

**Session:**

**Date 19 April: 11:25**

# **Simplify device management with data and AI**

—Peter van der Woude—



# Welcome to:



MODERN  
ENDPOINT  
MANAGEMENT

## SUMMIT 2024

APRIL 17 - 19

GOLD PARTNERS

control  UP

 Microsoft

# THANK YOU PARTNERS

## GOLD PARTNERS



## SILVER PARTNERS



## BRONZE PARTNERS



**SPEAKER**

## Peter van der Woude

 [www.petervanderwoude.nl](http://www.petervanderwoude.nl)  
 @pvanderwoude  
 /peterwoude



# Simplify device management with data and AI







Daar heb ik  
geen actieve  
herinnering aan

I have no active  
memory of that



I may be off key  
but I'm always Intune

 Microsoft



# Agenda



Why is it important to use data and AI to simplify device management



What are the available components of (Advanced) (Endpoint) Analytics



A closer look at the details of (Advanced) (Endpoint) Analytics



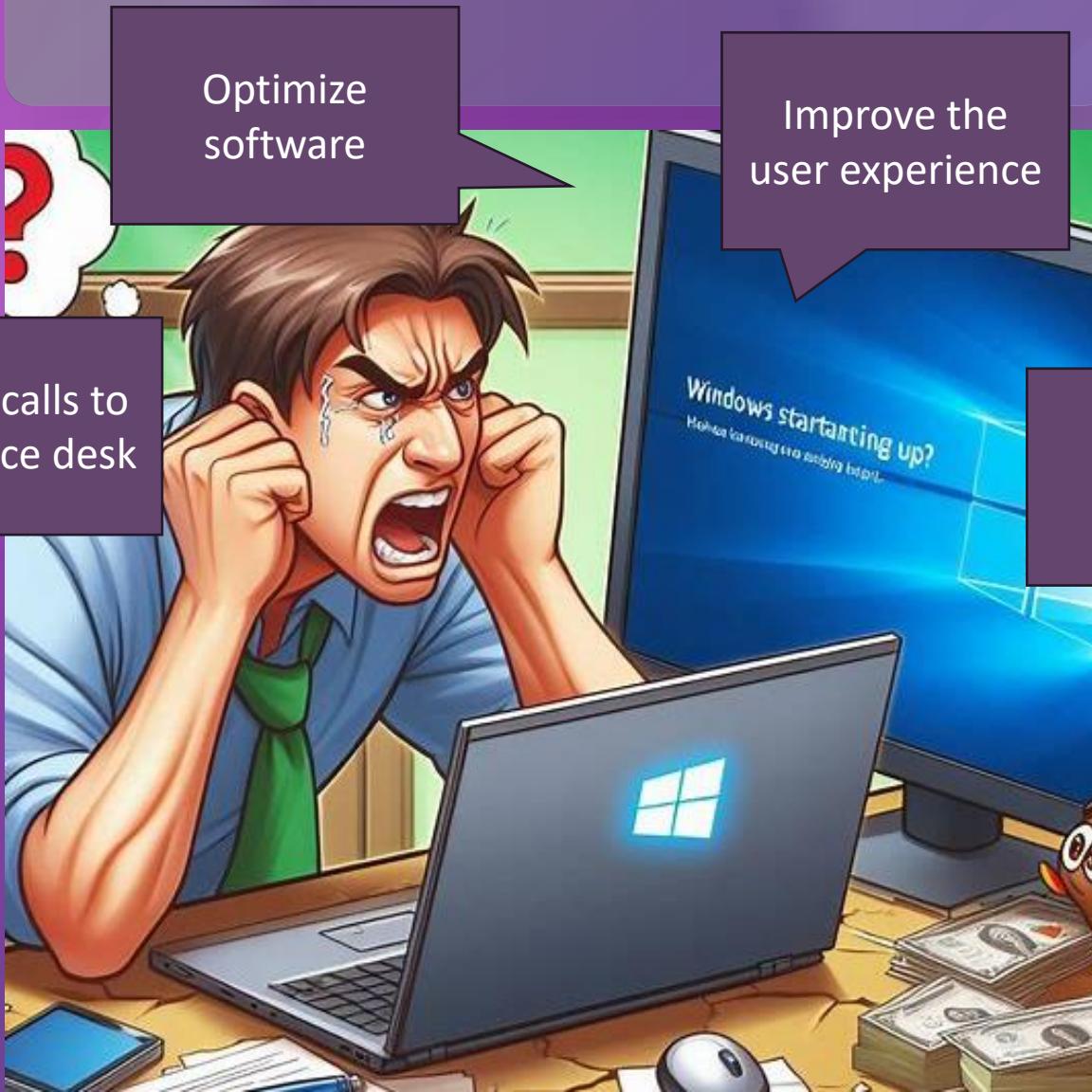
What about Device query

# Why is it important to use data and AI to simplify device management



Proactively  
detect issues

# Why is it important?



Optimize  
software



Improve the  
user experience



Prevent calls to  
the service desk



Replace legacy  
hardware on  
time



Eliminate  
productivity  
killers

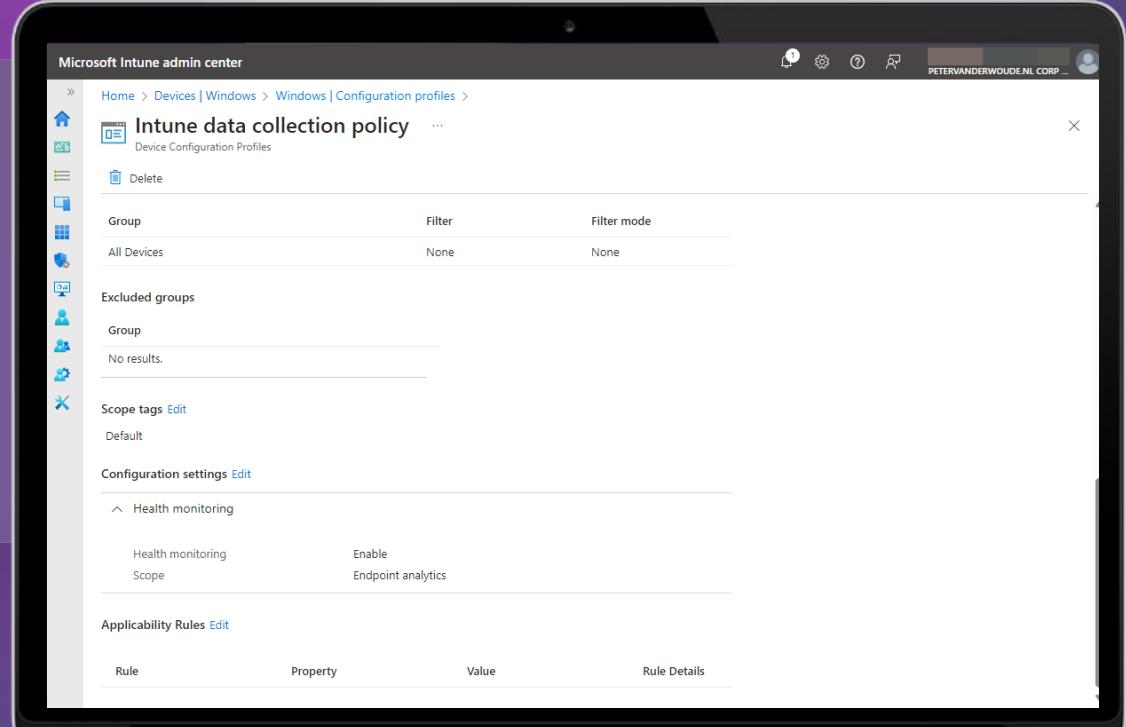
# But first: Getting started

And it starts with onboarding Endpoint analytics

# Getting started with Endpoint analytics

Basics to get started

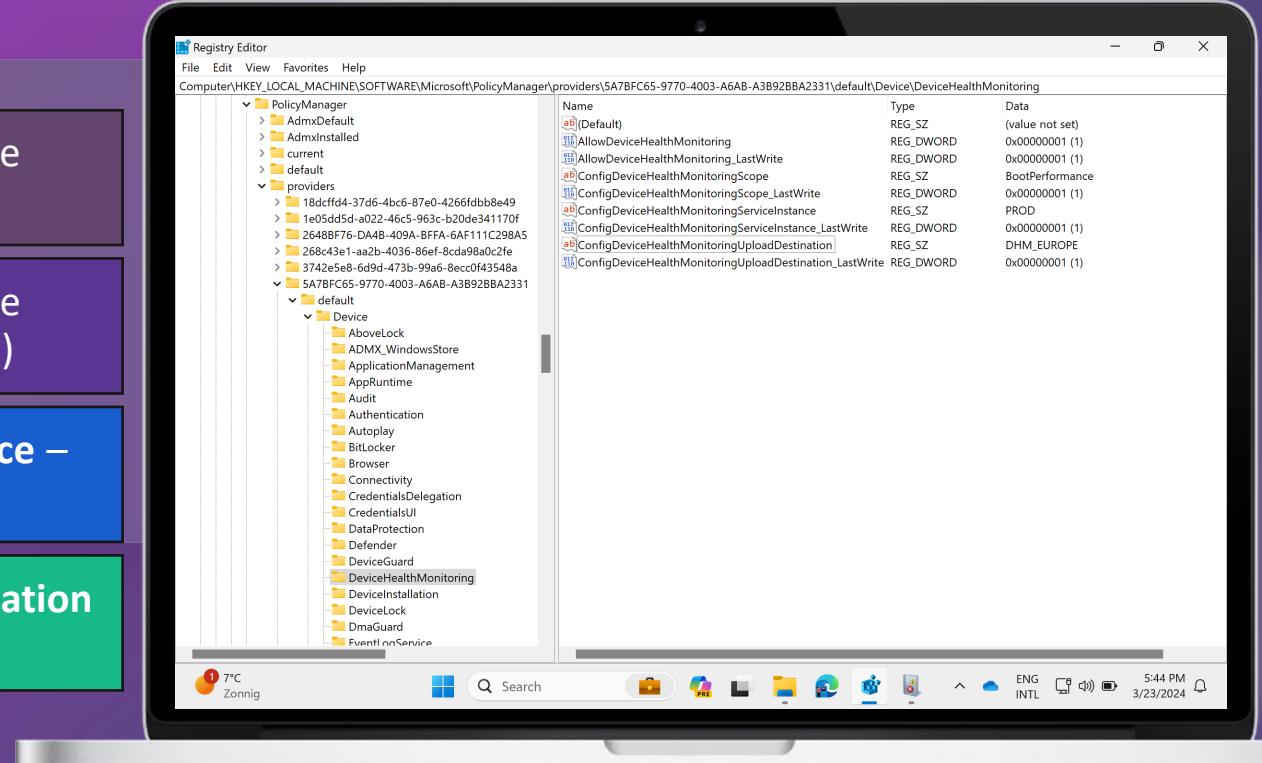
-  Verify the applicability of devices
-  Select the devices to collect data from
-  Verify the created configuration profile for collecting data

