

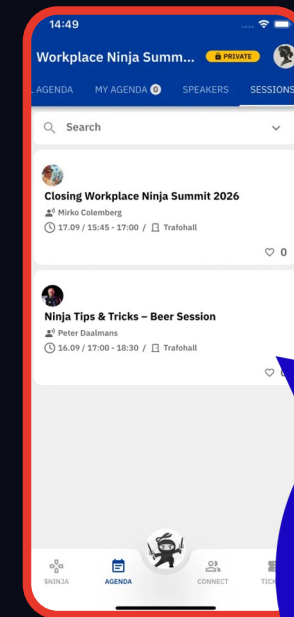
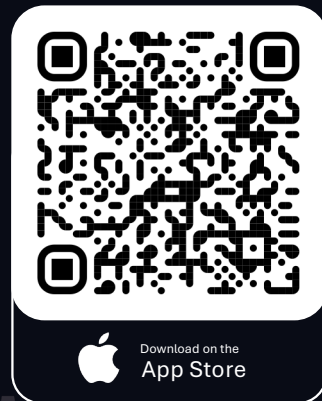
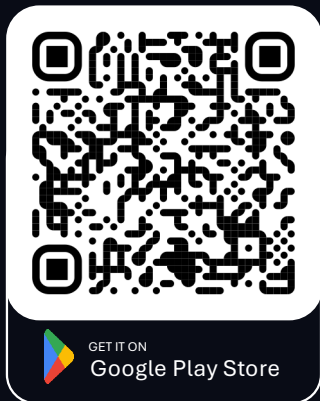
**SHARING KNOWLEDGE.
TOGETHER.**

**WORKPLACE
NINJA**

**SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT**



Check in and rate this session in the Workplace Ninja Summit 2026 app



We appreciate
your feedback!

Halle 36.3
room check-in



Welcome on stage



Session

The Hidden Risks in Your Entra Tenant –
A Housekeeping Guide

Speaker

Klaus Bierschenk

CGI Germany, Microsoft Security MVP



<https://nothingbutcloud.net/>



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



#wpninjas

Thank you to our sponsors!



