Troubleshooting the MEM managed Windows 11 Client - Deep Dive

Ronni Pedersen

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

Contact Info

- Mail: rop@apento.com
- Twitter: @ronnipedersen

APENTO

Jörgen Nilsson

- Principal Consultant
- 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
- Troubelshooting Subscription based activaton
- Troubleshooting Enrollment
- Troubleshooting Policies
- Applications
- Windows Autopilot

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/

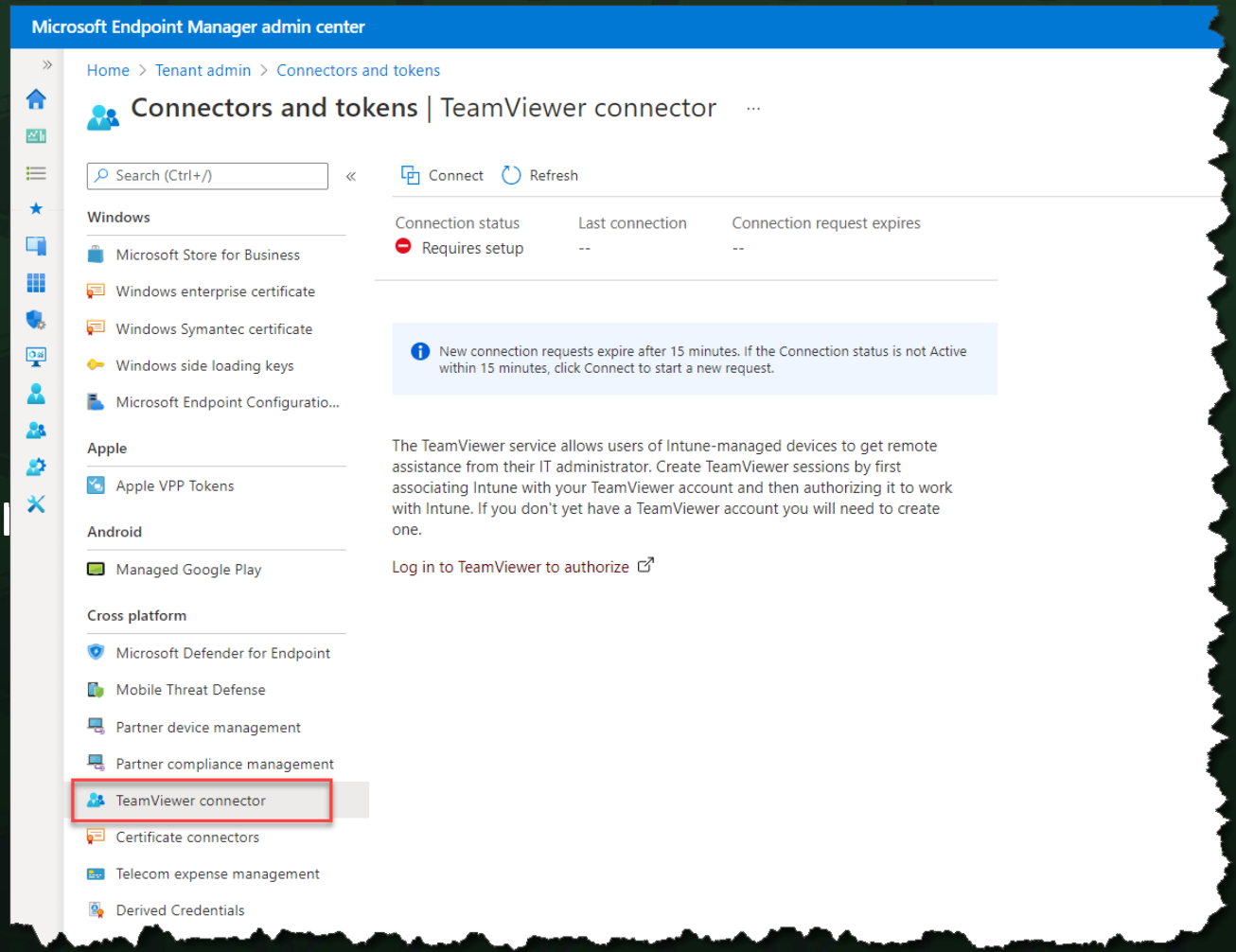
Configure the TeamViewer connector

- Easy setup and configuration

There are other options:

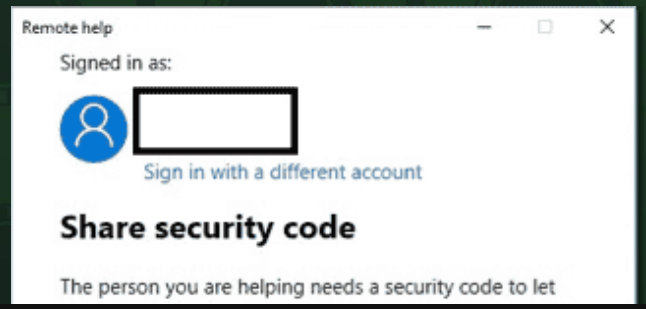
- Beyond Trust
- LogMeIn
- Remote Help!

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



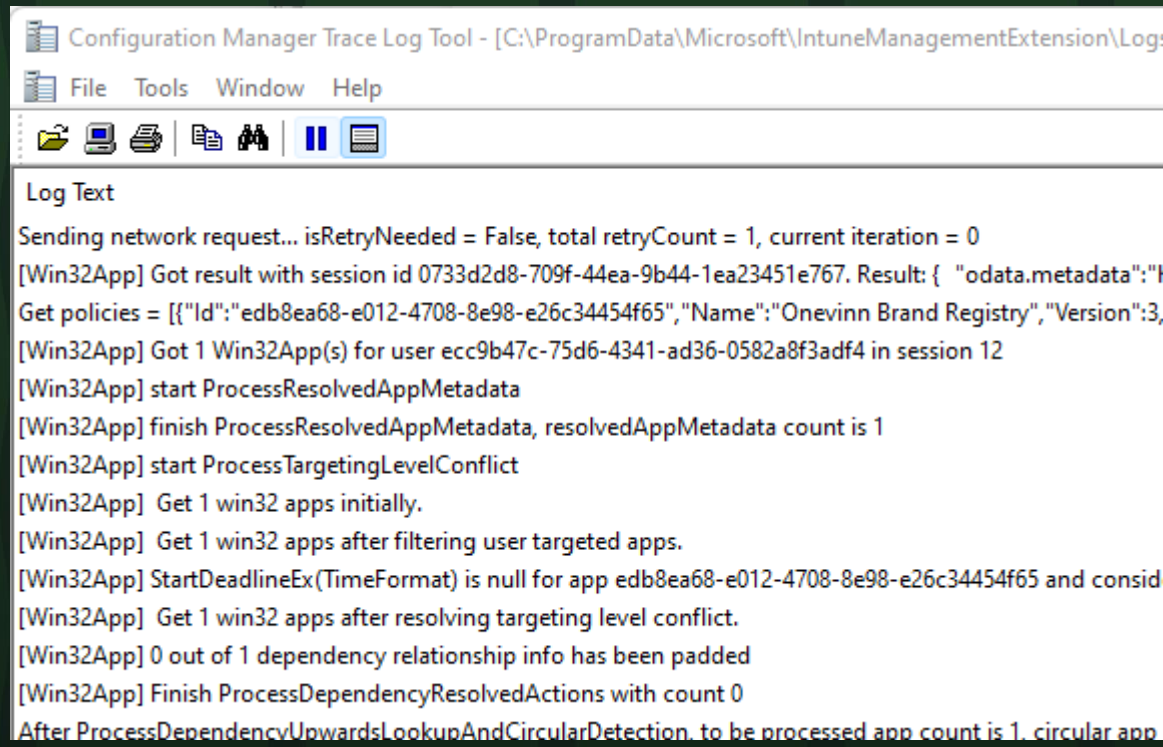
Microsoft Remote Help

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



CMtrace

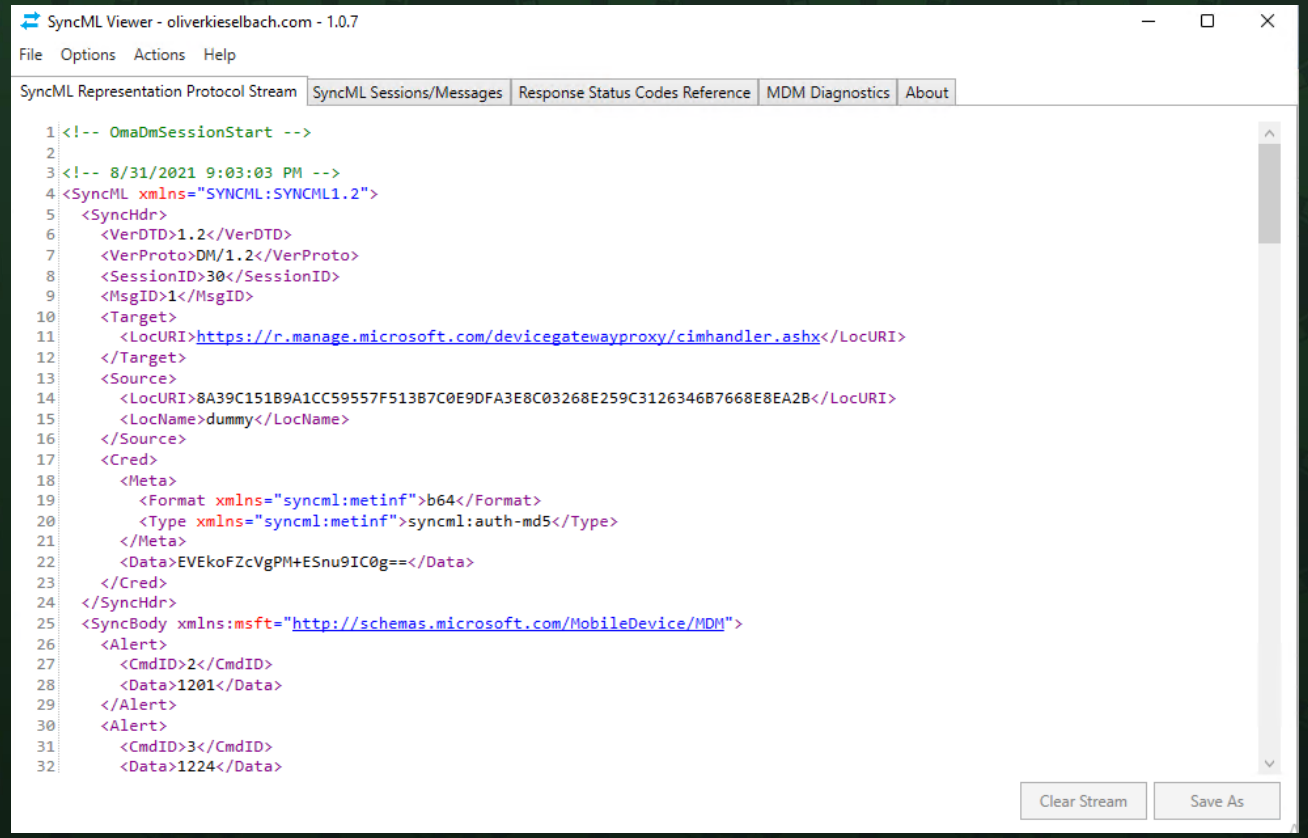
- Great log reader
- Not free but included in the Intune/MEM
- Deploy it to all clients



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

More Tools – advanced troubleshooting

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



[SyncMLViewer/SyncMLViewer/dist at master · okieselbach/SyncMLViewer · GitHub]

```
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>
```