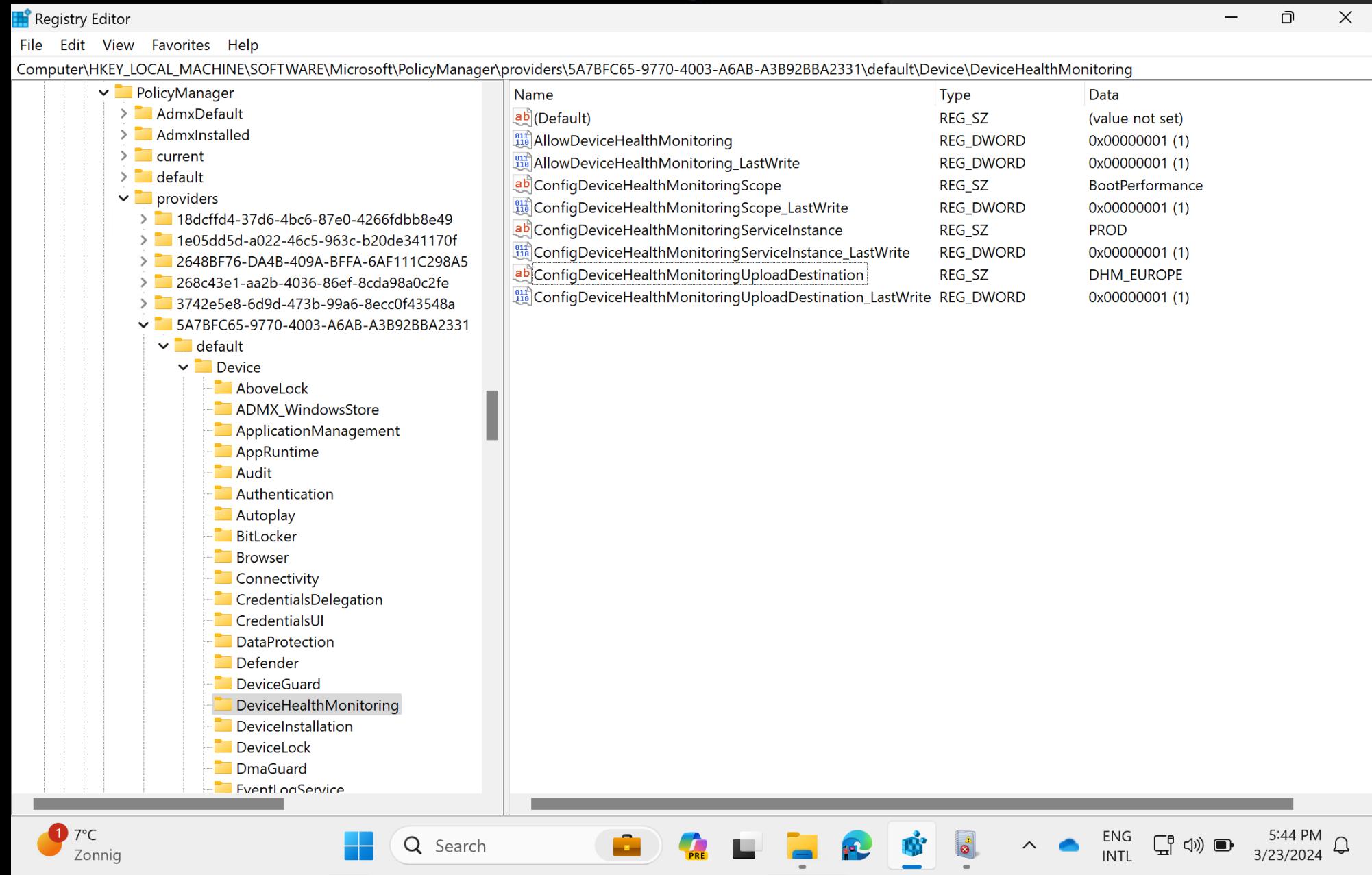


# Verifying the configuration on the device

Local configuration of **Policy CSP - DeviceHealthMonitoring**

-  **AllowDeviceHealthMonitoring** - Enable device health monitoring (required to collect data)
-  **ConfigDeviceHealthMonitoringScope** - Set the health events that are sent (*BootPerformance*)
-  **ConfigDeviceHealthMonitoringServiceInstance** – Set the service instance (*PROD*)
-  **ConfigDeviceHealthMonitoringUploadDestination** – Set the service location (*DHM\_EUROPE*)





# Important starting point

Basics to understand and keep in mind



The **Connected User Experiences and Telemetry** service must be running

The device requires a reboot before it starts sending data

It can take up to 24-hours before the data is populated

The collected data falls in the **Optional** data category

Available within Microsoft Intune P1

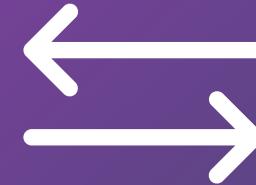
# What are the available components in Endpoint Analytics

What are the available components?

SCORES



BASELINES



INSIGHTS



(PROACTIVE)  
REMEDIATIONS



# Startup performance

The retention period for device boot and sign-in events is 29 days



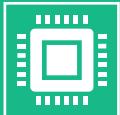
**Startup score** – Insights to improve startup performance to optimize the time from power-on of the device to productivity



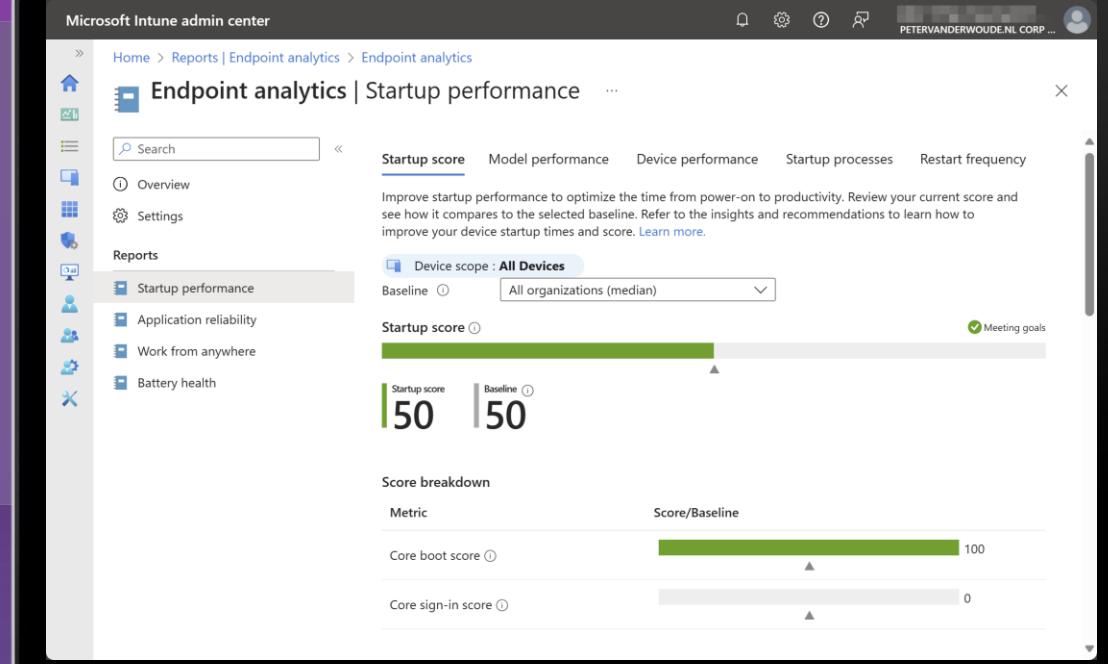
**Model performance** – Review the startup times and restart frequencies of all device models



**Device performance** – Review the startup times and restart frequencies of device



**Startup processes** – Review the time it takes for startup processes to load once desktop appears

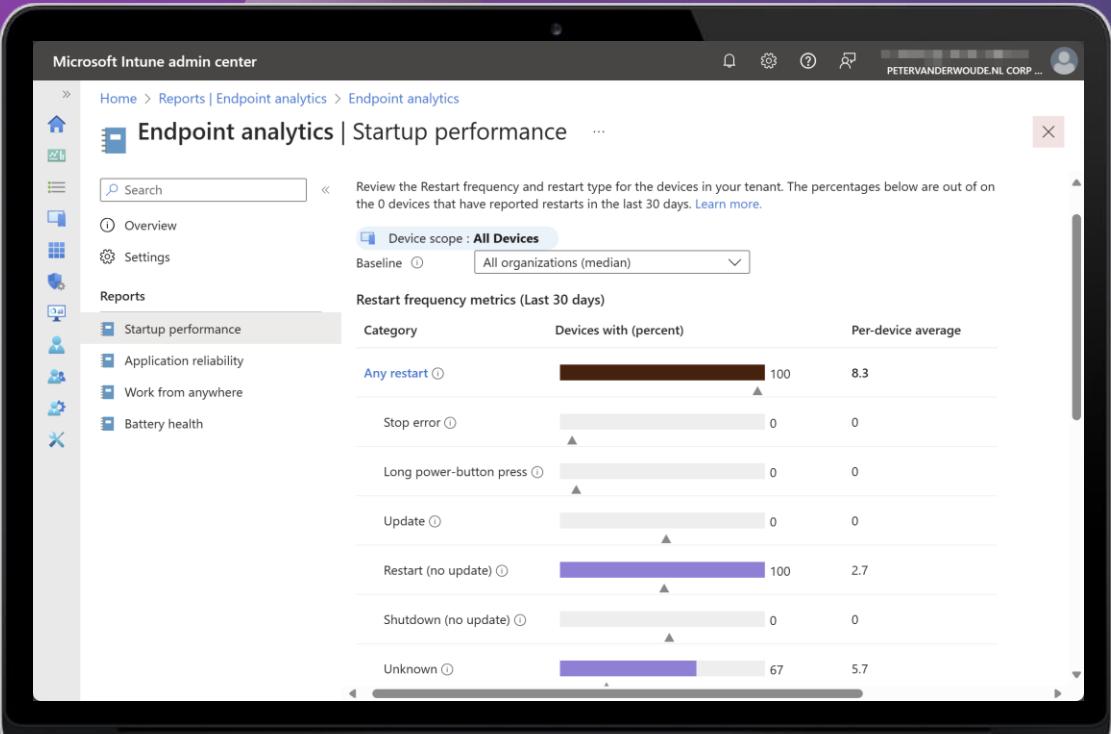
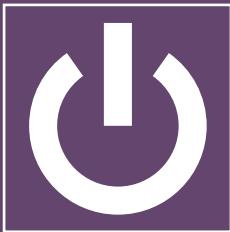


# Restart frequency

The retention period for device boot and sign-in events is 29 days

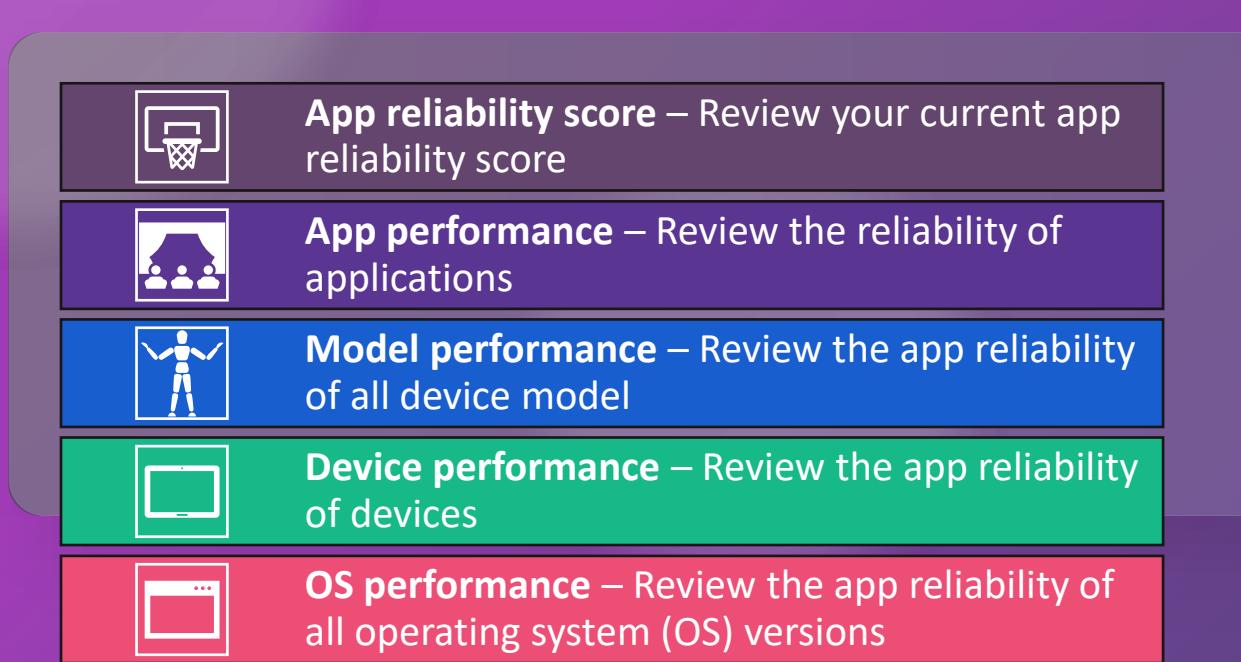
Review the restart frequency and restart type for the devices.

