

W E L C O M E

TO *Fabulous*

TECHORAMA

ANTWERP

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](https://twitter.com/ronnipedersen)





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](https://twitter.com/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 admin
console (for now)

The screenshot shows the Microsoft Endpoint Manager admin center interface. The left sidebar has a tree view with nodes like Home, Tenant admin, Connectors and tokens, and a search bar. The main content area is titled "Connectors and tokens | TeamViewer connector". It displays a table with columns for Connection status, Last connection, and Connection request expires. A note says "New connection requests expire after 15 minutes. If the Connection status is not Active within 15 minutes, click Connect to start a new request." Below this is a descriptive text about the TeamViewer service and a "Log in to TeamViewer to authorize" button. At the bottom, a list of connectors includes "TeamViewer connector" which is highlighted with a red box.

| Connection status | Last connection | Connection request expires |
|-------------------|-----------------|----------------------------|
| Requires setup | -- | -- |

New connection requests expire after 15 minutes. If the Connection status is not Active within 15 minutes, click Connect to start a new request.

The TeamViewer service allows users of Intune-managed devices to get remote assistance from their IT administrator. Create TeamViewer sessions by first associating Intune with your TeamViewer account and then authorizing it to work with Intune. If you don't yet have a TeamViewer account you will need to create one.

Log in to TeamViewer to authorize

- TeamViewer connector
- Certificate connectors
- Telecom expense management
- Derived Credentials

Microsoft Remote Help

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

The screenshot displays the Microsoft Endpoint Manager (MEM) portal interface. At the top, there are two windows: one titled "Remote help" showing a user profile and a "Share security code" button, and another window titled "Remote help" with a "CCMEXEC" logo. Below these, the main portal area shows a navigation bar with "Monitor", "Settings", and "Remote help sessions". A "Refresh" button is also present. The "Monitor" tab is selected, showing "Current active sessions" with a count of "2". A chart titled "Average session time" shows data from Jan 12 to Jan 18, with a value of "0 minutes" for Jan 18. Another chart titled "Total sessions" shows a single bar for Jan 18 reaching a value of "2".

Remote help

Signed in as:

Sign in with a different account

Share security code

The person you are helping needs a security code to let

Remote help

CCMEXEC

Monitor Settings Remote help sessions

Refresh

Current active sessions

2

Average session time

Jan 12 Jan 13 Jan 14 Jan 15 Jan 16 Jan 17 Jan 18

100
80
60
40
20
0

Total sessions

Jan 12 Jan 13 Jan 14 Jan 15 Jan 16 Jan 17 Jan 18

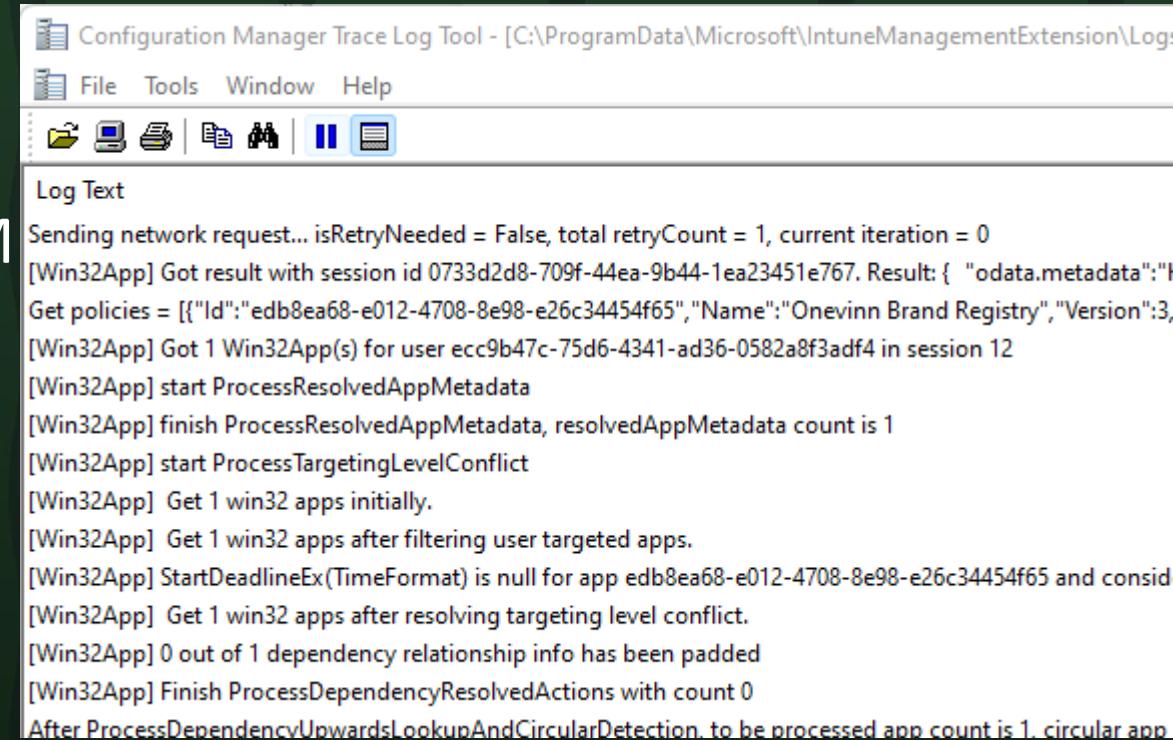
2
1.5
1
0.5
0

Jan 18 2 sessions

Jan 18 0 minutes

CMtrace

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



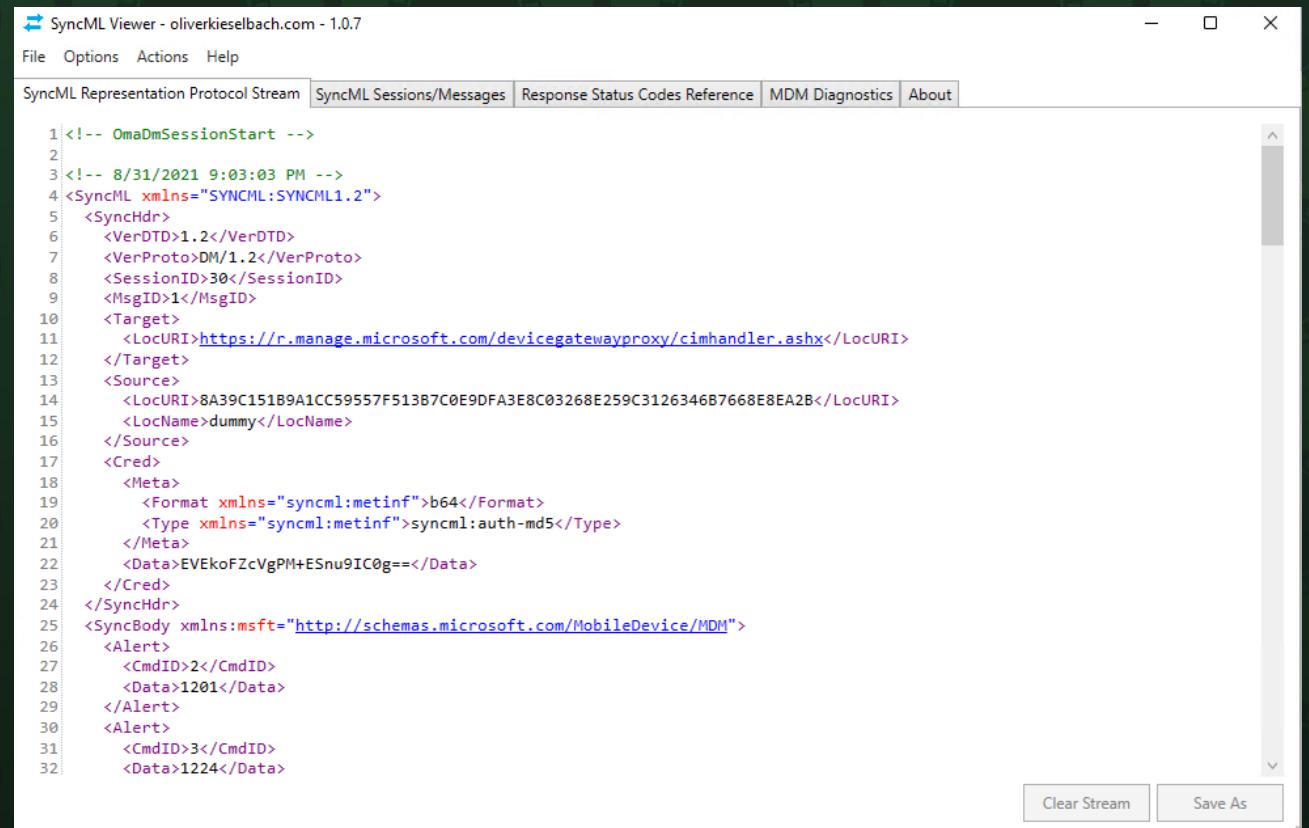
The screenshot shows the 'Configuration Manager Trace Log Tool' window. The title bar reads 'Configuration Manager Trace Log Tool - [C:\ProgramData\Microsoft\IntuneManagementExtension\Log]'. The menu bar includes 'File', 'Tools', 'Window', and 'Help'. Below the menu is a toolbar with icons for file operations.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

