

# Workplace Ninja France

Unlocking the secrets of Intune troubleshooting  
A deep dive into mastery



# About me...



## Ronni Pedersen

- Cloud Architect, APENTO
- Microsoft MVP: Enterprise Mobility
- MCSE/MCSA/MCITP/MCTS and more... 😊
- ITIL Foundation Certified
- Microsoft Certified Trainer (MCT)

## Contact Info

- Mail: [rop@apento.com](mailto:rop@apento.com)
- Twitter: [@ronnipedersen](https://twitter.com/ronnipedersen)



# About me...



## Jörgen Nilsson

- Principal Consultant, Onevinn
- Microsoft MVP: Enterprise Mobility
- MCSE/MCSA/MCITP/MCTS
- ITIL Foundation Certified
- Microsoft Certified Trainer (MCT)

## Contact Info

- Mail: [Jorgen.nilsson@onevinn.se](mailto:Jorgen.nilsson@onevinn.se)
- Twitter: [@ccmexec](https://twitter.com/ccmexec)



# Agenda

- Remote Control / Remote Help
- Tools and Log Files
- Troubleshooting Configuration Policies
- Troubleshooting Subscription based activation
- Troubleshooting Enrollment
- WUfB and Safeguard Holds
- Intune Management extension
- Troubleshooting Policy Processing



# Remote Control

- TeamViewer integrates in the Endpoint Management Portal
- Quick Assist is built-in
  - Lacks UAC support
  - No Logging
  - Maybe OK for smaller organizations
  - During AutoPilot (Alt+Win+Q) (If updated OS is installed)
  - Quick Assist requires an update from the Store since last spring.
    - PowerShell -ex bypass
    - Install-Script -Name Invoke-QuickAssist
    - Invoke-QuickAssist.ps1

[How to Remote Assist Autopilot Deployments with Quick Assist - Microsoft Community Hub](#)

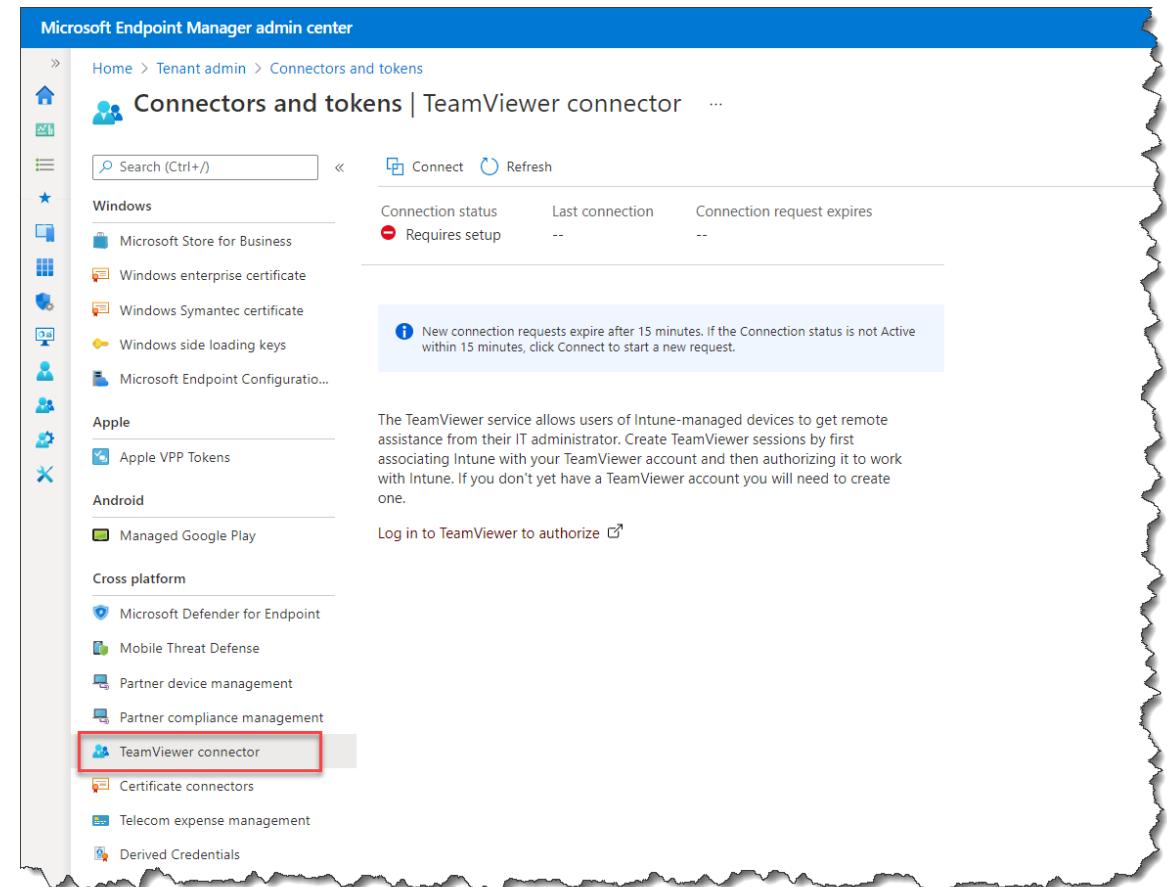
<https://oliverkieselbach.com/2020/03/03/quick-assist-the-built-in-remote-control-in-windows-10/>



# Configure the TeamViewer Connector

- Easy setup and configuration
- There are other options:
  - Beyond Trust
  - LogMeIn
  - Remote Help!

... And many more but **only** TeamViewer integrates in the admin console (for now)



# Microsoft Remote Help

- Adv management pack add-on
- Auditing in the MEM portal

The screenshot shows the Microsoft Endpoint Manager (MEM) portal interface. At the top, there is a navigation bar with 'Monitor' (underlined), 'Settings', and 'Remote help sessions'. Below the navigation bar, there is a 'Refresh' button and a section titled 'Current active sessions' which displays the number '2'. A chart titled 'Average session time' shows a value of '0 minutes' for the date 'Jan 18'. Another chart titled 'Total sessions' shows a value of '2 sessions' for the date 'Jan 18'. Above the charts, two windows are displayed: one titled 'Remote help' asking for a security code to be shared, and another window titled 'Remote help' showing the 'CCMEXEC' logo.

# Remote Troubleshooting

- Customer quote:

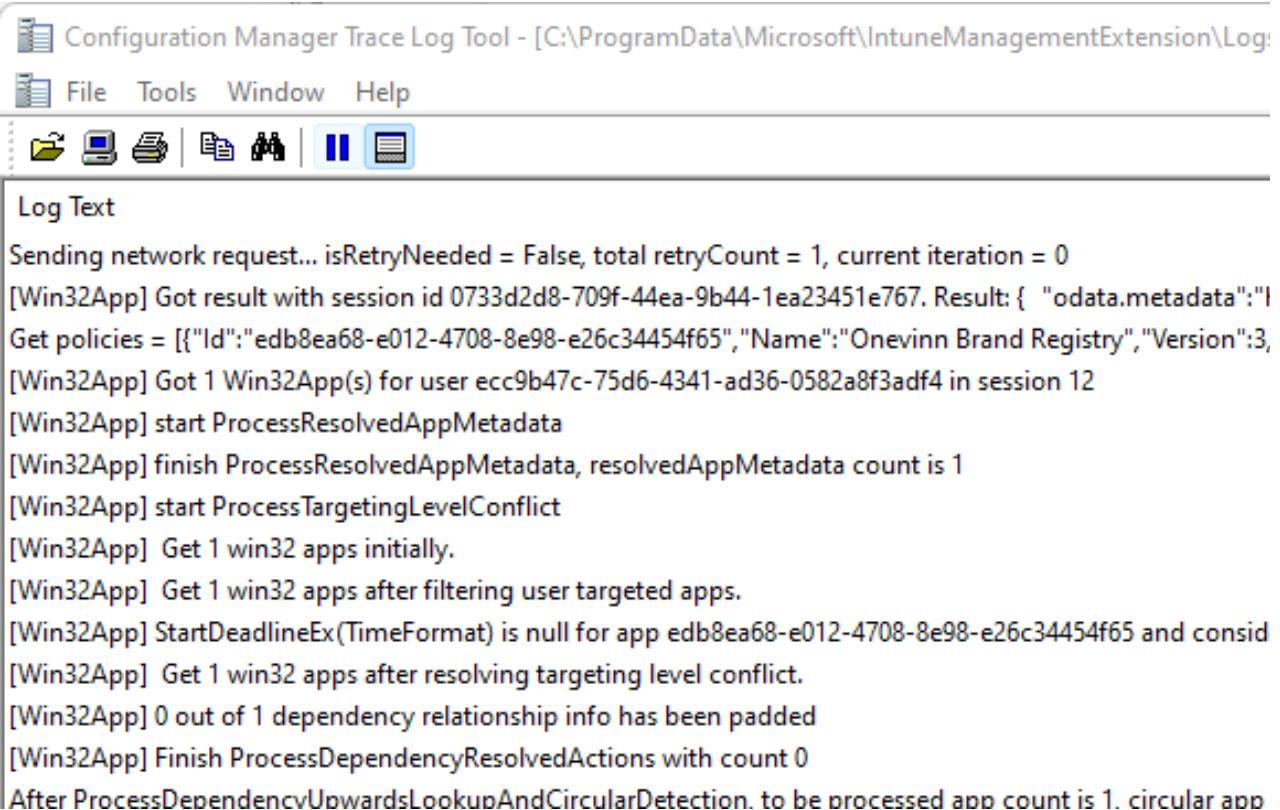
*“I haven’t spoken to an end-user in the last three years and I am not about to start now!”*

- ~~Challenge: Windows Firewall – Private/Public is the only options on a AAD joined device~~
- ~~Need to script the switch to Private profile~~
- ~~Local admin can always switch!~~
- LAPS is your friend!



# Log-reader = CMtrace

- Great log reader
- Not free but included in the Intune/MEM license
- Deploy it to all clients



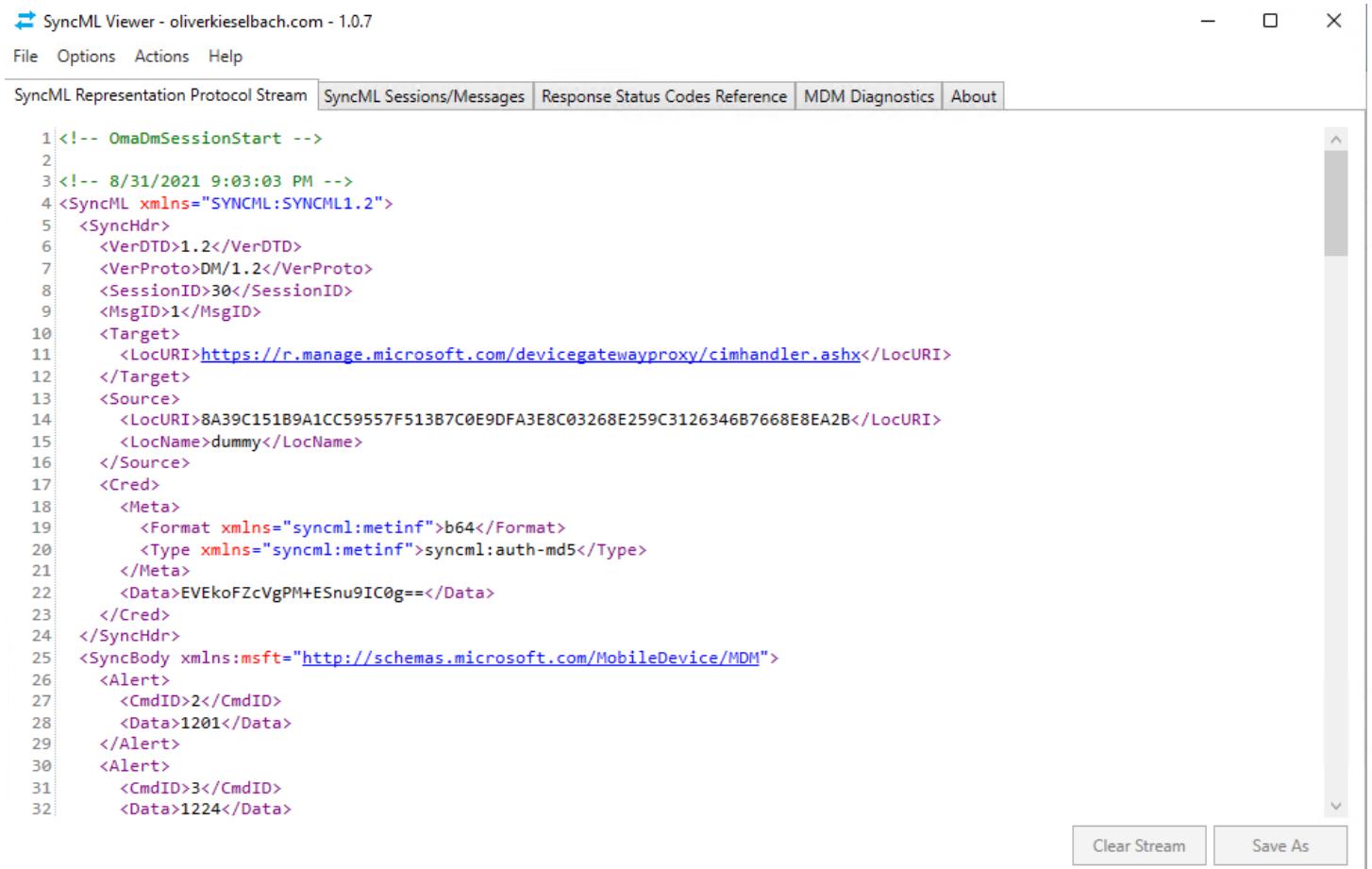
The screenshot shows the 'Configuration Manager Trace Log Tool' window. The title bar reads 'Configuration Manager Trace Log Tool - [C:\ProgramData\Microsoft\IntuneManagementExtension\Log]'. The menu bar includes 'File', 'Tools', 'Window', and 'Help'. Below the menu is a toolbar with icons for file operations. The main area is titled 'Log Text' and contains the following log entries:

```
Sending network request... isRetryNeeded = False, total retryCount = 1, current iteration = 0
[Win32App] Got result with session id 0733d2d8-709f-44ea-9b44-1ea23451e767. Result: { "odata.metadata":"
Get policies = [{"Id":"edb8ea68-e012-4708-8e98-e26c34454f65","Name":"Onevinn Brand Registry","Version":3,
[Win32App] Got 1 Win32App(s) for user ecc9b47c-75d6-4341-ad36-0582a8f3adf4 in session 12
[Win32App] start ProcessResolvedAppMetadata
[Win32App] finish ProcessResolvedAppMetadata, resolvedAppMetadata count is 1
[Win32App] start ProcessTargetingLevelConflict
[Win32App] Get 1 win32 apps initially.
[Win32App] Get 1 win32 apps after filtering user targeted apps.
[Win32App] StartDeadlineEx(TimeFormat) is null for app edb8ea68-e012-4708-8e98-e26c34454f65 and consid
[Win32App] Get 1 win32 apps after resolving targeting level conflict.
[Win32App] 0 out of 1 dependency relationship info has been padded
[Win32App] Finish ProcessDependencyResolvedActions with count 0
After ProcessDependencyUowardsLookupAndCircularDetection. to be processed app count is 1. circular app
```

