

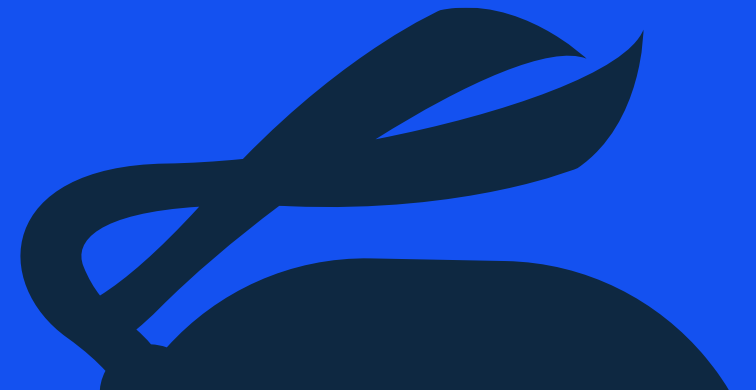
# SECURITY NINJA

GERMANY



SECURITY

# Servus Ninjas!



# About me



Session

## From Tenant Sprawl to Tenant Control: AI and Modern Governance in Microsoft Entra

Klaus Bierschenk

CGI Germany, Microsoft Security MVP



<https://nothingbutcloud.net/>



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



#SecNinjas

# Thank you to our Sponsors!

Host Partner



Gold

glueck  kanja

water   
IT Security & Defense

robopack 

**PROACT**

Silver

**WORKSIMPLE**  
EINFACH ARBEITEN

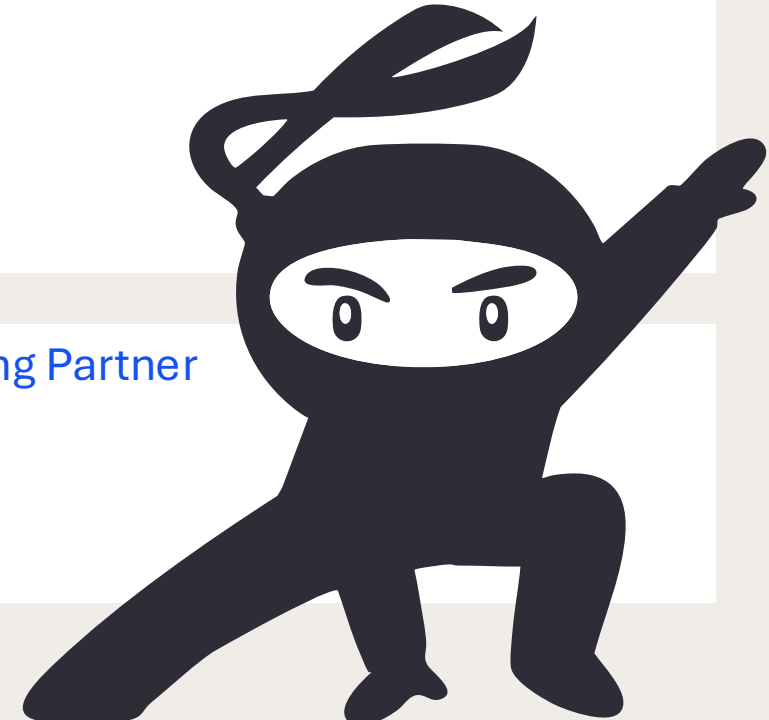
 **semperis**

Bronze

 **ugurlabs**

 **ic CONSULT**

Snacks & Networking Partner



## Setting the Stage

- ❖ What is the problem?
- ❖ Deterministic vs. AI: It's Not a Competition

## Exploring AI Approaches

- ❖ How Can AI Talk to Entra ID?
  - Agent Builder · Security Copilot · MCP Server for Enterprise



