Workplace Ninja France

Unlocking the secrets of Intune troubleshooting
A deep dive into mastery

workplaceninjas.fr @WPNinjasFRA

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
- Twitter: @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
- Twitter: @ccmexec

Agenda

- Remote Control / Remote Help
- Tools and Log Files
- Troubleshooting Configuration Policies
- Troubleshooting Subscription based activaton
- 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

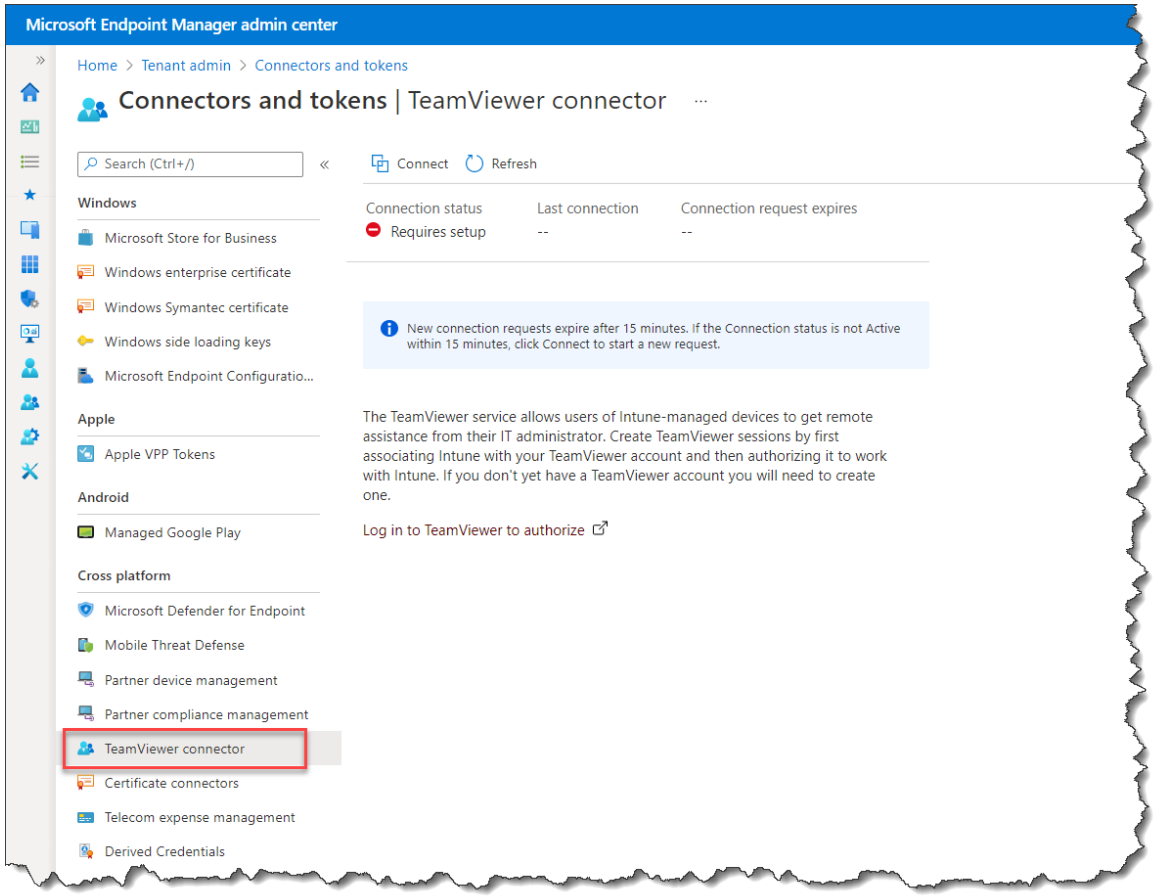
https://oliverkieselbach.com/2020/03/03/quick-assist-the-built-in-remote-control-in-windows-10/

Configure the TeamViewer Connector

- Easy setup and configuration

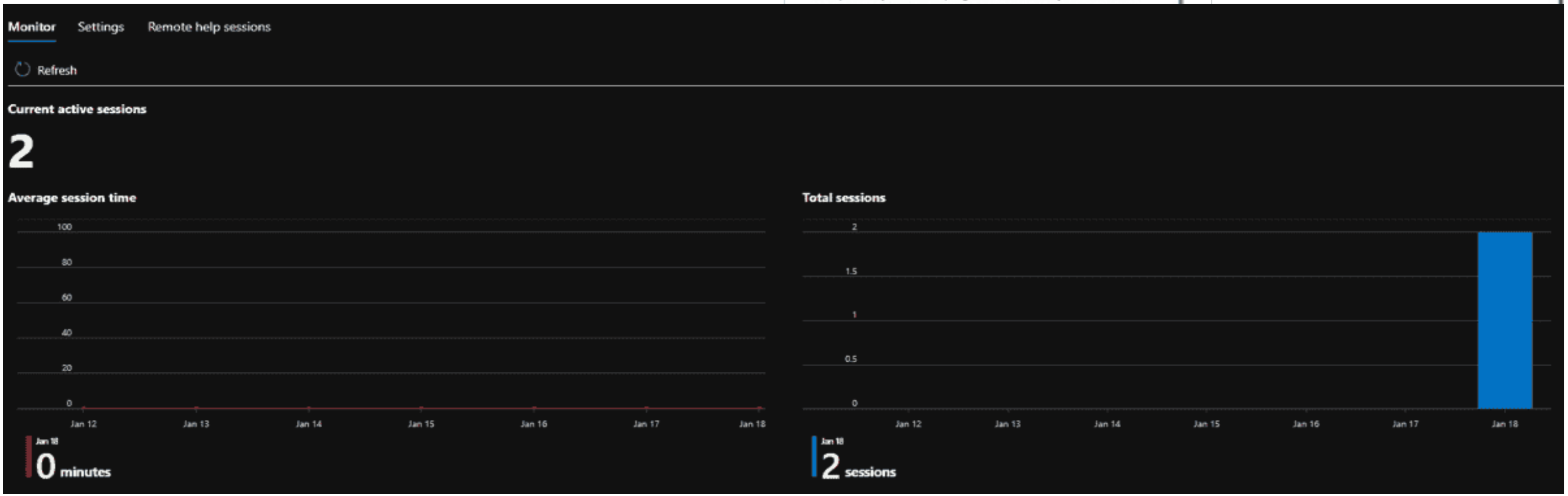
- There are other options:
  - Beyond Trust
  - LogMeIn
  - Remote Help!

... 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



Remote Troubleshooting

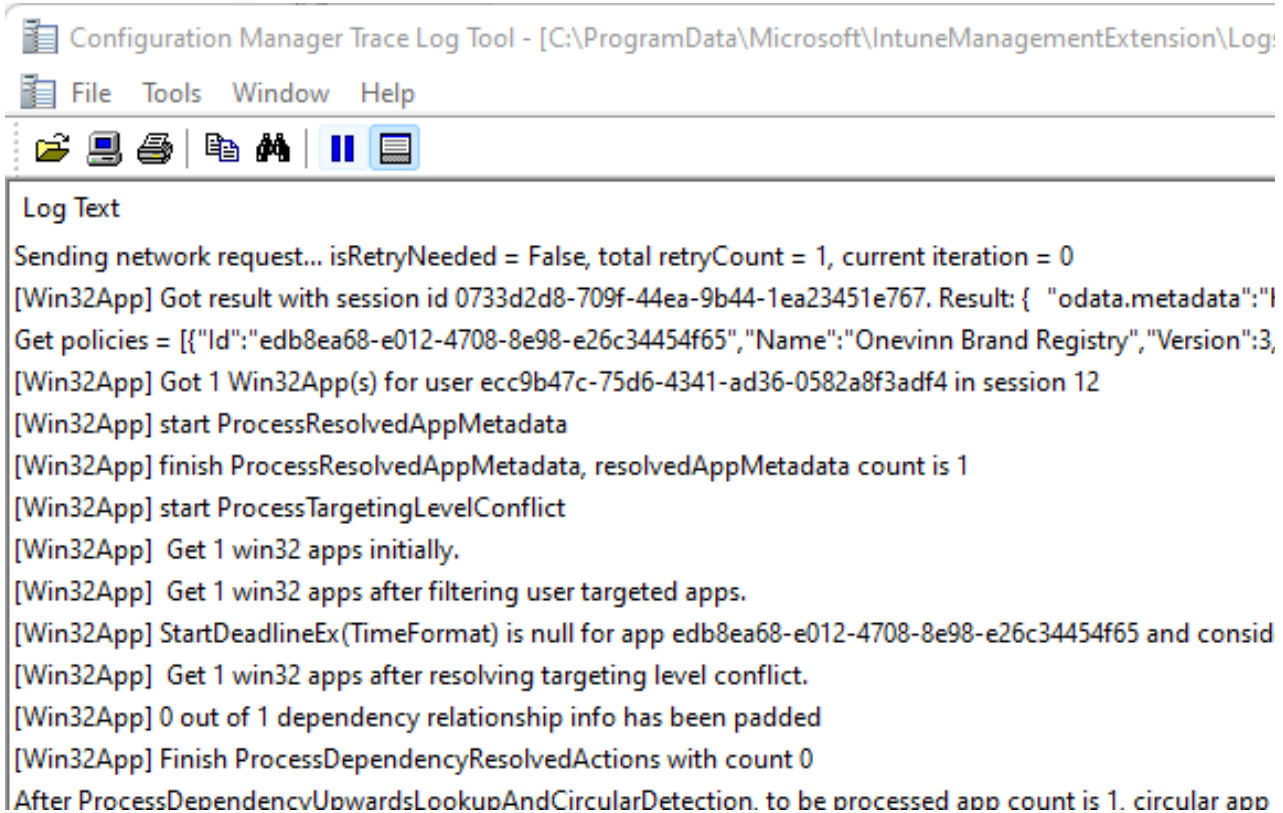
- Customer quote:

  “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

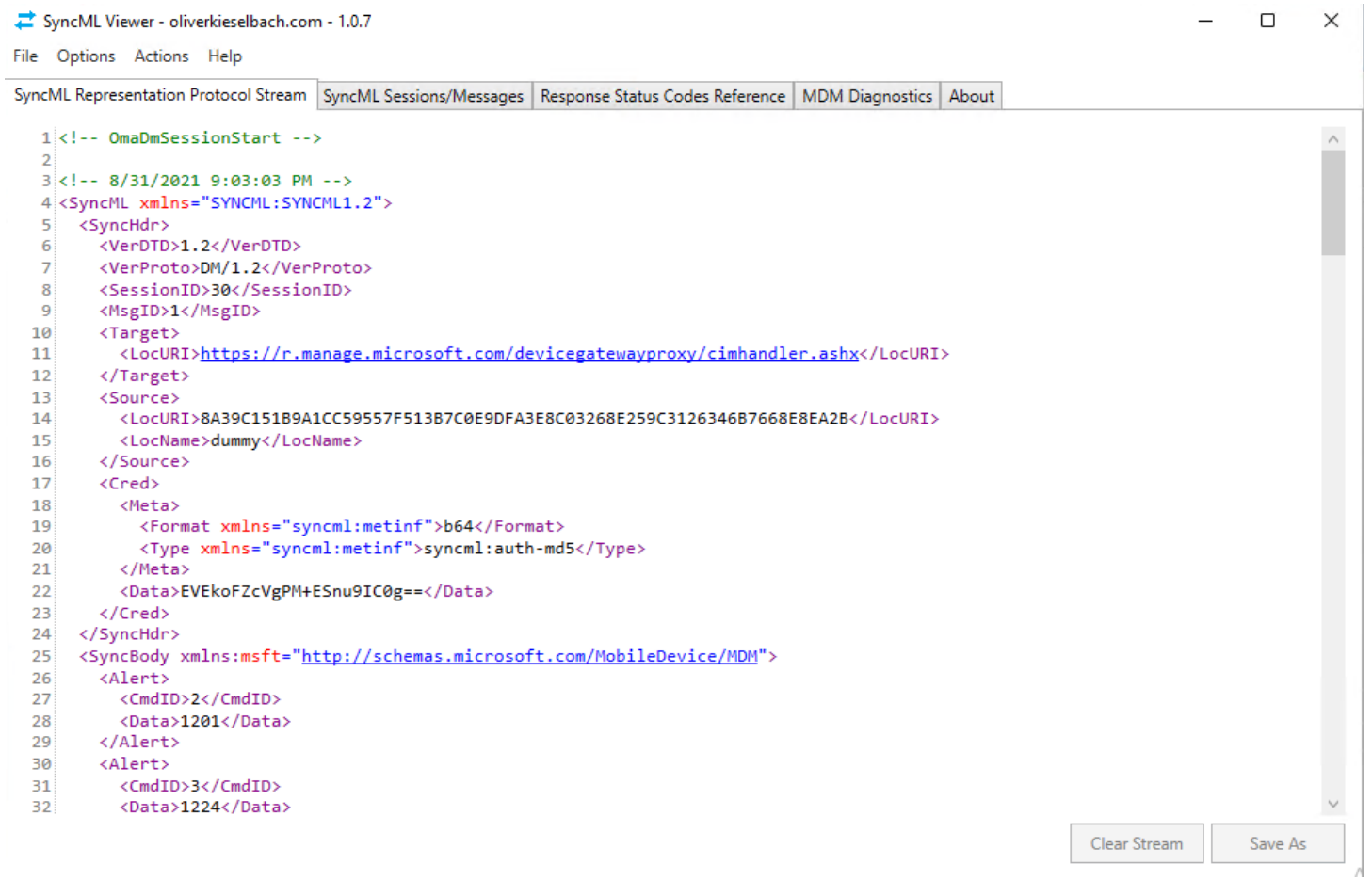
- Great log reader
- Not free but included in the Intune/MEM license
- Deploy it to all clients



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

More Tools – Advanced Troubleshooting

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



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

SyncMLViewer

```
1533    <Status>
1534      <CmdID>32</CmdID>
1535      <MsgRef>2</MsgRef>
1536      <CmdRef>25</CmdRef>
1537      <Cmd>Get</Cmd>
1538      <Data>200</Data>
1539    </Status>
1540    <Results>
1541      <CmdID>33</CmdID>
1542      <MsgRef>2</MsgRef>
1543      <CmdRef>25</CmdRef>
1544      <Item>
1545        <Source>
1546          <LocURI>./DevDetail/Ext/DeviceHardwareData</LocURI>
1547        </Source>
1548        <Data>T0EeBAEAHAAAAAoAMwDwVQAACgAaAfBVCnofKQQCCQgCABAACQABAAEAAgABAAAABQAZAAQAAAAAAAAAAAgAAAAAAACAAEAAwMAEQBHZW51aW5lSW50ZWwABAA0AEludGVsKFIpIENvcmUoVE0pIGk3LTg1NTlV
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>
```

LOG FILES

Collect diagnostics from a Windows Device

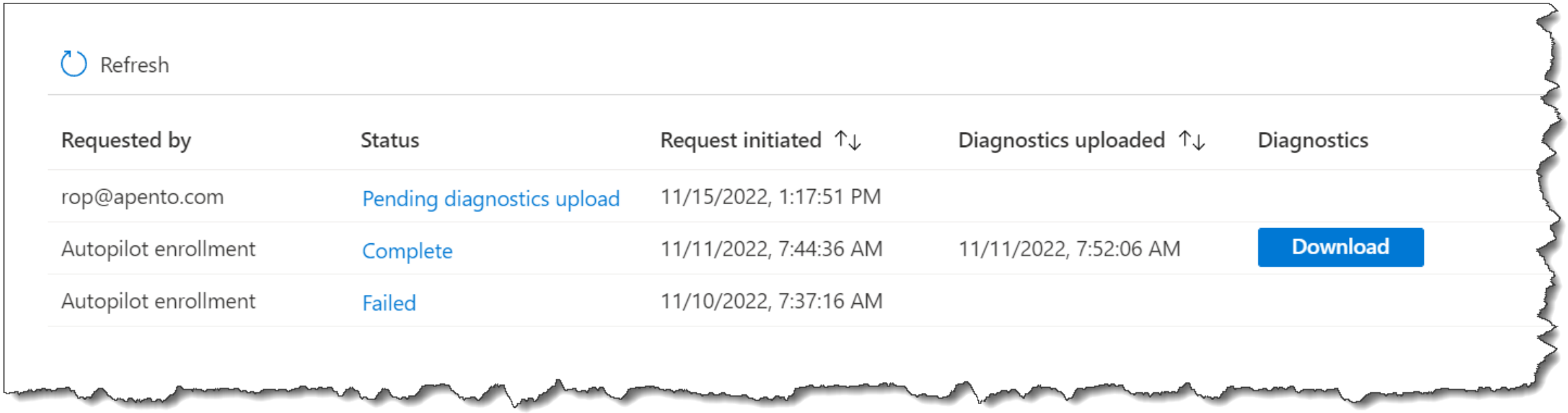
- Collecting Diagnostic Logs from Windows Devices
  - Windows 10 1909 and later
  - Windows 11
  - HoloLens 2 2004 and later
  - Both Intune and Co-Managed devices
  - Corporate-owned devices
  - Stored for 28 days and then deleted (up to 10 collections)
  - Bulk action (up to 25 devices)

