NIC

EMPOWER

November 13-15, Oslo Spektrum

Jörgen Nilsson & Ronni Pedersen

Unlocking the Secrets of Intune Troubleshooting A Deep Dive into Mastery

About me..

Jörgen Nilsson
- Principal Consultant, Onevinn
- Microsoft MVP: Security
- Microsoft Certified Trainer (MCT)

Contact Info
- Mail: Jorgen.nilsson@onevinn.se
- X: @ccmexec

NIC
EMPOWER

About me…

Ronni Pedersen

- Cloud Architect, APENTO
- Microsoft MVP: Security + Windows
- ITIL Certified
- Microsoft Certified Trainer (MCT)

Contact Info

- Mail: rop@apento.com
- Twitter (X): @ronnipedersen

NIC
EMPOWER

APENTO

Troubleshooting has changed

Troubleshoot Legacy client

- Configuration Manager
    - Many, many log files
    - Complex
- Group Policies
    - Gpresult
    - GPupdate

Troubleshoot Modern Client

- Event log
- Registry keys
    - Autopilot
    - PolicyManager
- IME log files
- M365 Apps Polices
- Edge Policies

From servicedesk ticket:
"*I have attached GPResult report from the machine*"

NIC
EMPOWER

Intune Policies

Configuration Policies

Recommended order for Windows devices
- Security Baselines (if required)
- Endpoint Security
- Settings Catalog
- Templates
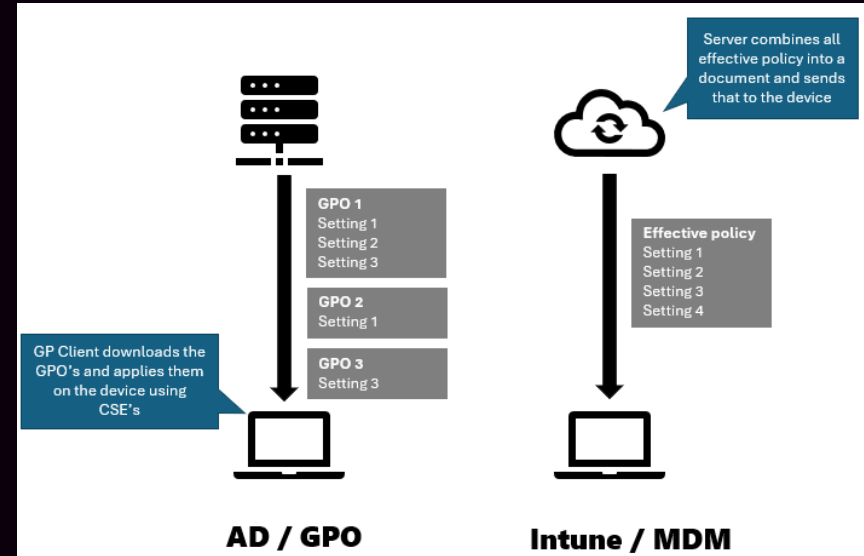- Custom ADMX ingestion (3rd. Party apps)
- PowerShell Scripts

Optional:
- Proactive Remediation
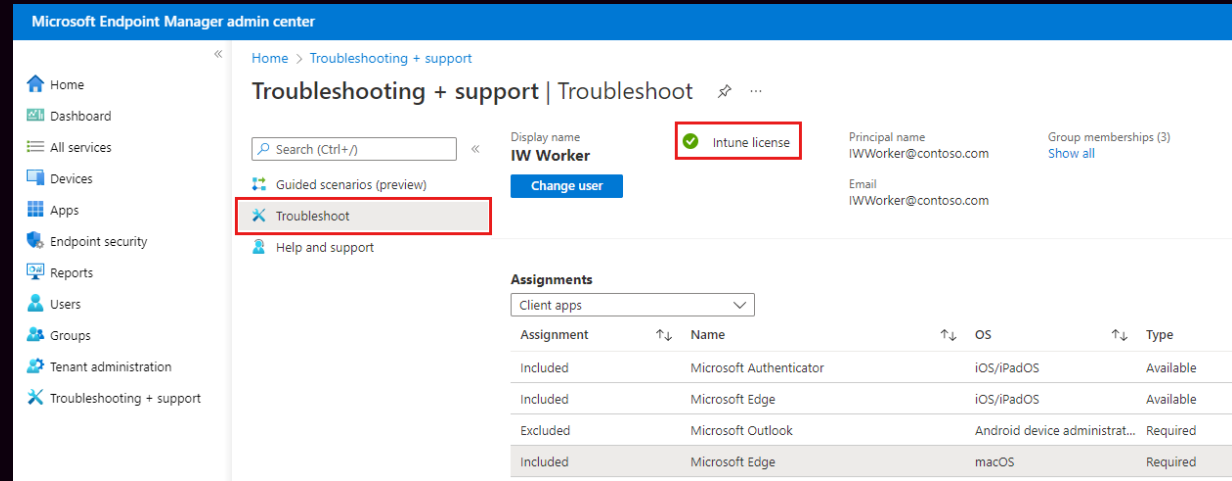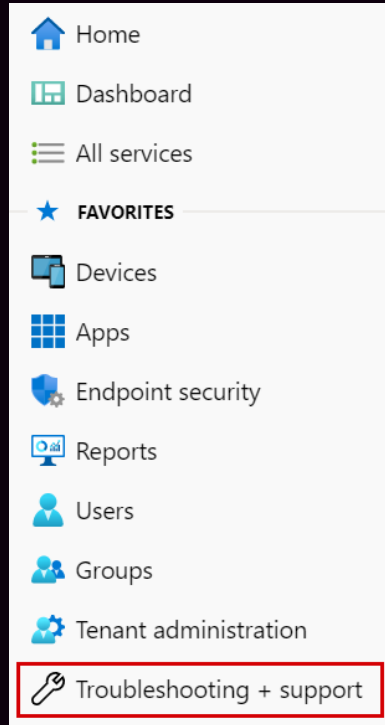 Note: Requires Windows Enterprise E3