# What is the problem?

| Object type       | What makes me suspicious                   | Why can't I just delete it?              | Existing tools                                                                                                                                                                                                                                                                   |
|-------------------|--------------------------------------------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Users             | No sign-in, no MFA, missing manager        | Owner of resources? Manager?             | lastSignInDateTime (PSH) EAC, Registered auth. Methods,  <b>Access Reviews</b>                                                                                                                |
| Guests            | Long inactive, no sponsor                  | External lifecycle / access still needed | lastSignInDateTime (PSH) EAC, Registered auth. Methods,  <b>Access Reviews</b><br>Guest Access Governance  |
| Groups            | No members, no owner, inactive owner       | Used for roles, apps or automation       | PowerShell, Groups Insight (Preview)                                                                                                                                                                                                                                             |
| Apps              | No sign-ins, no owner, old secrets         | Integration still required?              | Powershell, Enterprise Application Activity (EAC)                                                                                                                                                                                                                                |
| CA Policies       | No hits / overlapping / disabled           | Security dependency?                     | Workbooks                                                                                                                                                                                                                                                                        |
| Privileged access | Old or unused assignments, permanent roles | Operational dependency?                  | PIM Dashboard                                                                                                                                                                               |

# Deterministic vs. AI: It's Not a Competition

---

## DETERMINISTIC

PowerShell · KQL · Workbooks

- Delivers consistent and reproducible results
- Systematically checks objects against defined criteria
- Enables scheduled checks, reporting and automated remediation

## Artificial Intelligence

Security Copilot · MCP + LLM

- Can discover unexpected patterns and relationships
- Helps explain findings, understand context and identify risks
- Allows interactive investigations using natural language

**AI to explore. Scripts to prove. Humans to decide.**

# How Can AI talk to Entra ID?



Agent Builder  
(M365 Copilot)



Knowledge-  
based



Declarative  
Agent



Security Copilot



Embedded /  
Standalone



Security  
Agents



MCP Server for Enterprise



AI-Tool  
Integration



Entra ID  
Access



## Agent Builder (M365 Copilot)

- Works with documents, SharePoint content, and websites
- No direct access to Entra ID objects or configurations
- Agents can be shared and published for others to use

# How Can AI talk to Entra ID?



## Prompt-Example

*„You are reviewing Conditional Access policy names for compliance with our organization's naming convention. Evaluate the following policies exclusively against your configured knowledge source“*

### Entra Document Advisor

Using the configured naming convention:

**CA{NNN}--{Action} | {Scope} for {Persona} [when {Condition}]** with required elements sequence number, action, scope, and persona. github

| Policy Name                         | Compliant?            | Violations                                                                                                                                                               | Suggested Corrected Name*                                                                                            |
|-------------------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| CA001 - Require MFA for All Users   | ❌ No                  | Does not follow the documented format. Uses "CA001 -" instead of CA001-- Action. Missing the required `                                                                  | {Scope}` separator. "MFA" is included but the scope is not clearly separated from the persona. <small>github</small> |
| CA105-Require   All Apps for Admins | ✅ Yes (syntactically) | Matches the documented pattern: sequence number, action, scope, and persona are present. Semantic accuracy cannot be verified from the name alone. <small>github</small> | No change required                                                                                                   |
| Block Legacy Authentication         | ❌ No                  | Missing the required CA sequence number, action token, scope, and persona. The source                                                                                    | CA###-Block   Legacy Authentication for <Persona>                                                                    |

- ⊕

New chat
- 🔍

Search
- 📖

Library
- 🔗

Agents
- 📁

Notebooks

Chats

No chats yet. Once you start chatting, you can return to past conversations here.

# Agent Store

🔍

Search for an agent

## Your agents



Entra Document Advi...



Microsoft 365 Admin

## Built by Microsoft



Workflows (Frontier)

Build agent flows with natural language, no code needed.

★ 5.0 (1 ratings)



SharePoint page agent

Transform conversation results into SharePoint pages.