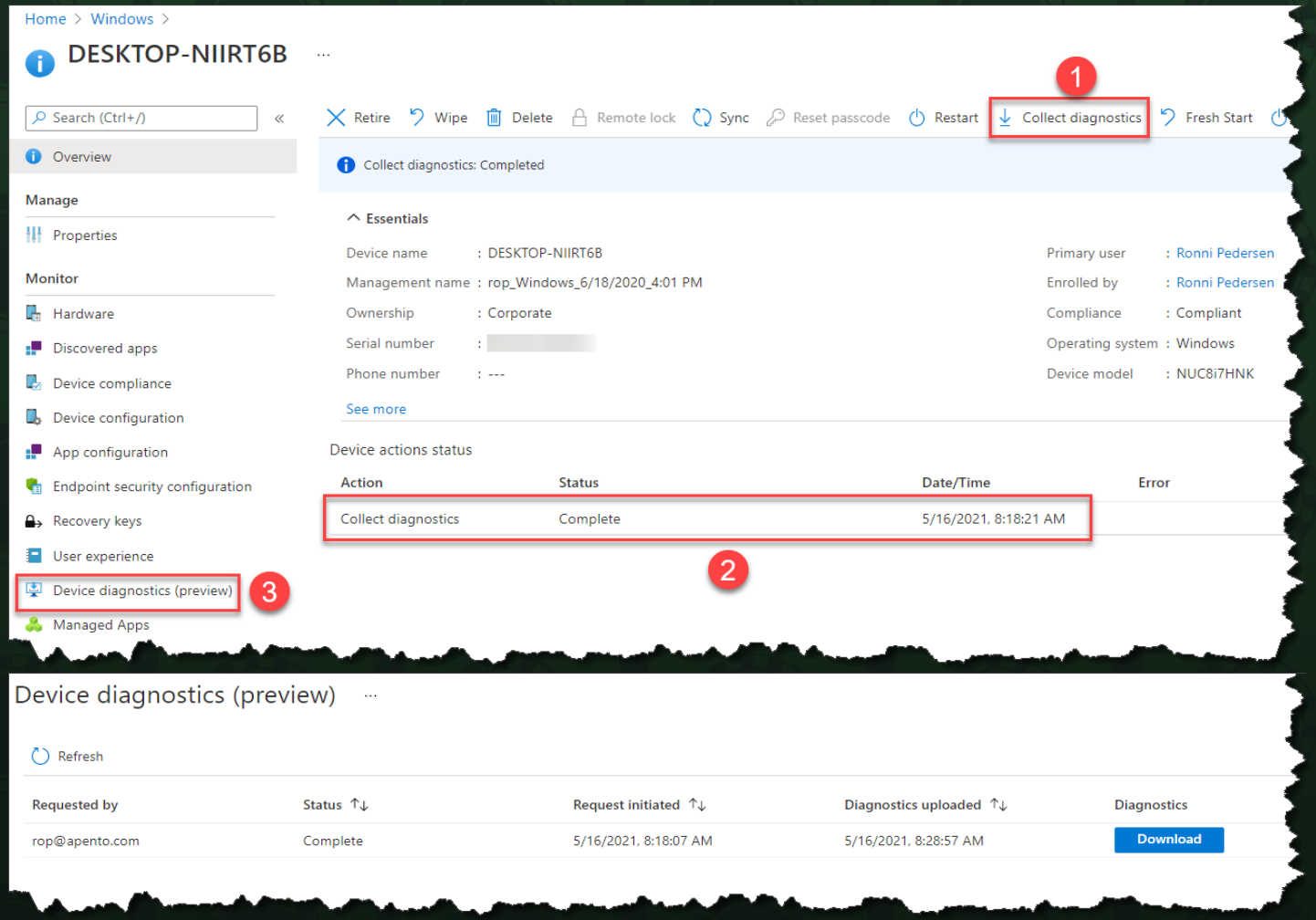
Log Files

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



Configuration Policy Process

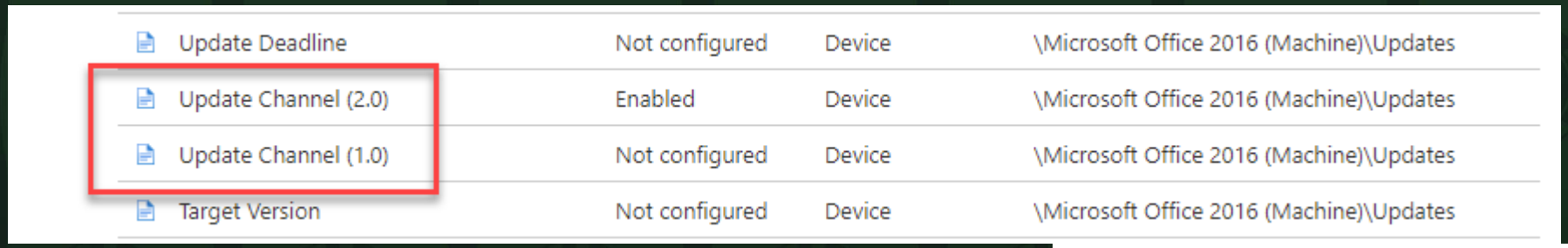
Microsoft 365 Apps Policy

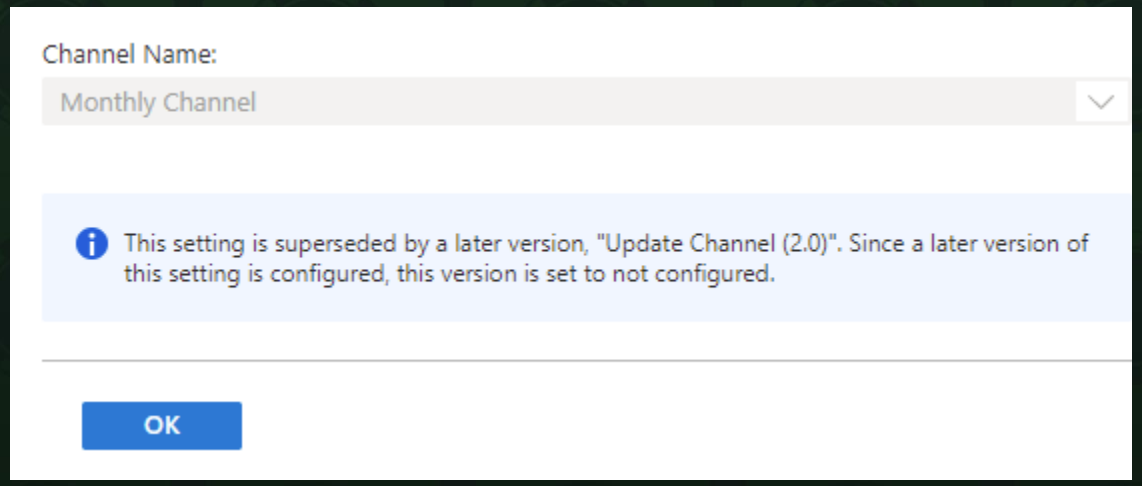
- Endpoint Manager Configuration:
  - Policy 1: Enable Microsoft 365 Apps Automatic Updates
  - Policy 2: Set the Update Channel

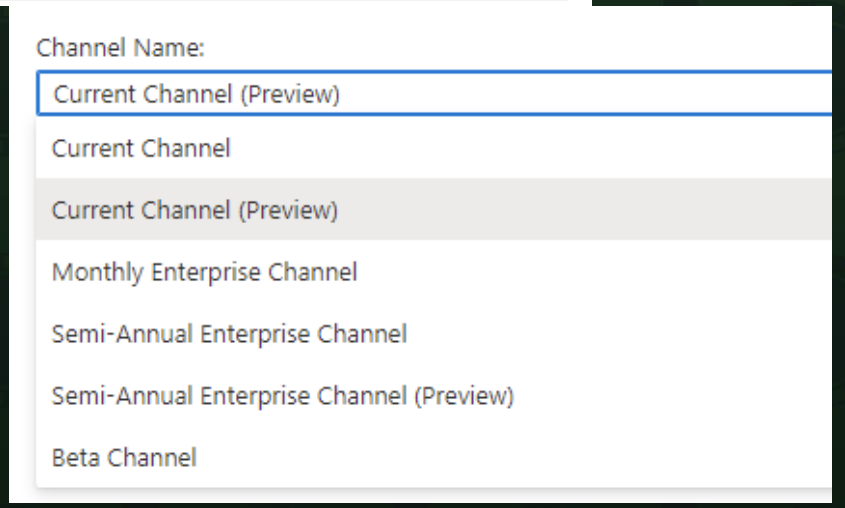
- Client-Side debugging:
  - #1 Check the Intune registry keys
  - #2 Check the Office registry keys
  - #3 Force Office automatic updates to run
  - #4 Force the Office synchronization to update account information

Administrative Templates

- Example using Administrative Templates

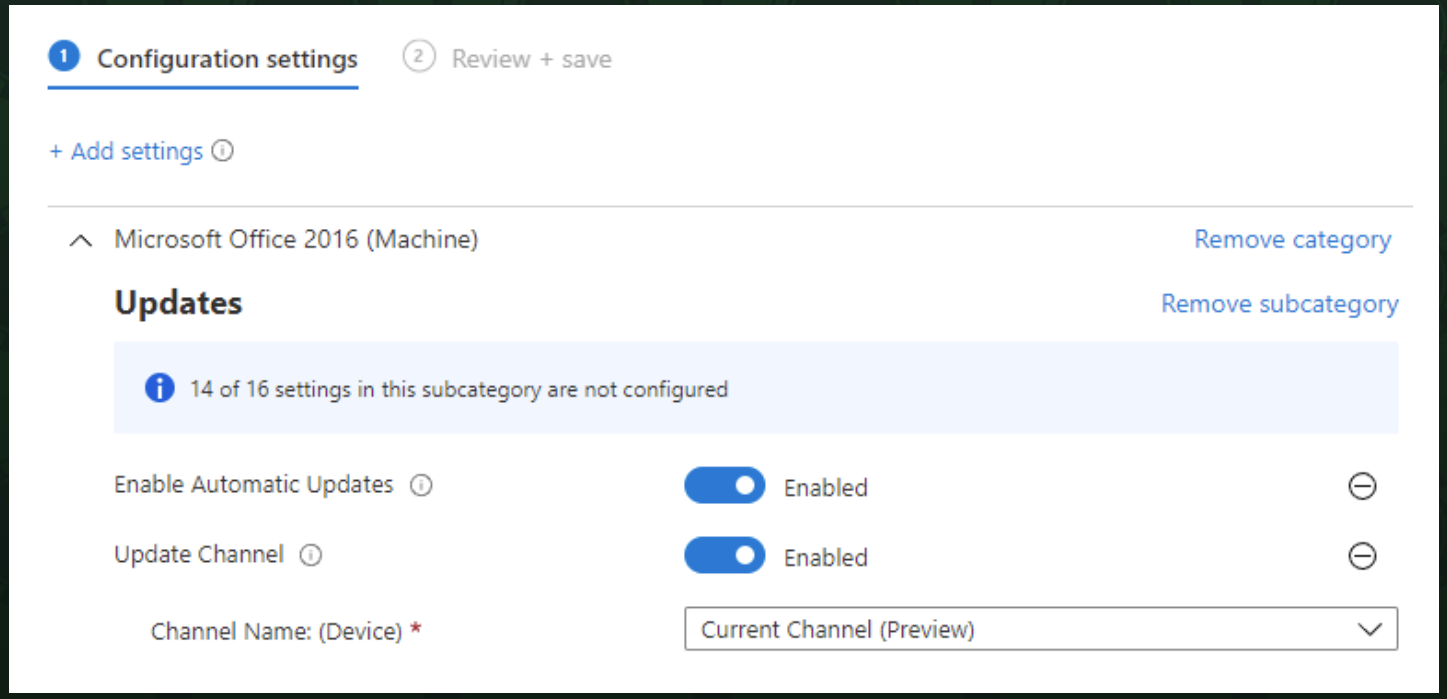






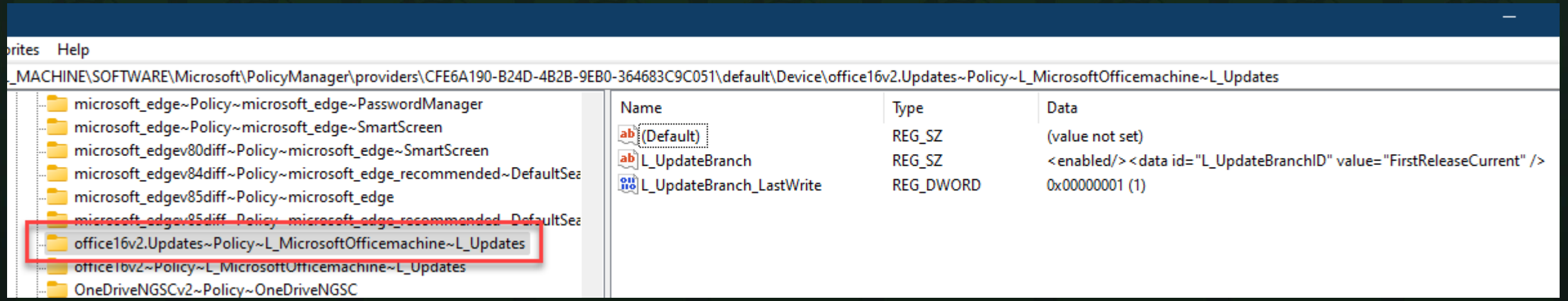
Using Settings Catalog (Preview)

- 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.

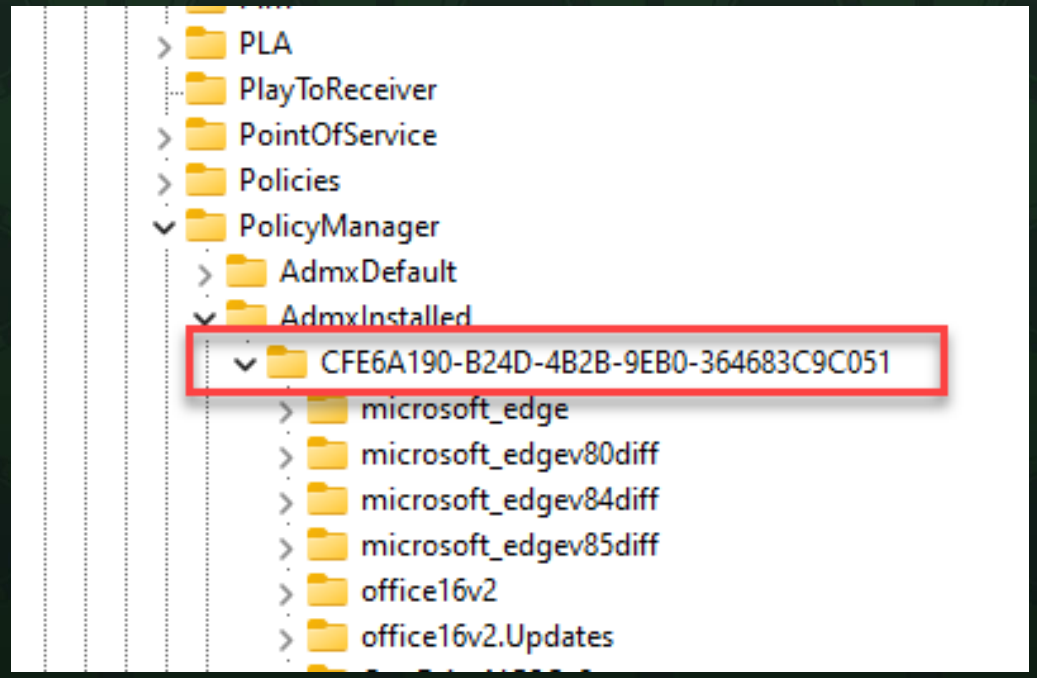


#TIP: Find the Provider ID

Find the provider ID for your device

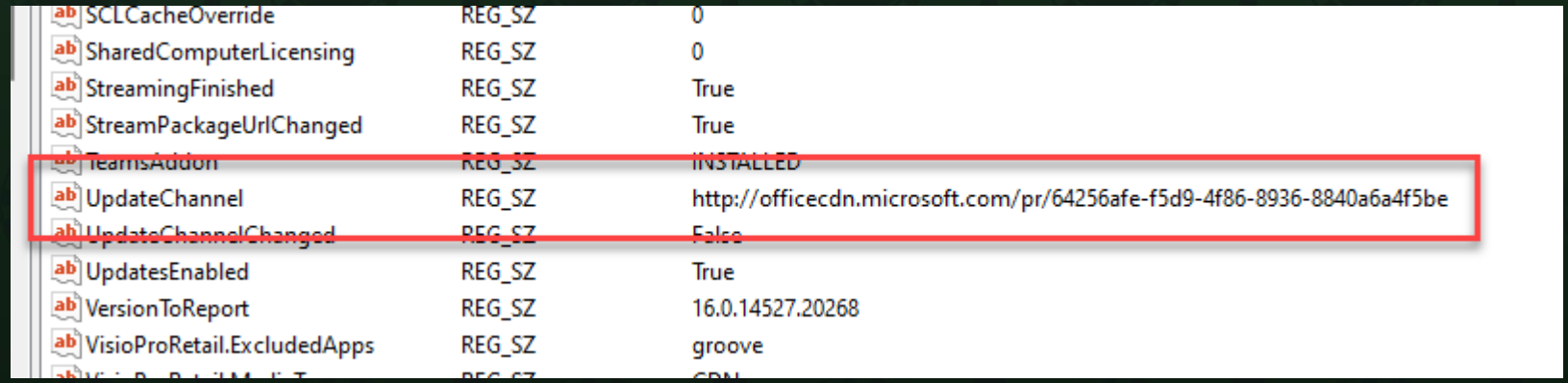
- Open the Registry Editor, and go to:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\AdmxInstalled



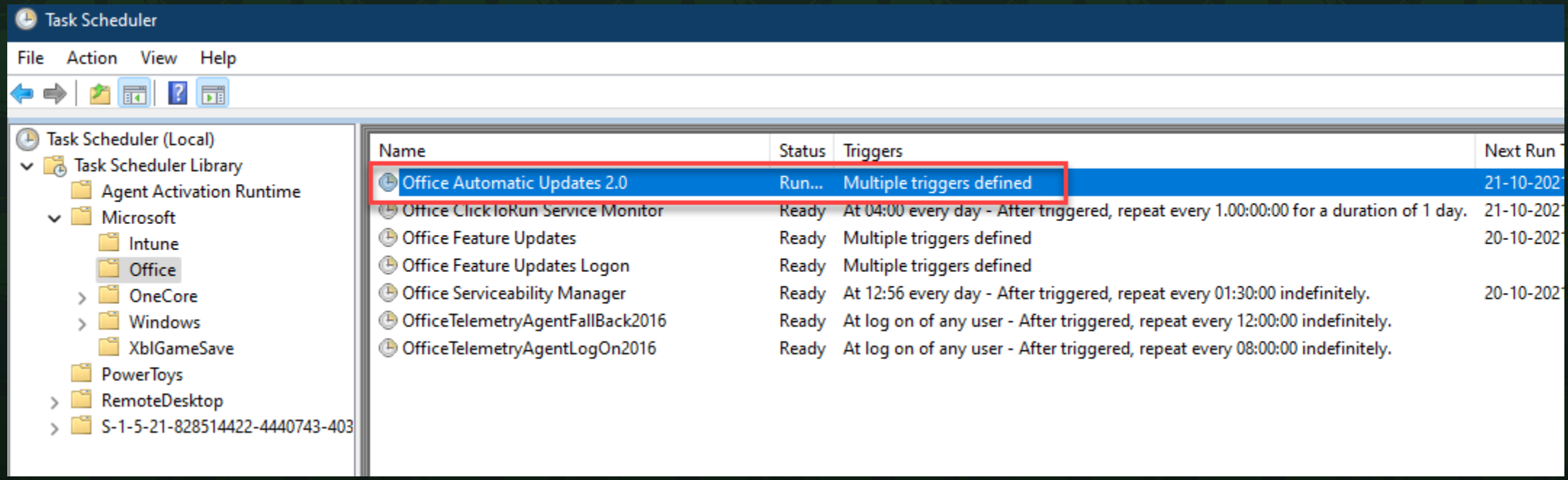
#2 Check the Office registry keys

- 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"



Device Scope vs. User Scope Settings

- **User Scope** policy writes to HKEY_CURRENT_USER (HKCU)
- **Device Scope** policy writes to HKEY_CURRENT_MACHINE (HKLM)

- When a device check-in to Intune, the device always presents a **deviceID**. The Device may or may not present a **userID**, depending on the check-in timeing and if a user is signed in.

