

Troubleshooting Devices in Intune: Tips From the Trenches



Speakers



Jörgen Nilsson

Trusted Advisor - Onevinn



[in/ccmexec/](https://www.linkedin.com/company/ccmexec/)



Sandy

Senior Cloud Architect

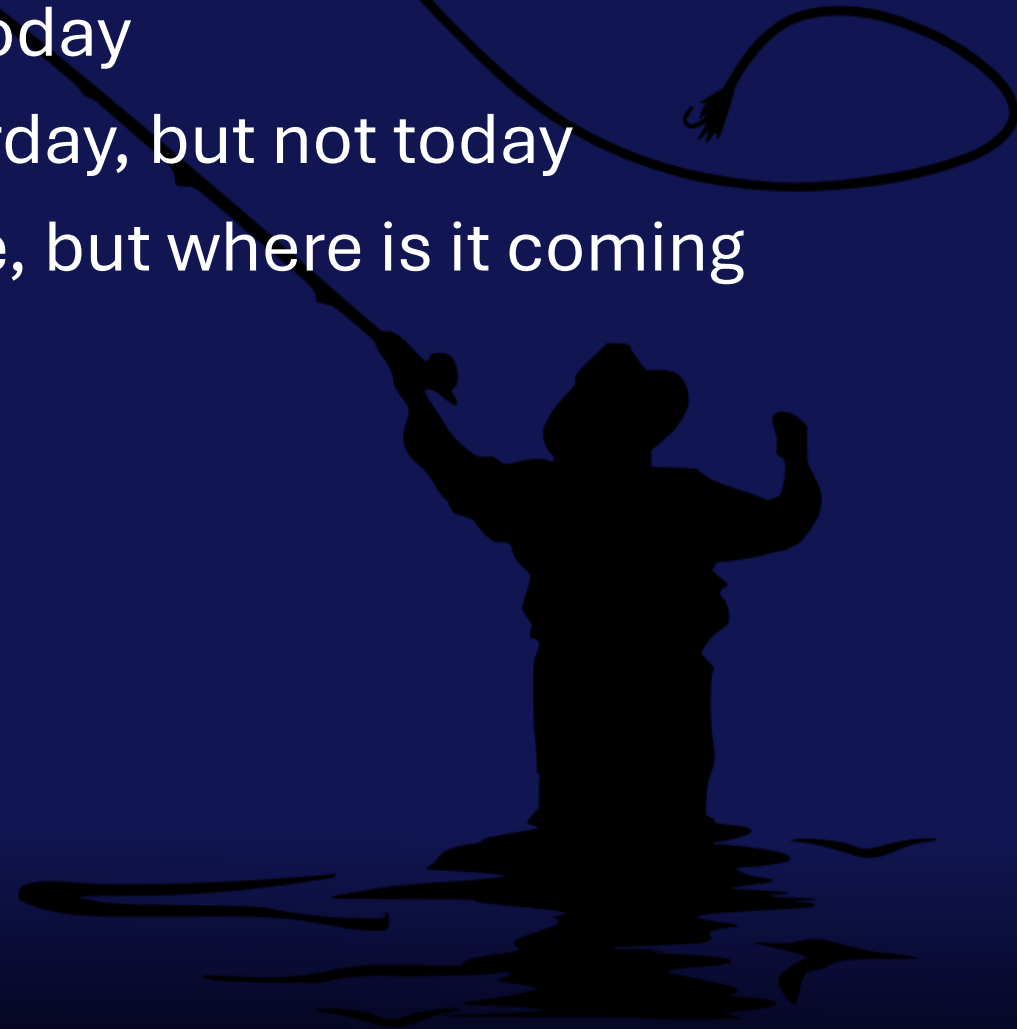


[in/sandy-tsang/](https://www.linkedin.com/company/sandy-tsang/)

Can't see our slides? Can't hear? Need to repeat the question? Call us out!

When we troubleshoot Intune?

- ◆ Device was working yesterday, but not today
- ◆ Autopilot enrollment was working yesterday, but not today
- ◆ I know there a setting broke the machine, but where is it coming from?
- ◆ Application installed failed
- ◆ Update doesn't install
- ◆ And many more....



Troubleshooting evolution

- ◆ Back in the olds days.
- ◆ Connecting to a BBS with a modem was how we could get information and hotfixes....

Or we ask a friend



Good old days...

Troubleshoot GPO/ConfigMgr

- ◆ Many, many log files
- ◆ Server sides/client side
- ◆ Complex but can see everything

Group Policies

- ◆ Gpresult
- ◆ RSOP
- ◆ GPupdate



Troubleshooting Intune

- ◆ Log files -> event log
- ◆ Registry values
- ◆ SyncML
- ◆ IME agent = log files 😊

Tools:

- ◆ Copilot
- ◆ Copilot for security
- ◆ ChatGPT...
- ◆ Community tools... Lots of them

Or we ask a friend or Microsoft



What is Intune?

- ◆ Intune is Cloud-based endpoint management solution
- ◆ We are not in control of backend changes anymore.

Take Action: Update network endpoints for ... ✕

Act By Date	12/27/2024, 9:00:00 AM
Message ID	MC964310
Category	Prevent or fix issue
Published On	12/23/2024, 6:44:18 PM
Message	On December 27, 2024 as a result of the Edgeio retirement , we are updating the required CDN endpoints for Win32 apps and PowerShell scripts. Refer to Network requirements for PowerShell scripts and Win32 apps for the updated list of CDN endpoints required for your tenant location.

Home > Tenant admin

Tenant admin | Tenant status

Search

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration**
- Troubleshooting + support

- Tenant status**
- Admin tasks
- Remote Help
- Microsoft Tunnel Gateway
- Cloud PKI
- Connectors and tokens
- Assignment filters
- Roles
- Microsoft Entra Privileged Identity Management
- Diagnostics settings
- Audit logs
- Device diagnostics
- Multi Admin Approval
- Intune add-ons
- Copilot (preview)
- Windows 365 Administration
 - Cloud PC encryption type
 - Maintenance Windows (Preview)
 - Partner Connectors

Tenant details Connector status **Service health and message center**

Service health

1 active

Search Add filters

Title	Service	ID	Status	User impact	Start time	Updated
Some users' Windows Intune de...	Microsoft Intune	IT1298282	Service restored	Users' Windows Intun...	4/28/2026, 3:30:00 PM	5/5/2026, 5:06:48 AM

[See past incidents/advisories](#)

Issues in your environment that require action

0 active

Search Add filters

Title	Service	ID	Status	User impact	Start time	Updated
No active incidents or advisories						

[See past incidents/advisories](#)

Message center

17 active

Search Add filters

Message title	Service	Act by	Category	Published	Message ID
Planned Maintenance Reminder: Windows 365 Service	Windows 365		Stay informed	5/5/2026	MC1301182
What's new in the Microsoft Intune service update for...	Microsoft Intune		Stay informed	5/2/2026	MC1297979
Plan for Change: Intune introduces support for Multip...	Microsoft Intune		Plan for change	4/25/2026	MC1290818

Add or remove favorites by pressing Ctrl+Shift+F

What went wrong?

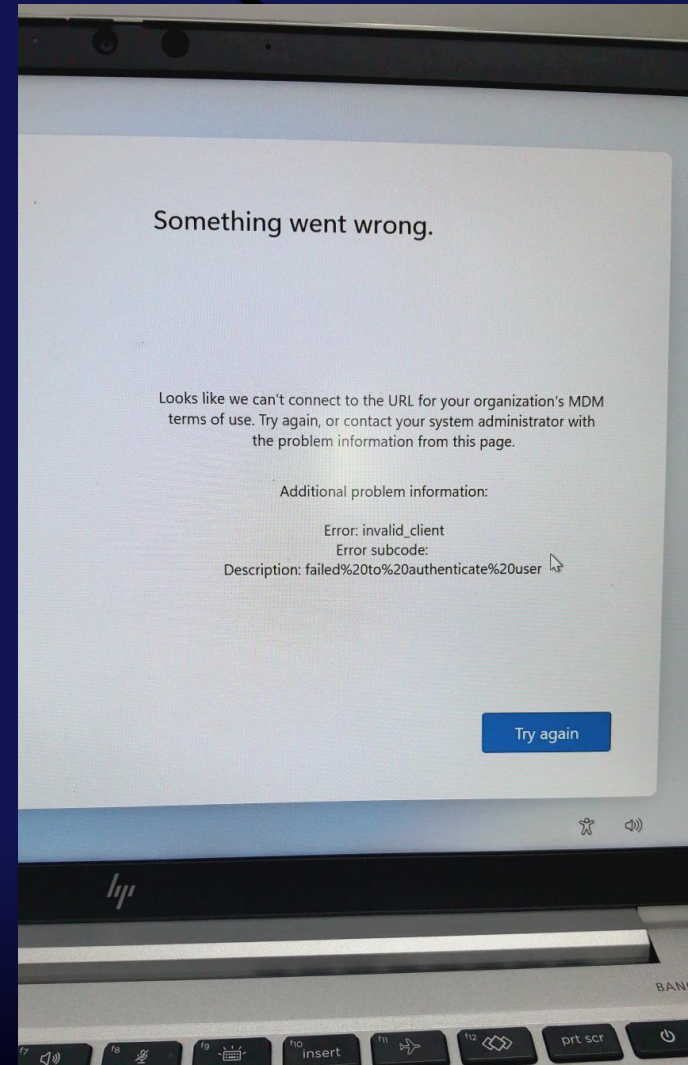
Customer: Hi Sandy, after MFA, this showed up, could you help us with this?

Sandy: during enroll the machine? or after everything is done?

Customer: during enroll the machine

Sandy: problem with one user?




Customer: 4 new users today, all have this problem






License


- ◆ Microsoft Intune is a **cloud-based endpoint management solution**

Make sure you have **enough**
Intune License!!!

 Add more products  Export to CSV  Refresh 1 item

Filters: **Subscription status: Active, Expired, Disabled , +1**  Add filter  Reset all

	Product name ↑	Assigned licenses	Purchased quantity	Availa
<input type="checkbox"/>	 Microsoft 365 Business Premium	61	60	0




This device cannot access company resources

Regain access
You need to make some changes to this device so that it can access Equinor ASA resources.

Intune license required
Contact your support person to confirm that your account is assigned a license to use Intune.
[Show less](#)

Compliance policies haven't been assigned to this device
Your device must receive compliance policies before it can be used to access your organization's resources. Contact your support person.
[Show less](#)

Status
 Cannot access company resources

Automatic upload Autopilot failure logs

Home > Tenant admin

Tenant admin | Device diagnostics

Search

- Roles
- Microsoft Entra Privileged Identity Management
- Diagnostics settings
- Audit logs
- Device diagnostics**
- Multi Admin Approval
- Intune add-ons
- Copilot (preview)
- Windows 365 Administration
 - Cloud PC encryption type
 - Maintenance Windows (Preview)

Microsoft personnel may access device diagnostics to assist in troubleshooting and resolving incidents. [Review our documentation for more information on device diagnostics.](#)

Device diagnostics are available for corporate-managed devices running Windows 10, version 1909 and later, or Windows 11. Diagnostics may include user identifiable information such as user or device name. ⓘ

Enabled

Automatically capture diagnostics when devices experience a failure during the Autopilot process on Windows 10 version 1909 or later and Windows 11. Diagnostics may include user identifiable information such as user or device name. ⓘ

Enabled

D diagnostic data is available only for devices managed by Intune app protection policy. The data could include user-identifiable information, such as user or device name. The data is stored in Microsoft support systems and isn't subject to Intune data management policies or protections. Some applications might collect and store data using systems other than Intune. For more info, check privacy documentation for each app. ⓘ

Enabled

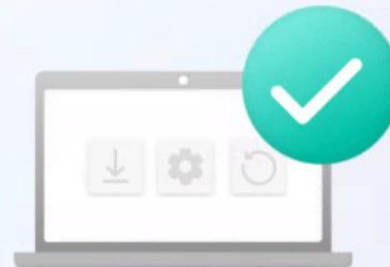
What went wrong?

