



Welcome at the Workplace Ninja User Group Belgium Meetup





MEET THE NINJAS



KENNY BUNTINX



NICKY DE WESTELINCK



MAXIME GUILLEMIN



JOERY VAN DEN BOSCH



DIETER KEMPENEERS



KIM HEYRMAN



OUR FOCUS

Microsoft 365 – Modern Work



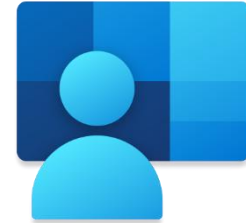
Microsoft Entra



Microsoft Security



Windows 365



Microsoft Intune



Microsoft
Security Copilot



AGENDA



18:30 – 19:00

Welcome by the Workplace Ninja User Group Belgium



19:00 – 20:00

Proactive Device Management Unleashed: Intune Advanced Analytics and Microsoft Security Copilot in Action by *Maxime Guillemin and Joery Van den Bosch*



20:00 – 20:30

Break



20:30 – 21:15

Managing your Mac in the Enterprise - Intune's Magic Potion by *Kenny Buntinx*



21:15 – 22:30

Closing Drinks & Networking



THANK YOU TO OUR SPONSOR



Arxus



Hybrid Cloud & Networking

Private Cloud &
Managed IaaS

Cloud Managed
Networking

Cloud Connectivity



Azure

Cloud Operations
Services

Application
Modernization &
DevOps Services

Microsoft Azure CSP



Modern Workplace

Cloud Managed
Workplace

Cloud Voice

Microsoft 365 CSP



Cloud Security

Cybersecurity
Services

SOC & CSIRT

Proactive Device Management Unleashed

Intune Advanced Analytics and Microsoft Security
Copilot with Intune in Action





About “Maxime Guillemin”

<https://wpninjas.be>
#WPNinjasbe

Focus

Microsoft Intune, MS Graph API & Automation

From

Modern Workplace Architect @



Arxus

My Blog

<https://cloudflow.be>



Certifications

Microsoft 365 Certified: Endpoint Administrator Associate

Microsoft Certified: Azure Administrator Associate

Microsoft 365 Certified: Security Administrator Associate

Hobbies

Skiing , Scuba Diving & Blogging



Contact

mg@cloudflow.be





About “Joery Van den Bosch”

<https://wpnijas.be>
#WPNinjasbe

Focus

Microsoft Intune Geek, Blogger

From

Modern Workplace Architect @



My Blog

<https://intunestuff.com>



Certifications



Hobbies

Food, Whisky, Formula 1 & My Family



Contact

Joery@intunestuff.com

LinkedIn : <https://www.linkedin.com/in/joery/>





Agenda

<https://wpninja.be>
#WPNinjasbe

Key takeaways:

- What is Copilot for Security and how to set it up
- What is Intune Advanced Analytics
- Device Query with Copilot
- How to use Copilot for Intune
- Q&A

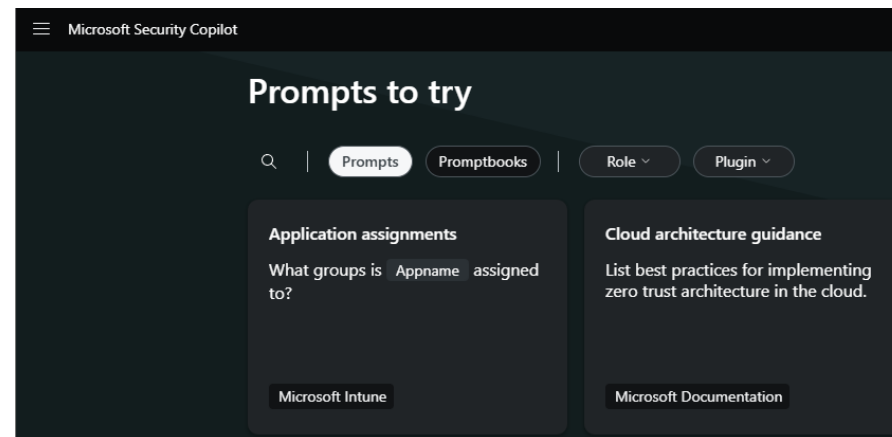




What is Copilot for Intune?

<https://wpninja.be>
#WPNinjasbe

- Copilot for Intune is a part of Copilot for Security
- Copilot for Intune is a plugin on Copilot for Security
- Integrates seamlessly with your Intune data
- Security Admin focused
- Access only Data based on users' permissions
- You need an active Azure subscription to use Copilot for Security



How Copilot can help

Copilot can make mistakes, so remember to verify the results.



Explore device

Get answers about this device's properties and the policies and apps assigned to it.



Compare to another device

Select another device and understand the differences in hardware and device configurations



Analyze error code

See an error code that you don't understand? Get answers and learn how you can remediate.





How to Setup Copilot for Security and enable Copilot for Intune

<https://wpninjas.be>
#WPNinjasbe

Microsoft Intune admin center

Home > Tenant admin

Tenant admin | Copilot (preview)

Search

Copilot hasn't been set up yet. To use Copilot, your Global or Billing Administrator will have to add capacity. Then have your Security Administrator set it up. [Learn more about setting up Copilot for Security](#)

Refresh

Copilot in Intune

Not set up

What can you do with Microsoft Copilot in Intune?

Copilot can help you with regular management tasks like policy management and troubleshooting devices. Look for Copilot throughout Intune to help you understand and manage your devices more efficiently and effectively. [Learn more about Copilot in Intune](#)

How Copilot works

How Copilot in Intune gets answers

When you ask Copilot a question in Intune, it gets sent to Copilot for Security, which processes the input and generates a response. Copilot for Security uses data from your tenant and authoritative Microsoft documentation sources to generate its response. The response comes back from Copilot for Security and is displayed in Intune. You can see all of your interactions in Copilot for Security by looking at your sessions in [Copilot for Security](#). [Privacy and data security in Microsoft Copilot for Security](#)

Interpreting Copilot's results

Monitoring usage

Let us know how Copilot is doing

Copilot can make mistakes so remember to verify the results. To help improve the experience, share your feedback with us as you use Copilot.

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

- Tenant status
- Remote Help
- Microsoft Tunnel Gateway
- Cloud PKI
- Connectors and tokens
- Filters
- Roles
- Microsoft Entra Privileged Identity Management
- Diagnostics settings
- Audit logs
- Device diagnostics
- Multi Admin Approval
- Intune add-ons
- Copilot (preview)**
 - End user experiences
 - Customization
 - Organizational messages
 - Custom notifications
 - Terms and conditions
 - Windows Autopatch
 - Tenant enrollment
 - Microsoft Managed Desktop
 - Tenant enrollment
 - Help and support
 - Help and support





How to Setup Copilot for Security and enable Copilot for Intune

<https://wpnijas.be>
#WPNinjasbe

Microsoft Copilot for Security interface showing incident investigation and script analysis results.

Continue your last session

Microsoft 365 Defender incident investigation

Incident Investigation | Phishing Attempt | Multi-Factor Authentication | +2

This report provides an overview of an informational severity incident that occurred on July 17, 2024, involving malicious URLs in email messages. The incident was detected and resolved within two minutes. The primary target was a user named 'Joery', who has Multi-Factor Authentication.

Updated 25 days ago

Script analysis

PowerShell | +4

The conversation involves an analysis of a PowerShell script that downloads an executable file from a specific URL, saves it t...

Device Information

+5

The assistant provides detailed information about a device with ID '34ac855f-be16-4ec2-b1c6-2166e92c601e'. The device is a...

[View all sessions](#)

Get started using these promptbooks

Promptbooks contain one or more prompts that run in sequence automatically. [Learn more](#)

Microsoft Sentinel incident investigation

Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.

Microsoft Security · 7 prompts

Suspicious script analysis

Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.

Microsoft Security · 6 prompts

Vulnerability impact assessment

Get a report summarizing the intelligence for a known vulnerability and how to address it.

Microsoft Security · 4 prompts

[View promptbook library](#)

How can Copilot for Security help?