Device Scope vs. User Scope Settings

- If a **Device Scope** policy is assigned to a **Device**, the **All Users** on that device have that setting applied.

- If a **User Scope** policy is assigned to a **Device**, the **All Users** on that device have that setting applied. This behaivor is like a ”loopback” set to ”merge”.

Device Scope vs. User Scope Settings

- If a **User Scope** policy is assigned to a **User**, then **Only That User** has that setting applied.

- If a **Device Scope** policy is assigned to a **User**, once that user signs in and the Intune sync occurs, then the **Device Scope** setting apply to **All Users** on the device.

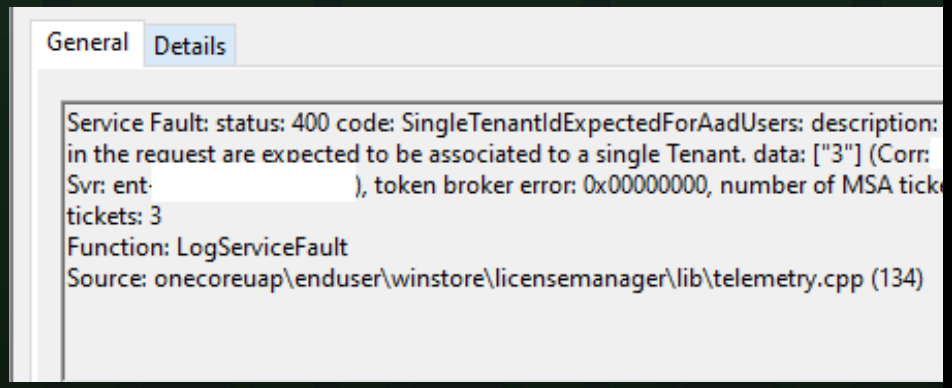
Troubleshoot Subscription based activation

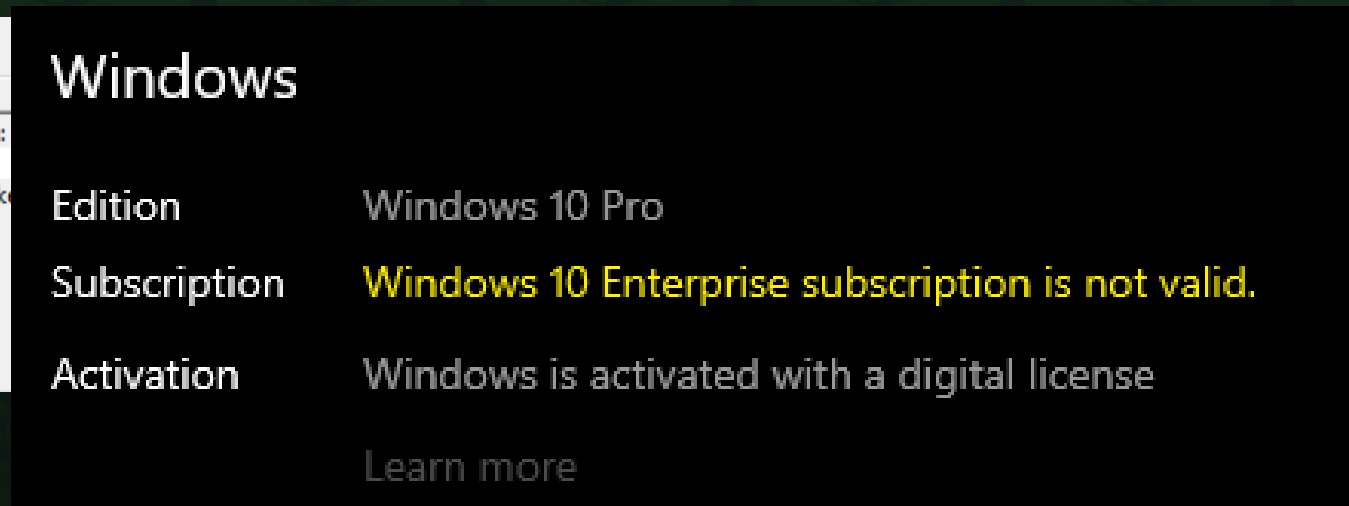
Subscription based activation

- 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)

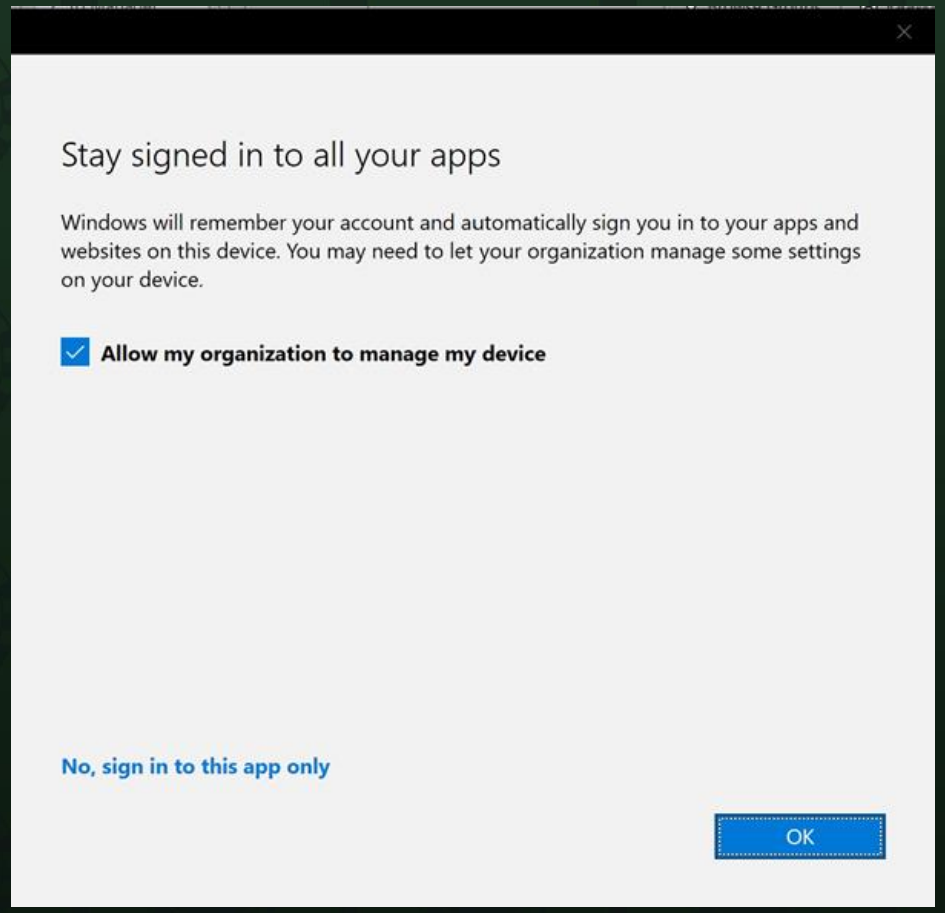
- The store does the renewal
  - In this case more than one AzureAD account was added under ”Access work or School”



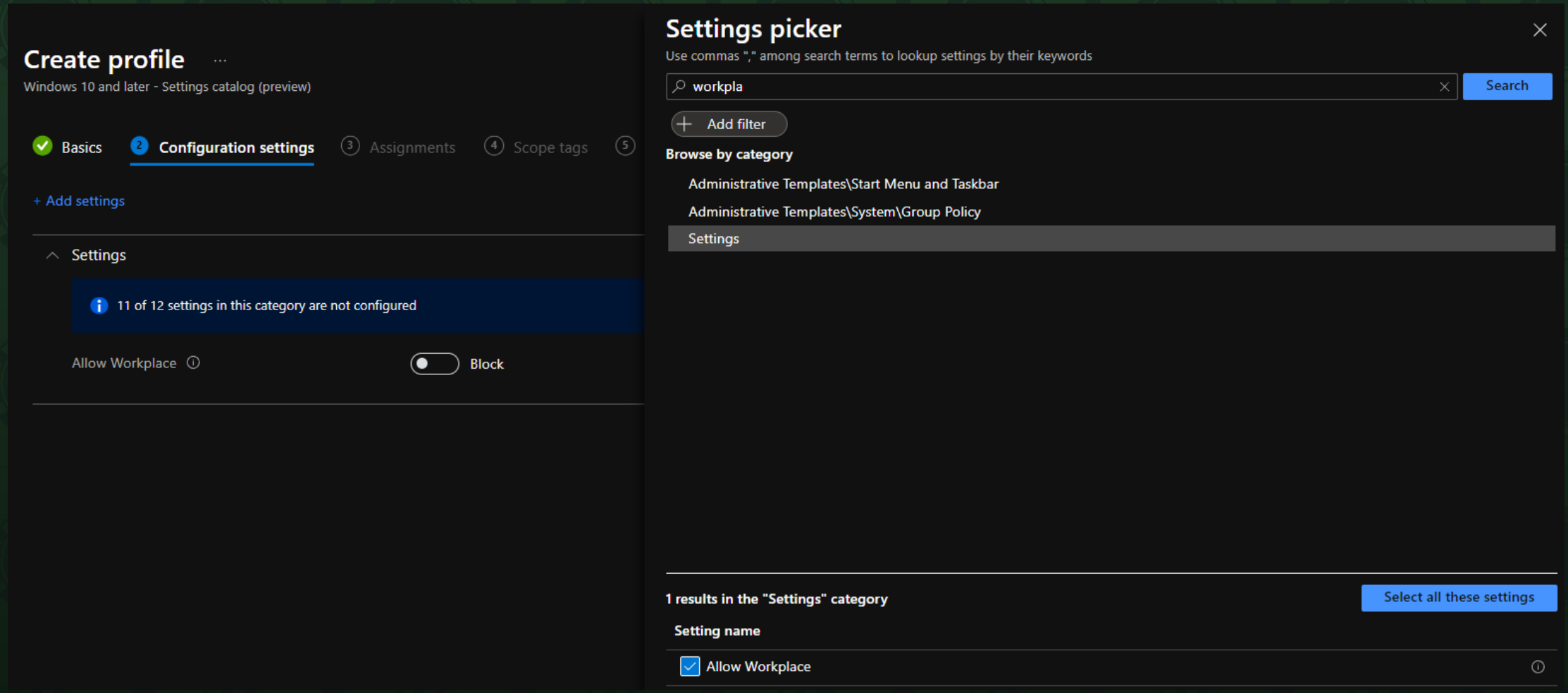


Stay signed in to all your apps = Evil

- “Stay signed in to all your apps” dialog in Microsoft Apps (outlook, Powerpoint, excel….)
- Recommended to block on Hybrid Join
- Needs to be blocked on all modern managed Windows 10!
  - Personal devices: Intune sync will fail
  - AzureAD Joined devices: Windows Activation will fail

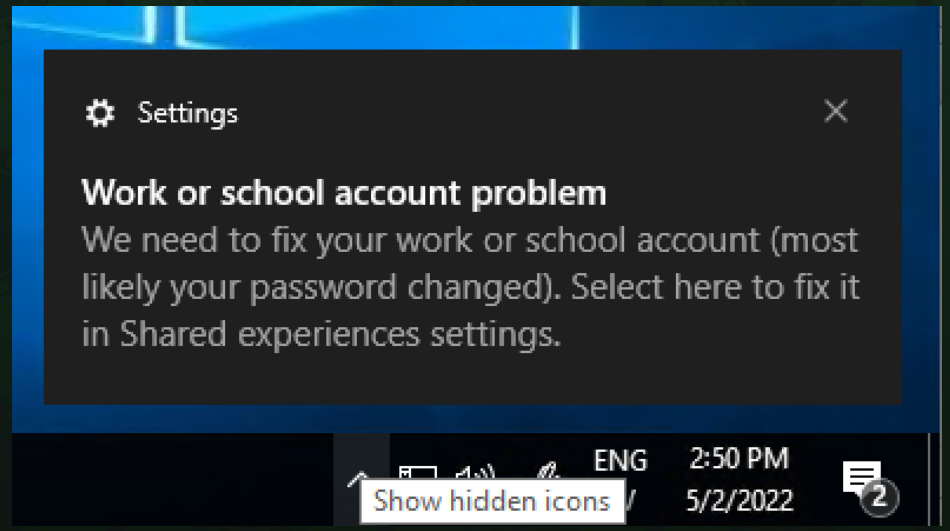


Blocking Workplace join



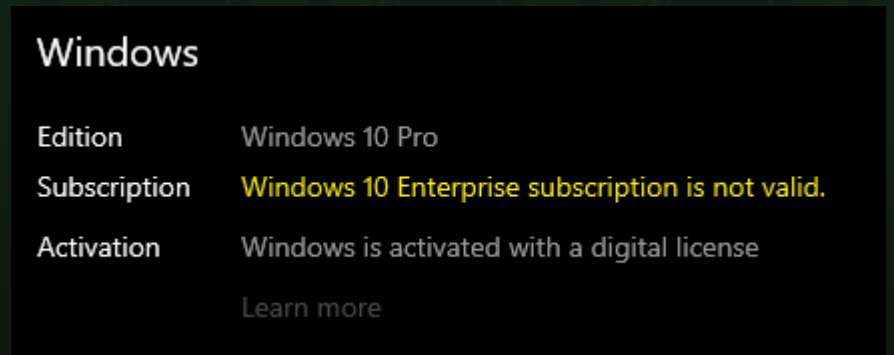
Subscription based licensing

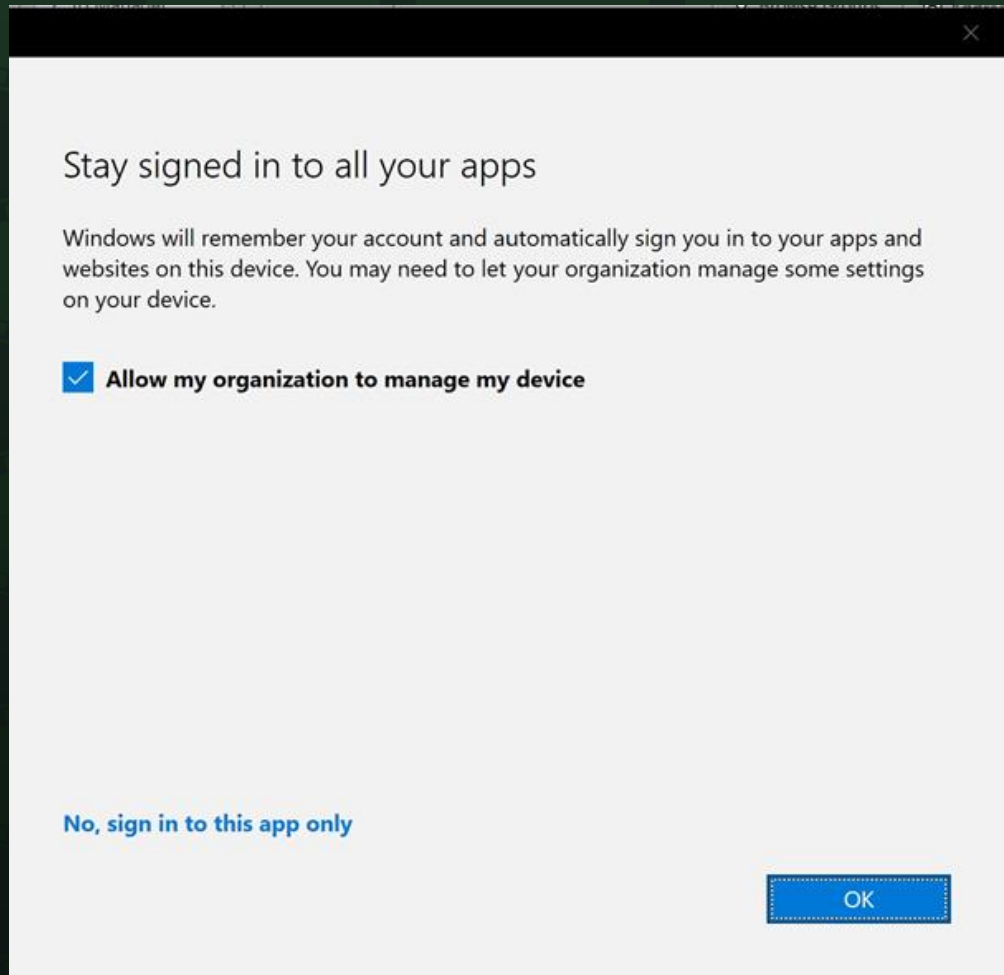
- Easiest way of upgrading to Enterprise from pro
- Re-activated every 30 days
- Can trigger the “access work or school as …”
- Important: Devices will automatically “migrate” from MAK, KMS and AD-based activation to Subscription when a user with an assigned license logs on.
- MFA, Conditional access

