

NIC **REBEL**  
**EDITION**



MVP Security (Identity & Access)  
LinkedIn | GitHub | Bluesky | X |  
@JanVidarElven

## Jan Vidar Elven

License to Assist - Bringing AI Agents to Entra ID

# Security Copilot in Microsoft Entra



- **Security Copilot Experiences**

- Standalone
- Embedded

- **Entra Scenarios**

- Entra ID
- Entra ID Protection
- Entra ID Governance
- Entra Internet Access & Private Access

- **Entra Agents**

- Conditional Access optimization agent
- Access Review agent (Preview)

## Requirements

Secure Compute Unit (SCU) & Azure Subscription.  
Entra Suite | Entra ID Premium | Entra ID Governance

Entra Agent  
demo

Conditional Access  
Optimization

Access Review  
Assistant



Provisioned units used

1 of 1 unit

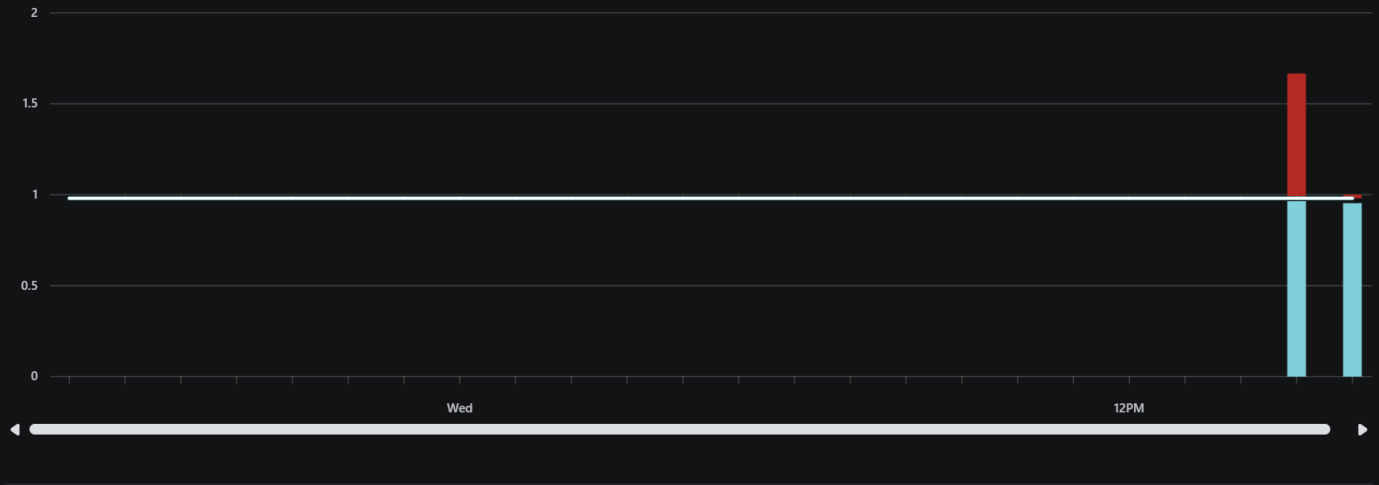
in the last hour

Workspace using this capacity

default

[Manage workspaces](#)