Intune Advanced Analytics

- **Device Scopes**
- **Battery Health Report**
- **Recourse performance Report**
- **Enhanced Device Timeline**
- **Anomaly Detection**
- **Device Query**





Who has used Intune Advanced Analytics

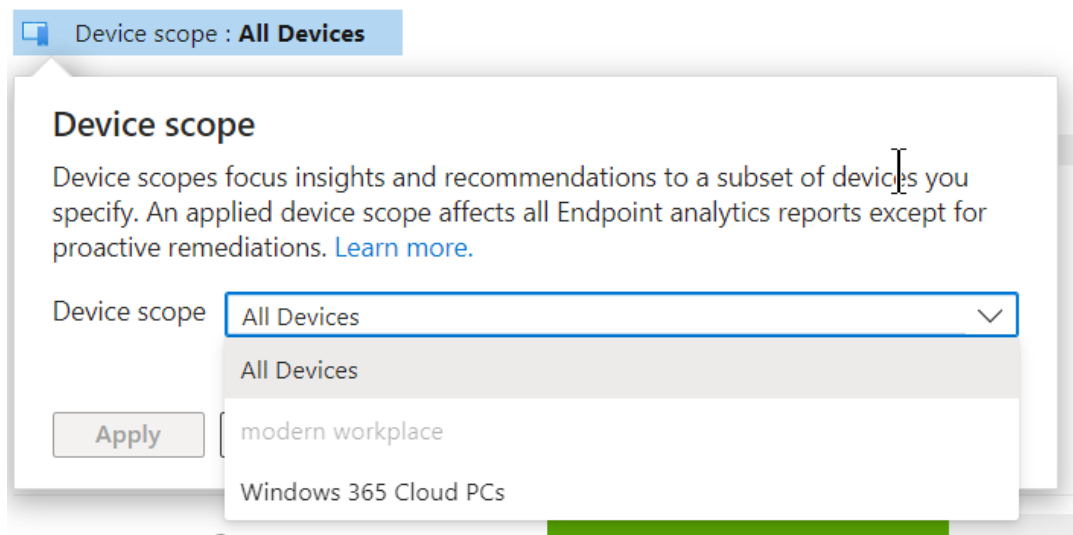
① Start presenting to display the poll results on this slide.



Device Scopes

<https://wpninja.be>
#WPNinjasbe

- Customized Reporting for Specific Device Groups
- Focused Insights and Recommendations
- Enhanced Management Efficiency
- Improved Security and Compliance

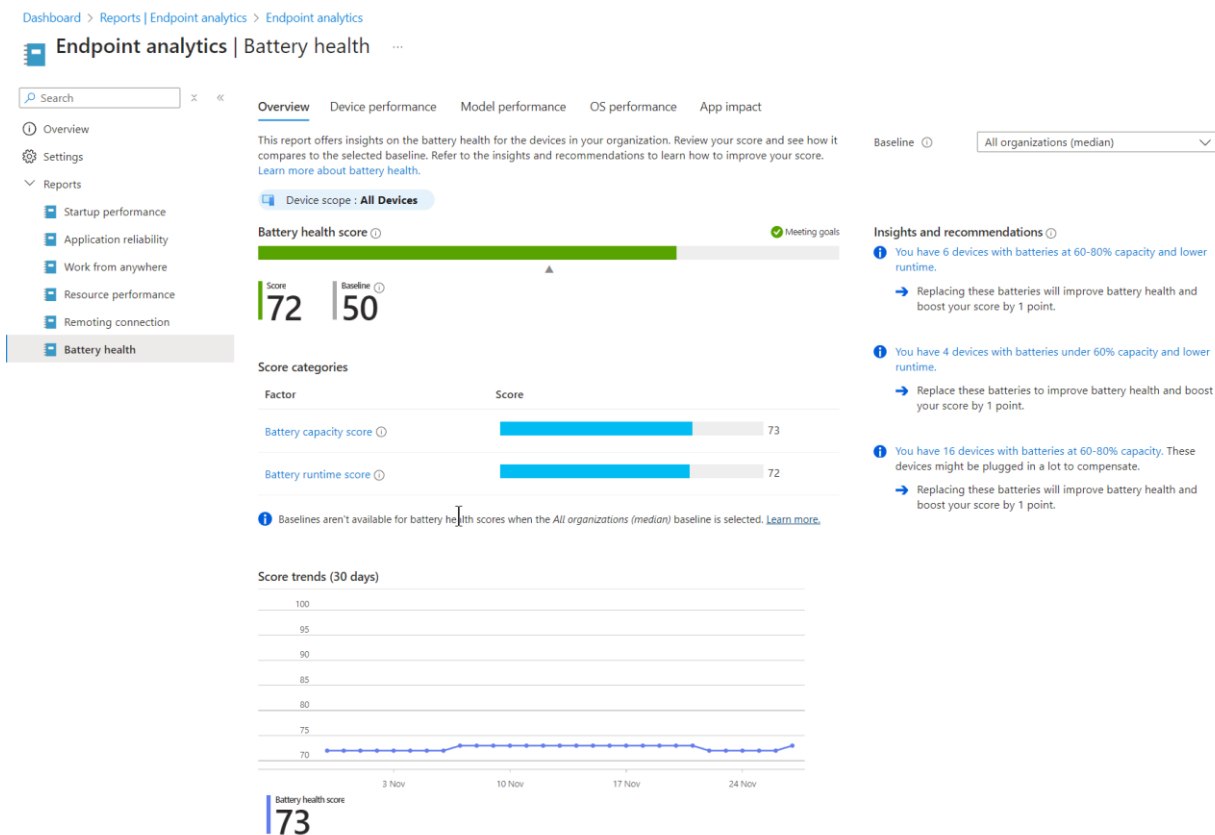




Battery Health Report

<https://wpninja.be>
#WPNinjasbe

- Easily Check How Your Device Batteries Are Doing
- Find Battery Problems Before They Cause Trouble
- Keep Your Team Working Smoothly
- Save Money by Using Warranties Wisely
- Make Smart Choices Using Real Data





Battery Health MS Graph API

<https://wpninja.be>
#WPNinjasbe

- <https://graph.microsoft.com/beta/deviceManagement/userExperienceAnalyticsBatteryHealthDevicePerformance>
- <https://graph.microsoft.com/beta/deviceManagement/userExperienceAnalyticsBatteryHealthModelPerformance>
- <https://graph.microsoft.com/beta/deviceManagement/userExperienceAnalyticsBatteryHealthOsPerformance>
- <https://graph.microsoft.com/beta/deviceManagement/userExperienceAnalyticsBatteryHealthAppImpact>

```
"value": [
  {
    "id": "d7fbcc3e-a3f5-4045-89d1-8e8e4914f880",
    "deviceId": "Surface Laptop 4",
    "deviceName": "Surface Laptop 4",
    "model": "Latitude 5520",
    "manufacturer": "Dell Inc.",
    "deviceModelName": "Latitude 5520",
    "deviceManufacturerName": "Dell Inc.",
    "maxCapacityPercentage": 40,
    "estimatedRuntimeInMinutes": 134,
    "batteryAgeInDays": 1331,
    "fullBatteryDrainCount": -1,
    "deviceBatteryCount": 1,
    "deviceBatteryTags": [],
    "deviceBatteryHealthScore": 37,
    "healthStatus": "needsAttention",
    "deviceBatteriesDetails": [
      {
        "batteryId": "LIP;41587;BYD;0",
        "maxCapacityPercentage": 40,
        "fullBatteryDrainCount": 0
      }
    ]
  }
],
```

```
{
  "id": "d7fbcc3e-a3f5-4045-89d1-8e8e4914f880",
  "activeDevices": 63,
  "model": "Surface Laptop 4",
  "manufacturer": "Microsoft Corporation",
  "deviceModelName": "Surface Laptop 4",
  "deviceManufacturerName": "Microsoft Corporation",
  "averageMaxCapacityPercentage": 84,
  "averageEstimatedRuntimeInMinutes": 12227,
  "averageBatteryAgeInDays": 785,
  "meanFullBatteryDrainCount": 216,
  "medianMaxCapacityPercentage": 84,
  "medianEstimatedRuntimeInMinutes": 285,
  "medianFullBatteryDrainCount": 199,
  "modelBatteryHealthScore": 71,
  "modelHealthStatus": "meetingGoals"
},
{
  "id": "84696f52-9101-47c8-943d-d349283fd4bd",
  "activeDevices": 50,
  "model": "Surface Laptop 5",
  "manufacturer": "Microsoft Corporation",
  "deviceModelName": "Surface Laptop 5",
  "deviceManufacturerName": "Microsoft Corporation",
  "averageMaxCapacityPercentage": 87,
  "averageEstimatedRuntimeInMinutes": 296,
  "averageBatteryAgeInDays": 319,
  "meanFullBatteryDrainCount": 71,
  "medianMaxCapacityPercentage": 87,
  "medianEstimatedRuntimeInMinutes": 272,
  "medianFullBatteryDrainCount": 59,
  "modelBatteryHealthScore": 74,
  "modelHealthStatus": "meetingGoals"
}
```

```
"value": [
  {
    "id": "fdaeb2ee-cf3e-46a0-97c9-14f17f01c526",
    "activeDevices": 60,
    "osVersion": "10.0.22631.4751",
    "osBuildNumber": "10.0.22631",
    "averageMaxCapacityPercentage": 82,
    "averageEstimatedRuntimeInMinutes": 242,
    "averageBatteryAgeInDays": 622,
    "meanFullBatteryDrainCount": 141,
    "medianMaxCapacityPercentage": 84,
    "medianEstimatedRuntimeInMinutes": 251,
    "medianFullBatteryDrainCount": 110,
    "osBatteryHealthScore": 67,
    "osHealthStatus": "meetingGoals"
  },
  {
    "id": "efc79a9a-27db-4178-a4b5-c2f35a453401",
    "activeDevices": 113,
    "osVersion": "10.0.26100.2894",
    "osBuildNumber": "10.0.26100",
    "averageMaxCapacityPercentage": 86,
    "averageEstimatedRuntimeInMinutes": 12257,
    "averageBatteryAgeInDays": 473,
    "meanFullBatteryDrainCount": 113,
    "medianMaxCapacityPercentage": 87,
    "medianEstimatedRuntimeInMinutes": 280,
    "medianFullBatteryDrainCount": 70,
    "osBatteryHealthScore": 74,
    "osHealthStatus": "meetingGoals"
  }
]
```

```
{
  "id": "60c5acd7-41e4-4259-aaf1-e2b8c2f53e02",
  "activeDevices": 132,
  "appName": "msedge.exe",
  "appDisplayName": "Microsoft Edge",
  "appPublisher": "Microsoft Corporation",
  "isForegroundApp": true,
  "batteryUsagePercentage": 10.12
},
{
  "id": "06b6905d-46aa-4773-a577-2c604e621dd0",
  "activeDevices": 171,
  "appName": "ms-teams.exe",
  "appDisplayName": "Microsoft Teams",
  "appPublisher": "Microsoft Corporation",
  "isForegroundApp": true,
  "batteryUsagePercentage": 9.19
},
{
  "id": "c085cea5-dbcd-4519-8945-4c9449e05b24",
  "activeDevices": 169,
  "appName": "MsSense.exe",
  "appDisplayName": "Microsoft Windows Operating System",
  "appPublisher": "Microsoft Corporation",
  "isForegroundApp": false,
  "batteryUsagePercentage": 5.79
}
```

