

# Troubleshooting Windows Updates

# Who are we?



Tim De Keukelaere

Freelance - Workplace Architect

Tim.De.Keukelaere@IT-Essence.be



@Tim\_DK



<http://be.linkedin.com/in/timdekeukelaere/>



<http://www.dekeukelaere.com>



Timdk\_itpro

Ken Goossens

Sr. Product Manager

Ken.Goossens@microsoft.com



@Goosken



<https://be.linkedin.com/in/getmodern>



<https://www.kengoossens.com>



N/A





# ◎ Agenda

1

## Reporting

How do I know that something went wrong?

2

## Troubleshooting

How do I figure out why it went wrong?

3

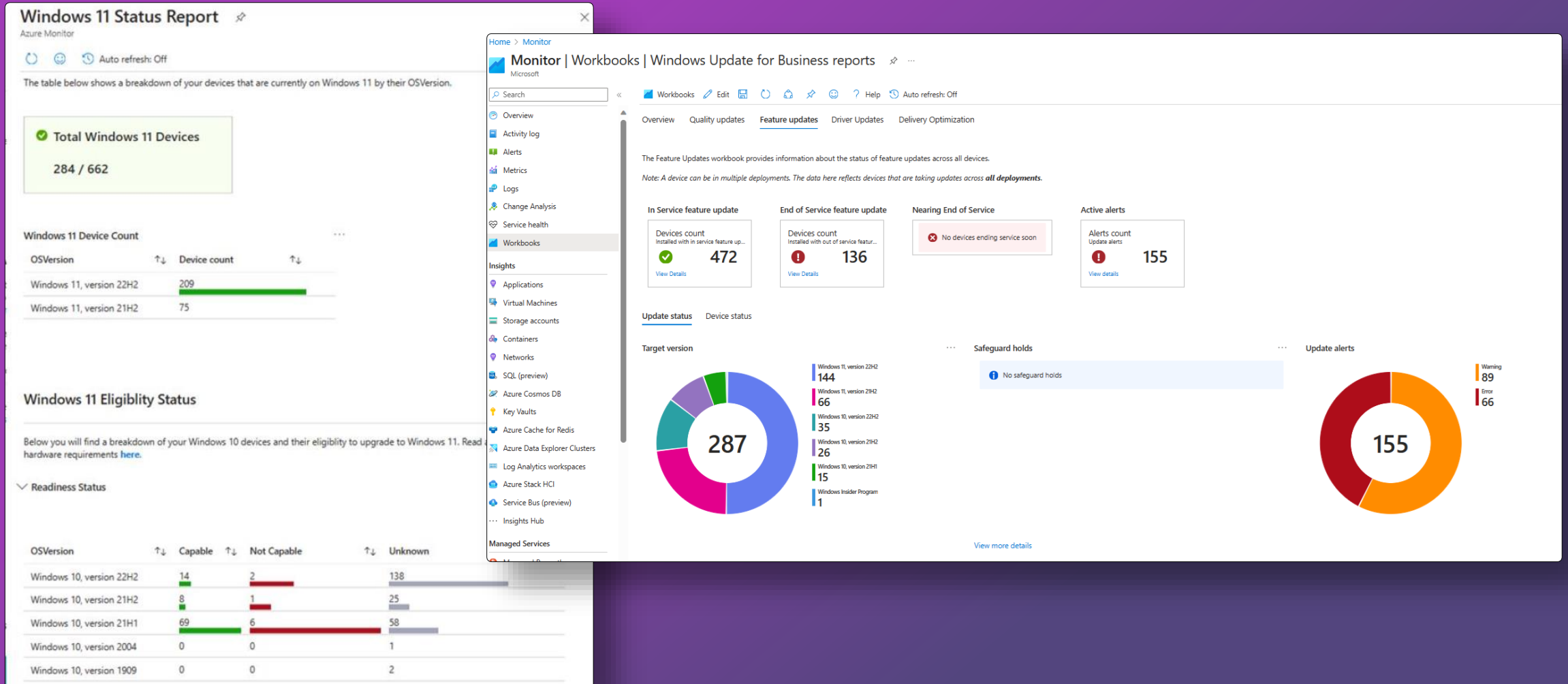
## Remediation

How do I fix it?

# Reporting

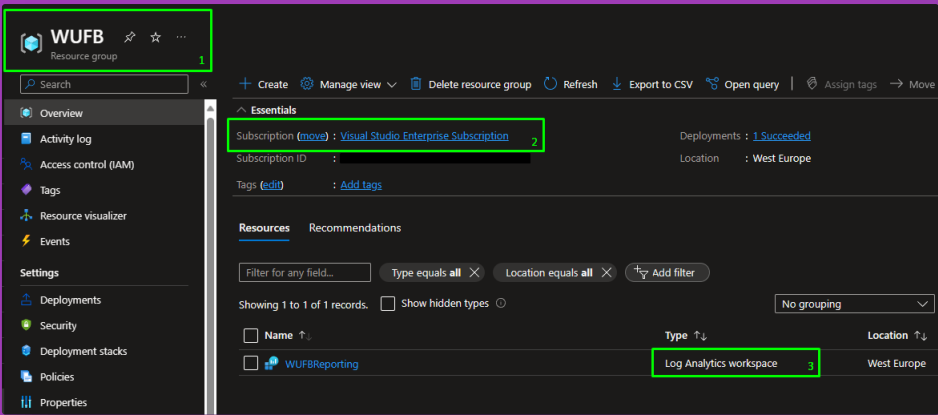
## Part 1

# Workbooks in Azure



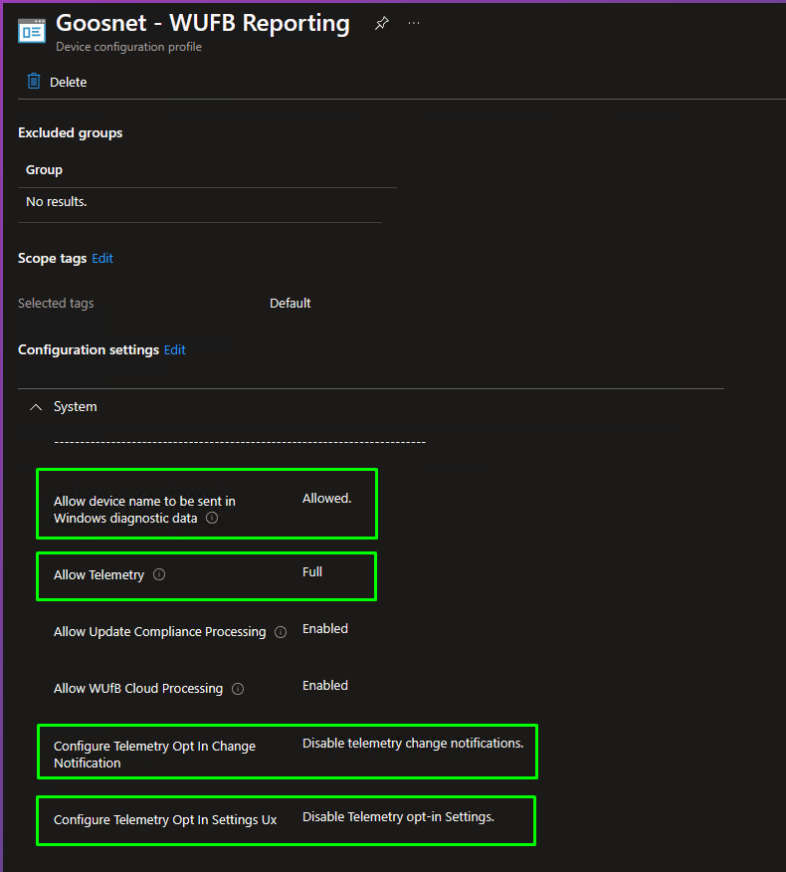


# Enable WUFB reporting



Azure Resources

- Azure Resource Group
- Log Analytics Workspace
- Monitor Workbook
- Coffee and time (48 – 72 hours)



## Device Configuration Policy

- Allow Device Name to be sent
- Allow Telemetry
- Disable Telemetry Change Notifications
- Disable Telemetry opt-in Settings

