

HTMD Conference 2021

20th Nov



Speaker



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)

Troubleshooting a MEM managed Windows 10/11

HTMD Conference 2021
20th Nov

Speaker



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)

Troubleshooting a MEM managed Windows 10/11

HTMD Conference 2021
20th Nov

Takeaways

- Tools
- The Log Files
- Configuration Policy Process
- Subscription Based Activation
- Troubleshooting Enrollment
- Troubleshooting Policies
- Intune Management Extension

Remote Control

- TeamViewer integrates in the Endpoint Management Portal
- Quick Assist is built-in
 - Lacks UAC support
 - No Logging
 - Maybe OK for smaller organizations
 - Can be used during AutoPilot



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



Let's set things up for your work or school

You'll use this info to sign in to your devices.



Sign in

e-mail

[Can't access your account?](#)

Choosing **Next** means that you agree to the [Microsoft Services Agreement](#) and [privacy and cookies statement](#).

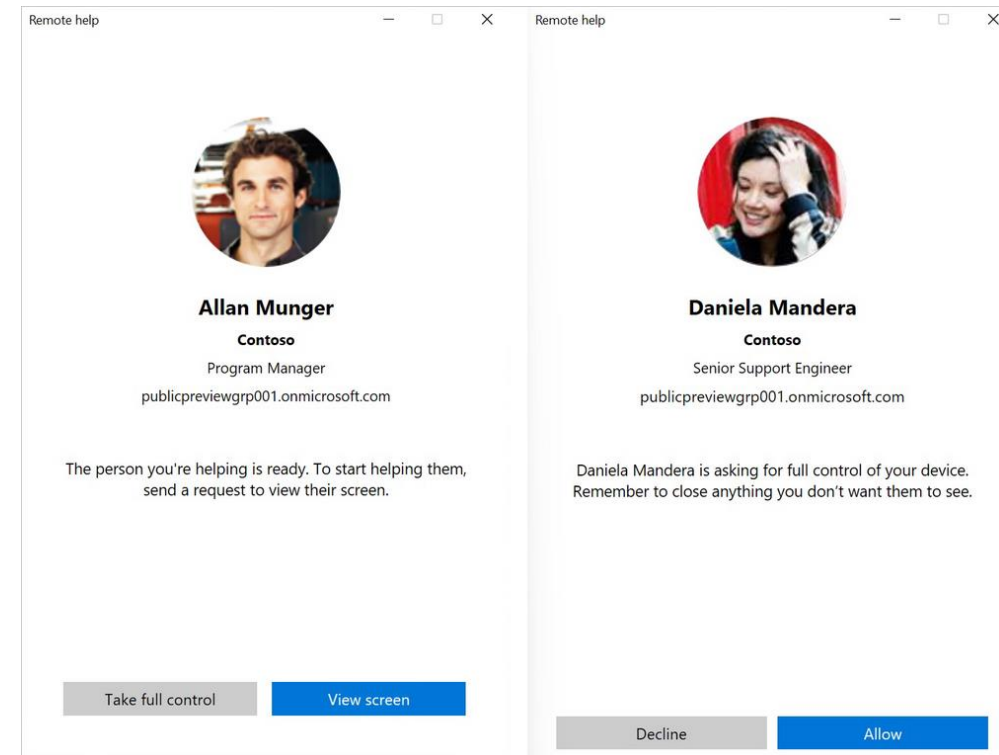
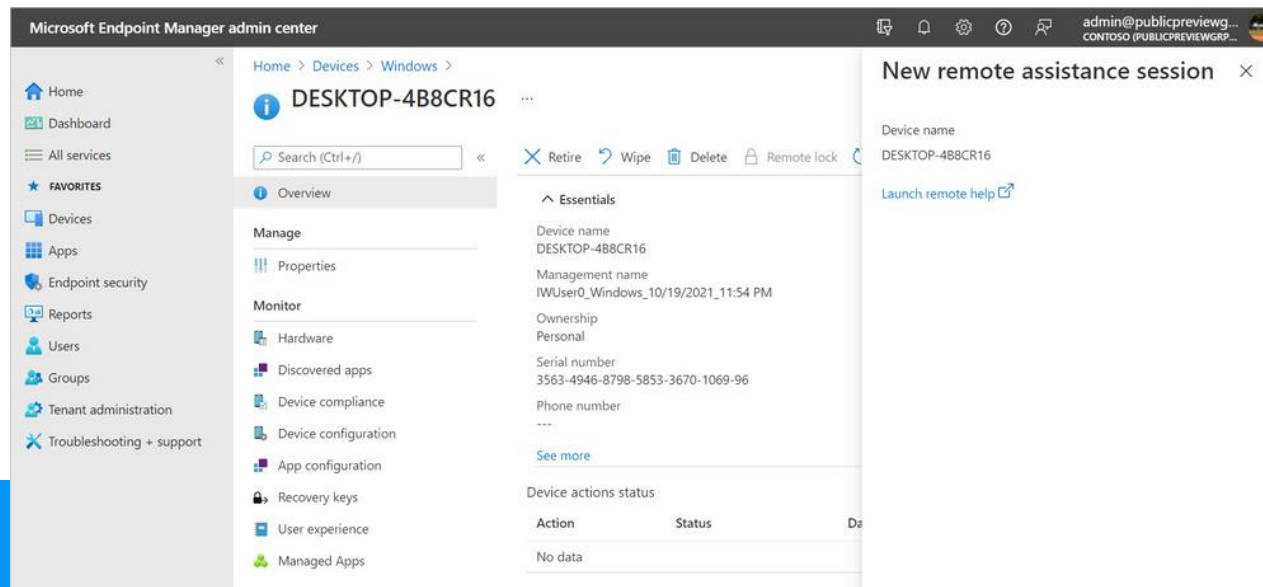
Next



Remote Help (Announced at Ignite)