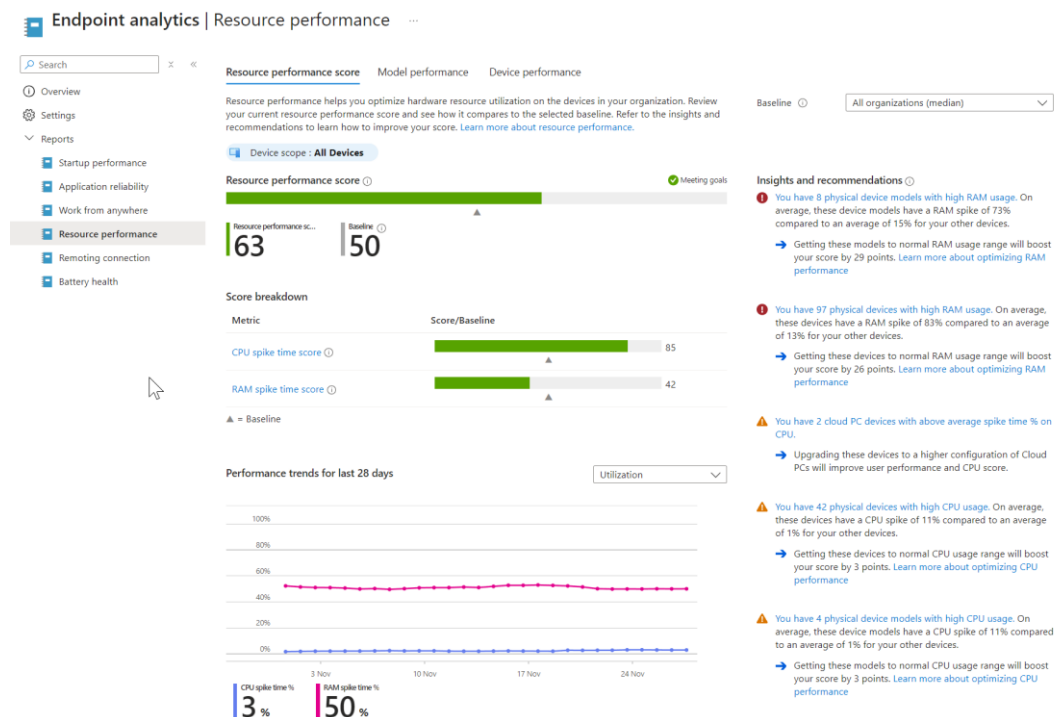




Resource Performance

<https://wpninja.be>
#WPNinjasbe

- Monitor Device Health Proactively
- Anticipate and Resolve Performance Issues Early
- Enhance User Experience and Efficiency
- Optimize Hardware Upgrades and Budgeting





Resource Performance MS Graph API

<https://wpninja.be>
#WPNinjasbe

- <https://graph.microsoft.com/beta/deviceManagement/userExperienceAnalyticsResourcePerformance>

```
"value": [  
  {  
    "id": "00000000-0000-0000-0000-000000000000",  
    "deviceId": "00000000-0000-0000-0000-000000000000",  
    "deviceName": "00000000-0000-0000-0000-000000000000",  
    "model": "Cloud PC Enterprise 8vCPU/32GB/512GB",  
    "deviceCount": -1,  
    "manufacturer": "Microsoft Corporation",  
    "cpuSpikeTimePercentage": 0,  
    "ramSpikeTimePercentage": 0,  
    "cpuSpikeTimeScore": 100,  
    "cpuSpikeTimePercentageThreshold": 15,  
    "ramSpikeTimeScore": 100,  
    "ramSpikeTimePercentageThreshold": 30,  
    "deviceResourcePerformanceScore": 94,  
    "averageSpikeTimeScore": 100,  
    "machineType": "virtual",  
    "cpuDisplayName": "AMD EPYC 7763 64-Core Processor",  
    "totalProcessorCoreCount": 4,  
    "cpuClockSpeedInMHz": 2445,  
    "totalRamInMB": 32716,  
    "diskType": "unknown",  
    "healthStatus": "meetingGoals"  
  },  
]
```





Enhanced Device Timeline

<https://wpninjas.be>
#WPNinjasbe

- Comprehensive Event History for Devices

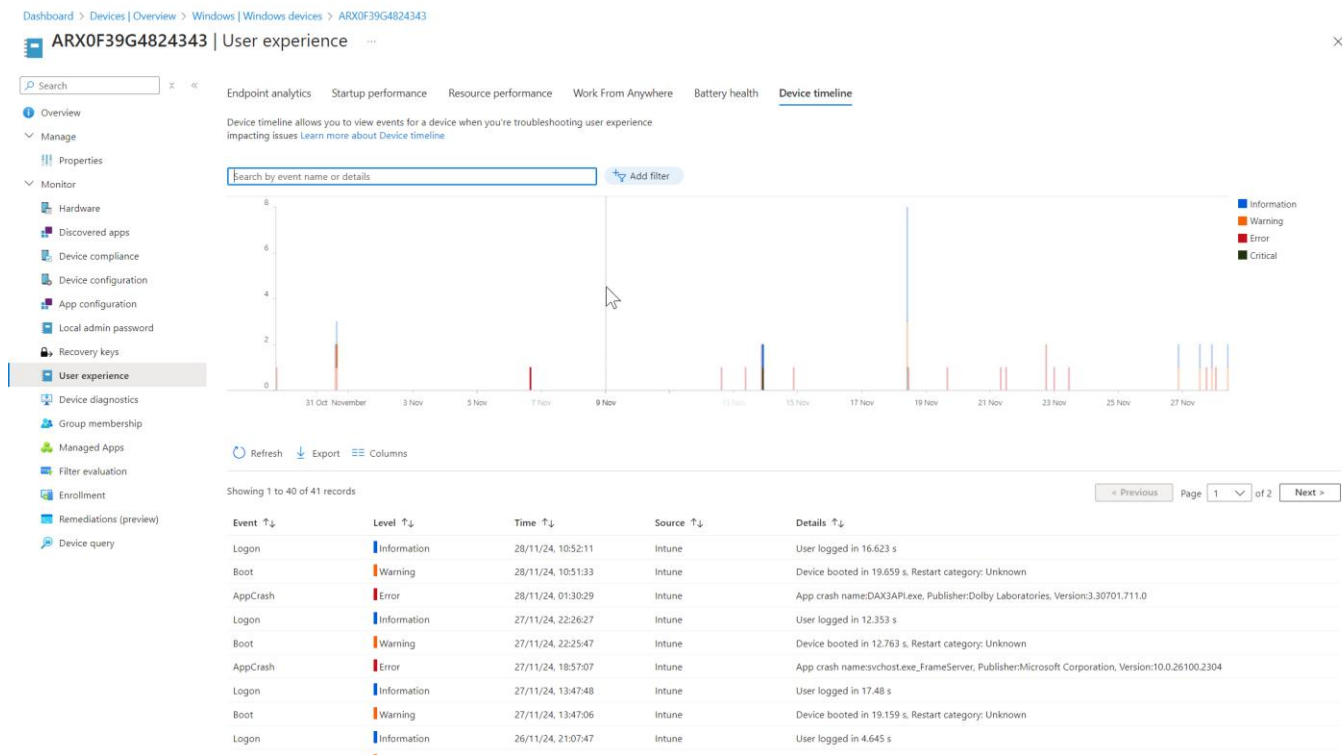
- Application Performance Insights

- Boot up Information

- Logon Information

- Streamlined Troubleshooting Process

- Customizable Filters for Targeted Insight





Enhanced Device Timeline

Home > Reports | Endpoint analytics > Endpoint analytics

Endpoint analytics | Application reliability

Search

Overview

Settings

Reports

- Startup performance
- Application reliability
- Work from anywhere
- Resource performance
- Battery health