PLATINUM SPONSORS

glueck  kanja

 PATCH MY PC

Recast

 2Pint

 Microsoft

GOLD SPONSORS

control  UP

 Admin
By Request
ZERO TRUST PLATFORM

eido

THREATLOCKER®
ZERO TRUST PLATFORM

inforcer 

baseVISION
Trusted Swiss Cybersecurity


robopack

 EPIC FUSION
BRING IT ALL TOGETHER


nerdio

SILVER SPONSORS

 systemcenterdudes

Apento

water 
IT Security & Defense

 ugurlabs

Agenda



If you don't clean up your tenant,
someone else might do it for you

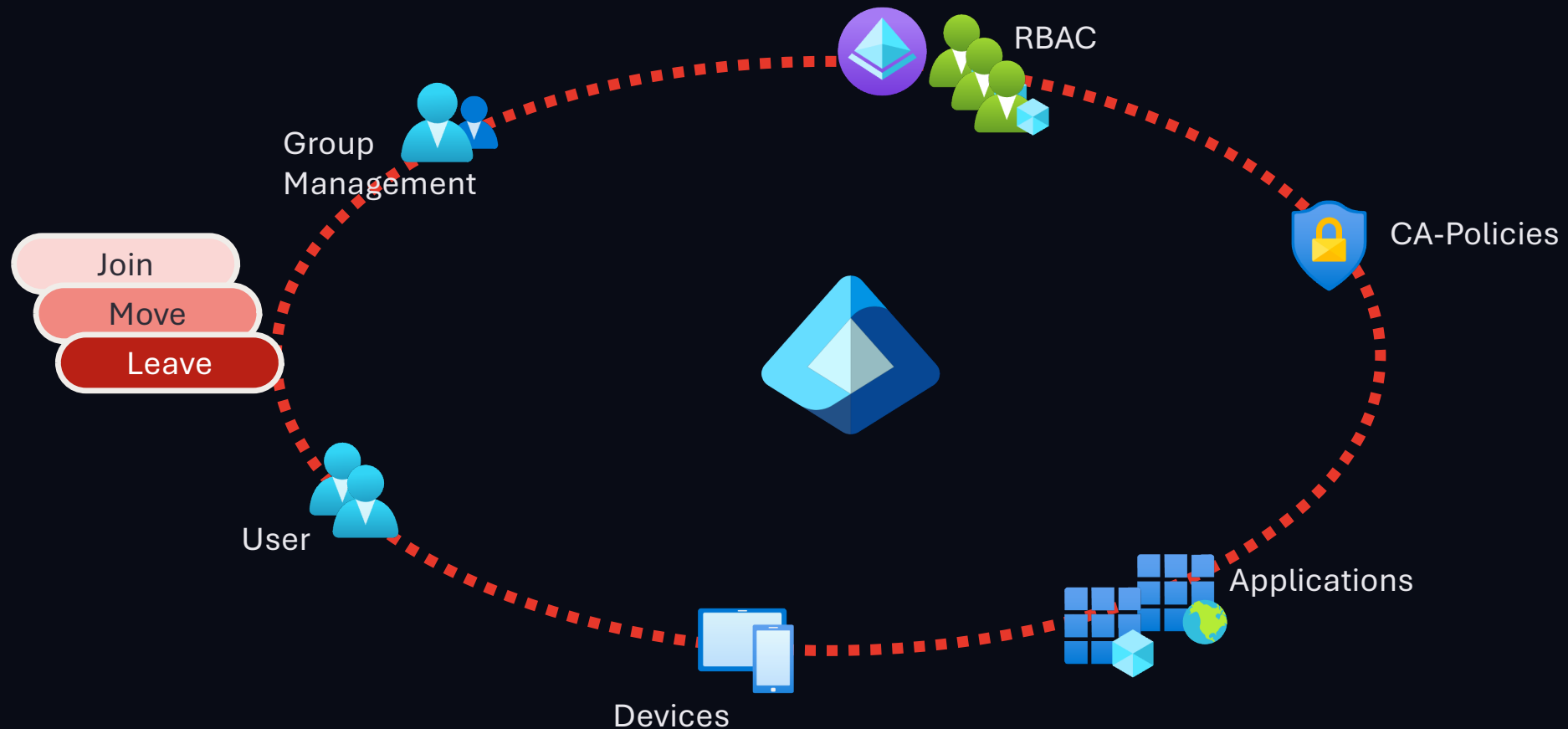
- ❖ The Causes
Where and how does tenant clutter arise?
- ❖ Tools for Housekeeping
How do I identify what is stale?
- ❖ AI-assisted Housekeeping –
what's actually useful?



See this symbol?
Referenced Blog Articles exist

#wpninja

How and where does tenant clutter arise?



Does this user still need an account?



Characteristics / Risks:

- Quickly created, bypassing standard processes
- Manager or other company attributes empty
- No MFA method
- Does this user still own resources or manage employees?

Actions:

- ✓ Entra Admin Center
- ✓ Registered Authentication Methods
- ✓ lastSignInDateTime / PS 
- ✓ Lifecycle Workflows
- ✗ Access Reviews (rather not)

Demo



Entra Admin Center
User Filter

Authentication Methods

PowerShell is your friend



Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot

1

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

Home > Groups | All groups > PIM-All-Helpdesk | Owners

Users

Main Identity LAB

3

Download users (Preview)

1

Edit columns

2

Last interactive sign-in time

63 users found

	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	kbcorp2021.onmicrosoft.com

Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot

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

Home > Authentication methods

Authentication methods

Main Identity LAB - Microsoft Entra ID Security

User registration details

Search

Download Refresh Columns Got feedback?

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)

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

UPN	Name	Multifactor authen...	Passwordless Ca...	Default multifactor auth...	Methods Registered	Last Updated Time
SecurityCopilotAgentUser-5	SecurityCop...	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
newBGA@kbcorp2021.onm	NewBGA	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
Frohike-ext_kbcorp2022t.or	Melvin Froh...	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
Student3_7b@kbrun.de	Student3 7b	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
Student4_7b@kbrun.de	Student4 7b	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
Student4_8a@kbrun.de	Student4 8a	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
EMP1586@kbcorp2021.onr	Maridel Carl...	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
SecurityCopilotAgentUser-e	SecurityCop...	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
Student5_8a_Protected@kb	Student5 8a...	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
JohannaL@kbcorp2021.onr	Johanna Lor...	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
HMuster@kbrun.de	Hans Muster	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
klabier_me.com#EXT#@kbc	klabier	Not Capable	Not Capable			23.05.26, 09:41:48 UTC
ADTeAADSyncServiceAppo	On-Premise	Not Capable	Not Capable			23.05.26, 09:41:48 UTC

