



TECH EVENTS WITH PERSPECTIVE

Visual Studio **LIVE!**
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

SQL Server **LIVE!**
TRAINING FOR DBAs AND IT PROS

TECHMENTOR
IN-DEPTH TRAINING FOR IT PROS

Artificial
Intelligence **LIVE!**
AI FOR DEVELOPERS AND DATA SCIENTISTS

Cloud &
Containers **LIVE!**
CLOUD-NATIVE, PaaS & SERVERLESS COMPUTING

Troubleshooting the Intune Managed Windows Client

Jörgen Nilsson
Principal Consultant
Onevinn

Ronni Pedersen
Cloud Architect
APENTO

Level: Advanced

The Ultimate Education Destination
ORLANDO 2022

About me...



Ronni Pedersen

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

Contact Info

- Mail: rop@apento.com
- Twitter: [@ronnipedersen](https://twitter.com/ronnipedersen)

About me...



Jörgen Nilsson

- Principal Consultant, Onevinn
- Microsoft MVP: Enterprise Mobility
- MCSE/MCSA/MCITP/MCTS
- ITIL Foundation Certified
- Microsoft Certified Trainer (MCT)

Contact Info

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

Agenda

- Tools
- Troubleshooting 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
 - During AutoPilot (Alt+Win+Q) (If updated OS is installed)

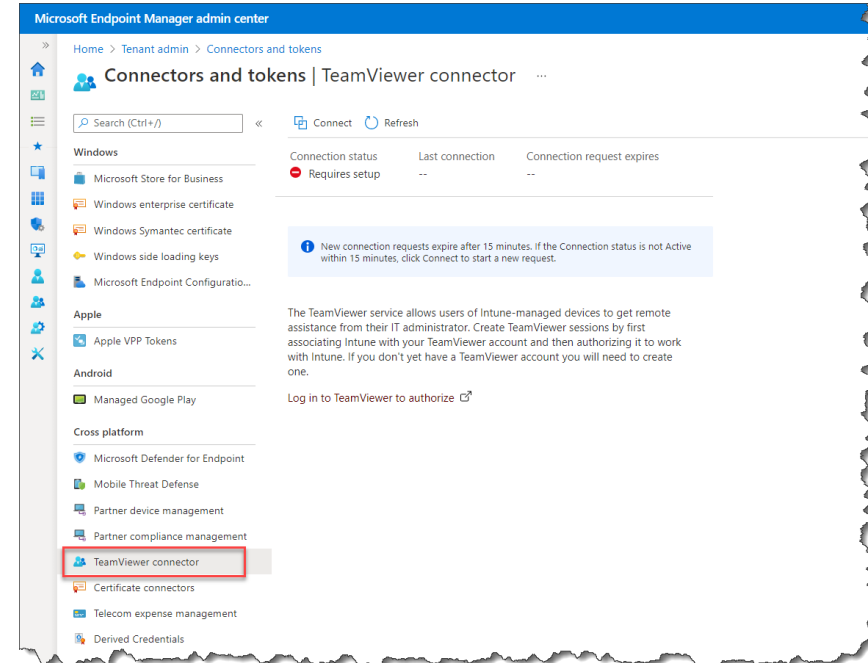


<https://oliverkieselbach.com/2020/03/03/quick-assist-the-built-in-remote-control-in-windows-10/>

Configure the TeamViewer Connector

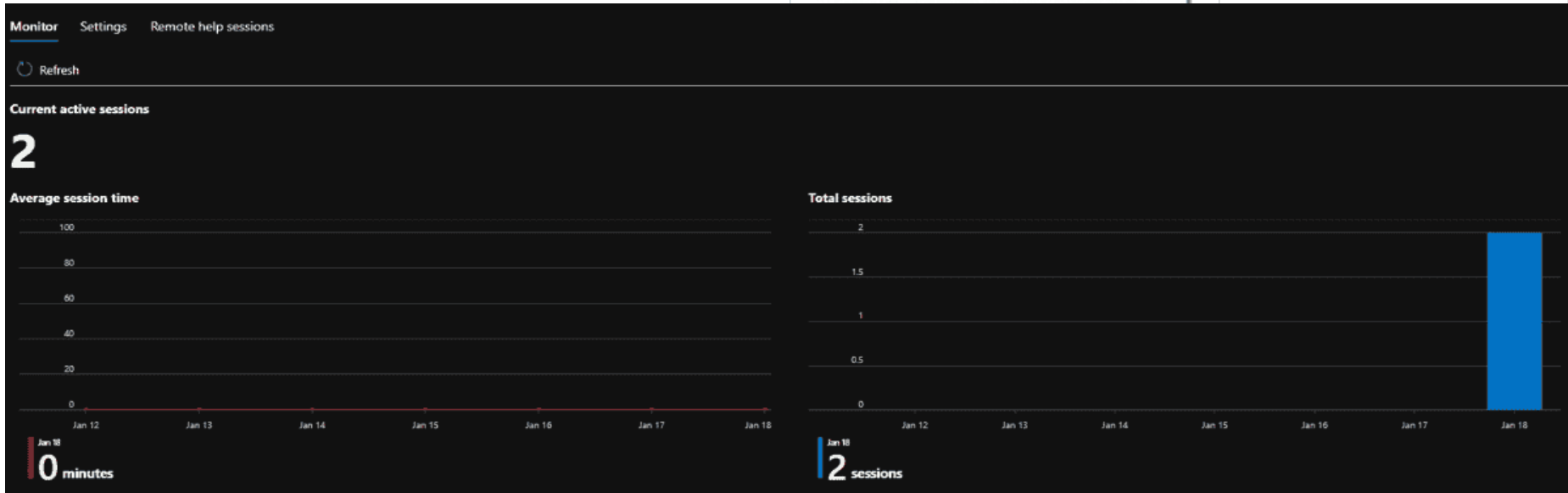
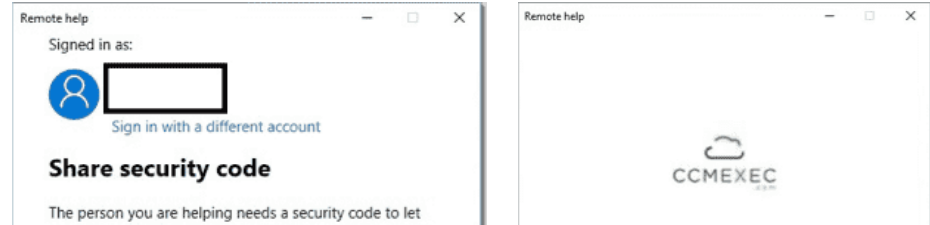
- Easy setup and configuration
- There are other options:
 - Beyond Trust
 - LogMeIn
 - Remote Help!

