
# Intune AI - Is it really worth it?

*Joery Van den Bosch*

*Jose Schenardie*

# Sponsors


onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

robopack

numecent

Microsoft

eido

Rimo3

## Joery Van den Bosch

**Microsoft MVP · Endpoint & Security**

### Role

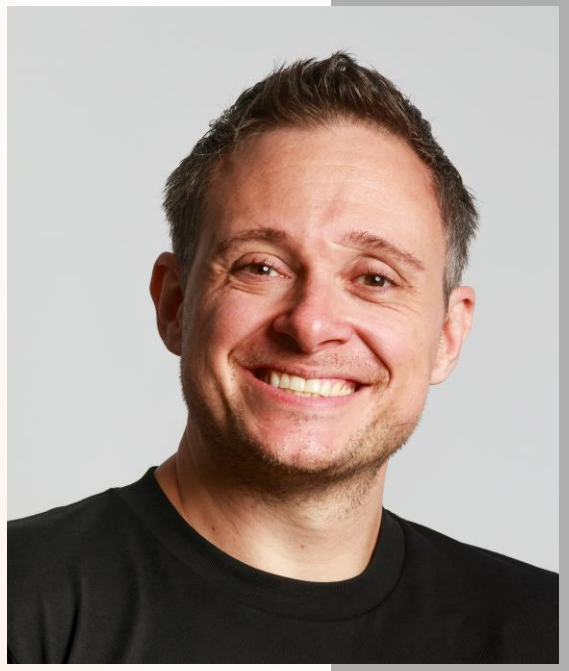
Modern Workplace Architect

### Focus

Intune · Security Copilot

### Blog

https://intunestuff.com/



**Jose Schenardie**
Microsoft MVP · Endpoint & Security

**Role**
CTO - Devicie

**Focus**
Intune · R&D · AI

**Blog**
https://msendpointmgr.com
https://intune.tech

# Agenda


- What? Why? How much?
- Intune Agents
- Security Copilot in Intune
- Intune Explorer
- Security Copilot Standalone
- Costs
- Is it really worth it?


# What? Why? How Much?

# What?


- AI capabilities built into Microsoft Intune that help admins manage devices, policies, and apps faster, using natural language instead of clicking through menus or writing queries.
- Embedded in the Intune Portal
- Security Copilot Standalone
- Agents

# Why?


- Save admin time
- Faster troubleshooting
- Lower skill barrier e.g. no KQL required for queries
- Fewer misconfigurations
- Stronger security posture

# How Much?


- Security Copilot required - SCU-based billing
- Entry point ~$2,920 / month (1 SCU, 24/7)
- Some agent may require extra licenses
- Consumption scales with usage - monitor SCU burn
- ROI: admin hours saved vs. monthly spend


# Intune Agents

# Four agents currently


- Change Review Agent
- Device Offboarding Agent - Deprecated
- Policy Configuration Agent
- Vulnerability Remediation Agent

# Change Review Agent


This agent evaluates the effect of approval requests in Intune and makes recommendations for the actions you can take.

# Change Review Agent Use Case


- Third-party script review. MSP or consultant submits a script, agent flags risks before approval
- Catching destructive commands. E.g. Remove-Item on system paths, registry wipes, mass-uninstalls flagged as high risk
- Junior admin submissions, senior reviewer gets an AI second opinion with context
- Understanding unfamiliar scripts, agent summarizes what the script actually does
- Insider-threat mitigation, adds a review layer before a script hits production devices

# How does it work?


- Reviews policy changes before they're applied
- Analyzes impact: affected devices, users, groups
- Flags conflicts with existing scripts
- Summarizes the change in plain English
- Recommends proceed, adjust, or roll back

# What doesn't work (yet)


- Only PowerShell scripts on Windows via Multi-Admin Approval
- No config, compliance, or app policies (yet)
- No device actions wipe, retire, sync, etc.
- Max 10 requests per run, manual trigger only no scheduling
- Public preview, public cloud only  not for gov clouds
- Not retroactive

The agent evaluates the effect of approval requests in Intune and makes recommendations for the actions you can take. Learn more

## Wipe Device

Not applied | Generated on 10/03/2026, 2:06:15 pm

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

### Suggested action: Reject

The script is designed to perform a remote device wipe using privileged WMI operations, which is a highly destructive and sensitive action. While the script's intent is clearly documented, the actions involve issuing wipe commands that could result in irreversible data loss if misused. The metrics require explicit checks and reversibility for destructive actions, but the supporting evidence does not indicate the presence of such safeguards. Other validation points do not show explicit violations, but the high-risk nature of the script content and insufficient compensating controls necessitate rejection.

The script is designed to issue a remote wipe command using the Windows Management Instrumentation (WMI) framework. It targets the `MDM_RemoteWipe` class within the `root\cimv2\mdm\dmmap` namespace and invokes the `doWipeMethod` method. This action is intended to remotely wipe a device, which is a critical operation often used in device management scenarios.

**Factors:**

- Script Purpose: The script performs a remote wipe, a highly destructive action. Metrics require explicit checks and reversibility for such actions, but the evidence does not show safeguards or reversibility. The script's purpose is legitimate for device management, but the risk is high and controls are insufficient.
- Approval/Rejection History: No prior security-risk rejections or concerning history found, so criteria are met.
- Business Justification: The justification provided is vague and does not address necessity, scope, controls, traceability, or privacy. Metrics are not satisfied due to lack of actionable business context.
- Requestor Risk Indicators: No risk indicators or recent high-risk events for the requestor; criteria are met.
- Alert History (Script): No details available for this factor. Agent couldn't retrieve any supporting data.

1 Change review agent | 2 Entra user risk summarization | +2 more

View request


approve

owerShell script ...

Script settings | Scope tags | 4 Review + submit for approval

fore this resource can be created, it must be approved by another admin. Before you can submit this request, you must enter ur business justification.

Wipe Device

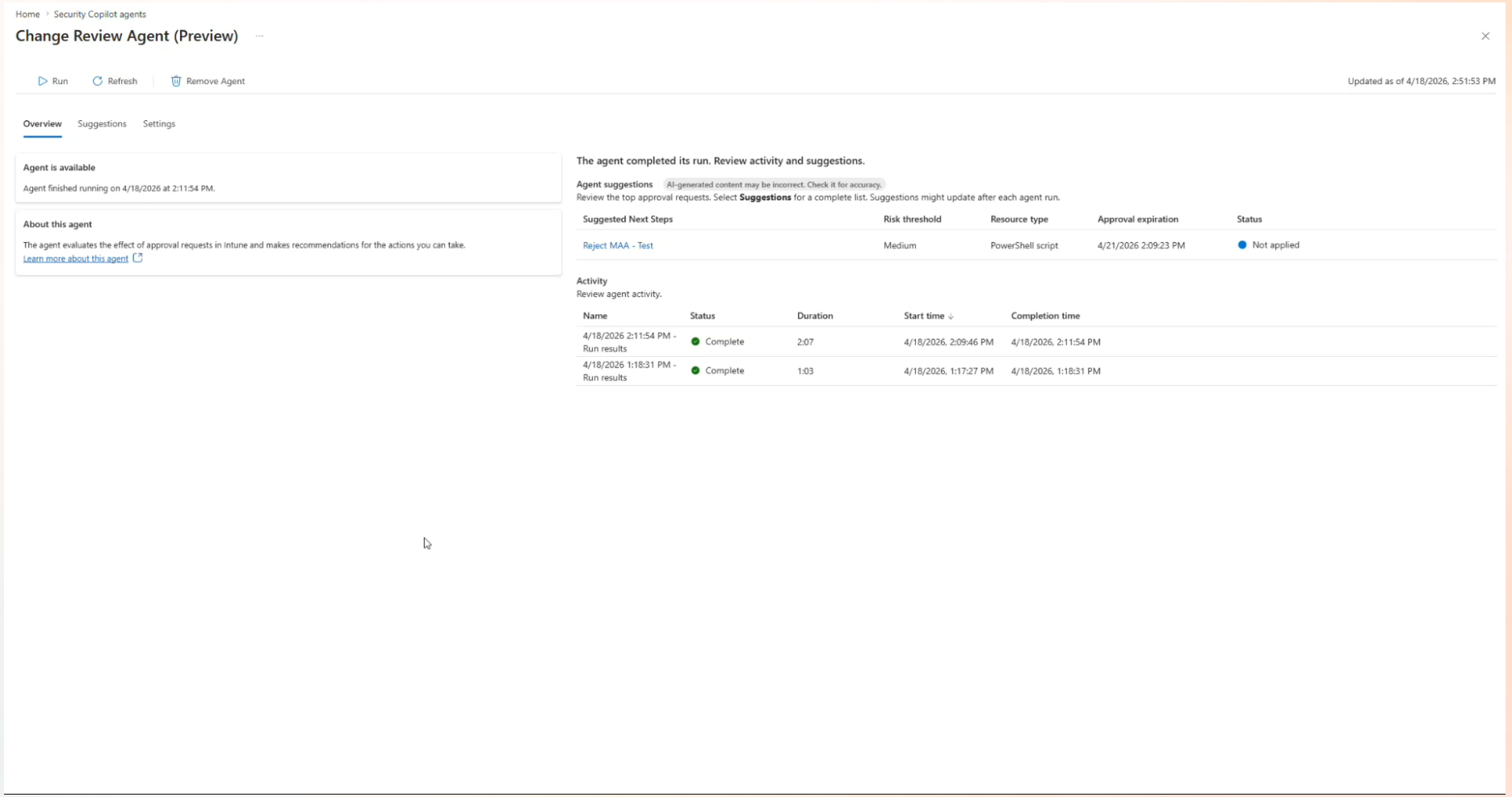
No Description

ttings

| Approval expiration | Status |
|---|---|
| 13/03/2026 2:05:10 pm | Not applied |