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

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

More Tools – advanced troubleshooting

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



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

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

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

[SyncMLViewer/SyncMLViewer/dist at master · okieselbach/SyncMLViewer · GitHub](https://github.com/okieselbach/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>T0EeBAEAHAAAAoAMwDwVQAACgAaAfBVCnofKQQCCQgCABAACQABAAEAAgABAAAABQAZAAQAAAAAAAAAgAAAAAAAACAAEAAwMAEQBHZW51aW51SW50ZWwABAA0AEEludGVsKFipIENvcmUoVE0pIGk3LTg1NTlV:
1549   </Item>
1550 </Results>
1551 <Status>
1552 <CmdID>34</CmdID>
1553 <MsgRef>2</MsgRef>
1554 <CmdRef>26</CmdRef>
```

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

Log Files

Collect diagnostics from a Windows Device

- Collecting Diagnostic Logs from Windows Devices
 - Windows 10 1909 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

The screenshot shows the Microsoft Intune interface for managing devices. The main window displays device details for 'DESKTOP-NIIRT6B' and a history of actions taken on the device.

Device Details:

- Device name: DESKTOP-NIIRT6B
- Management name: rop_Windows_6/18/2020_4:01 PM
- Ownership: Corporate
- Serial number: [REDACTED]
- Phone number: ---
- Primary user: Ronni Pedersen
- Enrolled by: Ronni Pedersen
- Compliance: Compliant
- Operating system: Windows
- Device model: NUC8i7HKN

Device Actions Status:

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

Device Diagnostics (Preview):

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

Navigation and Action Buttons:

- Search (Ctrl+ /)
- Retire
- Wipe
- Delete
- Remote lock
- Sync
- Reset passcode
- Restart
- Collect diagnostics (highlighted with red box and number 1)
- Fresh Start

Left Sidebar:

- Overview
- Properties
- Monitor
- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Endpoint security configuration
- Recovery keys
- User experience
- Device diagnostics (preview) (highlighted with red box and number 3)
- Managed Apps

Configuration Policy Process

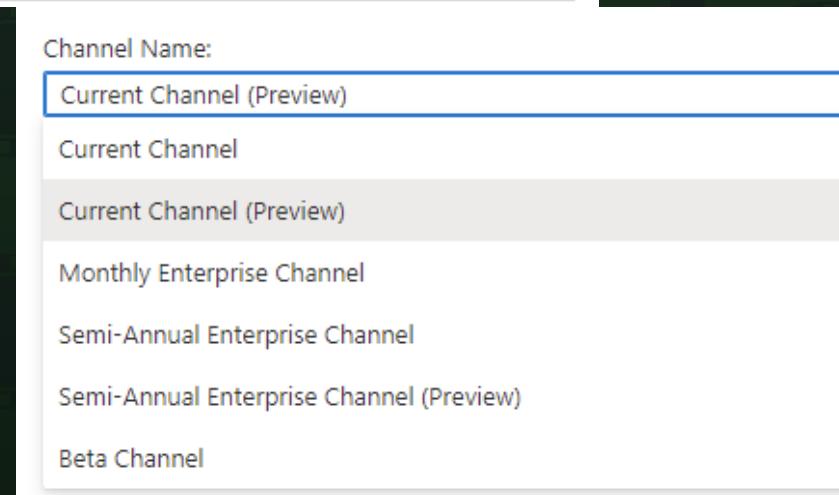
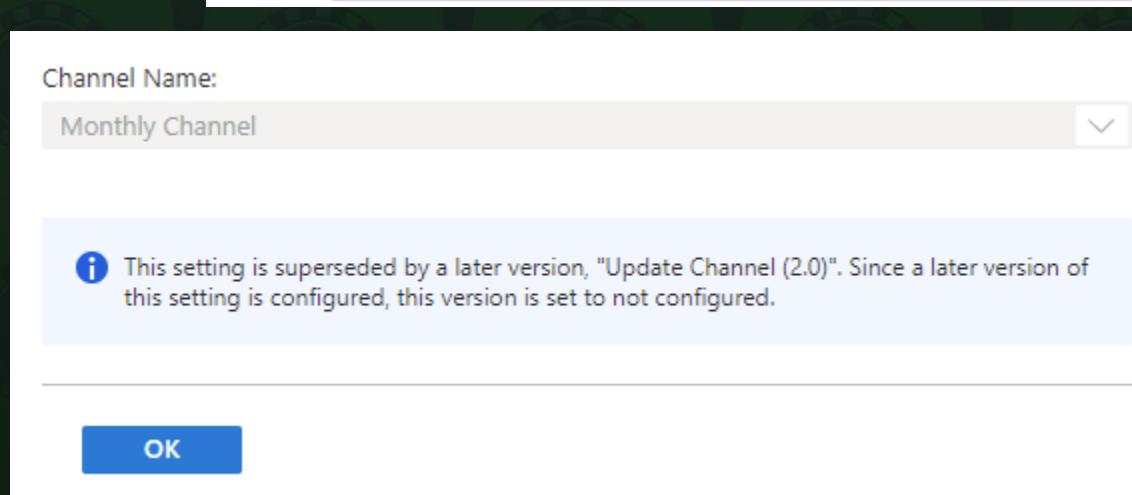
Microsoft 365 Apps Policy

- 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 |



Using Settings Catalog (Preview)

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