- Support UAC
- RBAC
- Logging/Tracking

Note: Comes with an additional cost

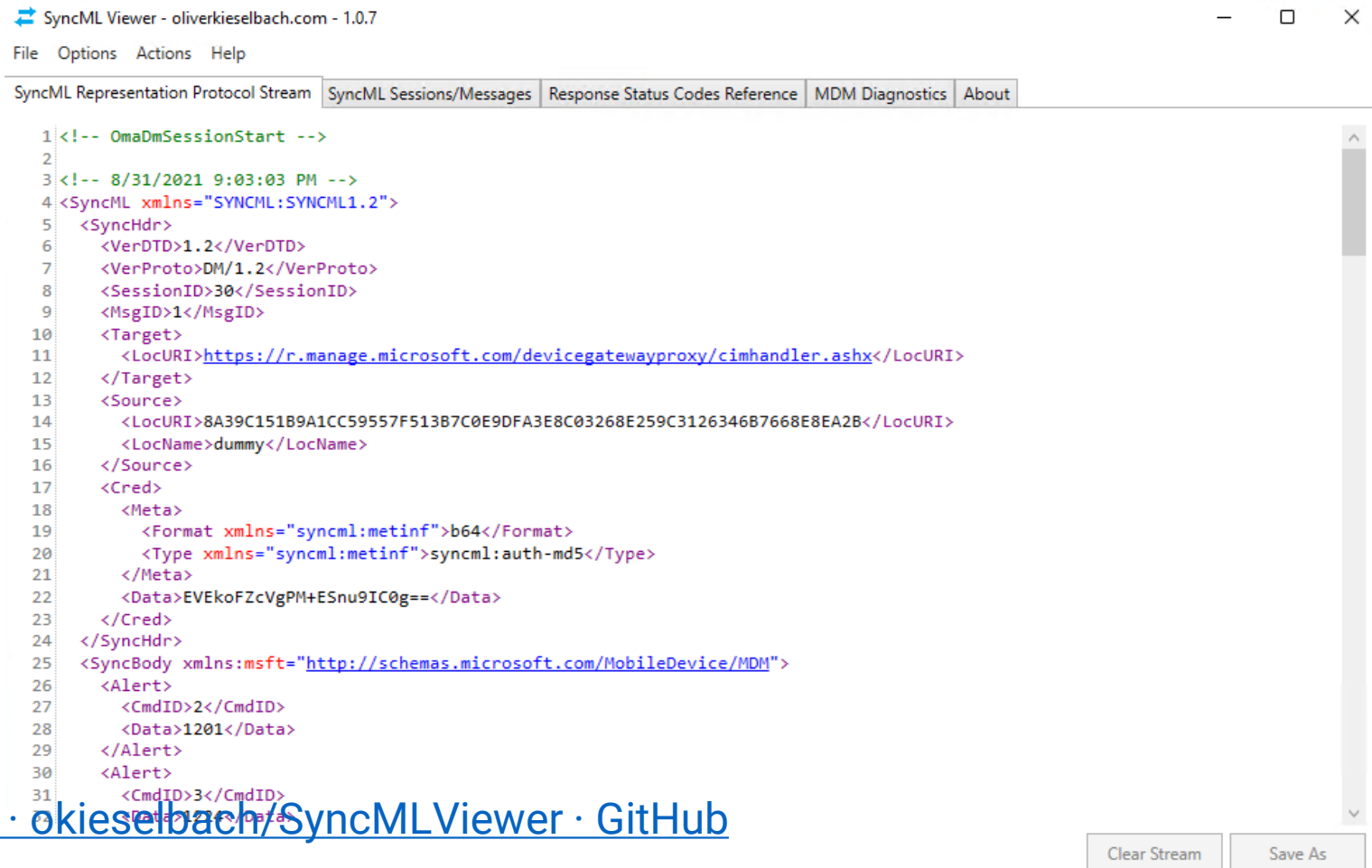


CMtrace

- Great log reader
 - Not free but included in the Intune/MEM license
 - Deploy it to all clients
-
- <https://ccmexec.com/2018/12/copy-and-associate-cmtrace-using-intune-win32app-and-powershell/>

More Tools – advanced troubleshooting

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



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". The tab bar shows "SyncML Representation Protocol Stream" (selected), "SyncML Sessions/Messages", "Response Status Codes Reference", "MDM Diagnostics", and "About". The main content area displays XML data with line numbers 1 through 31. The XML is a SyncML message with a session ID of 30 and a command ID of 2. The command data is "1201". The application has a "Clear Stream" button and a "Save As" button at the bottom right.

```
1 <!-- OmaDmSessionStart -->
2
3 <!-- 8/31/2021 9:03:03 PM -->
4 <SyncML xmlns="SYNML:SYNML1.2">
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>EVEkoFZcVgPM+ESnu9IC0g==</Data>
23    </Cred>
24  </SyncHdr>
25  <SyncBody xmlns:mst="http://schemas.microsoft.com/MobileDevice/MDM">
26    <Alert>
27      <CmdID>2</CmdID>
28      <Data>1201</Data>
29    </Alert>
30    <Alert>
31      <CmdID>3</CmdID>
```

[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>T0EeBAEAHAAAAAoAMwDwVQAACgAaAfBVCnofKQQCCQgCABAACQABAAEAAGABAAAABQAZAAQAAAAAAAAAAGAAAAAAAAACAAEAawMAEQBHZW51aW5lSW50ZWwABAA0AE1udGVsKFIPiENvcmUoVE0pIGk3LTg1NTlV
1549   </Item>
1550 </Results>
1551 <Status>
1552   <CmdID>34</CmdID>
1553   <MsgRef>2</MsgRef>
1554   <CmdRef>26</CmdRef>

```

```

<SyncML xmlns="SYNML:SYNML1.2" 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=CCMEEXEC%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

- All supported versions of Windows 10/11
- 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

Home > Windows >

DESKTOP-NIIRT6B

Search (Ctrl+/) « [Retire] [Wipe] [Delete] [Remote lock] [Sync] [Reset passcode] [Restart] **1** [Collect diagnostics] [Fresh Start]

Overview

Manage

- Properties

Monitor

- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Endpoint security configuration
- Recovery keys
- User experience
- 3** [Device diagnostics (preview)]
- Managed Apps

Collect diagnostics: Completed

Essentials

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 : NUC8i7HMK

[See more](#)

Device actions status

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

2

Device diagnostics (preview)

Refresh

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





Configuration Policy Process

Microsoft 365 Apps Policy

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


Administrative Templates

- Example using Administrative Templates

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

Channel Name:

Monthly Channel

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

OK

Channel Name:

Current Channel (Preview)

Current Channel

Current Channel (Preview)

Monthly Enterprise Channel

Semi-Annual Enterprise Channel

Semi-Annual Enterprise Channel (Preview)