Previous | Submit for approval

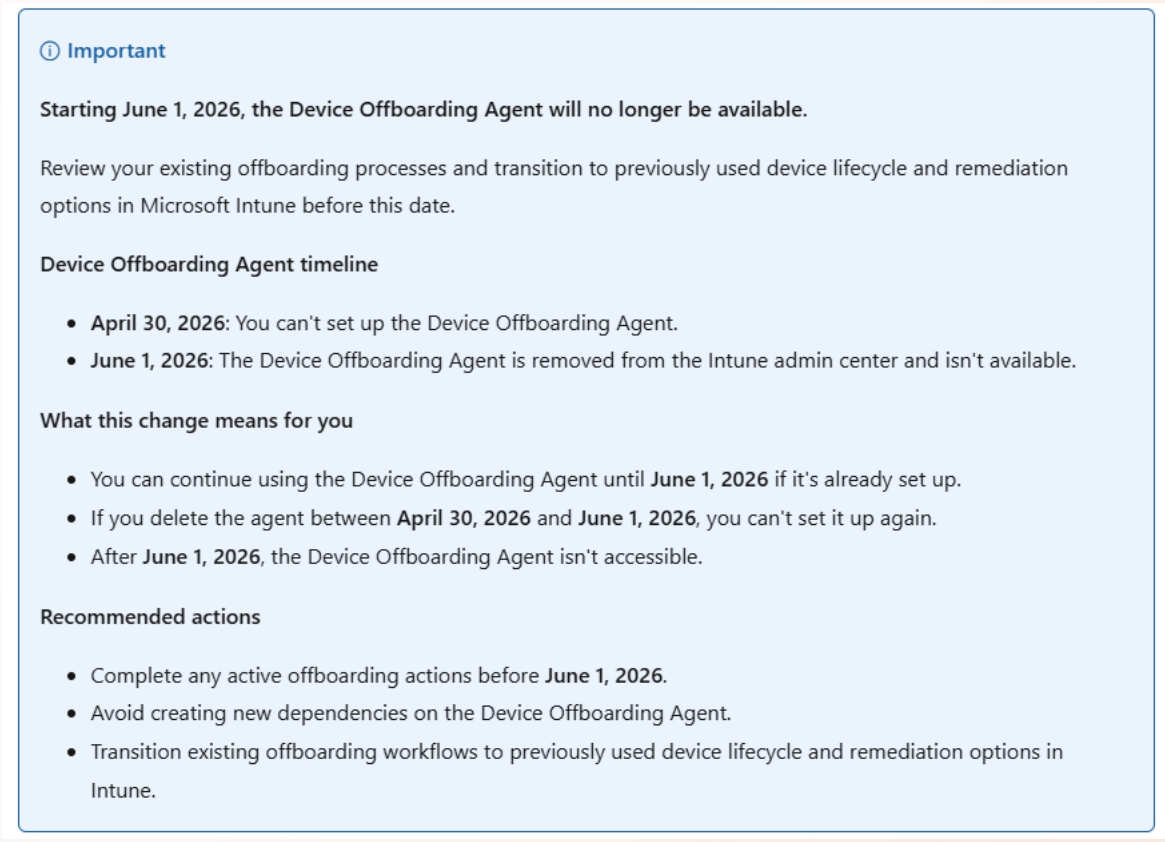
# Demo


Home › Security Copilot agents
Change Review Agent (Preview)
Run
Refresh
Remove Agent
Updated as of 4/18/2026, 2:51:53 PM
Overview
Suggestions
Settings
Agent is available
Agent finished running on 4/18/2026 at 2:11:54 PM.
About this agent
The agent evaluates the effect of approval requests in Intune and makes recommendations for the actions you can take.
Learn more about this agent
The agent completed its run. Review activity and suggestions.
Agent suggestions
AI-generated content may be incorrect. Check it for accuracy.
Review the top approval requests. Select Suggestions for a complete list. Suggestions might update after each agent run.
Suggested Next Steps
Risk threshold
Resource type
Approval expiration
Status
Reject MAA - Test
Medium
PowerShell script
4/21/2026 2:09:23 PM
Not applied
Activity
Review agent activity.
Name
Status
Duration
Start time
Completion time
4/18/2026 2:11:54 PM - Run results
Complete
2:07
4/18/2026, 2:09:46 PM
4/18/2026, 2:11:54 PM
4/18/2026 1:18:31 PM - Run results
Complete
1:03
4/18/2026, 1:17:27 PM
4/18/2026, 1:18:31 PM

# Device Offboarding Agent


The Device Offboarding Agent can find devices that were removed from Intune, but might linger in Microsoft Entra. It provides steps to properly remove them from Entra.

# Device Offboarding Agent

ⓘ Important

**Starting June 1, 2026, the Device Offboarding Agent will no longer be available.**

Review your existing offboarding processes and transition to previously used device lifecycle and remediation options in Microsoft Intune before this date.

**Device Offboarding Agent timeline**

- **April 30, 2026**: You can't set up the Device Offboarding Agent.
- **June 1, 2026**: The Device Offboarding Agent is removed from the Intune admin center and isn't available.

**What this change means for you**

- You can continue using the Device Offboarding Agent until **June 1, 2026** if it's already set up.
- If you delete the agent between **April 30, 2026** and **June 1, 2026**, you can't set it up again.
- After **June 1, 2026**, the Device Offboarding Agent isn't accessible.

**Recommended actions**

- Complete any active offboarding actions before **June 1, 2026**.
- Avoid creating new dependencies on the Device Offboarding Agent.
- Transition existing offboarding workflows to previously used device lifecycle and remediation options in Intune.

https://learn.microsoft.com/en-us/intune/copilot/agents/device-offboarding-agent

# How it works?


- Enable Agent
- Run agent
- Follow tasks to remove devices

# How doesn’t it work?


**Device platform requirements**

The agent supports devices managed by Intune across multiple platforms, including Windows, iOS/iPadOS, macOS, Android, and Linux.
It applies to both corporate-owned and BYOD (bring-your-own-device) scenarios.

The agent doesn't support:

- Hybrid Entra-joined Windows devices
- Windows Autopilot devices
- Shared devices
- Microsoft Teams Phones

# Policy Configuration Agent


The Policy Configuration Agent turns your command or written security baselines like STIGs, CIS, or your own requirement docs into Intune Settings Catalog policies. It maps each requirement to the matching setting so you don't have to build the policy by hand.

# Policy Configuration Use Case


- New regulatory baseline, turn a fresh CIS or NIST release into an Intune policy draft in minutes
- Government / defense tenants, map STIG requirements to Settings Catalog without hand-mapping
- Custom internal hardening doc, upload your security team's Word/PDF baseline and generate a draft
- Client onboarding (MSPs) quickly stand up baseline policies aligned to the customer's framework
- Audit prep, prove baseline coverage by generating policies directly from the audit framework

# How does it work?


- Upload a baseline document (STIG, CIS, custom) - up to 25 KB
- Create your own query to have the agent create your policy
- Agent maps requirements to Intune Settings Catalog
- Review draft with rationale per setting
- Agent creates a Settings Catalog configuration profile
- Admin assigns, scope-tags, and deploys as normal