Intune policy

- Intune policies are processed in the cloud
- Group Policies are processed on the client
  - Local Policy
  - Site
  - Domain
  - OU
- We can have different values at different levels to handle exclusions
- That is not possible with Intune Policies

Use the built-in Troubleshoot pane

Troubleshooting

- Collect log files using Intune
- MDMDiagnosticsTool
- Settings -> Access work or school

https://learn.microsoft.com/en-us/windows/client-management/mdm-collect-logs

Advanced Diagnostic Report

Your IT or support person may want additional information to help with troubleshooting.

Create report

Name		Date modified
DeviceManagement-Enterprise-Diagn...		2024-04-25 12:54
MDMDiagReport		2024-04-25 12:54
MDMDiagReport.xml		2024-04-25 12:54
Microsoft-Windows-AAD		2024-04-25 12:54
Microsoft-Windows-Shell-Core		2024-04-25 12:54

Retire   Wipe   Delete   Remote lock   Sync   Reset passcode   Restart   Collect diagnostics

**Collect diagnostics - W11DELL01**

Intune will attempt to collect the diagnostics that are on this device. To download and view the diagnostics, go to Monitor > Device diagnostics. Continue with diagnostics collection?

Yes   No

Build your own log collection tool

- Why? Builtin to slow, to much data
- Remediation script send to azure storage, sharepoing, teams
- Fast runs in a couple of minutes
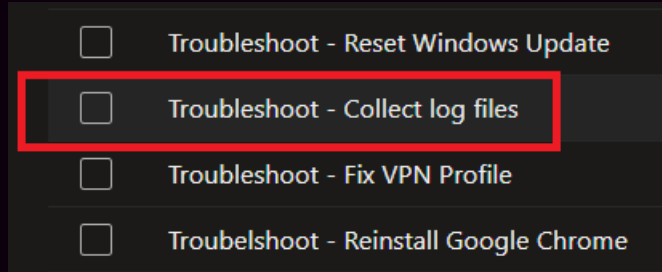
[Using on-demand Remediation to collect all logs you want on Intune devices | Syst & Deploy](#)

NIC
EMPOWER

Intune Device Details GUI – Petri Paavola

- Shows relevant device info
- Targeted apps and configuration profiles
- Including how Apps and Configuration Profiles are targeted
- Autopilot information
- Version 3.0 +Remediation scripts
- And much more

