

W
E
L
C
O
M
E

T
O

WORKPLACE NINJAS NORWAY



SHARING KNOWLEDGE. TOGETHER.



Entra ID Housekeeping

Identifying and Removing Abandoned Objects to Reduce Risk

By Klaus Bierschenk

#WPNinjasNO

SHARING KNOWLEDGE. TOGETHER.





Thank you sponsors

Gold Sponsors

Fortytwo.io POINT:TAKEN



PATCH
MY PC

Recast

robopack 
empowered by SOFTWARE
CENTRAL

Silver Sponsors

control ^{UP} 

glueck  kanja

software **one**

 2Pint

twoday

Bronze Sponsors

 CloudWay

spirhed







About Klaus Bierschenk

Focus

Identity / Security

From

Murnau / Germany (1h south of Munich)

My Blog

<https://Nothingbutcloud.net>



Certifications



Hobbies

Sports, Mountains

Contact



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



Klaus@nothingbutcloud.net /



“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?



Agenda

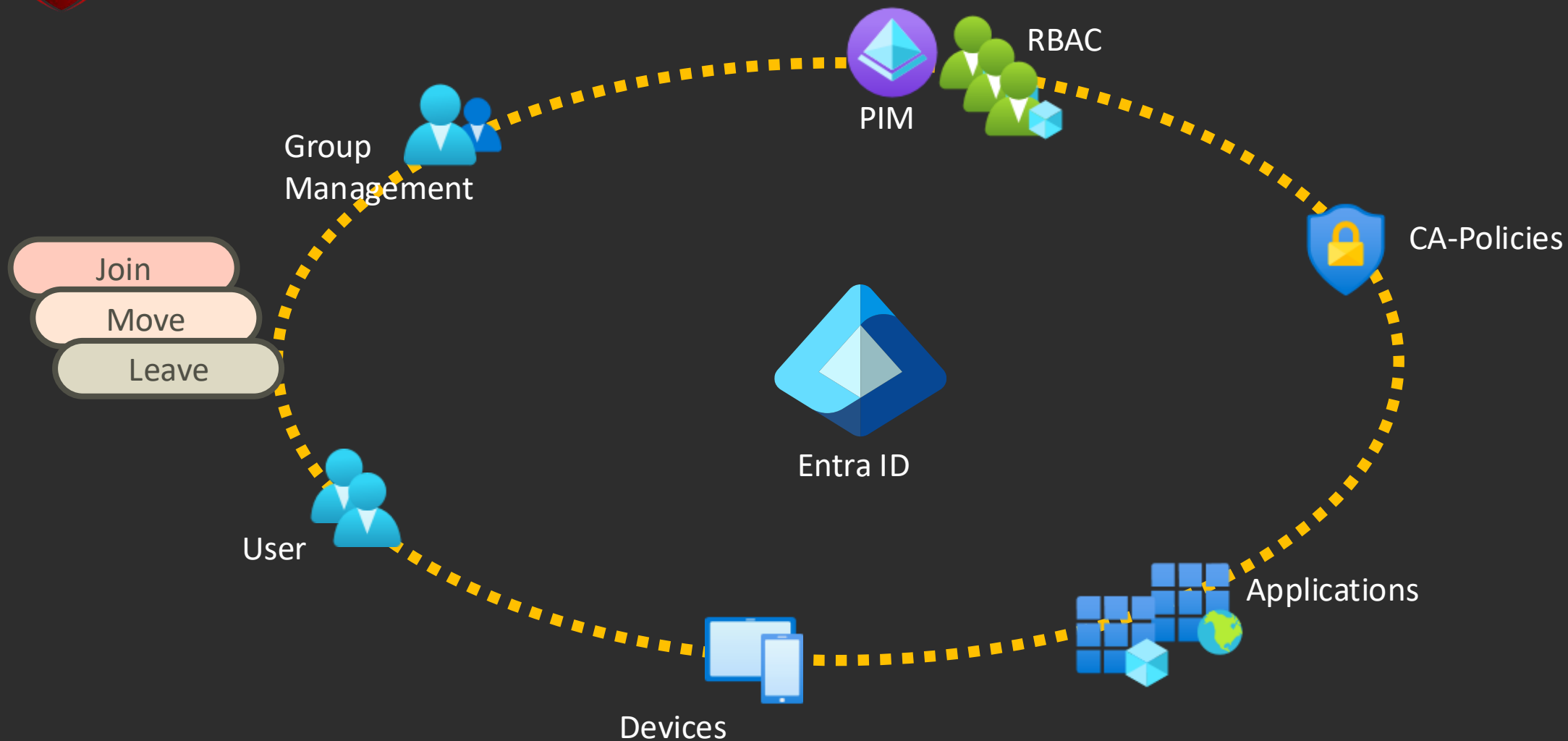
If you don't clean up your tenant,
someone else might do it for you

