



# Build Your Own AI Assistant for Microsoft Intune

*Niels Kok & Stefan Dingemanse*

# Sponsors



# Niels Kok

---

- Sysadmin/Consultant -> DevOps Engineer
- Microsoft MVP – Intune + Azure Virtual Desktop
- Freelance



# Niels Kok

---

- Sysadmin/Consultant -> DevOps Engineer
- Microsoft MVP – Intune + Azure Virtual Desktop
- Freelance





**BRAINPULSE IT**  
CONSULTANCY & TRAINING

# Stefan Dingemanse

Microsoft Cloud Consultant & Architect



Microsoft MVP · AVD / Windows 365 · MCT



Dordrecht, Netherlands · Brainpulse IT



Co-Founder AVD Community & Dutch VDI User Group



Hybrid Athlete - Running & Weightlifting



# Quick show of hands



**Who uses a personal AI  
subscription?**

ChatGPT · Claude · Perplexity · Gemini




**Who uses Microsoft Security  
Copilot?**

In production right now

# What we're covering today

01 |  Microsoft Security Copilot in Intune

---

02 |  The challenges


---

03 |  Our solution, two approaches

---

04 |  Live demos

---

05 |  Takeaways & how to get started



SECTION 1

# Microsoft Security Copilot for Intune

# Two ways to access Security Copilot



## Embedded in Intune

**Copilot button** - context-aware in the admin center.

Compliance summary, root cause & remediation next to any device.

**Explorer tab** - guided natural-language queries, pre-built by Microsoft.



## Standalone portal

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

Full free-form chat across all connected Microsoft security products.

Intune · Defender · Entra · Purview - all in one prompt session.

# Copilot summarizing a policy in Intune

The screenshot displays the Microsoft Intune admin center interface. The main content area shows the configuration for the policy "BL-WIN-SC-Bitlocker-V1.2". A Copilot chat window is open on the right, summarizing the policy settings.

**Microsoft Intune admin center**

Home > Devices | Configuration

## BL-WIN-SC-Bitlocker-V1.2

Device configuration profile

Summarize with Copilot Delete

### Device and user check-in status

Succeeded: 6 | Error: 0 | Conflict: 0 | Not applicable: 0 | In Progress: 0

[View report](#)

[Device assignment status](#)  
This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

[Per setting status](#)  
View the configuration status of each setting for this policy across all devices and users.

### Properties

**Basics** [Edit](#)

Name	BL-WIN-SC-Bitlocker-V1.2
Description	Deze policy heeft een update qua Bitlocker settings. Hierdoor is de extra endpoint protection policy niet meer nodig.
Platform	Windows

**Assignments** [Edit](#)

**Included groups**

### Copilot

Summarize this policy

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

The policy "BL-WIN-SC-Bitlocker-V1.2" is a Windows 10 device configuration policy focused on enforcing BitLocker encryption and related security controls. Below is a detailed summary of its settings and assignment scope, as requested.

**Policy Settings Summary:**

- Prevent installation of devices using drivers that match specified device setup classes** is enabled, blocking installation or updates of device drivers for listed device setup class GUIDs. This setting takes precedence over others and also applies to already installed matching devices, enhancing device control and reducing the risk of unauthorized hardware.
- BitLocker Drive Encryption Method and Cipher Strength** is set to XTS-AES 256-bit for fixed, operating system, and removable drives, which is a stronger encryption standard than the Windows default (XTS-AES 128-bit).
- BitLocker Recovery Options for Fixed Drives** are configured to allow a 256-bit recovery key, allow a 48-digit recovery password, enable data recovery agents, and back up both recovery passwords and key packages to Active Directory. The setup wizard omits recovery options, enforcing policy-driven recovery.
- Enforce Drive Encryption Type on Fixed Data Drives** is enabled, requiring "Used Space Only" encryption, which encrypts only the used portion of the drive.
- Allow Devices Compliant with InstantGo or HSTI to Opt Out of Pre-Boot PIN** is disabled, ensuring pre-boot authentication is enforced where possible.
- Allow Enhanced PINs for Startup** is enabled, permitting complex PINs for BitLocker startup, increasing security.
- BitLocker Recovery Options for OS Drives** require a 48-digit recovery password, do not allow 256-bit recovery keys, do not allow data recovery agents, and require recovery information to

Start typing to choose a prompt.