https://github.com/petripaavola/IntuneDeviceDetailsGUI

NIC EMPOWER
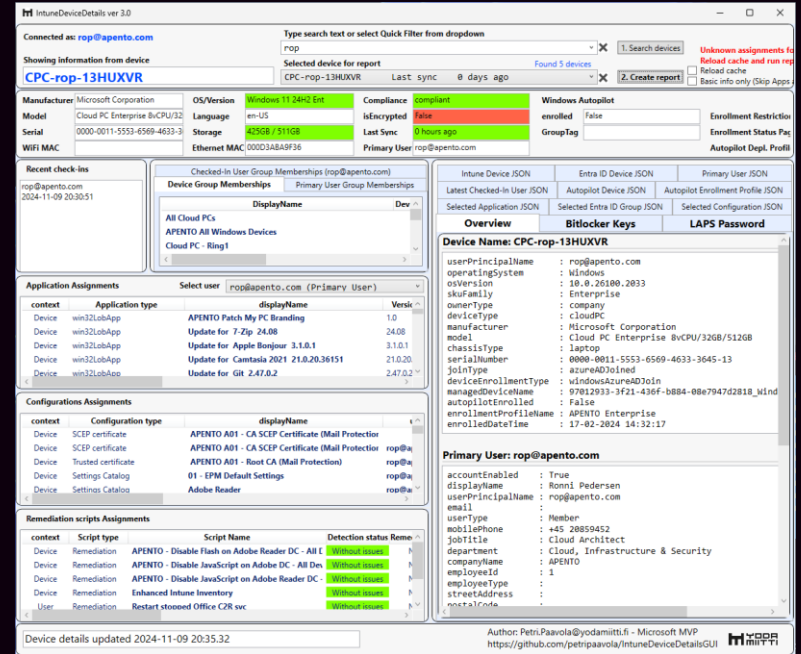
SyncMLViewer

- Tool Author:
  Oliver Kieselbach([@okieselb](https://github.com/okieselbach))
  - https://github.com/okieselbach/SyncMLViewer
- Easily troubleshoot the SyncML stream
- MDM & MMP-C Sync
- Run MDMDiagnosticstool
- Open registry
- Connection profiles
- Available in WinGet repo!
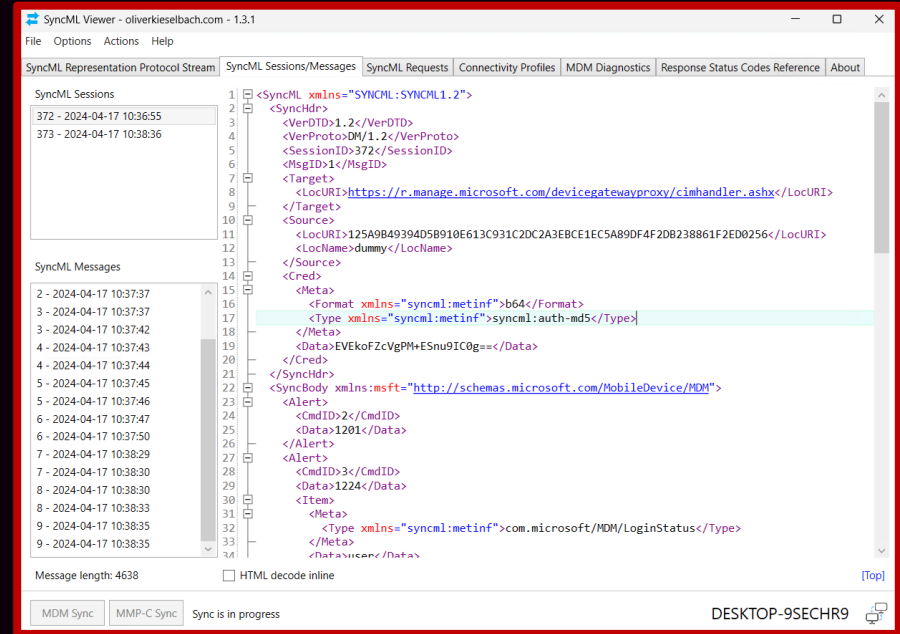
Policy/Profile Conflicts

- Intune policies are compiled server side.
- 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.

NIC
EMPOWER

Removing a policy (Policy Tattoo)

- Does not necessarily change the value back, depends on the CSP

> ⓘ **Note**
>
> When a profile is removed or no longer assigned to a device, different things can happen, depending on the settings in the profile. The settings are based on CSPs, and each CSP can handle the profile removal differently. For example, a setting might keep the existing value, and not revert back to a default value. The behavior is controlled by each CSP in the operating system. For a list of Windows CSPs, see **configuration service provider (CSP) reference**.
>
> To change a setting to a different value, create a new profile, configure the setting to **Not configured**, and assign the profile. Once applied to the device, users should have control to change the setting to their preferred value.
>
> When configuring these settings, we suggest deploying to a pilot group. For more Intune rollout advice, see **create a rollout plan.**

https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign

NIC
EMPOWER

Microsoft Policy Migration

Please see below for details on each template's migration experience and note that these are subject to change as migration efforts develop. We'll provide updates to this post as needed:

- **Delivery optimization:** This template can still be configured in the same location.
- **Identity protection (Account protection):** This template will be moving to the Endpoint security blade.
- **Microsoft Defender for Endpoint (EDR):** This template can still be configured in the same location.
- **Device restrictions (Windows 10 Team):** This template can still be configured in the same location.
- **Network boundary:** This template will no longer be available. Settings in this template can be configured via settings catalog only. Migrated policies will show 'Settings catalog' as the policy type.
- **Device restrictions:** This template will no longer be available. Settings in this template be configured via settings catalog only. Migrated policies will show 'Settings catalog' as the policy type.
- **Administrative templates:** This template will no longer be available. Settings in this template can be configured via settings catalog only. Migrated policies will show 'Settings catalog' as the policy type.
- **Kiosk:** This template can still be configured in the same location.
- **Custom OMA-URI:** This template will still be available, but only settings that do not exist in the settings catalog can be configured via custom OMA URI. This change will happen in a phased approach starting in mid-August by blocking the least used settings and in mid-September slowly expand to the remaining settings available in settings catalog.
- **Domain join:** To be determined.
- **Edition upgrade and mode switch:** To be determined.

https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-windows-device-configuration-policies-migrating-to/ba-p/4189665

Message Center

Timing when removing a user policy

- Removing a user from an Entra ID group with a policy assigned to it.

- A profile applies to a user group. Later, a user is removed from the group. For the settings to be removed from that user, it can take up to 7 hours or more for:
  - The profile to be removed from the policy assignment in the Intune admin center
  - The device to sync with the Intune object using the platform-specific policy refresh cycle (in this article)

https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

Compliance Policy in error state

- New behavior since May.
- A device in error state will become non-compliant after 7 days

Device status

⊘ Can't access company resources

This device does not meet Onevinn compliance and security policies. You need to make some changes to this device so that you can access company resources.

Device must have firewall enabled.   Less ∧

   This device must have the firewall enabled. Contact your IT administrator for help.

Setting	State	State details
Firewall	⊗ Error	2016345612(Syncml(500): The recipient encountered an unexpected condition which prevented it from fulfilling the request)

organization's support.

Sync

Check access

NIC
EMPOWER

Policies to keep an eye on!

- Credential guard – Intune sets the Configured value
- Need to make sure it is running
  - Defender for Endpoint
  - Remediation

Kernel DMA Protection	On
Virtualisation-based security	Running
Virtualisation-based security required security properties	Base Virtualisation Support, Secure Boot
Virtualisation-based security available security properties	Base Virtualisation Support, Secure Boot, DMA Protection, Secure Memory Overwrite, UEFI Code Readonly
Virtualisation-based security services configured	Credential Guard, Hypervisor enforced Code Integrity, Secure Launch
Virtualisation-based security services running	Hypervisor enforced Code Integrity, Secure Launch
Windows Defender Application Control policy	Enforced

NIC
EMPOWER

Policies that causes a reboot during Autopilot

Main issue: Security Baselines (Device target)

Solution: Target them to users

- Device Lock
- DMA Guard
- Credential Guard
- VBS
- Lock Screen

Configuration settings Edit

∨	Administrative Templates
∨	Device Guard
∨	Device Lock
∨	Dma Guard
∨	Virtualization Based Technology

MDMWinsOverGPO (Hybrid-only)

- Only applicable to the Policy CSP!

> ⓘ **Note**
>
> MDMWinsOverGP only applies to policies in Policy CSP. MDM policies win over Group Policies where applicable; not all Group Policies are available via MDM or CSP. It does not apply to other MDM settings with equivalent GP settings that are defined in other CSPs such as the **Defender CSP**.

Policy Manager

- Registry location for all policies coming from MDM

- Ingested ADMX files

- Current values

- For ADMX backed polices -> Policymanager -> Polices values
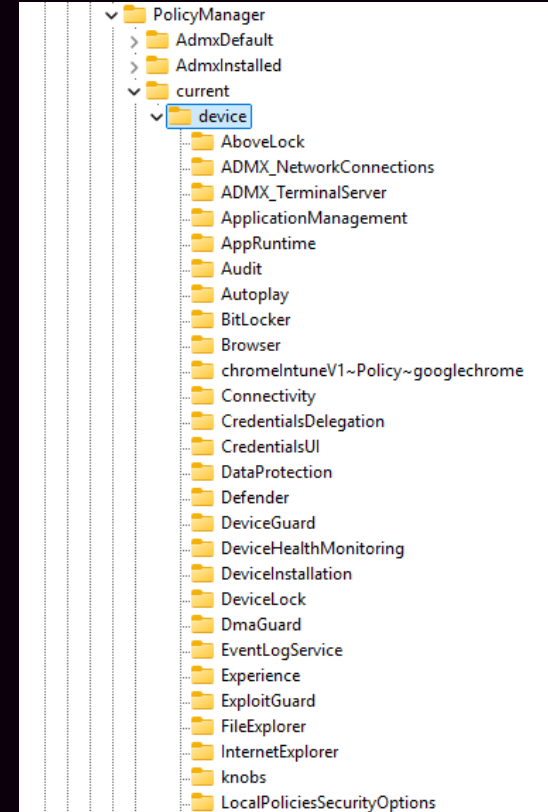
Config Refresh