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



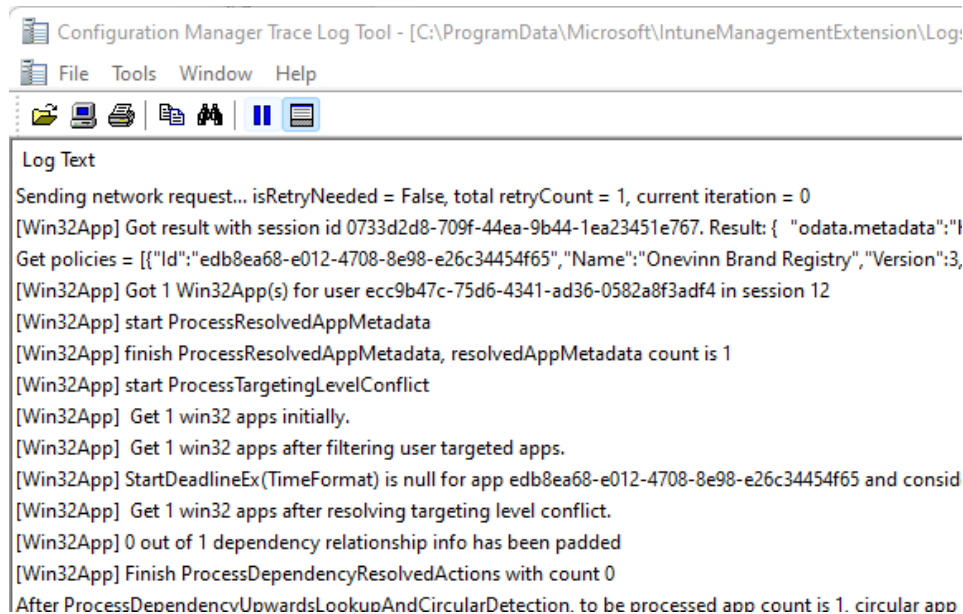
Microsoft Remote Help

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



Log-reader = CMtrace

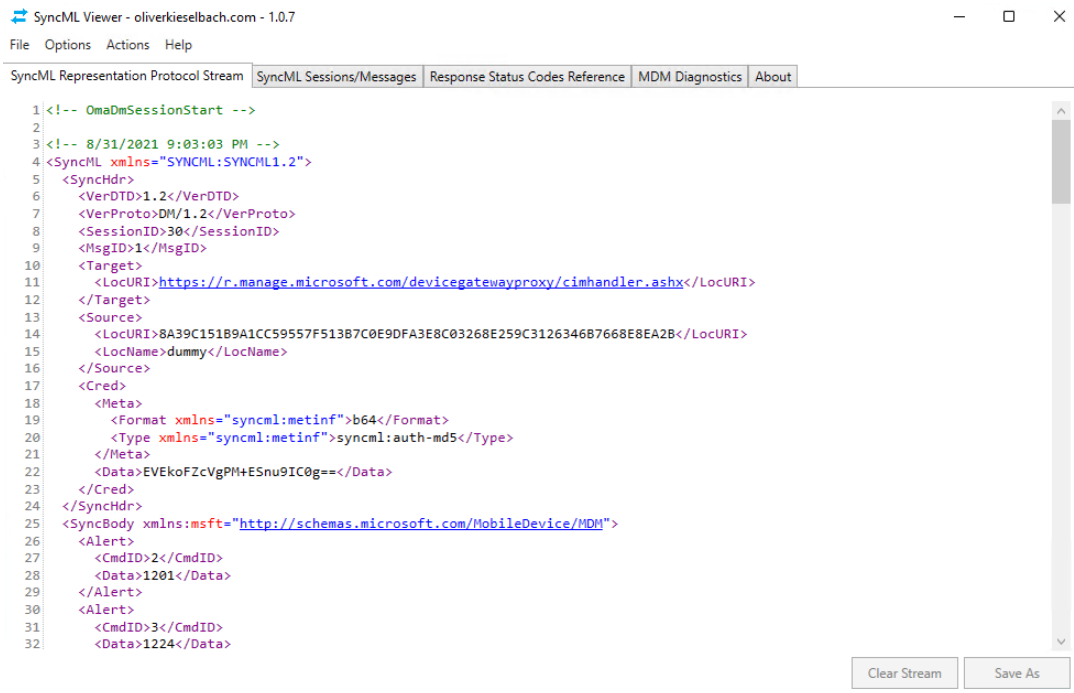
- Great log reader
- Not free but included in the Intune/MEM license
- Deploy it to all clients



<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 Sessions/Messages" tab is active, displaying an XML message. 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>

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>T0EeBAEAAAAAAAAoAMwDwVQAACgAaAfBVCnofKQCCQgCABAACQABAAEAAGABAAAABQAZAAQAAAAAAAAAAgAAAAAAAACAAEAAwMAEQBHZW51aW51SW50ZWwABAA0AEIudGVsKFIPiENvcmUoVE0pIGk3LTg1NTlV
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 and later
 - Windows 11
 - HoloLens 2 2004 and later
 - Both Intune and Co-Managed devices
 - Corporate-owned devices
 - Stored for 28 days and then deleted (up to 10 collections)
 - Bulk action (up to 25 devices)
- Upload URL:
 - `lgmsapeweu.blob.core.windows.net`
- More information:
 - <https://docs.microsoft.com/en-us/mem/intune/remote-actions/collect-diagnostics>



Device Diagnostics

- Autopilot enrollment failure

 Refresh				
Requested by	Status	Request initiated ↑↓	Diagnostics uploaded ↑↓	Diagnostics
rop@apento.com	Pending diagnostics upload	11/15/2022, 1:17:51 PM		
Autopilot enrollment	Complete	11/11/2022, 7:44:36 AM	11/11/2022, 7:52:06 AM	Download
Autopilot enrollment	Failed	11/10/2022, 7:37:16 AM		

Collecting Diagnostic Logs

Home > Windows >

DESKTOP-NIIRT6B ...