Reboot frequency can affect a user's experience. A device that reboots daily due to Stop errors results in poor user experience even if the boot times are fast.



# Application reliability

The app performance uses data from the past 14 days



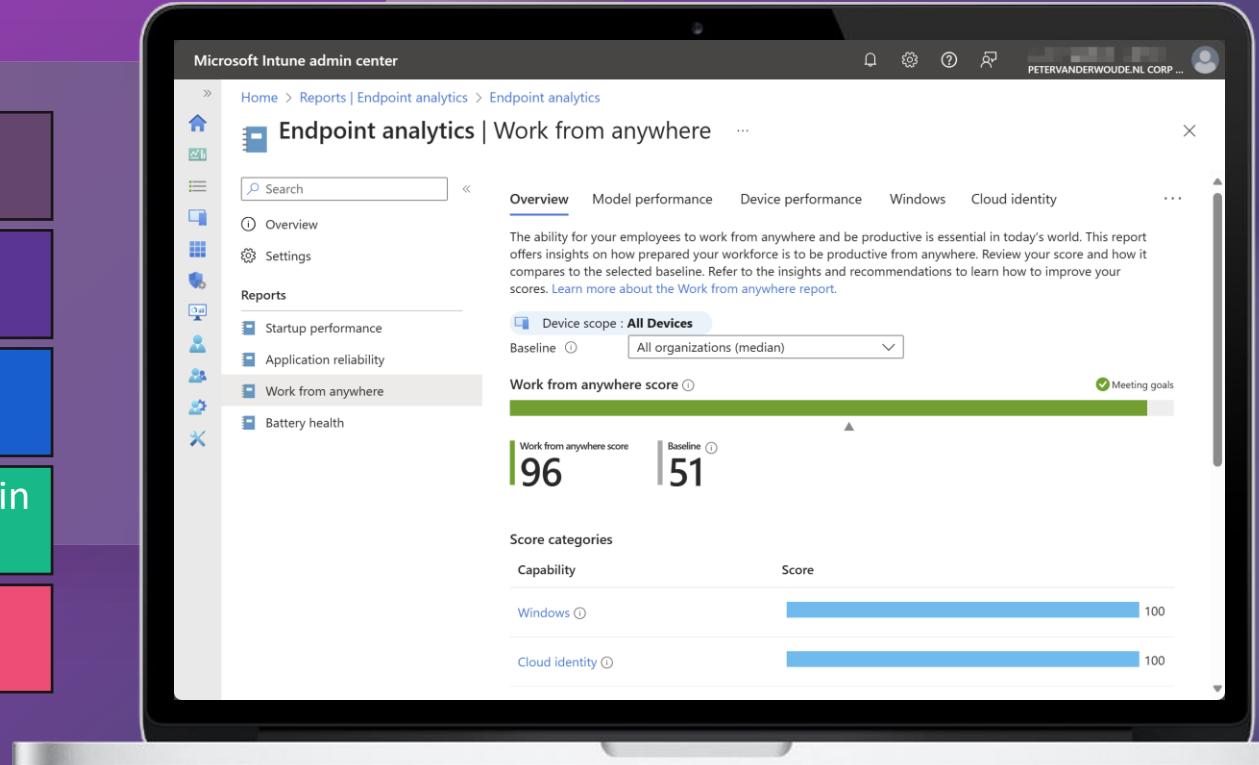
The screenshot shows the Microsoft Intune admin center interface. The left sidebar lists various management categories: Home, Reports, Device management, Device compliance, Device configuration, Group policy analytics, Windows updates, Cloud attached devices (preview), Cloud PC overview, Endpoint security, Microsoft Defender Antivirus, Firewall, Analytics, and Intune data warehouse. The main content area is titled 'Reports | Windows updates'. It features a search bar and two tabs: 'Summary' and 'Reports'. Under 'Reports', there are four options: 'Windows Feature Update Report' (Generate a report for Windows feature update status), 'Windows Expedited Update Report' (Generate a report for Windows quality update status), 'Windows Feature Update Device Readiness Report' (Select a target version of Windows and generate a report of device update readiness status), and 'Windows Feature Update Compatibility Risks Report' (Select a target version of Windows and generate a report of app and driver compatibility risks).

**BONUS:** Windows updates reports for even more insights

# Work from anywhere

The retention period for device boot and sign-in events is 29 days

-  **Overview** – Insights on how prepared your workforce is to be productive from anywhere
-  **Model performance** – Review the model performance for models
-  **Device performance** – Review the device performance for individual devices
-  **Windows** – Review devices that are evaluated in the Windows metric
-  **Cloud identity/management/provisioning** – Review devices that evaluated in cloud metrics

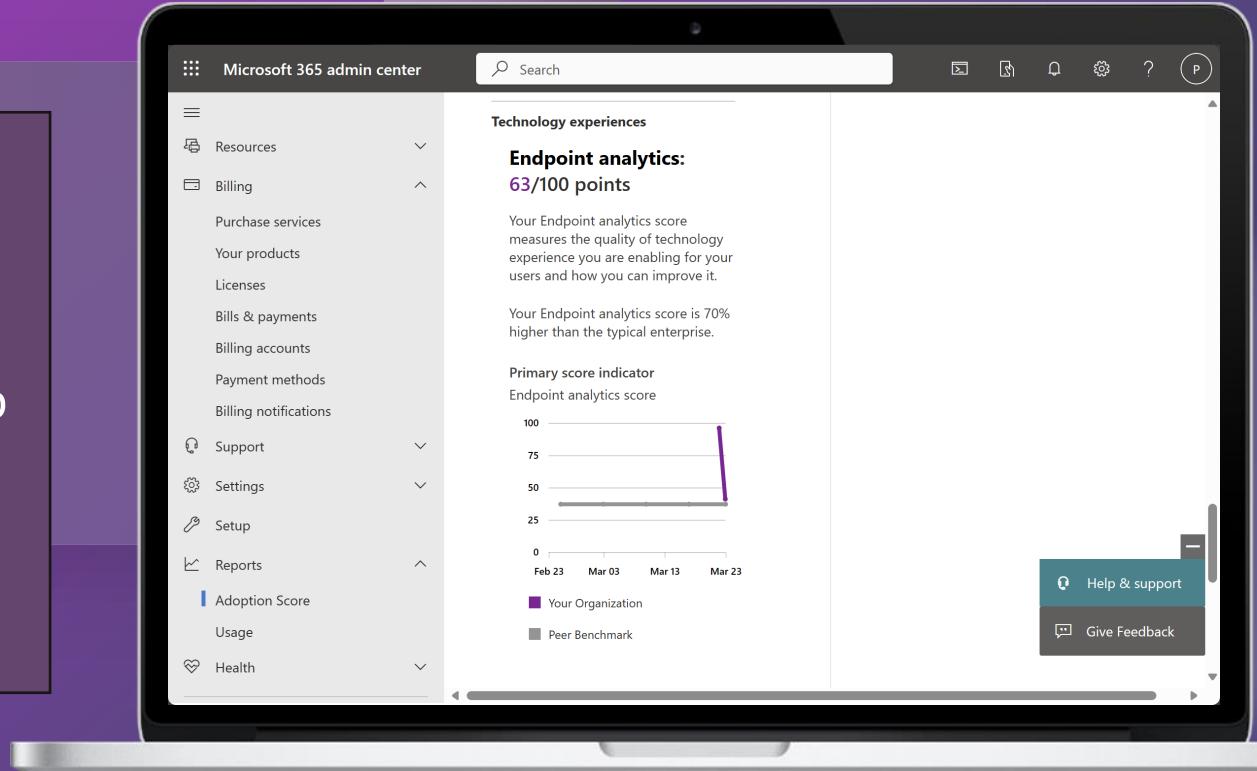


# Integration within Adoption Score

Understanding how devices contribute to the user's experience



Displaying these insights to Microsoft Adoption Score users allows them to use the data to help drive transformation efforts across the entire organization





Resources



Billing



Purchase services

Your products

Licenses

Bills &amp; payments

Billing accounts

Payment methods

Billing notifications

Support



Settings



Setup

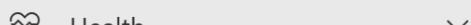
Reports



Adoption Score

Usage

Health



## Technology experiences

### Endpoint analytics:

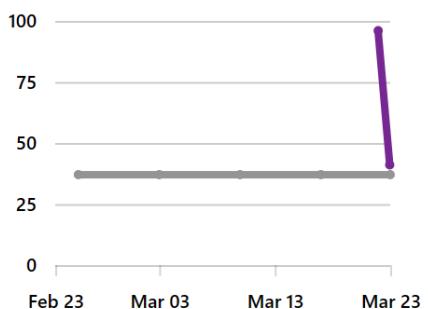
**63/100 points**

Your Endpoint analytics score measures the quality of technology experience you are enabling for your users and how you can improve it.

Your Endpoint analytics score is 70% higher than the typical enterprise.

#### Primary score indicator

Endpoint analytics score



■ Your Organization

■ Peer Benchmark

Help &amp; support

Give Feedback



Available within Microsoft Intune Suite

# What are the available components in Advanced Analytics

# Organizations still seek to fill gaps

Many still use third-party solutions



Application management lifecycle



Assist employees wherever they are



Access to corporate resources for BYO



Improve end user outcomes:  
reducing IT efforts



Enable least privilege access  
enabling standard users



Certificate management

...and they're augmenting endpoint management with 3<sup>rd</sup>-party solutions.

