



Troubleshooting the MEM managed Windows Client

Jörgen Nilsson & Ronni Pedersen

Workplace Ninja Summit 2022



Platinum Sponsor



PATCH MY PC



Microsoft
Security

Gold Sponsor

glueckkanja■gab

baseVISION
SECURE & MODERN WORKPLACE



RECAST SOFTWARE

LIQUIT

Lenovo



Snapdragon

Silver and Special Sponsors



LUZERN
FINANZEN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPP MAN

APP MANAGEVENT.COM
2022 | OCTOBER 7 NETHERLANDS

dinext.

Preparing for WP Ninjas like a BOSS!

What could go wrong?

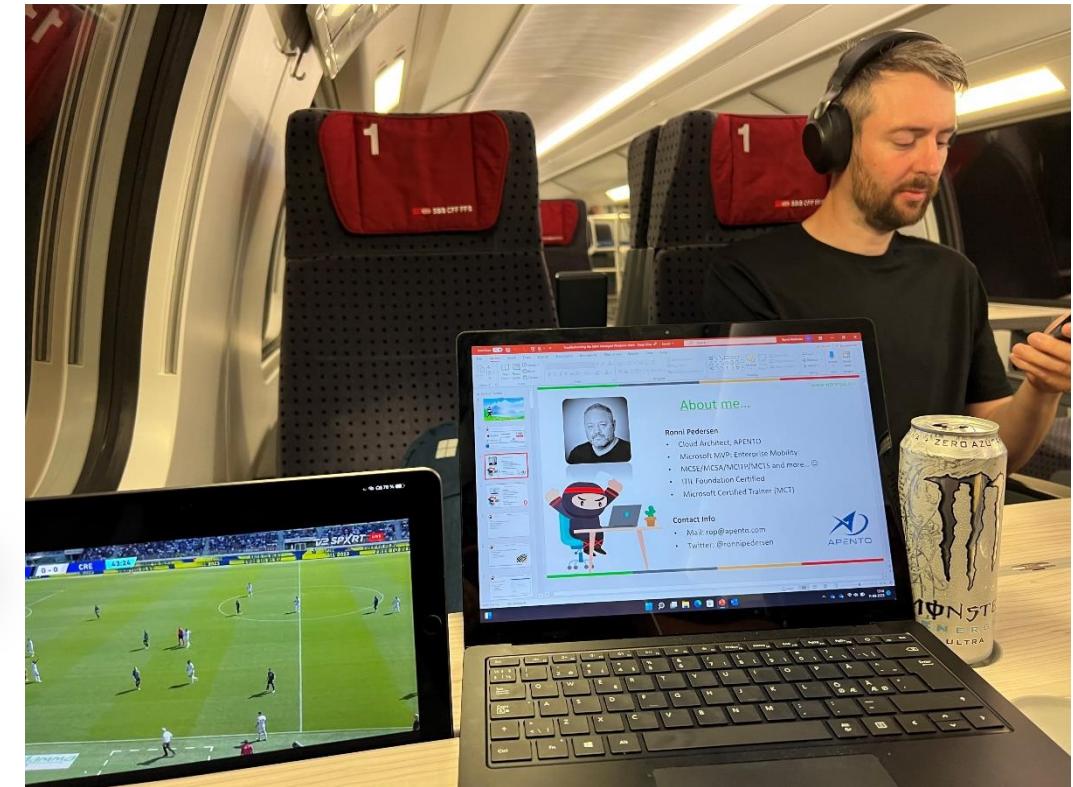






What could go wrong?

www.wpninjas.eu
#WPNinjaS





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...

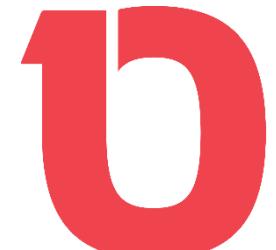


Jörgen Nilsson

- 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

www.wpninjas.eu

- Tools
- Troubleshooting Subscription based activation
- Troubleshooting Enrollment
- Troubleshooting Policies
- Intune Management extension





Remote Control

www.wpninjas.eu

- 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

www.wpninjas.eu

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

The screenshot shows the Microsoft Endpoint Manager admin center interface. The left sidebar lists various connectors and tokens, including Windows, Apple, and Android options. The 'TeamViewer connector' option is highlighted with a red box. A callout box provides information about the TeamViewer service, stating it allows users of Intune-managed devices to get remote assistance from their IT administrator. It also mentions creating TeamViewer sessions by associating Intune with a TeamViewer account and authorizing it to work with Intune. A link to 'Log in to TeamViewer to authorize' is provided.

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



Microsoft Remote Help

www.wpninjas.eu

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

The screenshot shows the Microsoft Endpoint Manager (MEM) portal interface. At the top, there's a navigation bar with 'Monitor' (underlined), 'Settings', and 'Remote help sessions'. Below it is a 'Refresh' button and a section titled 'Current active sessions' which displays the number '2'. On the left, a chart titled 'Average session time' shows a value of '0 minutes' for the period from Jan 12 to Jan 18. On the right, a chart titled 'Total sessions' shows a count of '2 sessions' for the same period. Two windows are overlaid on the page: one titled 'Remote help' asking for a security code, and another titled 'Remote help' showing a connection from 'CCMEXEC'.

