Session:

Date 19 April: 11:25

Simplify device management with data and AI

Peter van der Woude

MODERN ENDPOINT MANAGEMENT

Welcome to:

MODERN
ENDPOINT
MANAGEMENT

SUMMIT 2024

APRIL 17 - 19

GOLD PARTNERS

controlUP

Microsoft

THANK YOU PARTNERS

GOLD PARTNERS

controlUP

Microsoft

SILVER PARTNERS

adaptiva

LIQUIT
Part of RECAST SOFTWARE

PATCH MY PC

TANIUM

Rimo3

BRONZE PARTNERS

Synapsys

SPEAKER

Peter van der Woude

www.petervanderwoude.nl

@pvanderwoude

/peterwoude

MODERN ENDPOINT MANAGEMENT SUMMIT EMEA 2024

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
DELL

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

Why is it important?

Proactively detect issues

Prevent calls to the service desk

Optimize software

Improve the user experience

Replace legacy hardware on time

Eliminate productivity killers

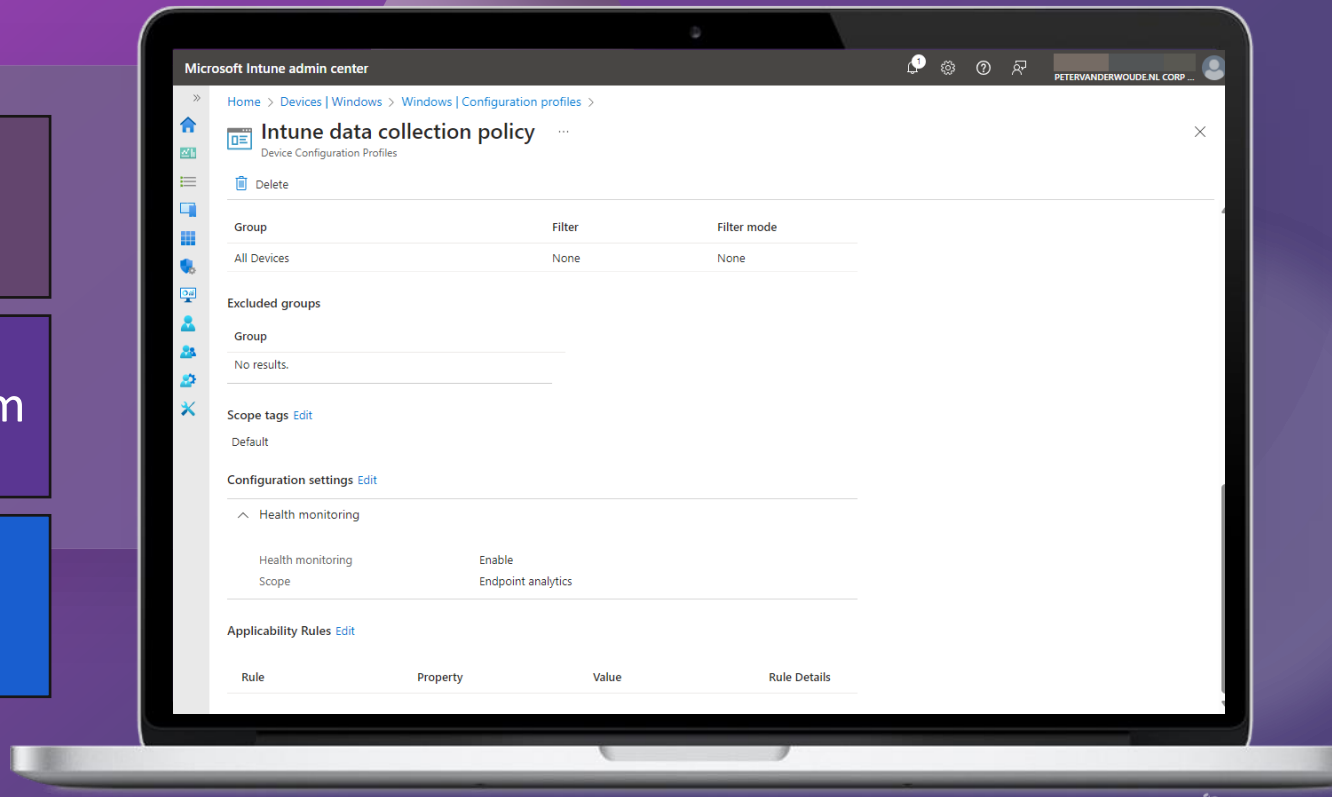
But first: Getting started

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

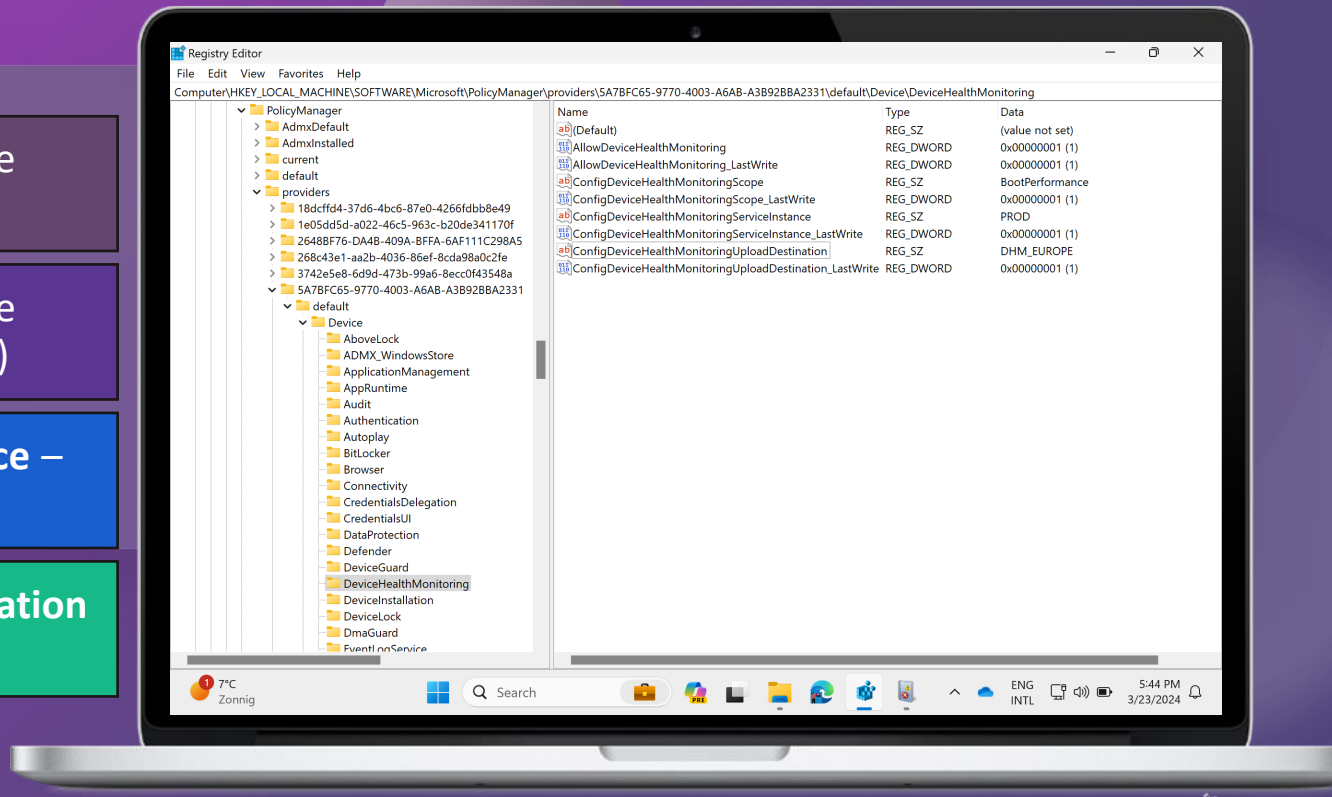


MODERN ENDPOINT MANAGEMENT

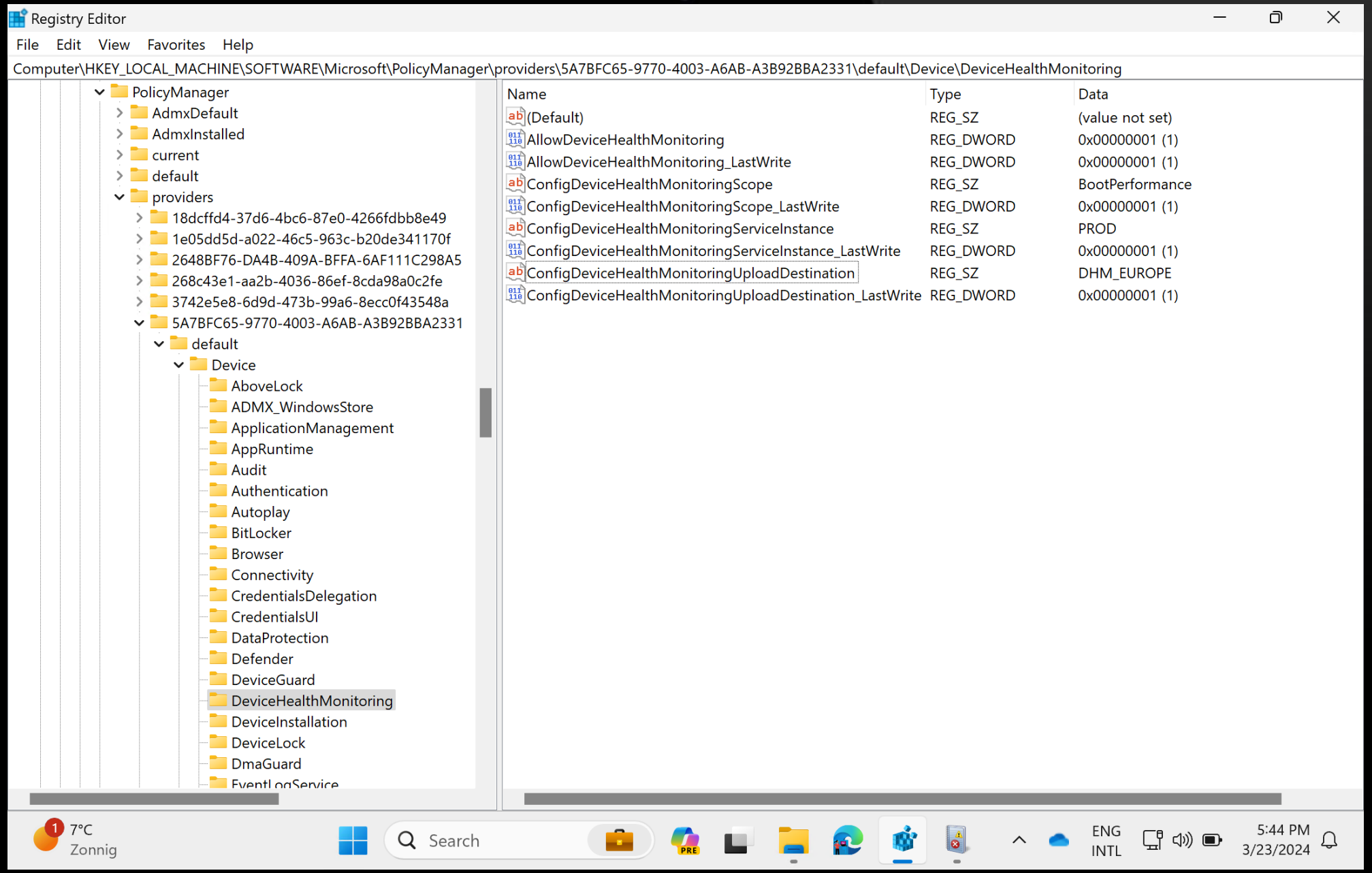
Verifying the configuration on the device

