Troubleshooting the MEM managed Windows Client

Jörgen Nilsson & Ronni Pedersen

www.wpninjas.eu
#WPNinjaS

Platinum Sponsor

PATCH MY PC

Microsoft Security

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Snapdragon

Silver and Special Sponsors

SD:>_ SwissDev Jobs

LUZERN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPPMAN

AppManagEvent.com
2022
October 7
Netherlands

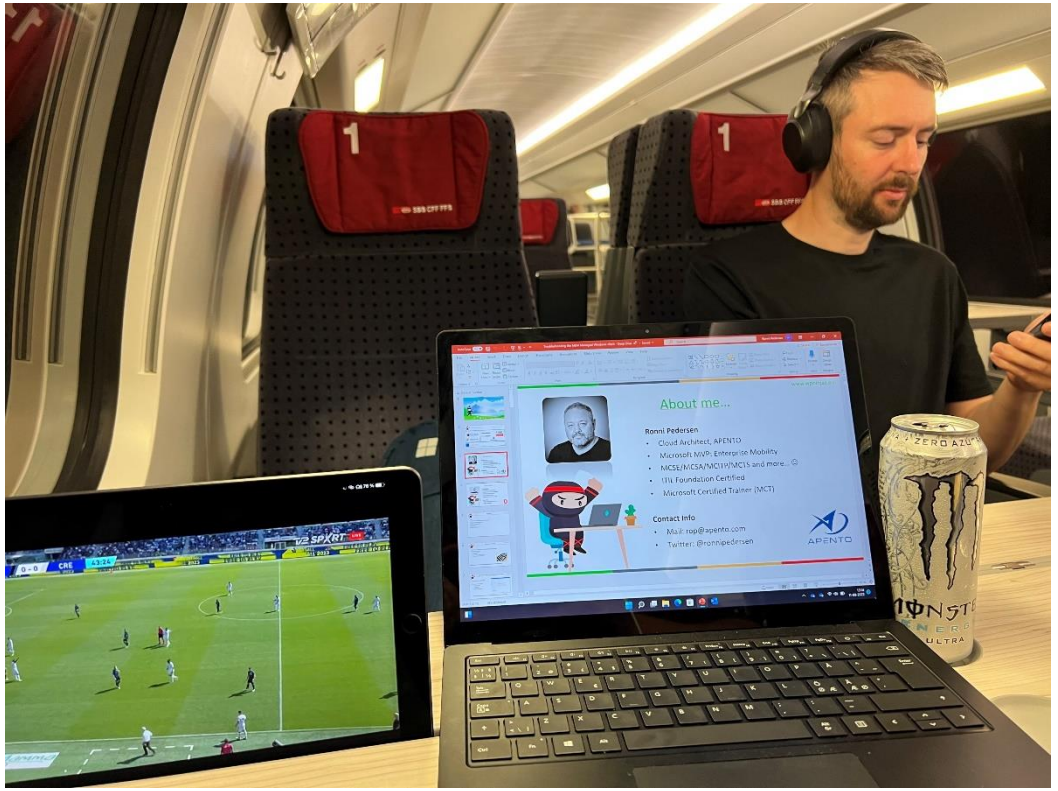
dinext.

Preparing for WP Ninjas like a BOSS!

What could go wrong?


"OM SOMMEREN TÆNKER JEG TIT
GID JEG KUNNE SVØMME
NØGEN LANGS STRANDEN"

What could go wrong?



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

APENTO

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

- Tools
- Troubleshooting Subscription based activaton
- Troubleshooting Enrollment
- Troubleshooting Policies
- Intune Management extension

Remote Control

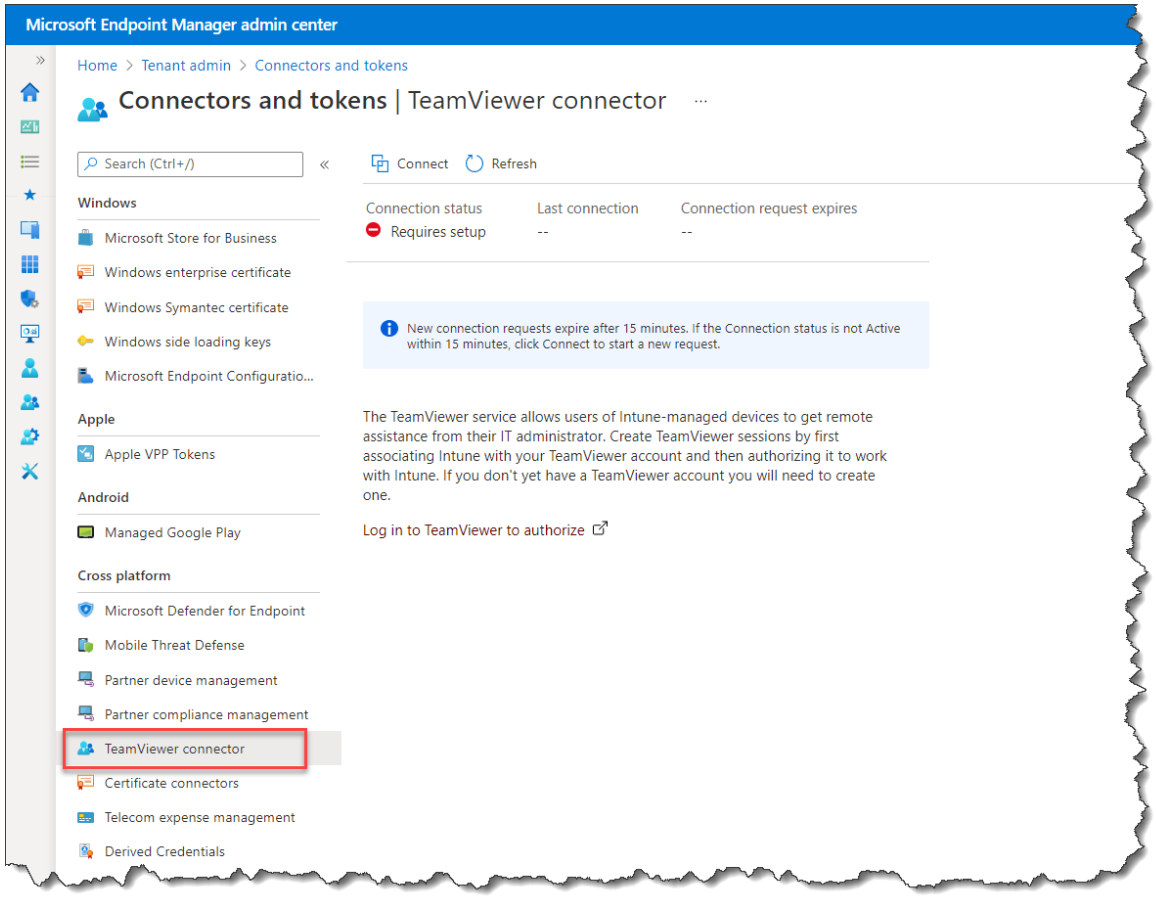
- TeamViewer integrates in the Endpoint Management Portal
- Quick Assist is built-in
  - Lacks UAC support
  - No Logging
  - Maybe OK for smaller organizations
  - During AutoPilot (Alt+Win+Q)

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

Configure the TeamViewer Connector

- Easy setup and configuration

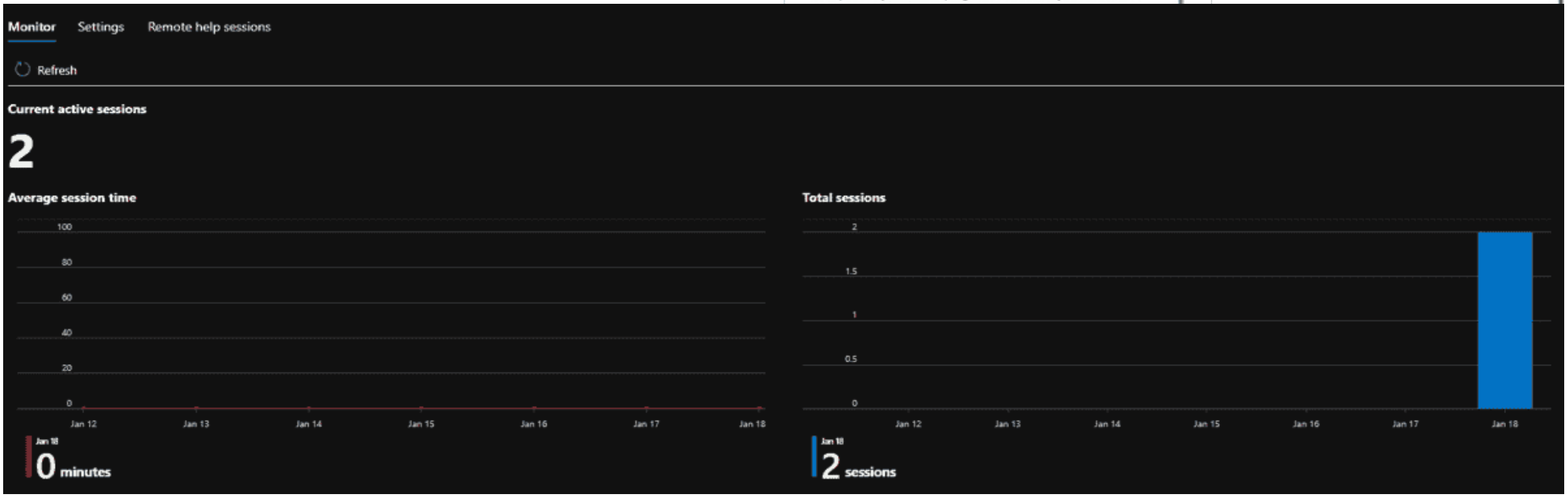
- There are other options:
  - Beyond Trust
  - LogMeIn
  - Remote Help!



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

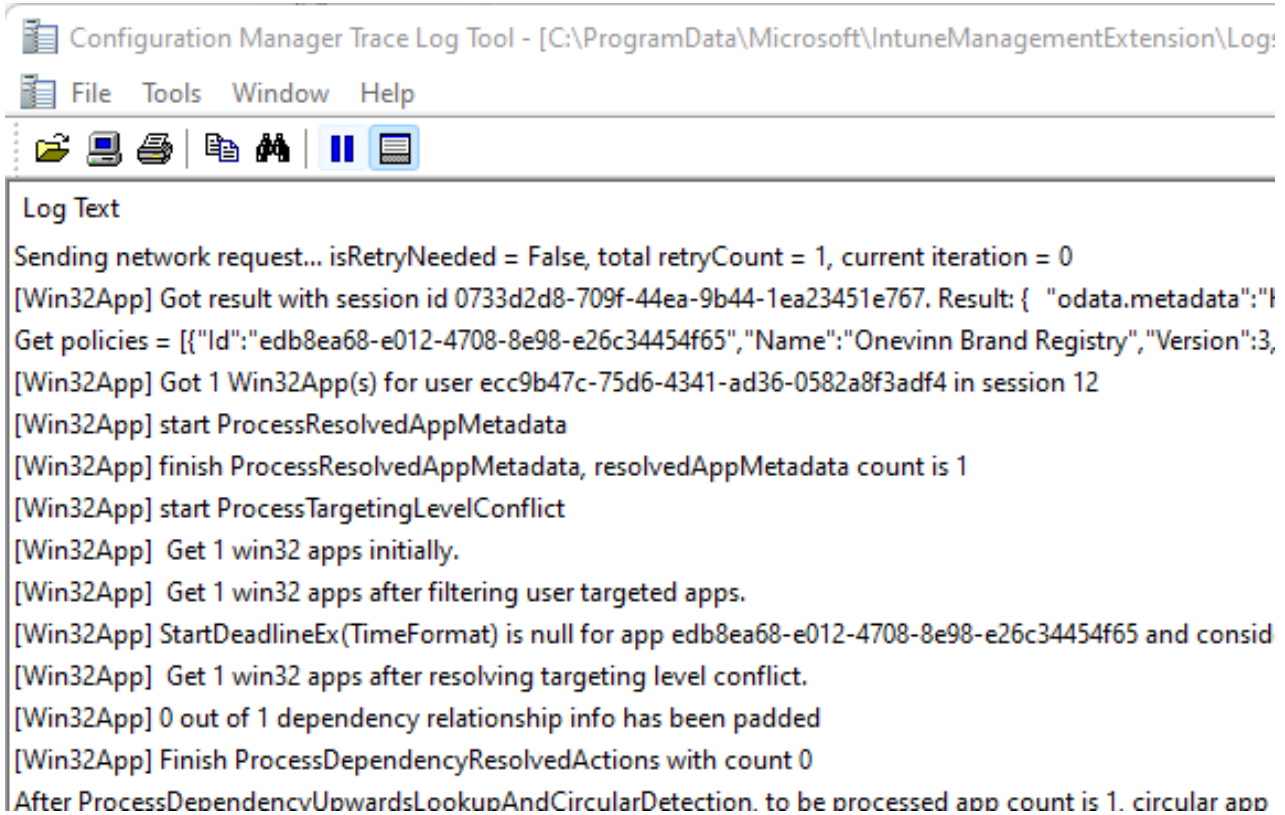
Microsoft Remote Help

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



CMtrace

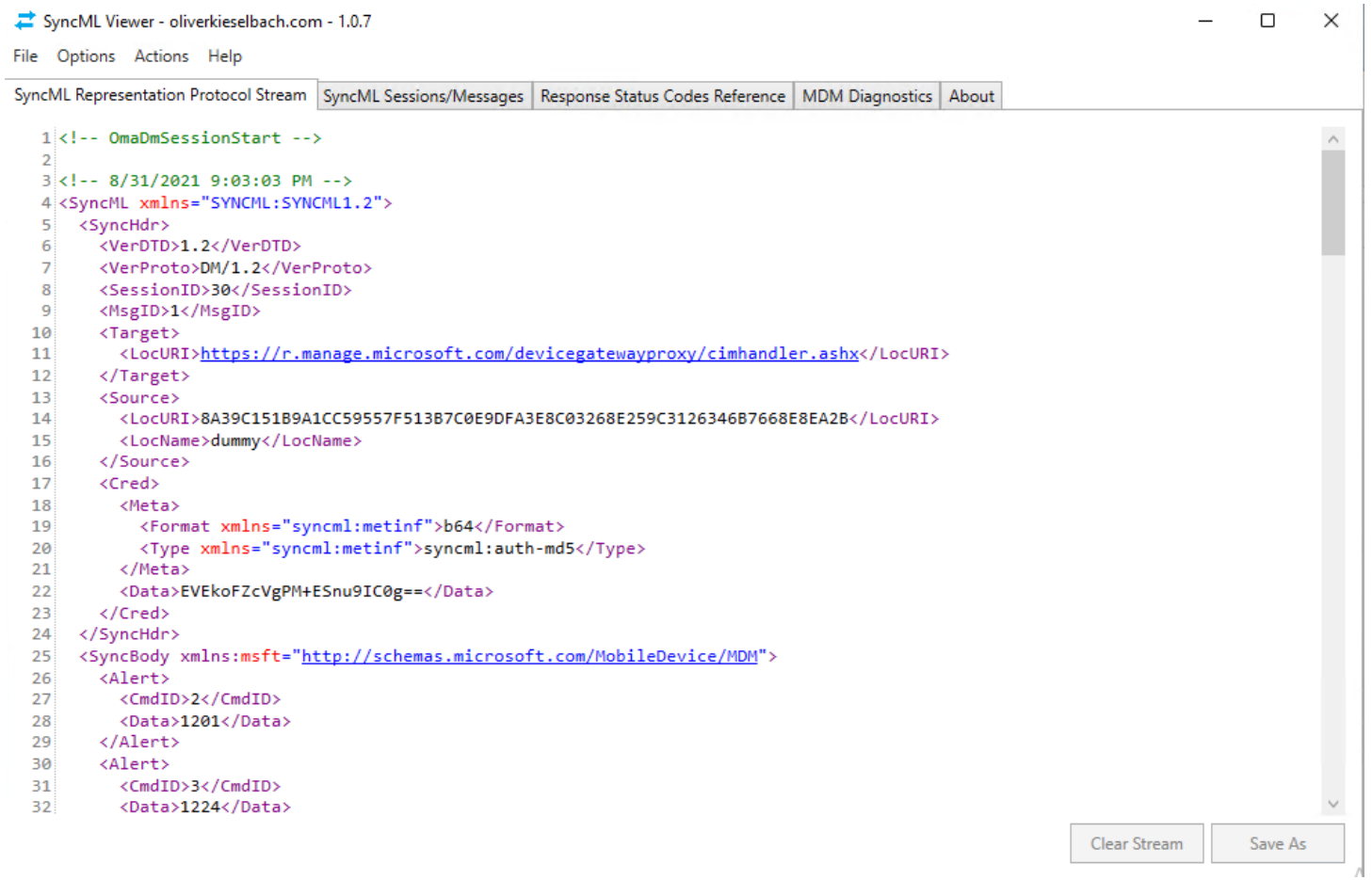
- Great log reader
- Not free but included in the Intune/MEM license
- Deploy it to all clients



