

Unlocking the Secrets of Intune Troubleshooting: A Deep Dive into Mastery





Thank you Sponsors

liquidware™



2Pint

Gold



RECAST SOFTWARE

Silver



Technical Partners

CONSULTEQ

PROXSYS*


Daalmans
consulting


Secure At Work



About Jörgen Nilsson

Focus

Windows 365, Intune, Endpoint Security

From

Sweden

My Blog

[Https://ccmexec.com](https://ccmexec.com)

Certifications

MVP Security + Windows & Devices, MCT

Hobbies

Barbecue

Contact

www.linkedin.com/in/ccmexec





About Ronni Pedersen

Focus

Microsoft Intune, Security

From

Denmark

My Blog

<https://ronnipedersen.com/>



Certifications

2 x MVP: Security & Windows

Hobbies

Hiking, BBQ

Contact

[linkedin.com/in/ronnipedersen](https://www.linkedin.com/in/ronnipedersen)

The evolution of Troubleshooting

A walk down the memory lane...





The Evolution of Troubleshooting

Back in the day...

- Dial-up modems screeching their song of connection
- Logging into a BBS to hunt for fixes
- Downloading a single patch could take all night





How we used to do it...

Troubleshooting with ConfigMgr

- Endless log files everywhere
- Both client side and server side
- Complex? Absolutely. But you *could* see every little detail

Troubleshooting Group Policy

- gpresult - Your policy X-ray machine
- gpupdate = The “hit refresh & hope” button
- RSOP = Your policy crystal ball





Troubleshooting in the Intune Era

The "Classic" Intune Toolkit

- Log files (MDM) → Event Viewer
- Registry values
- IME Agent = Log files 😊

Your new superpowers!

- **Microsoft Copilot** → Your AI sidekick 🧑
- **Copilot for Security** → Cyber shield & sword?
- **ChatGPT** → Your troubleshooting oracle



Intune Policies





Configuration Policies

Recommended order for Windows devices

- Security Baselines (if required)
- Endpoint Security
- Settings Catalog
- Custom ADMX ingestion (3rd. Party apps)
- PowerShell Scripts

Optional:

- Remediation scripts

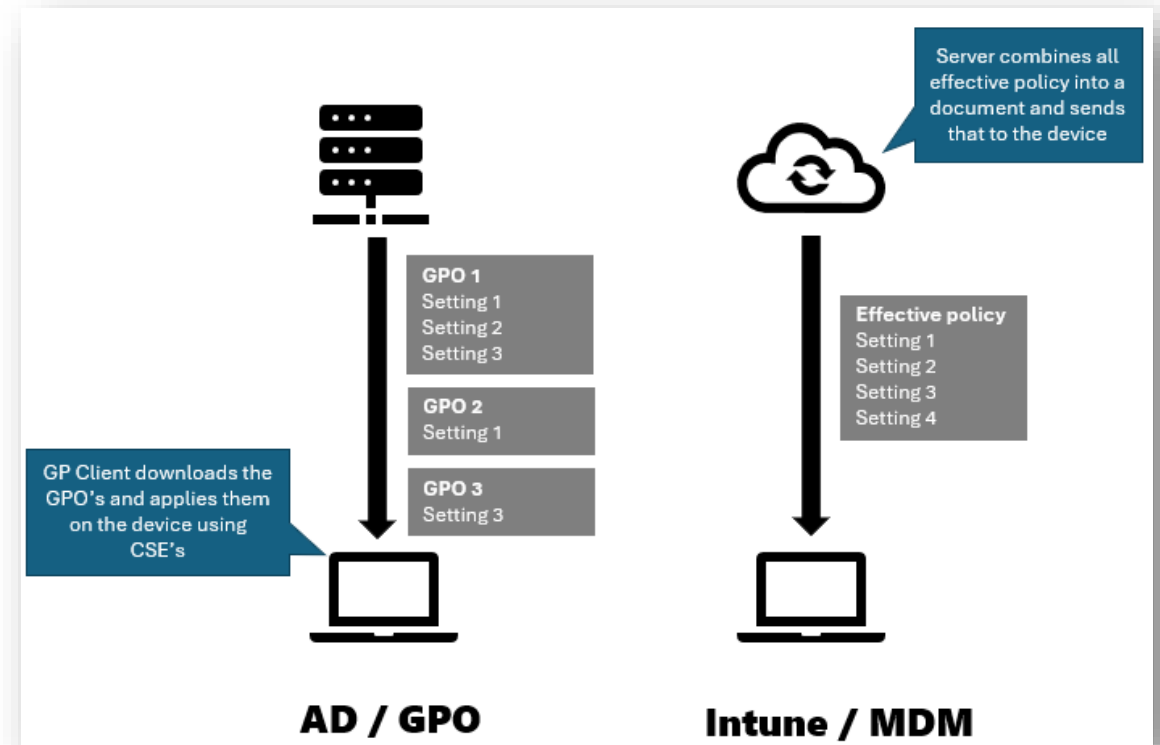
Note: Requires a Windows Enterprise E3 license





Intune policy

- Intune policies are processed in the cloud
- Group Policies are processed on the client
 - Local Policy
 - Site
 - Domain
 - OU
- We can have different values at different levels to handle exclusions
 - That is not possible with Intune Policies