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*)



MODERN ENDPOINT MANAGEMENT


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\providers\5A7BFC65-9770-4003-A6AB-A3B92BBA2331\default\Device\DeviceHealthMonitoring
PolicyManager
AdmxDefault
AdmxInstalled
current
default
providers
18dcffd4-37d6-4bc6-87e0-4266fdbb8e49
1e05dd5d-a022-46c5-963c-b20de341170f
2648BF76-DA4B-409A-BFFA-6AF111C298A5
268c43e1-aa2b-4036-86ef-8cda98a0c2fe
3742e5e8-6d9d-473b-99a6-8ecc0f43548a
5A7BFC65-9770-4003-A6AB-A3B92BBA2331
default
Device
AboveLock
ADMX_WindowsStore
ApplicationManagement
AppRuntime
Audit
Authentication
Autoplay
BitLocker
Browser
Connectivity
CredentialsDelegation
CredentialsUI
DataProtection
Defender
DeviceGuard
DeviceHealthMonitoring
DeviceInstallation
DeviceLock
DmaGuard
EventLogService
Name Type Data
(Default) REG_SZ (value not set)
AllowDeviceHealthMonitoring REG_DWORD 0x00000001 (1)
AllowDeviceHealthMonitoring_LastWrite REG_DWORD 0x00000001 (1)
ConfigDeviceHealthMonitoringScope REG_SZ BootPerformance
ConfigDeviceHealthMonitoringScope_LastWrite REG_DWORD 0x00000001 (1)
ConfigDeviceHealthMonitoringServiceInstance REG_SZ PROD
ConfigDeviceHealthMonitoringServiceInstance_LastWrite REG_DWORD 0x00000001 (1)
ConfigDeviceHealthMonitoringUploadDestination REG_SZ DHM_EUROPE
ConfigDeviceHealthMonitoringUploadDestination_LastWrite REG_DWORD 0x00000001 (1)
7°C
Zonnig
Search
ENG
INTL
5:44 PM
3/23/2024

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 update 24-hours before the data is populated
- The collected data falls in the **Optional** data category

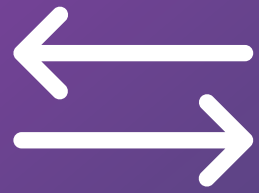
Available within Microsoft Intune P1

What are the available components in Endpoint Analytics

What are the available components?

SCORES

BASELINES



INSIGHTS

(PROACTIVE) REMEDIATIONS

MODERN ENDPOINT MANAGEMENT

Startup performance

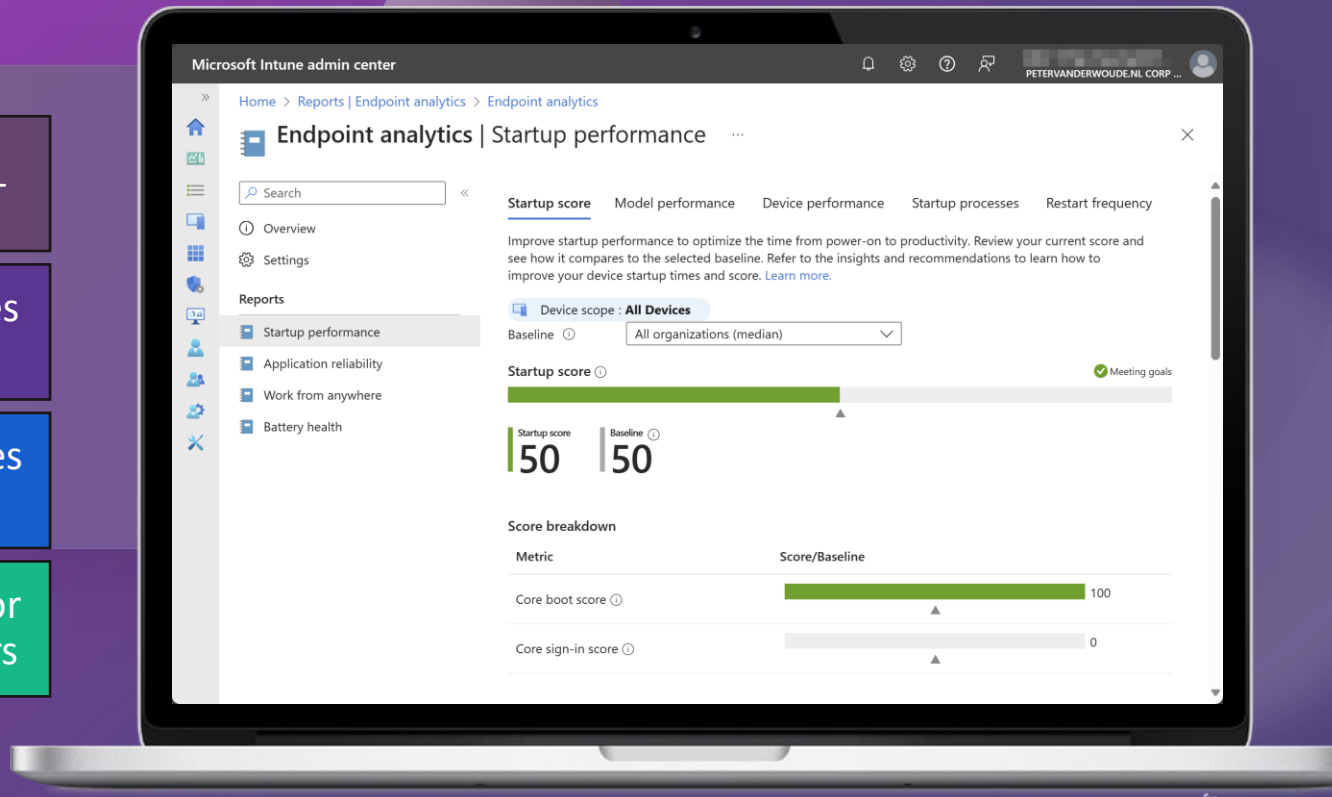
The retention period for device boot and sign-in events is 29 days

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



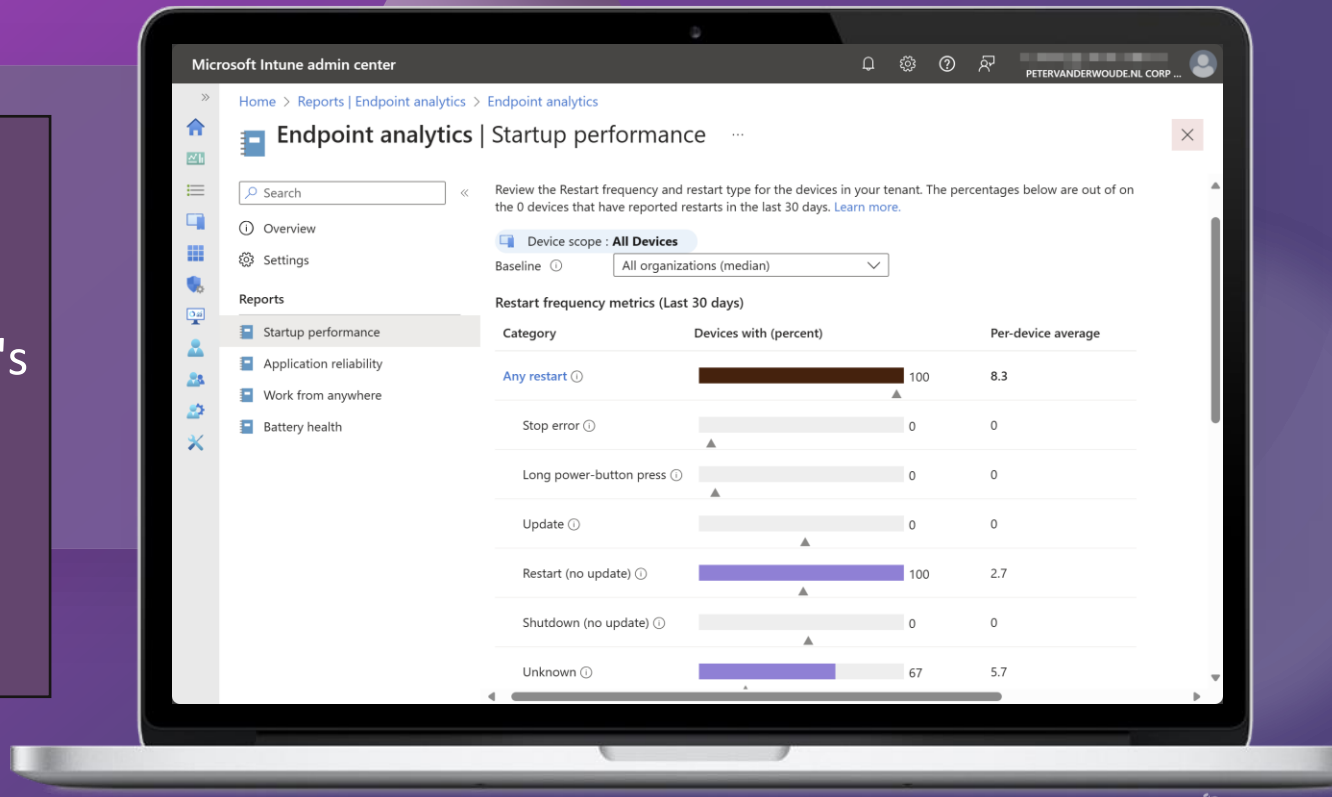
MODERN ENDPOINT MANAGEMENT

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.