Date: Last 24 hours ▾

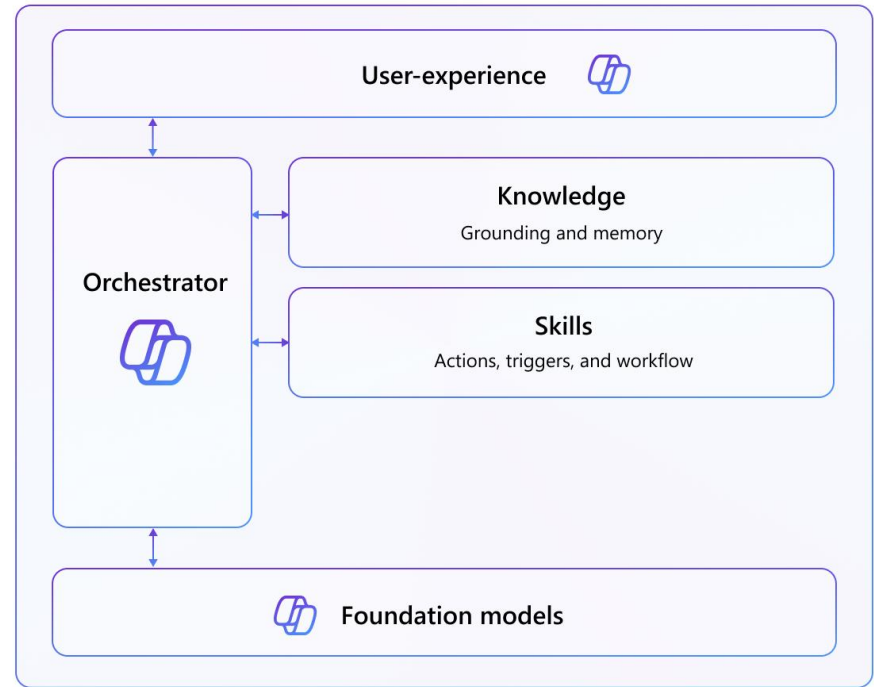


Session ID	Date ▾	Units used <sup>①</sup>	Initiated by	Category	Type	Copilot experience	Plugins used
07f99d5c-f8fd-4c1f-b8fd-3a5d2d3ab6a0	Oct 29, 04:11 PM	2.3	Jan Vidar Elven	User prompt	Manual	Unknown	
07f99d5c-f8fd-4c1f-b8fd-3a5d2d3ab6a0	Oct 29, 04:11 PM	0.3	Jan Vidar Elven	User prompt	Manual	Unknown	
07f99d5c-f8fd-4c1f-b8fd-3a5d2d3ab6a0	Oct 29, 04:10 PM	0.2	Jan Vidar Elven	User prompt	Manual	Unknown	

# Declarative Agents

- Customized versions of Microsoft 365 Copilot
- Build with
  - Agents Toolkit
  - Copilot Studio Full
  - Copilot Studio Lite
  - SharePoint