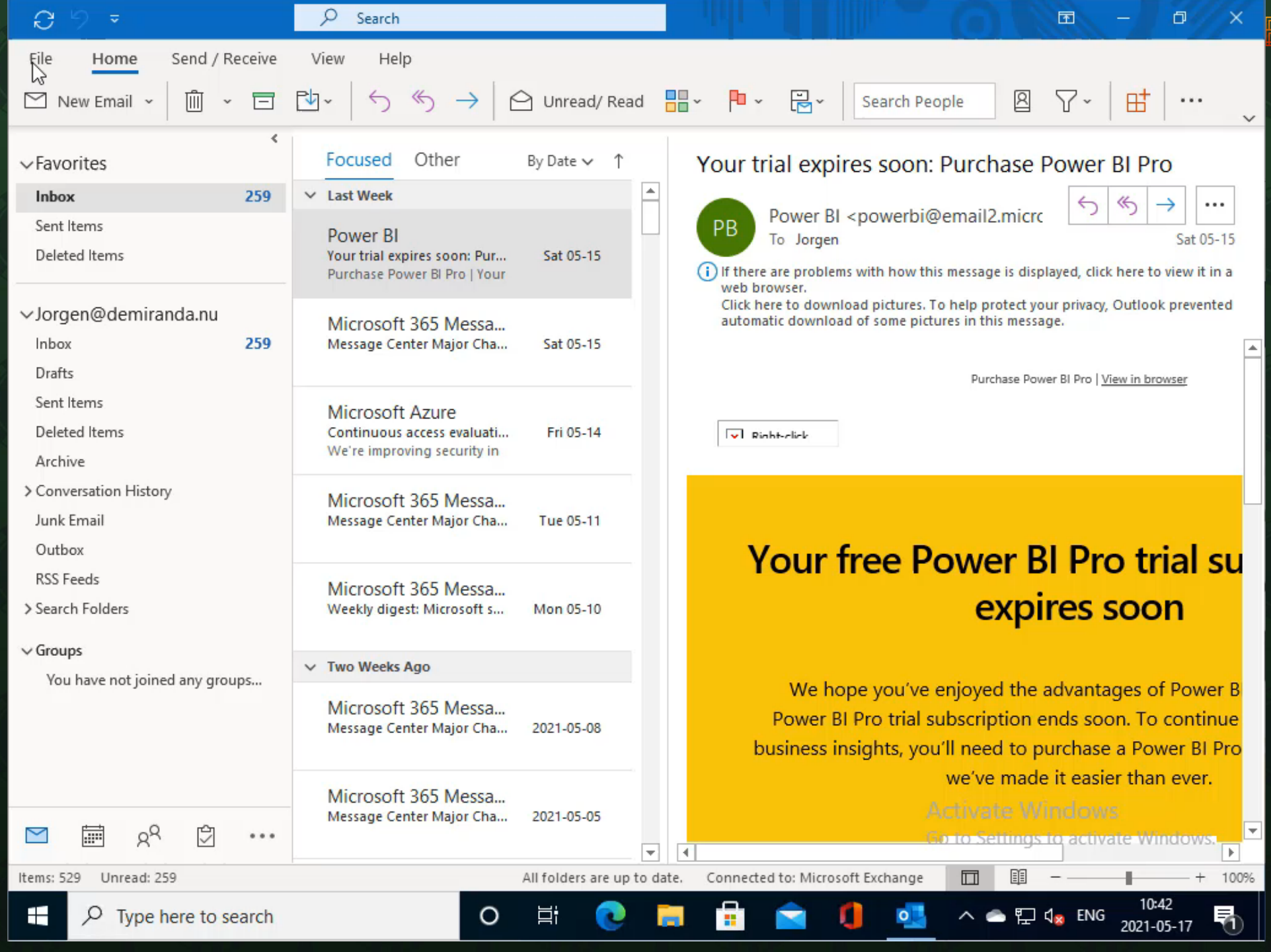


Windows 10 / M365 Apps

- “Stay signed in to all your apps” dialog in Microsoft Apps (Outlook, Powerpoint, excel….)
- Recommended to block on Hybrid Join
- Needs to be blocked on all modern managed Windows 10!
  - Personal devices: Intune sync will fail
  - AzureAD Joined devices: Windows Activation will fail






Search
File
Home
Send / Receive
View
Help
New Email
Unread/ Read
Search People
Favorites
Inbox 259
Sent Items
Deleted Items
Jorgen@demiranda.nu
Inbox 259
Drafts
Sent Items
Deleted Items
Archive
Conversation History
Junk Email
Outbox
RSS Feeds
Search Folders
Groups
You have not joined any groups...
Focused
Other
By Date
Last Week
Power BI
Your trial expires soon: Pur...
Purchase Power BI Pro | Your
Sat 05-15
Microsoft 365 Messa...
Message Center Major Cha...
Sat 05-15
Microsoft Azure
Continuous access evaluati...
We're improving security in
Fri 05-14
Microsoft 365 Messa...
Message Center Major Cha...
Tue 05-11
Microsoft 365 Messa...
Weekly digest: Microsoft s...
Mon 05-10
Two Weeks Ago
Microsoft 365 Messa...
Message Center Major Cha...
2021-05-08
Microsoft 365 Messa...
Message Center Major Cha...
2021-05-05
Your trial expires soon: Purchase Power BI Pro
PB
Power BI <powerbi@email2.micrc
To Jorgen
Sat 05-15
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
Purchase Power BI Pro | View in browser
Your free Power BI Pro trial su
expires soon
We hope you've enjoyed the advantages of Power B
Power BI Pro trial subscription ends soon. To continue
business insights, you'll need to purchase a Power BI Pro
we've made it easier than ever.
Activate Windows
Go to Settings to activate Windows.
Items: 529
Unread: 259
All folders are up to date.
Connected to: Microsoft Exchange
100%
Type here to search
ENG
10:42
2021-05-17

Subscription based activation

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)

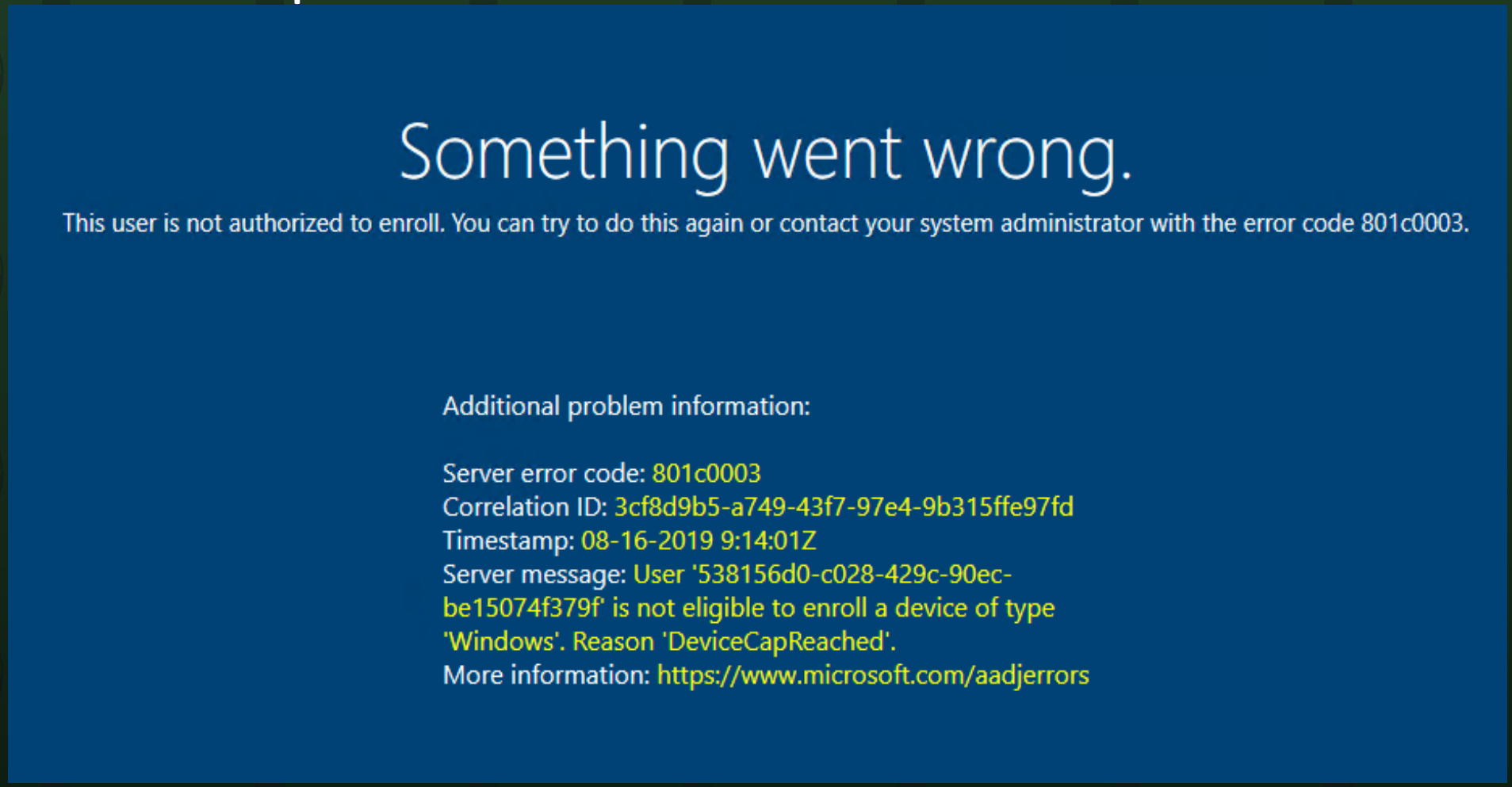
https://ccmexec.com/2021/01/mem-windows-10-personal-device-and-sync-issues/

Enrollment

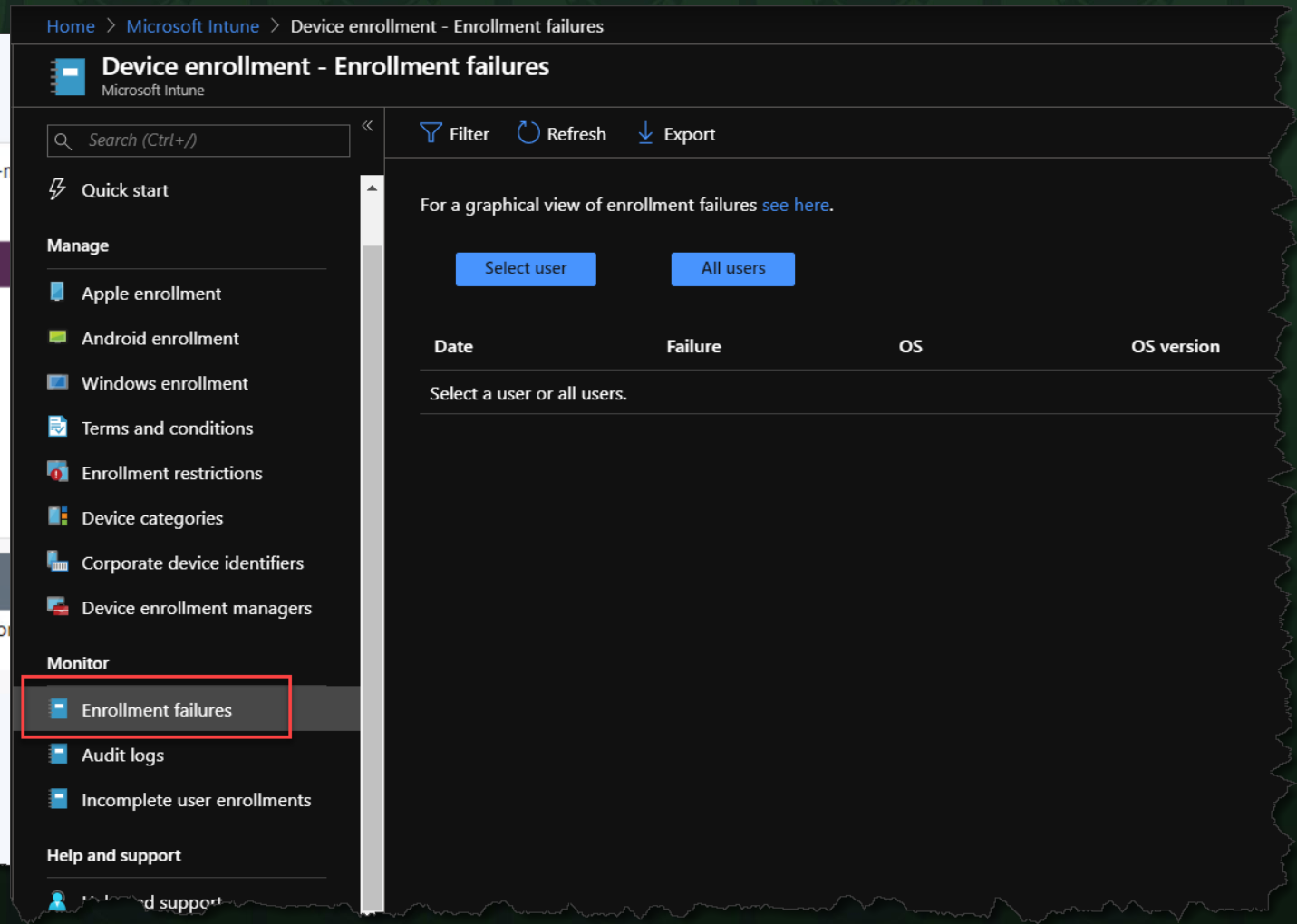
Troubleshooting Windows enrollemnt in Intune