Remote help
Signed in as:
Sign in with a different account

Share security code
The person you are helping needs a security code to let

Remote help
CCMEXEC

Monitor Settings Remote help sessions

Refresh

Current active sessions

2

Average session time

0 minutes

Total sessions

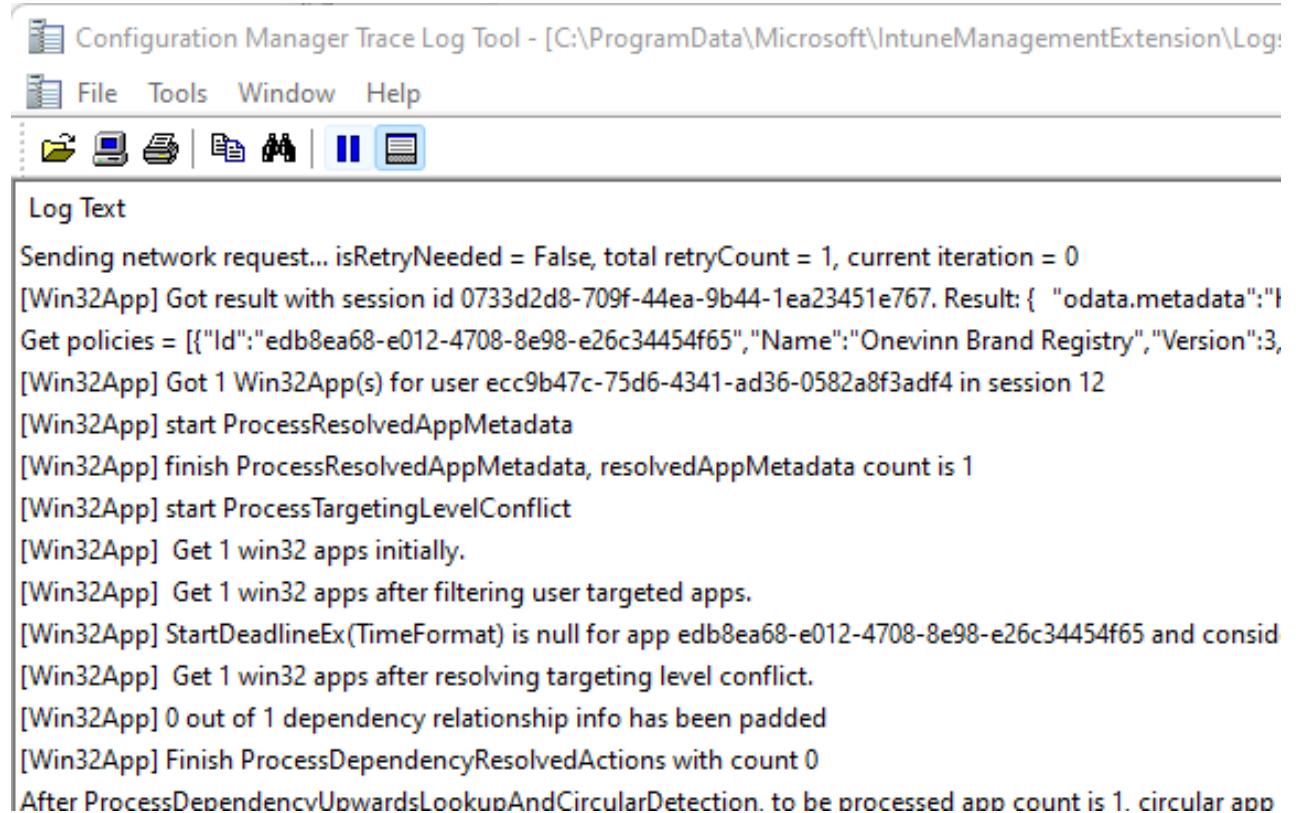
2 sessions



CMtrace

www.wpninjas.eu

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



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

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

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



More Tools – Advanced Troubleshooting

www.wpninjas.eu

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

SyncML Viewer - oliverkieselbach.com - 1.0.7

File Options Actions Help

SyncML Representation Protocol Stream SyncML Sessions/Messages Response Status Codes Reference MDM Diagnostics About

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

Clear Stream Save As

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



```
1533    <----->
1534    <Status>
1535        <CmdID>32</CmdID>
1536        <MsgRef>2</MsgRef>
1537        <CmdRef>25</CmdRef>
1538        <Cmd>Get</Cmd>
1539        <Data>200</Data>
1540    </Status>
1541    <Results>
1542        <CmdID>33</CmdID>
1543        <MsgRef>2</MsgRef>
1544        <CmdRef>25</CmdRef>
1545        <Item>
1546            <Source>
1547                <LocURI>./DevDetail/Ext/DeviceHardwareData</LocURI>
1548                <Data>T0EeBAEAHAAAAoAMwDwVQAACgAaAfBVCnofKQQCCQgCABAACQABAAEAAgABAAAABQAZAAQAAAAAAAAAgAAAAAAAACAAEAAwMAEQBHZW51aW51SW50ZWlwABAA0AEEludGVsKFIpIENvcmUoVE0pIGk3LTg1NTlV:
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>
  </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

www.wpninjas.eu

- 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

www.wpninjas.eu

Home > Windows >

DESKTOP-NIIRT6B ...

Search (Ctrl+ /) <>

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

1

Collect diagnostics: Completed

Overview

Manage

- Properties
- Monitor
- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Endpoint security configuration
- Recovery keys
- User experience
- Device diagnostics (preview)** 2
- Managed Apps

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	:	[REDACTED]	Operating system	:	Windows
Phone number	:	---	Device model	:	NUC8i7HNC

See more

Device actions status

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

3

The screenshot shows the Microsoft Intune Device diagnostics (preview) interface. At the top, there's a header with a Refresh button and a status message: "Requested by rop@apento.com, Status: Complete". Below this is a table with columns: Requested by, Status, Request initiated, Diagnostics uploaded, and Diagnostics. The "Diagnostics" column contains a blue "Download" button. The "Status" column shows "Complete" for all rows.

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

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

www.wpninjas.eu

- 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

www.wpninjas.eu

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

Edit Event Filter

Filter XML

To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
<Query Id="0" Path="Microsoft-Windows-NetworkProfile/Operational">
  <Select Path="Microsoft-Windows-NetworkProfile/Operational">
*[System[(EventID=10000)]] and *[EventData[(Data[@Name="Name"] = "demiranda.nu")]]
  </Select>
</Query>
</QueryList>
```

Task Scheduler

File Action View Help

Task Scheduler (Local)

Task Scheduler Library

Name	Status	Triggers
MicrosoftEdgeUpdateTask...	Ready	Multiple triggers defined
MicrosoftEdgeUpdateTask...	Ready	At 10:49 AM every day - After
OneDrive Reporting Task-S...	Ready	At 8:06 AM on 9/10/2022 - Af
OneDrive Standalone Upda...	Ready	At 7:00 AM on 5/1/1992 - Aft
SensorFramework-LogonTa...	Ready	At log on of any user
SwitchFirewall	Ready	Multiple triggers defined

Configuration Policy Process





Microsoft 365 Apps Policy

www.wpninjas.eu

- 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

www.wpninjas.eu

- 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

i 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)

www.wpninjas.eu

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

The screenshot shows the Microsoft Settings Catalog interface. At the top, there are two tabs: **1 Configuration settings** (underlined in blue) and **2 Review + save**. Below the tabs is a button **+ Add settings**. A category tree shows **Microsoft Office 2016 (Machine)** expanded, with a **Remove category** link. Underneath, a subcategory **Updates** is shown, with a **Remove subcategory** link. A status message indicates **14 of 16 settings in this subcategory are not configured**. Two settings are listed: **Enable Automatic Updates** (status: Enabled) and **Update Channel** (status: Enabled). A dropdown menu for **Channel Name: (Device) *** is set to **Current Channel (Preview)**.