App reliability score

App performance

Model performance

Device performance

OS versions performance

Refresh

Export

Columns

Review the app reliability of devices in your tenant. Select a device to view app reliability event details for that device. [Learn more.](#)

Search by device name, manufacturer or model

Device scope : All Devices

< Previous

Page 1 of 5

Next >

Add filter

Device name	Model	Manufacturer	Device app reliability score	Total app crashes (14 days)	Mean time to app failure	Health status
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	4	23	3 hours, 3 minutes	Needs attention
Surface Laptop 5	Surface Laptop 5	Microsoft Corporation	8	24	2 hours, 35 minutes	Needs attention
Surface Laptop 5	Surface Laptop 5	Microsoft Corporation	15	18	2 hours, 57 minutes	Needs attention
Latitude 5520	Latitude 5520	Dell Inc.	20	10	5 hours, 26 minutes	Needs attention
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	22	8	8 hours, 56 minutes	Needs attention
Cloud PC Enterprise 8vCPU/32GB/512GB	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	38	4	13 hours, 32 minutes	Meeting goals
82Y4	82Y4	LENOVO	39	3	10 hours, 51 minutes	Meeting goals
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	40	3	11 hours, 54 minutes	Meeting goals
21K5CT01WW	21K5CT01WW	LENOVO	43	3	14 hours, 47 minutes	Meeting goals
Latitude 5550	Latitude 5550	Dell Inc.	47	1	11 hours, 50 minutes	Meeting goals
Latitude 5520	Latitude 5520	Dell Inc.	50	0	No crash events	Meeting goals
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	50	1	19 hours, 45 minutes	Meeting goals
Surface Laptop Studio 2	Surface Laptop Studio 2	Microsoft Corporation	51	4	19 hours, 31 minutes	Meeting goals
Latitude 5540	Latitude 5540	Dell Inc.	51	1	22 hours, 3 minutes	Meeting goals
Surface Laptop 5	Surface Laptop 5	Microsoft Corporation	52	3	20 hours, 13 minutes	Meeting goals
Surface Laptop 5	Surface Laptop 5	Microsoft Corporation	52	1	23 hours, 16 minutes	Meeting goals
Latitude 5550	Latitude 5550	Dell Inc.	52	4	20 hours, 19 minutes	Meeting goals
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	52	2	21 hours, 44 minutes	Meeting goals
Microsoft Surface Laptop, 7th Edition	Microsoft Surface Laptop, 7th Edition	Microsoft Corporation	57	2	27 hours, 14 minutes	Meeting goals
Latitude 5540	Latitude 5540	Dell Inc.	57	2	27 hours, 19 minutes	Meeting goals
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	58	1	34 hours, 7 minutes	Meeting goals
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	59	2	29 hours, 6 minutes	Meeting goals
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	60	2	29 hours, 56 minutes	Meeting goals
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	61	2	30 hours, 25 minutes	Meeting goals
Surface Laptop 5	Surface Laptop 5	Microsoft Corporation	62	1	39 hours, 15 minutes	Meeting goals
Surface Laptop 5	Surface Laptop 5	Microsoft Corporation	63	1	39 hours, 50 minutes	Meeting goals
Surface Laptop 4	Surface Laptop 4	Microsoft Corporation	64	1	40 hours, 27 minutes	Meeting goals





Enhanced Device Timeline

Home > Reports | Endpoint analytics > Endpoint analytics

Endpoint analytics | Application reliability

Search

Overview

Settings

Reports

Startup performance

Application reliability

Work from anywhere

Resource performance

Battery health

App reliability score

App performance

Model performance

Device performance

OS versions performance

Review the reliability of applications within your tenant. Select an application to drill down to the version level. [Learn more.](#)

Refresh

Export

Columns

Search by application name or publisher

Device scope: All Devices

< PreviousPage 1 of 2Next >

Showing 1 to 40 of 79 records

Add filter

App name	App publisher	Active devices (14 days)	App reliability score	Total usage duration (14 days)	Total crashes (14 days)	Mean time to failure
csc_ui.exe	Cisco Systems, Inc.	101	41	9 hours, 19 minutes	42	13 minutes
firefox.exe	Mozilla Corporation	65	85	925 hours, 16 minutes	18	51 hours, 24 minutes
RemoteDesktopManager.exe	Devolutions inc.	64	47	175 hours, 55 minutes	10	17 hours, 35 minutes
PBIDesktop.exe	Microsoft Corporation	10	40	13 hours, 36 minutes	7	1 hour, 56 minutes
chrome.exe	Google LLC	96	100	1352 hours, 44 minutes	6	225 hours, 27 minutes
EXCELEXE	Microsoft Corporation	133	83	249 hours, 57 minutes	5	49 hours, 59 minutes
WindowsTerminal.exe	Microsoft Corporation	73	32	40 hours, 33 minutes	5	8 hours, 6 minutes
OUTLOOK.EXE	Microsoft Corporation	102	100	669 hours, 21 minutes	4	167 hours, 20 minutes
Widgets.exe	Microsoft Corporation	62	50	18 minutes	4	4 minutes
Windows365.exe	Microsoft Corporation	11	50	7 minutes	4	1 minute
ms-teams.exe	Microsoft Corporation	172	43	10 hours, 36 minutes	3	3 hours, 32 minutes
msedge.exe	Microsoft Corporation	126	100	1535 hours, 12 minutes	3	511 hours, 44 minutes
msedgewebview2.exe	Microsoft Corporation	176	100	1449 hours, 57 minutes	3	483 hours, 19 minutes
notepad++ .exe	Don HO don.h@free.fr	42	40	33 hours, 58 minutes	3	11 hours, 19 minutes
1Password.exe	1Password	8	49	47 minutes	2	23 minutes
Acrobat.exe	Adobe Systems Incorporated	21	46	6 hours, 16 minutes	2	3 hours, 8 minutes
ONENOTE.EXE	Microsoft Corporation	79	100	141 hours, 15 minutes	2	70 hours, 37 minutes
WINWORD.EXE	Microsoft Corporation	91	100	152 hours, 59 minutes	2	76 hours, 29 minutes
LogonUI.exe		179	100	81 hours, 11 minutes	1	81 hours, 11 minutes
ManicTimeClient.exe	Finkit d.o.o.	128	100	149 hours, 14 minutes	1	149 hours, 14 minutes
OneDrive.exe	Microsoft Corporation	121	49	2 hours, 8 minutes	1	2 hours, 8 minutes
ShellHost.exe		92	48	3 hours, 38 minutes	1	3 hours, 38 minutes
SnippingTool.exe	Microsoft Corporation	99	48	3 hours, 24 minutes	1	3 hours, 24 minutes
WhatsApp.exe		29	46	9 hours, 59 minutes	1	9 hours, 59 minutes
conhost.exe		21	49	2 hours, 3 minutes	1	2 hours, 3 minutes
olk.exe	Microsoft Corporation	80	47	6 hours, 11 minutes	1	6 hours, 11 minutes
powershell.exe	Microsoft Corporation	17	49	2 hours, 10 minutes	1	2 hours, 10 minutes





Enhanced Device Timeline Graph Api

<https://wpninja.be>
#WPNinjasbe

- <https://graph.microsoft.com/beta/deviceManagement/userExperienceAnalyticsDeviceTimelineEvent/{userExperienceAnalyticsDeviceTimelineEventId}>

```
{
  "id": "2aa48423-0084-4626-8634-05c5b33dd39c",
  "deviceId": "bd2f1384-66e4-4790-9bb6-48000f3df1e3",
  "eventDateTime": "2025-01-21T08:51:16Z",
  "eventLevel": "information",
  "eventSource": "Intune",
  "eventName": "Boot",
  "eventDetails": "Device booted in 19.707 s, Restart category: RestartWithoutUpdate"
},
{
  "id": "46bc88f4-e6c6-4cbf-b84f-fb33cb2daf47",
  "deviceId": "bd2f1384-66e4-4790-9bb6-48000f3df1e3",
  "eventDateTime": "2025-01-20T08:13:21Z",
  "eventLevel": "error",
  "eventSource": "Intune",
  "eventName": "AppCrash",
  "eventDetails": "App crash name:svchost.exe_FrameServer, Publisher:Microsoft Corporation, Version:10.0.26100.2304"
},
{
  "id": "50743585-c605-49d2-a458-24cc7e45b25e",
  "deviceId": "bd2f1384-66e4-4790-9bb6-48000f3df1e3",
  "eventDateTime": "2025-01-19T19:00:18Z",
  "eventLevel": "information",
  "eventSource": "Intune",
  "eventName": "Logon",
  "eventDetails": "User logged in 0.0 s"
}
```

