



Workplace Ninja

User Group Finland

**Navigating Intune's Inventory & Analytics
Ecosystem**



Panu Saukko
ProTrainIT Oy

MVP – Microsoft Intune &
Microsoft Security Copilot

Panu Saukko | LinkedIn
Panu.Saukko@protrainit.fi



Workplace Ninja
User Group Finland



Multiple ways to get data out from cloud-native devices

1. Classic inventory

 Hardware

 Discovered apps

2. Enhanced inventory

 Device inventory

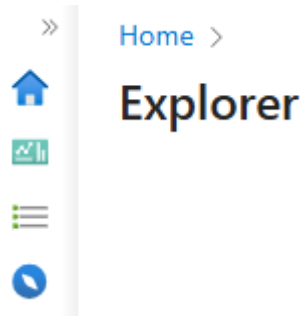
 Device query

3. Endpoint analytics

 Endpoint analytics

 Advanced analytics

4. Explorer



“Requires” SCUs

5. Microsoft Defender for Endpoint



6. WUfB reports

Home >
Windows Update for Business reports
Azure Monitor

Requires Log analytics



Intune Suite with M365 E3/E5

1. Which Intune related capabilities are included in each plan?

Here is a summary of the Microsoft 365 plan changes related to Microsoft Intune:

Microsoft 365 plans	Included capabilities
Microsoft Enterprise Mobility and Security E3 (EMS E3) <i>(included in Microsoft 365 E3)</i>	<ul style="list-style-type: none">Intune Remote HelpIntune Advanced AnalyticsIntune Plan 2
Microsoft 365 E5	All Microsoft 365 E3 features plus: <ul style="list-style-type: none">Intune Endpoint Privilege ManagementMicrosoft Cloud PKIIntune Enterprise App Management
Microsoft 365 E5	<ul style="list-style-type: none">Microsoft Security Copilot

3. When do these changes take effect?

For the 2026 planned product additions to Microsoft 365, a Microsoft 365 admin center notification will be posted for administrators of eligible organizations 30 days in advance of the effective change.



[Microsoft 365 adds advanced Microsoft Intune solutions at scale - Microsoft Intune Blog](#)

DEMOS



Classic hw inventory

- Enabled by default
- Updates every 7 days

Operating system

Operating system	Windows
Operating system version	10.0.26200.7392
Operating system language	en-US
Operating system edition	Enterprise
Operating system SKU	Windows 10/11 Enterprise (4)
Security patch level	

Subscription

Status	Unknown
--------	---------

Storage

Total storage space	921.59 GB
Free storage space	393.79 GB
Total physical memory	32.00 GB

System enclosure

IMEI	
MEID	
Manufacturer	Intel(R) Client Systems
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	192.168.50.67, 172.24.16.1

Network service

Enrolled date	1/2/2023, 9:29:08 AM
Last contact	1/5/2026, 3:47:38 AM

Classic hw inventory

- Benefits:
 - Nicely integrated with Intune portal (new columns/export)
 - Free disk space! 😊
 - Can use Graph queries to find information
 - Can be synced to Log analytics for additional insights
- Issues
 - Rarely changes
 - Expensive for Microsoft to add new data
 - Some peculiar shortcomings
 - New inventory data not part of export/sync to Log analytics
 - Export missing: Wired IPv4 Address, OS Language/SKU
 - Log analytics: many more... 😞



Discovered Apps

- Updates every 7 days
- Intune Management Extension finds Win32 apps every 24h
 - Win32AppInventory.log
- Store apps:
 - Get-AppxProvisionedPackage –online
| fl DisplayName, Version

Refresh Export Columns

Search

Application name	Application version
28944Stefanvd.NetworkStatusChecker	1.2.6.0
Adobe Acrobat (64-bit)	25.001.20997
AdobeAcrobatReaderCoreApp	24.0.0.1
AppUp.IntelGraphicsExperience	1.100.5688.0
CMPivot	5.2303.1089.1000
Clipchamp.Clipchamp	4.4.10720.0
Configuration Manager Support Center	5.2107.1082.1000
Download Manager	1.0.5
Google Chrome	143.0.7499.170
Intel(R) Wireless Bluetooth(R)	23.160.0.9
Intel® Driver & Support Assistant	25.4.36.6
IntuneDebugTools	2.3
MSTeams	25332.1210.4188.1171
Microsoft .NET Runtime - 8.0.22 (x64)	8.0.22.35427
Microsoft 365 -sovellukset suuryrityksille - fi-fi	16.0.19328.20266
Microsoft 365 Apps for enterprise - en-us	16.0.19328.20266
Microsoft ASP.NET Core 8.0.22 - Shared Framework (x86)	8.0.22.25528

Discovered apps report

Discovered apps

Multiple issues with app report!