Search (Ctrl+/) «

Retire Wipe Delete Remote lock Sync Reset passcode Restart Collect diagnostics Fresh Start

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Endpoint security configuration

Recovery keys

User experience

Device diagnostics (preview)

Managed Apps

Collect diagnostics: Completed

Essentials

Device name : DESKTOP-NIIRT6B Primary user : Ronni Pedersen

Management name : rop_Windows_6/18/2020_4:01 PM Enrolled by : Ronni Pedersen

Ownership : Corporate Compliance : Compliant

Serial number : Operating system : Windows

Phone number : --- 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	Download

Remote Troubleshooting

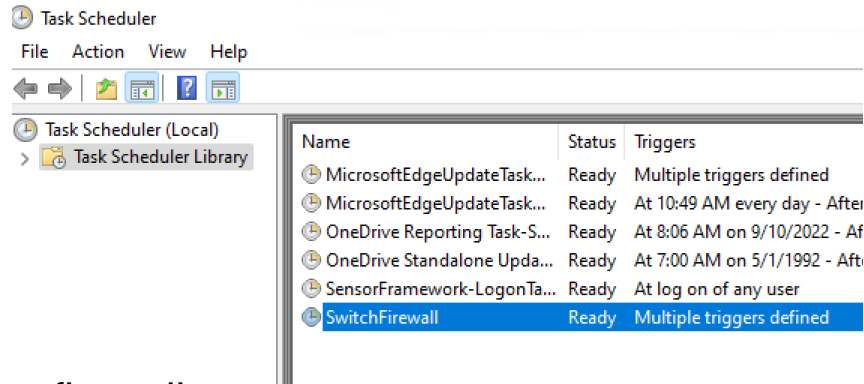
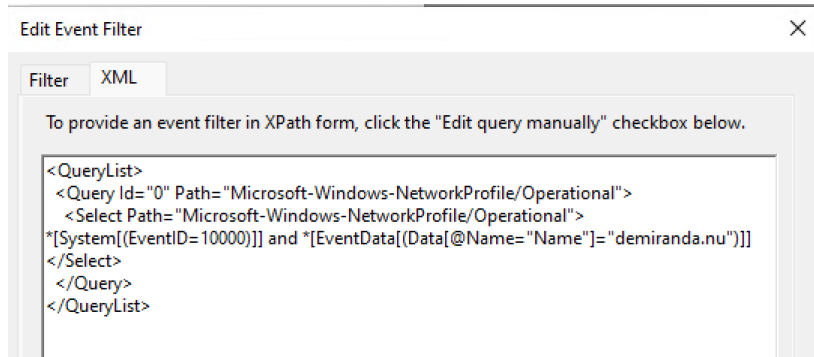
- Customer quote:

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

- Challenge: Windows Firewall – Private/Public is the only options on a AAD joined device
- Need to script the switch to Private profile
- Local admin can always switch!
- LAPS is your friend!

Solution

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



<https://ccmexec.com/2022/10/switch-to-private-firewall-profile-on-aad-joined-when-connected-to-specific-network/>





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

Use Settings Catalog

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

The screenshot shows the 'Configuration settings' tab for 'Microsoft Office 2016 (Machine)'. Under the 'Updates' subcategory, there is a notification that 14 of 16 settings are not configured. Two settings are visible: 'Enable Automatic Updates' and 'Update Channel', both of which are currently 'Enabled'. The 'Update Channel' is set to 'Current Channel (Preview)'.

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

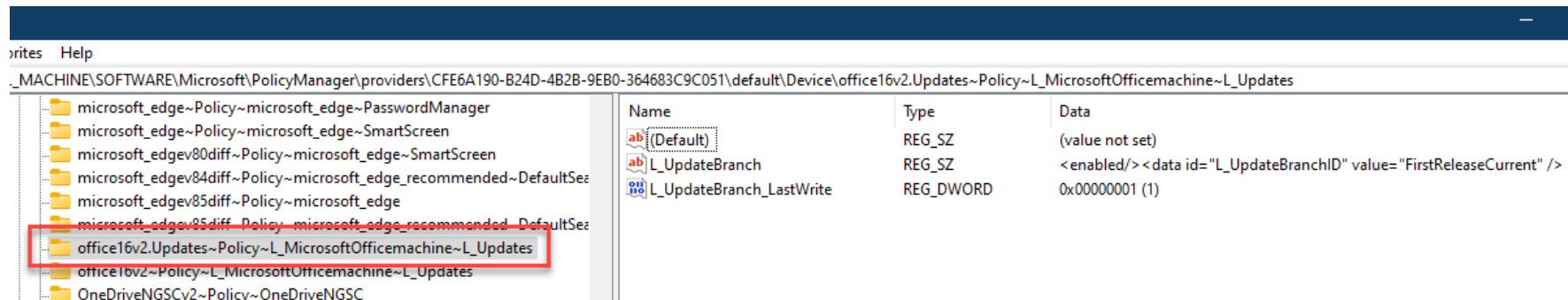
Enable Automatic Updates ⓘ ☒ Enabled ⊖

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.

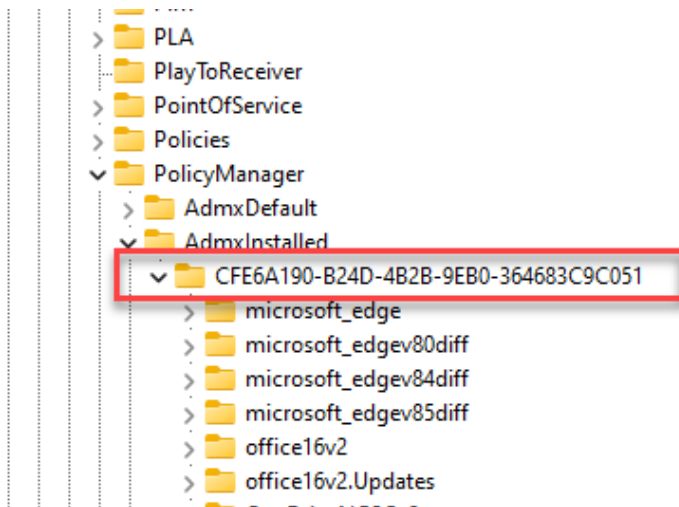


Find the Provider ID

Find the provider ID for your device

- Open the Registry Editor, and go to:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policy Manager\Admx\Installed



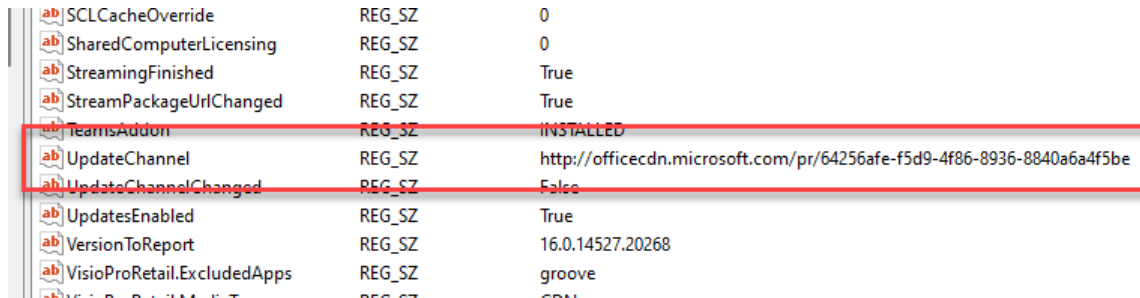
#2 Check the Office registry keys

- Go to the Office policy path:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\Configuration

- Check the **UpdateChannel** value:

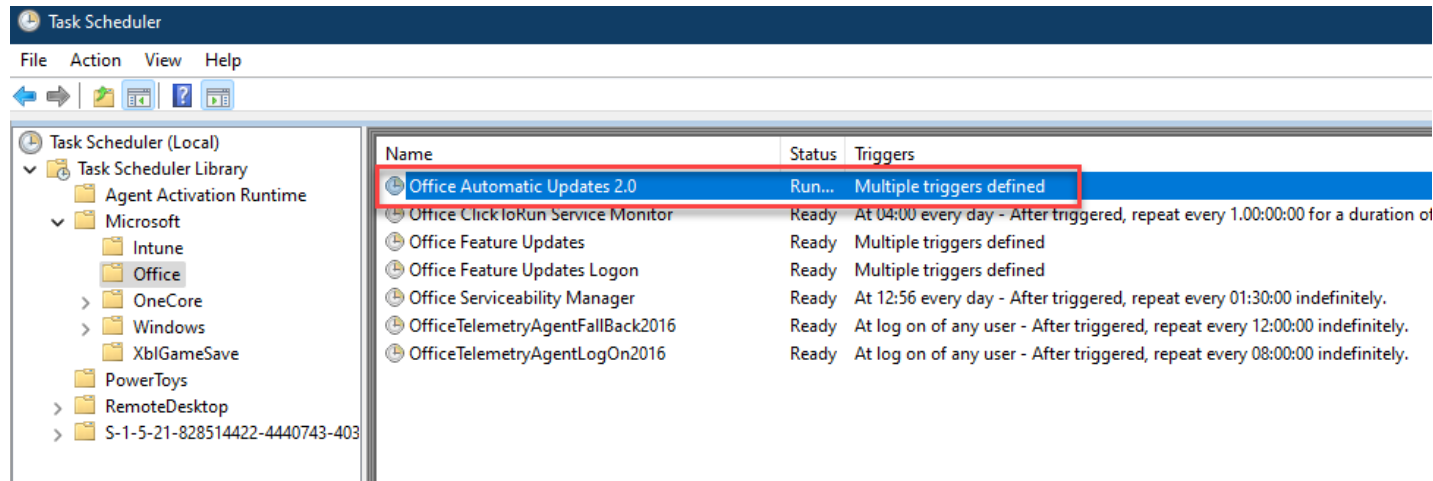
- Monthly Enterprise Channel = 55336b82-a18d-4dd6-b5f6-9e5095c314a6
- Current Channel = 492350f6-3a01-4f97-b9c0-c7c6ddf67d60
- Current Channel (Preview) = 64256afe-f5d9-4f86-8936-8840a6a4f5be**
- Semi-Annual Enterprise Channel = 7ffbc6bf-bc32-4f92-8982-f9dd17fd3114
- Semi-Annual Enterprise Channel (Preview) = b8f9b850-328d-4355-9145-c59439a0c4cf
- Beta Channel = 5440fd1f-7ecb-4221-8110-145efaa6372f

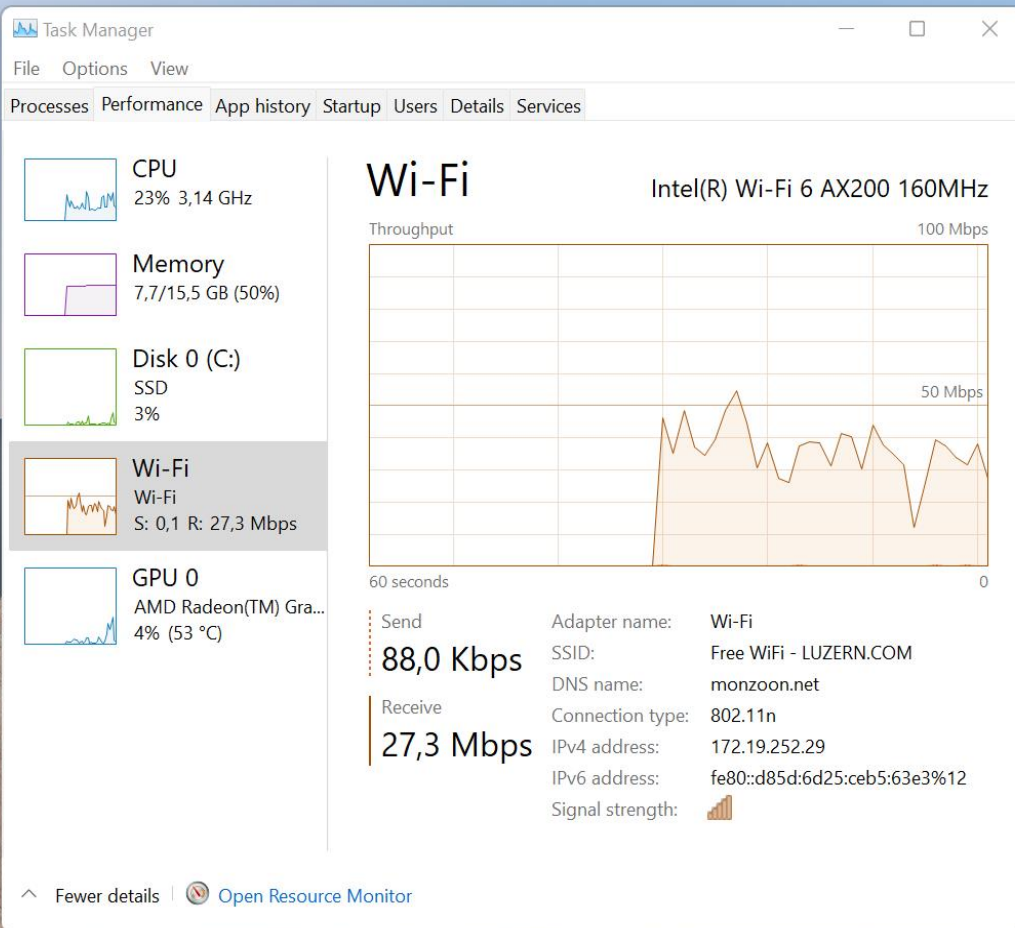


ab SCLCacheOverride	REG_SZ	0
ab SharedComputerLicensing	REG_SZ	0
ab StreamingFinished	REG_SZ	True
ab StreamPackageUrlChanged	REG_SZ	True
ab TeamsAddon	REG_SZ	INSTALLED
ab UpdateChannel	REG_SZ	http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-8936-8840a6a4f5be
ab UpdateChannelChanged	REG_SZ	False
ab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

#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**”