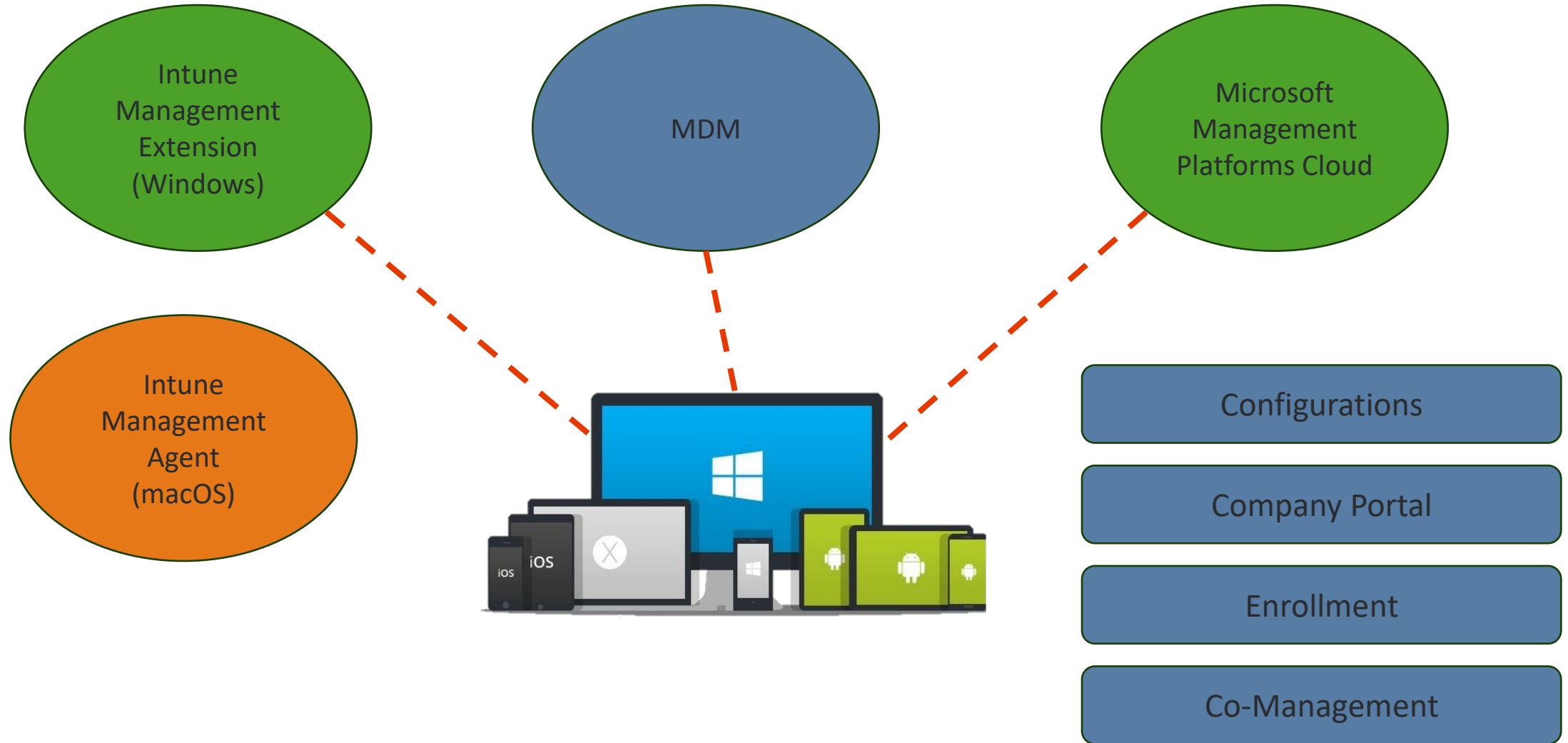
Policy/Profile Conflicts

- Intune policies are compiled server side.
- Compliance policy settings always have precedence over configuration profile settings.
- Compliance policy conflicts: The most restrictive compliance policy setting applies.
 - Conflict is shown in Intune. Manually resolve these conflicts.
- Some conflicts are shown as error depending on setting type.





Overview

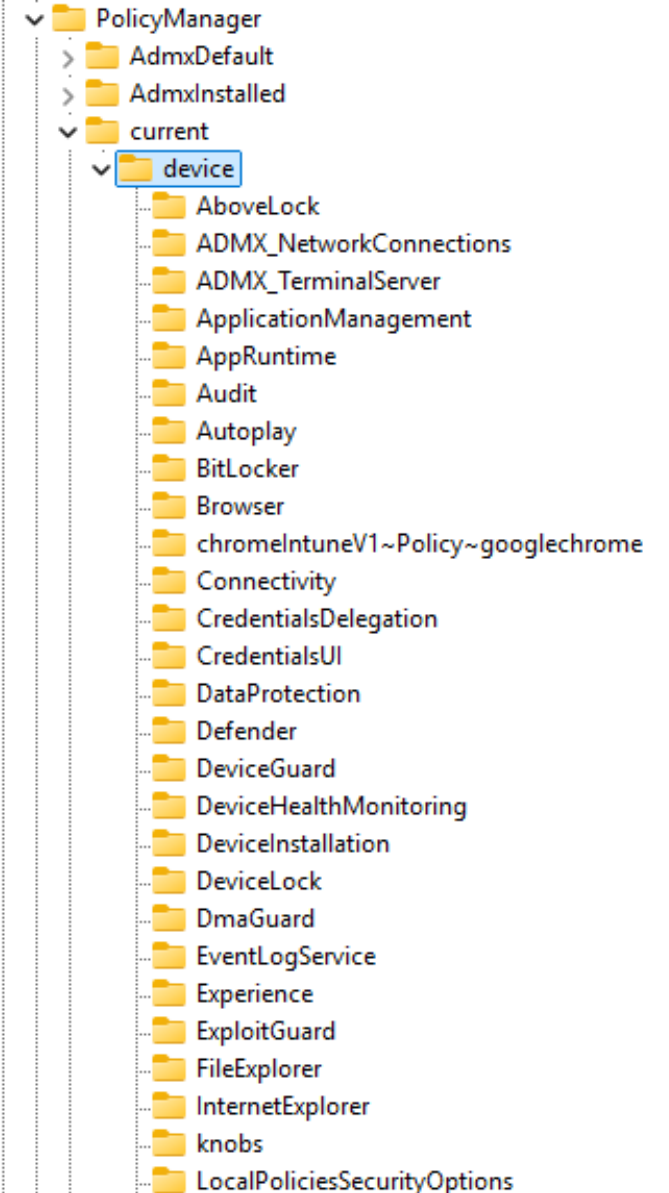




Policy Manager

- Registry location for all policies coming from MDM
- Ingested ADMX files
- Current values
- For ADMX backed policies -> Policy Manager -> Policies values

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager





Removing a policy (Policy Tattoo)

- Does not necessarily change the value back, depends on the CSP

ⓘ Note

When a profile is removed or no longer assigned to a device, different things can happen, depending on the settings in the profile. The settings are based on CSPs, and each CSP can handle the profile removal differently. For example, a setting might keep the existing value, and not revert back to a default value. The behavior is controlled by each CSP in the operating system. For a list of Windows CSPs, see [configuration service provider \(CSP\) reference](#).

To change a setting to a different value, create a new profile, configure the setting to **Not configured**, and assign the profile. Once applied to the device, users should have control to change the setting to their preferred value.

When configuring these settings, we suggest deploying to a pilot group. For more Intune rollout advice, see [create a rollout plan](#).

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign>



Timing when removing a user policy

- Removing a user from an Entra ID group with a policy assigned to it.

