NORDIC
– VIRTUAL SUMMIT –

Unleashing Windows Device Insights with Intune

Petri Paavola – Microsoft MVP – Windows and Intune

Panu Saukko – Microsoft MVP - Intune

Panu Saukko

ProTrainIT Oy

Microsoft Certified Trainer

Intune (20 years!)

@PanuSaukko

@panusaukko.bsky.social

Panu.Saukko@protrainit.fi

Petri Paavola

Microsoft MVP – Windows and Devices

Senior Modern Management Principal

Petri.Paavola@yodamiitti.fi

Microsoft Most Valuable Professional MVP

@petripaavola

https://github.com/petripaavola

Intune.ninja

Powershell.ninja

🦋@Intune.ninja

Skills

- Windows Autopilot + Intune + Intune for Education
- Windows 10&11 Deployment and Management
- Powershell / Graph API
- Traditional on-prem deployment and management
- Consulting
- Training

Over 24 years of work experience

Current:

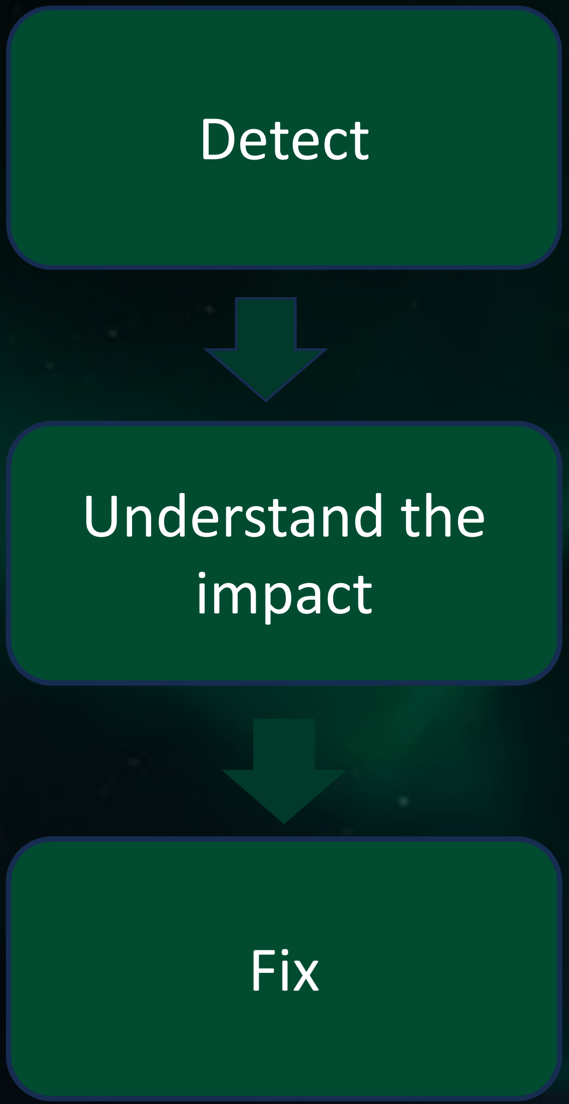
- Yodamiitti Oy / Owner
  Consulting / Training

Past:

- Aalto university / IT-services
  Responsible for Workstation service
  (Windows, macOS and Linux)

YODA MIITTI

Our problem


Detect

Understand the impact

Fix

You found out that there is some issue on one device!

How many devices have the same issue?

?

How do you fix the problem devices on scale?

Different tools
In different phases!

Examine a single device remotely

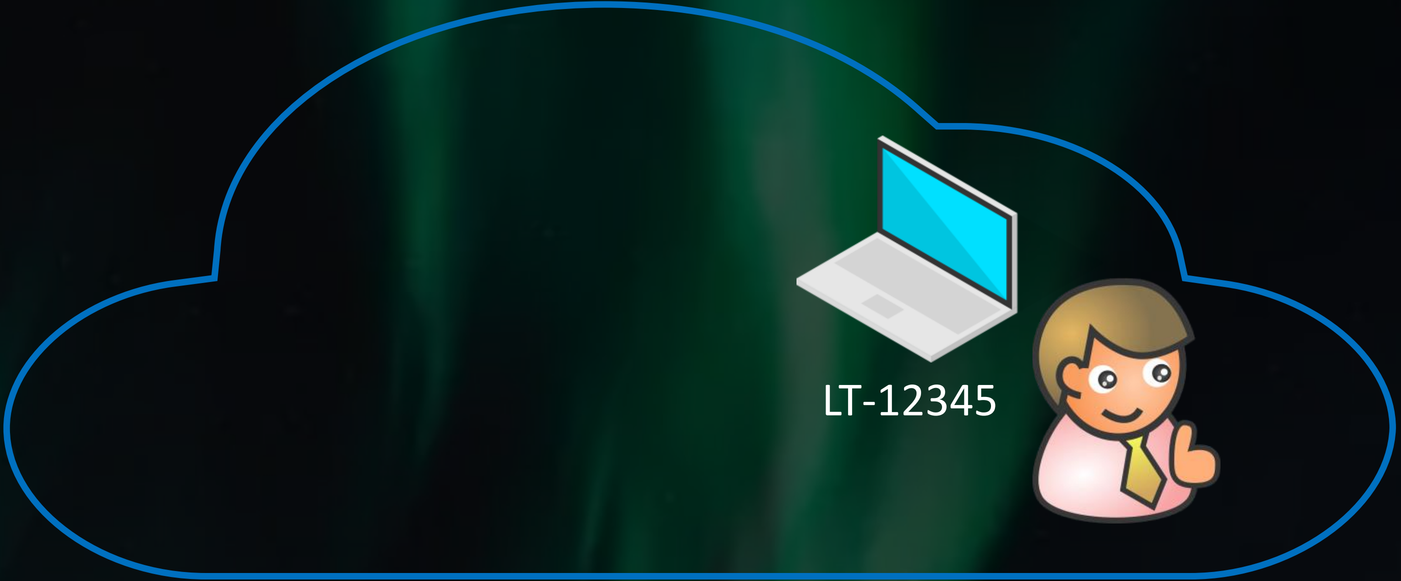
Microsoft Intune admin center

LT-12345

- Hardware
- Resource explorer
- Collect diagnostics
- Remediations
- User experience
- Device query