# What works well?

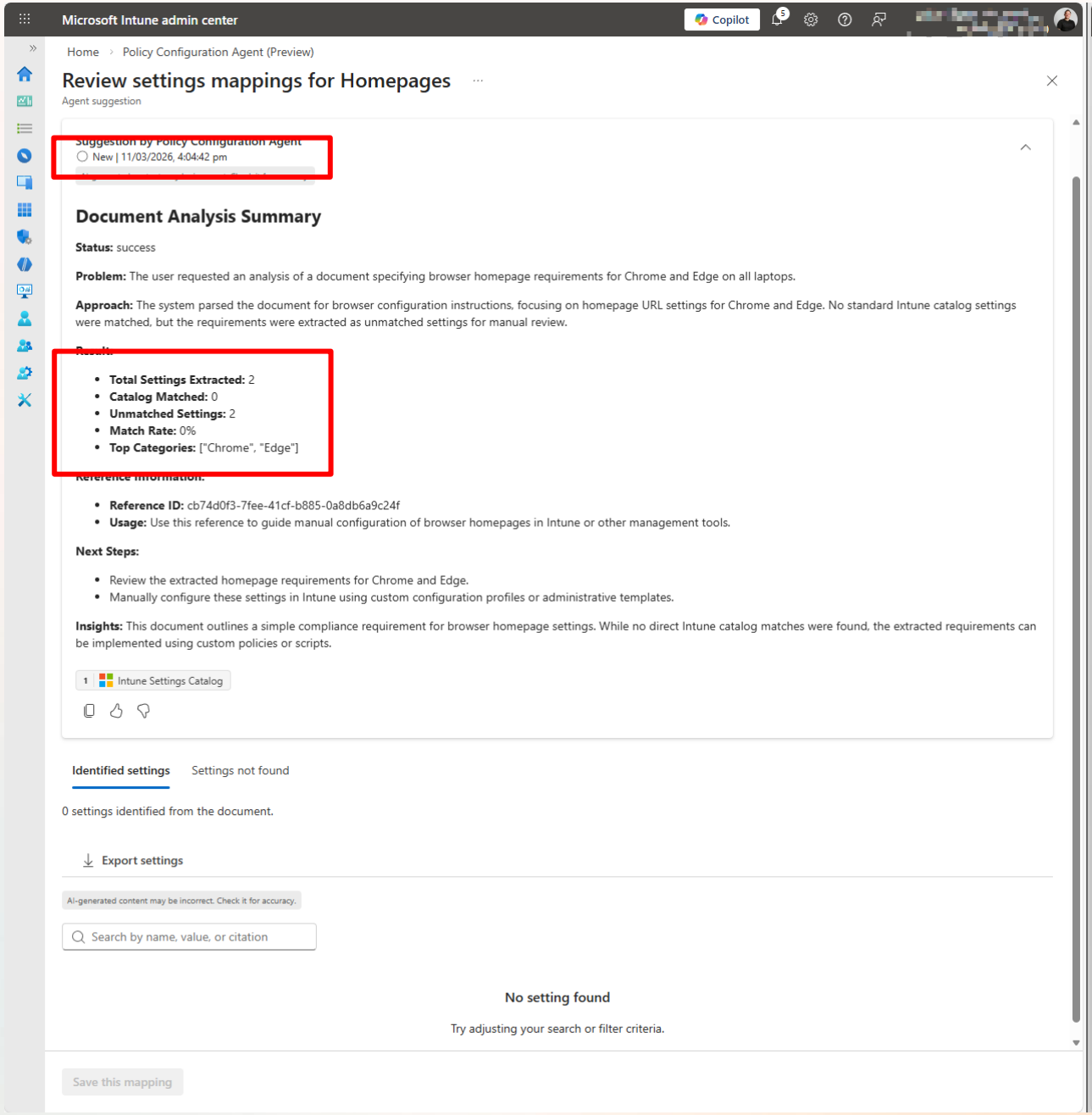

- Turns written compliance into policy drafts in minutes
- Handles known baselines - STIG, CIS, NIST
- Shows reasoning per setting - not a black box
- Lowers the skill barrier for baseline hardening
- Natural-language prompts also supported

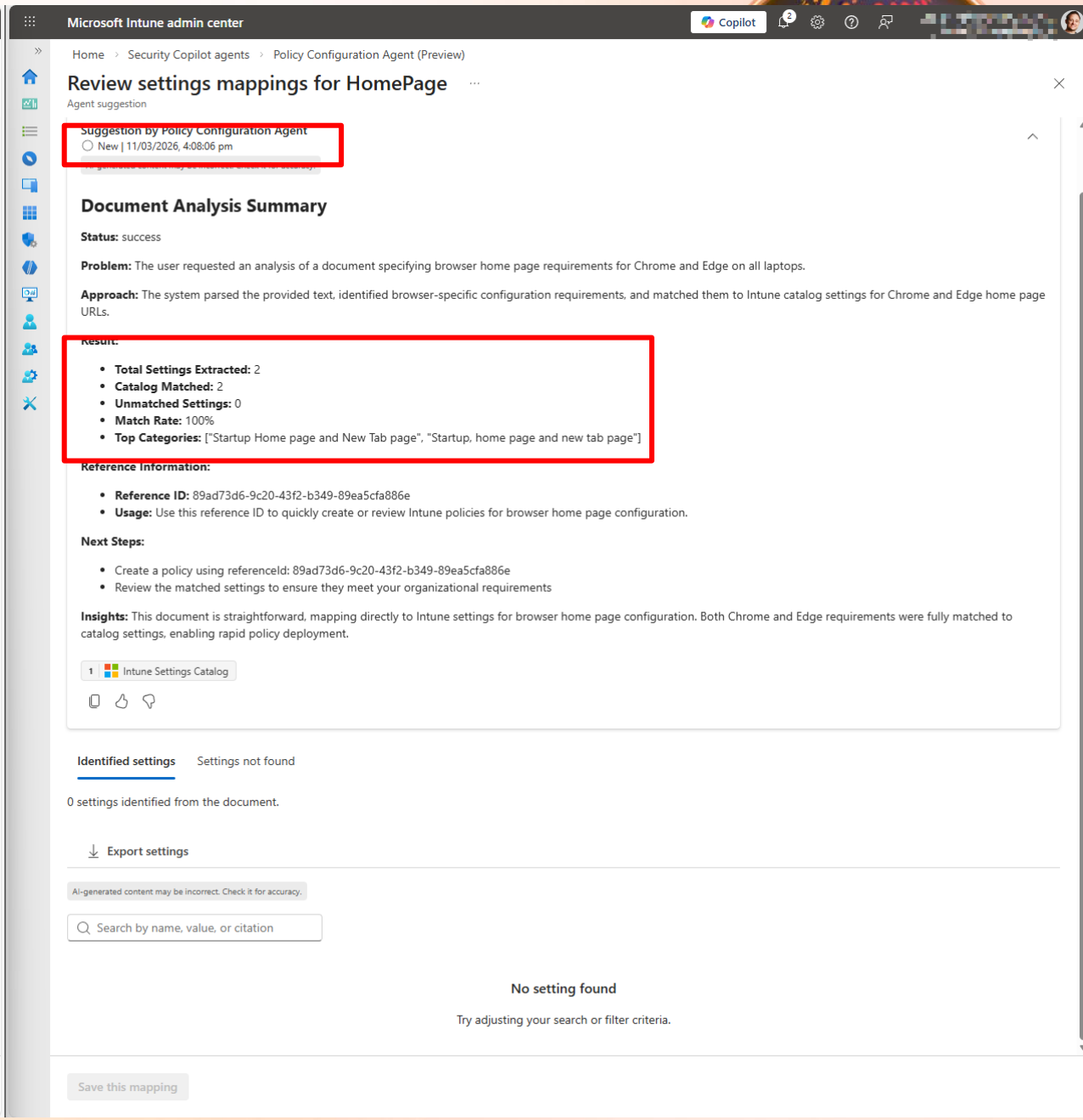
# What doesn't work (yet)?


- Settings Catalog only - no Templates, Compliance, App Protection, or Endpoint Security
- One document per run, 25 KB max
- Not every requirement maps - unsupported items must be handled manually
- Manual trigger only - no scheduling
- Public preview, public cloud only - not for gov clouds
- Every run burns SCU