- A profile applies to a user group. Later, a user is removed from the group. For the settings to be removed from that user, it can take up to 7 hours or more for:
 - The profile to be removed from the policy assignment in the Intune admin center
 - The device to sync with the Intune object using the [platform-specific policy refresh cycle](#) (in this article)

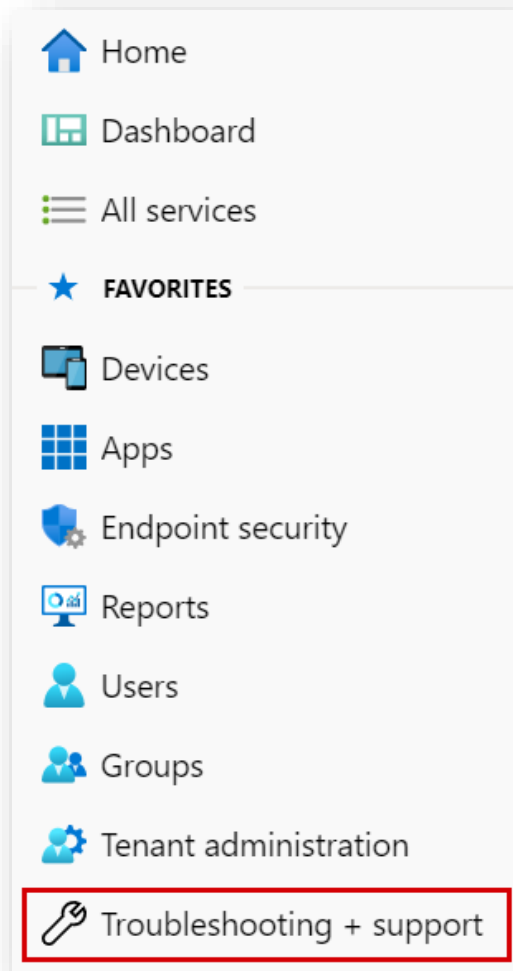
<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot>

Troubleshooting Options





Use the built-in Troubleshoot pane



Microsoft Endpoint Manager admin center

Home > Troubleshooting + support

Troubleshooting + support | Troubleshoot

Search (Ctrl+ /) <<

Guided scenarios (preview)

Troubleshoot

Help and support

Display name
IW Worker

Intune license

Change user

Principal name
IWWWorker@contoso.com

Group memberships (3)
[Show all](#)

Email
IWWWorker@contoso.com

Assignments

Client apps

Assignment	↑↓	Name	↑↓	OS	↑↓	Type
Included		Microsoft Authenticator		iOS/iPadOS		Available
Included		Microsoft Edge		iOS/iPadOS		Available
Excluded		Microsoft Outlook		Android device administrat...		Required
Included		Microsoft Edge		macOS		Required

URL: aka.ms/Intunetroubleshooting



Troubleshooting

- MDMDiagnosticsTool
 - Settings -> Access work or school
 - **MdmDiagnosticsTool.exe -out c:\temp**

- Collect log files using Intune

<https://learn.microsoft.com/en-us/windows/client-management/mdm-collect-logs>

Advanced Diagnostic Report

Your IT or support person may want additional information to help with troubleshooting.

Create report

Name	Date modified
DeviceManagement-Enterprise-Diagn...	2024-04-25 12:54
MDMDiagReport	2024-04-25 12:54
MDMDiagReport.xml	2024-04-25 12:54
Microsoft-Windows-AAD	2024-04-25 12:54
Microsoft-Windows-Shell-Core	2024-04-25 12:54

Retire Wipe Delete Remote lock Sync Reset passcode Restart Collect diagnostics

Collect diagnostics - W11DELL01

Intune will attempt to collect the diagnostics that are on this device. To download and view the diagnostics, go to Monitor > Device diagnostics. Continue with diagnostics collection?

Yes

No



MDM Diagnostics Tool (Local)

```
Command Prompt  X  Windows PowerShell  X  +  v
PS C:\Users\RonniPedersen> MdmDiagnosticsTool.exe -out C:\WPNinjaDemo

Report location folder C:\WPNinjaDemo
PS C:\Users\RonniPedersen>
```

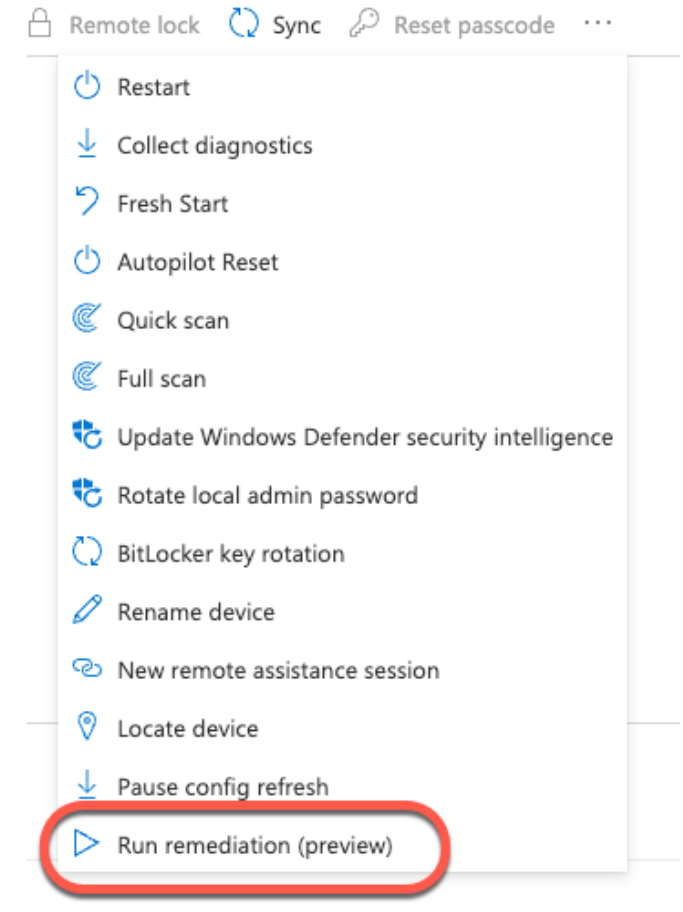
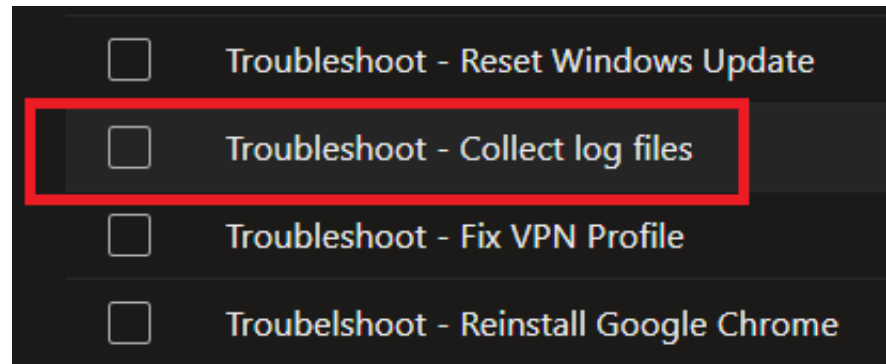
The image shows a Windows File Explorer window titled 'WPNinjaDemo'. The address bar indicates the path 'This PC > Windows (C:) > WPNinjaDemo'. The left sidebar shows the 'WPNinjaDemo' folder selected. The main pane displays a list of files and folders with columns for Name, Date modified, Type, and Size.

