

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

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](https://twitter.com/ronnipedersen)



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 Policies
- Edge Policies

From servicedesk ticket:

"I have attached GPResult report from the machine"

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

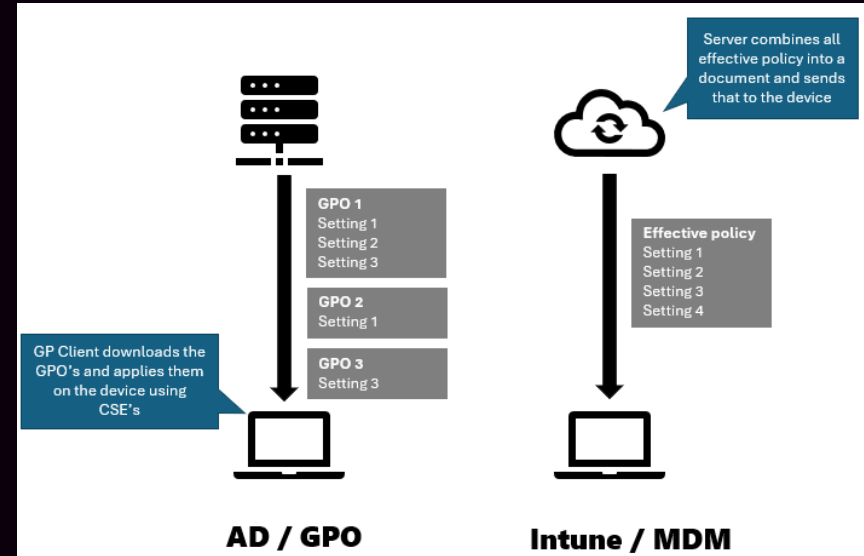
Optional:

- Proactive Remediation
Note: Requires Windows Enterprise E3



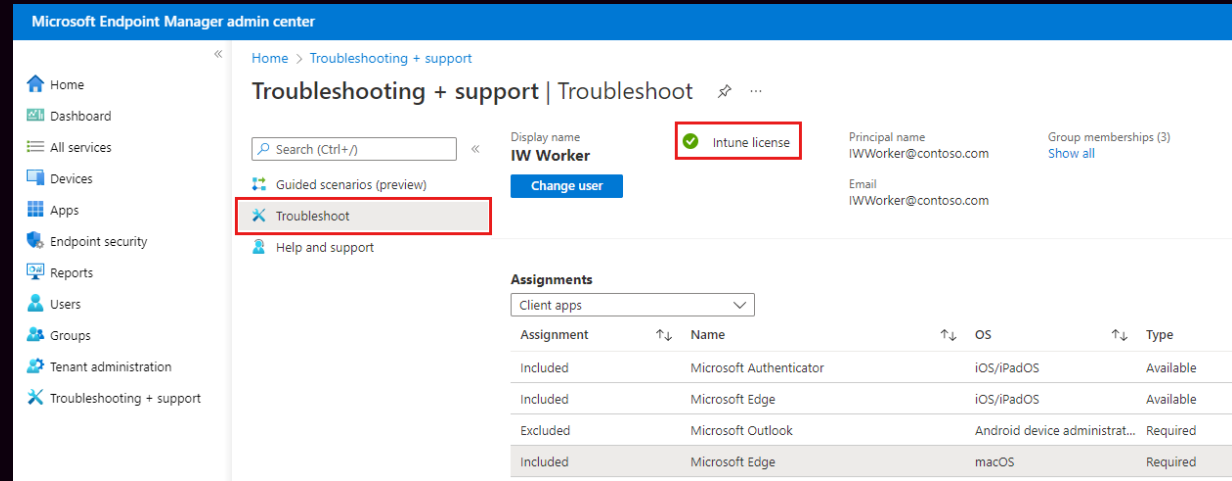
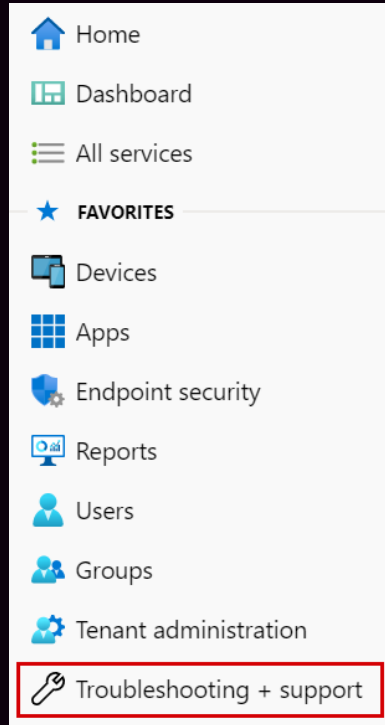
Intune policy

