



May 31 – June 2, Oslo Spektrum

10th anniversary

# Troubleshooting the MEM Managed Windows Client



## 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](mailto: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](mailto:Jorgen.nilsson@onevinn.se)
- Twitter: [@ccmexec](https://twitter.com/ccmexec)



# Agenda

- Tools
- Troubleshooting Subscription based activation
- 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)

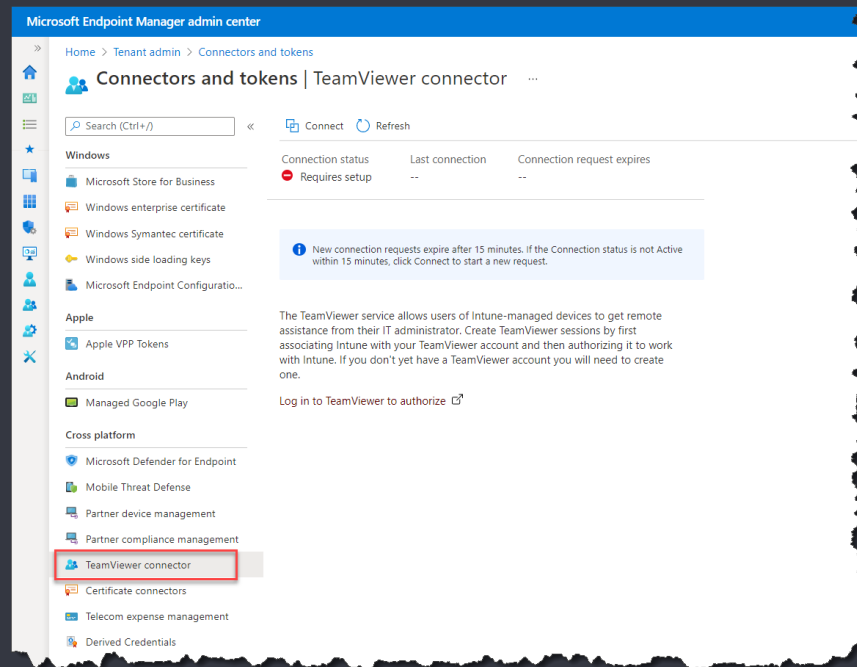


<https://oliverkieselbach.com/2020/03/03/quick-assist-the-built-in-remote-control-in-windows-10/>

# Configure the TeamViewer Connector

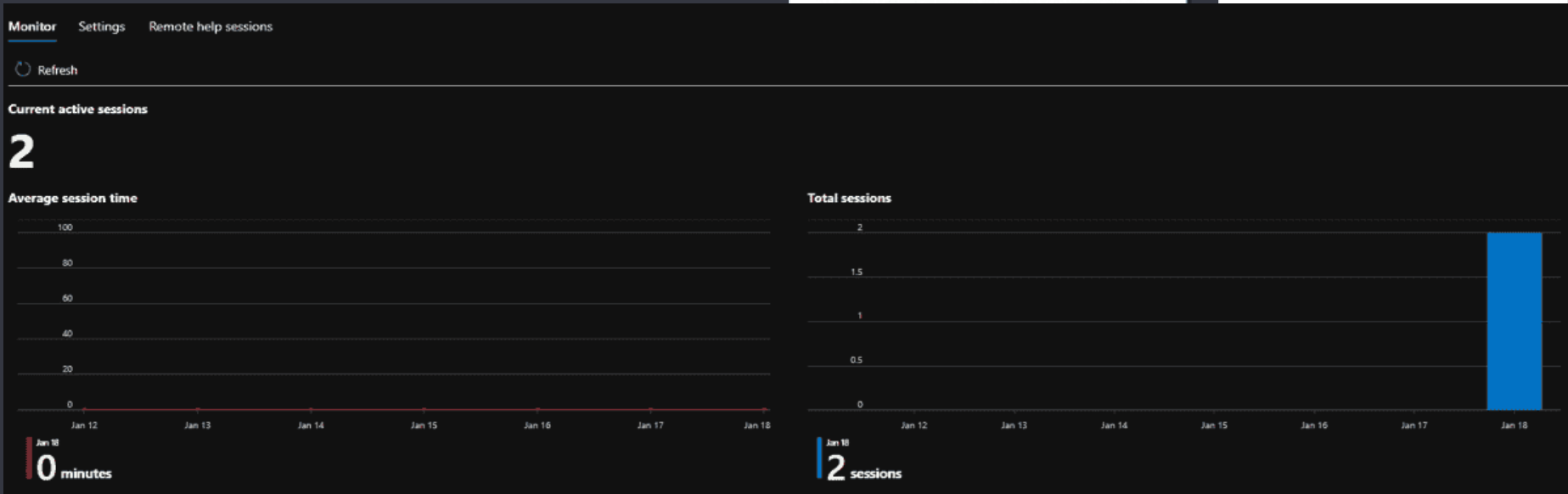
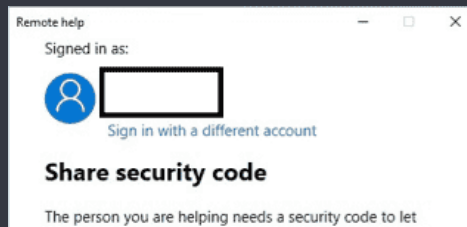
- Easy setup and configuration
- There are other options:
  - Beyond Trust
  - LogMeIn
  - Remote Help!

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



# Microsoft Remote Help

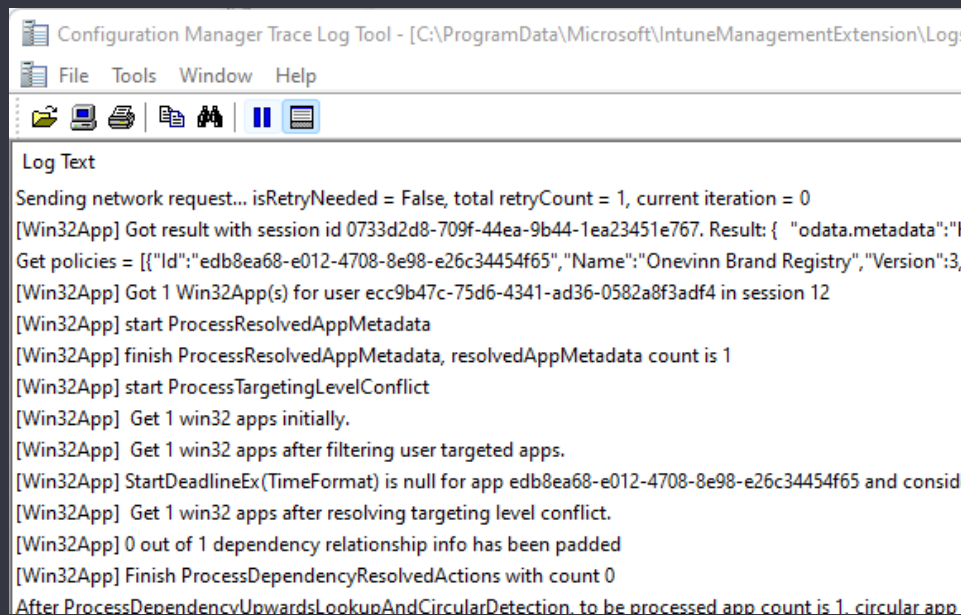
- Adv management pack add-on
- Auditing in the MEM portal