# Demo

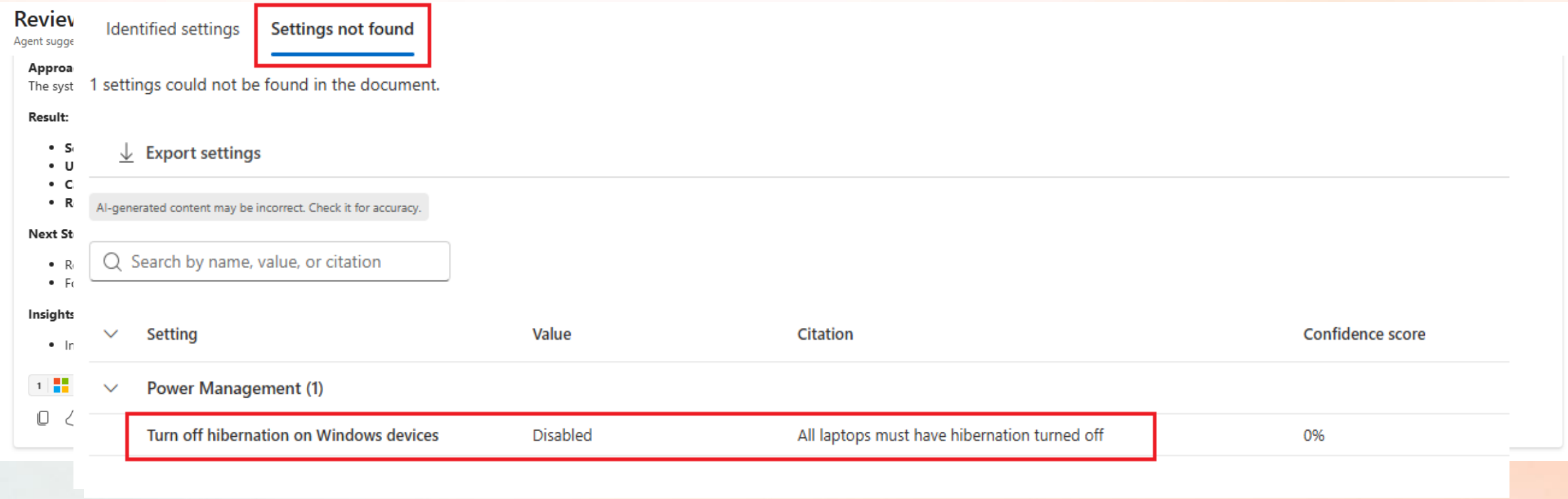

Home
Policy Configuration Agent (Preview)
Create New
Refresh
Remove Agent
Updated as of 4/18/2026, 3:06:42 PM
Overview
Knowledge
Suggestions
Settings
Agent is available
About this agent
Import a document or write instructions in plain language. The agent will match those instructions to the Settings Catalog and help create a policy. Policy Configuration Agent currently supports policy for Windows devices only. Support for additional platforms will be introduced in future updates. Learn more about this agent
Agent suggestions
AI-generated content may be incorrect. Check it for accuracy.
Based on the information you provided, the agent suggests the new policies listed here. Select a policy or knowledge source to review its details. You can then make edits if needed, and then go on to deploy the policy or save the knowledge source when you're ready.
Suggested next steps
Suggestion type
Status
Last updated
No agent suggestions yet
To see suggestions, the agent will need to complete a run. This should take a few minutes.
Activity
Review agent activity.
Name
Status
Duration
Start time
Completion time


Microsoft Intune admin center
Copilot
Home
Policy Configuration Agent (Preview)
Review settings mappings for Homepages
Agent suggestion
Suggestion by Policy Configuration Agent
New | 11/03/2026, 4:04:42 pm
Document Analysis Summary
Status: success
Problem: The user requested an analysis of a document specifying browser homepage requirements for Chrome and Edge on all laptops.
Approach: The system parsed the document for browser configuration instructions, focusing on homepage URL settings for Chrome and Edge. No standard Intune catalog settings were matched, but the requirements were extracted as unmatched settings for manual review.
Result:
Total Settings Extracted: 2
Catalog Matched: 0
Unmatched Settings: 2
Match Rate: 0%
Top Categories: ["Chrome", "Edge"]
Reference Information:
Reference ID: cb74d0f3-7fee-41cf-b885-0a8db6a9c24f
Usage: Use this reference to guide manual configuration of browser homepages in Intune or other management tools.
Next Steps:
Review the extracted homepage requirements for Chrome and Edge.
Manually configure these settings in Intune using custom configuration profiles or administrative templates.
Insights: This document outlines a simple compliance requirement for browser homepage settings. While no direct Intune catalog matches were found, the extracted requirements can be implemented using custom policies or scripts.
1 Intune Settings Catalog
Identified settings
Settings not found
0 settings identified from the document.
Export settings
AI-generated content may be incorrect. Check it for accuracy.
Search by name, value, or citation
No setting found
Try adjusting your search or filter criteria.
Save this mapping


Microsoft Intune admin center
Copilot
Home
Security Copilot agents
Policy Configuration Agent (Preview)
Review settings mappings for HomePage
Agent suggestion
Suggestion by Policy Configuration Agent
New | 11/03/2026, 4:08:06 pm
Document Analysis Summary
Status: success
Problem: The user requested an analysis of a document specifying browser home page requirements for Chrome and Edge on all laptops.
Approach: The system parsed the provided text, identified browser-specific configuration requirements, and matched them to Intune catalog settings for Chrome and Edge home page URLs.
Result:
Total Settings Extracted: 2
Catalog Matched: 2
Unmatched Settings: 0
Match Rate: 100%
Top Categories: ["Startup Home page and New Tab page", "Startup, home page and new tab page"]
Reference Information:
Reference ID: 89ad73d6-9c20-43f2-b349-89ea5cfa886e
Usage: Use this reference ID to quickly create or review Intune policies for browser home page configuration.
Next Steps:
Create a policy using referenceId: 89ad73d6-9c20-43f2-b349-89ea5cfa886e
Review the matched settings to ensure they meet your organizational requirements
Insights: This document is straightforward, mapping directly to Intune settings for browser home page configuration. Both Chrome and Edge requirements were fully matched to catalog settings, enabling rapid policy deployment.
1 Intune Settings Catalog
Identified settings
Settings not found
0 settings identified from the document.
Export settings
AI-generated content may be incorrect. Check it for accuracy.
Search by name, value, or citation
No setting found
Try adjusting your search or filter criteria.
Save this mapping

# Word mismatch issue

All laptops must have ***hibernation*** turned off and a lock screen policy of 10 minutes when inactive.



# Word mismatch issue

All laptops must have ***hibernate*** turned off and a lock screen policy of 10 minutes when inactive.


**Identified settings** | Settings not found

2 settings identified from the document.

Export settings

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

Search by name, value, or citation

| Setting | Value | Citation | Confidence score |
|---|---|---|---|
| **Device Lock (1)** | | | |
| Max Inactivity Time Device Lock | 10 minutes | lock screen policy of 10 minutes when inactive | 95% |
| **Power (1)** | | | |
| Allow Hibernate | Disabled | All laptops must have hibernate turned off | 100% |

# Vulnerability Remediation Agent*


The Vulnerability Remediation Agent for Security Copilot in Intune uses data from Microsoft Defender Vulnerability Management to identify Common Vulnerabilities and Exposures (CVEs) on your managed devices.

* Limited public preview

# Vulnerability Remediation Use Case


- Patch Tuesday triage: agent ranks this month's CVEs by real exposure in your fleet
- Zero-day response: quickly see which devices are exposed and what update to deploy
- Third-party app vulnerabilities: flags outdated Chrome, Zoom, Adobe versions with fix guidance
- Audit / compliance reporting: show prioritized CVE backlog and remediation progress over time
- Small security team: focus limited hours on the highest-impact fixes first

* Limited public preview

# How does it work?


- Pulls CVE data from Microsoft Defender Vulnerability Management
- AI prioritizes CVEs by severity and device exposure
- Generates a ranked list of suggestions in the Intune admin center
- Provides step-by-step remediation guidance per CVE
- Admin deploys the fix through normal Intune workflows

* Limited public preview

# What works well?


- Focuses attention on what matters - top CVEs ranked by impact
- Bridges Defender and Intune in one view
- Actionable guidance - tells you what to deploy, not just what's broken
- Shows affected device counts and CVSS scores
- Accessible from both Endpoint Security and Agents nodes