EXPLORER

- POWERSHELL
 - .vscode
 - AAD_Secret_Infos
 - AutomationRunbookLab
 - BackupCAs_Examples
 - Bulk_Operations_CSVs
 - CreateSecCopilotSCU
 - CSV2SCIM
 - Entra - Local Git with EntraExporter
 - EntraHouseKeeping
 - 01 User-Beispiele.ps1
 - 02 Groups-Example.ps1
 - 03 Devices-Beispiele.ps1
 - SCIMAPIDemo
 - CODE_OF_CONDUCT.md
 - LICENSE
 - README.md
 - UnusedObjects.xlsx
- OUTLINE
- TIMELINE

02 Groups-Example.ps1 03 Devices-Beispiele.ps1 01 User-Beispiele.ps1

EntraHouseKeeping > 01 User-Beispiele.ps1 > ...

```
27 # The good old SQL days... order by :-)
28 #Get-MgUser -ConsistencyLevel eventual -Count userCount -Filter "startsWith(DisplayName, 'A')" -OrderBy
29
30 # Bestimmte Eigenschaften einschließlich des Datums der letzten Anmeldung
31 #Get-MgUser -All -Property UserprincipalName, Displayname, CreatedDateTime, SignInActivity `
32 # | Select-Object DisplayName, UserPrincipalName, @{N="Last SignIn";E={$_.SignInActivity.LastSignInD
33
34 # Liste der Benutzer mit Anmeldung vor einem spezifischem Anmeldedatum
35 #Get-MgUser -Filter "signInActivity/lastSignInDateTime le 2025-12-31T00:00:00Z"
36
37 # Liste aller Geräte die länger als 90 Tage nicht benutzt wurden
38 $date = (Get-Date (Get-Date).AddDays(-90) -Format u).Replace(' ', 'T')
39
40 # ... und das ganze selektiert vor einem Zeitpunkt
41 Get-MgUser -Filter "signInActivity/lastSignInDateTime le $date" `
42 -Property UserprincipalName, Displayname, CreatedDateTime, SignInActivity `
43 | Select-Object DisplayName,
44 | @{N="Last SignIn";E={$_.SignInActivity.LastSignInDateTime}}, `
45 UserPrincipalName,
46 CreatedDateTime `
47 | Export-Excel $xlsFile -WorksheetName "Internal User" -ClearSheet -AutoSize
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

Writing objects: 100% (10/10), 1.50 KiB | 765.00 KiB/s, done.
Total 10 (delta 6), reused 0 (delta 0), pack-reused 0 (from 0)
remote: Resolving deltas: 100% (6/6), completed with 4 local objects.
To https://github.com/KlaBier/Powershell.git
ba0474d..4e806c6 main -> main
PS C:\Users\klaus\OneDrive\GitContent\Powershell>

Klaus Bierschenk (now) Ln 8, Col 47 Spaces: 2 UTF-8 CRLF {} PowerShell

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



#wpninja



I WANT YOU