Advanced analytics/
Intune Suite

~~Remote Desktop Connection~~



NORDIC

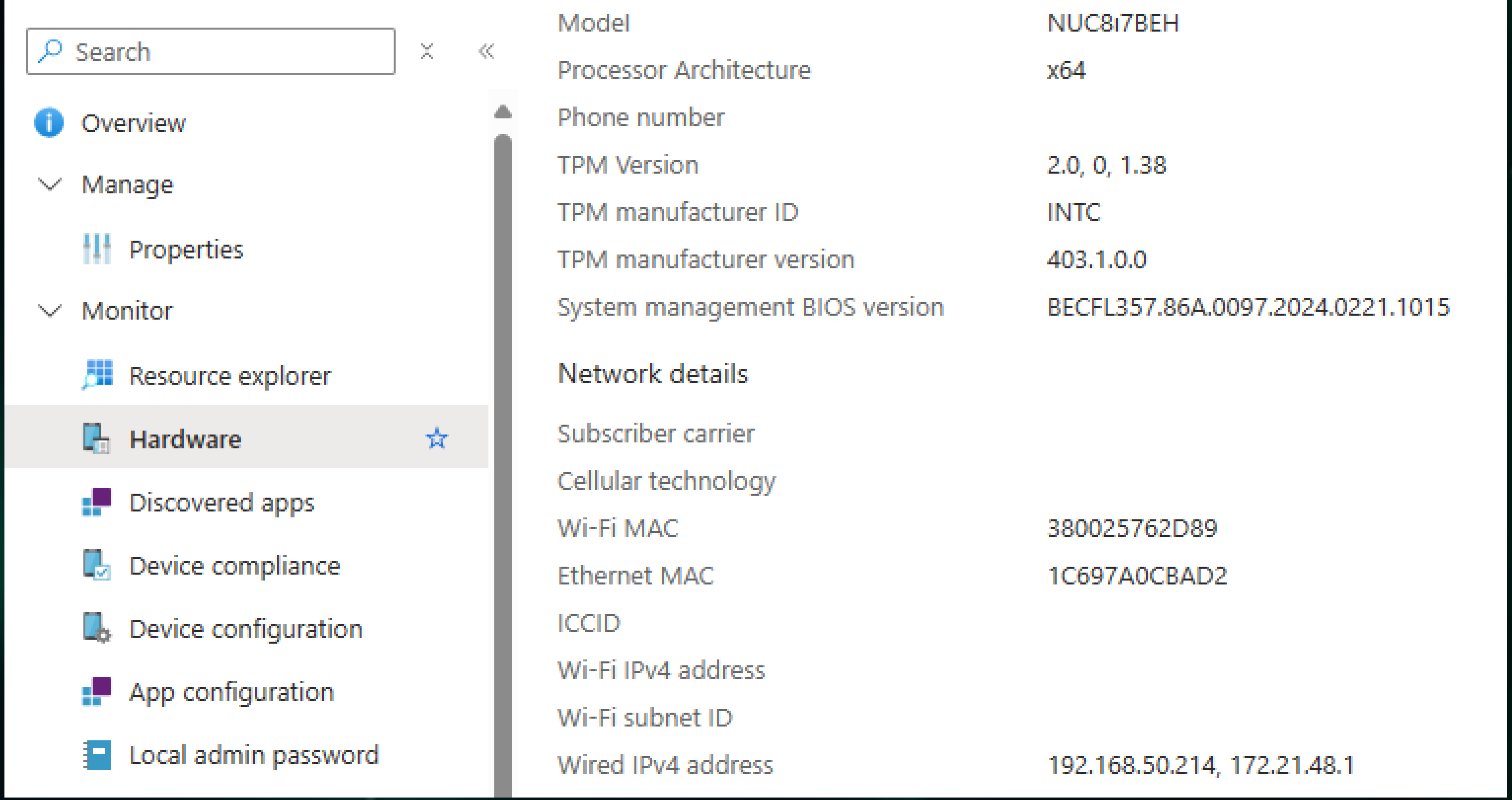
— VIRTUAL SUMMIT —

Demo 1: Single device

Examples

- Find Ethernet MAC address/IP addresses
- Has the device the latest CU?
- When the latest CU has been installed? Windows CU installation times?
- Current IP addresses from registry
- Google Chrome version? Or Google Chrome installed?
- Collect Diagnostics → Analyze Diagnostics dump manually or with scripts

IP/MAC addresses



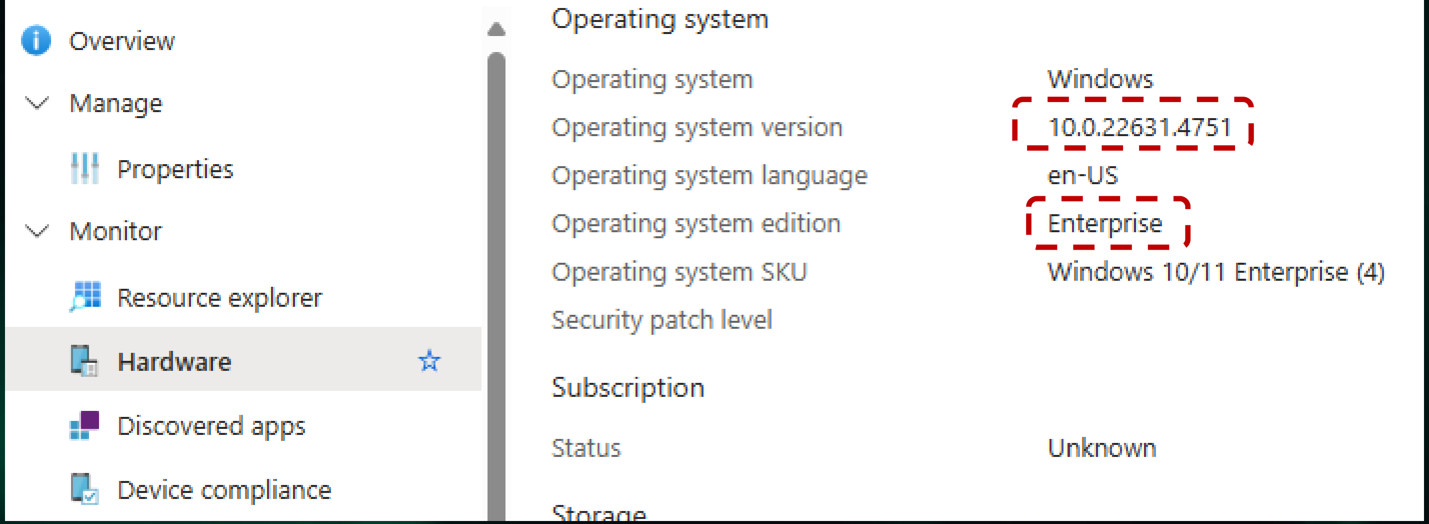
Model	NUC8i7BEH
Processor Architecture	x64
Phone number	
TPM Version	2.0, 0, 1.38
TPM manufacturer ID	INTC
TPM manufacturer version	403.1.0.0
System management BIOS version	BECFL357.86A.0097.2024.0221.1015

Network details

Subscriber carrier	
Cellular technology	
Wi-Fi MAC	380025762D89
Ethernet MAC	1C697A0CBAD2
ICCID	
Wi-Fi IPv4 address	
Wi-Fi subnet ID	
Wired IPv4 address	192.168.50.214, 172.21.48.1

NORDIC
— VIRTUAL SUMMIT —

Latest CU installed



Operating system

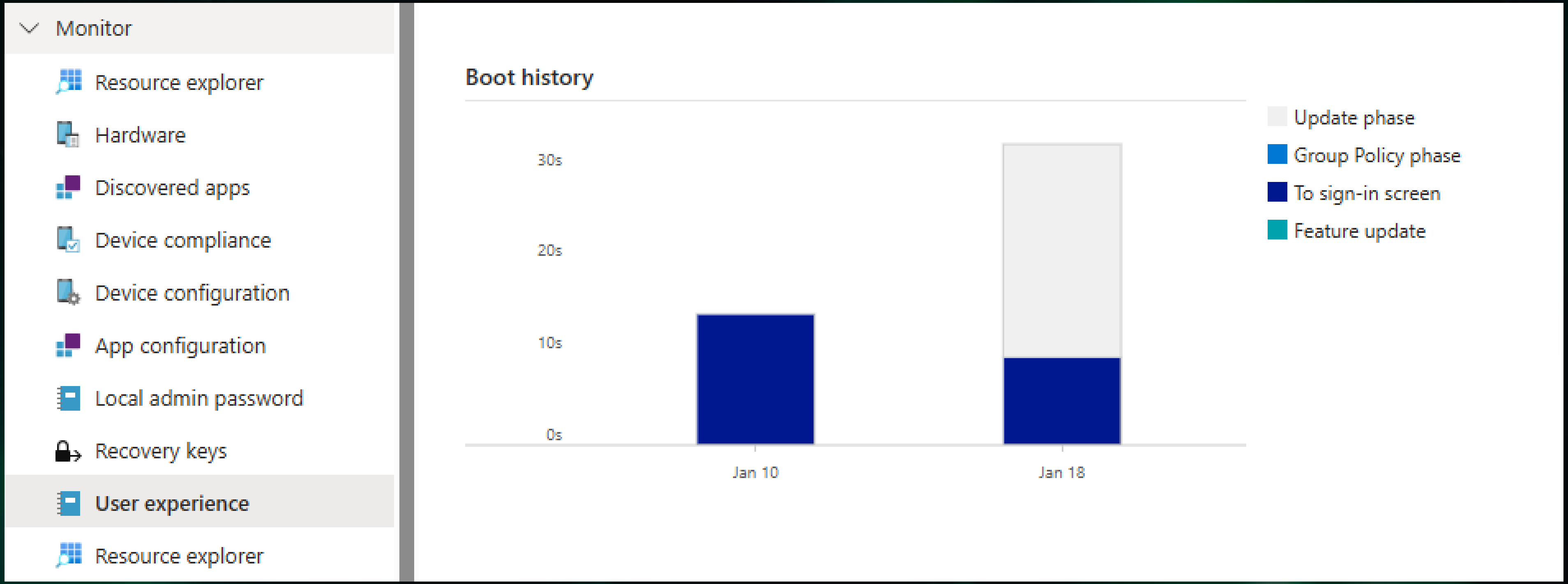
Operating system	Windows
Operating system version	10.0.22631.4751
Operating system language	en-US
Operating system edition	Enterprise
Operating system SKU	Windows 10/11 Enterprise (4)
Security patch level	

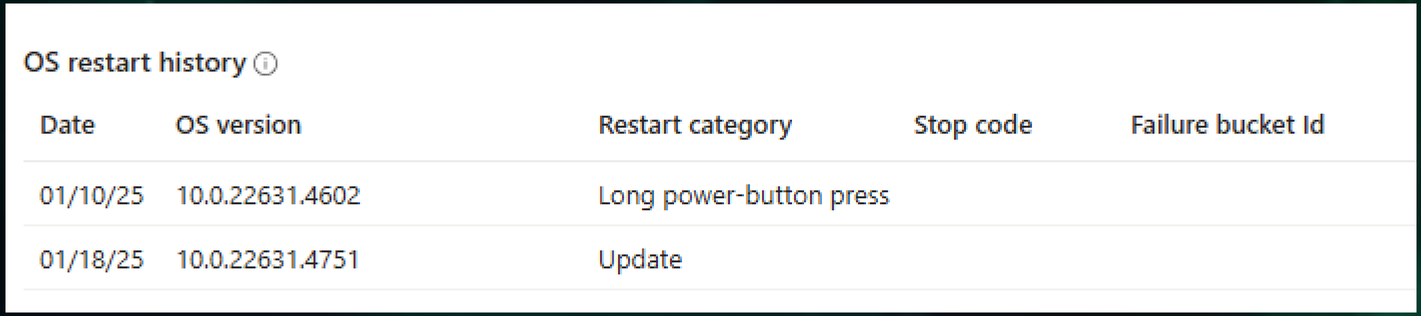
Subscription

Status	Unknown

Storage

When the CU has been installed?