# CMtrace

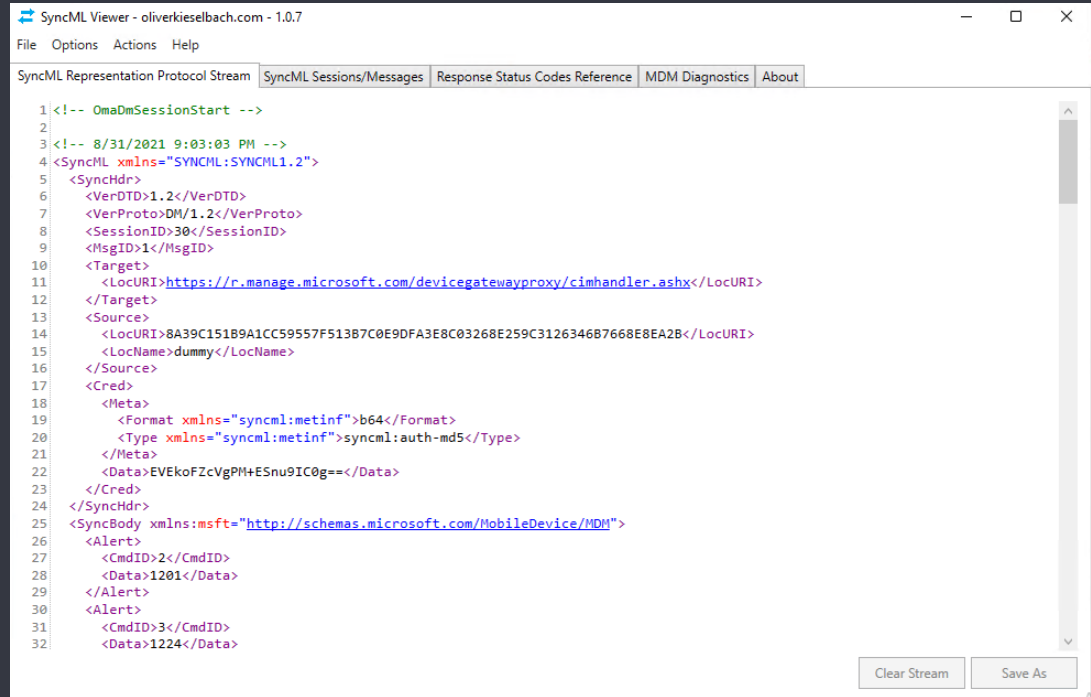
- Great log reader
- Not free but included in the Intune/MEM license
- Deploy it to all clients



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

# More Tools – Advanced Troubleshooting

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



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 main window has a tabbed interface with the following tabs: "SyncML Representation Protocol Stream", "SyncML Sessions/Messages", "Response Status Codes Reference", "MDM Diagnostics", and "About". The "SyncML Representation Protocol Stream" tab is active, displaying an XML stream of a SyncML session. The XML content is as follows:

```
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>8A39C151B9A1CC59557F513B7C0E9DFA3E8C03268E259C312634687668E8EA2B</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: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, there are two buttons: "Clear Stream" and "Save As".

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

```

1533 <Status>
1534   <CmdID>32</CmdID>
1535   <MsgRef>2</MsgRef>
1536   <CmdRef>25</CmdRef>
1537   <Cmd>Get</Cmd>
1538   <Data>200</Data>
1539 </Status>
1540 <Results>
1541   <CmdID>33</CmdID>
1542   <MsgRef>2</MsgRef>
1543   <CmdRef>25</CmdRef>
1544   <Item>
1545     <Source>
1546       <LocURI>./DevDetail/Ext/DeviceHardwareData</LocURI>
1547     </Source>
1548     <Data>T0EeBAEAAAAAAAAoAMwDwVQAACgAaAfBVCnofKQQCCQgCABAACQABAAEAAGABAAAABQAZAAQAAAAAAAAAagAAAAAAAACAAEAAwMAEQBHZW51aW51SW50ZWwABAA0AEIudGVsKFipIENvcmlUVE0pIGk3LTg1NTlV:
1549   </Item>
1550 </Results>
1551 <Status>
1552   <CmdID>34</CmdID>
1553   <MsgRef>2</MsgRef>
1554   <CmdRef>26</CmdRef>

```

```

<SyncML xmlns="SYNCHML:SYNCHML1.2" 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

Home > Windows >

**DESKTOP-NIIRT6B** ...

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

Overview

**Collect diagnostics: Completed**

**Manage**

- Properties

**Monitor**

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

**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	

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	<a href="#">Download</a>

# 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

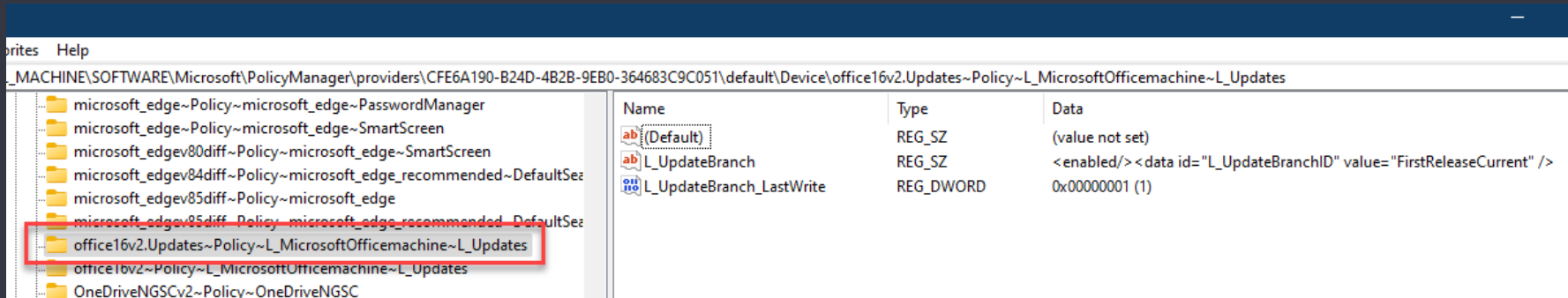
Enable Automatic Updates ⓘ ☒ Enabled ⌵

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.

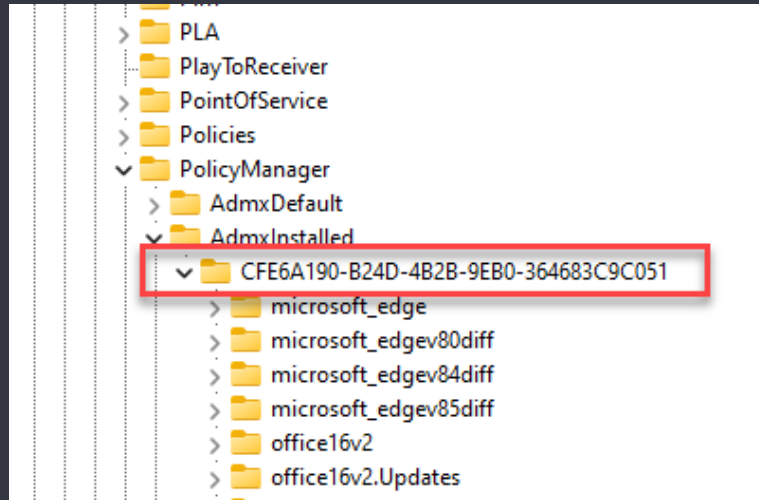


# Find the Provider ID

## Find the provider ID for your device

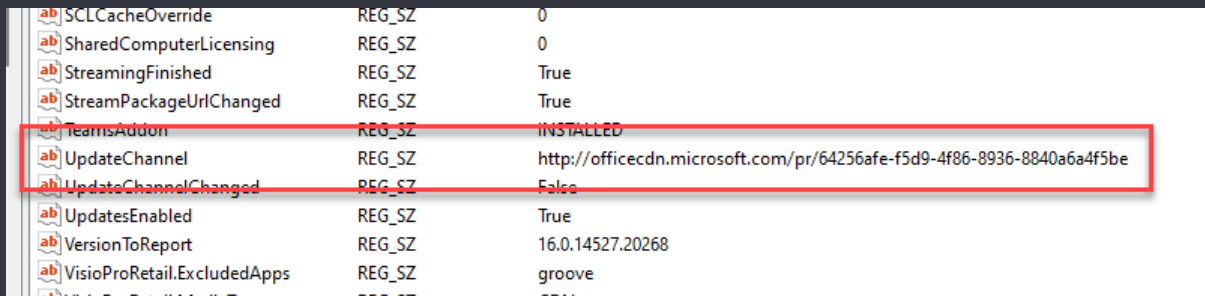
- Open the Registry Editor, and go to:

**Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\PolicyManager\AdmxInstalled**



## #2 Check the Office registry keys

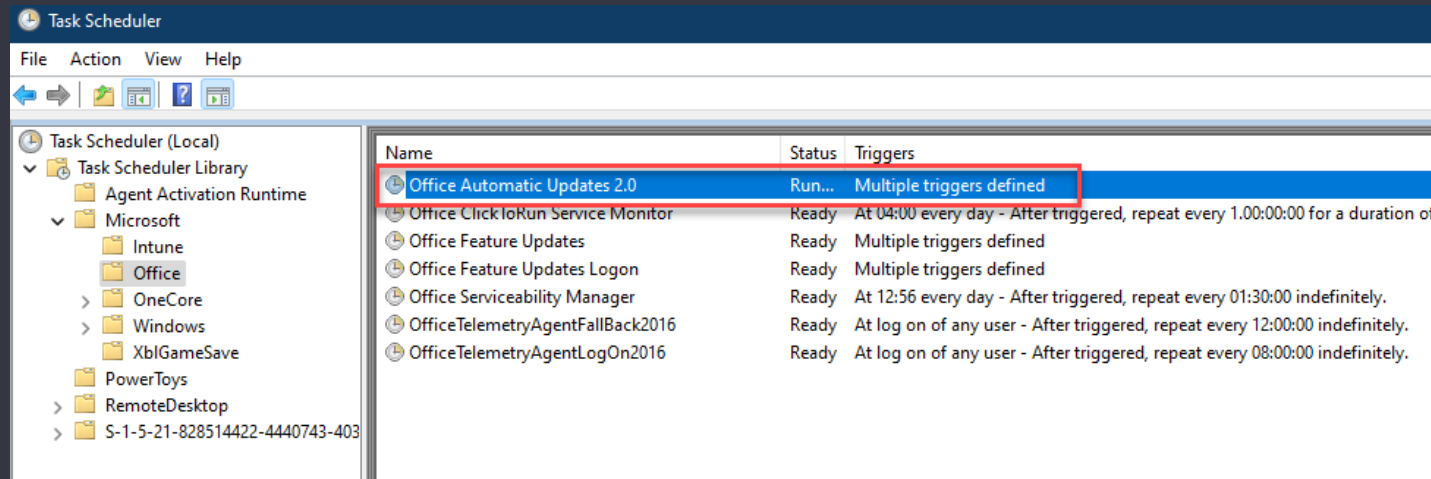
- Go to the Office policy path:  
**Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\Configuration**
- Check the **UpdateChannel** value:
  - Monthly Enterprise Channel = 55336b82-a18d-4dd6-b5f6-9e5095c314a6
  - Current Channel = 492350f6-3a01-4f97-b9c0-c7c6ddf67d60
  - Current Channel (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) 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**
  - Edit the **UpdateDetectionLastRunTime** key > delete the value data.
  - Launch Task Scheduler > Microsoft > Office
    - Run “**Office Automatic Updates 2.0**”

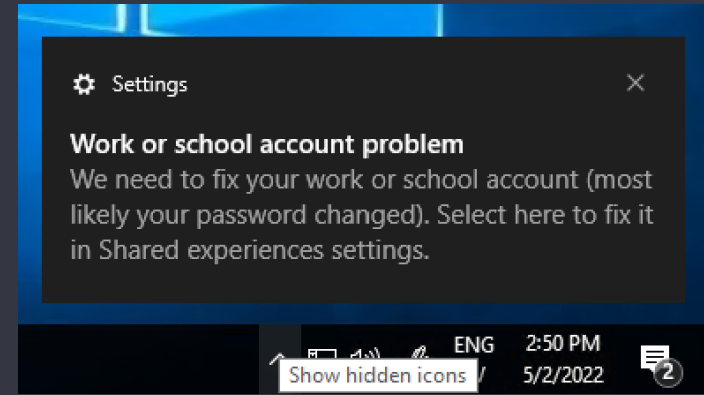


# Troubleshooting Subscription Based Activation



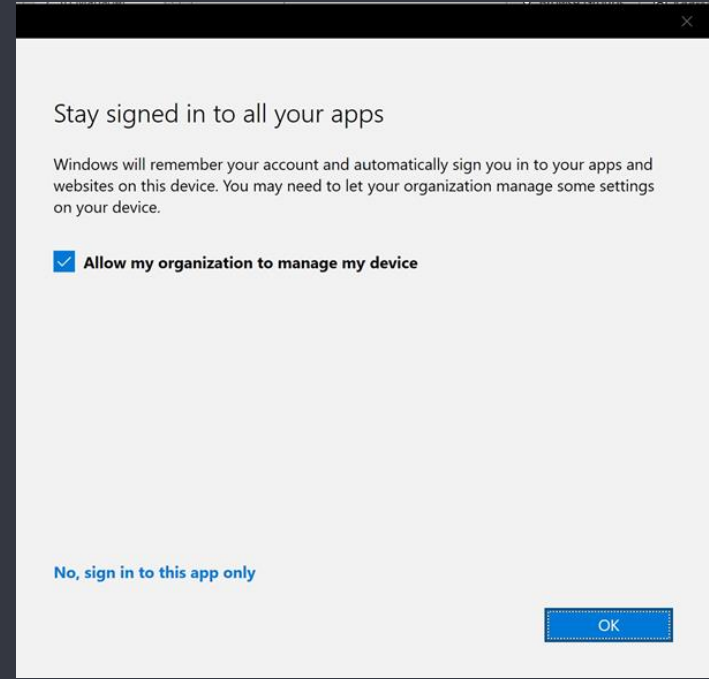
# Subscription based licensing

- 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, can cause this.



# Stay signed in to all your apps = Evil

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



# 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
Enable Windows Update	Enabled				Completed successfully. (0x0)
License Acquisition	Enabled				

## Windows

Edition Windows 10 Pro

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

Activation Windows is activated with a digital license

[Learn more](#)

Function: LogServiceFault  
Source: onecoreuap\enduser\winstore\licensemanager\lib\telemetry.cpp (134)

- The store  
• In “Work or School”

# 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

☒ Allow Workplace

File

Home

Send / Receive

View

Help

New Email

Unread/ Read

Search People

Favorites

Inbox259

Sent Items

Deleted Items

Jorgen@demiranda.nu

Inbox259

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

Right-click

Your free Power BI Pro trial su  
expires soon

We hope you've enjoyed the advantages of Power BI  
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%

Windows Start Menu

Type here to search

Taskbar

System Tray

# Subscription Based Activation

- Store Event Log + Schedule Task

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
EnableLicenseAcquisition	Ready	Multiple triggers defined		2021-09-29 07:34:23	The operation completed successfully. (0x0)
LicenseAcquisition	Ready	Multiple triggers defined	2021-09-30 04:44:30	2021-09-29 07:34:30	(0x87E10BF2)