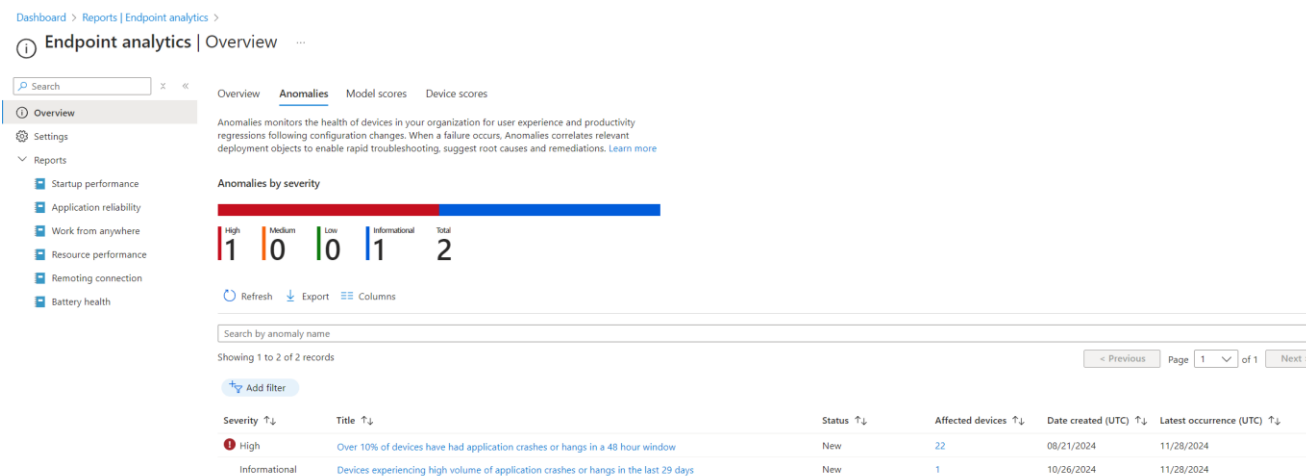




Anomaly Detection

<https://wpninjas.be>
#WPNinjasbe

- Early Warning System for Device Issues
- Proactive Identification of User Experience Regressions
- Correlated Insights for Rapid Troubleshooting





Anomaly Detection MS Graph API

<https://wpnijas.be>
#WPNinjasbe

- <https://graph.microsoft.com/beta/deviceManagement/userExperienceAnalyticsAnomaly>

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/userExperienceAnalyticsAnomaly",
  "@odata.count": 1,
  "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For example: GET deviceManagement/userExperienceAnalyticsAnomaly?$select=anomalyFirstOccurrenceDateTime,anomalyId",
  "value": [
    {
      "id": "dae1842d-dc64-4010-a857-bbd80a8dcca9",
      "anomalyId": "2119838075",
      "anomalyName": "Over 5% of devices have had application crashes or hangs in a 48 hour window",
      "deviceImpactedCount": 10,
      "severity": "medium",
      "state": "new",
      "anomalyType": "device",
      "anomalyFirstOccurrenceDateTime": "2025-01-10T00:00:00Z",
      "anomalyLatestOccurrenceDateTime": "2025-01-22T00:00:00Z",
      "detectionModelId": "1",
      "issueId": "0",
      "assetName": "",
      "assetVersion": "",
      "assetPublisher": ""
    }
  ]
}
```



Create Your own Reports

<https://wpninjas.be>
#WPNinjasbe

- Dashboard
- M365 Subscriptions
- Cloud Custodian
- Reporting
- Advise Center
- Server Management
- Vulnerability Management
- Endpoint Management
- Alerting
- Cloud Voice
- Azure Reservations
- Tenant Configuration
- SSL Certificates
- DNS Management
- VPN
- Customer Management

Intune Device Performance Data

Intune Device Performance Data Details

Intune Windows Update

Intune Application Data

Device Performance Threshold %

70%

Device Model

All

Date

Last

1

Months

10/30/2023 - 11/29/2023



56

Average Score



56

Average Boot Score



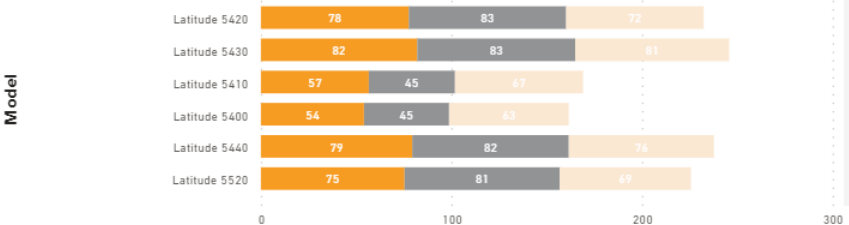
56

Average Login Score

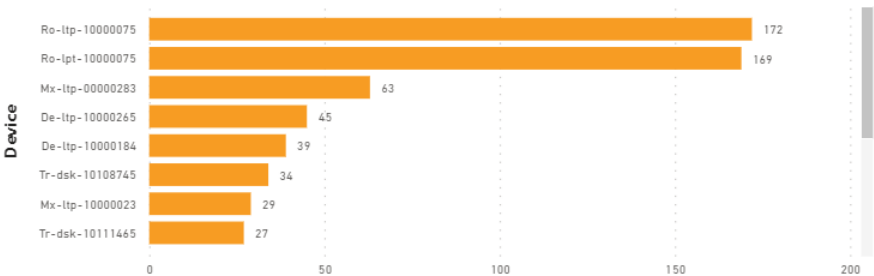


Average device performance per model

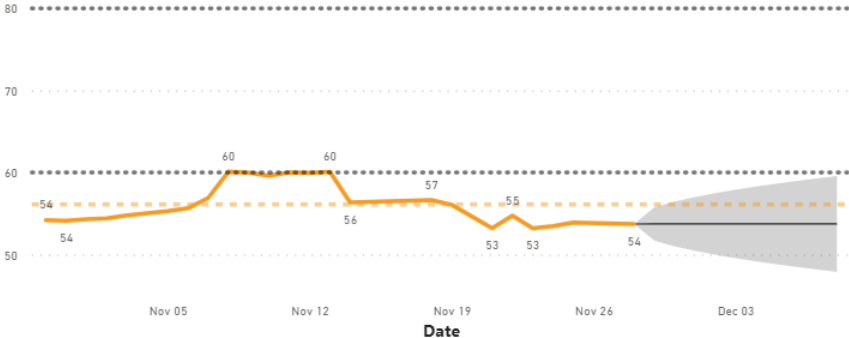
Average Score Average Boot Score Average Login Score



Top 15 most bluescreened devices from: 14-11-2023 until: 28-11-2023



Average score over time



Devices performing 70% under average performance

User Name	Device Name	Model	Average Score	Average Boot Score	Average Login Score	Threshold
	0000011	Latitude E7470	21	31	11	39
	0000013	Latitude 5400	26	43	9	39
	0000021	20FN000PAD	33	43	23	39
	0000022	20N2000CUE	39	29	48	39
	0000025	20FNS0N800	23	45	0	39
	0000026	20HD0013AD	32	49	14	39
	0000034	20N2000CUE	37	31	42	39
	0000044	Latitude 5410	37	18	55	39
	0000060	VivoBook 15_ASUS Laptop X540UB	22	5	40	39
	0000093	XPS 13 7390	31	17	43	39
	0000100	Latitude 5430	28	28	26	39
	0000005	Latitude 5490	23	15	30	39
	0000016	Latitude 5490	27	10	43	39
	0000024	Latitude 5410	28	31	23	39
Total			24	30	18	39





Device Query With Copilot

<https://wpnijas.be>
#WPNinjasbe

- Real-Time Device Information Retrieval
- Powerful Troubleshooting with KQL Integration
- Remote Actions from a Single Interface
- Enhanced Security and Compliance Monitoring

Home > Devices | Windows > Windows | Windows devices > CF-WIN11-02

CF-WIN11-02 | Device query

Properties

Search

Properties list:

- ✓ BiosInfo
- ✓ Certificate
- ✓ Cpu
- ✓ DiskDrive
- ✓ EncryptableVolume
- ✓ FileInfo
- ✓ LocalGroup
- ✓ LocalUserAccount
- ✓ LogicalDrive
- ✓ MemoryInfo
- ✓ OsVersion
- ✓ Process

Run Clear input Cancel Query with Copilot

1 DiskDrive

Get started Results

Columns Device Actions 1 items

DriveId	PartitionCount	DriveIndex	InterfaceType	PnpDeviceId	SizeBytes
\\.\PHYSICALD...	3	0	IDE	SCSI\DISK&VE...	68713989120



slido

Please download and install the Slido app on all computers you use



Who has used Device Query

① Start presenting to display the poll results on this slide.

Show Latest Application Installations

```
WindowsEvent('Application', 30d)  
| where Message contains 'Installation completed successfully'
```

Show Services That Have Started

```
WindowsEvent('Application', 7d)  
| where Message contains 'Service started'
```

Successful User Account Login