Refresh Export Columns

548 items

Search



Application name ↑	Platform	Application version	Device count	Application publisher
7-Zip 18.05 (x64)	windows	18.05	1	Igor Pavlov
7-Zip 24.06 (x64 edition)	windows	24.06.00.0	1	Igor Pavlov
7-Zip 25.01 (x64 edition)	windows	25.01.00.0	1	Igor Pavlov
7EE7776C.LinkedInforWindows	windows	2025.220.1915.0	1	CN=DDCCB5DA-E820-43B5-B58C-BEF830E60516
8338Giuapps.Inkodo	windows	3.11.32.0	1	CN=7B817064-9E29-40EC-B2F9-3D8C5B47ACB9
AD2F1837.HPPrinterControl	windows	162.3.1128.0	1	CN=ED346674-0FA1-4272-85CE-3187C9C86E26
Adobe Acrobat (64-bit)	windows	25.001.20997	2	Adobe
Adobe Acrobat (64-bit)	windows	25.001.20997	1	Adobe
Adobe Acrobat Reader	windows	24.005.20320	2	Adobe Systems Incorporated
Google Chrome	windows	143.0.7499.110	1	Google LLC
Google Chrome	windows	142.0.7444.176	1	Google LLC
Google Chrome	windows	143.0.7499.170	2	Google LLC
Google Chrome	windows	143.0.7499.170	1	Google LLC
Google Chrome	windows	142.0.7444.176	1	Google LLC

Enhanced inventory

New inventory architecture

Prereq

- Create properties catalog profile

Home > Devices | Windows > Windows | Configuration >

Create profile

Windows 10 and later - Properties catalog

☒ Basics ☒ Configuration properties ☐ Scope tags ☐ Assignments

Properties catalog
Select the properties you want to collect. Select **Add properties** to add properties you want to collect.
[Learn more](#)