<https://ccmexec.com/2018/12/copy-and-associate-cmtrace-using-intune-win32app-and-powershell/>

# More Tools – Advanced Troubleshooting

- Wireshark
- Fiddler
- Netmon
- **SyncMLViewer**



The screenshot shows the SyncML Viewer application window. The title bar reads "SyncML Viewer - oliverkieselbach.com - 1.0.7". The menu bar includes File, Options, Actions, and Help. Below the menu is a navigation bar with tabs: SyncML Representation Protocol Stream (selected), SyncML Sessions/Messages, Response Status Codes Reference, MDM Diagnostics, and About. The main content area displays a multi-line XML document representing a SyncML session. The XML code is as follows:

```
1<!-- OmaDmSessionStart -->
2
3<!-- 8/31/2021 9:03:03 PM -->
4<SyncML xmlns="SYNCML:SYNCML1.2">
5  <Synchdr>
6    <VerDTD>1.2</VerDTD>
7    <VerProto>DM/1.2</VerProto>
8    <SessionID>30</SessionID>
9    <MsgID>1</MsgID>
10   <Target>
11     <LocURI>https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx</LocURI>
12   </Target>
13   <Source>
14     <LocURI>8A39C151B9A1CC59557F513B7C0E9DFA3E8C03268E259C3126346B7668E8EA2B</LocURI>
15     <LocName>dummy</LocName>
16   </Source>
17   <Cred>
18     <Meta>
19       <Format xmlns="syncml:metinf">b64</Format>
20       <Type xmlns="syncml:metinf">syncml:auth-md5</Type>
21     </Meta>
22     <Data>EV EkoFZcVgPM+ESnu9IC0g==</Data>
23   </Cred>
24 </Synchdr>
25 <SyncBody xmlns:msft="http://schemas.microsoft.com/MobileDevice/MDM">
26   <Alert>
27     <CmdID>2</CmdID>
28     <Data>1201</Data>
29   </Alert>
30   <Alert>
31     <CmdID>3</CmdID>
32     <Data>1224</Data>

```

At the bottom right of the application window are two buttons: "Clear Stream" and "Save As".

<https://github.com/okieselbach/SyncMLViewer/tree/master/SyncMLViewer/dist>

# SyncMLViewer

```
1533      <----->
1534      <Status>
1535          <CmdID>32</CmdID>
1536          <MsgRef>2</MsgRef>
1537          <CmdRef>25</CmdRef>
1538          <Cmd>Get</Cmd>
1539          <Data>200</Data>
1540      </Status>
1541      <Results>
1542          <CmdID>33</CmdID>
1543          <MsgRef>2</MsgRef>
1544          <CmdRef>25</CmdRef>
1545          <Item>
1546              <Source>
1547                  <LocURI>./DevDetail/Ext/DeviceHardwareData</LocURI>
1548                  <Data>T0EeBAEAHAAAAoAMwDwVQAACgAaAfBVCnofKQQCCQgCABAACQABAAEAAgABAAAABQAZAAQAAAAAAAAAAgAAAAAAAAACAAEAAwMAEQBHZW51aW51SW50ZWwABAA0AEEludGVsKFIpIENvcmUoVE0pIGk3LTg1NTlV:
1549              </Item>
1550          </Results>
1551      <Status>
1552          <CmdID>34</CmdID>
1553          <MsgRef>2</MsgRef>
1554          <CmdRef>26</CmdRef>
```

```
<SyncML xmlns="SYNCML:SYNCML1.2" xmlns:A="syncml:metinf">
  <SyncHdr>
    <VerDTD>1.2</VerDTD>
    <VerProto>DM/1.2</VerProto>
    <SessionID>120</SessionID>
    <MsgID>6</MsgID>
    <Target>
      <LocURI>8A39C151B9A1CC59557F513B7C0E9DFA3E8C03268E259C3126346B7668E8EA2B</LocURI>
    </Target>
    <Source>
      <LocURI>https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx</LocURI>
    </Source>
    <Meta>
      <A:MaxMsgSize>524288</A:MaxMsgSize>
    </Meta>
  </SyncHdr>
  <SyncBody>
    <Status>
      <CmdID>1</CmdID>
      <MsgRef>6</MsgRef>
      <CmdRef>0</CmdRef>
      <Cmd>SyncHdr</Cmd>
      <Data>200</Data>
    </Status>
    <Replace>
      <CmdID>2</CmdID>
      <Item>
        <Target>
          <LocURI>./Vendor/MSFT/NodeCache/MS%20DM%20Server/Nodes/4929/NodeUri</LocURI>
        </Target>
        <Data>./cimv2/MDM_WebApplication/MDM_WebApplication.PackageName=CCMEXEC%20-%20Not%20Managed/PackageUrl</Data>
      </Item>
    </Replace>
    <Replace>
      <CmdID>3</CmdID>
      <Item>
        <Target>
          <LocURI>./Vendor/MSFT/NodeCache/MS%20DM%20Server/Nodes/4929/ExpectedValue</LocURI>
        </Target>
        <Data>https://ccmexec.com/</Data>
      </Item>
    </Replace>
  </SyncBody>
</SyncML>
```

# LOG FILES

# Collect diagnostics from a Windows Device

- Collecting Diagnostic Logs from Windows Devices
  - Windows 10 1909 and later
  - Windows 11
  - HoloLens 2 2004 and later
  - Both Intune and Co-Managed devices
  - Corporate-owned devices
  - Stored for 28 days and then deleted (up to 10 collections)
  - Bulk action (up to 25 devices)
- Upload URL:
  - lgmsapewe.u.blob.core.windows.net
- More information:
  - <https://docs.microsoft.com/en-us/mem/intune/remote-actions/collect-diagnostics>



# Device Diagnostics

- Autopilot enrollment failure

Refresh

Requested by	Status	Request initiated ↑↓	Diagnostics uploaded ↑↓	Diagnostics
rop@apento.com	Pending diagnostics upload	11/15/2022, 1:17:51 PM		
Autopilot enrollment	Complete	11/11/2022, 7:44:36 AM	11/11/2022, 7:52:06 AM	<a href="#">Download</a>
Autopilot enrollment	Failed	11/10/2022, 7:37:16 AM		

# Collecting Diagnostic Logs

The screenshot shows the Microsoft Intune Device diagnostics (preview) interface. The main window displays device information and a history of actions taken on the device.

**Device Information:**

- Device name: DESKTOP-NIIRT6B
- Management name: rop\_Windows\_6/18/2020\_4:01 PM
- Ownership: Corporate
- Serial number: [REDACTED]
- Phone number: ---
- Primary user: Ronni Pedersen
- Enrolled by: Ronni Pedersen
- Compliance: Compliant
- Operating system: Windows
- Device model: NUC8i7H NK

**Device actions status:**

Action	Status	Date/Time	Error
Collect diagnostics	Complete	5/16/2021, 8:18:21 AM	

**Navigation:**

- Home > Windows > DESKTOP-NIIRT6B
- Manage: Properties, Monitor, Hardware, Discovered apps, Device compliance, Device configuration, App configuration, Endpoint security configuration, Recovery keys, User experience, Device diagnostics (preview) (highlighted with red box), Managed Apps.

**Device diagnostics (preview) details:**

Requested by: rop@apento.com | Status: Complete | Request initiated: 5/16/2021, 8:18:07 AM | Diagnostics uploaded: 5/16/2021, 8:28:57 AM | Diagnostics: Download



# CONFIGURATION POLICY PROCESS

# Microsoft 365 Apps Policy

- Microsoft Intune Configuration:
  - Policy 1: Enable Microsoft 365 Apps Automatic Updates
  - Policy 2: Set the Update Channel
- Client-Side debugging:
  - #1 Check the Intune registry keys
  - #2 Check the Office registry keys
  - #3 Force Office automatic updates to run
  - #4 Force the Office synchronization to update account information



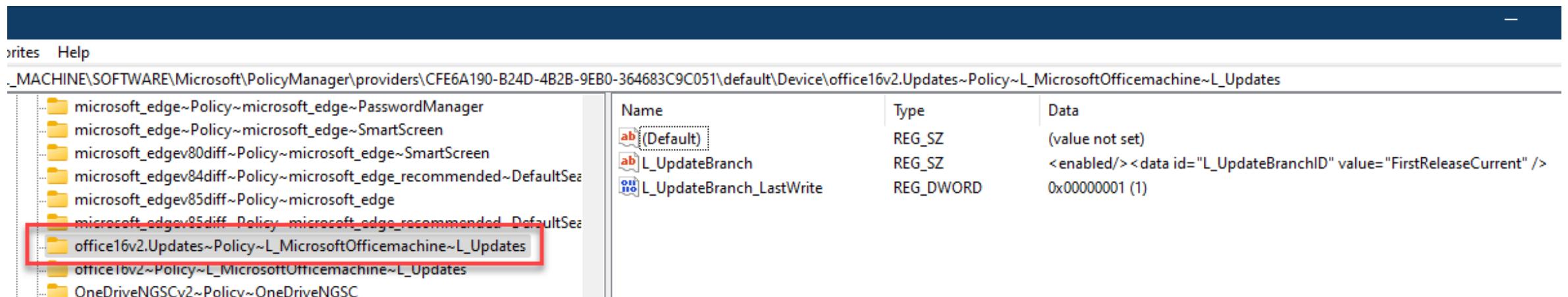
# Use Settings Catalog

- Policy Configuration:
  - Enable Microsoft 365 Apps Automatic Updates
  - Set the Update Channel

The screenshot shows the 'Configuration settings' tab of the Settings Catalog. At the top, there are two tabs: 'Configuration settings' (selected) and 'Review + save'. Below the tabs, there's a '+ Add settings' button. Under the 'Microsoft Office 2016 (Machine)' category, there's a 'Updates' subcategory. A message indicates '14 of 16 settings in this subcategory are not configured'. Two settings are listed: 'Enable Automatic Updates' (Enabled) and 'Update Channel' (Enabled). The 'Update Channel' setting has a dropdown menu set to 'Current Channel (Preview)'. There are also 'Remove category' and 'Remove subcategory' buttons.

# #1 Check the Intune registry keys

- Open the Registry Editor, and go to the Intune policy path:  
**HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\<Provider ID>\default\Device\office16~Policy~L\_MicrosoftOfficemachine~L\_Updates**
- When the policy is applied, you see the following registry keys:  
**L\_UpdateBranch**
- At this point, the Intune policy is **successfully applied** to the device.

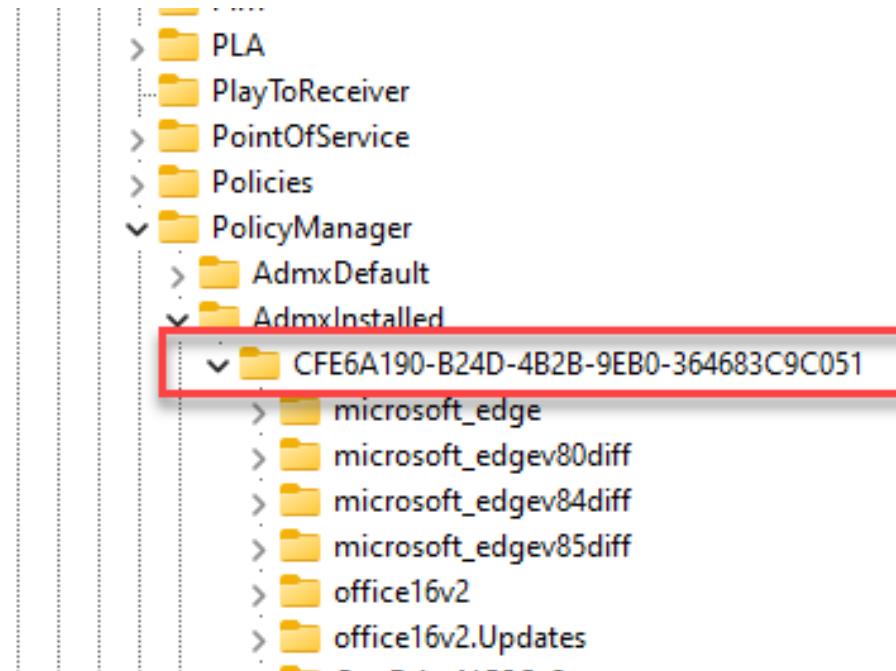


# Find the Provider ID

Find the provider ID for your device

- Open the Registry Editor, and go to:

**Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\PolicyManager\AdmxInstalled**



# #2 Check the Office registry keys

- Go to the Office policy path:

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\Configuration

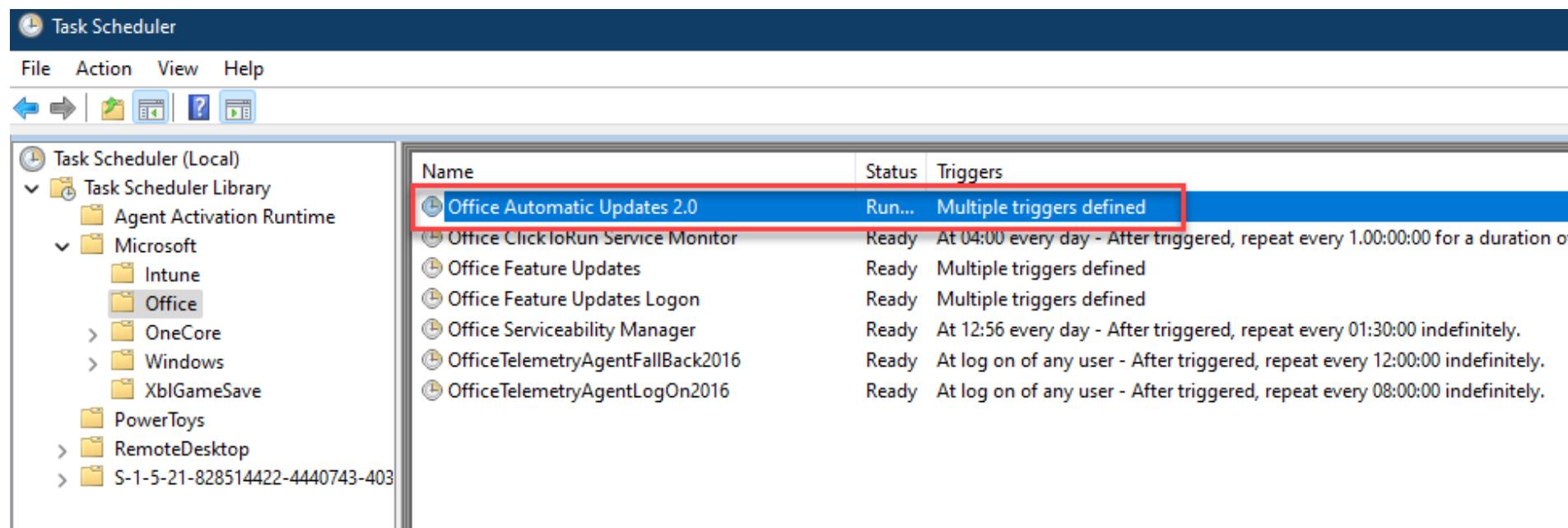
- Check the **UpdateChannel** value:

- Monthly Enterprise Channel = 55336b82-a18d-4dd6-b5f6-9e5095c314a6
- Current Channel = 492350f6-3a01-4f97-b9c0-c7c6ddf67d60
- **Current Channel (Preview) = 64256afe-f5d9-4f86-8936-8840a6a4f5be**
- Semi-Annual Enterprise Channel = 7ffbc6bf-bc32-4f92-8982-f9dd17fd3114
- Semi-Annual Enterprise Channel (Preview) = b8f9b850-328d-4355-9145-c59439a0c4cf
- Beta Channel = 5440fd1f-7ecb-4221-8110-145efaa6372f

ab SCLCacheOverride	REG_SZ	0
ab SharedComputerLicensing	REG_SZ	0
ab StreamingFinished	REG_SZ	True
ab StreamPackageUrlChanged	REG_SZ	True
ab TeamsAddon	REG_SZ	INSTALLED
<b>ab UpdateChannel</b>	<b>REG_SZ</b>	<b><a href="http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-8936-8840a6a4f5be">http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-8936-8840a6a4f5be</a></b>
ab UpdateChannelChanged	REG_SZ	False
ab UpdatesEnabled	REG_SZ	True
ab VersionToReport	REG_SZ	16.0.14527.20268
ab VisioProRetail.ExcludedApps	REG_SZ	groove
ab WindowsUpdate	REG_SZ	CNN

# #3 Force Office automatic updates to run

- To test the policy, we can force the policy settings on the device
  - Go to **HKLM\SOFTWARE\Microsoft\Office\ClickToRun\Updates**
  - Edit the **UpdateDetectionLastRunTime** key > delete the value data.
  - Launch Task Secheduler > Microsoft > Office
    - Run “**Office Automatic Updates 2.0**”



# Task Manager

File Options View

Processes Performance App history Startup Users Details Services



CPU  
23% 3,14 GHz



Memory  
7,7/15,5 GB (50%)



Disk 0 (C:)  
SSD  
3%



Wi-Fi  
Wi-Fi  
S: 0,1 R: 27,3 Mbps

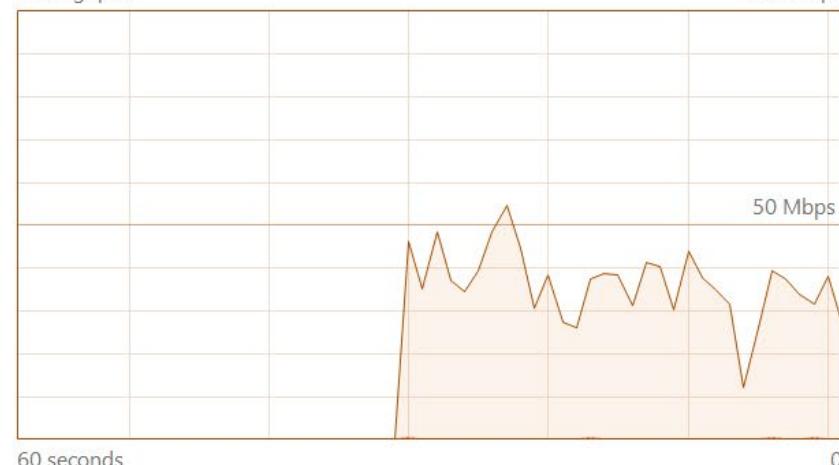


GPU 0  
AMD Radeon(TM) Gra...  
4% (53 °C)

## Wi-Fi

Intel(R) Wi-Fi 6 AX200 160MHz

Throughput



60 seconds

100 Mbps

50 Mbps

Send

**88,0 Kbps**

Receive

**27,3 Mbps**

Adapter name:

Wi-Fi

SSID:

Free WiFi - LUZERN.COM

DNS name:

monzoon.net

Connection type:

802.11n

IPv4 address:

172.19.252.29

IPv6 address:

fe80::d85d:6d25:ceb5:63e3%12

Signal strength:



^ Fewer details | Open Resource Monitor



Downloading Office updates...

You can keep using Office while we download in the background.



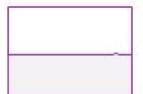
# Task Manager

File Options View

Processes Performance App history Startup Users Details Services



CPU  
31% 3.59 GHz



Memory  
7.3/15.5 GB (47%)



Disk 0 (C:)  
SSD  
4%



Wi-Fi  
Wi-Fi  
S: 0 R: 0 Kbps

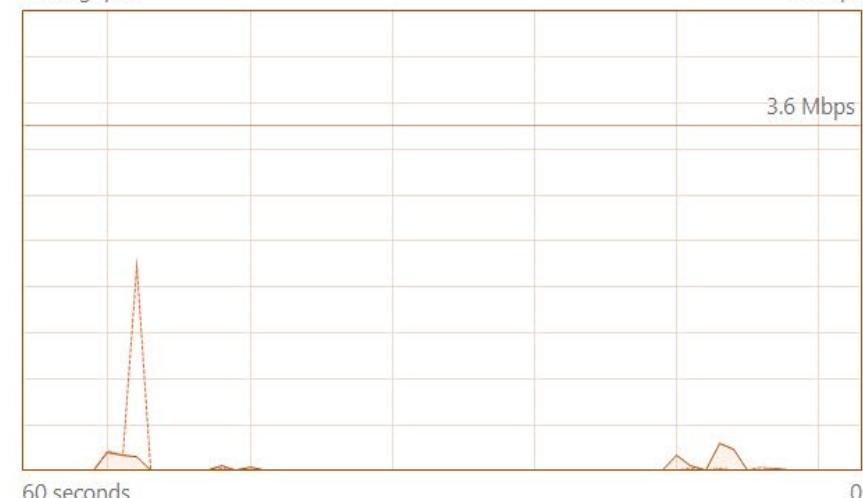


GPU 0  
AMD Radeon(TM) Gra...  
4% (53 °C)

## Wi-Fi

Intel(R) Wi-Fi 6 AX200 160MHz

Throughput



Send  
**0 Kbps**

Receive  
**0 Kbps**

Adapter name: Wi-Fi  
SSID: Free WiFi - LUZERN.COM  
DNS name: monzoon.net  
Connection type: 802.11n  
IPv4 address: 172.19.252.29  
IPv6 address: fe80::d85d:6d25:ceb5:63e3%12  
Signal strength:

^ Fewer details | Open Resource Monitor



## Updates were installed

Your Office updates have been installed. You can use your Office apps now.

**Close**

# Update history for Microsoft 365 Apps

## Update history for Microsoft 365 Apps

- <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date>

### Product Information



#### Subscription Product

Microsoft 365 Apps for enterprise

Belongs to: rop@apento.com

This product contains



[Manage Account](#)

[Change License](#)



#### Office Updates

Updates are automatically downloaded and installed.



#### About Word

Learn more about Word, Support, Product ID, and Copyright information.

[Version 2209 \(Build 15629.20058 Click-to-Run\)](#)

[Current Channel \(Preview\)](#)



#### What's New

See the most recently installed updates.

# TROUBLESHOOTING SUBSCRIPTION BASED ACTIVATION

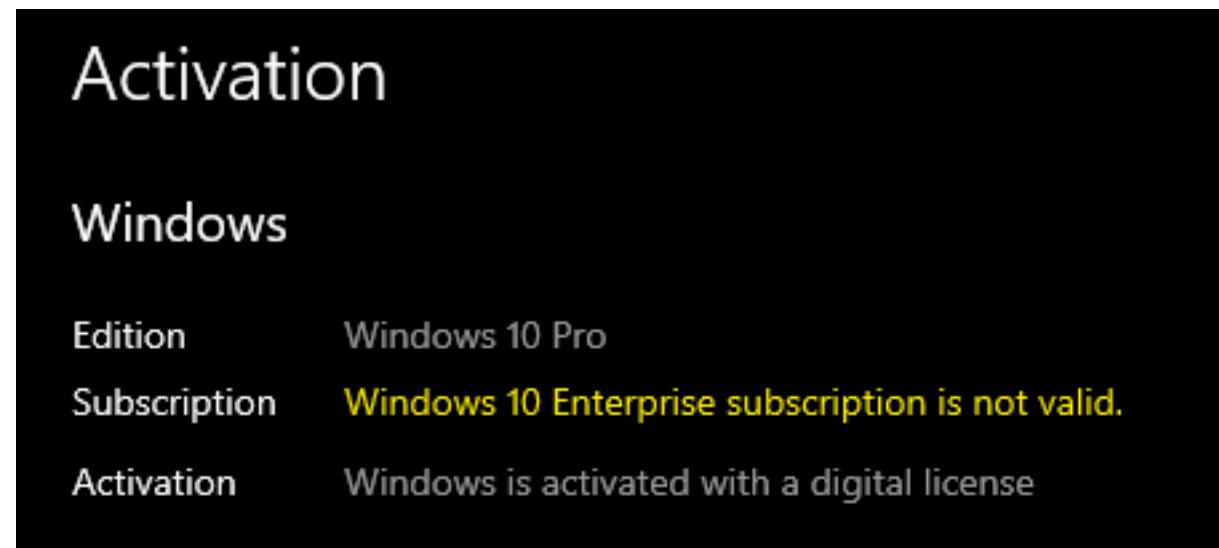
# Subscription Based activation

- Easiest way of upgrading to Enterprise from pro
- Re-activated every 30 days
- Each user can activate 5 devices
- Activating shared devices
  - Either all users must have a Windows e3 license assigned
  - Shared devices must be excluded and activated in a different way (KMS,MAK)

**HKEY\_Local\_Machine\System\Currentcontrolset\services\clipsvc\parameters**  
**Value: DisableSubscription Reg\_Dword Value=1**

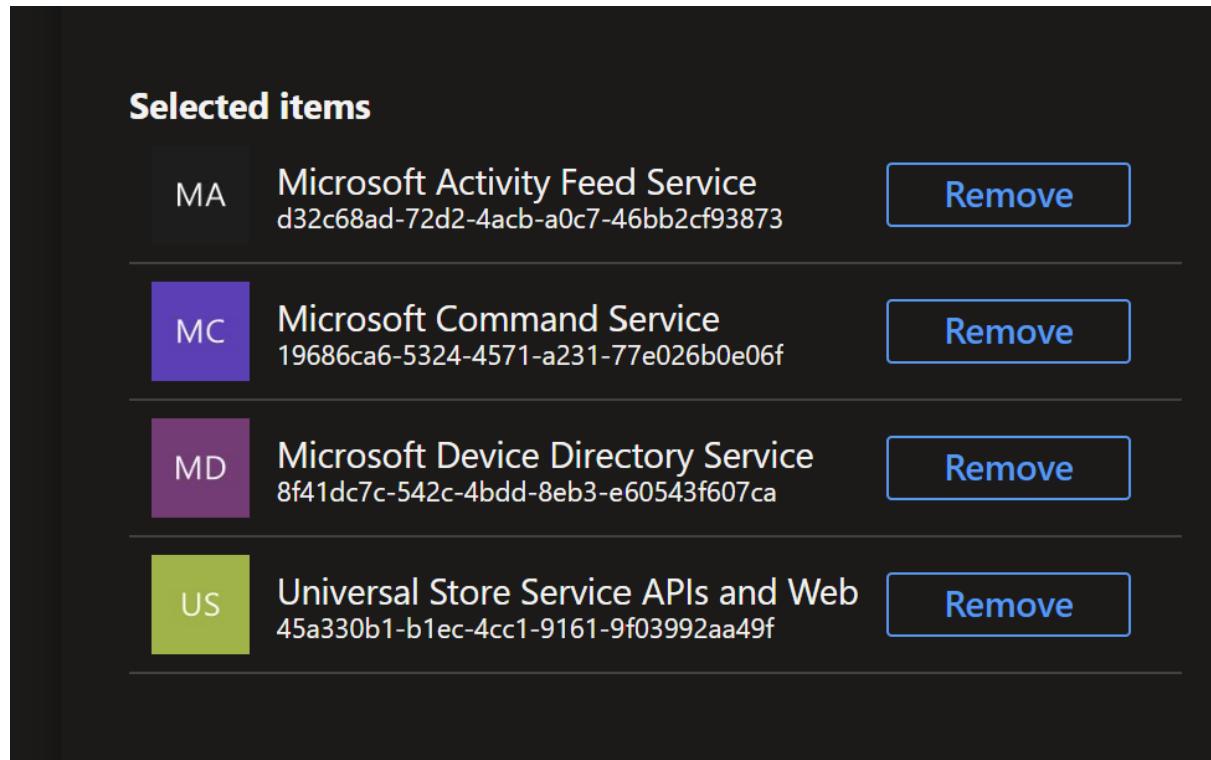
# Subscription based activation

- Important: Devices will automatically “migrate” from MAK, KMS and AD-based activation to Subscription when a user with an assigned license logs on.
- Blocked by the “Work or school account problem”
- Exclude **Universal Store Service APIs and Web Application** from your Conditional Access framework.