★ 5.0 (1 ratings)



Learning

Upskill in AI and other in-demand areas with personalized learning

★ 5.0 (5 ratings)



## Agent Builder (M365 Copilot)

- Works with documents, SharePoint content, and websites
- No direct access to Entra ID objects or configurations
- Agents can be shared and published for others to use

# How Can AI talk to Entra ID?



Agent Builder  
(M365 Copilot)



Knowledge-  
based



Declarative  
Agent



Security Copilot



Embedded /  
Standalone



Security  
Agents



MCP Server for Enterprise



AI-Tool  
Integration



Entra ID  
Access



## Security Copilot

- Embedded Experience → Integrated into the Entra admin center
- Standalone Experience → [securitycopilot.microsoft.com](https://securitycopilot.microsoft.com)
- Agents: Conditional Access Optimization Agent
- Capacity measured in Security Compute Units (SCUs)

*Billing depends on the applicable licensing and capacity model:  
Inclusion Capacity vs. Provisioned Capacity*

Demo

# How Can AI talk to Entra ID?



```
# For details check
# "Security Copilot - quickly turned on and off"
# https://nothingbutcloud.net/2025-01-16-SCU_ON_OFF/

# Connect to the correct tenant and subscription
Connect-AzAccount -Tenant 'f5c07476-f2f0-45bf-8745-34a90b6a2a1d' -SubscriptionId 'dda6b7d7-
#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
#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=4; crossGeoCompute="NotAllowed"; geo="EU"} `
  -force

# Don't forget to delete the SCU or the resource group afterwards
```

```
# Quick delete the entire RG with the associated SCU

Connect-AzAccount -Tenant 'f5c07476-f2f0-45bf-8745-34a90b6a2a1d'

Remove-AzResourceGroup -Name "SecurityCopilotRG" -force
```

Powershell / CreateSecCopilotSCU /

Klaus Bierschenk adds some comments

a60a3b6

| Name                    | Last commit message |
|-------------------------|---------------------|
| ..                      |                     |
| CreateSecCopilotSCU.ps1 | adds some comments  |
| DeleteSecCopilotSCU.ps1 | Update SKU Cmdlets  |

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



- 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 my Entra ID tenant. Identify policies that appear redundant, overly broad, or have no users or applications in scope. For each finding, include the policy name, explain the potential issue, and suggest an improvement. Export the results to an Excel file (.xlsx), with one row per finding.

>

23 steps completed

38 seconds

Oct 16, 3:10 PM

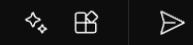
AI-generated content may be incorrect. Check it for accuracy.

Export to Excel

| Policy Name                                                          | Potential Issue                                                                         | Suggested Improvement                                                                                     |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA                  | Overly broad: Applies MFA to all users and all apps, except a few exclusions.           | Consider narrowing scope to high-risk users/apps or using risk-based policies for better user experience. |
| CA007-Global-IdentityProtection-SignInRiskMediumHigh-MFA             | Redundant: Nearly identical to "Require multifactor authentication for risky sign-ins". | Consolidate with similar policies to reduce management overhead and avoid conflicts.                      |
| Require multifactor authentication for risky sign-ins                | Redundant: Overlaps with "CA007-Global-IdentityProtection-SignInRiskMediumHigh-MFA".    | Merge with the other risk-based MFA policy for clarity and simplicity.                                    |
| CA002-Global-BaseProtection-AllApps-AnyPlatform-SessionLifetime12hrs | Disabled: Policy is not enforced, so has no effect.                                     | Remove or enable if session lifetime control is required.                                                 |

This table summarizes 11 Conditional Access policy findings based on redundancy, overly broad scope, or

How can Security Copilot help?



- Home
- Agents
- Promptbooks
- Build

Preview
- History

^

All history
- Owner

^

Owner settings

Plugin settings

Role assignment

Manage workspaces

Usage monitoring
- Security Store

# Usage monitoring

Last updated 3:14 PM

The security compute units available to your workspace per hour is determined by the number of provisioned units you've purchased, and any added overage units. [Learn more about usage](#)