+ Add properties

☒ Basics ☒ Configuration properties ☐ Scope tags ☐ Assignments ☐ Review + create

+ Add properties

Logical Drive Remove category ^

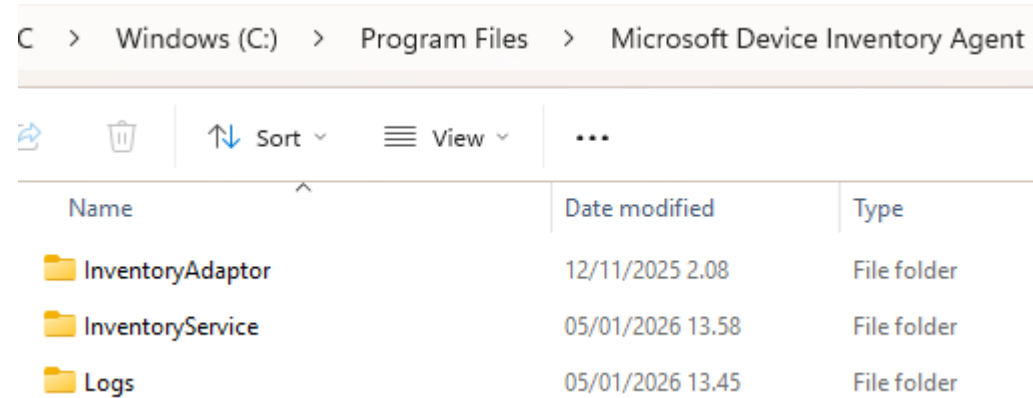
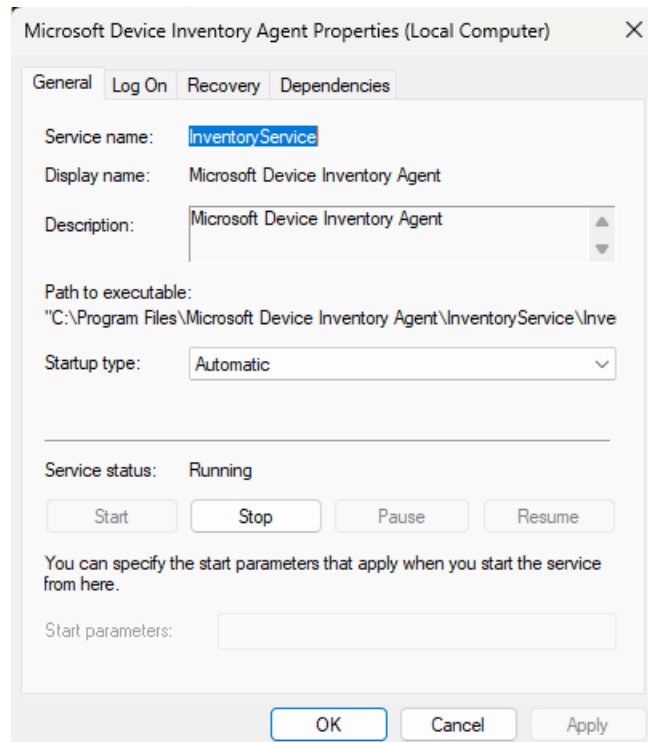
Disk Description	Refresh every 24 hours	⊖
Disk Size Bytes	Refresh every 24 hours	⊖
Drive Identifier	Refresh every 24 hours	⊖
Drive Type	Refresh every 24 hours	⊖
File System	Refresh every 24 hours	⊖

Properties picker

Search

- > ☐ Battery
- > ☐ Bios Info
- > ☐ CPU
- > ☐ Disk Drive
- > ☐ Encryptable Volume
- ✓ ☐ Logical Drive
 - ☐ Disk Description
 - ☐ Disk Size Bytes
 - ☐ Drive Identifier
 - ☐ Drive Type
 - ☐ File System
- > ☐ Memory Info

Enhanced inventory client components



WMI Namespace



SQLite DB

```
e_sqlite3.dll
InventoryServiceHarvesterDatabase.sqlite
InventoryUploader.sqlite
Microsoft.Data.Sqlite.dll
```

Enhanced inventory data

Home > Devices | Windows > Windows | Windows devices > NUC6

NUC6 | Device inventory

Overview

Manage

Properties

Monitor

Device inventory

Device query

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Local admin password

Recovery keys

User experience

BIOS info

CPU

Disk Drive

Encryptable Volume

Logical Drive

Memory Info

Network Adapter

OS Version

SimInfo

Export Columns

Last refreshed on 01/05/2026, 09:27

Drive Identifier ↑↓	Disk Description ↑↓	Disk Size Bytes ↑↓	Drive Type ↑↓	File System ↑↓	Last updated ↑↓
C:	Local Fixed Disk	998,546,337,792	LOCAL_DISK	NTFS	11/12/2025, 07:53:
D:	Local Fixed Disk	2,000,382,062,592	LOCAL_DISK	NTFS	11/12/2025, 07:53:



Enhanced inventory data

Microsoft has blocked Graph access to enhanced inventory data

GET

beta

https://graph.microsoft.com/beta/deviceManagement/managedDevices('b51b0f10-1366-40dd-8665-d3cd5827380a')/deviceInventories('MemoryInfo')

Run query

No resource was found matching this query

Request Body

Request Headers

Modify Permissions

Access token

Forbidden - 403 - 294 ms

Either the signed-in user does not have sufficient privileges, or you need to consent to one of the permissions on the **Modify permissions** tab