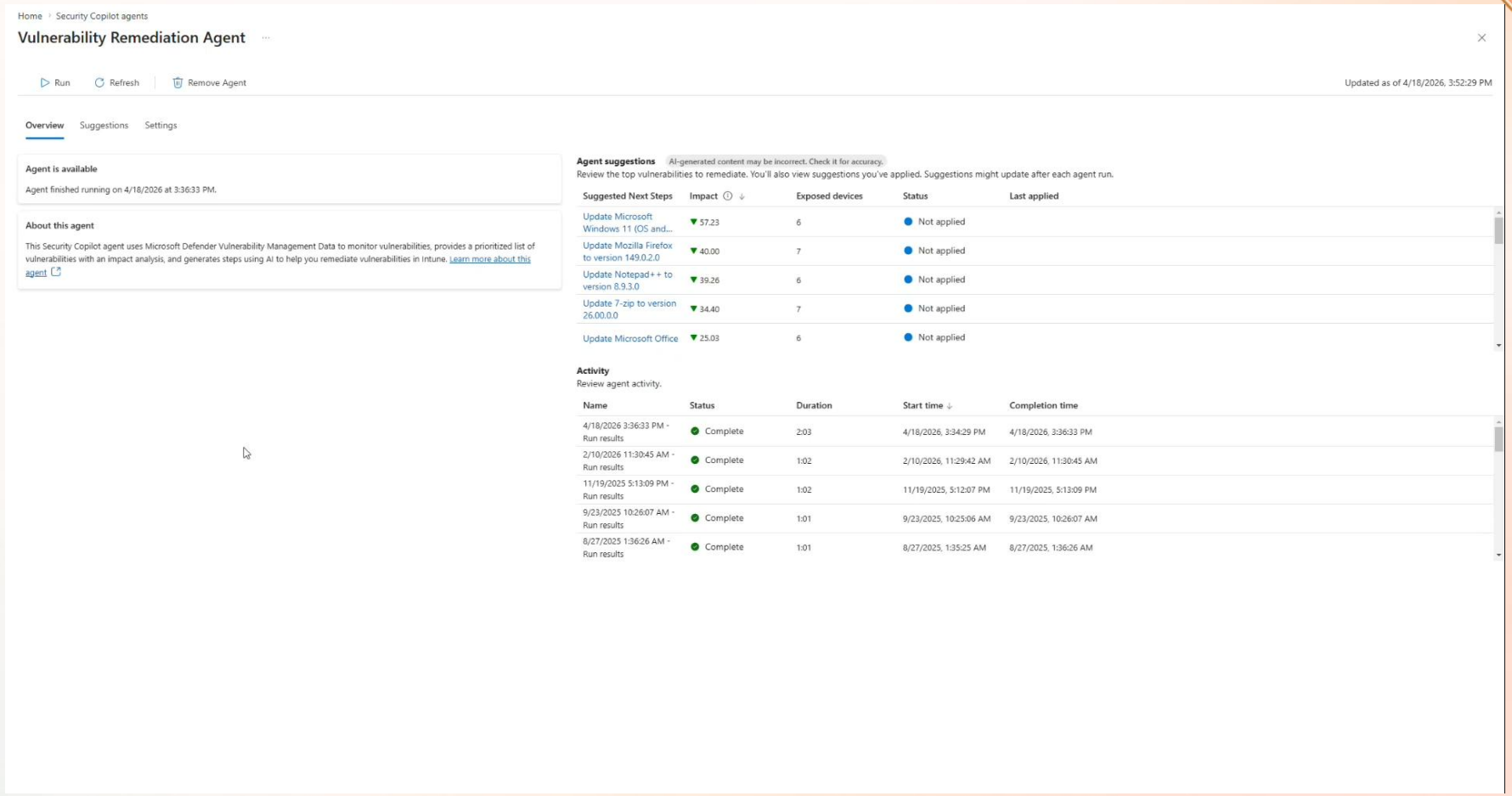
* Limited public preview

# What doesn't work (yet)?


- Limited public preview - access gated, request via Microsoft
- Windows client only - no Windows Server editions
- No scope tag support - all admins see all data
- Manual trigger only - no scheduling
- No auto-remediation - admin still deploys the fix
- Identity expires after 90 days inactivity - SCUs per run

* Limited public preview

# Demo




* Limited public preview

# Vulnerability Remediation Agent

ta to monitor vulnerabilities, provides a
AI to help you remediate vulnerabilities

Run | Refresh | Remove Agent

agent manually at any time.

Overview | **Suggestions** | Settings

Search | Add filters

| Suggested Next Steps | Remediation type | Impact | Exposed devices | Status | Last applied |
|---|---|---|---|---|---|
| Update Microsoft Edge Chromium-based | App update | 54.29 | 49 | Not applied | |
| Update Microsoft Edge Webview2 Runtime | App update | 48.86 | 45 | Not applied | |
| Update Microsoft Windows 11 (OS and built-in applications) | OS update | 22.14 | 39 | Not applied | |
| Update Microsoft Office | App update | 15.56 | 29 | Not applied | |
| Update Google Chrome to version 146.0.7680.80 | App update | 11.94 | 11 | Not applied | |
| Update Microsoft Teams | App update | 7.88 | 11 | Not applied | |
| Update Videolan Vlc Media Player | App update | 4.05 | 9 | Not applied | |
| Update Python | App update | 3.42 | 7 | Not applied | |
| Update Mozilla Firefox to version 148.0.2.0 | App update | 2.86 | 4 | Not applied | |
| Update Docker Desktop | App update | 1.94 | 4 | Not applied | |
| Update Notepad++ to version 8.9.2.0 | App update | 1.56 | 3 | Not applied | |
| Update Putty to version 0.83.0.0 | App update | 0.70 | 1 | Not applied | |
| Update Zoom Meetings to version 6.7.30439.0 | App update | 0.59 | 1 | Not applied | |
| Update Microsoft Visual Studio Code to version 1.111.0.0 | App update | 0.55 | 1 | Not applied | |
| Update Mcafee Webadvisor | App update | 0.33 | 1 | Not applied | |

tity at any time. Ensure the user who the
ent will fail to run. If agent is unused for
ntication

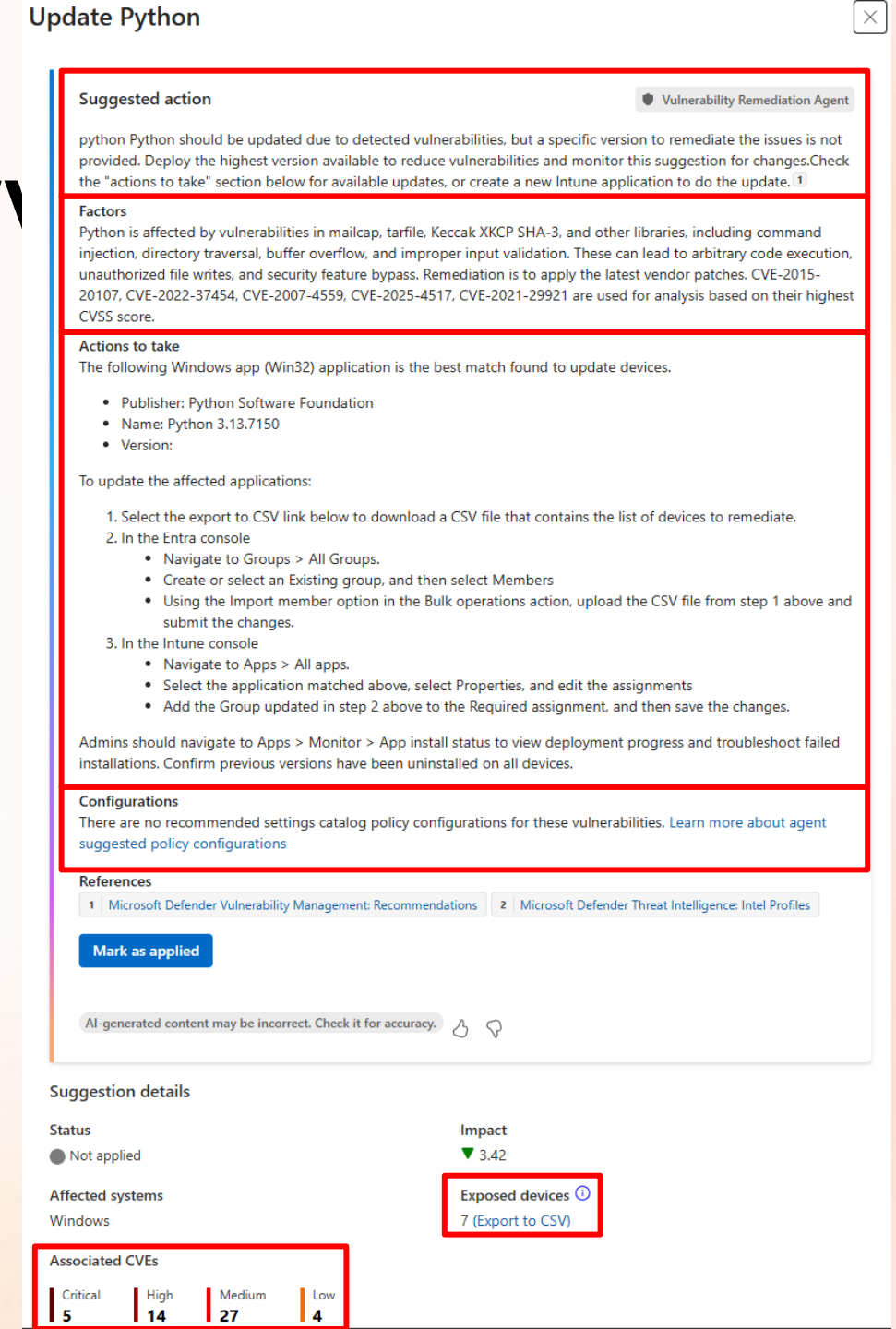
e automatically turned on only for this

r role. Learn more about RBAC roles

n agent mid-run. When the run finishes,

# Suggestions overv

- Suggested action
- Factors
- Actions to take
- Configurations
- CVE Count
- Exposed devices



# Issues to report

## Update Python

### Suggested action

Vulnerability Remediation Agent

python Python should be updated due to detected vulnerabilities, but a specific version to remediate the issues is not provided. Deploy the highest version available to reduce vulnerabilities and monitor this suggestion for changes.Check the "actions to take" section below for available updates, or create a new Intune application to do the update. [1]

**Factors**

Python is affected by vulnerabilities in mailcap, tarfile, Keccak XKCP SHA-3, and other libraries, including command injection, directory traversal, buffer overflow, and improper input validation. These can lead to arbitrary code execution, unauthorized file writes, and security feature bypass. Remediation is to apply the latest vendor patches. CVE-2015-20107, CVE-2022-37454, CVE-2007-4559, CVE-2025-4517, CVE-2021-29921 are used for analysis based on their highest CVSS score.

**Actions to take**

The following Windows app (Win32) application is the best match found to update devices.