Name	Date modified	Type	Size
DeviceManagement-Enterprise-Diagnostics-Provider.evtx	15-09-2025 20:54	Event Log	1.092 KB
MDMDiagReport.html	15-09-2025 20:54	Microsoft Edge HTML Document	291 KB
MDMDiagReport.xml	15-09-2025 20:54	Microsoft Edge HTML Document	3.798 KB
Microsoft-Windows-Shell-Core.evtx	15-09-2025 20:54	Event Log	1.092 KB
Microsoft-Windows-AAD.evtx	15-09-2025 20:54	Event Log	1.092 KB



Build your own log collection tool

- Why? Built-in too slow, too much data
- Remediation script send to Azure Storage, SharePoint, Teams etc.
- Fast! Runs in a couple of minutes.



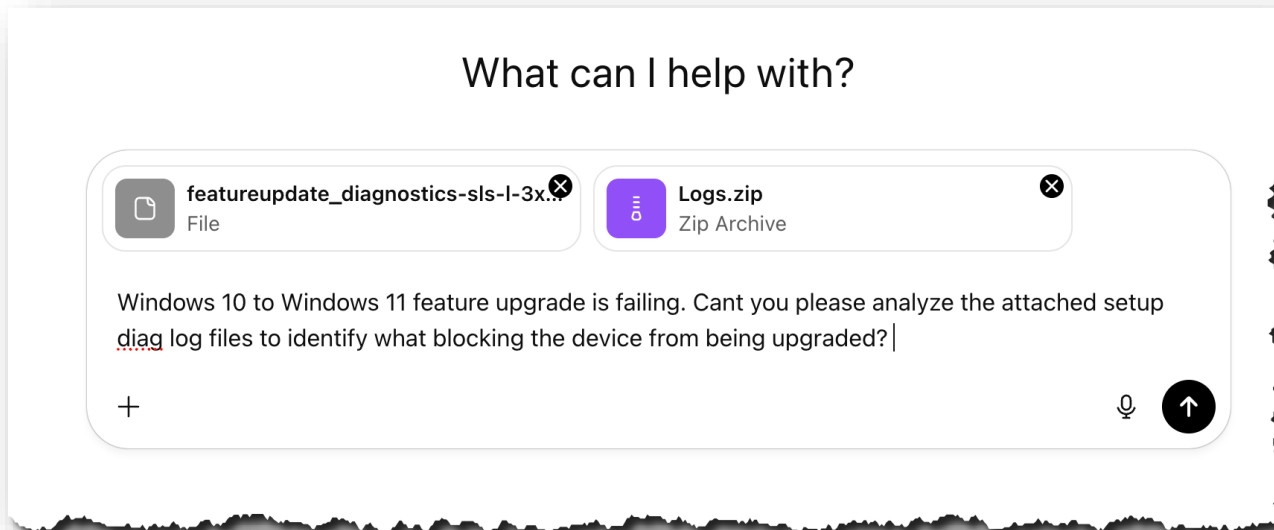
Troubleshooting in the AI Era...



Example #1: Feature Upgrade Failure

Scenario (Example)

- Feature upgrade is failing
- Collect log files...
- Analyze the logfiles... (Copilot, ChatGTP, etc.)



Microsoft 365 Copilot



 Copilot 

I've analyzed the **setupact.log** file you provided, and here's a clear summary of why the Windows 10 → Windows 11 feature upgrade is failing:

Primary Blocking Issue

- Insufficient disk space on the system drive (C:)
 - Available: ~800 MB to 1.4 GB
 - Required: 10–20 GB (depending on upgrade phase)
- Error Code: 0xC190020E (MOUPG – Insufficient disk space)
- Attempts to free space via silent cleanup and compression were unsuccessful.

Additional Observations

- External drive: Checked but not used for scratch space.
- Recovery image: Missing or not enough space to create a new WinRE image.
- Snapshot policy: Prevented creating upgrade snapshots due to low space.
- BitLocker: Enabled but handled gracefully (not the cause of failure).



ChatGPT



Short answer: it's a disk-space hard block.

What I found in your SetupDiag:

- Error: **0xC190020E – 0x4001E** (not enough free space on the system drive). featureupdate_diagnostics-sls-l...
- Required free space: **19,069 MB (~19 GB)** on the system drive before the upgrade can proceed. featureupdate_diagnostics-sls-l...
- Device: **Dell Latitude 7420**, Win10 22H2 (19045) → target **22H2 / 22621.5768**. featureupdate_diagnostics-sls-l...

How to fix (do these on the system drive, usually C:)

1. Free 20–25 GB to be safe, then retry the upgrade.

Fast wins:

- Empty Recycle Bin and %TEMP% (Win + R → %temp% → delete contents).
- Run **Storage Sense**: Settings → System → Storage → Cleanup recommendations.
- Clear Windows Update cache:
 1. Stop service: open elevated CMD → `net stop wuauerv` and `net stop bits`
 2. Delete contents of `C:\Windows\SoftwareDistribution\Download`
 3. Start services: `net start wuauerv` and `net start bits`
- Uninstall large/unused apps & move big local folders (Videos, VMs, ISO files) to another drive temporarily.
- Optional (saves several GB): disable hibernation (elevated CMD) → `powercfg -h off` (re-enable later with `powercfg -h on`).

2. Let Setup use external storage (if freeing space on C: is hard): plug in a USB drive (≥16–32 GB), then re-run the upgrade. Windows Setup can offload temporary files to it (your logs show no external drive was available during the attempt).

3. Retry the feature update after freeing space. If you use an in-place upgrade package/ISO, run `Setup.exe` from Windows and choose *Keep personal files and apps*.

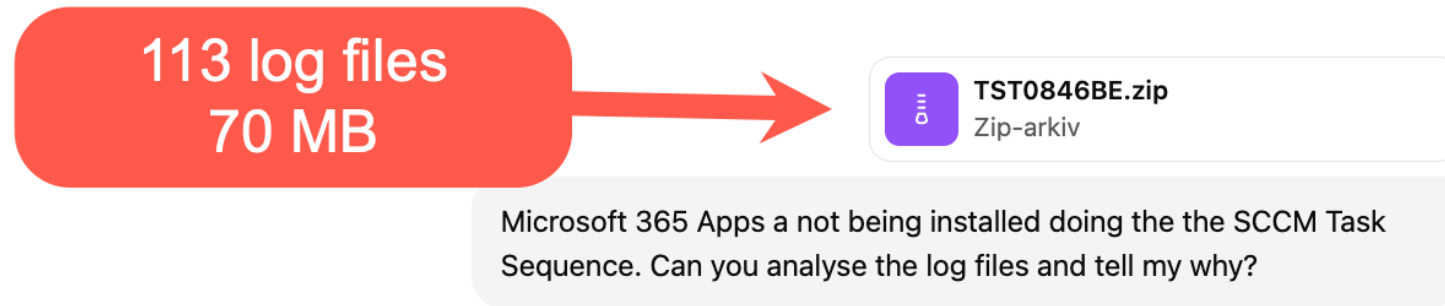
If you want, share the *current* free space on C: and I'll tailor the quickest mix of cleanups to hit the target. If the upgrade still fails after you've got >20 GB free, we can dig into the other logs for secondary issues—but right now the blocker is clearly the space hard block. featureupdate_diagnostics-sls-l...