Response preview

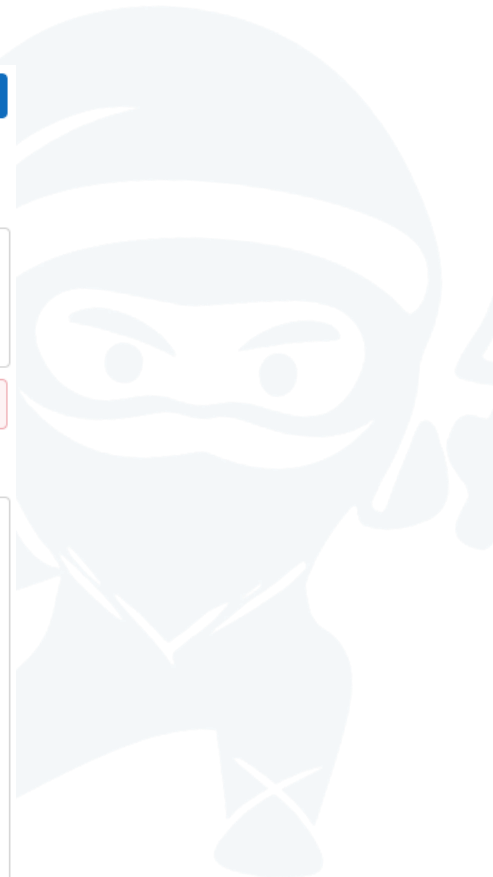
Response headers

Code snippets

Toolkit component

Adaptive cards

```
{
  "error": {
    "code": "Forbidden",
    "message": "{\r\n  \"_version\": 3,\r\n  \"Message\": \"An error has occurred - Operation ID (for customer support): 00000000-0000-0000-0000-000000000000 - Activity ID: 5aa5e1ee-699b-6feb-1401-3896ce78d0a7 - Url: https://proxy.msub02.manage.microsoft.com/DeviceFE/StatelessDeviceFEService/deviceManagement/managedDevices('b51b0f10-1366-40dd-8665-d3cd5827380a')/deviceInventories('MemoryInfo')?api-version=5025-09-08\", \r\n  \"CustomApiErrorPhrase\": \"\\\", \r\n  \"RetryAfter\": null, \r\n  \"ErrorSourceService\": \"\\\", \r\n  \"HttpHeaders\": \"{}\" \r\n}",
    "innerError": {
      "date": "2026-01-05T12:16:12",
      "request-id": "1ebc5d91-58a0-47fc-bc5f-c4731a7cbde0",
      "client-request-id": "5aa5e1ee-699b-6feb-1401-3896ce78d0a7"
    }
  }
}
```



Multi-device query

The way to access enhanced inventory data.
Part of Intune Suite's Advanced analytics.

Devices | Device query

Search

Overview

All devices

Device query

Monitor

By platform

Windows

iOS/iPadOS

macOS

Android

Linux

Device onboarding

Windows 365

Enrollment

Manage devices

Configuration

Compliance

Conditional access

Scripts and remediations

Group Policy analytics

Properties

Search

AppleAutoSetupAdminAc...

AppleDeviceStates

AppleUpdateSettings

Battery

BiosInfo

Bluetooth

Cellular

Cpu

Device

DeviceStorage

DiskDrive

EncryptableVolume

Enter a request to generate a query

Run Cancel

```
1 LogicalDrive
2 | where DriveIdentifier == 'C:'
3 | project Device, DiskSizeGB=DiskSizeBytes/1024/1024/1024
4 | top 10 by DiskSizeGB asc
```