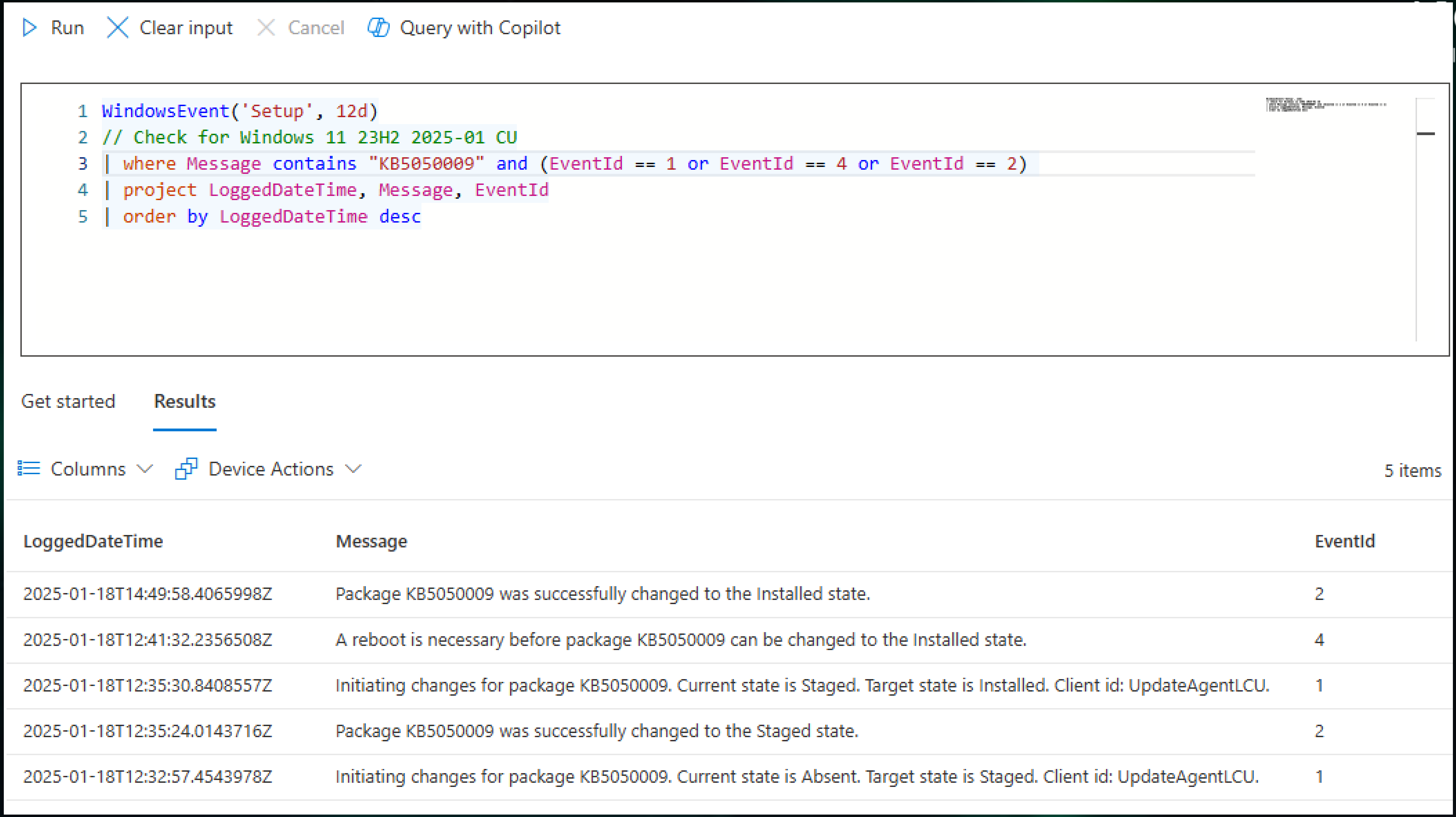




OS restart history ⓘ

Date	OS version	Restart category	Stop code	Failure bucket Id
01/10/25	10.0.22631.4602	Long power-button press		
01/18/25	10.0.22631.4751	Update		

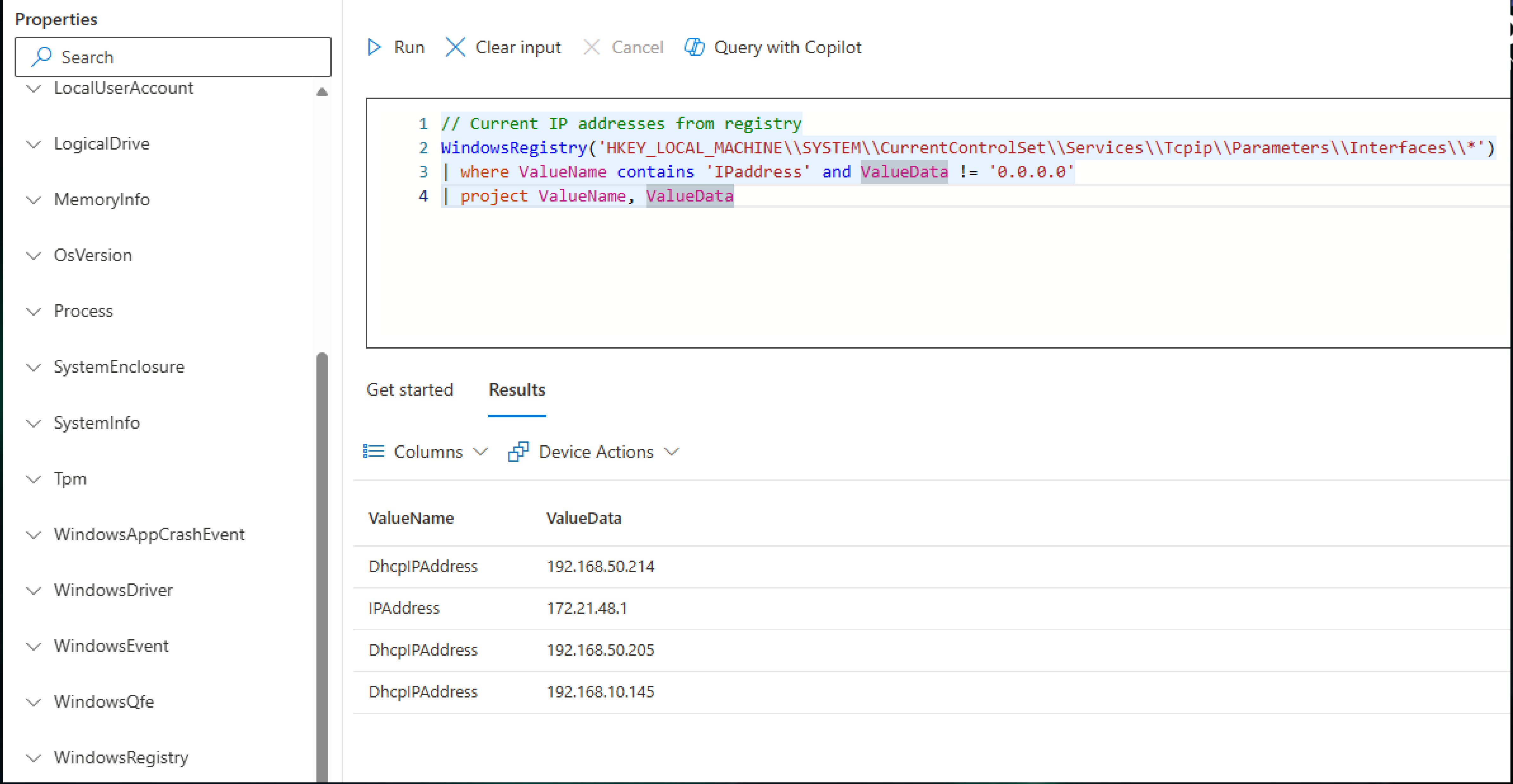
When the CU has been installed?



```
WindowsEvent('Setup', 12d)
// Check for Windows 11 23H2 2025-01 CU
| where Message contains "KB5050009" and (EventId == 1 or EventId == 4 or EventId == 2)
| project LoggedDateTime, Message, EventId
| order by LoggedDateTime desc
```