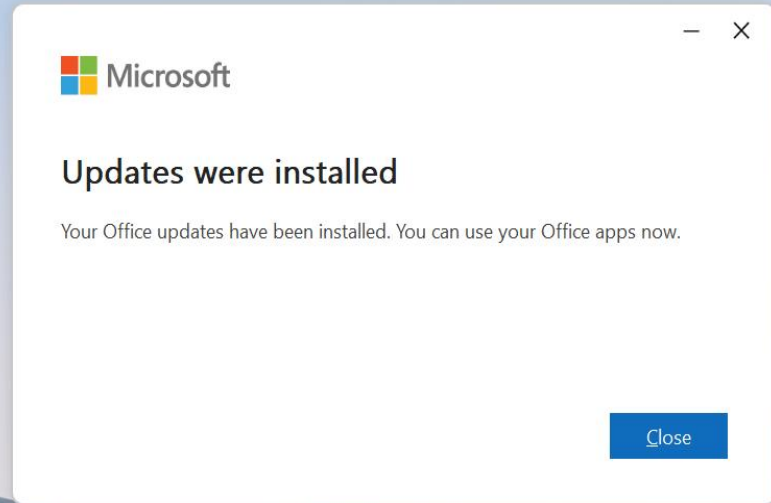
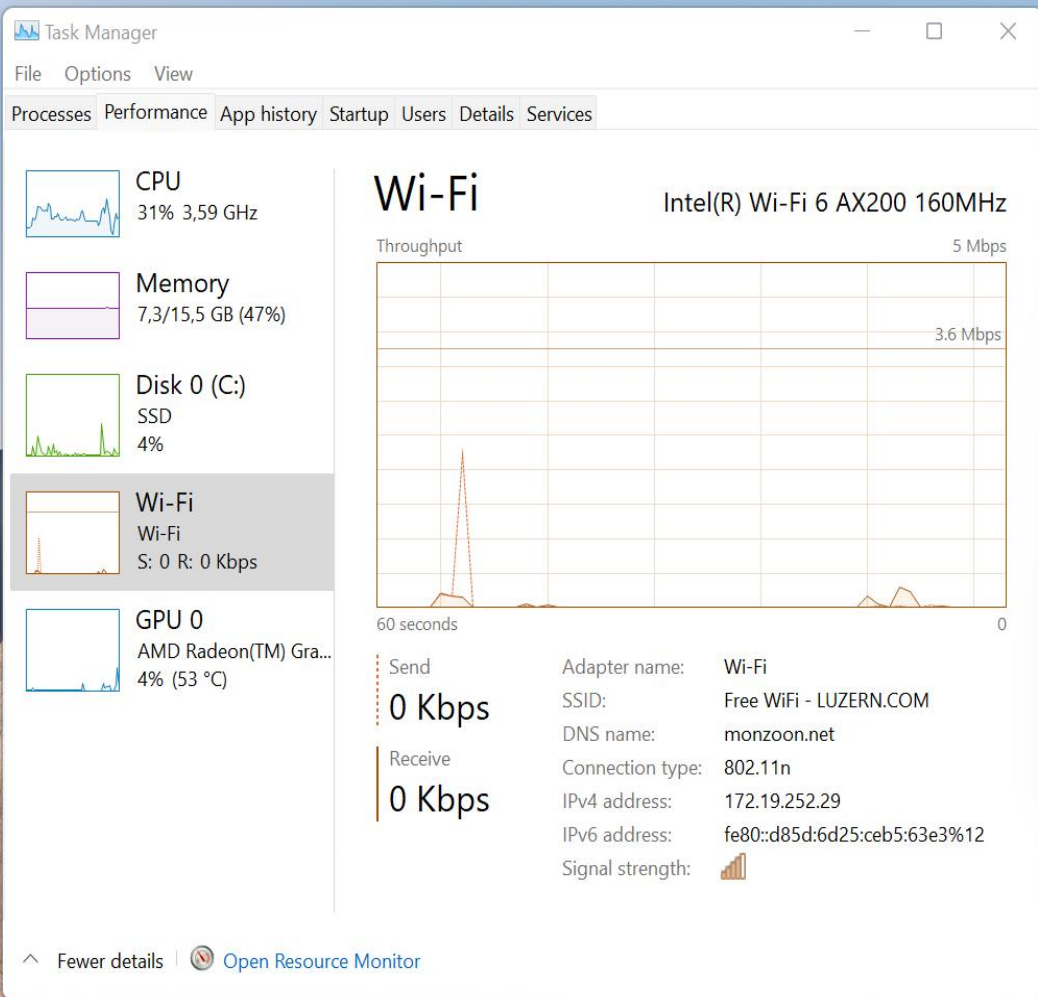




Microsoft

Downloading Office updates...

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



Update history for Microsoft 365 Apps

Update history for Microsoft 365 Apps

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

Product Information



Subscription Product

Microsoft 365 Apps for enterprise

Belongs to: rop@apento.com

This product contains



Manage Account

Change License



Update
Options ▾

Office Updates

Updates are automatically downloaded and installed.



About
Word

About Word

Learn more about Word, Support, Product ID, and Copyright information.

Version 2209 (Build 15629.20058 Click-to-Run)

Current Channel (Preview)



What's
New

What's New

See the most recently installed updates.

TROUBLESHOOTING SUBSCRIPTION BASED ACTIVATION

Subscription Based activation

- Easiest way of upgrading to Enterprise from pro
- Re-activated every 30 days
- Each user can activate 5 devices
- Activating shared devices
 - Either all users must have a Windows e3 license assigned
 - Shared devices must be excluded and activated in a different way (KMS,MAK)

HKEY_Local_Machine\System\Currentcontrolset\services\clipsvc\parameters

Value: DisableSubscription Reg_Dword Value=1

Subscription based activation

- Important: Devices will automatically “migrate” from MAK, KMS and AD-based activation to Subscription when a user with an assigned license logs on.
- Blocked by the “Work or school account problem”
- Exclude **Universal Store Service APIs and Web Application** from your Conditional Access framework.

Activation

Windows

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

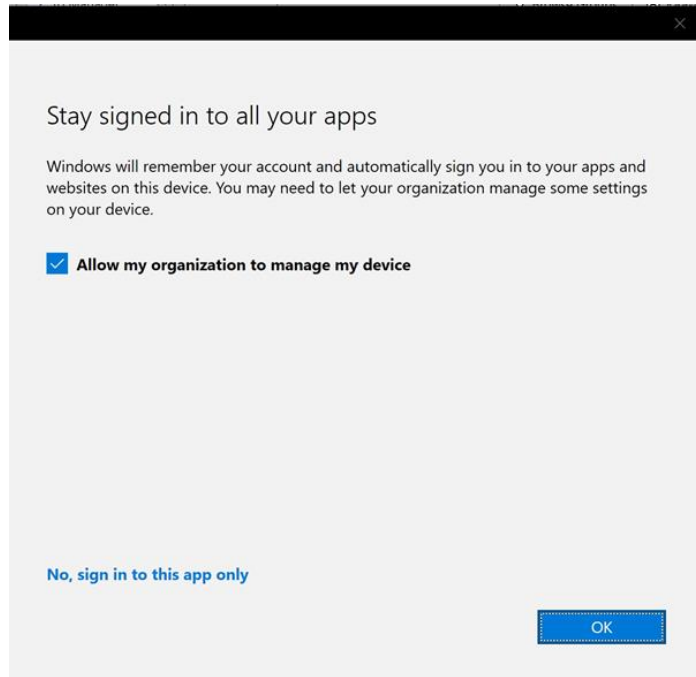
CA exclusions

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

Selected items		
MA	Microsoft Activity Feed Service d32c68ad-72d2-4acb-a0c7-46bb2cf93873	Remove
MC	Microsoft Command Service 19686ca6-5324-4571-a231-77e026b0e06f	Remove
MD	Microsoft Device Directory Service 8f41dc7c-542c-4bdd-8eb3-e60543f607ca	Remove
US	Universal Store Service APIs and Web 45a330b1-b1ec-4cc1-9161-9f03992aa49f	Remove