- A reset operation to reset any settings you manage which use the Policy CSP

- Configuration options to allow reset of managed settings to take place as frequently as every 30 minutes

- Offline functionality, not requiring connectivity to an MDM server

- Ability to pause Config Refresh for troubleshooting purposes with automatic resume after 24 hours

Important: Config Refresh is designed to work with MDM policies managed by the Policy CSP. Some policies, notably the BitLocker CSP, will also adhere to Config Refresh enablement. Other policies are outside of this scope, such as Firewall, AppLocker, PDE, and LAPS.

NIC
EMPOWER

DEMO (Fast version 😎)

Edge Policies

Microsoft Edge policies

- Microsoft Edge management service
- Enrollment token or user targeting
- Default: MDM/GPO Windows over Edge Polices
- EdgeManagementPolicyOverridesPlatformPolicy
- Multiple policies = highest priority wins
- Edge://Policies

> ⓘ **Note**
>
> Any policies you apply with Microsoft Edge management service will be overridden if they conflict with an existing Group Policy Object (GPO) or Mobile Device Management (MDM) policy that's set on the device.

Windows Security Zones

- Security Zones
  - Local Machine, Local Intranet, Trusted, Internet, and Restricted Sites.
- Someone at Microsoft "forgot" to document that this policy is limited to 200 entries
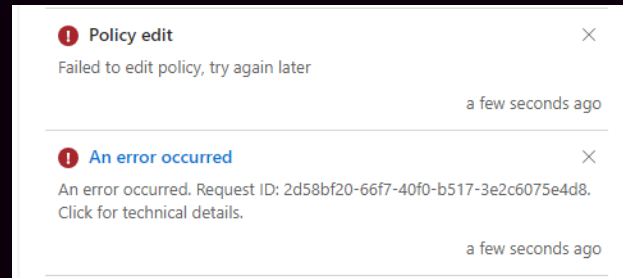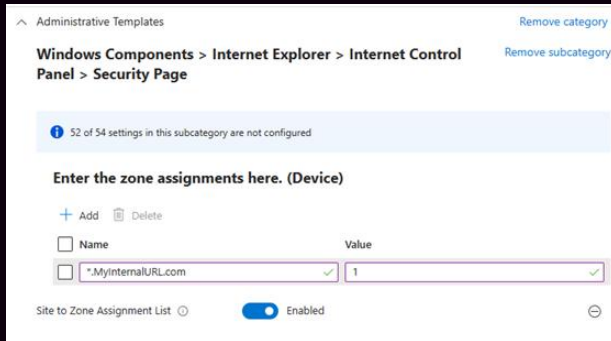
Microsoft 365 Apps Policies

Microsoft 365 apps policies

- Cloud Policy service for Microsoft 365
- A policy configuration can't be applied to volume licensed versions of Office that use Click-to-Run, such as Office LTSC Professional Plus 2021 or Office Standard 2019.
- Policies from Cloud Policy are applied only when the Office app is restarted
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Cloud\Office

NIC
EMPOWER

Windows Updates

Unexpected update to Windows 11 24H2

- Timing issue..
- Before a device is registered in WufBDS, it can install the update