```
WindowsEvent('Security', 7d)  
| where tostring(EventId) == '4624'
```

<https://www.kqlsearch.com/devicequery>



slido

Please download and install the Slido app on all computers you use



Who has used it in combination with Copilot

① Start presenting to display the poll results on this slide.



How to use Copilot for Intune – KQL Query – Live Demo

<https://wpninja.be>
#WPNinjasbe

Run

Clear input

Cancel

Qu

1

Get started

Results

Query the properties of this device on demand provided, write custom Kusto Query Language

Prerequisites

To use Device query in your tenant, you must have a device, the device must be enrolled in Endpo

Kusto database

[Learn about the Kusto query language](#)
[Learn more about entities you can query](#)
[Learn common operators for Kusto Query Language](#)

Copilot (preview)

×

Ask a question about this device using device query. Copilot will generate a Kusto Query Language (KQL) to get the data you're looking for.

What OS version is this device running?

Is this device protected by bitlocker?

Show me all active processes

Copilot can make mistakes so remember to verify the results. To help improve the experience, please share your feedback with us.

You can always use the prompt guide for suggestions by selecting this button






How to use Copilot for Intune – Devices – Live Demo


<https://wpninja.be>

#WPNinjasbe

 Copilot (preview) ×

Ready to explore this device? Copilot can provide AI-generated insights to help you troubleshoot.


Copilot can make mistakes so remember to verify the results. To help improve the experience, please share your feedback with us.

You can always use the prompt guide for suggestions by selecting this button 

Microsoft Security Copilot


Prompts to try

| Prompts Promptbooks | Role ▾ Plugin ▾

 **Check impact of an external threat article**
6-prompt sequence


Analyze any external (non MDTI) article, extract indicators, understand the relevant MDTI intelligence available and get hunting queries

➤ Get Started ...

 **Demo**
6-prompt sequence


Collabdays Zagreb

➤ Get Started ... Microsoft Entra

 **Microsoft 365 Defender incident investigation**
7-prompt sequence

Get a report about a specific incident, with related alerts, reputation scores, users, and devices.

➤ Get Started ...

 **Microsoft Sentinel incident investigation**
7-prompt sequence

Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.

➤ Get Started ...

A cartoon illustration of a ninja character in a black suit with a red headband, holding a black sword and a yellow cup.



How to use Copilot for Intune – Policies – Live Demo

<https://wpninja.be>

#WPNinjasbe



Copilot (preview)



Summarize this policy