BUILT-IN CAPABILITIES

# Pre-built prompts across Intune, Defender & Entra

Prompts to try

Q | Prompts | Promptbooks | Role | Plugin

<p><b>Application assignments</b></p> <p>What groups is <code>Appname</code> assigned to?</p> <p>Microsoft Intune</p>	<p><b>Cloud architecture guidance</b></p> <p>List best practices for implementing zero trust architecture in the cloud.</p> <p>Microsoft Documentation</p>	<p><b>Common cloud config issues</b></p> <p>List common cloud security misconfigurations and how to avoid them.</p> <p>Microsoft Documentation</p>	<p><b>Critical Sentinel incidents</b></p> <p>What are the critical Sentinel incidents right now?</p> <p>Microsoft Sentinel</p>
<p><b>Defender incident summary</b></p> <p>Provide a summary of Defender incident <code>Incident ID</code>.</p> <p>Incident Analysis</p>	<p><b>Device comparison</b></p> <p>Compare this device with another device.</p> <p>Microsoft Intune</p>	<p><b>Device group memberships</b></p> <p>What groups is <code>device name</code> a member of?</p> <p>Microsoft Intune</p>	<p><b>Failed user log-ins</b></p> <p>How many failed sign-ins occurred for <code>UPN</code> in the last 48 hours and tell me the reasons.</p> <p>Microsoft Entra</p>
<p><b>High severity Defender incidents</b></p> <p>What are the high severity Defender incidents right now?</p> <p>Microsoft Defender XDR</p>	<p><b>Identity management guidance</b></p> <p>List best practices for identity and access management in Azure.</p> <p>Microsoft Documentation</p>	<p><b>Identity policy creation</b></p> <p>Help me create an identity policy for <code>criteria</code>.</p> <p>Microsoft Documentation</p>	<p><b>Incidents by workspace</b></p> <p>List the last 5 incidents from Sentinel workspace <code>Workspace name</code>.</p> <p>Microsoft Sentinel</p>
<p><b>Incidents related to CVE</b></p> <p>Check Defender for vulnerabilities related to <code>CVE ID</code>.</p> <p>Microsoft Threat Intelligence</p>	<p><b>Managed apps by device</b></p> <p>Tell me about managed apps on <code>device name</code>.</p> <p>Microsoft Intune</p>	<p><b>Prioritize Data Loss alerts</b></p> <p>Which data loss prevention alerts should I start to work on first?</p> <p>Microsoft Purview</p>	<p><b>Prioritize threats</b></p> <p>Which threats should I focus on based upon their exposure scores?</p> <p>Microsoft Threat Intelligence</p>

How can Security Copilot help?   

# What Security Copilot can do in Intune



## Explore settings

Use Copilot to learn more about individual settings and recommended values.

*"What does the BitLocker encryption setting do?"*



## Summarize policies

Use Copilot to summarize an existing device configuration policy.

*"Summarize this compliance policy"*



## Generate KQL queries

Use Copilot to create KQL queries to get device details.

*"Show me non-compliant devices in EMEA"*

# Built-in agents

Change Review Agent

Device Offboarding Agent

Policy Configuration Agent

Vulnerability Remediation Agent

## Change Review Agent



The *Change Review Agent* evaluates the effect of approval requests in Intune and makes recommendations for the actions you can take.

[Learn more](#)

## Device Offboarding Agent



The *Device Offboarding Agent* identifies stale or misaligned devices across Intune and Microsoft Entra ID, providing actionable insights and requiring admin approval before offboarding any devices.

[Learn more](#)

## Policy Configuration Agent



With the *Policy Configuration Agent*, you import documents or write instructions in plain language. The agent uses this information to find matching settings in the Intune settings catalog and recommends values for these settings. You can then use the agent to create a policy with those settings and their values.

[Learn more](#)

## Vulnerability Remediation Agent



The *Vulnerability Remediation Agent* uses Defender data to monitor vulnerabilities and prioritize remediation with AI-driven risk assessments.

[Learn more](#)

*All agents require admin approval before acting*



SECTION 2

# The problem

# The cost reality of Security Copilot

~\$2,920

per month

at minimum (1 SCU × \$4/hr × 730 hrs)

- **Billed 24/7** whether you use it or not, provisioned capacity runs continuously
- **M365 E5 auto-activation** you may already be billed without knowingly enabling it
- **Overage at \$6/SCU** enabled by default, surprises happen fast with agents running
- **No usage = no refund** provisioned capacity billed regardless of prompt count

# Costs of Copilot (True cost of AI?)

At just 1 provisioned SCU, the estimated cost is \$2,920/month (\$4 × 730 hours) - before a single prompt is sent. Add overage, embed it across your team, and costs scale fast with no warning.

## Select the number of units

Security compute units are billed per hour and are needed for Security Copilot to work across your Microsoft Security products. There are two kinds: provisioned and overage. [Help me decide](#)

Provisioned security compute units per hour \*  
**\$ 4 USD** per unit

Estimated monthly cost 2920 USD/month

Note: your monthly bill may vary based on 1. overage SCUs consumed, 2. changes to provisioned SCUs during the billing period

Use overage units when needed  
\$ 6 USD per unit

### How overage units work

Overage units will be used after you've run out of provisioned units. You'll only pay for the overage units that you use.