Beta Channel

Using Settings Catalog (Preview)

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

1 Configuration settings 2 Review + save

[+ Add settings](#) ⓘ

^ Microsoft Office 2016 (Machine) [Remove category](#)

Updates [Remove subcategory](#)

i 14 of 16 settings in this subcategory are not configured

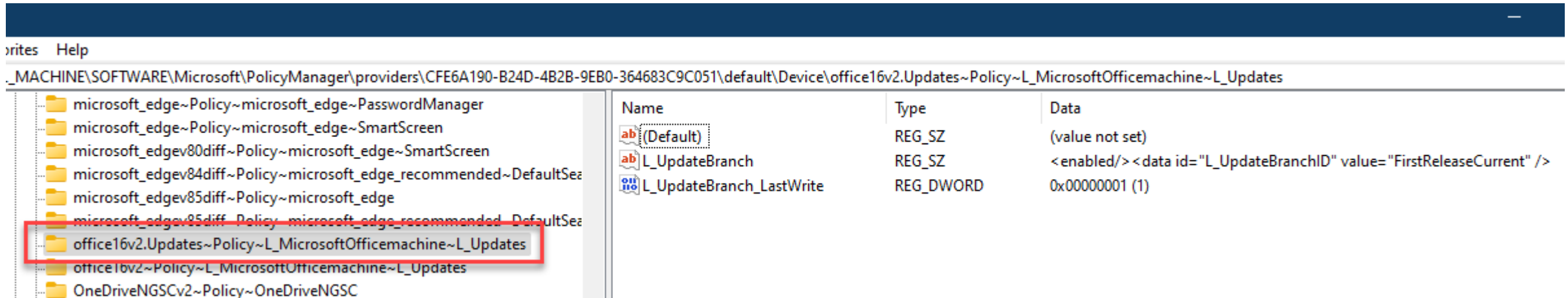
Enable Automatic Updates ⓘ ☒ Enabled ⓘ

Update Channel ⓘ ☒ Enabled ⓘ

Channel Name: (Device) *

#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.

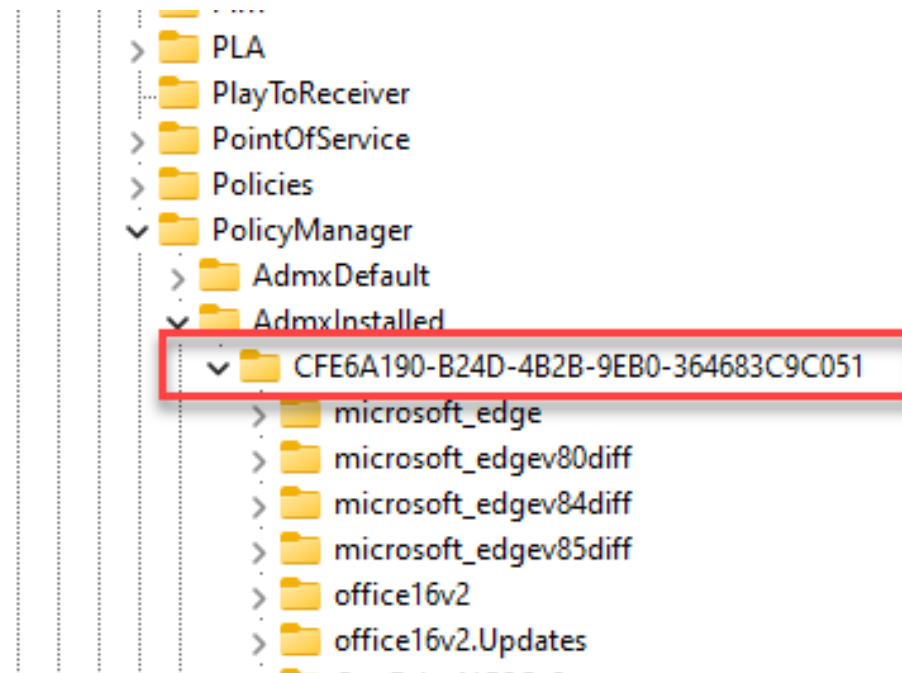


#TIP: Find the Provider ID

Find the provider ID for your device

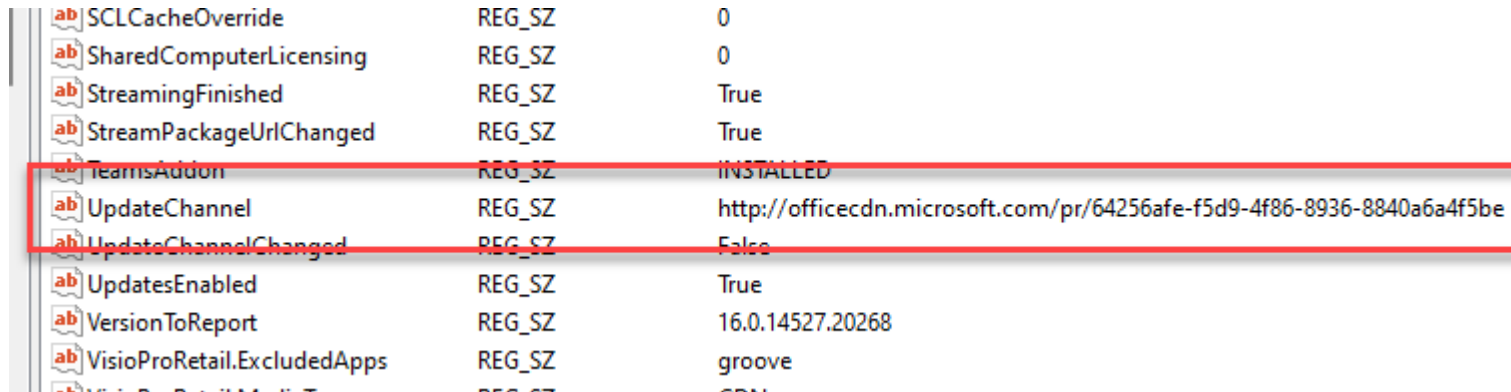
- Open the Registry Editor, and go to:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\AdmxInstalled