Stay signed in to all your apps = Evil

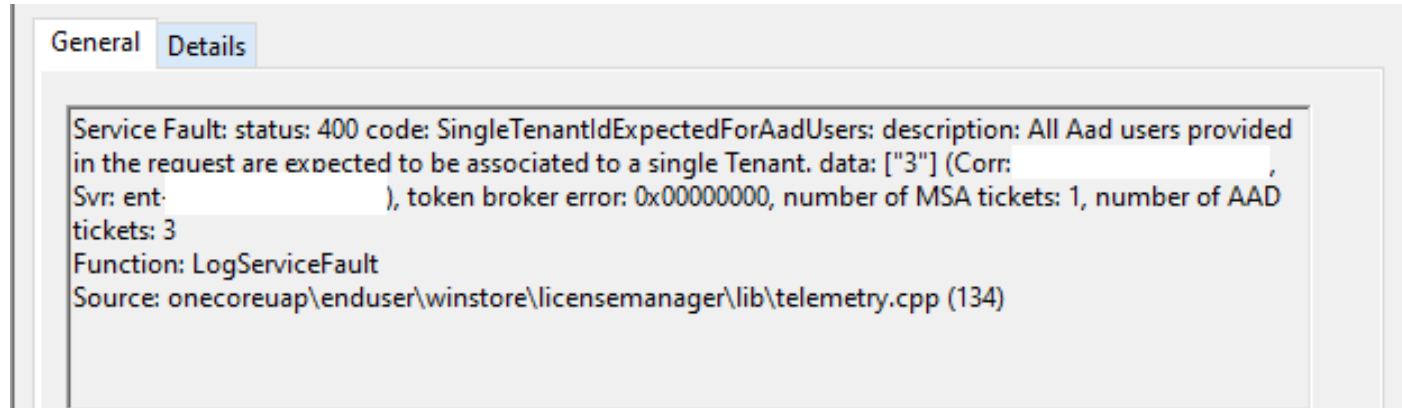
- “**Stay signed in to all your apps**” dialog in Microsoft Apps (outlook, Powerpoint, excel....)
- Recommended to block in Hybrid join
- Needs to be blocked on all modern managed Windows devices!
 - Personal devices: Intune sync will fail
 - AzureAD Joined devices: Windows Activation will fail



Subscription Based Activation

- Store Event Log + Schedule Task

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



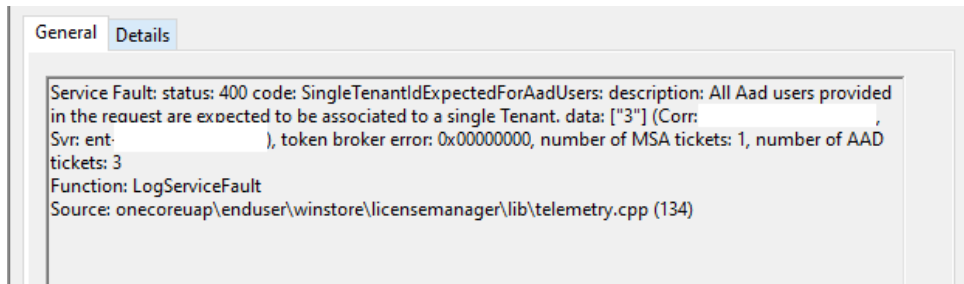
<https://ccmexec.com/2021/01/mem-windows-10-personal-device-and-sync-issues/>

Subscription based activation

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

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 renewal is done using the StoreAPI
 - In this case more than one AzureAD account was added under "Access work or School"



Create profile ...

Windows 10 and later - Settings catalog (preview)

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

+ Add settings

^ Settings

i 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

Search

+ Add filter

Browse by category

Administrative Templates\Start Menu and Taskbar

Administrative Templates\System\Group Policy

Settings

1 results in the "Settings" category

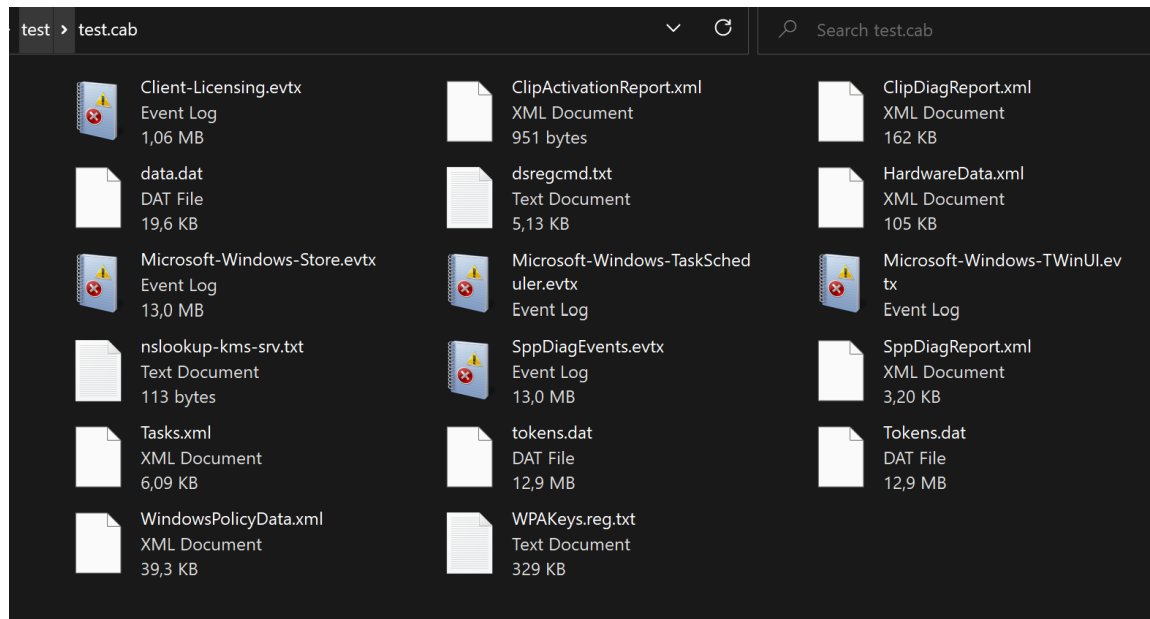
Select all these settings

Setting name

☒ Allow Workplace ⓘ

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+/) « ^ Essentials

 Overview

Created : 01/01/70, 1:00 AM Platforms configured : 6

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

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 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- [Copy]