The screenshot shows the 'Configuration settings' step of a policy configuration wizard. The top navigation bar includes 'Configuration settings' (step 1), 'Review + save' (step 2), and a 'Back' button. Below the navigation, there's a '+ Add settings' link. The main content area is titled 'Microsoft Office 2016 (Machine)' with a 'Remove category' link. Underneath, a 'Updates' section is shown with a note: '14 of 16 settings in this subcategory are not configured'. It contains two settings: 'Enable Automatic Updates' (status: Enabled) and 'Update Channel' (status: Enabled). Both settings have a help icon (info symbol) next to them. A dropdown menu for 'Channel Name: (Device)' is open, showing 'Current Channel (Preview)' as the selected option. There are also 'Remove subcategory' and 'Remove category' links on the right side of the updates section.

#1 Check the Intune registry keys

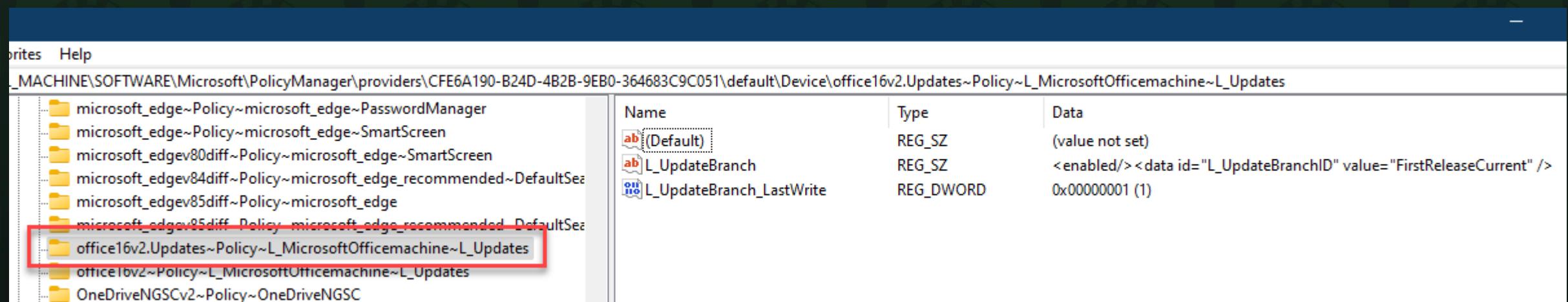
- Open the Registry Editor, and go to the Intune policy path:

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.

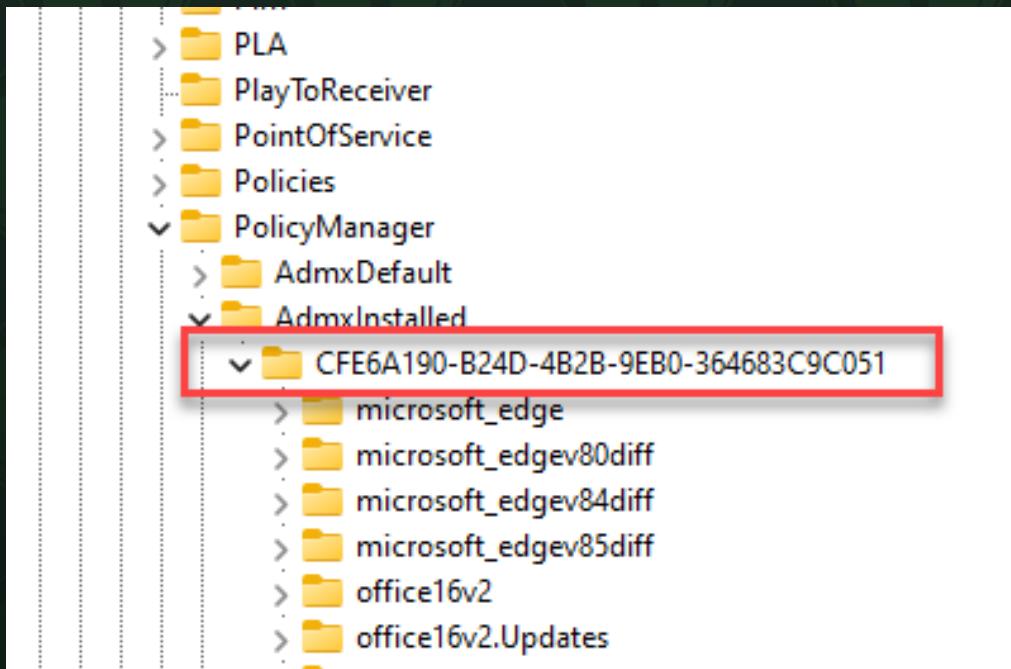


#TIP: Find the Provider ID

Find the provider ID for your device

- Open the Registry Editor, and go to:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\AdmxInstalled



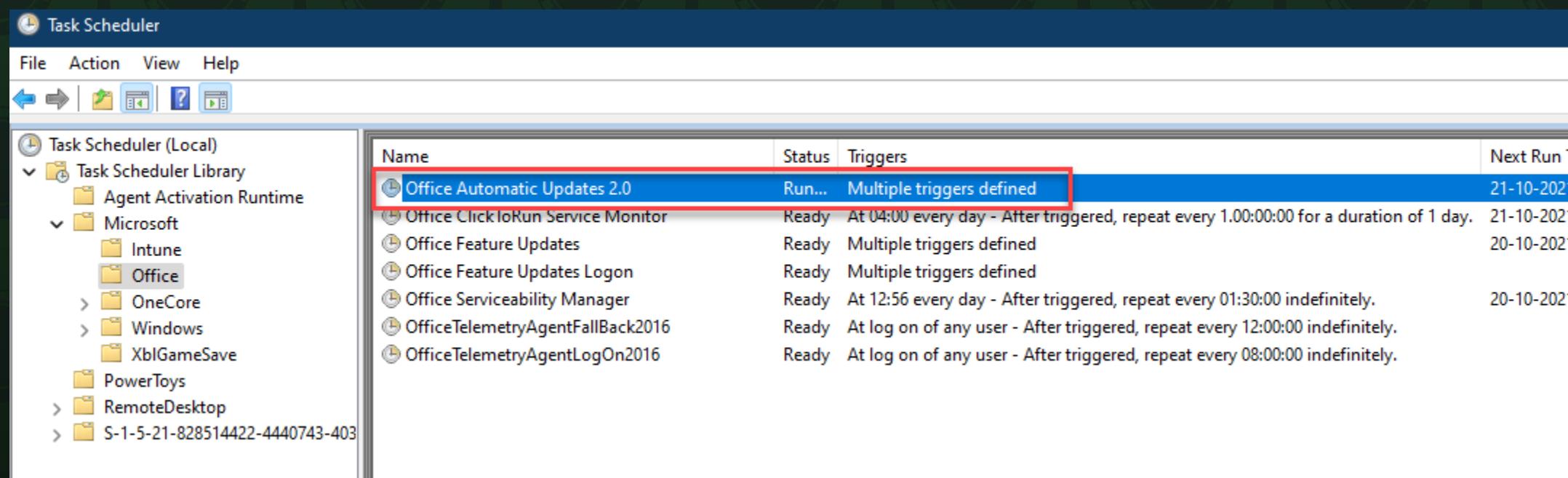
#2 Check the Office registry keys

- 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

| | | |
|--------------------------------|--------|---|
| ab SCLCacheOverride | REG_SZ | 0 |
| ab SharedComputerLicensing | REG_SZ | 0 |
| ab StreamingFinished | REG_SZ | True |
| ab StreamPackageUrlChanged | REG_SZ | True |
| ab TeamsAddOn | REG_SZ | INSTALLED |
| ab UpdateChannel | REG_SZ | http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-8936-8840a6a4f5be |
| ab UpdateChannelChanged | REG_SZ | False |
| ab UpdatesEnabled | REG_SZ | True |
| ab VersionToReport | REG_SZ | 16.0.14527.20268 |
| ab VisioProRetail.ExcludedApps | REG_SZ | groove |
| ab VSTO_PUBLISHMENT | REG_SZ | CDN |

#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 Scheduler > 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 behavior 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.

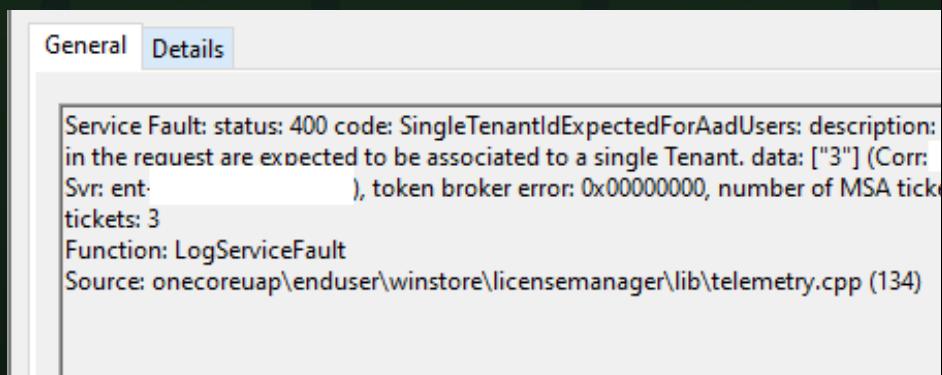
Troubleshoot Subscription based activation

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"



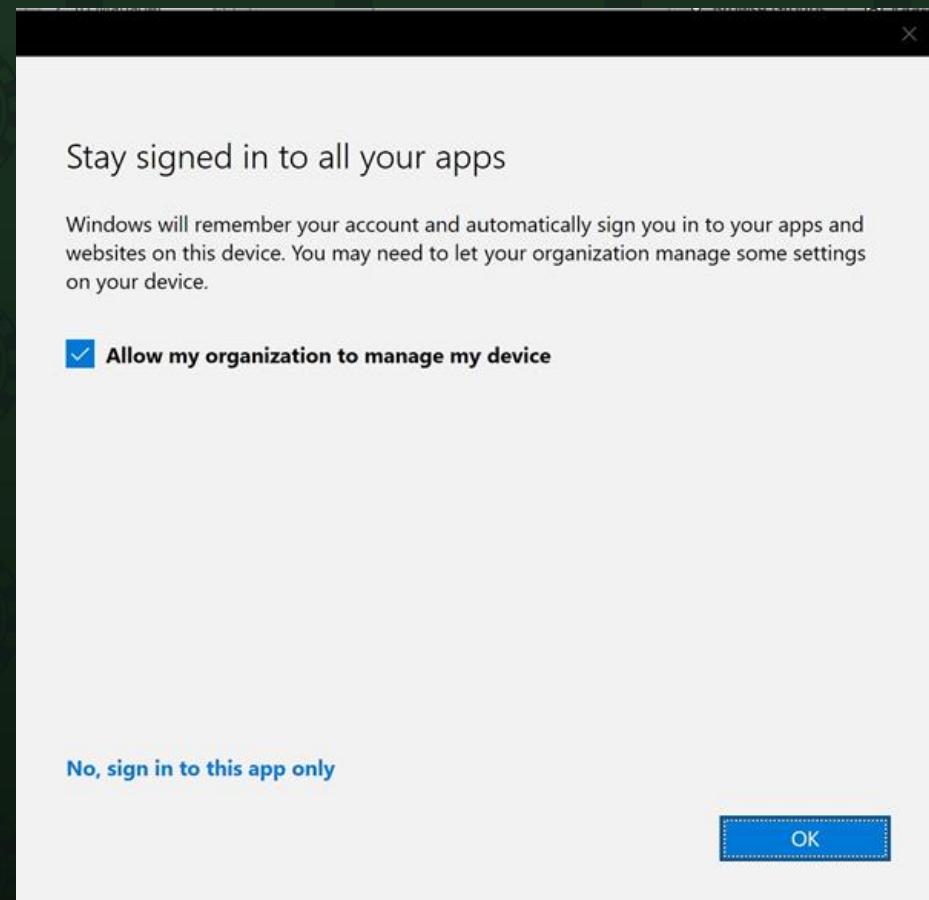
Windows

| | |
|--------------|--|
| Edition | Windows 10 Pro |
| Subscription | Windows 10 Enterprise subscription is not valid. |
| Activation | Windows is activated with a digital license |

[Learn more](#)

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

Create profile ...

Windows 10 and later - Settings catalog (preview)

Basics Configuration settings Assignments Scope tags

+ Add settings

Settings

Allow Workplace ⓘ Block

Settings picker

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

Search workpla

+ Add filter

Browse by category

Administrative Templates\Start Menu and Taskbar

Administrative Templates\System\Group Policy

Settings