◆ Autopilot failed...

It said:

Apps
(0x80070002)

Use “View
Diagnostics” or
Ctrl+Shift+D”



Setting up for work or school

Setup could not be completed. Please try again or contact your support person for help.

(Completed)

Device setup

● Error

Security policies (5 of 5 applied)

Certificates (No setup needed)

Network connections (No setup needed)

Apps (0x80070002)

Account setup

Previous step failed

For more details, view diagnostics.

Try again



Is this useful?

What is
Win32App_d39c78e2-
7a9a-4b38-afb1-
067ceff25d30_1 ?



Windows Autopilot diagnostics

Provider tracking list retrieval

✓ Provider Installation

Policy Status

./Device/Vendor/MSFT/Policy/Config/Update

! Installation

./Vendor/MSFT/DMClient/Provider/MS%20DM
%20Server

! Installation

App Status

./Device/Vendor/MSFT/EnrollmentStatusTrackin
g/Setup/Apps/Tracking/Sidecar/Win32App_d39
c78e2-7a9a-4b38-afb1-067ceff25d30_1

! Installation

Win32App_d39c78e2-7a9a-4b38-afb1-
067ceff25d30_1

Close

Export logs

Download diagnostic logs

Home > Devices | Windows > Windows | Windows devices > MVP24-002

MVP24-002 | Device diagnostics

Search

Refresh Columns

Requested by	Status	Request initiated	Diagnostics uploaded
Autopilot enrollment	Complete	5/7/2026, 6:35:00 AM	5/7/2026, 6:38:52 AM

Download

- Properties
- Monitor
 - Device inventory
 - All apps
 - Device query
 - Hardware
 - Discovered apps
 - Device compliance
 - Device configuration
 - App configuration
 - Local admin password
 - Recovery keys
 - User experience
 - Device diagnostics**
 - Group membership
 - Managed Apps
 - Filter evaluation

DEMO

Read logs



Autopilot troubleshooting – Community version

- ◆ Tool Author: Andrew taylor(@Andrew Taylor) -ish
- ◆ Autopilot v2 support
- ◆ Troubleshooting information from Autopilot
- ◆ Run offline from .cab files

AUTOPILOT DIAGNOSTICS

```
OS version: 10.0.22631
EntDMID: 29082613-66f5-4349-a1d4-69f328c4e8ef
Enrollment status page:
Device ESP enabled: True
User ESP enabled: False
ESP timeout: 60
ESP blocking: Yes
ESP allow try again: Yes
ESP continue anyway: Yes
Delivery Optimization statistics:
Total bytes downloaded: 1412692675
From peers: 2% (29094925)
From Connected Cache: 71% (1004068531)
```

OBSERVED TIMELINE:

Date	Status	Detail
2025-06-16 12:29:11Z	SCP discovery successful	Device Registration
2025-07-31 08:33:58Z	Download started	{B94DDEE8-A4C1-4949-A981-3BCE77F79784}
2025-07-31 08:34:04Z	Download started	{E5B693D7-0DE7-4AB6-81D8-6A4D8FAB051E}
2025-07-31 08:34:13Z	Download finished	{B94DDEE8-A4C1-4949-A981-3BCE77F79784}
2025-07-31 08:34:14Z	Installation started	{B94DDEE8-A4C1-4949-A981-3BCE77F79784}
2025-07-31 08:34:24Z	Download finished	{E5B693D7-0DE7-4AB6-81D8-6A4D8FAB051E}
2025-07-31 08:34:25Z	Installation finished	{B94DDEE8-A4C1-4949-A981-3BCE77F79784}
2025-07-31 08:34:31Z	Installation started	{E5B693D7-0DE7-4AB6-81D8-6A4D8FAB051E}
2025-07-31 08:35:05Z	Installation finished	{E5B693D7-0DE7-4AB6-81D8-6A4D8FAB051E}
2025-08-12 16:09:51Z	Download started	{E94ADF8C-4B5C-4B3B-9603-744A0F6BDDC3}
2025-08-12 16:09:59Z	Download finished	{E94ADF8C-4B5C-4B3B-9603-744A0F6BDDC3}
2025-08-12 16:10:00Z	Installation started	{E94ADF8C-4B5C-4B3B-9603-744A0F6BDDC3}
2025-08-12 16:10:14Z	Installation finished	{E94ADF8C-4B5C-4B3B-9603-744A0F6BDDC3}
2025-08-12 16:17:39Z	Download started	{8fa1c545-8a16-4c02-9892-8d6d7a4e620f}
2025-08-12 16:17:48Z	Download finished	{8fa1c545-8a16-4c02-9892-8d6d7a4e620f}
2025-08-12 16:18:11Z	Installation started	{8fa1c545-8a16-4c02-9892-8d6d7a4e620f}
2025-08-12 16:18:54Z	Installation finished	{8fa1c545-8a16-4c02-9892-8d6d7a4e620f}
2025-08-14 18:25:44Z	Download started	{1D9E7560-F2C4-45CC-985E-1F85375E67EE}
2025-08-14 18:25:52Z	Download finished	{1D9E7560-F2C4-45CC-985E-1F85375E67EE}
2025-08-14 18:25:54Z	Installation started	{1D9E7560-F2C4-45CC-985E-1F85375E67EE}
2025-08-14 18:26:02Z	Installation finished	{1D9E7560-F2C4-45CC-985E-1F85375E67EE}
2025-09-16 19:32:54Z	DownloadStart	Microsoft office C2R (16_0_19029_20244_I640_C2RX)
2025-09-16 19:33:55Z	DownloadCompleted	Microsoft office C2R (16_0_19029_20244_I640_C2RX)
2025-09-16 19:34:14Z	DownloadStart	Microsoft office C2R (16_0_19029_20244_I640_CAB)
2025-09-16 19:35:16Z	DownloadCompleted	Microsoft office C2R (16_0_19029_20244_I640_CAB)
2025-09-16 19:35:22Z	DownloadStart	Microsoft office C2R (16_0_19029_20244_A640_EXP_CAB)
2025-09-16 19:36:23Z	DownloadCompleted	Microsoft office C2R (16_0_19029_20244_A640_EXP_CAB)
2025-09-16 19:36:28Z	DownloadStart	Microsoft office C2R (16_0_19029_20244_S640_CAB)
2025-09-16 19:36:29Z	DownloadCompleted	Microsoft office C2R (16_0_19029_20244_S640_CAB)

Network (It is always DNS?)



SSL traffic inspection = NO!

- ◆ Must exclude necessary endpoints per-service not only Intune
- ◆ Example on results

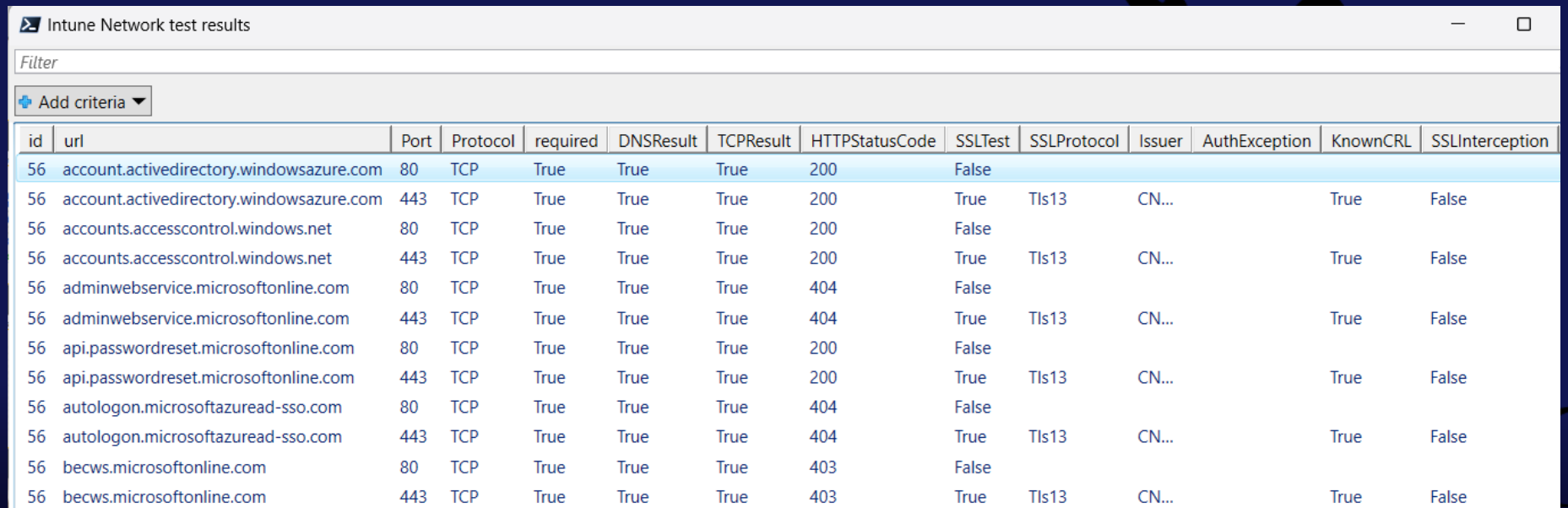
ⓘ Note

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 Himken (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, all with an id of 56. The results show that all tests passed (DNSResult, TCPResult, and HTTPStatusCode are all True or 200/403/404, and SSLTest is True or False).

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

Troubleshoot Policies



Where is my setting coming from?

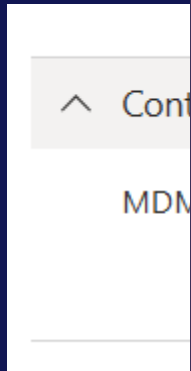
- ◆ Intune
- ◆ GPO, ConfigMgr (Hybrid co-managed)
- ◆ Cloud Policy (Edge, Office)
- ◆ Admin center (Copilot setting)

Resolve the conflict source!!!



MDMWinsOverGPO

- ◆ Only applies to the Policy CSP
- ◆ Settings



ⓘ 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. As a result, it is recommended that the same settings should not be configured in both GPO and MDM policies unless the settings are under the control of MDMWinsOverGP. Otherwise, there will be a race condition and no guarantee which one wins.