### Number of on-demand units

- No limit
- Set a max-limit

I acknowledge that I have read, understood, and agree to the [Terms and Conditions](#)

# What did I actually do with this?

Microsoft Security Copilot / My sessions nkocopilot

Home  
Agents  
Promptbooks  
Build Preview

History ^

- Summarize this policy
- Embedded Copilot Session - ...
- Embedded Copilot Session - ...
- 816feba2-1536-4a6e-9388-2...
- All history**

Owner ^

- Owner settings
- Plugin settings
- Role assignment
- Manage workspaces
- Usage monitoring

Security Store

## My sessions + New session

🔍 | All Recent 🔍

🗑️ Delete

<input type="checkbox"/>	Name	Last updated	Created
<input type="checkbox"/>	Summarize this policy	3:41 PM	3:41 PM
<input type="checkbox"/>	Embedded Copilot Session - 546ef992-292c-463d-aec6-e672b15f1dd0	Saturday 10:08 AM	Saturday 10:08 AM
<input type="checkbox"/>	Embedded Copilot Session - 4c672520-cc29-41c9-95d8-b6e8be3c7665	Friday 11:31 AM	Friday 11:31 AM
<input type="checkbox"/>	816feba2-1536-4a6e-9388-21a8d27b69a6-ondemand-5bab9490-fe9c-4e09-90aa-e7d51c565cec	2/18/2026, 2:54 PM	2/18/2026, 2:54 PM
<input type="checkbox"/>	816feba2-1536-4a6e-9388-21a8d27b69a6-ondemand-c0183dea-209c-4fa2-ae89-b11617e9dd37	2/18/2026, 2:49 PM	2/18/2026, 2:49 PM
<input type="checkbox"/>	Embedded Copilot Session - 58d275f0-b481-4436-9751-b9f572203006	2/18/2026, 2:43 PM	2/18/2026, 2:43 PM

# 1 SCU - estimated cost: \$2,920/month (1 × \$4 × 730 hours)

Home > Microsoft Security compute capacities > NKOLAB

Microsoft Secur... << <img alt="Microsoft logo icon" data-bbox="240 185 255 200"/>  
NielsKok.Tech - LAB (7141k.onmicrosoft.com)

+ Create <img alt="Gear icon" data-bbox="150 250 165 265"/> Manage view <img alt="Dropdown arrow" data-bbox="210 250 225 265"/> ...

- Name ↑
- <img alt="Refresh icon" data-bbox="135 345 150 360"/> NKOLAB

Showing 1 - 1 of 1. Display <input type="text" value="20"/> <img alt="Dropdown arrow" data-bbox="230 870 245 885"/>  
count:

**NKOLAB | Update Security Compute Units** ☆ ...  
Microsoft Security compute capacity

Search <input type="text" value="Search"/>

### Update Security Compute Units

Select the number of units you want to purchase for NKOLAB. Security compute units provide the computing power that drives the Copilot experience. (USD \$4 per provisioned unit, USD \$6 per overage unit)  
Note: your monthly bill may vary based on 1. overage SCUs consumed, 2. changes to provisioned SCUs during the billing period.  
[Learn more about Security Compute Units](#)

Provisioned security compute units per hour (min. 1) \* <input type="text" value="1"/>  
**Estimated monthly cost \$2920/month**

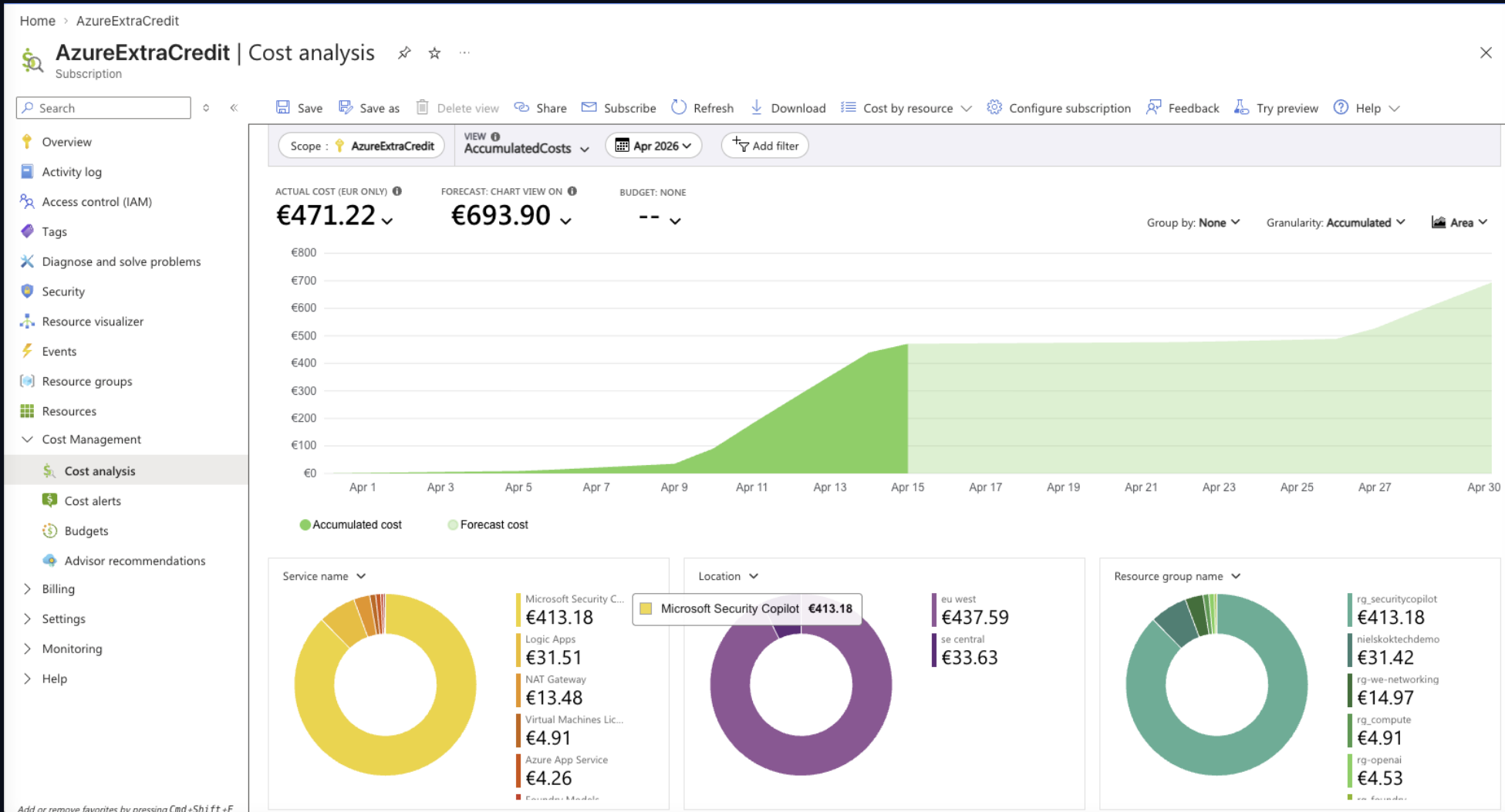
Overage Capacity Setup <input checked="" type="checkbox"/> Enable Overage Capacity