- Publisher: Python Software Foundation
- Name: Python 3.13.7150
- Version:

To update the affected applications:

1. Select the export to CSV link below to download a CSV file that contains the list of devices to remediate.
2. In the Entra console
   - Navigate to Groups > All Groups.
   - Create or select an Existing group, and then select Members
   - Using the Import member option in the Bulk operations action, upload the CSV file from step 1 above and submit the changes.
3. In the Intune console
   - Navigate to Apps > All apps.
   - Select the application matched above, select Properties, and edit the assignments
   - Add the Group updated in step 2 above to the Required assignment, and then save the changes.

Admins should navigate to Apps > Monitor > App install status to view deployment progress and troubleshoot failed installations. Confirm previous versions have been uninstalled on all devices.

**Configurations**

There are no recommended settings catalog policy configurations for these vulnerabilities. Learn more about agent suggested policy configurations

**References**

[1] Microsoft Defender Vulnerability Management: Recommendations [2] Microsoft Defender Threat Intelligence: Intel Profiles

Mark as applied

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

### Suggestion details

**Status**
Not applied

**Impact**
▼ 3.42

**Affected systems**
Windows

**Exposed devices**
7 (Export to CSV)

**Associated CVEs**

| Critical | High | Medium | Low |
|---|---|---|---|
| 5 | 14 | 27 | 4 |


# Security Copilot In Intune Embedded Experience

# Security Copilot Embedded


Security Copilot Embedded is the AI chat pane built directly into the Intune admin center. It answers questions in plain English about your tenant - policies, devices, users, apps - using data from Intune, Entra, and Defender. Instead of clicking through blades or writing queries, you ask and it explains.

# Security Copilot Embedded Use Case


- Quick policy summary - "What does this Conditional Access policy do?"
- Device troubleshooting - "Why is this device non-compliant?"
- Group / assignment tracing - "Why did this user get this app?"
- Policy comparison - spot differences between two similar policies
- Onboarding / training - junior admins ask in plain English instead of hunting in docs

# How does it work?


- Chat pane embedded directly in the Intune admin center
- Context-aware - knows what policy, device, or user you have open
- Backed by Security Copilot - same SCU billing as the agents
- Uses natural language - no KQL or Graph syntax required
- Read-only - answers questions but doesn't change configuration

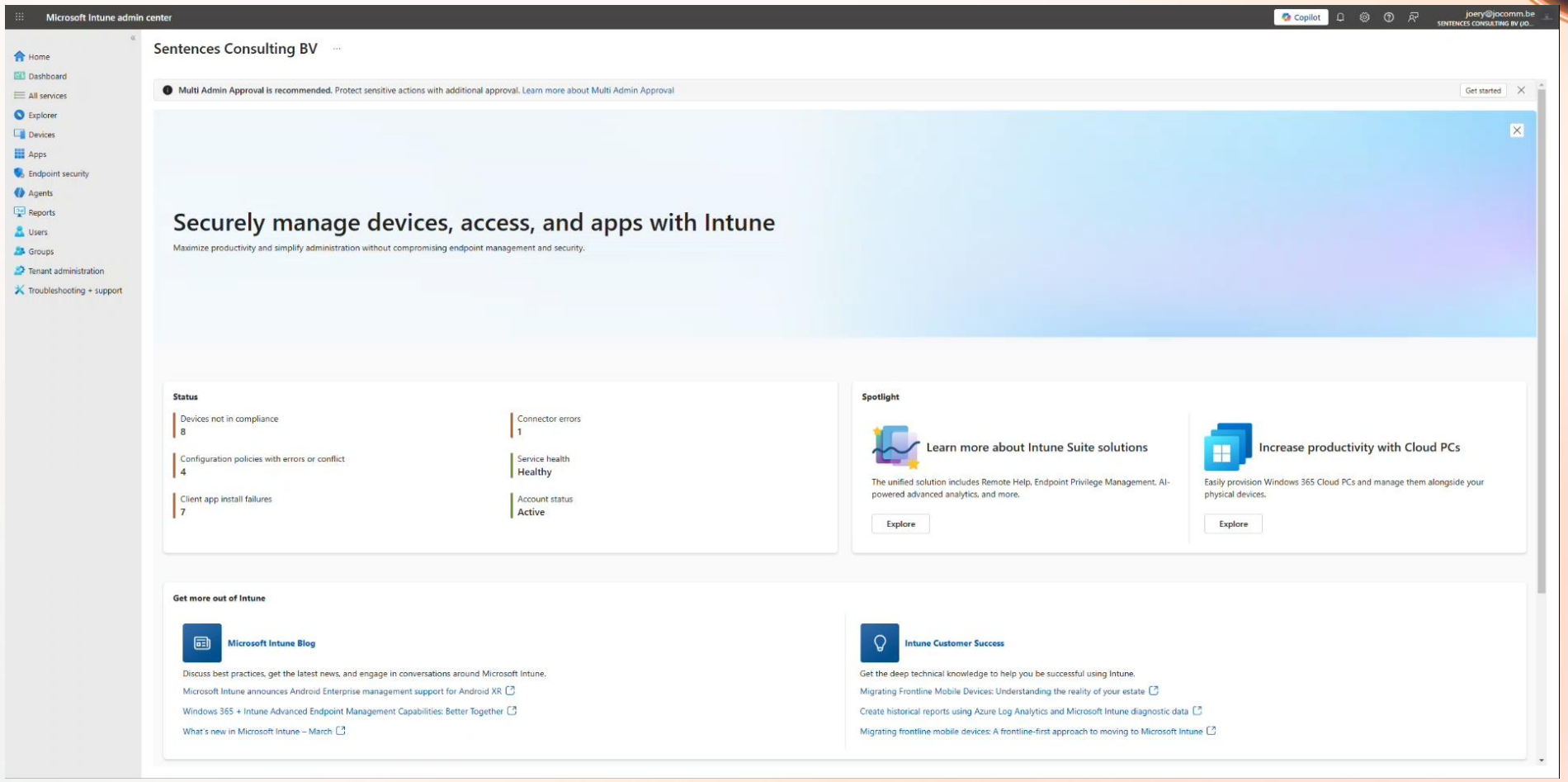
# What works well?


- Fast policy and device summaries in plain English
- Great for troubleshooting - explains why a device is failing compliance
- Surfaces data without switching blades or writing queries
- Lowers skill barrier - junior admins get answers faster
- Helps compare similar policies side by side

# What doesn't work (yet)?


- Read-only - can't create, edit, or assign policies for you
- Answers can be vague or generic - still need admin judgment
- Limited coverage - not every Intune blade or data type is supported
- Consumes SCUs per prompt - cost grows with usage
- Public cloud only - not available in government clouds
- Needs Security Copilot licensing - not included with Intune alone

# Demo


Microsoft Intune admin center
Copilot
joery@jocomm.be
SENTENCES CONSULTING BV (JO...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Sentences Consulting BV
Multi Admin Approval is recommended. Protect sensitive actions with additional approval. Learn more about Multi Admin Approval
Get started
Securely manage devices, access, and apps with Intune
Maximize productivity and simplify administration without compromising endpoint management and security.
Status
Devices not in compliance
8
Connector errors
1
Configuration policies with errors or conflict
4
Service health
Healthy
Client app install failures
7
Account status
Active
Spotlight
Learn more about Intune Suite solutions
The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.
Explore
Increase productivity with Cloud PCs
Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.
Explore
Get more out of Intune
Microsoft Intune Blog
Discuss best practices, get the latest news, and engage in conversations around Microsoft Intune.
Microsoft Intune announces Android Enterprise management support for Android XR
Windows 365 + Intune Advanced Endpoint Management Capabilities: Better Together
What's new in Microsoft Intune – March
Intune Customer Success
Get the deep technical knowledge to help you be successful using Intune.
Migrating Frontline Mobile Devices: Understanding the reality of your estate
Create historical reports using Azure Log Analytics and Microsoft Intune diagnostic data
Migrating frontline mobile devices: A frontline-first approach to moving to Microsoft Intune


# Intune Explorer

# Intune Explorer


Using natural language and your own words, you can query and explore your Intune data. An intelligent search matches your request to available query views that are built into Intune.

# What can be queried?


- Advanced Analytics
- App configuration and app protection
- Apps
- Audit logs
- Compliance
- Device Configuration
- Device updates
- Devices (device properties)
- Endpoint Privilege Management
- Role based access control (RBAC)
- Users and groups
- Windows Autopilot deployments

# What actions can be taken?


- Add devices to a group
- Add users to group


# Security Copilot Standalone

# Security Copilot Standalone


Security Copilot standalone is Microsoft's dedicated generative-AI workspace for security, accessed through its own portal. Unlike the embedded experience in Intune, it can pull signals across Defender, Sentinel, Entra, Purview, Intune, and third-party plugins in one place - giving SOC and security teams a unified chat surface for investigations, threat hunting, and reporting.