- ❖ 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



How and where does tenant clutter arise?






Does the user still exist?

Characteristics / Risks:

- Quickly created, bypassing standard processes
- Manager or other company attributes empty
- No MFA method
- Is Owner? Manager?
- Exceptions in CA Policies - *often forgotten, rarely reviewed*

Actions:

- ✓ Entra Admin Center
- ✓ Registered Authentication Methods
- ✓ lastSignInDateTime / PS 
- ✓ Lifecycle Workflows
- ✓ Natural Language Query:
„List all users with no login since 90 days“
- ✗ Access Reviews (rather not)





Demo

Entra Admin Center
User Filter
Authentication Methods
PowerShell is your friend



Users

Main Identity LAB

- + New user
- Edit
- Delete
- Download users (Preview)**
- Bulk operations
- Refresh
- ...

Azure Active Directory is now Microsoft Entra ID.

Search Add filter

63 users found

<input type="checkbox"/>	Display name ↑	User principal name ↕	Last interactive sign-in time	User type	On-premises sy...	Identities
<input type="checkbox"/>	Adele Vance (Helpdesk)	AdeleV@kbcorp2...	9. Mai 2025, 19:08	Member	No	kbcorp2021.onmicrosoft.com
<input type="checkbox"/>	Adele Zetta	EMP1941@kbcor...	19. Jan. 2025, 09:42	Member	No	kbcorp2021.onmicrosoft.com
<input type="checkbox"/>	Alex Wilber (Helpdesk)	AlexW@kbrun.de	23. Okt. 2025, 17:45	Member	No	kbcorp2021.onmicrosoft.com
<input type="checkbox"/>	Alvin Herrera	Alvin.Herrera@kb...		Member	Yes	kbcorp2021.onmicrosoft.com
<input type="checkbox"/>	Andreas	Andreas_kbcorp2...	28. Dez. 2025, 10:12	Member	No	ExternalAzureAD
<input type="checkbox"/>	Anna	Anna_kbcorp2022...		Member	No	ExternalAzureAD
<input type="checkbox"/>	Anthony Rodgers	Anthony.Rodgers...		Member	Yes	kbcorp2021.onmicrosoft.com

- Manage view > **Edit columns**
- Per-user MFA
- Copy link to view
- Got feedback?

3

2

1

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
HMaster@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
ADTAAADS...	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

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

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 Anmelde datum  
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>



#WPNinjasNO



I WANT YOU

To take care of your
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 foreign Tenant
- Admin roles assigned
- CA-Policies applied to guests?
- Sponsor attribute

Actions:

- ✓ Check Guest (Tenant) Settings
- ✓ Who is allowed to invite?
- ✓ Governance – View Inactive Guests
- ✓ Lifecycle Workflows
- ✓ Natural Language Query:
„list all guest accounts without a sponsor set“
- ✓ Access Reviews!