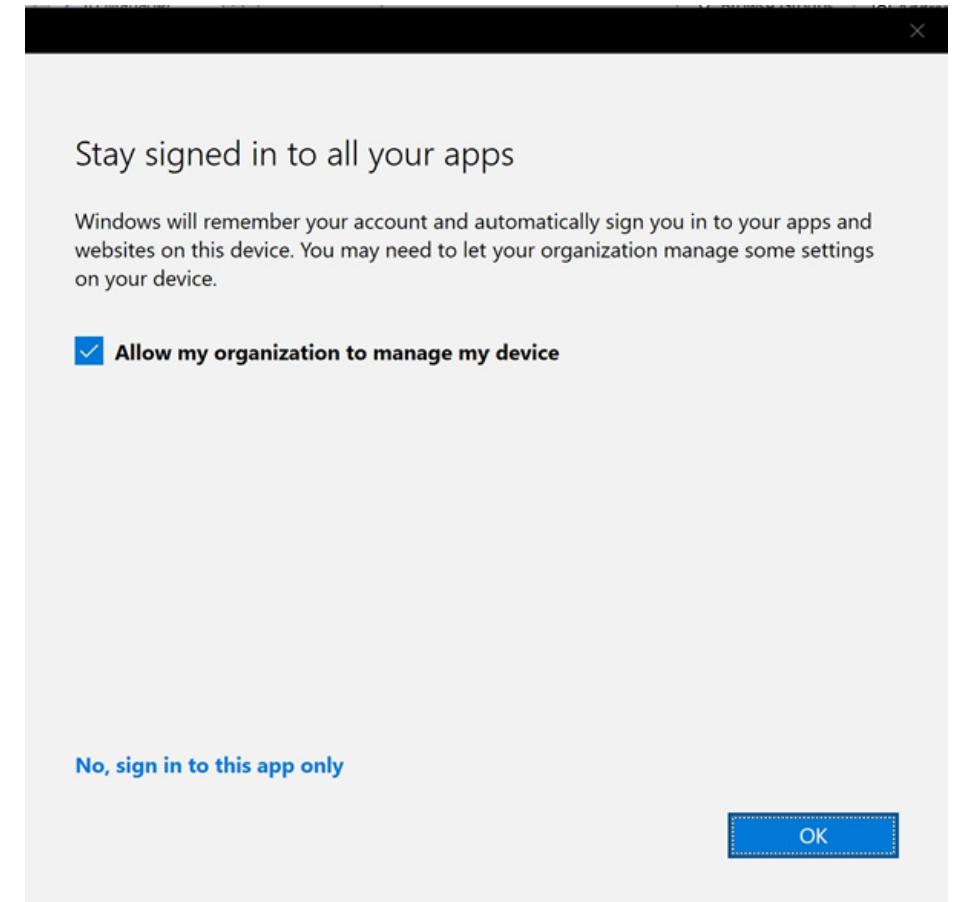
# CA exclusions

If Windows Hello for business is not used the following endpoints can be excluded from MFA to make sure Licensing works and prevent the pop-up “Work or School Account Problem” dialog to show up.



# Stay signed in to all your apps = Evil

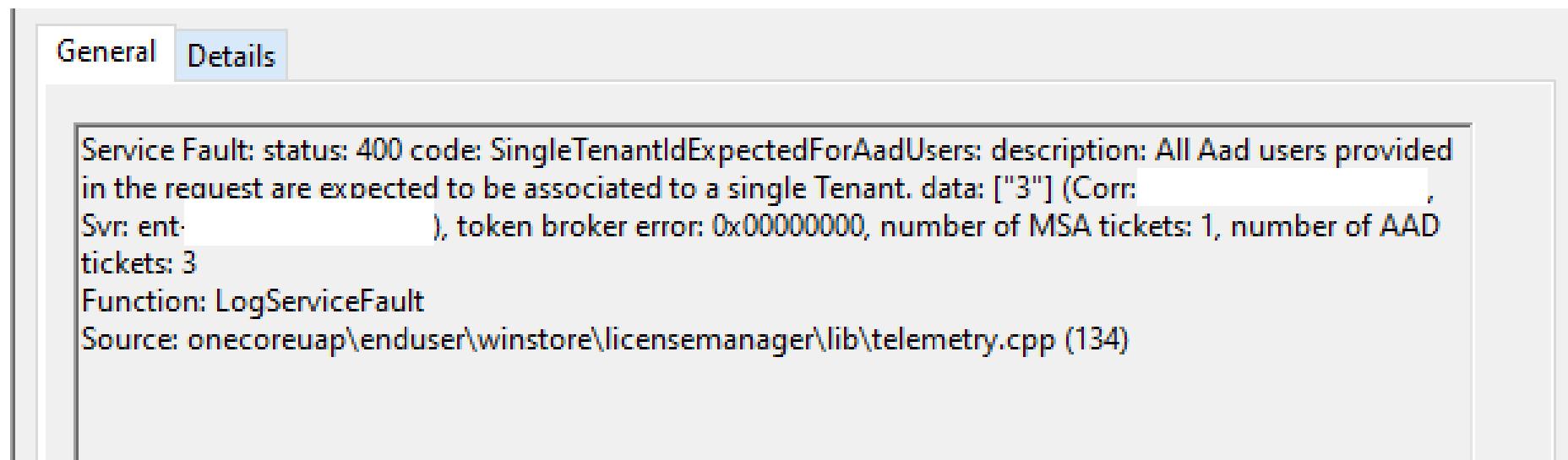
- “**Stay signed in to all your apps**” dialog in Microsoft Apps (outlook, Powerpoint, excel....)
- Recommended to block in Hybrid join
- Needs to be blocked on all modern managed Windows devices!
  - Personal devices: Intune sync will fail
  - AzureAD Joined devices: Windows Activation will fail



# Subscription Based Activation

- Store Event Log + Schedule Task

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
EnableLicenseAcquisition	Ready	Multiple triggers defined		2021-09-29 07:34:23	The operation completed successfully. (0x0)
LicenseAcquisition	Ready	Multiple triggers defined	2021-09-30 04:44:30	2021-09-29 07:34:30	(0x87E10BF2)

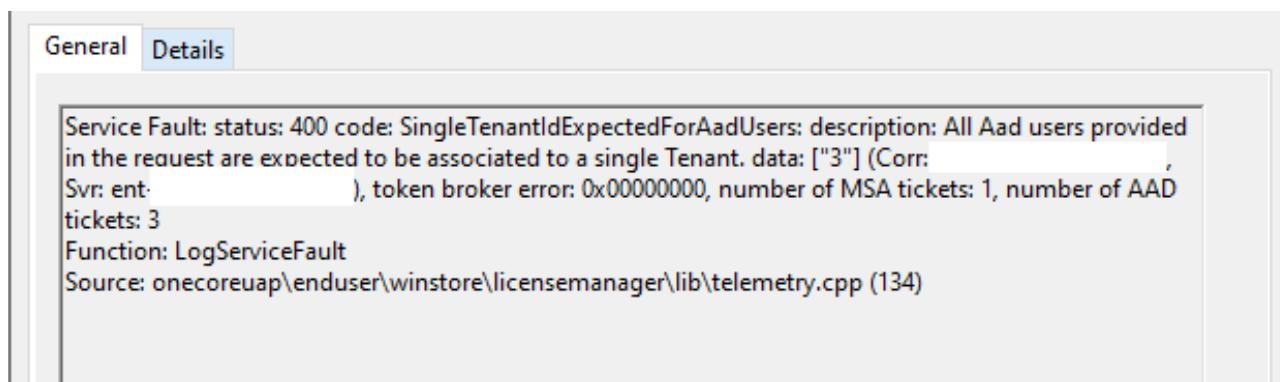


# Subscription based activation

- Re-activated every 30 days
- Two scheduled tasks triggers License Acquisition

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
EnableLicenseAcquisition	Ready	Multiple triggers defined		2021-09-29 07:34:23	The operation completed successfully. (0x0)
LicenseAcquisition	Ready	Multiple triggers defined	2021-09-30 04:44:30	2021-09-29 07:34:30	(0x87E10BF2)

- The renewal is done using the StoreAPI
  - In this case more than one AzureAD account was added under "Access work or School"



## Create profile ...

Windows 10 and later - Settings catalog (preview)

Basics Configuration settings Assignments Scope tags

+ Add settings

Settings

Allow Workplace ⓘ  Block

### Settings picker

Use commas "," among search terms to lookup settings by their keywords

+ Add filter

Browse by category

- Administrative Templates\Start Menu and Taskbar
- Administrative Templates\System\Group Policy
- Settings

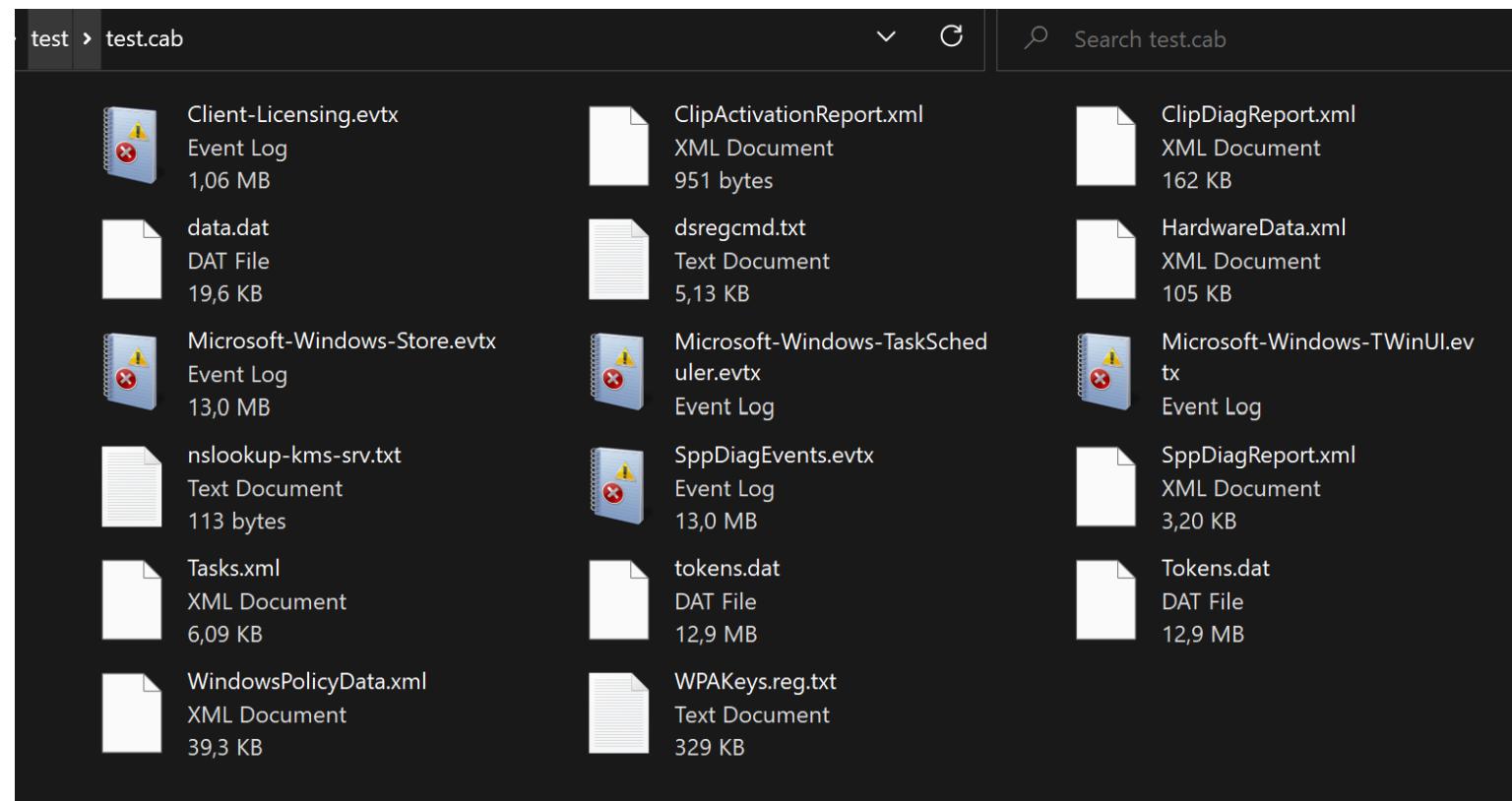
1 results in the "Settings" category

Select all these settings

Setting name
<input checked="" type="checkbox"/> Allow Workplace ⓘ

# Collecting information

- **Licensingdiag -cab c:\test\test.cab**
- Collects all registry entries and event logs related to licensing



# ENROLLMENT

# Troubleshooting Windows enrollment

- Valid License assigned to the user?
- Is the user allowed to enroll a device?
- Network issues, proxy etc.?
- Enrollment restrictions that blocks enrollment?
- Number of devices already enrolled (Device Limit)
- MDM Terms of use not correct

# Hybrid Azure AD Join

- Group Policy (No Offset) (User Token)
- Co-Management (Offset) (Device token -> User Token)
  - Schedules enrollment with an offset
  - If the enrollment fails, SCCM will retry 2 times every 15 mins
- Common issues
  - The user is not in AAD
  - The device is not Synced (Hybrid Azure AD Join)
- Will be flagged as Corporate

<https://www.imab.dk/auto-mdm-enrollment-fails-with-error-code-0x8018002a-troubleshooting-mdm-enrollment-errors-co-management-with-sccm-and-intune/>

# Co-Managed device enrollment

- Co-managed devices will always try to enroll using a Device token
- If it fails it will try using the user token, depending on MFA settings this can fail as well.

Enrolling device to MDM... Try #1 out of 3

Enrolling device with RegisterDeviceWithManagementUsingAADDeviceCredentials

Processing GET for assignment (Scopeld\_B54C7DB5-E99F-4BC7-95DD-C383A9E555A9/ConfigurationPolicy\_96925c8d-7753-4899-a44c-79f6...)