#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.

The screenshot shows the Windows Registry Editor interface. The title bar says "Registry Editor". The address bar shows the path: `_MACHINE\SOFTWARE\Microsoft\PolicyManager\providers\CFE6A190-B24D-4B2B-9EB0-364683C9C051\default\Device\office16v2.Updates~Policy~L_MicrosoftOfficemachine~L_Updates`. The left pane displays a tree view of registry keys under this path, with several keys highlighted by a red box. The right pane shows a table with three columns: Name, Type, and Data. The table contains the following data:

Name	Type	Data
(Default)	REG_SZ	(value not set)
L_UpdateBranch	REG_SZ	<enabled/><data id="L_UpdateBranchID" value="FirstReleaseCurrent" />
L_UpdateBranch_LastWrite	REG_DWORD	0x00000001 (1)



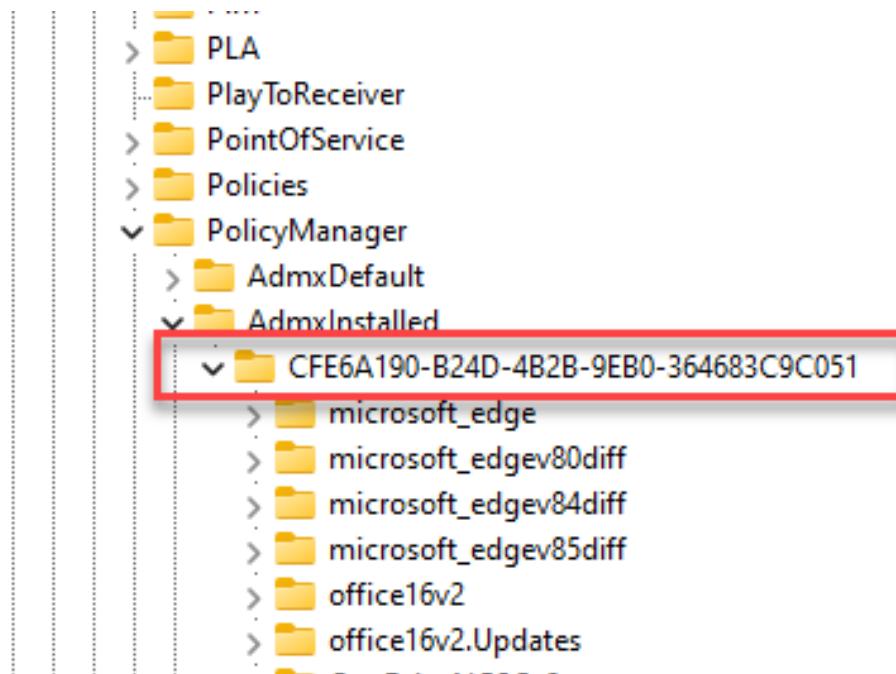
Find the Provider ID

www.wpninjas.eu

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	com



#3 Force Office automatic updates to run

www.wpninjas.eu

- 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”

The screenshot shows the Windows Task Scheduler interface. The left pane displays the Task Scheduler (Local) library structure, with the Microsoft folder expanded to show sub-folders like Intune, Office, OneCore, Windows, XblGameSave, PowerToys, RemoteDesktop, and a security identifier. The right pane lists tasks in a grid format. The task "Office Automatic Updates 2.0" is highlighted with a red border. The grid columns are Name, Status, and Triggers. The "Name" column lists the task names, the "Status" column shows they are all Ready, and the "Triggers" column details the scheduling for each task.

Name	Status	Triggers
Office Automatic Updates 2.0	Run...	Multiple triggers defined
Office Click ToRun Service Monitor	Ready	At 04:00 every day - After triggered, repeat every 1:00:00:00 for a duration of
Office Feature Updates	Ready	Multiple triggers defined
Office Feature Updates Logon	Ready	Multiple triggers defined
Office Serviceability Manager	Ready	At 12:56 every day - After triggered, repeat every 01:30:00 indefinitely.
OfficeTelemetryAgentFallback2016	Ready	At log on of any user - After triggered, repeat every 12:00:00 indefinitely.
OfficeTelemetryAgentLogOn2016	Ready	At log on of any user - After triggered, repeat every 08:00:00 indefinitely.

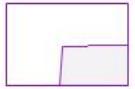
Task Manager

File Options View

Processes Performance App history Startup Users Details Services



CPU
23% 3,14 GHz



Memory
7,7/15,5 GB (50%)



Disk 0 (C:)
SSD
3%



Wi-Fi
Wi-Fi
S: 0,1 R: 27,3 Mbps



GPU 0
AMD Radeon(TM) Gra...
4% (53 °C)

Wi-Fi

Intel(R) Wi-Fi 6 AX200 160MHz

Throughput



Send

88,0 Kbps

Receive

27,3 Mbps

Adapter name:

Wi-Fi

SSID:

Free WiFi - LUZERN.COM

DNS name:

monzoon.net

Connection type:

802.11n

IPv4 address:

172.19.252.29

IPv6 address:

fe80::d85d:6d25:ceb5:63e3%12

Signal strength:

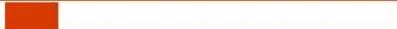


^ Fewer details | Open Resource Monitor



Downloading Office updates...