Solution

- Deploy Target Release Version & Product Version using settings catalog och Custom CSP
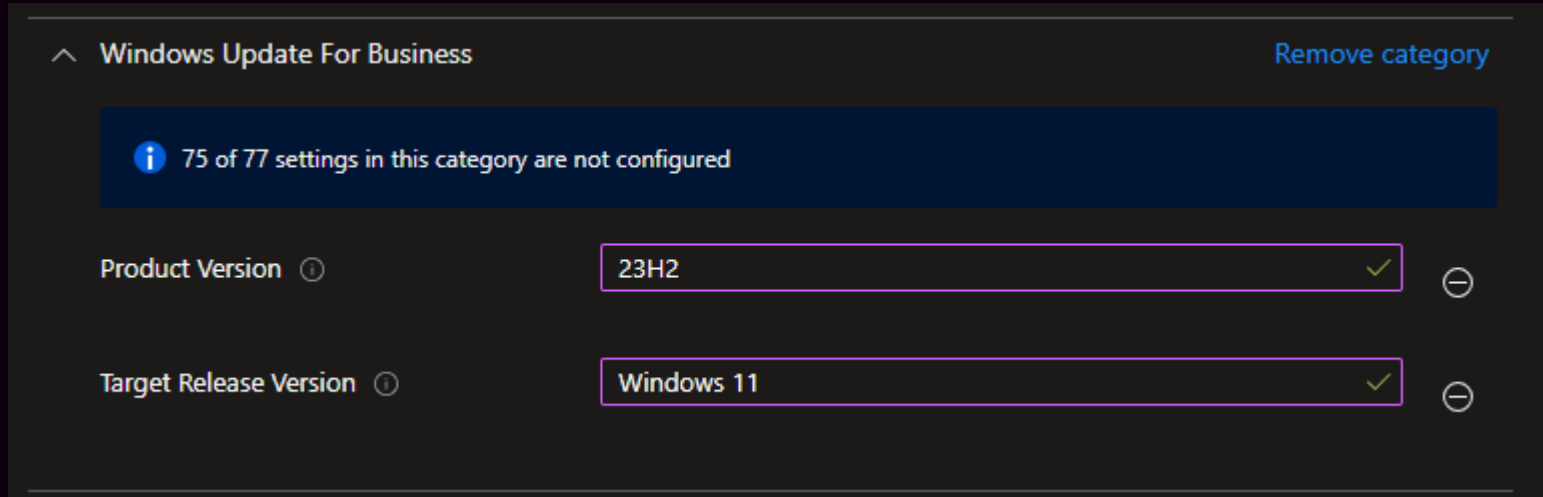
Policies are in a new location

Sense agent not installed in Windows 11 24H2 per default

- A user buys a new device that has the Pro SKU, and the OEM did not install the required feature.

[KB5043950: Microsoft Defender for Endpoint known issue - Microsoft Support](#)

NIC
EMPOWER

Network

SSL traffic inspection = BAD

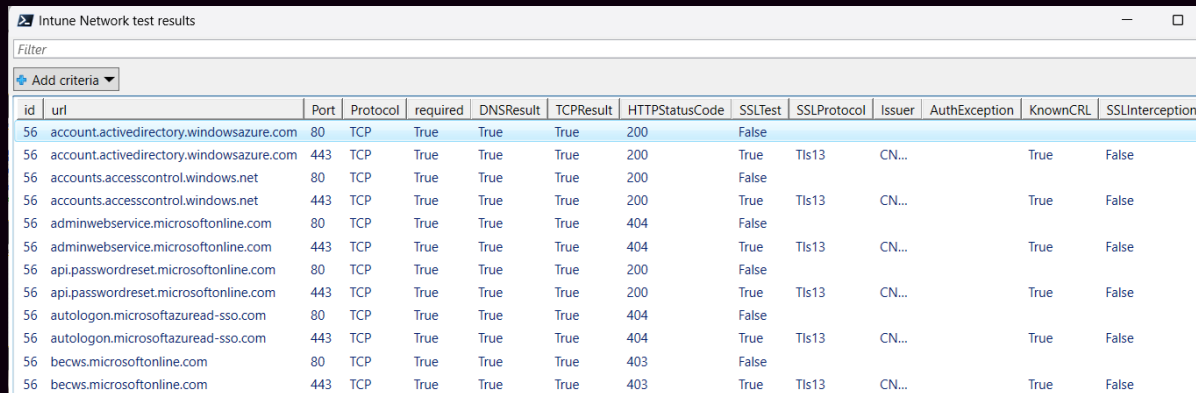- Must exclude necessary endpoints
- Example on results

> ⓘ **Note**
>
> SSL traffic inspection is not supported for 'manage.microsoft.com', 'dm.microsoft.com', or the **Device Health Attestation (DHA) endpoints listed in the compliance section**.

Device name	Managed by ↓	Ownership	Compliance	OS ▽	OS version ▽
5f256f7b-9e37-4824-b5...	Co-managed	Unknown	See ConfigMgr	Windows	0.0.0.0
7ededf06-8c41-4d91-90...	Co-managed	Unknown	See ConfigMgr	Windows	0.0.0.0

NIC
EMPOWER

[Network endpoints for Microsoft Intune | Microsoft Learn](#)

Intune Network Requirements

- By Martin Hinken (more comprehensive than MS..)

- Test network connectivity required by Intune, Autopilot, Device registration, TPM and more..