Getting/Merging value for setting 'CoManagementSettings\_AutoEnroll'

Merged value for setting 'CoManagementSettings\_AutoEnroll' is 'true'

Getting/Merging value for setting 'CoManagementSettings\_Allow'

Merged value for setting 'CoManagementSettings\_Allow' is 'true'

Date/Time: 2022-05-09 22:22:08 Component: CoManagementHandler

Thread: 12896 (0x3260) Source: mdmreglib.cpp:164

Enrolling device with RegisterDeviceWithManagementUsingAADDeviceCredentials

# Enrollment restrictions and “All Users”

- Important: the default enrollment restriction policy “All Users” is applied to “All Devices”

Home > Devices > Enroll devices >

The screenshot shows the 'All Users' restriction policy details. The 'Overview' tab is selected. Key information includes:

- All Users** (highlighted with a red box)
- Search (Ctrl+ /)**
- Essentials**: Created: 01/01/70, 1:00 AM; Last modified: 05/11/20, 11:20 AM; Platforms configured: 6
- Assigned to**: All devices (highlighted with a red box)
- Manage**
- Properties**

Below the policy details, there is a list of recent errors:

- New merged workloadflags value with co-management max capabilities '16383' is '3'
- Failed to enroll with RegisterDeviceWithManagementUsingAADDeviceCredentials with error code 0x80180014.
- MDM enrollment failed with error code 0x80180014 'Specific platform or version is not supported'. Will retry in 240 minut...
- Could not check enrollment url, 0x00000001:

# Enrollment Failures

Microsoft Endpoint Manager admin center

Home > Monitor

## Monitor | Enrollment failures

Search (Ctrl+ /) Filter Refresh Export

Configuration

- Assignment status
- Assignment failures (preview)
- Devices with restricted apps
- Encryption report
- Certificates

Compliance

- Noncompliant devices
- Devices without compliance policy
- Setting compliance
- Policy compliance
- Noncompliant policies (preview)
- Windows health attestation report
- Threat agent status

Enrollment

- Autopilot deployments (preview)
- Enrollment failures**
- Incomplete user enrollments

Software updates

Per update ring deployment state

Date Failure OS OS version

05/13/21, 7:50 AM	Device cannot be enrolled as personal	Windows 10	10.0.18363.0
05/13/21, 1:19 PM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/14/21, 9:13 AM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/17/21, 8:08 PM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/17/21, 10:08 PM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/13/21, 8:49 PM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/17/21, 9:06 AM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/16/21, 2:29 PM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/17/21, 11:22 PM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/12/21, 5:01 PM	Device cannot be enrolled as personal		
05/13/21, 7:30 AM	Device cannot be enrolled as personal	Windows 10	10.0.19041.0
05/13/21, 12:56 PM	Device cannot be enrolled as personal	Windows 10	10.0.16299.0
05/14/21, 7:20 AM	Device cannot be enrolled as personal	Windows 10	10.0.19041.0
05/17/21, 7:29 AM	Device cannot be enrolled as personal	Windows 10	10.0.19041.0
05/17/21, 11:08 AM	Device cannot be enrolled as personal	Windows 10	10.0.19042.0
05/13/21, 9:08 AM	Device cannot be enrolled as personal	Windows 10	10.0.19041.0

### Enrollment failure

#### DETAILS

This device can't be enrolled as a personal device while the platform is Blocked under Device Type Restrictions.

#### RECOMMENDED STEPS

The user must use a different platform of personal device to enroll. If this is a corporate device make sure that the user is enrolling correctly and that you have added the device to the Corporate device identifiers list if needed. You can check your personal platform restrictions under Device enrollment > Enrollment restrictions > choose a restriction > Configure platform.

#### ADDITIONAL RESOURCES

[Learn more about Enrollment Restrictions.](#)  
[Learn more about Enrollment Restrictions.](#)

#### DEVICE DETAILS

Enrollment Start	5/14/2021 9:13:42 AM
OS	Windows 10
OS Version	10.0.19042.0

#### GET SUPPORT

If you can't resolve this issue, [contact support](#) and paste the below Activity ID into the ticket details.

Activity ID: 112401f7

# DeviceCapReached = Device Limits

Something went wrong.

This user is not authorized to enroll. You can try to do this again or contact your system administrator with the error code 801c0003.

Additional problem information:

Server error code: 801c0003

Correlation ID: 3cf8d9b5-a749-43f7-97e4-9b315ffe97fd

Timestamp: 08-16-2019 9:14:01Z

Server message: User '538156d0-c028-429c-90ec-be15074f379f' is not eligible to enroll a device of type 'Windows'. Reason 'DeviceCapReached'.

More information: <https://www.microsoft.com/aadjerrors>

# Enrollment limit restrictions

- Are not applied when enrolling a device in the following scenarios:
  - Co-managed enrollments
  - Group Policy (GPO) enrollments
  - Azure Active Directory (Azure AD) joined enrollments, including bulk enrollments
  - Windows Autopilot enrollments
  - Device enrollment manager enrollments

# Client Health

- How do you verify that a client is working as expected ?
- Co-management to the rescue!
- In Intune we can now see:
  - Configuration Manager agent state
  - Last Configuration Manager agent check in time
- Intune-enrolled devices connect to the cloud service 3 times a day, approximately every 8 hours.

The screenshot shows the Microsoft Intune Device Overview page for a device named APENTO-Bndfil1Z. The device is managed by Ronni Pedersen and has a Corporate ownership status. It is running Windows and is a Virtual Machine. The device actions status shows 'No results'. In the co-management section, it is noted that the Configuration Manager agent state is Unknown. The last Configuration Manager agent check-in time was 05-06-2019 15:10:12. The Intune managed workloads listed include Client Apps, Resource Access Profiles, Device Configuration, Compliance Policy, Windows Update for Business, Endpoint Protection, and Office Click-to-Run.

Search (Ctrl+ /) «

X Retire ↻ Wipe 🗑 Delete 🔒 Remote lock Sync 🔑 Reset passcode ⚡ Restart ↻ Fresh Start ⚡ Autopilot Reset ⚡ Quick scan

① Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Recovery keys

Managed Apps

Device name : APENTO-Bndfil1Z

Management name : mail\_Windows\_5/26/2019\_6:52 PM

Ownership : Corporate

Serial number : 7987-3600-6266-3074-4536-7994-21

Phone number : ---

Primary User : Ronni Pedersen

Enrolled by : Ronni Pedersen

Compliance : Not Compliant

Operating system : Windows

Device model : Virtual Machine

See more

Device actions status

Action	Status	Date/Time
No results		

Co-management

Ronni Pedersen's Windows PC is being co-managed between Intune and Configuration Manager. Configuration Manager agent state is shown below, if the state is a there are a few steps that help with this. [Learn more](#)

Configuration Manager agent state

Unknown

Details

Details about the client's state are only reported for Configuration Manager version 1806 and later. Make sure that the Configuration Manager client is present on your device and is running a supported version.

Last Configuration Manager agent check in time

05-06-2019 15:10:12

Intune managed workloads

Client Apps; Resource Access Profiles; Device Configuration; Compliance Policy; Windows Update for Business; Endpoint Protection; Office Click-to-Run

# **WUFB / SAFEGUARD HOLDS**

# Safeguard Holds

## What is a Safeguard hold?

- Microsoft uses quality and compatibility data to identify issues that might cause a Windows client feature update to fail or roll back.
- When we find such an issue, we might apply safeguard holds to the updating service to prevent affected devices from installing the update in order to safeguard them from these experiences.
- Source: <https://learn.microsoft.com/en-us/windows/deployment/update/safeguard-holds>

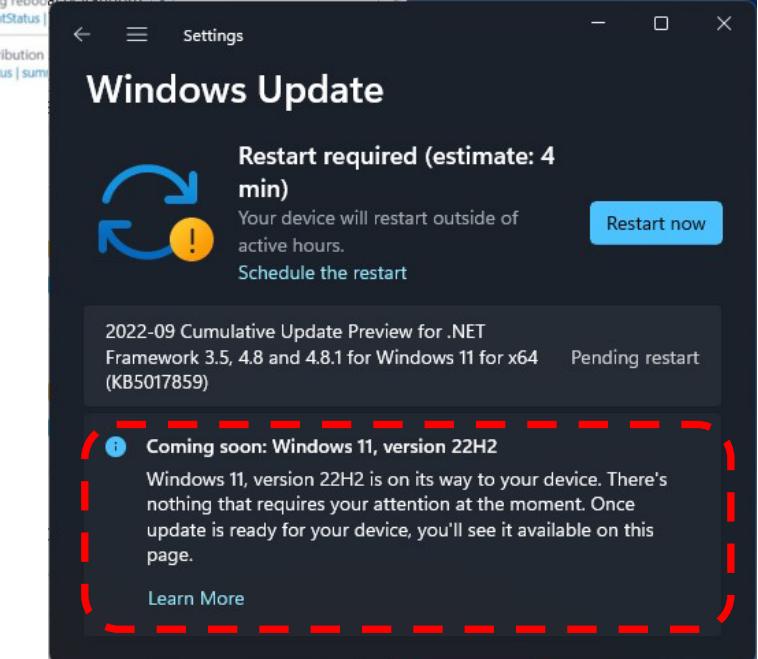
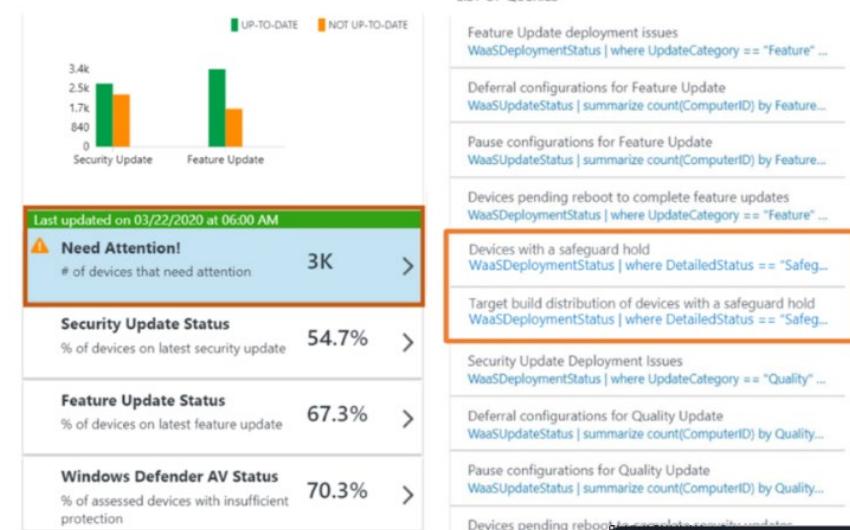


# Safeguard Holds

- Diagnostic Data is used to determine whether a devices are ready for a feature update...
- Goal: To ensure a smooth experience!

A screenshot of the Microsoft Log Analytics interface. At the top, there's a search bar with 'New Query 1\*' and a red arrow pointing to the 'Run' button. Below the search bar, the URL 'LogAnalyticsWorkspaceIntune' is visible. The main area shows a table with two rows of data. The columns are: TimeGenerated [UTC], Computer, ComputerID, OSVersion, OSBuild, and DetailedStatus. Both rows have 'DetailedStatus' set to 'Safeguard Hold'. A red box highlights the 'DetailedStatus' column.

TimeGenerated [UTC]	Computer	ComputerID	OSVersion	OSBuild	DetailedStatus
11/18/2020, 7:00:00.000 PM	Win10client02	g:6825777654129695	1909	18363.1198	Safeguard Hold
11/18/2020, 7:00:00.000 PM	Win10client02	g:6825777654129695	1909	18363.1198	Safeguard Hold



# Get the Blocker ID (Local)

## Command:

```
reg query "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\NI22H2"
```

## Output:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\NI22H2
```

```
DX12 REG_SZ 0  
DestBuildNum REG_SZ 22621  
DestBuildNumList REG_SZ 22621,22622,22623  
GStatus REG_SZ 0  
GatedBlockId REG_MULTI_SZ 41928397\041332279  
GatedBlockReason REG_MULTI_SZ Other\00Other  
GatedFeature REG_MULTI_SZ None"
```



# SafeGuardHoldLookupSample.ps1

- Author: Gary Blok
- Blog: <https://garytown.com/>

## Script:

- <https://github.com/gwablok/garytown/blob/master/Feature-Updates/SafeGuardHolds/SafeGuardHoldLookupSample.ps1>

# Output (Example)

```
APP_NAME      : Devices with Integrated 4-Channel Mic and have used Voice Recorder app
SafeguardId   : 41928397
EXE_ID        : {8b5f77d7-26d2-4221-8ab0-059f56532d5b}
PICK_ONE      :
AppName       : Devices with Integrated 4-Channel Mic and have used Voice Recorder app
VENDOR        : Microsoft
NAME          :
BlockType     : GatedBlock
```

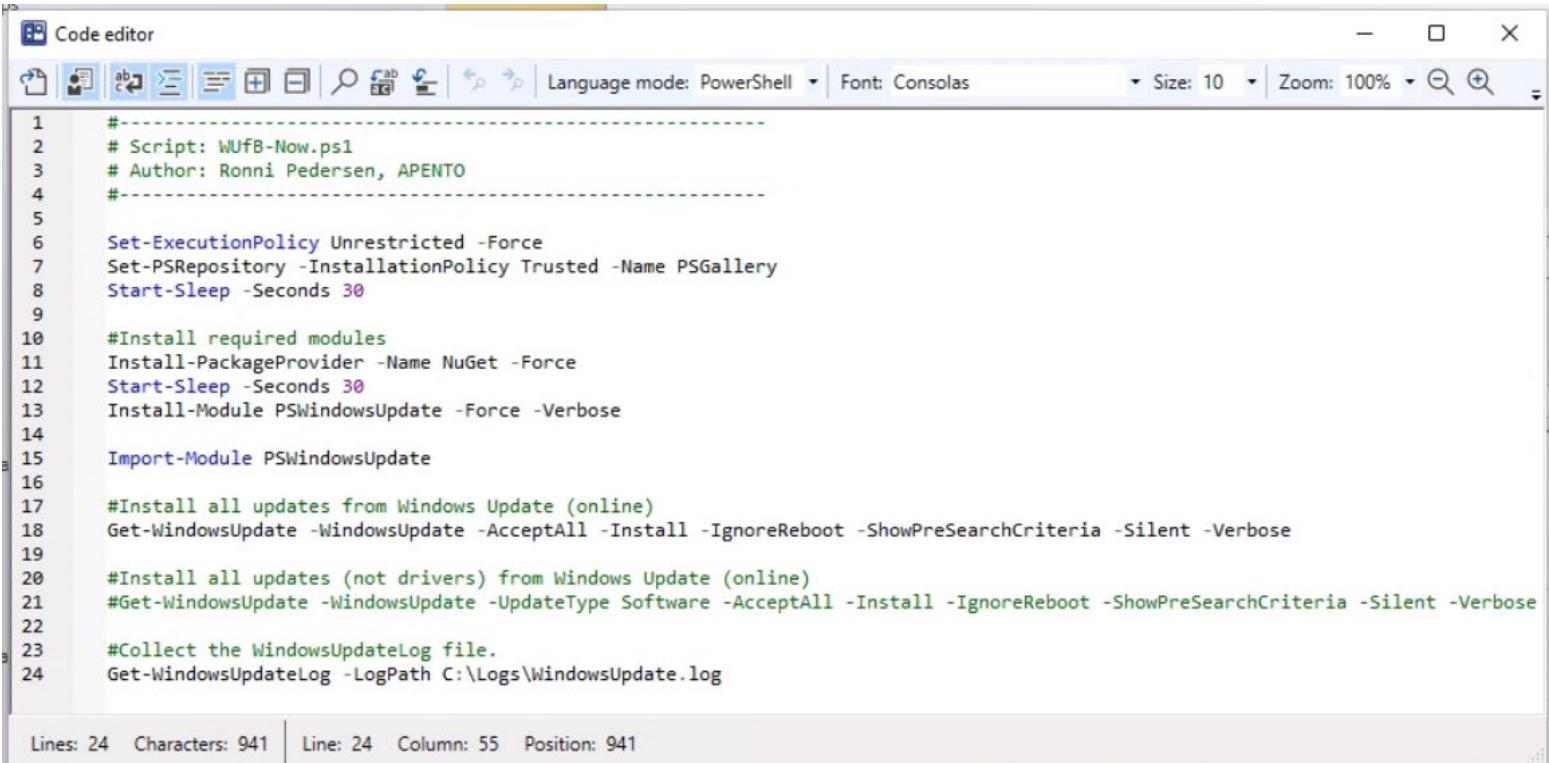
Fix: Update driver and/or firmware