To control of
Guest Accounts

Is the guest account still needed?



Characteristics / Risks:

- Invitations can happen in many ways
- Without a lifecycle process, immortal
- Source of truth (management) in another Tenant
- Admin roles assigned
- Sponsor attribute

Actions:

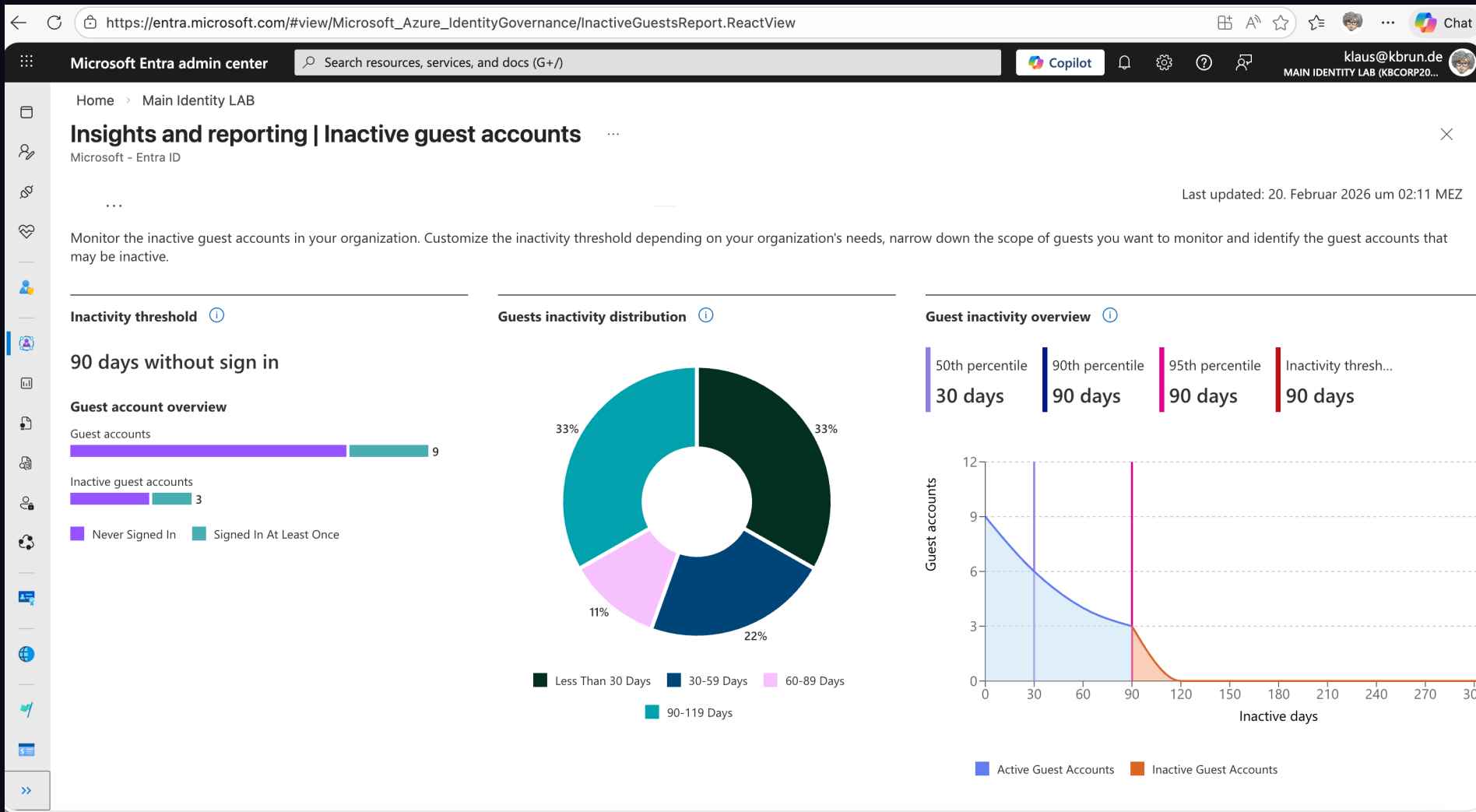
- ✓ Check Guest (Tenant) Settings
- ✓ Who is allowed to invite?
- ✓ Governance – View Inactive Guests
- ✓ Lifecycle Workflows
- ✓ Access Reviews! 👍

Demo



Guest Access Governance
Access Reviews
- automatic Account removal
Lifecycle Workflows





Clean out old groups



Characteristics / Risks:

- Groups without members
- Groups without an Owner
- Owner inactive

Actions:

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

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 | User registration details > Main Identity LAB > Insights and reporting | Inactive guest accounts

Groups | Insights (Preview)

Main Identity LAB

Overview

All groups

Insights (Preview)

Deleted groups

Diagnose and solve problems

Settings

General

Expiration

Naming policy

Activity

Privileged Identity Management

Access reviews

Audit logs

Bulk operation results

Troubleshooting + Support

New support request

Owner

Groups with No Owners

52

View data

Groups with Service Principals as Owners

0

View data

Groups with Guest Users as Owners

0

View data

Groups with Service Principals as Owners or Members

No groups with service principals found

Groups with service principal owners or members will appear here

Member

Groups with Complicated Rules

0

View data

Groups with Low Efficient Operators

2

View data

Lifecycle

Newly created groups

Expiring groups

Group Insights Feature

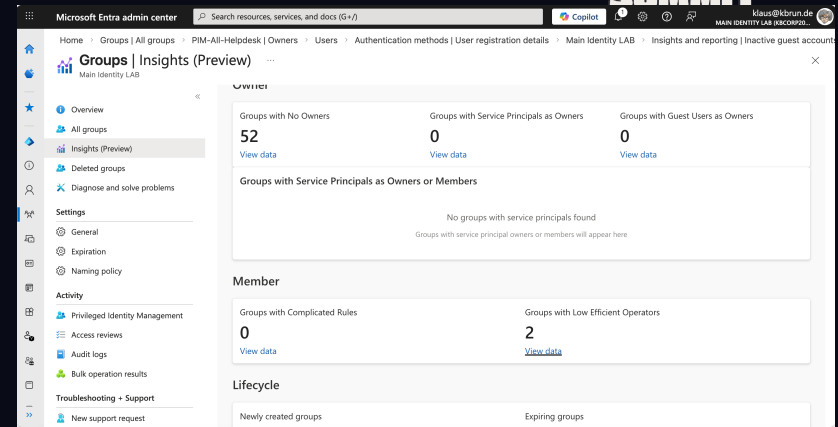


- Currently in preview

- Info on 2 levels:

1 Portal UI

-> Visual overview of group clutter



2 API Endpoint

-> Data source for custom reports (custom parameters)

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

Enterprise Apps / App Registrations



Who actually created this?

- No Owner
- No Sign-ins
- AssignmentRequired = Yes, but 0 Assignments
- Secret Hygiene? (App Registrations)
- PowerShell / EAC