#2 Check the Office registry keys

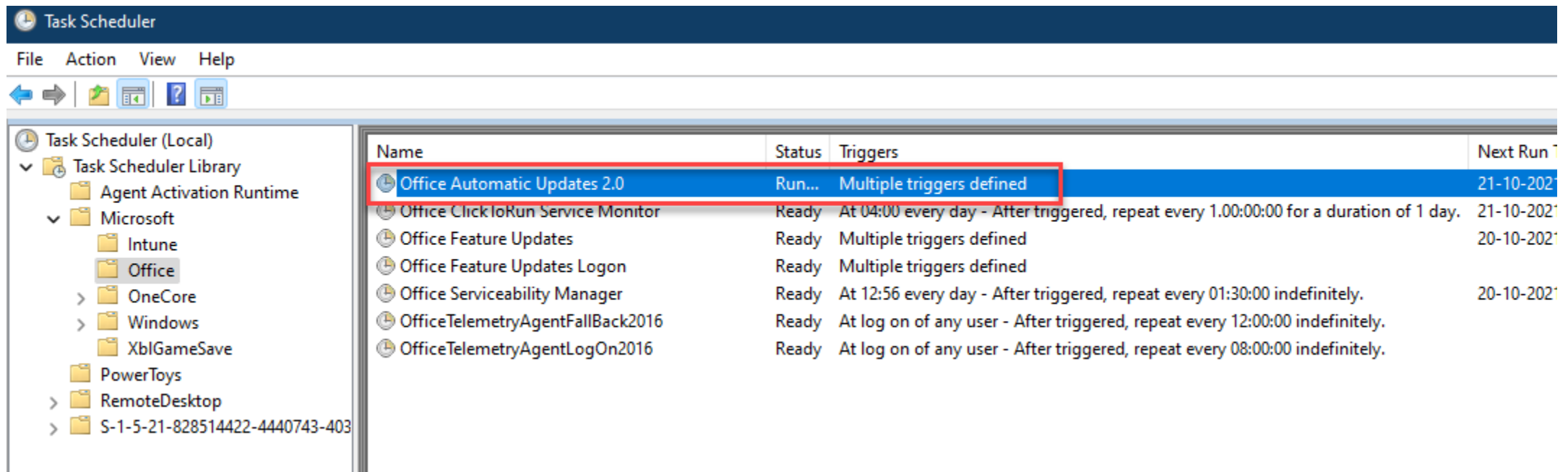
- Go to the Office policy path: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\Configuration`
- Check the **UpdateChannel** value:
 - Monthly Enterprise Channel = 55336b82-a18d-4dd6-b5f6-9e5095c314a6
 - Current Channel = 492350f6-3a01-4f97-b9c0-c7c6ddf67d60
 - **Current Channel (Preview)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



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

#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**
UpdateDetectionLastRunTime key > delete the value data.
 - Launch Task Scheduler > Microsoft > Office
Office Automatic Updates 2.0



Troubleshooting Subscription based activation

Subscription based activation

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

Windows

Edition Windows 10 Pro

Subscription **Windows 10 Enterprise subscription is not valid.**

Activation Windows is activated with a digital license

[Learn more](#)

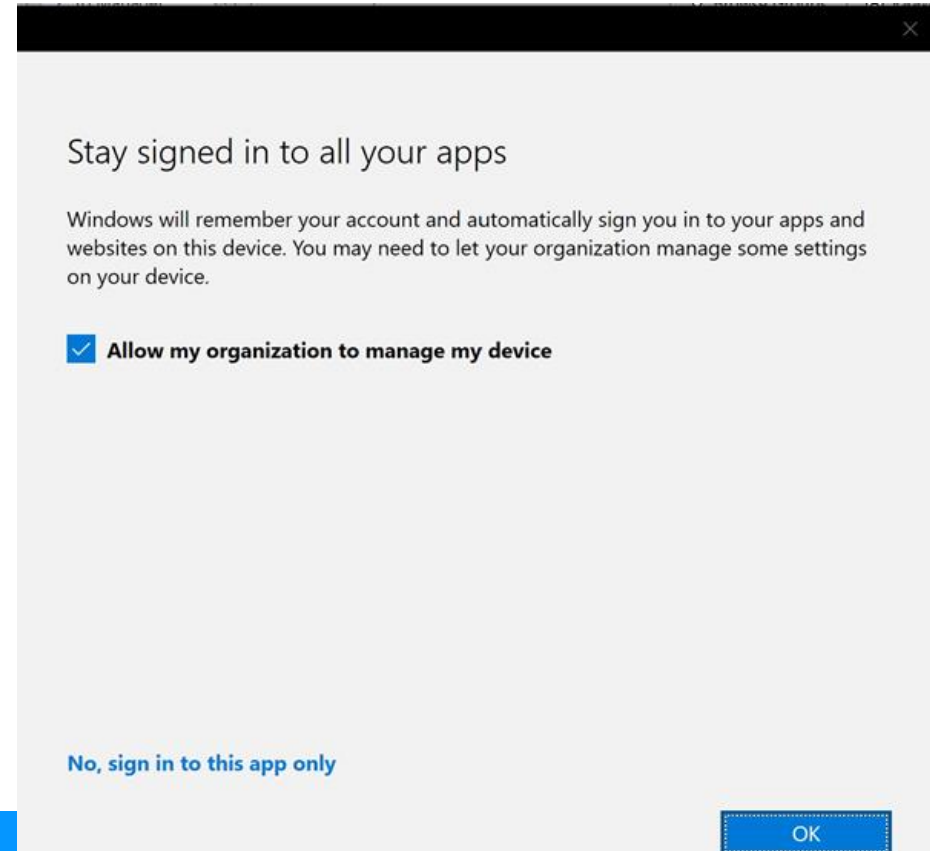
Service Fault: status: 400 code: SingleTenantIdExpectedForAadUsers: description: All Aad users provided in the request are expected to be associated to a single Tenant. data: ["3"] (Corr: Svr: ent:), token broker error: 0x00000000, number of MSA tickets: 1, number of AAD tickets: 3
Function: LogServiceFault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

result
on completed successfully. (0x0)

ork 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

Create profile

Windows 10 and later - Settings catalog (preview)

✓ Basics **2 Configuration settings** 3 Assignments 4 Scope tags 5

+ Add settings

Settings

11 of 12 settings in this category are not configured

Allow Workplace ☐ Block

Settings picker

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

workpla

+ Add filter

Browse by category

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

1 results in the "Settings" category

Select all these settings

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

Troubleshoot 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

Something went wrong.