- Overview
- Activity log
- Access control (IAM)
- Resource visualizer
- Settings
  - Properties
  - Locks
- Update
  - Update Security Compute Units**
  - Automation
  - Help

Ok

Add or remove favorites by pressing Cmd+Shift+F

# What did it cost



## LIMITATIONS

# It's good. But it's closed.

- ✗ Predefined prompt templates, limited flexibility
- ✗ 4 built-in agents only
- ✗ UI-only: no API, no automation, no bulk operations
- ✗ No integration (ServiceNow, ITSM, custom logic)
- ✗ SCU model, cost scales unpredictably
- ✗ Government cloud: not available
- ✗ You don't own the logic, Microsoft does

# Can we replicate those scenarios?

- **Not rebuilding Security Copilot** replicating some Intune scenarios with our own stack
  - **Target scenarios** policy summarization, compliance queries, conflict detection, •
- Success criteria** same quality output, your data, your infrastructure, predictable cost



SECTION 3

# Our DIY Solution

# Before we built: two different bets

	Niels	Stefan
Data	Static export (file storage + JSON)	Live Graph API
Tool layer	Foundry AI + Logic Apps + MCP	Foundry AI + Azure Functions
Monthly cost	~\$40	~\$15-22
Freshness	Point-in-time snapshot	Always live
Complexity	Low	High

# Static data vs live data



## File Storage (Niels)

- Point-in-time export
- Export pipeline needed
- Re-export when policies change



## Graph API (Stefan)

- Real-time, always current
- App Registration and functions

# What we wanted it to do



## List all policies

Name, type, and assignment for all 12 Intune policy types



## Policy details

Full settings, values, and scope for any individual policy



## Summarize

Plain-English explanation of what a policy does and why



## Compliance status

Device compliance summary across the tenant



## Conflict detection

Cross-policy conflict analysis with source profiles



## CIS benchmark

Gap analysis against CIS Level 1/2 for Windows endpoints

# The feature we're replicating

**In Security Copilot for Intune: select a policy → "Summarize this policy"**

Returns a plain-English explanation of what the policy does, what settings are configured, and what the impact is on users and devices.