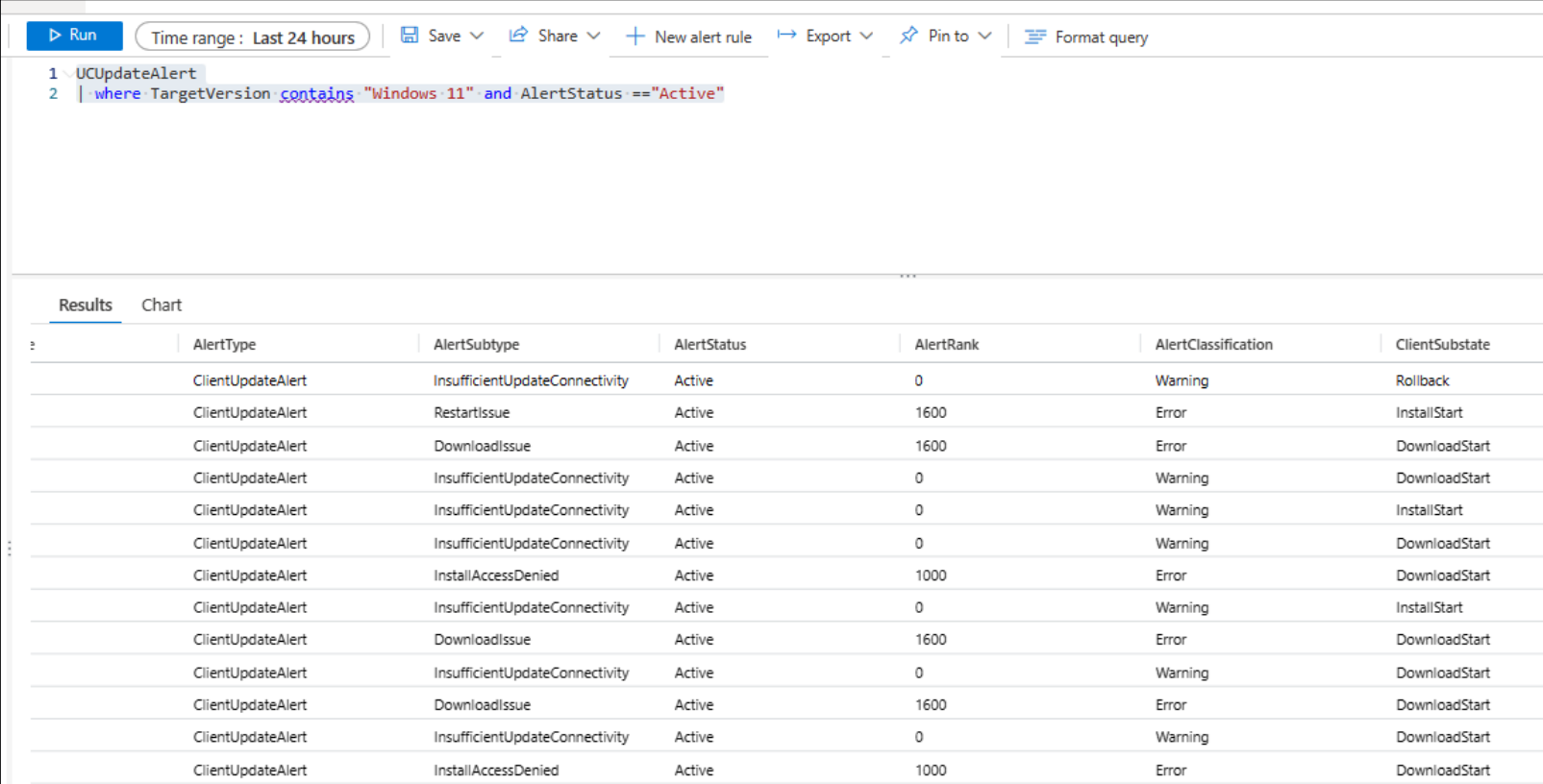


# Interesting queries to troubleshoot

Find all issues that are blocking upgrades to Windows 11

UCUpdateAlert

| where TargetVersion contains "Windows 11" and AlertStatus == "Active"



The screenshot shows a query interface with a toolbar at the top containing buttons for 'Run', 'Time range: Last 24 hours', 'Save', 'Share', 'New alert rule', 'Export', 'Pin to', and 'Format query'. The query editor contains two lines of Kusto query language:

```
1 UCUpdateAlert
2 | where TargetVersion contains "Windows 11" and AlertStatus == "Active"
```

Below the query editor, the 'Results' tab is selected, displaying a table with 7 columns: AlertType, AlertSubtype, AlertStatus, AlertRank, AlertClassification, and ClientSubstate. The table contains 13 rows of data, all with 'Active' status.

AlertType	AlertSubtype	AlertStatus	AlertRank	AlertClassification	ClientSubstate
ClientUpdateAlert	InsufficientUpdateConnectivity	Active	0	Warning	Rollback
ClientUpdateAlert	RestartIssue	Active	1600	Error	InstallStart
ClientUpdateAlert	DownloadIssue	Active	1600	Error	DownloadStart
ClientUpdateAlert	InsufficientUpdateConnectivity	Active	0	Warning	DownloadStart
ClientUpdateAlert	InsufficientUpdateConnectivity	Active	0	Warning	InstallStart
ClientUpdateAlert	InsufficientUpdateConnectivity	Active	0	Warning	DownloadStart
ClientUpdateAlert	InstallAccessDenied	Active	1000	Error	DownloadStart
ClientUpdateAlert	InsufficientUpdateConnectivity	Active	0	Warning	InstallStart
ClientUpdateAlert	DownloadIssue	Active	1600	Error	DownloadStart
ClientUpdateAlert	InsufficientUpdateConnectivity	Active	0	Warning	DownloadStart
ClientUpdateAlert	DownloadIssue	Active	1600	Error	DownloadStart
ClientUpdateAlert	InsufficientUpdateConnectivity	Active	0	Warning	DownloadStart
ClientUpdateAlert	InstallAccessDenied	Active	1000	Error	DownloadStart



# More interesting queries

---

Get key information about a specific error-code

```
UCUpdateAlert  
| where ErrorCode == "0X8024000b"
```

Get all active alerts and summarize device count by AlertSubType

```
UCUpdateAlert  
| where AlertStatus == "Active"  
| summarize Devices = count() by AlertSubtype
```

Get all policies that you have targeting Windows 11 22H2

```
UCClientUpdateStatus  
| where TargetVersion == "Windows 11, version 22H2"  
| summarize by TargetKBNumber, DeviceName
```

Is the device online, what is the last WU (Windows update) Scan time

For all clients:

```
UCClient
```

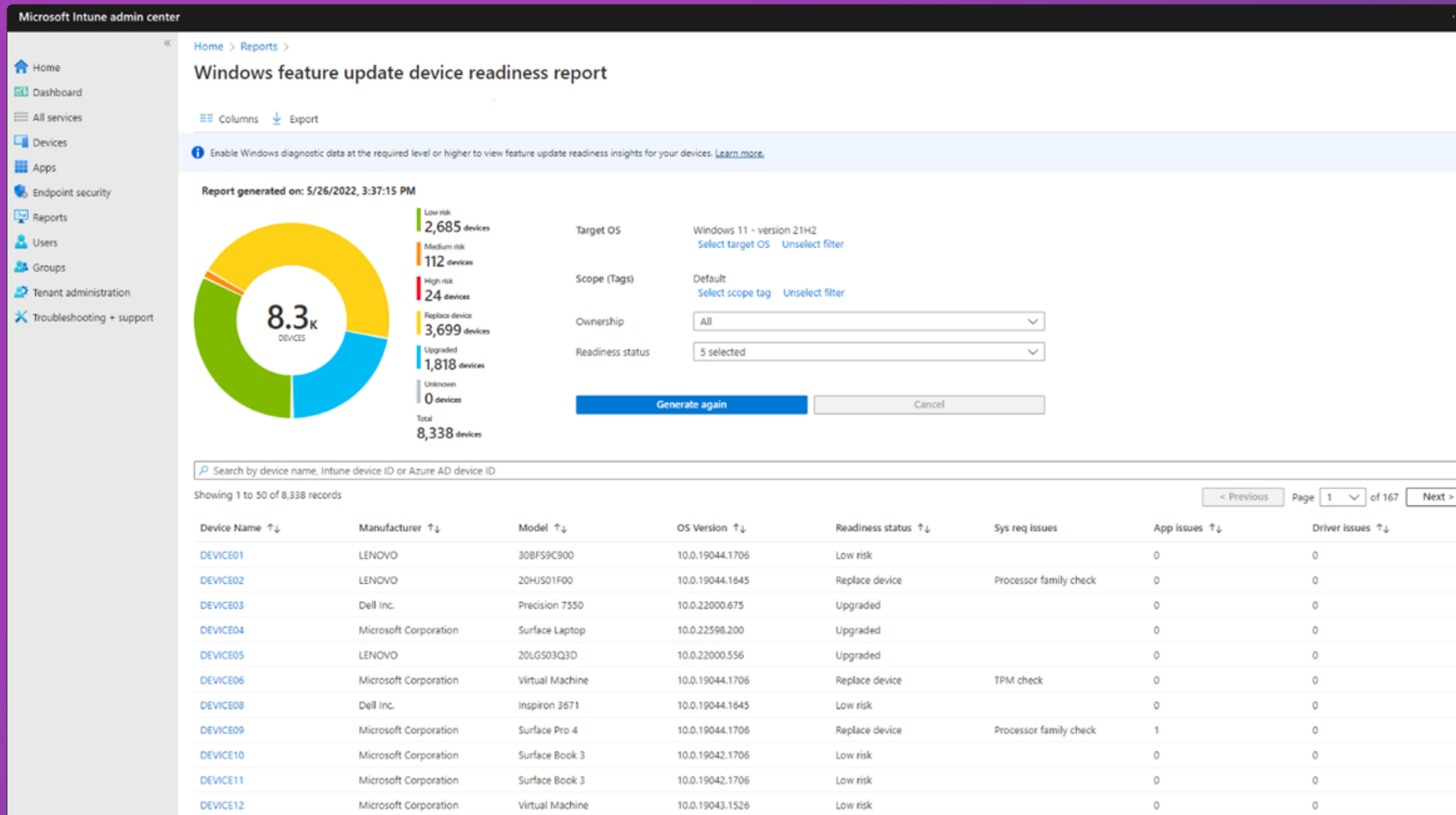
For a single device:

```
UCClient
```

```
| where DeviceName == "Hostname"
```



# Windows Feature Update Readiness



Comprehensive view on readiness

System requirement issues

Manufacturer & model

Include details on app compat

Include details on driver compat

# Work from anywhere

The screenshot displays the Microsoft Endpoint Manager admin center interface. The left sidebar contains navigation options: Home, Endpoint analytics, Overview, Settings, Reports, Startup performance, Proactive remediations, Application reliability, and Work from anywhere (selected). The main content area is titled 'Endpoint analytics | Work from anywhere' and includes tabs for Overview, Windows (selected), Cloud identity, Cloud management, and Cloud provisioning. A search bar and a list of reports are visible. The 'Work from anywhere' report is expanded, showing a table of device readiness data. The table has columns for Device, Managed by, OS version, Windows 11 readiness status, and Windows 11 readiness reason. The data shows various desktop devices with different OS versions and readiness statuses, with reasons for non-readiness including storage, TPM, system firmware, CPU cores, and CPU family.