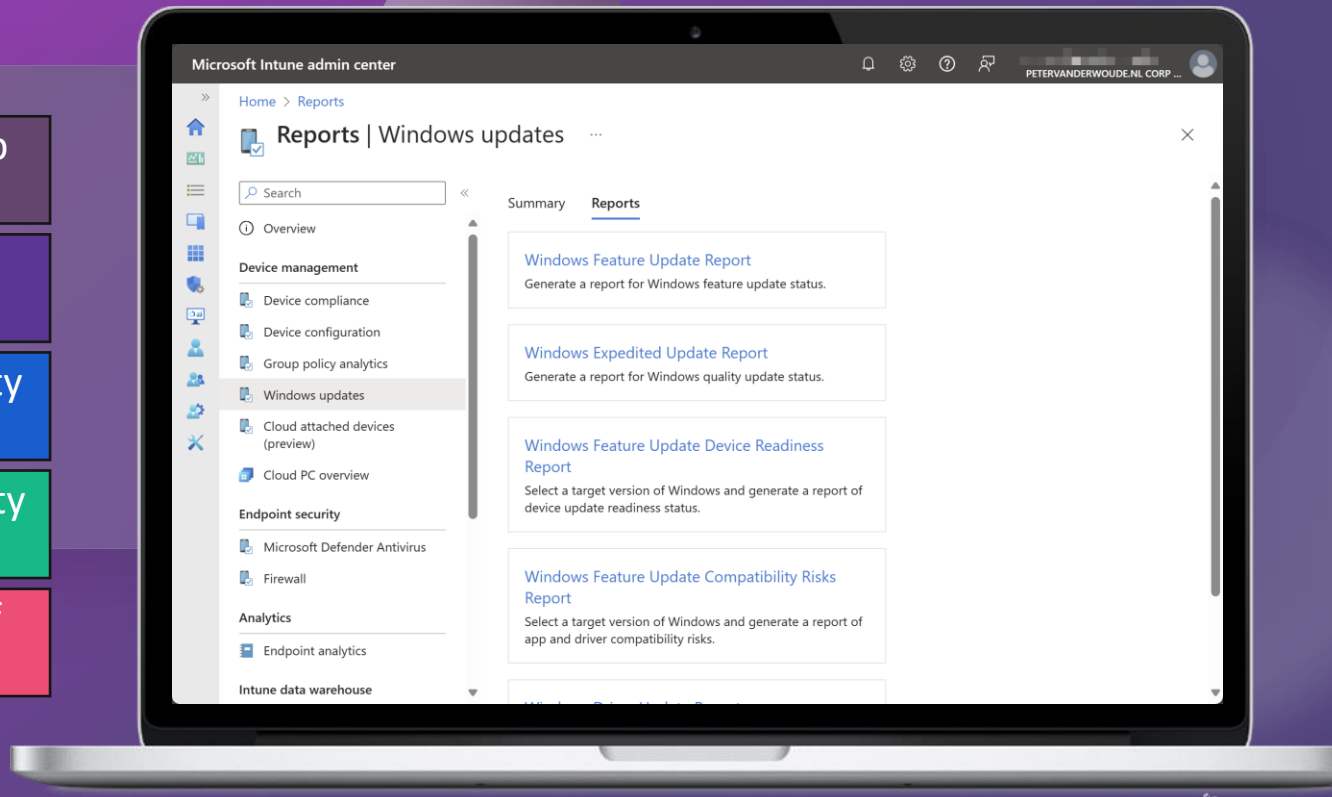


MODERN ENDPOINT MANAGEMENT

Application reliability

The app performance uses data from the past 14 days

- **App reliability score** – Review your current app reliability score
- **App performance** – Review the reliability of applications
- **Model performance** – Review the app reliability of all device model
- **Device performance** – Review the app reliability of devices
- **OS performance** – Review the app reliability of all operating system (OS) versions

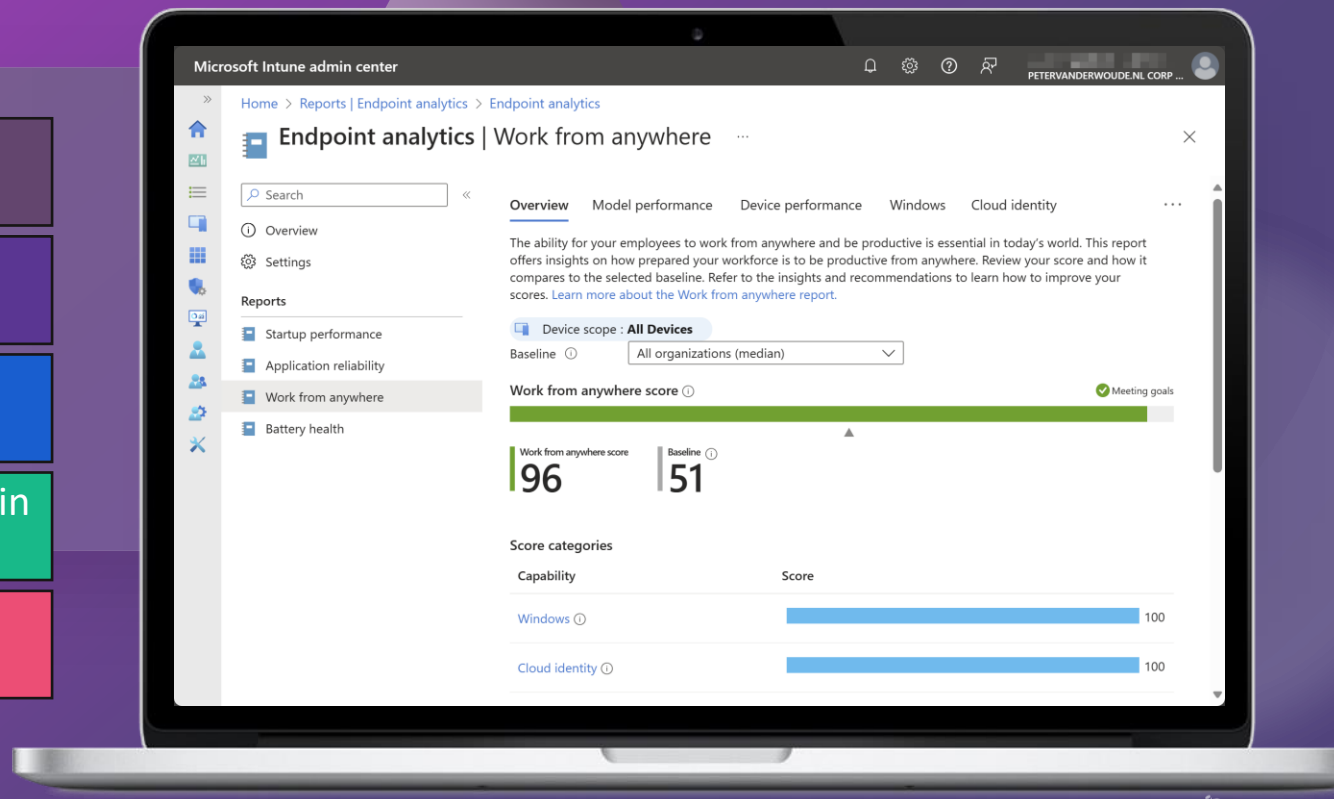


BONUS: Windows updates reports for even more insights

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

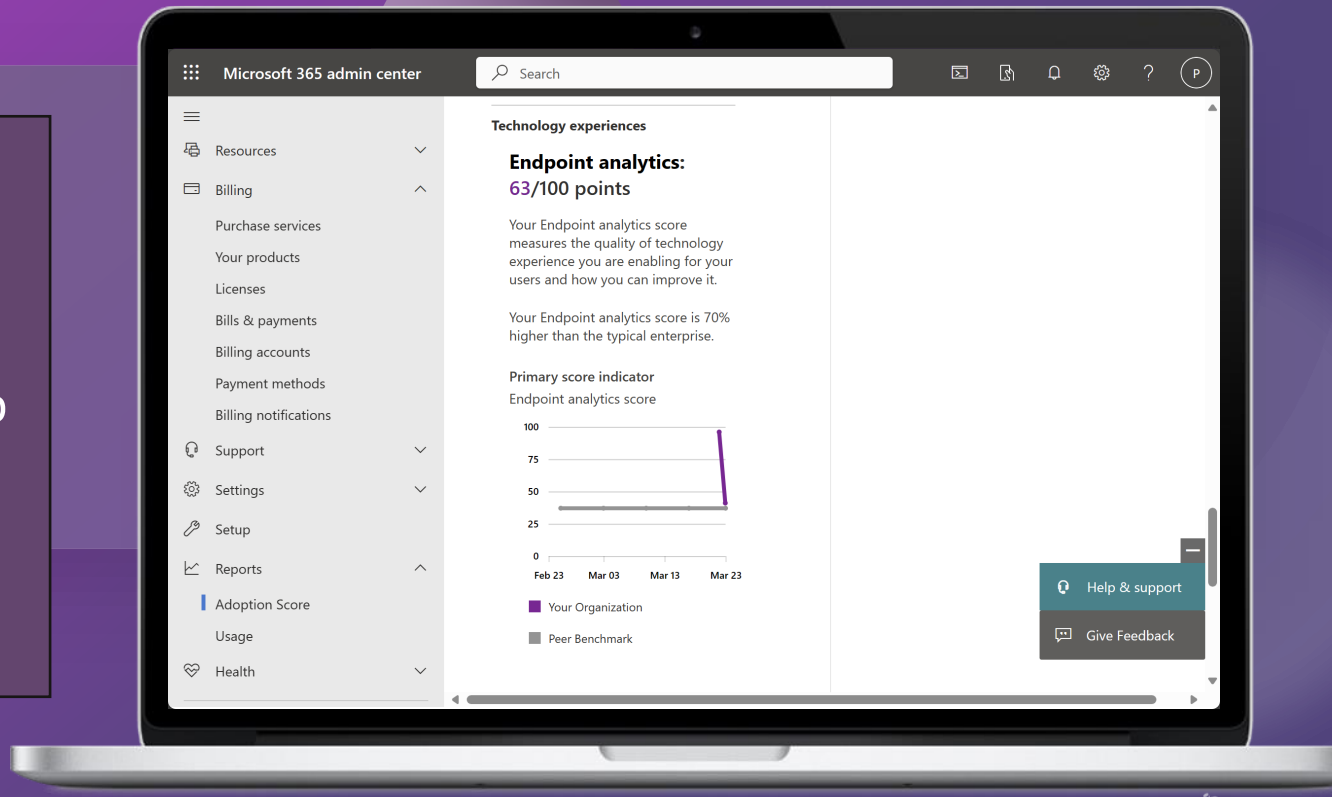


MODERN ENDPOINT MANAGEMENT

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



MODERN ENDPOINT MANAGEMENT

Microsoft 365 admin center

Search

P

Resources

Billing

Purchase services

Your products

Licenses

Bills & payments

Billing accounts

Payment methods

Billing notifications

Support

Settings

Setup

Reports

Adoption Score

Usage

Health

Technology experiences

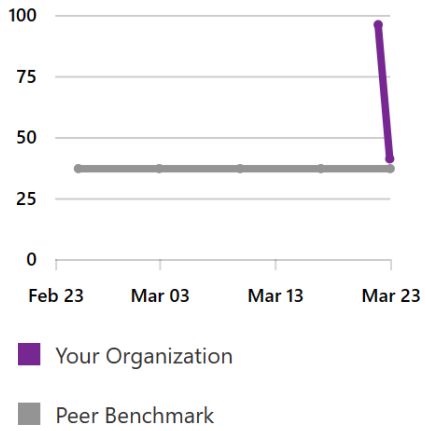
Endpoint analytics:
63/100 points

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



Help & 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 3rd-party solutions.

MODERN ENDPOINT MANAGEMENT

What are the available components?