<https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict#mdmwinsovergp>

Intune

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device

- > Outlook Express
- > Palm
- > Personalization
- > Phone
- > Photos
- > Pim
- > PLA
- > PlayToReceiver
- > PointOfService
- > Policies
- > PolicyManager
 - > AdmxDefault
 - > AdmxInstalled
 - > current
 - > device
 - AboveLock
 - ADMX_CredentialProviders
 - ADMX_MSS-legacy
 - ADMX_WindowsExplorer
 - AdobeDC~Policy~Adobe_Reader_DC_31~Prefere
 - ApplicationManagement
 - AppRuntime
 - Audit
 - Authentication
 - Autoplay
 - BitLocker
 - Browser
 - chromeIntuneV1~Policy~googlechrome
 - chromeIntuneV1~Policy~googlechrome~Extensic
 - chromeIntuneV1~Policy~googlechrome~HTTPAu
 - chromeIntuneV1~Policy~googlechrome~NativeM
 - chromeIntuneV1~Policy~googlechrome~Passwor
 - chromeIntuneV1~Policy~googlechrome~Startup
 - Connectivity
 - ControlPolicyConflict
 - CredentialProviders
 - CredentialsDelegation
 - CredentialsUI
 - DataProtection
 - Defender
 - DeliveryOptimization

Name

ab (Default)



Intune Management extension(IME) and Win32Apps



Intune Management extension

Installs automatically

Updates automatically

Extends Intune functionality with:

- ◆ PowerShell scripts
- ◆ Win32 apps
- ◆ Microsoft Store apps (WinGET)
- ◆ Custom compliance policy script
- ◆ Proactive remediations
- ◆ Software Inventory



Intune Management extension sync

◆ IME Sync schedule

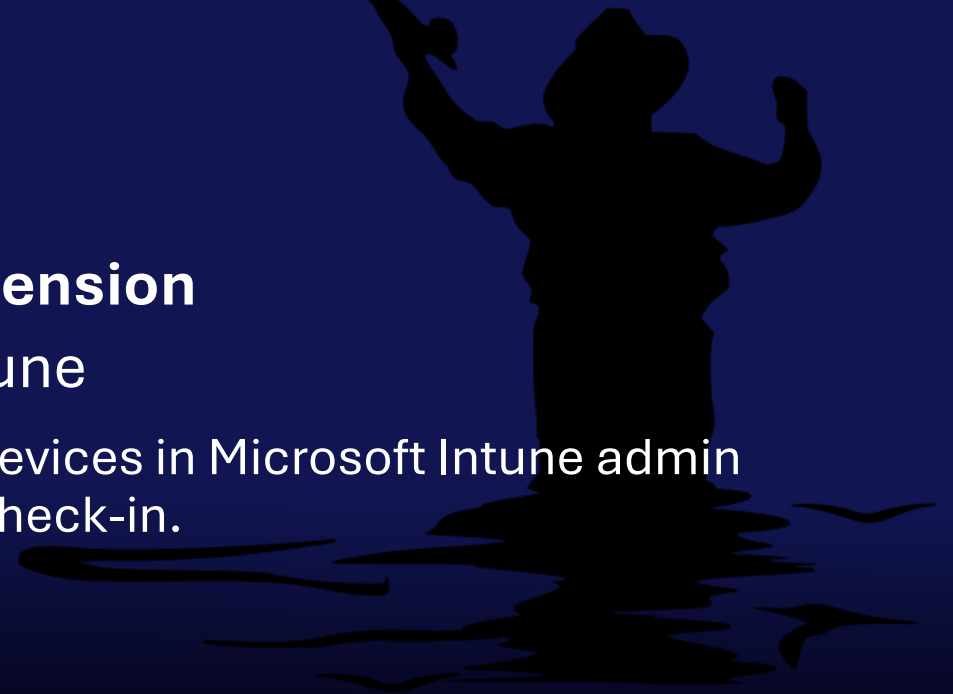
- ◆ Checks with Intune services every 8 hour (maintenance)
- ◆ This check-in process is independent of the MDM check-in.

◆ Manually initiate an IME check-in

- ◆ **Company Portal > Settings > Sync.**
- ◆ Initiates an **MDM** check-in and **IME** check-in.

◆ Alternative

- ◆ Restart the service **IntuneManagementExtension**
- ◆ The restart will initiating a check-in with Intune
- ◆ Note: The Sync actions from either the Settings app or Devices in Microsoft Intune admin center initiate an MDM check-in but don't force an IME check-in.



Apps: company Portal



All

Apps

Documents

Settings

People

Folders

Photos



Best match for apps



Company Portal
App

Apps



Database Compare

Preview



Spreadsheet Compare



Command Prompt

Store



Company Portal
App



Open



Sync this device

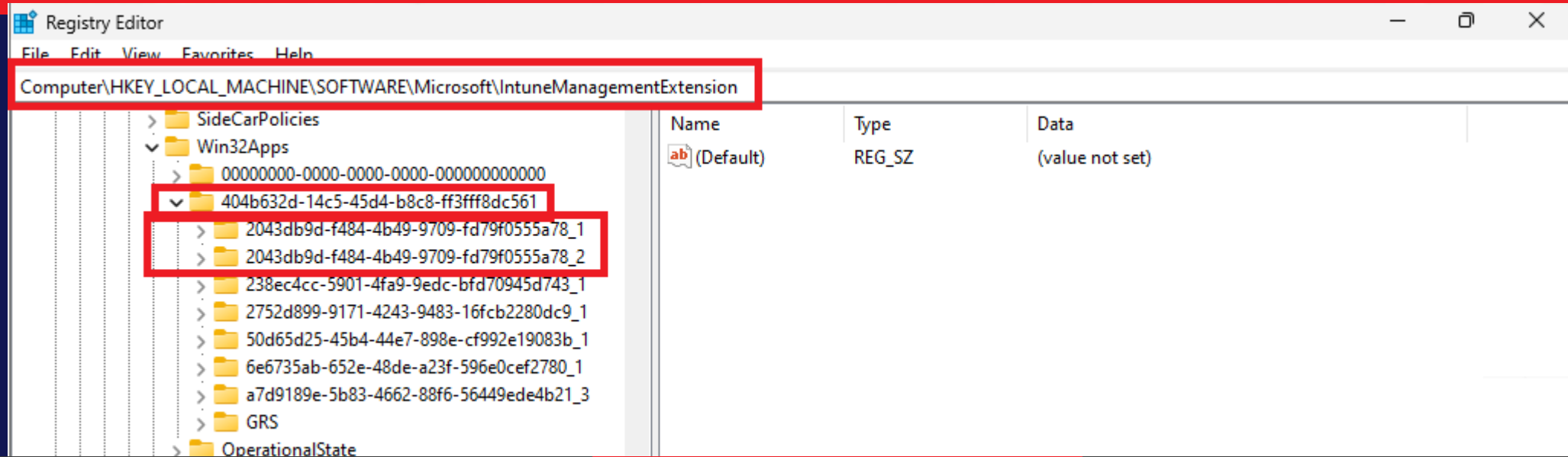


Global Reevaluation Schedule (GRS)

A silhouette of a cowboy in a dark suit and hat, standing in a field and herding a horse. The cowboy is holding a lasso that is looped around the horse's head. The background is a dark blue gradient.

- ◆ **Initial Installation Attempt:**
 - ◆ Intune deploys a Win32 app and the IME-agent executes the installation command.
- ◆ **Failure:**
 - ◆ If the app fails to install, the IME will retry it up to **3** times.
- ◆ **GRS Activation:**
 - ◆ If all 3 attempts fail, the app is placed in the **Global Reevaluation Schedule (GRS)**.
- ◆ **24-Hour Wait:**
 - ◆ The GRS prevent the IME from endlessly retrying a known-to-fail app.
 - ◆ It will wait for 24 hours from the last failed attempt before considering a retry.
- ◆ **Scheduled Reevaluation:**
 - ◆ The system checks for GRS expiration to determine when to attempt the installation again. After the 24-hours.
- ◆ **Repeat:**
 - ◆ The process then repeats, with another set of 3 installation attempts.

Registry



Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension

Name	Type	Data
(Default)	REG_SZ	(value not set)

https://intune.microsoft.com/#view/Microsoft_Intune_Apps/SettingsMenu/~/?appId/2043db9d-f484-4b49-9709-fd79f0555a78

Intune admin center

Home > Apps | Windows > Windows | Windows apps > Remote Help

Remote Help | Properties

Client Apps

Search

Overview

App information Edit

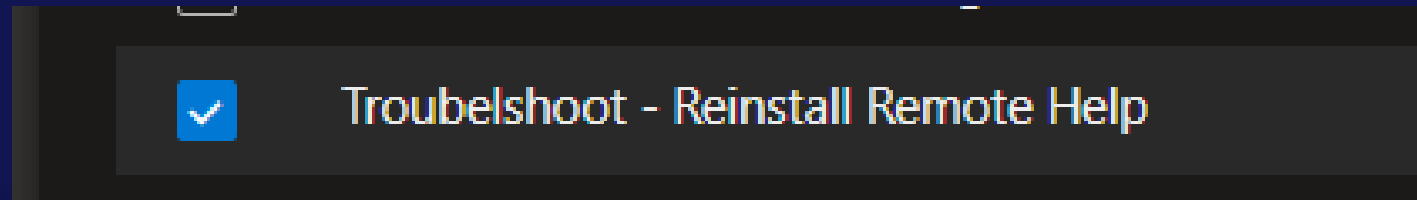
Manage

Name

Remote Help

Reinstalling app remotely

- ◆ Uninstall the app if installed
- ◆ Remove the AppID in the registry
- ◆ Remove the GRS association
- ◆ Launch a new PowerShell process that restarts IME agent



<https://ccmexec.com/2025/01/reinstall-a-required-win32app-using-remediation-on-demand/>

Restart IME agent remotely

“Application installation is slow”

- ◆ Empower ServiceDesk with a remediation they can run on demand and restart IME Agent.
- ◆ Important to train them and explain why as well.