**Our goal:** Same output. Your infrastructure. Your data. ~\$15–40/month instead of ~\$2,920.



APPROACH 1

# Static data with Logic Apps

# Approach 1 - Static data with Logic Apps



## Azure AI Foundry

GPT-4.1 agent + system prompt



## Logic Apps

MCP server exposing tools to agent



## Azure File Storage

Pre-exported Intune JSON / CSV



# Azure Subscription

Microsoft Foundry



Microsoft Foundry

Logic App + API Connection



Logic App + API Connection



Storage Account



Storage Account



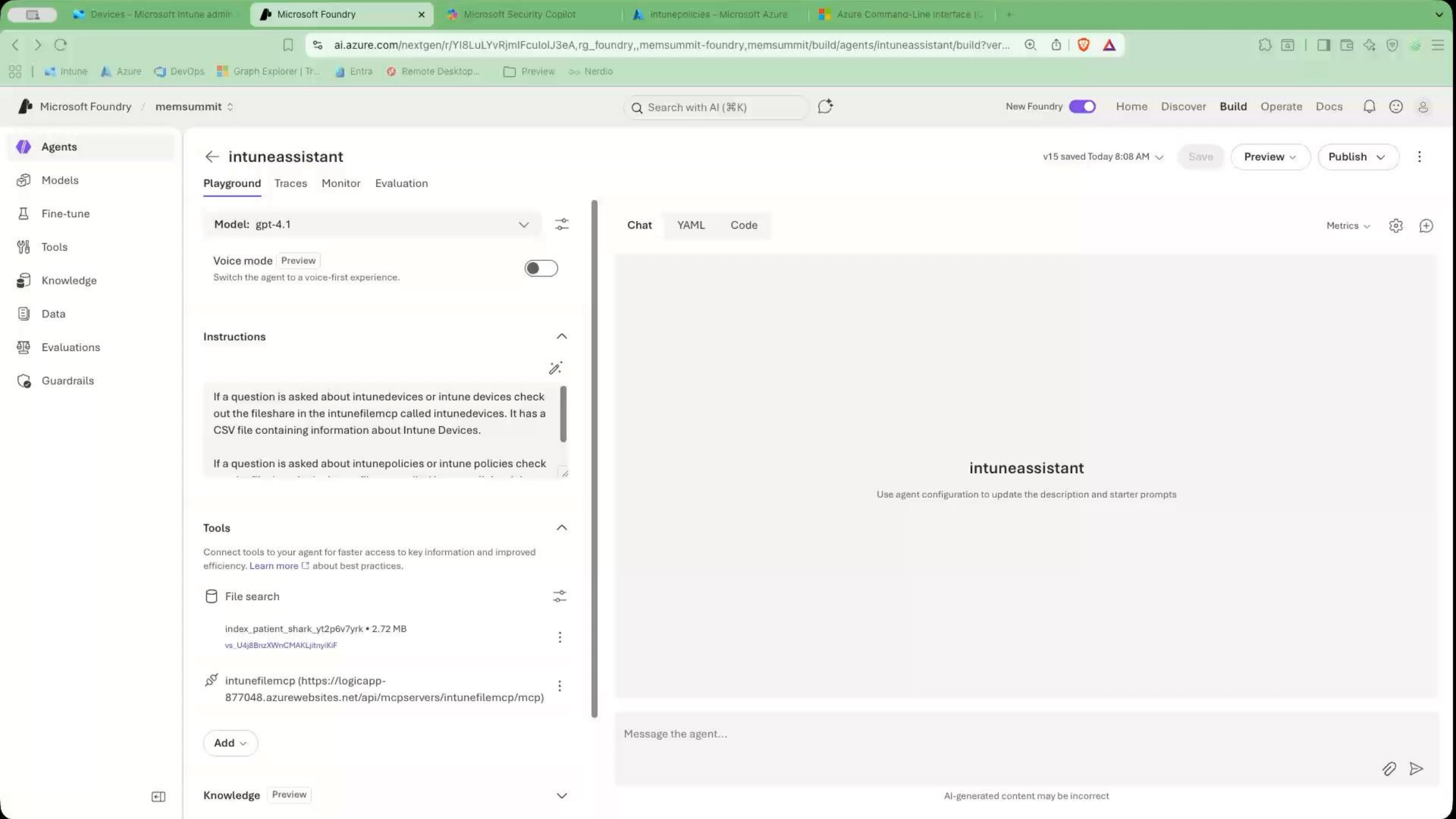
Container:  
Managed Devices



Container:  
Intune Policies

# Demo - Microsoft Foundry (static data)

- Describe Microsoft Intune with 5 words
- Demo agent with Intune files and policies
- Agent 1 (Niels): Blob Storage via Logic Apps MCP



## ← intuneassistant

v15 saved Today 8:08 AM

Save

Preview

Publish

Playground Traces Monitor Evaluation

Model: gpt-4.1

Voice mode Preview  Switch the agent to a voice-first experience.

Instructions

If a question is asked about intunedevices or intune devices check out the fileshare in the intunefilemcp called intunedevices. It has a CSV file containing information about Intune Devices.

If a question is asked about intunepolicies or intune policies check

Tools

Connect tools to your agent for faster access to key information and improved efficiency. Learn more about best practices.

File search

index\_patient\_shark\_yt2p6v7yrk • 2.72 MB vs\_U4j8BnzXWnCMaKJjtnyKiF

intunefilemcp (https://logicapp-877048.azurewebsites.net/api/mcpservers/intunefilemcp/mcp)