1 results in the "Settings" category

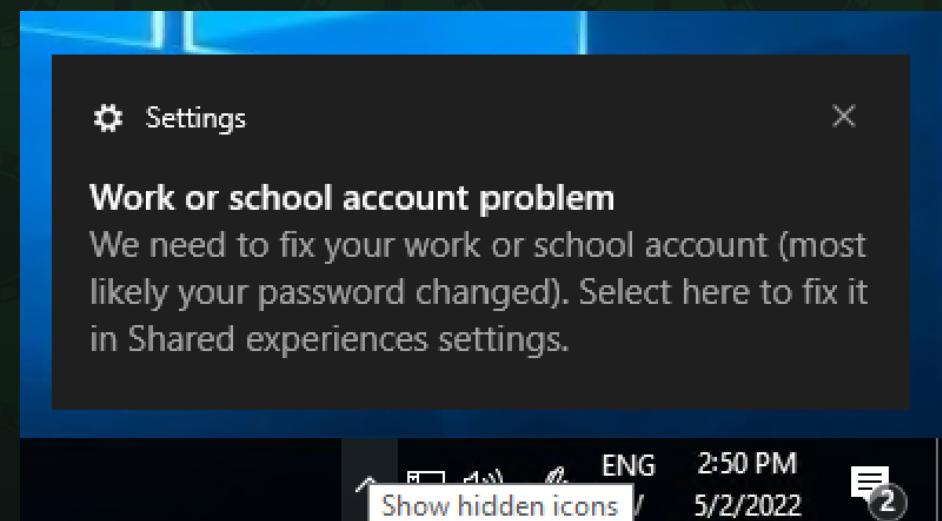
Select all these settings

Setting name

Allow Workplace ⓘ

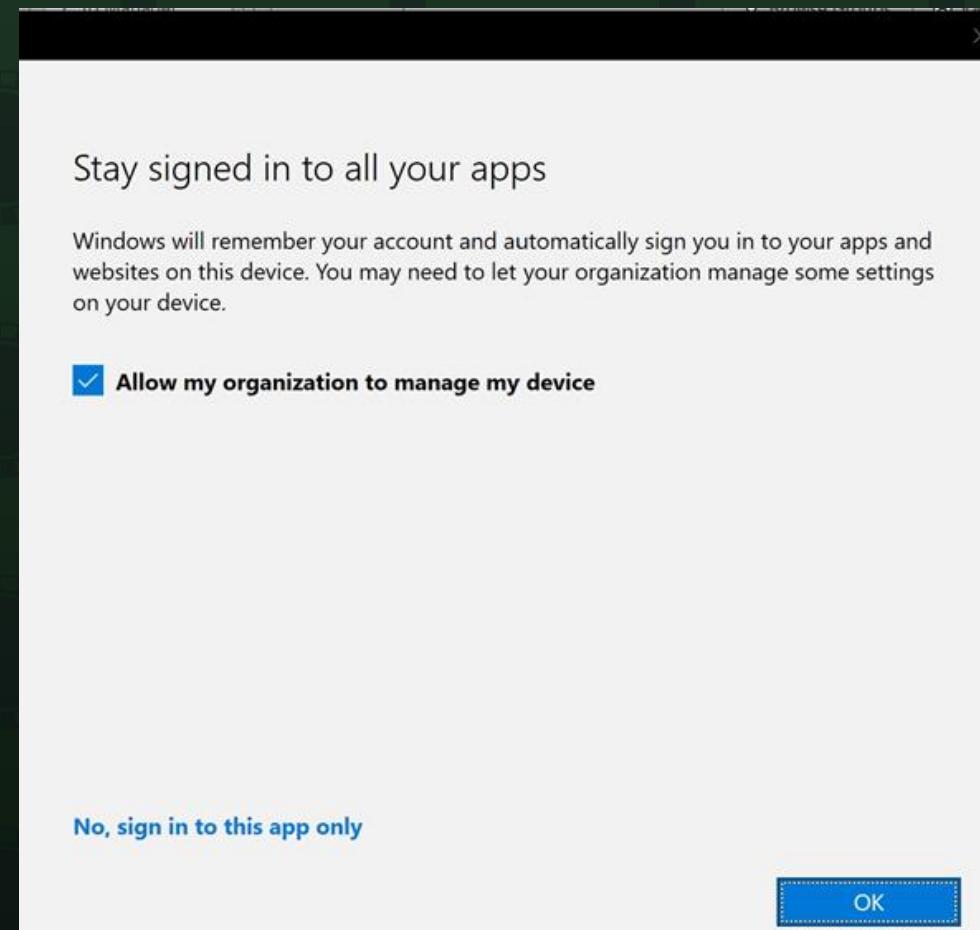
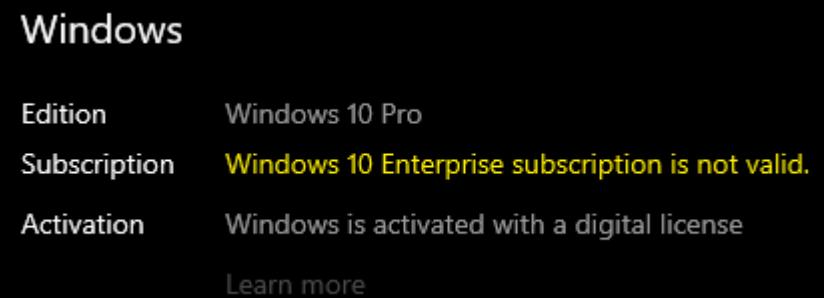
Subscription based licensing

- 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 259
Inbox
Drafts
Sent Items
Deleted Items
Archive
Conversation History
Junk Email
Outbox
RSS Feeds
Search Folders

Groups
You have not joined any groups...

Items: 529 Unread: 259 All folders are up to date. Connected to: Microsoft Exchange

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

Power BI <powerbi@email2.micr... 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

Right-click

Your free Power BI Pro trial subscription expires soon

We hope you've enjoyed the advantages of Power BI. Your Power BI Pro trial subscription ends soon. To continue getting the most out of your business insights, you'll need to purchase a Power BI Pro license. It's easier than ever.

Activate Windows
Go to Settings to activate Windows.

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 reauest 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 enrollemt 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

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

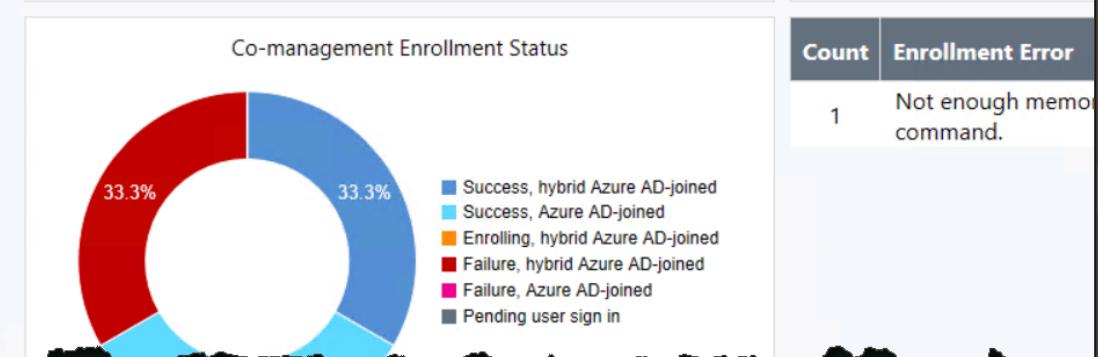
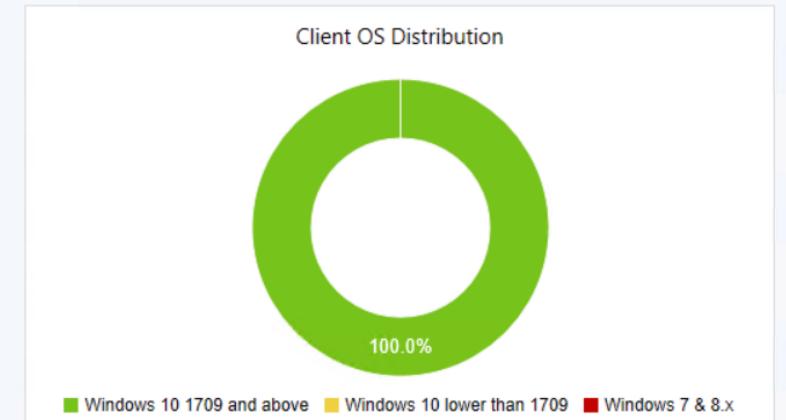
Timestamp: 08-16-2019 9:14:01Z

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>

Cloud Attach

Co-management



Home > Microsoft Intune > Device enrollment - Enrollment failures

Device enrollment - Enrollment failures

Microsoft Intune

Search (Ctrl+ /) Filter Refresh Export

Quick start

Manage

- Apple enrollment
- Android enrollment
- Windows enrollment
- Terms and conditions
- Enrollment restrictions
- Device categories
- Corporate device identifiers
- Device enrollment managers

Monitor

- Enrollment failures** (highlighted with a red box)
- Audit logs
- Incomplete user enrollments

Help and support

Select user All users

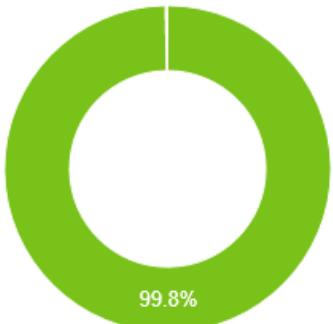
Date Failure OS OS version

Select a user or all users.

Cloud Attach

Co-management

Client OS Distribution



■ Windows 10 1709 and above ■ Windows 10 lower than 1709 ■ Windows 7 & 8.x

Co-management Status

Eligible devices

18157

Scheduled

17873

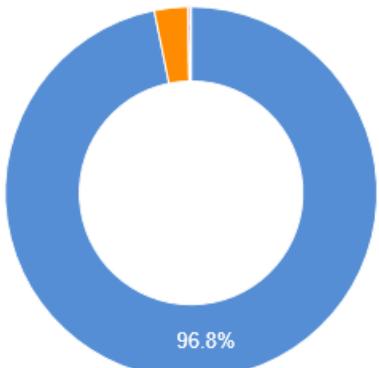
Enrollment Initiated

17871

Enrolled

17352

Co-management Enrollment Status



■ Success, hybrid Azure AD-joined
■ Success, Azure AD-joined
■ Enrolling, hybrid Azure AD-joined
■ Failure, hybrid Azure AD-joined
■ Failure, Azure AD-joined
■ Pending user sign in

| 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

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