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


```
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>T0EeBAEAHAAAAAoAMwDwVQAACgAaAfBVCnofKQQCCQgCABAACQABAAEAAgABAAAABQAZAAQAAAAAAAAAAAgAAAAAAAACAAEAAwMAEQBHZW51aW5lSW50ZWwABAA0AEludGVsKFIpIENvcmUoVE0pIGk3LTg1NTlV
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>
```

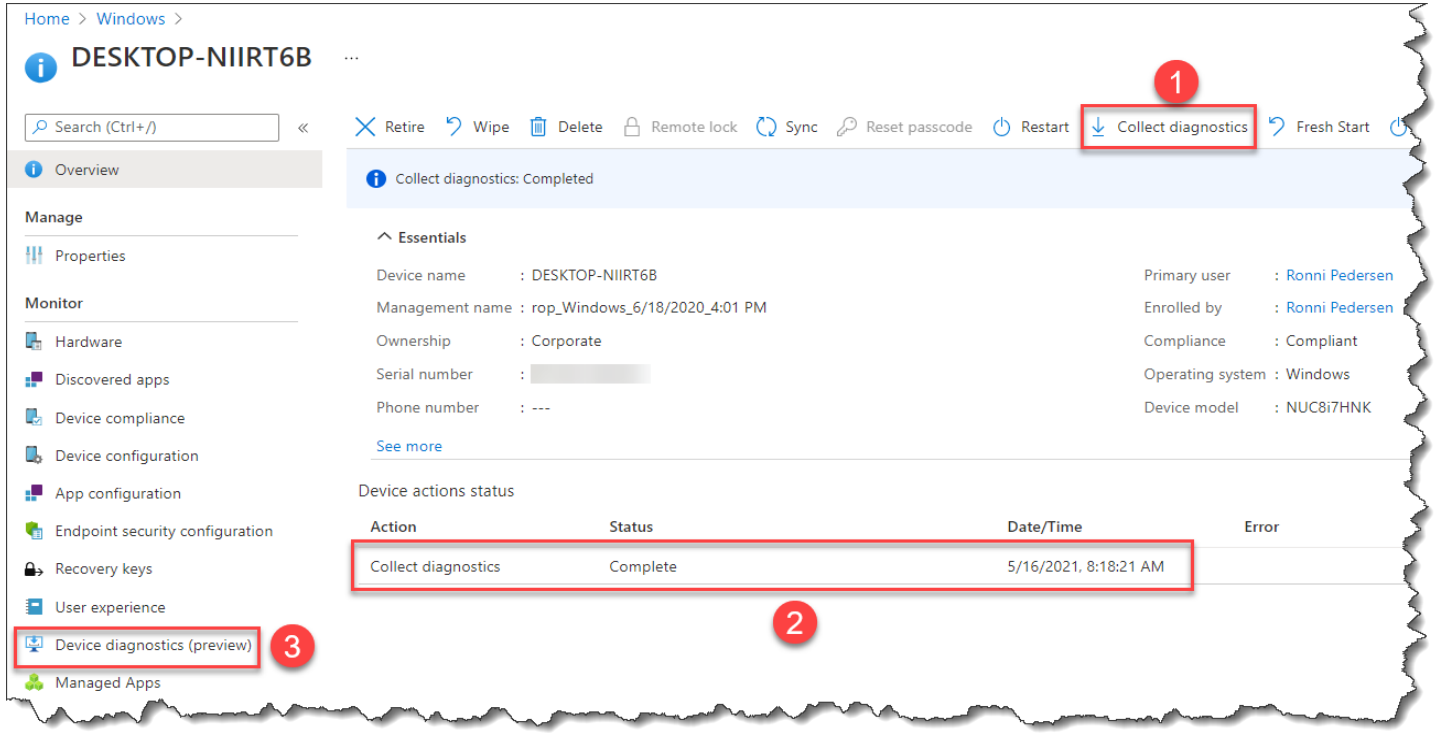
Log Files

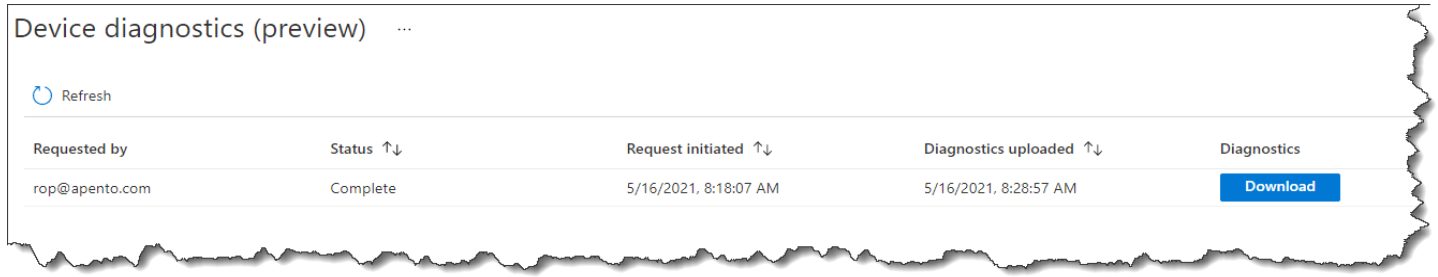
Collect diagnostics from a Windows Device

- Collecting Diagnostic Logs from Windows Devices
  - Windows 10 1909 or newer
  - Windows 11
  - HoloLens 2
  - Both Intune and Co-Managed devices
  - Corporate-owned devices only

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

Collecting Diagnostic Logs





Remote Troubleshooting

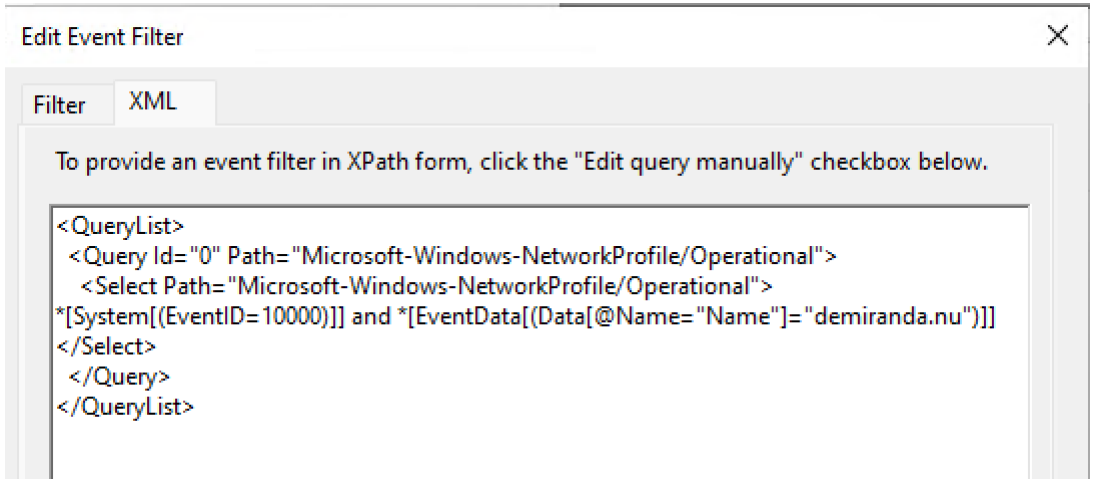
- Customer quote:

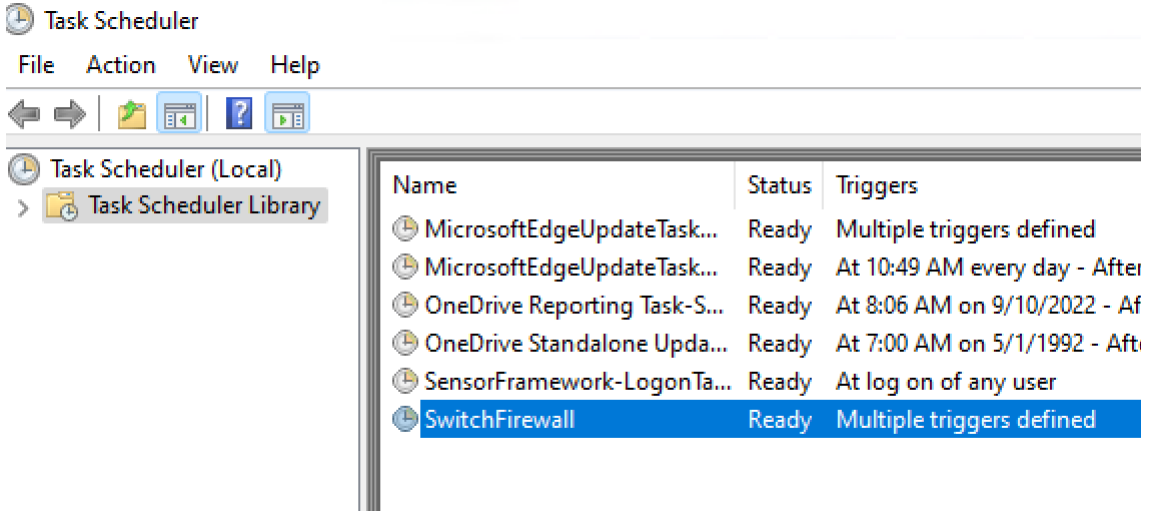
  “I haven’t spoken to an end-user in the last three years and I am not about to start now!”

- 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!

Solution

- Event triggered schedule task
- Triggers a PowerShell script that switches the firewall profile to Private





Configuration Policy Process

Microsoft 365 Apps Policy

- Endpoint Manager 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

Administrative Templates

- Example using Administrative Templates

Update Deadline	Not configured	Device	\Microsoft Office 2016 (Machine)\Updates
Update Channel (2.0)	Enabled	Device	\Microsoft Office 2016 (Machine)\Updates
Update Channel (1.0)	Not configured	Device	\Microsoft Office 2016 (Machine)\Updates
Target Version	Not configured	Device	\Microsoft Office 2016 (Machine)\Updates

Channel Name:

Monthly Channel

This setting is superseded by a later version, "Update Channel (2.0)". Since a later version of this setting is configured, this version is set to not configured.

OK

Channel Name:

Current Channel (Preview)

Current Channel

Current Channel (Preview)

Monthly Enterprise Channel

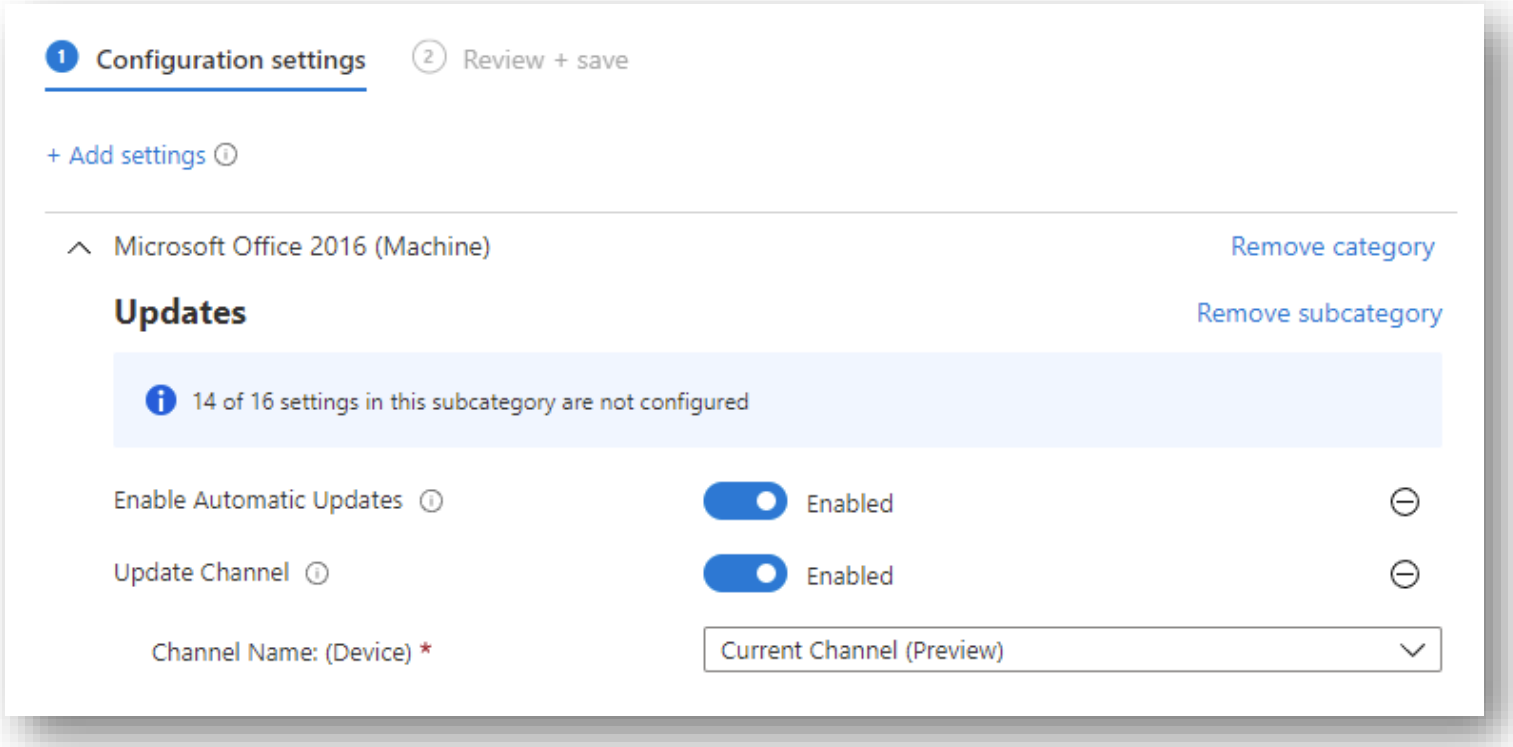
Semi-Annual Enterprise Channel

Semi-Annual Enterprise Channel (Preview)