Device ...	Managed by	OS version	Windows 11 readiness status	Windows 11 readiness reason
DESKTOP-2...	Intune	10.0.18362.10024	Not capable	Storage, TPM, System firmware, CPU cores, CPU family
DESKTOP-V...	Co-managed	10.0.18363.1854	Not capable	System firmware, CPU family
DESKTOP-3...	Intune	10.0.19043.1237	Unknown	--
DESKTOP-U...	Intune	10.0.19043.1288	Not capable	CPU family
DESKTOP-P9...	Intune	10.0.19043.1288	Not capable	TPM
DESKTOP-B...	Intune	10.0.19043.1288	Not capable	RAM, TPM
DESKTOP-IT...	Intune	10.0.19043.1288	Not capable	TPM
DESKTOP-IL...	Intune	10.0.19043.1288	Capable	--

Does not require data diagnostic

Windows readiness status

Windows readiness reason

# Windows 11 hardware readiness script

## Hardware Readiness PowerShell script (aka.ms)

```
> HardwareReadiness.ps1 2
D: > OneDriveFolders > Business > OneDrive - Microsoft > FY22FY23 > Hackathon > 2023 > HardwareReadiness.ps1 > ...
1 #=====
2 #
3 # Script Name:      HardwareReadiness.ps1
4 # Description:      Verifies the hardware compliance. Return code 0 for success.
5 #                  In case of failure, returns non zero error code along with error message.
6
7 # This script is not supported under any Microsoft standard support program or service and is distributed under the MIT license
8
9 # Copyright (C) 2021 Microsoft Corporation
10
11 # Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation
12 # files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy,
13 # modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software
14 # is furnished to do so, subject to the following conditions:
15
16 # The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
17
18 # THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
19 # WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR
20 # COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
21 # ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
22
23 #=====
24
25 $ExitCode = 0
26
27 [int]$MinOSDiskSizeGB = 64
28 [int]$MinMemoryGB = 4
29 [UInt32]$MinClockSpeedMHz = 1000
30 [UInt32]$MinLogicalCores = 2
31 [UInt16]$RequiredAddressWidth = 64
32
33 $PASS_STRING = "PASS"
34 $FAIL_STRING = "FAIL"
35 $FAILED_TO_RUN_STRING = "FAILED TO RUN"
```

### returnReason

Storage

Memory

TPM

Processor

SecureBoot

### returnCode Definition

returnCode	Definition
-2	FAILED TO RUN – the script encountered an error
-1	UNDETERMINED – one or more of the hardware requirement checks failed to execute properly
0	CAPABLE – the device meets all assessed Windows 11 hardware requirements
1	NOT CAPABLE – the device does not meet one or more of the assessed Windows 11 hardware requirements

- Autopatch feature update
  - Trends and summary
  - Review by phase
  - Rich filtering

**Feature update status**

Refresh Export Columns

Search Add filter

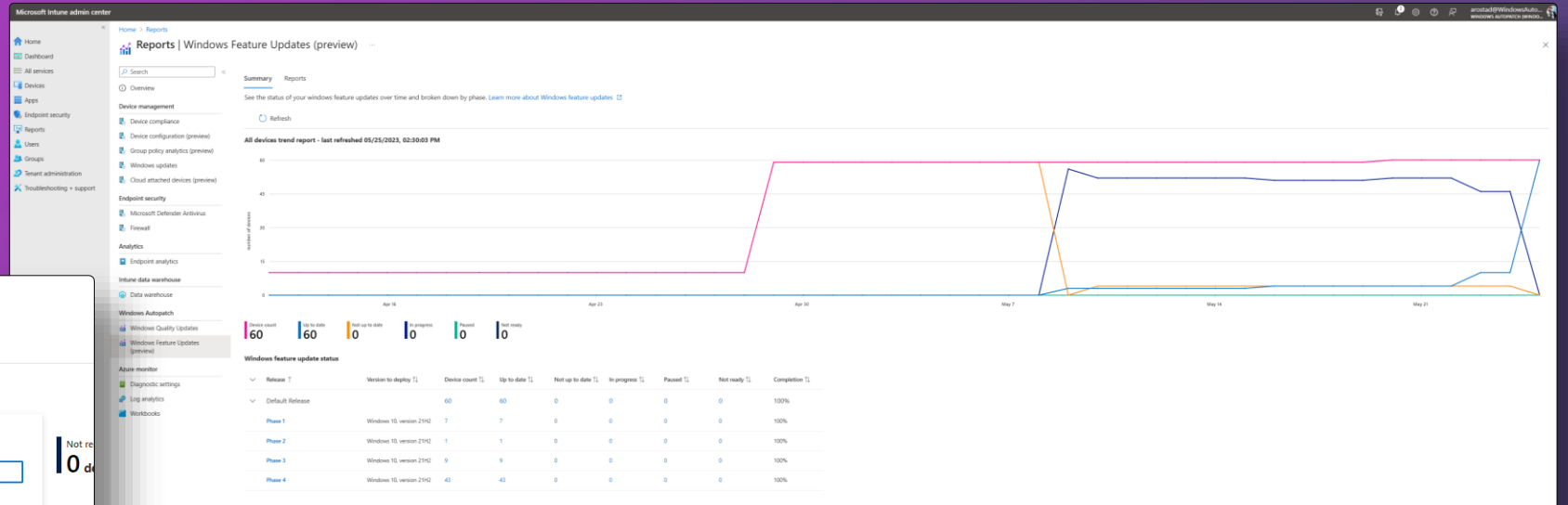
Device count: 60 devices Up to date: 60 devices Not ready: 0 devices

Add filter

search for filter type

- Current OS
- Target OS
- OS Status
- Update Status
- Readiness
- Pause Status
- Client State
- Client Substate
- Release
- Phase
- Servicing Channel

Device Name	Current OS	Target OS	OS Status	Update Status	Readiness	Pause Status	Client State	Client Substate	Release	Phase	Servicing Channel
CPC-Allan-VPKG2	Windows 10, versi...	20H2	In Servicing	Up to Date							
CPC-Andre-01YMP	Windows 10, versi...	20H2	In Servicing	Up to Date							
AVD-Ap-11	Windows 10, versi...	20H2	In Servicing	Up to Date							
CPC-chris-H2R7D	Windows 10, versi...	20H2	In Servicing	Up to Date							
AVD-Ap-17	Windows 10, versi...	W	In Servicing	Up to Date							
CPC-jeffh-SEMFC	Windows 10, versi...	W	In Servicing	Up to Date							
CPC-alici-G99L0	Windows 10, versi...	20H2	In Servicing	Up to Date							
CPC-Chris-83EUQ	Windows 10, versi...	20H2	In Servicing	Up to Date							
CPC-Grady-69CL3	Windows 10, versi...	20H2	In Servicing	Up to Date							
CPC-Debra-DLX00	Windows 10, versi...	20H2	In Servicing	Up to Date							
AVD-Ap-14	Windows 10, versi...	20H2	In Servicing	Up to Date							
AVD-Ap-8	Windows 10, versi...	Windows 10, versi...	In Servicing	Up to Date							



# Windows Autopatch

This PC > Data (D:) > Temp > Troubleshooting Logs > WindowsUpdateLogs > Users > kegoosse > AppData > Local > Temp > 2712fc3c-7d81-420b-a0b4-45d39e2c7a77 >

Name	Date modified	Type	Size
CBS	1/18/2024 2:35 PM	File folder	
DISM	1/18/2024 2:35 PM	File folder	
PNP	1/18/2024 2:35 PM	File folder	
Setup	1/18/2024 2:35 PM	File folder	
SIH	1/18/2024 2:35 PM	File folder	
USO	1/18/2024 2:38 PM	File folder	
UX	1/18/2024 2:35 PM	File folder	
WaaSMedic	1/18/2024 2:35 PM	File folder	
WU	1/18/2024 2:35 PM	File folder	
AppModelVersion	1/18/2024 1:34 PM	Text Document	1 KB
BuildInfo	1/18/2024 1:34 PM	Text Document	1 KB
registry_appx	1/18/2024 1:34 PM	Text Document	14 KB
registry_DO	1/18/2024 1:34 PM	Text Document	1 KB
registry_FirmwareResources	1/18/2024 1:34 PM	Text Document	1 KB
registry_langpack	1/18/2024 1:34 PM	Text Document	1 KB
registry_peruser_wupolicy	1/18/2024 1:34 PM	Text Document	1 KB
registry_Setup	1/18/2024 1:34 PM	Text Document	29 KB
registry_sih	1/18/2024 1:34 PM	Text Document	1 KB
registry_StorePolicy	1/18/2024 1:34 PM	Text Document	1 KB
registry_StoreWUApproval	1/18/2024 1:34 PM	Text Document	1 KB
registry_superfetch	1/18/2024 1:34 PM	Text Document	1 KB
registry_waasassessment	1/18/2024 1:34 PM	Text Document	1 KB
registry_WindowsSelfhost	1/18/2024 1:34 PM	Text Document	2 KB
registry_wu	1/18/2024 1:34 PM	Text Document	1 KB
registry_wuhandlers	1/18/2024 1:34 PM	Text Document	2 KB
registry_wupolicy	1/18/2024 1:34 PM	Text Document	1 KB
registry_wupolicy_mdm	1/18/2024 1:34 PM	Text Document	1 KB
registry_wupolicy_ux	1/18/2024 1:34 PM	Text Document	1 KB
SQMMachineId	1/18/2024 1:34 PM	Text Document	1 KB