Example #2: SCCM Task Sequence Failure

Scenario

- 3 Apps are not installed during OS provisioning



Thought for 10m 17s >

Short answer: the Office step never truly completed during the task sequence. The TS *did* kick off the Microsoft 365 Apps install, waited for status multiple times, then considered it "successful" and immediately rebooted—while Office hadn't actually finished installing. Adobe Reader and VLC genuinely failed in the same window.

ADMX





ADMX files

- Supports upload of ADMX files
- However updating them is not that easy...

Upload Status

✖ The upload of this ADMX file has failed. To continue, you will need to delete this upload, address the action in the error details and try again.

ADMX file	firefox.admx
State	failed
Last modified date	2025-02-05
Error Details	Definitions from file still in use in configurations: Windows 1.0 Mozilla Firefox

Use remediation scripts instead

Compliance policies





Compliance policies

Builtin checks

- Has a compliance policy assigned
- Is active
- A device in error state will become non-compliant after 7 days
- Enrolled user exists

Device status

! Can't access company resources

This device does not meet Onevinn compliance and security policies. You need to make some changes to this device so that you can access company resources.

Device must have firewall enabled.

[Less](#) ^

This device must have the firewall enabled. Contact your IT administrator for help.

Compliance setting in error state for more than 7 days.

[Less](#) ^

Intune couldn't determine your device's compliance with one or more settings for at least 7 days. Sometimes these errors are resolved by restarting your device and selecting Check compliance. If you do this and get this message again, contact your organization's support.

Sync

Check access

Setting

State

State details

Firewall

✖ Error

2016345612(Syncml(500): The recipient encountered an unexpected condition which prevented it from fulfilling the request)



Troubleshooting custom compliance scripts

- Are executed by the Intune Management extensions agent which reports back the result to intune.
- Checking for new or updated PowerShell scripts every **eight hours**.
- Running the discovery scripts every eight hours.
- Running scripts when a user selects Check Compliance on the device. However, there is no check for new or updated scripts when Check Compliance is run. As running the script is done by the IME channel.

It is not possible to push notifications to a device to enable custom compliance to run on demand.



Policies needing extra attention!

- Credential guard, Bitlocker .. – Intune sets the Configured value
- Need to make sure it is running
 - Defender for Endpoint
 - Remediation

Kernel DMA Protection

Virtualisation-based security

Virtualisation-based security required security properties

Virtualisation-based security available security properties

Virtualisation-based security services configured

Virtualisation-based security services running

Windows Defender Application Control policy

On

Running

Base Virtualisation Support, Secure Boot

Base Virtualisation Support, Secure Boot, DMA Protection, Secure Memory Overwrite, UEFI Code Readonly

Credential Guard, Hypervisor enforced Code Integrity, Secure Launch

Hypervisor enforced Code Integrity, Secure Launch

Enforced

<https://ccmexec.com/2024/03/intune-custom-compliance-check-that-credential-guard-is-running/>

Edge Policies





Microsoft Edge policies

- Microsoft Edge management service
- Enrollment token or user targeting
- Default: MDM/GPO Windows over Edge Policies
 - EdgeManagementPolicyOverridesPlatformPolicy - CSP
- Multiple policies = highest priority wins
- Edge://Policies

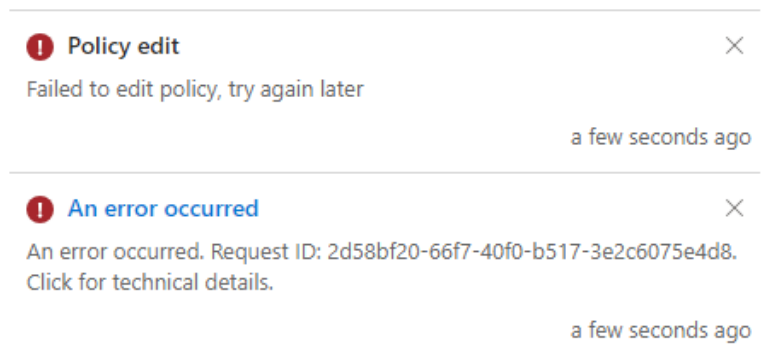
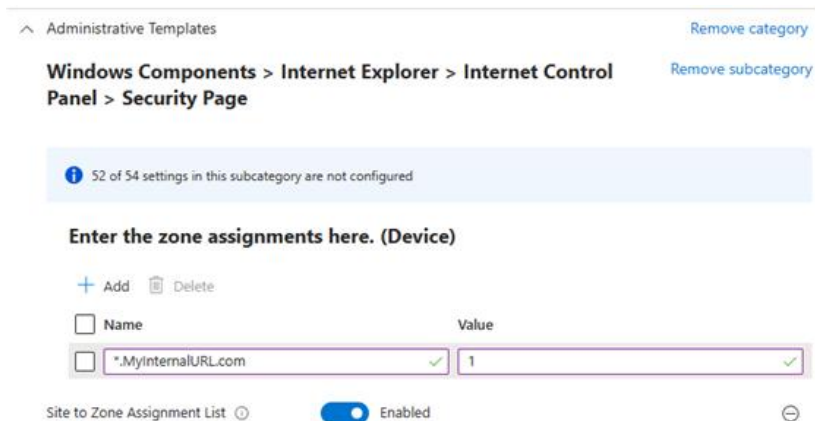
📌 Note

Any policies you apply with Microsoft Edge management service will be overridden if they conflict with an existing Group Policy Object (GPO) or Mobile Device Management (MDM) policy that's set on the device.



Windows Security Zones

- Security Zones
 - Local Machine
 - Local Intranet
 - Trusted
 - Internet
 - Restricted Sites.
- Someone at Microsoft "forgot" to document that this policy is limited to 200 entries



Windows Update





Quality update errors

- We have seen an increase in Quality updates errors during this spring.

Windows Update



Updates failed

Your device is missing important security updates. Make sure to keep your device on and plugged in so updates can complete.