Beta Channel

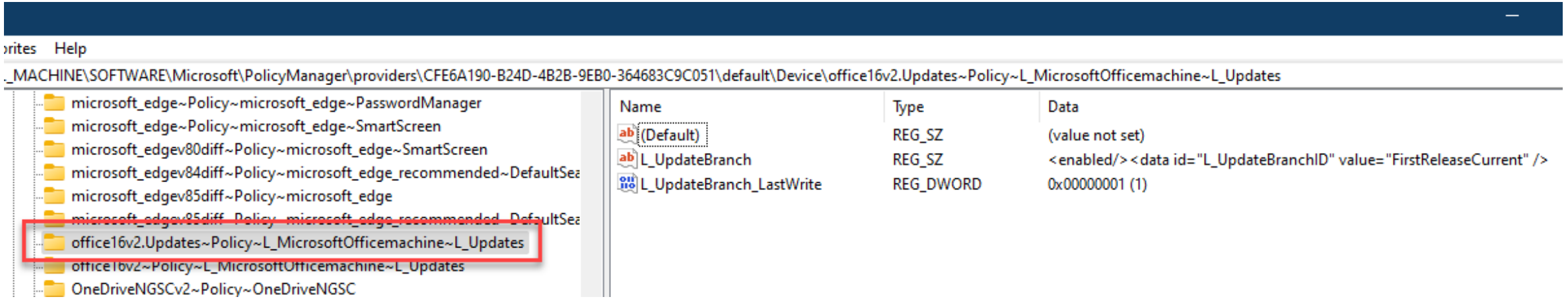
Using Settings Catalog (Preview)

- 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.

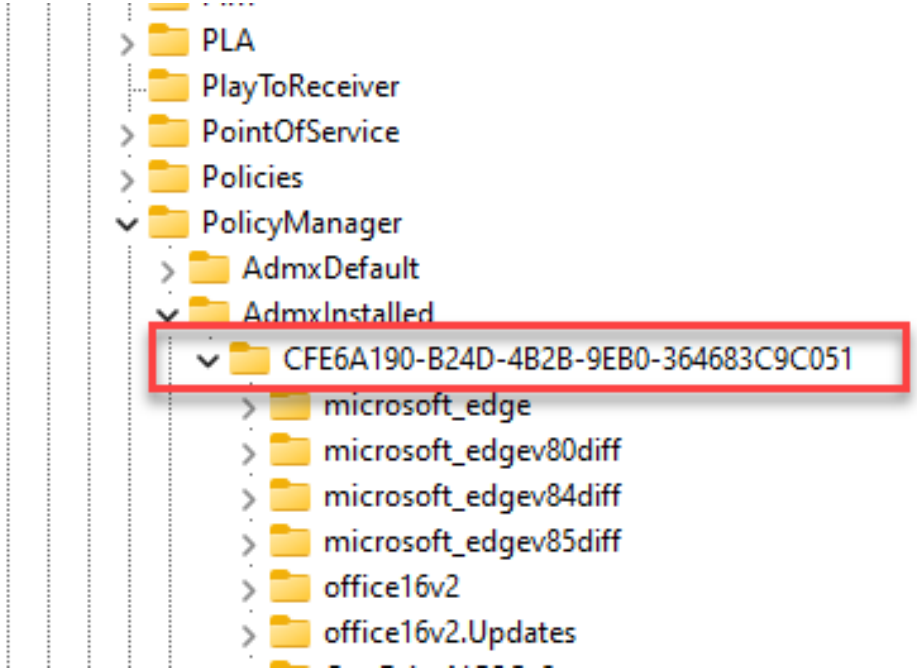


Find the Provider ID

Find the provider ID for your device

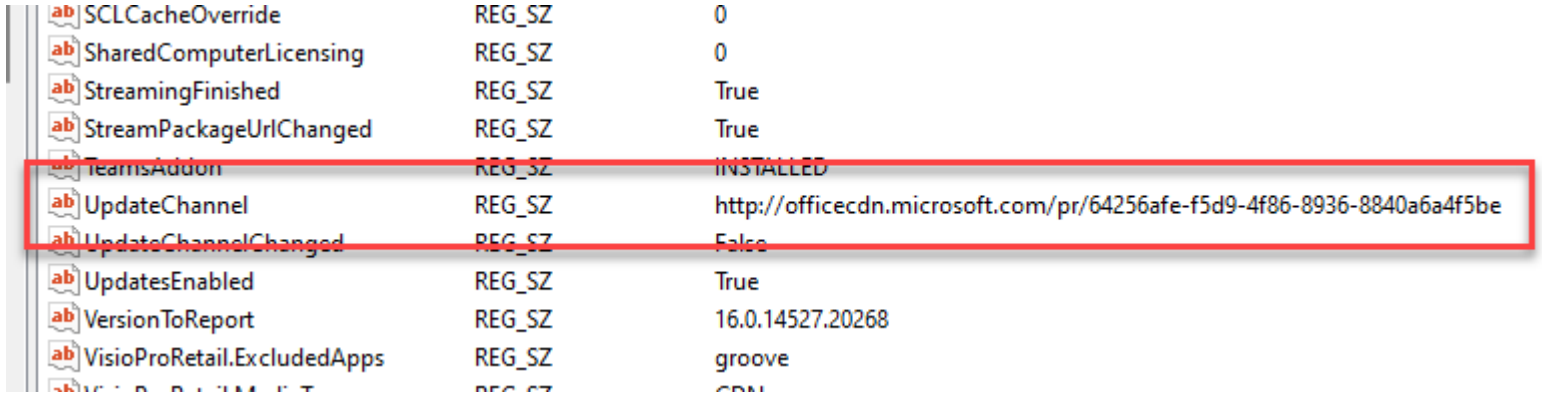
- Open the Registry Editor, and go to:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\AdmxInstalled



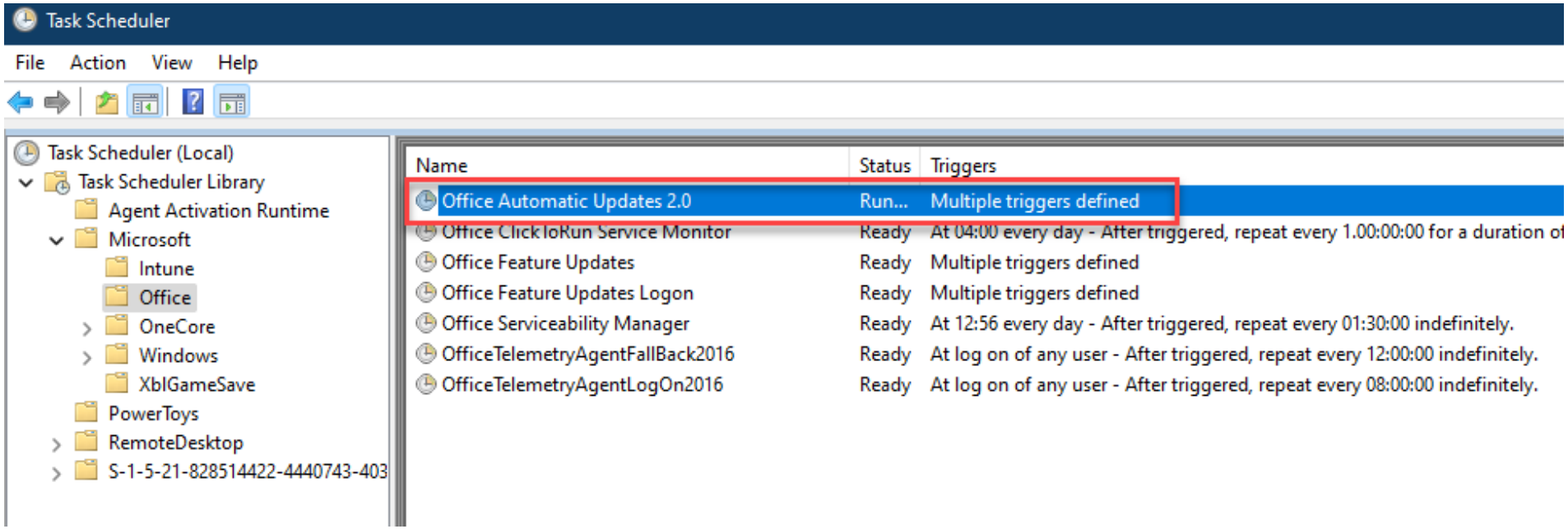
#2 Check the Office registry keys

- 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

Send
88,0 Kbps

Receive
27,3 Mbps

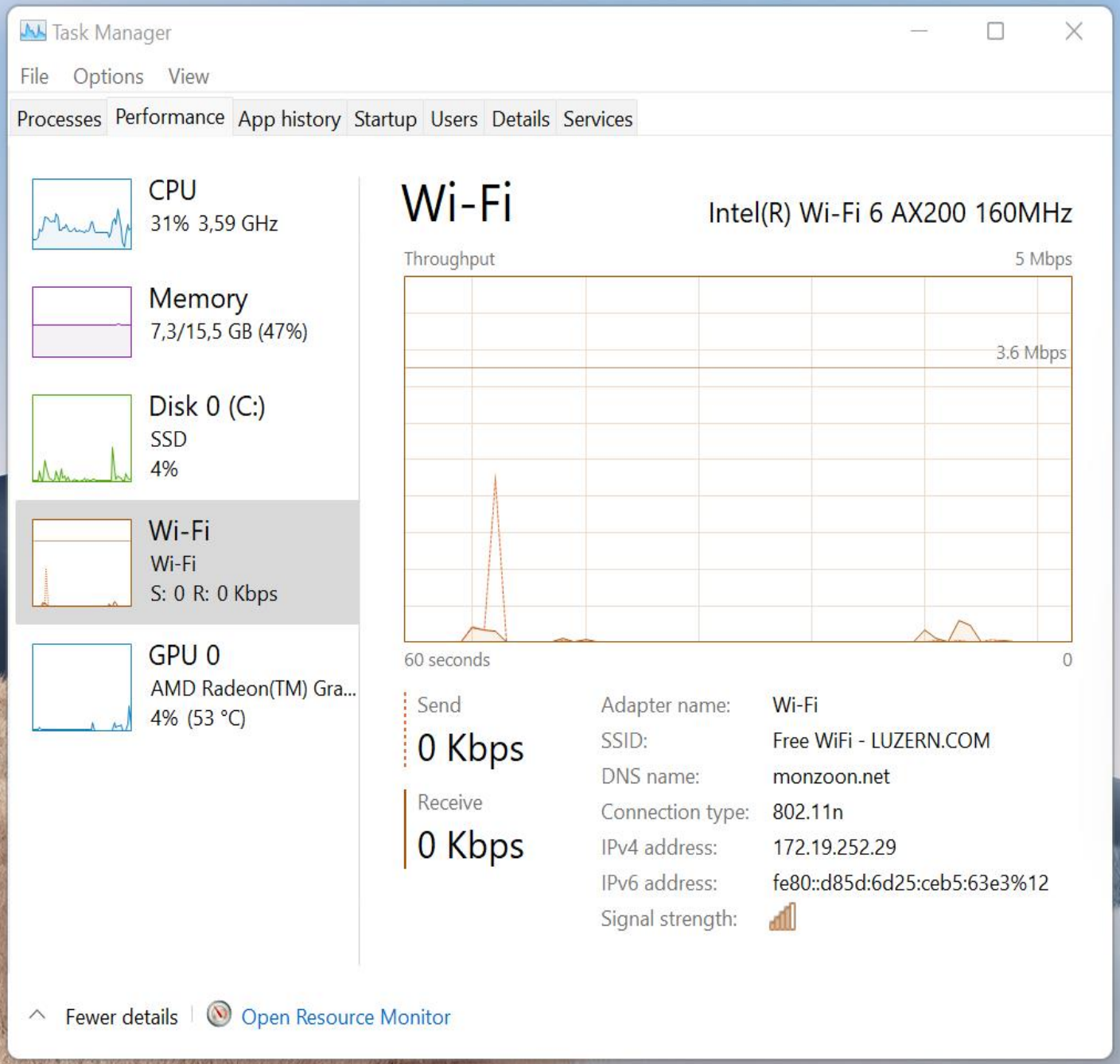
Adapter name:	Wi-Fi
SSID:	Free WiFi - LUZERN.COM
DNS name:	monzoon.net
Connection type:	802.11n
IPv4 address:	172.19.252.29
IPv6 address:	fe80::d85d:6d25:ceb5:63e3%12
Signal strength:	

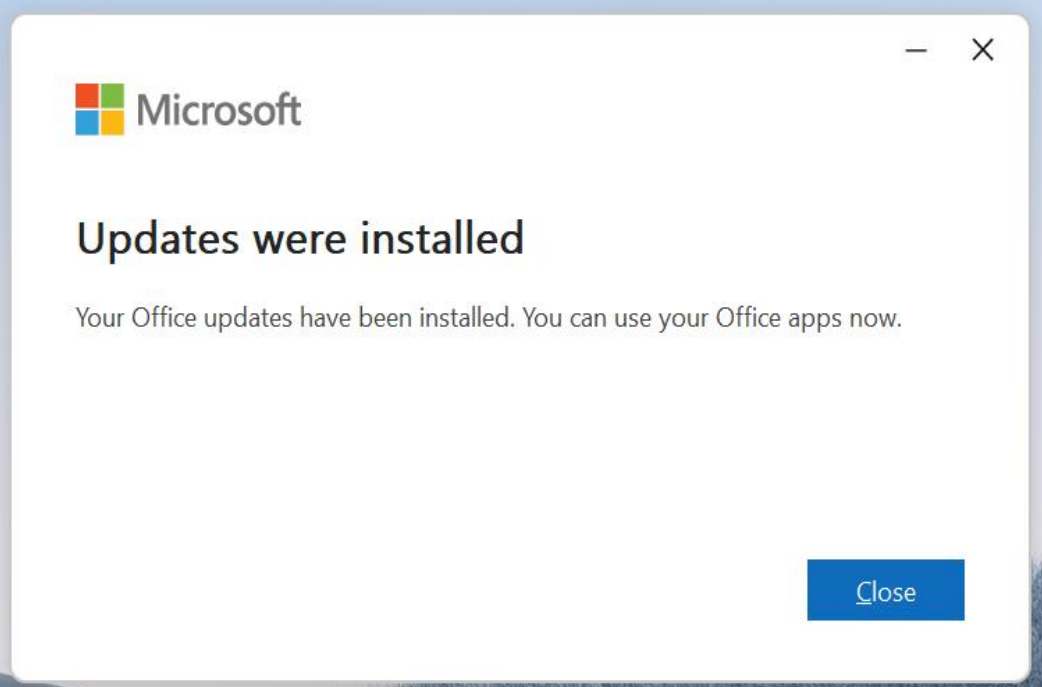
Fewer details | Open Resource Monitor

Microsoft

Downloading Office updates...

