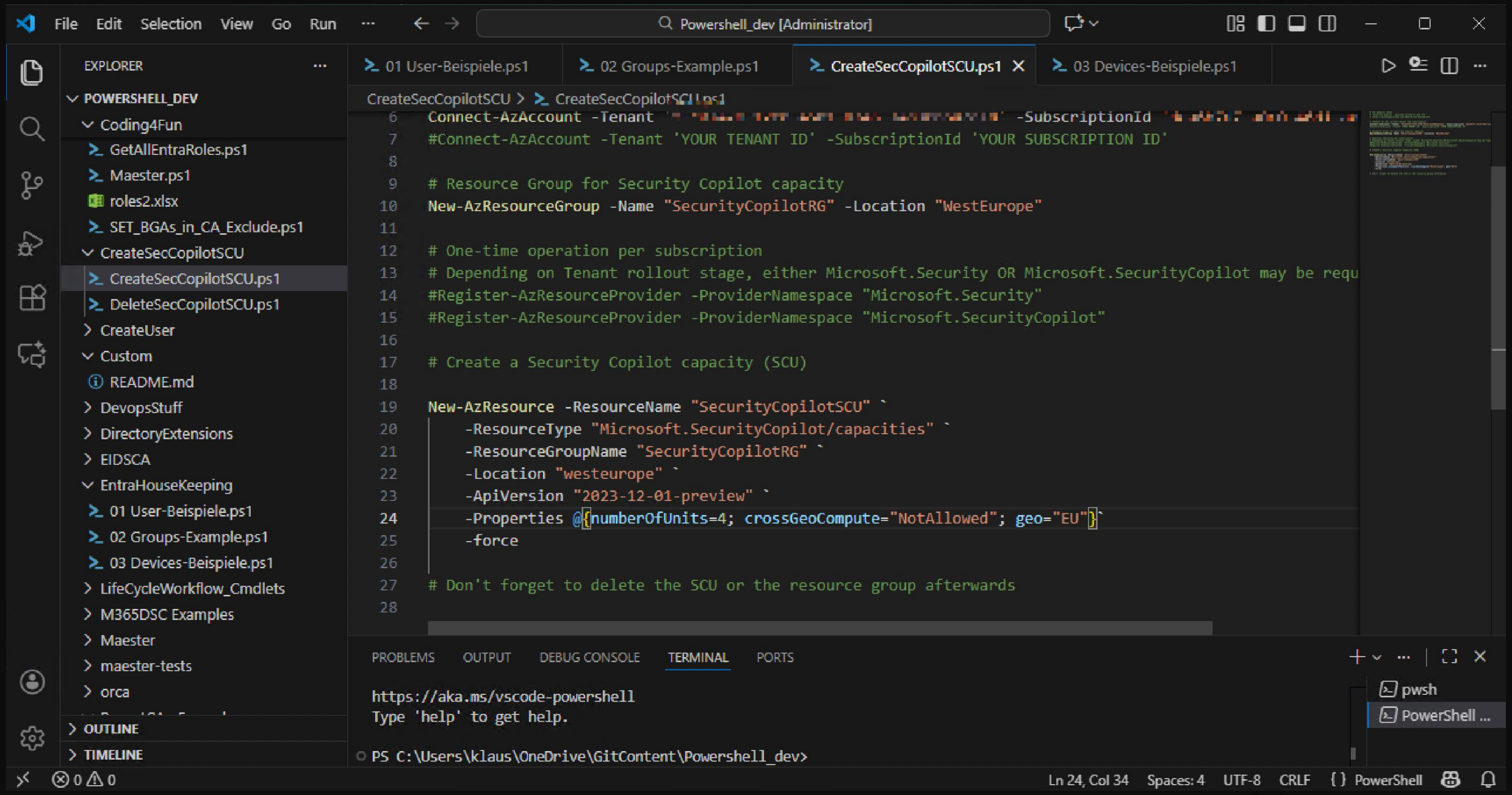
The dilemma with unused objects in Azure AD

Lifecycle Workflows and Custom Extensions - step-by-step-guide

How to Build a Log Analytics Workbook for Unused CA Policies

secIT by heise
HANNOVER 2026

Backup


File Edit Selection View Go Run ···
Powershell_dev [Administrator]
EXPLORER
POWERSHELL_DEV
Coding4Fun
GetAllEntraRoles.ps1
Maester.ps1
roles2.xlsx
SET_BGAs_in_CA_Exclude.ps1
CreateSecCopilotSCU
CreateSecCopilotSCU.ps1
DeleteSecCopilotSCU.ps1
CreateUser
Custom
README.md
DevopsStuff
DirectoryExtensions
EIDSCA
EntraHouseKeeping
01 User-Beispiele.ps1
02 Groups-Example.ps1
03 Devices-Beispiele.ps1
LifeCycleWorkflow_Cmdlets
M365DSC Examples
Maester
maester-tests
orca
OUTLINE
TIMELINE
01 User-Beispiele.ps1
02 Groups-Example.ps1
CreateSecCopilotSCU.ps1
03 Devices-Beispiele.ps1
CreateSecCopilotSCU > CreateSecCopilotSCU.ps1
6 Connect-AzAccount -Tenant [redacted] -SubscriptionId [redacted]
7 #Connect-AzAccount -Tenant 'YOUR TENANT ID' -SubscriptionId 'YOUR SUBSCRIPTION ID'
8
9 # Resource Group for Security Copilot capacity
10 New-AzResourceGroup -Name "SecurityCopilotRG" -Location "WestEurope"
11
12 # One-time operation per subscription
13 # Depending on Tenant rollout stage, either Microsoft.Security OR Microsoft.SecurityCopilot may be requ
14 #Register-AzResourceProvider -ProviderNamespace "Microsoft.Security"
15 #Register-AzResourceProvider -ProviderNamespace "Microsoft.SecurityCopilot"
16
17 # Create a Security Copilot capacity (SCU)
18
19 New-AzResource -ResourceName "SecurityCopilotSCU" `
20 -ResourceType "Microsoft.SecurityCopilot/capacities" `
21 -ResourceGroupName "SecurityCopilotRG" `
22 -Location "westeurope" `
23 -ApiVersion "2023-12-01-preview" `
24 -Properties @{numberOfUnits=4; crossGeoCompute="NotAllowed"; geo="EU"}`
25 -force
26
27 # Don't forget to delete the SCU or the resource group afterwards
28
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
https://aka.ms/vscode-powershell
Type 'help' to get help.
PS C:\Users\klaus\OneDrive\GitContent\Powershell_dev>
pwsh
PowerShell ...
0 0
Ln 24, Col 34 Spaces: 4 UTF-8 CRLF { } PowerShell