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

Additional problem information:

Server error code: 801c0003

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

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

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

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

Enrollment Failures

Microsoft Endpoint Manager admin center

Home > Monitor

Monitor | Enrollment failures

Search (Ctrl+/) Filter Refresh Export

Configuration

Assignment status

Assignment failures (preview)

Devices with restricted apps

Encryption report

Certificates

Compliance

Noncompliant devices

Devices without compliance policy

Setting compliance

Policy compliance

Noncompliant policies (preview)

Windows health attestation report

Threat agent status

Enrollment

Autopilot deployments (preview)

Enrollment failures

Incomplete user enrollments

Software updates

Per update ring deployment state

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

ADDITIONAL RESOURCES

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

DEVICE DETAILS

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

GET SUPPORT

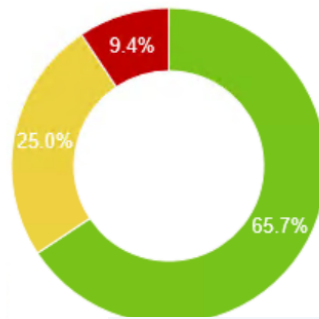
If you can't resolve this issue, [contact support](#) and paste the below Activity ID into the ticket details.

Activity ID: 112401f7-

Co-Management Enrollment Status

Co-management

Client OS Distribution



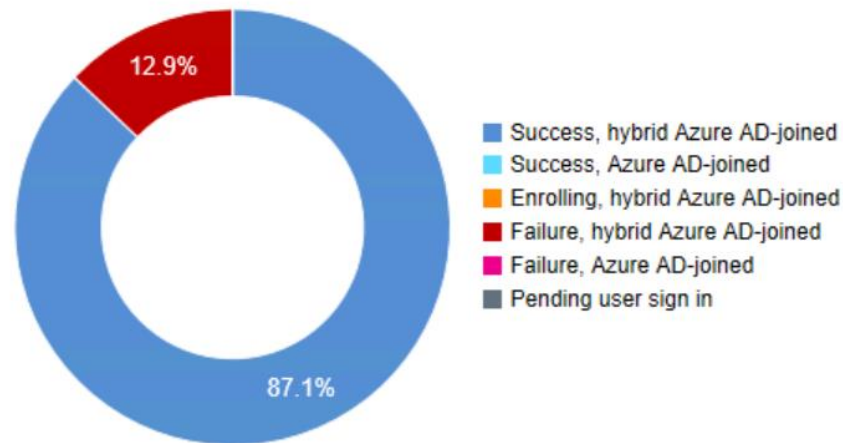
■ Windows 10 1709 and above ■

Co-management Status

Eligible devices
Scheduled
Enrollment
Initiated
Enrolled



Co-management Enrollment Status



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

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”

Home > Devices > Enroll devices >

All Users ...

Search (Ctrl+ /) <<

^ Essentials

Created : 01/01/70, 1:00 AM

Last modified : 05/11/20, 11:20 AM

Platforms configured : 6

Assigned to : All devices.

Overview

Manage

Properties

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 10/11 devices will schedule 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-A364-98DBD5B8ECB7
 - VirtualizationBasedIsolation
 - 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 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 04-04-2020 - After triggered, repeat every 7:00:00:00 for a duration of 19:00:00:00.
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
- Current Limitation:
 - By design (to avoid denial of service)
 - Not the same for all platforms
 - Workaround: Use script to connect to all clients and force a sync



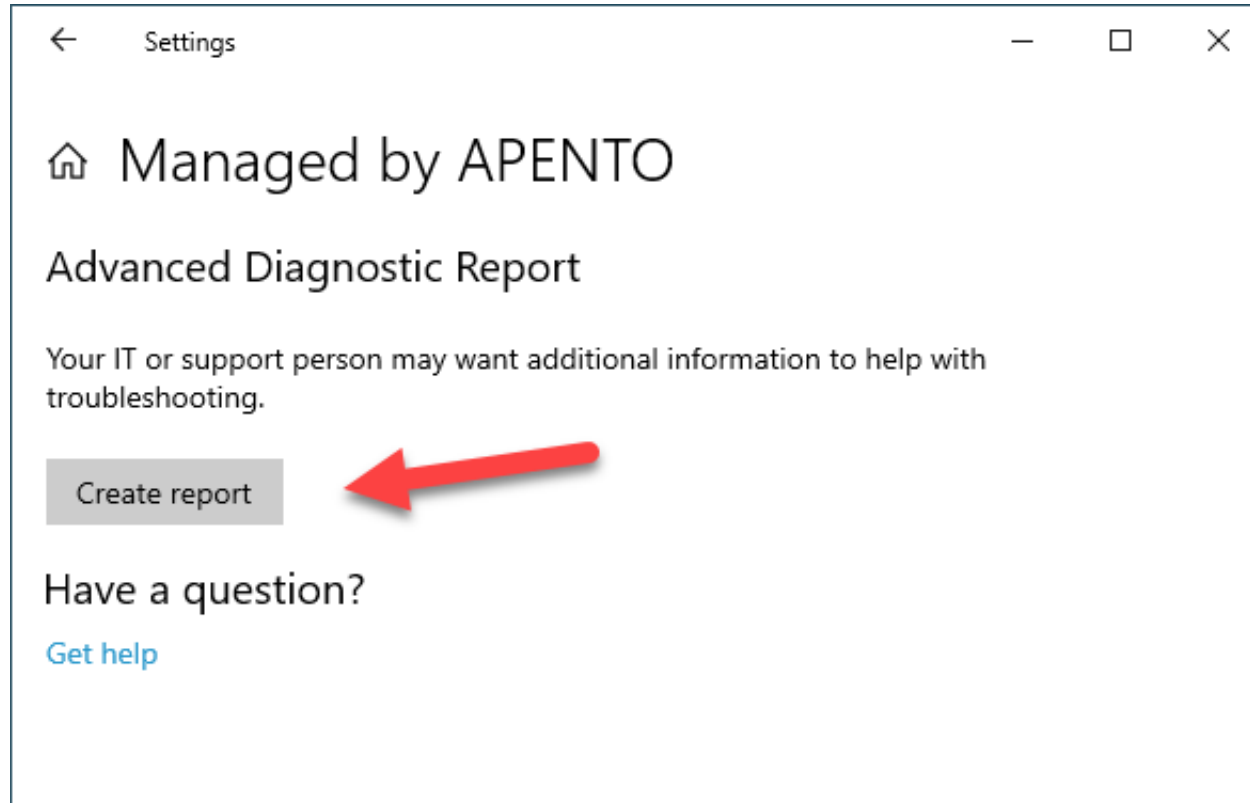
Policy/Profile Conflicts

- Compliance policy settings always have precedence over configuration profile settings.
- Compliance policy conflicts: The most restrictive compliance policy setting applies.
- Configuration Profile Conflicts: Shown in Intune.
 - Manually resolve these conflicts