ANOMALY DETECTION

DEVICE SCOPES

ENHANCED DEVICE TIMELINE

BATTERY HEALTH

DEVICE QUERY

MODERN ENDPOINT MANAGEMENT

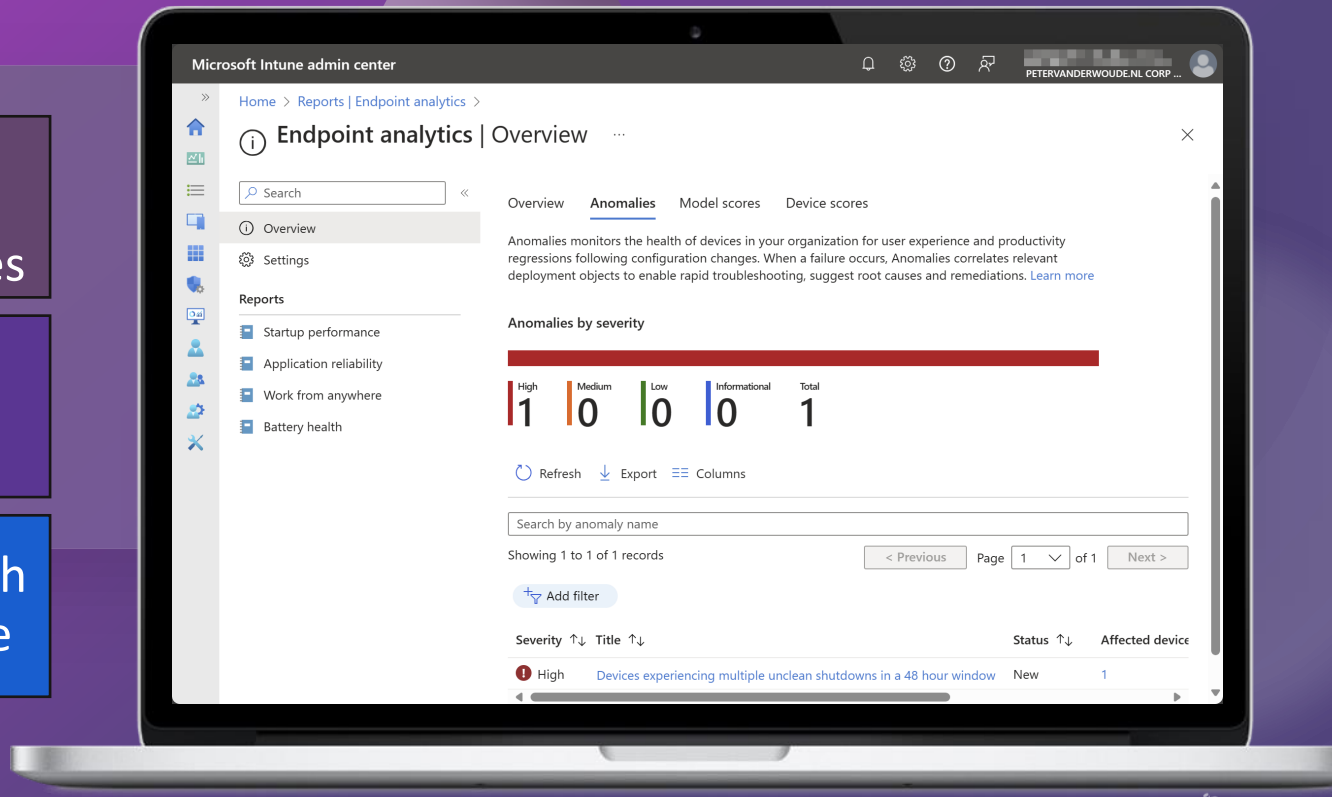
Anomaly detection

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



MODERN ENDPOINT MANAGEMENT

Microsoft Intune admin center











... > 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

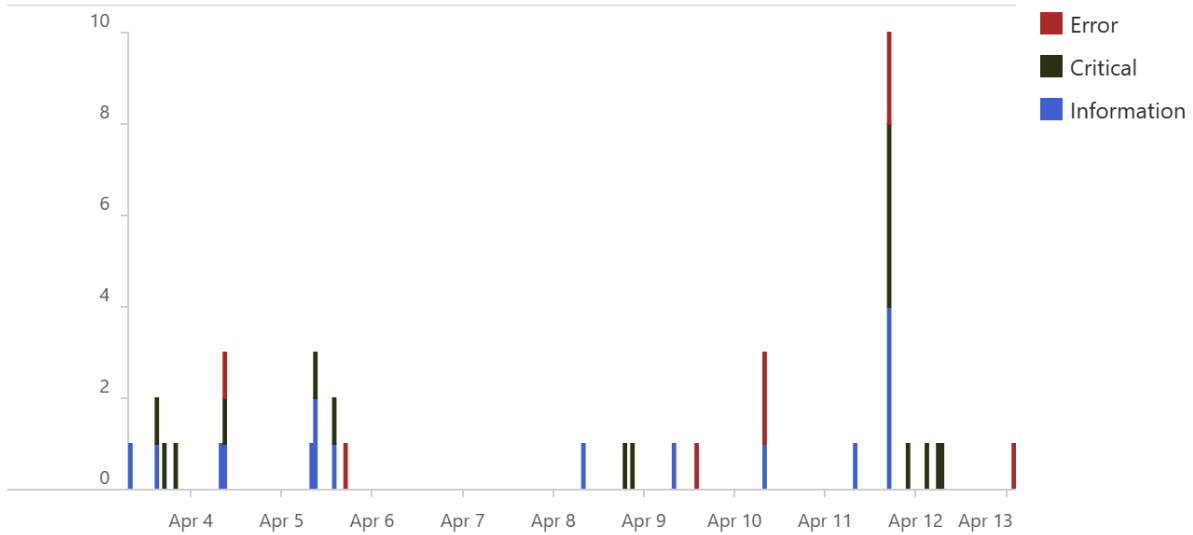
Recovery keys

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

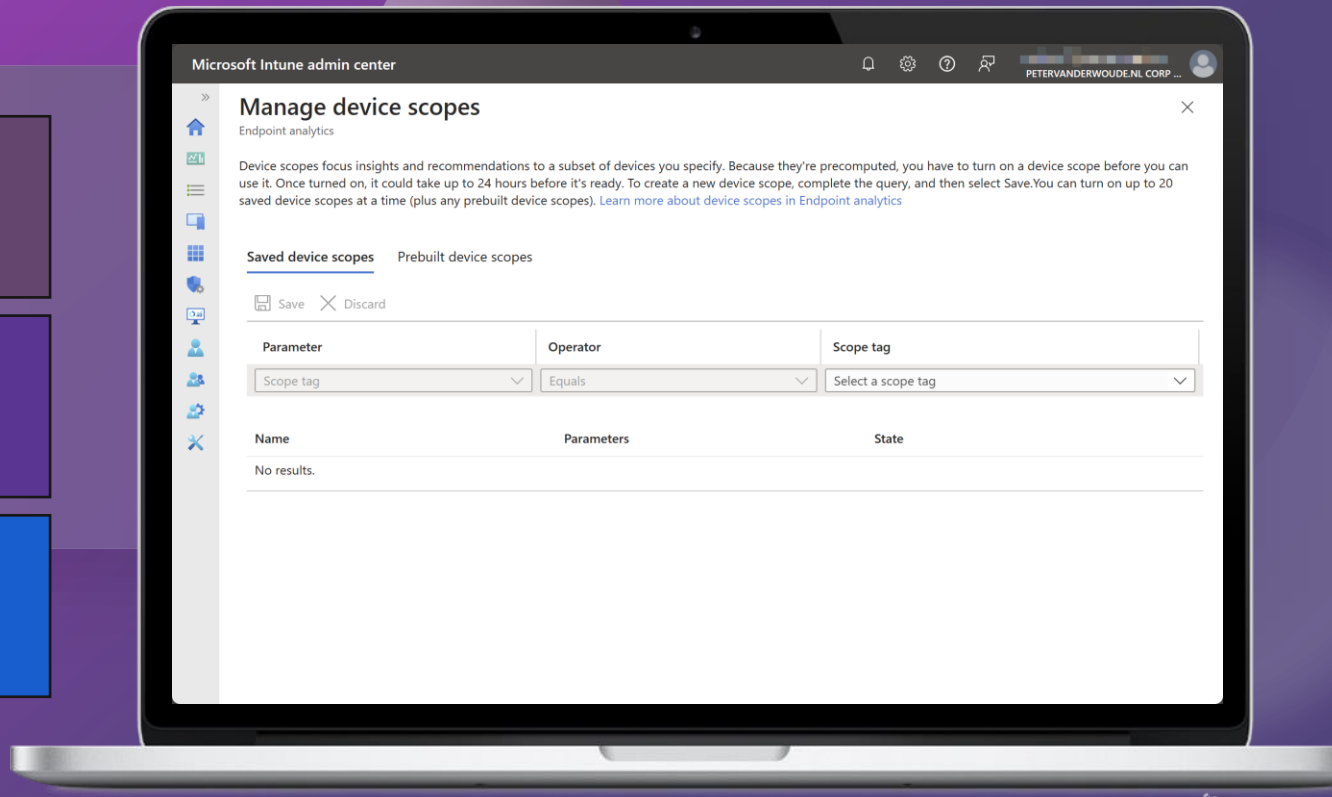
Paired t-tests model – This model is a mathematical method that compares pairs of observations in a dataset, looking for a statistically significant distance between their means