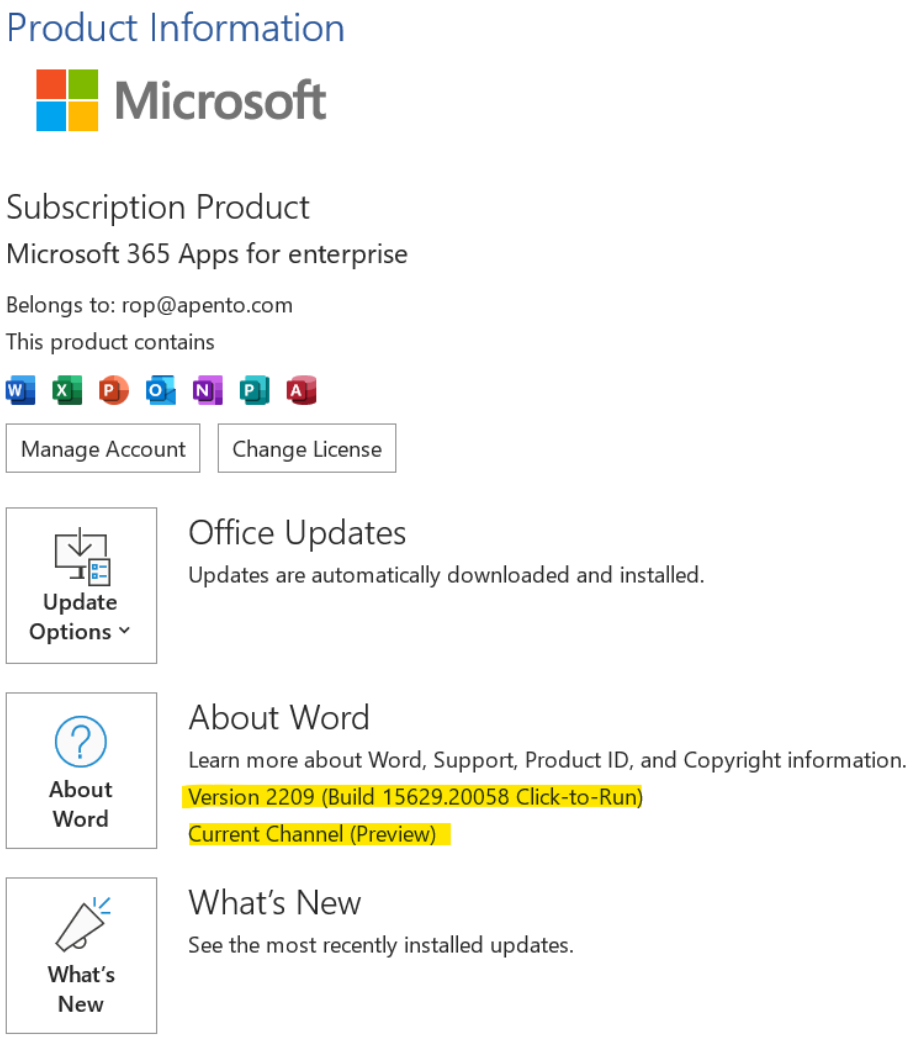
You can keep using Office while we download in the background.


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

www.wpninjas.eu



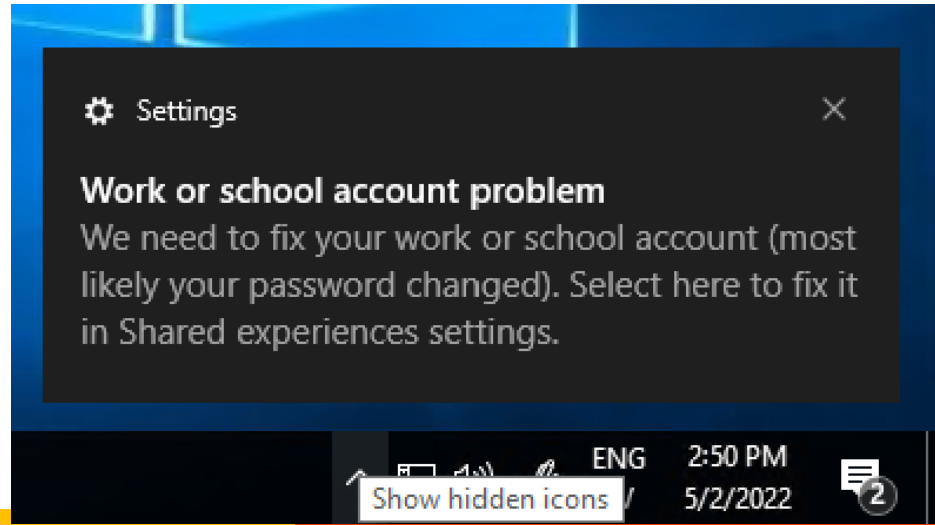
Update history for Microsoft 365 Apps

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

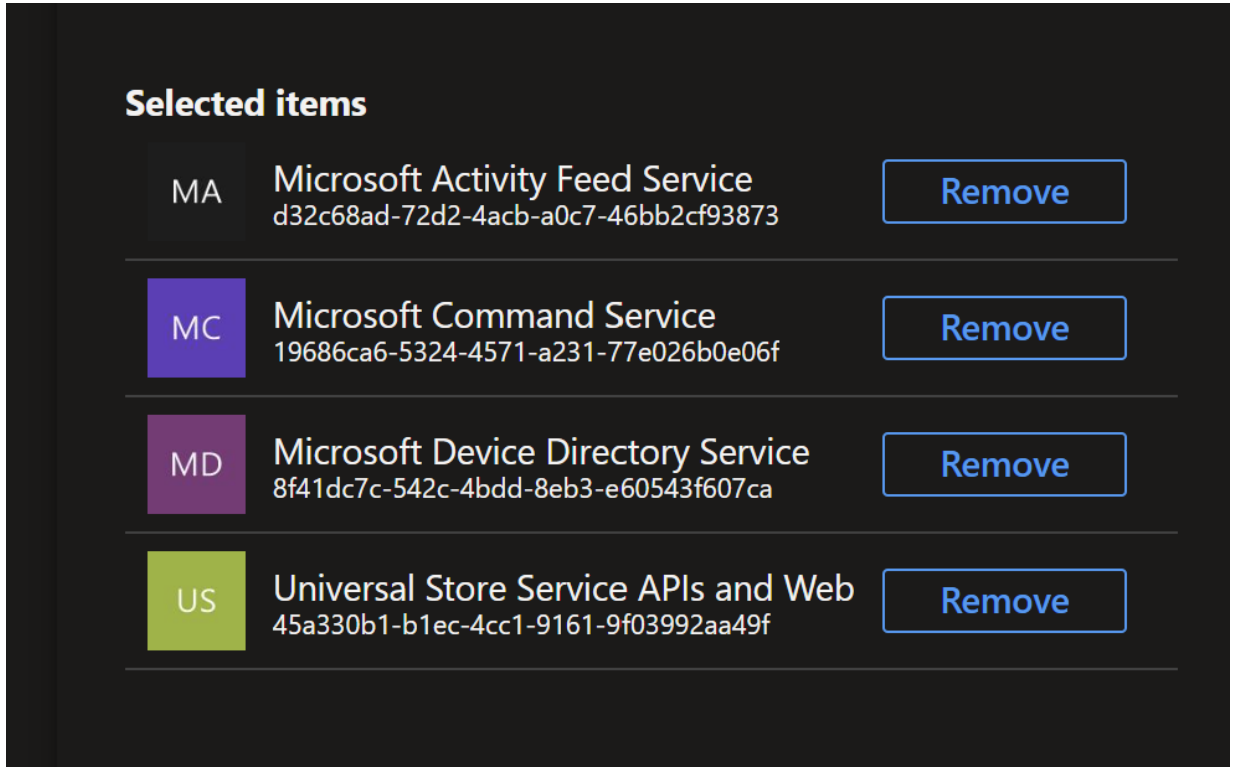
Troubleshooting
Subscription Based Activation

Subscription based activation

- Easiest way of upgrading to Enterprise from pro
- Re-activated every 30 days
- Blocked by the “access work or school as …”
- Important: Devices will automatically “migrate” from MAK, KMS and AD-based activation to Subscription when a user with an assigned license logs on.
- Exclude **Universal Store Service APIs and Web Application** from your Conditonal access framework.

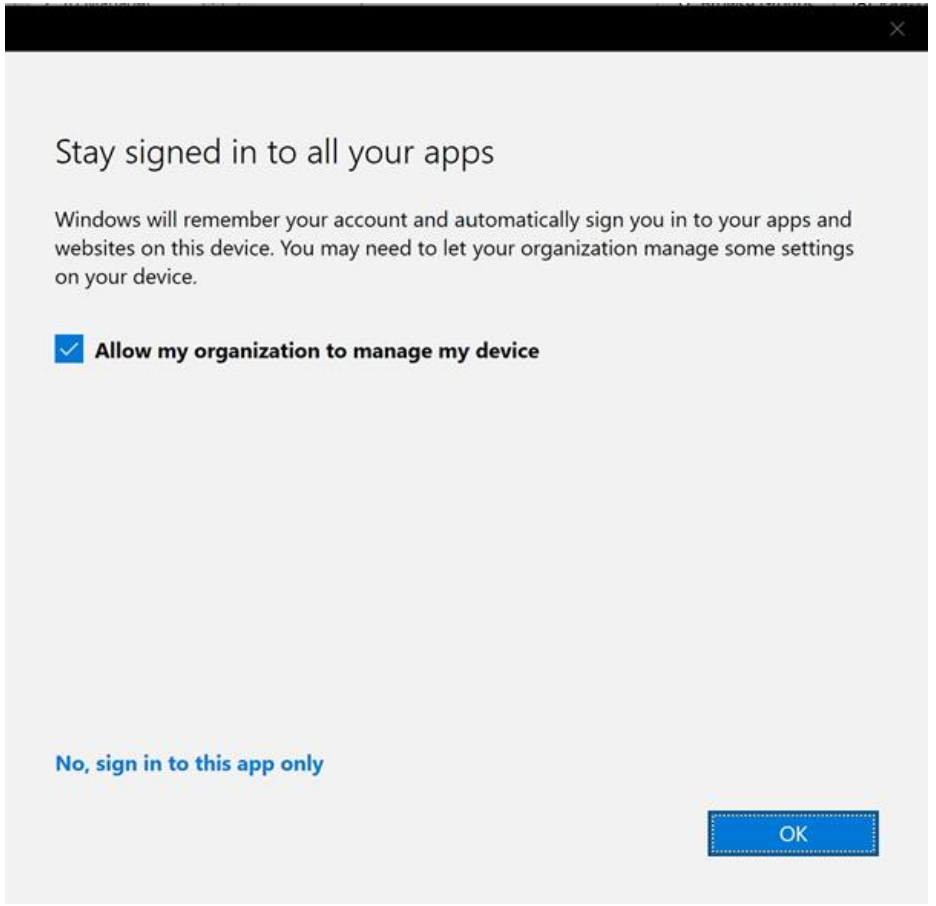


- If not Windows Hello for business is used the following endpoints can be excluded from MFA to make sure Licensing works and the pop-up ”Work or School Account Problem” is shown.



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)

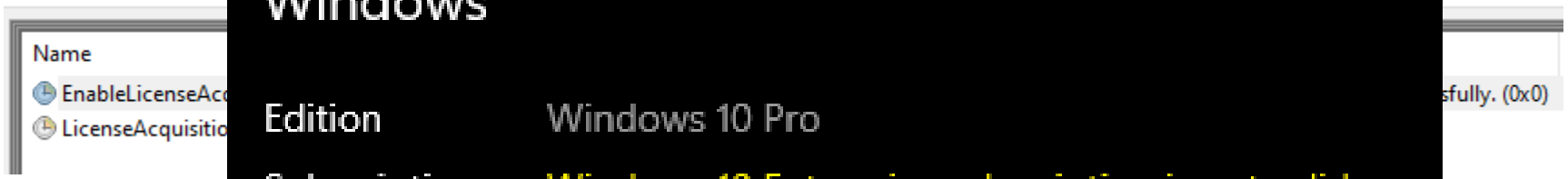
General | Details

Service Fault: status: 400 code: SingleTenantIdExpectedForAadUsers: description: All Aad users provided in the request are expected to be associated to a single Tenant. data: ["3"] (Corr: , Svr: ent), token broker error: 0x00000000, number of MSA tickets: 1, number of AAD tickets: 3
Function: LogServiceFault
Source: onecoreuap\enduser\winstore\licensemanager\lib\telemetry.cpp (134)

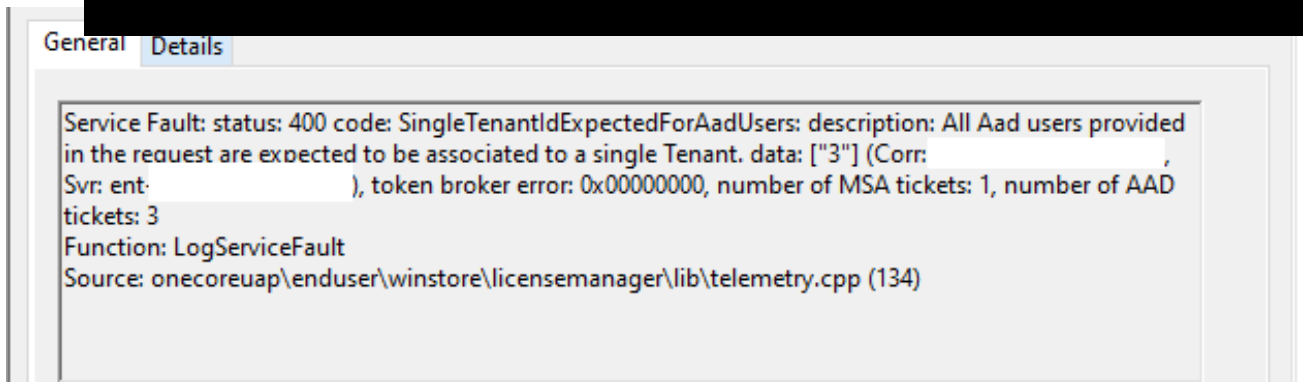
https://ccmexec.com/2021/01/mem-windows-10-personal-device-and-sync-issues/