PC > Data (D:) > Temp > Troubleshooting Logs > WindowsUpdateLogs > Users > kegoosse > AppData > Local > Temp > 2712fc3c-7d81-420b-a0b4-45d39e2c7a77 >

Name	Date modified	Type	Size
MoUsoCoreWorker.0c6b6991-9321-4733-b302-9d138b6971a5.1.etl	1/18/2024 9:12 AM	ETL File	20 KB
MoUsoCoreWorker.0f550dc3-643c-4b0a-ab48-447d09c45403.1.etl	1/18/2024 8:58 AM	ETL File	76 KB
MoUsoCoreWorker.0f550dc3-643c-4b0a-ab48-447d09c45403.2.etl	1/18/2024 8:59 AM	ETL File	12 KB
MoUsoCoreWorker.1ee2db10-069b-4a90-8e09-8c03a1f4911b.1.etl	1/17/2024 7:46 PM	ETL File	32 KB
MoUsoCoreWorker.2e0c8dde-4f7e-4371-9d30-653221a134ce.1.etl	1/17/2024 5:58 PM	ETL File	76 KB
MoUsoCoreWorker.2e0c8dde-4f7e-4371-9d30-653221a134ce.2.etl	1/17/2024 5:59 PM	ETL File	8 KB
MoUsoCoreWorker.2f51b001-f0fd-4ead-bcc0-58d9398cbc44.1.etl	1/16/2024 6:42 PM	ETL File	72 KB
MoUsoCoreWorker.2f51b001-f0fd-4ead-bcc0-58d9398cbc44.2.etl	1/16/2024 6:57 PM	ETL File	28 KB
MoUsoCoreWorker.2fd01b49-4d17-47ab-8d15-6954fe9942fa.1.etl	1/18/2024 1:13 AM	ETL File	20 KB
MoUsoCoreWorker.4aca0c38-dcf3-45b6-b5f1-3ad5b449f569.1.etl	1/18/2024 12:28 AM	ETL File	36 KB
MoUsoCoreWorker.4aef0ef2-8167-4bf4-9a61-e56b1aa31439.1.etl	1/17/2024 6:21 PM	ETL File	32 KB
MoUsoCoreWorker.4e37054a-8c1f-475f-bd50-a0473b5b025b.1.etl	1/16/2024 10:29 PM	ETL File	28 KB
MoUsoCoreWorker.5f354b07-99c8-4b35-afe1-206efb28636a.1.etl	1/17/2024 7:34 PM	ETL File	36 KB
MoUsoCoreWorker.06ec83b5-cc89-4b69-a013-cc0d20c0b080.1.etl	1/18/2024 12:26 PM	ETL File	64 KB
MoUsoCoreWorker.6ee4c7b7-65d4-475c-8c67-d118048a80ca.1.etl	1/16/2024 10:27 AM	ETL File	28 KB
MoUsoCoreWorker.7a4614d4-75d6-44df-8804-57cb6f8f727e.1.etl	1/16/2024 8:14 AM	ETL File	52 KB

# Look up the alerts

## Device alerts - Windows Deployment | Microsoft Learn

Filter by title

Windows Autopatch

> Overview

> Prepare

> Deploy

> Operate

> Software update management

> Windows quality and feature update reports overview

Windows quality and feature update reports overview

> Windows quality update reports

> Windows feature update reports

Windows quality and feature update device alerts

Policy health and remediation

Maintain the Windows Autopatch environment

Manage driver and firmware updates

Submit a support request

Exclude a device

### Alert resolutions

Alert resolutions are provided through the Windows Update service and provide the reason why an update didn't perform as expected. The recommended actions are general recommendations and if additional assistance is needed, [submit a support request](#).

Alert message	Description	Windows Autopatch recommendation(s)
CancelledByUser	User canceled the update	The Windows Update service has reported the update was canceled by the user. It's recommended to work with the end user to allow updates to execute as scheduled.
DamagedMedia	The update file or hard drive is damaged	The Windows Update service has indicated the update payload might be damaged or corrupt. It's recommended to run <code>chkdsk /F</code> on the device with administrator privileges, then retry the update. For more information, see <a href="#">chkdsk</a> .
DeploymentConflict	Device is in more than one deployment of the same update type. Only the first	The Windows Update service has reported a policy conflict. For more information, see the <a href="#">Windows Autopatch Policy Health dashboard</a> .



# Troubleshooting

## Part 2

# Troubleshooting Flow

---

1. You try to troubleshoot yourself
2. You file a support case (or submit via FeedbackHub)
3. Support will attempt to provide an answer
4. If it is a tricky one, they will escalate to an escalation engineer in the area who has more expertise in the update area
5. If it is a super tricky one and/or an actual bug it will escalate further to the actual Windows update product team
6. We will then do all the steps I'm about to tell you to do to figure out what is going wrong, why, and how to fix it. **You can leverage a lot of how we do this to better troubleshoot** in step 1!

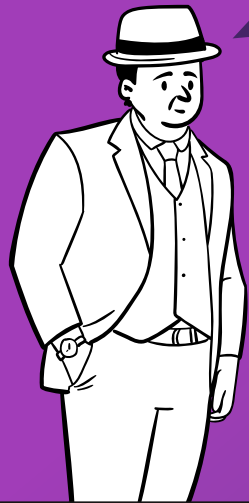
# Behind the Scenes

---

>> 2 days ago, Tim's devices weren't updating.

>> Tim's state == Frustrated

>> Tim called Ken to figure out what was going wrong.



20% of devices aren't updating!

Can you be more specific?  
What update(s) did you  
expect that the devices are  
not receiving?



1

**Tip - Be specific** about what you want the outcome to be.

Focusing on the goal rather than what you think is wrong is very helpful when troubleshooting / having support recommend the right remediation.



The devices aren't getting the Windows 11, 22H2 feature update

Got it! Have you checked that they are properly configured to be offered the update?



2

**Tip - Always** check that the device are properly configured to achieve the outcome that you want.

*Tim when his devices aren't working*

*Ken calmly wishing this wasn't the third time today...*

# 2

When checking policies are configured correctly:

- First, check that it is configured to what it should be with the tool it should be
- Second, check that it is not configured to something else with a different tool

Aka check:

- ☐ Graph API enrollment
- ☐ CSPs configured
- ☐ GPs configured

# Check Graph API

Common error case where the device is invalid (*probably WPI, which is unsupported in the deployment service*).



```
GET beta https://graph.microsoft.com/beta/admin/windows/updates/updatableAssets

Request body Request headers Modify permissions Access token

OK - 200 - 1712ms

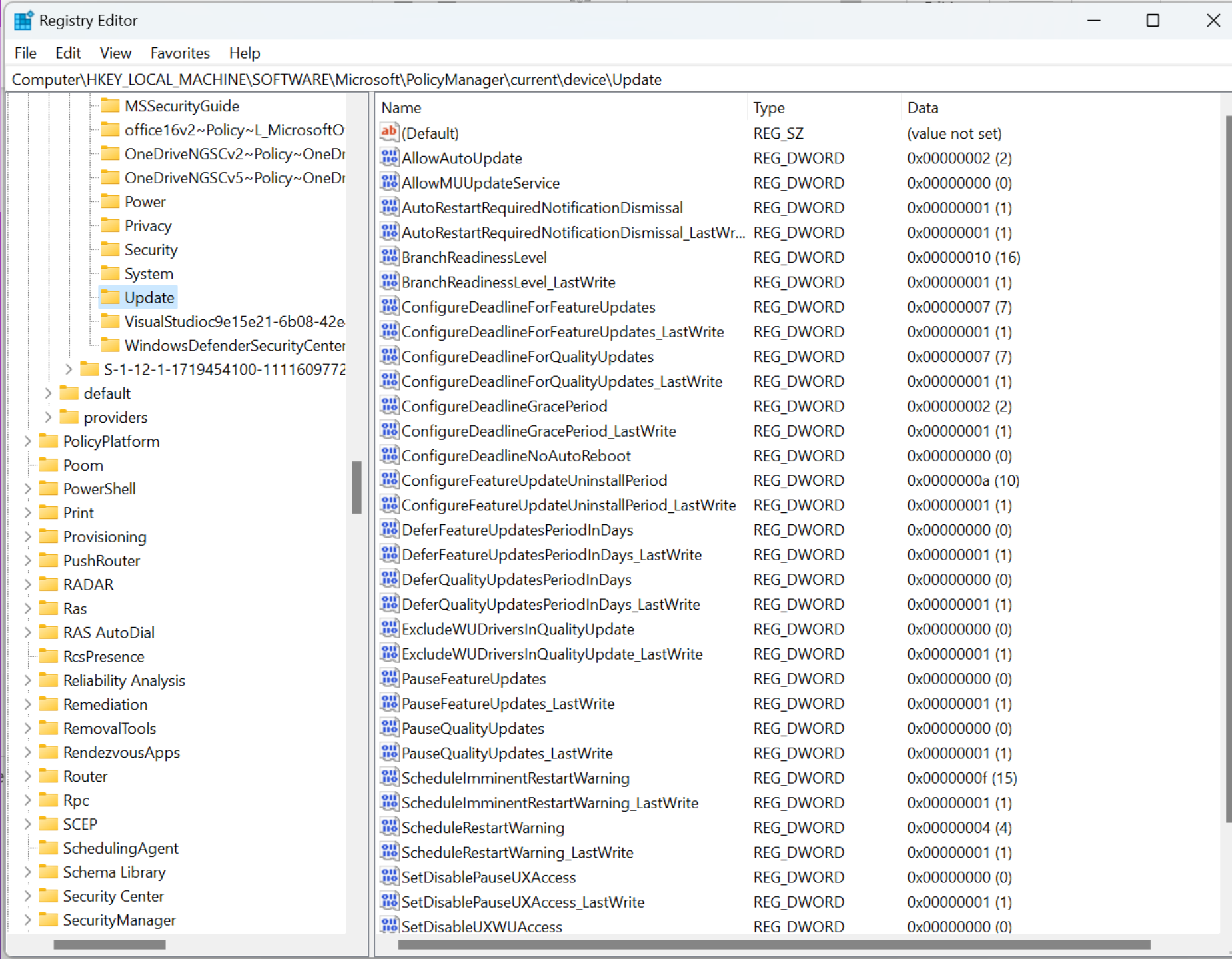
Response preview Response headers Code snippets Toolkit component Adaptive cards

{
  "@odata.type": "#microsoft.graph.windowsUpdates.azureADDevice",
  "id": "a210e167-8df1-4f34-a3a0-eaca2a8434e4",
  "errors": [
    {
      "@odata.type": "#microsoft.graph.windowsUpdates.azureADDeviceRegistrationError",
      "reason": "invalidAzureADJoin"
    }
  ],
  "enrollments": [
    {
      "@odata.type": "#microsoft.graph.windowsUpdates.updateManagementEnrollment",
      "updateCategory": "feature"
    },
    {
      "@odata.type": "#microsoft.graph.windowsUpdates.updateManagementEnrollment",
      "updateCategory": "driver"
    }
  ]
},
{
  "@odata.type": "#microsoft.graph.windowsUpdates.azureADDevice",
  "id": "78483fd3-eaec-45cd-8ee7-443e408b7cd7",
  "errors": [],
  "enrollments": [
    {
      "@odata.type": "#microsoft.graph.windowsUpdates.updateManagementEnrollment",
      "updateCategory": "feature"
    },
    {
      "@odata.type": "#microsoft.graph.windowsUpdates.updateManagementEnrollment",
      "updateCategory": "driver"
    }
  ]
}
]
```



# CSP Path

...\\SOFTWARE\\Microsoft\\PolicyMa  
nager\\current\\device\\Update



Registry Editor

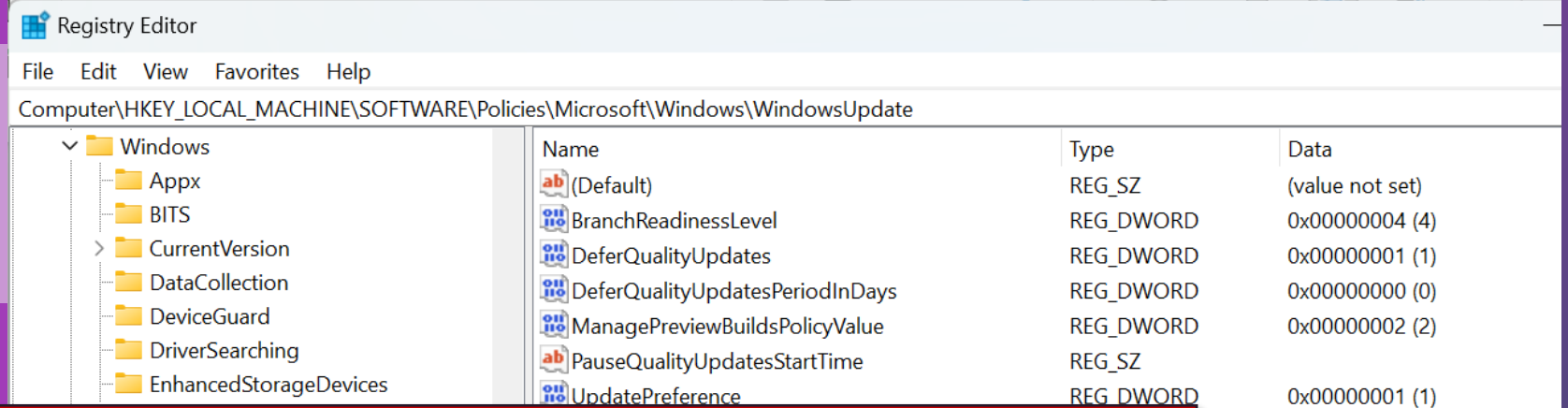
File Edit View Favorites Help

Computer\\HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\PolicyManager\\current\\device\\Update

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowAutoUpdate	REG_DWORD	0x00000002 (2)
AllowMUUpdateService	REG_DWORD	0x00000000 (0)
AutoRestartRequiredNotificationDismissal	REG_DWORD	0x00000001 (1)
AutoRestartRequiredNotificationDismissal_LastWrite	REG_DWORD	0x00000001 (1)
BranchReadinessLevel	REG_DWORD	0x00000010 (16)
BranchReadinessLevel_LastWrite	REG_DWORD	0x00000001 (1)
ConfigureDeadlineForFeatureUpdates	REG_DWORD	0x00000007 (7)
ConfigureDeadlineForFeatureUpdates_LastWrite	REG_DWORD	0x00000001 (1)
ConfigureDeadlineForQualityUpdates	REG_DWORD	0x00000007 (7)
ConfigureDeadlineForQualityUpdates_LastWrite	REG_DWORD	0x00000001 (1)
ConfigureDeadlineGracePeriod	REG_DWORD	0x00000002 (2)
ConfigureDeadlineGracePeriod_LastWrite	REG_DWORD	0x00000001 (1)
ConfigureDeadlineNoAutoReboot	REG_DWORD	0x00000000 (0)
ConfigureFeatureUpdateUninstallPeriod	REG_DWORD	0x0000000a (10)
ConfigureFeatureUpdateUninstallPeriod_LastWrite	REG_DWORD	0x00000001 (1)
DeferFeatureUpdatesPeriodInDays	REG_DWORD	0x00000000 (0)
DeferFeatureUpdatesPeriodInDays_LastWrite	REG_DWORD	0x00000001 (1)
DeferQualityUpdatesPeriodInDays	REG_DWORD	0x00000000 (0)
DeferQualityUpdatesPeriodInDays_LastWrite	REG_DWORD	0x00000001 (1)
ExcludeWUDriversInQualityUpdate	REG_DWORD	0x00000000 (0)
ExcludeWUDriversInQualityUpdate_LastWrite	REG_DWORD	0x00000001 (1)
PauseFeatureUpdates	REG_DWORD	0x00000000 (0)
PauseFeatureUpdates_LastWrite	REG_DWORD	0x00000001 (1)
PauseQualityUpdates	REG_DWORD	0x00000000 (0)
PauseQualityUpdates_LastWrite	REG_DWORD	0x00000001 (1)
ScheduleImminentRestartWarning	REG_DWORD	0x0000000f (15)
ScheduleImminentRestartWarning_LastWrite	REG_DWORD	0x00000001 (1)
ScheduleRestartWarning	REG_DWORD	0x00000004 (4)
ScheduleRestartWarning_LastWrite	REG_DWORD	0x00000001 (1)
SetDisablePauseUXAccess	REG_DWORD	0x00000000 (0)
SetDisablePauseUXAccess_LastWrite	REG_DWORD	0x00000001 (1)
SetDisableUXWUAccess	REG_DWORD	0x00000000 (0)

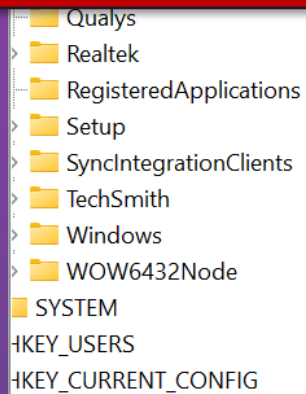
# Group Policy Path

...\\SOFTWARE\\Policies\\Microsoft\\Windows\\WindowsUpdate



Name	Type	Data
(Default)	REG_SZ	(value not set)
BranchReadinessLevel	REG_DWORD	0x00000004 (4)
DeferQualityUpdates	REG_DWORD	0x00000001 (1)
DeferQualityUpdatesPeriodInDays	REG_DWORD	0x00000000 (0)
ManagePreviewBuildsPolicyValue	REG_DWORD	0x00000002 (2)
PauseQualityUpdatesStartTime	REG_SZ	
UpdatePreference	REG_DWORD	0x00000001 (1)