- Upload URL:
  - lgmsapeweu.blob.core.windows.net

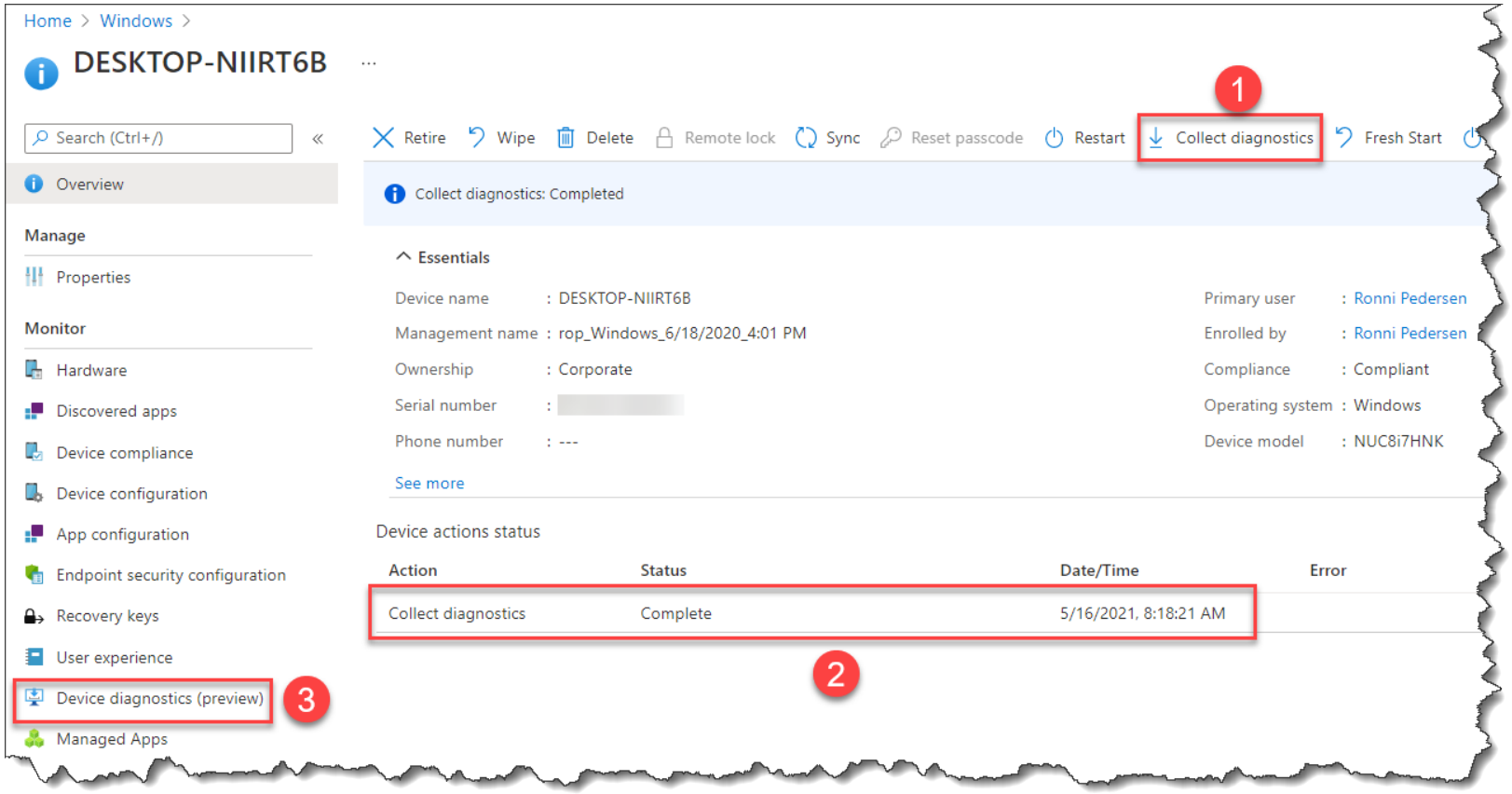
- More information:
  - https://docs.microsoft.com/en-us/mem/intune/remote-actions/collect-diagnostics

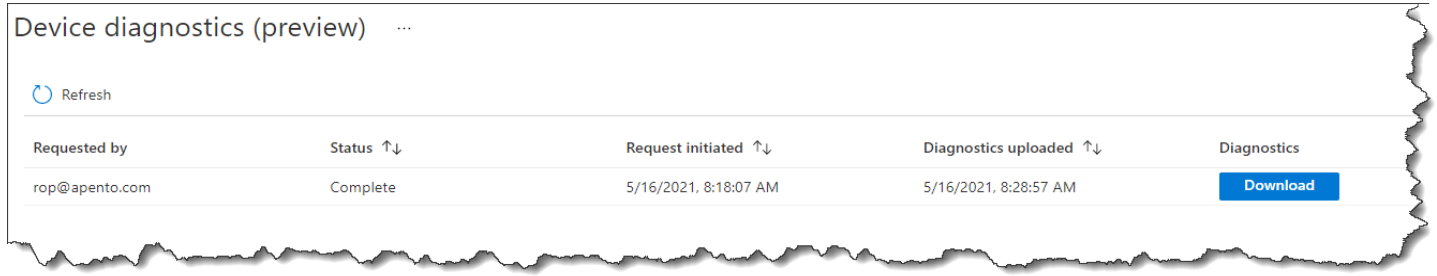
Device Diagnostics

- Autopilot enrollment failure



Collecting Diagnostic Logs





CONFIGURATION POLICY PROCESS

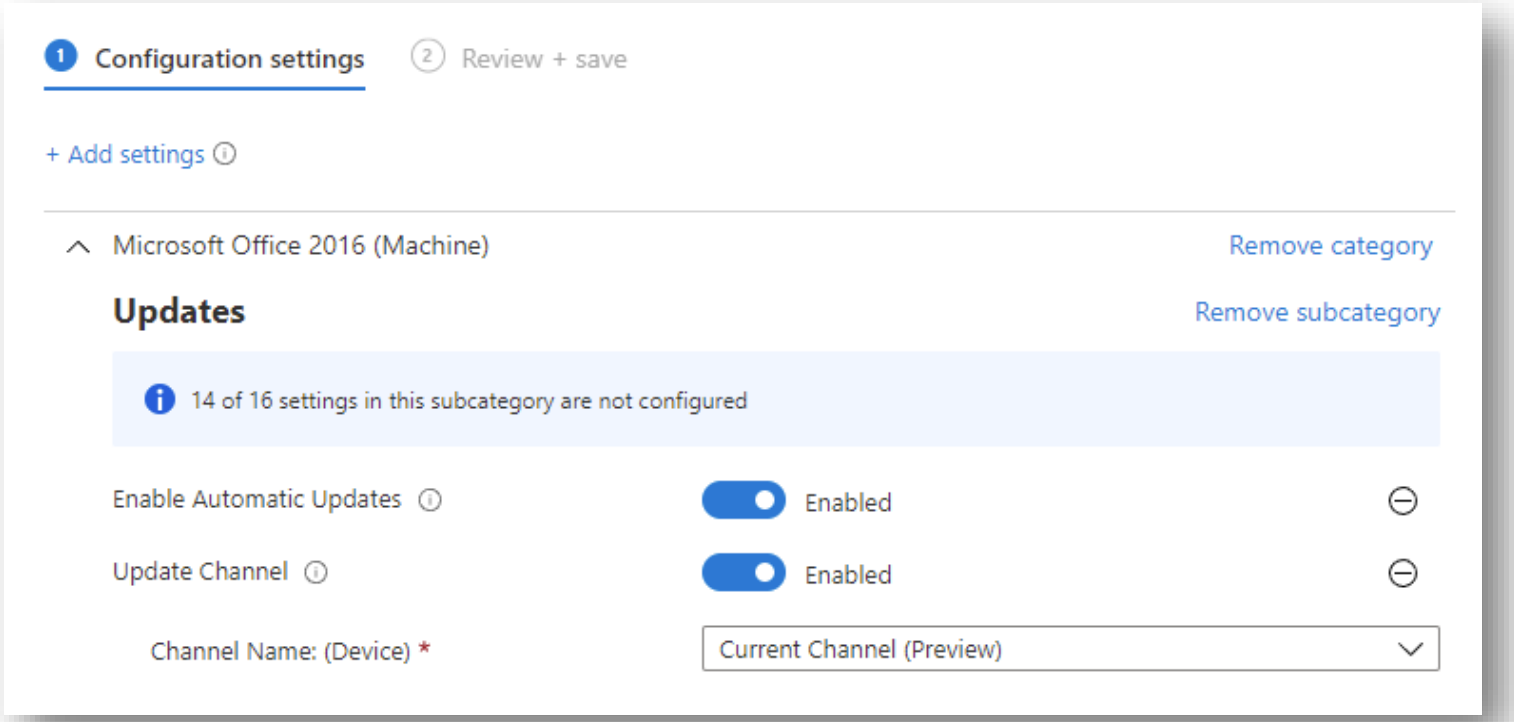
Microsoft 365 Apps Policy

- 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

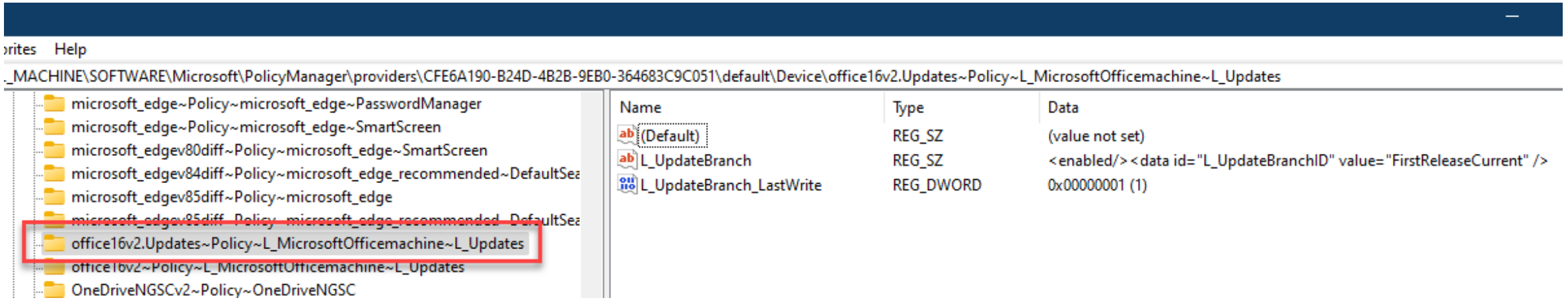
Use Settings Catalog

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



#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.

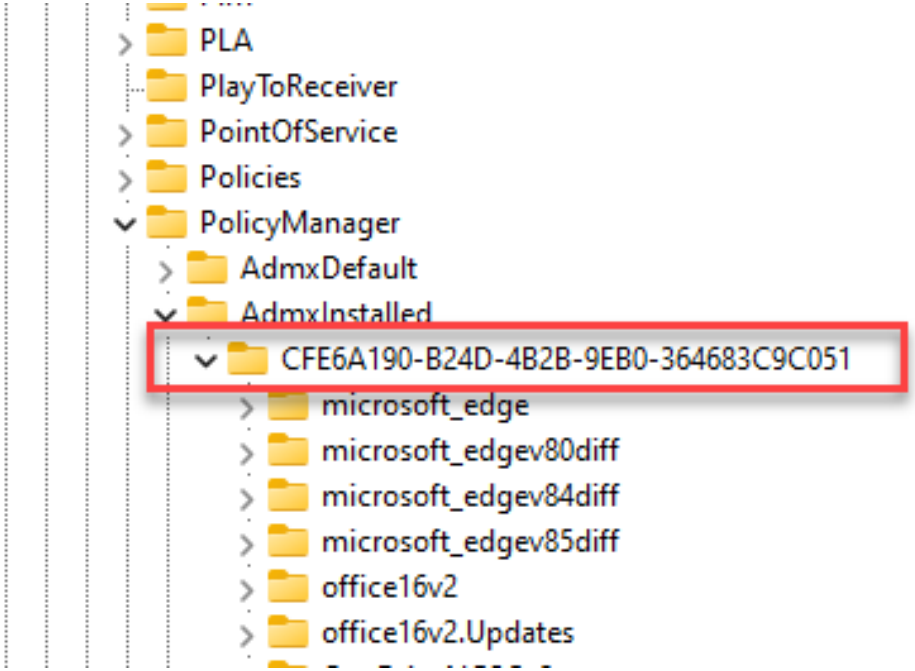


Find the Provider ID

Find the provider ID for your device

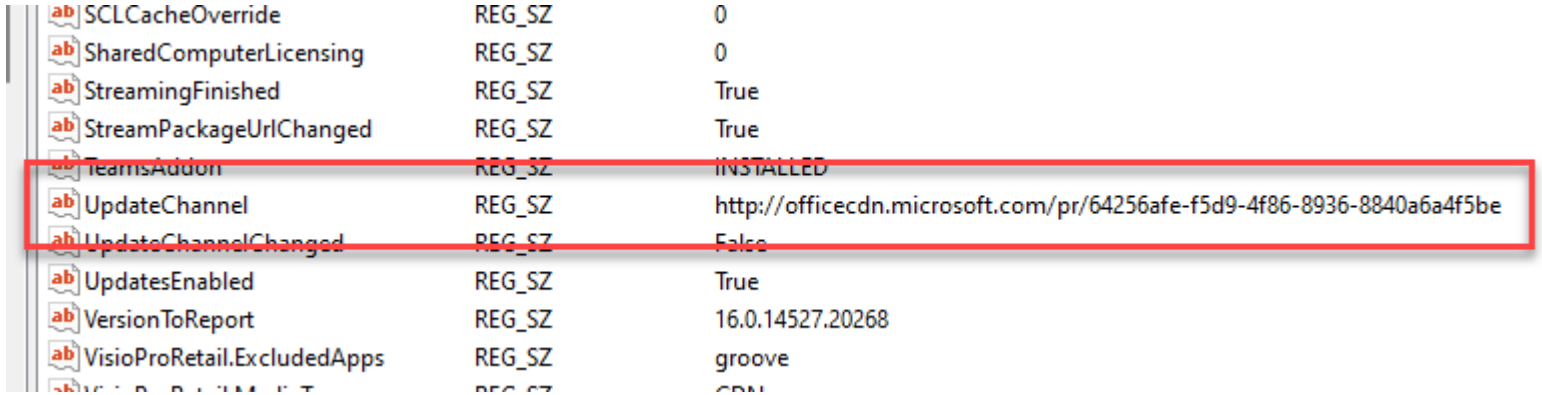
- Open the Registry Editor, and go to:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\AdmxInstalled