```
APP_NAME      : Devices with printer using Microsoft IPP Class Driver (Wu Offer Block)
SafeguardId   : 41332279
EXE_ID        : {cce5bc0a-4441-4c83-9633-a4c1ec4731ff}
PICK_ONE      :
AppName       : Devices with printer using Microsoft IPP Class Driver (Wu Offer Block)
VENDOR        : Microsoft
NAME          :
BlockType     : GatedBlock
```

Fix: Update or remove the printer driver

# WUFB-Now.ps1 / PSWindowsUpdate

- Total Devices: 23.000
- Devices with old Feature Updates: 1.272
- After Script: 307
- Script deployed from
  - SCCM
  - Intune



The screenshot shows a PowerShell code editor window with the following details:

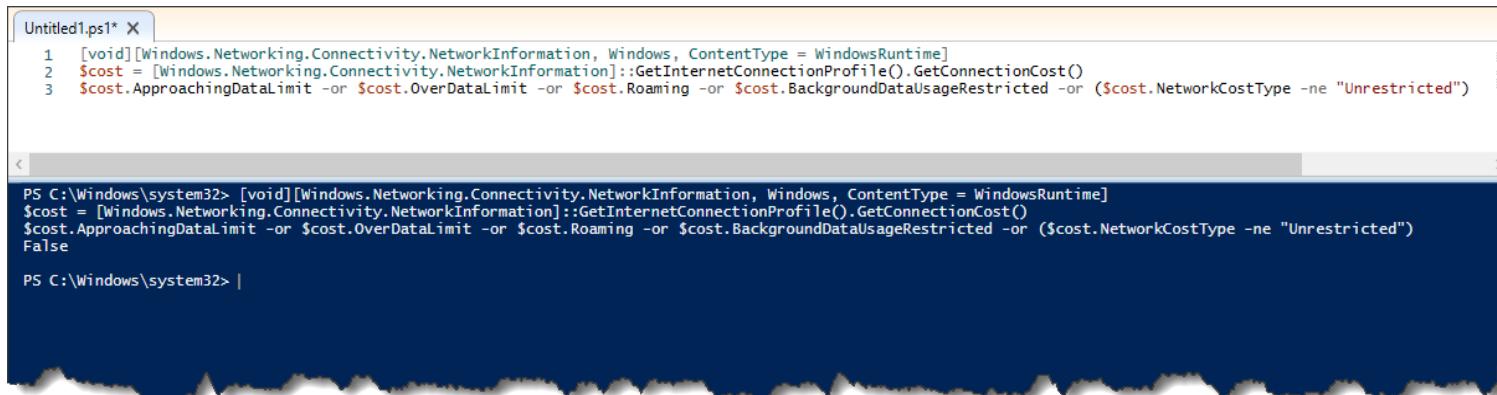
- Title Bar:** Code editor
- Toolbar:** Includes icons for file operations (New, Open, Save, Print), search, and zoom.
- Status Bar:** Lines: 24 Characters: 941 | Line: 24 Column: 55 Position: 941
- Language Mode:** PowerShell
- Font:** Consolas
- Zoom:** Size: 10 | Zoom: 100%

The script content is as follows:

```
1 #-----
2 # Script: WUFB-Now.ps1
3 # Author: Ronni Pedersen, APENTO
4 #-----
5
6 Set-ExecutionPolicy Unrestricted -Force
7 Set-PSRepository -InstallationPolicy Trusted -Name PSGallery
8 Start-Sleep -Seconds 30
9
10 #Install required modules
11 Install-PackageProvider -Name NuGet -Force
12 Start-Sleep -Seconds 30
13 Install-Module PSWindowsUpdate -Force -Verbose
14
15 Import-Module PSWindowsUpdate
16
17 #Install all updates from Windows Update (online)
18 Get-WindowsUpdate -WindowsUpdate -AcceptAll -Install -IgnoreReboot -ShowPreSearchCriteria -Silent -Verbose
19
20 #Install all updates (not drivers) from Windows Update (online)
21 #Get-WindowsUpdate -WindowsUpdate -UpdateType Software -AcceptAll -Install -IgnoreReboot -ShowPreSearchCriteria -Silent -Verbose
22
23 #Collect the WindowsUpdateLog file.
24 Get-WindowsUpdateLog -LogPath C:\Logs\WindowsUpdate.log
```

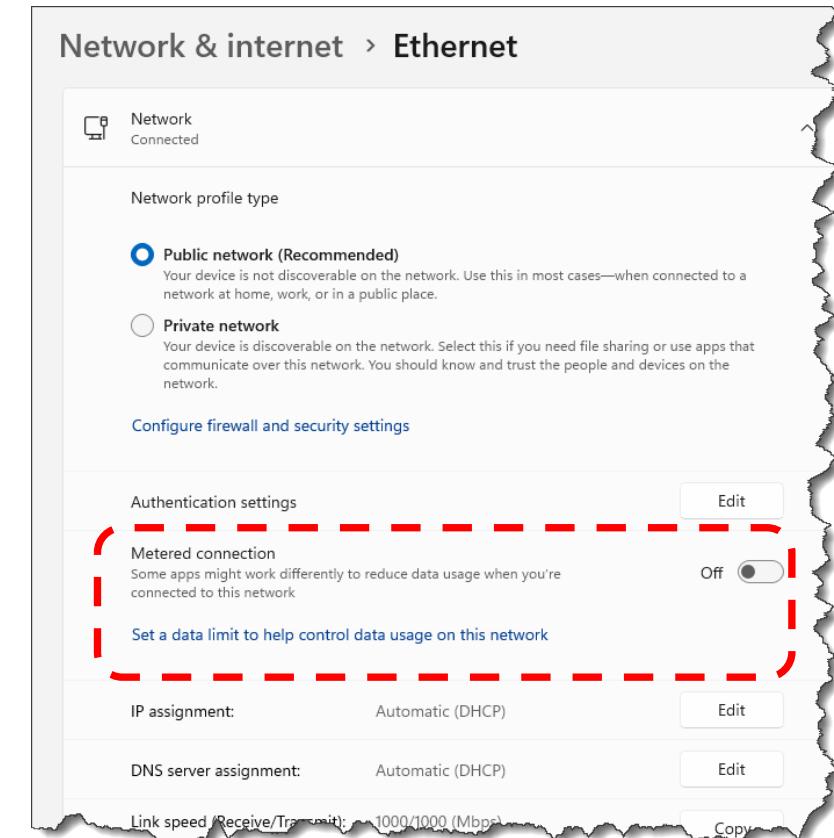
# Metered Network Issue

- “Metered network” = Enabled
- Result = Not downloading updates
- Impacted Clients: 60-70
- Solution
  - Check if metered network is enabled
  - Run script remotely using PowerShell Remoting



```
Untitled1.ps1* X
1 [void][Windows.Networking.Connectivity.NetworkInformation, Windows, ContentType = WindowsRuntime]
2 $cost = [Windows.Networking.Connectivity.NetworkInformation]::GetInternetConnectionProfile().GetConnectionCost()
3 $cost.ApproachingDataLimit -or $cost.OverDataLimit -or $cost.Roaming -or $cost.BackgroundDataUsageRestricted -or ($cost.NetworkCostType -ne "Unrestricted")
```

```
PS C:\Windows\system32> [void][Windows.Networking.Connectivity.NetworkInformation, Windows, ContentType = WindowsRuntime]
$cost = [Windows.Networking.Connectivity.NetworkInformation]::GetInternetConnectionProfile().GetConnectionCost()
$cost.ApproachingDataLimit -or $cost.OverDataLimit -or $cost.Roaming -or $cost.BackgroundDataUsageRestricted -or ($cost.NetworkCostType -ne "Unrestricted")
False
PS C:\Windows\system32> |
```



# SCCM Clients / Metered Connections

- Solution/Fix: SCCM (Script), GPO, Intune Policy

The image shows two side-by-side screenshots. On the left, a Visual Studio Code interface displays two PowerShell scripts: `autopilotFetch.ps1` and `Remediate-MeteredConnection.ps1`. The `Remediate-MeteredConnection.ps1` script is highlighted and contains the following code:

```
$CCMNetworkCost = (Invoke-CimMethod -Namespace "root\ccm\ClientSDK" -ClassName "CCM_ClientUtilities" -MethodName GetNetworkCost).Value
Write-Host "ConfigMgr Cost: $($CCMNetworkCost)"

If($CCMNetworkCost -ne 1) {
    #Set metering to 1, restart client so it will check in, remove the policy instance, then get new policies
    $PolicyNameSpace = "root\ccm\Policy\Machine\ActualConfig"
    $NwClassName = "CCM_NetworkSettings"
    $obj = Get-CIMInstance -Namespace $PolicyNameSpace -ClassName $NwClassName
    If($obj.MeteredNetworkUsage -ne 1) {
        Write-Host "ConfigMgr MeteredNetworkUsage is set to $($obj.MeteredNetworkUsage)"
        Write-Host "Resetting ConfigMgr CCM_NetworkSettings Policy"
        $obj | Set-CIMInstance -Property @{MeteredNetworkUsage=1}
        Restart-Service -Name ccexec -ErrorAction SilentlyContinue
    }
}
```

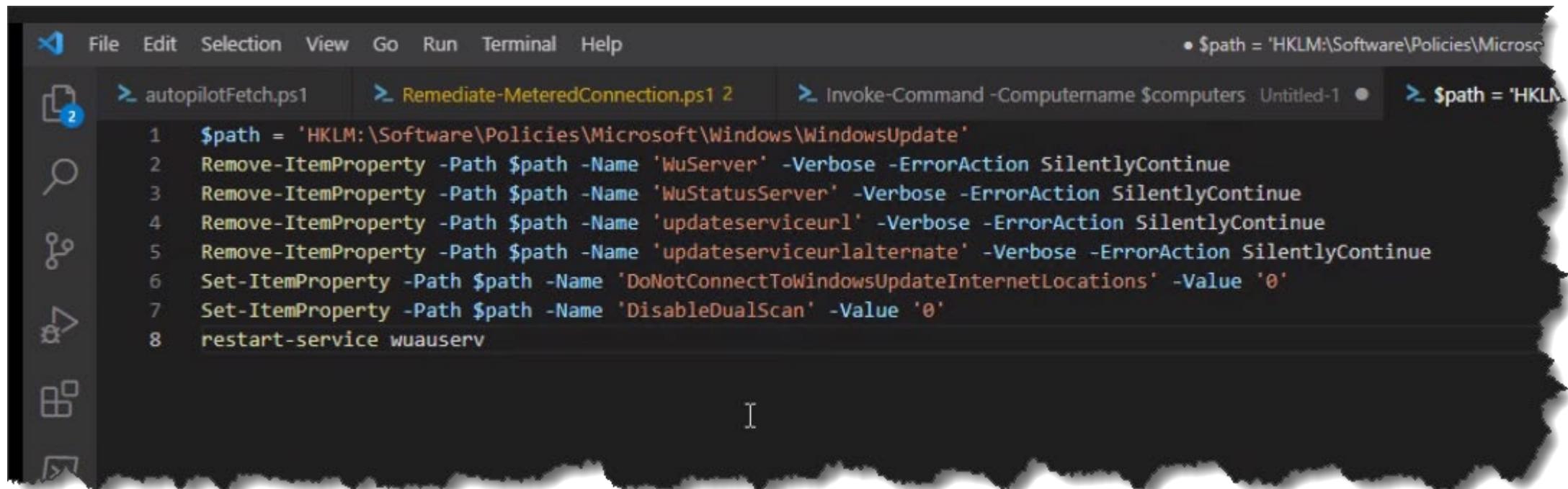
On the right, a screenshot of the Windows Settings Catalog shows the "Edit profile - Allow windows updates over metered networks" configuration settings. A specific setting, "Allow Auto Windows Update Download Over Metered Network", is highlighted with a red border.

Script:

<https://github.com/AdamGrossTX/Toolbox/blob/master/ConfigMgr/Troubleshooting/Remove-NetworkMetering.ps1>

# Remove legacy policies (GPO)

- Quick Fix: A simple script to clean up the registry



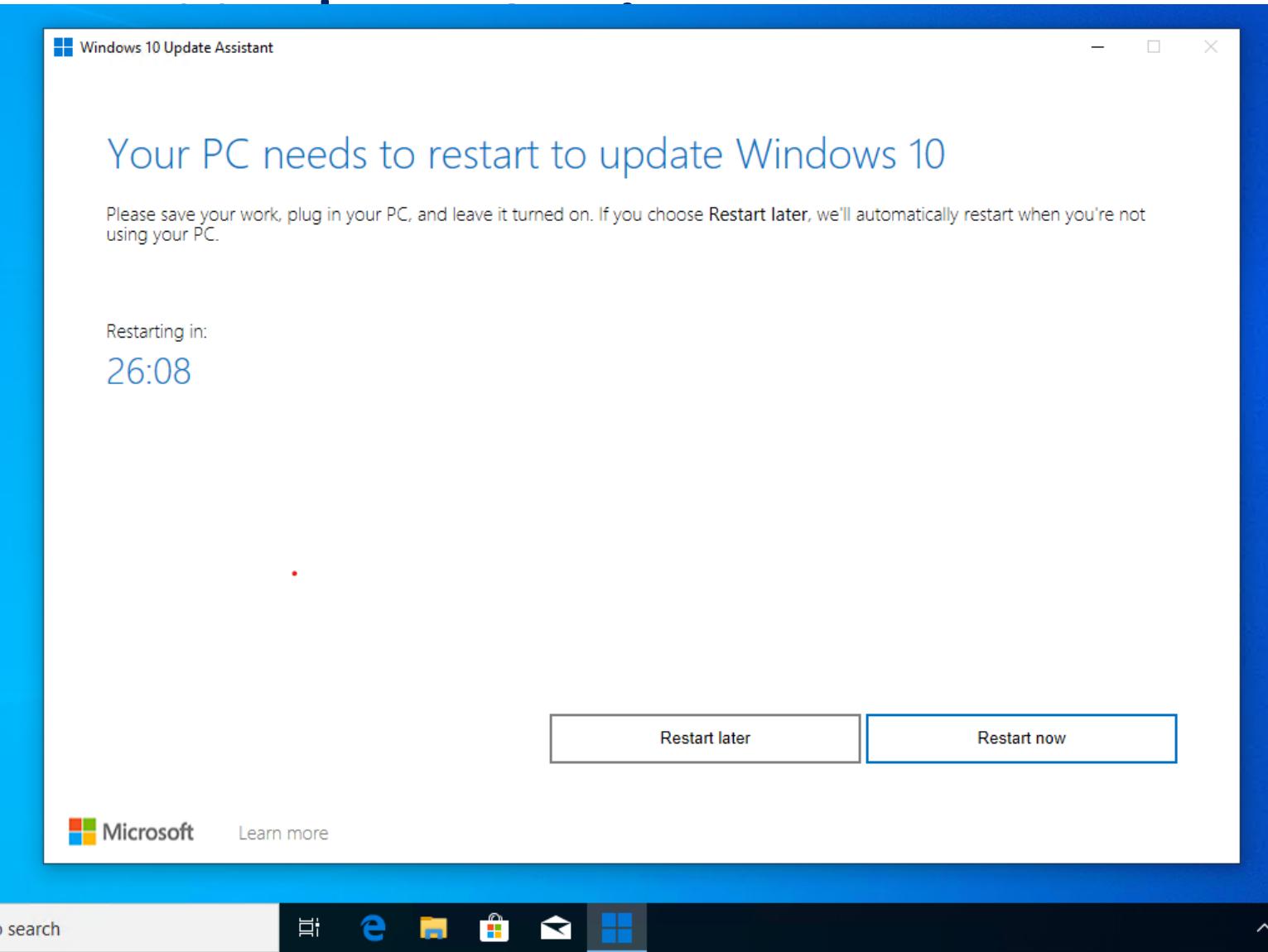
The screenshot shows a PowerShell ISE window with two tabs open. The left tab contains a script named 'Remediate-MeteredConnection.ps1' which removes specific registry keys under 'HKLM:\Software\Policies\Microsoft\Windows\WindowsUpdate'. The right tab shows a command to run this script across multiple computers using 'Invoke-Command -Computername \$computers'.