**WARNING:** MDM Wins Over GPO does  
**NOT** apply to the Windows Update policies  
*(or a variety of other areas)*

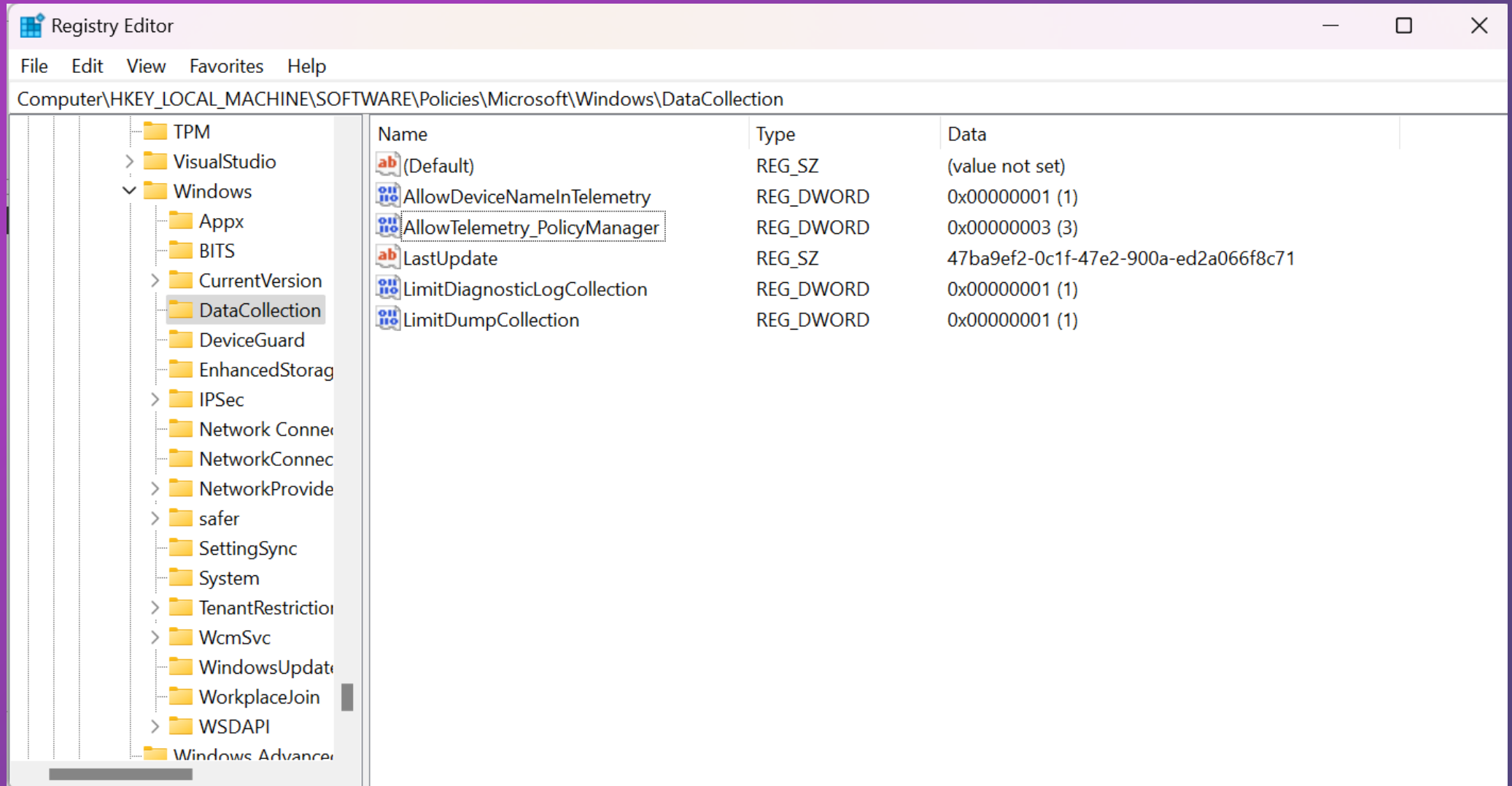


Qualys  
Realtek  
RegisteredApplications  
Setup  
SyncIntegrationClients  
TechSmith  
Windows  
WOW6432Node  
SYSTEM  
HKEY\_USERS  
HKEY\_CURRENT\_CONFIG

While you're in the registry, may as well check telemetry, safeguards and eligibility as well.

Appraiser Markers

# Check Telemetry is being sent



# Safeguards & Win 11 eligibility

- GStatus
- UpgEx

Registry Editor

File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\NI22H2

Name	Type	Data
DataRelDate	REG_SZ	08/11/2023
DataRelDateEpoch	REG_SZ	1691712000
DataVer	REG_SZ	2651
DataVerRecommended	REG_SZ	TRUE
DestBuildNum	REG_SZ	22621
DestBuildNumList	REG_SZ	22621,22622,22623,22631
FailedPrereqs	REG_MULTI_SZ	None
Fam	REG_SZ	0
Fing	REG_SZ	0
Free	REG_SZ	gt64
GatedBlockId	REG_MULTI_SZ	None
GatedBlockReason	REG_MULTI_SZ	None
GatedFeature	REG_MULTI_SZ	None
GenTelRunTimestamp	REG_SZ	133364043732970120
Genuine	REG_SZ	1
GStatus	REG_SZ	2
Guest	REG_SZ	0
InboxDataVersion	REG_SZ	2650
MCE	REG_SZ	0
OemPref	REG_SZ	0
Office	REG_SZ	1
Paper	REG_SZ	0
Perf	REG_SZ	Unknown
RedReason	REG_MULTI_SZ	None
SdbVer	REG_SZ	2651
Timestamp	REG_QWORD	0x1d9cde4301925dc (1333640439273323
TimestampEpochString	REG_SZ	1691930792
Touch	REG_SZ	1
UpgEx	REG_SZ	Green
UpgExU	REG_SZ	Green
Version	REG_SZ	12
WIP	REG_SZ	1

#FunFact – over 50% of cases where “updates are not being offered” that we see are because WSUS is still being configured on the device *(often by Configuration Manager)*.



**Check your configurations!**



Yes! Of course I checked the policies were configured correctly

Great! Did you pull WU Logs from some of the devices?  
([aka.ms/wucopylogsexternal](https://aka.ms/wucopylogsexternal))



3

When in doubt – **pull logs**

*Tim when his devices aren't working*

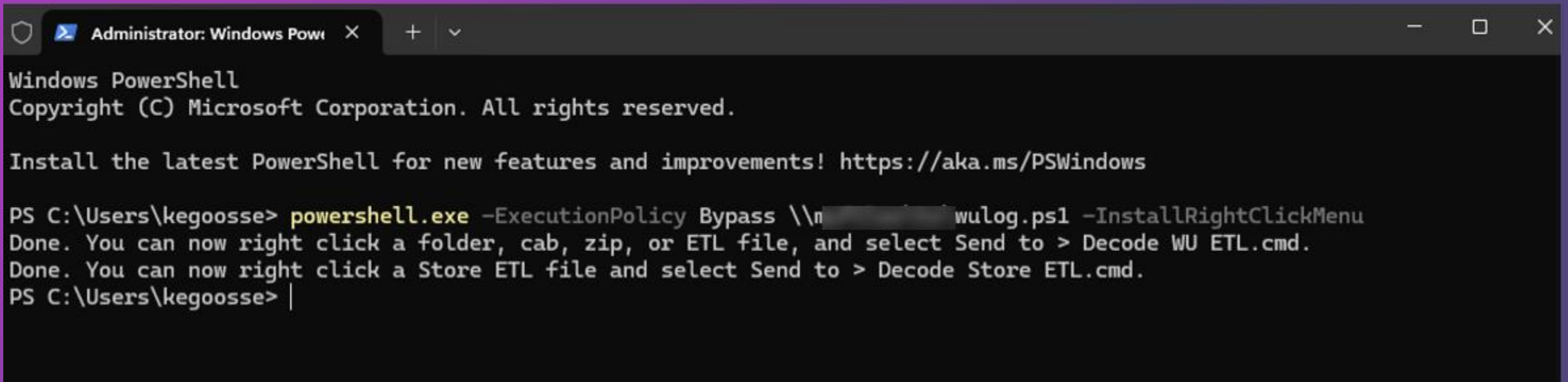
*Ken calmly wishing this wasn't the third time today...*