Retry all

2025-08 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5063878) (26100.4946)

Some update files are missing or have problems. We'll try to download the update again later. Error code: (0x80073712)

Retry



Reinstall your current version of Windows to repair system files and components

Reinstall Now

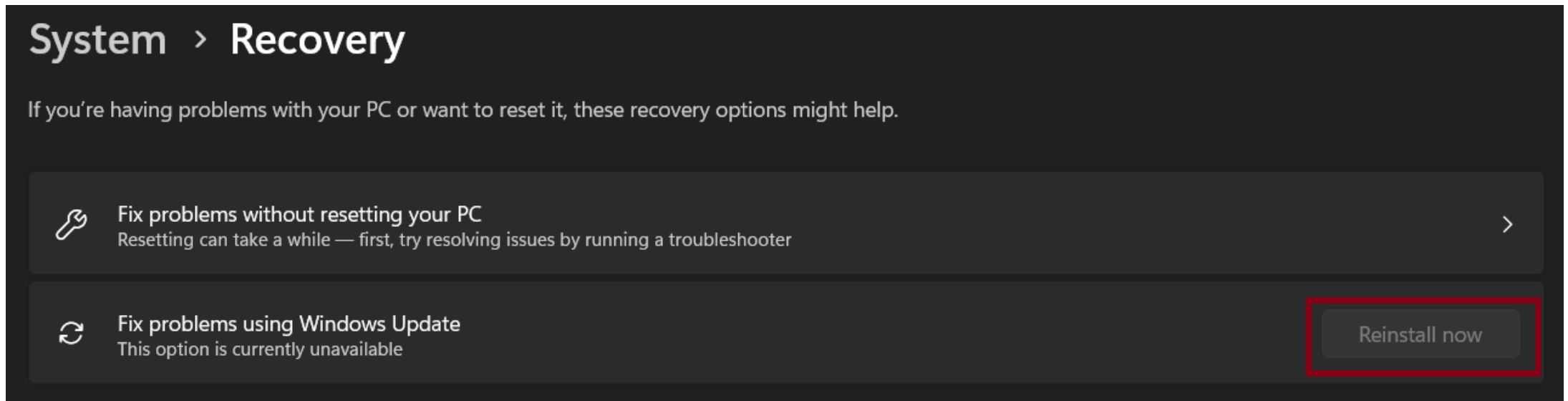




Quality updates

- Solution: in-place upgrade to the same version of Windows 11!

1. Win32app with the Windows 11 installation files
2. setup.exe /auto upgrade /eula accept



[Fix issues by reinstalling the current version of Windows - Microsoft Support](#)



Application control for business – unsigned DLL's

- Managed installer in Intune marks every file installed by the IME as trusted.

“Fsutil file querya remoteHelp.exe”

```
C:\Program Files\Remote Help>fsutil file queryea RemoteHelp.exe
```

```
Extended Attributes (EA) information for file C:\Program Files\Remote Help\RemoteHelp.exe:
```

```
Total Ea Size: 0x2db
```

```
Ea Buffer Offset: 0
```

```
Ea Name: $KERNEL.SMARTLOCKER.ORIGINCLAIM
```

```
Ea Value Length: 12c
```

```
0000: 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 .....
0010: b3 a9 3e 01 e5 be b8 82 c6 09 12 45 b2 6b b5 2b ..>.....E.k.+
0020: 3f 7b 63 e1 11 f0 d6 f8 4b b9 ed 0d 70 71 40 dc ?{c.....K...pq@.
0030: 00 00 00 00 00 00 00 00 ea 00 00 00 5c 00 3f 00 .....\.?.
0040: 3f 00 5c 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 ?.\.C.:.\.P.r.o.
0050: 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 g.r.a.m. .F.i.l.
0060: 65 00 73 00 20 00 28 00 78 00 38 00 36 00 29 00 e.s. .(x.8.6.).
0070: 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 \.M.i.c.r.o.s.o.
0080: 66 00 74 00 20 00 49 00 6e 00 74 00 75 00 6e 00 f.t. .I.n.t.u.n.
0090: 65 00 20 00 4d 00 61 00 6e 00 61 00 67 00 65 00 e. .M.a.n.a.g.e.
00a0: 6d 00 65 00 6e 00 74 00 20 00 45 00 78 00 74 00 m.e.n.t. .E.x.t.
00b0: 65 00 6e 00 73 00 69 00 6f 00 6e 00 5c 00 4d 00 e.n.s.i.o.n.\.M.
00c0: 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 i.c.r.o.s.o.f.t.
00d0: 2e 00 4d 00 61 00 6e 00 61 00 67 00 65 00 6d 00 ..M.a.n.a.g.e.m.
00e0: 65 00 6e 00 74 00 2e 00 53 00 65 00 72 00 76 00 e.n.t...S.e.r.v.
00f0: 69 00 63 00 65 00 73 00 2e 00 49 00 6e 00 74 00 i.c.e.s...I.n.t.
0100: 75 00 6e 00 65 00 57 00 69 00 6e 00 64 00 6f 00 u.n.e.W.i.n.d.o.
0110: 77 00 73 00 41 00 67 00 65 00 6e 00 74 00 2e 00 w.s.A.g.e.n.t...
0120: 65 00 78 00 65 00 00 00 00 00 00 00 00 00 e.x.e.....
```



Error	2025-09-27 19:43:43	MsiInstaller	11723	None
Information	2025-09-27 19:43:39	Security-SPP	16384	None

Event 11723, MsiInstaller

General Details

Product: Microsoft EPM Agent -- Error 1723. There is a problem with this Windows Installer package. A DLL required for this install to complete could not be run. Contact your support personnel or package vendor. Action SchedXmlFile, entry: SchedXmlFile, library: C:\Windows\Installer\MSI773B.tmp

Log Name:	Application	Logged:	2025-09-27 19:43:43
Source:	MsiInstaller	Task Category:	None
Event ID:	11723	Keywords:	Classic
Level:	Error	Computer:	PAW-819B3DQ2
User:	SYSTEM		
OpCode:	Info		

Autopilot





Policies that causes a reboot during Autopilot

Most common issue: Security Baselines (Device target)

Solution: Target them to users

- Device Lock
- DMA Guard
- Credential Guard
- VBS
- Lock Screen

Configuration settings [Edit](#)