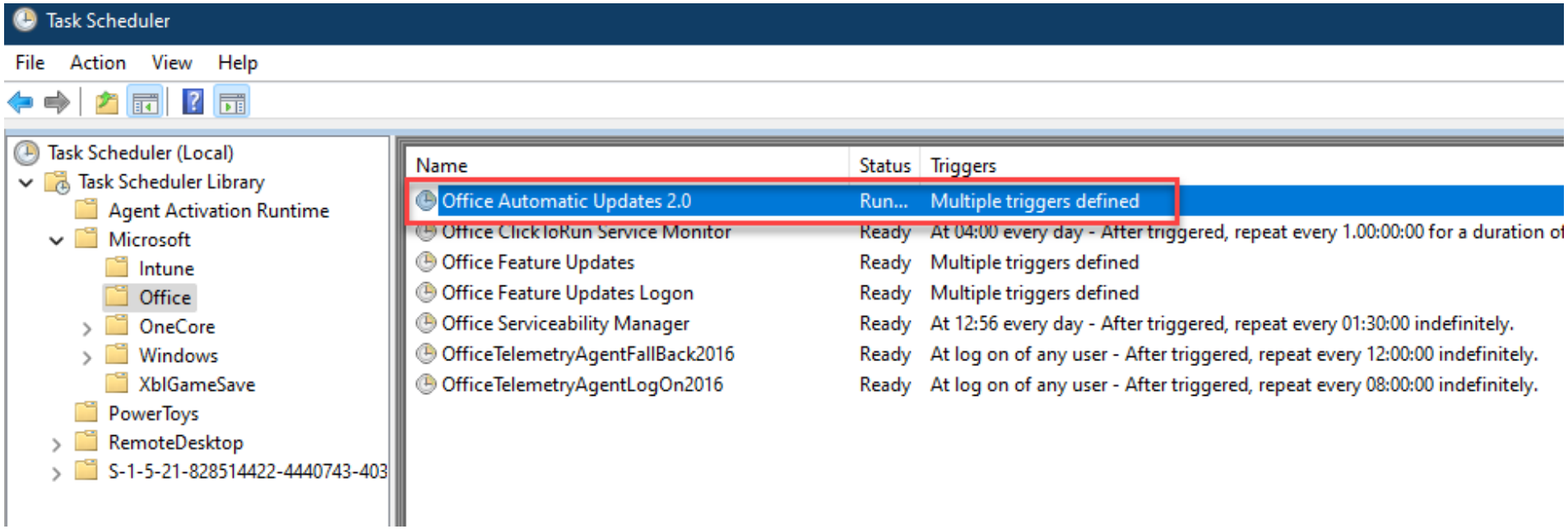
#2 Check the Office registry keys

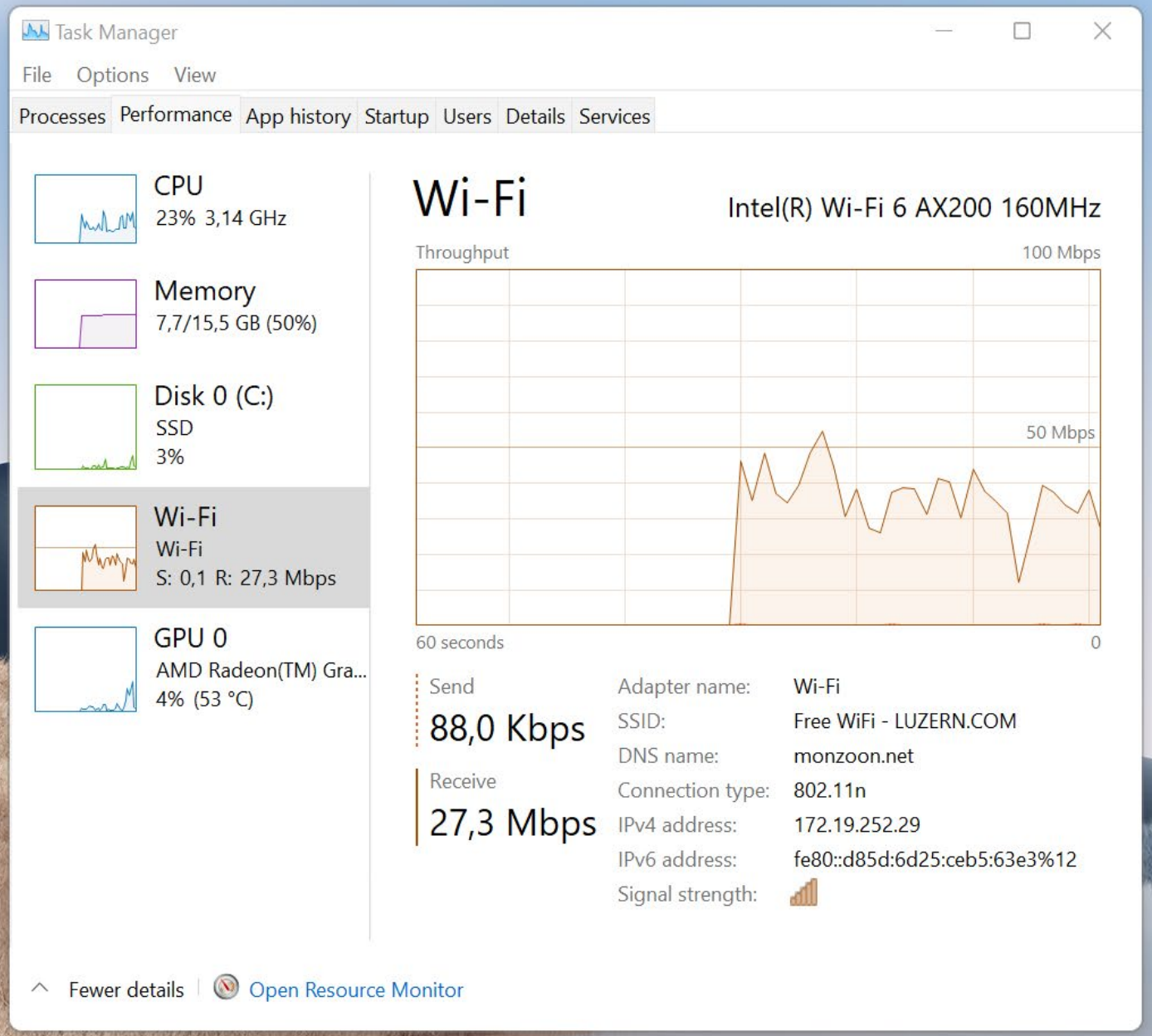
- Go to the Office policy path:
  Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\Configuration
- Check the UpdateChannel value:
  - Monthly Enterprise Channel = 55336b82-a18d-4dd6-b5f6-9e5095c314a6
  - Current Channel = 492350f6-3a01-4f97-b9c0-c7c6ddf67d60
  - Current Channel (Preview) = 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

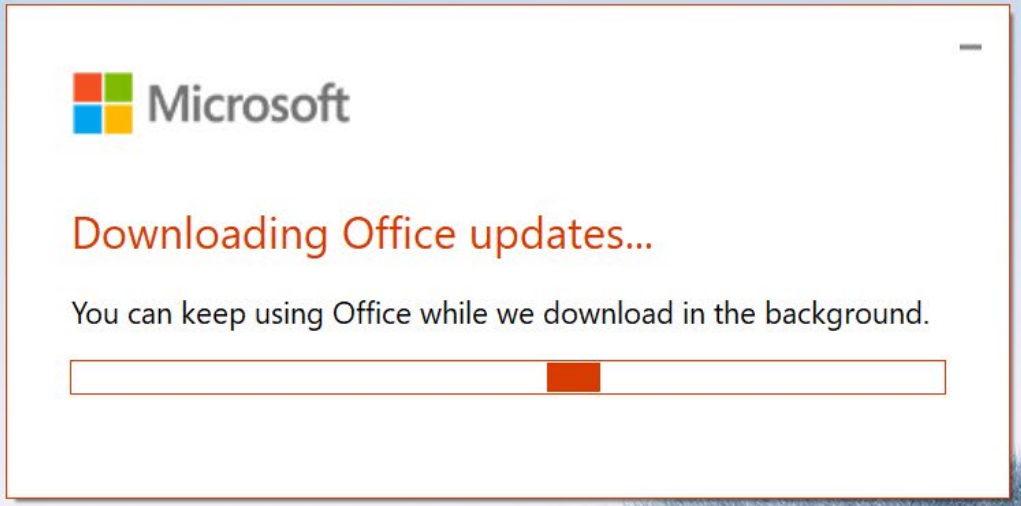


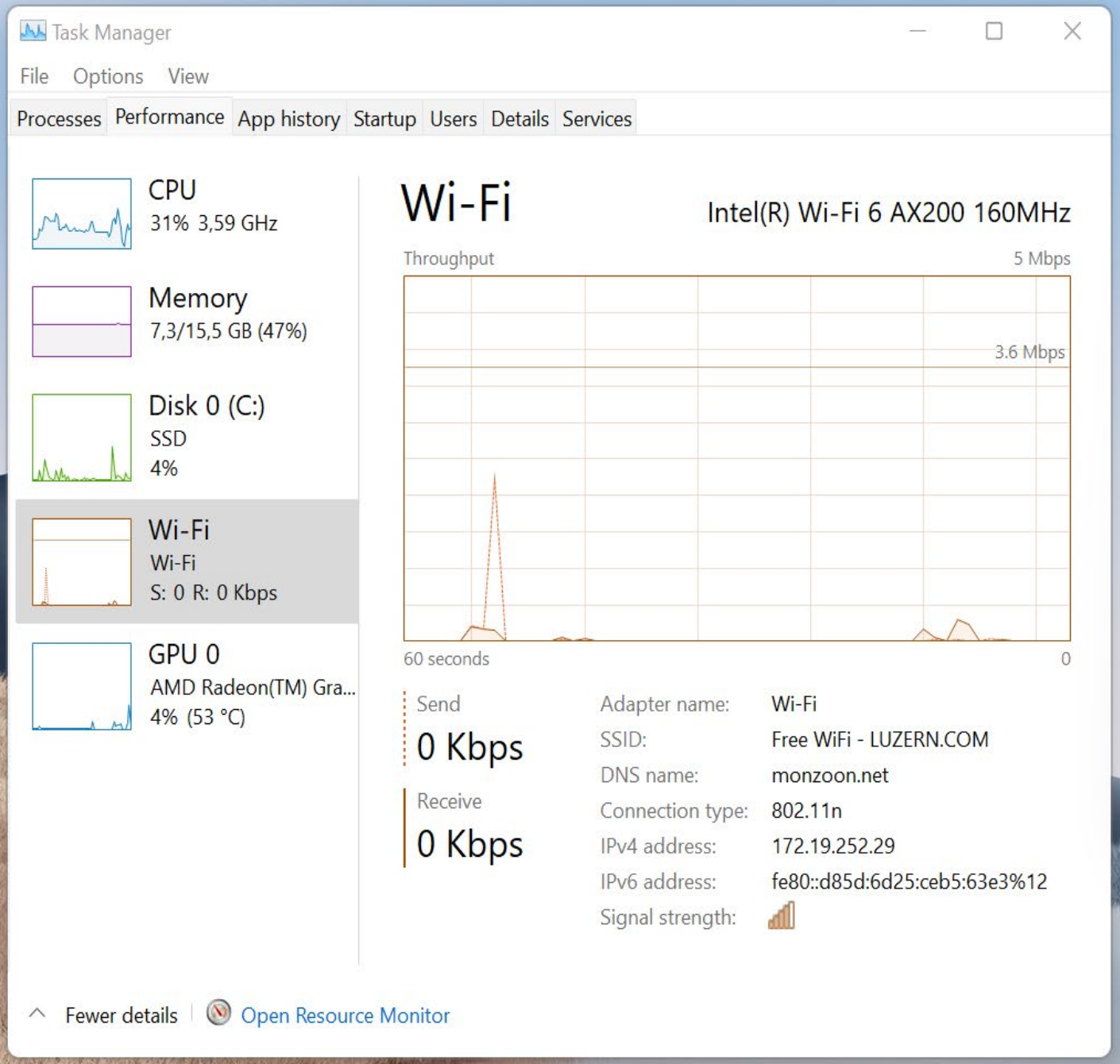
#3 Force Office automatic updates to run

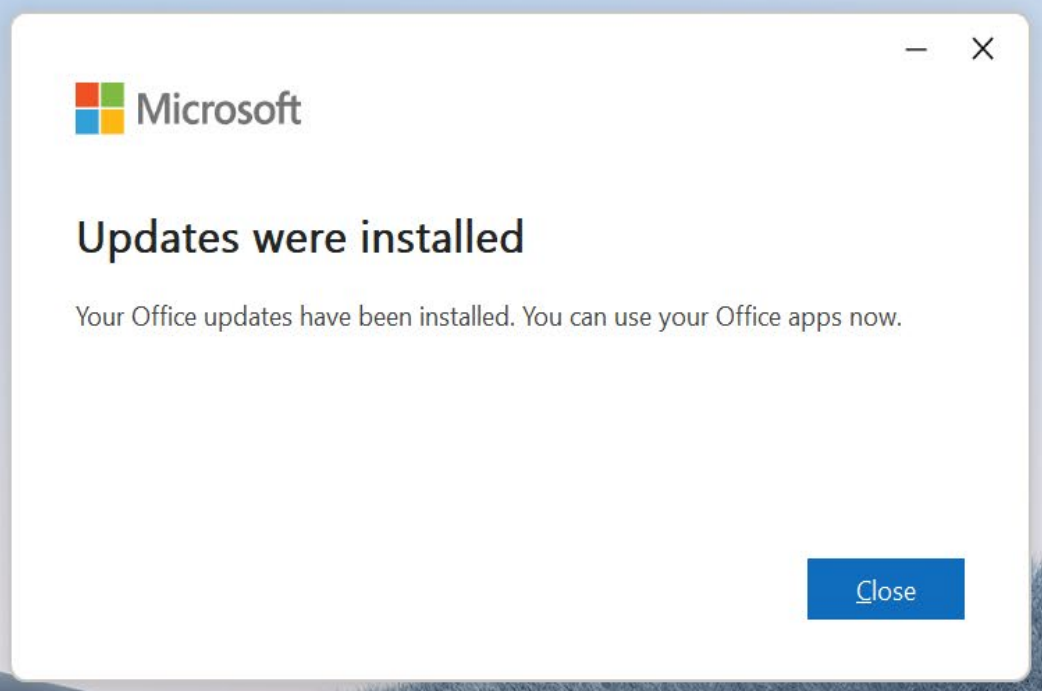
- To test the policy, we can force the policy settings on the device
  - Go to HKLM\SOFTWARE\Microsoft\Office\ClickToRun\Updates
  - Edit the UpdateDetectionLastRunTime key > delete the value data.
  - Launch Task Secheduler > Microsoft > Office
    - Run "Office Automatic Updates 2.0"




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
100 Mbps
50 Mbps
60 seconds
0
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


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

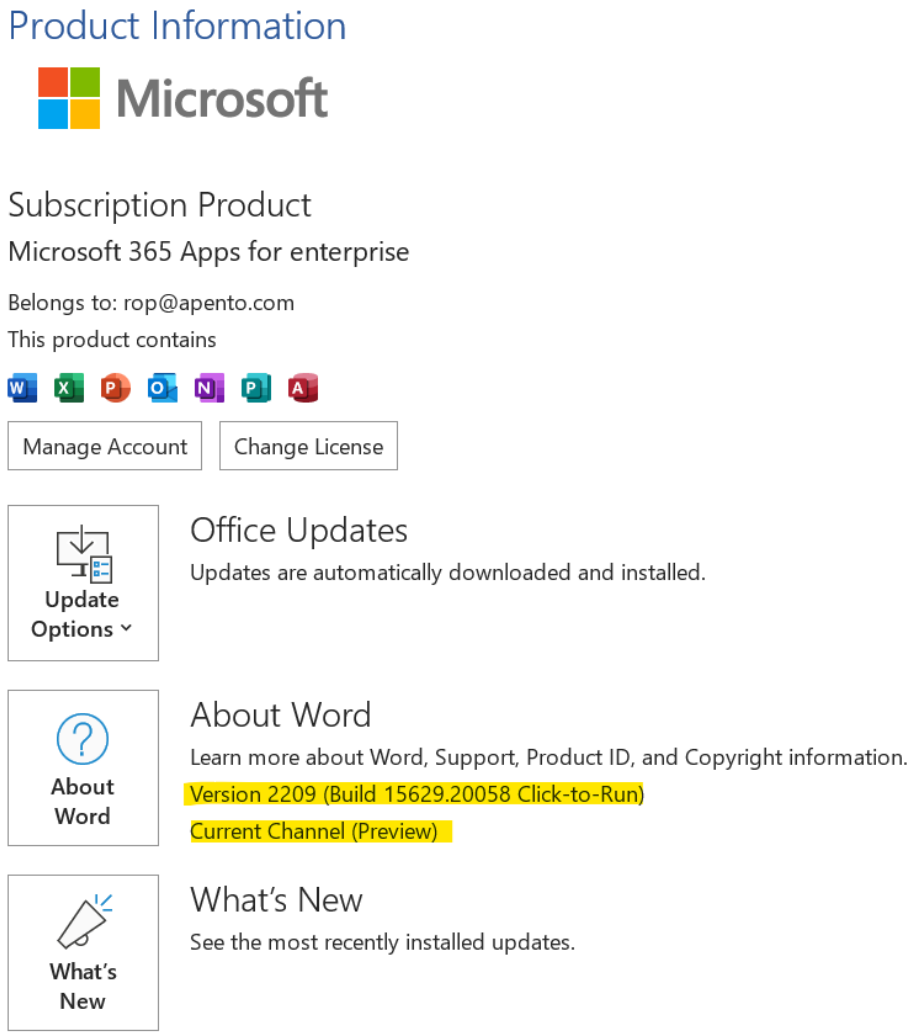

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
31% 3,59 GHz
Memory
7,3/15,5 GB (47%)
Disk 0 (C:)
SSD
4%
Wi-Fi
Wi-Fi
S: 0 R: 0 Kbps
GPU 0
AMD Radeon(TM) Gra...
4% (53 °C)
Wi-Fi
Intel(R) Wi-Fi 6 AX200 160MHz
Throughput
5 Mbps
3.6 Mbps
60 seconds
0
Send
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