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



Task Manager

File Options View

Processes Performance App history Startup Users Details Services



CPU
31% 3.59 GHz



Memory
7.3/15.5 GB (47%)



Disk 0 (C:)
SSD
4%



Wi-Fi
Wi-Fi
S: 0 R: 0 Kbps

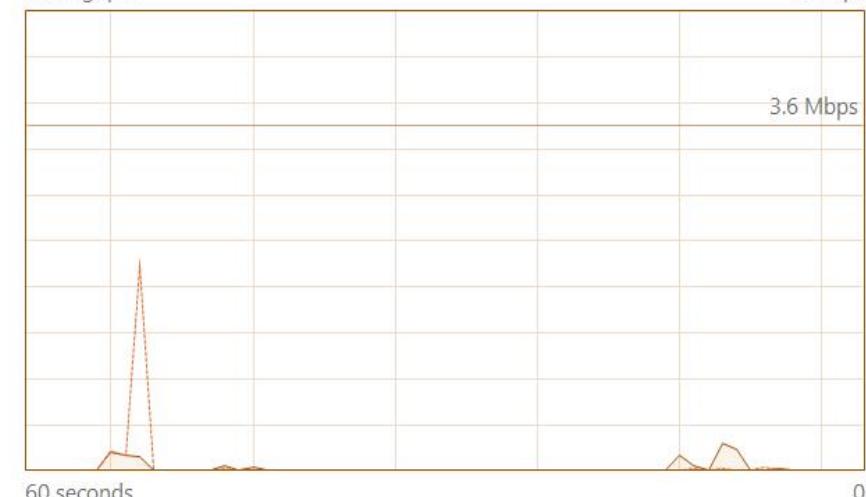


GPU 0
AMD Radeon(TM) Gra...
4% (53 °C)

Wi-Fi

Intel(R) Wi-Fi 6 AX200 160MHz

Throughput



Send
0 Kbps

Receive
0 Kbps

Adapter name: Wi-Fi
SSID: Free WiFi - LUZERN.COM
DNS name: monzoon.net
Connection type: 802.11n
IPv4 address: 172.19.252.29
IPv6 address: fe80::d85d:6d25:ceb5:63e3%12
Signal strength: 

^ Fewer details |  Open Resource Monitor



Updates were installed

Your Office updates have been installed. You can use your Office apps now.

Close



Update history for Microsoft 365 Apps

www.wpninjas.eu

Product Information



Subscription Product

Microsoft 365 Apps for enterprise

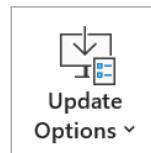
Belongs to: rop@apento.com

This product contains



Manage Account

Change License



Office Updates

Updates are automatically downloaded and installed.



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

See the most recently installed updates.

Update history for Microsoft 365 Apps

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

Troubleshooting Subscription Based Activation

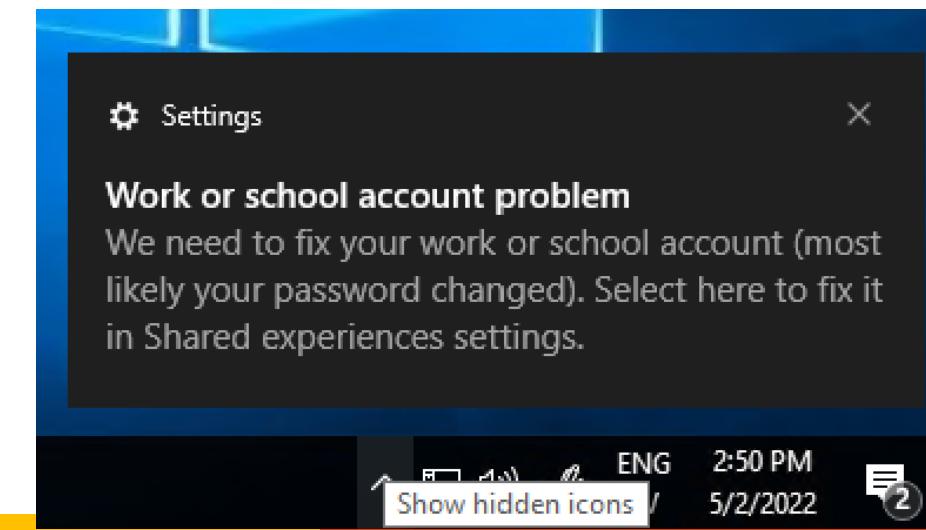




Subscription based activation

www.wpninjas.eu

- Easiest way of upgrading to Enterprise from pro
- Re-activated every 30 days
- Blocked by 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.
- Exclude **Universal Store Service APIs and Web Application** from your Conditional access framework.





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

Selected items

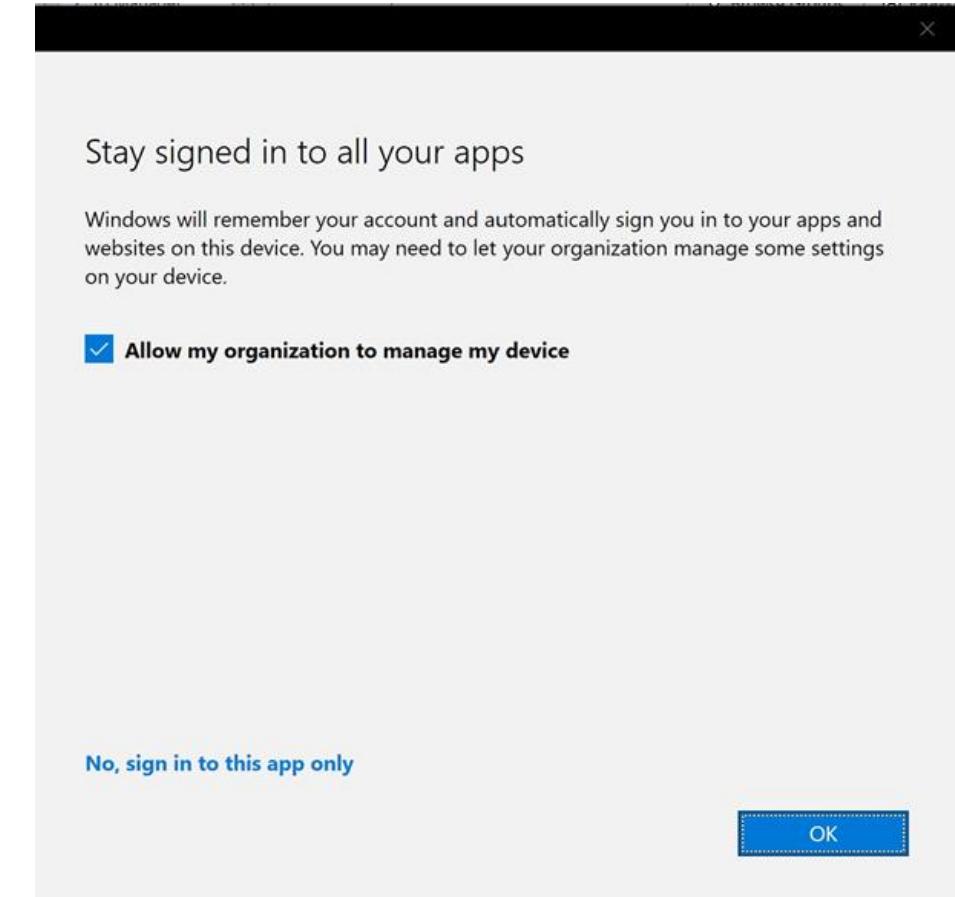
MA	Microsoft Activity Feed Service d32c68ad-72d2-4acb-a0c7-46bb2cf93873	Remove
MC	Microsoft Command Service 19686ca6-5324-4571-a231-77e026b0e06f	Remove
MD	Microsoft Device Directory Service 8f41dc7c-542c-4bdd-8eb3-e60543f607ca	Remove
US	Universal Store Service APIs and Web 45a330b1-b1ec-4cc1-9161-9f03992aa49f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