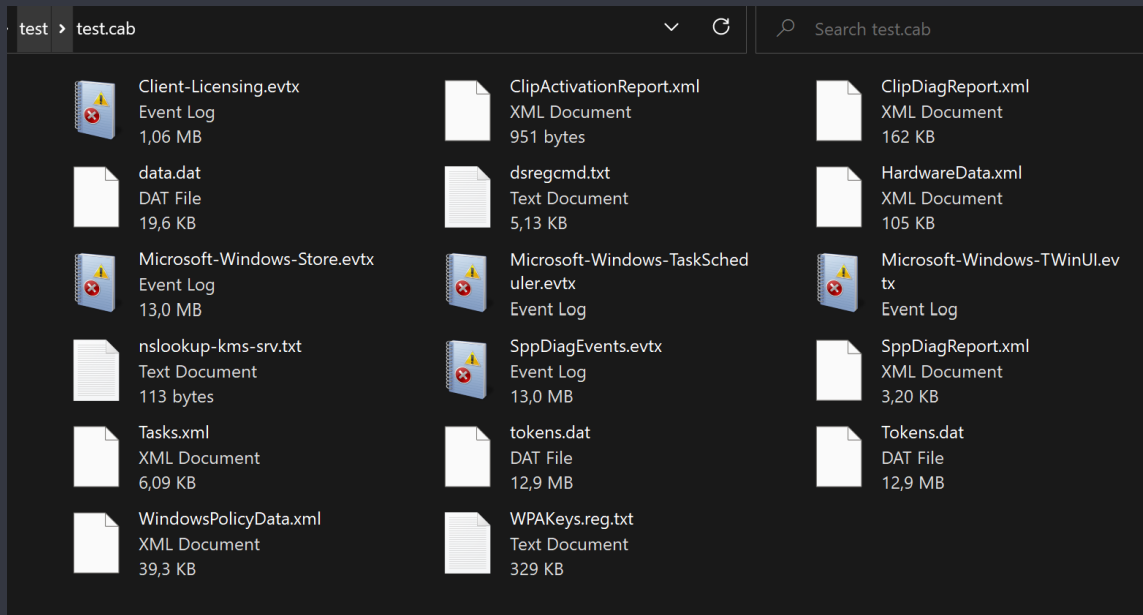
General Details

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

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

# Collecting information

- `licensingdiag -cab c:\test\test.cab`
- Collects all registry entries and event logs related to licensing



# Enrollment



# Troubleshooting Windows enrollment

- Valid License assigned to the user?
- Is the user allowed to enroll a device?
- Network issues, proxy etc.?
- Enrollment restrictions that blocks enrollment?
- Number of devices already enrolled (Device Limit)
- MDM Terms of use not correct

# Hybrid Azure AD Join

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

<https://www.imab.dk/auto-mdm-enrollment-fails-with-error-code-0x8018002a-troubleshooting-mdm-enrollment-errors-co-management-with-sccm-and-intune/>

# Co-Managed device enrollment

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

Enrolling device to MDM... Try #1 out of 3

Enrolling device with RegisterDeviceWithManagementUsingAADDeviceCredentials

Processing GET for assignment (Scopeld\_B54C7DB5-E99F-4BC7-95DD-C383A9E555A9/ConfigurationPolicy\_96925c8d-7753-4899-a44c-79f6...

Getting/Merging value for setting 'CoManagementSettings\_AutoEnroll'

Merged value for setting 'CoManagementSettings\_AutoEnroll' is 'true'

Getting/Merging value for setting 'CoManagementSettings\_Allow'

Merged value for setting 'CoManagementSettings\_Allow' is 'true'

**Date/Time:** 2022-05-09 22:22:08      **Component:** CoManagementHandler

**Thread:** 12896 (0x3260)      **Source:** mdmreglib.cpp:164

Enrolling device with RegisterDeviceWithManagementUsingAADDeviceCredentials

# Enrollment restrictions and “All Users”

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

Home > Devices > Enroll devices >

**All Users** ...

Search (Ctrl+J) << ^ Essentials

Overview

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

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

Platforms configured : 6

Assigned to : **All devices.**

Manage

Properties

New merged workloadflags value with co-management max capabilities '16383' is '3'

Failed to enroll with RegisterDeviceWithManagementUsingAADDeviceCredentials with error code 0x80180014.

MDM enrollment failed with error code 0x80180014 'Specific platform or version is not supported'. Will retry in 240 minut...

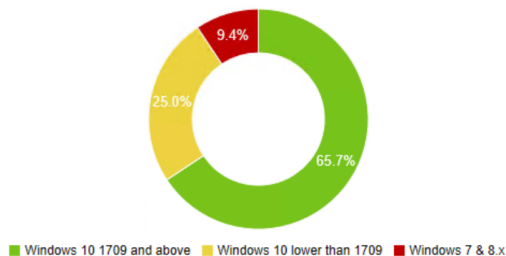
Could not check enrollment url, 0x00000001:

# Co-Management Enrollment Status

- Console page
- Co-managementhandler.log on the client

## Co-management

Client OS Distribution



Co-management Status

Eligible devices

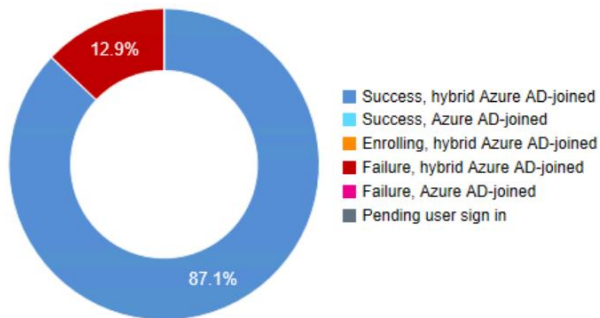
Scheduled

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

# 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-

ML edition

# DeviceCapReached = Device Limits

## Something went wrong.

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

### Additional problem information:

Server error code: 801c0003

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

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

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

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

# Client Health

- How do you verify that a client is working as expected ?
- Co-management to the rescue!
- In Intune we can now see:
- Configuration Manager agent state
- Last Configuration Manager agent check in time
- Intune-enrolled devices connect to the cloud service 3 times a day, approximately every 8 hours.



Search (Ctrl+ /)

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Recovery keys

Managed Apps

RetireWipeDeleteRemote lockSyncReset passcodeRestartFresh StartAutopilot ResetQuick 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 : ---

See more

Primary User : Ronni Pedersen

Enrolled by : Ronni Pedersen

Compliance : Not Compliant

Operating system : Windows

Device model : Virtual Machine

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 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

**NIC** X edition

# 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 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
            - 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 40:00:00:00.
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

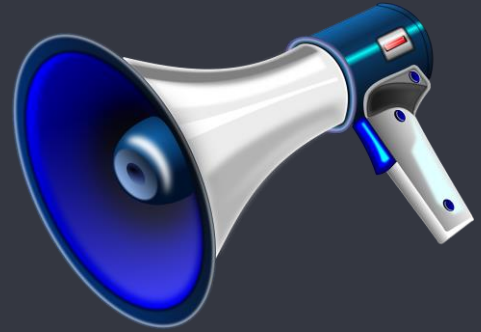
General Triggers Actions Conditions Settings History (disabled)