SecurityCopilotSCU + New capacity

Change units View billing in Azure

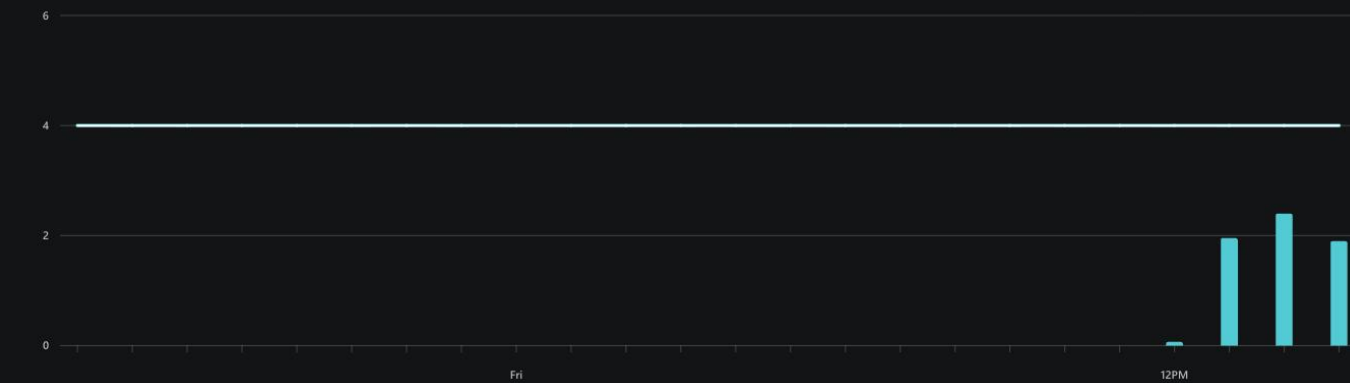
Provisioned units used  
1.9 of 4 units  
in the last hour

Workspace using this capacity

default

Manage workspaces

Date: Last 24 hours



| Session ID                                        | Date ↓           | Units used | Initiated by              | Category    | Type   | Copilot experience         | Plugins used               |
|---------------------------------------------------|------------------|------------|---------------------------|-------------|--------|----------------------------|----------------------------|
| 77f9a9b2-2e86-4840-a136-842f78ec24c6              | Oct 16, 03:10 PM | 1.9        | <div>KA</div> Klaus Admin | User prompt | Manual | Security Copilot portal    | Microsoft Entra            |
| <div>☑</div> e1d813b7-5a9c-4ad1-97f0-862620434b99 | Oct 16, 02:48 PM | 2.2        | <div>KA</div> Klaus Admin | User prompt | Manual | Copilot in Microsoft Entra | Query Microsoft Graph data |
| e1d813b7-5a9c-4ad1-97f0-862620434b99              | Oct 16, 02:48 PM | 0.7        | <div>KA</div> Klaus Admin | User prompt | Manual | Copilot in Microsoft Entra | Query Microsoft Graph data |
| e1d813b7-5a9c-4ad1-97f0-862620434b99              | Oct 16, 02:26 PM | 1.6        | <div>KA</div> Klaus Admin | User prompt | Manual | Copilot in Microsoft Entra | Query Microsoft Graph data |
| <div><div></div> SecurityCopilotAgentUse</div>    |                  |            |                           |             |        |                            |                            |



## Security Copilot (Inclusion Capacity)

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

### 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>

# How Can AI talk to Entra ID?



Agent Builder  
(M365 Copilot)



Knowledge-  
based



Declarative  
Agent



Security Copilot



Embedded /  
Standalone



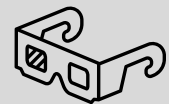
Security  
Agents



MCP Server for Enterprise



AI-Tool  
Integration



Entra ID  
Access



## MCP Server for Enterprise

- **Easy integration** with AI clients (Claude, ChatGPT, etc.)
- **Delegated permissions** – granular access control
- **No secrets or certificates** – OAuth 2.0 with PKCE (Public Clients)
- **Microsoft-hosted service** – no infrastructure to maintain

Claude

+ New

📁 Projects

📦 Artifacts

</> Code

📁 Customize

Chats and tasks

📁 Customize Claude for you

○ Your first chat with Claude

🔍 Search

Settings

⚙️ General

👤 Account

🔒 Privacy

💰 Billing

📦 Capabilities

🕒 Memory

⚖️ Reflect

🕒 Time and focus

</> Claude Code

Customize

📖 Skills

📦 Connectors

🔌 Plugins

Connectors

Yours

Discover

🔍 Search

⚙️

+ Add

▼

| Connector    | Type | Status             |
|--------------|------|--------------------|
| <div>🔄</div> |      | <div>Connect</div> |

Add custom connector

×

Connect Claude to your data and tools. [Learn more about connectors](#) or get started with [pre-built ones](#).