Policy Summary: V5-IMS-BP-U-Disable new Outlook Admin-Controlled

Policy Settings:

1. Admin-Controlled Migration to New Outlook (User):

- **Description:** This policy controls the ability of IT admins to initiate the migration of users from classic Outlook to new Outlook.

summarize the intune policy V5-IMS-BP-U-Disable new Outlook Admin-Controlled

> 3 steps completed 16 seconds

Jan 29, 2:15 PM

The Intune policy "V5-IMS-BP-U-Disable new Outlook Admin-Controlled" has the following settings:

1. **Admin-Controlled Migration to New Outlook (User):** This setting is disabled. It controls the ability of IT admins to initiate the migration of users from classic Outlook to new Outlook. When disabled, the migration process to new Outlook will be stopped, keeping users on their current version of Outlook without transitioning to new Outlook.
2. **Hide the "Try the new Outlook" toggle in Outlook (User):** This setting is enabled. It controls whether the "Try the new Outlook" toggle is displayed in Outlook. When enabled, the toggle for "Try the new Outlook" will be hidden, and users will not have the ability to switch between the existing and new Outlook experiences.





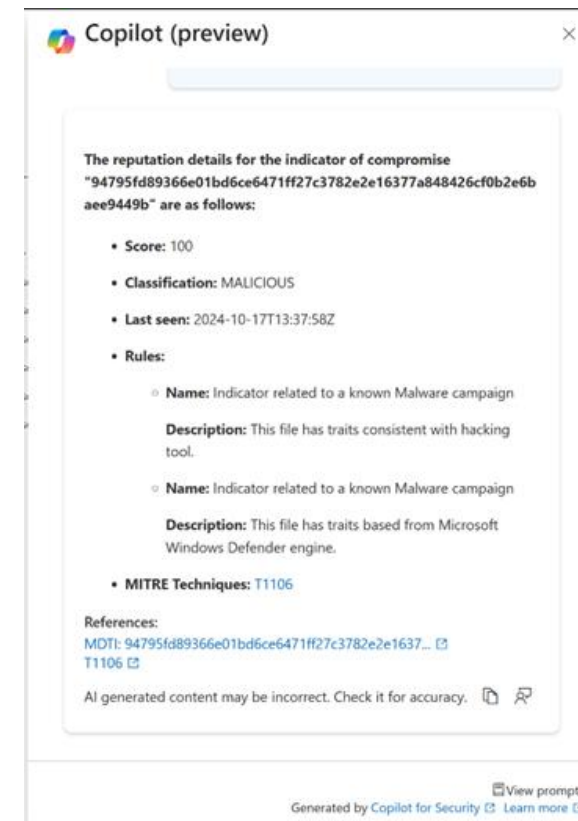
How to use Copilot for Intune – Security Copilot website – Live Demo

<https://wpninja.be>

#WPNinjasbe

<https://securitycopilot.microsoft.com/>

- Can you tell me in which security groups user joery@jocomm.be is?
- Can you tell me which devices belong to joery@jocomm.be?
- Is the intune setting Allow Hibernate already configured in an intune policy?
- I have conflicting settings in this intune policy V4-IMS-BP-Office Emergency Update, can you tell me in which other policy the conflicting settings are?
- Can you analyze the endpoint privilege manangement approval request for this executable Advanced_IP_Scanner_2.5.4594.1.exe





How to use Copilot for Intune – SCU's

<https://wpninja.be>
#WPNinjasbe

<https://securitycopilot.microsoft.com/>

When your SCU run out of capacity you will get this message. This means that either you need to wait for an hour before you can continue because the SCU usage is calculated on the hour or create more SCU's.



Due to your organization's high usage, Copilot can't respond to requests. Contact a Security Administrator to increase the allowed usage, or try again later. [Learn more](#)

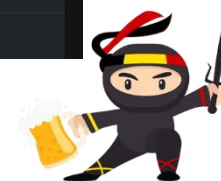
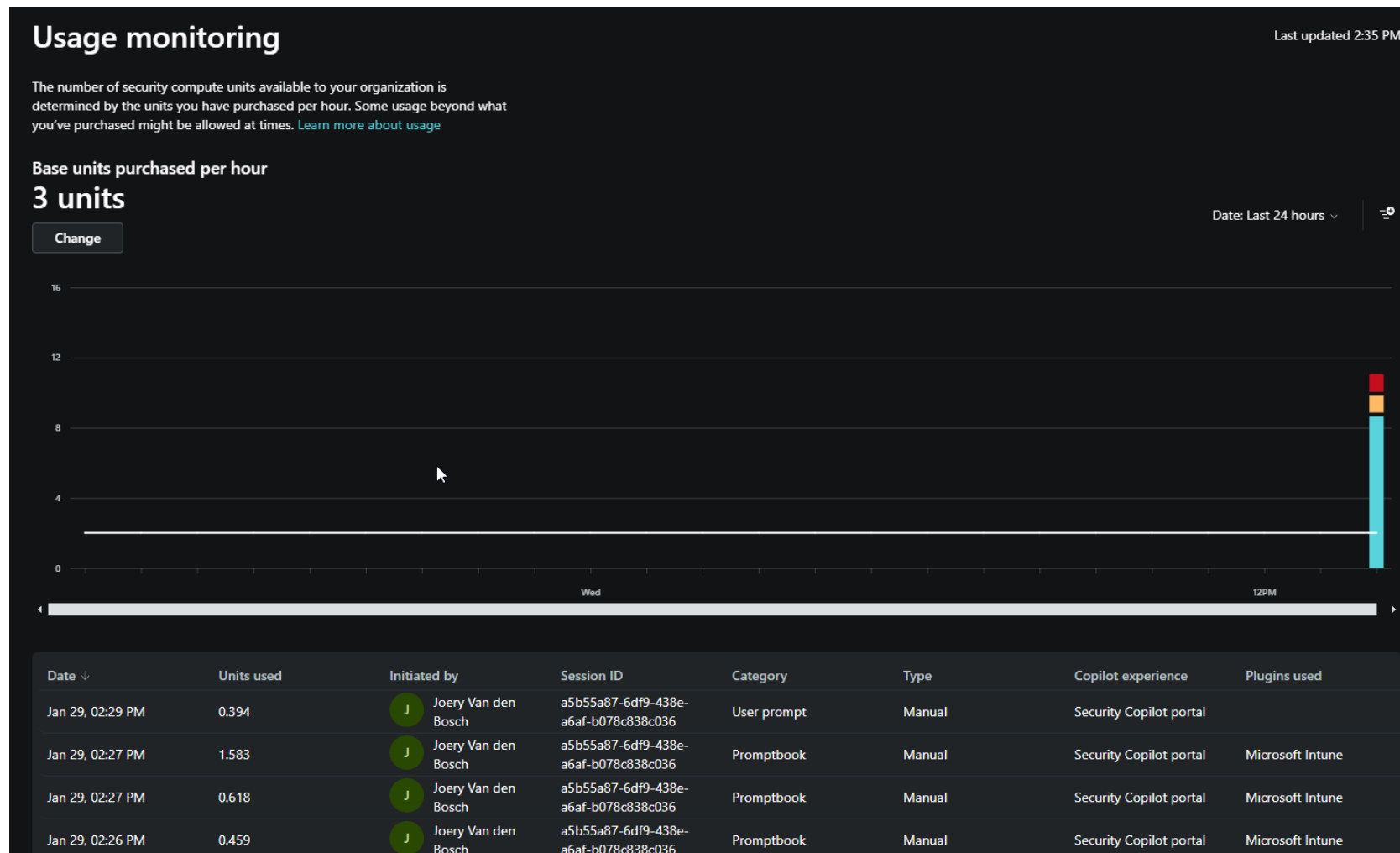




How to use Copilot for Intune – SCU's

<https://wpnijas.be>
#WPNinjasbe

Microsoft has made very good improvements to the overview of cost calculation of the use of the SCU's as you can see now exactly how many units have been used with every prompt.



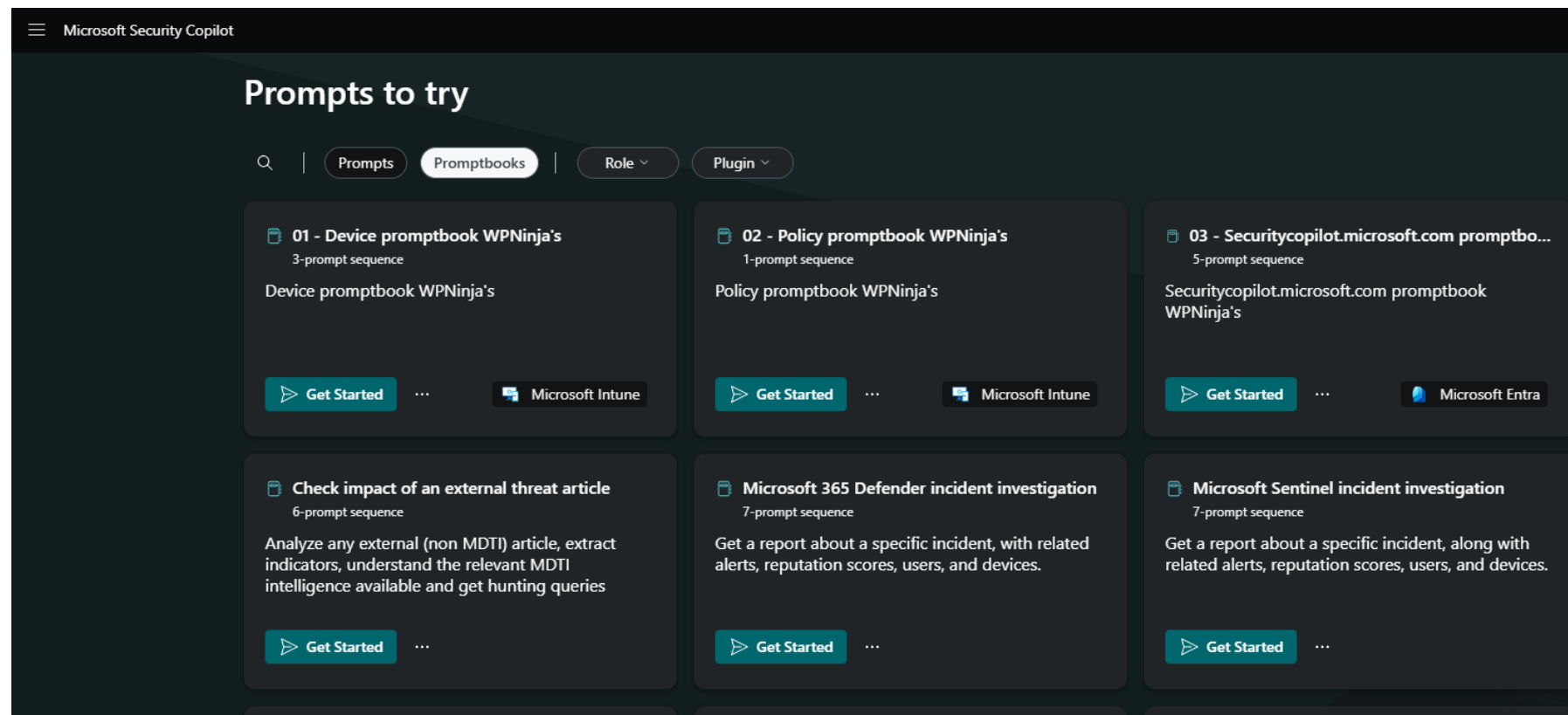