| 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 or 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 |

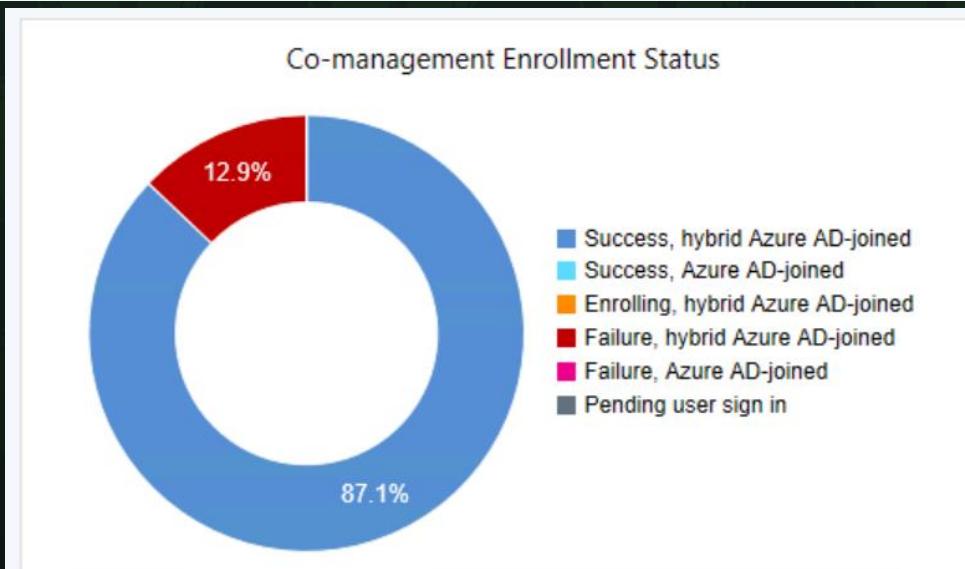
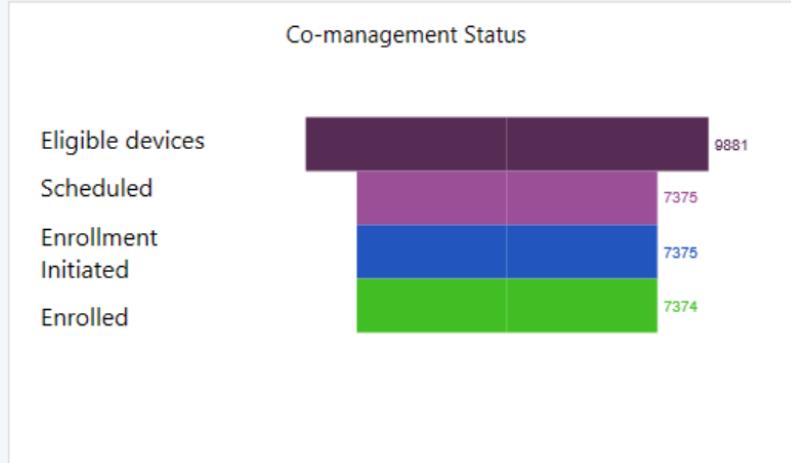
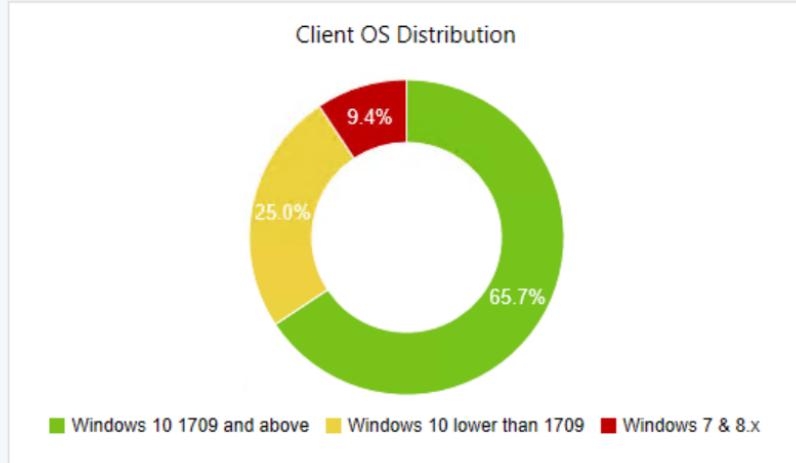
GET SUPPORT

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

Activity ID: 112401f7

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”

The screenshot shows the Microsoft Intune interface for managing device enrollment. The URL in the address bar is "Home > Devices > Enroll devices >". A red box highlights the "All Users" button under the "Restriction policy" section. Below this, there is a search bar with the placeholder "Search (Ctrl+/" and a "..." button. The "Overview" tab is selected, indicated by a grey background. The "Essentials" section displays the following details:

- Created : 01/01/70, 1:00 AM
- Last modified : 05/11/20, 11:20 AM
- Platforms configured : 6
- Assigned to : All devices.

A red box also highlights the "Assigned to : All devices." text. On the left side, there are navigation links for "Manage" and "Properties".

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+ /) <>

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

Overview

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 : ---
[See more](#)

Primary User : Ronni Pedersen
Enrolled by : Ronni Pedersen
Compliance : Not Compliant
Operating system : Windows
Device model : Virtual Machine

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Recovery keys

Managed Apps

Device actions status

| Action | Status | Date/Time |
|------------|--------|-----------|
| No results | | |

Co-management

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

Configuration Manager agent state
Unknown

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

Last Configuration Manager agent check in time
05-06-2019 15:10:12

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

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

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 | |
| File Classification | |

Name

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

[General](#) [Triggers](#) [Actions](#) [Conditions](#) [Settings](#) [History \(disabled\)](#)

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

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

Intune notifications / Sync immediately

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



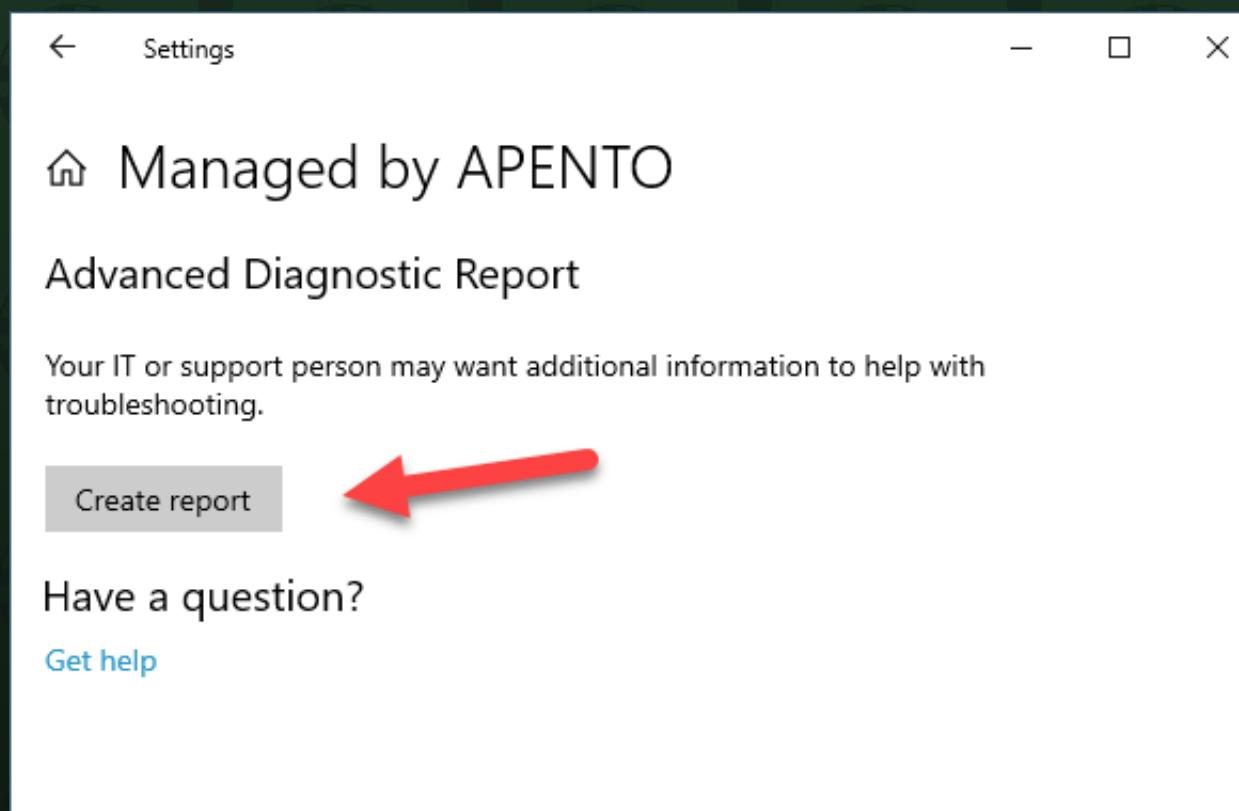
Policy/Profile Conflicts

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



Troubleshooting MDM Policies

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



Managed policies

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

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