Stay signed in to all your apps = Evil

www.wpninjas.eu

- “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

www.wpninjas.eu

- 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"] (Correlation ID: 00000000-0000-0000-0000-000000000000), 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/>



Subscription based activation

www.wpninjas.eu

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

A screenshot of a Windows activation window titled "Windows". It displays the following information:

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

Below the window, a tooltip provides more 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)



Blocking Workplace join

www.wpninjas.eu

Create profile ...

Windows 10 and later - Settings catalog (preview)

Basics Configuration settings Assignments Scope tags

+ Add settings

Settings

Allow Workplace ⓘ Block

Settings picker

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

Search

workpla

Add filter

Browse by category

Administrative Templates\Start Menu and Taskbar

Administrative Templates\System\Group Policy

Settings

1 results in the "Settings" category

Select all these settings

Setting name

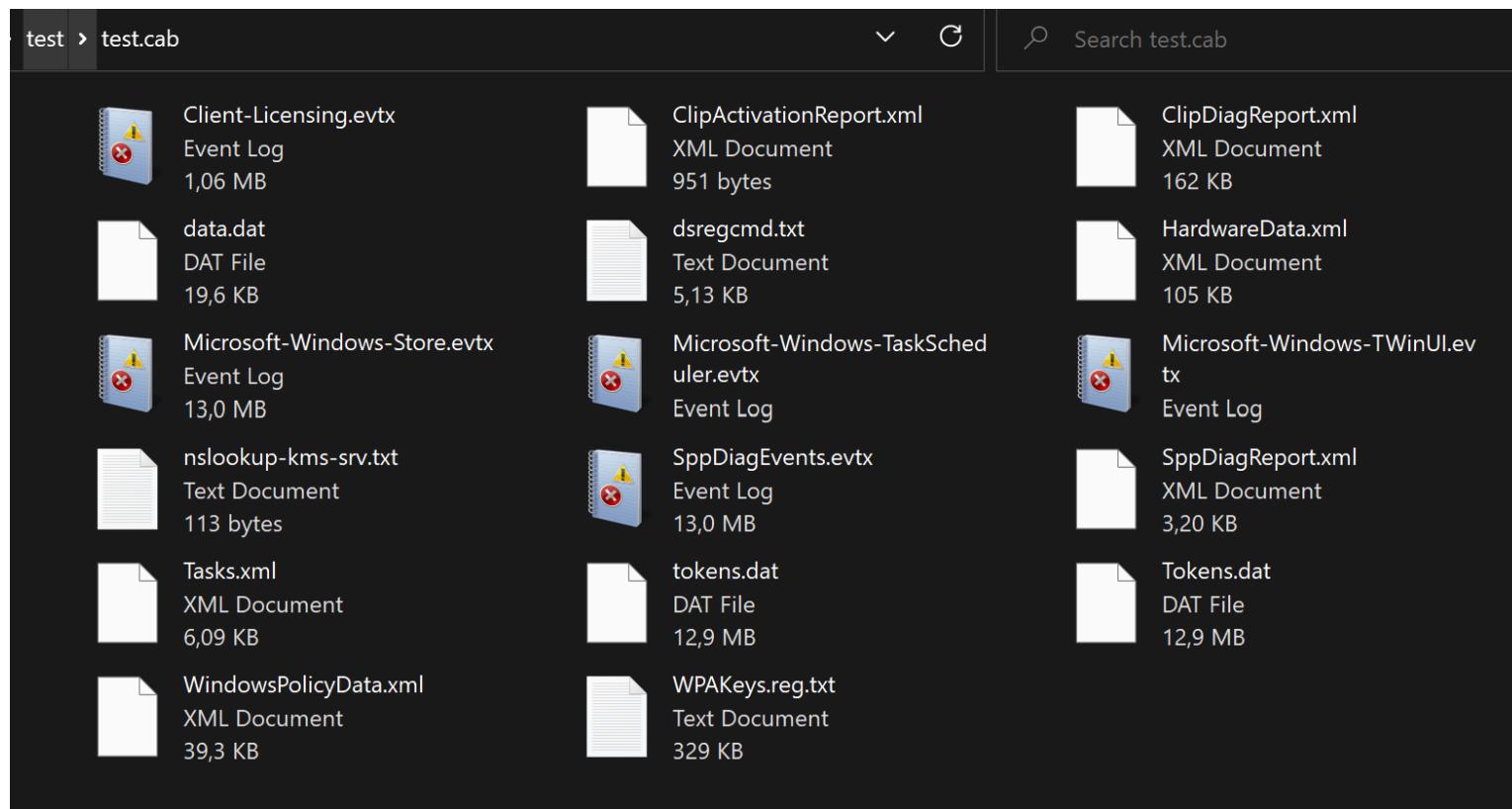
Allow Workplace ⓘ



Collecting information

www.wpninjas.eu

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



Enrollment





Troubleshooting Windows enrollment

www.wpninjas.eu

- 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

www.wpninjas.eu

- 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 user 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

www.wpninjas.eu

- 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”

www.wpninjas.eu

- 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

www.wpninjas.eu

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



DeviceCapReached = Device Limits

www.wpninjas.eu

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'.

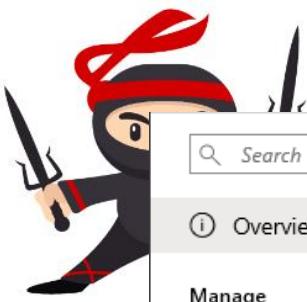
More information: <https://www.microsoft.com/aadjerrors>



Client Health

www.wpninjas.eu

- 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.



X Retire ⚡ Wipe 🗑 Delete 🔒 Remote lock Sync 🔑 Reset passcode ⚡ Restart ⚡ Fresh Start ⚡ Autopilot Reset ⚡ Quick scan

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Recovery keys

Managed Apps

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 device and running a supported version.