- 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

DeviceCapReached = Device Limits



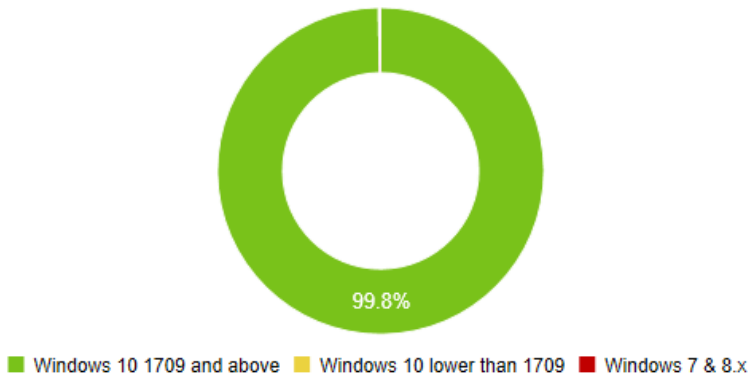
Cloud Attach



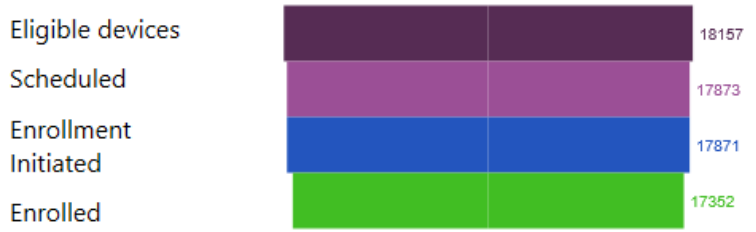
Cloud Attach

Co-management

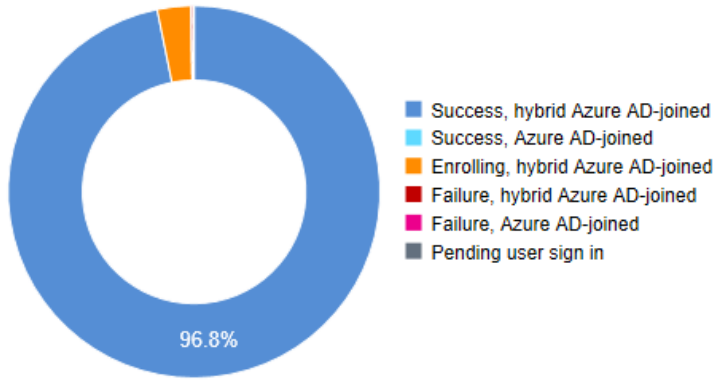
Client OS Distribution



Co-management Status

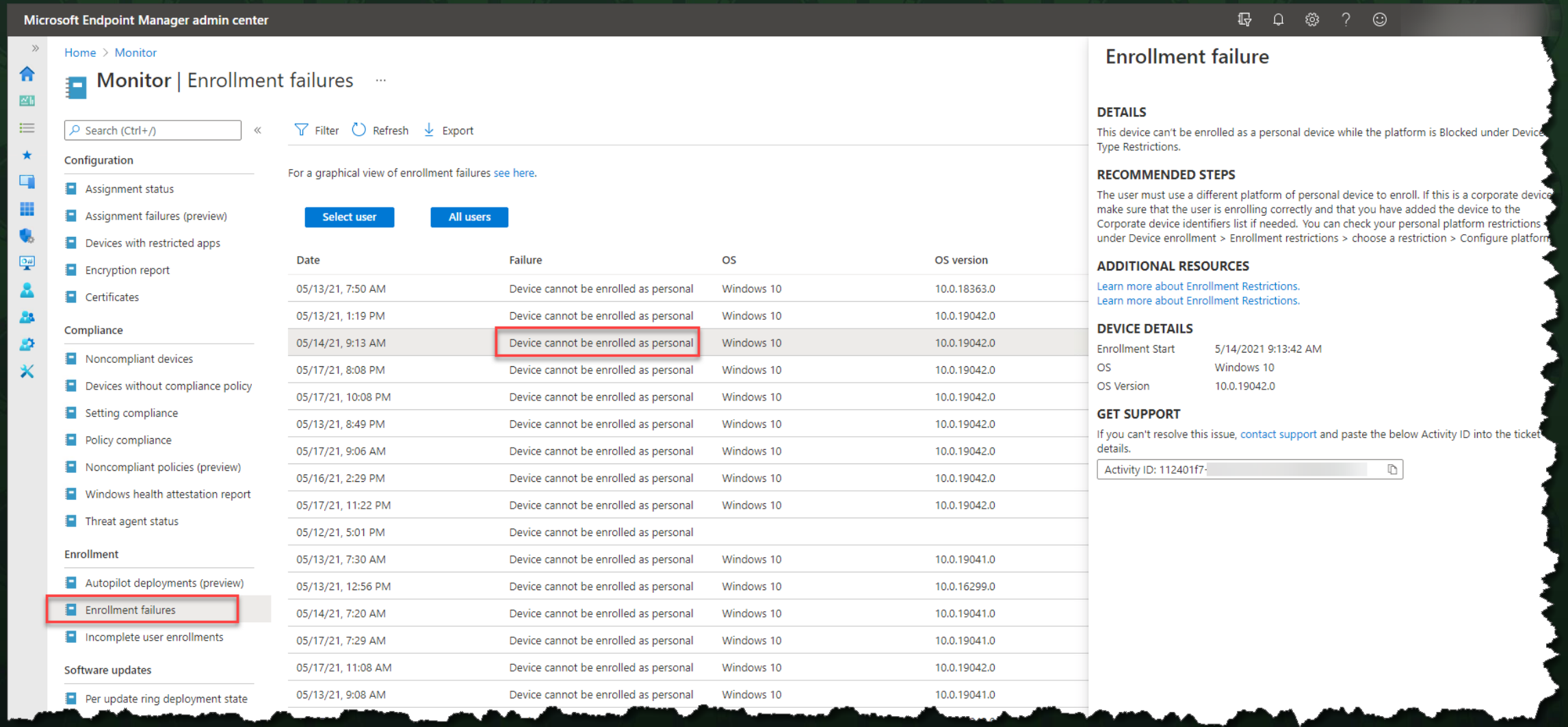


Co-management Enrollment Status



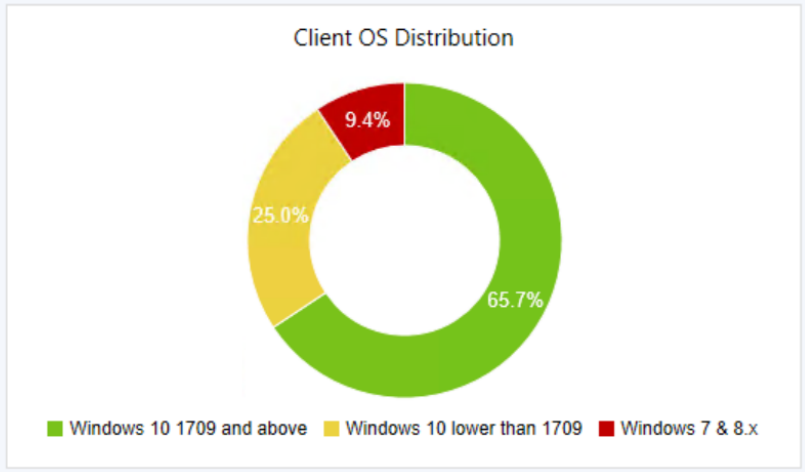
Count	Enrollment Error
16	Undefined
11	License of user is in bad state blocking enrollment
4	MDM enrollment hasn't been configured yet on AAD, or the enrollment url isn't expected.
4	The Internet connection has timed out
2	Not enough memory resources are available to process this command.
1	Account type is unknown.
1	Authorization grant failed for this assertion.
1	Incorrect function.

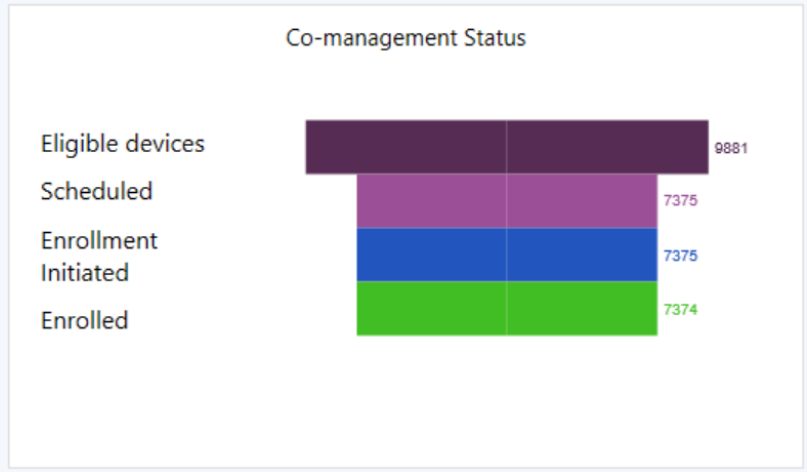
Enrollment Failures

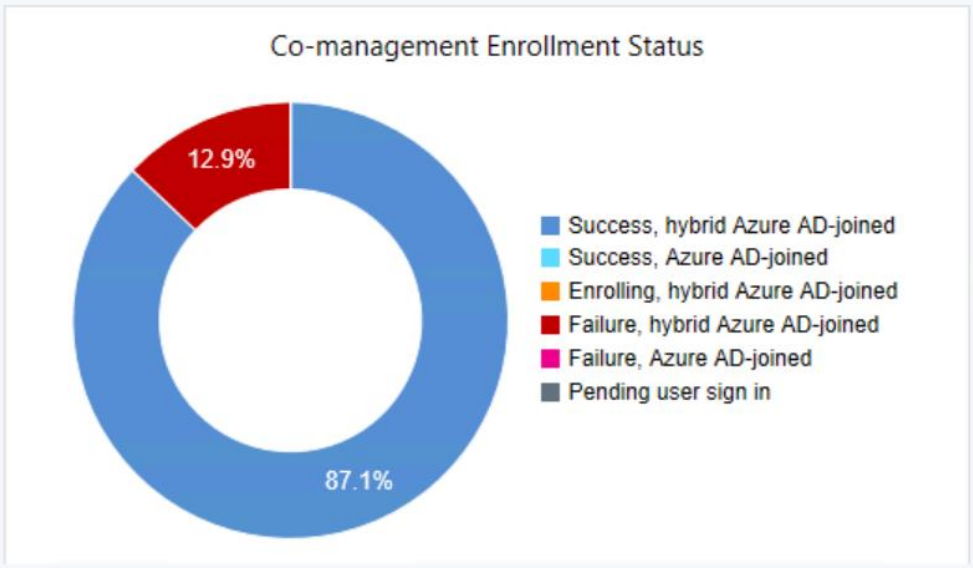


Co-Management Enrollment Status

Co-management







Count	Enrollment Error
706	License of user is in bad state blocking enrollment
382	Undefined
6	Element not found.
5	Catastrophic failure
4	The Internet connection has timed out
2	MDM enrollment hasn't been configured yet on AAD, or the enrollment url isn't expected.
1	The user canceled the operation

Hybrid Azure AD Join

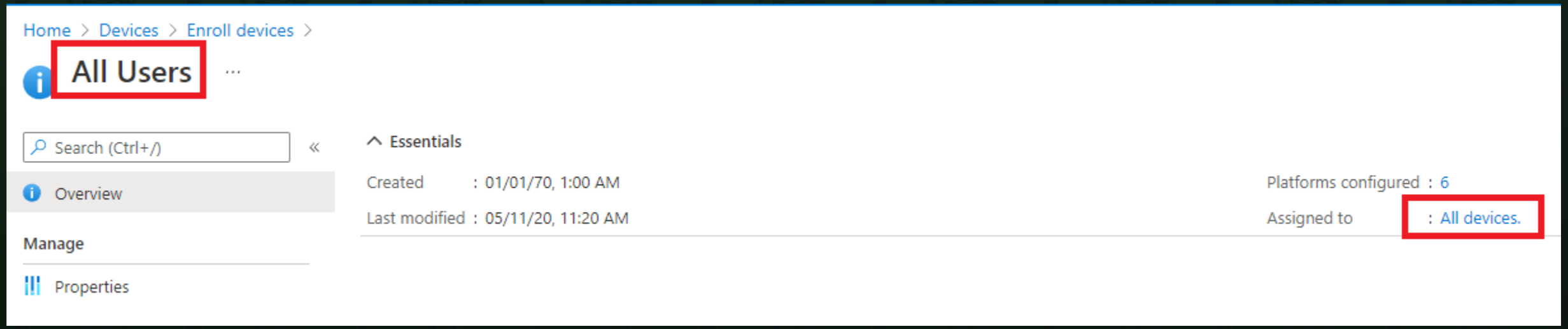
- Group Policy (No Offset) (User Token)
- Co-Management (Offset) (Device token -> User Token)
  - Schedules enrollment with an offset
  - If the enrollment fails, SCCM will retry 2 times every 15 mins
- Common issues
  - The users is not in AAD
  - The device is not Synced (Hybrid Azure AD Join)
- Will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

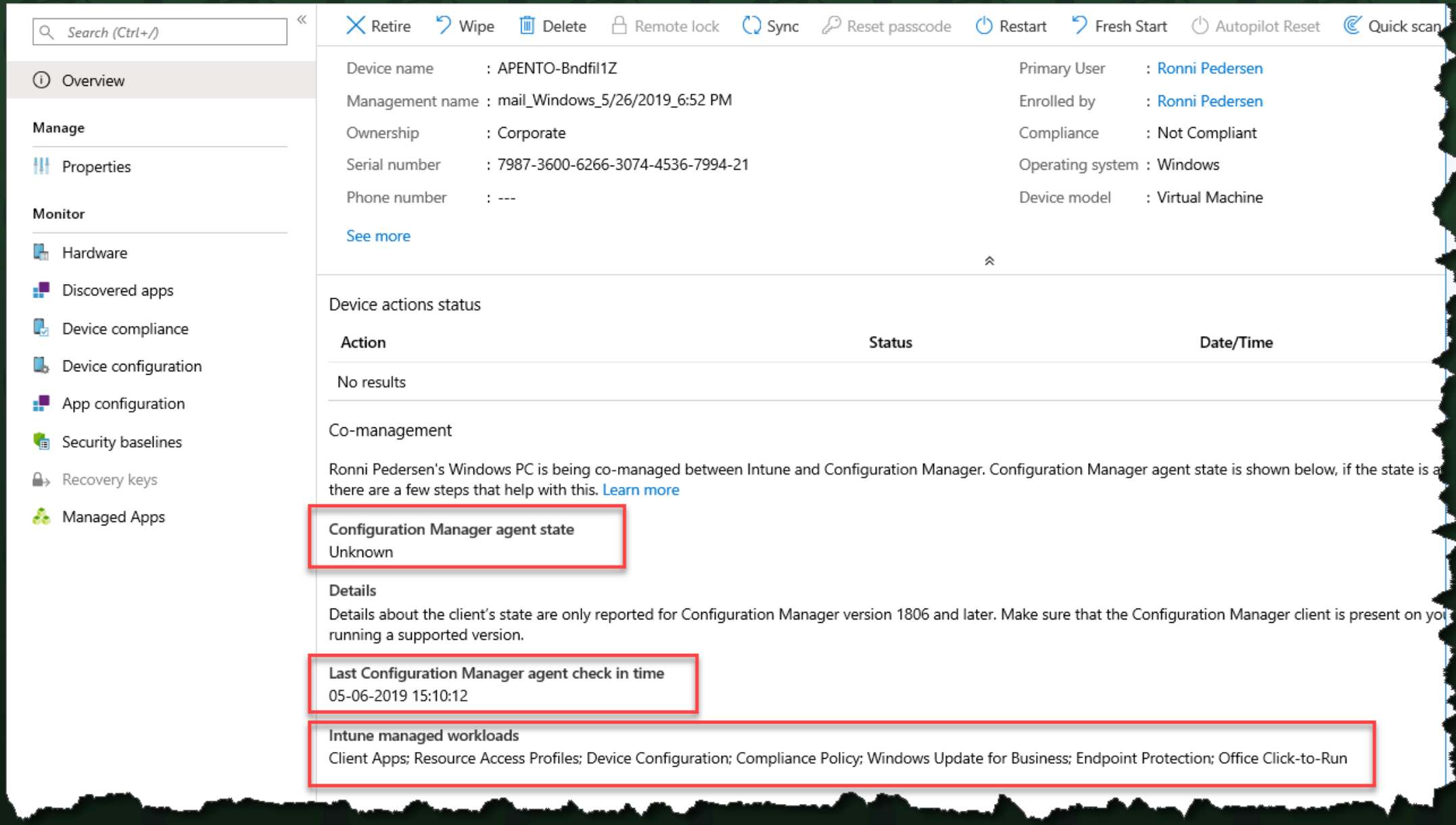
Important: the default enrollment restriction policy “All Users” is applied to “All Devices“