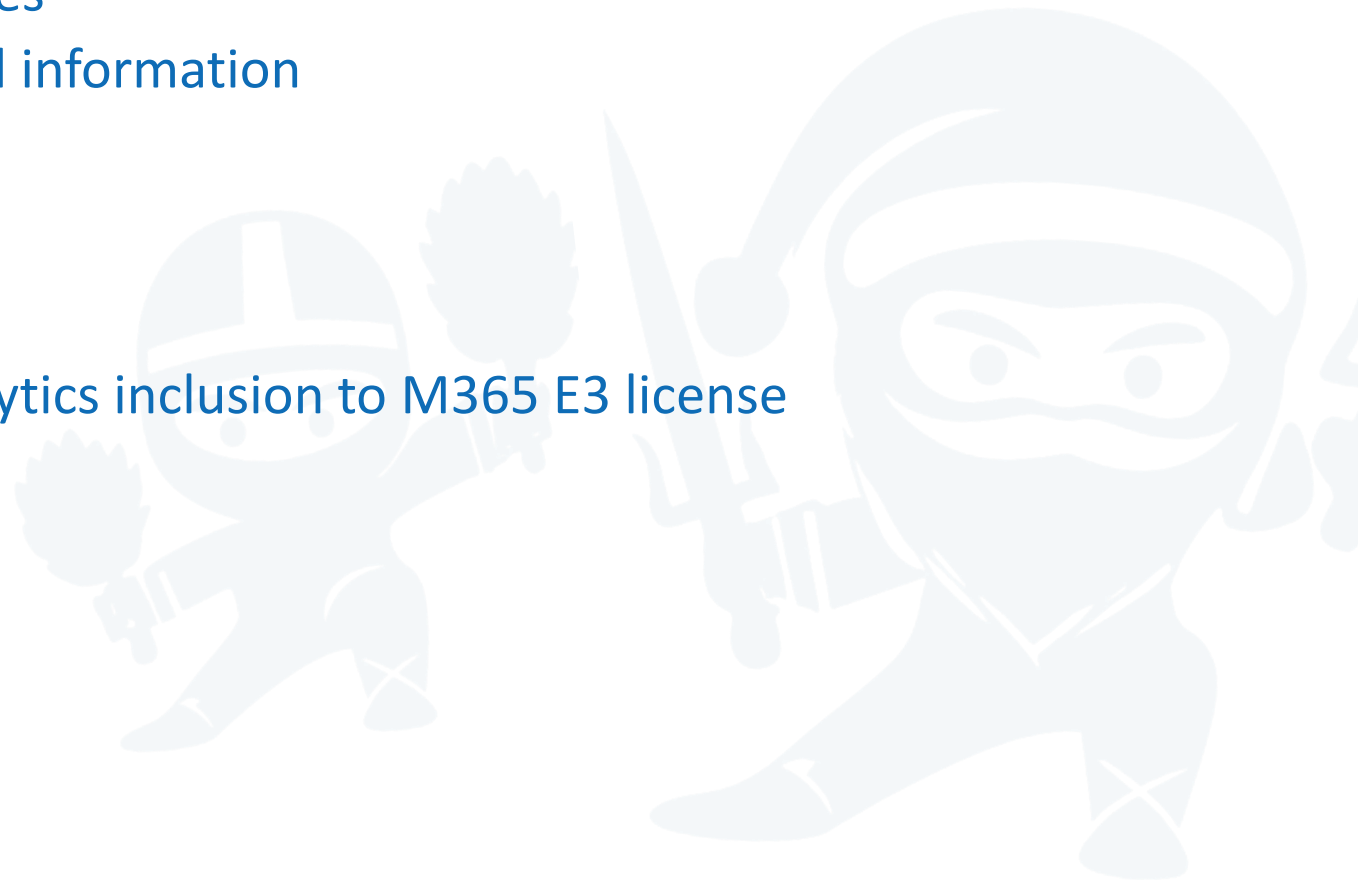
Get started Results

Export Columns Add all items to a group

Device	DiskSizeGB
SANTAPC169	98

Enhanced inventory

- Benefits:
 - OS agnostic architecture
 - Easier for Microsoft to add new attributes
 - Multi-device query is a great tool to find information
- Issues
 - Currently only “static” information
 - No Graph access to custom scripting
 - Most customers wait for Advanced analytics inclusion to M365 E3 license



Endpoint analytics (EA)

Mostly performance related information.
Remember to enable!
Free vs paid functionalities

Endpoint analytics | Overview

Search

Overview

Settings

Reports

Startup performance

Application reliability

Work from anywhere

Resource performance

Battery health

Overview

Anomalies

Model scores

Device scores

Proactively optimize the user experience and track your progress [Learn more](#)

Device scope : **All Devices**

Refresh

Endpoint analytics score

Meeting goals

Endpoint analytics score

69

Baseline

50

Score categories

Metric	Score
Startup performance	61
Application reliability	0
Resource performance	85
Work from anywhere	95
Battery health	74

▲ = Baseline

Preview reports do not contribute to your Endpoint analytics score

Baseline

All organizations (median)

Insights and recommendations

You have 2 physical devices with high RAM usage. On average, these devices have a RAM spike of 100% compared to an average of 0% for your other devices.