```
$path = 'HKLM:\Software\Policies\Microsoft\Windows\WindowsUpdate'
Remove-ItemProperty -Path $path -Name 'WuServer' -Verbose -ErrorAction SilentlyContinue
Remove-ItemProperty -Path $path -Name 'WuStatusServer' -Verbose -ErrorAction SilentlyContinue
Remove-ItemProperty -Path $path -Name 'updateserviceurl' -Verbose -ErrorAction SilentlyContinue
Remove-ItemProperty -Path $path -Name 'updateserviceurlalternate' -Verbose -ErrorAction SilentlyContinue
Set-ItemProperty -Path $path -Name 'DoNotConnectToWindowsUpdateInternetLocations' -Value '0'
Set-ItemProperty -Path $path -Name 'DisableDualScan' -Value '0'
restart-service wuauserv
```

# Windows 10

- Custom
- Runs 1
- Autom

```
Code editor
1 $currentdate = Get-Date -f
2 $dir = "C:\Logs\Win10Feature"
3 New-Item $dir -ItemType Di
4 $webClient = New-Object Sy
5 $url = 'https://go.microso
6 $file = "$($dir)\Windows10
7 $webClient.DownloadFile($u
8 Start-Process -FilePath $f
```



# Last Resort Fix

## Disclaimer:

- This method is not supported
- I've reconnected multiple devices using this script and it worked great!
- So, if you are at the dead end, it may serve you well! ☺
- Source:  
<https://universecitiz3n.tech/powershell/Reenroll/>