How to use Copilot for Intune – Promptbooks – Live Demo

<https://wpninjas.be>
#WPNinjasbe

<https://securitycopilot.microsoft.com/>

Within copilot for Security you can create promptbooks to combine some prompts you need more often, so you don't need to type in the prompts every single time. Microsoft also has some pre-defined promptbooks for you.



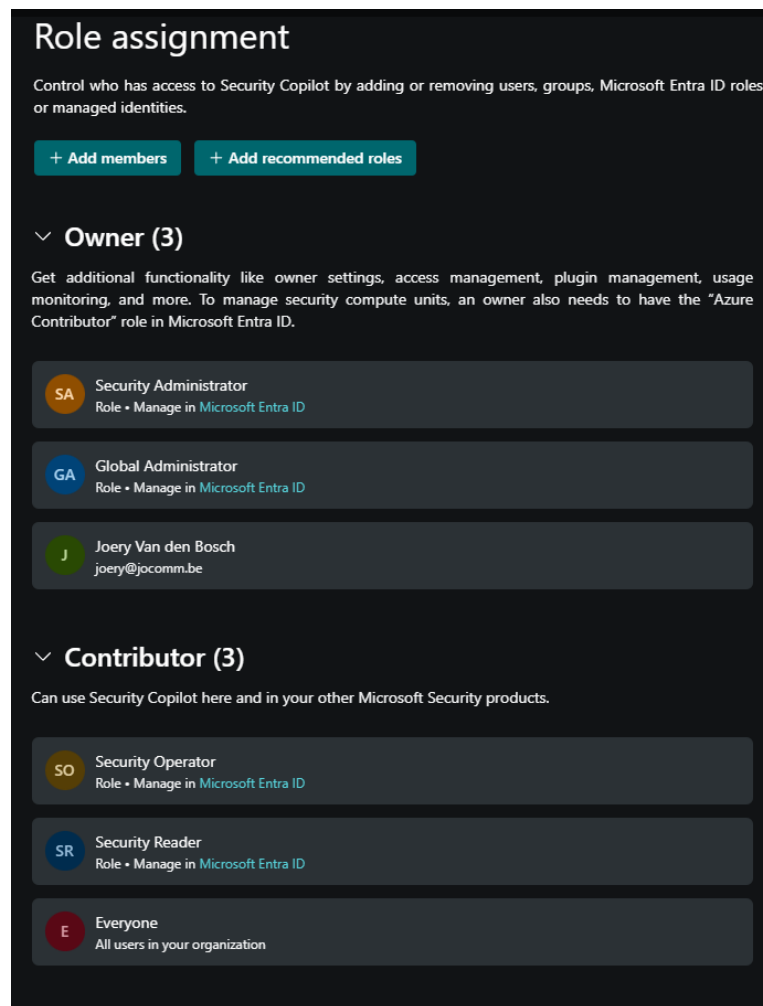
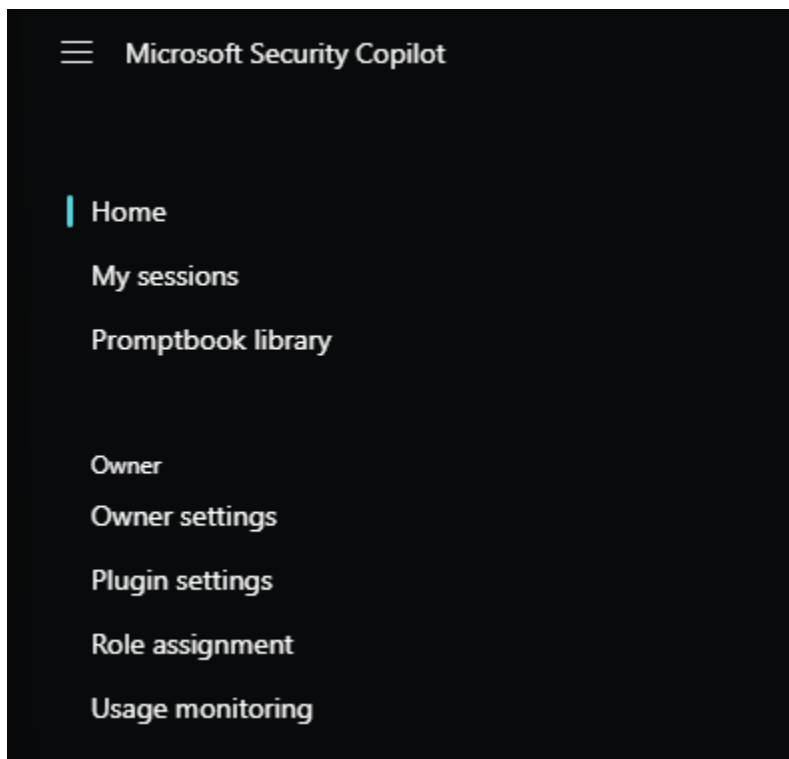


How to use Copilot for Intune – The Settings – Live Demo

<https://wpninja.be>
#WPNinjasbe

<https://securitycopilot.microsoft.com/>

Within copilot for Security there are some settings that you can adjust.



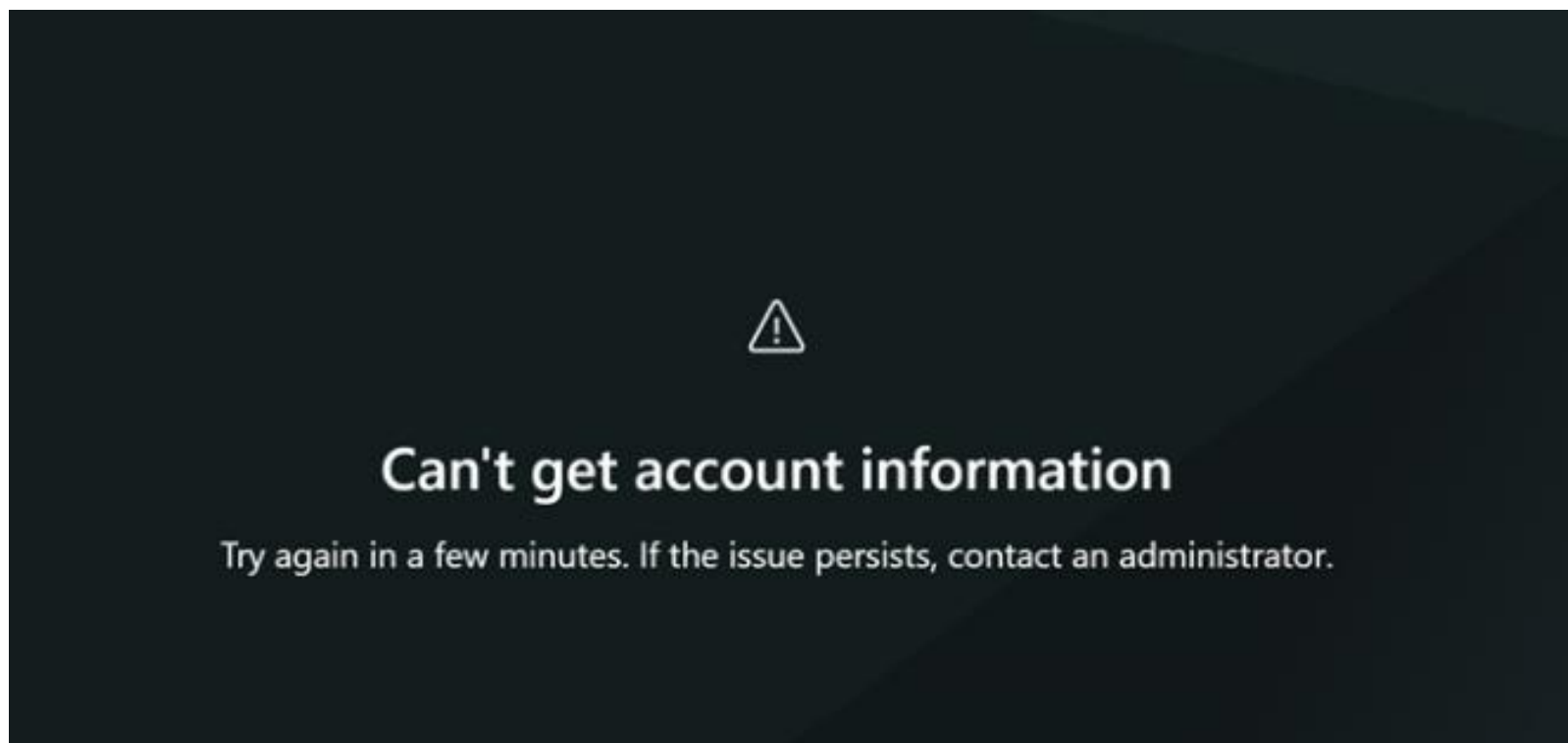


How to use Copilot for Intune – Errors and troubleshooting

<https://wpninja.be>
#WPNinjasbe

I got this error during the setup of Copilot for Security.

<https://securitycopilot.microsoft.com/>





How to use Copilot for Intune – Errors and troubleshooting

<https://wpninja.be>
#WPNinjasbe

<https://securitycopilot.microsoft.com/>

Try rewording your prompt...

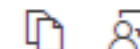
Summarize this policy

SOLVED



Try rewording your prompt and submit it again. If that doesn't work, ask your Copilot for Security owner for troubleshooting help.

Retry





How to use Copilot for Intune – Errors and troubleshooting

<https://wpninja.be>

#WPNinjasbe

<https://securitycopilot.microsoft.com/>

The policy with id ***
could not be found

SOLVED

Summarize this policy

The policy with the ID `8fb7b0da-3cdc-45f0-ac8f-9aebef7c0de0` could not be found. Please ensure that the policy ID is correct and try again.

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





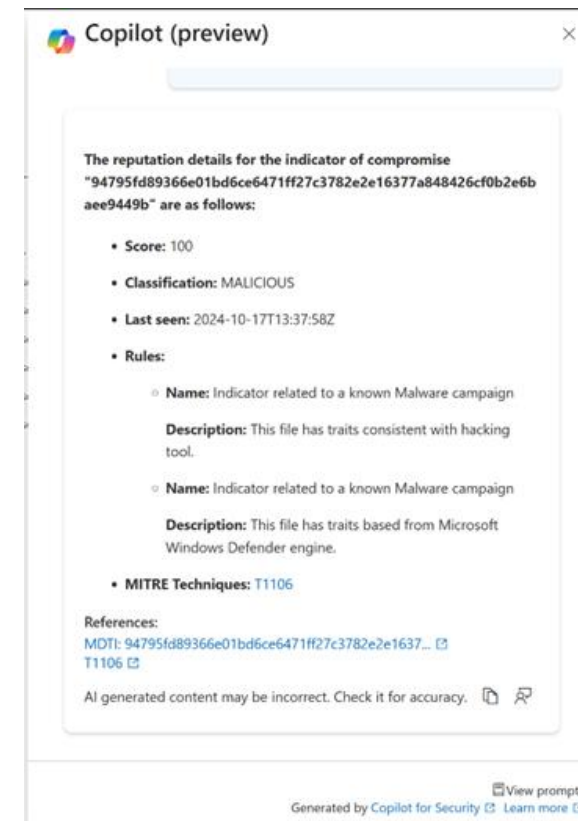
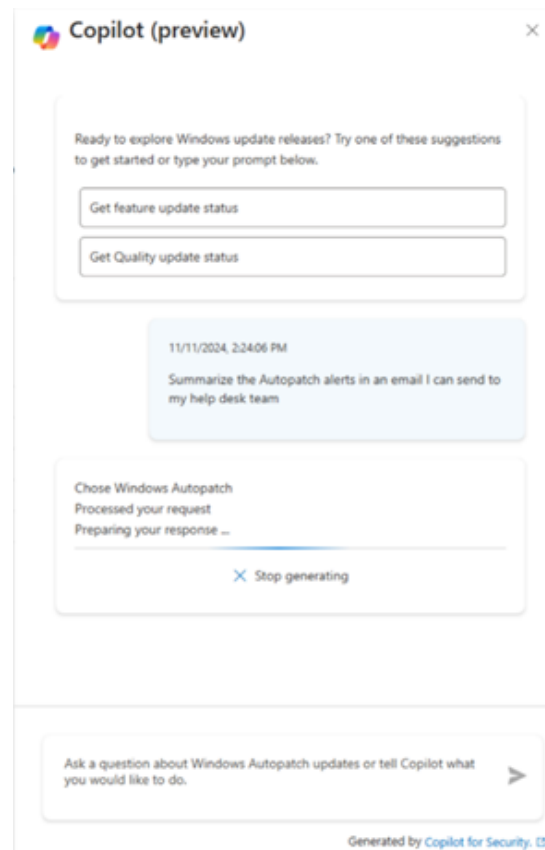
How to use Copilot for Intune – Things to look out for in the future

<https://wpninjas.be>

#WPNinjasbe

<https://securitycopilot.microsoft.com/>

- Strengthen security by reducing your attack surface – analyze an application request in EPM.
- Enhancing policy management with Copilot – has this setting been configured in any other policy?
- Open-prompting experience in Copilot that understands the settings and policies in your environment using a more natural language approach. **GA NOW**
- Streamline updates with Copilot-assisted insights – Copilot for Intune for Autopatch





How to use Copilot for Intune – The Elephant in the room

<https://wpninja.be>
#WPNinjasbe

Microsoft recommends provisioning 3 SCUs per hour to start your Copilot for Security exploration.

Provisioned \$4/hour \$2880/month per SCU





We love your feedback

<https://forms.microsoft.com/e/2MMjWayLXC>



SAVE THE DATE

20/03/2025
Workplace Ninja
User Group Belgium
Meetup #2

Thank You!