Intune Troubleshooting Pane

- Intune portal page
 - <https://aka.ms/intunetroubleshooting>
- Displays information focused around a particular user
 - See info about assignments, devices, enrollment failures, etc.
- For more info:
<https://docs.microsoft.com/en-us/intune/help-desk-operators>

The screenshot shows the Microsoft Intune - Troubleshoot page for a user named Anna Anderson. The top navigation bar includes 'Dashboard' and 'Microsoft Intune - Troubleshoot'. A sidebar on the left contains links for Device compliance, Device configuration, Devices, Client apps, Device security, eBooks, Conditional access, Exchange access, Users, Groups, Roles, Software updates, Monitoring, Diagnostics settings, Help and support (with 'Help and support' and 'Tenant Status' listed), and Troubleshoot (which is highlighted). The main content area displays the user's account status as 'Active' with a green checkmark. It shows the user's display name, principal name (anna@contoscm.com), and email. Below this, under 'GROUP MEMBERSHIP', it lists 'AutoPilot Users'. Under 'ASSIGNMENTS', there is a dropdown menu set to 'Client apps' showing a table with columns: ASSIGNMENT, NAME, OS, TYPE, and L. The table lists five assignments: AutopilotBranding (Included, Windows P..., required, 4), Chrome (Included, Windows P..., required, 3), Office 365 ProPlus (Included, Windows 10..., required, 3), paint.net (Included, Windows P..., required, 2), and VPNSetup (Included, Windows P..., required, 1). Under 'DEVICES', there is a table with columns: DEVICE, MDM, NOT ENROLLED, CORP, TROUBLESHOOT, AZURE AD, ANDROID, OS. The table shows one device entry: AAD-573... (MDM: Not ...; Corp: Yes; Troubleshoot: Yes; Azure Ad: NA; Android: Win).

| ASSIGNMENT | NAME | OS | TYPE | L |
|------------|---------------------------|---------------|----------|---|
| Included | AutopilotBranding | Windows P... | required | 4 |
| Included | Chrome | Windows P... | required | 3 |
| Included | Office 365 ProPlus (cu... | Windows 10... | required | 3 |
| Included | paint.net | | required | 2 |
| Included | VPNSetup | Windows P... | required | 1 |

| DEVICE | MDM | NOT ENROLLED | CORP | TROUBLESHOOT | AZURE AD | ANDROID | OS |
|------------|-----|--------------|--|--------------|----------|---------|-----|
| AAD-573... | MDM | Not ... | Corp... Yes | Yes | NA | | Win |

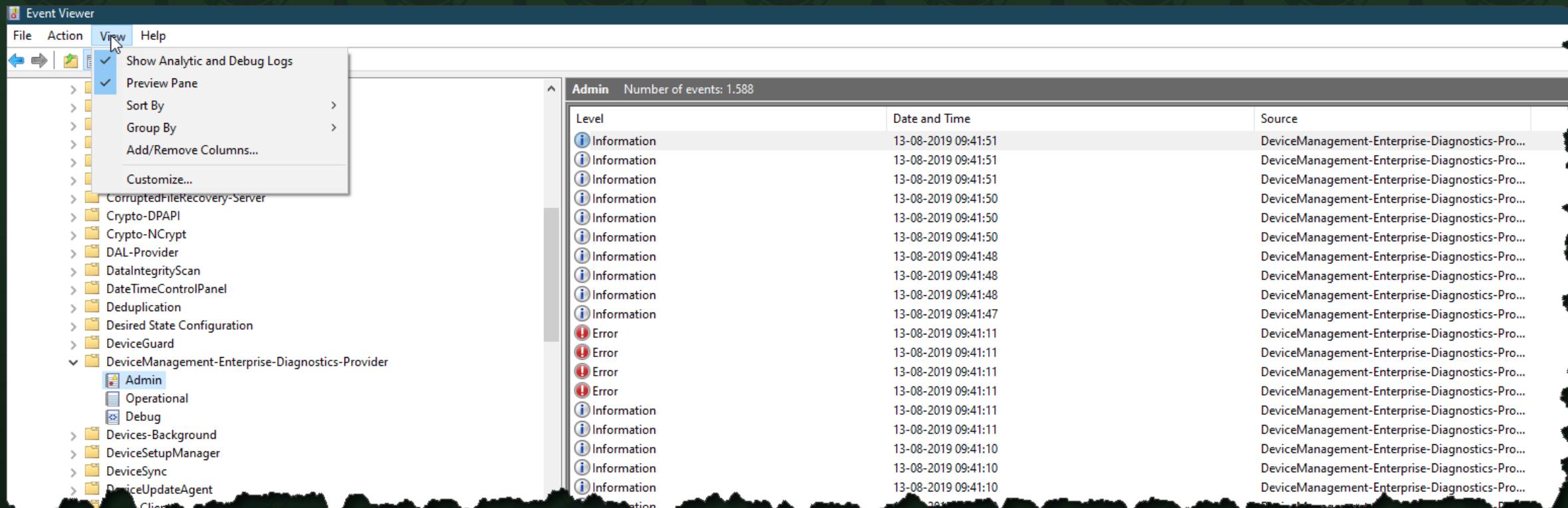
Device Profiles - Where is my logs?

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