# Security Copilot Standalone Use Case


- Incident investigation - summarize a Defender incident and pivot across connected products
- Threat hunting - natural-language KQL across Sentinel and Defender data
- Script & malware analysis - paste a suspicious script or command line, get an explanation
- Executive reporting - turn incident data into plain-English summaries for management
- Custom promptbooks - automate recurring investigation flows for SOC analysts

# How does it work?


- Dedicated portal at securitycopilot.microsoft.com
- Connect plugins - Defender, Sentinel, Entra, Intune, Purview, 3rd-party
- Ask in natural language - Copilot picks the right plugin automatically
- Runs on SCUs (Security Compute Units) - billed per hour of provisioned capacity
- Promptbooks - reusable prompt chains for recurring tasks

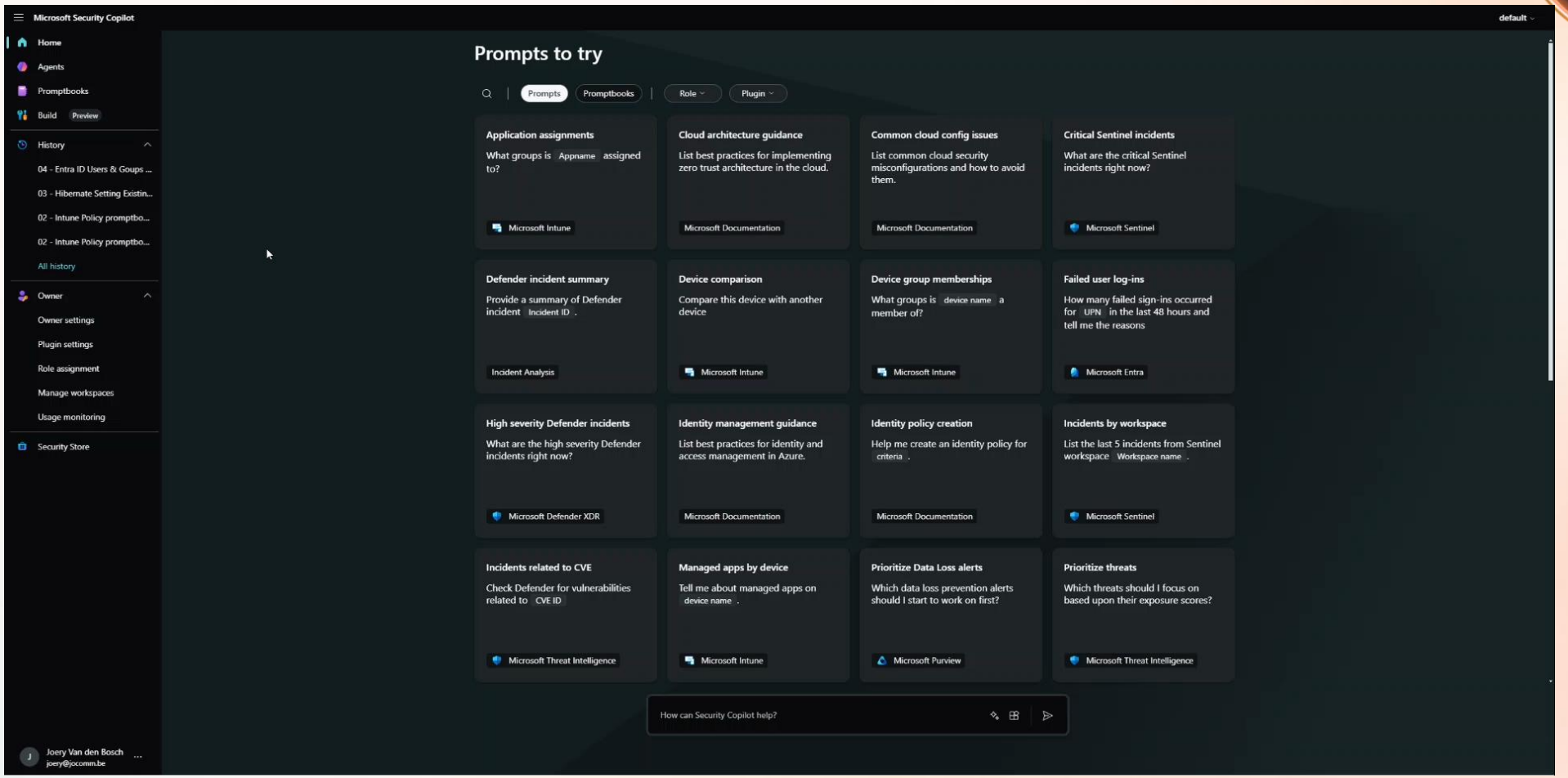
# What works well?


- One surface across the whole Microsoft security stack
- Script and incident summaries save hours of analyst time
- Lowers the skill floor for KQL and threat hunting
- Audit trail - every prompt and response is logged
- Extensible - custom and partner plugins beyond Microsoft's own products

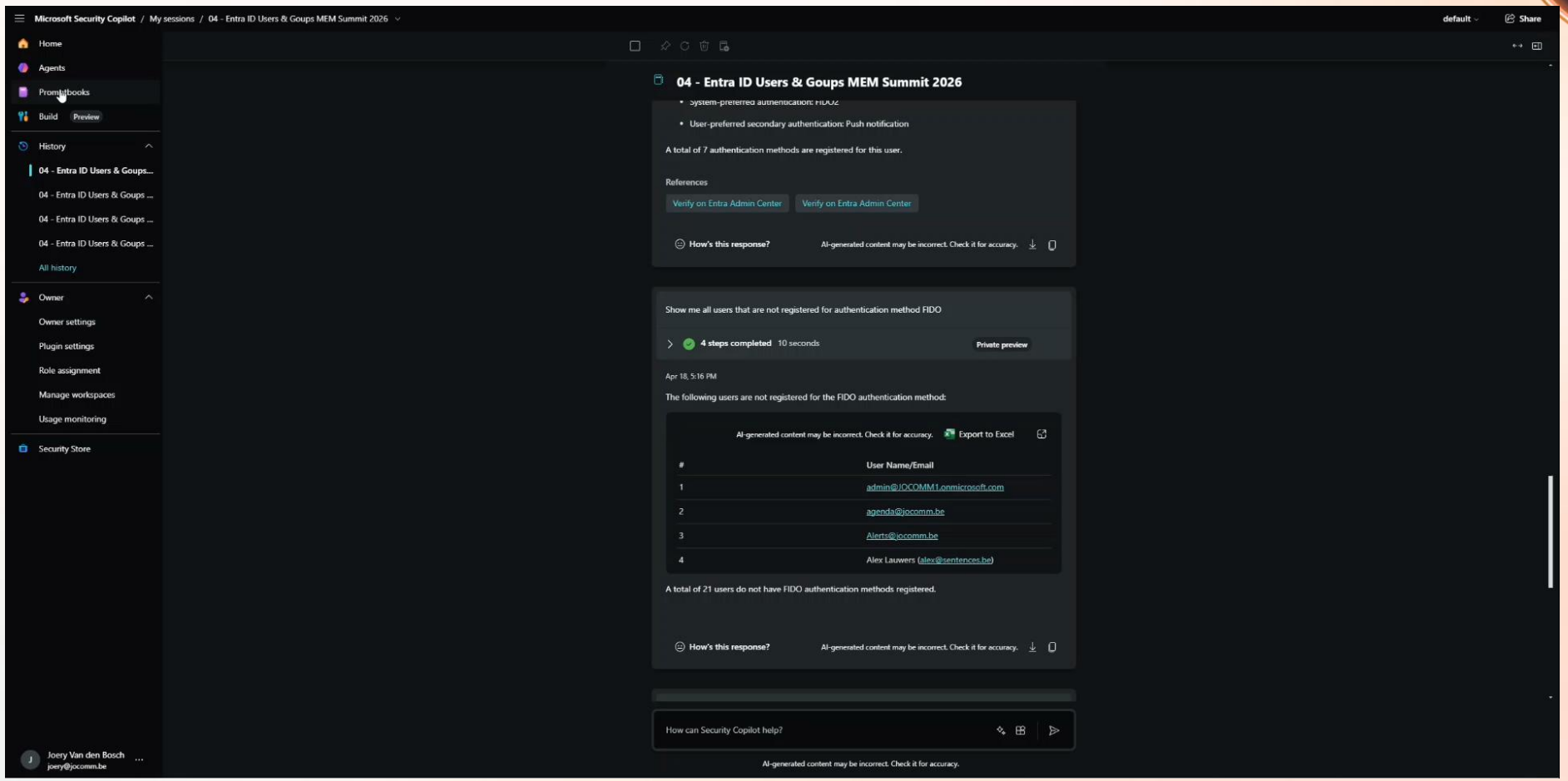
# What doesn't work (yet)?