# What are the available components?

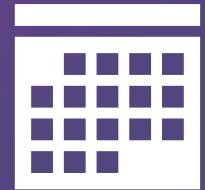
ANOMALY  
DETECTION



DEVICE  
SCOPES



ENHANCED  
DEVICE  
TIMELINE



BATTERY  
HEALTH



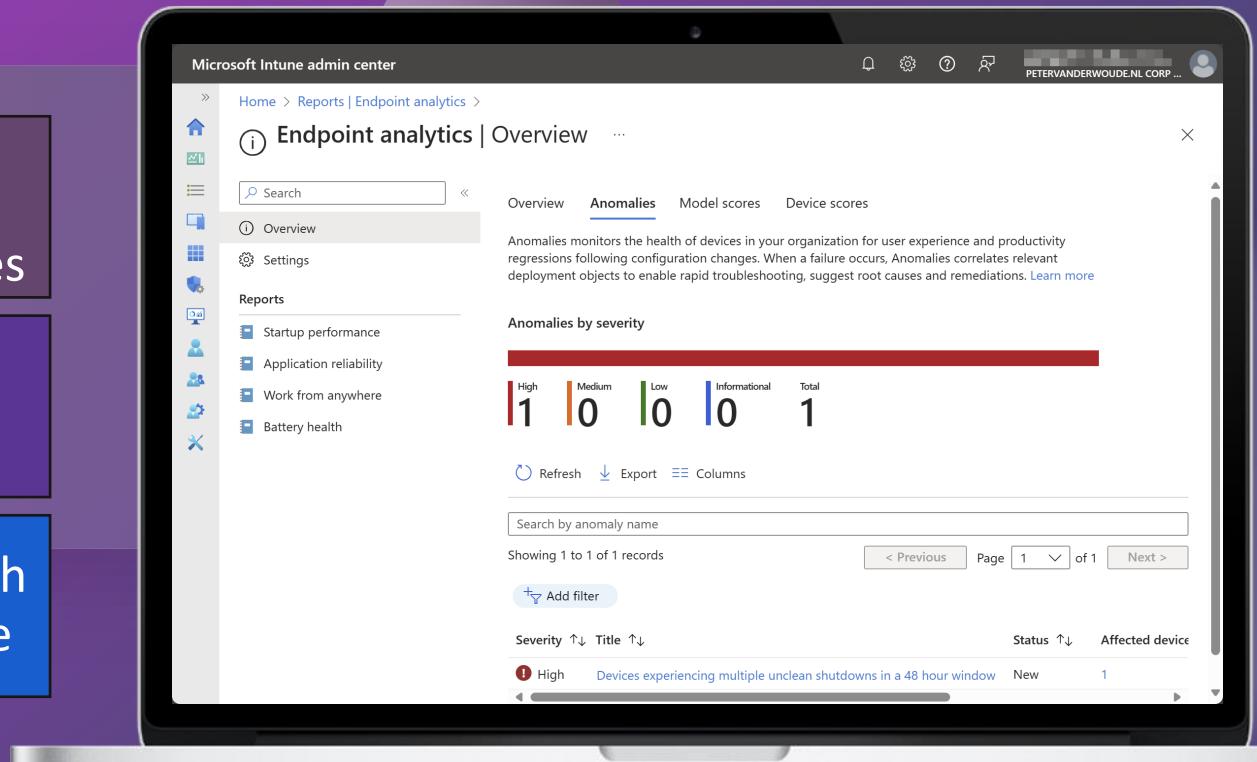
DEVICE  
QUERY



# Anomaly detection

Detecting potential problems in a system before they become a serious issue

-  **Anomalies** – Monitors the health of devices for user experience and productivity regressions after changes
-  **Correlation** – Devices are correlated based on shared attributes such as app version, OS version and model
-  **Affected devices** – List of devices with key attributes relevant to each device





... > Endpoint analytics | Overview > Devices experiencing multiple unclean shutdowns in a 48 hour window > INSPARK-1771889

## INSPARK-1771889 | User experience



Search

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Local admin password

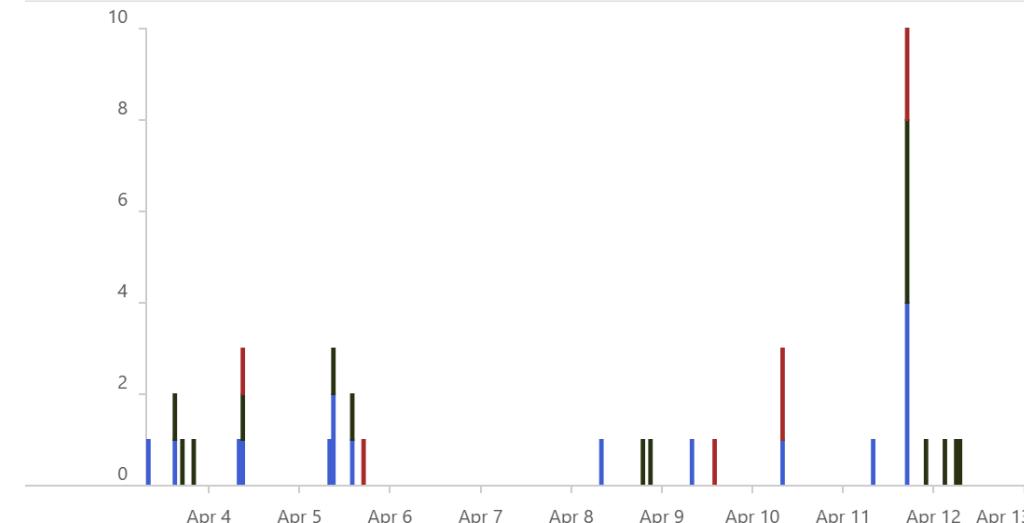
Recovery keys

User experience

Device diagnostics

Group membership

Managed Apps



Refresh

Export

Columns

Showing 1 to 40 of 127 records

< Previous

Page 1 of 4

Next >

Event ↑↓

Level ↑↓

Time ↑↓

Source ↑↓

Details ↑↓

Device Anomaly

Error

04/13/24, 02:00:00 AM

Intune anomaly detect...

Devices experiencing ...

Boot

Critical

04/12/24, 07:27:48 AM

Intune

Device booted in 26.2...

# Statistical models for determining anomalies

Brief introduction in the analytical models



**Threshold based heuristic model** – This model involves setting one or more threshold values for Application Hangs/Crashes or Stop Error Restarts



**Paired t-tests model** – This model is a mathematical method that compares pairs of observations in a dataset, looking for a statistically significant distance between their means



**Population Z-score model** – This model involves calculating standard deviation and mean of a dataset, and then using those values to determine which data points are anomalous



**Time Series Z-score model** – This model is a variation of the standard Z-score model designed for detecting anomalies in time series data

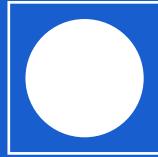
# Device scopes



Device scopes can be used to verify the data for only a subset of devices



Device scopes are based on *Scope tags* and only one *Scope tag* can be used per custom device scope



Up to 100 custom device scopes can be saved and up to 20 can be active

The screenshot shows the Microsoft Intune admin center interface. The title bar reads "Microsoft Intune admin center" and "Manage device scopes". Below the title, there is a brief description: "Device scopes focus insights and recommendations to a subset of devices you specify. Because they're precomputed, you have to turn on a device scope before you can use it. Once turned on, it could take up to 24 hours before it's ready. To create a new device scope, complete the query, and then select Save. You can turn on up to 20 saved device scopes at a time (plus any prebuilt device scopes). Learn more about device scopes in Endpoint analytics." There are two tabs: "Saved device scopes" (selected) and "Prebuilt device scopes". Below the tabs, there is a "Save" and "Discard" button. A search bar allows filtering by "Parameter", "Operator", and "Scope tag". A table below lists saved device scopes with columns for "Name", "Parameters", and "State". The table currently displays "No results."

# Enhanced device timeline



Enhanced device timeline contains the history of events for the selected device



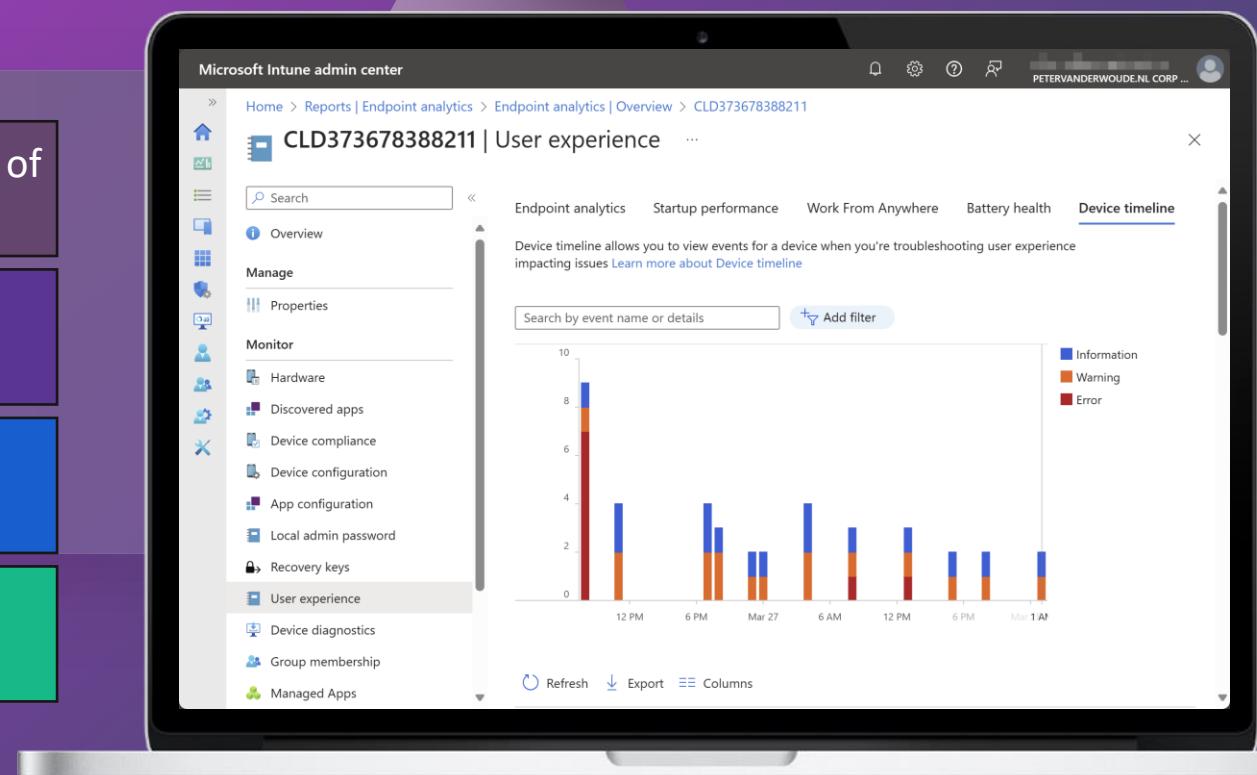
The enhanced device timeline contains app crash, app unresponsive, device boot, device logon, and anomaly detected events