Subscription based activation

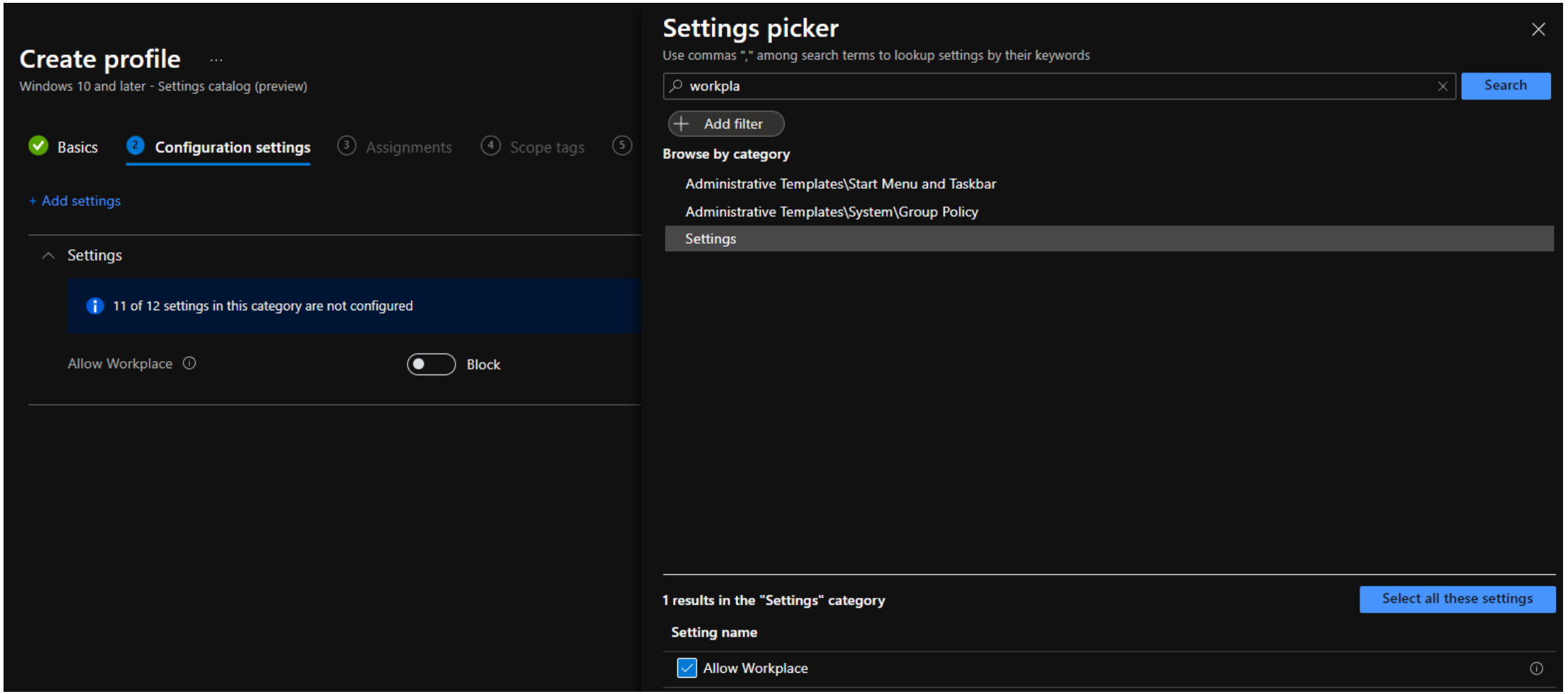
- Re-activated every 30 days
- Two scheduled tasks triggers License Acquisition



- The store does the
  - In this case more

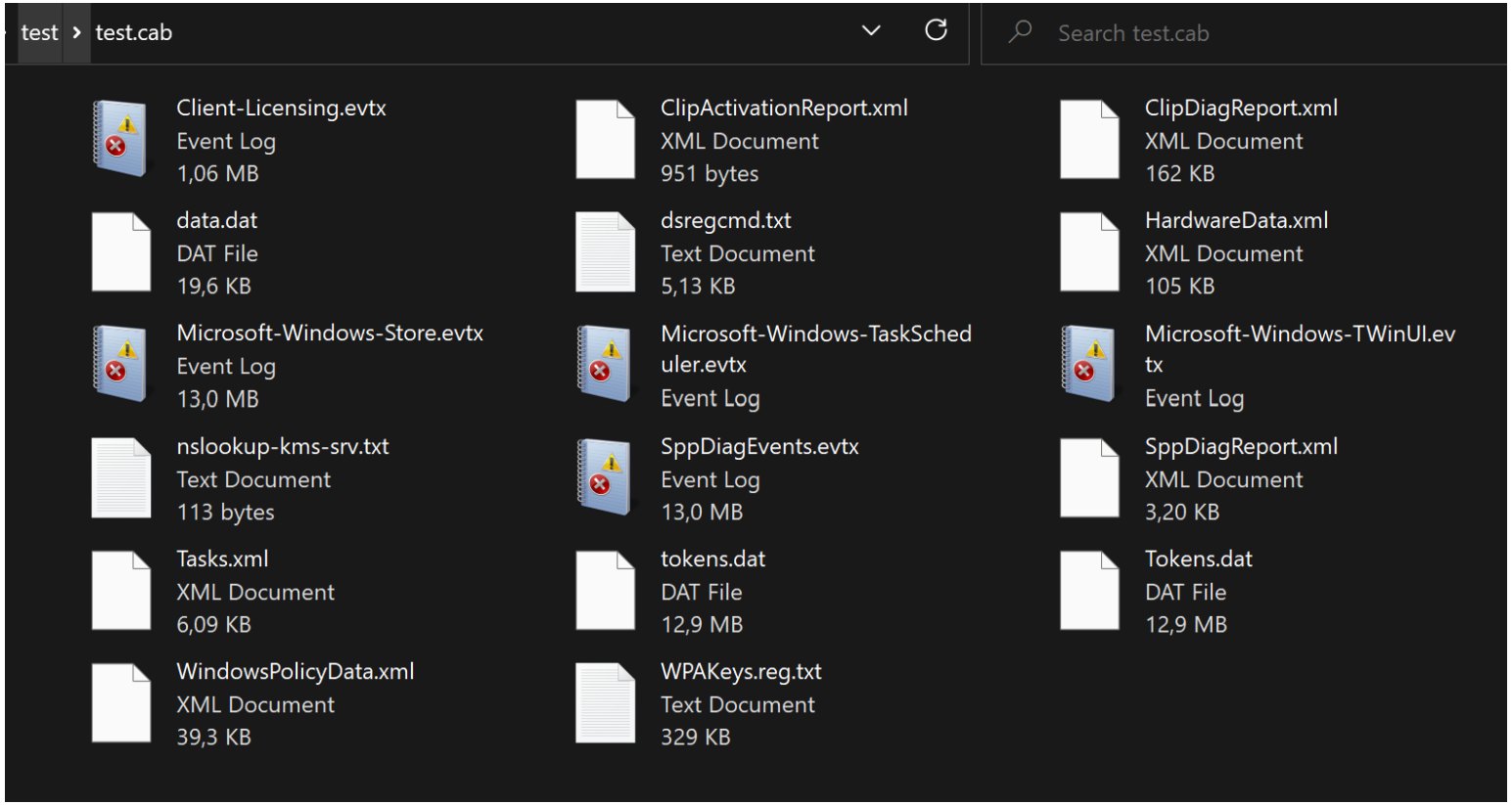


Blocking Workplace join



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.

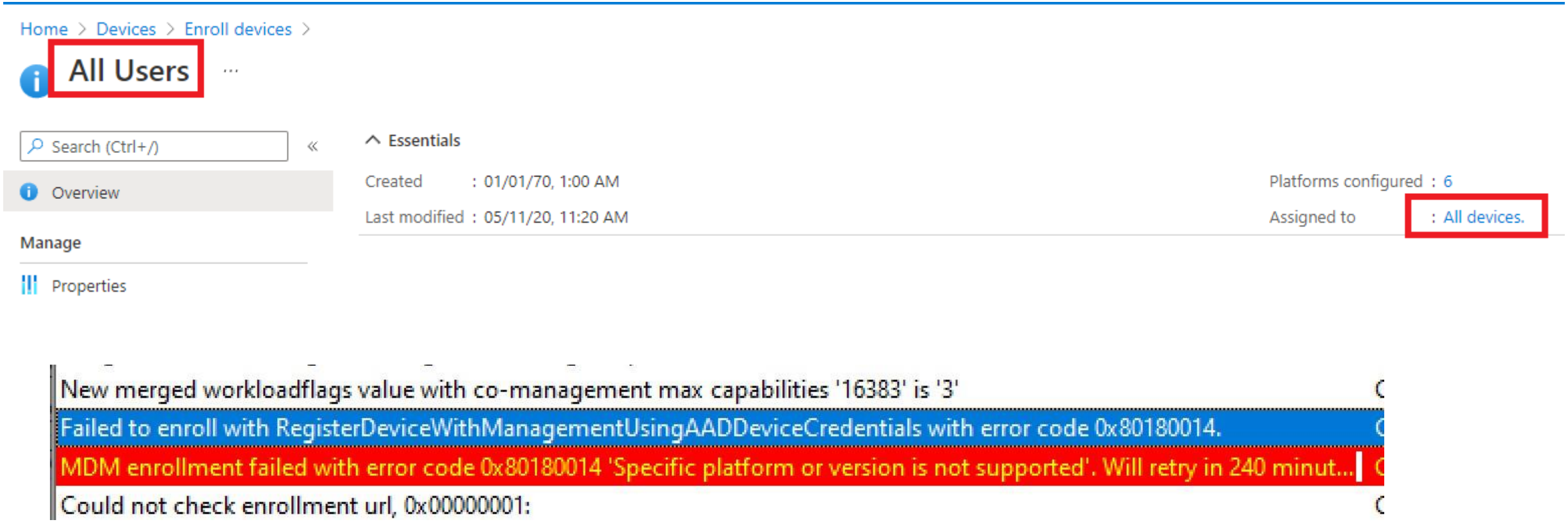
Enrolling device to MDM... Try #1 out of 3
Enrolling device with RegisterDeviceWithManagementUsingAADDeviceCredentials
Processing GET for assignment (ScopeId_B54C7DB5-E99F-4BC7-95DD-C383A9E555A9/ConfigurationPolicy_96925c8d-7753-4899-a44c-79f6...
Getting/Merging value for setting 'CoManagementSettings_AutoEnroll'
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“



Enrollment Failures

www.wpninjas.eu

Microsoft Endpoint Manager admin center

Home > Monitor

Monitor | Enrollment failures

Search (Ctrl+/)

Filter Refresh Export

For a graphical view of enrollment failures see here.

Select user All users

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.

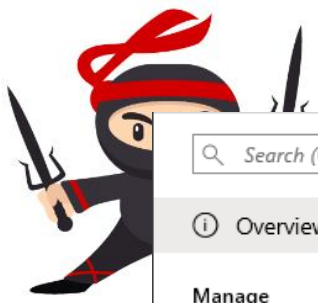
Additional problem information:

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

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.



Search (Ctrl+/)

- Overview

Manage

- Properties

Monitor

- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Security baselines
- Recovery keys
- Managed Apps

Retire | Wipe | Delete | Remote lock | Sync | Reset passcode | Restart | Fresh Start | Autopilot Reset | Quick scan

Device name	: APENTO-Bndfil1Z	Primary User	: Ronni Pedersen
Management name	: mail_Windows_5/26/2019_6:52 PM	Enrolled by	: Ronni Pedersen
Ownership	: Corporate	Compliance	: Not Compliant
Serial number	: 7987-3600-6266-3074-4536-7994-21	Operating system	: Windows
Phone number	: ---	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 yo
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

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

Policy and Profile refresh cycles

Existing Devices

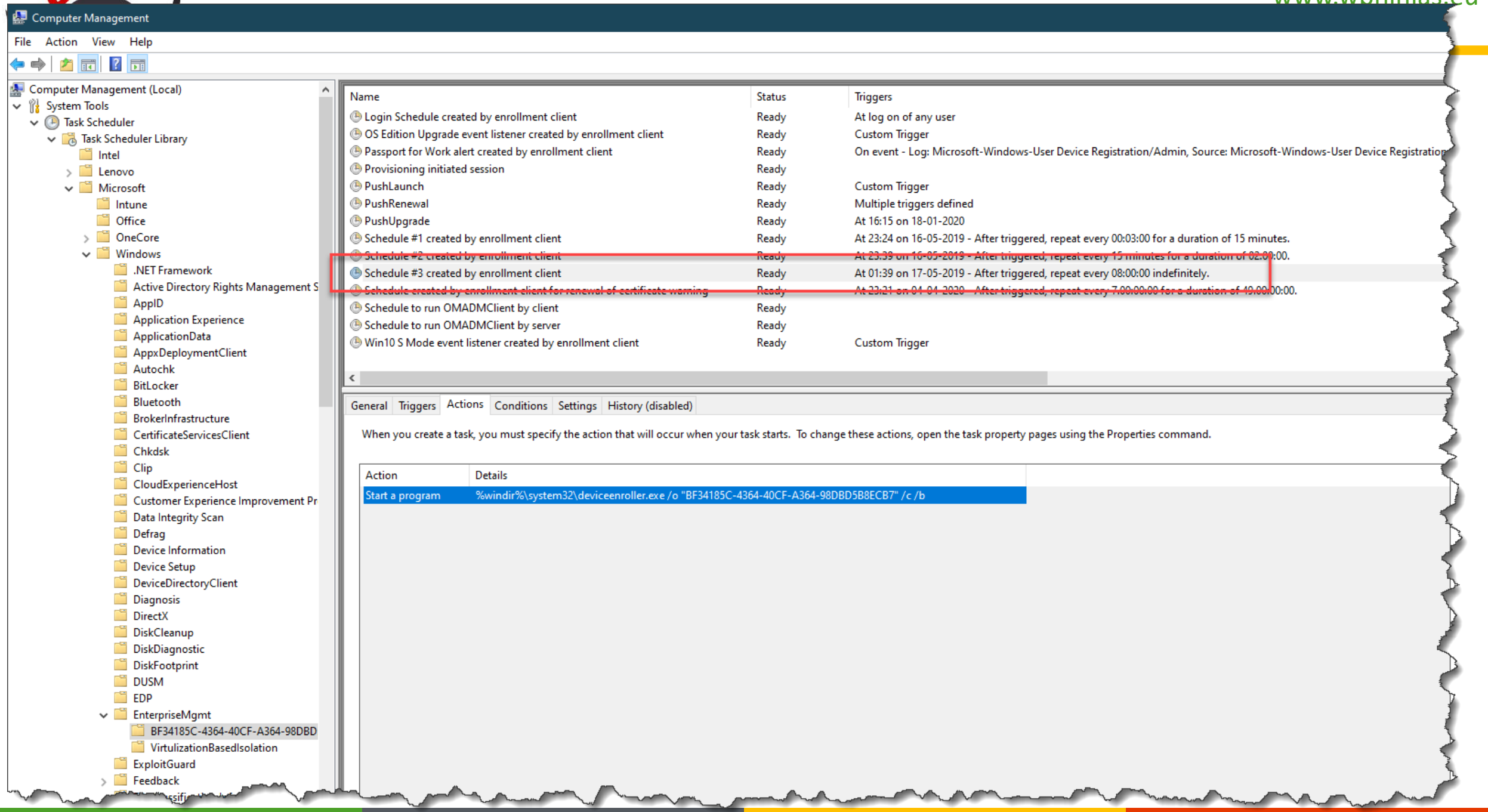
- Windows devices will schedule check-in with the Intune service: About every 8 hours