Microsoft
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



TROUBLESHOOTING SUBSCRIPTION BASED ACTIVATION

Subscription Based activation

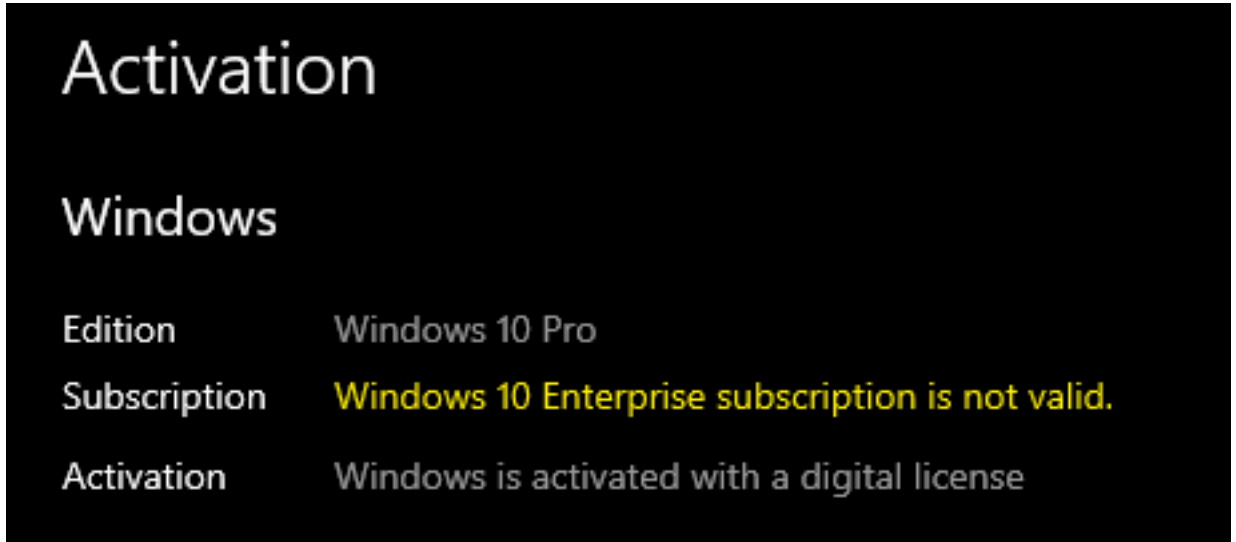
- Easiest way of upgrading to Enterprise from pro
- Re-activated every 30 days
- Each user can activate 5 devices
- Activating shared devices
  - Either all users must have a Windows e3 license assigned
  - Shared devices must be excluded and activated in a different way (KMS,MAK)

  HKEY_Local_Machine\System\Currentcontrolset\services\clipsvc\parameters

  Value: DisableSubscription Reg_Dword Value=1

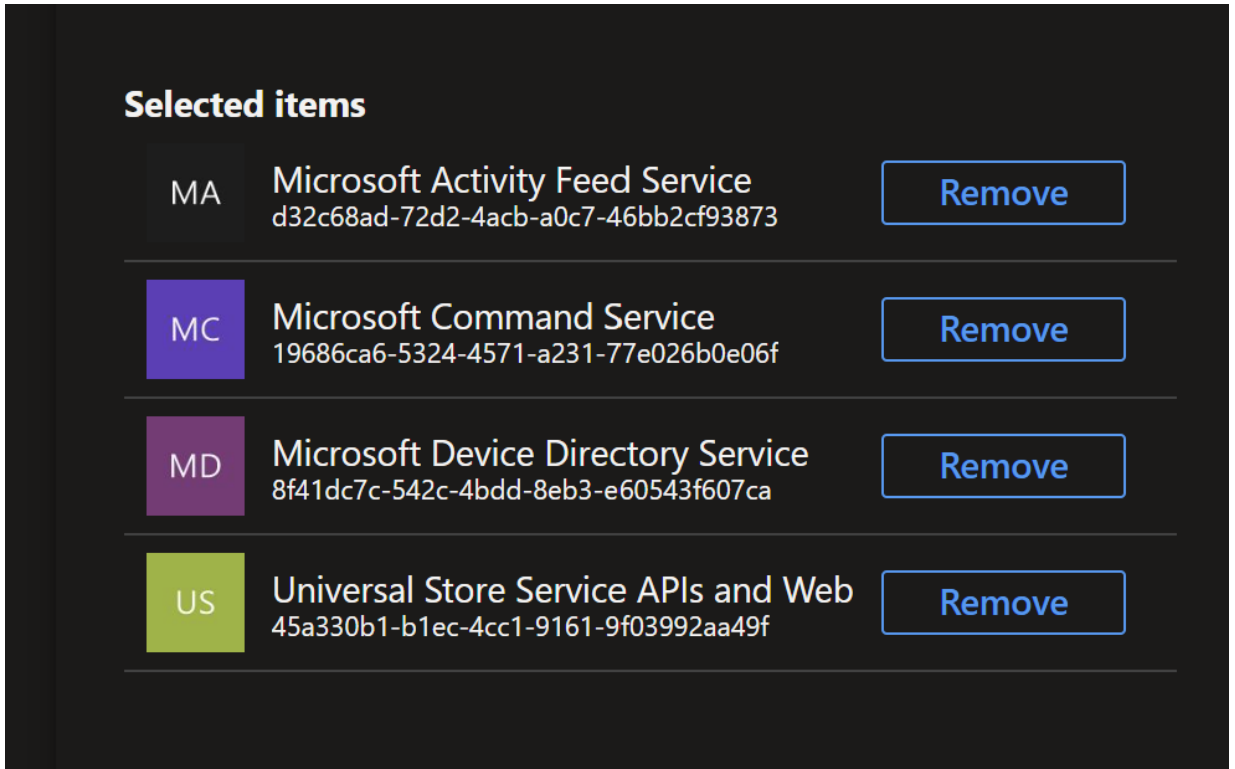
Subscription based activation

- 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.



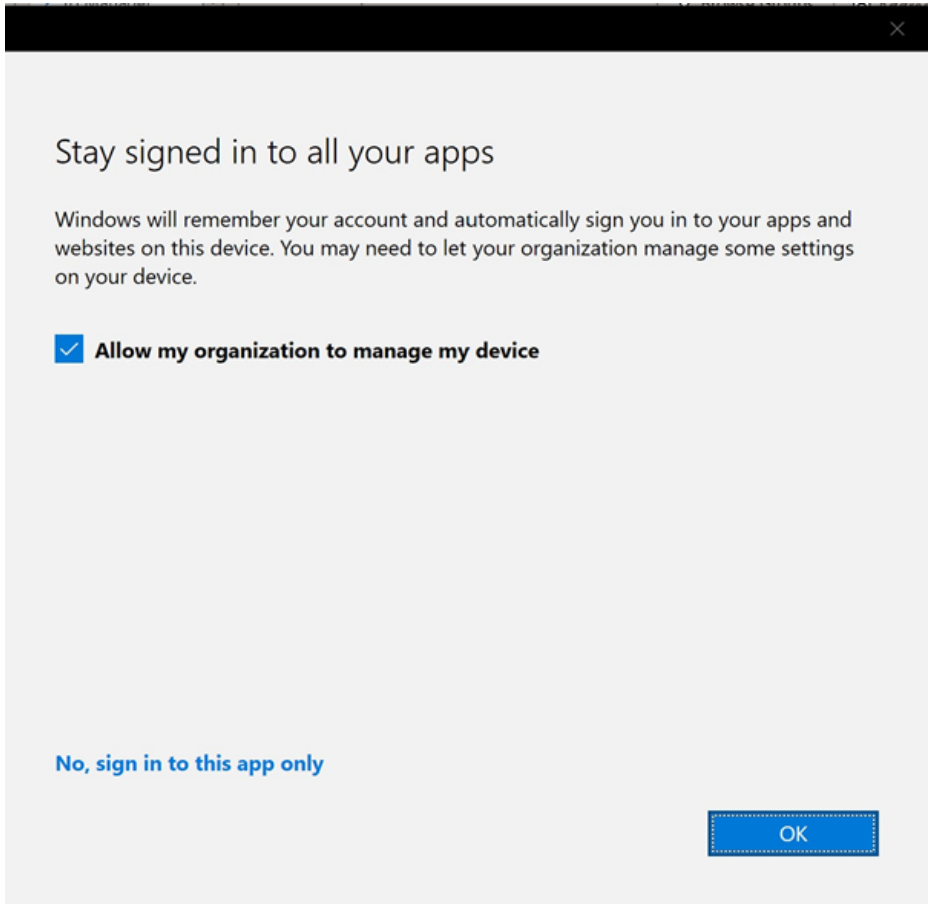
CA exclusions

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.



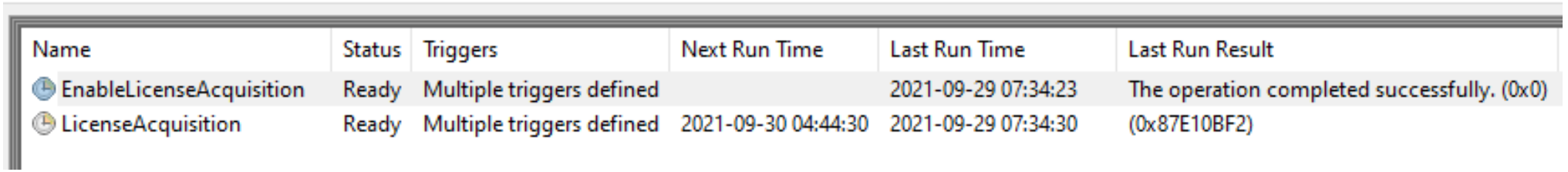
Stay signed in to all your apps = Evil

- "**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

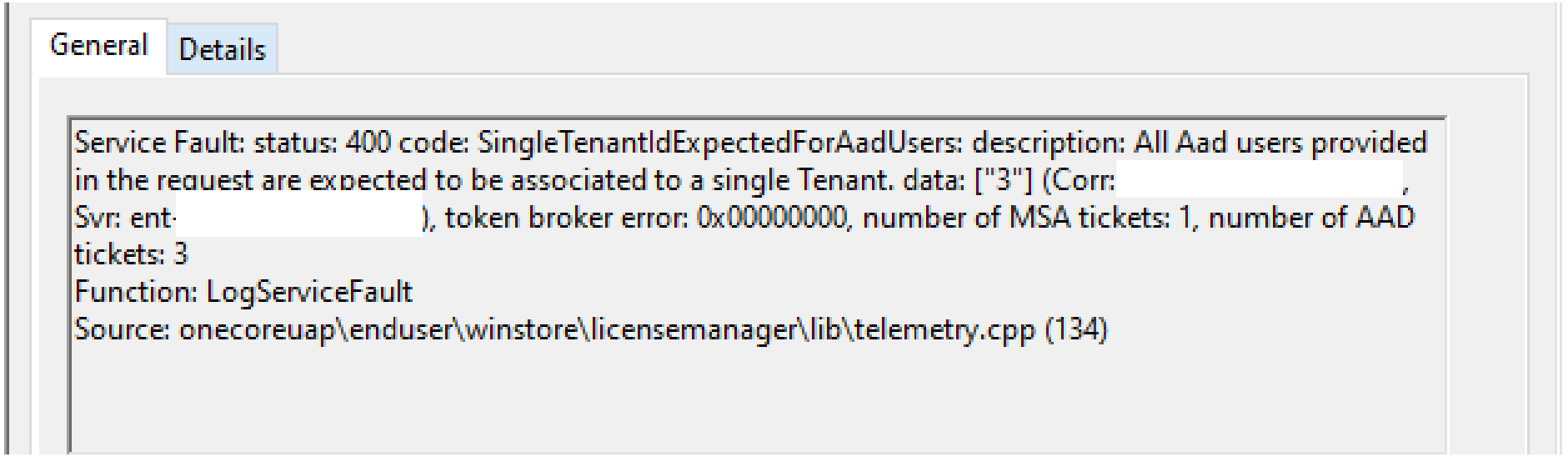


Subscription Based Activation

- 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)



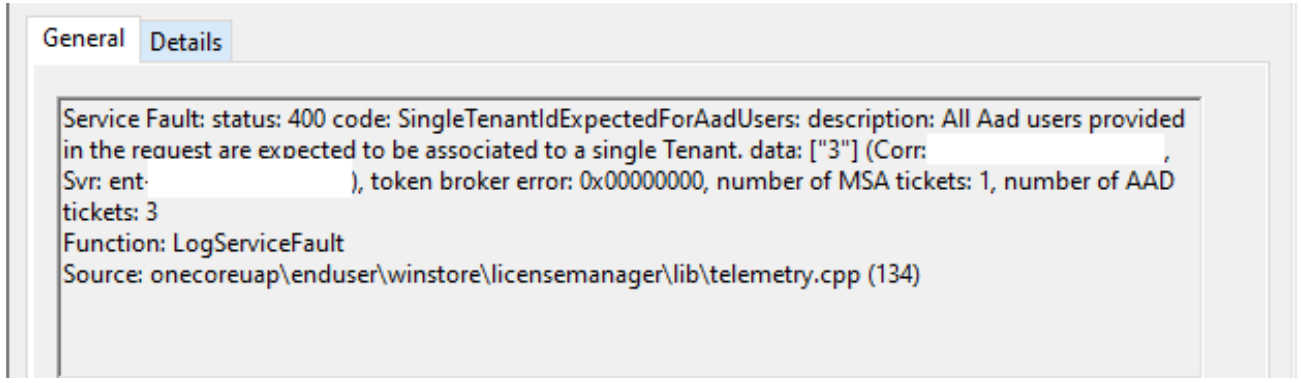
https://ccmexec.com/2021/01/mem-windows-10-personal-device-and-sync-issues/

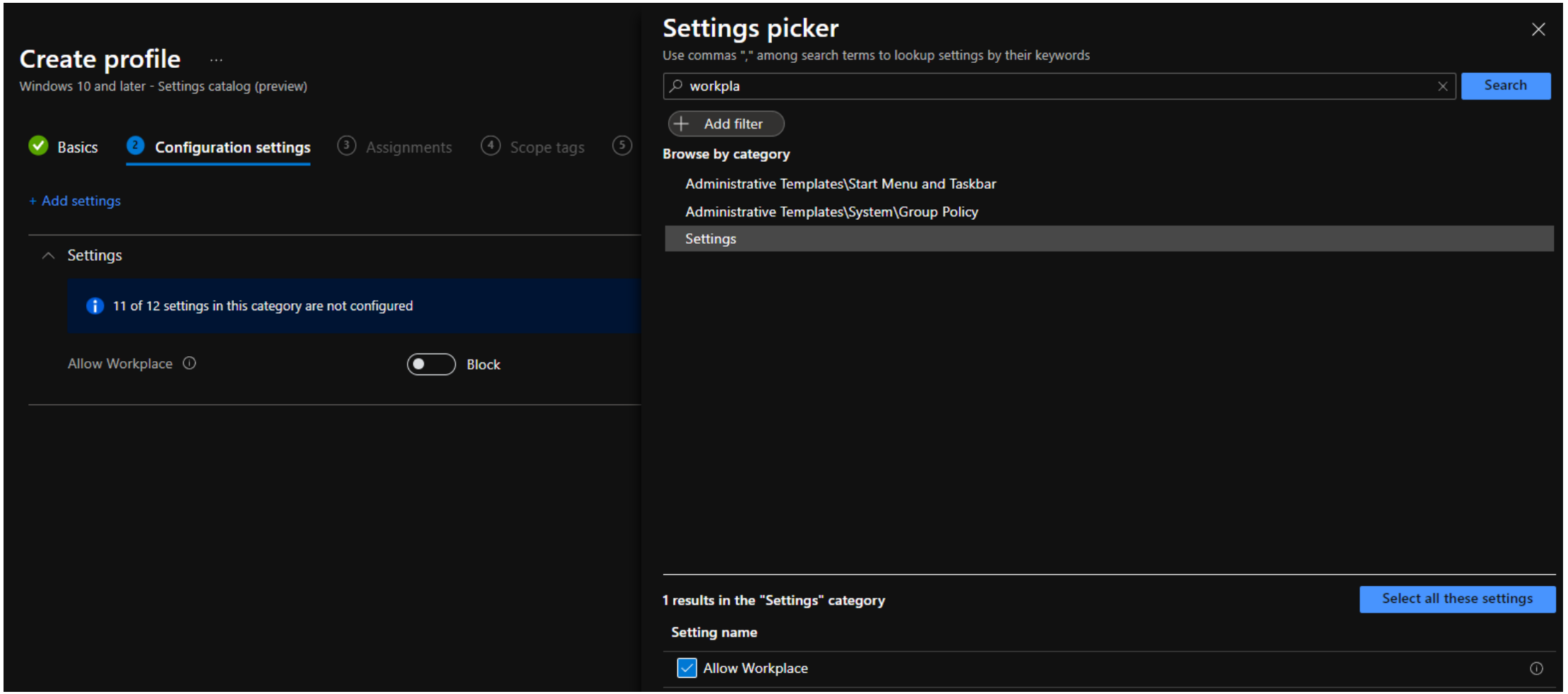
Subscription based activation

- 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)