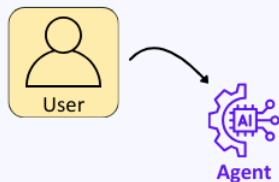
Anatomy of  
Declarative agent



# Transformation of AI Agents

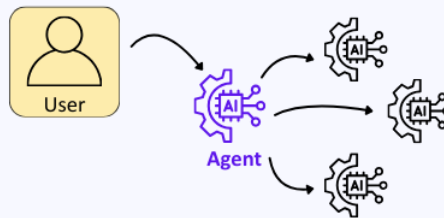
## Interactive agent

Single, specific, repetitive, defined task



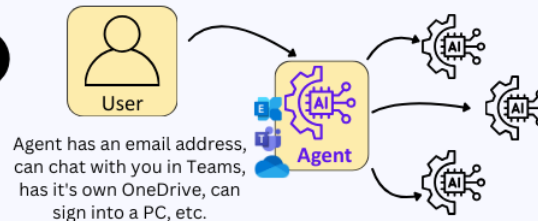
## Autonomous agent

Complex, goal oriented, creates plans to achieve outcome



## Digital employee

Learning driven, emulate human decision making



# Agents should have their own Identity



User ID



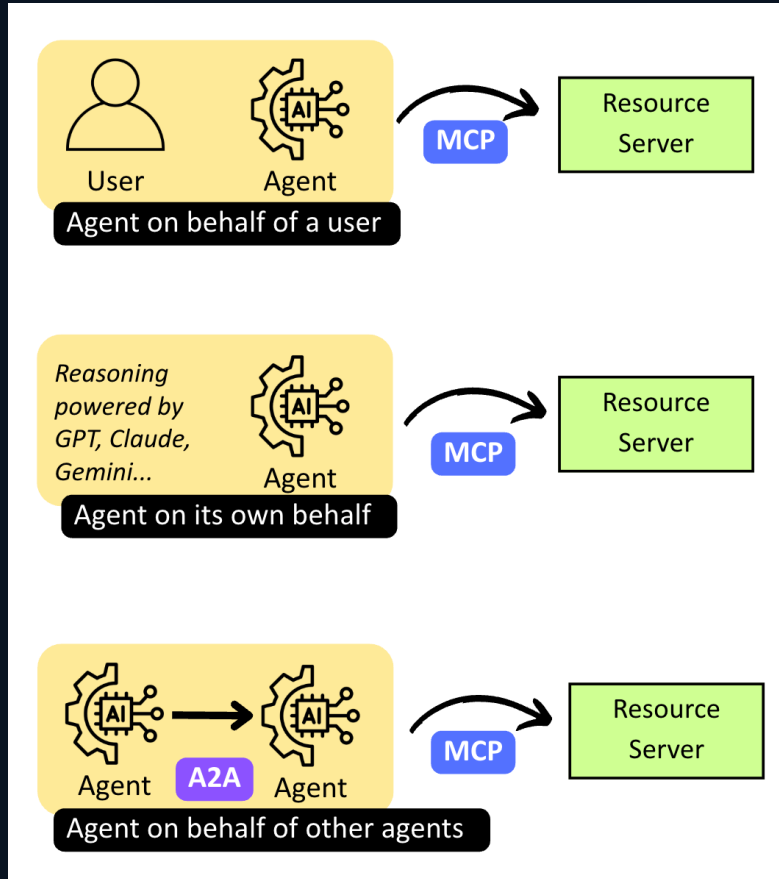
Client ID



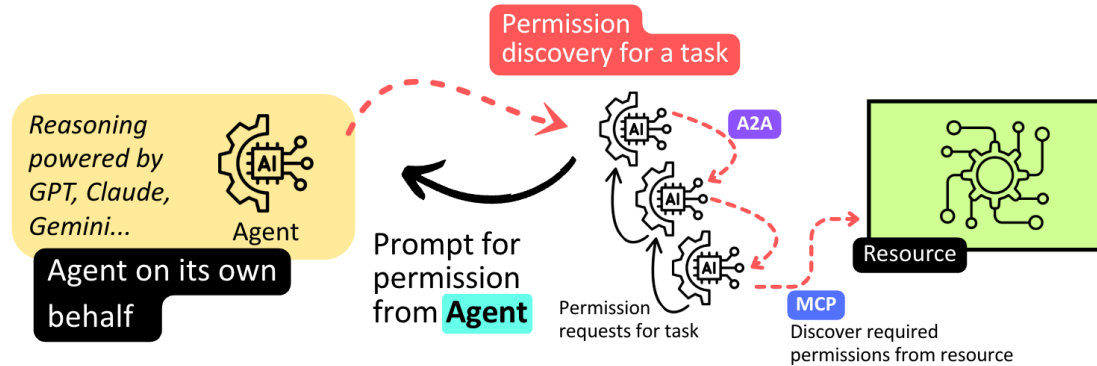
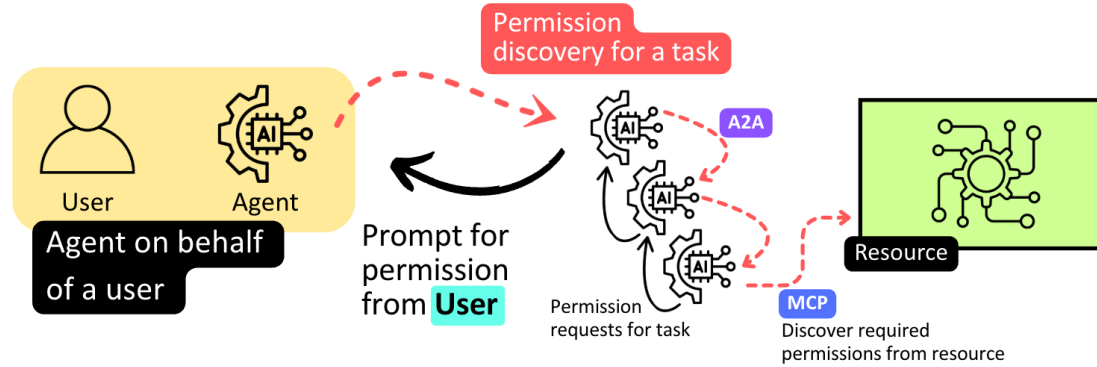
Agent ID