Last Configuration Manager agent check in time

05-06-2019 15:10:12

Intune managed workloads

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

Troubleshooting Policies





Configuration Policies

www.wpninjas.eu

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

www.wpninjas.eu

- 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

www.wpninjas.eu

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
- VirtulizationBasedIsolation

ExploitGuard

Feedback

si

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

General Triggers Actions Conditions Settings History (disabled)

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

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



Intune notifications / Sync immediately

www.wpninjas.eu

- 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

www.wpninjas.eu

- 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

www.wpninjas.eu

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

The screenshot shows a web-based diagnostic report interface. At the top, there's a back arrow labeled "Settings" and window control buttons (minimize, maximize, close). Below that, the text "Managed by APENTO" is displayed next to a house icon. Underneath, it says "Advanced Diagnostic Report". A message reads: "Your IT or support person may want additional information to help with troubleshooting." At the bottom left, there are two buttons: "Create report" (highlighted with a red arrow) and "Get help".



Managed policies

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

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



Intune Troubleshooting Pane

www.wpninjas.eu

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** Intune license Principal name rop@apento.com Group memberships (16) Show all

Change user

2 devices noncompliant Email rop@apento.com

Assignments

Assignment	Name	OS	Type	Last
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 type	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-NIIRT6B	Intune	AzureAD	Corporate	Yes	Yes	pending
Ronni'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?

www.wpninjas.eu

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

The screenshot shows the Windows Event Viewer interface. On the left, there's a navigation pane with a tree view of event sources. The 'Admin' source under 'DeviceManagement-Enterprise-Diagnostics-Provider' is expanded, showing categories like Admin and Operational. The main pane displays a table of events. The table has three columns: Level, Date and Time, and Source. Most events are of level 'Information' and occurred at 13-08-2019 09:41:10. One event is highlighted in blue, showing an 'Error' level log at 13-08-2019 09:41:11. The source for all events is 'DeviceManagement-Enterprise-Diagnostics-Pro...'. A cursor arrow is visible at the bottom center of the table area.

Admin Number of events: 1.588		
Level	Date and Time	Source
Information	13-08-2019 09:41:51	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:51	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:51	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:50	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:50	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:50	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:48	DeviceManagement-Enterprise-Diagnostics-Pro...
Error	13-08-2019 09:41:11	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:11	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:11	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:10	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:08	DeviceManagement-Enterprise-Diagnostics-Pro...



Enable debug mode

www.wpninjas.eu

The screenshot shows the Windows Event Viewer interface. The 'View' menu is open, with 'Show Analytic and Debug Logs' selected. The main pane displays event logs for the 'Admin' source. The table has columns for Level, Date and Time, and Source. Most events are 'Information' level, occurring at 13-08-2019 09:41:51. There are also four 'Error' level events at 13-08-2019 09:41:11.

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

Intune Management Extension





Intune Management Extension

www.wpninjas.eu

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





Intune Management Extension Event log

www.wpninjas.eu

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

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists various Windows services and providers. A red box highlights the 'DeviceManagement-Enterprise-Diagnostics-Provider' node under 'Admin'. An arrow points from this node to the main log viewer on the right. The log viewer title bar says 'Admin Number of events: 1.792' and 'Filtered: Log: Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin; Levels: Critical, Error,'. The main pane displays a table of errors, with the last entry highlighted by a red box and a blue callout bubble pointing to it, containing the text 'Look for event id 1924'. The details pane at the bottom shows the error message: 'EnterpriseDesktopAppManagement CSP: An application install has failed. Examine the MSI log (C:\WINDOWS\system32\config\systemprofile\AppData\Local\mdm\093ea47b-ef2c-4f46-a022-6f57a50e39a2.log) for more details. Install command: ("C:\WINDOWS\system32\msiexec.exe" /quiet /I "C:\WINDOWS\system32\config\systemprofile\AppData\Local\mdm\093ea47b-ef2c-4f46-a022-6f57a50e39a2.log" /qn /I "C:\WINDOWS\system32\config\systemprofile\AppData\Local\mdm\{B9BDE5CE-DD33-4D55-A992-A874F601627D}.msi"), MSI ProductCode: 093ea47b-ef2c-4f46-a022-6f57a50e39a2, User SID: (S-0-0-0000000000-0000000000-0000000000-0000), Result: (Fatal error during installation.).'

Level	Date and Time	Source	Event ID	Task Ca...
Error	04/02/2020 17.02.45	Device...	404	None
Error	04/02/2020 09.38.12	Device...	404	None
Error	04/02/2020 09.36.49	Device...	404	None
Error	04/02/2020 04.45.16	Device...	404	None
Error	04/02/2020 01.02.38	Device...	404	None
Error	03/02/2020 17.02.42	Device...	404	None
Error	03/02/2020 16.04.37	Device...	1903	None
Error	03/02/2020 16.04.32	Device...	1903	None
Error	03/02/2020 12.25.21	Device...	404	None
Error	03/02/2020 12.22.39	Device...	404	None
Error	03/02/2020 12.02.23	Device...	404	None
Error	03/02/2020 12.00.37	Device...	404	None
Error	03/02/2020 11.59.50	Device...	454	None
Error	03/02/2020 11.59.43	Device...	1924	None



Intune Management Extension File System

www.wpninjas.eu

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	

File Home Share View

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

50 items



Intune Management Extension Log files

www.wpninjas.eu

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

A screenshot of a Windows File Explorer window titled 'Logs'. The address bar shows the path: This PC > Local Disk (C:) > ProgramData > Microsoft > IntuneManagementExtension > Logs. The file list displays four log files:

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

www.wpninjas.eu

- Yellow: IME Root Registry Key
- Green: Azure AD Object ID of the User
- Red: Application / Policy GUID

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\Polices`. The right pane shows a table of registry values for the selected key.

Selected Key: `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	9t14ElVlp1sII\$JA3/Viu3D0llsfk/HLLxCKM5VOJE=
Result	REG_SZ	Success
ResultDetails	REG_SZ	My super advanced PowerShell script has executed!