LoggedDateTime	Message	EventId
2025-01-18T14:49:58.4065998Z	Package KB5050009 was successfully changed to the Installed state.	2
2025-01-18T12:41:32.2356508Z	A reboot is necessary before package KB5050009 can be changed to the Installed state.	4
2025-01-18T12:35:30.8408557Z	Initiating changes for package KB5050009. Current state is Staged. Target state is Installed. Client id: UpdateAgentLCU.	1
2025-01-18T12:35:24.0143716Z	Package KB5050009 was successfully changed to the Staged state.	2
2025-01-18T12:32:57.4543978Z	Initiating changes for package KB5050009. Current state is Absent. Target state is Staged. Client id: UpdateAgentLCU.	1

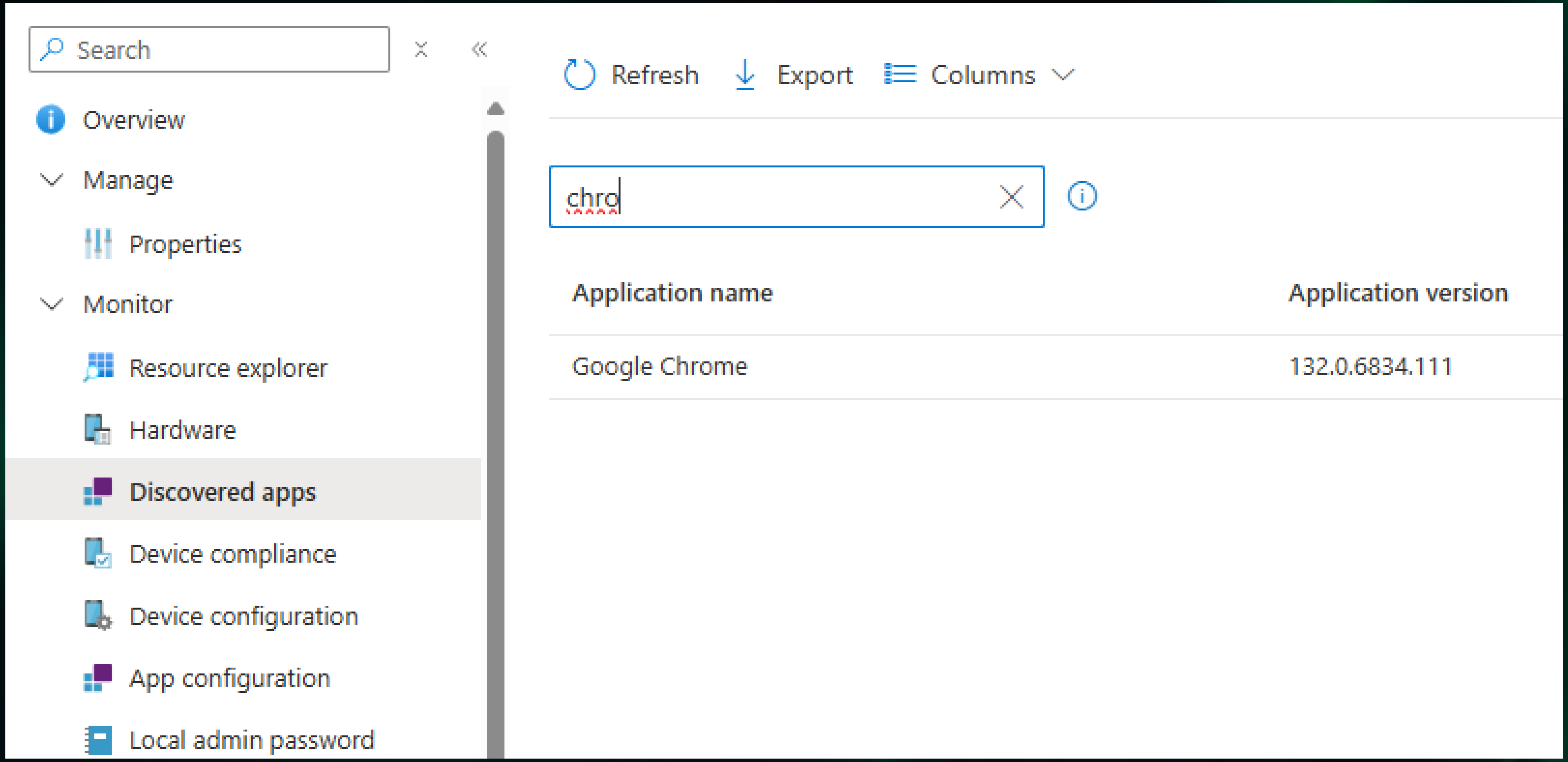
Current IP addresses from registry



```
// Current IP addresses from registry
WindowsRegistry('HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Tcpip\\Parameters\\Interfaces\\*')
| where ValueName contains 'IPaddress' and ValueData != '0.0.0.0'
| project ValueName, ValueData
```

ValueName	ValueData
DhcpIPAddress	192.168.50.214
IPAddress	172.21.48.1
DhcpIPAddress	192.168.50.205
DhcpIPAddress	192.168.10.145

Google Chrome version



Application name	Application version
Google Chrome	132.0.6834.111

NORDIC

— VIRTUAL SUMMIT —

Understanding the Impact

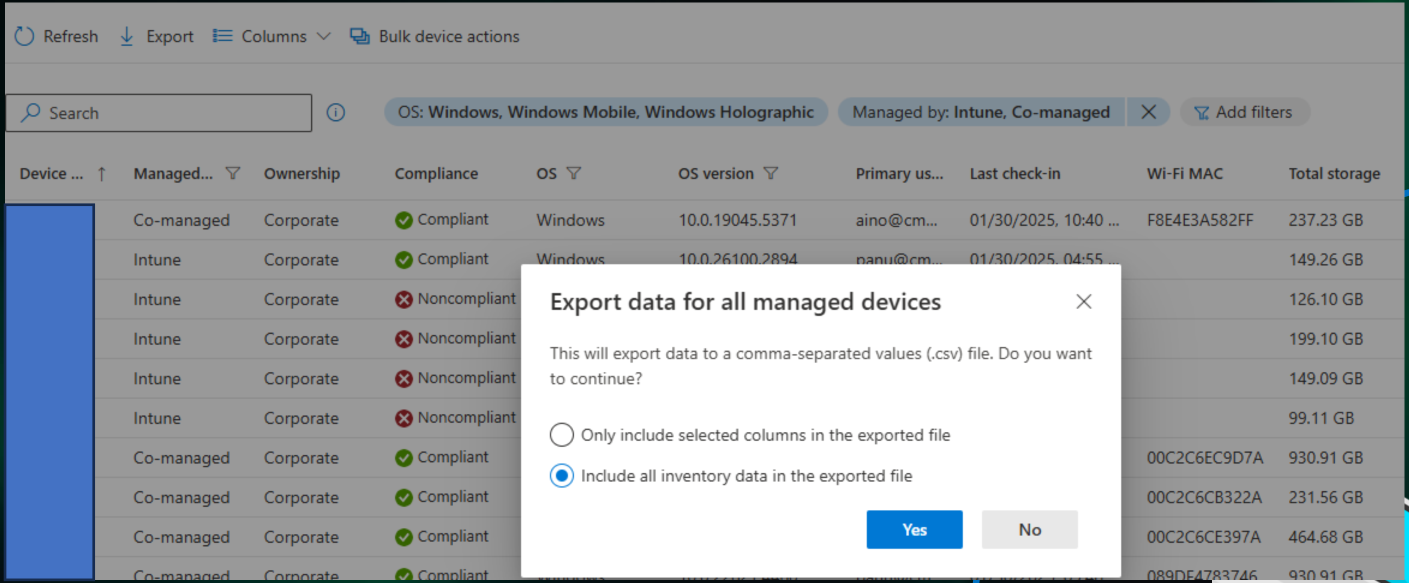
Ways to Assess the Impact

- Can be anything from easy → complex!
- Intune portal
  - Export to CSV → Excel
- Add Intune device information to Log Analytics workspace
  - Run KQL queries
- Multi-device query
  - In development
  - Part of Intune Suite's Advanced analytics
- Remediations

Assess the Impact: Export to CSV → Excel

NORDIC
— VIRTUAL SUMMIT —

Microsoft Intune admin center



OS: Windows, Windows Mobile, Windows Holographic

Managed by: Intune, Co-managed

Device ...	Managed...	Ownership	Compliance	OS	OS version	Primary us...	Last check-in	Wi-Fi MAC	Total storage
[redacted]	Co-managed	Corporate	✓ Compliant	Windows	10.0.19045.5371	aino@cm...	01/30/2025, 10:40 ...	F8E4E3A582FF	237.23 GB
[redacted]	Intune	Corporate	✓ Compliant	Windows	10.0.26100.2894	panu@cm...	01/30/2025, 04:55 ...		149.26 GB
[redacted]	Intune	Corporate	✗ Noncompliant						126.10 GB
[redacted]	Intune	Corporate	✗ Noncompliant						199.10 GB
[redacted]	Intune	Corporate	✗ Noncompliant						149.09 GB
[redacted]	Intune	Corporate	✗ Noncompliant						99.11 GB
[redacted]	Co-managed	Corporate	✓ Compliant					00C2C6EC9D7A	930.91 GB
[redacted]	Co-managed	Corporate	✓ Compliant					00C2C6CB322A	231.56 GB
[redacted]	Co-managed	Corporate	✓ Compliant					00C2C6CE397A	464.68 GB
[redacted]	Co-managed	Corporate	✓ Compliant					089DF4783746	930.91 GB

Export data for all managed devices

This will export data to a comma-separated values (.csv) file. Do you want to continue?