#Restart IME service

```
Start-Process -FilePath powershell -ArgumentList '-Executionpolicy bypass -command "& {Start-Sleep 90 ; Restart-Service -Name IntuneManagementExtension -Force}"'
```

#Exit script

Exit 0

Remediations on demand = RBAC

- ◆ Remediations on demand is a great
- ◆ Perfect in a Zero-trust scenario
- ◆ Requires RBAC to filter script
- ◆ Create your own repository



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 2.0 Report run: 2023-09-27 08:31 Computer Name: DESKTOP-9SECHR9 Download Report Author: Petri Paavola

Win32App WinGetApp Powershell script Remediation

Status: All (122) Info (4) Not Detected (12)

Type: All Intent: All

Search: X Reset filters

Date	Status	Type	Intent	Detail
1900-01-01 23:59:59.0000000	Info			Possible Microsoft 365 Apps and Intune LOB MSI Apps are not shown in this report
2023-09-24 15:39:40.1318561	Success	Remediation	Detect	a5b99738-46f6-43f8-840c-64f0dee38c84
2023-09-24 15:40:02.3519185	Not Detected	Remediation	Detect	8bacef2a-77b0-46e7-b5b0-85ea5f1d00cb
2023-09-24 15:40:17.2905948	Success	Remediation	Detect	d78c1822-e082-491a-b3a7-4a701836481e
2023-09-24 16:02:39.2325044	Info			##### Not in ESP detected #####
2023-09-24 16:02:44.0776896	Detected	Win32App	Required Install	Remote Desktop
2023-09-24 16:02:44.1142084	Detected	Win32App	Required Install	Remote Help
2023-09-24 16:02:44.1582090	Detected	Win32App	Required Install	Universal Print Printer Provisioning
2023-09-24 16:02:44.2012185	Detected	Win32App	Required Install	RemoveConsumerTeams.ps1
2023-09-24 16:02:44.3192529	Detected	Win32App	Required Install	Microsoft Teams -script
2023-09-24 16:02:44.3562530	Detected	Win32App	Required Install	CMTrace
2023-09-24 16:02:45.3123146	Detected	WinGetApp	Required Install	Company Portal 11.2.179.0
2023-09-24 16:02:45.3513070	Detected	Win32App	Required Install	Windows Remove Apps 1.3.2
2023-09-24 16:02:47.8423335	Detected	Win32App	Required Install	M365 Apps -Script
2023-09-24 22:56:43.8641425	Detected	Win32App	Available Install	Poly Lens 1.2.0.5875 (MSI-x86)
2023-09-24 22:56:46.1162307	Detected	WinGetApp	Available Install	Spotify - Music and Podcasts 1.220.1218.0
2023-09-24 22:56:46.1472430	Not Detected	Win32App	Available Install	TeamsNew. Not Detected after App install (-2147024894)
2023-09-24 22:56:47.5716846	Detected	Win32App	Available Install	Notepad++ 8.5.7 (x64)
2023-09-25 00:27:03.4306032	Detected	Win32App	Required Install	Remote Desktop
2023-09-25 00:27:03.4601231	Detected	Win32App	Required Install	Remote Help
2023-09-25 00:27:03.5051290	Detected	Win32App	Required Install	Universal Print Printer Provisioning

Application Control



Application Control for Business

Managed Installer policy in Intune – enables it during Autopilot for it to work

Requires the files to be signed (hash exceptions is also possible, but must be handled manually)

Unsigned installer files is a big issue, even for some Microsoft Software.

Known issues:

- ◆ Adds time to Autopilot V1
- ◆ WIX 3 custom action dll's are not signed
- ◆ WIX 4 and later custom action dll's are signed, but not by Microsoft

Policy name ↑	Author	Status
Managed Installer Test	Microsoft Corp	✓ Active
SideCar ManagedInstaller Script	Microsoft	✓ Active

```
C:\Program Files\Remote Help>fsutil file queryea RemoteHelp.exe
```

```
Extended Attributes (EA) information for file C:\Program Files\Remote Help\RemoteHelp.exe:
```

```
Total Ea Size: 0x2db
```

```
Ea Buffer Offset: 0
```

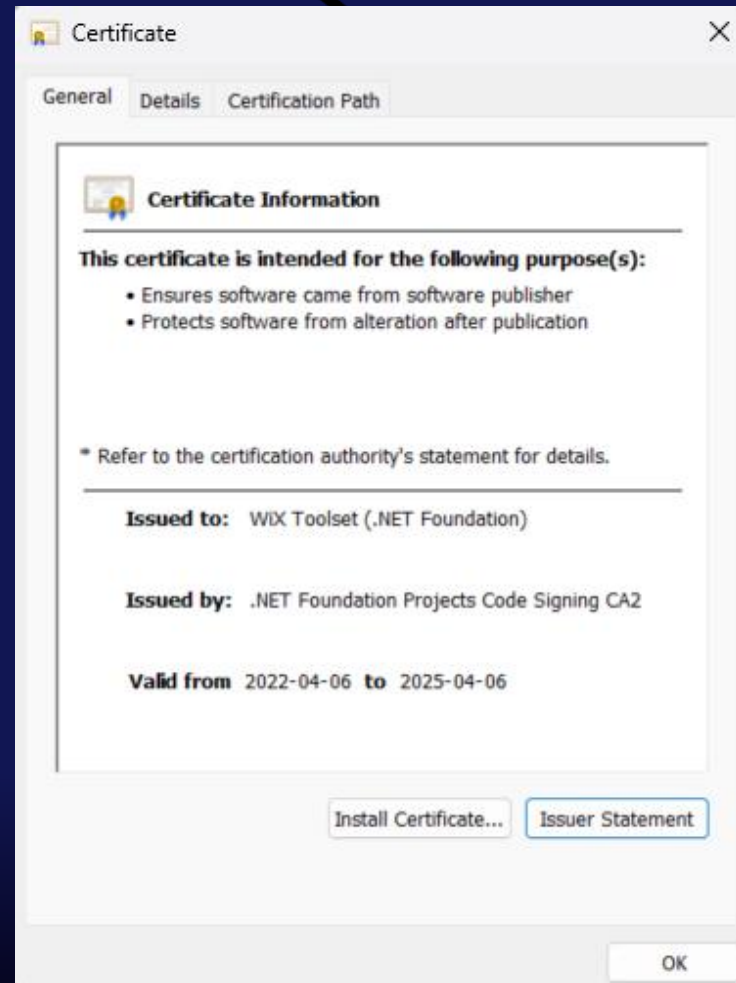
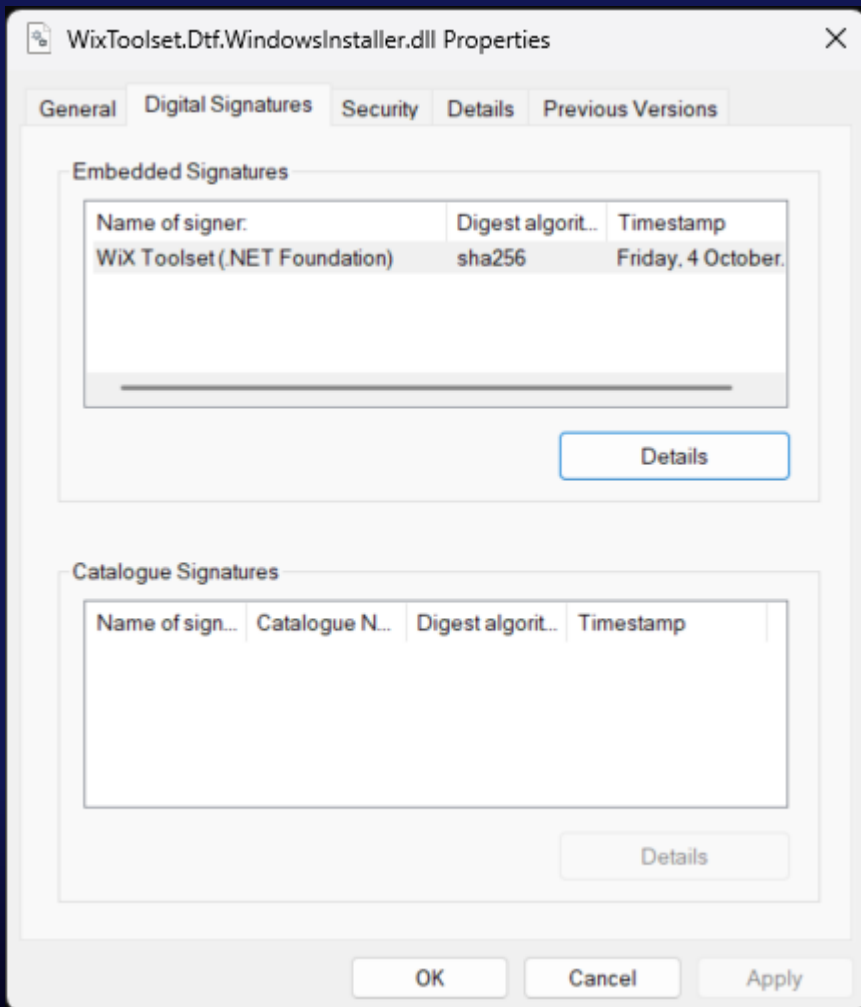
```
Ea Name: $KERNEL.SMARTLOCKER.ORIGINCLAIM
```

```
Ea Value Length: 12c
```

```
0000: 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 .....
0010: b3 a9 3e 01 e5 be b8 82 c6 09 12 45 b2 6b b5 2b ..>.....E.k.+
0020: 3f 7b 63 e1 11 f0 d6 f8 4b b9 ed 0d 70 71 40 dc ?{c.....K...pq@.
0030: 00 00 00 00 00 00 00 00 ea 00 00 00 5c 00 3f 00 .....\.?.
0040: 3f 00 5c 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 ?.\.C.:.\.P.r.o.
0050: 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 g.r.a.m. .F.i.l.
0060: 65 00 73 00 20 00 28 00 78 00 38 00 36 00 29 00 e.s. (.x.8.6.).
0070: 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 \.M.i.c.r.o.s.o.
0080: 66 00 74 00 20 00 49 00 6e 00 74 00 75 00 6e 00 f.t. .I.n.t.u.n.
0090: 65 00 20 00 4d 00 61 00 6e 00 61 00 67 00 65 00 e. .M.a.n.a.g.e.
00a0: 6d 00 65 00 6e 00 74 00 20 00 45 00 78 00 74 00 m.e.n.t. .E.x.t.
00b0: 65 00 6e 00 73 00 69 00 6f 00 6e 00 5c 00 4d 00 e.n.s.i.o.n.\.M.
00c0: 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 i.c.r.o.s.o.f.t.
00d0: 2e 00 4d 00 61 00 6e 00 61 00 67 00 65 00 6d 00 ..M.a.n.a.g.e.m.
00e0: 65 00 6e 00 74 00 2e 00 53 00 65 00 72 00 76 00 e.n.t...S.e.r.v.
00f0: 69 00 63 00 65 00 73 00 2e 00 49 00 6e 00 74 00 i.c.e.s...I.n.t.
0100: 75 00 6e 00 65 00 57 00 69 00 6e 00 64 00 6f 00 u.n.e.W.i.n.d.o.
0110: 77 00 73 00 41 00 67 00 65 00 6e 00 74 00 2e 00 w.s.A.g.e.n.t...
0120: 65 00 78 00 65 00 00 00 00 00 00 00
```