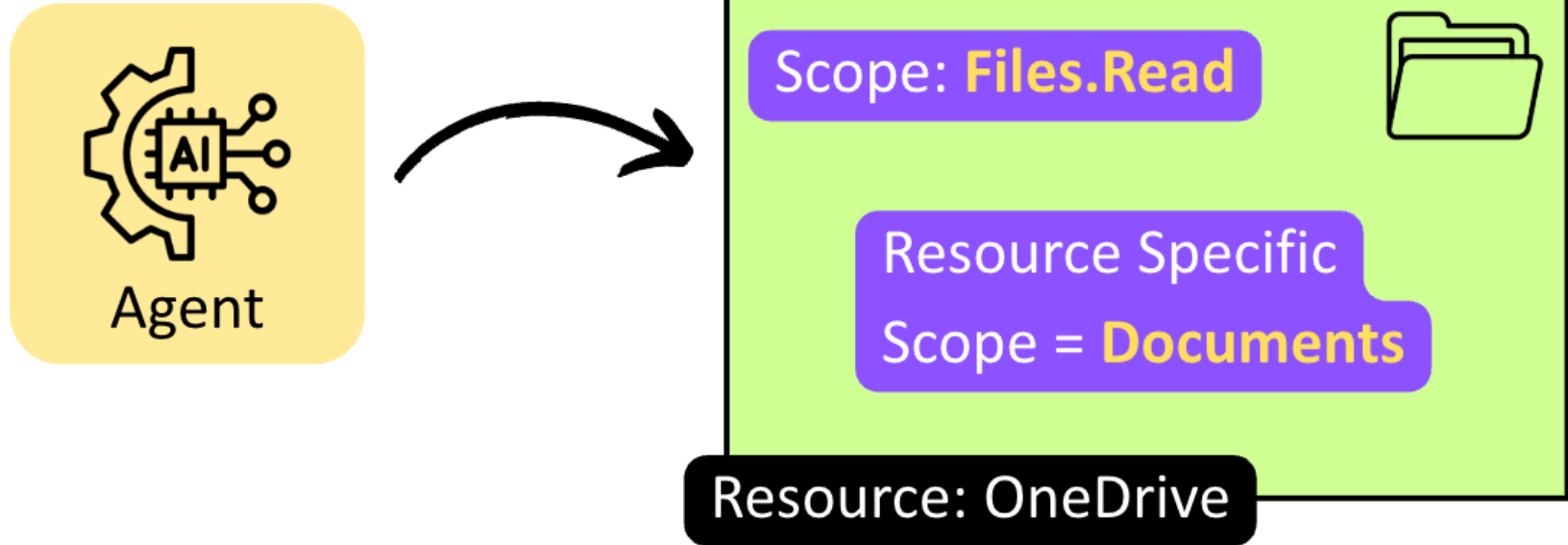
# Transparent and Traceable Agent Actions