- 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



Troubleshooting 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

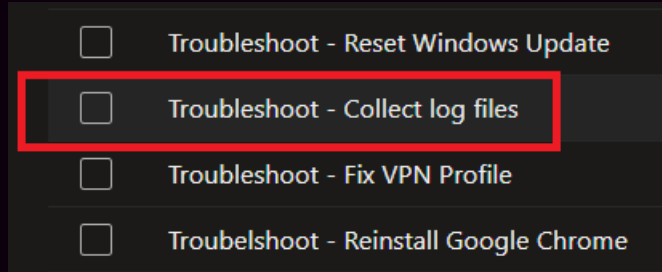
Intune will attempt to collect the diagnostics that are on this device. To download and view the diagnostics, go to Monitor > Device diagnostics. Continue with diagnostics collection?

Yes

No

Build your own log collection tool

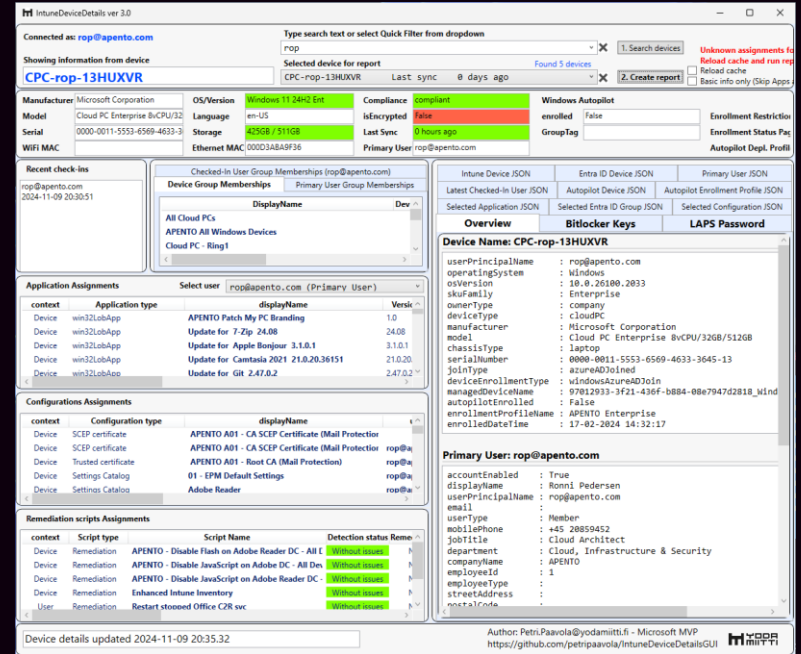
- Why? Builtin to slow, to much data
- Remediation script send to azure storage, sharepoing, teams
- Fast runs in a couple of minutes



[Using on-demand Remediation to collect all logs you want on Intune devices | Syst & Deploy](#)