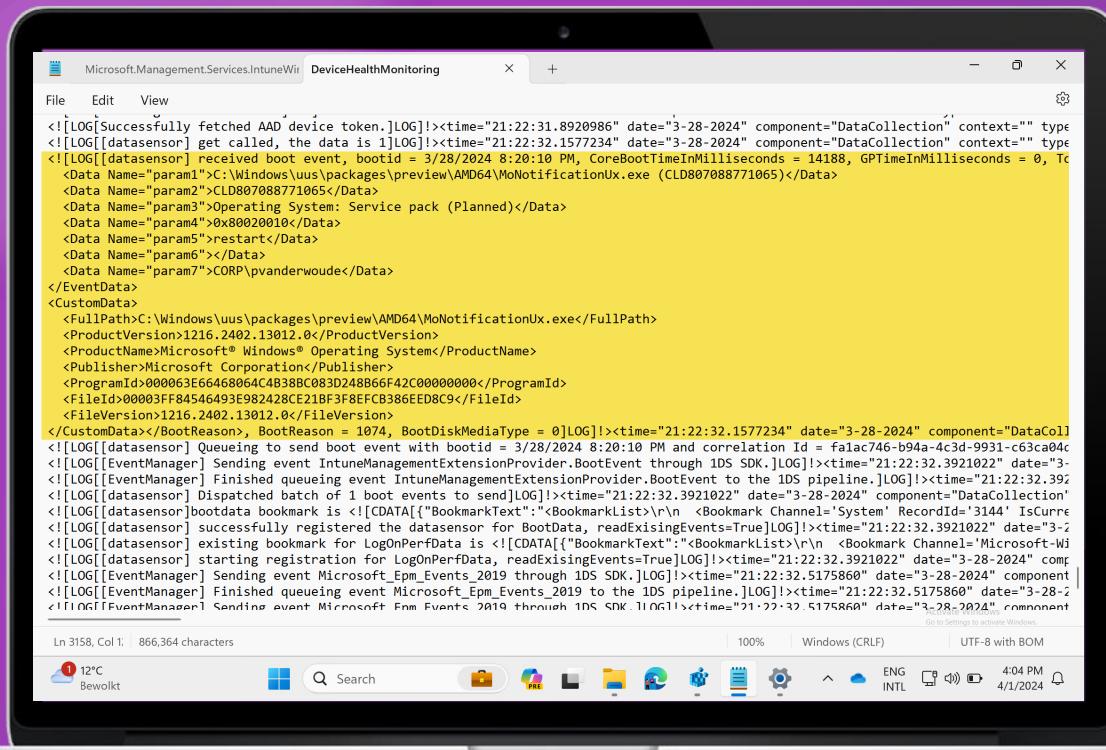
The **Device timeline** tab replaces the **Application reliability** tab when Advanced Analytics licenses are available



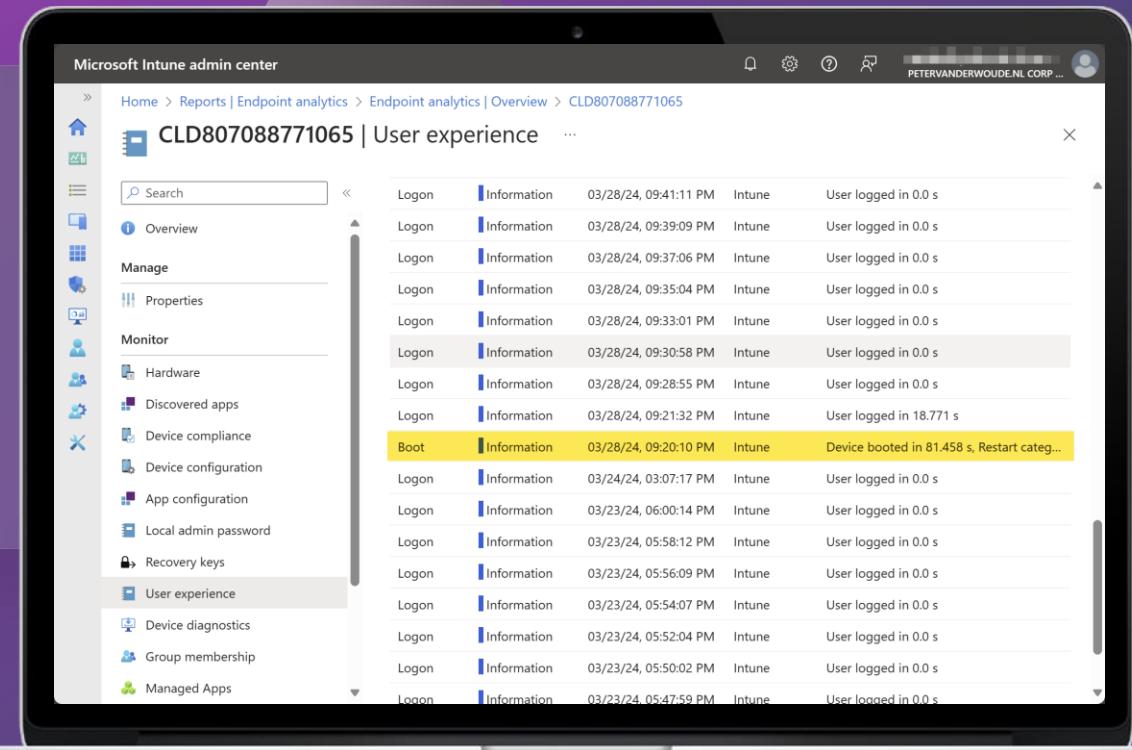
The end-to-end latency is generally under 24 hours



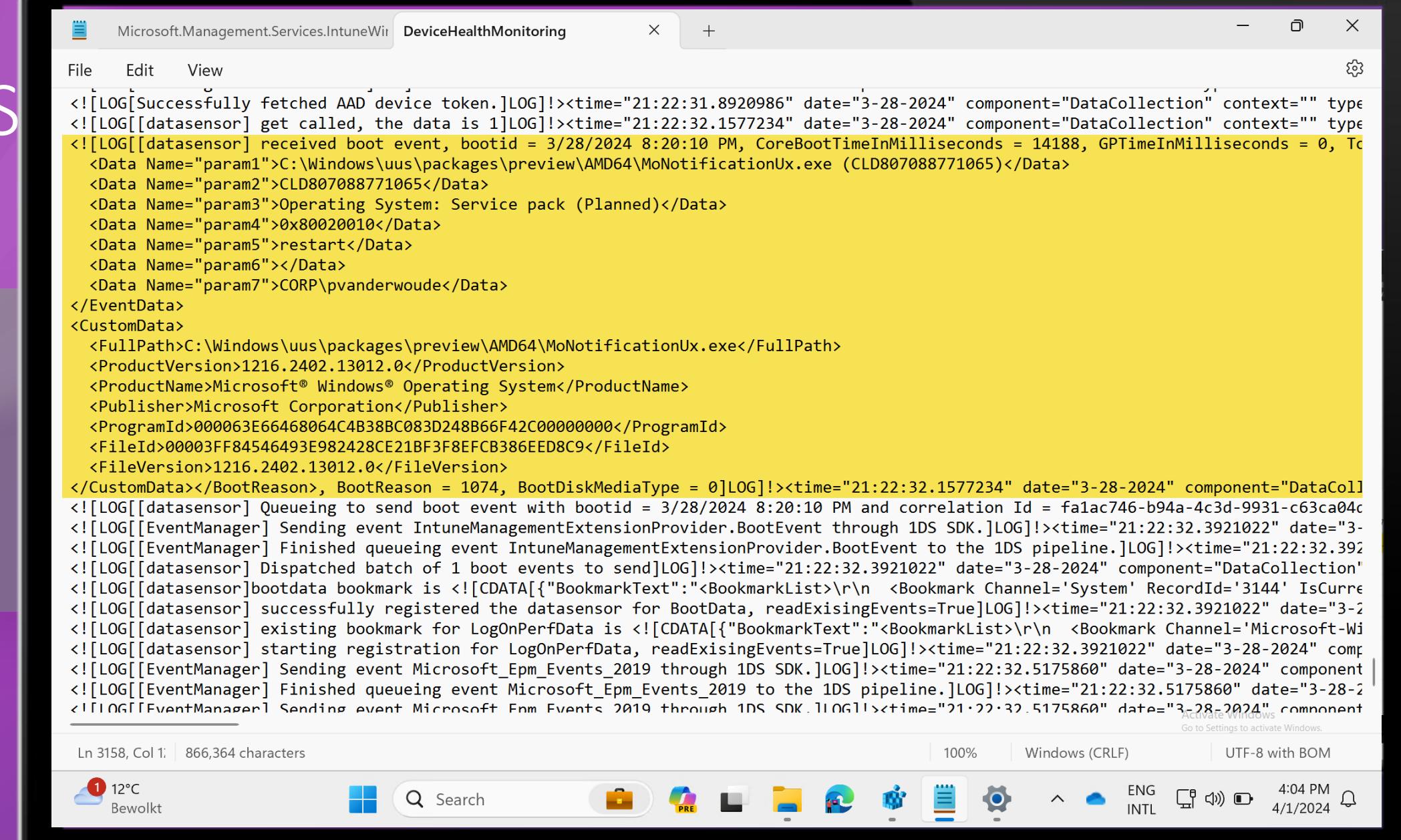
# Side-step: Following the data



```
<![LOG[Successfully fetched AAD device token.]LOG!><time="21:22:31.8920986" date="3-28-2024" component="DataCollection" context="" type="Information">
<![LOG[[datasensor] get called, the data is 1]LOG!><time="21:22:32.1577234" date="3-28-2024" component="DataCollection" context="" type="Information">
<![LOG[[datasensor] received boot event, bootid = 3/28/2024 8:20:10 PM, CoreBootTimeInMilliseconds = 14188, GPTimeInMilliseconds = 0, ToDataName="param1"]><:WIndows\us\packages\preview\AMD64\MoNotificationUx.exe (CLD807088771065)</Data>
<Data Name="param2">CLD807088771065</Data>
<Data Name="param3">Operating System: Service pack (Planned)</Data>
<Data Name="param4">0x80020010</Data>
<Data Name="param5">restart</Data>
<Data Name="param6"></Data>
<Data Name="param7">CORP\pvanderwoude</Data>
</EventData>
<CustomData>
<FullPath>C:\Windows\us\packages\preview\AMD64\MoNotificationUx.exe</FullPath>
<ProductVersion>1216.2402.13012.0</ProductVersion>
<ProductName>Microsoft® Windows® Operating System</ProductName>
<Publisher>Microsoft Corporation</Publisher>
<ProgramId>000063E6468064C4B38BC083D248B66F42C00000000</ProgramId>
<FileId>00003FF84546493E982428CE21BF3F8FCB386ED8C9</FileId>
<FileVersion>1216.2402.13012.0</FileVersion>
</CustomData></BootReason>, BootReason = 1074, BootDiskMediaType = 0]LOG!><time="21:22:32.1577234" date="3-28-2024" component="DataCollection" type="Information">
<![LOG[[datasensor] Queueing to send boot event with bootid = 3/28/2024 8:20:10 PM and correlation Id = fa1ac746-b94a-4c3d-9931-c63ca04c]LOG!><time="21:22:32.3921022" date="3-28-2024" component="EventManager" type="Information">
<![LOG[[EventManager] Sending event IntuneManagementExtensionProvider.BootEvent through IDS SDK.]LOG!><time="21:22:32.3921022" date="3-28-2024" component="EventManager" type="Information">
<![LOG[[EventManager] Finished queueing event IntuneManagementExtensionProvider.BootEvent to the IDS pipeline.]LOG!><time="21:22:32.3921022" date="3-28-2024" component="EventManager" type="Information">
<![LOG[[datasensor] Dispatched batch of 1 boot events to send]LOG!><time="21:22:32.3921022" date="3-28-2024" component="DataCollection" type="Information">
<![LOG[[datasensor] successfully registered the datasensor for BootData, readExistingEvents=True]LOG!><time="21:22:32.3921022" date="3-28-2024" component="EventManager" type="Information">
<![LOG[[datasensor] existing bookmark for LogOnPerfData is <!CDATA["BookmarkText":<BookmarkList>\r\n <Bookmark Channel='System' RecordId='3144' IsCurrent='true'>\r\n</BookmarkList>"]LOG!><time="21:22:32.3921022" date="3-28-2024" component="EventManager" type="Information">
<![LOG[[datasensor] starting registration for LogOnPerfData, readExistingEvents=True]LOG!><time="21:22:32.5175860" date="3-28-2024" component="EventManager" type="Information">
<![LOG[[EventManager] Sending event Microsoft_Epm_Events_2019 through IDS SDK.]LOG!><time="21:22:32.5175860" date="3-28-2024" component="EventManager" type="Information">
<![LOG[[EventManager] Finished queueing event Microsoft_Epm_Events_2019 to the IDS pipeline.]LOG!><time="21:22:32.5175860" date="3-28-2024" component="EventManager" type="Information">
<![LOG[[EventManager] Sending event Microsoft_Epm_Events_2019 through IDS SDK.]LOG!><time="21:22:32.5175860" date="3-28-2024" component="EventManager" type="Information">
```