The screenshot shows the Windows Event Viewer interface. On the left, there is a navigation pane with a tree view of log sources. The 'DeviceManagement-Enterprise-Diagnostics-Provider' source is expanded, showing its sub-categories: Admin and Operational. Under Admin, there are three log entries: one Error event and two Information events, all occurring at 13-08-2019 09:41:11. Under Operational, there are 15 Information events, all occurring between 13-08-2019 09:41:10 and 13-08-2019 09:41:51. The main pane displays a table of events with columns for Level, Date and Time, and Source. The first 15 rows correspond to the events listed in the navigation pane, while the last row is a summary: 'Number of events: 1.588'. The 'Source' column for the Admin events shows 'DeviceManagement-Enterprise-Diagnostics-Pro...', and for the Operational events, it shows 'DeviceManagement-Enterprise-Diagnostics-Pro...'. The 'Level' column shows 'Information' for most events and 'Error' for the first three Admin events.

| Level | Date and Time | Source |
|-------------|---------------------|--|
| Information | 13-08-2019 09:41:51 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:51 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:51 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:50 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:50 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:50 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:48 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:48 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:48 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:47 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Error | 13-08-2019 09:41:11 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Error | 13-08-2019 09:41:11 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Error | 13-08-2019 09:41:11 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:11 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:11 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:10 | DeviceManagement-Enterprise-Diagnostics-Pro... |
| Information | 13-08-2019 09:41:08 | DeviceManagement-Enterprise-Diagnostics-Pro... |

Enable debug mode



Intune Management Extension

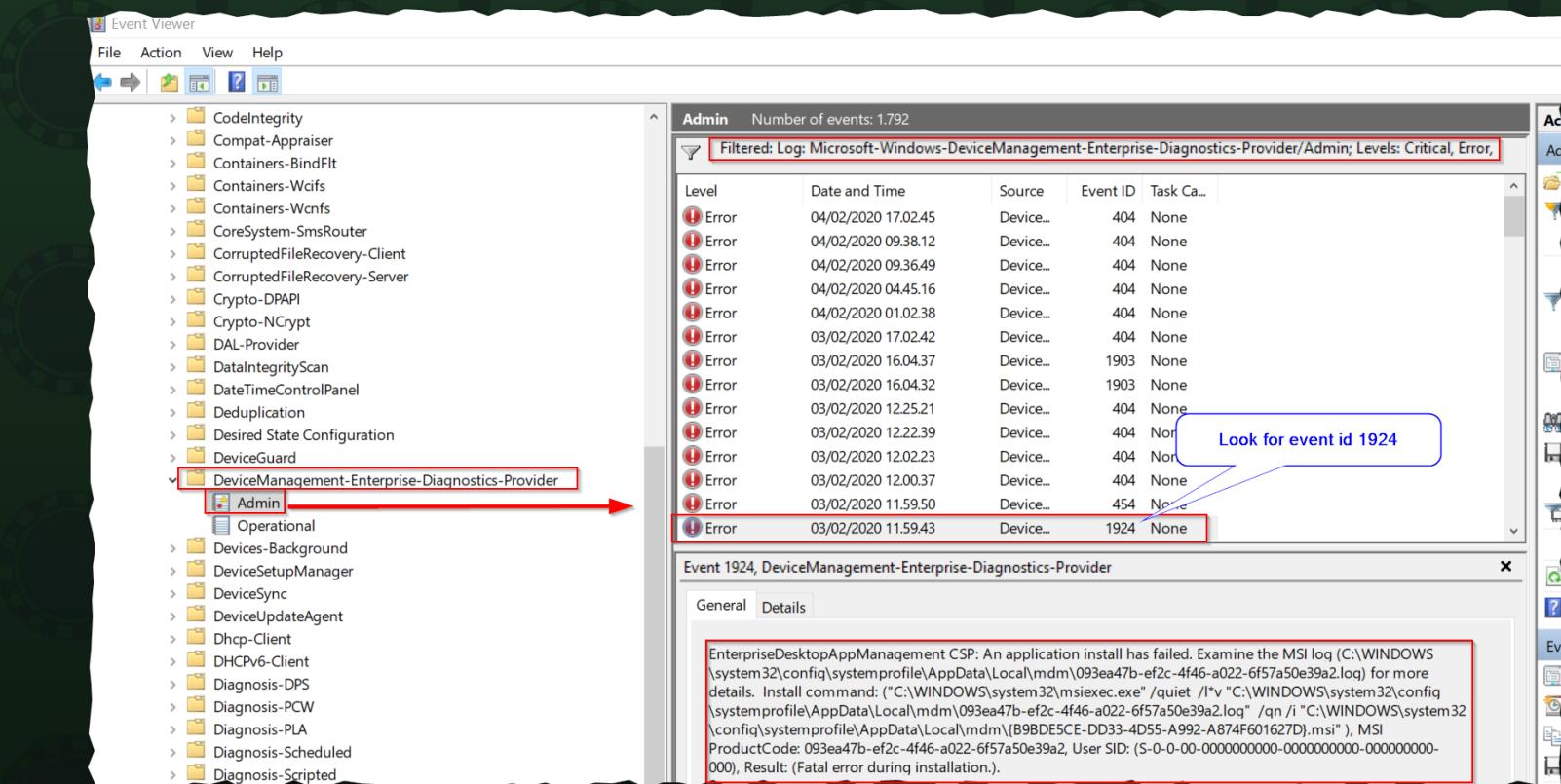
Intune Management Extension

- 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

The screenshot displays two Windows File Explorer windows illustrating the file structure of the Microsoft Intune Management Extension.

Left Window: Shows the main directory structure:

- Local Disk (C:) > Program Files (x86) > Microsoft Intune Management Extension > Content
- Content folder structure:
 - DetectionScripts (File folder)
 - Incoming (File folder)
 - Staging (File folder)

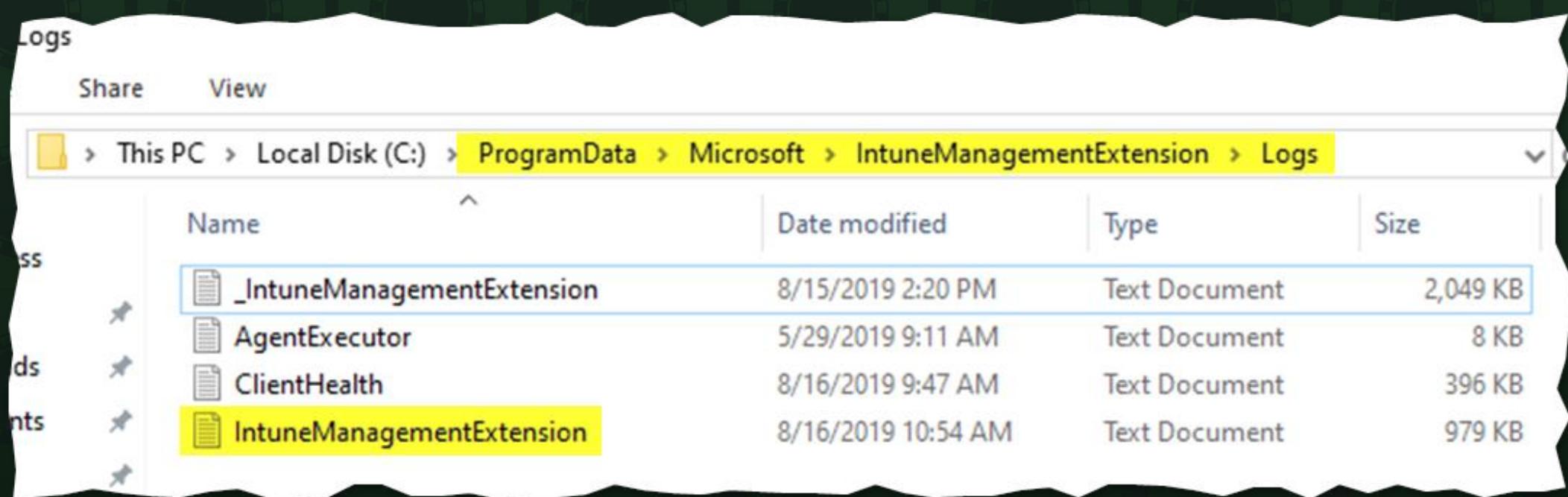
Right Window: Shows the contents of the "Content" folder:

| Name | Date modified | Type | Size |
|-----------------------------|------------------|----------------------|--------|