MCP Server for Enterprise

Shown in the connectors list.

https://mcp.svc.cloud.microsoft/enterprise

The HTTPS address where the server accepts MCP requests, for example https://mcp.example.com/mcp.

Only use connectors from developers you trust. Anthropic does not control which tools developers make available and cannot verify that they will work as intended or that they won't change.

Building an MCP server? [Report issues and subscribe to updates here](#)

Cancel

Continue

- + New
- Projects
- Artifacts
- Code
- Customize

## Chats and tasks

- Customize Claude for you
  - Your first chat with Claude

## Settings

- General
- Account
- Privacy
- Billing
- Capabilities
- Memory
- Reflect
- Time and focus
- Claude Code

## Customize

- Skills
- Connectors**
- Plugins

## Add custom connector



Connect Claude to your data and tools. [Learn more about connectors](#) or get started with [pre-built ones](#).

## MCP Server for Enterprise

https://mcp.svc.cloud.microsoft/enterprise

## Authentication ⓘ

- ☒ **Sign in now** Detected  
Each user signs in through the server's OAuth flow before they can use any tools or resources.
- ☐ **Sign in when needed**  
Claude connects without credentials first and prompts users to sign in when the server asks. Pick this for servers that offer some tools without an account.
- ☐ **No sign-in**  
Pick this for servers with open access, or for servers that use an API key instead of OAuth.

## OAuth client ⓘ

- ☐ **Use Claude's published identity**  
The server reads Claude's client details from a URL Anthropic hosts (CIMD). Nothing to set up, but the server must support it.
- ☐ **Register automatically**  
Claude registers OAuth clients with the server as users connect (DCR). Works with most servers, but creates many client registrations on busy ones.
- ☒ **Use your own OAuth client** Detected  
Enter a client ID you registered with the server yourself. Leave the secret blank unless your authorization server requires one.

The public identifier from your provider's OAuth app settings. Not an API key or token.

Leave blank unless your authorization server requires a client secret.