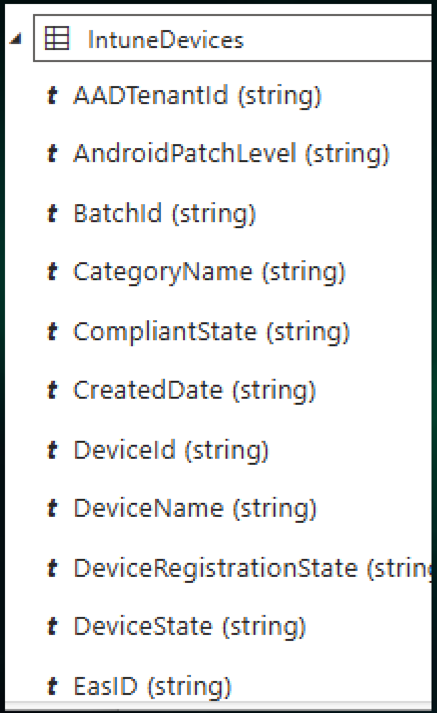
○ Only include selected columns in the exported file

● Include all inventory data in the exported file

Yes No

KQL enabled data sources

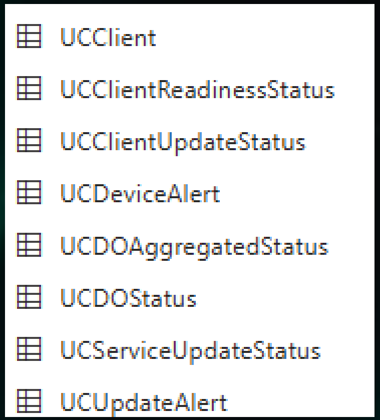
Log analytics workspace
With Intune integration



- IntuneDevices
  - AADTenantId (string)
  - AndroidPatchLevel (string)
  - BatchId (string)
  - CategoryName (string)
  - CompliantState (string)
  - CreatedDate (string)
  - DeviceId (string)
  - DeviceName (string)
  - DeviceRegistrationState (strin
  - DeviceState (string)
  - EasID (string)

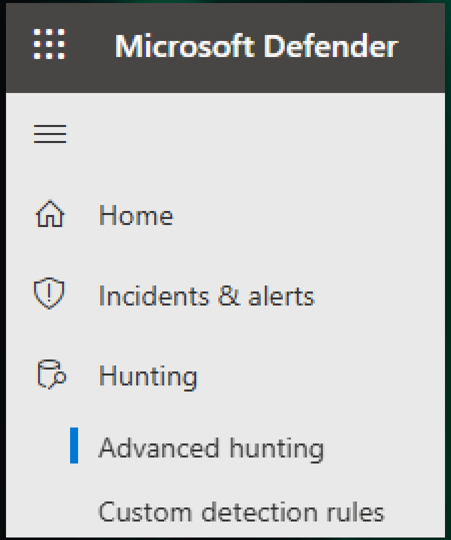
~Intune “classic” hw inventory

Log analytics workspace
With WUfB Reports
https://aka.ms/wufbreports



- UCClient
- UCClientReadinessStatus
- UCClientUpdateStatus
- UCDeviceAlert
- UCDOAggregatedStatus
- UCDOStatus
- UCServiceUpdateStatus
- UCUpdateAlert

Microsoft Defender for Endpoint
Advanced hunting

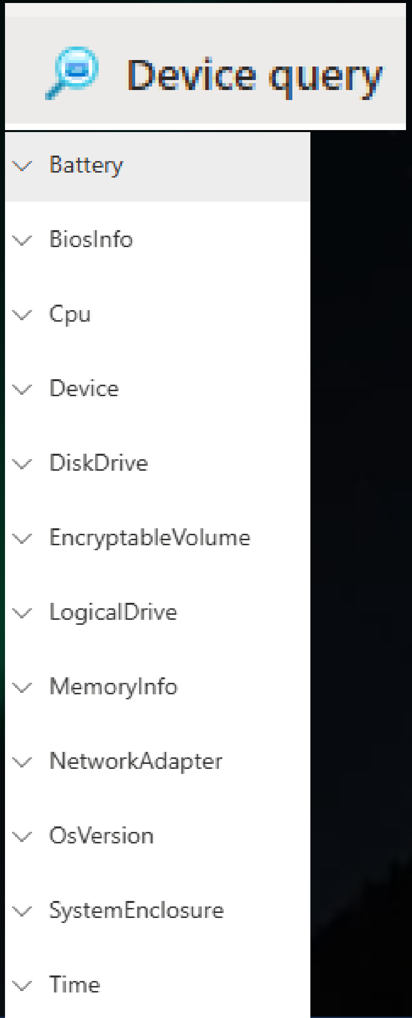


Microsoft Defender

- Home
- Incidents & alerts
- Hunting
  - Advanced hunting
  - Custom detection rules

A lot of data!!!!

Intune Suite
Advanced analytics

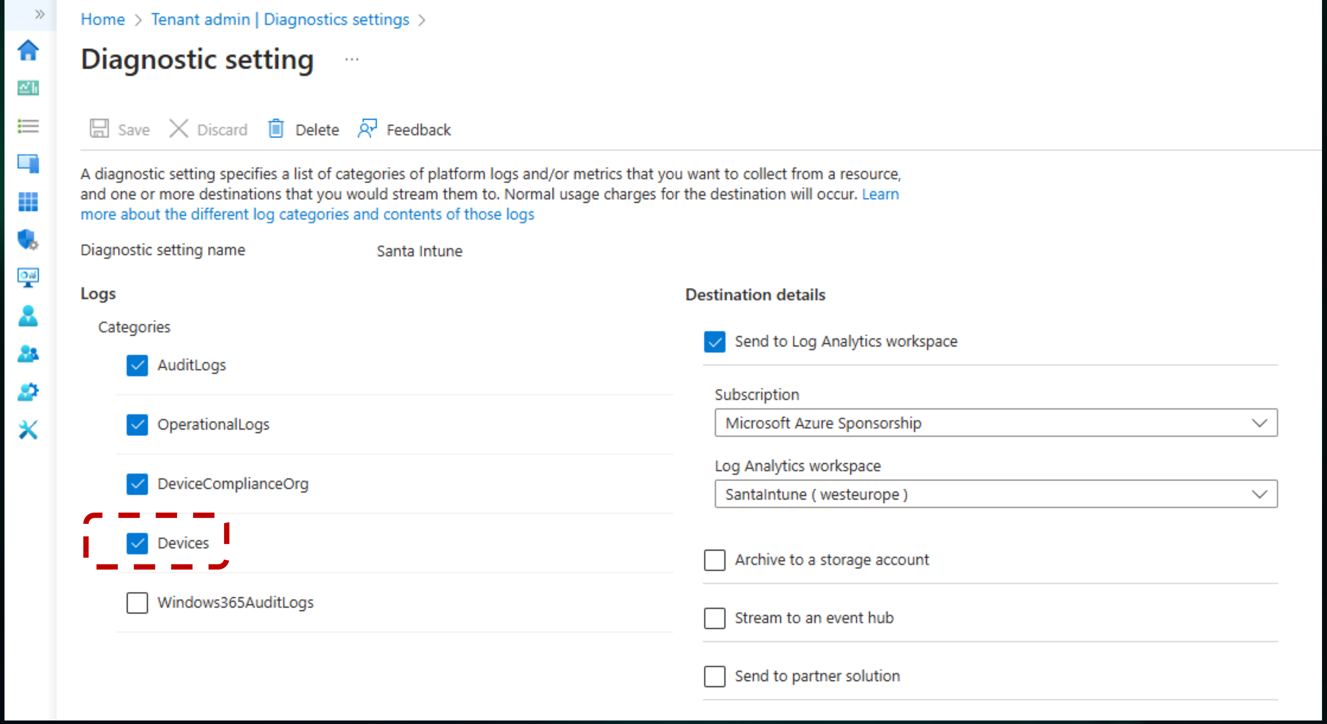


Device query

- Battery
- BiosInfo
- Cpu
- Device
- DiskDrive
- EncryptableVolume
- LogicalDrive
- MemoryInfo
- NetworkAdapter
- OsVersion
- SystemEnclosure
- Time