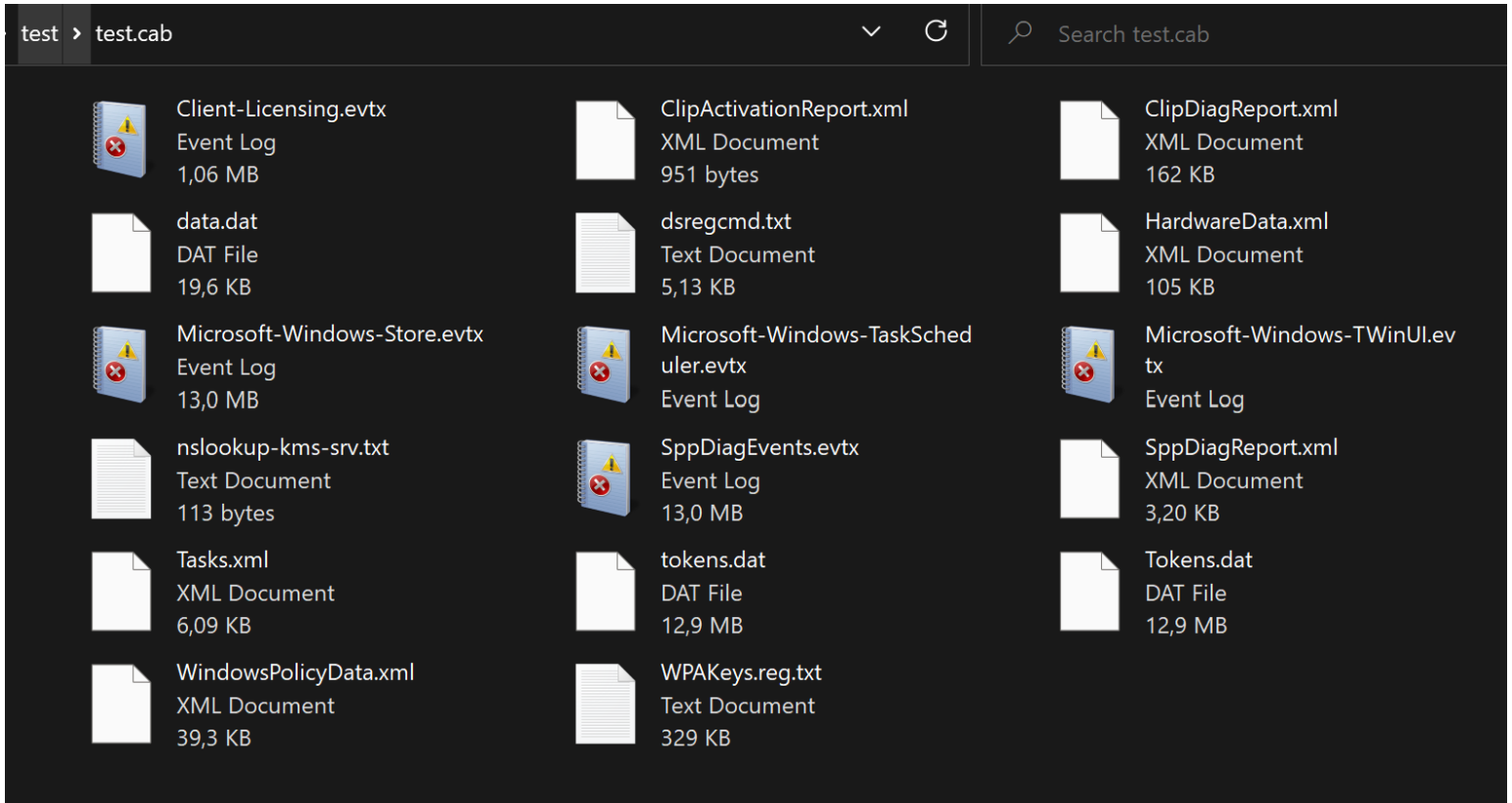
- The renewal is done using the StoreAPI
  - In this case more than one AzureAD account was added under ”Access work or School”




Create profile
Windows 10 and later - Settings catalog (preview)
Basics
2 Configuration settings
3 Assignments
4 Scope tags
5
+ Add settings
Settings
11 of 12 settings in this category are not configured
Allow Workplace
Block
Settings picker
Use commas "," among search terms to lookup settings by their keywords
workpla
Search
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
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

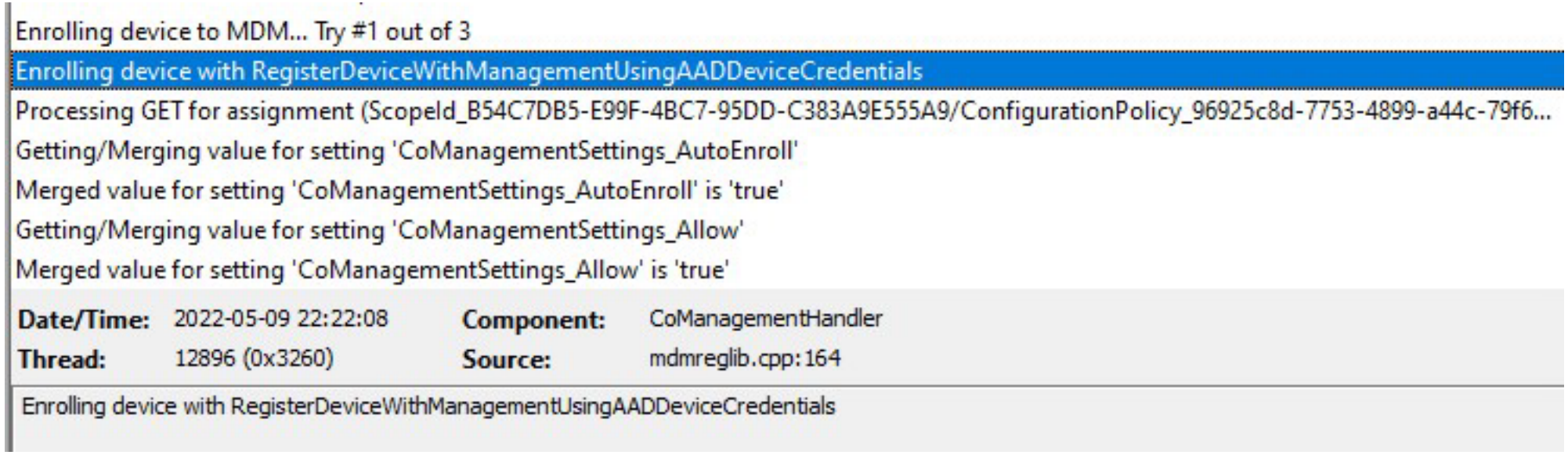
Hybrid Azure AD Join

- 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 users 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/

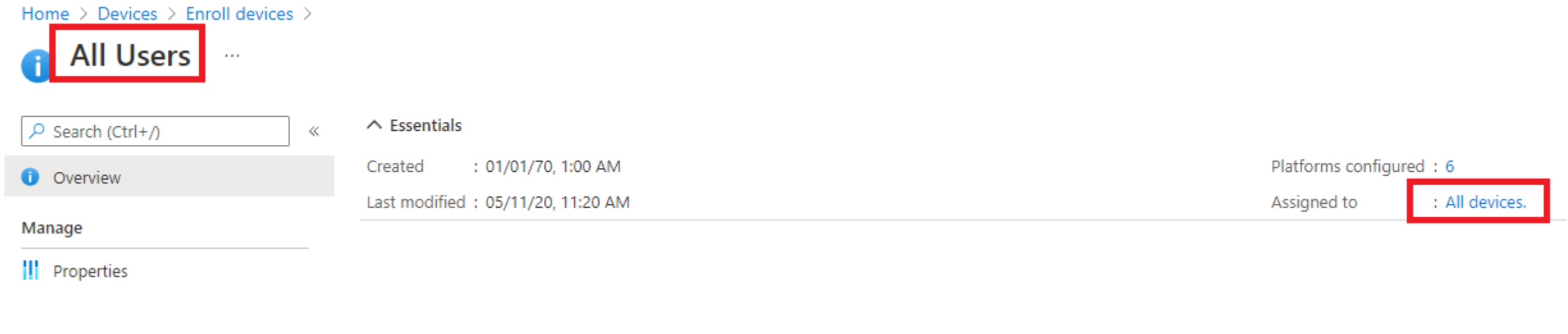
Co-Managed device enrollment

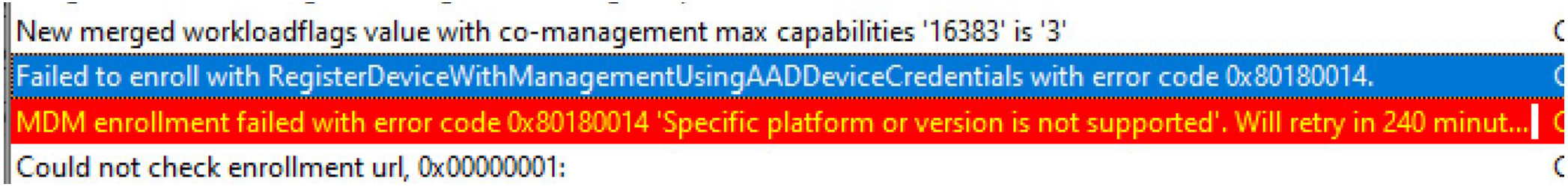
- Co-managed devices will always try to enroll using a Device token
- If it fails it will try using the user token, depending on MFA settings this can fail as well.



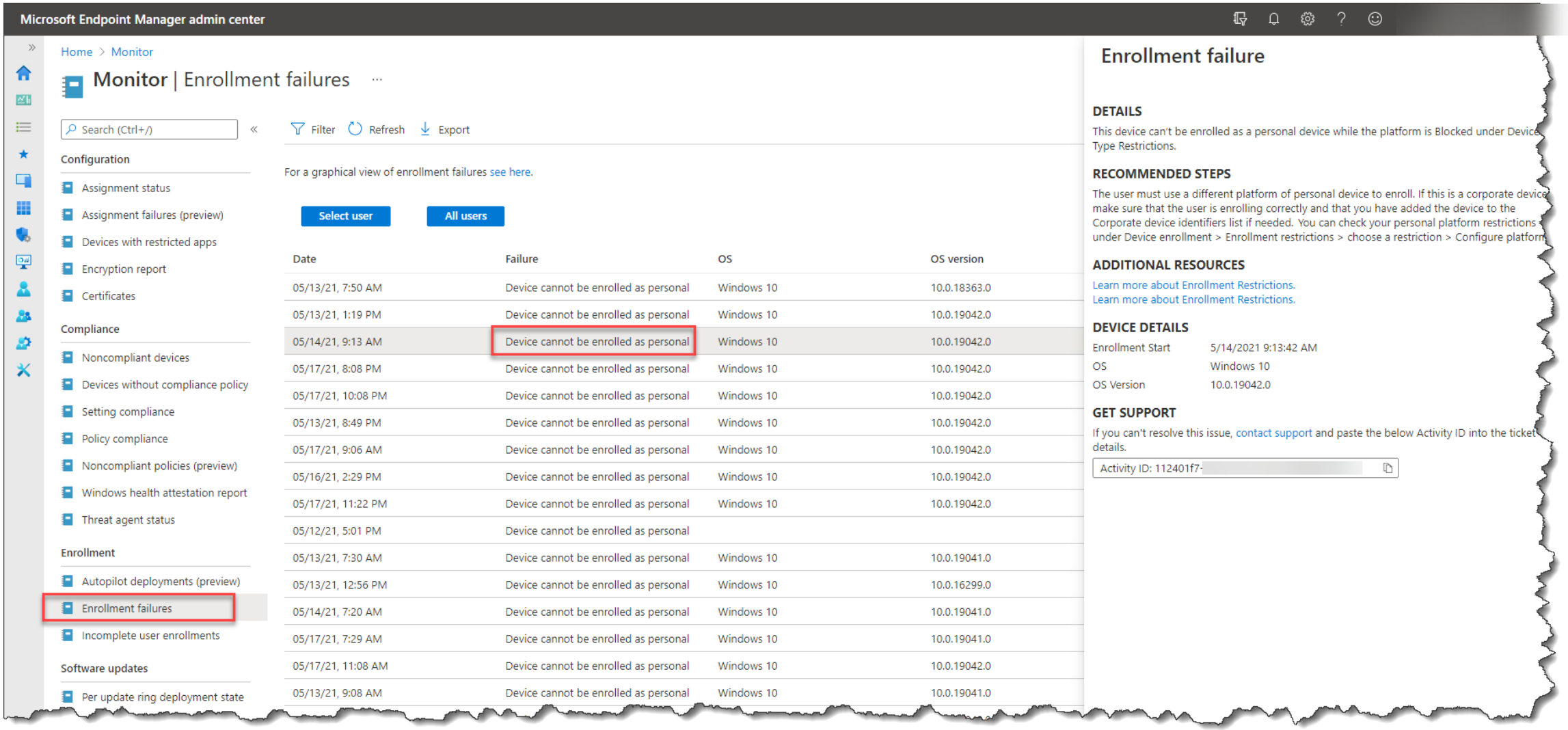
Enrollment restrictions and “All Users”