- Expensive - SCU billing stacks up fast (~$2,920/mo for 1 SCU, 24/7) – or not???? Stay Tuned ;-)
- Answer quality varies - can hallucinate or give vague results
- Steep learning curve - prompt skill heavily impacts output quality
- No agentic actions - it analyzes, but doesn't remediate automatically
- Public cloud only - not available in government clouds
- Data scope depends on configured plugins and permissions

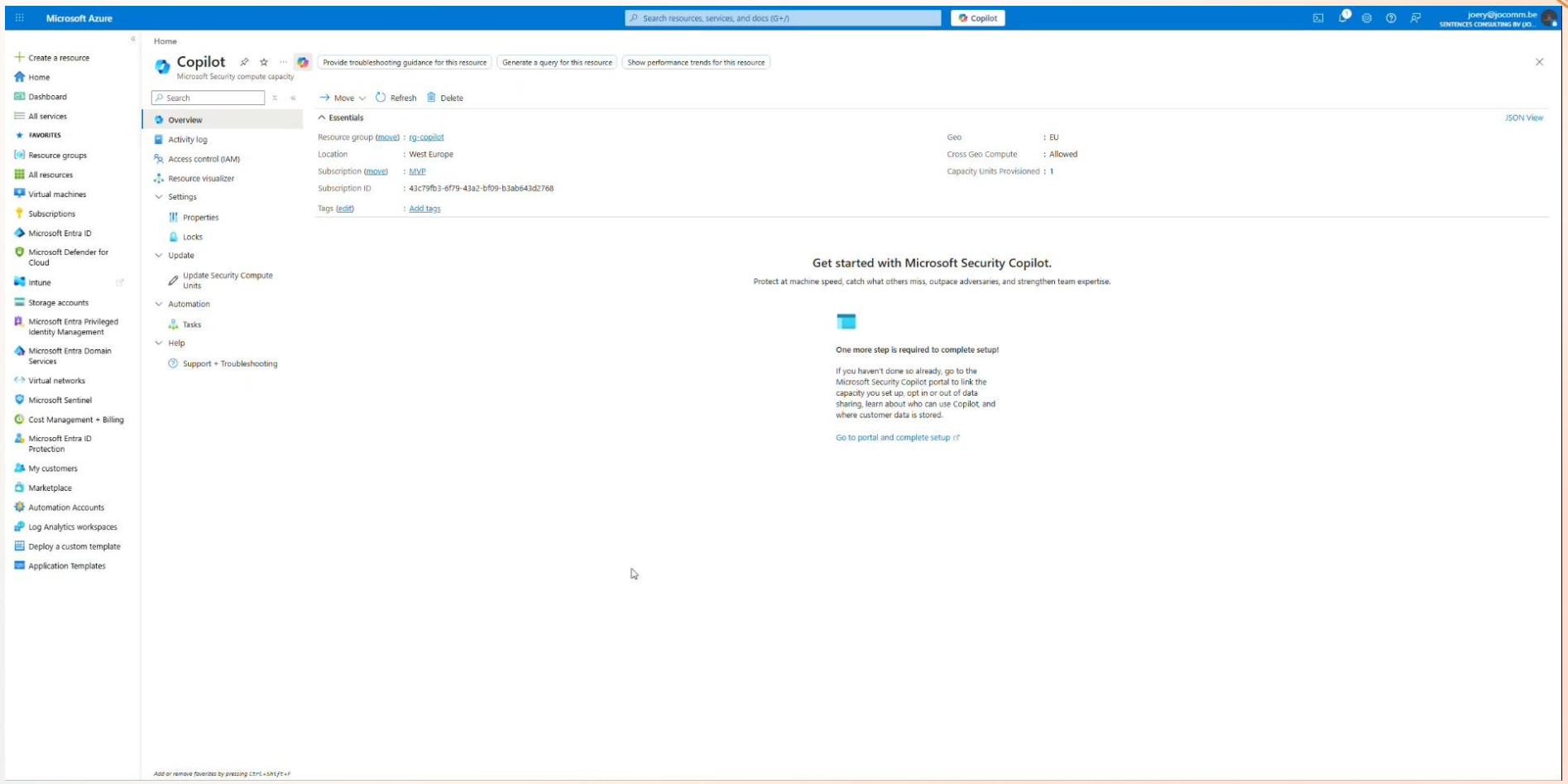
# Demo


Microsoft Security Copilot
default
Home
Agents
Promptbooks
Build
Preview
History
04 - Entra ID Users & Goups ...
03 - Hibernate Setting Existin...
02 - Intune Policy promptbo...
02 - Intune Policy promptbo...
All history
Owner
Owner settings
Plugin settings
Role assignment
Manage workspaces
Usage monitoring
Security Store
Joery Van den Bosch
joery@jocomm.be
Prompts to try
Prompts
Promptbooks
Role
Plugin
Application assignments
What groups is Appname assigned to?
Microsoft Intune
Cloud architecture guidance
List best practices for implementing zero trust architecture in the cloud.
Microsoft Documentation
Common cloud config issues
List common cloud security misconfigurations and how to avoid them.
Microsoft Documentation
Critical Sentinel incidents
What are the critical Sentinel incidents right now?
Microsoft Sentinel
Defender incident summary
Provide a summary of Defender incident Incident ID .
Incident Analysis
Device comparison
Compare this device with another device
Microsoft Intune
Device group memberships
What groups is device name a member of?
Microsoft Intune
Failed user log-ins
How many failed sign-ins occurred for UPN in the last 48 hours and tell me the reasons
Microsoft Entra
High severity Defender incidents
What are the high severity Defender incidents right now?
Microsoft Defender XDR
Identity management guidance
List best practices for identity and access management in Azure.
Microsoft Documentation
Identity policy creation
Help me create an identity policy for criteria .
Microsoft Documentation
Incidents by workspace
List the last 5 incidents from Sentinel workspace Workspace name .
Microsoft Sentinel
Incidents related to CVE
Check Defender for vulnerabilities related to CVE ID
Microsoft Threat Intelligence
Managed apps by device
Tell me about managed apps on device name .
Microsoft Intune
Prioritize Data Loss alerts
Which data loss prevention alerts should I start to work on first?
Microsoft Purview
Prioritize threats
Which threats should I focus on based upon their exposure scores?
Microsoft Threat Intelligence
How can Security Copilot help?

# Demo


Microsoft Security Copilot / My sessions / 04 - Entra ID Users & Goups MEM Summit 2026
default
Share
Home
Agents
Promptbooks
Build
Preview
History
04 - Entra ID Users & Goups...
04 - Entra ID Users & Goups ...
04 - Entra ID Users & Goups ...
04 - Entra ID Users & Goups ...
All history
Owner
Owner settings
Plugin settings
Role assignment
Manage workspaces
Usage monitoring
Security Store
Joery Van den Bosch
joery@jocomm.be
04 - Entra ID Users & Goups MEM Summit 2026
User-preferred secondary authentication: Push notification
A total of 7 authentication methods are registered for this user.
References
Verify on Entra Admin Center
Verify on Entra Admin Center
How's this response?
AI-generated content may be incorrect. Check it for accuracy.
Show me all users that are not registered for authentication method FIDO
4 steps completed 10 seconds
Private preview
Apr 18, 5:16 PM
The following users are not registered for the FIDO authentication method:
AI-generated content may be incorrect. Check it for accuracy.
Export to Excel
# User Name/Email
1 admin@JOCOMM1.onmicrosoft.com
2 agenda@jocomm.be
3 Alerts@jocomm.be
4 Alex Lauwers (alex@sentences.be)
A total of 21 users do not have FIDO authentication methods registered.
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.

# Costs


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
joery@jocomm.be
SENTENCES CONSULTING BV (JO...
Home
Create a resource
Home
Dashboard
All services
FAVORITES
Resource groups
All resources
Virtual machines
Subscriptions
Microsoft Entra ID
Microsoft Defender for Cloud
Intune
Storage accounts
Microsoft Entra Privileged Identity Management
Microsoft Entra Domain Services
Virtual networks
Microsoft Sentinel
Cost Management + Billing
Microsoft Entra ID Protection
My customers
Marketplace
Automation Accounts
Log Analytics workspaces
Deploy a custom template
Application Templates
Copilot
Microsoft Security compute capacity
Provide troubleshooting guidance for this resource
Generate a query for this resource
Show performance trends for this resource
Search
Overview
Activity log
Access control (IAM)
Resource visualizer
Settings
Properties
Locks
Update
Update Security Compute Units
Automation
Tasks
Help
Support + Troubleshooting
Move
Refresh
Delete
Essentials
JSON View
Resource group (move) : rg-copilot
Location : West Europe
Subscription (move) : MVP
Subscription ID : 43c79fb3-6f79-43a2-bf09-b3ab643d2768
Tags (edit) : Add tags
Geo : EU
Cross Geo Compute : Allowed
Capacity Units Provisioned : 1
Get started with Microsoft Security Copilot.
Protect at machine speed, catch what others miss, outpace adversaries, and strengthen team expertise.
One more step is required to complete setup!
If you haven't done so already, go to the Microsoft Security Copilot portal to link the capacity you set up, opt in or out of data sharing, learn about who can use Copilot, and where customer data is stored.
Go to portal and complete setup
Add or remove favorites by pressing Ctrl+Shift+F


# Is it really worth it?


Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

# Thanks!