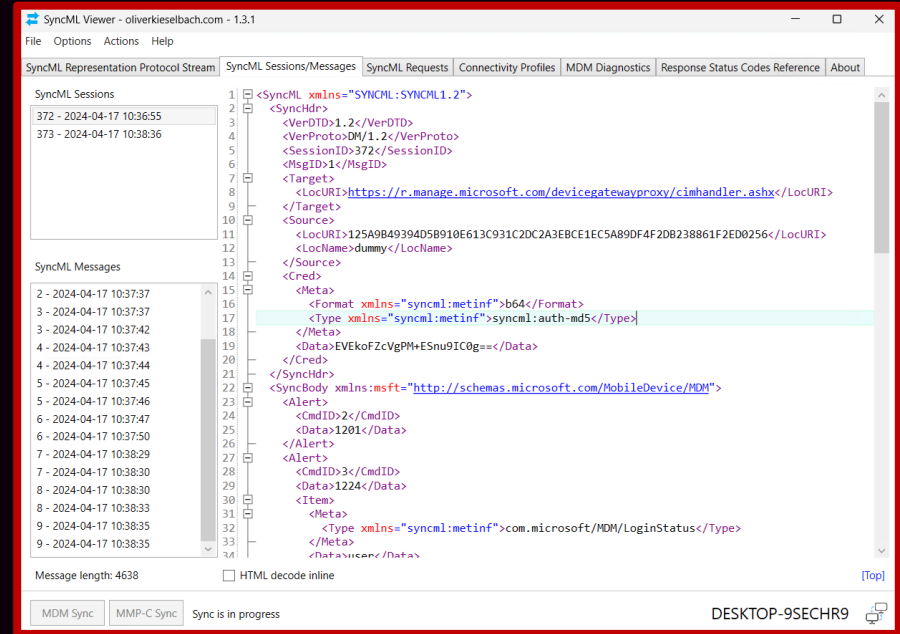
Intune Device Details GUI – Petri Paavola

- 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



SyncMLViewer

- Tool Author:
Oliver Kieselbach([@okieselb](https://github.com/okieselbach/SyncMLViewer))
 - <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.



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](#).

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.



Message Center

Message center

Search ⊞ ⚙️ Add filters

Message title	↑↓ Service	↑↓ Act by	↑↓ Category
Plan for Change: Creation of new Administrative Templates configuration profiles for Windows will not be supported	Microsoft Intune		Plan for change
Microsoft Intune In Development for November 2024 is now available	Microsoft Intune		Stay informed
What's new in the Microsoft Intune Service Update for October 2024	Microsoft Intune		Stay informed
Windows 365 OS Optimization Image Deprecation – Update Your Provisioning Policies to Windows Microsoft 365 ...	Windows 365		Plan for change
Plan for change: Transition to Cloud PC Connection Quality Report	Windows 365		Plan for change
Take Action: Update to the latest Intune App SDK for iOS and Intune App Wrapping Tool for iOS	Microsoft Intune		Plan for change
Microsoft Intune ending support for Android device administrator on devices with GMS access	Microsoft Intune	12/31/2024	Plan for change
What's new in Windows 365 for September 2024	Windows 365		Stay informed

Plan for Change: Creation of new Administr... ×

Act By Date

Message ID MC925389

Category Plan for change

Published On 5.11.2024, 00.54.22

Message

As a follow up to our announcement on [Windows device configuration policies migrating to unified settings platform](#), expected with [Intune's December \(2412\) service release](#), you will not be able to create any new Administrative Templates for Windows devices. Specifically, these are the profiles created by navigating to **Devices > Configuration > Create > New policy > Windows 10 and later > Templates** in the Microsoft Intune admin center. The same settings found in the Administrative Templates can be configured with the [settings catalog](#).

How this will affect your organization:

After this change, you will not be able to create any new Administrative Templates from the Intune admin center. Existing Administrative templates can still be viewed, updated, or deleted.

Note: While this change does not impact the creation of new Administrative Templates through 'deviceManagement/groupPolicyConfigurations' Microsoft Graph API you should switch to the new 'deviceManagement/configurationPolicies' API graph endpoint for policy creation as soon as possible.

What you need to do to prepare:

If you are using Administrative Templates, use the settings catalog for configuring new settings going forward. As part of the migration of Windows configuration profiles, the existing Administrative Templates will eventually be migrated automatically. Review the blog for more information: [Windows device configuration policies migrating to unified settings platform](#)

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)

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	<div>✖ Error</div>	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

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



MDMWinsOverGPO (Hybrid-only)