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

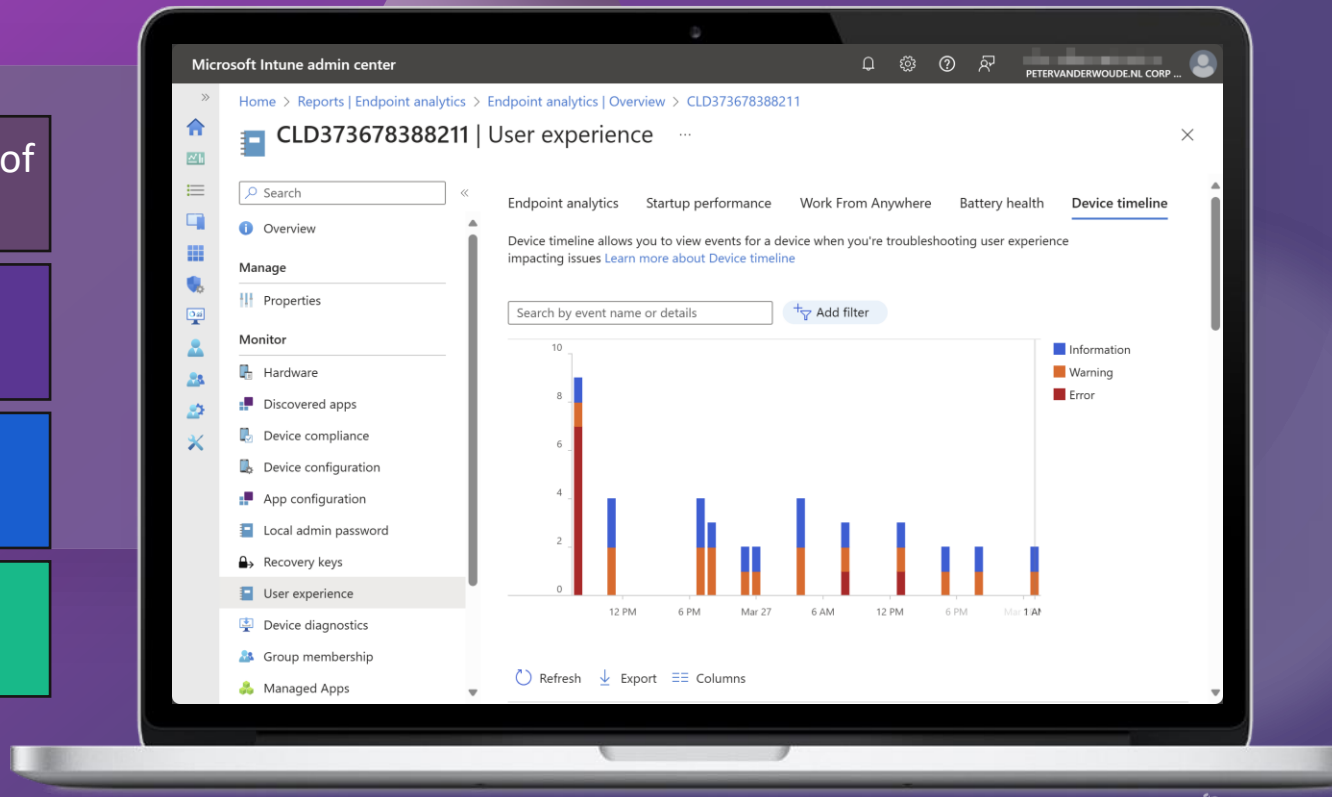
- Device scopes can be used to verify the data for only a subset of devices
- Device scopes are based on *Scope tags* and only one *Scope tag* can be used per custom device scope
- Up to 100 custom device scopes can be saved and up to 20 can be active