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

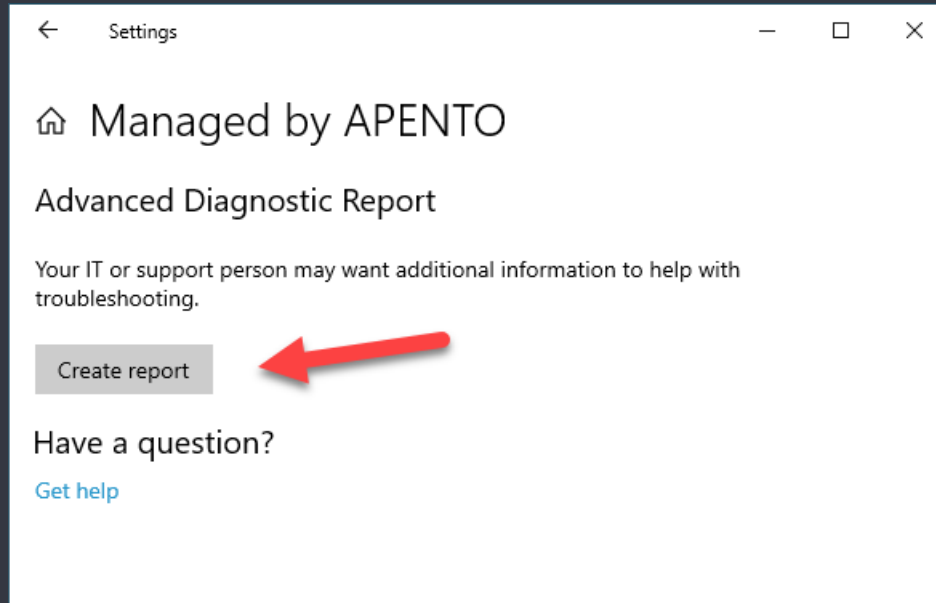
- Compliance policy settings always have precedence over configuration profile settings.
- Compliance policy conflicts: The most restrictive compliance policy setting applies.
- Conflict is shown in Intune. Manually resolve these conflicts.
- Some conflicts are shown as error depending on setting type.





# 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-A364-98DBD588ECB7=1
BitLocker	EncryptionMethodByDriveType			device		BF34185C-4364-40CF-A364-98DBD588ECB7=<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-A364-98DBD588ECB7=<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-A364-98DBD588ECB7=1
Defender	AllowArchiveScanning	1		device		BF34185C-4364-40CF-A364-98DBD588ECB7=1
Defender	RealTimeScanDirection	0		device		BF34185C-4364-40CF-A364-98DBD588ECB7=1
Defender	AllowEmailScanning	0		device		BF34185C-4364-40CF-A364-98DBD588ECB7=1
Defender	AllowOnAccessProtection	1		device		BF34185C-4364-40CF-A364-98DBD588ECB7=1
Defender	AllowIntrusionPreventionSystem	1		device		BF34185C-4364-40CF-A364-98DBD588ECB7=1
Defender	PUAProtection	0		device		BF34185C-4364-40CF-A364-98DBD588ECB7=2
Defender	AVGCPULoadFactor	50		device		BF34185C-4364-40CF-A364-98DBD588ECB7=50
Defender	AllowClearProtection	1		device		BF34185C-4364-40CF-A364-98DBD588ECB7=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 Intune Troubleshooting Pane for user Ronni Pedersen. The page is titled "Troubleshooting + support | Troubleshoot" and includes a "Change user" button. The user's display name is Ronni Pedersen, principal name is rop@apento.com, and email is rop@apento.com. The Intune license status is "Intune license" (green checkmark), and there are "2 devices noncompliant" (red X). The group memberships are 16, with a "Show all" link.

**Assignments**

Client apps

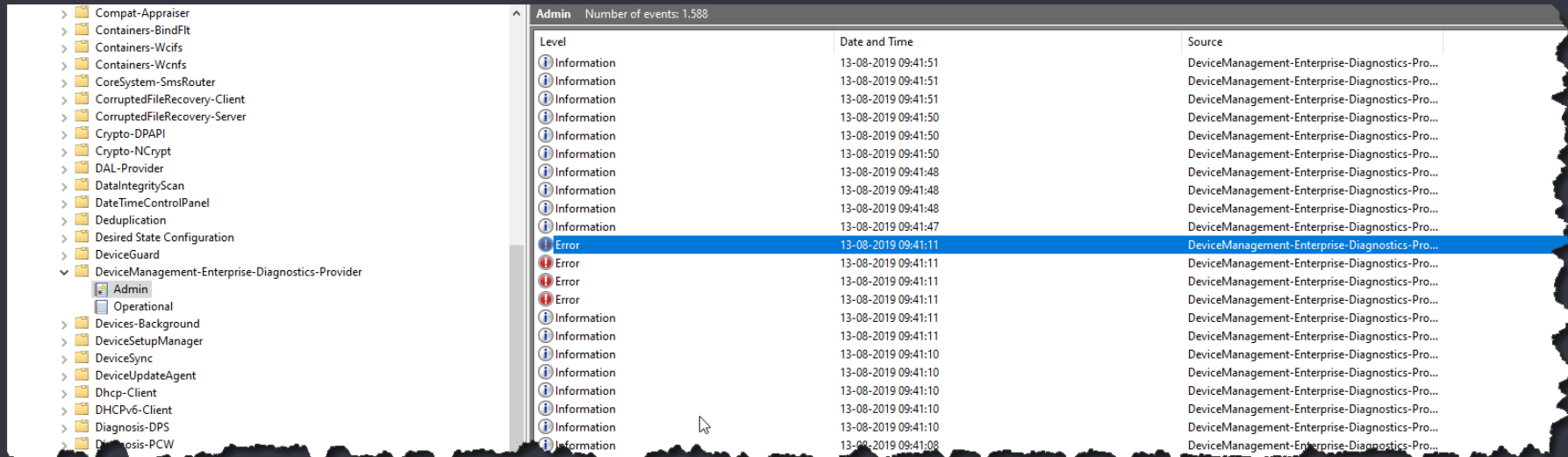
Assignment	↑↓	Name	↑↓	OS	↑↓	Type	↑↓	Last sync
Included		7-Zip 21.07 (MSI-x64)		Windows 10 and later		Available		3/8
Included		Adobe Acrobat Reader DC 22.001.20117		Windows 10 and later		Available		4/3
Included		Amazon WorkSpaces 4.0.6.2415 (x64)		Windows 10 and later		Available		3/8
Included		Camtasia 2021 21.0.19.35860 (MSI-x64)		Windows 10 and later		Available		5/1
Included		Company Portal		Windows 10 and later		Required		8/1