+ Add ▾

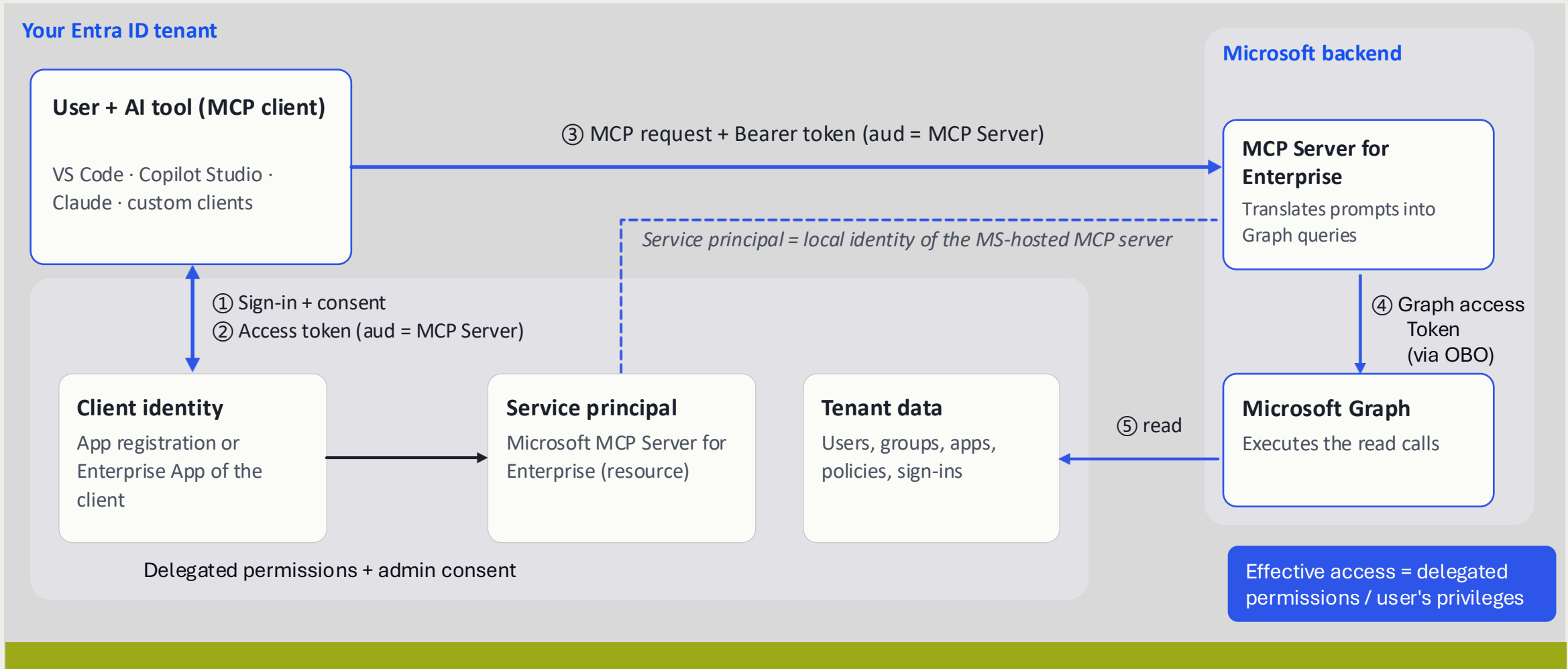
## Status

Connect

# How Can AI talk to Entra ID?



## MCP Server for Enterprise – components and token flow

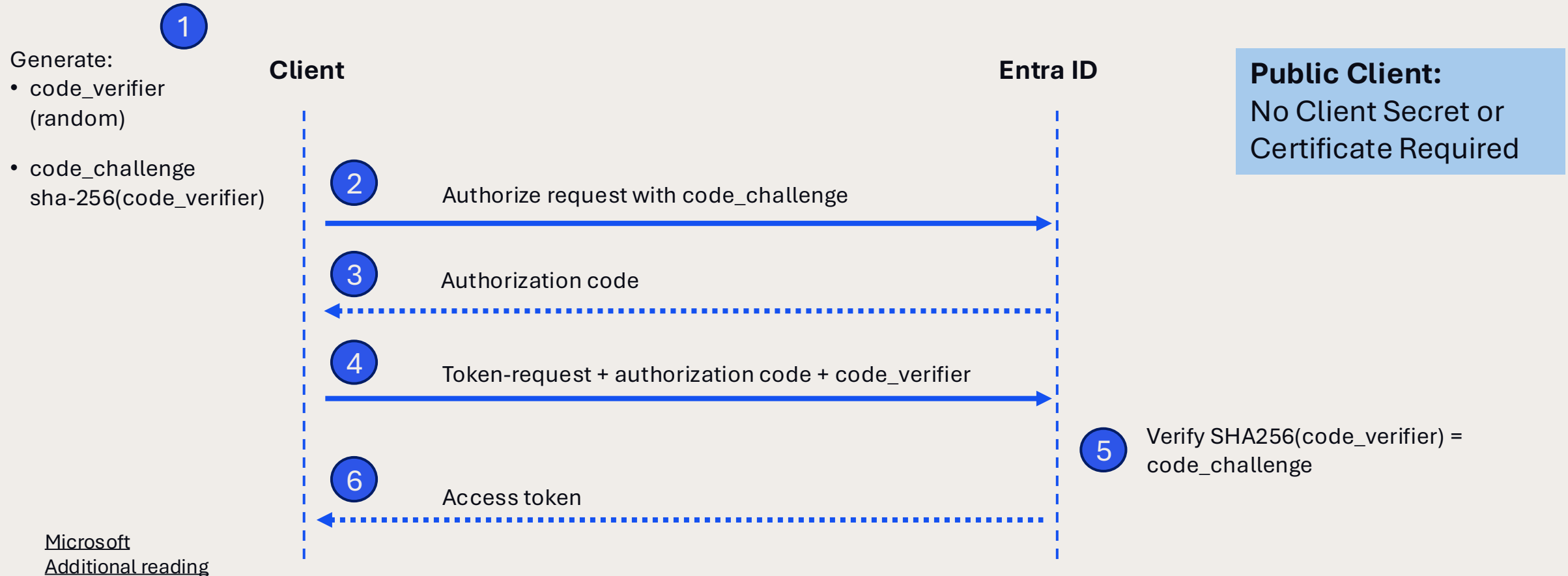


# How Can AI talk to Entra ID?



MCP Server for Enterprise

Authorization Code Flow with PKCE (Proof Key for Code Exchange)





🔍 Search

+ New

📁 Projects

🔗 Artifacts

🕒 Scheduled

🛠 Customize

> More

Recents > 🔧

🌟 Good evening, Klaus

How can I help you today?



Project or folder ▾

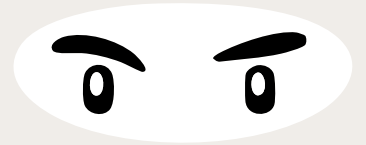
Opus 5.5 Medium Auto



# MCP Server for Enterprise – Key Takeaways

---

- Natural language access to Entra ID
- Delegated permissions & Entra RBAC
- OAuth with PKCE – no client secret required for public clients
- One app registration, multiple administrators
- Flexible choice of AI clients, read-only access to Entra



Access control is only half the story. Data privacy is the other.

# Same App, Different User – Access Denied

Claude

+ New

Projects

Artifacts

Scheduled

Customize

> More

Recents >

CA policies audit

Used MCP-Server-For-Enterprise, 1 failed >

I couldn't read the policies: Graph returned **403 Forbidden** on `/identity/conditionalAccess/policies`.

The scopes on the MCP connection are fine, since the request got past consent. The block is on the signed-in account. It doesn't currently hold a directory role that can read Conditional Access. Graph accepts any of these:

- Global Reader or Security Reader (enough for read-only review)
- Conditional Access Administrator, Security Administrator or Global Administrator
- Devices Admin or Entra Network Access Administrator