Edge Datei Bearbeiten Anzeigen Verlauf Favoriten Profile Tab Fenster Hilfe

Main Identity LAB - Microsoft En X Recommendation to remove unu X

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView/initialValue//tabId/recommendationResourceId//fromNav/Identity

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

Usage & insights | Microsoft Entra application activity (Preview) Main Identity LAB Remove unused applications Main Identit

Main Identity LAB

+ Add Manage tenants What's new Preview features Got feedback?

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Overview Monitoring Properties Recommendations Setup guides

51 recommendations found

Priority	Recommendation	Required licenses	Release type	Secu
Medium	Enable password hash sync if hybrid	Microsoft Entra ID Free	Generally available	5/5
High	Do not expire passwords	Microsoft Entra ID Free	Generally available	8/8
Low	Use least privileged administrative roles	Microsoft Entra ID Free	Generally available	1/1
Low	Enable self-service password reset	Microsoft Entra ID P1	Generally available	1/1
High	Protect all users with a sign-in risk policy	Microsoft Entra ID P2	Generally available	0/7
Medium	Remove unused credentials from applications	Microsoft Entra Workload ID	Preview	N/A
Medium	Remove unused applications	Microsoft Entra Workload ID	Preview	N/A
High	Protect all users with a user risk policy	Microsoft Entra ID P2	Generally available	6.57,

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

#wpninjas

Housekeeping: Conditional Access Policies



Admin, looking into his CA
Policies to find unused
elements

#wpninja

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

Sign-ins using Legacy Aut... Sign-ins Access Package Activity Application Role Assignm...

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

Housekeeping: Privileged Roles - Privileged Identity Management (PIM)

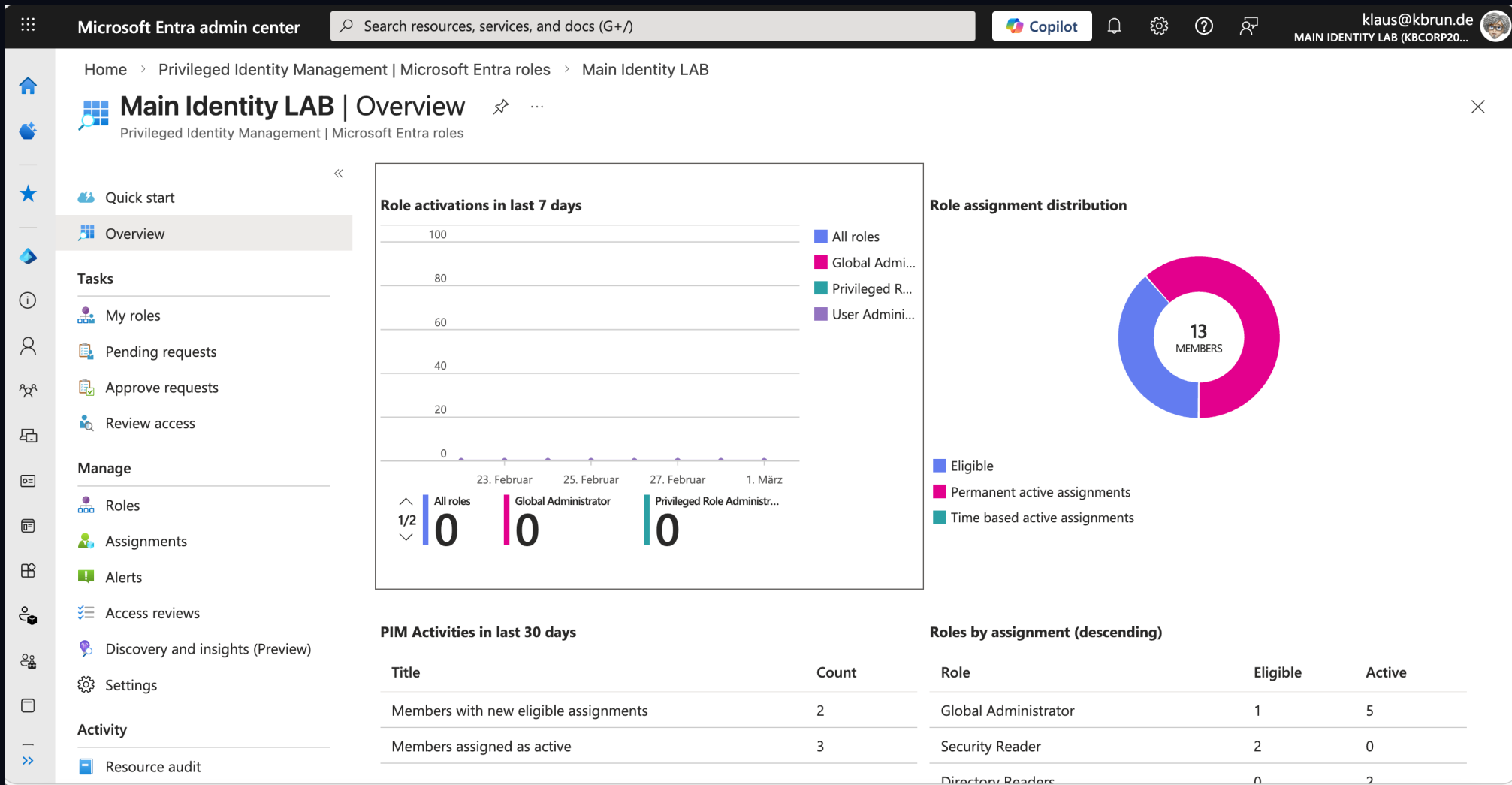


Sure, give everyone Global Admin!
What could possibly go wrong?

“Stale accounts with administrative privileges
are attractive targets”

— Microsoft Entra Security Guidance, 2026

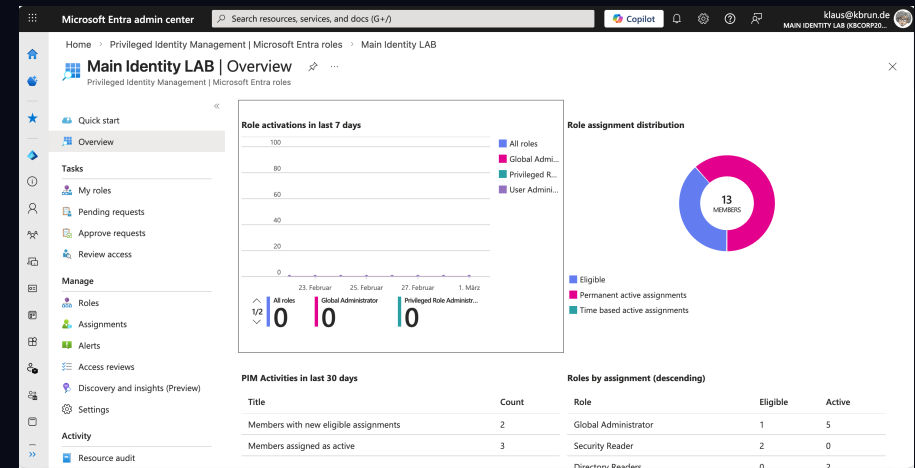
**So why do stale privileged accounts and unnecessary role assignments
remain in our tenants?**