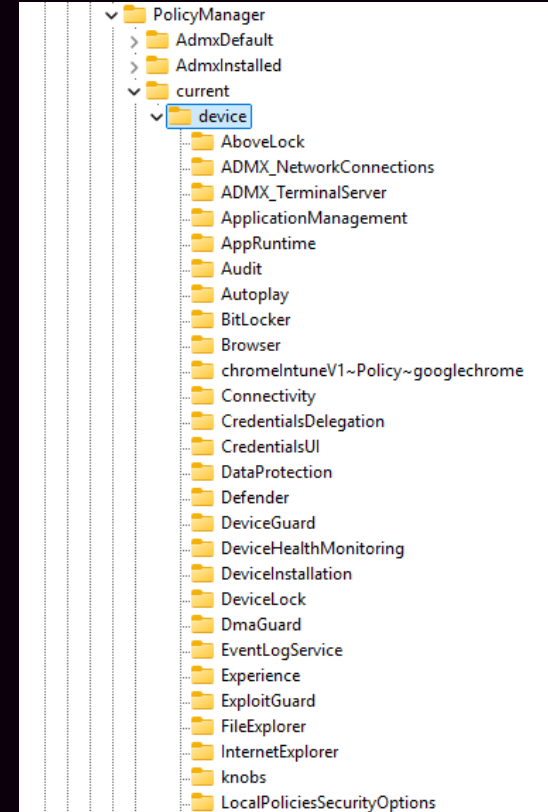
- Only applicable to the Policy CSP!

ⓘ 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 policies -> Policymanager -> Policies 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.

DEMO (Fast version 🕶️)



Edit pro
Task S
File Ac

Schedule created by dm client to refresh se

General Triggers Actions Conditions Se

When you create a task, you can specify the

Trigger	Details
One time	At 19:57 on 12-11-2024 - A

Edit Trigger

Begin the task: ☐ On a sc

Settings

☒ One time ☐ Daily
☐ Weekly
☐ Monthly

Advanced settings

☐ Delay task for up to

☒ Repeat task every:

☐ Stop all runs

☐ Stop task if it runs lo

☐ Expires: 12-11-2025

☒ Enabled

All Intune policies are working again!

- edge
- edge_recommended-Startup_recommended
- edge~ContentSettings
- edge~Extensions
- edge~HTTPAuthentication
- edge~NativeMessaging
- edge~PasswordManager
- edge~SmartScreen
- ossoft_edge
- ossoft_edge~SmartScreen
- ossoft_edge_recommended~DefaultSearchProvider_recommen
- ossoft_edge
- ossoft_edge_recommended~DefaultSearchProvider_recommen
- ossoftOfficemachine~L_Updates
- emachine~L_Updates
- emachine~L_Updates
- ANGSC
- ate~Cat_Applications
- at_Applications~Cat_MicrosoftEdge

Edge Policies

Microsoft Edge policies

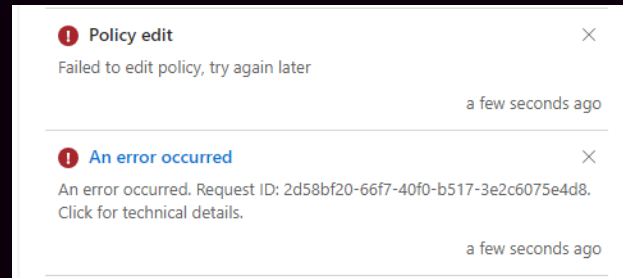
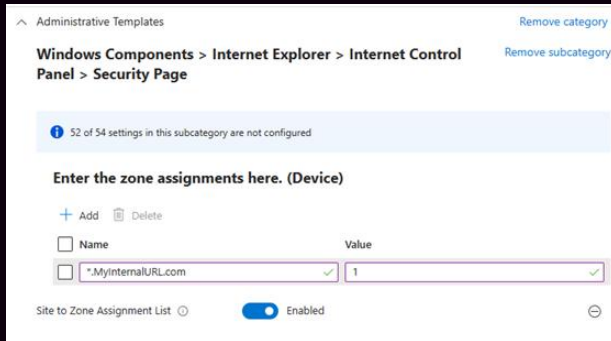
- Microsoft Edge management service
- Enrollment token or user targeting
- Default: MDM/GPO Windows over Edge Policies
- EdgeManagementPolicyOverridesPlatformPolicy
- Multiple policies = highest priority wins
- Edge://Policies