Demo

Guest access governance
Access Reviews
Lifecycle Workflows



Home > Main Identity LAB

Insights and reporting | Inactive guest accounts

Microsoft - Entra ID

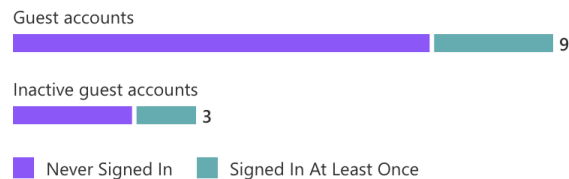
Last updated: 20. Februar 2026 um 02:11 MEZ

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.

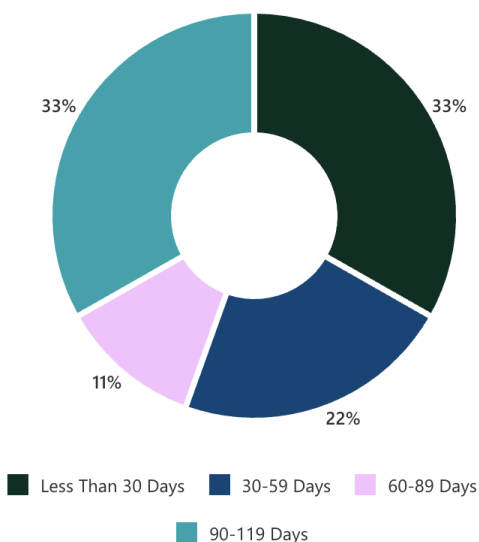
Inactivity threshold

90 days without sign in

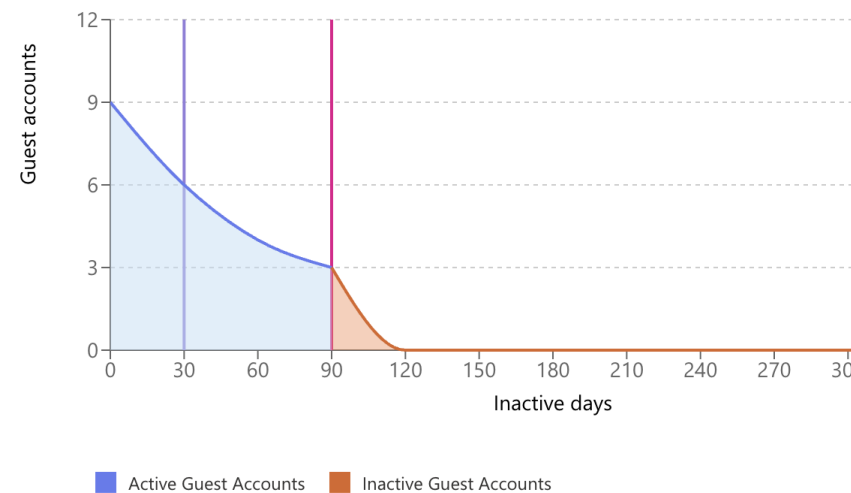
Guest account overview



Guests inactivity distribution



Guest inactivity overview





Clean out old groups

Characteristics / Risks:

- Groups without members
- Groups without Owner
- Owner inactive

Actions:

- ✓ Groups Insights (Preview)
- ✓ Powershell / Graph
- ✓ Source of truth?
- ✓ Natural Language Example:
„list all groups with no sponsor, no member or with any other topics relevant for housekeeping“
- ✓ Managed by vs. Owner



Microsoft Entra admin center Search resources, services, and docs (G+)

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	Groups with Service Principals as Owners	Groups with Guest Users as Owners
52 View data	0 View data	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	Groups with Low Efficient Operators
0 View data	2 View data

Lifecycle

Newly created groups	Expiring groups

EAC -> Groups -> Groups Insight (Preview)



Group Insights Feature

- Currently in preview

- Info on 2 levels:

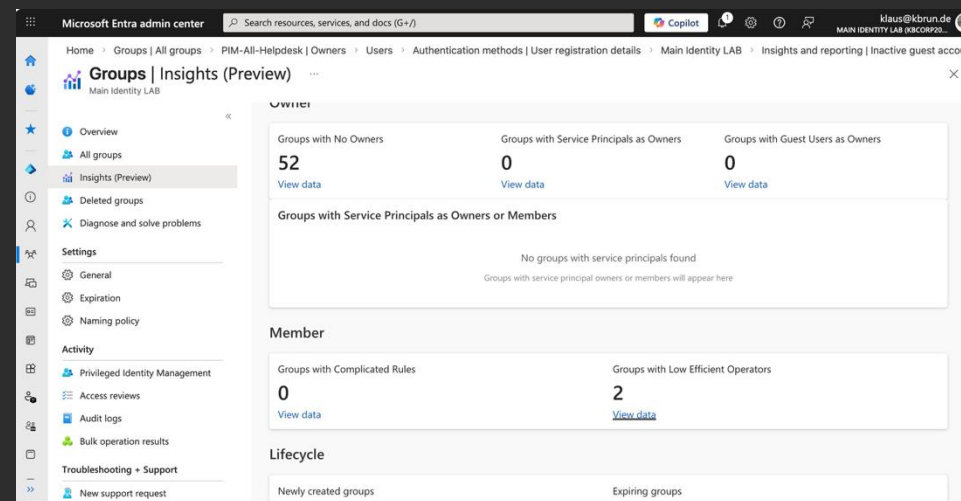
1 Portal UI

-> 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





Enterprise Apps / App Registrations

Microsoft Entra admin center

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

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



Housekeeping: Conditional Access Policies



**Admin, looking into his CA
Policies to find unused elements**

- 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 Auth...
- 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

Microsoft Azure Search resources, services, and docs (G+)

Home > Log Analytics workspaces > LA-WS-AAD

LA-WS-AAD | Workbooks | CA Policy Usage

Log Analytics workspace

Search

Workbooks Edit Save Refresh Share Help Auto refresh: Off

CA-Policy Summary

Data coverage
30 days of history available – first entry 30.01.2026

Column Legend
Success = granted
Failure = blocked
NotApplied = conditions not met
ReportOnly = simulation
EnforcedCount = Success + Failure

PolicyName	PolicyId	Success	Failure	NotApplied	Report
CA001-Global-BaseProtection-AllApps-AnyPlatform-Bloc...	cdc3ac53-e78f-45ff-840b-09059df290a6	0	0	0	
CA002-Global-BaseProtection-AllApps-AnyPlatform-Sessi...	acbe4875-9545-4d8c-9ea4-60e1c4d83d56	0	0	0	
CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA	049fab0d-a309-43b9-a3f9-e2f25aa9caf8	455	2	10	
CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA...	c8cfb111-9041-49ed-a46f-c69e1b6c389c	0	0	0	
CA004-Global-EntraTerms-AllApps-AnyPlatform-ToU xxx	0d8db2f1-acb9-4f2f-9fd0-c25230404a8d	0	0	0	
CA007-Global-IdentityProtection-SignInRiskMediumHigh...	b6206cf6-2cc5-4ffe-a5b5-ed447d62682f	0	0	467	
CA008-Global-IdentityProtection-UserRiskHigh-ChangePW	320d5244-2109-4428-b3f6-7eb7e9f59d8d	0	0	467	
CA100-Admins-BaseProtection-AllApps-AnyPlatform-MF...	c4c15e2f-b6d4-48a3-acd6-33099b15c414	362	2	103	
CA101-Klaus-BaseProtection-AllApps-AnyPlatform-Sign...	22a1da8b-0402-459b-b92c-202d56022e2c	0	0	0	





Housekeeping: Privileged Roles - Privileged Identity Management (PIM)



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



Housekeeping - PIM

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

Role	Count
All roles	0
Global Administrator	0
Privileged Role Administrator	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