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="EncryptionMethodWithXtsFdvDropDown_Name" value="7"/> <data id="EncryptionMethodWithXtsRdvDropDown_Name" value="7"/>
BitLocker	SystemDrivesRecoveryOptions			device		BF34185C-4364-40CF-A364-98DBD5B8ECB7= <enable d/> <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	NewCloudProtection	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>

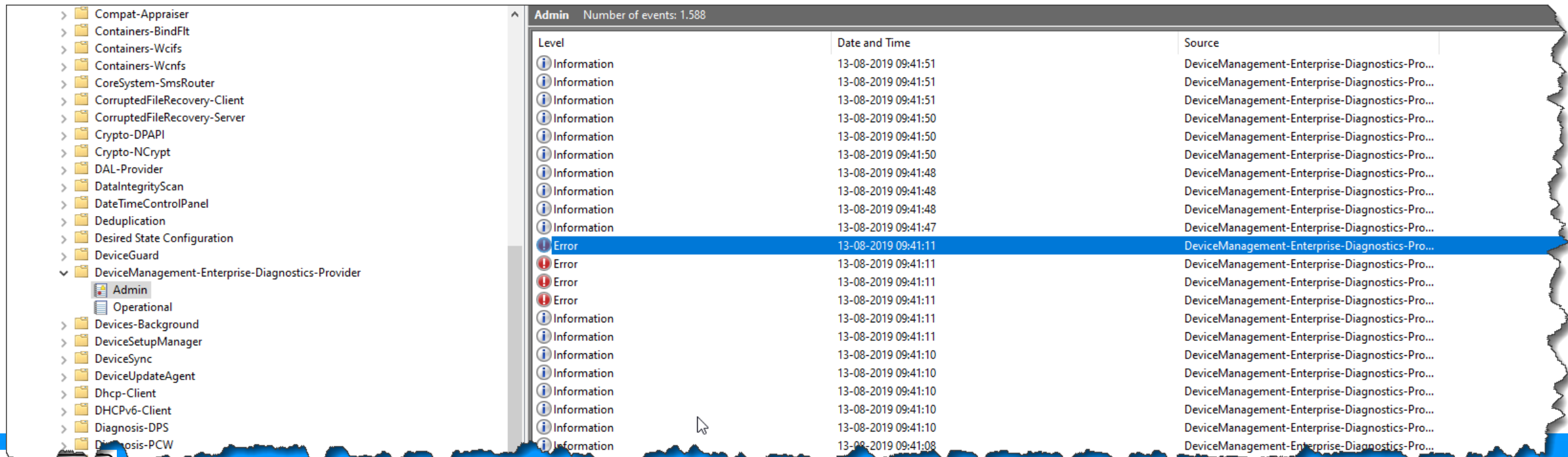
The screenshot shows the Microsoft Intune Troubleshooting interface for user Anna Anderson. The left sidebar contains a navigation menu with categories like Device compliance, Device configuration, Devices, Client apps, Device security, eBooks, Conditional access, Exchange access, Users, Groups, Roles, Software updates, Monitoring, Diagnostics settings, and Help and support. The 'Troubleshoot' option is selected. The main content area displays the user's account status as 'Active' and provides details for Anna Anderson, including a 'Change' button. Below this, there are sections for 'Intune license' (showing 99 non-compliant devices), 'GROUP MEMBERSHIP' (listing AutoPilot Users), 'ASSIGNMENTS' (a table of client app assignments), and 'DEVICES' (a table of enrolled devices).

ASSIGNME...	NAME	OS	TYPE	LAST M
Included	AutopilotBranding	Windows P...	required	4/20/...
Included	Chrome		required	3/10/...
Included	Office 365 ProPlus (cu...	Windows 10...	required	3/28/...
Included	paint.net		required	2/1/2...
Included	VPNSetup	Windows P...	required	11/27...

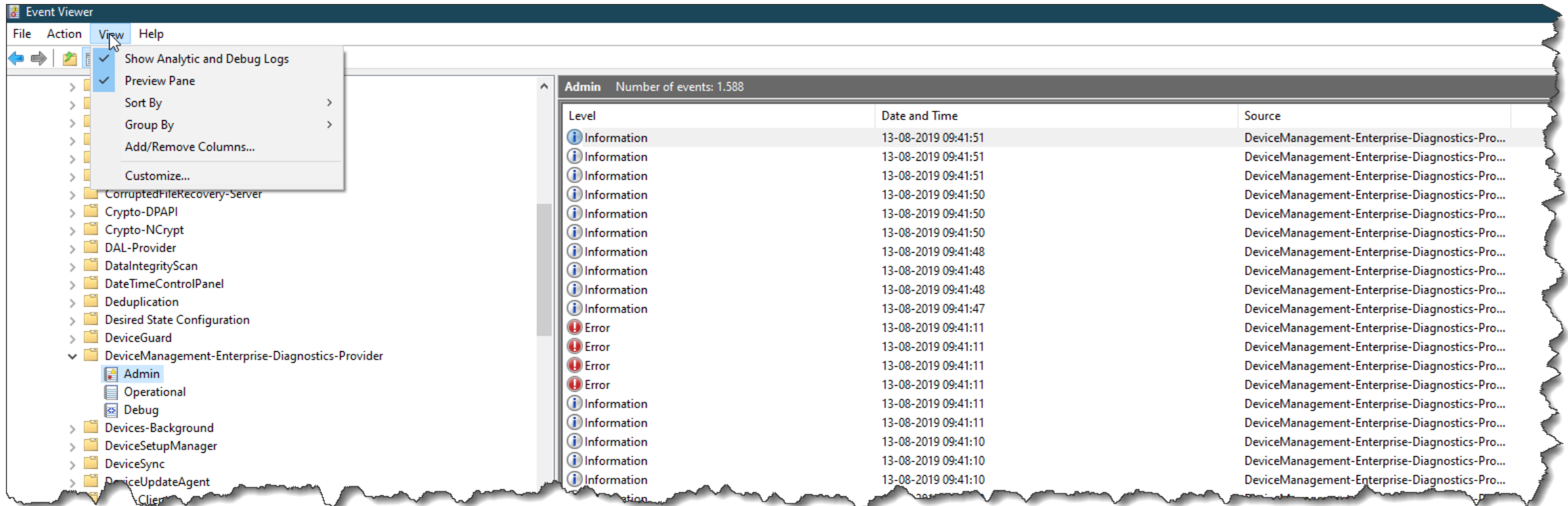
DEVIC...	...	A...	O...	INTU...	AZURE ...	A...	OS
AAD-573...	MDM	Not ...	Corp...	Yes	NA		Win...