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

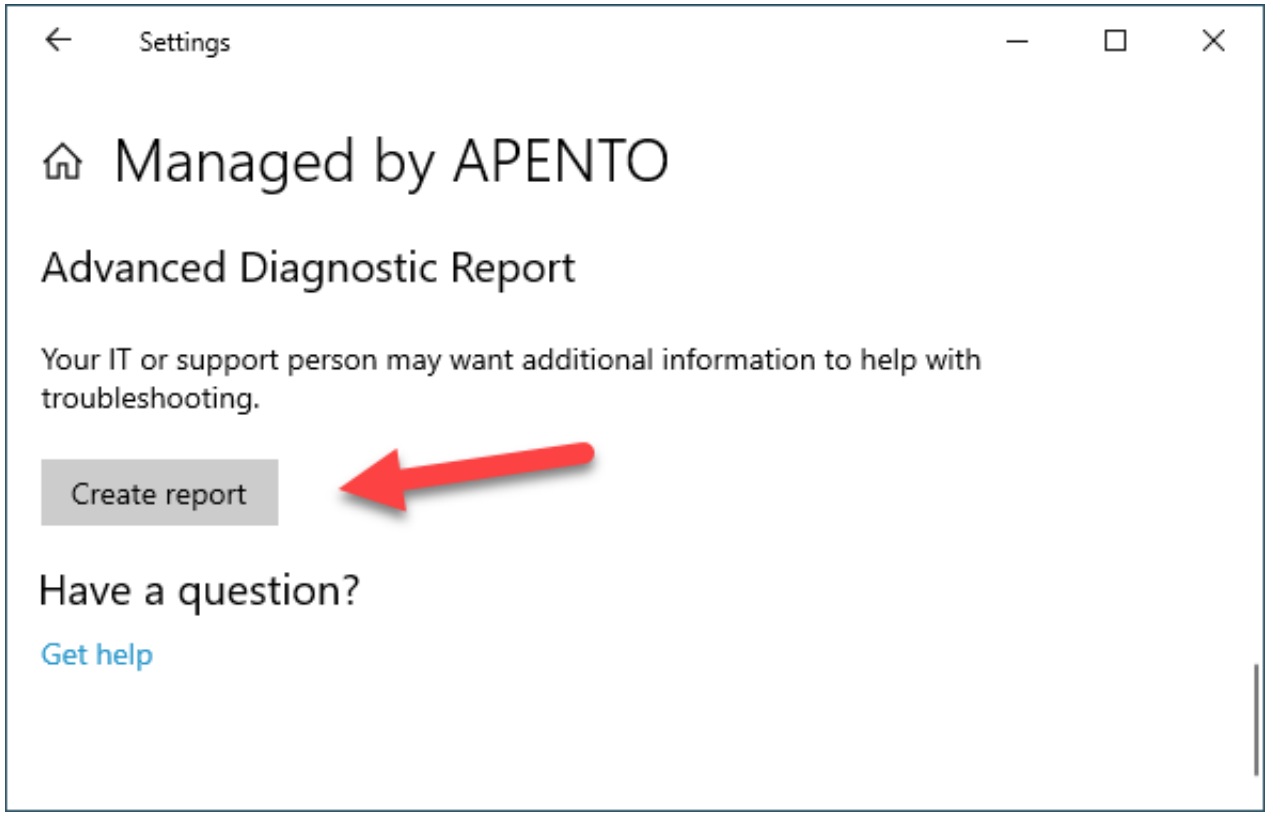
- Manually using Script

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

www.wpninjas.eu

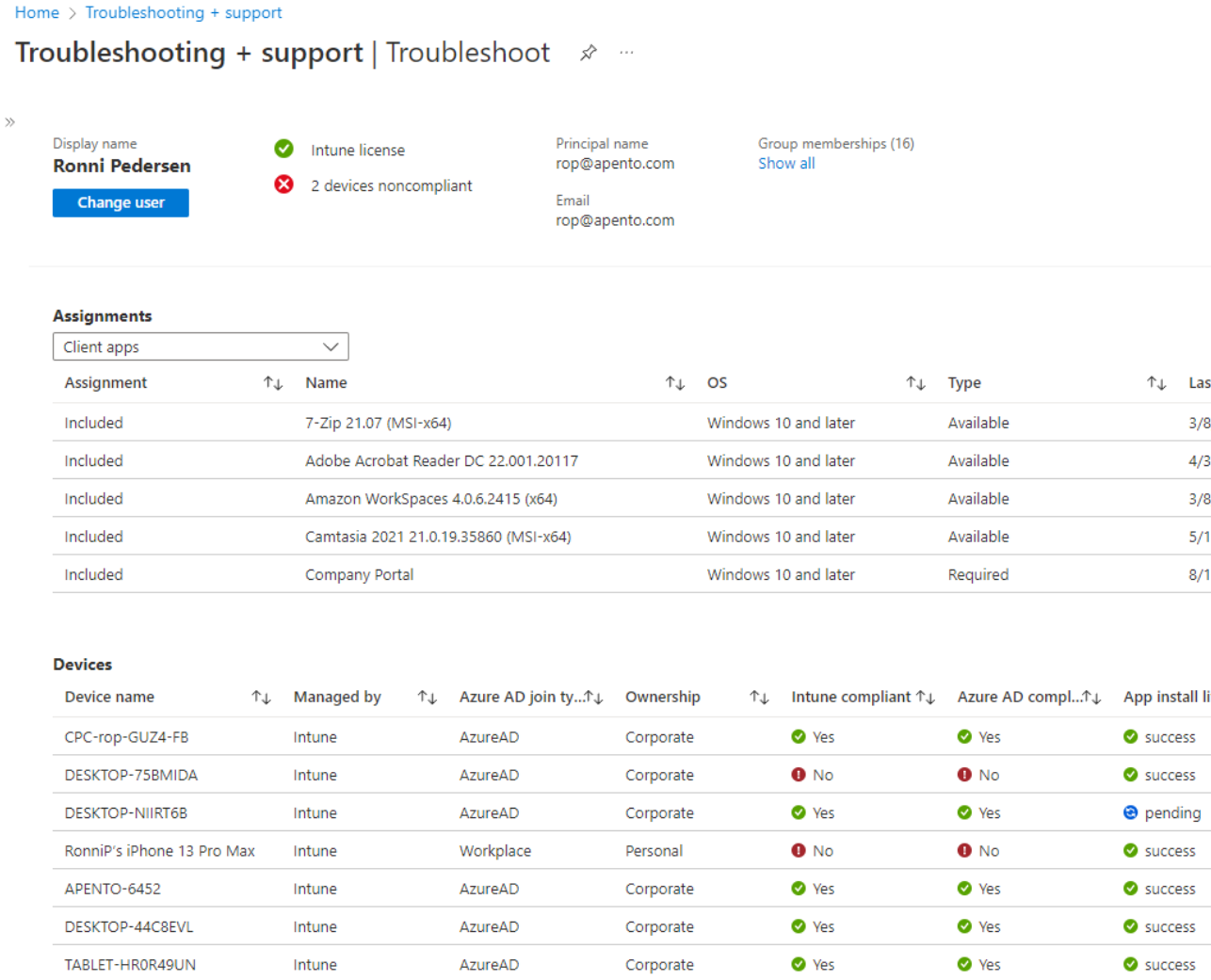
Intune portal page

- https://aka.ms/intunetroubleshooting

Displays information focused around a particular user

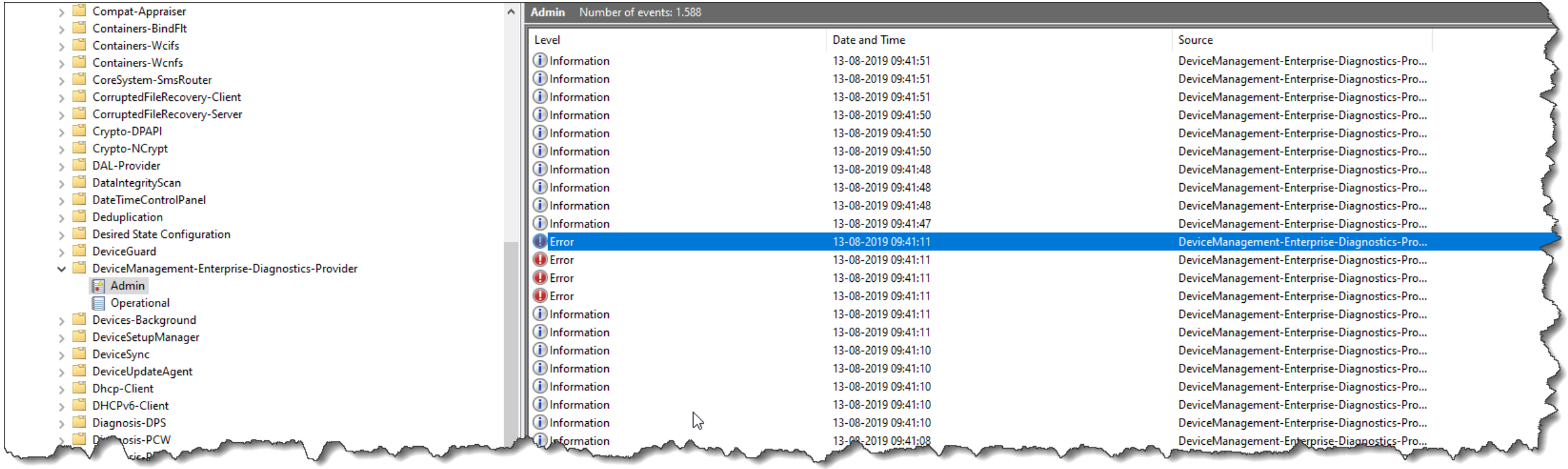
- See info about assignments, devices, enrollment failures, etc.

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

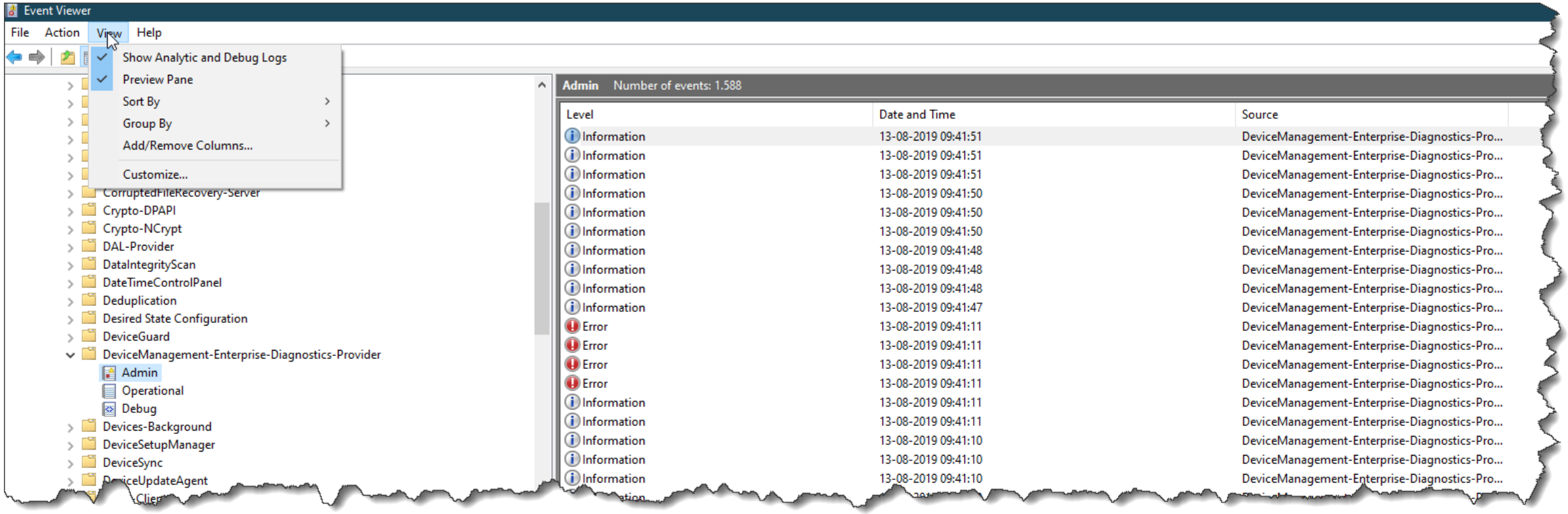


Device Profiles - Where is my logs?