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
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 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

Device Settings in Microsoft Intune

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 10 devices will scheduled check-in with the Intune service, which is estimated at: 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

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

Computer Management

File Action View Help

- Computer Management (Local)
  - System Tools
    - Task Scheduler
      - Task Scheduler Library
        - Intel
        - Lenovo
        - Microsoft
          - Intune
          - Office
          - OneCore
          - Windows
            - .NET Framework
            - Active Directory Rights Management S
            - AppID
            - Application Experience
            - ApplicationData
            - AppxDeploymentClient
            - Autochk
            - BitLocker
            - Bluetooth
            - BrokerInfrastructure
            - CertificateServicesClient
            - Chkdsk
            - Clip
            - CloudExperienceHost
            - Customer Experience Improvement Pr
            - Data Integrity Scan
            - Defrag
            - Device Information
            - Device Setup
            - DeviceDirectoryClient
            - Diagnosis
            - DirectX
            - DiskCleanup
            - DiskDiagnostic
            - DiskFootprint
            - DUSM
            - EDP
            - EnterpriseMgmt
              - BF34185C-4364-40CF-A364-98DBD
              - VirtulizationBasedIsolation
            - ExploitGuard
            - Feedback

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 Registratio
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 04-04-2020 - After triggered, repeat every 7.00:00:00 for a duration of 49.00:00:00.
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

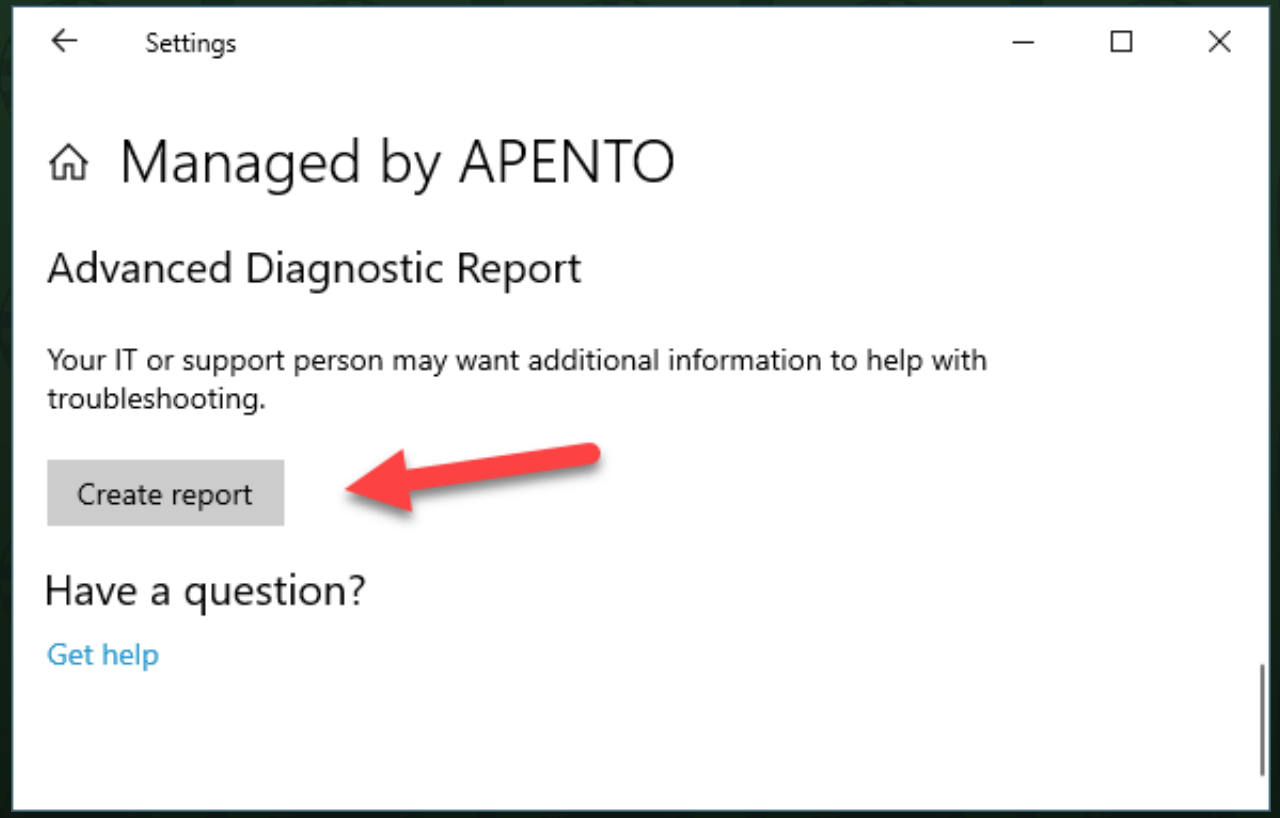
- Manually using Script

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



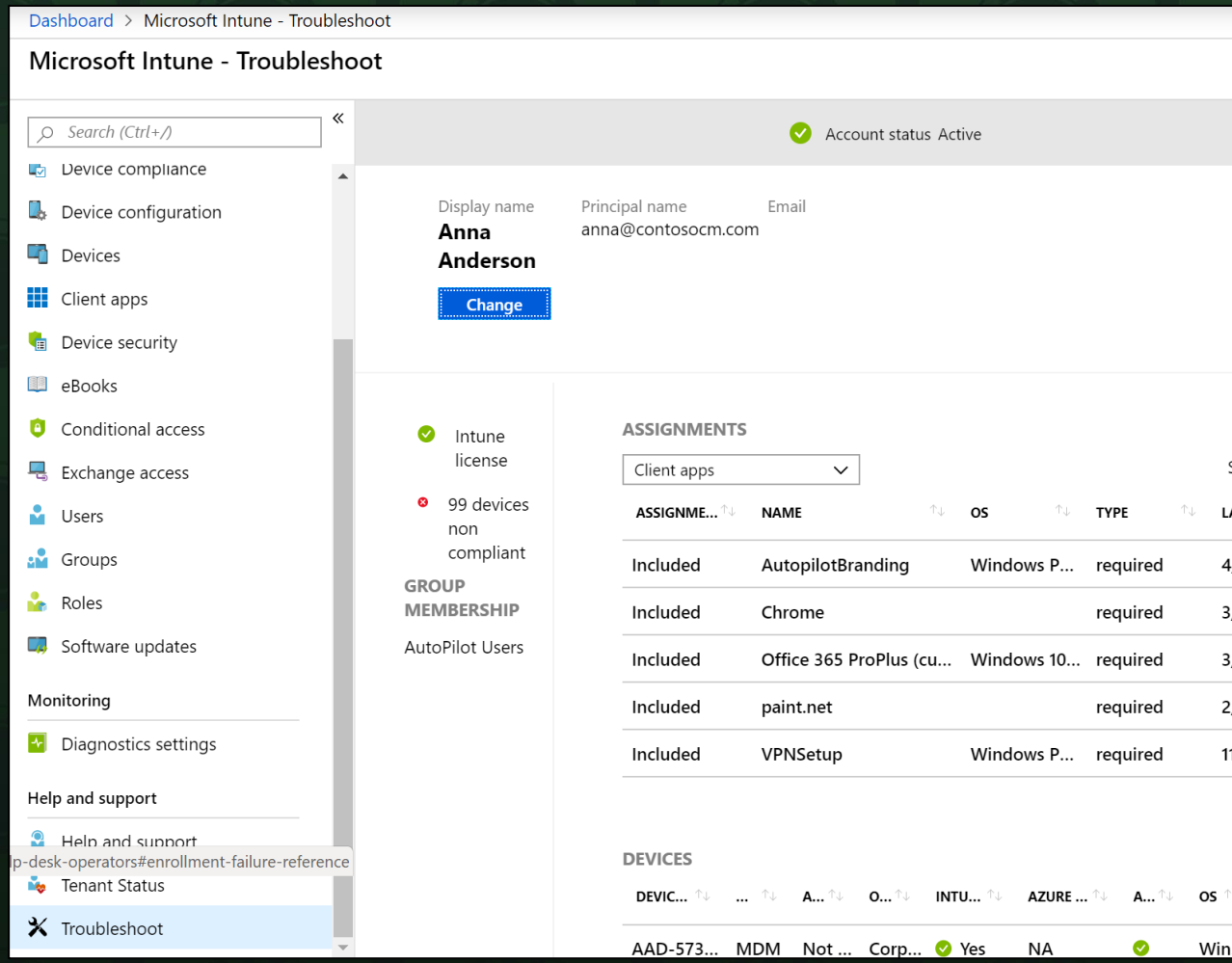
Managed policies

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=<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]owCloudProtection	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1

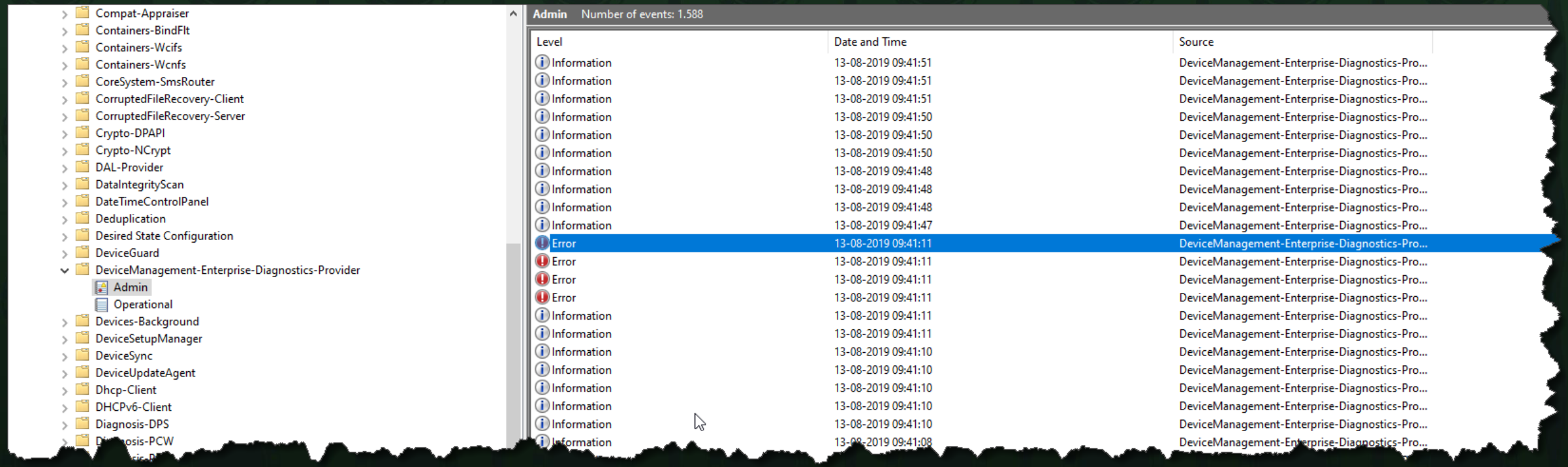
Intune Troubleshooting Pane

- 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

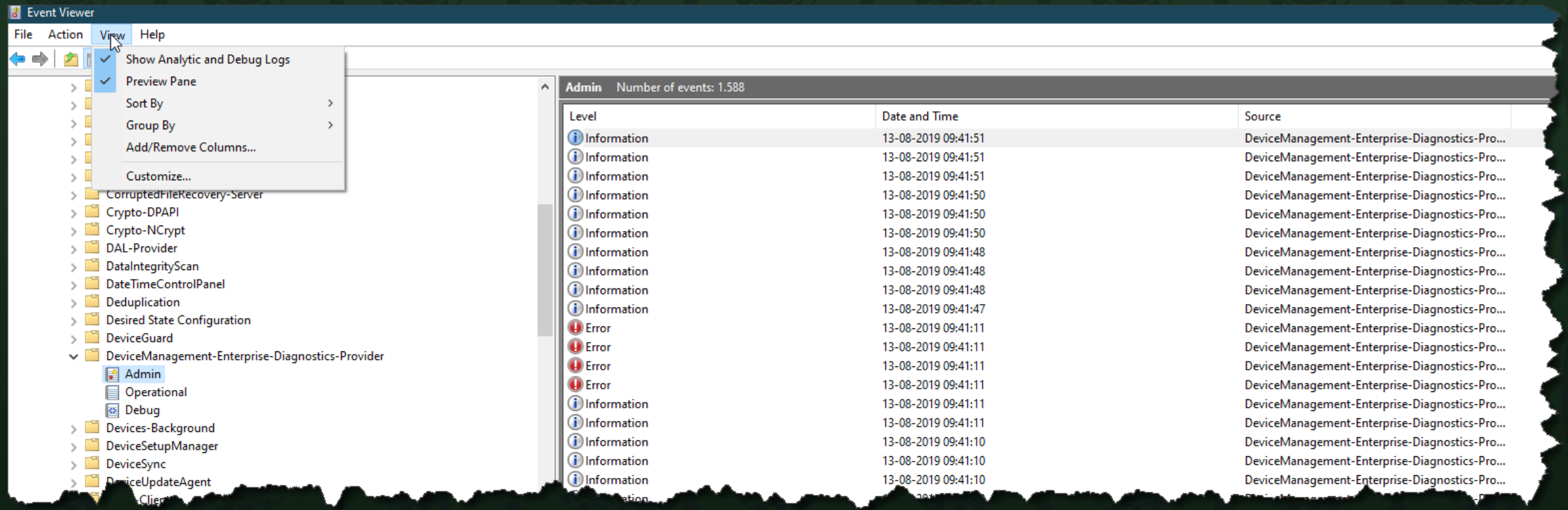


Device Profiles - Where is my logs?