| fi | 18-07-2019 08:51 | File folder | |
| fr | 18-07-2019 08:51 | File folder | |
| hu | 18-07-2019 08:51 | File folder | |
| it | 18-07-2019 08:51 | File folder | |
| ja | 18-07-2019 08:51 | File folder | |
| ko | 18-07-2019 08:51 | File folder | |
| nl | 18-07-2019 08:51 | File folder | |
| no | 18-07-2019 08:51 | File folder | |
| pl | 18-07-2019 08:51 | File folder | |
| Policies | 16-05-2019 23:23 | File folder | |
| pt-br | 18-07-2019 08:51 | File folder | |
| ro | 18-07-2019 08:51 | File folder | |
| ru | 18-07-2019 08:51 | File folder | |
| sv | 18-07-2019 08:51 | File folder | |
| tr | 18-07-2019 08:51 | File folder | |
| zh-HANS | 18-07-2019 08:51 | File folder | |
| zh-HANT | 18-07-2019 08:51 | File folder | |
| AgentExecutor | 11-07-2019 17:10 | Application | 52 KB |
| AgentExecutor.exe.config | 06-05-2019 10:29 | CONFIG File | 1 KB |
| ClientHealthEval | 11-07-2019 17:10 | Application | 51 KB |
| ClientHealthEval.exe.config | 06-05-2019 10:29 | CONFIG File | 1 KB |
| conct140.dll | 20-01-2017 14:20 | Application exten... | 239 KB |
| HealthCheck | 06-05-2019 10:29 | XML Document | 3 KB |
| HealthReport.json | 13-08-2019 07:43 | JSON File | 1 KB |
| ImeUI | 11-07-2019 17:10 | Application | 22 KB |
| ImeUI.exe.config | 06-05-2019 10:29 | CONFIG File | 1 KB |

50 items

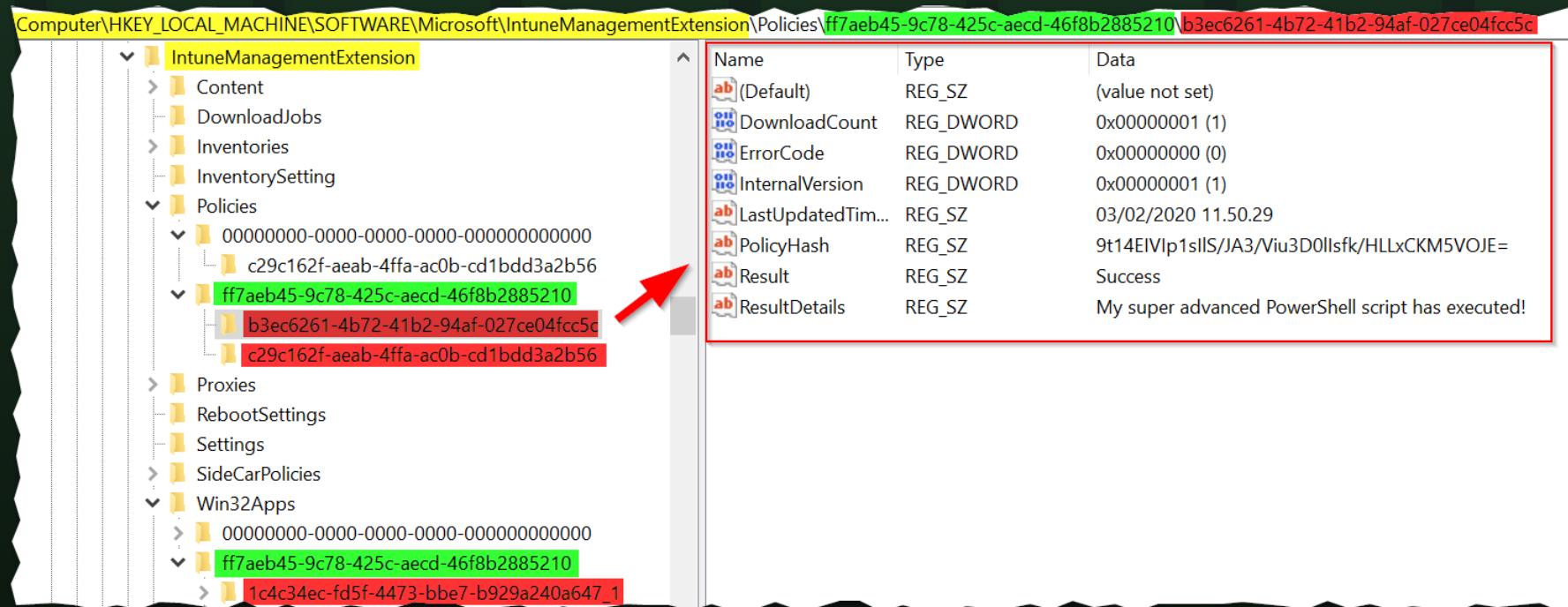
Intune Management Extension Log files

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



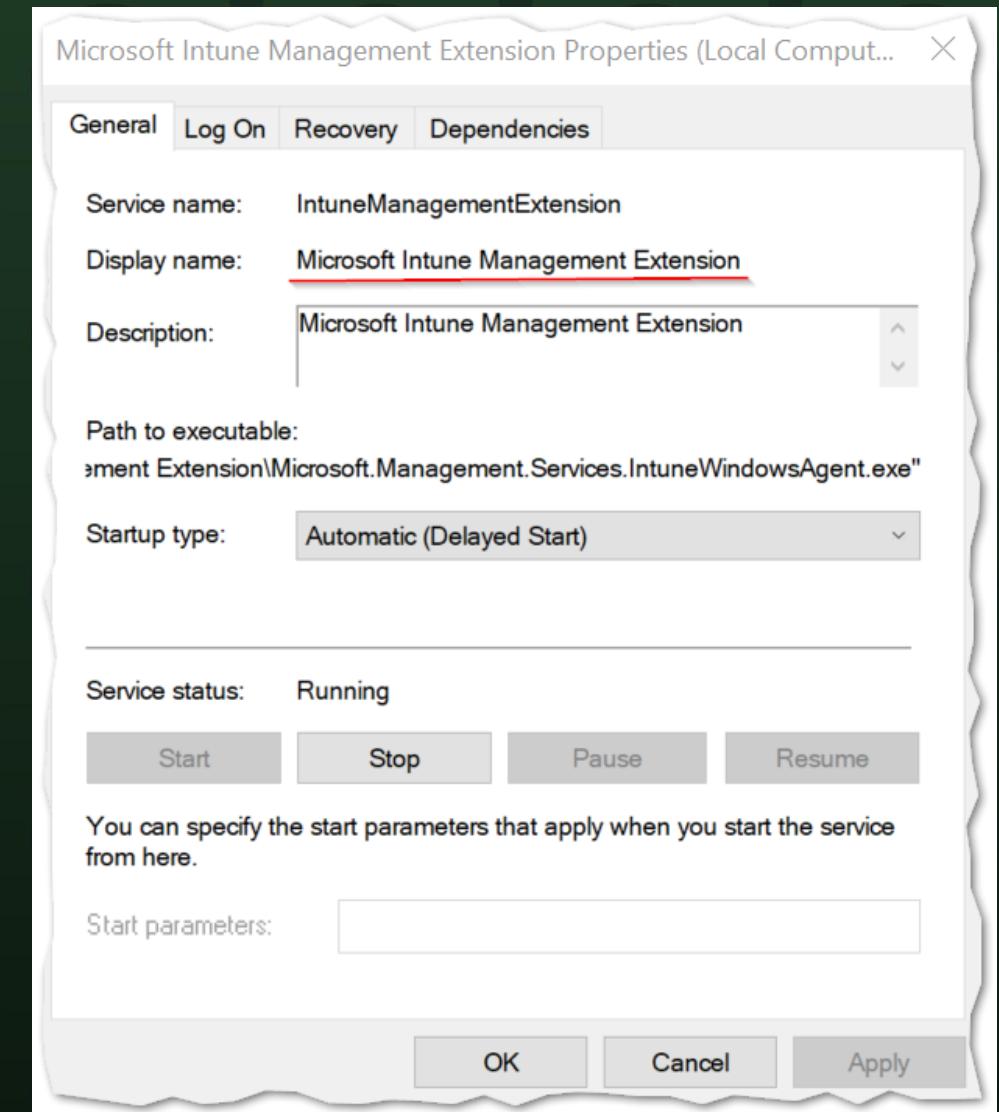
Intune Management Extension The Registry

- 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?



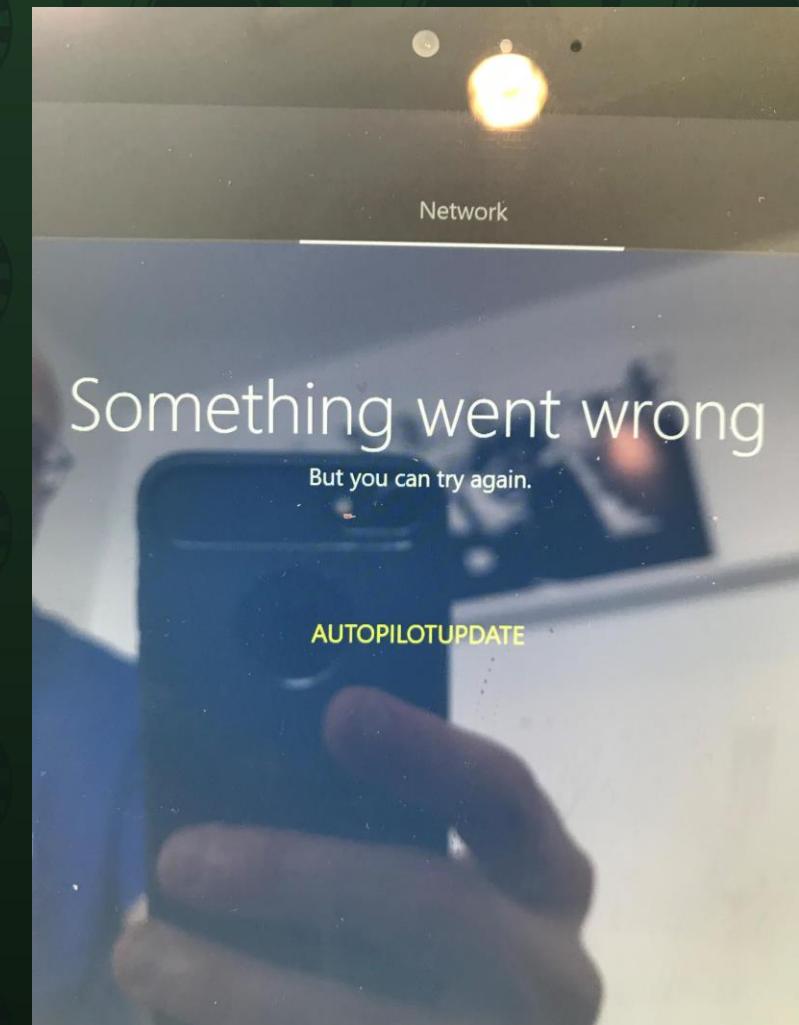
<https://docs.microsoft.com/en-us/intune/apps/intune-management-extension#prerequisites>



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.

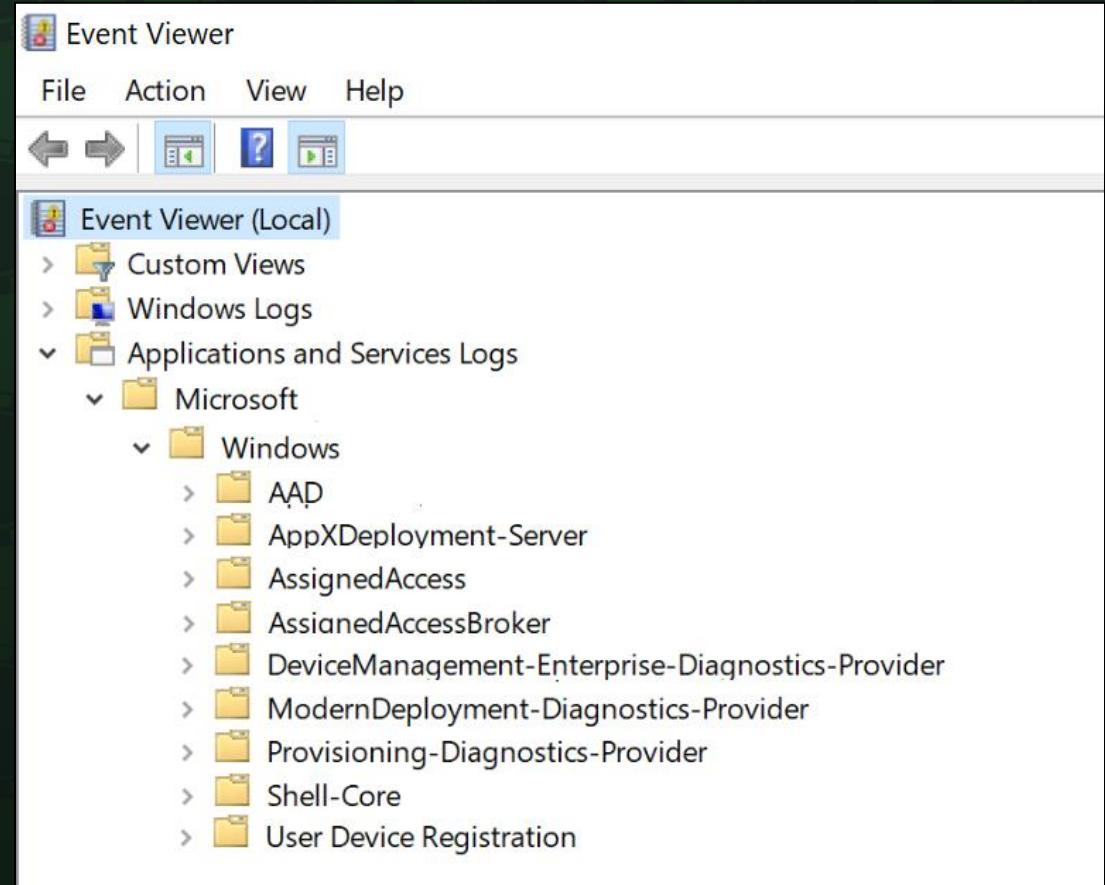
QuickAssist + AutoPilot

The image shows a screenshot of a Microsoft setup wizard window titled "Let's set things up for your work or school". The window has a light blue header bar with a back arrow icon. Below the header, there is a decorative graphic featuring a blue notebook, a clipboard with a checklist, and an orange pie chart. The main text reads "Let's set things up for your work or school" followed by "You'll use this info to sign in to your devices." To the right of the text is a "Sign in" form with an "e-mail" input field. Below the input field is a link "Can't access your account?". At the bottom of the window, there is a note about agreeing to the Microsoft Services Agreement and privacy statement, followed by a "Next" button. The window is centered on a dark green background with a repeating circular pattern.

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



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!