Getting these devices to normal RAM usage range will boost your score by 7 points. [Learn more about optimizing RAM performance](#)

You have 2 physical device models with high RAM usage. On average, these device models have a RAM spike of 100% compared to an average of 0% for your other devices.

Getting these models to normal RAM usage range will boost your score by 7 points. [Learn more about optimizing RAM performance](#)

You have 1 physical devices with high CPU usage. On average, these devices have a CPU spike of 28% compared to an average of 0% for your other devices.

Getting these devices to normal CPU usage range will boost your score by 3 points. [Learn more about optimizing CPU performance](#)

You have 1 physical device models with high CPU usage. On average, these device models have a CPU spike of 28% compared to an average of 0% for your other devices.

Getting these models to normal CPU usage range will boost your score by 3 points. [Learn more about optimizing CPU performance](#)

EA's free vs advanced features

- Free functionality

- Startup performance (boot/logon) per device/hw model
- Device reboots (blue screens!)
- Application reliability and usage
- Work from anywhere

- Advanced functions

- Part of Advanced analytics
- CPU/RAM usage
- Battery health
- Device timeline
- Anomalies



Endpoint analytics

- Benefits
 - Great performance/reliability related information
 - Free basic features
- Issues
 - Not enabled by default
 - Need to check periodically
 - Some features require Advanced analytics license



Explorer

Collection of queries. Requires SCUs even, even though doesn't use them.

Query your data

Start typing to search your Intune data, or see below for examples



Find the Intune data you're looking for

Search your tenant for info about devices, users, apps, compliance, or updates. Copilot can also help you understand what kind of questions you can ask and how to ask them.

Show examples for:

All categories



Apps

Get the top [Number Of Apps](#) apps with the highest number of [App Install Status](#) on [Managed App Platform](#)



Apps

Get all managed app install results for user [/User](#)



Compliance

Get [Platform](#) devices that are [Compliance](#) state due to the compliance setting [Compliance Setting Name](#)



Apps

Get the current deployment status of [/Managed App](#) across all devices



Endpoint Privilege Management

Get managed vs unmanaged elevation counts for last month



Endpoint Privilege Management

Get the top 10 most frequently elevated applications

All categories

Advanced Analytics

App Configuration

App Protection

Apps

Audit logs

Autopilot

Compliance

Device Configuration

Device Updates

Devices

Endpoint Privilege Management

Groups

Roles



Secure Compute Unit for Explorer

Security compute units

Select the number of units you want to purchase for SecCopilot. Security compute units provide the computing power that drives the Security Copilot experience. [Read more about security compute units](#)

0

Provisioned security compute units per hour *

\$ 4 USD per unit

Estimated monthly cost 0 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

6

units per hour

Apply

Cancel

...



Explorer

Explore data in your tenant based on device, app, and management properties. [Learn more about exploring data, including what's coming soon](#)

Query your data Get **Windows** devices that have discovered app with name containing **chrome** installed

 Copilot Summary

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

▼ Overall Summary

There are 6 items in the results list. This query retrieves information about devices on specified platforms that have discovered applications with names containing a particular string. DeviceName, DeviceId, and EntraDeviceId. This helps administrators identify which devices have specific applications installed across different platforms in their Intune environment.

> Other Useful Queries

> Next steps to consider

 Export  Columns ▼  Add devices to group

 Search   Add filters

<input type="checkbox"/> Device ↑	App Name	Platform	Publisher	App Version
<input type="checkbox"/> AINON-LAPTOP	Google Chrome	Windows	Google LLC	143.0.7499.170
<input type="checkbox"/> KOTINUC	Google Chrome	Windows	Google LLC	143.0.7499.192
<input type="checkbox"/> NUC3	Google Chrome	Windows	Google LLC	143.0.7499.170
<input checked="" type="checkbox"/> SANTAPC233	Google Chrome	Windows	Google LLC	142.0.7444.59
<input checked="" type="checkbox"/> SANTAPC499	Google Chrome	Windows	Google LLC	142.0.7444.176



Explorer

- Benefits
 - Many different queries already available
 - Microsoft invests to new queries
 - Some options to utilize the results
- Issues
 - Requires SCUs, but no SCU usage (yet)
 - Some queries complex to use
 - More queries needed