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

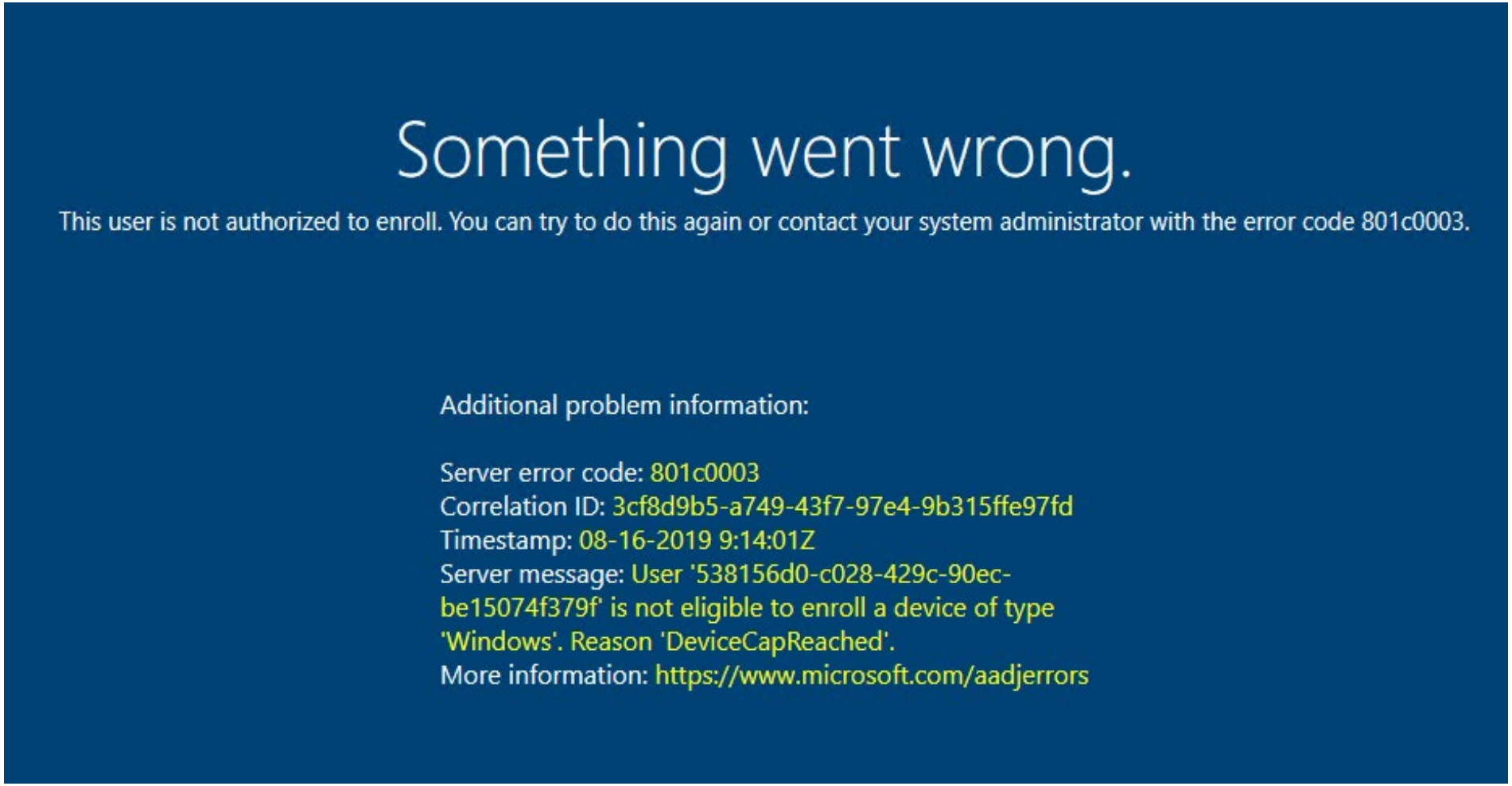




Enrollment Failures



DeviceCapReached = Device Limits



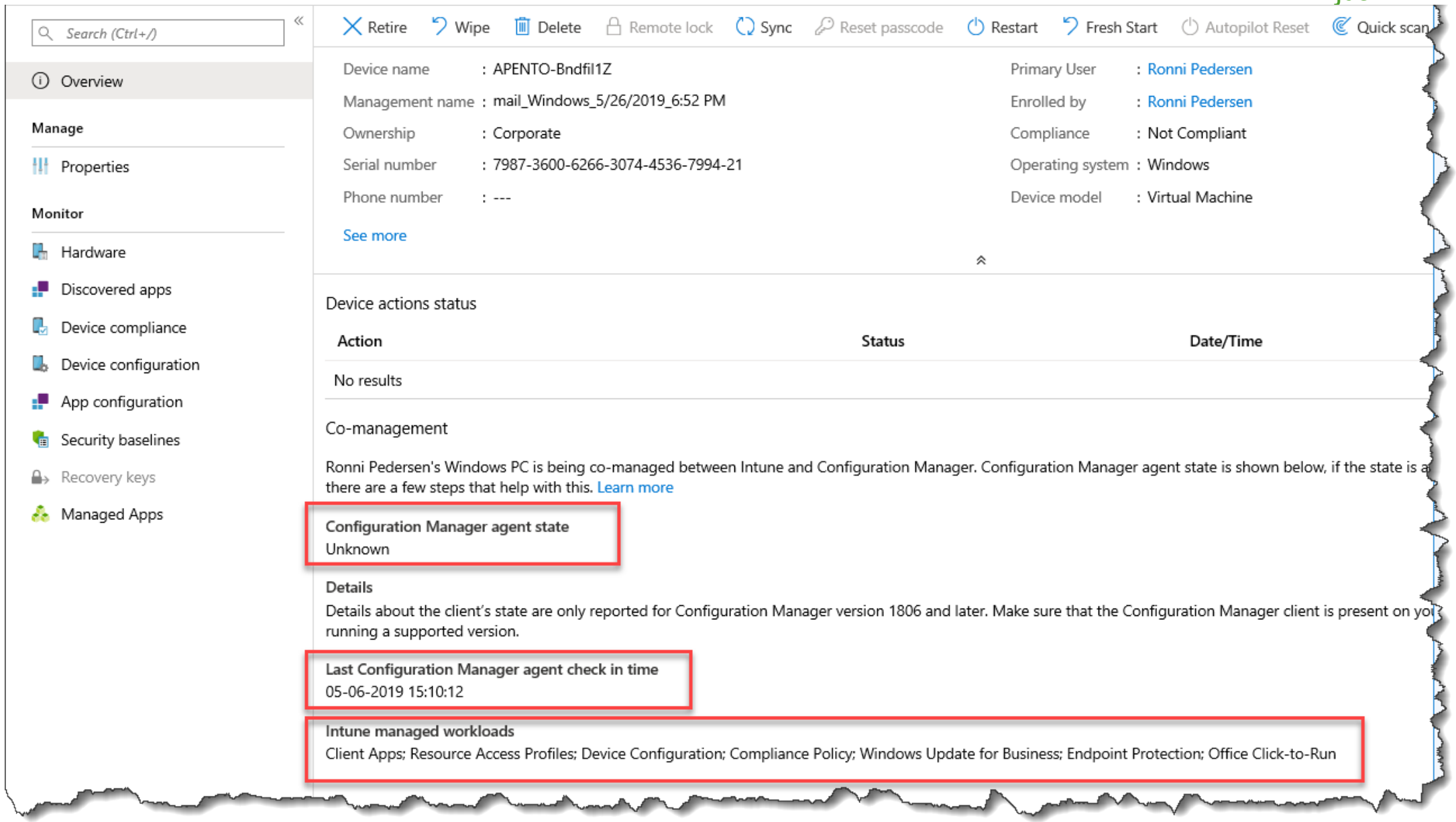
Enrollment limit restrictions

- 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.



WUFB / SAFEGUARD HOLDS

Safeguard Holds

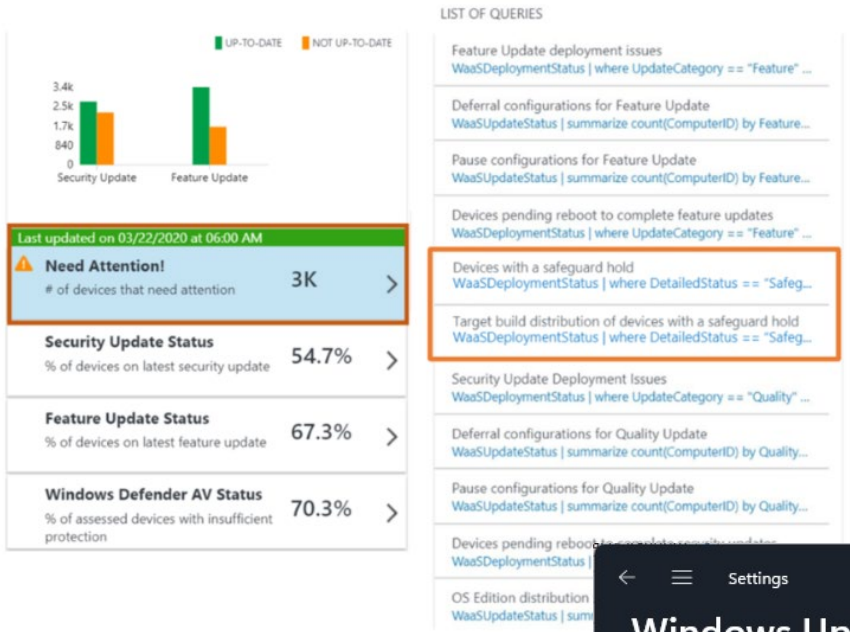
What is a Safeguard hold?

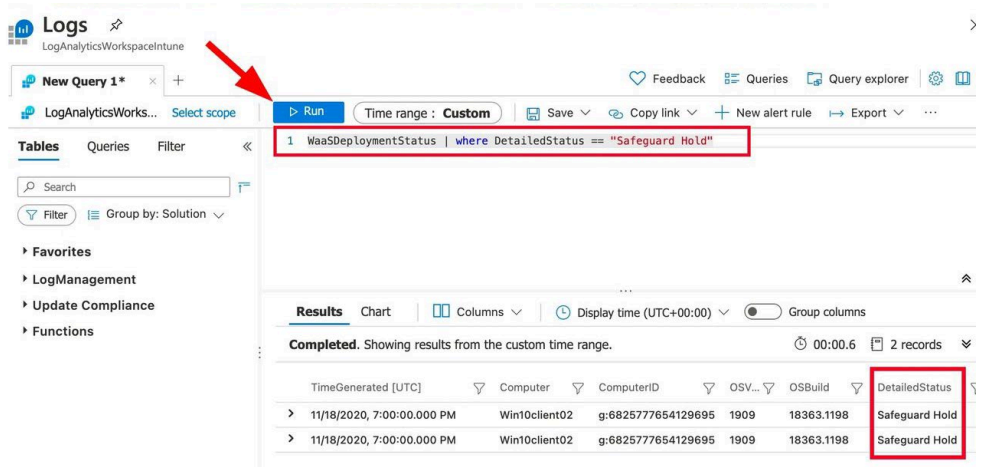
- Microsoft uses quality and compatibility data to identify issues that might cause a Windows client feature update to fail or roll back.
- When we find such an issue, we might apply safeguard holds to the updating service to prevent affected devices from installing the update in order to safeguard them from these experiences.

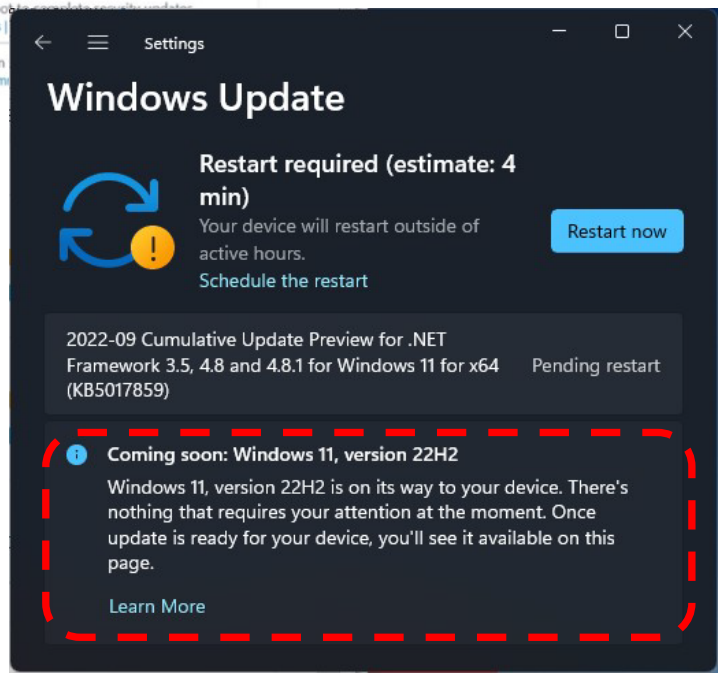
- Source: https://learn.microsoft.com/en-us/windows/deployment/update/safeguard-holds

Safeguard Holds

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







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\0Other

GatedFeature REG_MULTI_SZ None”

SafeGuardHoldLookupSample.ps1

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

Script:

- https://githuBb.com/gwblok/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

Code editor

Language mode: PowerShell | Font: Consolas | Size: 10 | Zoom: 100%

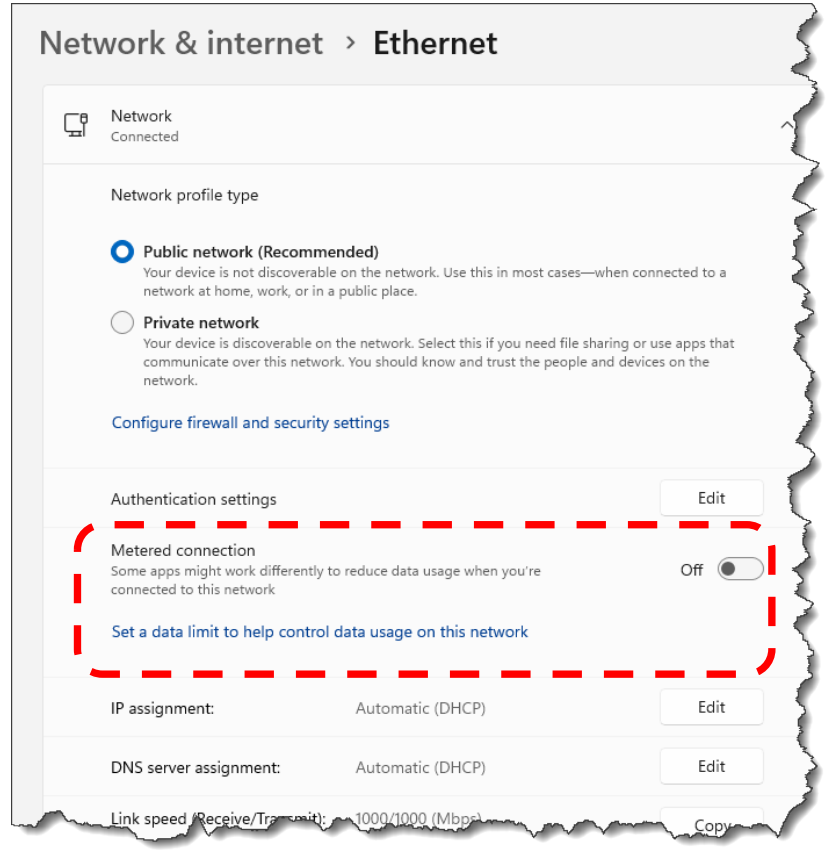
```powershell
#-----------------------------------------------------------
# Script: WUfB-Now.ps1
# Author: Ronni Pedersen, APENTO
#-----------------------------------------------------------

Set-ExecutionPolicy Unrestricted -Force
Set-PSRepository -InstallationPolicy Trusted -Name PSGallery
Start-Sleep -Seconds 30

#Install required modules
Install-PackageProvider -Name NuGet -Force
Start-Sleep -Seconds 30
Install-Module PSWindowsUpdate -Force -Verbose

Import-Module PSWindowsUpdate

#Install all updates from Windows Update (online)
Get-WindowsUpdate -WindowsUpdate -AcceptAll -Install -IgnoreReboot -ShowPreSearchCriteria -Silent -Verbose

#Install all updates (not drivers) from Windows Update (online)
#Get-WindowsUpdate -WindowsUpdate -UpdateType Software -AcceptAll -Install -IgnoreReboot -ShowPreSearchCriteria -Silent -Verbose

#Collect the WindowsUpdateLog file.
Get-WindowsUpdateLog -LogPath C:\Logs\WindowsUpdate.log
```

Lines: 24 Characters: 941 | Line: 24 Column: 55 Position: 941

Metered Network Issue

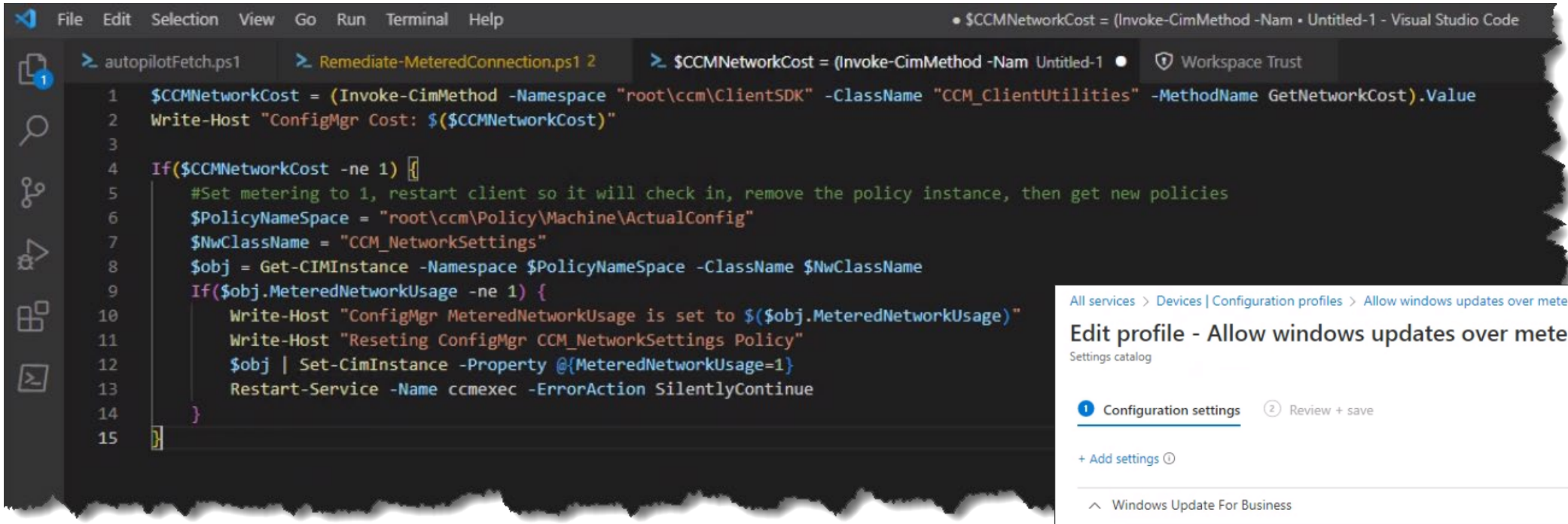
- “Metered network” = Enabled
- Result = Not downloading updates
- Impacted Clients: 60-70
- Solution
  - Check if metered network is enabled
  - Run script remotely using PowerShell Remoting