**Devices**

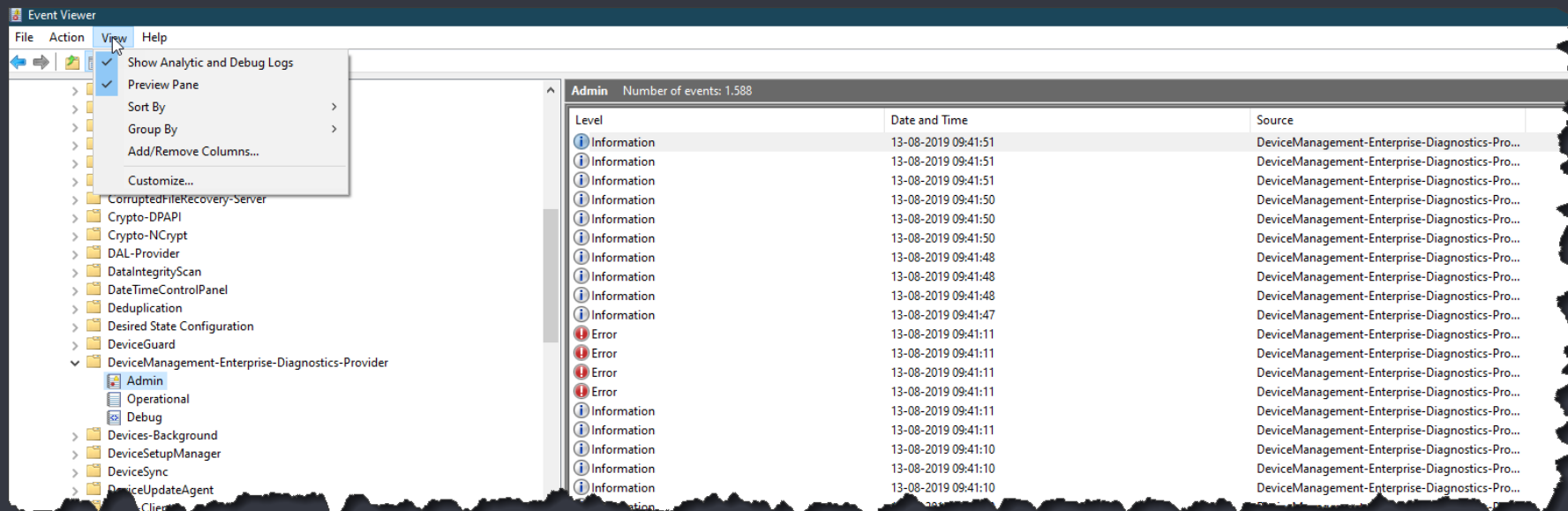
Device name	↑↓	Managed by	↑↓	Azure AD join ty...↑↓	Ownership	↑↓	Intune compliant ↑↓	Azure AD compl...↑↓	App install li...
CPC-rop-GUZ4-FB		Intune		AzureAD	Corporate		✔ Yes	✔ Yes	✔ success
DESKTOP-75BMIDA		Intune		AzureAD	Corporate		❌ No	❌ No	✔ success
DESKTOP-NIIRT68		Intune		AzureAD	Corporate		✔ Yes	✔ Yes	🔄 pending
RonniP's iPhone 13 Pro Max		Intune		Workplace	Personal		❌ No	❌ No	✔ success
APENTO-6452		Intune		AzureAD	Corporate		✔ Yes	✔ Yes	✔ success
DESKTOP-44C8EVL		Intune		AzureAD	Corporate		✔ Yes	✔ Yes	✔ success
TABLET-HR0R49UN		Intune		AzureAD	Corporate		✔ Yes	✔ Yes	✔ success