- Event viewer is your new best friend
  - Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider



Enable debug mode



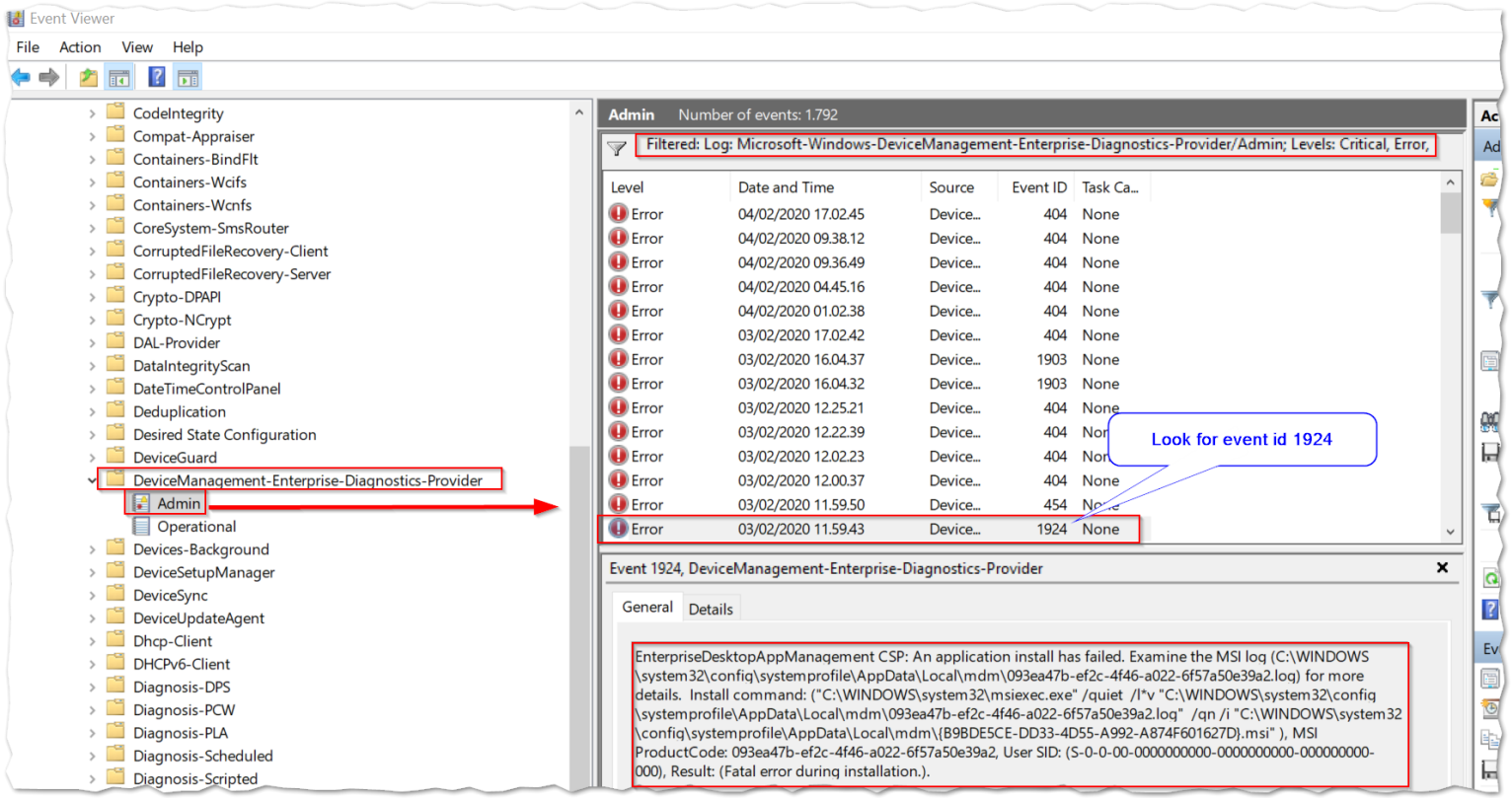
Intune Management Extension

Intune Management Extension

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

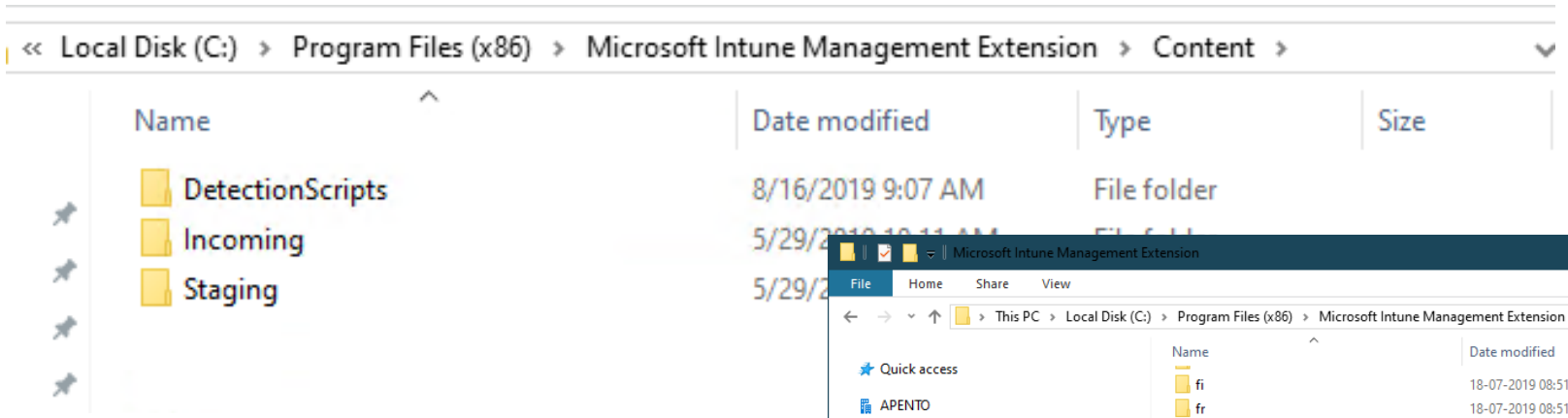
Intune Management Extension Event log

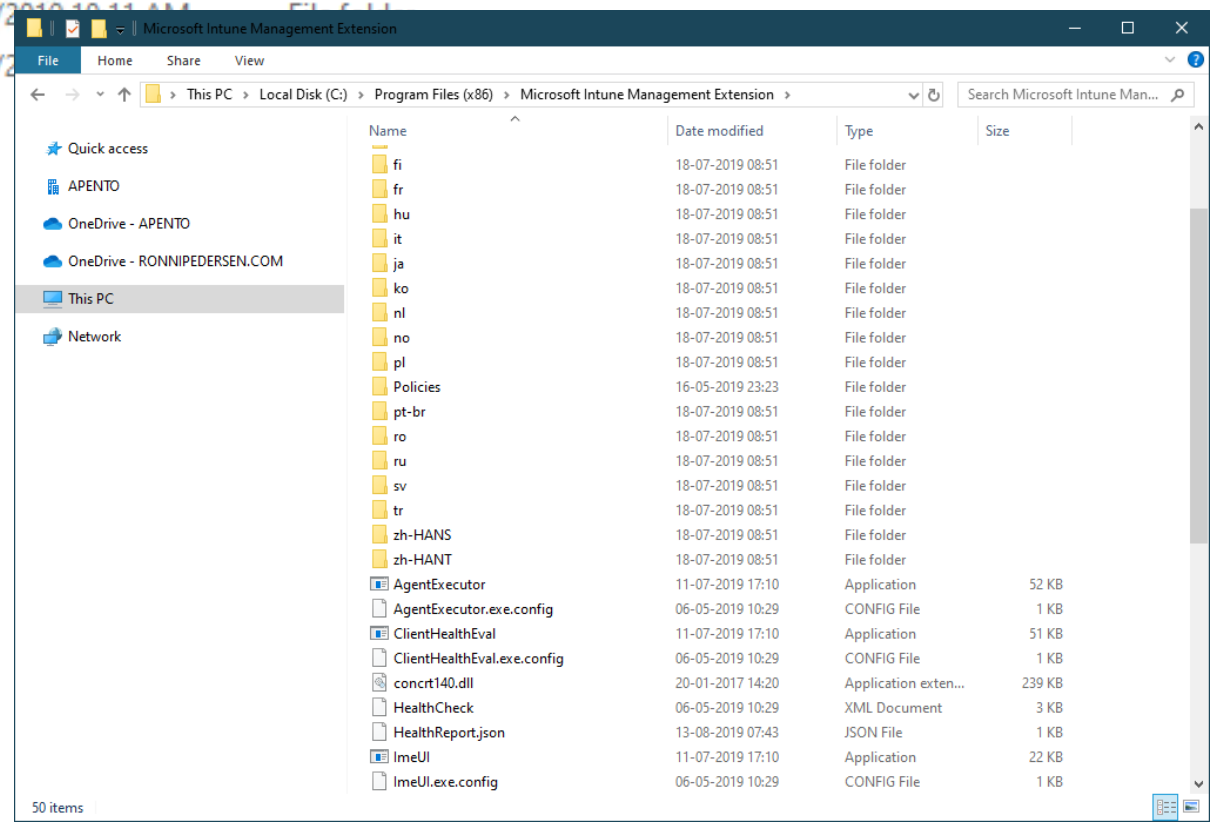
- Applications and services logs\Microsoft\Windows\DeviceManage…



Intune Management Extension File System

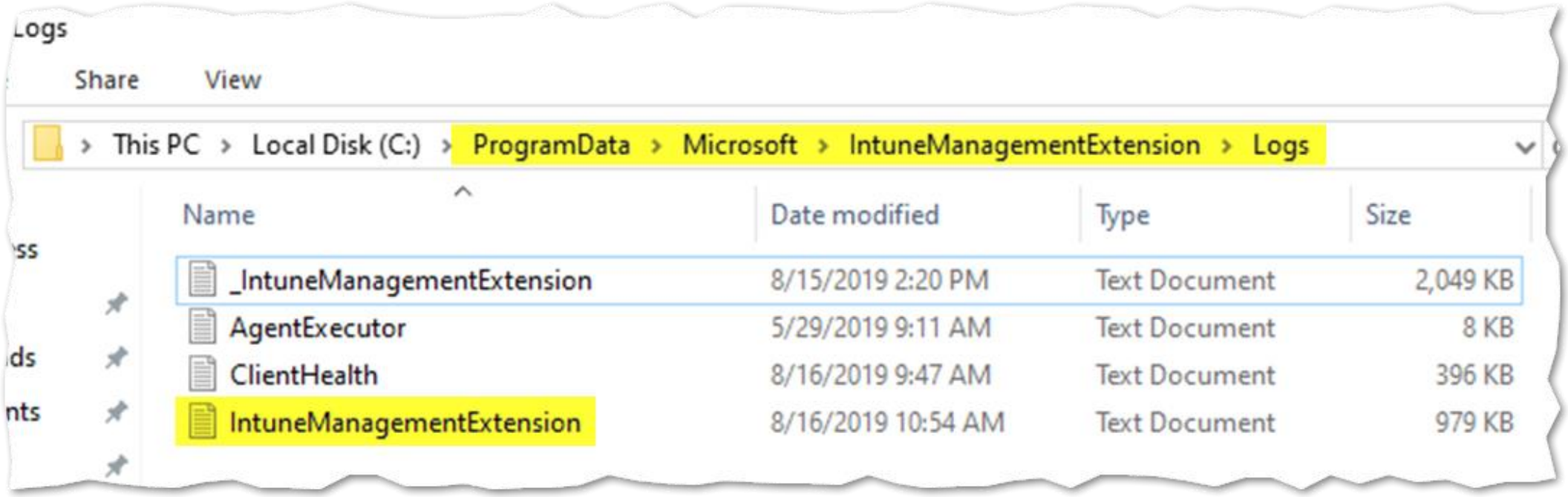
www.wpninjas.eu





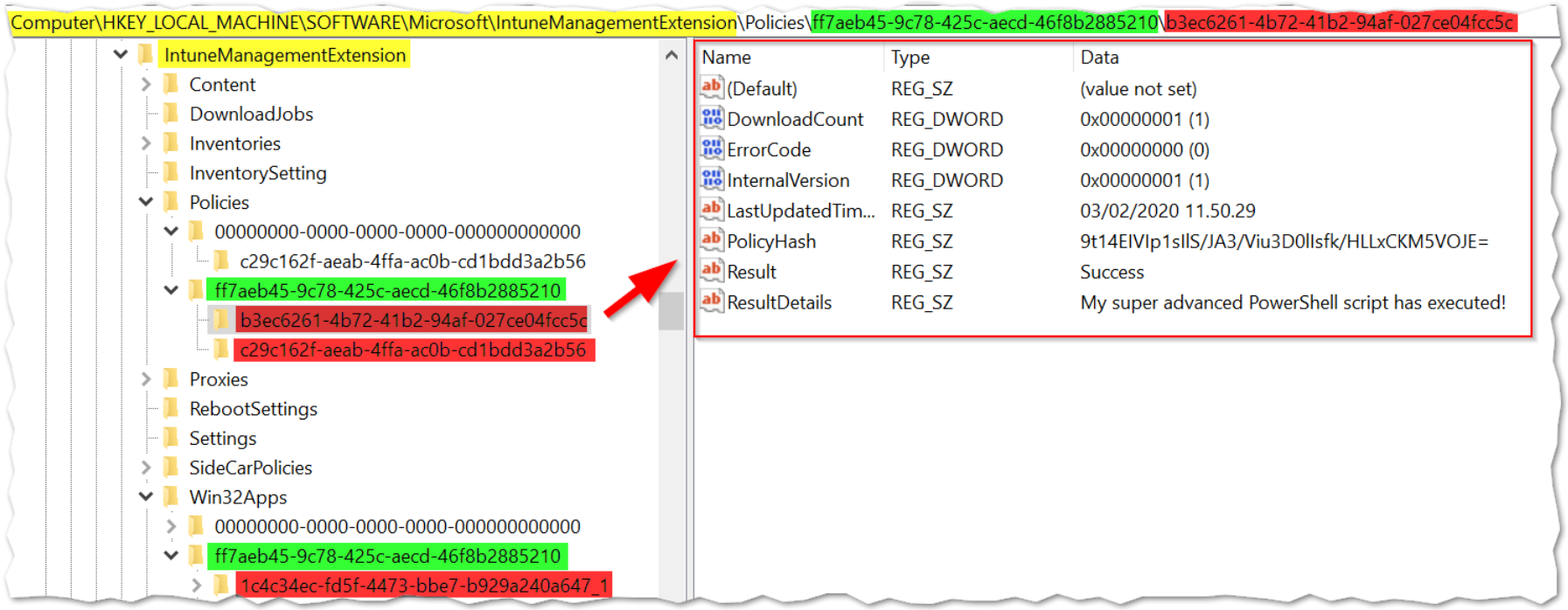
Intune Management Extension Log files

- Log files: "C:\ProgramData\Microsoft\IntuneManagementExtension\logs"