Intune Device info to Log Analytics

- Very useful and not expensive
- Need to have Azure subscription and Log Analytics workspace
- Not all Intune inventory info replicated to Log Analytics



Home > Tenant admin | Diagnostics settings >

Diagnostic setting

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name: Santa Intune

Logs

Categories

- ☑ AuditLogs
- ☑ OperationalLogs
- ☑ DeviceComplianceOrg
- ☑ Devices
- ☐ Windows365AuditLogs

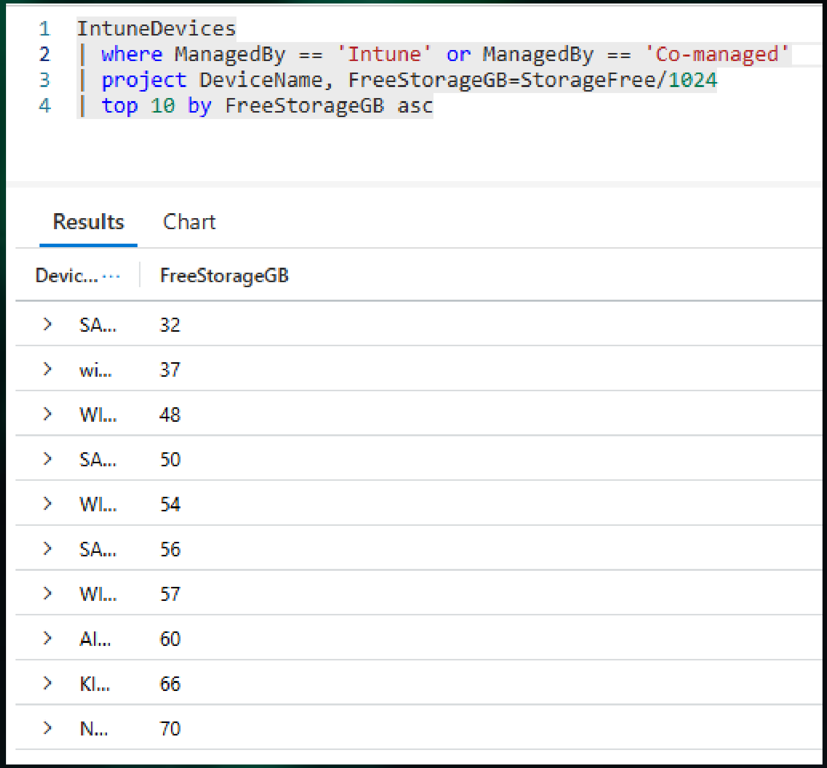
Destination details

- ☑ Send to Log Analytics workspace

Subscription: Microsoft Azure Sponsorship

Log Analytics workspace: SantaIntune (westeurope)

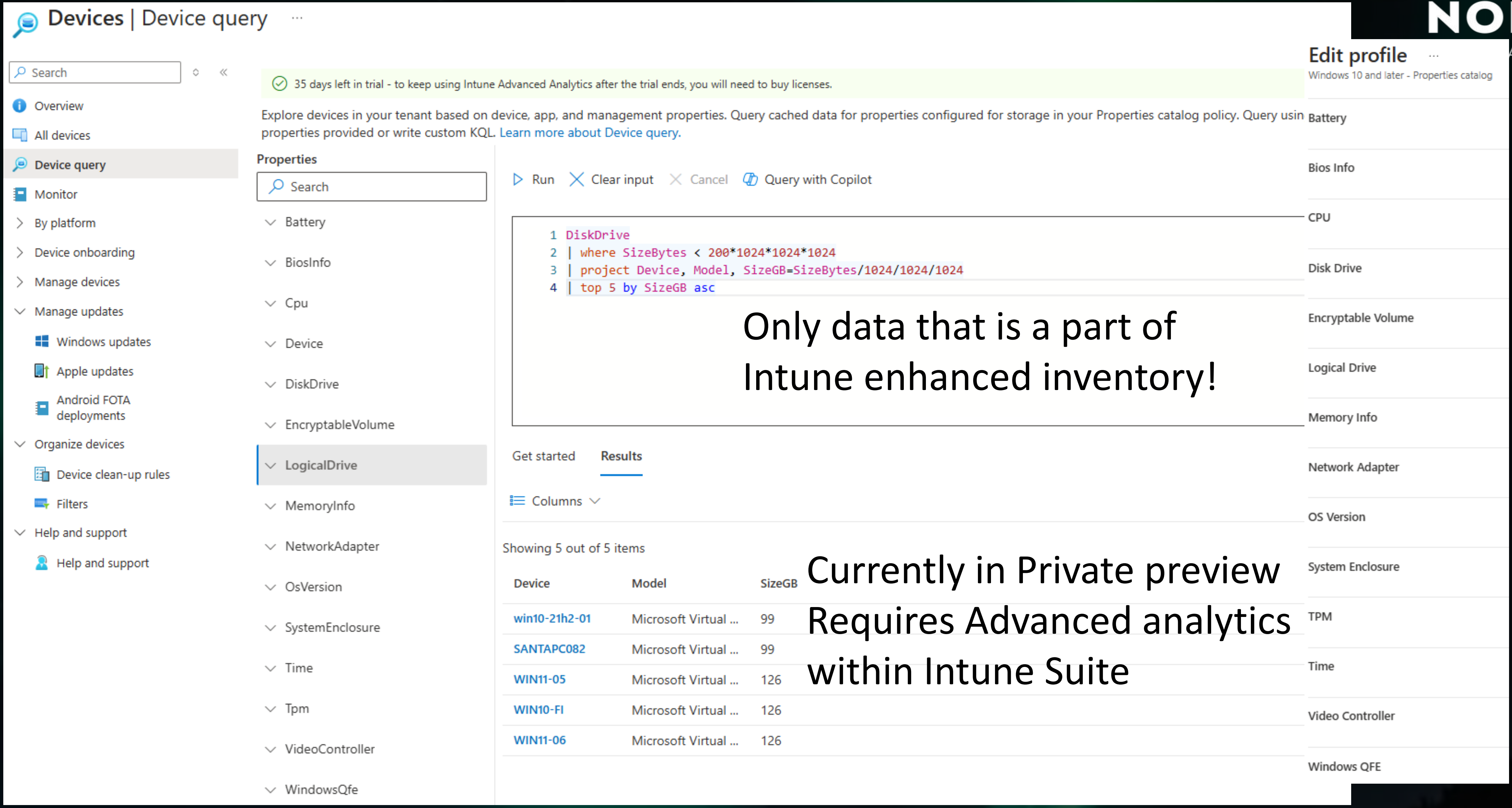
- ☐ Archive to a storage account
- ☐ Stream to an event hub
- ☐ Send to partner solution



```
IntuneDevices
| where ManagedBy == 'Intune' or ManagedBy == 'Co-managed'
| project DeviceName, FreeStorageGB=StorageFree/1024
| top 10 by FreeStorageGB asc
```

Devic...	FreeStorageGB
SA...	32
wi...	37
WI...	48
SA...	50
WI...	54
SA...	56
WI...	57
AI...	60
KI...	66
N...	70

Multi-Device Query



35 days left in trial - to keep using Intune Advanced Analytics after the trial ends, you will need to buy licenses.

Explore devices in your tenant based on device, app, and management properties. Query cached data for properties configured for storage in your Properties catalog policy. Query usin properties provided or write custom KQL. Learn more about Device query.

```
DiskDrive
| where SizeBytes < 200*1024*1024*1024
| project Device, Model, SizeGB=SizeBytes/1024/1024/1024
| top 5 by SizeGB asc
```

Only data that is a part of Intune enhanced inventory!