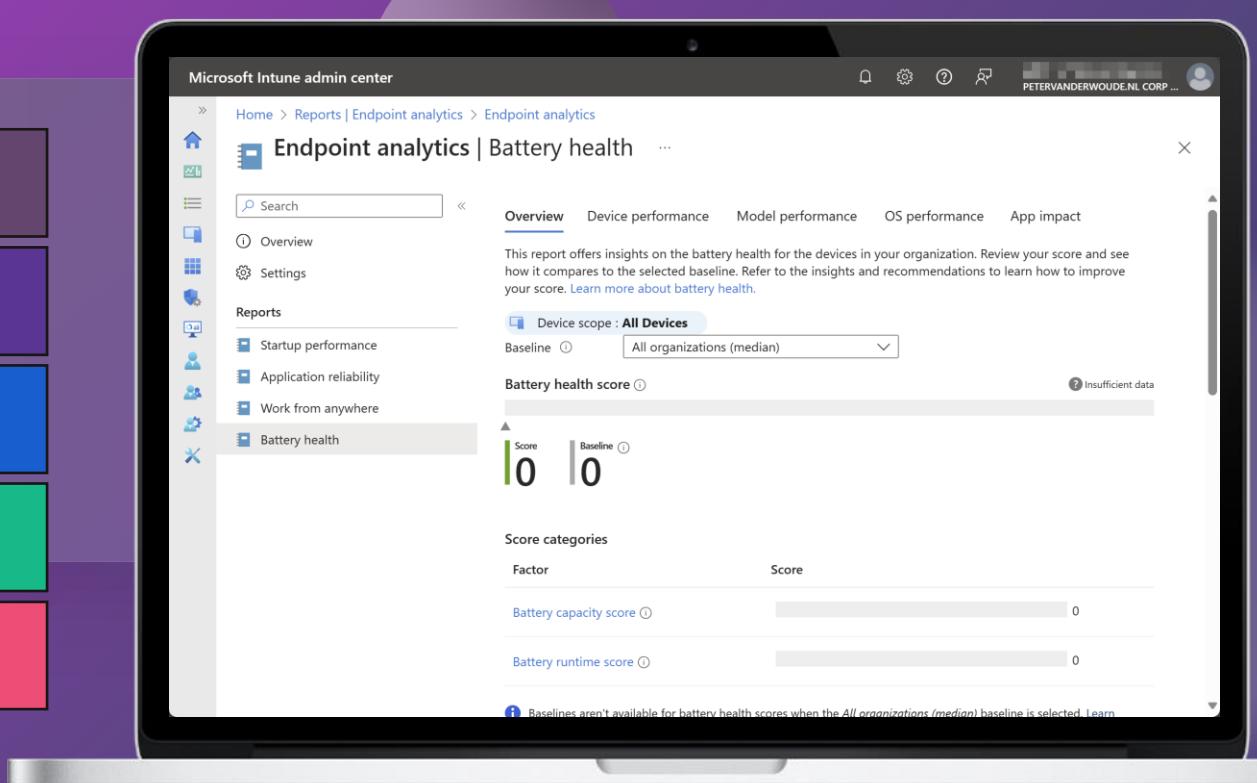
Logon	Information	03/28/24, 09:41:11 PM	Intune	User logged in 0.0 s
Logon	Information	03/28/24, 09:39:09 PM	Intune	User logged in 0.0 s
Logon	Information	03/28/24, 09:37:06 PM	Intune	User logged in 0.0 s
Logon	Information	03/28/24, 09:35:04 PM	Intune	User logged in 0.0 s
Logon	Information	03/28/24, 09:33:01 PM	Intune	User logged in 0.0 s
Logon	Information	03/28/24, 09:30:58 PM	Intune	User logged in 0.0 s
Logon	Information	03/28/24, 09:28:55 PM	Intune	User logged in 0.0 s
Logon	Information	03/28/24, 09:21:32 PM	Intune	User logged in 18.771 s
Boot	Information	03/28/24, 09:20:10 PM	Intune	Device booted in 81.458 s, Restart category...
Logon	Information	03/24/24, 03:07:17 PM	Intune	User logged in 0.0 s
Logon	Information	03/23/24, 06:00:14 PM	Intune	User logged in 0.0 s
Logon	Information	03/23/24, 05:58:12 PM	Intune	User logged in 0.0 s
Logon	Information	03/23/24, 05:56:09 PM	Intune	User logged in 0.0 s
Logon	Information	03/23/24, 05:54:07 PM	Intune	User logged in 0.0 s
Logon	Information	03/23/24, 05:52:04 PM	Intune	User logged in 0.0 s
Logon	Information	03/23/24, 05:50:02 PM	Intune	User logged in 0.0 s
Logon	Information	03/23/24, 05:47:59 PM	Intune	User logged in 0.0 s



# Battery health

Battery health uses data from the past 14 days

-  **Overview** – Insights on the battery health for the devices in your organization
-  **Device performance** – Review battery health information for devices
-  **Model performance** – Review battery health information for device models
-  **OS performance** – Review battery health information for all OS versions
-  **App impact** – Review the device usage and average battery usage for the apps



The screenshot shows the Microsoft Intune admin center interface. The top navigation bar includes Home, Reports, Endpoint analytics, and the current page, Endpoint analytics | Battery health. Below the navigation is a search bar and a sidebar with links for Overview, Settings, Reports, and specific metrics like Startup performance, Application reliability, Work from anywhere, and Battery health. The main content area displays the 'Battery health score' with a current score of 0 and a baseline of 0. It also shows 'Score categories' for Battery capacity score (0) and Battery runtime score (0). A note at the bottom states: 'Baselines aren't available for battery health scores when the All organizations (median) baseline is selected. Learn more.'

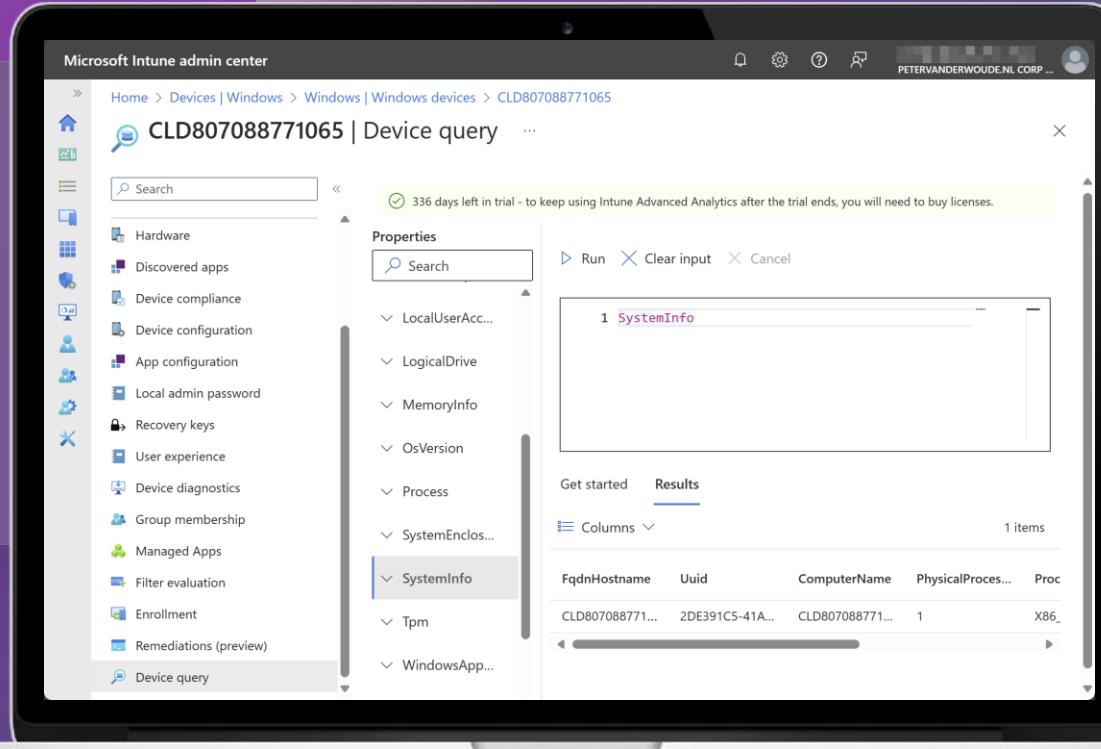
Available within Microsoft Intune Suite

# What about Device query

# Device query

Device query use real-time data by relying on the Windows push Notification Services (WNS)

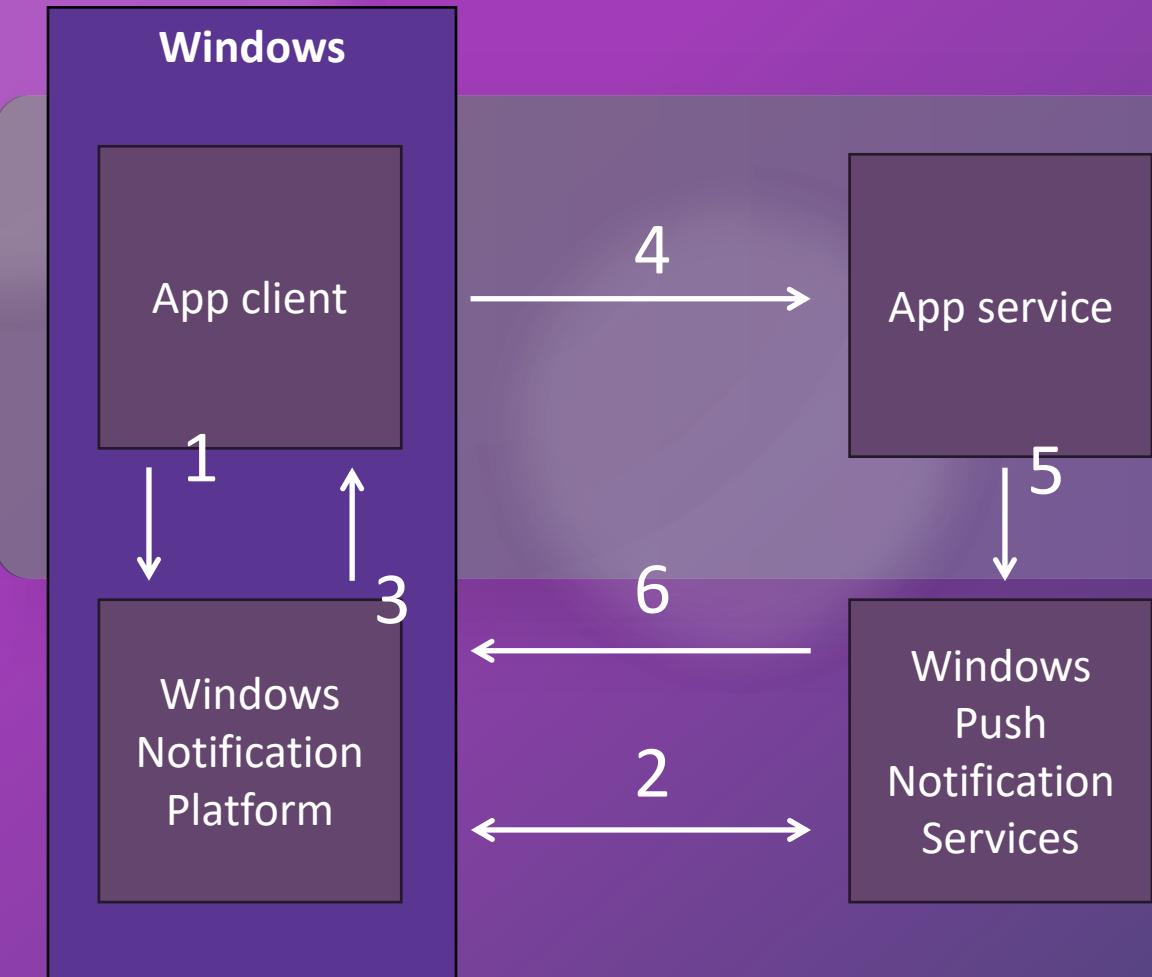
-  Device query allows you to quickly gain on-demand information about the state of devices
-  Kusto Query Language (KQL) as query language
-  Single device only with a maximum of 15 queries per minute
-  Intune data platform