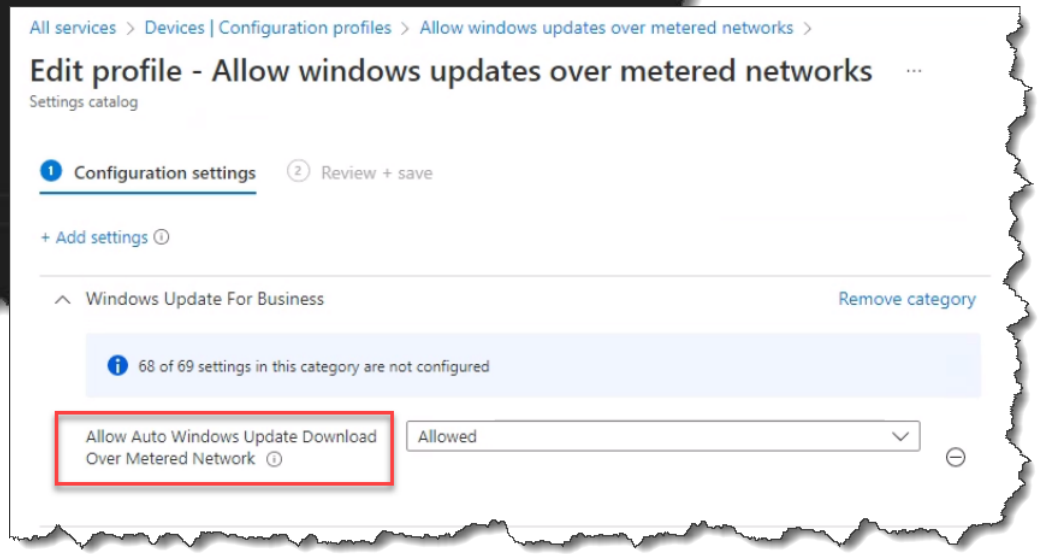
```
Untitled1.ps1*
1  [void][Windows.Networking.Connectivity.NetworkInformation, Windows, ContentType = WindowsRuntime]
2  $cost = [Windows.Networking.Connectivity.NetworkInformation]::GetInternetConnectionProfile().GetConnectionCost()
3  $cost.ApproachingDataLimit -or $cost.OverDataLimit -or $cost.Roaming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

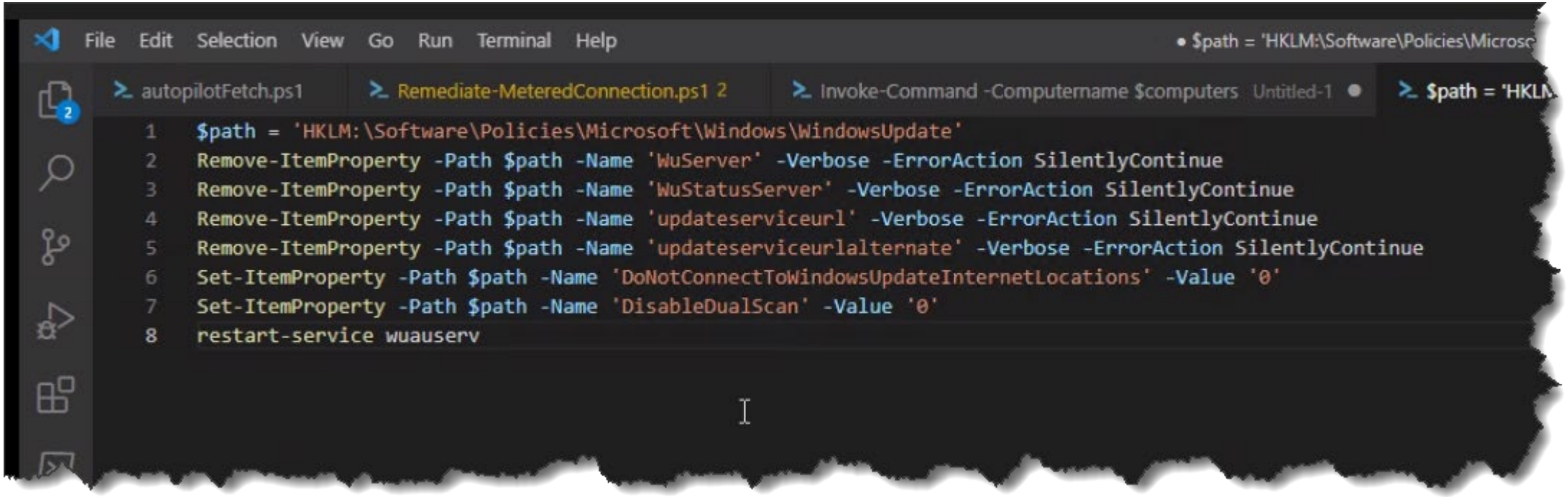




Script:
https://github.com/AdamGrossTX/Toolbox/blob/master/ConfigMgr/Troubleshooting/Remove-NetworkMetering.ps1

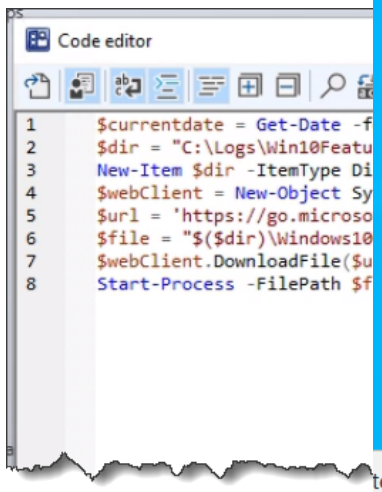
Remove legacy policies (GPO)

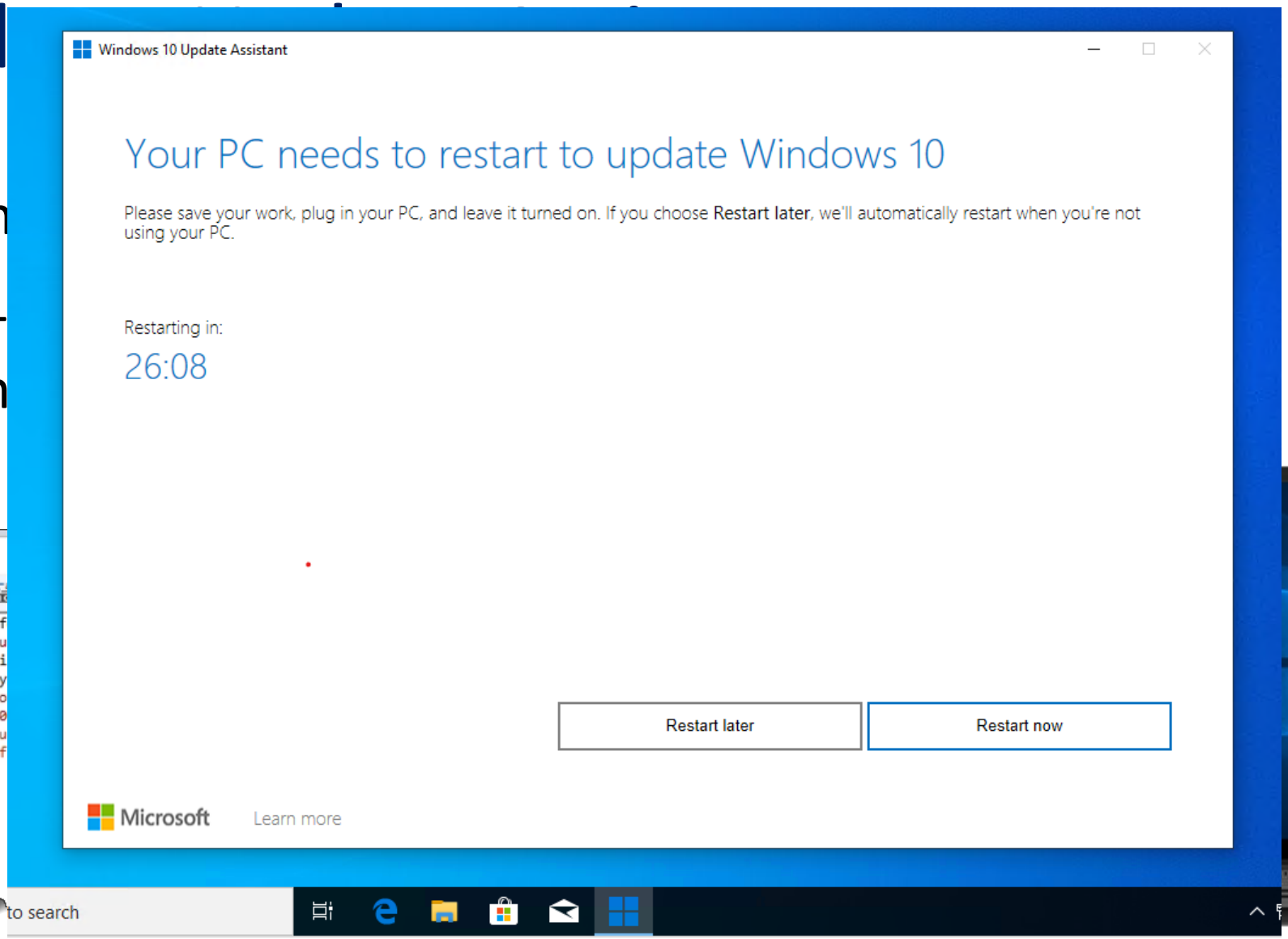
- Quick Fix: A simple script to clean up the registry



Wind

- Custon
- Runs 1
- Autom





Last Resort Fix

Disclaimer:

- This method is **not** supported
- I've reconnected multiple devices using this script and it worked great!

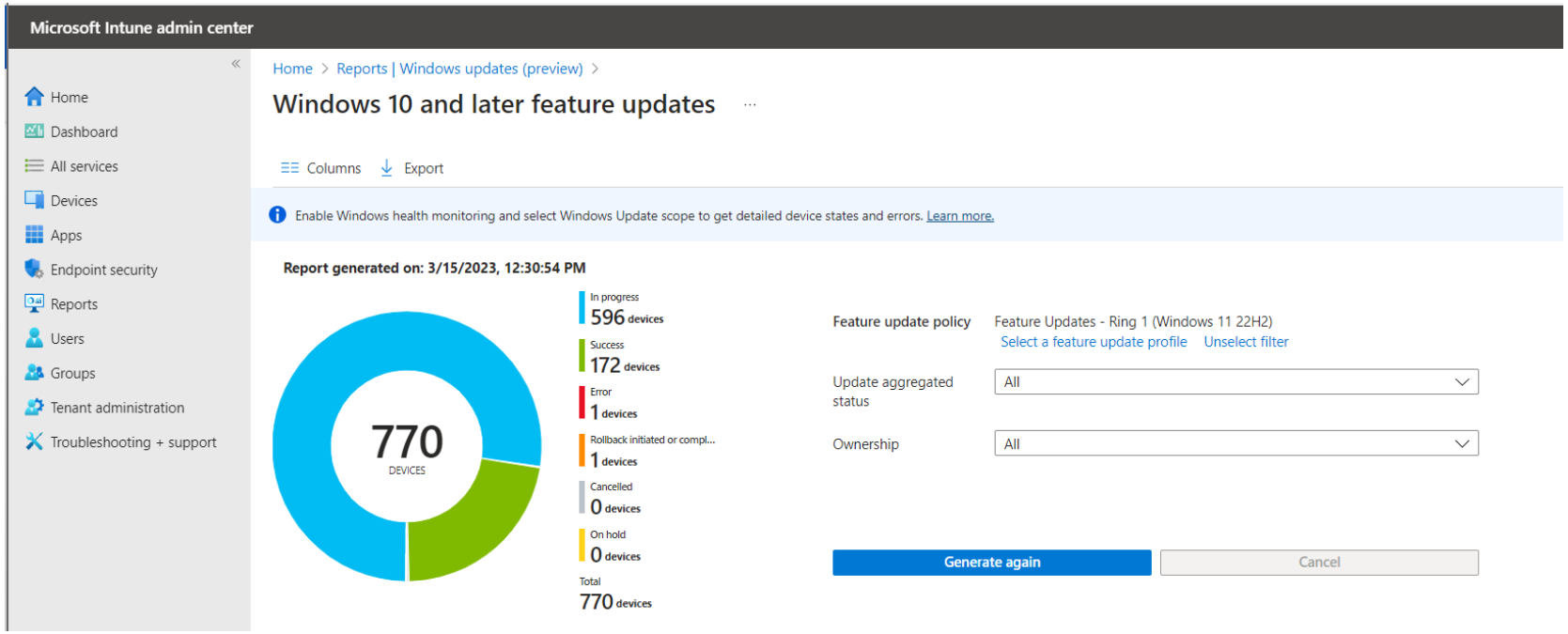
- So, if you are at the dead end, it may serve you well! ☺

- Source: https://universecitiz3n.tech/powershell/Reenroll/

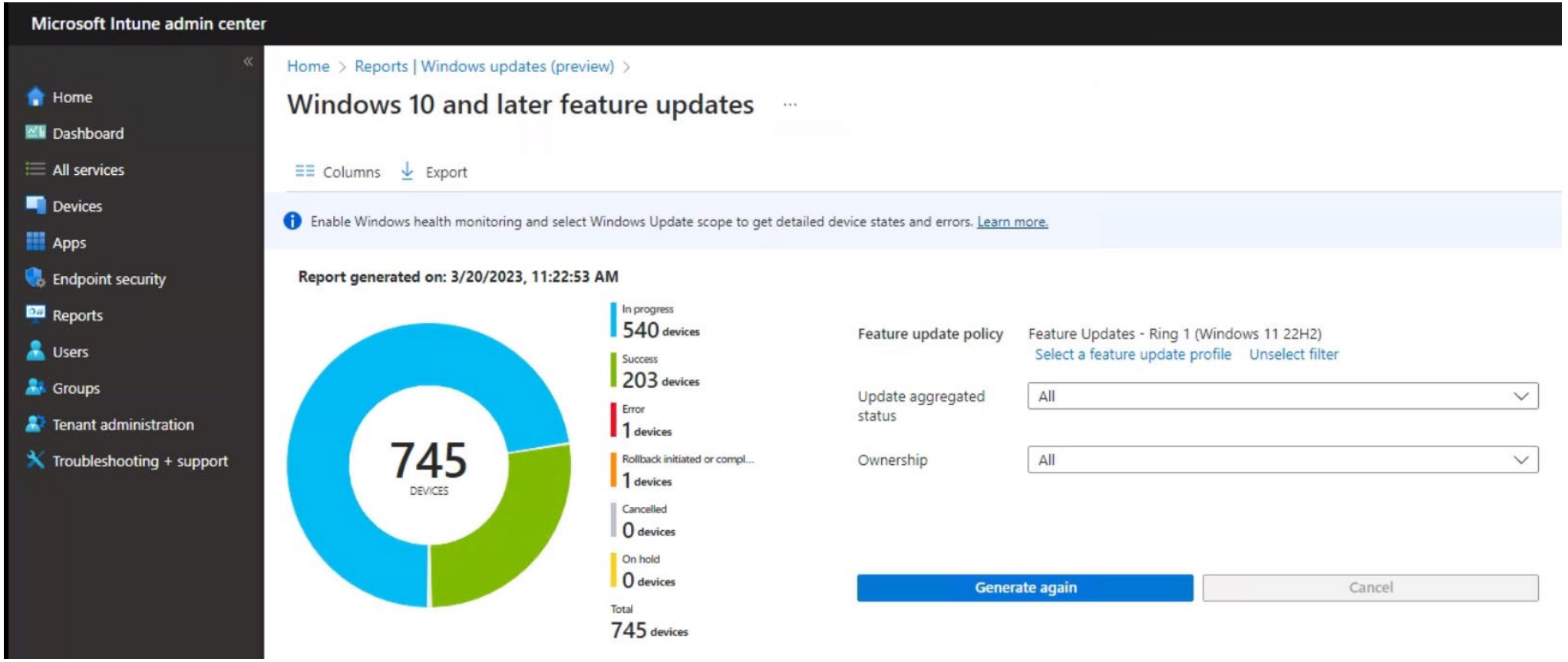
```
$Global:ErrorActionPreference = 'Stop'
Write-Host "Stopping Intune Service" -ForegroundColor Yellow
Get-Service *intune* | Stop-Service
Write-Host "Check if device is AAD Joined" -ForegroundColor Yellow
$DSREGCMD = dsregcmd /status
$AADJoinCheck = $null
$AADJoinCheck = $DSREGCMD | Select-String -Pattern 'AzureAdJoined : YES'
if ($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
$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 $psitem -Verbose -Confirm:$fa
} 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).



Status today….