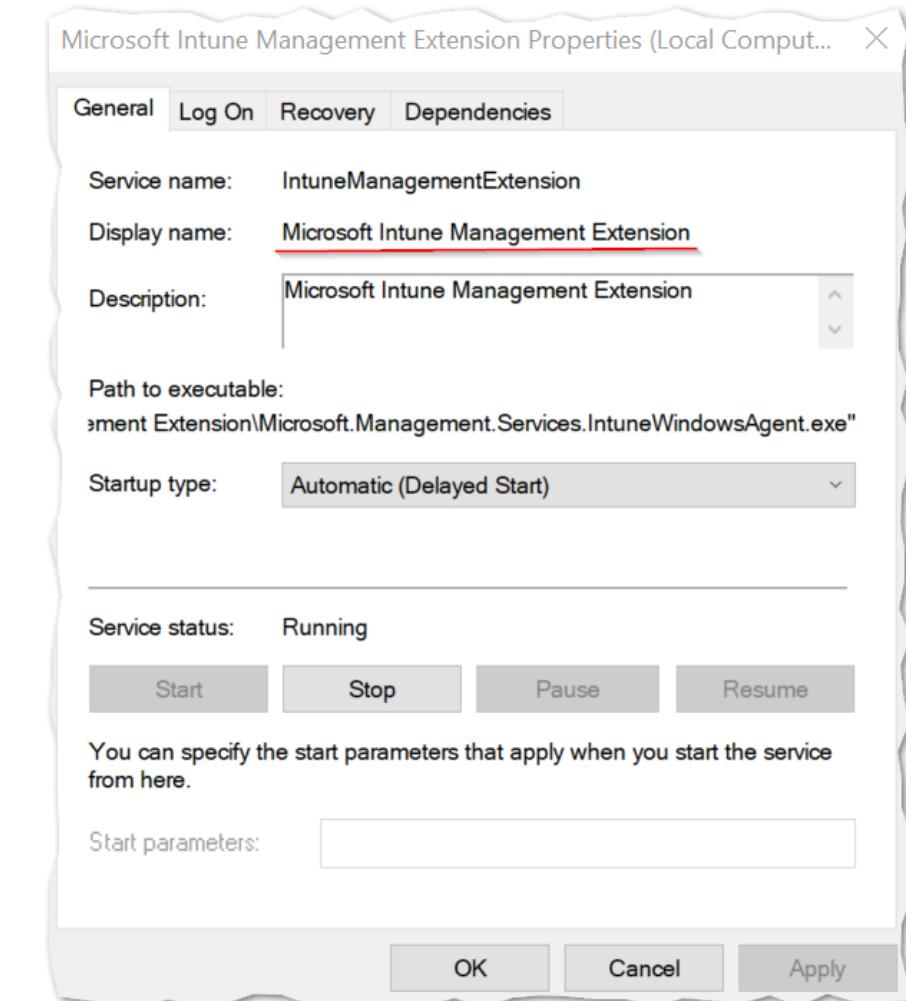


Intune Management Extension

www.wpninjas.eu

- 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

www.wpninjas.eu

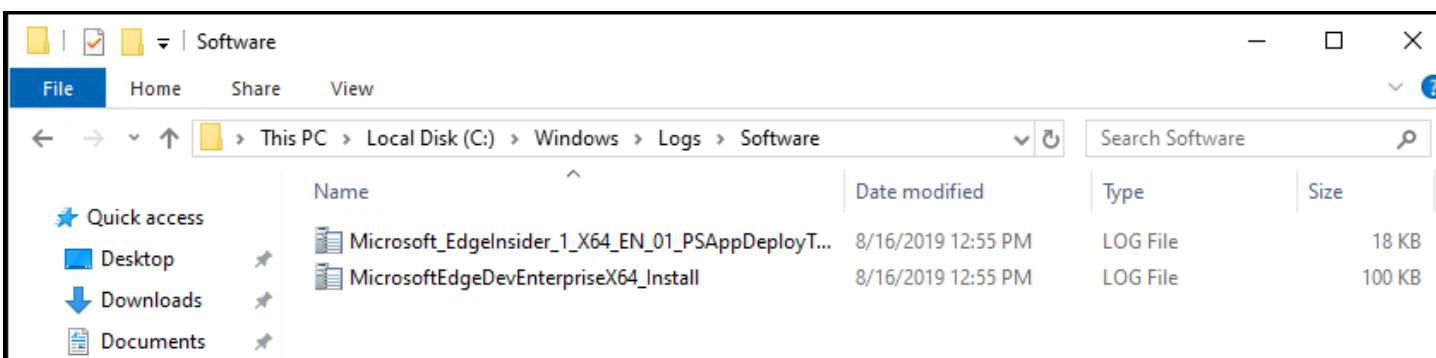
- **Easy To Use** – Any PowerShell beginner can use the template!
- **Consistent** – Consistent look and feel for all application deployments.
- **Powerful** – install/uninstall, setting registry keys, copying files, etc.
- **User Interface** – Custom dialogs boxes, progress dialogs and balloon tips.
- **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



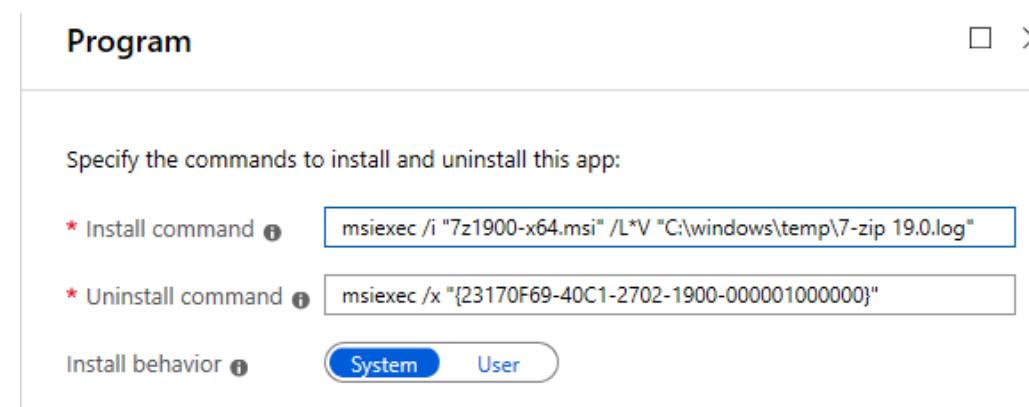
Use the tools you know

www.wpninjas.eu

- PS App Deployment Toolkit logging example:



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



Windows AutoPilot

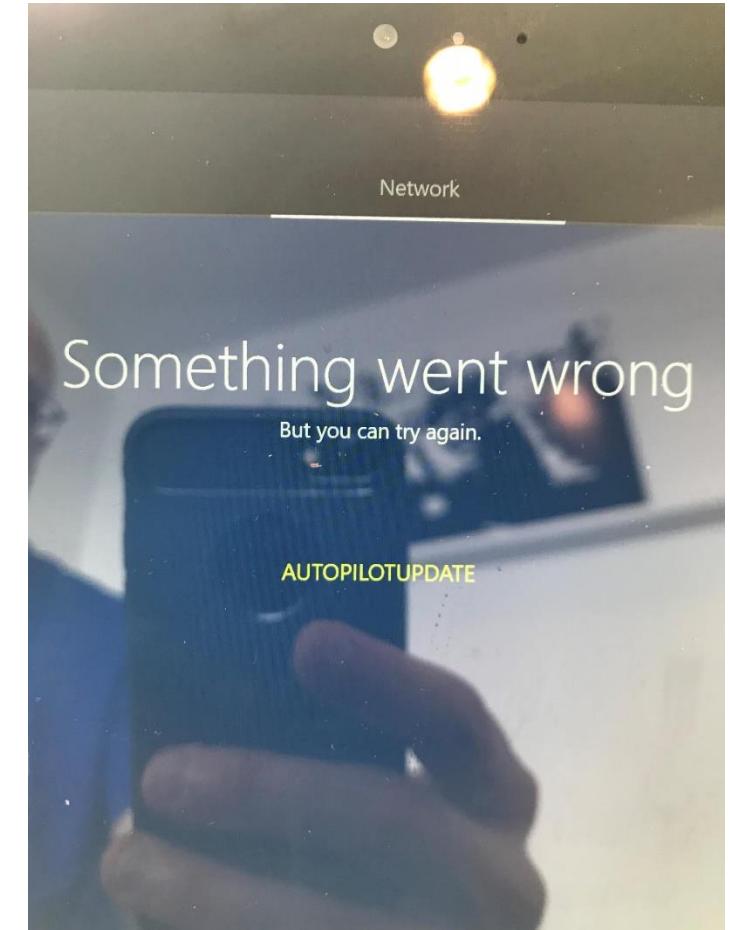




Network

www.wpninjas.eu

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





Meet BOB – your new network admin

www.wpninjas.eu





Network issues – we have seen

www.wpninjas.eu

- “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

www.wpninjas.eu

- 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

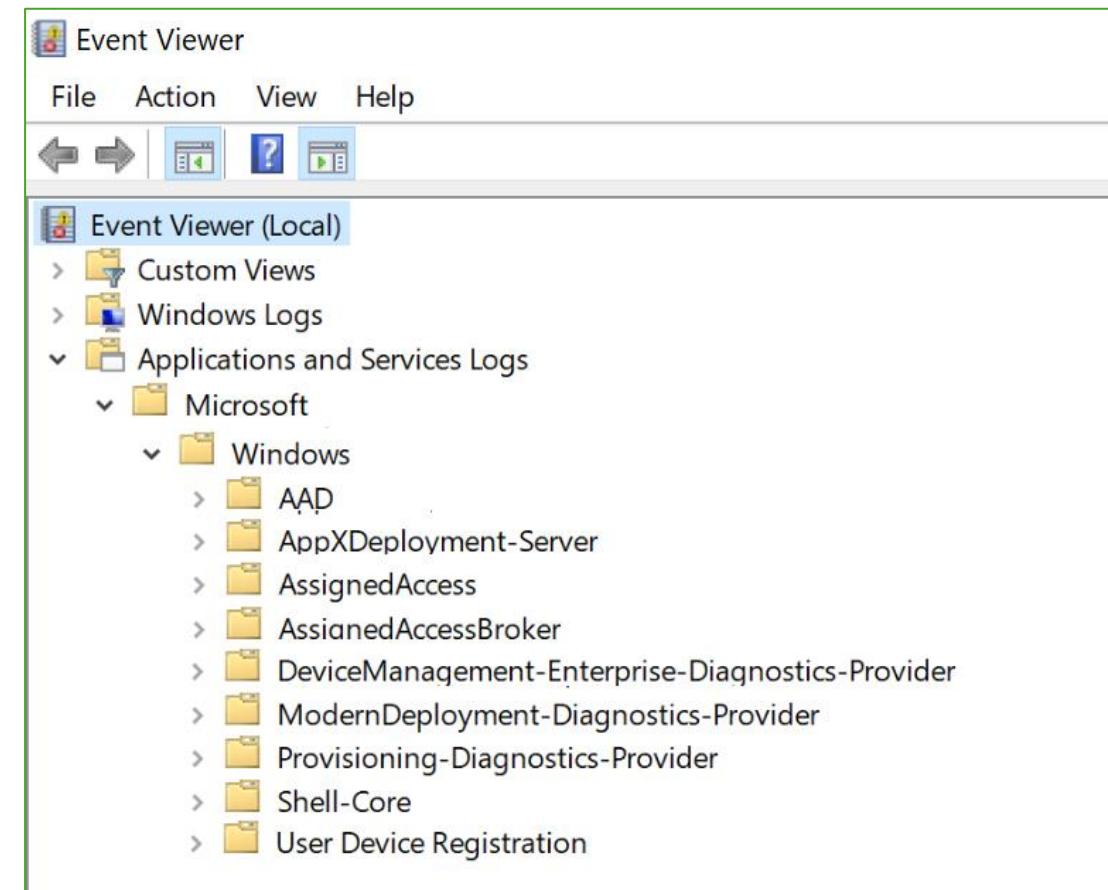




Troubleshooting

www.wpninjas.eu

- 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

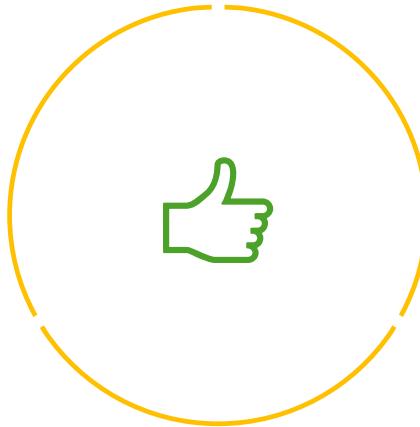
✓ Device-Targeted Network Profiles
Installation

✓ Device-Targeted Certificates
Installation

⚠ User-Targeted Apps Installation

Close

Export logs



Thank You



Workplace Ninja Summit 2022