# How to get the decode tool

- VPN Connection Required
- Run the command below in PowerShell

```
powershell.exe -ExecutionPolicy Bypass \\%path%\wulog.ps1 -InstallRightClickMenu
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

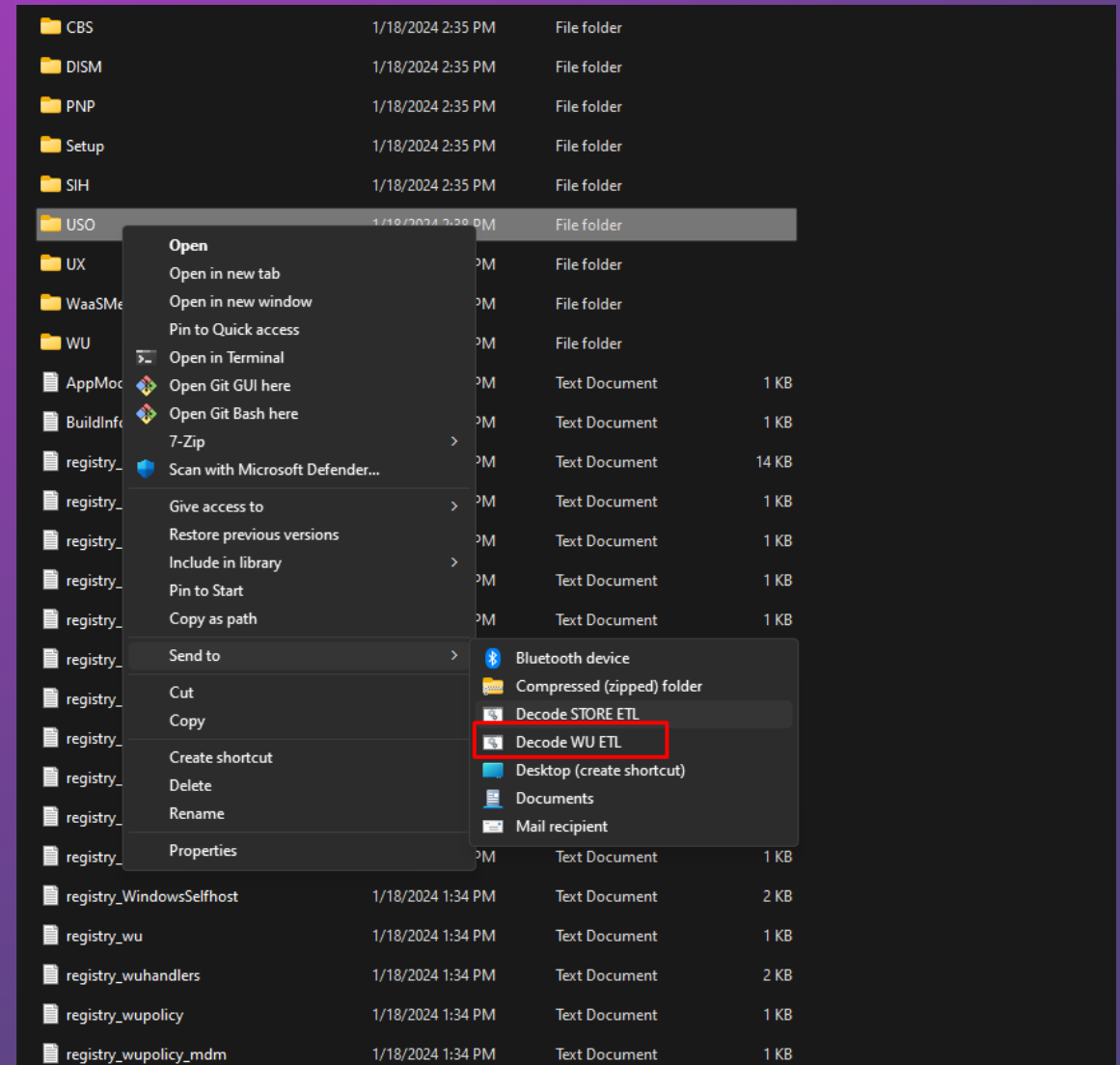
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\kegoosse> powershell.exe -ExecutionPolicy Bypass \\n[REDACTED]wulog.ps1 -InstallRightClickMenu
Done. You can now right click a folder, cab, zip, or ETL file, and select Send to > Decode WU ETL.cmd.
Done. You can now right click a Store ETL file and select Send to > Decode Store ETL.cmd.
PS C:\Users\kegoosse> |
```

# What just happened on my computer?

2 options are added the Send to function when you right click a file or folder

- Decode STORE ETL
- Decode WU ETL



# Demo

---

We are going to demo pulling and decoding Windows update logs.



InPrivate

Windows feature updates - Micro x

Monitor - Microsoft Azure x

New InPrivate tab x

+

←

↺

🔍 Search or enter web address

☆

📖

☆

🔗

🛡️

📄

⋮

CAT MMD

CAT MMD Reports

CAT MMD Engage...

CAT MMD Images

CAT MMD Forms

Microsoft Perks

Wiki's

MS Field Support

Home Automation

Qbus

Feedback Triage


Lunch Tracker

Acropolis CloudPC

Last Epoch

>

Other favorites



InPrivate browsing

InPrivate search with Microsoft Bing

🔍

✔️ What InPrivate browsing does

Deletes your browsing info when you close all InPrivate windows

Saves collections, favorites, and downloads (but not download history)

Prevents Microsoft Bing searches from being associated with you

✖️ What InPrivate browsing doesn't do

Hide your browsing from your school, employer, or internet service provider

Give you additional protection from [tracking](#) by default

Add additional protection to what's available in normal browsing

Always use "Strict" tracking prevention when browsing InPrivate

☐

If this is off, we'll use the same tracking prevention setting as a normal browsing window

↓ More details

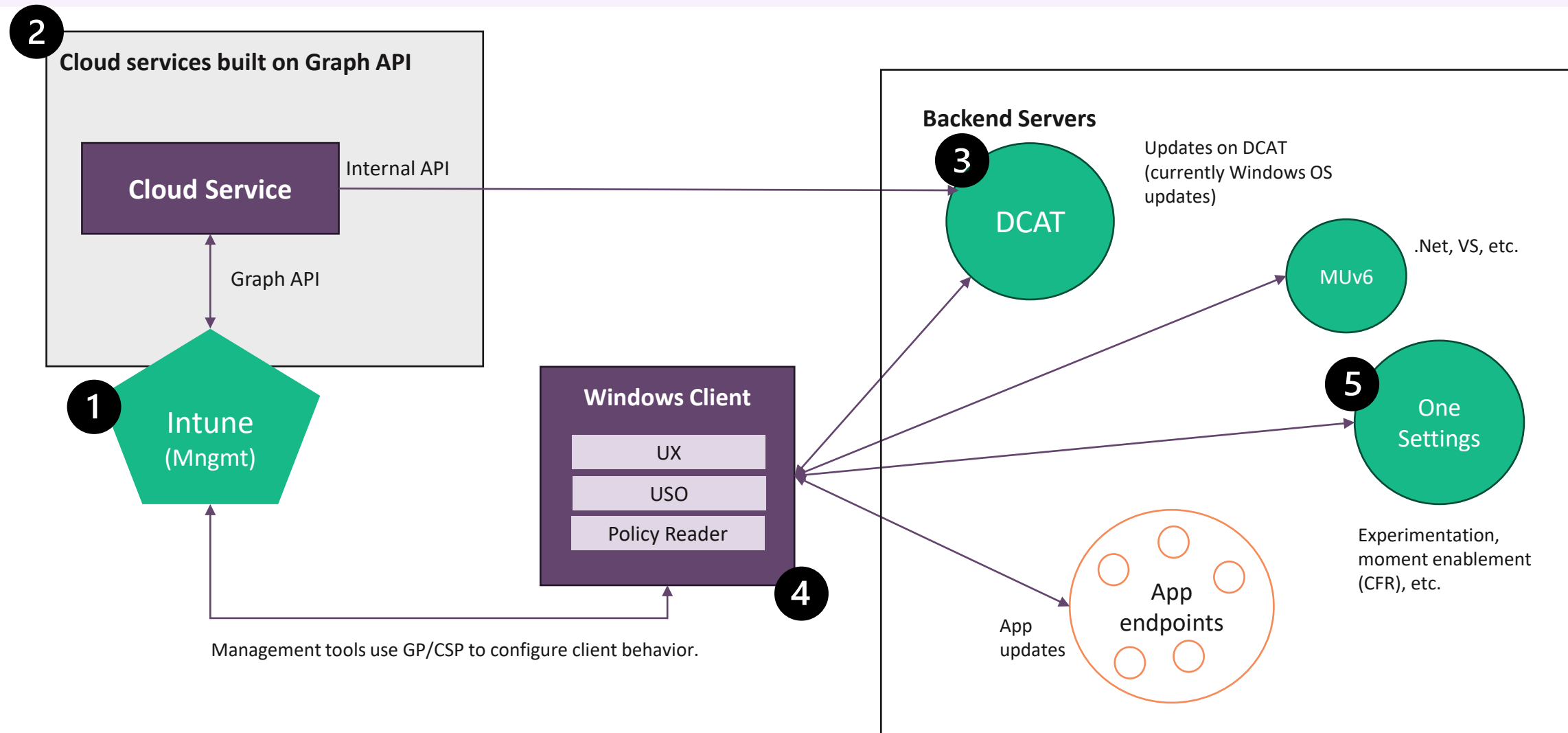
Before going into the logs, we need to learn:

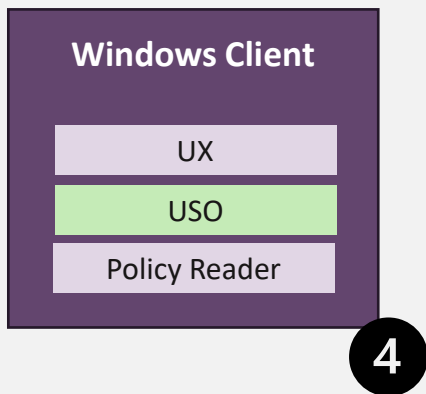
---

>> What are the systems involved and what do they do?