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

TECH EVENTS WITH PERSPECTIVE

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 limit restrictions

- Are not applied when enrolling a device in the following scenarios:
 - Co-managed enrollments
 - Group Policy (GPO) enrollments
 - Azure Active Directory (Azure AD) joined enrollments, including bulk enrollments
 - Windows Autopilot enrollments
 - Device enrollment manager enrollments

Client Health

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

Search (Ctrl+/)

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Recovery keys

Managed Apps

Retire

Wipe

Delete

Remote lock

Sync

Reset passcode

Restart

Fresh Start

Autopilot Reset

Quick scan

Device name : APENTO-Bndfil1Z

Primary User : Ronni Pedersen

Management name : mail_Windows_5/26/2019_6:52 PM

Enrolled by : Ronni Pedersen

Ownership : Corporate

Compliance : Not Compliant

Serial number : 7987-3600-6266-3074-4536-7994-21

Operating system : Windows

Phone number : ---

Device model : Virtual Machine

See more

Device actions status

Action	Status	Date/Time
No results		

Co-management

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

Configuration Manager agent state

Unknown

Details

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

LIVE!

360

TECH EVENTS WITH PERSPECTIVE

TROUBLESHOOTING POLICIES

Configuration Policies

Recommended order for Windows devices

- Endpoint Security
- Settings Catalog (Preview)
- Templates
 - Configuration Policies
 - Built-In Administrative Templates
 - OMA-URI (Custom CSP)
- Custom ADMX ingestion (3rd. Party apps)
- PowerShell Scripts

Optional:

- Proactive Remediation (Requires a Windows Enterprise E3 license)



Profile Tattooing

- Removing the assignment of the profile does not always revert the setting.
 - The behavior depends on the CSP.
 - Some setting remains until configured to a different value
 - Some CSPs remove the setting, and some CSPs keep the setting.
- Profiles applies to a **User Group** and a user is removed from the group.
 - Note: It can take up to **7 hours + the platform-specific policy refresh cycle**.
- Wi-Fi, VPN, Certificate, and Email Profiles
 - These profiles are removed from all supported enrolled devices

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot#what-happens-when-a-profile-is-deleted-or-no-longer-applicable>

Policy and Profile refresh cycles

Existing Devices

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

Recently Enrolled Devices

- #1 - Every 3 minutes for 15 minutes
- #2 - Every 15 minutes for 2 hours
- #3 - Every 8 hours

Manual Refresh

- Open the Company Portal app and sync the device to immediately check for policy or profile updates.
- This device check-in will not refresh the already applied Policy CSP settings.
- Trigger Task Scheduler (Recommended for troubleshooting)
- Scripted methods

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



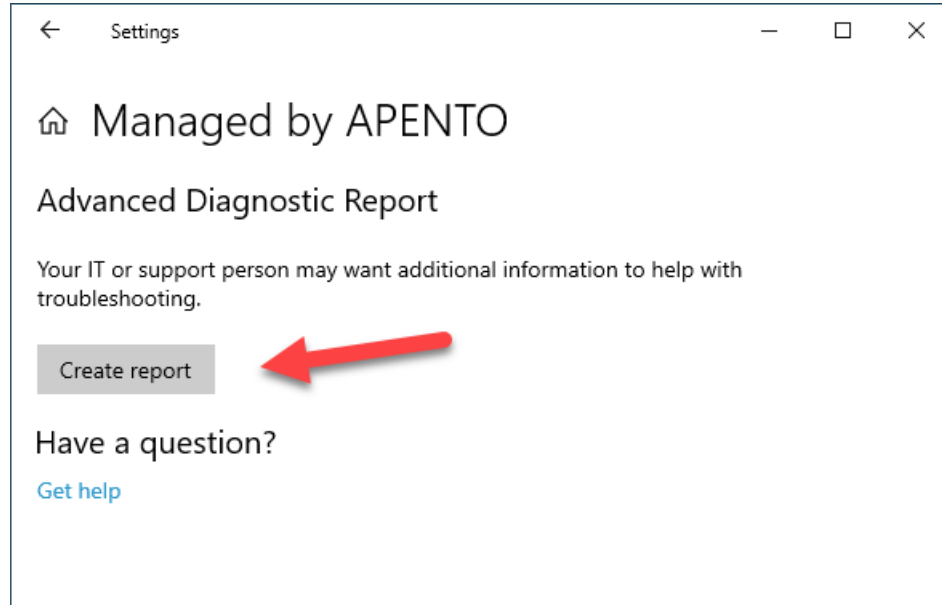
Policy/Profile Conflicts

- 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	WindowsClearProtection	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>

[Home](#) > [Troubleshooting + support](#)

Troubleshooting + support | Troubleshoot ✕ ...

»

Display name
Ronni Pedersen

[Change user](#)

Intune license
2 devices noncompliant

Principal name
rop@apento.com

Email
rop@apento.com

Group memberships (16)
[Show all](#)

Assignments

Client apps

Assignment	↑↓	Name	↑↓	OS	↑↓	Type	↑↓	Last modified
Included		7-Zip 21.07 (MSI-x64)		Windows 10 and later		Available		3/8/2022 2:3
Included		Adobe Acrobat Reader DC 22.001.20117		Windows 10 and later		Available		4/30/2022 9
Included		Amazon WorkSpaces 4.0.6.2415 (x64)		Windows 10 and later		Available		3/8/2022 2:0
Included		Camtasia 2021 21.0.19.35860 (MSI-x64)		Windows 10 and later		Available		5/19/2022 4:
Included		Company Portal		Windows 10 and later		Required		8/16/2021 9:

Devices

Device name	↑↓	Managed by	↑↓	Azure AD join ty...	↑↓	Ownership	↑↓	Intune compliant	↑↓	Azure AD compl...	↑↓	App install lifecy...	↑↓
CPC-rop-GUZ4-FB		Intune		AzureAD		Corporate		Yes		Yes		success	
DESKTOP-75BMIDA		Intune		AzureAD		Corporate		No		No		success	
DESKTOP-NIIRT6B		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	