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



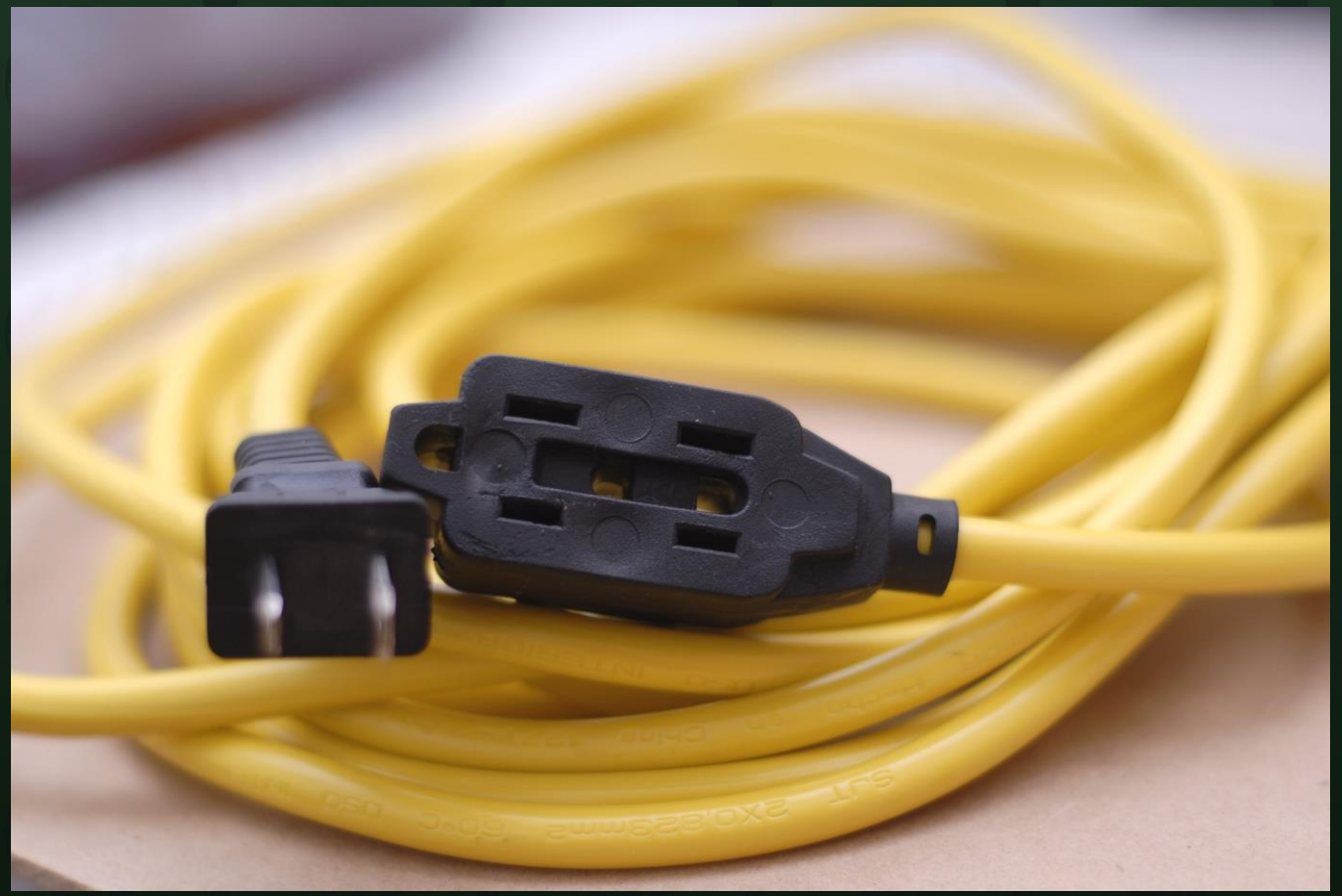
Enable debug mode



Intune Management Extension

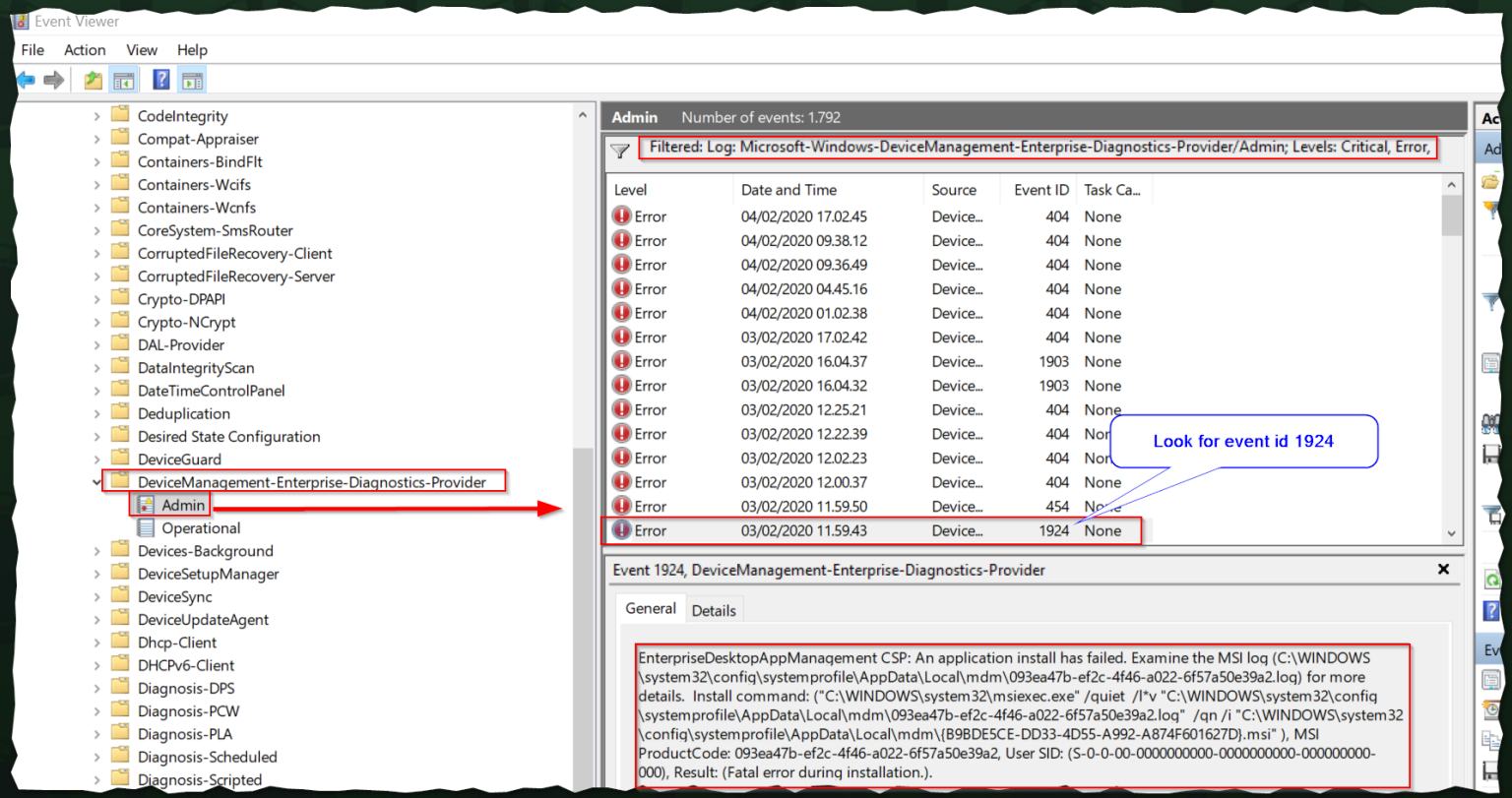
Intune Management Extension

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

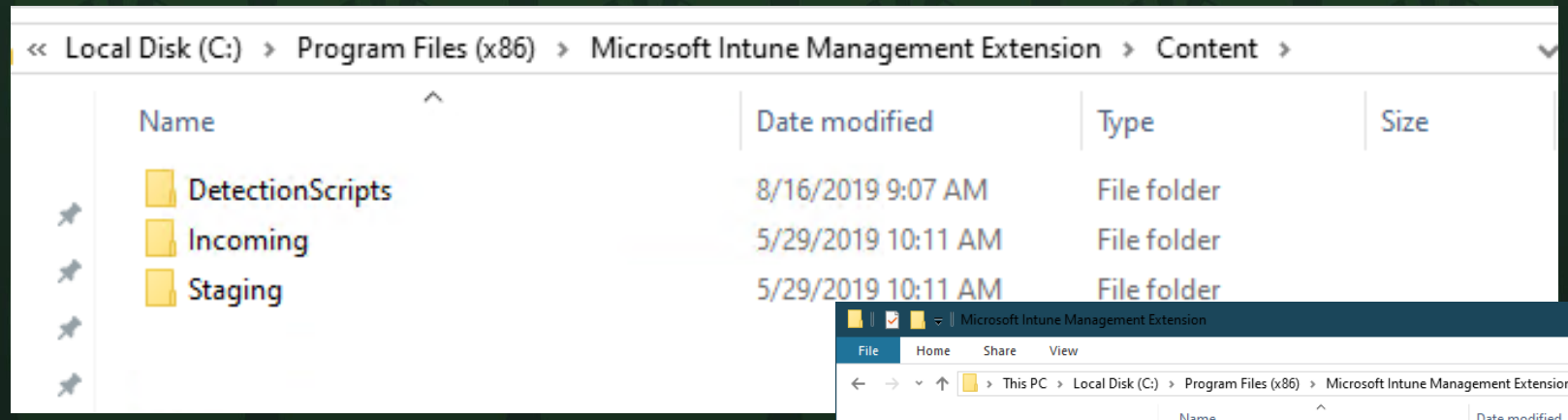


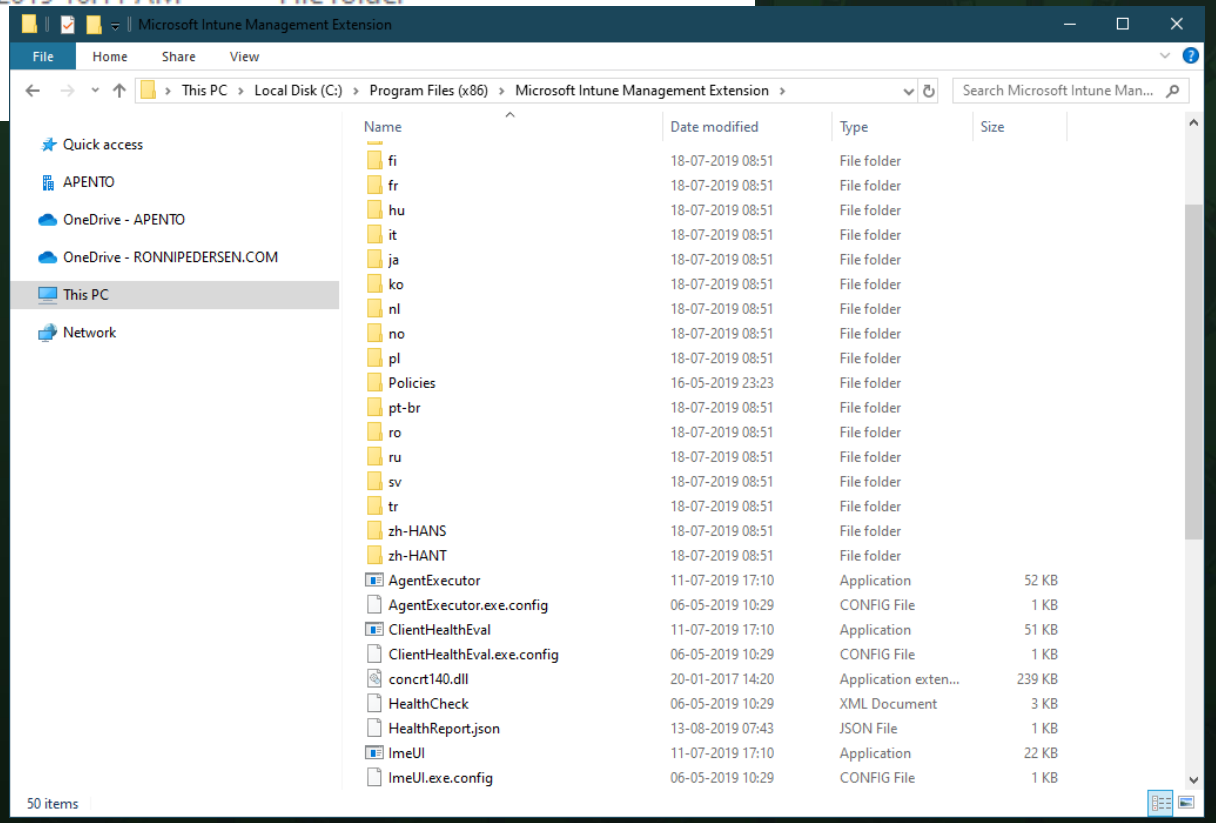
Intune Management Extension Event log

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



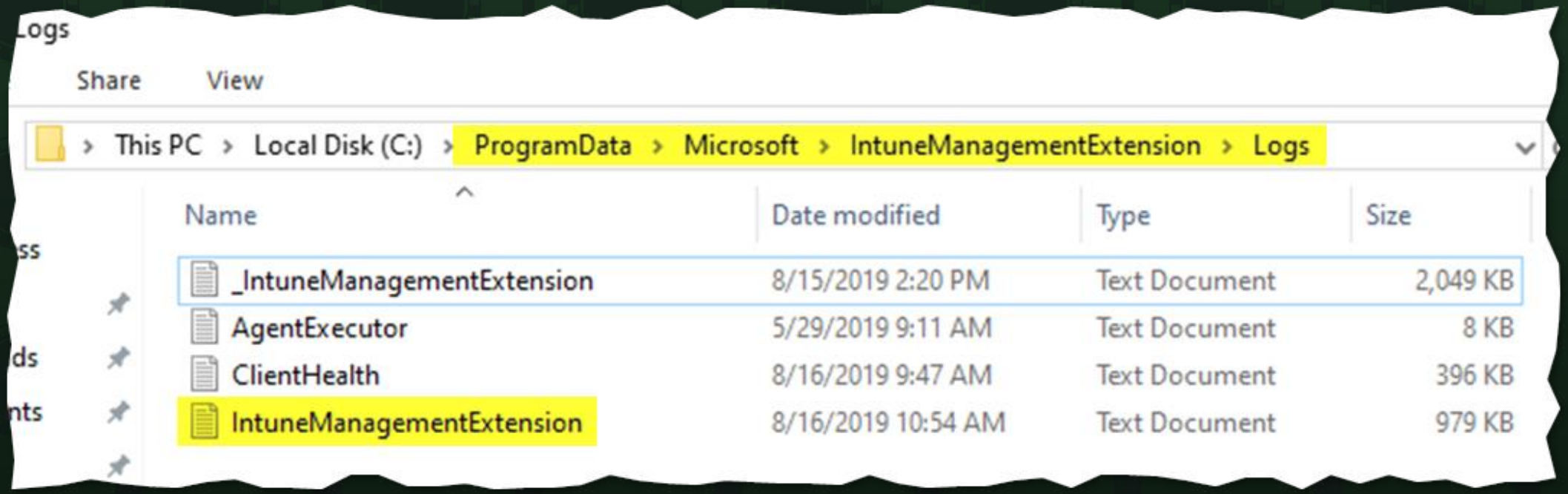
Intune Management Extension File System





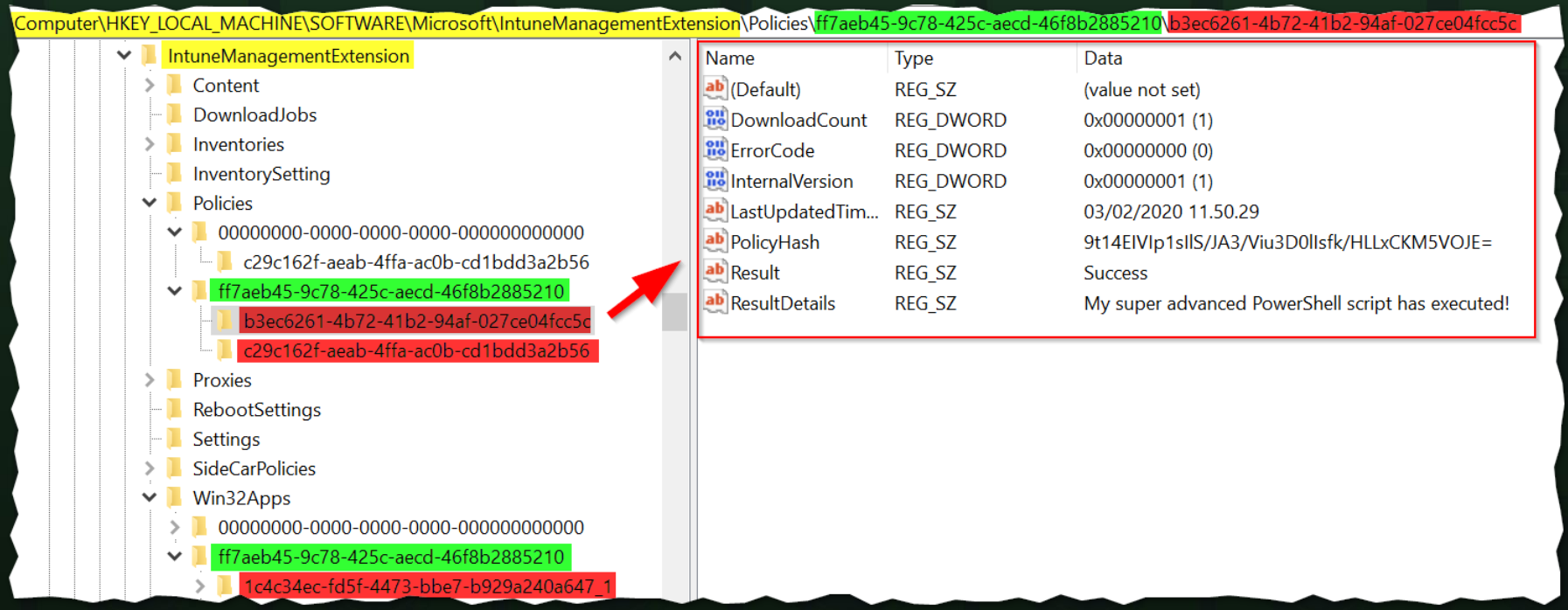
Intune Management Extension Log files

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



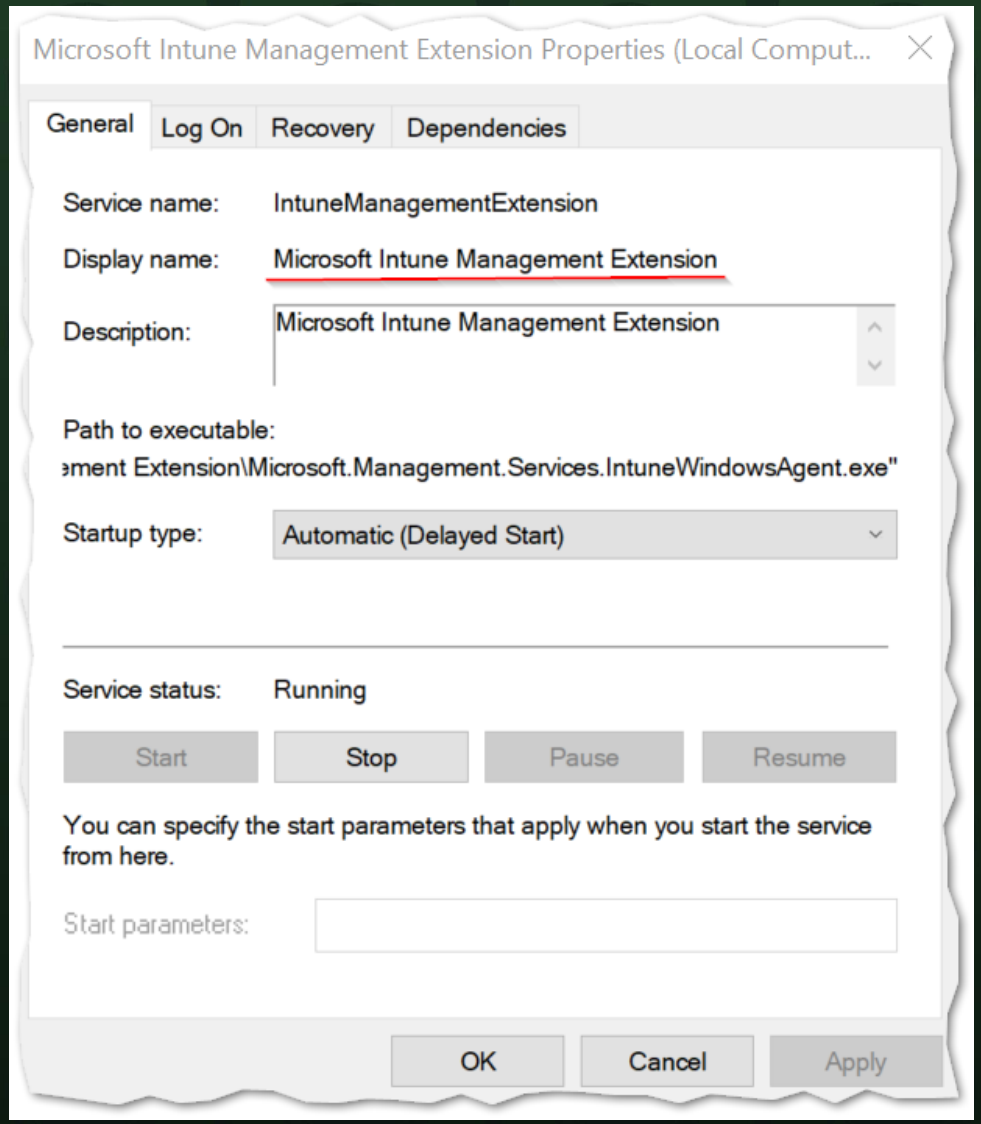
Intune Management Extension The Registry

- 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?

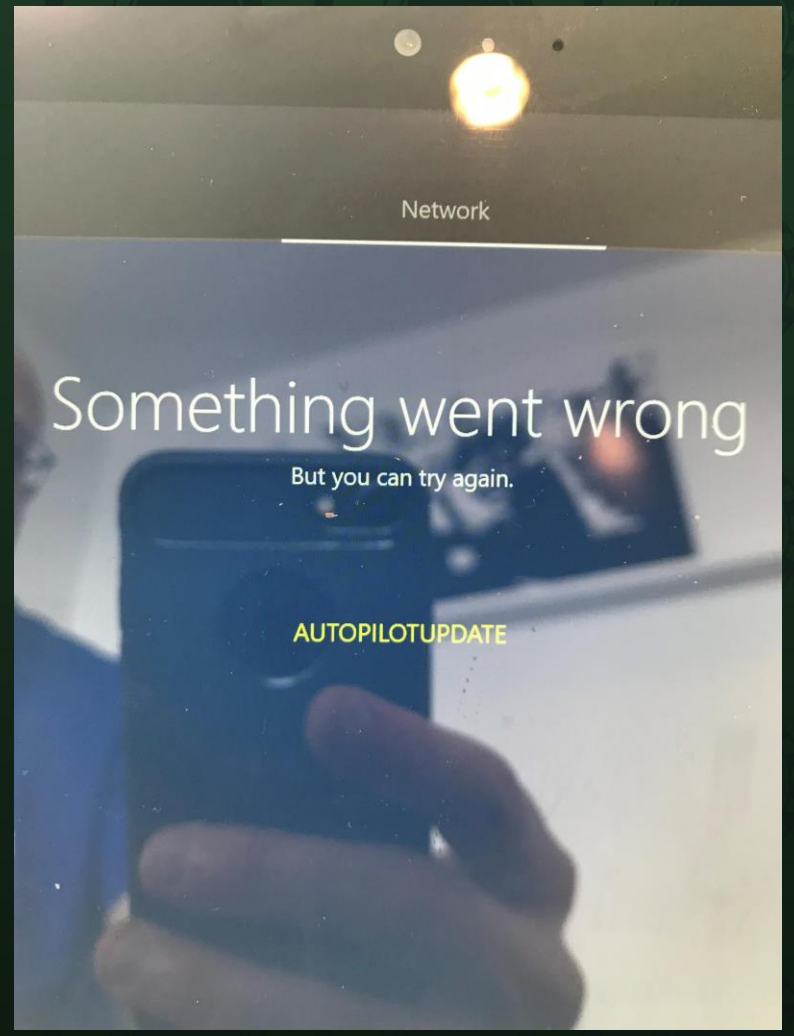


https://docs.microsoft.com/en-us/intune/apps/intune-management-extension#prerequisites

Windows AutoPilot

Network

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