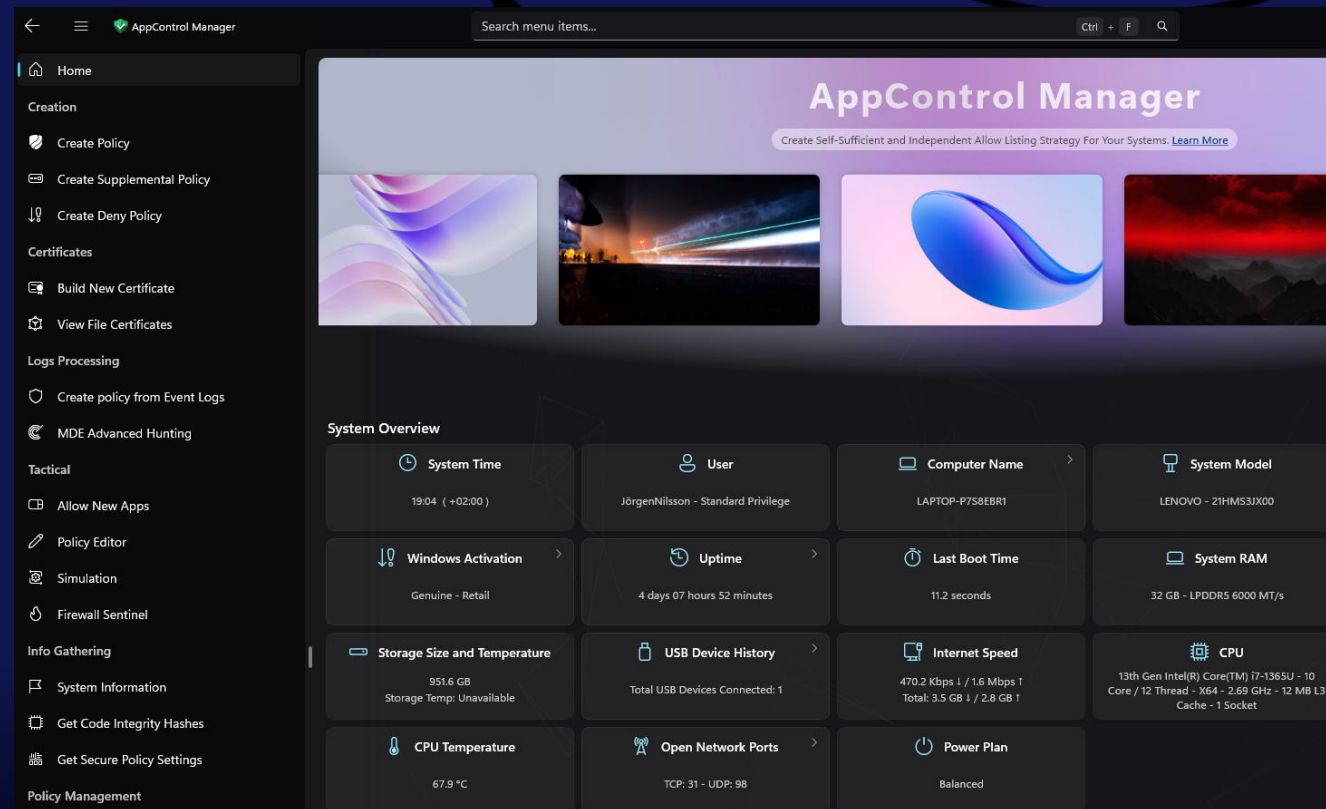
noteHelp.exe:





AppControl Manager

- ◆ Great to manage AppControl policies
- ◆ Available in the Microsoft Store
- ◆ THE tool to use to manage AppControl



The screenshot displays the AppControl Manager web interface. The left sidebar contains a navigation menu with categories: Creation (Create Policy, Create Supplemental Policy, Create Deny Policy), Certificates (Build New Certificate, View File Certificates), Logs Processing (Create policy from Event Logs, MDE Advanced Hunting), Tactical (Allow New Apps, Policy Editor, Simulation, Firewall Sentinel), Info Gathering (System Information, Get Code Integrity Hashes, Get Secure Policy Settings), and Policy Management.

The main content area features a header with the title "AppControl Manager" and a sub-header "Create Self-Sufficient and Independent Allow Listing Strategy For Your Systems. [Learn More](#)". Below the header is a "System Overview" dashboard with a grid of system metrics:

System Time	User	Computer Name	System Model
19:04 (+02:00)	JörgenNilsson - Standard Privilege	LAPTOP-P7S8EBR1	LENOVO - 21HMS3JX00
Windows Activation	Uptime	Last Boot Time	System RAM
Genuine - Retail	4 days 07 hours 52 minutes	11.2 seconds	32 GB - LPDDR5 6000 MT/s
Storage Size and Temperature	USB Device History	Internet Speed	CPU
951.6 GB Storage Temp: Unavailable	Total USB Devices Connected: 1	470.2 Kbps I / 1.6 Mbps T Total: 3.5 GB I / 2.8 GB T	13th Gen Intel(R) Core(TM) i7-1365U - 10 Core / 12 Thread - X64 - 2.69 GHz - 12 MB L3 Cache - 1 Socket
CPU Temperature	Open Network Ports	Power Plan	
67.9 °C	TCP: 31 - UDP: 98	Balanced	

<https://apps.microsoft.com/detail/9PNG1JDDTGP8?hl=en-us&gl=SE&ocid=pdpshare>

Conditional Access





Test



Welcome

MI

Microsoft Intune

0000000a-0000-0000-c000-0000000000...



MA

Microsoft Activity Feed Service

d32c68ad-72d2-4acb-a0c7-46bb2cf93873



MC

Microsoft Command Service

19686ca6-5324-4571-a231-77e026b0e06f



MD

Microsoft Device Directory Ser...

8f41dc7c-542c-4bdd-8eb3-e60543f607ca



WS

Windows Store for Business

45a330b1-b1ec-4cc1-9161-9f03992aa49f



Subscription Based activation

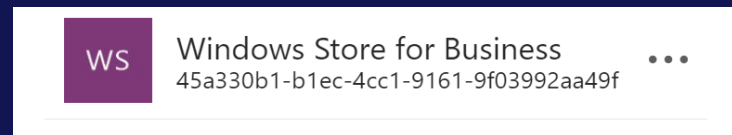


- ◆ Easiest way of upgrading to Enterprise from pro
- ◆ Re-activated every 30 days
- ◆ Each user can activate 5 devices
- ◆ Activating shared devices
 - ◆ Either all users must have a Windows e3 license assigned
 - ◆ Shared devices must be excluded and activated in a different way (KMS,MAK)
 - ◆ HKEY_Local_Machine\System\Currentcontrolset\services\clipsvc\parameters
 - ◆ Value: DisableSubscription Reg_Dword Value=1

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#existing-enterprise-deployments>

Subscription based activation

- ◆ Important: Devices will automatically “migrate” from MAK, KMS and AD-based activation to Subscription when a user with an assigned license logs on.
- ◆ Blocked by the “Work or school account problem”
- ◆ Exclude **Windows Store for business: AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f** from your Conditional Access framework.



Don't use Per-User MFA, should change to Disabled

Home >

Per-user multifactor authentication

Bulk update | Got feedback?

This is the new per-user MFA management experience. For the legacy experience please click [here](#).

Users | Service settings

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive C...

Before you begin, take a look at the [multifactor authentication deployment guide](#).

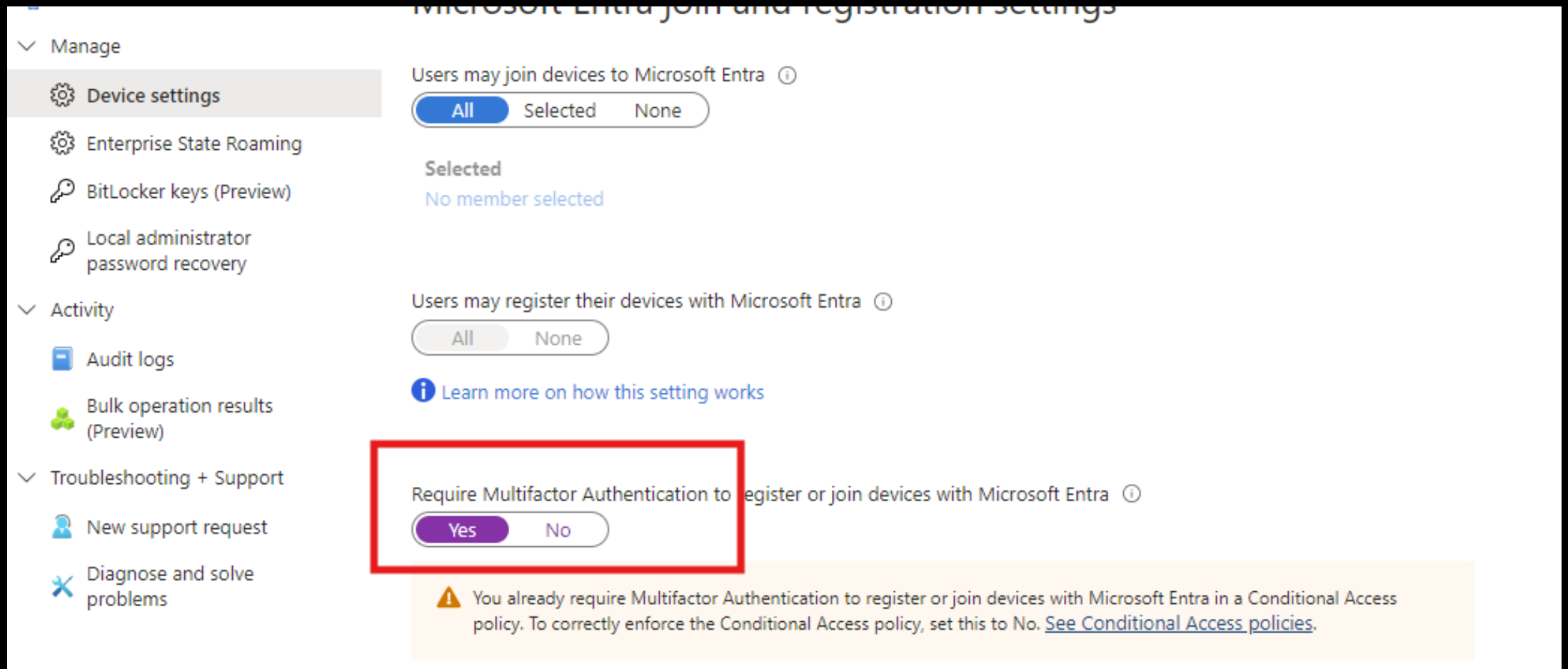
Enable MFA | Disable MFA | Enforce MFA | User MFA settings

Search

Status: All | View: Sign-in allowed users

<input type="checkbox"/>	Name ↓	UPN	Status
<input type="checkbox"/>	Admin	admin@mvp24.onmicrosoft.com	Disabled
<input type="checkbox"/>	Modern Device Management	ModernDeviceManagement@mvp24.onmicrosoft.com	Disabled
<input type="checkbox"/>	BreakOut2	BreakOut2@mvp24.onmicrosoft.com	Disabled
<input type="checkbox"/>	On-Premises Directory Synchroni...	Sync_ADCONNECT_d98c2c1d9e36@mvp24.onmicrosoft.cc	Disabled
<input type="checkbox"/>	Sandy Zeng	sandy@smsboot.com	Disabled
<input type="checkbox"/>	no-reply	no-reply@smsboot.com	Enabled
<input type="checkbox"/>	On-Premises Directory Synchroni...	Sync_ADCONNECT_581eb620be72@mvp24.onmicrosoft.c	Disabled

Don't use enforce MFA here, you should change it to No, and use Conditional Access policy instead



Microsoft Entra join and registration settings

Manage

- Device settings
- Enterprise State Roaming
- BitLocker keys (Preview)
- Local administrator password recovery

Activity

- Audit logs
- Bulk operation results (Preview)