- Comprehensive tests

[Intune Network Requirements - everything I learned – mAnimA.de](https://mAnimA.de)

Troubleshoot registration

- https://learn.microsoft.com/en-us/samples/azure-samples/dsregtool/dsregtool/

```
=============================================================
        Device Registration Troubleshooter Tool
=============================================================

Please provide any feedback, comment or suggestion

Enter (1) to troubleshoot Microsoft Entra Register

Enter (2) to troubleshoot Microsoft Entra join device

Enter (3) to troubleshoot Microsoft Entra hybrid join

Enter (4) to verify Service Connection Point (SCP)

Enter (5) to verify the health status of the device

Enter (6) to Verify Primary Refresh Token (PRT)

Enter (7) to collect the logs

Enter (Q) to Quit

DSRegTool log file has been created.


Please make a selection, and press Enter:
```

NIC
EMPOWER

Applications

IME - Facts

- Installed when first needed to run (we always need it!)
  - Scripts
  - Remediation scripts
  - Win32App
  - Software Inventory
- IntuneWin32App run as 32-bits, becareful where you put your registry keys
- Syncs every 60 Minutes per default
- Tries to install app 3 times (5 minutes apart) if it fails
- Every 24 hours after that (GRS – Global Reevaluation Scheme)

NIC
EMPOWER

IME – Log files

- C:\ProgramData\Microsoft\IntuneManagementExtension\Logs
  - AgentExecution.log – Log file for PowerShell detection methods
  - ClientHealth.log – Log file for IME health and remediation actions
  - DeviceHealthMonitoring – Log file for Appcrash, app events
  - HealthScripts – Log file for remediation scripts
  - IntuneManagementExtension.log – IME related events, sync
  - **AppWorkload.log – added 2024-08 – App related events**
  - Sensor.log – Log file for subscribed events.
 - AppActionProcessor.log – Log file for AppActions

Content Cache location:

- Win32Apps - C:\Program Files (x86)\Microsoft Intune Management Extension\Content\Incoming\
- Remediation scripts - C:\Windows\IMECache\HealthScripts

NIC.
EMPOWER

Run PowerShell Scripts and Remediat...

```
PowerShell] Script Default Timer is set to 24 hour
Detect whether the managed installer is enabled.
starting task
Win32AppTimer interval is : 3600000 ms
Starting Win32AppOnTimer task...
[EmsAgentService:RequiredAppTask] Device is either not in 'Win 10 S Mode' or not a '19H2 (Win 10 S supported) or later' build.
set timer, delayed seconds = 140 for workload Win32RequiredApp
Starting Available app timer task...
[EmsAgentService:AvailableAppTask] Device is either not in 'Win 10 S Mode' or not a '19H2 (Win 10 S supported) or later' build.
set timer, delayed seconds = 30 for workload Win32AvailableApp
Starting content manager...
```

```
Successfully updated throttling info. workload AgentCheckIn, currentCnt = 4
Finish throttle checking.
[Win32AppInventory] Saving throttle info in inventory flow
[Win32AppInventory] Inventory collector thread starts.
[Win32AppInventory] CollectApplicationInventory starts
[Win32AppInventory] Starting Win32 app inventory collection via WMI (Expanded)
[Win32AppInventory] Id: 0000570fddd7afde62bd641f2d4232008ba90000ffff Name: Notepad++ (64-bit x64) Version: 8.5.7
[Win32AppInventory] Id: 0000f70290ca1beb3a22ec29cc1b41732ae60000ffff Name: Microsoft 365 Apps for enterprise - en-us Version: 16.0.16626.20208
```