✓ Administrative Templates

✓ Device Guard

✓ Device Lock

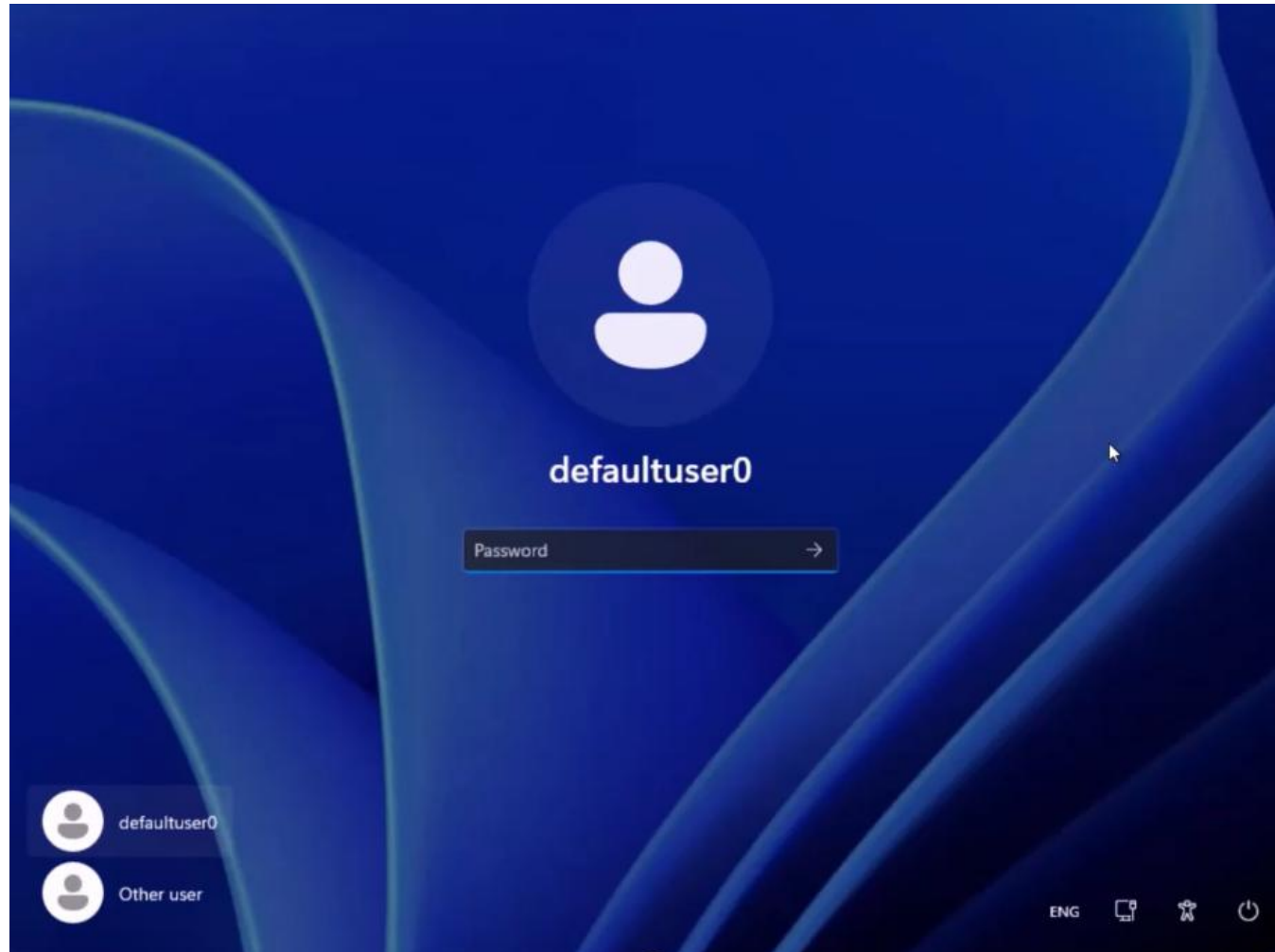
✓ Dma Guard

✓ Virtualization Based Technology



Breaking Autopilot







- MSS: (AutoAdminLogon) Enable Automatic Logon





Event ID 2800

- Always logged when a policy is applied that breaks the Autopilot experience both for user and device!

Admin Number of events: 1 239				
Filtered: Log: Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin; Source: ; Event ID: 2800. Number of events: 6				
Level	Date and Time	Source	Event ID	Task Category
 Information	2025-05-21 09:47:15	DeviceManagemen...	2800	None
 Information	2025-05-21 09:47:15	DeviceManagemen...	2800	None
 Information	2025-05-21 09:47:15	DeviceManagemen...	2800	None
 Information	2025-05-21 09:47:15	DeviceManagemen...	2800	None
 Information	2025-05-21 09:47:15	DeviceManagemen...	2800	None
 Information	2025-05-21 09:04:52	DeviceManagemen...	2800	None



Reboot without generating eventid 2800

These will cause a reboot without trigger 2800 event ID

- Interactive logon:
 - Message title for users attempting to log on
 - Message text for users attempting to log on
 - Require Windows Hello for Business or smart card
 - Solution: Disable first sign-in animation or assign policy to users
- User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode - Prompt for credentials on the secure desktop
- Preferred Aad Tenant Domain Name
- Block Non Admin User Install



Network





SSL traffic inspection = BAD

- Must exclude necessary endpoints
- Example on results

ⓘ Note

SSL traffic inspection is not supported for 'manage.microsoft.com', 'dm.microsoft.com', or the [Device Health Attestation \(DHA\) endpoints listed in the compliance section](#).

Device name	Managed by ↓	Ownership	Compliance	OS ∨	OS version ∨
5f256f7b-9e37-4824-b5...	Co-managed	Unknown	See ConfigMgr	Windows	0.0.0.0
7ededf06-8c41-4d91-90...	Co-managed	Unknown	See ConfigMgr	Windows	0.0.0.0



Intune Network Requirements

- By Martin Hinken (more comprehensive than MS..)
- Test network connectivity required by Intune, Autopilot, Device registration, TPM and more..
- Comprehensive tests

Intune Network test results													
Filter													
+ Add criteria ▼													
id	url	Port	Protocol	required	DNSResult	TCPResult	HTTPStatusCode	SSLTest	SSLProtocol	Issuer	AuthException	KnownCRL	SSLInterception
56	account.activedirectory.windowsazure.com	80	TCP	True	True	True	200	False					
56	account.activedirectory.windowsazure.com	443	TCP	True	True	True	200	True	Tls13	CN...		True	False
56	accounts.accesscontrol.windows.net	80	TCP	True	True	True	200	False					
56	accounts.accesscontrol.windows.net	443	TCP	True	True	True	200	True	Tls13	CN...		True	False
56	adminwebservice.microsoftonline.com	80	TCP	True	True	True	404	False					
56	adminwebservice.microsoftonline.com	443	TCP	True	True	True	404	True	Tls13	CN...		True	False
56	api.passwordreset.microsoftonline.com	80	TCP	True	True	True	200	False					
56	api.passwordreset.microsoftonline.com	443	TCP	True	True	True	200	True	Tls13	CN...		True	False
56	autologon.microsoftazuread-sso.com	80	TCP	True	True	True	404	False					
56	autologon.microsoftazuread-sso.com	443	TCP	True	True	True	404	True	Tls13	CN...		True	False
56	becws.microsoftonline.com	80	TCP	True	True	True	403	False					
56	becws.microsoftonline.com	443	TCP	True	True	True	403	True	Tls13	CN...		True	False

Applications





IME Log files

- C:\ProgramData\Microsoft\IntuneManagementExtension\Logs
 - AgentExecution.log – Log file for PowerShell detection methods
 - ClientHealth.log – Log file for IME health and remediation actions
 - DeviceHealthMonitoring – Log file for Appcrash, app events
 - HealthScripts – Log file for remediation scripts
 - IntuneManagementExtension.log – IME related events, sync
 - AppWorkload.log – App related events
 - Sensor.log – Log file for subscribed events.
 - AppActionProcessor.log – Log file for AppActions
 - Win32AppInventory.log – Log file for inventory
 - ClientCertCheck.log - Tracks device client certificate checks