Microsoft Defender for Endpoint

- Collect a lot of information from devices
- Advanced hunting is a great way to get installed applications from cloud-managed devices

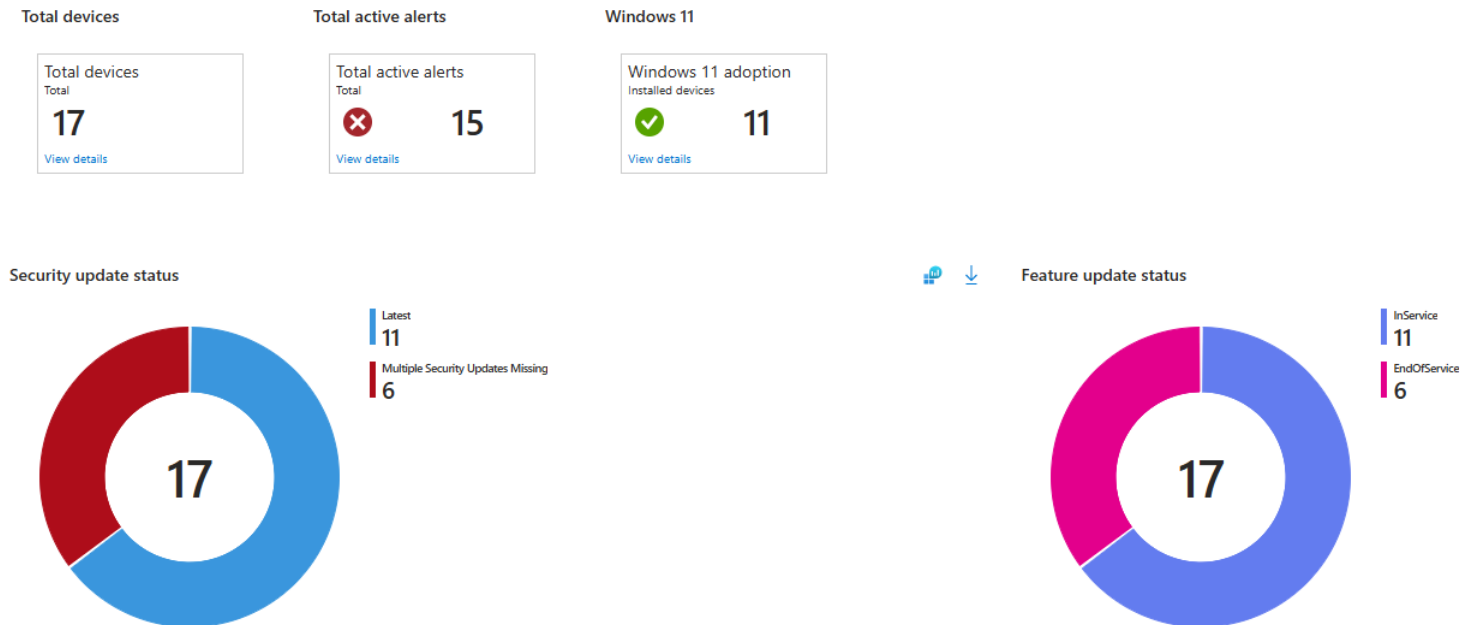
```
// Devices with Google Chrome
DeviceInfo
| join (DeviceTvmSoftwareInventory
|   | where SoftwareName has 'Chrome') on DeviceId
| project DeviceName, OSDistribution, OSVersionInfo, SoftwareName, SoftwareVersion
| order by DeviceName asc
```

```
// Windows Workstations without Google Chrome
let DevicesWithChrome = DeviceTvmSoftwareInventory
|   | where SoftwareName has "chrome"
|   | distinct DeviceId;
DeviceInfo
| summarize arg_max(Timestamp, *) by DeviceId
| where isnotempty(DeviceId) and isnotempty(DeviceName) and OSPlatform !contains "Server" and OnboardingStatus == 'Onboarded'
| join kind=leftanti (DevicesWithChrome) on DeviceId
| project DeviceName, OSPlatform, OSVersion
| order by DeviceName asc
```



WUfB Reports

- Lot of information about Cumulative/feature/driver updates
 - Installation status
 - Potential problems
 - Delivery optimization usage
- Requires Log analytics workspace
 - Enablement: aka.ms/wufbreports