Add

Knowledge Preview

Chat YAML Code

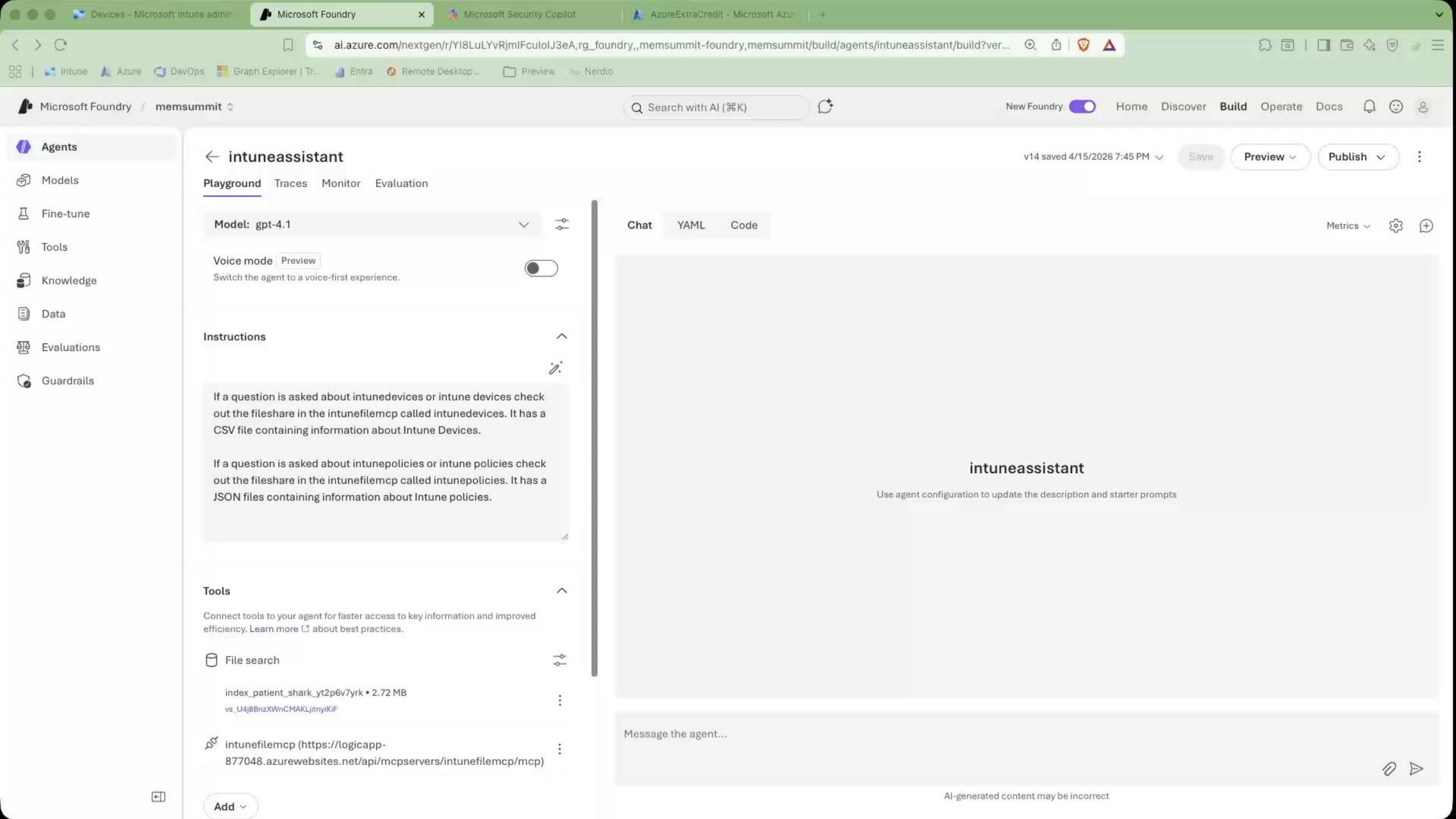
Metrics

### intuneassistant

Use agent configuration to update the description and starter prompts

Message the agent...

AI-generated content may be incorrect



## ← intuneassistant

v14 saved 4/15/2026 7:45 PM

Save

Preview

Publish

Playground Traces Monitor Evaluation

Model: gpt-4.1

Voice mode Preview  Switch the agent to a voice-first experience.

### Instructions

If a question is asked about intunedevices or intune devices check out the fileshare in the intunefilemcp called intunedevices. It has a CSV file containing information about Intune Devices.

If a question is asked about intunepolicies or intune policies check out the fileshare in the intunefilemcp called intunepolicies. It has a JSON files containing information about Intune policies.

### Tools

Connect tools to your agent for faster access to key information and improved efficiency. Learn more about best practices.

File search

index\_patient\_shark\_yt2p6v7yrk • 2.72 MB vs\_U4j8BnzXWnCMAKLjityiKiF

intunefilemcp (https://logicapp-877048.azurewebsites.net/api/mcpservers/intunefilemcp/mcp)

Add

Chat YAML Code

Metrics

## intuneassistant

Use agent configuration to update the description and starter prompts

Message the agent...

AI-generated content may be incorrect

```
PS /Users/nko/VSCoDeWorkspaces/NK0> 1..20 | ForEach-Object {
  /Users/nko/codex/scripts/Invoke-FoundryResponse.ps1 `
    -Endpoint 'https://memsummit-foundry.services.ai.azure.com/api/projects/memsummit' `
    -AccessToken $bearerToken `
    -AgentName "intuneassistant" `
    -AgentVersion "13" `
    -Prompt 'Describe Microsoft Intune in 5 words'
}
```

```
Cloud-based mobile device management.
Cloud-based mobile device management platform.
Cloud-based mobile device management.
Cloud-based unified device management platform.
Cloud-based device management and security.
Cloud-based mobile device management.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based unified endpoint management solution.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Device management and security platform.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based mobile device management platform.
Cloud-based endpoint management and security.
```

```
PS /Users/nko/VSCoDeWorkspaces/NK0>
PS /Users/nko/VSCoDeWorkspaces/NK0> 1..20 | ForEach-Object {
  /Users/nko/codex/scripts/Invoke-FoundryResponse.ps1 `
    -Endpoint 'https://memsummit-foundry.services.ai.azure.com/api/projects/memsummit' `
    -AccessToken $bearerToken `
    -AgentName "intuneassistant" `
    -AgentVersion "14" `
    -Prompt 'Describe Microsoft Intune in 5 words'
}
```

```
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
Cloud-based device management and security.
```

```
PS /Users/nko/VSCoDeWorkspaces/NK0>
```