The screenshot shows the Microsoft Intune admin center interface. The top navigation bar includes Home, Devices, Windows, Windows devices, and a specific device ID (CLD807088771065). The main content area is titled "CLD807088771065 | Device query". On the left, there's a sidebar with a tree view of device properties: Hardware, Discovered apps, Device compliance, Device configuration, App configuration, Local admin password, Recovery keys, User experience, Device diagnostics, Group membership, Managed Apps, Filter evaluation, Enrollment, Remediations (preview), and Device query. The "SystemInfo" node under "Properties" is expanded. In the center, there's a search bar with placeholder "Search" and a "Run" button. Below it, a results table has one item listed: "1 SystemInfo". The table has columns: FqdnHostname, Uuid, ComputerName, PhysicalProces..., and Proc. The first row shows values: CLD807088771..., 2DE391C5-41A..., CLD807088771..., 1, X86\_.

# Windows push notification services

Brief introduction in the Windows push Notification Services (WNS)



1. The app requests a push notification channel from WNS
- 2a. Windows asks WNS to create a notification channel
- 2b. WNS returns the created channel as an URI
3. The channel URI is returned by WNS to the app
4. The app sends the URI to their own cloud service
5. The cloud service can send an update by notifying WNS using the channel URI
6. WNS receives the request and routes the notification to the appropriate device

# Intune data platform

A general overview



Device query allows you to quickly assess the state of devices in your environment and take action. When you enter a query on a selected device, Device query runs a query in real time. The data returned can then be filtered, grouped, and refined to answer questions, troubleshoot issues in environment, or respond to security threats

The screenshot shows a Microsoft Intune documentation page titled "Intune data platform". The page includes a sidebar with navigation links like "Overview", "Intune Advanced Analytics", "Data platform schema" (which is highlighted), and "Battery health". The main content area contains a summary of what Device query does, a "Feedback" link, and a note about the article's scope.

Microsoft Intune Product documentation ▾ Learn Intune Developer resources ▾ Troubleshooting Resources ▾ Portal Free account

Learn / Microsoft Intune / Endpoint analytics / Intune data platform Article • 02/01/2024 • 1 contributor Feedback

In this article

- BiosInfo
- Certificate
- CPU
- DiskDrive

Show 17 more

Applies to: Microsoft Intune

This article goes over the properties supported in the Intune Data Platform.

Device query allows you to quickly assess the state of devices in your environment and take action. When you enter a query on a selected device, Device query runs a query in real time. The data returned can then be filtered, grouped, and refined to answer business questions, troubleshoot issues in your environment, or respond to security threats.

Each table (entity) in this page lists the types of queries that are supported.

# Intune data platform

An overview of the available entities

- BiosInfo
- Certificate
- CPU
- DiskDrive
- EncryptableVolume
- FileInfo
- LocalGroup
- LocalUserAccount
- LogicalDrive
- MemoryInfo

- OsVersion
- Process
- SystemEnclosure
- SystemInfo
- Tpm
- WindowsAppCrashEvent
- WindowsDriver
- WindowsEvent
- WindowsQfe
- WindowsRegistry

- WindowsService

# Automating Device query

Using Device query via Microsoft Graph to still try to achieve multi-device query

The diagram illustrates the process of generating a query. It starts with a square icon containing an upward-pointing arrow, followed by the URL <https://graph.microsoft.com/beta/deviceManagement/managedDevices/5cf82b64-24c2-4191-8418-1901b9ff263e/createQuery>. Below this is a skeleton icon, followed by the JSON payload: { "query": "U3lzdGVtSW5mbw=="}.

<https://graph.microsoft.com/beta/deviceManagement/managedDevices/5cf82b64-24c2-4191-8418-1901b9ff263e/createQuery>

{ "query": "U3lzdGVtSW5mbw=="}

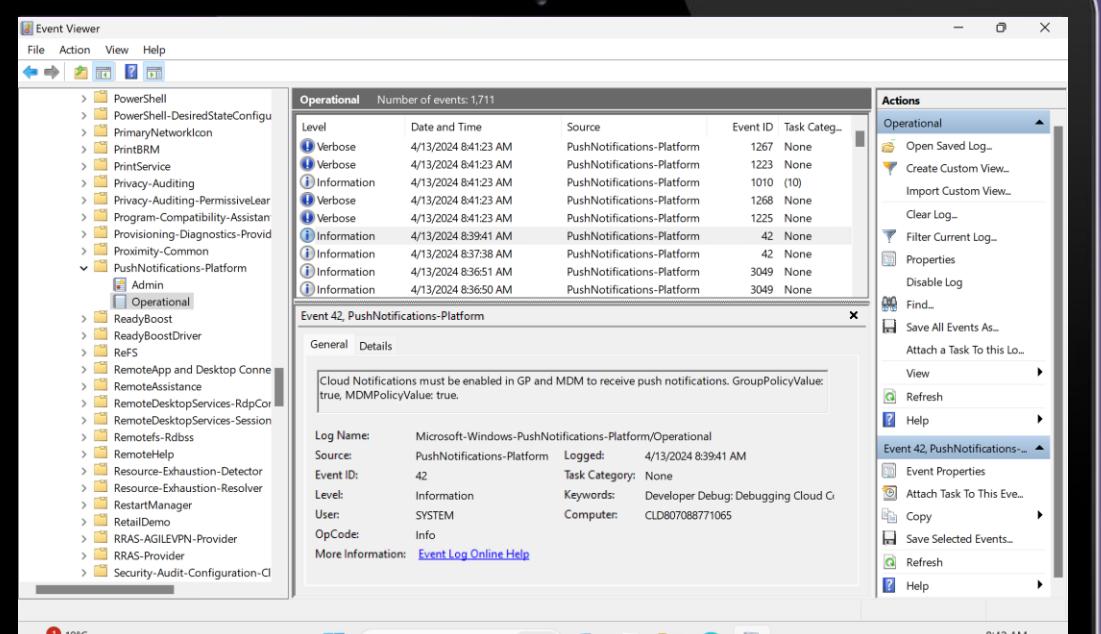
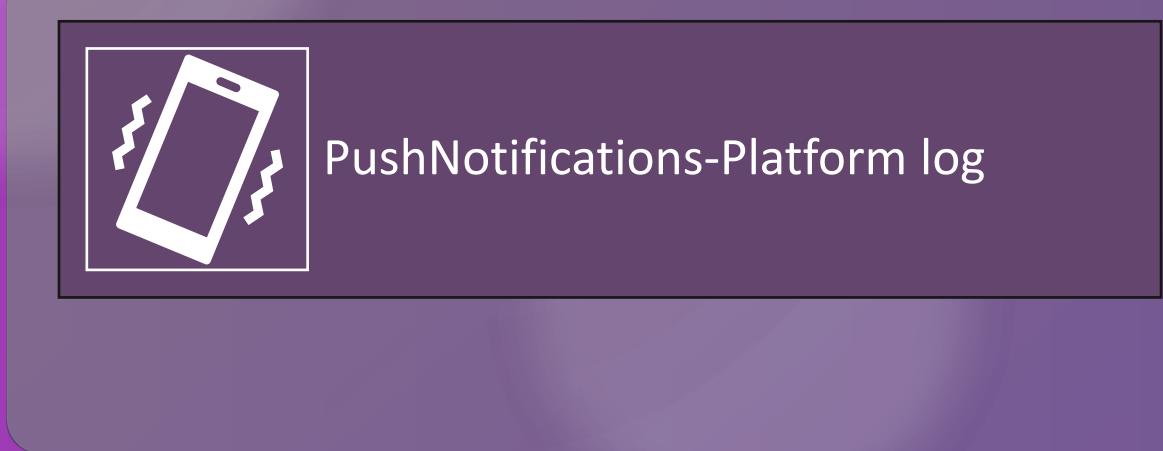
<https://graph.microsoft.com/beta/deviceManagement/managedDevices/5cf82b64-24c2-4191-8418-1901b9ff263e/queryResults/c9e307e4-12c0-4d3e-ad5f-d09cef95576f>

The screenshot shows the Microsoft Graph Explorer tool. The URL entered is <https://graph.microsoft.com/beta/deviceManagement/managedDevices/5cf82b64-24c2-4191-8418-1901b9ff263e/createQuery>. The request body contains the JSON payload: { "query": "U3lzdGVtSW5mbw=="}.

The response preview shows a 403 Forbidden error:

```
{
  "error": {
    "code": "Forbidden",
    "message": "( \\"version\\": 3, \\"Message\\": \"Application is not authorized to perform this operation. Application must have one of the following scopes: DeviceManagementManagedDevices.ReadWrite.All - Operation ID (for customer support): 00000000-0000-0000-0000-000000000000 - Activity ID: 9f67addc-c0e4-7c04-cabd-751b5963474c - Url: https://fe1.amsub0502.manage.microsoft.com/DeviceFE/StatelessDeviceEService/deviceManagement/managedDevices('5cf82b64-24c2-4191-8418-1901b9ff263e')/microsoft.management.services.api.createQuery/api-version=5023-12-26\", \\"CustomApiErrorPhrase\\": \"\", \\"RetryAfter\\": null, \\"ErrorSourceService\\": \"\", \\"HttpHeaders\\": \"{}\" },
    "innerError": {
      "date": "2024-03-30T14:41:06",
      "request-id": "92e22531-d9f5-4bbd-922a-aa23bfed9d0a",
      "client-request-id": "92e22531-d9f5-4bbd-922a-aa23bfed9d0a"
    }
}
```

# Following Device query



The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists various Windows services and components. In the center, the 'Operational' log for 'PushNotifications-Platform' is displayed, showing multiple entries. One specific event is highlighted:

Level	Date and Time	Source	Event ID	Task Category
Information	4/13/2024 8:39:41 AM	PushNotifications-Platform	42	None

Details for Event 42, PushNotifications-Platform:

General Details

Cloud Notifications must be enabled in GP and MDM to receive push notifications. GroupPolicyValue: true, MDMPolicyValue: true.