ⓘ 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

Windows Updates

Unexpected update to Windows 11 24H2

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

Name	Type	Data
(Default)	REG_SZ	(value not set)
enrollmentcheckedon	REG_SZ	2024-09-30T06:18:44Z
enrollmenttype	REG_SZ	FeatureUpdate, DriversUpdate

Deployment settings ⓘ Review + save

ⓘ Enable Windows health monitoring and select Windows Update scope to get detailed device states and errors. [Learn more](#)

Name * W11 - Feature Update

Description

Feature deployment settings

Feature update to deploy ⓘ Windows 11, version 23H2

☒ Make available to users as a required update

☐ Make available to users as an optional update

☐ When a device isn't eligible to run Windows 11, install the latest Windows 10 feature update

ⓘ By selecting this Feature update to deploy you are agreeing that when applying this operating system to a device either (1) the applicable Windows license was purchased through volume licensing, or (2) that you are authorized to bind your organization and are accepting on its behalf the relevant Microsoft Software License Terms to be found here <https://go.microsoft.com/fwlink/?linkid=2171206>.

Rollout options *

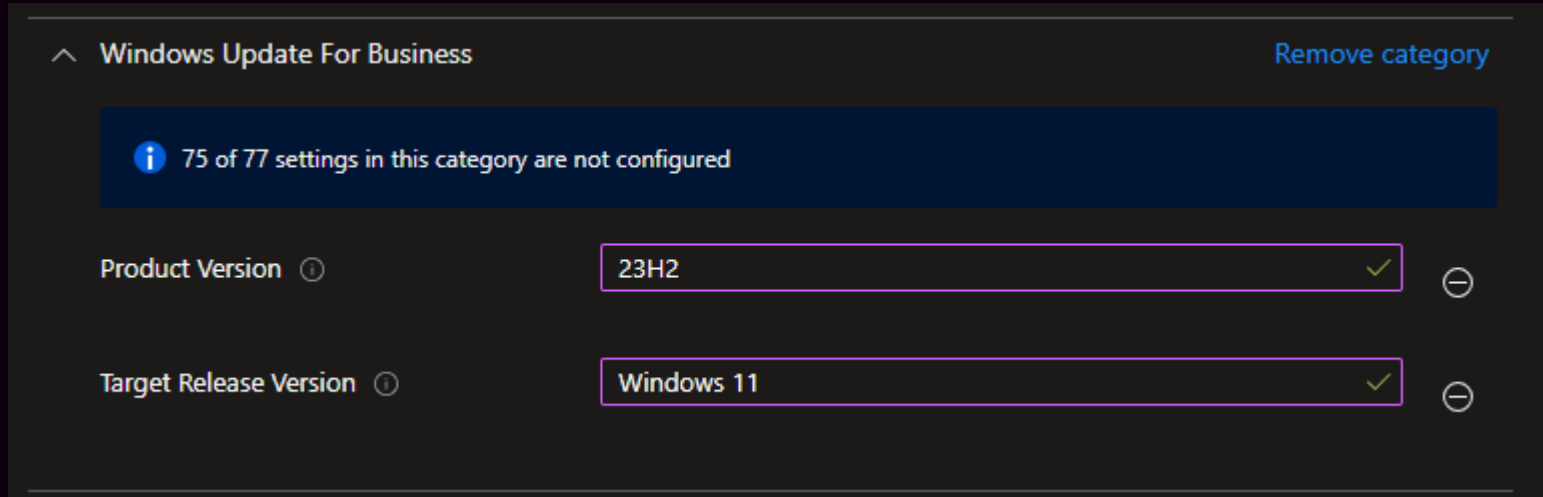
☒ Make update available as soon as possible

☐ Make update available on a specific date

☐ Make update available gradually

Solution

- Deploy Target Release Version & Product Version using settings catalog och Custom CSP