# Security Copilot - Knowledge

The screenshot displays the Security Copilot Knowledge management interface. On the left is a navigation sidebar with options like Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Home' and features a card for 'Policy Configuration Agent (Preview)'. A red box highlights this card, which contains a message: 'Agent run failed. The agent encountered an error and did not finish the run. T'. Below this message are buttons for '+ Create New', 'Refresh', and 'Remove Agent'. The 'Knowledge' tab is selected, showing a search bar and 'Add filters' button. A table with columns 'Name', 'Status', and 'Created time' is visible but empty. On the right, a 'Create new knowledge source' dialog is open. It has a close button (X) in the top right. The 'Knowledge Source name' field contains 'CISBenchmark'. The 'Description' field contains 'Document with CIS benchmark Windows 11 4.0.0'. Under the 'Upload document' section, there is a note: 'Only .txt files up to 25 KB are supported. Uploading in this format allows the agent to access its content and provide organization-specific answers. Uploaded docs will automatically be assessed for their impact on the agent.' A file upload area shows a preview of a file named 'CIS\_Microsoft\_Intune\_for\_Windows\_11\_Benchmark\_v4.0.0.pr' with a 'Browse for files' button. A red box highlights this area, which also contains an error message: 'File is too large. Maximum file size is 25KB.' Below this, there are 'Examples documents to upload' listed as bullet points: 'Documents describing device configuration requirements', 'Compliance frameworks or standards describing settings', 'Change management or risk assessment guidelines for device configuration', and 'Best practice documents for device configuration'. At the bottom right of the dialog are 'Cancel' and 'Review' buttons.

Home

Policy Configuration Agent (Preview) ...

Agent run failed. The agent encountered an error and did not finish the run. T

+ Create New Refresh Remove Agent

Overview Knowledge Suggestions Settings

Search Add filters

Name	Status	Created time ↓
------	--------	----------------

Kn

### Create new knowledge source

Knowledge Source name \*

CISBenchmark

Description

Document with CIS benchmark Windows 11 4.0.0

Upload document ⓘ

Only .txt files up to 25 KB are supported. Uploading in this format allows the agent to access its content and provide organization-specific answers. Uploaded docs will automatically be assessed for their impact on the agent.

CIS\_Microsoft\_Intune\_for\_Windows\_11\_Benchmark\_v4.0.0.pr

Browse for files

File is too large. Maximum file size is 25KB.

#### Examples documents to upload

- Documents describing device configuration requirements
- Compliance frameworks or standards describing settings
- Change management or risk assessment guidelines for device configuration
- Best practice documents for device configuration