MODERN ENDPOINT MANAGEMENT

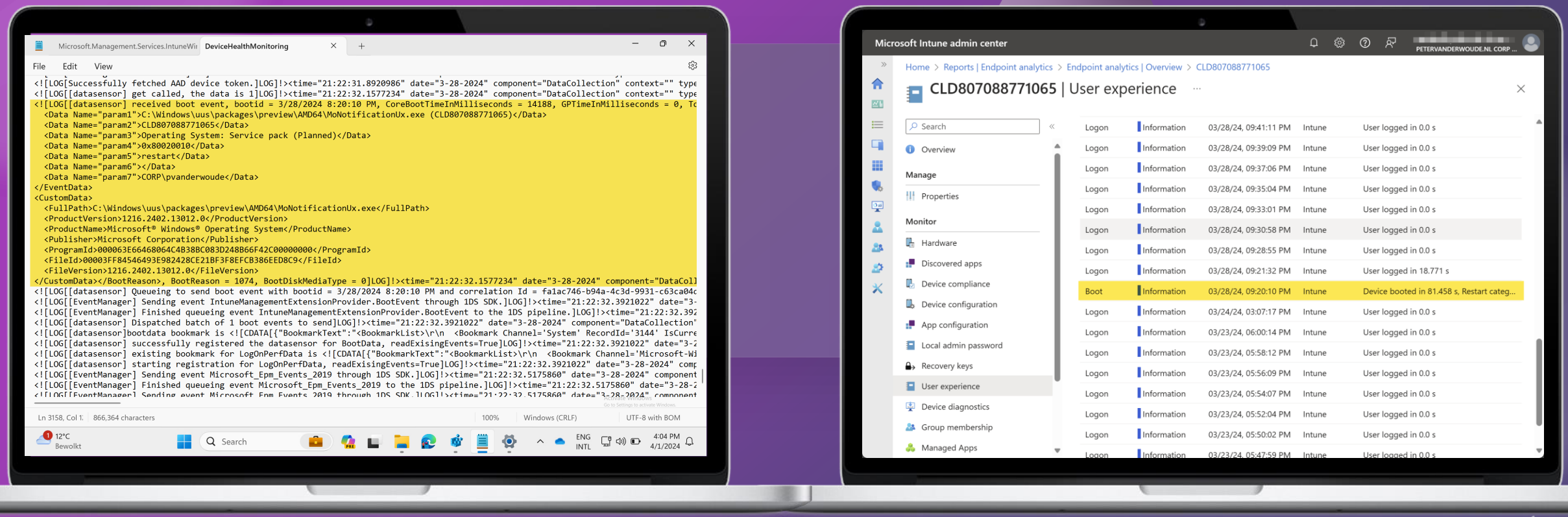
Enhanced device timeline

- 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

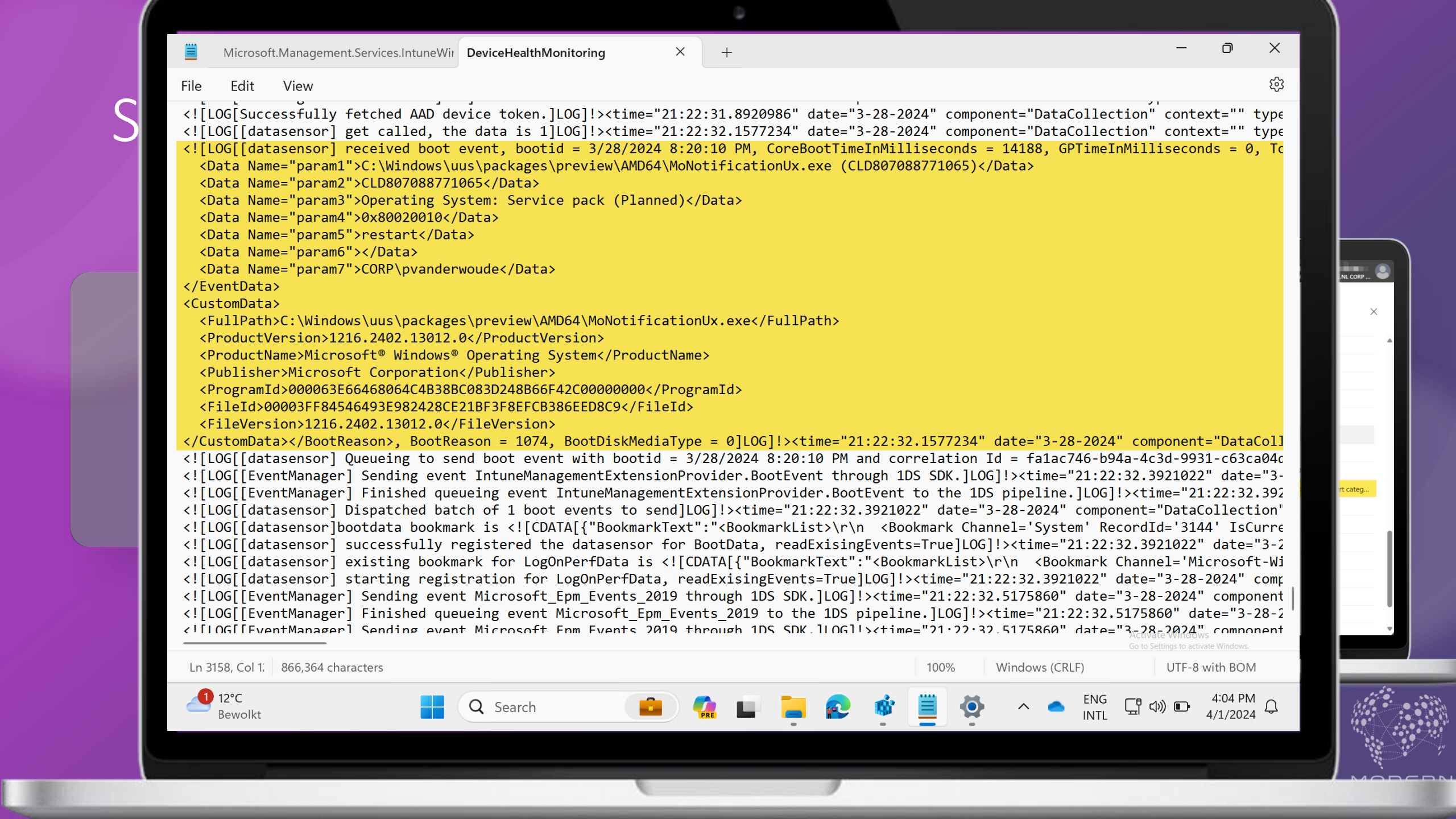


MODERN ENDPOINT MANAGEMENT

Side-step: Following the data



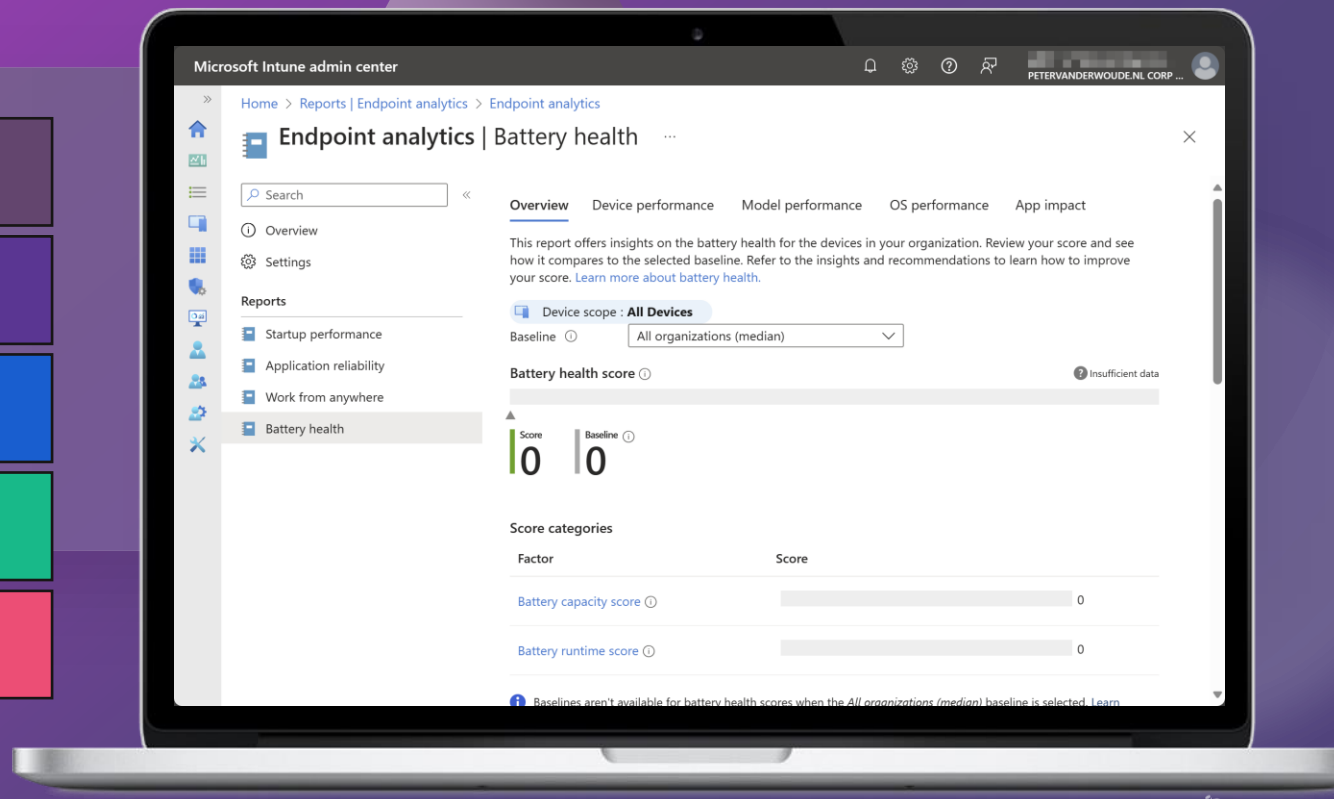
MODERN ENDPOINT MANAGEMENT


Microsoft.Management.Services.IntuneWi
DeviceHealthMonitoring
File
Edit
View
<![LOG[Successfully fetched AAD device token.]LOG]!><time="21:22:31.8920986" date="3-28-2024" component="DataCollection" context="" type
<![LOG[[datasensor] get called, the data is 1]LOG]!><time="21:22:32.1577234" date="3-28-2024" component="DataCollection" context="" type
<![LOG[[datasensor] received boot event, bootid = 3/28/2024 8:20:10 PM, CoreBootTimeInMilliseconds = 14188, GPTimeInMilliseconds = 0, Tc
<Data Name="param1">C:\Windows\uus\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\uus\packages\preview\AMD64\MoNotificationUx.exe</FullPath>
<ProductVersion>1216.2402.13012.0</ProductVersion>
<ProductName>Microsoft® Windows® Operating System</ProductName>
<Publisher>Microsoft Corporation</Publisher>
<ProgramId>000063E66468064C4B38BC083D248B66F42C00000000</ProgramId>
<FileId>00003FF84546493E982428CE21BF3F8EFCB386EED8C9</FileId>
<FileVersion>1216.2402.13012.0</FileVersion>
</CustomData></BootReason>, BootReason = 1074, BootDiskMediaType = 0]LOG]!><time="21:22:32.1577234" date="3-28-2024" component="DataCol
<![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[[EventManager] Sending event IntuneManagementExtensionProvider.BootEvent through 1DS SDK.]LOG]!><time="21:22:32.3921022" date="3-
<![LOG[[EventManager] Finished queueing event IntuneManagementExtensionProvider.BootEvent to the 1DS pipeline.]LOG]!><time="21:22:32.392
<![LOG[[datasensor] Dispatched batch of 1 boot events to send]LOG]!><time="21:22:32.3921022" date="3-28-2024" component="DataCollection"
<![LOG[[datasensor]bootdata bookmark is <![CDATA[{"BookmarkText":"<BookmarkList>\r\n <Bookmark Channel='System' RecordId='3144' IsCurre
<![LOG[[datasensor] successfully registered the datasensor for BootData, readExisingEvents=True]LOG]!><time="21:22:32.3921022" date="3-2
<![LOG[[datasensor] existing bookmark for LogOnPerfData is <![CDATA[{"BookmarkText":"<BookmarkList>\r\n <Bookmark Channel='Microsoft-Wi
<![LOG[[datasensor] starting registration for LogOnPerfData, readExisingEvents=True]LOG]!><time="21:22:32.3921022" date="3-28-2024" comp
<![LOG[[EventManager] Sending event Microsoft_Epm_Events_2019 through 1DS SDK.]LOG]!><time="21:22:32.5175860" date="3-28-2024" component
<![LOG[[EventManager] Finished queueing event Microsoft_Epm_Events_2019 to the 1DS pipeline.]LOG]!><time="21:22:32.5175860" date="3-28-2
Ln 3158, Col 1
866,364 characters
100%
Windows (CRLF)
UTF-8 with BOM
12°C
Bewolkt
Search
ENG
INTL
4:04 PM
4/1/2024

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



MODERN ENDPOINT MANAGEMENT

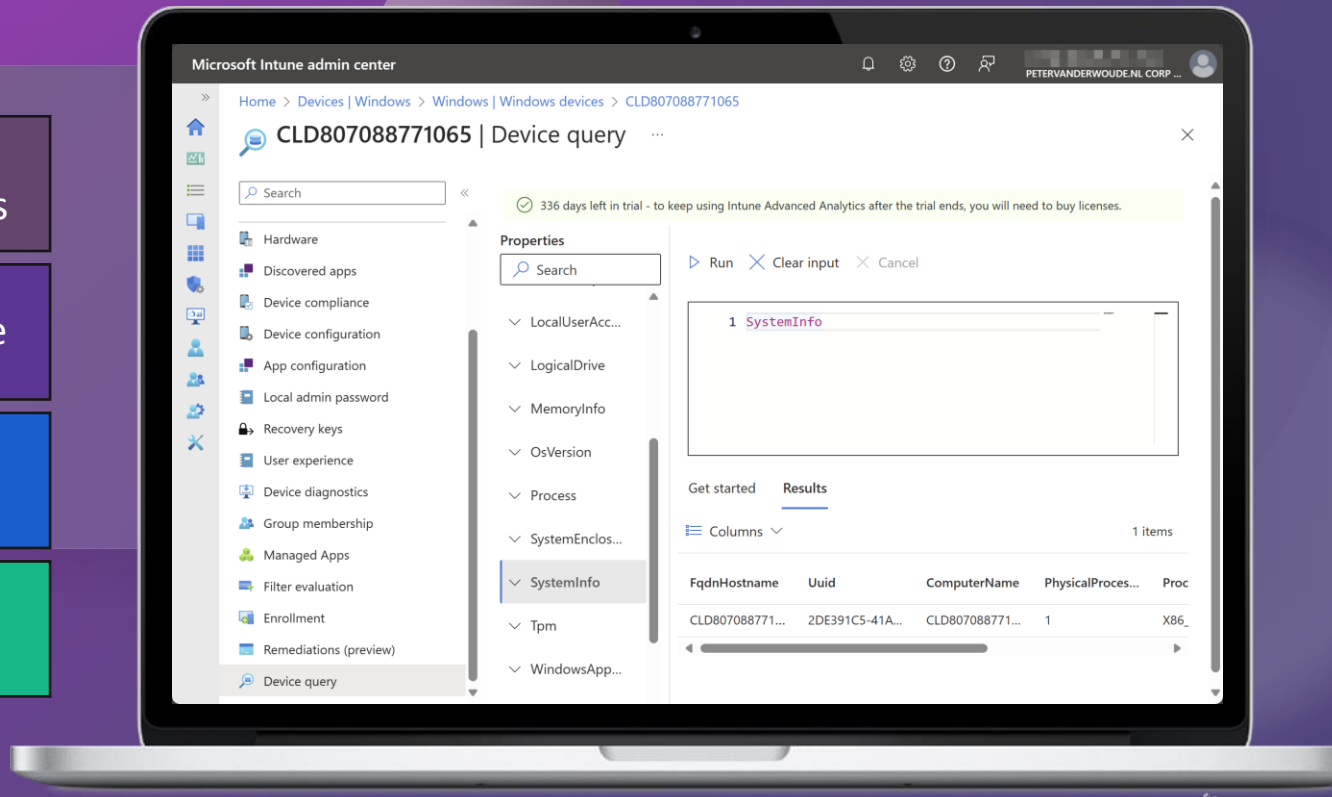
Available within Microsoft Intune Suite

What about Device query

Device query

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

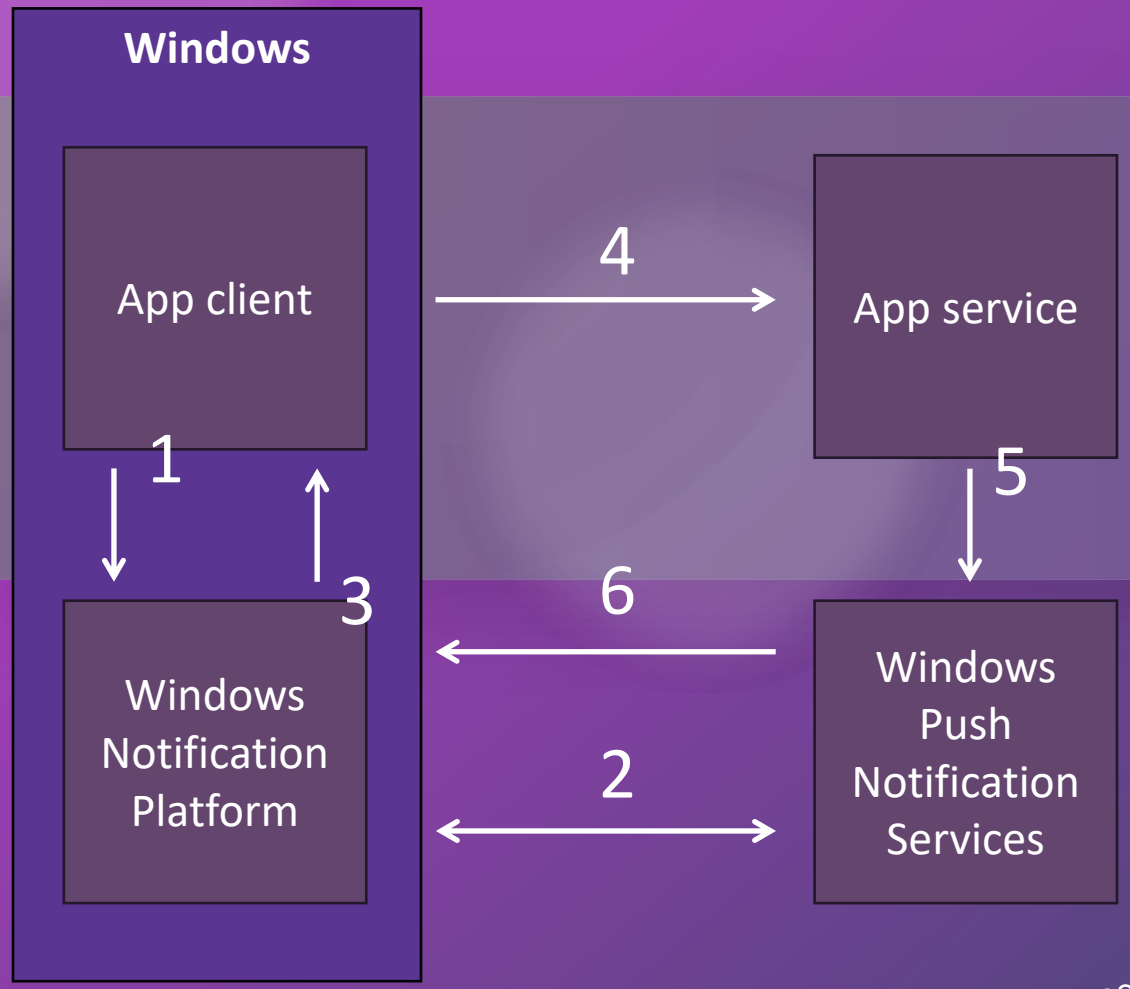
- Device query allows you to quickly gain on-demand information about the state of devices
- Kusto Query Language (KQL) as query language
- Single device only with a maximum of 15 queries per minute
- Intune data platform