Privileged Roles - PIM



- PIM – Dashboards -> Alerts
- Access Reviews for roles
- Alerts and Access Reviews are related to Privileged Roles
- PIM for Groups? -> Access Reviews (Groups)





Security Copilot and other AI



**Powerful it is.
Validate its answers, you must.**

Security Copilot for Housekeeping?



- Embedded Experience -> embedded in EAC
- Standalone Edition -> securitycopilot.microsoft.com
- Agents: Conditional Access Optimization Agent 
- Billed via Security Compute Units (SCUs)
SCUs measure Security Copilot capacity; pricing depends on the applicable capacity model.
- Create / remove SCU temporarily via Script 

Security Copilot for Housekeeping?



Security Copilot: Standalone - Portal / Edition

Microsoft Security Copilot / My sessions / Analyze the Conditional Access policies in our tenant and point out any that ...

default Share

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	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.

Security Copilot for Housekeeping?



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					

#wpninjas

Security Copilot for Housekeeping?



Security Copilot: Embedded Experience Entra Admin Center

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

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.

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

+

#wpninja

Security Copilot for Housekeeping?



Eligible Microsoft 365 E5 and E7 customers receive 400 SCUs per month per 1,000 paid user licenses, up to 10,000 SCUs per month

Example 1:

An organization with 400 seats receives 160 SCUs/month

Example 2:

An organization with 4,000 seats receives 1,600 SCUs/month.

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

MCP Server for Enterprise



- Extend your AI Client to Entra ID for Natural Language Prompting
- No additional license required for MCP Server for Enterprise itself
- Use read-only permissions for discovery and reporting
- Check out Merrill Fernando's Lokka Project / or Ugur Koc Developments
- Additional considerations, setup instructions and additional aspect in my blog post



MCP Server for Enterprise



Can you check CA Policies if there a overlapping settings, misconfigs, empty policies etc?