NIC
EMPOWER

Registry
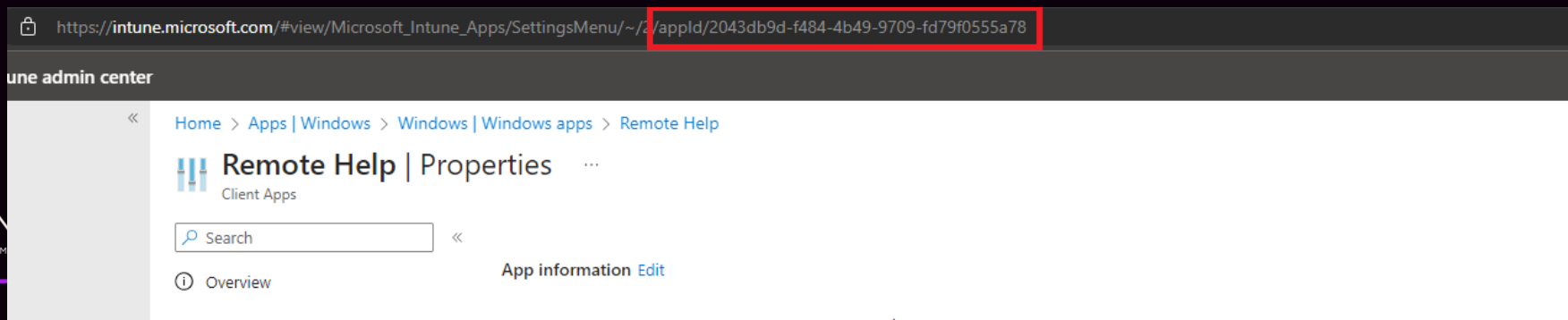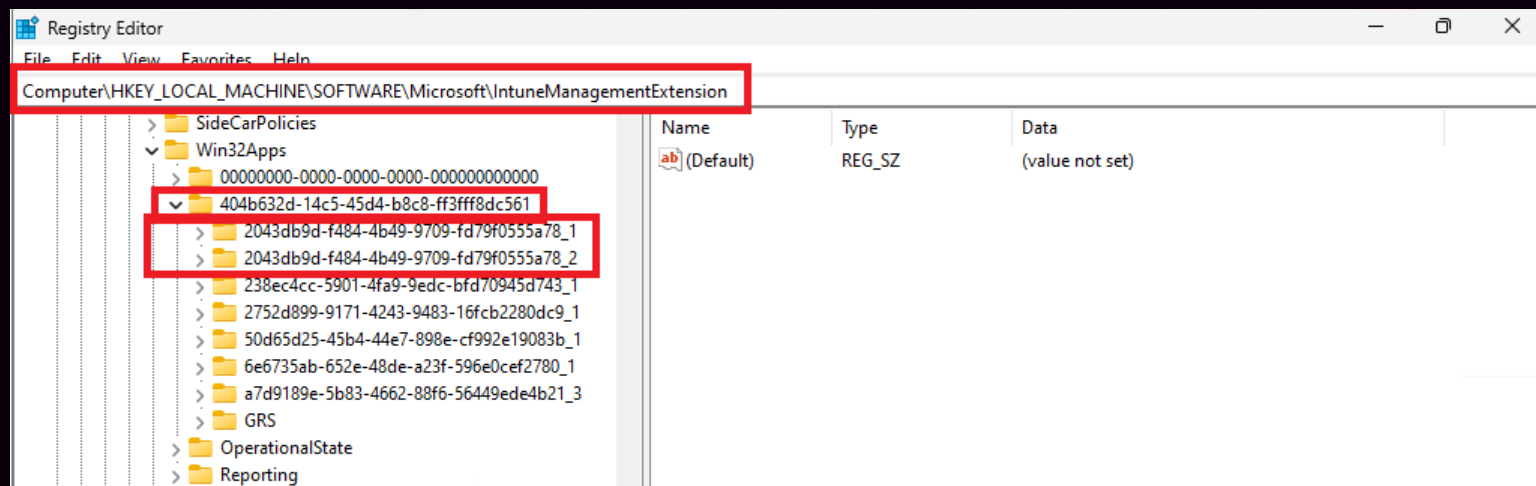
Intune Logreader – Petri Paavola

- Analyzes Microsoft Intune Management Extension (IME) log(s)

- Timeline of events

- Capable LogViewer

- HTML output

- -Online option will get real names for Remediations and PowerShell scripts.

https://github.com/petripaavola/Get-IntuneManagementExtensionDiagnostics

Reinstall app required app using Powershell/remediation

- Remediations on demand is great!

- Powershell script that clears out registry and restarts IME


```
1    #Define variables
2    $AppID = "f3f8ea42-2a57-42e5-999e-399d01337e9b"
3    $MSIProductCode = "{1E06C136-5B6F-4A98-8296-CEFE858DEEE6}"
4
5    try {
6        #Uninstall application
7        Start-Process "C:\Windows\System32\msiexec.exe" -ArgumentList "/x $MSIProductCode /quiet /noreboot" -Wait
8    }
9    catch {
10       $errorMessage = $_.Exception.Message
11       Write-Host $errorMessage
12       exit 1
13   }
14
15   #Clear IME registry values
16   $Regpath = "HKLM:\SOFTWARE\Microsoft\IntuneManagementExtension\Win32Apps"
17   Get-ChildItem -Path $Regpath -Recurse -Exclude "*AppAuthority*" | Where-Object { $_.PSChildName -like "*$AppId*" -or $_.Property -like "*$AppId*" } | Remove-Item -Recurse -Force
18
19   #Restart IME service
20   Restart-Service -Name "IntuneManagementExtension" -Force
21
22   #Exit script
23   Exit 0
24
```

Summary

- Build your own troubleshooting tool set
- Train admins, servicesdesk, site support
- More than Intune polices to troubleshoot going forward
- Keep up with changes coming!

NIC
EMPOWER

Thank you!

NIC
EMPOWER