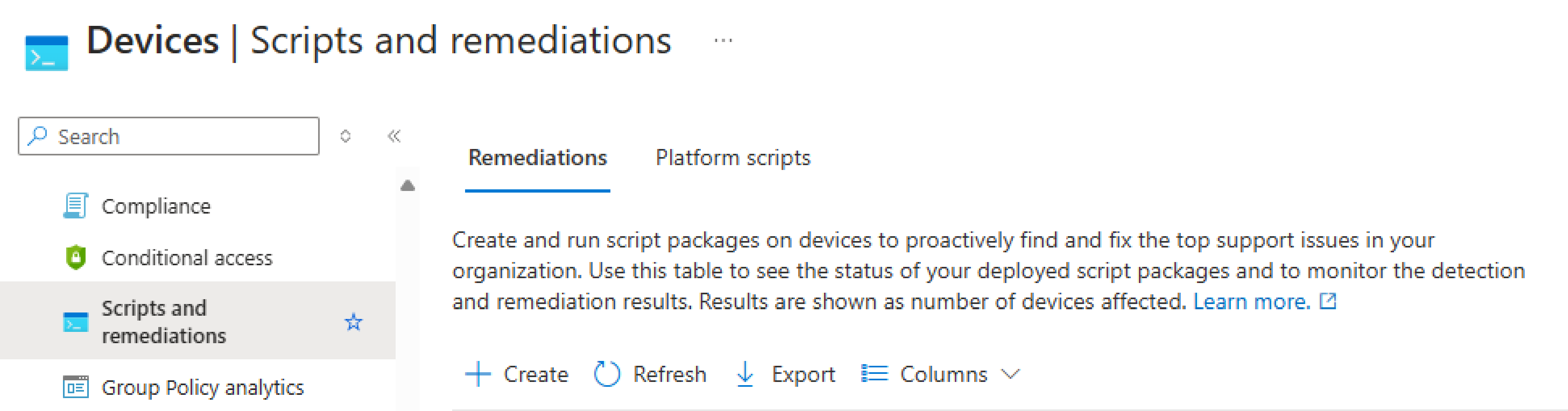
Showing 5 out of 5 items

Device	Model	SizeGB
win10-21h2-01	Microsoft Virtual ...	99
SANTAPC082	Microsoft Virtual ...	99
WIN11-05	Microsoft Virtual ...	126
WIN10-FI	Microsoft Virtual ...	126
WIN11-06	Microsoft Virtual ...	126

Currently in Private preview
Requires Advanced analytics within Intune Suite

Remediations

- Detect and optionally fix issues
  - Only “detect” function is very useful
- Requires Windows 10/11 Enterprise license
  - Not included in M365 Business Premium ☹



Devices | Scripts and remediations

Create and run script packages on devices to proactively find and fix the top support issues in your organization. Use this table to see the status of your deployed script packages and to monitor the detection and remediation results. Results are shown as number of devices affected. Learn more.

NORDIC
— VIRTUAL SUMMIT —

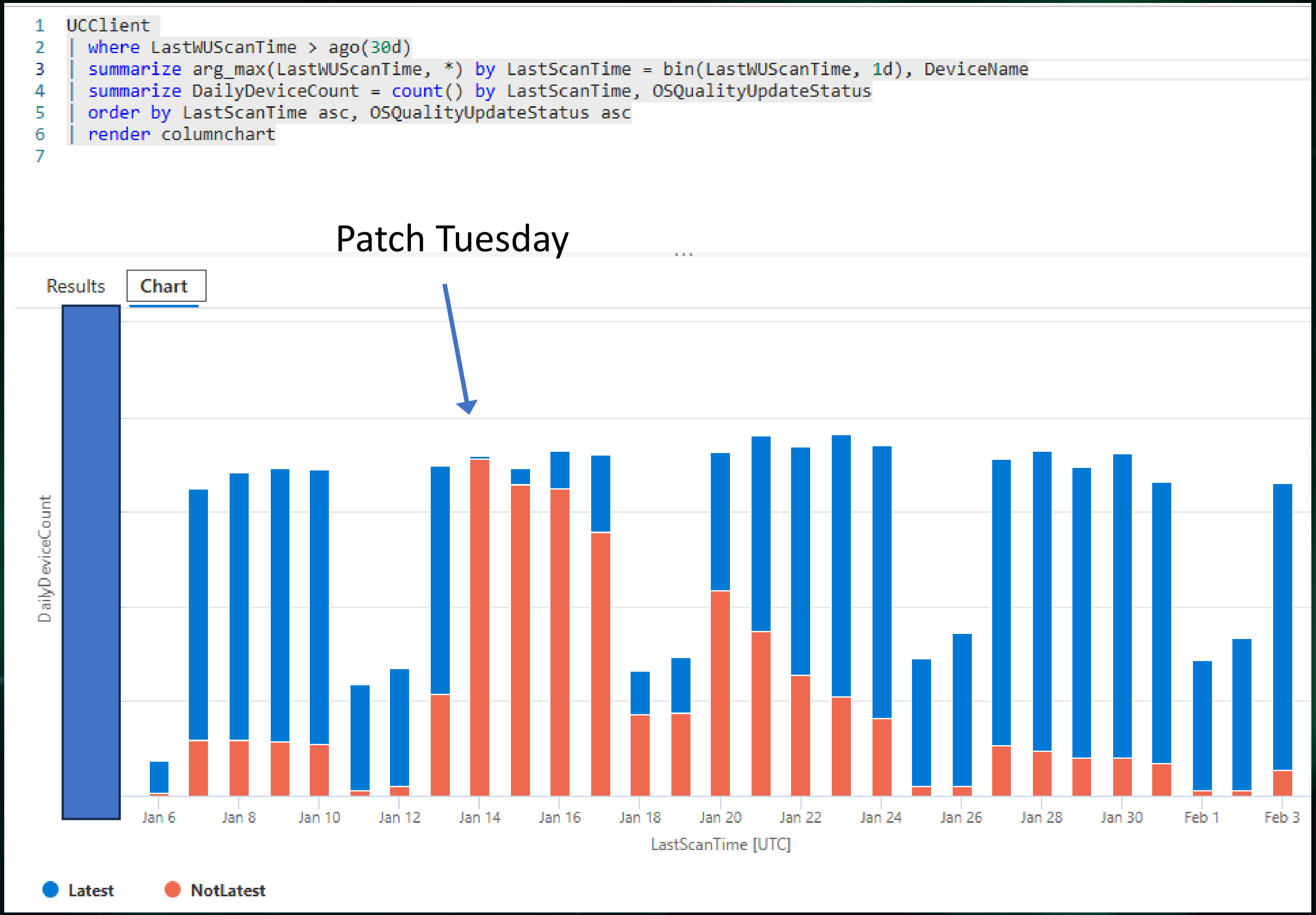
Demo 2: Multiple devices

Examples

- Specific registry value set? WSUS WU?
- Windows activation status (Remediation)
- Get Network Information (Remediation)
- Has the device the latest CU?
- Google Chrome version? Or Google Chrome installed?

WUfB Reports

Devices with the latest update

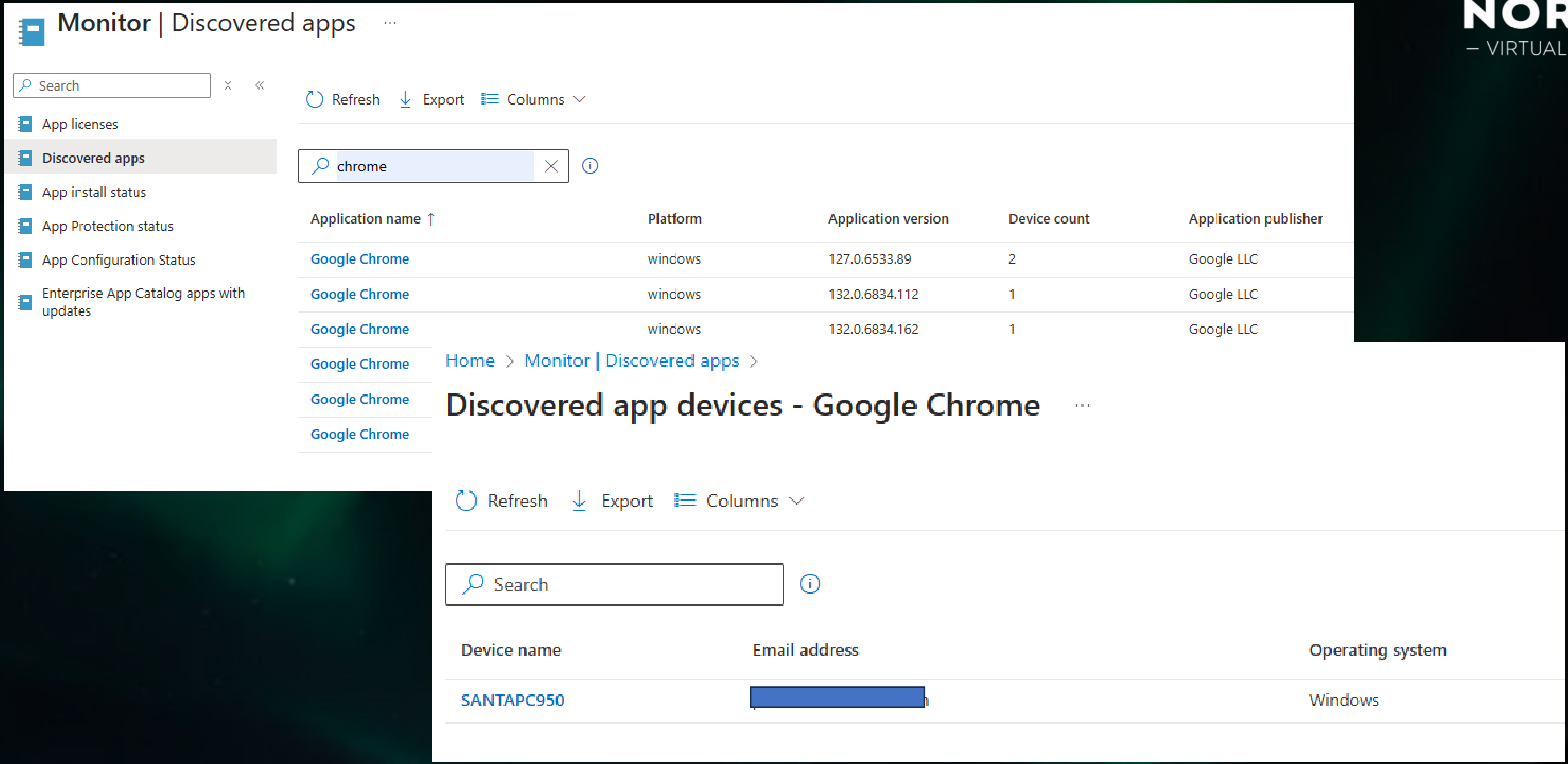


```
UCClient
| where LastWUScanTime > ago(30d)
| summarize arg_max(LastWUScanTime, *) by LastScanTime = bin(LastWUScanTime, 1d), DeviceName
| summarize DailyDeviceCount = count() by LastScanTime, OSQualityUpdateStatus
| order by LastScanTime asc, OSQualityUpdateStatus asc
| render columnchart
```