Log Name: Microsoft-Windows-PushNotifications-Platform/Operational  
Source: PushNotifications-Platform Logged: 4/13/2024 8:39:41 AM  
Event ID: 42 Task Category: None  
Level: Information Keywords: Developer Debug: Debugging Cloud G  
User: SYSTEM Computer: CLD807088771065  
OpCode: Info  
More Information: [Event Log Online Help](#)

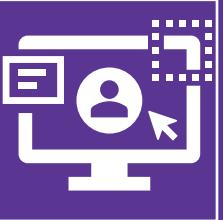
Actions

- Operational
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To This Log...
- View
- Refresh
- Help

# Following Device query



PushNotifications-Platform log



IntuneManagementExtenison.log

```
IntuneManagementExtension
```

File Edit View

```
<!LOG[OnSessionChange: ConsoleConnect]LOG!><time="14:55:24.7875572" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[DeviceAction] Receive message from push notification event. message is {
```

NotificationIntent': 5,  
"NotificationID": "72da7daa-313a-45d6-a600-2e9fd587e7c1",  
"Version": 1,  
"Arguments": {}  
"QueryID": "56278a51-d0e2-42a8-c6f71f77a761"

```
}
```

```
<!LOG[><time="14:55:37.0871113" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[DeviceAction] PushNotification workload start with id: 72da7daa-313a-45d6-a600-2e9fd587e7c1,intent: IntunePivot , version
```

Successfully updated throttling info. workload DeviceActionCheckIn, currentCnt = 1<LOG>|><time="14:55:37.0871113" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[Finish throttle checking.]LOG!><time="14:55:37.0871113" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[DeviceAction] saving throttle info<LOG!><time="14:55:37.0871113" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[Found 1 MDM certificates from Local Computer Store.]LOG!><time="14:55:37.0871113" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[DeviceAction] Refreshed MDM device certificate, CN is CN=5cf82b64-24c2-4191-8418-1901b9f263e, expiry is 3/3/2025 4:57:07 AM<LOG>
<!LOG[DeviceAction] Get 2 active user sessions<LOG!><time="14:55:37.1028170" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[starting impersonation, session id = 1]><time="14:55:37.1028170" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[After impersonation: CORPvanderwoude]><LOG!><time="14:55:37.1028170" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[TokenManager :GetTokenForNewRequestUsingDeviceCheckInAppId]><LOG!><time="14:55:37.1028170" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[provider id = https://login.microsoft.com, authority = organizations]><LOG!><time="14:55:37.1184193" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[get provider, provider name = Work or school account]><LOG!><time="14:55:37.1184193" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[Successfully get the token with client id fc0f3af4-6835-4174-b806-f7db311fd2f3 and resource id 26a4ae64-5862-427f-a9b0-044e62572&ampgt<LOG!><time="14:55:37.1497155" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[Valid AAD user session id : 1]><LOG!><time="14:55:37.1497155" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[starting impersonation, session id = 159]><LOG!><time="14:55:37.1497155" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[LogonUser failed with error code : 1008]><LOG!><time="14:55:37.1497155" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="22" file="">
<!LOG[AAD User check is failed, exception is System.ComponentModel.Win32Exception (0x80004005): An attempt was made to reference a token at Microsoft.Management.Services.IntuneWindowsAgent.AgentCommon.ImpersonateHelper.<DoAction>withImpersonation>d\_\_4.MoveNext() --- End of stack trace from previous location where exception was thrown --- at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task) at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)

Ln 1, Col 1 2,980,572 characters

11°C Bewolkt

Search

File Edit View

Activate Windows  
Go to Settings to activate Windows

100% Show hidden icons

UTF-8 with BOM

3:01 PM ENG INTL 4/1/2024

F  
L  
E

# IntuneManagementExtension

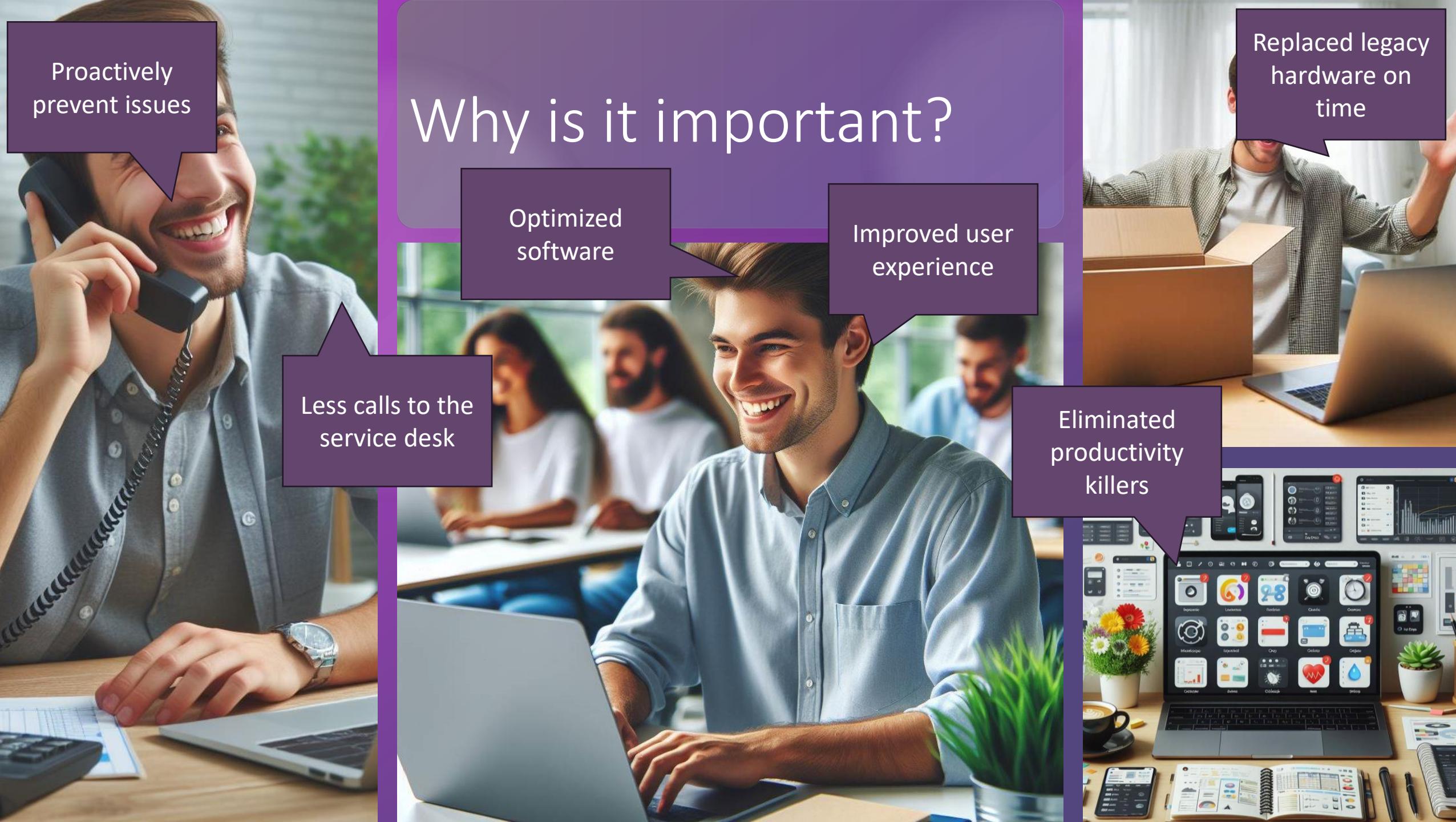
File Edit View 

```
Microsoft Azure TLS Issuing CA 05:DigiCert Global Root G2|7/29/2020 2:30:00 PM|6/28/2024 1:59:59 AM|6C3AF02E7F269AA73AFD0EFF2A88A4A1F04E  
DeviceQuerySigning.manage.microsoft.com:Microsoft Azure TLS Issuing CA 05|12/1/2023 12:04:10 AM|6/28/2024 1:59:59 AM|A3401A56F7AE5A142CF  
]LOG!]><time="14:55:37.7946673" date="4-1-2024" component="IntuneManagementExtension" context="" type="1" thread="33" file="">  
<!LOG[[IntunePivot] Validated device query with data protection for QueryId 56278a51-d0e2-42a8-8fb0-c6f71f77a761]LOG!]><time="14:55:38.  
<!LOG[[IntunePivot] Getting entity]LOG!]><time="14:55:38.0305209" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[IntunePivot] Parsed Query]LOG!]><time="14:55:38.0305209" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[IntunePivot] Finished evaluating Query]LOG!]><time="14:55:38.0616996" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[IntunePivot] Encrypting and signing query result for QueryId = 56278a51-d0e2-42a8-8fb0-c6f71f77a761]LOG!]><time="14:55:38.0616996" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[IntunePivot] Encryption/signing complete for QueryId = 56278a51-d0e2-42a8-8fb0-c6f71f77a761]LOG!]><time="14:55:38.1092940" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[IntunePivot] Completed getting results, return code: 0]LOG!]><time="14:55:38.1092940" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[IntunePivot] Ran query complete, query result: QueryId = 56278a51-d0e2-42a8-8fb0-c6f71f77a761; QueryReturnCode=0; QueryErrorMessage=""]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[IntunePivot] Sending query result with GW session id b1951cf5-8113-4606-b50b-5eb7fea427a1 ...]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[send query results to service..]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[ServiceBase], check in using device check in AAD App]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[SendWebRequestInternal] iteration [0] started, total retryCount: 0]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[PrepareHeaders, client-request-id: c52fb245-1aa8-48a4-bbb1-7e94eb380bc7, Method: PUT]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[Getting UserToken For Web Request...]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[starting impersonation, session id = 1]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[After impersonation: CORP\pvanderwoude]LOG!]><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[TokenManager::GetTokenForNewRequestUsingDeviceCheckInAppId]]LOG!]><time="14:55:38.1404811" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[provider id = https://login.microsoft.com, authority = organizations]LOG!]><time="14:55:38.1404811" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[get provider, provider name = Work or school account]LOG!]><time="14:55:38.1404811" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[Successfully get the token with client id fc0f3af4-6835-4174-b806-f7db311fd2f3 and resource id 26a4ae64-5862-427f-a9b0-044e62572a]LOG!]><time="14:55:38.1560118" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[Add UserToken with length 1963 into WebRequest]LOG!]><time="14:55:38.1560118" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[Found 1 MDM certificates from Local Computer Store.]LOG!]><time="14:55:38.1560118" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[Add MdmDeviceCertificate 8BFA0DB7E35B73AA8395C9BE717E20C219A67034 into WebRequest with True]LOG!]><time="14:55:38.1560118" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[SendWebRequestInternal] Sending network request... Current proxy is https://fef.amsub0502.manage.microsoft.com/TrafficGateway/1]LOG!]><time="14:55:38.15641396" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[SendWebRequestInternal] Succeeded]LOG!]><time="14:55:38.15641396" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[Query results are successfully sent.]LOG!]><time="14:55:38.15641396" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"  
<!LOG[[DeviceAction] event thread stopped.]LOG!]><time="14:55:38.15641396" date="4-1-2024" component="IntuneManagementExtension" context="" type="1"
```

Activate Windows  
Go to Settings to activate Windows.

Ln 13146, Col 1 | 2,980,572 characters | 100% | Windows (CRLF) | UTF-8 with BOM

Nieuws Hobbyboer laat...   Search         ENG INTL 3:19 PM 4/1/2024 



# Why is it important?

Proactively prevent issues

Less calls to the service desk

Optimized software

Improved user experience

Eliminated productivity killers

Replaced legacy hardware on time