Content Cache location:

- Win32Apps - C:\Program Files (x86)\Microsoft Intune Management Extension\Content\Incoming\
- Remediation scripts - C:\Windows\IMECache\HealthScripts



Global Reevaluation Schedule (GRS)

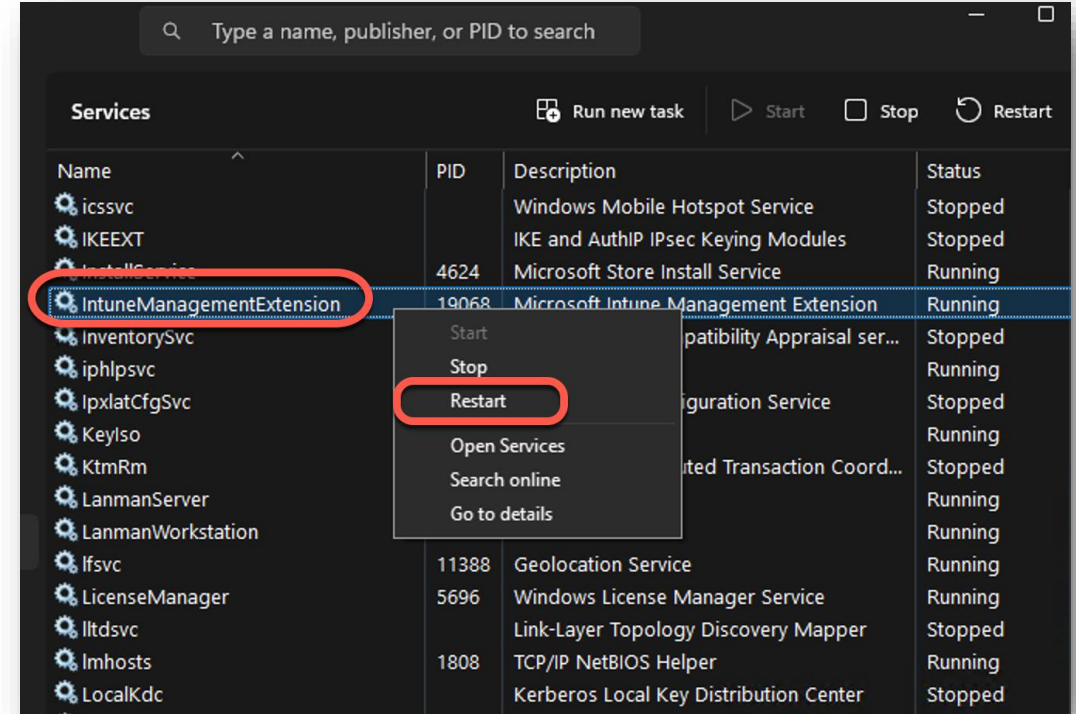
- **Initial Installation Attempt:**
 - Intune deploys a Win32 app and the IME-agent executes the installation command.
- **Failure:**
 - If the app fails to install, the IME will retry it up to **3** times.
- **GRS Activation:**
 - If all 3 attempts fail, the app is placed in the **Global Reevaluation Schedule (GRS)**.
- **24-Hour Wait:**
 - The GRS prevent the IME from endlessly retrying a known-to-fail app.
 - It will wait for 24 hours from the last failed attempt before considering a retry.
- **Scheduled Reevaluation:**
 - The system checks for GRS expiration to determine when to attempt the installation again. After the 24-hours.
- **Repeat:**
 - The process then repeats, with another set of 3 installation attempts.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\Win32Apps



IME Sync

- IME Sync
 - Checks with Intune services every 8 hours.
 - This check-in process is independent of the MDM check-in.
- Manually initiate an IME check-in
 - **Company Portal > Settings > Sync.**
 - Initiates an **MDM** check-in and **IME** check-in.
- Alternative
 - Restart the service **IntuneManagementExtension**
 - The restart will initiate a check-in with Intune



Note: The **Sync** actions from either the **Settings** app or **Devices** in Microsoft Intune admin center initiate an MDM check-in but don't force an IME check-in.



Registry

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension

	Name	Type	Data
> SideCarPolicies			
> Win32Apps			
> 00000000-0000-0000-0000-000000000000			
> 404b632d-14c5-45d4-b8c8-ff3fff8dc561			
> 2043db9d-f484-4b49-9709-fd79f0555a78_1			
> 2043db9d-f484-4b49-9709-fd79f0555a78_2			
> 238ec4cc-5901-4fa9-9edc-bfd70945d743_1			
> 2752d899-9171-4243-9483-16fcb2280dc9_1			
> 50d65d25-45b4-44e7-898e-cf992e19083b_1			
	(Default)	REG_SZ	(value not set)

https://intune.microsoft.com/#view/Microsoft_Intune_Apps/SettingsMenu/~/?appld/2043db9d-f484-4b49-9709-fd79f0555a78

Intune admin center

<< Home > Apps | Windows > Windows | Windows apps > Remote Help

Remote Help | Properties

Client Apps

Search <<

Overview

Manage

Properties

Monitor

- Device install status
- User install status
- Dependency viewer
- Supersedence viewer

App information Edit

Name	Remote Help
Description	RemoteHelpInstaller.exe
Publisher	Microsoft
App Version	3.8.0.6
Category	--
Show this as a featured app in the Company Portal	No
Information URL	--



Reinstall required app using Powershell/remediation

- Remediations on demand is the best!
- Powershell script that
 - Uninstall application if installed
 - Clears out registry values
 - restarts IME

```
1  #Define variables
2  $AppID = "f3f8ea42-2a57-42e5-999e-399d01337e9b"
3  $MSIProductCode = "{1E06C136-5B6F-4A98-8296-CEFE858DEEE6}"
4
5  try {
6      #Uninstall application
7      Start-Process "C:\Windows\System32\msiexec.exe" -ArgumentList "/x $MSIProductCode /quiet /noreboot" -Wait
8  }
9  catch {
10     $ErrorMessage = $_.Exception.Message
11     Write-Host $ErrorMessage
12     exit 1
13 }
14
15 #Clear IME registry values
16 $Regpath = "HKLM:\SOFTWARE\Microsoft\IntuneManagementExtension\Win32Apps"
17 Get-ChildItem -Path $Regpath -Recurse -Exclude "**AppAuthority*" | Where-Object { $_.PSChildName -like "$AppID*" -or $_.Property -like "$AppID*" } | Remove-Item -Recurse -Force
18
19 #Restart IME service
20 Restart-Service -Name "IntuneManagementExtension" -Force
21
22 #Exit script
23 Exit 0
24
```



Thank You