Used MCP Server for Entra Partner Lab Integration, loaded tools >

Now let me fetch the full details of each policy to do a thorough analysis:

Used MCP Server for Entra Partner Lab Integration >

I now have all the data I need. Here's a thorough analysis:

🔍 Conditional Access Policy Audit

You have 5 policies total. Here's what I found:

✅ Healthy Policies

CA02-All:MFA-AdminAccounts and **CA03-All:MFA-UserAccounts** are well-structured and complementary. CA02 targets 12 admin roles, CA03 targets all users — together they provide MFA coverage. Both correctly exclude the same break-glass group (`1394bdc7...`).

CA01-All: SessionLifetime12h-AllUser enforces session controls (sign-in frequency: 16h, persistent browser: never) for all users. Note: The name says "12h" but the configured value is **16 hours** — a naming inconsistency worth fixing.

⚠️ Issues Found

1. 🚫 Overlap — Admins get MFA twice

CA02 targets admin roles with MFA. **CA03** targets **All users** with MFA. Since admins are also users, every admin account is covered by *both* policies simultaneously. This isn't necessarily harmful (MFA is still just MFA), but it's redundant and adds evaluation overhead. You should either:

- Exclude admin roles from CA03, or
- Consolidate into a single MFA policy with "All users" scope.

This looks like it may have been created for a specific workflow (step-up auth via authentication context). The naming is confusing and it has **never been modified** since creation (April 2025). Recommend reviewing whether this is intentional and renaming it to reflect its actual purpose (e.g., `CA04-GlobalAdmins:MFA-AuthContext-c1`).

4. 🟡 Session Policy Has No Grant Control

CA01 has `grantControls: null` — it only enforces session lifetime but doesn't require MFA or any other access requirement as a precondition. This is architecturally fine (session policies often stand alone), but means a user could have a long-lived session established without step-up. Evaluate whether adding a compliant device or MFA grant would be appropriate.

5. 🟡 Naming Inconsistency in CA01

Policy name says "SessionLifetime12h" but `signInFrequency.value` is **16 hours**. Low severity but misleading for operators.