Network issues – we have seen

- Pie-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”.

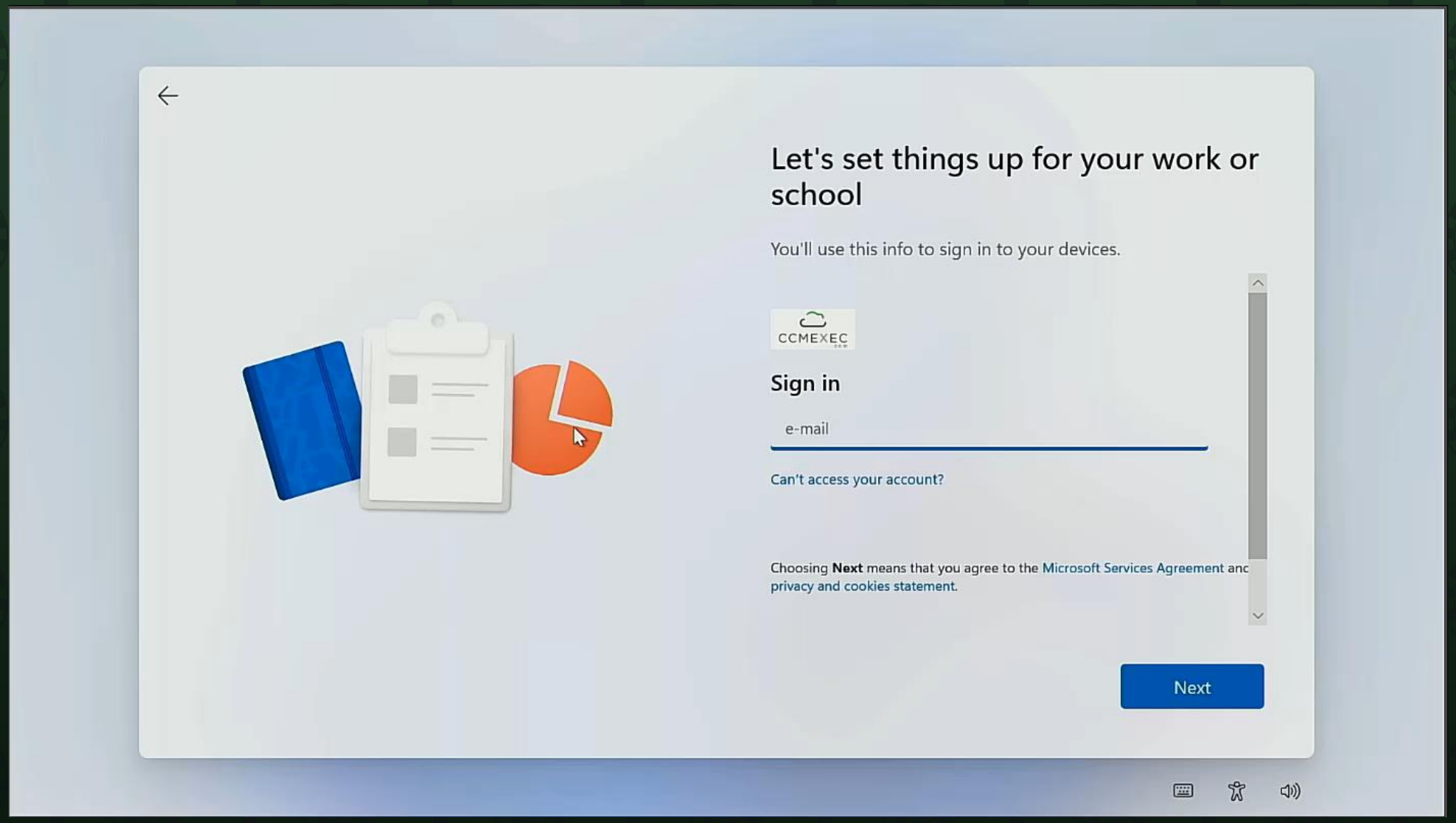
“It is a different organization name showing up when I start my computer”.

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.

QuickAssist + AutoPilot



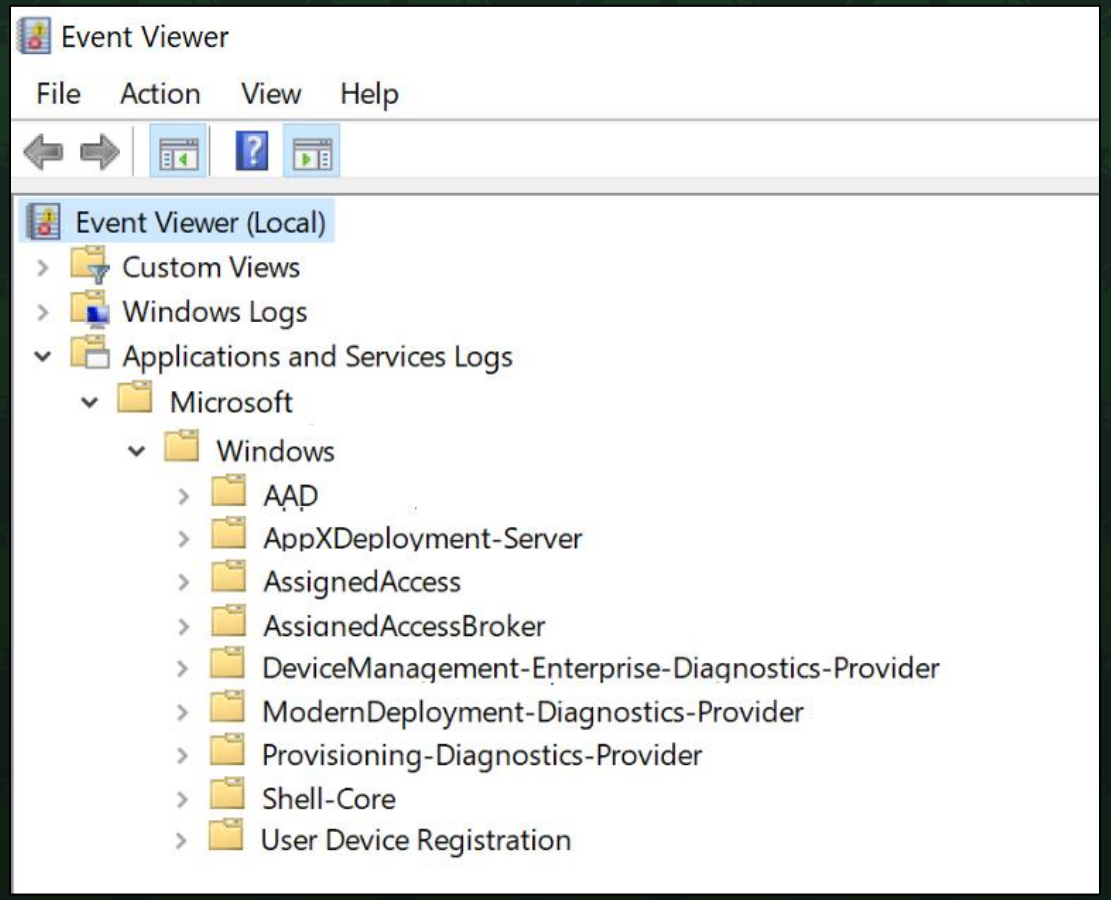
Troubelshooting

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



Windows Autopilot Win32 Error Codes

- 8007 : Win32 errors (network, etc.)

  0x800705B4 = timeout
  0x80070774 = domain controller not found

- 801C : Azure AD join / device registration

  0x801C0003 = device authorization error (not authorized to join AAD, exceeded device limit)

- 8018 : MDM enrollment

  0x80180003 = authorization error (user not authorized to enroll)
  0x80180005 = server error (enrollment rejected, scenario not enabled, etc.)
  0x80180014 = device not supported (enrollment restriction)
  0x80180018 = no user license (AAD Premium or Intune)

- 8000: Windows errors

  0x80004005 = generic error (fail)


Thank You!