INTUNE MANAGEMENT EXTENSION

Intune Management Extension

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

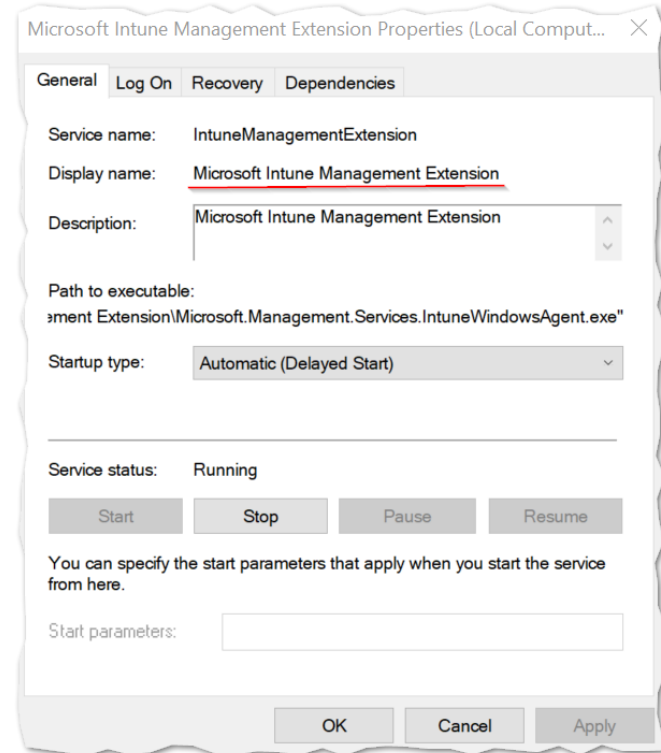


Intune Management Extension

Troubleshooting

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

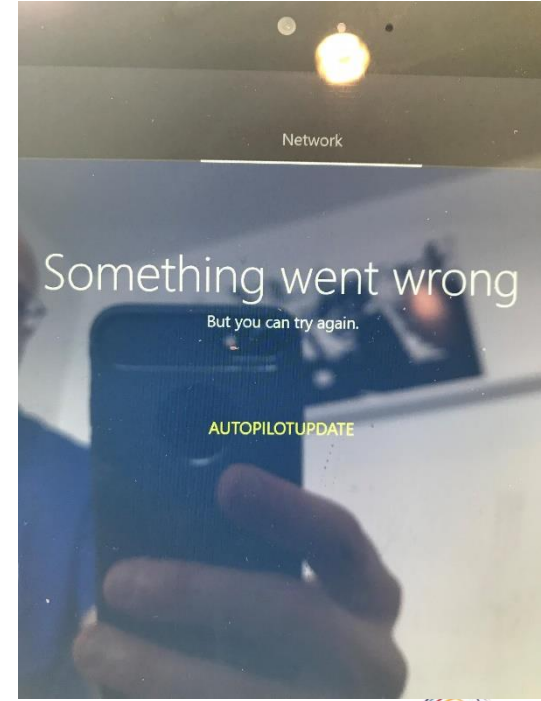
<https://docs.microsoft.com/en-us/intune/apps/intune-management-extension#prerequisites>



WINDOWS AUTOPILOT

Network

- A network for enrollment is needed
- Guest network, open network
- All ports, URL required must be opened
- HTTPS/SSL Inspection cannot be used



Meet “Bengt” – your new network admin



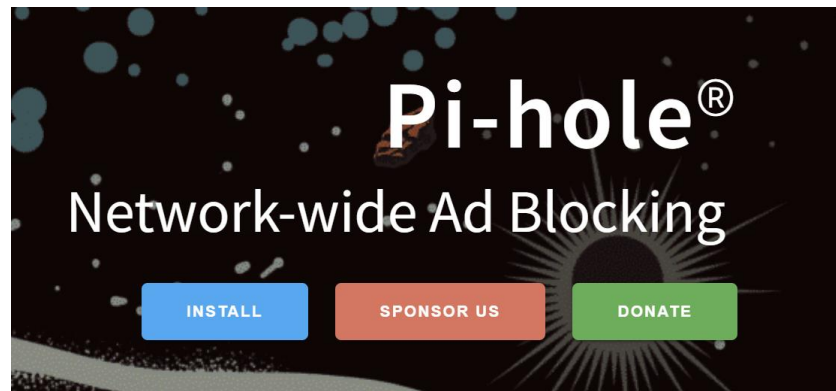
Network issues – we have seen

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

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

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

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



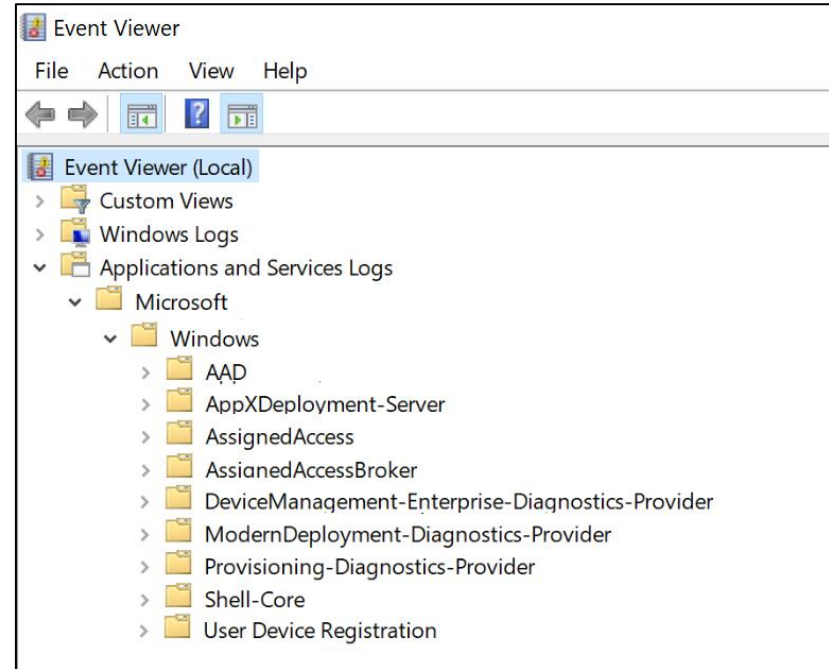
Shift+F10

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

TROUBLESHOOTING

Troubleshooting

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



Setting up for work or school

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



Device preparation ▼

✔ Completed

Device setup ^

● Error

Security policies (1 of 1 applied)

Certificates (1 of 1 applied)

Network connections (No setup needed)

Apps (0x81036502)

Account setup ▼

Waiting

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

[Continue anyway](#)

[Reset device](#)

[Try again](#)

Windows Autopilot diagnostics



Policy Provider Installation



Device-Targeted Apps Installation ^

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

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

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



Device-Targeted Policies Installation



Device-Targeted Network Profiles Installation



Device-Targeted Certificates Installation



User-Targeted Apps Installation



Close

Export logs

Always manage local admin group

- When there have been an service degradation in Autopilot a couple of times the device is enrolled but ignores the enrollment profile settings = enrolling user ends up as local admin!

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!