Troubleshooting + Support

- New support request
- Diagnose and solve problems

Users may join devices to Microsoft Entra ⓘ

All Selected None

Selected

No member selected

Users may register their devices with Microsoft Entra ⓘ

All None

Learn more on how this setting works

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

Yes No

⚠ You already require Multifactor Authentication to register or join devices with Microsoft Entra in a Conditional Access policy. To correctly enforce the Conditional Access policy, set this to No. [See Conditional Access policies.](#)

Updates



Quality update errors

- ◆ We have seen an increase in Quality updates errors during 2025

DISM.log

2025-08-06 15:02:44, Info CBS Exec: Processing complete. Session: 31196882_605738186, Package: HyperV-OptionalFeature-VirtualMachinePlatform-Client-Disabled-FOD-Package~31bf3856ad364e35~amd64~~10.0.26100.1, Identifier: KB777778 [HRESULT = 0x80073712 -

ERROR_SXS_COMPONENT_STORE_CORRUPT]

2025-08-06 15:02:44, Error CBS Failed to perform operation. [HRESULT = 0x80073712 -
ERROR_SXS_COMPONENT_STORE_CORRUPT]

2026/3/19:22:40:58.012 (F) Attempting to mark store corrupt with category [1:21 ml:22]'CorruptComponentValue'[gle=0x80004005]
c able to find \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\amd64_microsoft-wind
c find WindowsCopilot.adml in component Microsoft-Windows-Shell-GroupPolicy.Resources, version 10.0.26100.7920, arch amd64, culture [1:5]'sv-SE', nonSxS, pkt {
Moved file \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\amd64_microsoft-windows-
5) Staging WindowsInkWorkspace.adml (FD)
c able to find \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\WinSxS\amd64_microsof
c able to find \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\amd64_microsoft-wind
Component Microsoft-Windows-Shell-GroupPolicy.Resources, version 10.0.26100.7920, arch amd64, culture [1:5]'fi-FI', nonSxS, pkt {1:8 b:31bf3856ad364e35} does
(F) Component directory missing. Dir: \SystemRoot\WinSxS\amd64_microsoft-windows-s..ouppolicy.resources_31bf3856ad364e35_10.0.26100.712_fi-fi_6408f8a0487d62b0
2026/3/19:22:40:58.012 (F) onecore\base\wcp\componentstore\storelayout.cpp(2203): Error 800f0983 [Warning, Facility=15 (0x000f), Code=2435 (0x0983)] originated

2026/3/19:22:40:58.012 (F) Attempting to mark store corrupt with category [1:21 ml:22]'CorruptComponentValue'[gle=0x80004005]
c find WindowsInkWorkspace.adml in component Microsoft-Windows-Shell-GroupPolicy.Resources, version 10.0.26100.7920, arch amd64, culture [1:5]'fi-FI', nonSxS,
Moved file \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\amd64_microsoft-windows-
4) Staging WindowsInkWorkspace.adml (FD)
c able to find \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\WinSxS\amd64_microsof
c able to find \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\amd64_microsoft-wind
Component Microsoft-Windows-Shell-GroupPolicy.Resources, version 10.0.26100.7920, arch amd64, culture [1:5]'nb-NO', nonSxS, pkt {1:8 b:31bf3856ad364e35} does
(F) Component directory missing. Dir: \SystemRoot\WinSxS\amd64_microsoft-windows-s..ouppolicy.resources_31bf3856ad364e35_10.0.26100.712_nb-no_7fef3d2fdb187113
2026/3/19:22:40:58.012 (F) onecore\base\wcp\componentstore\storelayout.cpp(2203): Error 800f0983 [Warning, Facility=15 (0x000f), Code=2435 (0x0983)] originated

2026/3/19:22:40:58.012 (F) Attempting to mark store corrupt with category [1:21 ml:22]'CorruptComponentValue'[gle=0x80004005]
c find WindowsInkWorkspace.adml in component Microsoft-Windows-Shell-GroupPolicy.Resources, version 10.0.26100.7920, arch amd64, culture [1:5]'nb-NO', nonSxS,
Moved file \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\amd64_microsoft-windows-
50) Staging WindowsInkWorkspace.adml (FD)
c able to find \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\WinSxS\amd64_microsof
Component Microsoft-Windows-Shell-GroupPolicy.Resources, version 10.0.26100.7920, arch amd64, culture [1:5]'sv-SE', nonSxS, pkt {1:8 b:31bf3856ad364e35} does
c able to find \\?\C:\Windows\SoftwareDistribution\Download\3098c1ec1634ae859359ccf1e1bd5a23\Package_for_RollupFix~~amd64~~26100.8037.1.19\amd64_microsoft-wind
(F) Component directory missing. Dir: \SystemRoot\WinSxS\amd64_microsoft-windows-s..ouppolicy.resources_31bf3856ad364e35_10.0.26100.712_sv-se_aa3e99389b6a84e3
2026/3/19:22:40:58.012 (F) onecore\base\wcp\componentstore\storelayout.cpp(2203): Error 800f0983 [Warning, Facility=15 (0x000f), Code=2435 (0x0983)] originated



DEMO

Troubleshoot updates



Windows Update



Updates failed

Your device is missing important security updates. Make sure to keep your device on and plugged in so updates can complete.

Retry all

2025-08 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5063878) (26100.4946)

Some update files are missing or have problems. We'll try to download the update again later. Error code: (0x80073712)

Retry

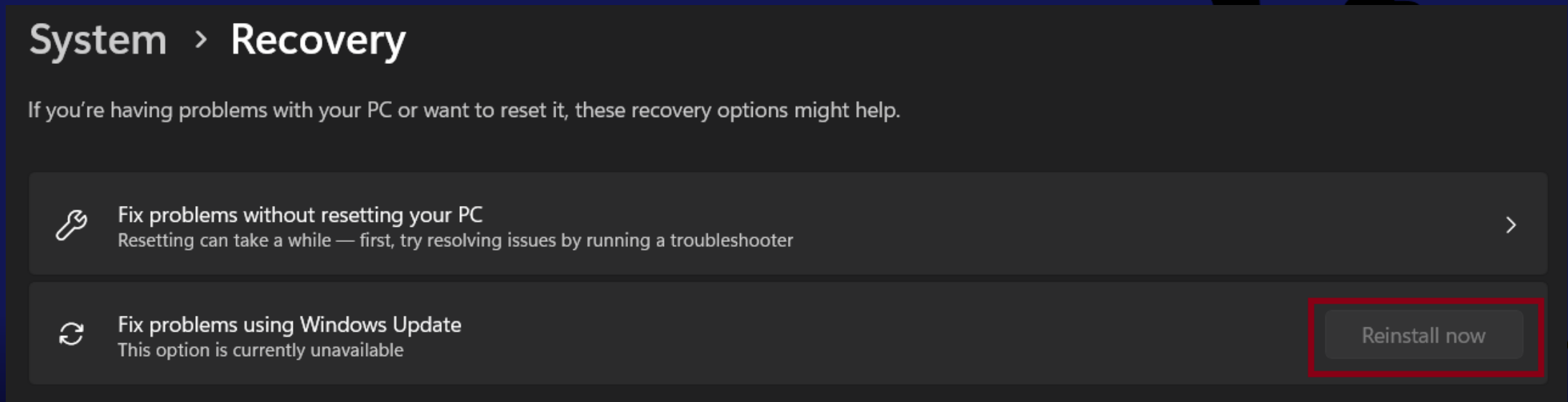
! Reinstall your current version of Windows to repair system files and components

Reinstall Now



Quality updates

- ◆ Solution: in-place upgrade to the same version of Windows 11!
 1. Win32app with the Windows 11 installation files
 2. `setup.exe /auto upgrade /eula accept /DynamicUpdate disable`



SAVE THE DATES

Oct 25-28, 2026



May 2-6, 2027



Oct 10-13, 2027



Extended Q&A



2Pint

Recast

robopack
empowered by SOFTWARE
CENTRAL

SquaredUp

CODETWO

baramundi

ninjaOne

Rimo3



TeamViewer

numecent

aiden

When do we need to troubleshoot?

- ◆ What is the expectation? Should it actually work like this?
- ◆ Configuration is indeed wrong
- ◆ Always check Service Health and message center

The screenshot displays the 'Service health and message center' page for a tenant. It is divided into three main sections: Service health, Issues in your environment that require action, and Message center.

Service health (1 active):

Title	Service	ID	Status	User impact	Start time	Updated
Some managed devices ...	Microsoft Intune	IT1028182	Service degradation	Affected devices can't receive ...	3/11/2025, 2:21:06 AM	3/21/2025, 6:47:55 PM

Issues in your environment that require action (0 active):

No active incidents or advisories.

Message center (13 active):

Message title	Service	Act by	Category	Published	Message ID
Planned Maintenance: Intune Service	Microsoft Intune	4/19/2025	Plan for change	3/20/2025	MC1036573
Plan for Change: Enhanced Security for Windows 365 Cl...	Windows 365		Plan for change	3/19/2025	MC1035715

Service health

1 active

ⓘ Add filters

Title	↑↓ Service	↑↓ ID	↑↓ Status	↑↓ User impact	↑↓ Start time	↑↓ Updated
Some managed devices ...	Microsoft Intune	IT1028182	Service degradation	Affected devices can't receive ...	3/11/2025, 2:21:06 AM	3/21/2025, 6:47:55 PM

[See past incidents/advisories](#)

Issues in your environment that require action

0 active

ⓘ Add filters

Title	↑↓ Service	↑↓ ID	↑↓ Status	↑↓ User impact	↑↓ Start time	↑↓ Updated
No active incidents or advisories						

[See past incidents/advisories](#)

Message center

13 active

ⓘ Add filters

Message title	↑↓ Service	↑↓ Act by	↑↓ Category	↑↓ Published	↑↓ Message ID
Planned Maintenance: Intune Service	Microsoft Intune	4/19/2025	Plan for change	3/20/2025	MC1036573
Plan for Change: Enhanced Security for Windows 365 Clo	Windows 365		Plan for change	3/19/2025	MC1035715





Support



Settings



Setup



Reports



Health



Service health

Windows release health

Message center

Product feedback

Network connectivity

Directory sync status

Software updates

Service health

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscription.