# Permission discovery and delegation



# Fine-grained, resource specific, least-privilege access



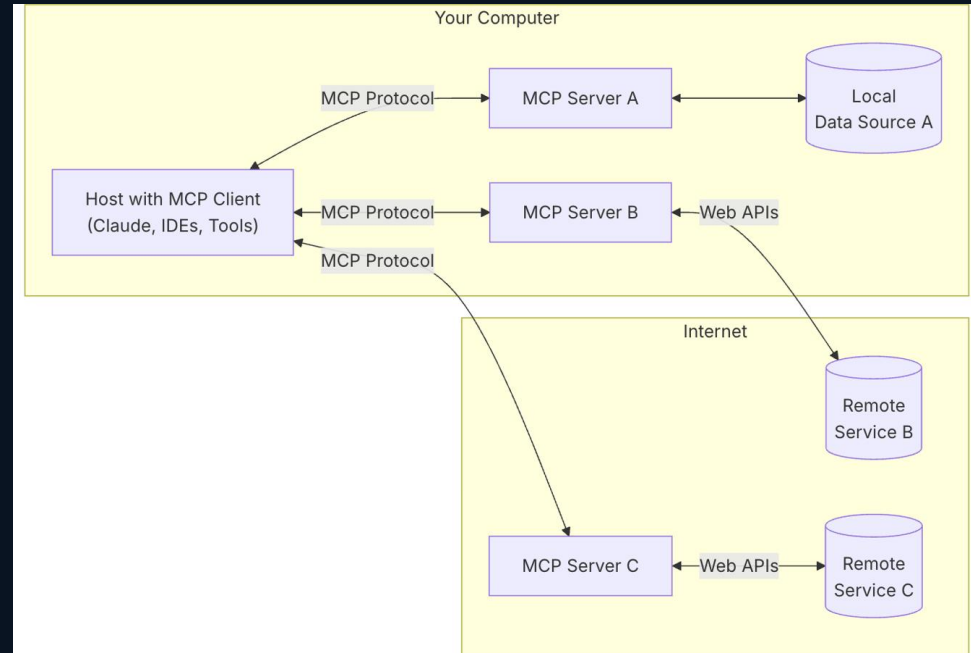
Declarative  
Agent demo

Microsoft Graph API  
Own Custom APIs

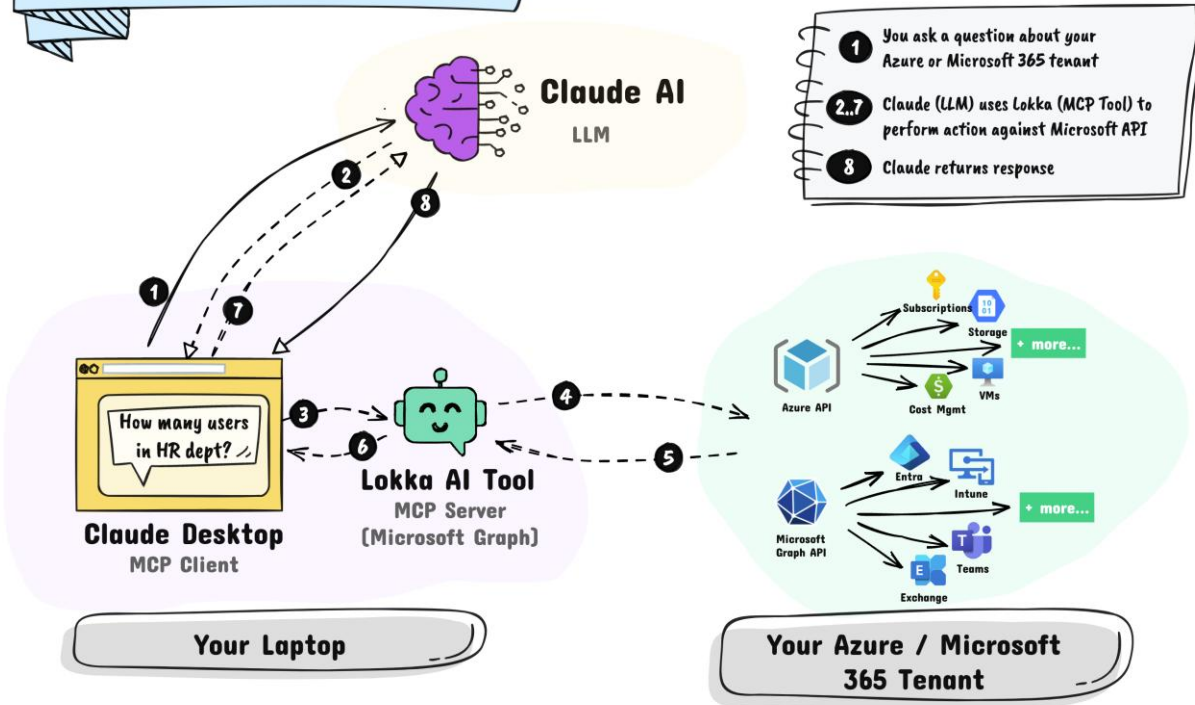


# MCP

- “USB-C” standard for your AI tools



## How does Lokka work?



# MCP Demo

lokka.dev



# Agent ID Monitoring & Insights in Microsoft Entra



- Portal
  - Application Type filter
- Sign-In Logs
  - Is Agent
  - Agent Type
- Microsoft Graph API

```
{  
  "@odata.type":  
    "#microsoft.graph.agentic.agentSignIn",  
  "agentType": "String",  
  "parentAppId": "String"  
}
```



# Agent ID Governance Demo

[entra.microsoft.com](https://entra.microsoft.com)



# Thank you!

## Questions?

You can reach me at

- @JanVidarElven
- <https://github.com/janvidarelven/entra-agents-demos>