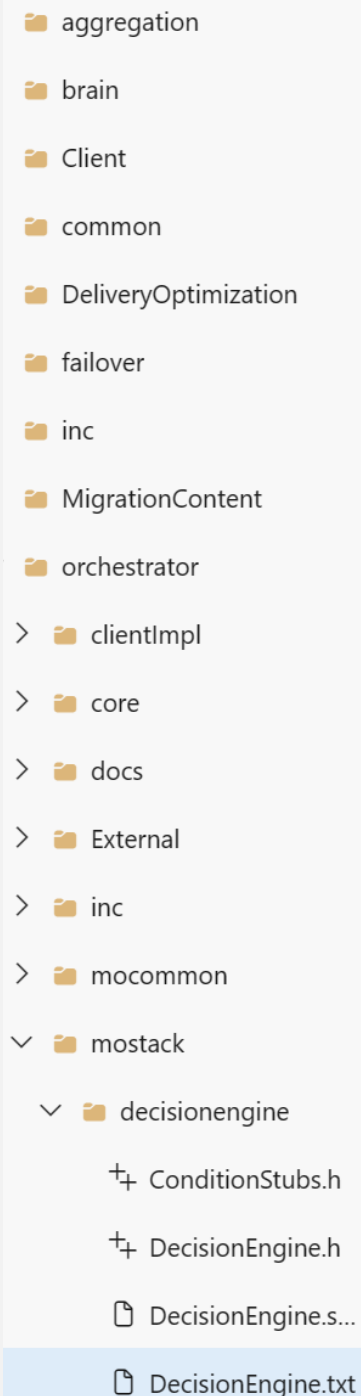
*Avoid blindly searching in logs →*

# High Level Architecture





Policy Reader passes policies to the update stack (USO) which will then take actions based upon them



main / src / orchestrator / mostack / decisionengine / DecisionEngine.txt

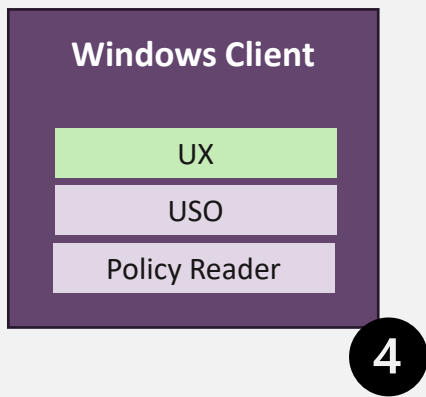
## DecisionEngine.txt

Contents History Compare Blame

```
99
100 #####
101
102 Action Notify policy requirement met : false
103 Action Honor AutoUpdate Download Policy = true
104 Policy Notify To Download = true
105
106 Action Notify policy requirement met : false
107 Action Honor AutoUpdate Install Policy = true
108 Policy Notify To Install = true
109 Immediate install preferred = false
110
111 Action Notify policy requirement met : true
112
113 #####
114
115 Exclusivity requirement met : false
116 Action is exclusive = true
117 Same action is running = true
118
119 Exclusivity requirement met : true
120
121 #####
122
123 Action active hours requirement met : false
124 Policy active hours restricted = true
125 System inside active hours = true
126
127 Action active hours requirement met : true
128
129 #####
130
131 Serialization should block : false
132 System volume available space MB >= 4000
133
134 Serialization should block : false
135 Update critical = true
136
137 Serialization should block : false
```

notify





The update stack (USO) triggers UX Broker to take action to show notifications, toasts, etc.

## Restart required by 4/4/2024 (estimate: 4 min)

① Microsoft manages your update settings

Microsoft requires important updates be installed.

Ready? Restart now. Not ready? We'll restart outside of your active hours, or you can schedule the restart.

Restart now

Pick a time

Let my device restart later

# Which information are you looking for?

01

Where is the update facing problems?

*USO logs*

02

Is the device rebooting or receiving notifications?

*UX logs*

03

My device is facing an update problem, why is that happening?

*Reporting Events & WU logs*

# 1 - Where is the problem?

(USO == MoUSOCoreWorker)

**The key:** check for non 0 hresults for *\*scan\**, *\*download\**, *\*install\**, and *\*commit\** - these indicate that that part of the process for that specific update is failing. Note down the update id.

- **Scan:** ctrl+F “\*scan\*” to find non 0 hresults – this indicates that scan has an issue.
- **Download:** ctrl+F “\*download\*” to find a non 0 hrseult
- **Install:** ctrl+F “\*install\*” to find a non 0 hrseult
- **Commit:** ctrl+F “\*commit\*” to find a non 0 hresult

*Note down the update id for any non 0 hresults*

## 2- What did my end user see?

*There are three different UX logs:*

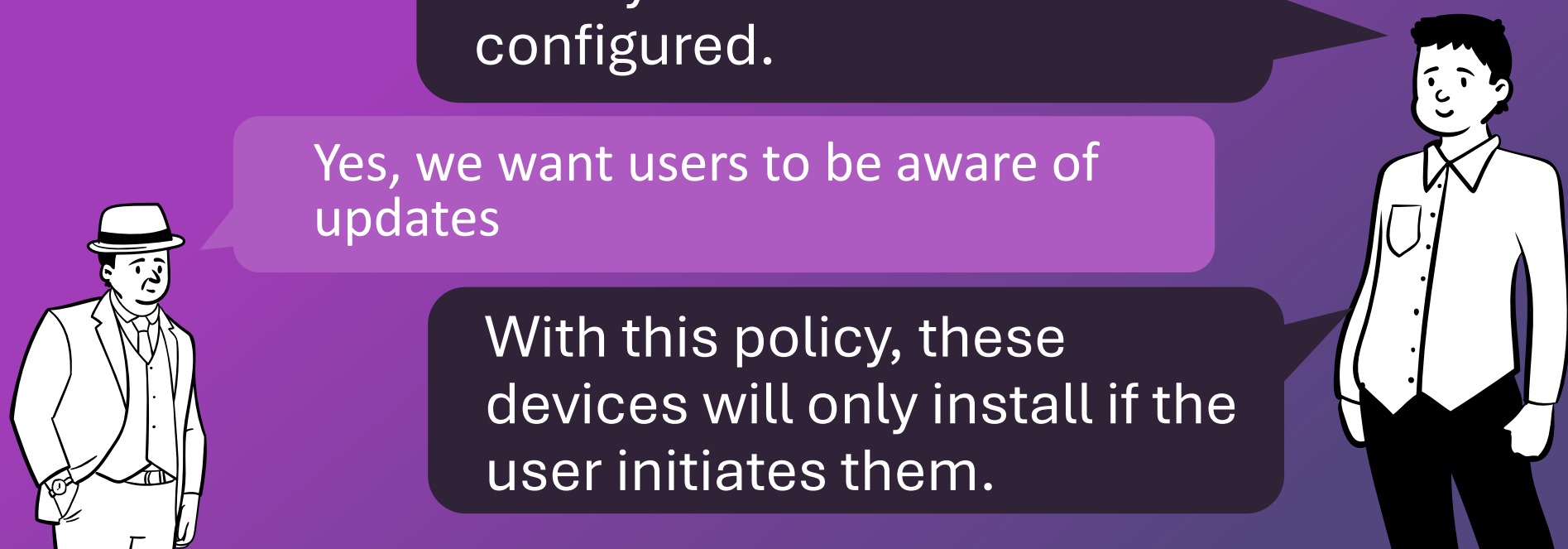
- **MoUxCoreWorker** – policies and reboot timing
- **UpdateUx** – settings page issues
- **MoNotificationUX** – notification issues

Did the reboot and notifications happen when they were supposed to? (UX == MoUXCoreWorker)

### **P.s. use Windows 11**

*(You probably won't find these logs on 10...)*

- Check config
- Did it succeed? Check if 'update' is found for that update
- When was the update installed?
- Did it actually happen then? See if 'defer restart' = True
- Did the user see a notification? Check if 'display notification' = True



Looking at logs, you have  
“notify to install”  
configured.

Yes, we want users to be aware of  
updates

With this policy, these  
devices will only install if the  
user initiates them.

4

It is usually a policy misconfiguration or a misunderstanding of how the policy is supposed to work that causes undesired experiences. Be sure to check out the latest documentation for how a policy should impact your user’s experience.

Ps if you already know where the update went wrong you can skip all this, start here:

- [Reportingevents logs](#)
- [Windows Update error code list by component - Windows Deployment | Microsoft Learn](#)

**I found the issue!**

Uh, Now What?



# Remediation

## Part 3

# Ways to fix things

- Configure your policies per recommendations *(you can fix)*
- Look at the common error + recommended remediations section to see if you can follow the suggested solutions *(you can fix)*
- If your issue is not in that section and there is a download/install error, let the device retry – there is a lot of self-healing and retrying is often best *(let it fix itself)*
- If that doesn't work, file a bug via Feedback hub or support case to escalate to our engineers – it may then be a bug in the code *(let us fix that)*

# 55 Errors and what you can do about them

ENUM	Display Name	Recommended Remediation
1	Unexpected Shutdown	Ensure the device remains on during Windows installation.
2	Install Access Denied	Retry the installation.
3	Damaged Media	Run Chkdsk /F on the device with administrator privileges, then retry the update.
4	Cancelled By User	Retry the installation.
5	Install Issue Redirection	Report to Microsoft if this is encountered more than once.
6	Windows Repair Required	Run the Startup Repair Tool on this device.
7	File Not Found	Download the update again, and then retry the installation.
8	Install System Error	Check that the BIOS and drivers are up to date. Retry the download.
9	Install Setup Error	Check that the BIOS and drivers are up to date. Retry the download.
10	WU Component Missing	Run <code>dism /online /cleanup-image /restorehealth</code> on the device with administrator privileges, then retry the update. If the commands fails, a reinstall of Windows may be required.
11	Incompatible Architecture	Make sure the target operating system architecture matches the host operating system architecture.
12	Superseded	Update your media sources to the most recently available version.
13	Download Credentials Issue	Retry. If it fails again, review your network configuration to make sure that this computer can access the internet. If you need help, contact support.