Policies are in a new location

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\PolicyState				
	Name	Type	Data	
	(Default)	REG_SZ	(value not set)	
	BranchReadinessLevel	REG_SZ	CB	
	DeferFeatureUpdates	REG_DWORD	0x00000001 (1)	
	DeferQualityUpdates	REG_DWORD	0x00000001 (1)	
	ExcludeWUDrivers	REG_DWORD	0x00000000 (0)	
	FeatureUpdatesDeferralInDays	REG_DWORD	0x00000000 (0)	
	IsDeferralsActive	REG_DWORD	0x00000001 (1)	
	IsWUFBConfigured	REG_DWORD	0x00000000 (0)	
	IsWUFBDualScanActive	REG_DWORD	0x00000000 (0)	
	PolicySources	REG_DWORD	0x00000004 (4)	
	QualityUpdatesDeferralInDays	REG_DWORD	0x00000000 (0)	
	SetPolicyDrivenUpdateSourceForDriverUpdates	REG_DWORD	0xffffffff (4294967295)	
	SetPolicyDrivenUpdateSourceForFeatureUpdates	REG_DWORD	0xffffffff (4294967295)	
	SetPolicyDrivenUpdateSourceForOtherUpdates	REG_DWORD	0xffffffff (4294967295)	
	SetPolicyDrivenUpdateSourceForQualityUpdates	REG_DWORD	0xffffffff (4294967295)	
	TemporaryEnterpriseFeatureControlState	REG_DWORD	0x00000001 (1)	
	UseUpdateClassPolicySource	REG_DWORD	0x00000000 (0)	

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.

Network

SSL traffic inspection = BAD

- Must exclude necessary endpoints
- Example on results

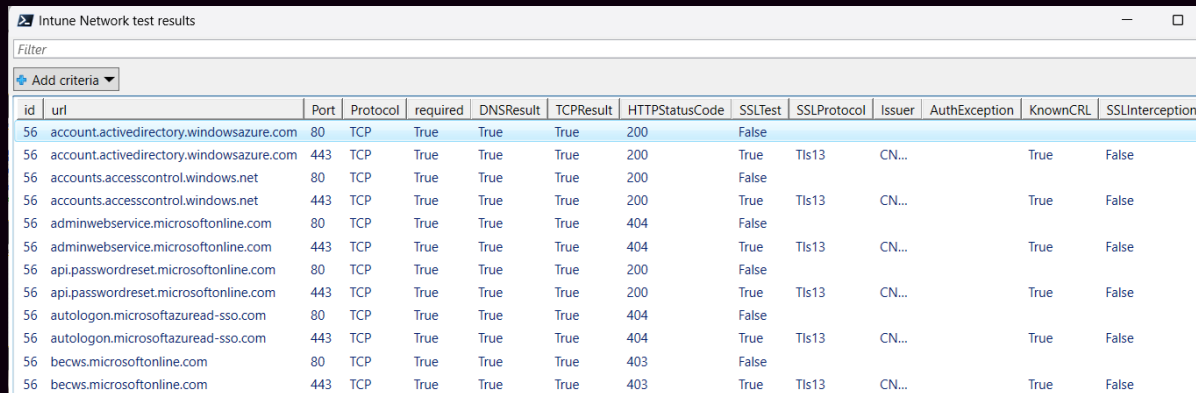
ⓘ Note

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

Intune Network Requirements

- By Martin Hinken (more comprehensive than MS..)
- Test network connectivity required by Intune, Autopilot, Device registration, TPM and more..
- Comprehensive tests



The screenshot shows a window titled "Intune Network test results" with a table of test results. The table has 14 columns: id, url, Port, Protocol, required, DNSResult, TCPResult, HTTPStatusCode, SSLTest, SSLProtocol, Issuer, AuthException, KnownCRL, and SSLInterception. The table contains 14 rows of test results for various Microsoft services.