Report an issue Customize

Active issues Microsoft is working on

Issue title

Some managed devices can't receive configurations, apps, and policies from Microsoft

Service status

Service	Status
Microsoft Intune	1 advisory
Microsoft Clipchamp	Healthy
Microsoft Entra	Healthy
OneDrive for Business	Healthy
Universal Print	Healthy

Customize

Page view Email

Send me email notifications about service health

Enter up to 2 email addresses, separated by a semicolon

Include these issue types *

- Incidents
- Advisories
- Issues in your environment that require action

Include these services *



- Dynamics 365 Apps
- Exchange Online
- Microsoft 365 apps
- Microsoft 365 for the web
- Microsoft 365 suite
- Microsoft Bookings

Save

Service health

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscrip






 Report an issue  Customize

Active issues Microsoft is working on

Issue title

Some managed devices can't receive configurations, apps, and policies from Microsoft

Service status

Service	Status
Microsoft Intune	 1 advisory
Microsoft Clipchamp	 Healthy
Microsoft Entra	 Healthy
OneDrive for Business	 Healthy
Universal Print	 Healthy



Customize

Page view **Email**

Send me email notifications about service health

Enter up to 2 email addresses, separated by a semicolon

Include these issue types *

- Incidents
- Advisories
- Issues in your environment that require action

Include these services *

- Dynamics 365 Apps
- Exchange Online
- Microsoft 365 apps
- Microsoft 365 for the web
- Microsoft 365 suite
- Microsoft Bookings


Save


Windows release health

May 10, 2025, 9:00 PM GMT

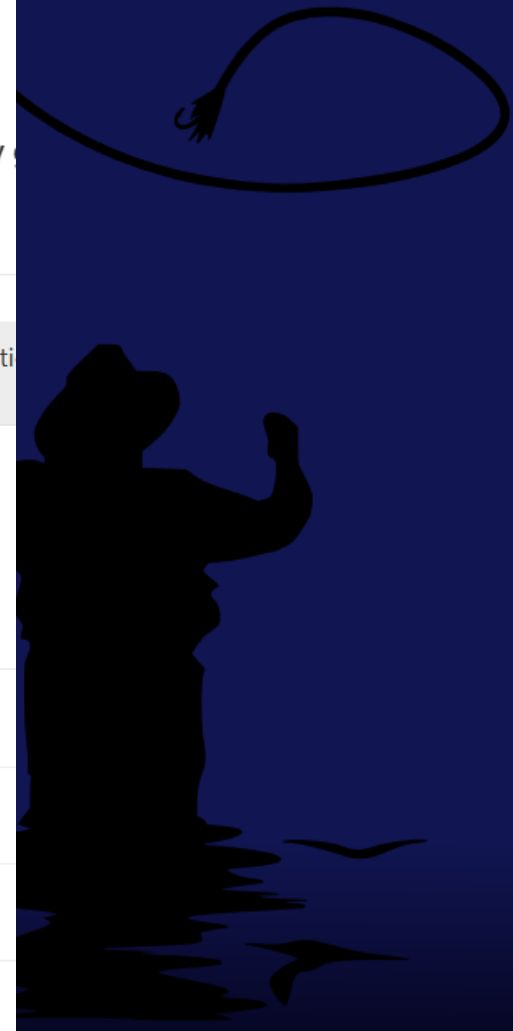
All versions Known Issues History

Find information about known issues for currently supported versions of the Windows operating system. To programmatically access this known issue information, use the [Windows Updates API in Microsoft Graph](#)

 We are now offering Windows release health known issue email notifications. Please select the Preferences icon to customize your email notification settings.

 Preferences

Version ↓	Active and recently resolved	History
Windows 11, version 24H2	View	View
Windows 11, version 23H2	View	View
Windows 11, version 22H2	View	View
Windows 11, version 21H2	No Issues	No Issues



Logon might fail with Windows Hello in Key Trust mode...



Windows release health <winhealth-noreply@microsoft.com>
To yinghua.ts@hotmail.com

Reply

If there are problems with how this message is displayed, click here to view it in a web browser.



Logon might fail with Windows Hello in Key Trust mode and log Kerberos Events

Status

Confirmed

Affected platforms

Server Versions	Message ID	Originating KB	Resolved KB
Windows Server 2025	WI1068853	KB5055523	-
Windows Server 2022	WI1068854	KB5055526	-
Windows Server 2019	WI1068855	KB5055519	-

Message center

Each message gives you a high-level overview of a planned change and how it may affect your users, and links out to more detailed information to help you prepare. [Learn more about message changes](#)

Inbox Archive

⚙ Preferences ⚙ Planner syncing

Filters: Service Tag Message state Relevance Status for your org

- Message title ☆
- The March 2025 Windows non-security preview update is now available for some supported versions of Windows** ⋮
- Planned Maintenance: Group and filter membership rule update** ⋮
- (Updated) Final Reminder: Upgrade to the latest version of Microsoft Entra Connect Sync by April 7, 2025 to avoid impact** ⋮
- Planned Maintenance: Intune Service** ⋮
- (Updated) Device Management Changes for Microsoft Teams Android Devices (Intune AOSP migration)** ⋮

Preferences

- Primary e-mail address: (admin@mvp24.onmicrosoft.com)
- Other e-mail addresses

Enter up to two email addresses, separated by a semicolon.

Choose which emails you want to get

We may occasionally notify you about important updates that aren't covered by these settings.

- Send me emails for major updates
- Send me emails for data privacy messages
- Send me a weekly digest about services I select
 - Basic Mobility & Security
 - Dynamics 365 Apps
 - Exchange Online
 - General announcement
 - Microsoft 365 Apps
 - Microsoft 365 for the web
 - Microsoft 365 suite
 - Microsoft Bookings
 - Microsoft Clipchamp

Save

Intune troubleshooting

◆ Aka.ms/Intunetroubleshooting

Home > Troubleshooting + support

Troubleshooting + support | Troubleshoot

Search

User: Jane Doe

Device: Filter by device

Guided scenarios (preview)

Troubleshoot

Help and support

Jane Doe
Email: Jane@demiranda.nu
User principal name: Jane@demiranda.nu

User status

- Account enabled
- Intune licensed

Summary | Devices | Groups | Policy | Applications | App protection policy | Updates | Enrollment restrictions | Diagnostics

Policy

Compliant	Error	Non compliant	Conflict	Pending	Not applicable
263	21	1	18	0	14

Compliance

Compliant	Error	Non compliant	Conflict	Pending	Not applicable
16	0	8	0	0	10

Who made a change?

- ◆ Audit Logs for the win!
- ◆ Send diagnostic settings to:
 - ◆ Log Analytics
 - ◆ Storage account
 - ◆ Stream to event hub
 - ◆ Partner solution

Diagnostic setting ...

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

Logs

Categories

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg
- Devices
- Windows365AuditLogs

Destination details

- Send to Log Analytics workspace
- Archive to a storage account
- Stream to an event hub
- Send to partner solution

◆ <https://msendpointmgr.com/2022/10/28/msendpointmgr-intune-audit-dashboard/>

Intune Audit Dashboard

This dashboard provides an overview of administrative actions carried out within the Intune environment.

Dashboards include:

- Actions over time
- Top accounts performing actions
- Full audit details with filtering and hyperlinked details page

This report uses the Intune Audit log to render data. The last update time is listed to the right.

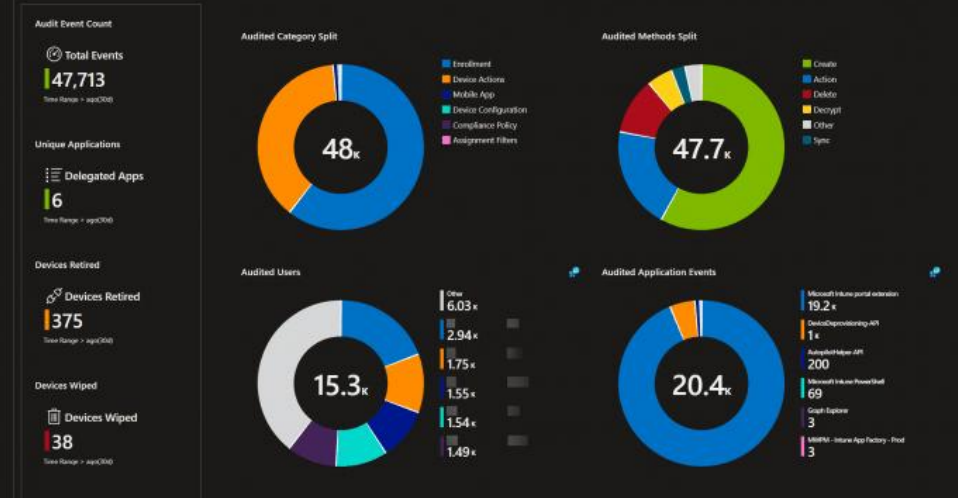
Type: IntuneAuditLogs | TimeGenerated: 10/28/2022 2:12:33 PM | Service State: Service OK

Time Range: Last 30 days

Summary | Device Targeted Actions | Targeted Actions | Admin Actions | Application Actions | Detailed Audit Log

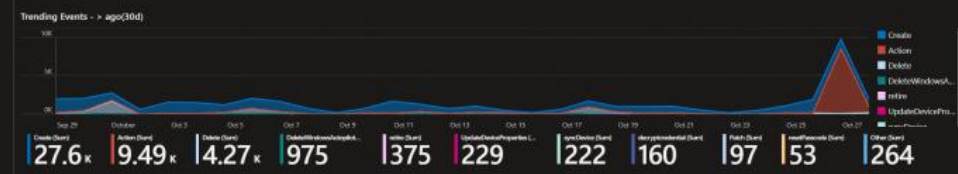
Audit Summary

Below are summaries of the main audited functions over the previous Last 30 days. Clicking on each of the tabs will allow you to drill down and display more specific data.



Trending Events

The below trend graphs provide an overview of the actions carried out in your tenant on a daily basis over the previous Last 30 days.



Test device registration connectivity

```
=====
Test Device Registration Connectivity
=====

Test-DeviceRegConnectivity log file has been created.

Testing Internet Connectivity...
Checking winHTTP proxy settings...
    Access Type : DIRECT

Checking winInet proxy settings...
    Proxy Enabled : No
    Proxy Server List :
    Proxy Bypass List :
    AutoConfigURL :

Testing Device Registration Endpoints...
Testing connection via winInet...

Connection to login.microsoftonline.com ..... Succeeded.
Connection to device.login.microsoftonline.com ..... Succeeded.
Connection to enterpriseregistration.windows.net ..... Succeeded.

Test passed: Device is able to communicate with MS endpoints successfully under system context

Script completed successfully.
```

[Test Device Registration Connectivity - Code Samples | Microsoft Learn](#)

Troubleshoot registration

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

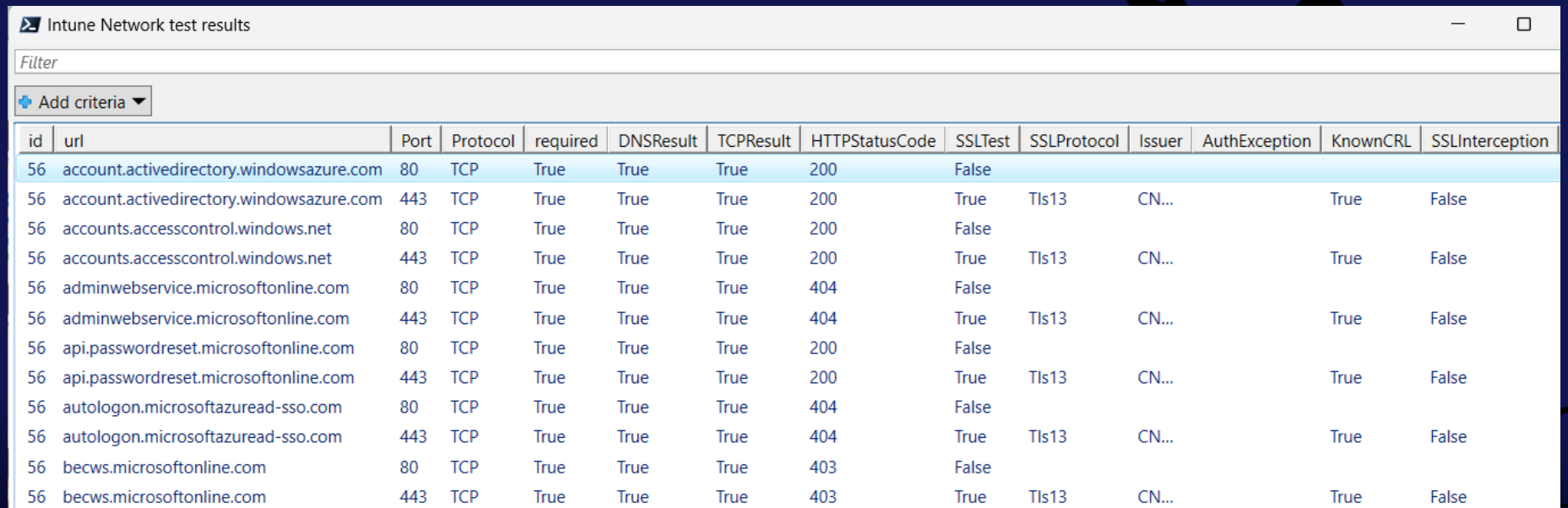
DSRegTool log file has been created.