Cancel Review

Blog

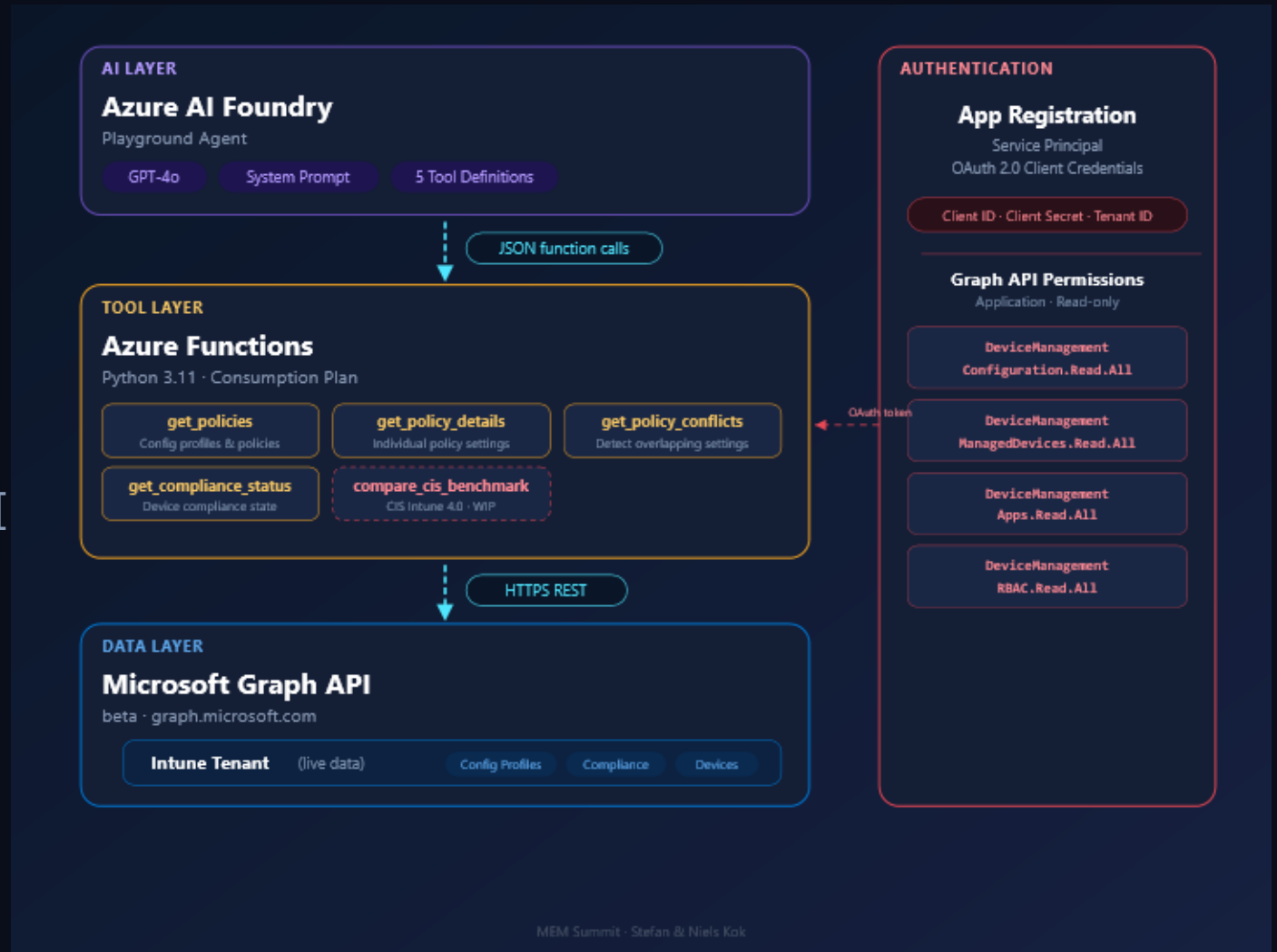




APPROACH 2

# Live data with Azure Functions

# Approach 2 - Architecture



# Approach 2 - Live data with Azure Functions



## Azure AI Foundry Playground

GPT-4o + System Prompt + Tool Definitions (5 tools)

↓ JSON function calls



## Azure Functions (Python)

get\_policies() | get\_policy\_details() | get\_compliance\_status()  
compare\_cis\_benchmark() | get\_policy\_conflicts()





↓ JSON function calls / HTTPS REST, OAuth 2.0



## Microsoft Graph API

v1.0 + beta → Your Intune Tenant (live data)  
HTTPS REST, OAuth 2.0

# What I wanted the agent to do

 <code>get_policies()</code>	Lists all Intune policy types
 <code>get_policy_details()</code>	Full settings + assignments for one policy
 <code>get_compliance_status()</code>	Device compliance summary across tenant
<code>get_policy_conflicts()</code>	Cross-policy conflict detection
 <code>compare_cis_benchmark()</code>	Gap analysis vs CIS 4.0

*Adding a 6th tool = one new Python function + registering it in the OpenAPI spec*

# Prompts to try

> List all settings catalog policies in this tenant

> Summarize this policy: BL-WIN-SC-Bitlocker-V1.1

> Compare this policy BL-WIN-SC-Bitlocker-V1.1 with CIS Level 1

# Real monthly costs from Azure Cost Management

rg-bps-foundry		Sweden Central	rg-intune-assistant		EU West
stefan-foundry	Cognitive Services	€6.96	intune-func	Function App	<€0.01
GPT-4.1 tokens · text-embedding-3 · Input & Output			intunestor	Storage Account	€0.01
			intune-law	Log Analytics	€0.02
<b>Subtotal</b>		<b>€6.96 / month</b>	<b>Subtotal</b>		<b>€0.02 / month</b>

## AI Foundry Usage (last 30 days)

<b>2.1M</b> Total Tokens	<b>64</b> Agent Runs	<b>42</b> Completed
-----------------------------	-------------------------	------------------------

**TOTAL MONTHLY COST** ~€7 / month



SECTION 5

# Takeaways & how to get started

# One thing you need to know



**Azure AI Foundry agents with tools: NOT available in West Europe**

Use Sweden Central or East US, this is the most common deployment mistake

# Take Aways

- ✓ You don't need Microsoft's full stack to build AI on your own Intune data

---

- ✓ Azure AI Foundry + Graph API = full control, predictable cost (~\$15–40/month vs ~\$2,920)

---

- ✓ Start with one use case, just start small

# How to get started

- 1. Create an Azure AI Foundry**  
Deploy in Sweden Central or East US (not West Europe)

---

- 2. Connect to your Intune data**  
Export policies to file storage (quick start) or wire up Graph API (live data)

---

- 3. Build one agent with a system prompt**  
Start with policy summarization, easiest win, most visible to colleagues

---

- 4. Tune temperature and Top-P**  
0.2–0.4 for factual queries; higher for summaries and explanations

---

- 5. Learn Python**  
AI leans on Python

# Remove Security Copilot



Notes from the field, even if you don't use it, it will cost money

- **Billing starts on creation** provisioned capacity bills the moment it is created, even before your first prompt
- **How to deprovision** Azure Portal → Security Copilot capacity → delete the resource
- **Monitor weekly** Azure Cost Management → set a budget alert immediately

# Costs - Security Copilot vs DIY

~\$2,920

Security Copilot / month

1 SCU minimum, 24/7

~\$40

Approach 1 / month

Niels - Blob + Logic Apps

~\$15-22

Approach 2 / month

Stefan - Graph API + Functions

QUESTIONS

# Questions?

Feel free to ask anything

Niels LinkedIn



Stefan LinkedIn



# Sponsors