WUfB Reports KQL queries

```
7 UCUpdateAlert
8 | where AlertStatus == 'Active'
9 | summarize count() by Recommendation
10 | order by count_ desc
11
```

Results Chart

Recommendation

- > Make sure that the device is sufficiently active and connected to the internet so it can complete the update installation
- > Run "dism /online /cleanup-image /restorehealth" from a command prompt as an administrator. If the command fails reinstall Windows or contact support. If it succeeds try reinstalling the update. If the update won't install contact support.
- > This error is likely transient. If it persists, use the included information troubleshoot further or contact Microsoft support.
- > Retry the update. If that fails, restart the device and retry the update. If that fails, contact Update Compliance support.

```
> 12 UCUpdateAlert
> 13 | where UpdateCategory == 'WindowsQualityUpdate' and Recommendation has "/online /cleanup-image" and AlertStatus == 'Active' and isnotempty( DeviceName)
> 14 | project DeviceName, AlertSubtype, ClientSubstate, AlertStatus, TargetBuild, Recommendation
> 15 | order by DeviceName asc
> 16 | take 100
```

Results Chart

D...	AlertSubtype	ClientSubstate	AlertStatus	TargetBuild	Recommendation
>	WindowsComponentCorruption	InstallStart	Active	10.0.26100.7092	Run "dism /online /cleanup-image /restorehealth" from a command prompt as an ad...
>	WindowsComponentCorruption	InstallStart	Active	10.0.26100.7392	Run "dism /online /cleanup-image /restorehealth" from a command prompt as an ad...
>	WindowsComponentCorruption	DownloadComplete	Active	10.0.22631.6199	Run "dism /online /cleanup-image /restorehealth" from a command prompt as an ad...
>	WindowsComponentCorruption	UserCancelled	Active	10.0.22631.6199	Run "dism /online /cleanup-image /restorehealth" from a command prompt as an ad...
>	InstallCancelled	InstallStart	Active	10.0.22631.6199	Run "dism /online /cleanup-image /restorehealth" from command prompt as an admi...
>	WindowsComponentCorruption	InstallStart	Active	10.0.22631.6345	Run "dism /online /cleanup-image /restorehealth" from a command prompt as an ad...
>	WindowsComponentCorruption	InstallStart	Active	10.0.22631.6199	Run "dism /online /cleanup-image /restorehealth" from a command prompt as an ad...
>	InstallCancelled	InstallStart	Active	10.0.22631.6060	Run "dism /online /cleanup-image /restorehealth" from command prompt as an admi...
>	WindowsComponentCorruption	InstallStart	Active	10.0.22631.6199	Run "dism /online /cleanup-image /restorehealth" from a command prompt as an ad...



WUfB Reports

- Benefits
 - Interesting data about updates
 - Finds issues that might be difficult to otherwise notice
 - Custom KQL queries enables custom reports
- Issues
 - Requires implementation
 - Takes some time to learn the data structure
 - Too difficult to utilize the data within Intune

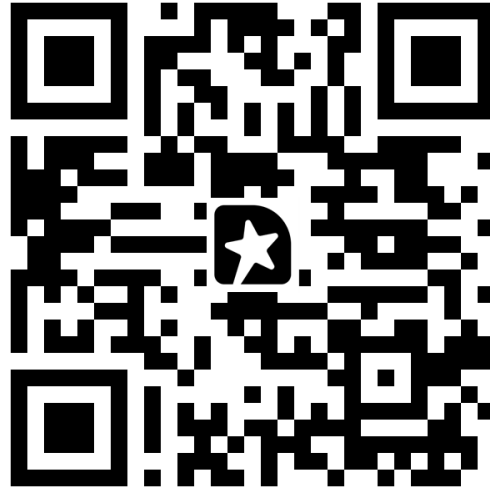


Summary

- Multiple places where you find information about cloud-native devices
 - For historical reasons...
- Need to know where to look for different data points
- Doing actions based on inventory is challenging
 - Do X on all devices which have Y
 - Some early steps available (add to a group)
 - More to come



Feedback!



Navigating Intune's Inventory & Analytics Ecosystem



Thank you!