id	url	Port	Protocol	required	DNSResult	TCPResult	HTTPStatusCode	SSLTest	SSLProtocol	Issuer	AuthException	KnownCRL	SSLInterception
56	account.activedirectory.windowsazure.com	80	TCP	True	True	True	200	False					
56	account.activedirectory.windowsazure.com	443	TCP	True	True	True	200	True	Tls13	CN...		True	False
56	accounts.accesscontrol.windows.net	80	TCP	True	True	True	200	False					
56	accounts.accesscontrol.windows.net	443	TCP	True	True	True	200	True	Tls13	CN...		True	False
56	adminwebservice.microsoftonline.com	80	TCP	True	True	True	404	False					
56	adminwebservice.microsoftonline.com	443	TCP	True	True	True	404	True	Tls13	CN...		True	False
56	api.passwordreset.microsoftonline.com	80	TCP	True	True	True	200	False					
56	api.passwordreset.microsoftonline.com	443	TCP	True	True	True	200	True	Tls13	CN...		True	False
56	autologon.microsoftazuread-sso.com	80	TCP	True	True	True	404	False					
56	autologon.microsoftazuread-sso.com	443	TCP	True	True	True	404	True	Tls13	CN...		True	False
56	becws.microsoftonline.com	80	TCP	True	True	True	403	False					
56	becws.microsoftonline.com	443	TCP	True	True	True	403	True	Tls13	CN...		True	False

Device enrollment/registration

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:

Applications

IME - Facts

- Installed when first needed to run (we always need it!)
 - Scripts
 - Remediation scripts
 - Win32App
 - Software Inventory
- IntuneWin32App run as 32-bits, be careful 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)

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

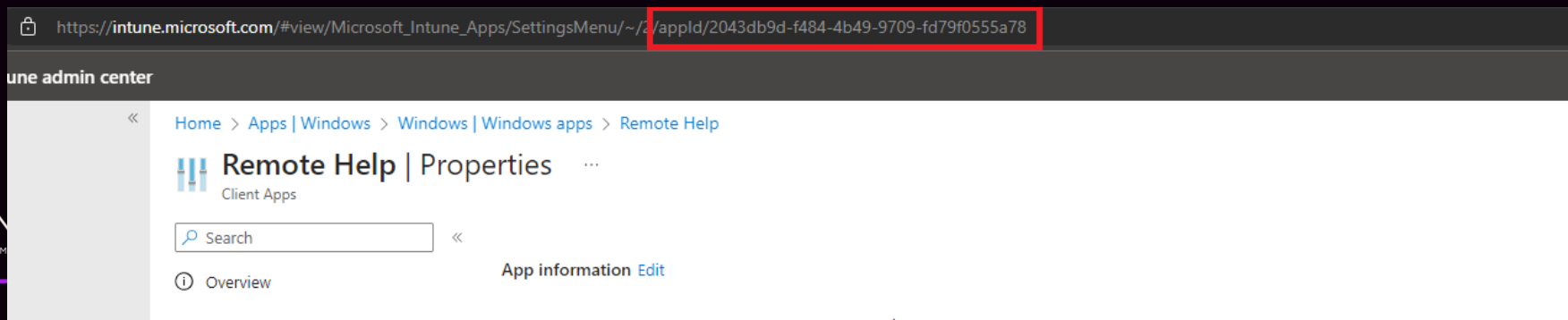
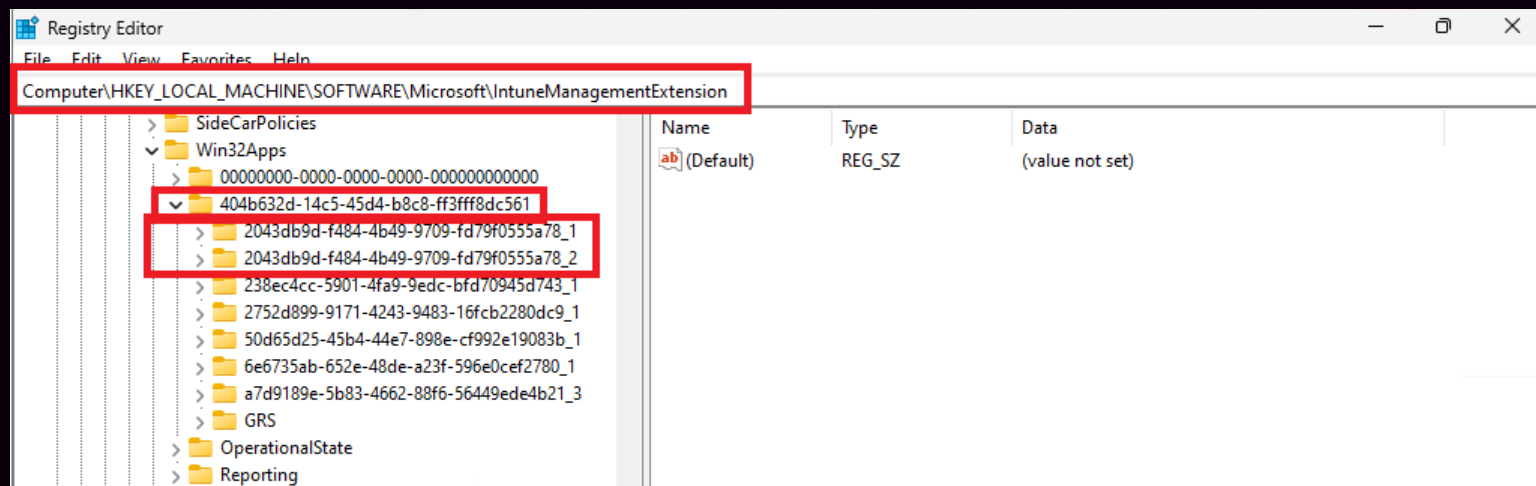
Content Cache location:

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

```
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...
Load in Task Mode from persistent settings
```

```
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
```

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.

Get-IntuneManagementExtensionDiagnostics ver 3.0 Report run: 2024-11-12 19:19 Computer Name: DESKTOP-9SECHR9 Download Report tool from GitHub Author: Petri Paavola - Microsoft MVP

☒ Win32App ☐ WinGetApp ☐ Powershell script ☐ Remediation

Status: All (102) Info (26) Not Detected (11)

Type: All Intent: All

Search: [X] Reset filters

Date	Status	Type	Intent	Detail	Seconds	LogEntry
2024-11-11 09:12:09.0266596	Detected	Win32App	Available	Adobe Acrobat Reader DC MUI 24.004.20243 (x64)		Line 879
2024-11-11 09:12:11.2795597	Detected	Win32App	Available	Notepad++ 8.7.1 (x64)		Line 930
2024-11-11 10:47:18.7684273	Detected	Win32App	Required	Corporate teams backgrounds		Line 1334
2024-11-11 10:47:18.7964450	Detected	Win32App	Required	Universal Print Printer Provisioning		Line 1369
2024-11-11 10:47:18.8689703	Detected	Win32App	Required	Remote Help 10.3.10130.1000		Line 1452
2024-11-11 10:47:18.8709698	Detected	Win32App	Required	Remote Help 10.3.10130.1000		Line 1455
2024-11-11 10:47:18.8719698	Detected	Win32App	Required	Remote Help 10.3.10130.1000		Line 1458
2024-11-11 10:47:21.7543473	Detected	Win32App	Required	Google Chrome 130.0.6723.117		Line 1509
2024-11-11 10:47:23.0548301	Detected	Win32App	Required	Ccmexec		Line 1558
2024-11-11 10:47:23.0808361	Detected	Win32App	Required	CMTrace		Line 1594
2024-11-11 10:47:29.0689687	Detected	Win32App	Required	Remote Desktop		Line 1747
2024-11-11 10:47:32.4316657	Detected	Win32App	Required	Windows Remove Apps 1.3.2		Line 1951
2024-11-11 10:47:34.0187468	Detected	Win32App	Required	M365 Apps - Script		Line 1999
2024-11-11 10:47:36.5483097	Detected	Win32App	Required	Microsoft Teams New		Line 2047
2024-11-11 16:13:12.4313899	Detected	Win32App	Required	Corporate teams backgrounds		Line 3373
2024-11-11 16:13:12.4803741	Detected	Win32App	Required	Universal Print Printer Provisioning		Line 3408
2024-11-11 16:13:12.5593541	Detected	Win32App	Required	Remote Help 10.3.10130.1000		Line 3491

Reinstall app required app using Powershell/remediation

- Remediations on demand is great!
- Powershell script that clears out registry and restarts IME

- ☐ Troubelshoot - Reinstall Google Chrome
- ☒ Troubelshoot - Reinstall Remote Help
- ☐ Troubelshoot - Clear DNS Cache

```
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 policies to troubleshoot going forward
- Keep up with changes coming!



Thank you!