The most likely cause is an eligible PIM assignment that isn't active right now. That fits a Sunday session where nothing has been elevated yet. Activate Global Reader or Security Reader in PIM and tell me when it's done. I'll run the query again. A new token may be needed before the activation takes effect, so if it still fails, reconnect the connector.

Once I have access, I'll pull the full policy objects (conditions, grant and session controls) and check them for:

- Duplicate or overlapping policies: same users/apps/conditions with the same or conflicting controls
- Policies stuck in report-only or disabled that look like they were meant to be enforced
- Missing or one-sided break-glass exclusions
- Exclusions that reference deleted users, groups or named locations
- Legacy auth gaps, MFA gaps for admin roles, and policies targeting "All users" with no exclusions
- Grant controls set to OR where AND was probably intended, and conflicting session controls

Reply

+ 🔊 🗨️

Klaus · Pro

Claude is AI and can make mistakes.

Opus 5.5 Medium Auto

- Same App Registration
- Different User
- No Entra Admin Role

Export the results to an Excel file (.xlsx), with one row per finding.

I'll pull your Conditional Access policies from the tenant, analyze them for redundancy, overly broad scope and empty scope, and build the Excel file.

Used MCP-Server-For-Enterprise, updated tasks, 2 failed >

The tenant connection works, but it doesn't have access to Conditional Access: both the v1.0 and beta reads of `/identity/conditionalAccess/policies` came back **403, not authorized by the available scopes**. The MCP Server for Enterprise client hasn't been granted `Policy.Read.All`, so I haven't pulled any policy data and haven't built the file. I won't produce findings without the actual policy set.