# 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

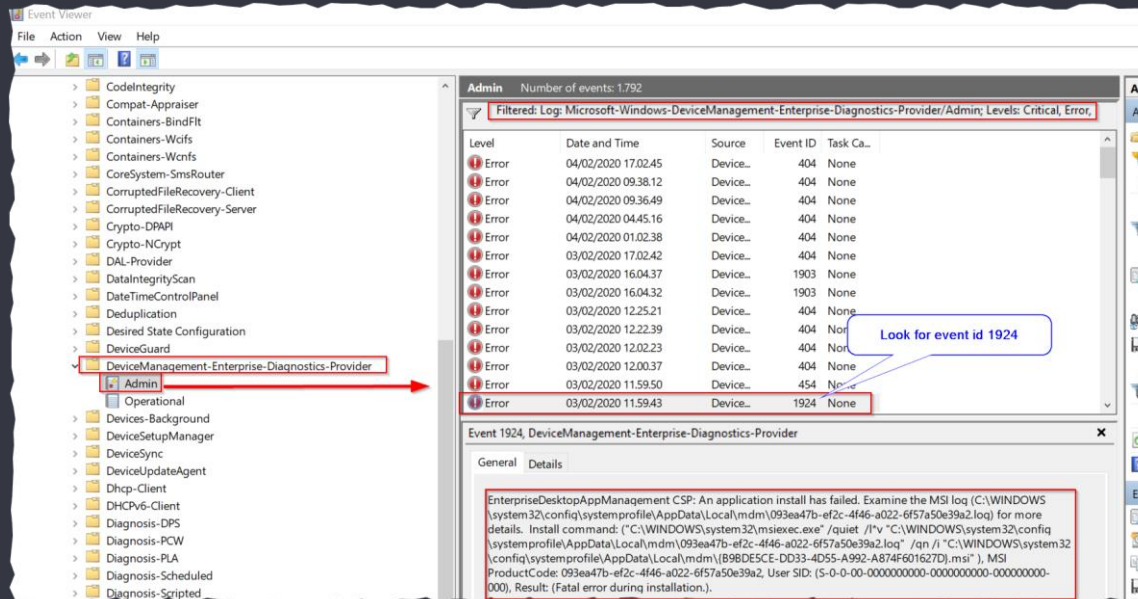
# Intune Management Extension

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



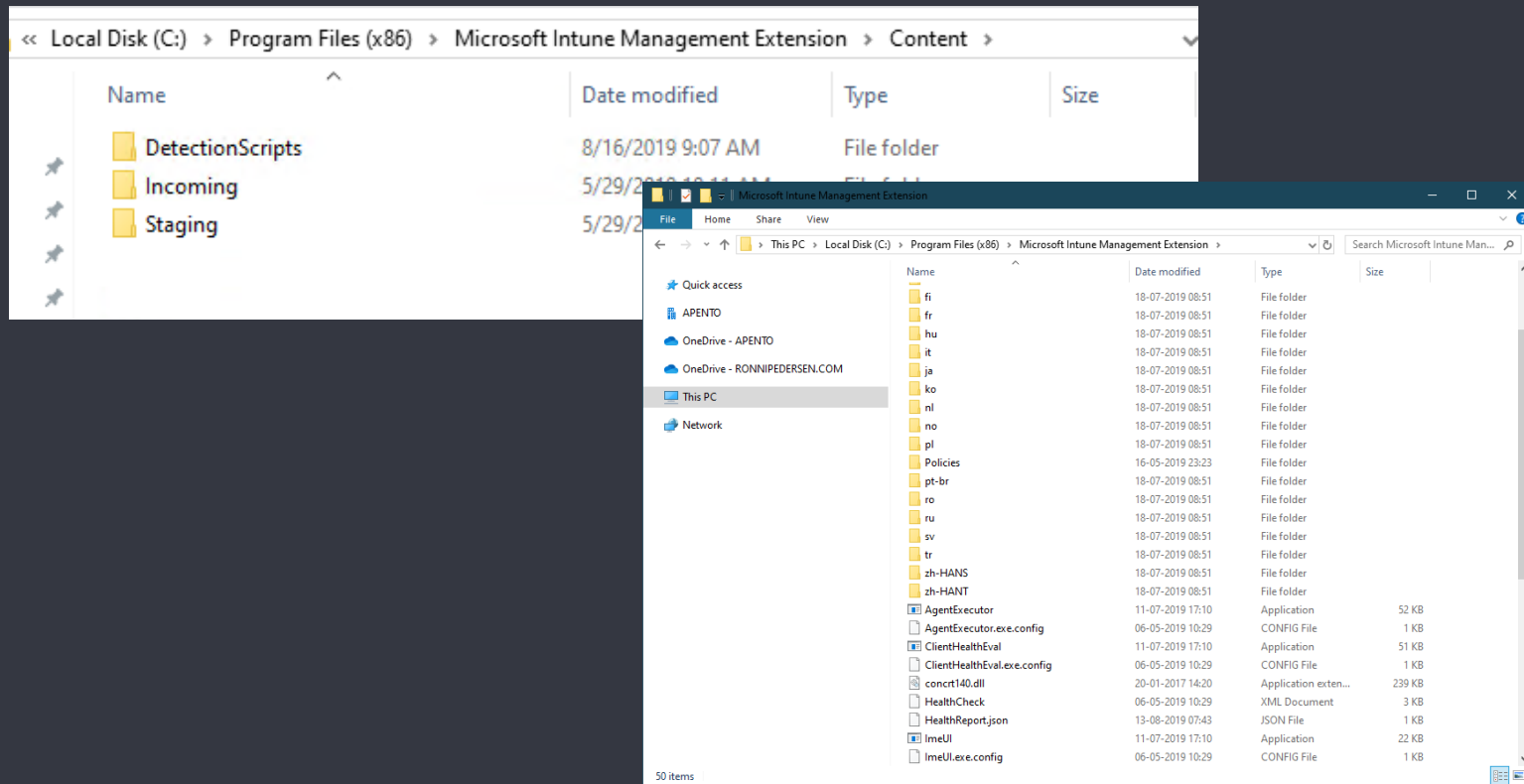
# Intune Management Extension Event log

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



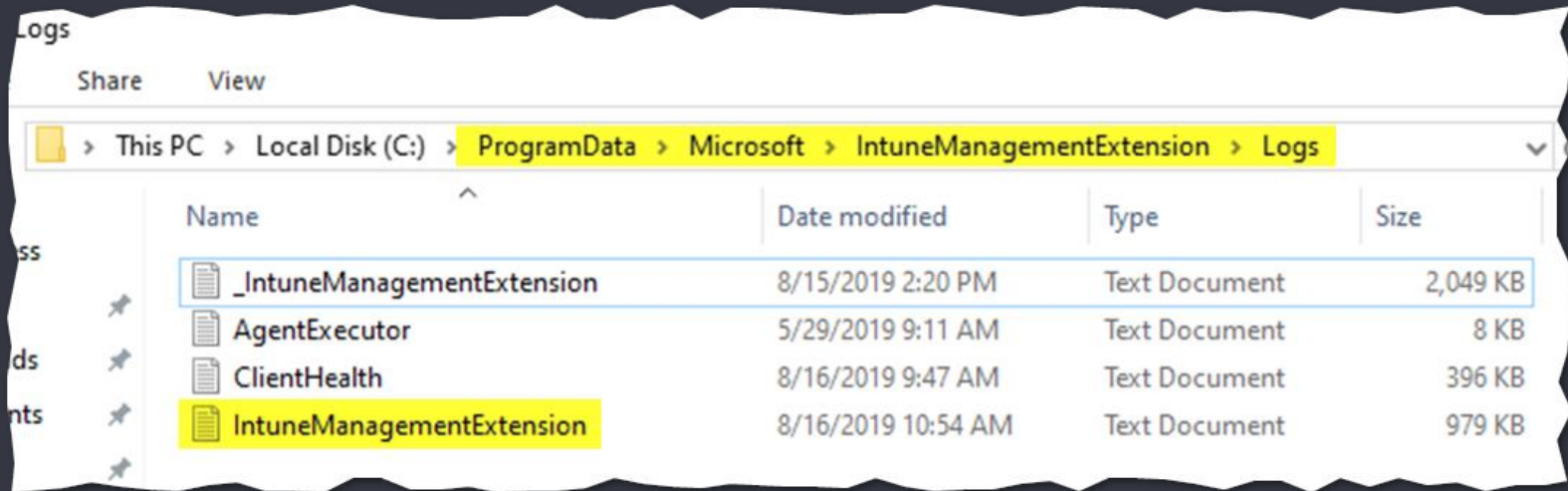


# Intune Management Extension File System



# 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

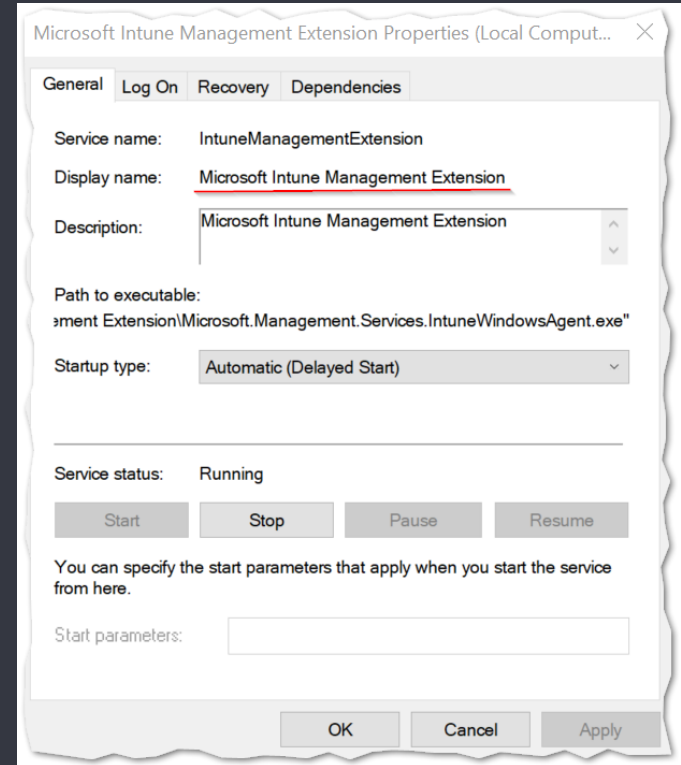
Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\Policies\ff7aeb45-9c78-425c-aecd-46f8b2885210\b3ec6261-4b72-41b2-94af-027ce04fcc5c

Name	Type	Data
(Default)	REG_SZ	(value not set)
DownloadCount	REG_DWORD	0x00000001 (1)
ErrorCode	REG_DWORD	0x00000000 (0)
InternalVersion	REG_DWORD	0x00000001 (1)
LastUpdatedTim...	REG_SZ	03/02/2020 11.50.29
PolicyHash	REG_SZ	9t14EIVip1sILS/JA3/Viu3D0llsfk/HLLxCKM5VOJE=
Result	REG_SZ	Success
ResultDetails	REG_SZ	My super advanced PowerShell script has executed!

# Intune Management Extension

- Troubleshooting
  - Check that the service is installed and running
  - Verify deployment in MDMDiagReport.html
  - Are you meeting the Prerequisites?

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



# Win32 Apps

# TIP #1

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

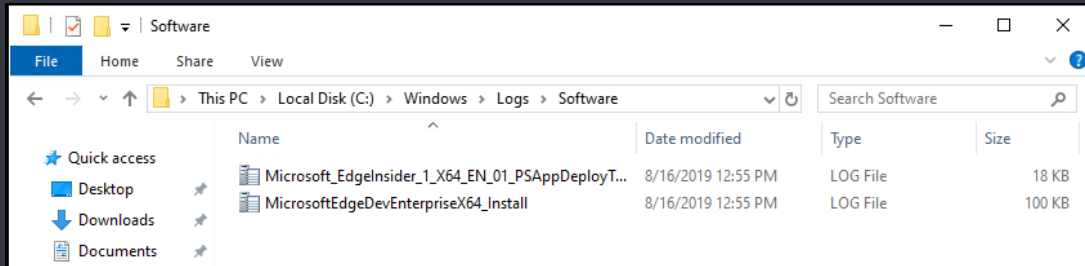


# PowerShell App Deployment Toolkit

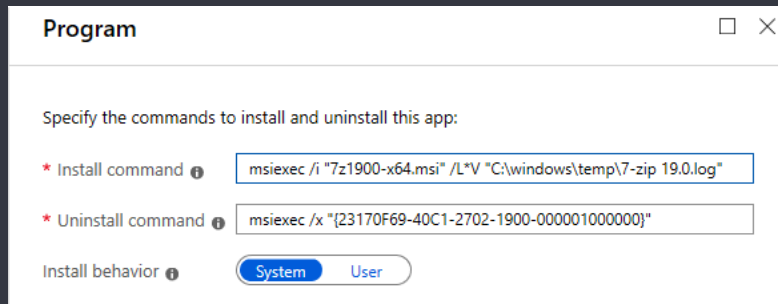
- **Easy To Use** – Any PowerShell beginner can use the template!
- **Consistent** – Consistent look and feel for all application deployments.
- **Powerful** – install/uninstall, setting registry keys, copying files, etc.
- **User Interface** – Custom dialogs boxes, progress dialogs and balloon tips.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