MODERN ENDPOINT MANAGEMENT

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

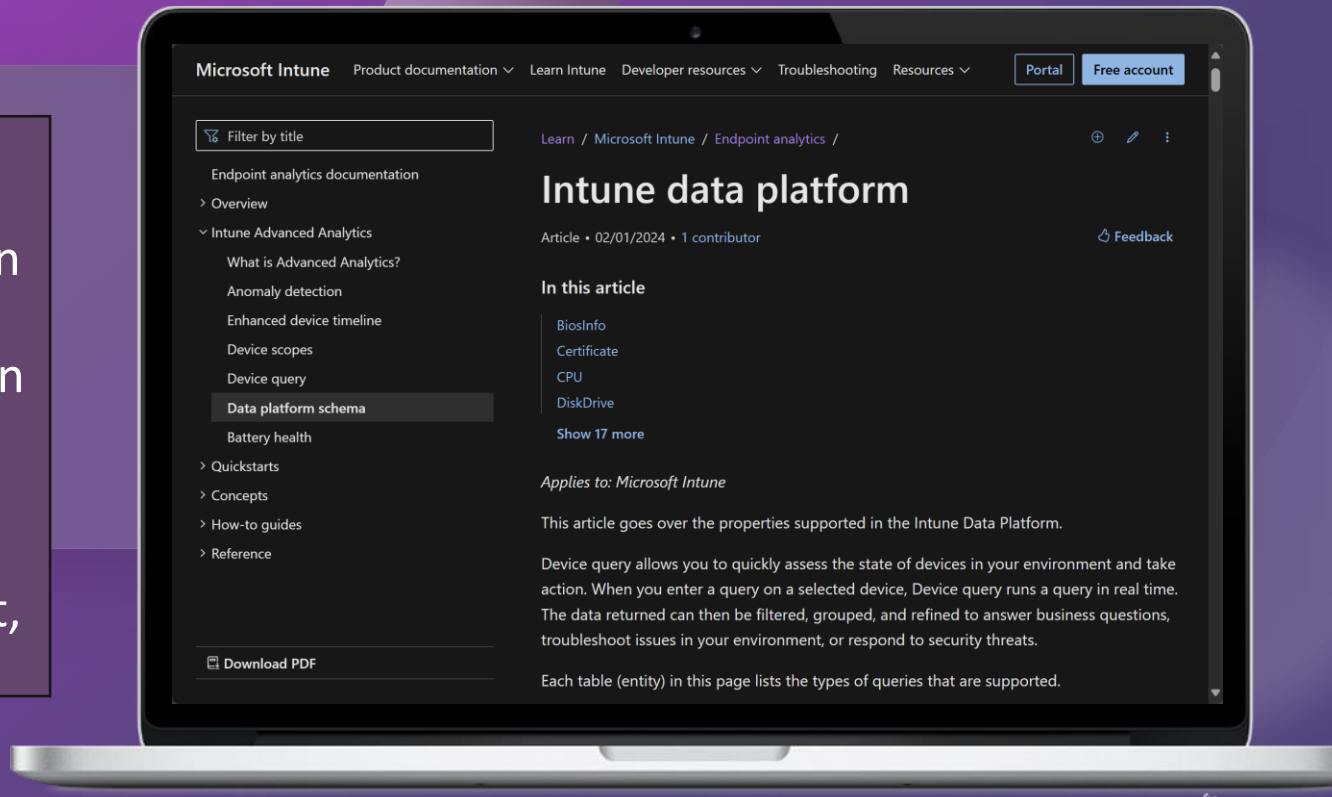
5. The cloud service can send an update by notifying WNS using the channel URI

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



MODERN ENDPOINT MANAGEMENT

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

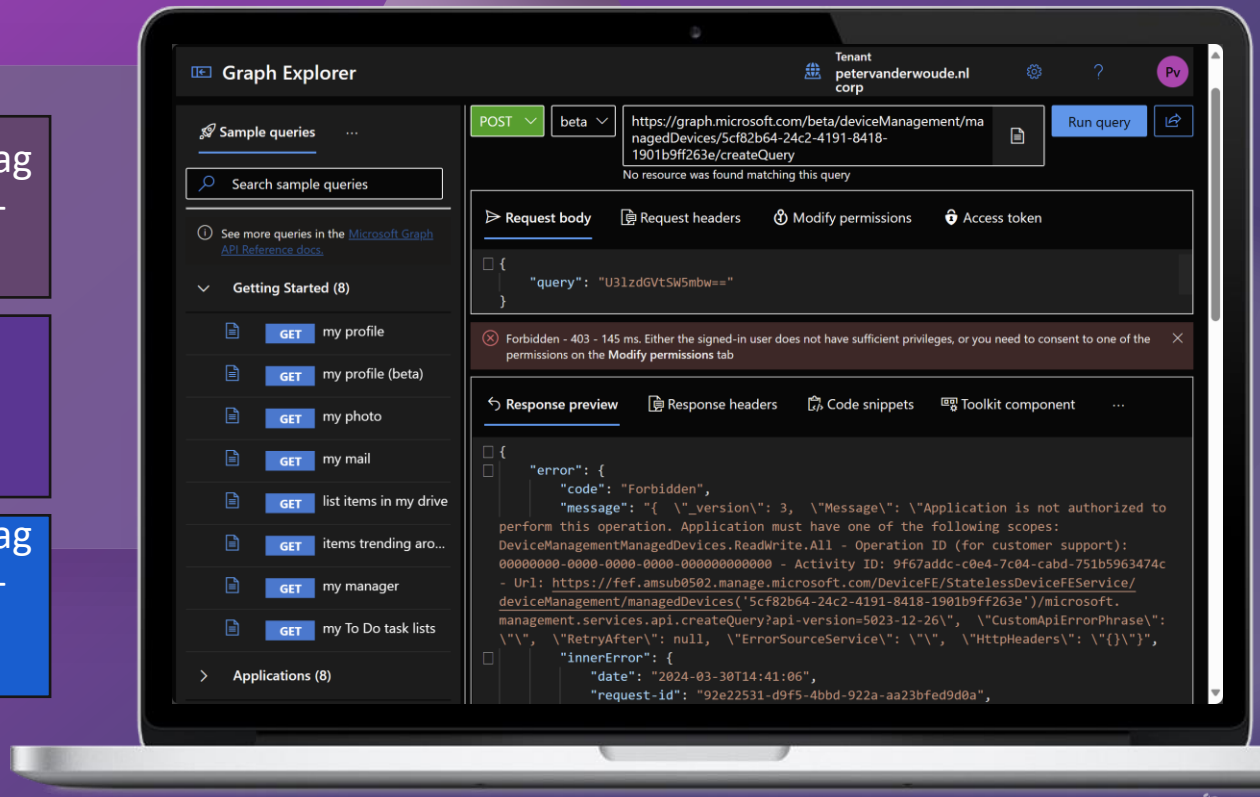
Automating Device query

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

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

{ “query”: “U3lzdGVtSW5mbw==“ }

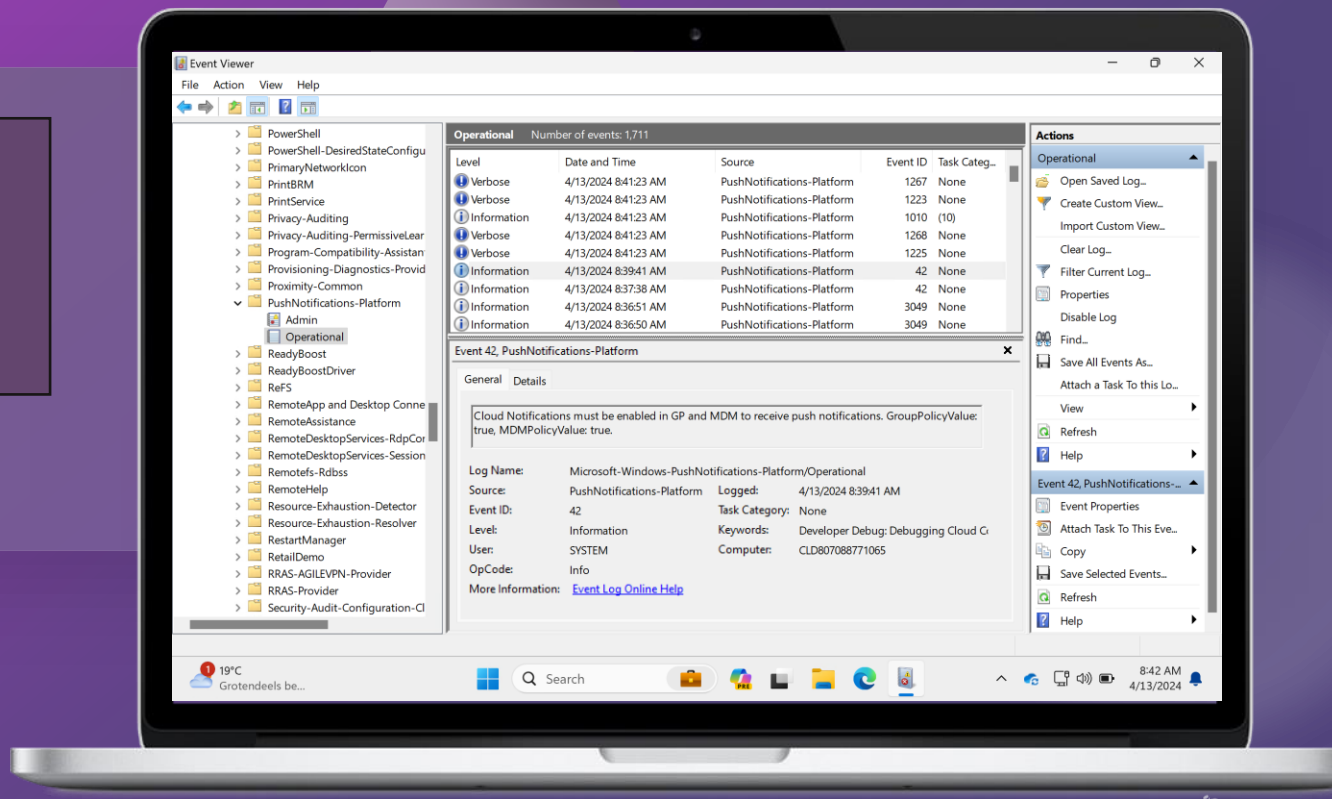
https://graph.microsoft.com/beta/deviceManagement/managedDevices/5cf82b64-24c2-4191-8418-1901b9ff263e/queryResults/c9e307e4-12c0-4d3e-ad5f-d09cef95576f