You can unblock this in one of two ways:

1. **Grant the scope to the MCP client.** Add delegated `Policy.Read.All` to the MCP Server for Enterprise client's permissions and admin-consent it. For readable findings I also need to resolve the object IDs in includes and excludes into names. That requires `GroupMember.Read.All` or `Directory.Read.All` for users, groups and roles, and `Application.Read.All` for apps. Once those scopes are live, ask again here and I'll run the whole analysis directly against the tenant.

2. **Attach an export.** For example, run `Get-MgIdentityConditionalAccessPolicy -All | ConvertTo-Json -Depth 10 > ca.json` and attach the file. If you also want named locations evaluated, add `Get-MgIdentityConditionalAccessNamedLocation`. With an export I can do the full analysis. The limitation is that unresolved group and app GUIDs will show up as IDs, and I can't check whether a scoped group is actually empty, unless you include a group member count.

Reply



Progress

×

- Pull CA policies and resolve referenced objects
- Analyze for redundancy, broad scope, empty scope
- Build and verify Excel findings file

Used in this session

- 🗑️ Connectors
- MCP-Server-For-Enterprise

# Summary: Which Tool for Which Job?

---



Agent Builder  
(M365 Copilot)

Knowledge-based assistance using your own content and documentation



Security Copilot

Security investigations, risk analysis and specialized agents



MCP Server for  
Enterprise

Interactive analysis of live Entra ID data with your preferred AI client



Deterministic  
approach

Reliable, repeatable changes. AI recommends, deterministic tools execute



## [Microsoft Learn](#)

<https://learn.microsoft.com/de-de/microsoft-365/copilot/extendability/agent-builder>

<https://github.com/microsoft/EnterpriseMCP/blob/main/README.md>

[Use Microsoft Entra groups to manage role assignments](#)

[Create an access review of Azure resource and Microsoft Entra roles in PIM](#)



## [Best Practices & Community & Local LLMs](#)

[Merill Fernando – Lokka](#)

[LMStudio](#)

[Ollama](#)



## [NothingButCloud Blog](#)

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

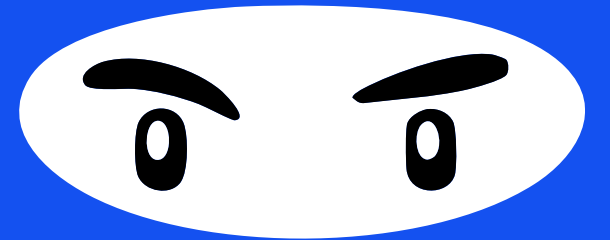
[KlaBier Github: CreateSecCopilotSCU PowerShell](#)

[The dilemma with unused objects in Azure AD](#)

**Thank You,  
Ninjas!**



See you  
next Year!



Backup slides

# Deterministic vs. AI: Its Not a Competition

| Criteria                        | Deterministic (PowerShell, KQL, workbooks)                                             | AI (Security Copilot, MCP + LLM)                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Consistency</b>              | Same logic produces reproducible results, assuming the underlying data hasn't changed. | Not guaranteed. Results, interpretations and wording may vary between runs.                       |
| <b>Discovery &amp; Coverage</b> | Finds what you explicitly query or have defined in your detection logic.               | Can identify unexpected patterns and relationships. Naming mismatch e.g.                          |
| <b>Time to first answer</b>     | Existing scripts results quickly. New scenarios may require development                | Often seconds, using natural language                                                             |
| <b>Explains findings</b>        | Predefined logic; interpretation often manual                                          | Can explain findings, provide context, highlight risks and suggest next steps.                    |
| <b>Completeness at scale</b>    | Systematic queries, pagination required                                                | May miss objects or details due to context limits, incomplete retrieval or tool limitations.      |
| <b>How it fails</b>             | Errors may be visible, but incorrect logic can produce misleading results.             | Can produce plausible, confident answers that are incomplete or simply wrong.                     |
| <b>Flexibility</b>              | New questions often require modifying queries, scripts or detection rules.             | Follow-up questions allow investigations to evolve without rewriting queries manually.            |
| <b>Best for</b>                 | Recurring checks, evidence, automation                                                 | Exploration, identifying potential risks, investigations and understanding complex relationships. |