📄 Summary Table

Policy	State	Issue
CA01 - SessionLifetime12h-AllUser	✅ Enabled	Name says 12h, config is 16h
CA02 - MFA-AdminAccounts	✅ Enabled	Overlaps with CA03 (admins are also "All users")
CA03 - MFA-UserAccounts	✅ Enabled	Overlaps with CA02
AllowDeletedItems	⚠️ Enabled	Confusing name, auth context scope, needs review
test	🚫 Report-only	Empty policy — targets no users, no apps. Delete it.

Recommended Actions

- Delete or reconfigure the `test` policy immediately.
- Rename `AllowDeletedItems` to something meaningful and document its intent.
- Fix the name of CA01 to reflect the actual 16h sign-in frequency.
- Consider excluding admin roles from CA03 to eliminate the MFA overlap, keeping the policies clean and non-redundant.
- Review CA01 to decide if a grant control (e.g., compliant device) should accompany session enforcement.

#wpninjas

Takeaways – Housekeeping Principles



- ✓ No recent activity is a reason to investigate, not a reason to delete
- ✓ An owner field is not enough, someone must actively take responsibility
- ✓ Users, guests, groups, and service principals need different inactivity criteria
- ✓ Prefer reversible remediation before permanent deletion

❖ **Housekeeping is not a project – it is a process** ❖



#wpninja

Further resources



Microsoft Learn

[Embrace cloud-first posture: Convert Group Source of Authority to the cloud resources](#)

[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

[Merill Fernando – Lokka](#)

[Ugur Koc OpenAdminOS](#)



NothingButCloud Blog

[Natural Language Queries Against Entra ID — No Extra License Required](#) ← **Blog Post (Claude and Entra)**

[KlaBier Github: CreateSecCopilotSCU PowerShell](#)

[KlaBier Github: Powershell Housekeeping examples](#) ← **WPNinjas examples**

[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](#)

#wpninjas

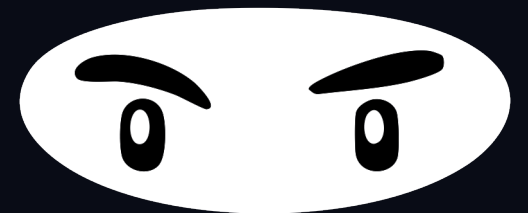
**Thank You,
Ninjas!**



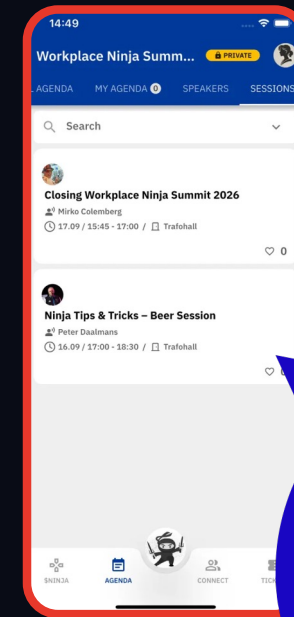
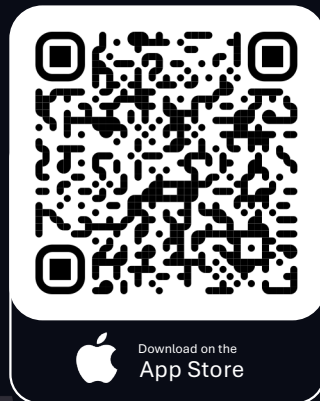
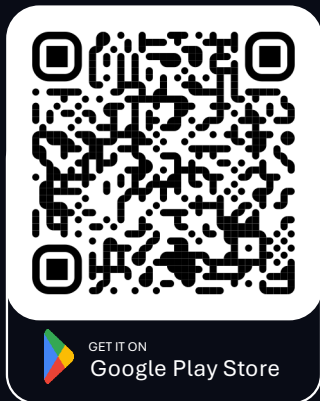
See You
Next Year!



SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT



Download the app and never miss any updates



We appreciate
your feedback!