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 Prerequisites

- Installed when first needed by Win32App or PowerShell script.
- Installed only on “Corporate” and “personal” devices (personal device context only, added in late 2020-but not supported?!...)

① Note

Once the Intune management extension prerequisites are met, the Intune management extension is installed automatically when a PowerShell script or Win32 app is assigned to the user or device. For more information, see [Intune Management Extensions prerequisites](#).

PowerShell scripts, which are not officially supported on Workplace join (WPJ) devices, can be deployed to WPJ devices. Specifically, device context PowerShell scripts work on WPJ devices, but user context PowerShell scripts are ignored by design. User context scripts will be ignored on WPJ devices and will not be reported to the Microsoft Endpoint Manager console.

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

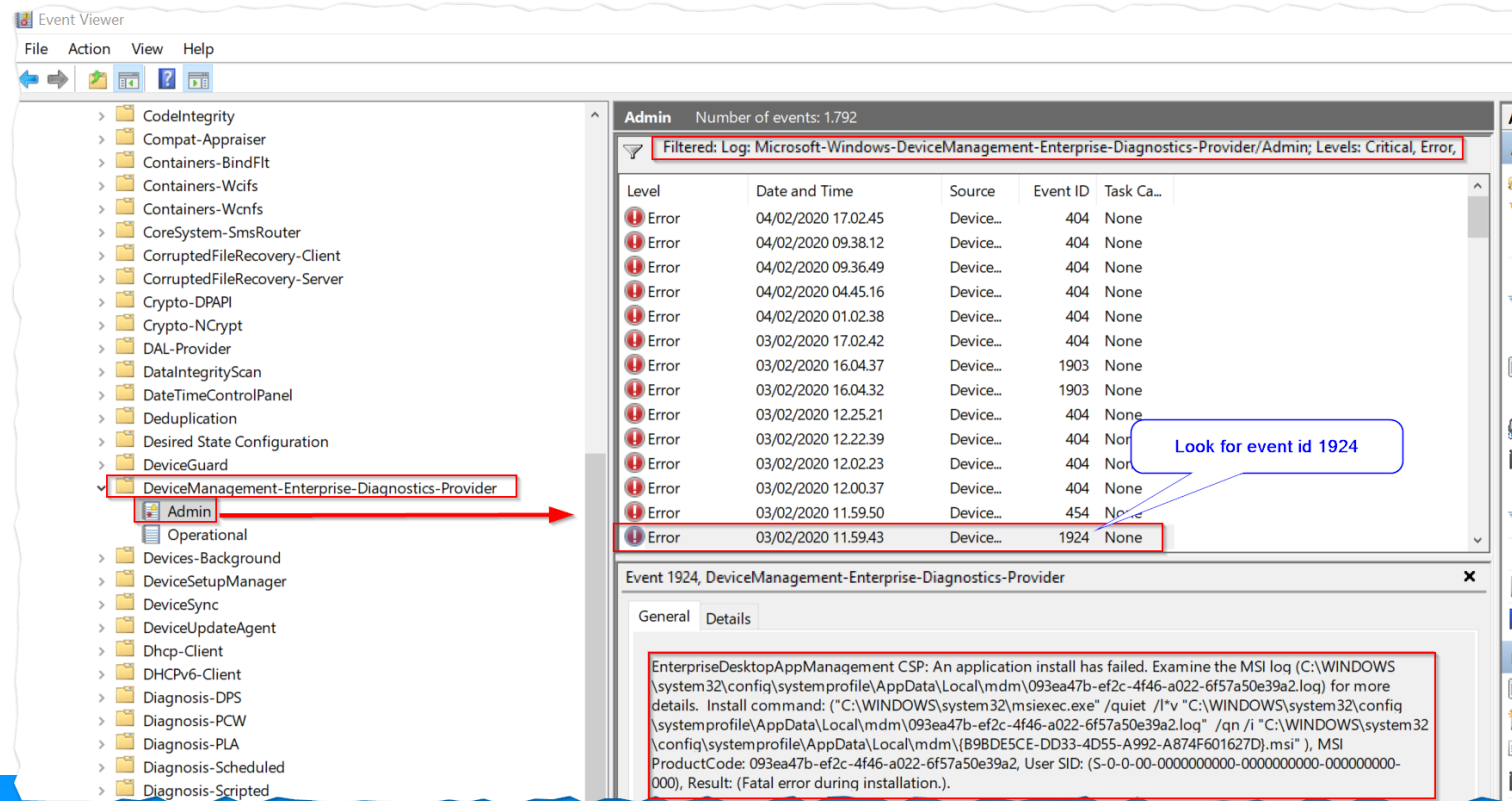
What is a Corporate Device?

- The enrolling user is using a device enrollment manager account.
- The device enrolls through Windows Autopilot.
- The device enrolls through a bulk provisioning package.
- The device enrolls through GPO
 - or automatic enrollment from SCCM for co-management.