```
$Global:ErrorActionPreference = 'Stop'
Write-Host "Stopping Intune Service" -ForegroundColor Yellow
Get-Service *intune* | Stop-Service
Write-Host "Check if device is AAD Joined" -ForegroundColor Yellow
$DSREGCMD = dsregcmd /status
$AADJoinCheck = $null
$AADJoinCheck = $DSREGCMD | Select-String -Pattern 'AzureAdJoined : YES'
if ($null -eq $AADJoinCheck) {
    Write-Host "Device is not AAD Joined!!! Stopping!" -ForegroundColor Red
    Break
} else {
    Write-Host "Device is AAD Joined - OK" -ForegroundColor Green
}
Write-Host "Searching for enrollment ID"
$Tasks = Get-ScheduledTask | Where-Object { $psitem.TaskPath -like "\Microsoft\Windows\EnterpriseMgmt\Reenrollment"
$EnrollID = $Tasks[0].TaskPath.Split('\\')[-2]
if ($EnrollID -match '\w{8}-\w{4}-\w{4}-\w{4}-\w{12}') {
    Write-Host "Found EnrollID - $EnrollID" -ForegroundColor Green
} else {
    Write-Host "Error parsing EnrollID. Stopping" -ForegroundColor Red
    Break
}
Write-Host "Removing scheduledTasks" -ForegroundColor Yellow
Try {
    $Tasks | ForEach-Object { Unregister-ScheduledTask -InputObject $psitem -Verbose -Confirm:$false }
} catch {
    Throw $_.Exception.Message
}
Write-Host "Done" -ForegroundColor Green
Write-Host "Trying to remove tasks folder" -ForegroundColor Yellow
$TaskFolder = Test-Path "C:\windows\System32\Tasks\Microsoft\Windows\EnterpriseMgmt\$EnrollID"
```

# Status on Windows 11 Upgrade

- Ring 1 (about 750 devices)
  - Roll up started Friday (March 10). This was status Tuesday (March 15).

Microsoft Intune admin center

Home > Reports | Windows updates (preview) >

### Windows 10 and later feature updates

Report generated on: 3/15/2023, 12:30:54 PM

770 DEVICES

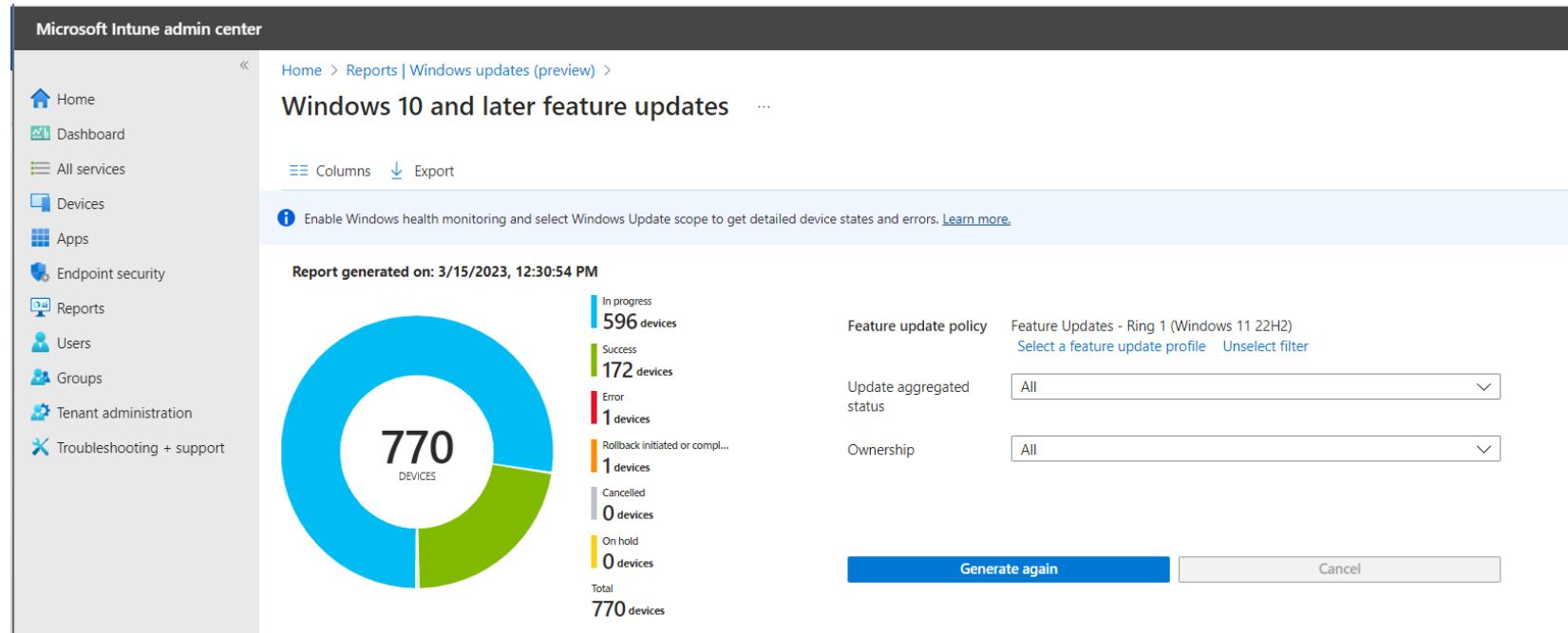
Status	Count
In progress	596 devices
Success	172 devices
Error	1 devices
Rollback initiated or compl...	1 devices
Cancelled	0 devices
On hold	0 devices
Total	770 devices

Feature update policy: Feature Updates - Ring 1 (Windows 11 22H2)  
Select a feature update profile   Unselect filter

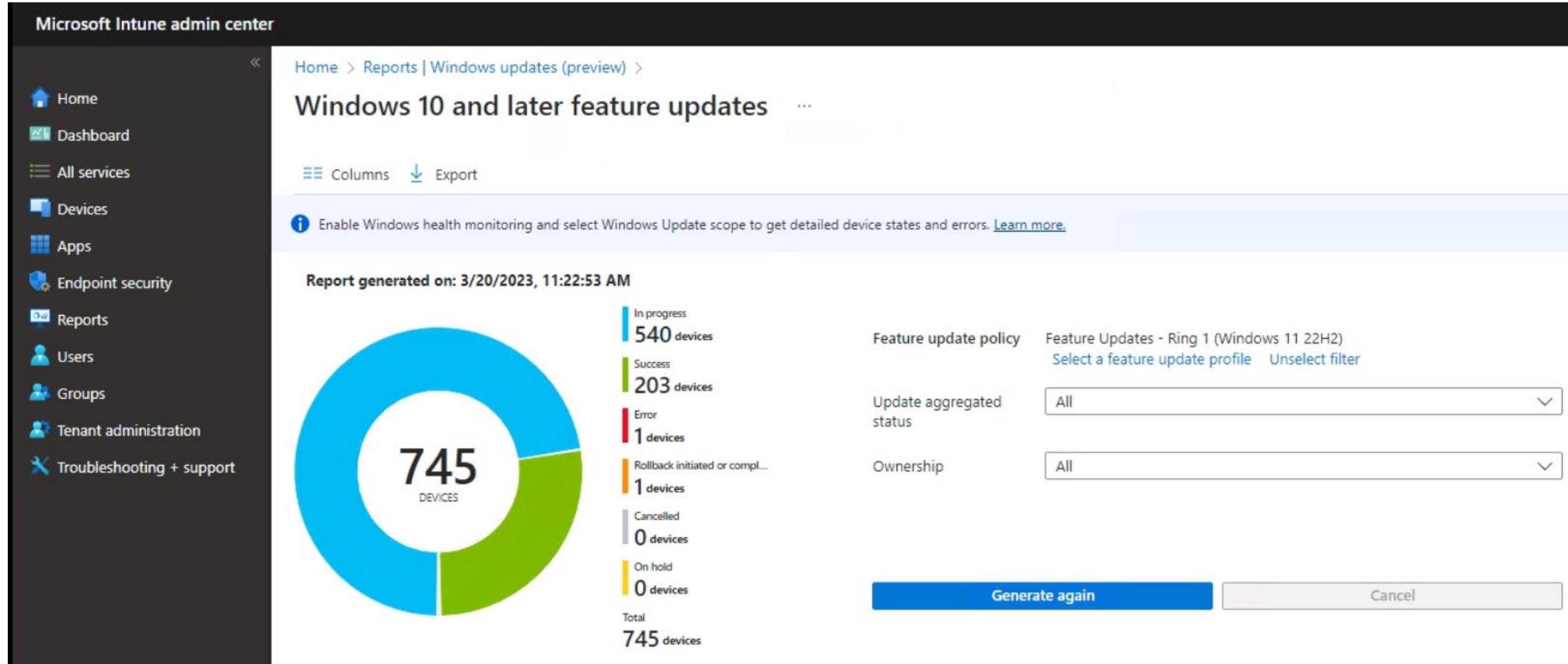
Update aggregated status: All

Ownership: All

Generate again Cancel



# Status today....



# INTUNE MANAGEMENT EXTENSION

# Intune Management Extension

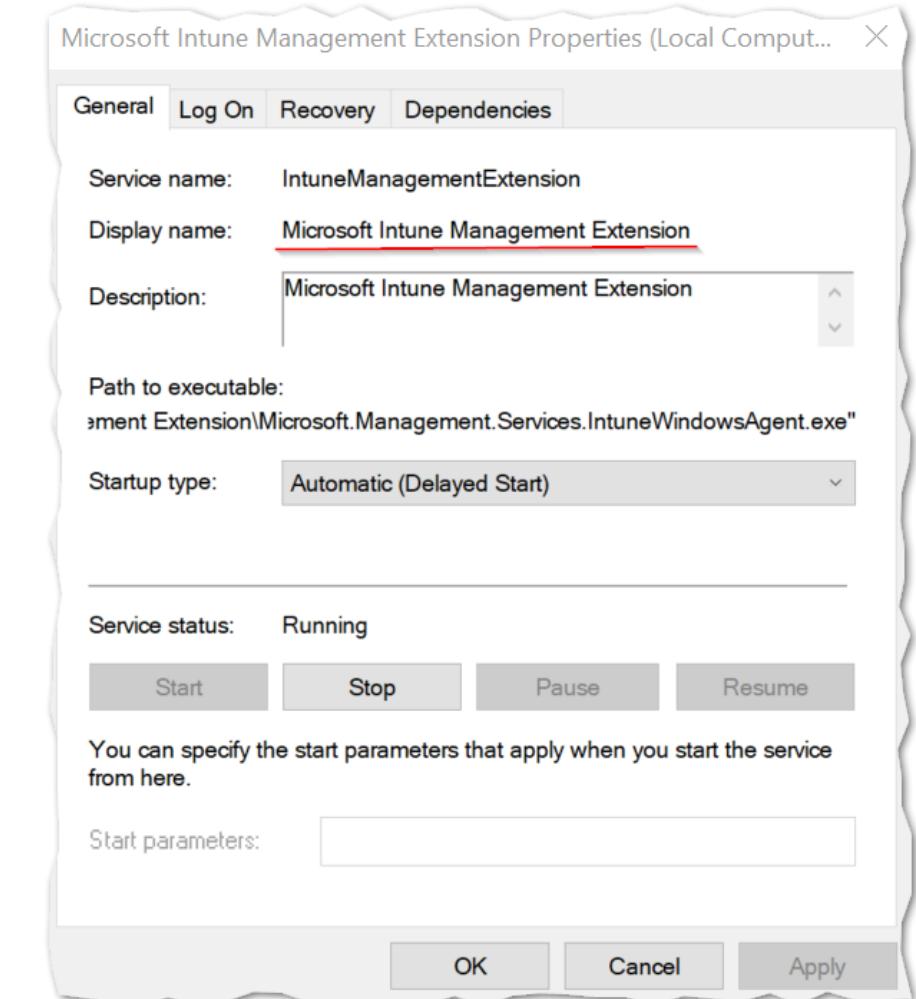
- An Introduction...
  - Know it
  - Plan it
  - Own it!
- Used by
  - Win32 apps
  - PowerShell scripts
  - Proactive remediations



# Intune Management Extension

## Troubleshooting

- Check that the service is installed and running
- Verify deployment in MDMDiagReport.html
- Are you meeting the Prerequisites?



<https://docs.microsoft.com/en-us/intune/apps/intune-management-extension#prerequisites>

# TROUBLESHOOTING POLICIES

# Configuration Policies

Recommended order for Windows devices

- Endpoint Security
- Settings Catalog (Preview)
- Templates
  - Configuration Policies
  - Built-In Administrative Templates
  - OMA-URI (Custom CSP)
- Custom ADMX ingestion (3rd. Party apps)
- PowerShell Scripts



Optional:

- Proactive Remediation (Requires a Windows Enterprise E3 license)

# Profile Tattooing

- Removing the assignment of the profile does not always revert the setting.
  - The behavior depends on the CSP.
  - Some setting remains until configured to a different value
  - Some CSPs remove the setting, and some CSPs keep the setting.
- Profiles applies to a **User Group** and a user is removed from the group.
  - Note: It can take up to **7 hours + the platform-specific policy refresh cycle**.
- Wi-Fi, VPN, Certificate, and Email Profiles
  - These profiles are removed from all supported enrolled devices

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot#what-happens-when-a-profile-is-deleted-or-no-longer-applicable>

# Policy and Profile refresh cycles

## Existing Devices

- Windows devices will schedule check-in with the Intune service: About every 8 hours

## Recently Enrolled Devices

- #1 - Every 3 minutes for 15 minutes
- #2 - Every 15 minutes for 2 hours
- #3 - Every 8 hours

## Manual Refresh

- Open the Company Portal app and sync the device to immediately check for policy or profile updates.
- This device check-in will not refresh the already applied Policy CSP settings.
- Trigger Task Scheduler (Recommended for troubleshooting)
- Scripted methods

## Computer Management

File Action View Help



Computer Management (Local)

Name	Status	Triggers
Login Schedule created by enrollment client	Ready	At log on of any user
OS Edition Upgrade event listener created by enrollment client	Ready	Custom Trigger
Passport for Work alert created by enrollment client	Ready	On event - Log: Microsoft-Windows-User Device Registration/Admin, Source: Microsoft-Windows-User Device Registration
Provisioning initiated session	Ready	
PushLaunch	Ready	Custom Trigger
PushRenewal	Ready	Multiple triggers defined
PushUpgrade	Ready	At 16:15 on 18-01-2020
Schedule #1 created by enrollment client	Ready	At 23:24 on 16-05-2019 - After triggered, repeat every 00:03:00 for a duration of 15 minutes.
Schedule #2 created by enrollment client	Ready	At 23:39 on 16-05-2019 - After triggered, repeat every 15 minutes for a duration of 02:00:00.
Schedule #3 created by enrollment client	Ready	At 01:39 on 17-05-2019 - After triggered, repeat every 08:00:00 indefinitely.
Schedule created by enrollment client for renewal of certificate warning	Ready	At 23:21 on 01-04-2020 - After triggered, repeat every 7,00:00:00 for a duration of 10,00:00:00.
Schedule to run OMADMClient by client	Ready	
Schedule to run OMADMClient by server	Ready	
Win10 S Mode event listener created by enrollment client	Ready	Custom Trigger

General Triggers Actions Conditions Settings History (disabled)

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	%windir%\system32\deviceenroller.exe /o "BF34185C-4364-40CF-A364-98DBD5B8ECB7" /c /b

# Intune notifications / Sync immediately

- Some actions will trigger a sync notification to the device
- When a Policy, Profile, or App is:
  - Assigned (or unassigned)
  - Updated
  - Deleted
- Manually from the Company Portal
- Manually using Script



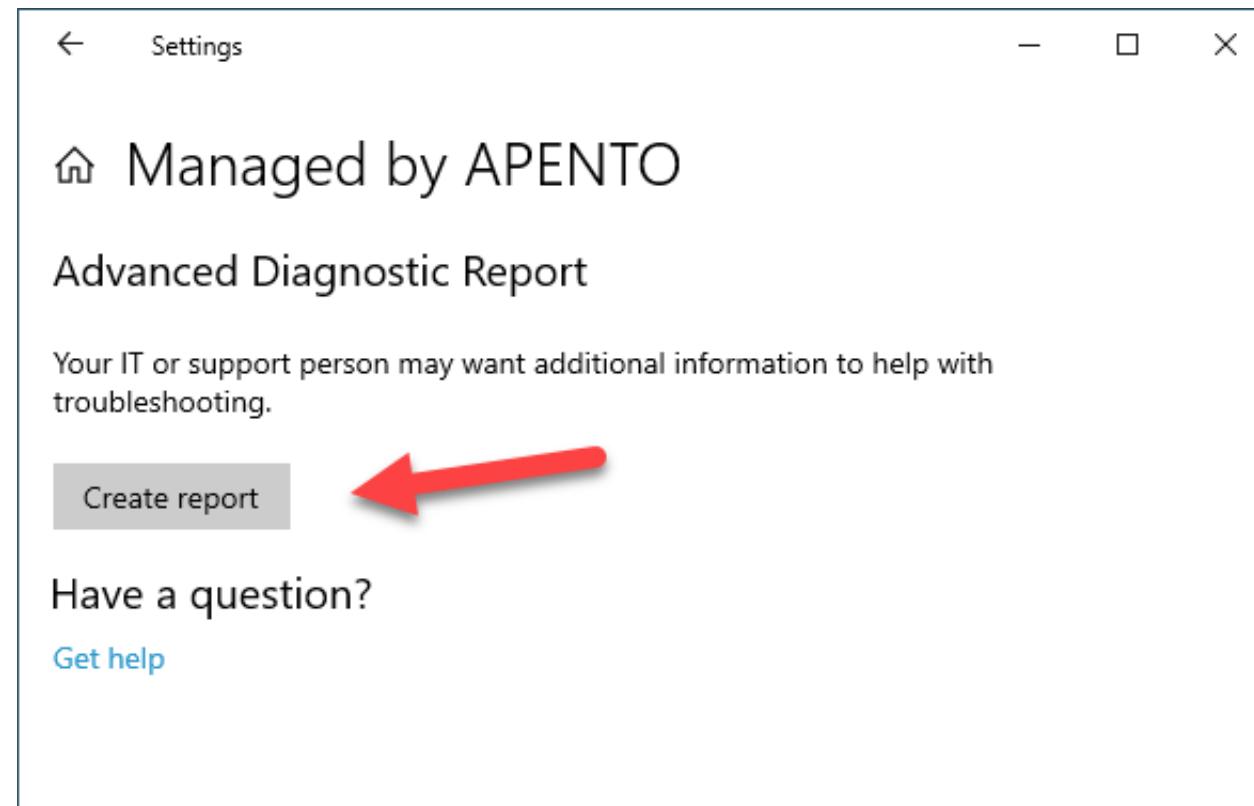
# Policy/Profile Conflicts

- 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.



# Troubleshooting MDM Policies

- C:\Users\Public\Documents\MDMDiagnostics\MDMDiagReport.html



## Managed policies

Policies that are not set to the default value or have a configuration source applied

Area	Policy	Default Value	Current Value	Target	Dynamic	Config Source
Authentication	EnableWebSignIn	0	1	device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
BitLocker	EncryptionMethodByDriveType			device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=<enable d/><data id="EncryptionMethodWithXtsOsDropDown_Name" value="7"/><data id="EncryptionMethodWithXt sFdvDropDown_Name" value="7"/><data id="Encrypti onMethodWithXtsRdvDropDown_Name" value="7"/>
BitLocker	SystemDrivesRecoveryOptions			device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=<enable d/><data id="OSAllowDRA_Name" value="true"/><dat a id="OSRecoveryPasswordUsageDropDown_Name" val ue="2"/><data id="OSRecoveryKeyUsageDropDown_N ame" value="2"/><data id="OSHideRecoveryPage_N ame" value="false"/><data id="OSActiveDirectoryBackup_ Name" value="true"/><data id="OSActiveDirectoryBack upDropDown_Name" value="1"/><data id="OSRequire ActiveDirectoryBackup_Name" value="true"/>
BitLocker	RequireDeviceEncryption	0	1	device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	AllowArchiveScanning	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	RealTimeScanDirection	0		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	AllowEmailScanning	0		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	AllowOnAccessProtection	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	AllowIntrusionPreventionSystem	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	PUAProtection	0		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=2
Defender	AVGCPULoadFactor	50		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=50
Defender	CloudProtection	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1

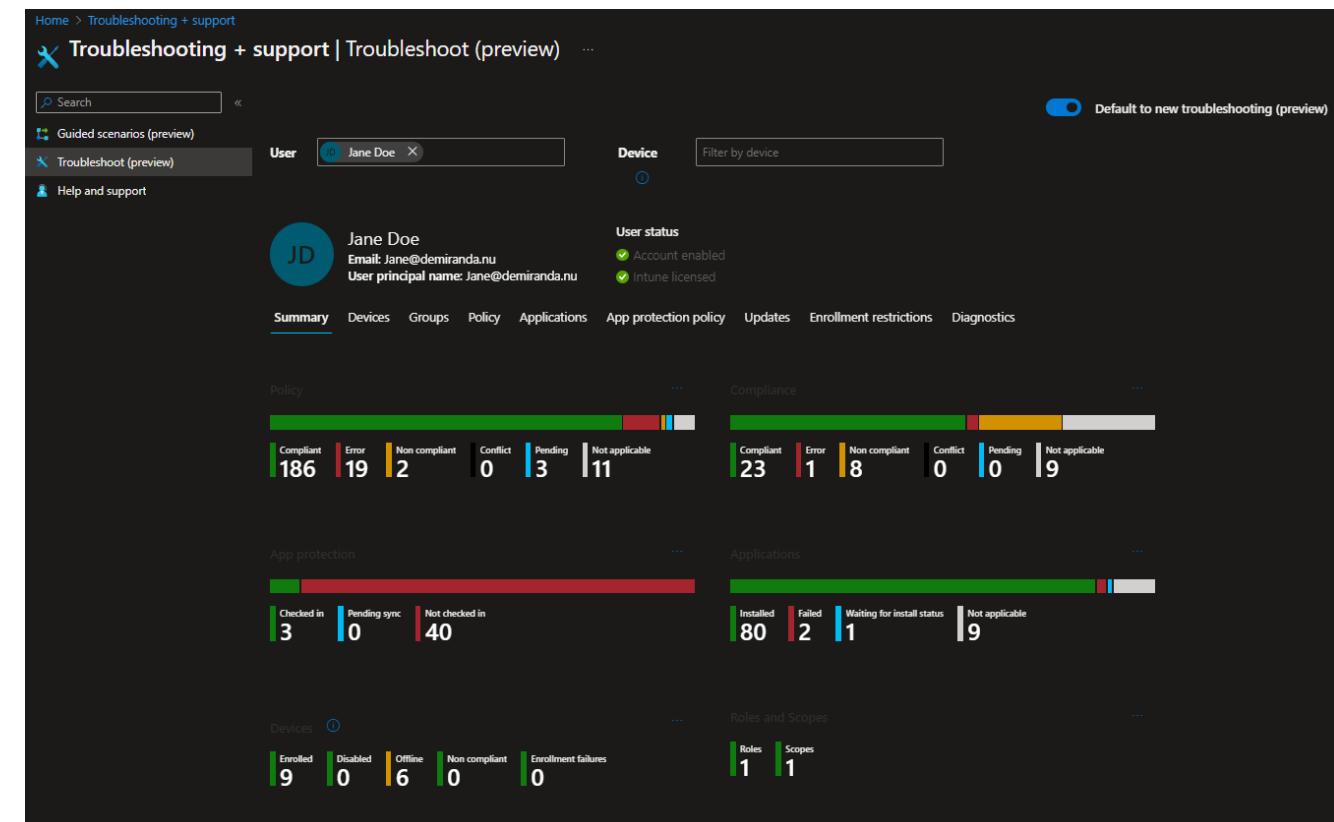
# Intune Troubleshooting Pane

Intune portal page

- <https://aka.ms/intunetroubleshooting>

Displays information focused around a particular user

- See info about assignments, devices, enrollment failures, etc.



For more info:

<https://docs.microsoft.com/en-us/intune/help-desk-operators>



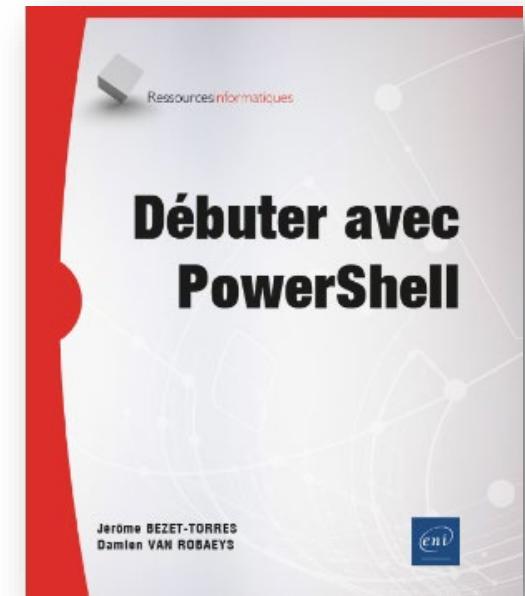
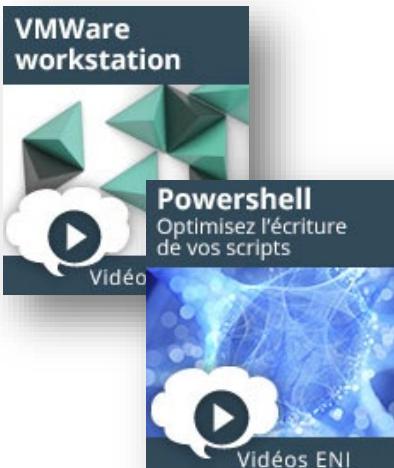
Thank You





# Livres et formations

workplaceninjas.fr  
#WPNinjasFRA



A paraître Avril 2023