Patch Tuesday

Remember: Windows Update Distribution report Intune report!

Intune Discovered Apps Report



Monitor | Discovered apps

chrome

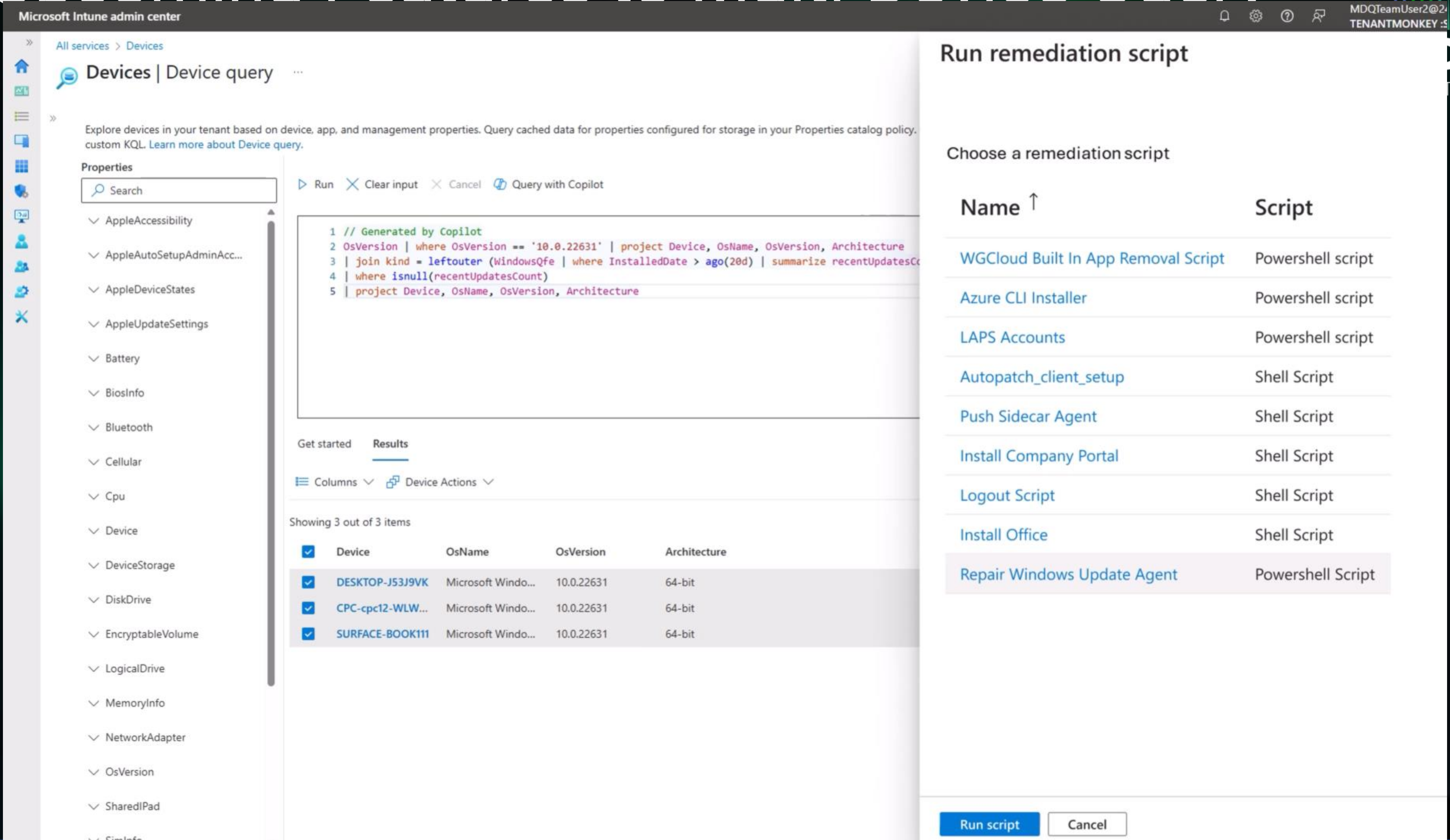
Application name ↑	Platform	Application version	Device count	Application publisher
Google Chrome	windows	127.0.6533.89	2	Google LLC
Google Chrome	windows	132.0.6834.112	1	Google LLC
Google Chrome	windows	132.0.6834.162	1	Google LLC
Google Chrome				
Google Chrome				
Google Chrome				

Home > Monitor | Discovered apps >

Discovered app devices - Google Chrome

Device name	Email address	Operating system
SANTAPC950	[redacted]	Windows

Upcoming Features to Multi-Device Query



Explore devices in your tenant based on device, app, and management properties. Query cached data for properties configured for storage in your Properties catalog policy. custom KQL. Learn more about Device query.

```
// Generated by Copilot
OsVersion | where OsVersion == '10.0.22631' | project Device, OsName, OsVersion, Architecture
| join kind = leftouter (WindowsQfe | where InstalledDate > ago(20d) | summarize recentUpdatesC
| where isnull(recentUpdatesCount)
| project Device, OsName, OsVersion, Architecture
```

Showing 3 out of 3 items

☑	Device	OsName	OsVersion	Architecture
☑	DESKTOP-J53J9VK	Microsoft Windo...	10.0.22631	64-bit
☑	CPC-cpc12-WLW...	Microsoft Windo...	10.0.22631	64-bit
☑	SURFACE-BOOK111	Microsoft Windo...	10.0.22631	64-bit

Run remediation script

Choose a remediation script

Name ↑	Script
WGCloud Built In App Removal Script	Powershell script
Azure CLI Installer	Powershell script
LAPS Accounts	Powershell script
Autopatch_client_setup	Shell Script
Push Sidecar Agent	Shell Script
Install Company Portal	Shell Script
Logout Script	Shell Script
Install Office	Shell Script
Repair Windows Update Agent	Powershell Script

NORDIC

— VIRTUAL SUMMIT —

Fix the Issues

Fix Centrally Issues: Options

- Remediations
  - Main tool (if you have required licenses)
  - Stateful → Run fix only if needed
  - Can output information to Intune console
- Win32 apps
  - With payload files
  - Custom requirements
  - Custom detection checks
  - End user self-service for "Remediations"
  - Stateful → Run fix only if needed
- (Platform) PowerShell scripts
  - No payload files
  - Can't see script content and no output in Intune console
  - In system context runs on every user logged in!

NORDIC
— VIRTUAL SUMMIT —

Demo: Fix centrally

Examples

- Specific registry value set? WSUS WU?
- Win32 application "Remediation"

If Co-managed

- Extensible inventory & collections can be used to find issues
  - Collections can be synced to Entra ID groups if needed
- CMPivot & PowerShell scripts would be useful
- Configuration items & baselines
- Topic for another session ☺

Summary

- Where to find the issue from a single device?
  - Registry, files, WMI, events?
  - Which tool to use to get the info
- Know what info Intune provides built-in
- Remediations is very useful tool!
- Remember other data sources: MDE, WUfB
- Advanced analytics has many benefits
  - Will be improved in the future
- Key knowledge required
  - PowerShell
  - KQL

Control to Pete

From: https://ignite.microsoft.com/en-US/sessions/BRK319

Scripts and query examples

Control to Pete

https://github.com/petripaavola/Intune

From: https://ignite.microsoft.com/en-US/sessions/BRK319

Thank you!