# Use the tools you know

- PS App Deployment Toolkit logging example:



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

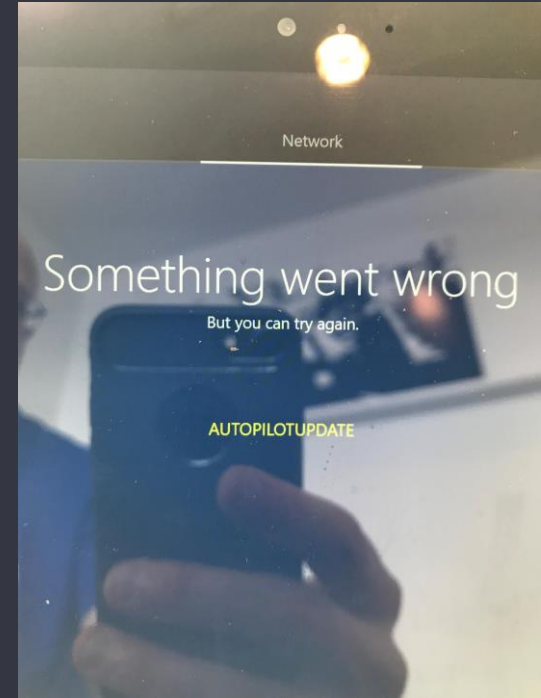




# Windows AutoPilot

# Network

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



# 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”.

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

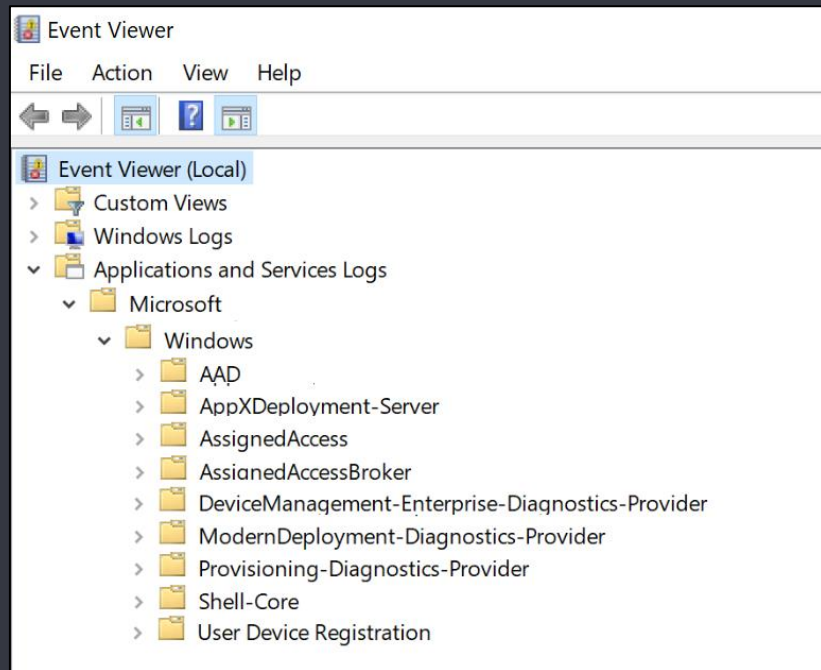
# Shift+F10















































- Great for troubleshooting
  - Can be a security concern for some customers
- Disable by placing **DisableCMDRequest.TAG** in the **C:\Windows\Setup\Scripts** folder.
  - Needs to be there when the computer starts up. Must be added by OEM.

# Troubleshooting

# Troubleshooting

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



 _IntuneManagementExtension.log Text Document	 AgentExecutor.log Text Document 762 KB	 AgentExecutor-20220303-074439.log Text Document	 CertReq_enrollaik_Output.txt Text Document 3,59 KB
 CertUtil_tpmInfo_Output.txt Text Document 9,54 KB	 ClientHealth.log Text Document 1,90 MB	 DeviceHash_JORGEN-X1X.csv Microsoft Excel Comma Sepa... 3,96 KB	 DiagnosticLogCSP_Collector_A utopilot_2022_5_2_20_41_45.etl ETL File
 DiagnosticLogCSP_Collector_A utopilot_2022_5_17_11_17_29... ETL File	 DiagnosticLogCSP_Collector_A utopilot_2022_5_20_7_41_13.etl ETL File	 DiagnosticLogCSP_Collector_A utopilot_2022_6_2_11_4_15.etl ETL File	 DiagnosticLogCSP_Collector_D eviceProvisioning_2022_5_18_... ETL File
 DiagnosticLogCSP_Collector_D eviceProvisioning_2022_5_23_... ETL File	 DiagnosticLogCSP_Collector_D eviceProvisioning_2022_5_29_... ETL File	 DiagnosticLogCSP_Collector_D eviceProvisioning_2022_5_31_... ETL File	 DiagnosticsFrameworkData.js on JSON File
 IntuneManagementExtension.l og Text Document	 IntuneManagementExtension- 20220524-091719.log Text Document	 IntuneManagementExtension- 20220601-102737.log Text Document	 LicensingDiag.cab
 LicensingDiag_Output.txt Text Document 900 bytes	 MdmDiagLogMetadata.json JSON File 95 bytes	 MdmDiagReport_RegistryDum p.reg Registration Entries	 MdmLogCollectorFootPrint.txt Text Document 8,87 KB
 microsoft-windows-aad-operat ional.evtx Event Log	 microsoft-windows-appxdepl oymentsserver-operational.evtx Event Log	 microsoft-windows-assignedac cess-admin.evtx Event Log	 microsoft-windows-assignedac cessbroker-admin.evtx Event Log
 microsoft-windows-assignedac cessbroker-operational.evtx Event Log	 microsoft-windows-assignedac cess-operational.evtx Event Log	 microsoft-windows-crypto-ncr ypt-operational.evtx Event Log	 microsoft-windows-deviceman agement-enterprise-diagnost... Event Log
 microsoft-windows-deviceman agement-enterprise-diagnost... Event Log	 microsoft-windows-deviceman agement-enterprise-diagnost... Event Log	 microsoft-windows-deviceman agement-enterprise-diagnost... Event Log	 microsoft-windows-modernde ployment-diagnostics-provid... Event Log
 microsoft-windows-modernde ployment-diagnostics-provid... Event Log	 microsoft-windows-modernde ployment-diagnostics-provid... Event Log	 microsoft-windows-provisionin g-diagnostics-provider-admi... Event Log	 microsoft-windows-shell-core- operational.evtx Event Log
 microsoft-windows-user device_registration-admin.evtx Event Log	 Sensor.log Text Document 30,3 KB	 Sensor-20220601-125219.log Text Document 3,00 MB	 Sensor-20220602-110322.log Text Document 3,00 MB
 setupact.log Text Document 81,1 KB	 TpmHllInfo_Output.txt Text Document 212 bytes		

## Setting up for work or school

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



### Device preparation ▼

✔ Completed

### Device setup ▲

● Error

Security policies (1 of 1 applied)

Certificates (1 of 1 applied)

Network connections (No setup needed)

Apps (0x81036502)

### Account setup ▼

Waiting

For more details, [view diagnostics](#).

[Continue anyway](#)

[Reset device](#)

[Try again](#)



## Windows Autopilot diagnostics



Policy Provider Installation



Device-Targeted Apps Installation



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

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

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



Device-Targeted Policies Installation



Device-Targeted Network Profiles Installation



Device-Targeted Certificates Installation



User-Targeted Apps Installation



Close

Export logs

Thank you!

Slides and demos from the conference will be available at

**<https://github.com/nordicinfrastructureconference/2022>**