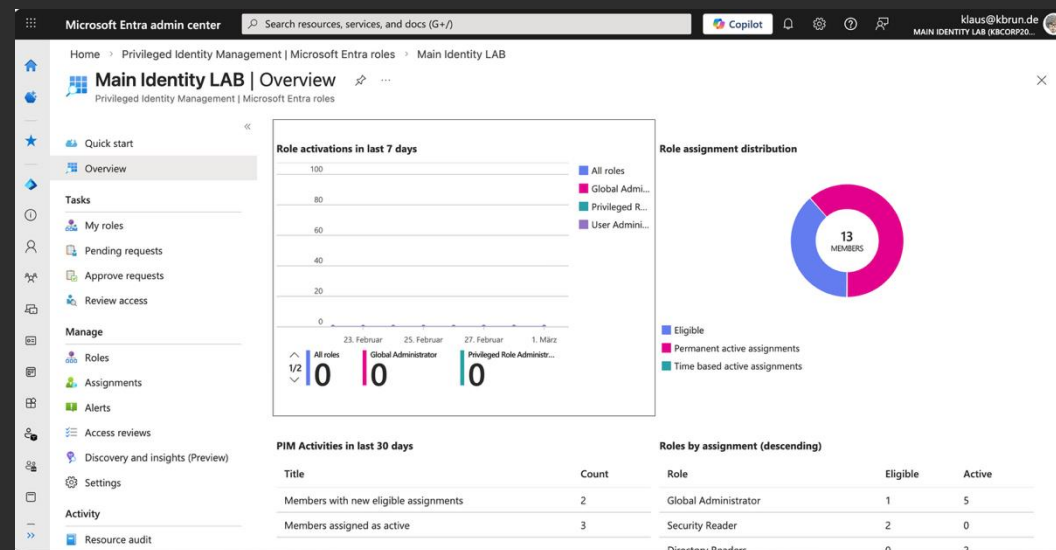
Roles by assignment (descending)

Role	Eligible	Active
Global Administrator	1	5
Security Reader	2	0
Directory Readers	0	2



Housekeeping - 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



Much it can do. Know 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)
Computing Units - technical consumption unit, \$4 per hour
- Create / remove SCU temporarily via Script 



Security Copilot for Housekeeping?

Security Copilot:
Standalone -
Portal / Edition

The screenshot displays the Microsoft Security Copilot interface. The top navigation bar includes 'Home', 'Agents', 'Promptbooks', 'Build', 'History', 'Owner', and 'Security Store'. The main content area shows a session titled '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.' The analysis is completed in 33 seconds. A table lists the identified issues:

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

Additional details include a note about CA999, a 'References' section with a link to 'Verify on Entra Admin Center', and a 'How's this response?' section. The interface also features an 'Export to Excel' button and a footer with the user's name 'Klaus Admin' and email 'klaus@kbrun.de'.



Security Copilot for Housekeeping?

	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					



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 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.

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

[+](#) [→](#)



Security Copilot for Housekeeping?

Eligible Microsoft 365 E5 customers receive
**400 Security Compute Units (SCUs) per month per
1,000 E5 licenses** (max. 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 Licensing costs
- Read Only Operations
- Check out Merrill Fernando's Lokka Project



- Additional reading how to setup and additional aspect in my latest blog post





We value your feedback

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

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



Takeaways

- ✓ Consistently eliminate orphaned identities
 - Users, groups, applications
 - Powershell and automation ([Blog Article](#))
 - Documentation
- ✓ Define a Governance Strategie
 - Access Review
 - Lifecycle Workflows
- ✓ Housekeeping is not a project – it is a process





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

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

[Merill Fernando - Locca](#)



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](#)





Any questions



Thank You

Please rate
this session!



Entra ID Housekeeping - Identifying and Removing Abandoned
Objects to Reduce Risk