Intune Management Extension Event log

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



Intune Management Extension File System

<< Local Disk (C:) > Program Files (x86) > Microsoft Intune Management Extension > Content >

Name	Date modified	Type	Size
DetectionScripts	8/16/2019 9:07 AM	File folder	
Incoming	5/29/2019 10:11 AM	File folder	
Staging	5/29/2019 10:11 AM	File folder	

Microsoft Intune Management Extension

File Home Share View

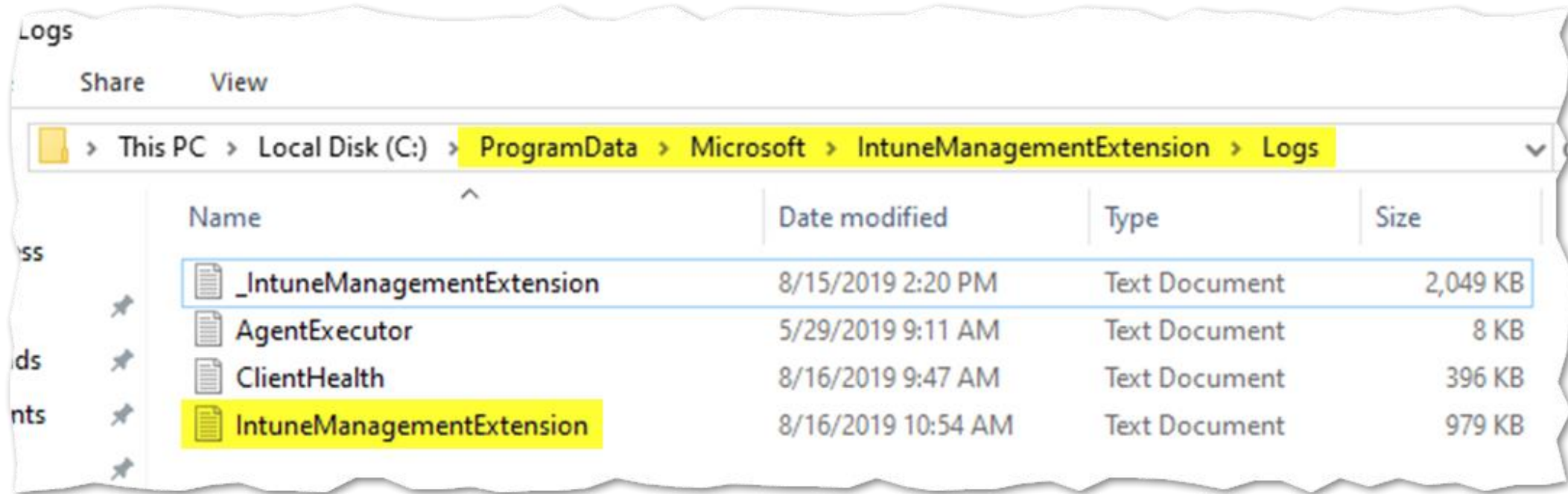
< > > This PC > Local Disk (C:) > Program Files (x86) > Microsoft Intune Management Extension >

Search Microsoft Intune Man...

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
concr140.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

Intune Management Extension Log files

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

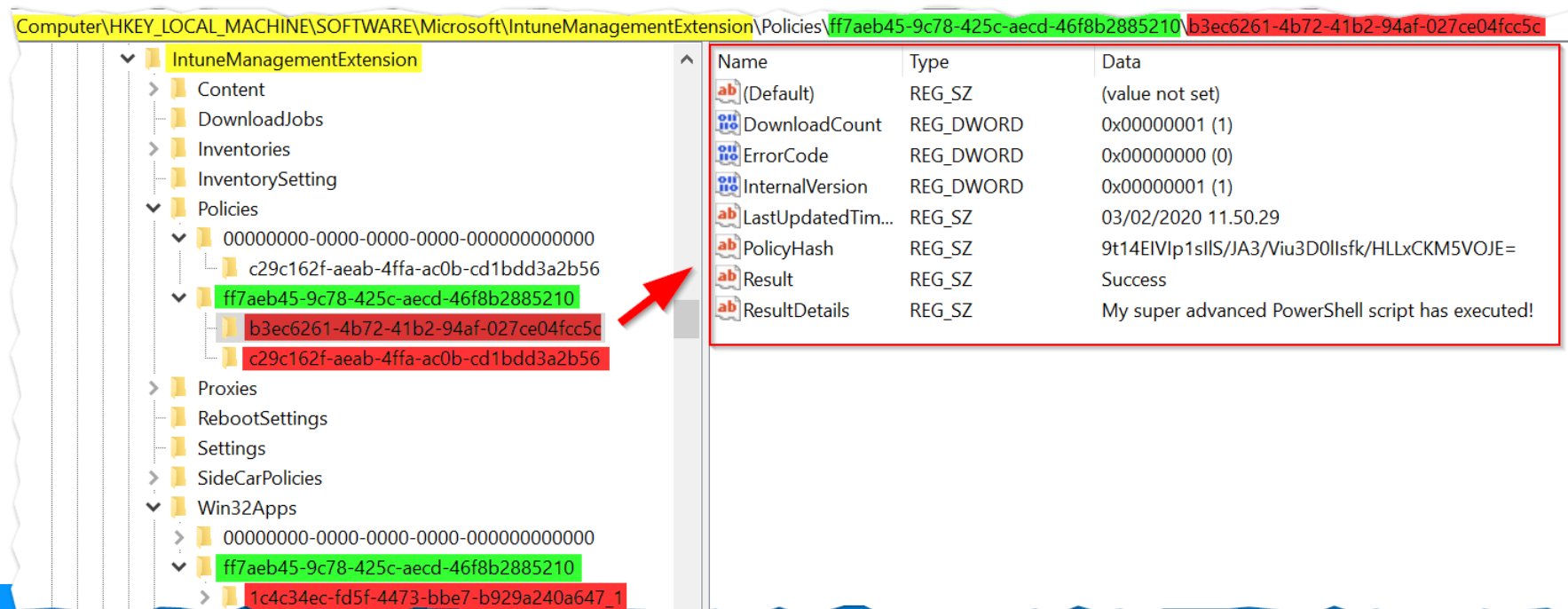


The screenshot shows a Windows File Explorer window titled 'Logs'. The address bar displays the path: This PC > Local Disk (C:) > ProgramData > Microsoft > IntuneManagementExtension > Logs. The main area shows a list of files with columns for Name, Date modified, Type, and Size. The file 'IntuneManagementExtension' is highlighted in yellow.

Name	Date modified	Type	Size
_IntuneManagementExtension	8/15/2019 2:20 PM	Text Document	2,049 KB
AgentExecutor	5/29/2019 9:11 AM	Text Document	8 KB
ClientHealth	8/16/2019 9:47 AM	Text Document	396 KB
IntuneManagementExtension	8/16/2019 10:54 AM	Text Document	979 KB

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>