MODERN ENDPOINT MANAGEMENT

Following Device query

PushNotifications-Platform log

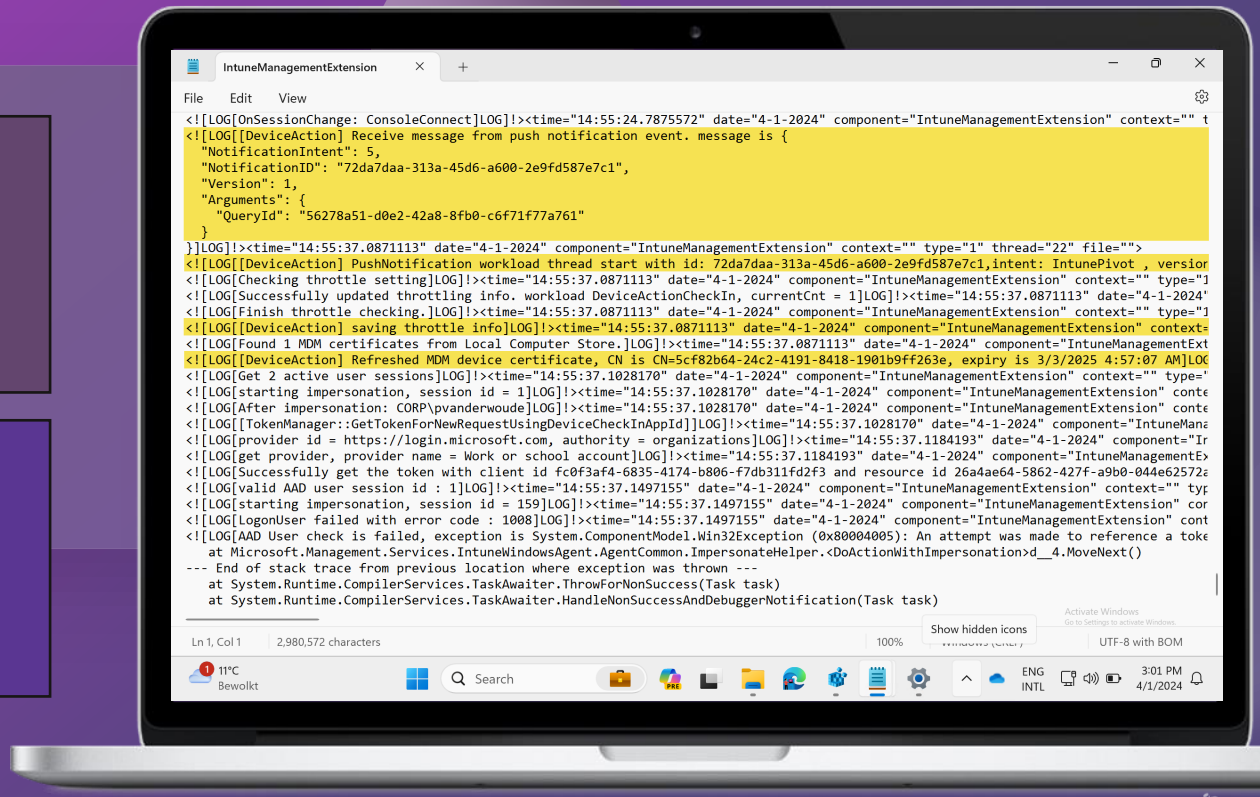


MODERN ENDPOINT MANAGEMENT

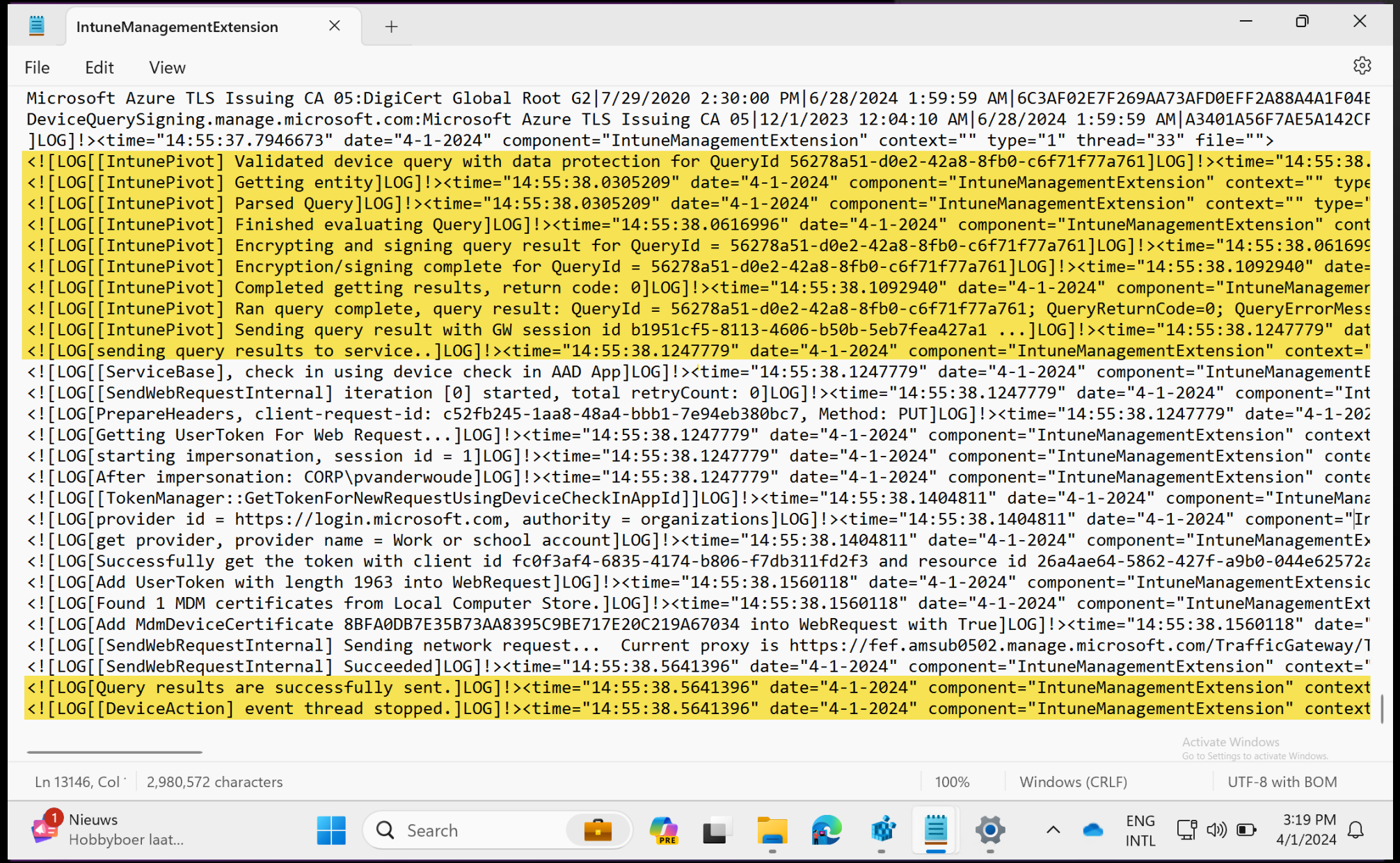
Following Device query

PushNotifications-Platform log

IntuneManagementExtenison.log



MODERN ENDPOINT MANAGEMENT


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
<![LOG[[IntunePivot] Parsed Query]LOG]!><time="14:55:38.0305209" date="4-1-2024" component="IntuneManagementExtension" context="" type="
<![LOG[[IntunePivot] Finished evaluating Query]LOG]!><time="14:55:38.0616996" date="4-1-2024" component="IntuneManagementExtension" cont
<![LOG[[IntunePivot] Encrypting and signing query result for QueryId = 56278a51-d0e2-42a8-8fb0-c6f71f77a761]LOG]!><time="14:55:38.061699
<![LOG[[IntunePivot] Encryption/signing complete for QueryId = 56278a51-d0e2-42a8-8fb0-c6f71f77a761]LOG]!><time="14:55:38.1092940" date=
<![LOG[[IntunePivot] Completed getting results, return code: 0]LOG]!><time="14:55:38.1092940" date="4-1-2024" component="IntuneManagemer
<![LOG[[IntunePivot] Ran query complete, query result: QueryId = 56278a51-d0e2-42a8-8fb0-c6f71f77a761; QueryReturnCode=0; QueryErrorMess
<![LOG[[IntunePivot] Sending query result with GW session id b1951cf5-8113-4606-b50b-5eb7fea427a1 ...]LOG]!><time="14:55:38.1247779" dat
<![LOG[sending query results to service..]LOG]!><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context="
<![LOG[[ServiceBase], check in using device check in AAD App]LOG]!><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementE
<![LOG[[SendWebRequestInternal] iteration [0] started, total retryCount: 0]LOG]!><time="14:55:38.1247779" date="4-1-2024" component="Int
<![LOG[PrepareHeaders, client-request-id: c52fb245-1aa8-48a4-bbb1-7e94eb380bc7, Method: PUT]LOG]!><time="14:55:38.1247779" date="4-1-202
<![LOG[Getting UserToken For Web Request...]LOG]!><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" context
<![LOG[starting impersonation, session id = 1]LOG]!><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" conte
<![LOG[After impersonation: CORP\pvanderwoude]LOG]!><time="14:55:38.1247779" date="4-1-2024" component="IntuneManagementExtension" conte
<![LOG[[TokenManager::GetTokenForNewRequestUsingDeviceCheckInAppId]]LOG]!><time="14:55:38.1404811" date="4-1-2024" component="IntuneMana
<![LOG[provider id = https://login.microsoft.com, authority = organizations]LOG]!><time="14:55:38.1404811" date="4-1-2024" component="Ir
<![LOG[get provider, provider name = Work or school account]LOG]!><time="14:55:38.1404811" date="4-1-2024" component="IntuneManagementEx
<![LOG[Successfully get the token with client id fc0f3af4-6835-4174-b806-f7db311fd2f3 and resource id 26a4ae64-5862-427f-a9b0-044e62572a
<![LOG[Add UserToken with length 1963 into WebRequest]LOG]!><time="14:55:38.1560118" date="4-1-2024" component="IntuneManagementExtensic
<![LOG[Found 1 MDM certificates from Local Computer Store.]LOG]!><time="14:55:38.1560118" date="4-1-2024" component="IntuneManagementExt
<![LOG[Add MdmDeviceCertificate 8BFA0DB7E35B73AA8395C9BE717E20C219A67034 into WebRequest with True]LOG]!><time="14:55:38.1560118" date="
<![LOG[[SendWebRequestInternal] Sending network request... Current proxy is https://fef.amsub0502.manage.microsoft.com/TrafficGateway/T
<![LOG[[SendWebRequestInternal] Succeeded]LOG]!><time="14:55:38.5641396" date="4-1-2024" component="IntuneManagementExtension" context="
<![LOG[Query results are successfully sent.]LOG]!><time="14:55:38.5641396" date="4-1-2024" component="IntuneManagementExtension" context
<![LOG[[DeviceAction] event thread stopped.]LOG]!><time="14:55:38.5641396" date="4-1-2024" component="IntuneManagementExtension" context
Activate Windows
Go to Settings to activate Windows.
Ln 13146, Col
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

Replaced legacy hardware on time

Eliminated productivity killers