INTUNE MANAGEMENT EXTENSION

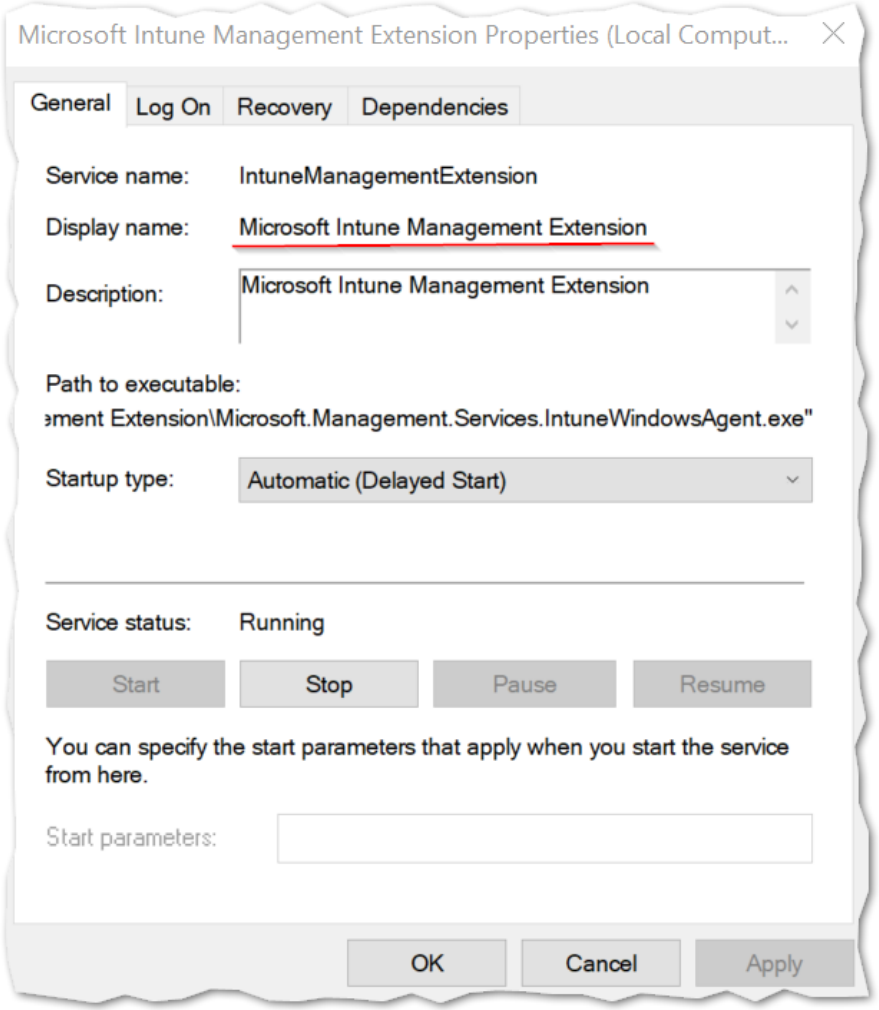
Intune Management Extension

- 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

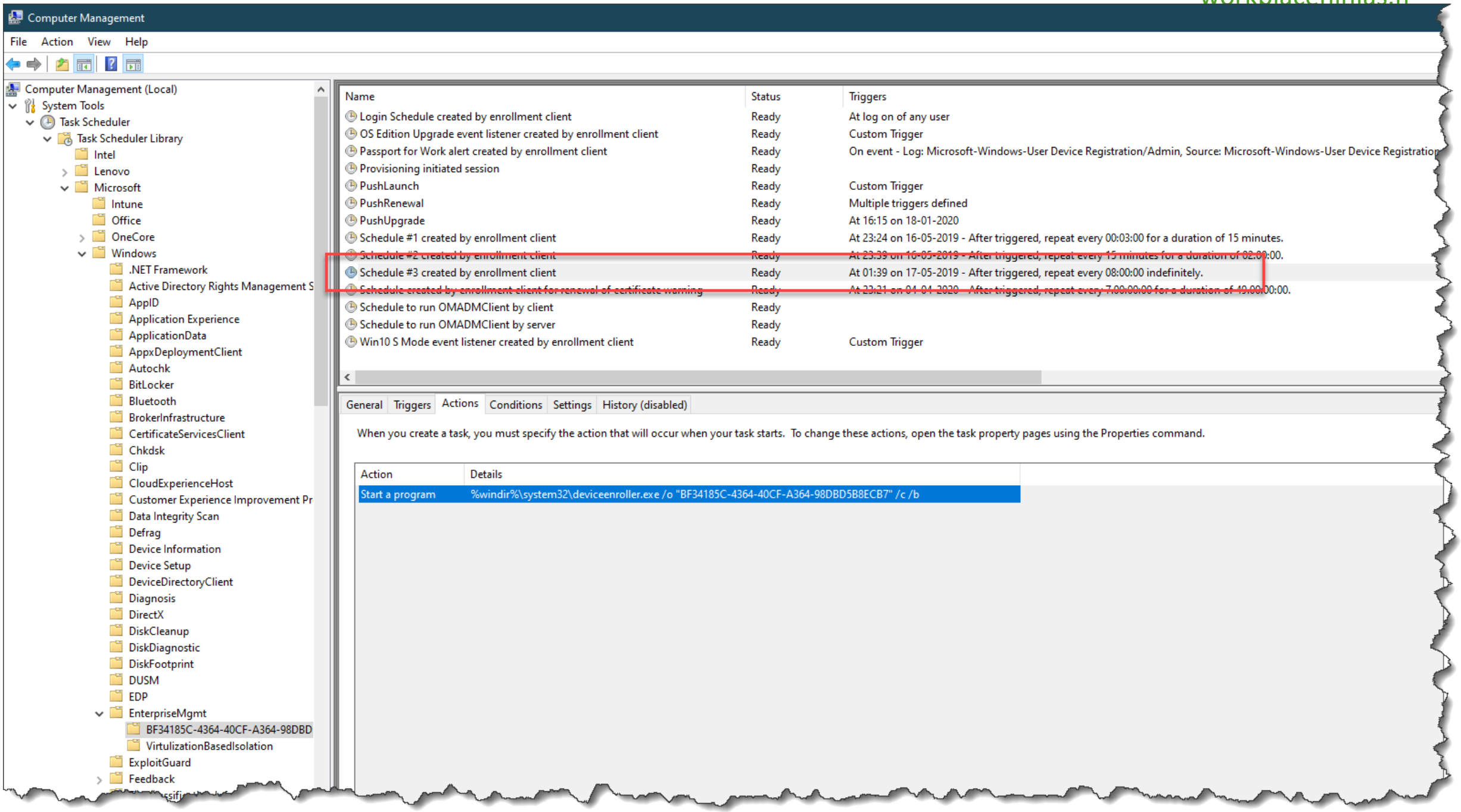
- Windows devices will schedule check-in with the Intune service: About every 8 hours

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



Intune notifications / Sync immediately

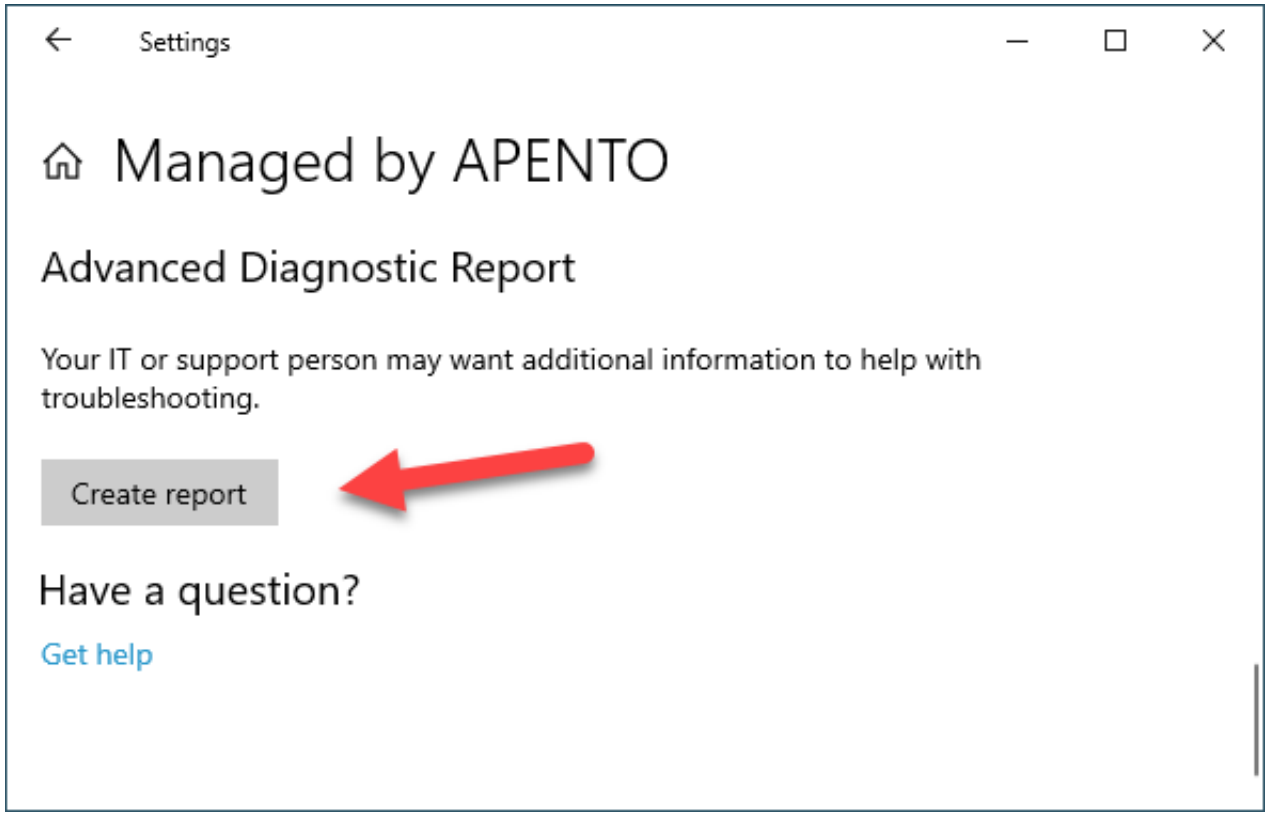
- Some actions will trigger a sync notification to the device
- When a Policy, Profile, or App is:
  - Assigned (or unassigned)
  - Updated
  - Deleted
- Manually from the Company Portal
- Manually using Script

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=<enabled/><data id="EncryptionMethodWithXtsOsDropDown_Name" value="7"/><data id="EncryptionMethodWithXtsFdvDropDown_Name" value="7"/><data id="EncryptionMethodWithXtsRdvDropDown_Name" value="7"/>
BitLocker	SystemDrivesRecoveryOptions			device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=<enabled/><data id="OSAllowDRA_Name" value="true"/><data id="OSRecoveryPasswordUsageDropDown_Name" value="2"/><data id="OSRecoveryKeyUsageDropDown_Name" value="2"/><data id="OSHideRecoveryPage_Name" value="false"/><data id="OSActiveDirectoryBackup_Name" value="true"/><data id="OSActiveDirectoryBackupDropDown_Name" value="1"/><data id="OSRequireActiveDirectoryBackup_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	[illegible]wCloudProtection	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1

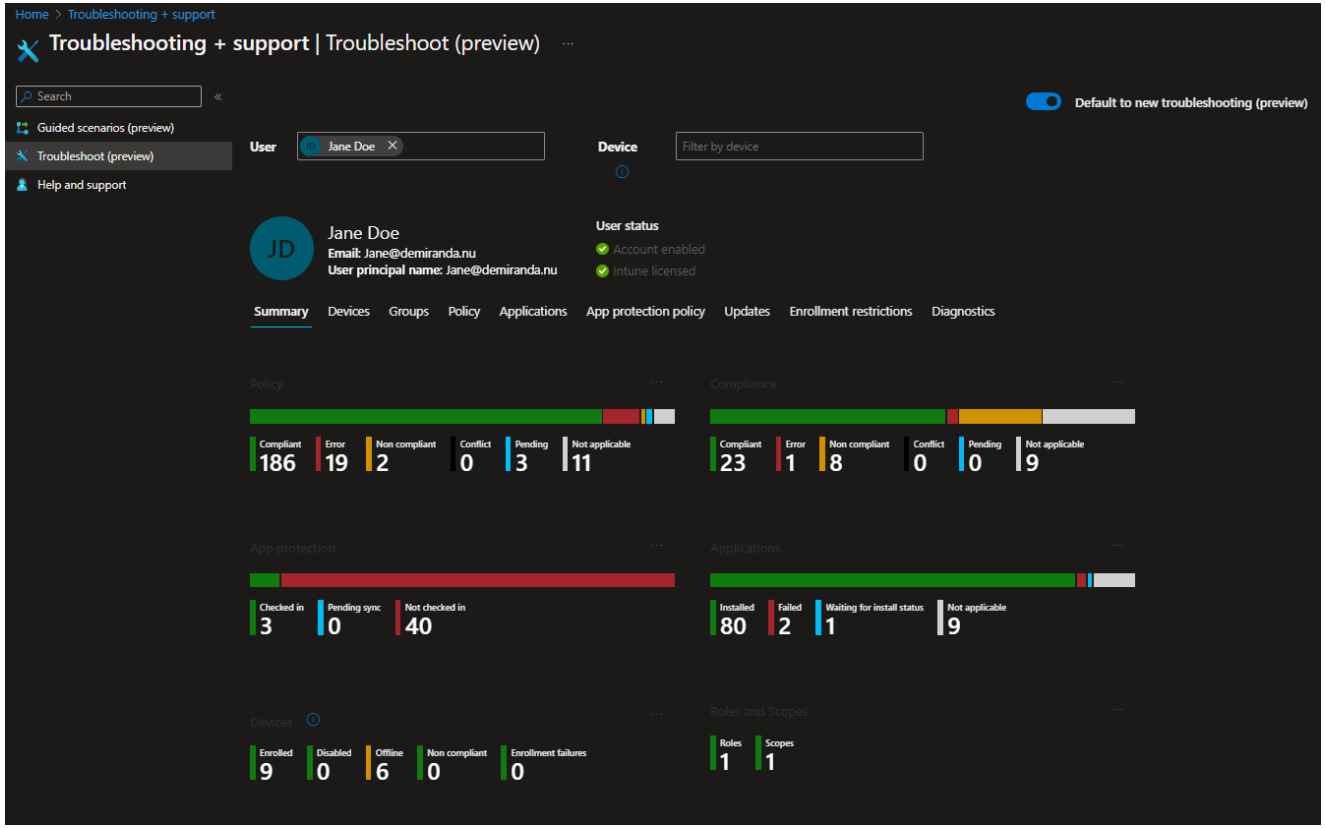
Intune Troubleshooting Pane

Intune portal page

- https://aka.ms/intunetroubleshooting

Displays information focused around a particular user

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



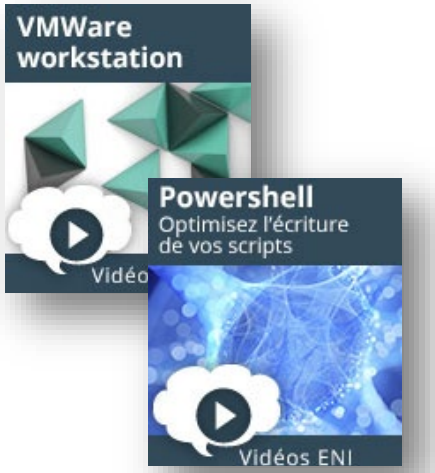
For more info:
https://docs.microsoft.com/en-us/intune/help-desk-operators

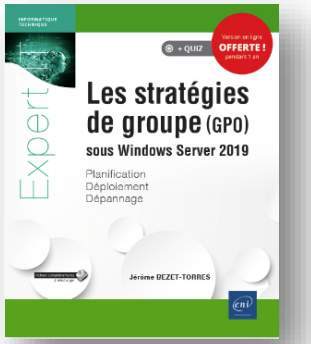
Thank You

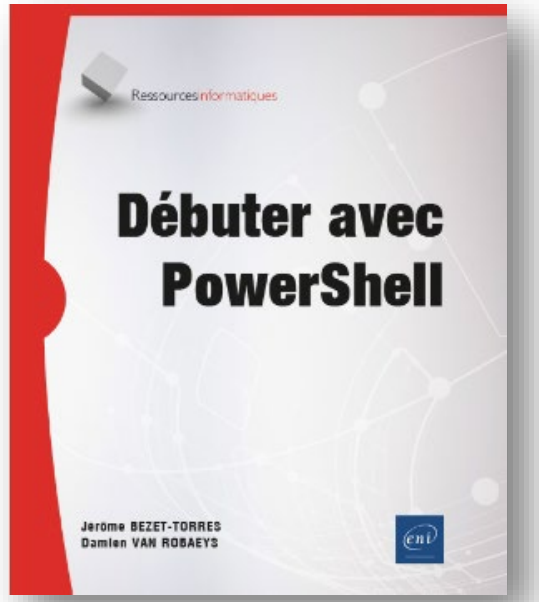
Workplace Ninja
User Group France

Livres et formations

workplaceninjas.fr
#WPNinjasFRA







A paraitre Avril 2023