Intune Management Extension The Registry

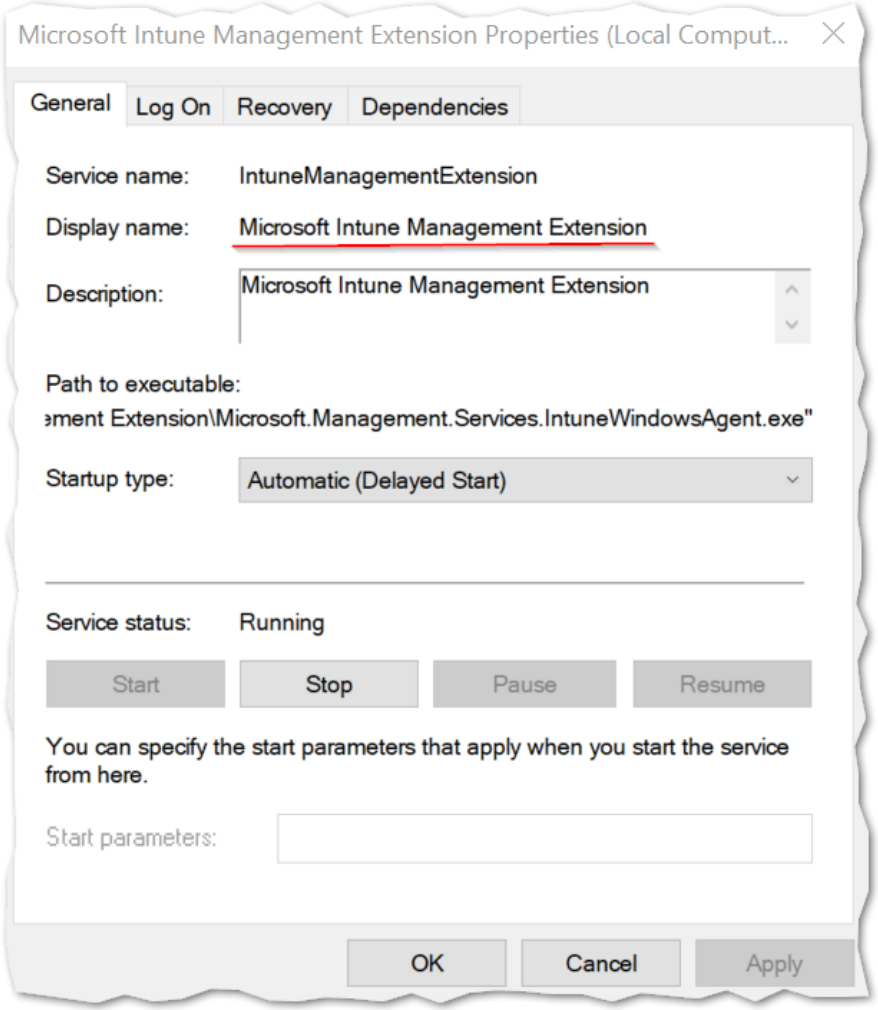
- Yellow: IME Root Registry Key
- Green: Azure AD Object ID of the User
- Red: Application / Policy GUID



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



Win32 apps

TIP #1

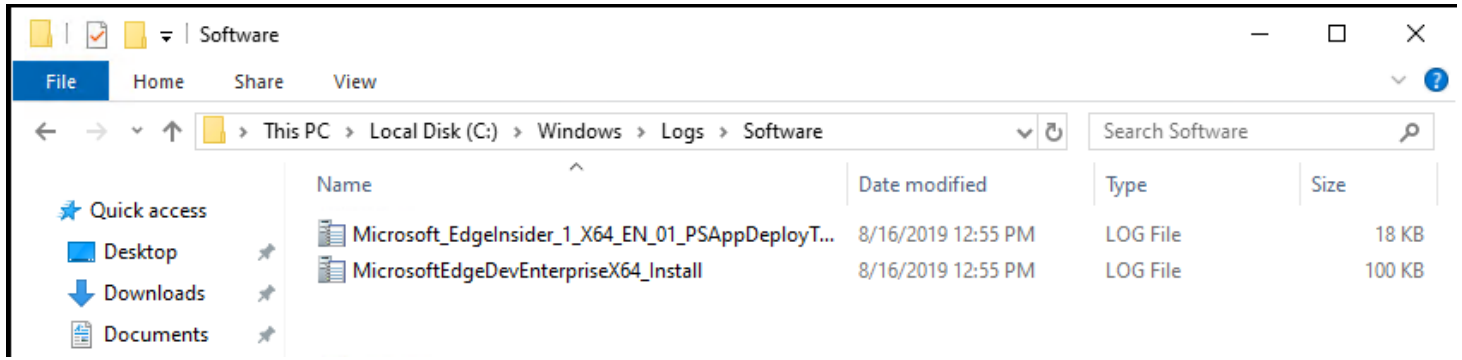
- **Always** test the application outside of Intune first !!!

PowerShell App Deployment Toolkit

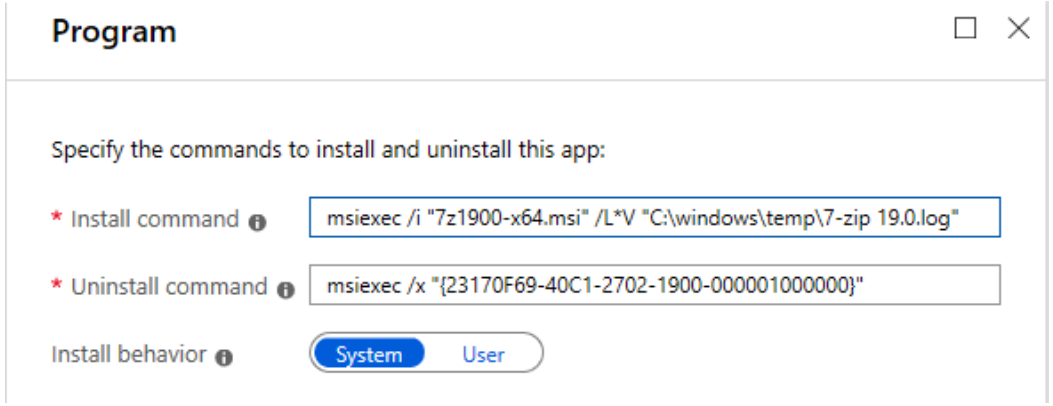
- **Easy To Use** – Any PowerShell beginner can use the template!
- **Consistent** – Consistent look and feel for all application deployments.
- **Powerful** – install/uninstall, setting registry keys, copying files, etc.
- **User Interface** – Custom dialogs boxes, progress dialogs and balloon tips.
- **Localized** – The UI is localized in several languages.
- **Extensible** – Can be extended to add custom scripts and functions.
- **Helpful** – Detailed logging of all actions performed

Use the tools you know

- PS App Deployment Toolkit logging example:



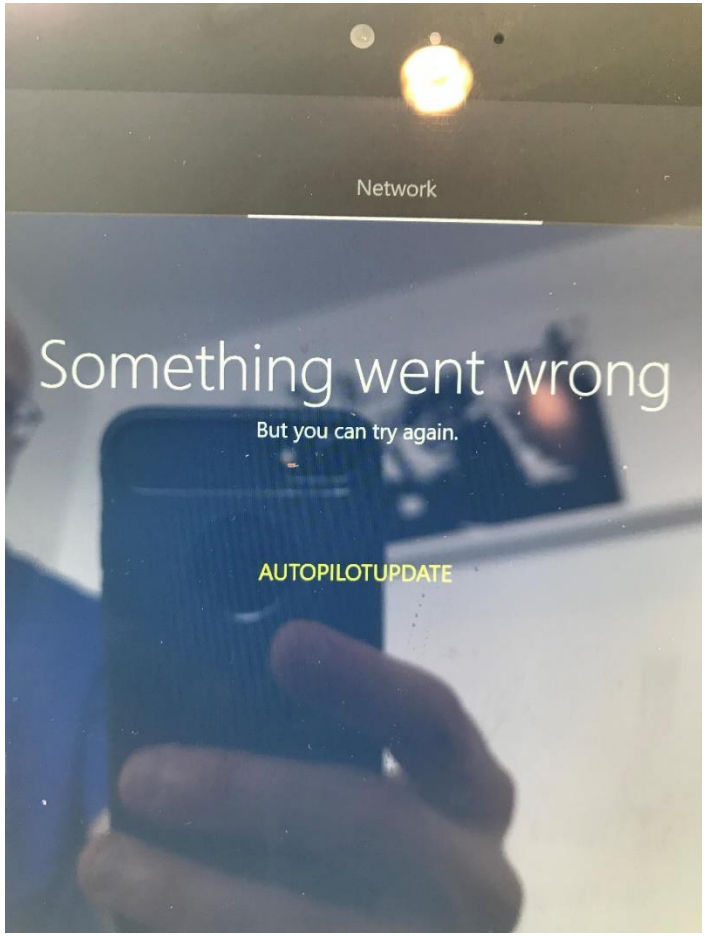
- Use /L*V for MSiexec command lines so we have log files



Windows AutoPilot

Network

- A network for enrollment is needed
- Guest network, open network
- All ports, URL required must be opened



Meet BOB – your new network admin

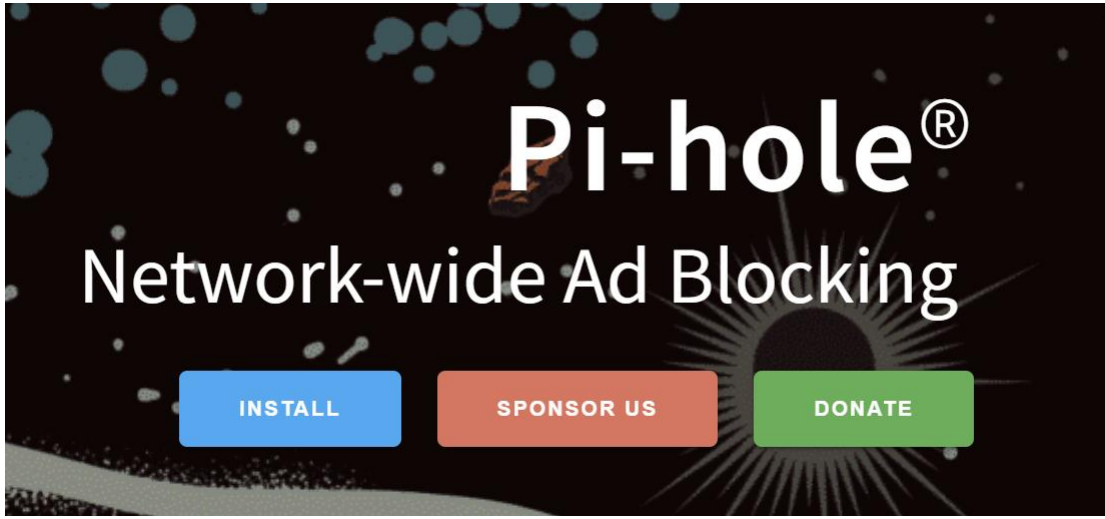
Network issues – we have seen

- “Pi-Hole” blocking all traffic to Microsoft URLs used.
- Home routers/Wi-Fi with IPS.

“My son setup our home network, no idea what he did”.

“It is a different organization name showing up when I start my computer”.

Your co-workers kids or neighbor are the new network department!



Shift+F10

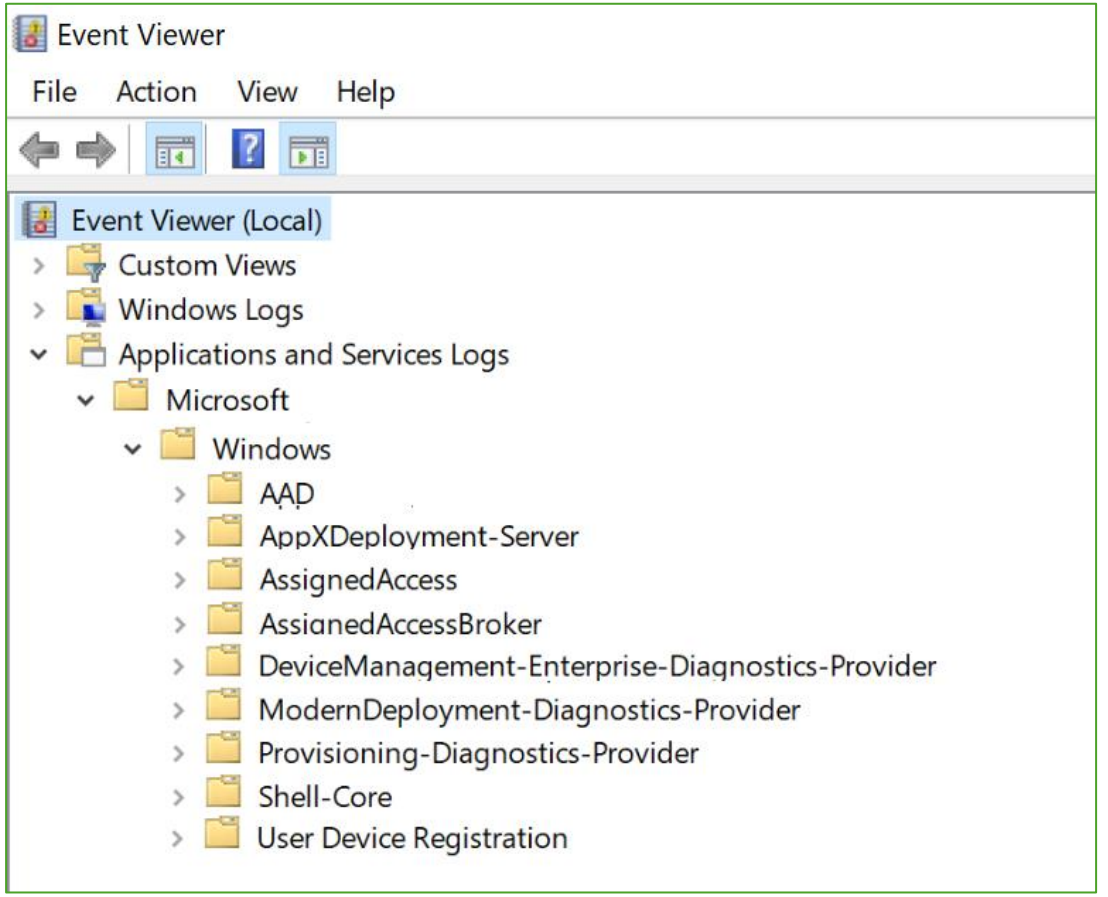
- Great for troubleshooting
  - Can be a security concern for some customers

- Disable by placing **DisableCMDRequest.TAG** in the **C:\Windows\Setup\Scripts** folder.
  - Needs to be there when the computer starts up. Must be added by OEM.

Troubleshooting

Troubleshooting

- Grab all potentially-interesting information:
  - Event logs
  - Registry, configuration data
  - TPM details (1809+)
  - ETL trace files
- Windows 10/11
  - MDMDiagnosticsTool.exe -area Autopilot;TPM -cab C:\temp\Autopilot.cab
- Analyze offline



Setting up for work or school

We ran into a problem with one of the following setup steps.
For more help, contact your organization's support person.

Device preparation

Completed

Device setup

Error

Security policies (1 of 1 applied)
Certificates (1 of 1 applied)
Network connections (No setup needed)
Apps (0x81036502)

Account setup

Waiting

For more details, view diagnostics.

Continue anyway

Reset device

Try again

Windows Autopilot diagnostics

Policy Provider Installation

Device-Targeted Apps Installation

Start Time 2022-05-22 01:05:12

Finish Time 2022-05-22 01:08:36

Device-targeted apps installation encountered an error and could not be completed. Error: 0x00000000

Device-Targeted Policies Installation

Device-Targeted Network Profiles Installation

Device-Targeted Certificates Installation

User-Targeted Apps Installation

Close

Export logs

Thank You