Please make a selection, and press Enter:

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

Intune Network Requirements

- ◆ By Martin Himken (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, all with an id of 56. The results show that all tests passed (DNSResult, TCPResult, and HTTPStatusCode are all True or 200/403/404, and SSLTest is True or False).

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-ss.com	80	TCP	True	True	True	404	False					
56	autologon.microsoftazuread-ss.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

SSL traffic inspection = BAD

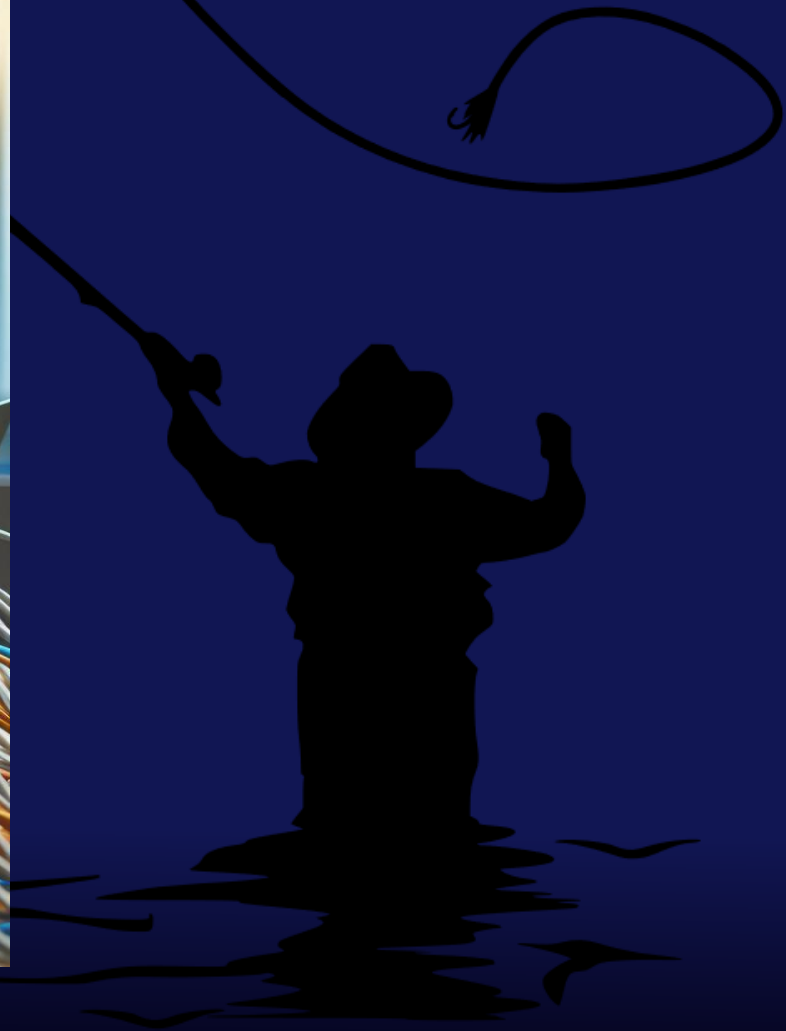
- ◆ Must exclude necessary endpoints
- ◆ Example on results

ⓘ 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

Your new network admin



Conditional Access

Conditional Access done correctly is a win!

Conditional Access done incorrectly is an EPIC fail!

Why so many prompts during Autopilot?

Pay attention to the apps you are targeting

Select what this policy applies to

User actions

Select the action this policy will apply to

Register security information

Register or join devices

MI Microsoft Intune Enrollment d4ebce55-015a-49b5-a083-c84d1797ae...

MI Microsoft Intune 0000000a-0000-0000-c000-0000000000...

WS Windows Store for Business 45a330b1-b1ec-4cc1-9161-9f03992aa49f

Don't use Per-User MFA, should change to Disabled

Home >

Per-user multifactor authentication

Bulk update | Got feedback?

This is the new per-user MFA management experience. For the legacy experience please click [here](#).

Users | Service settings

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive C...

Before you begin, take a look at the [multifactor authentication deployment guide](#).

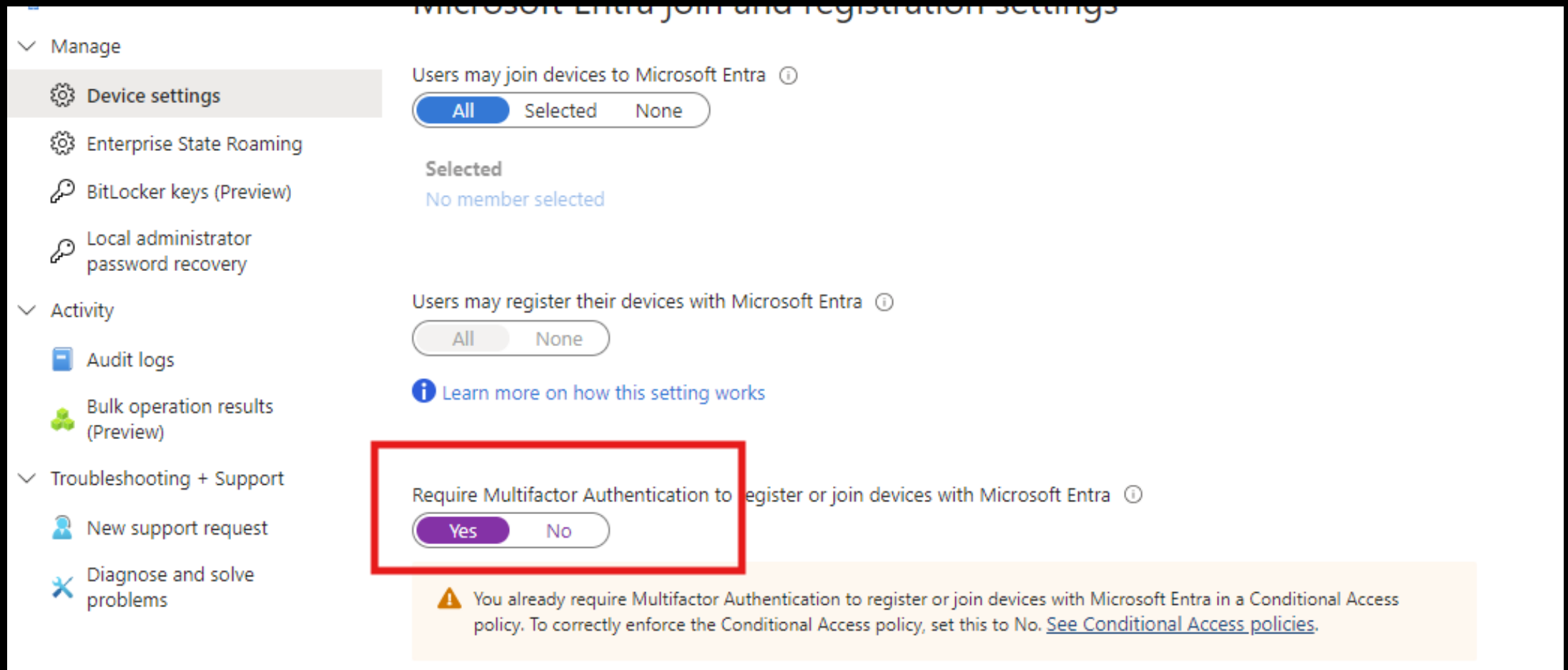
Enable MFA | Disable MFA | Enforce MFA | User MFA settings

Search

Status: All | View: Sign-in allowed users

<input type="checkbox"/>	Name ↓	UPN	Status
<input type="checkbox"/>	Admin	admin@mvp24.onmicrosoft.com	Disabled
<input type="checkbox"/>	Modern Device Management	ModernDeviceManagement@mvp24.onmicrosoft.com	Disabled
<input type="checkbox"/>	BreakOut2	BreakOut2@mvp24.onmicrosoft.com	Disabled
<input type="checkbox"/>	On-Premises Directory Synchroni...	Sync_ADCONNECT_d98c2c1d9e36@mvp24.onmicrosoft.cc	Disabled
<input type="checkbox"/>	Sandy Zeng	sandy@smsboot.com	Disabled
<input type="checkbox"/>	no-reply	no-reply@smsboot.com	Enabled
<input type="checkbox"/>	On-Premises Directory Synchroni...	Sync_ADCONNECT_581eb620be72@mvp24.onmicrosoft.c	Disabled

Don't use enforce MFA here, you should change it to No, and use Conditional Access policy instead



Microsoft Entra join and registration settings

Manage

- Device settings
- Enterprise State Roaming
- BitLocker keys (Preview)
- Local administrator password recovery

Activity

- Audit logs
- Bulk operation results (Preview)

Troubleshooting + Support

- New support request
- Diagnose and solve problems

Users may join devices to Microsoft Entra ⓘ

All Selected None

Selected

No member selected

Users may register their devices with Microsoft Entra ⓘ

All None

Learn more on how this setting works

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

Yes No

⚠ You already require Multifactor Authentication to register or join devices with Microsoft Entra in a Conditional Access policy. To correctly enforce the Conditional Access policy, set this to No. [See Conditional Access policies.](#)

Subscription Based activation

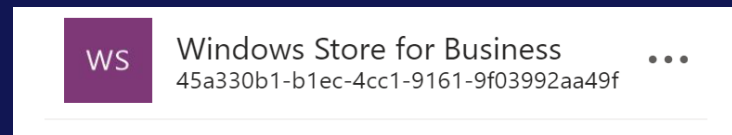


- ◆ Easiest way of upgrading to Enterprise from pro
- ◆ Re-activated every 30 days
- ◆ Each user can activate 5 devices
- ◆ Activating shared devices
 - ◆ Either all users must have a Windows e3 license assigned
 - ◆ Shared devices must be excluded and activated in a different way (KMS,MAK)
 - ◆ HKEY_Local_Machine\System\Currentcontrolset\services\clipsvc\parameters
 - ◆ Value: DisableSubscription Reg_Dword Value=1

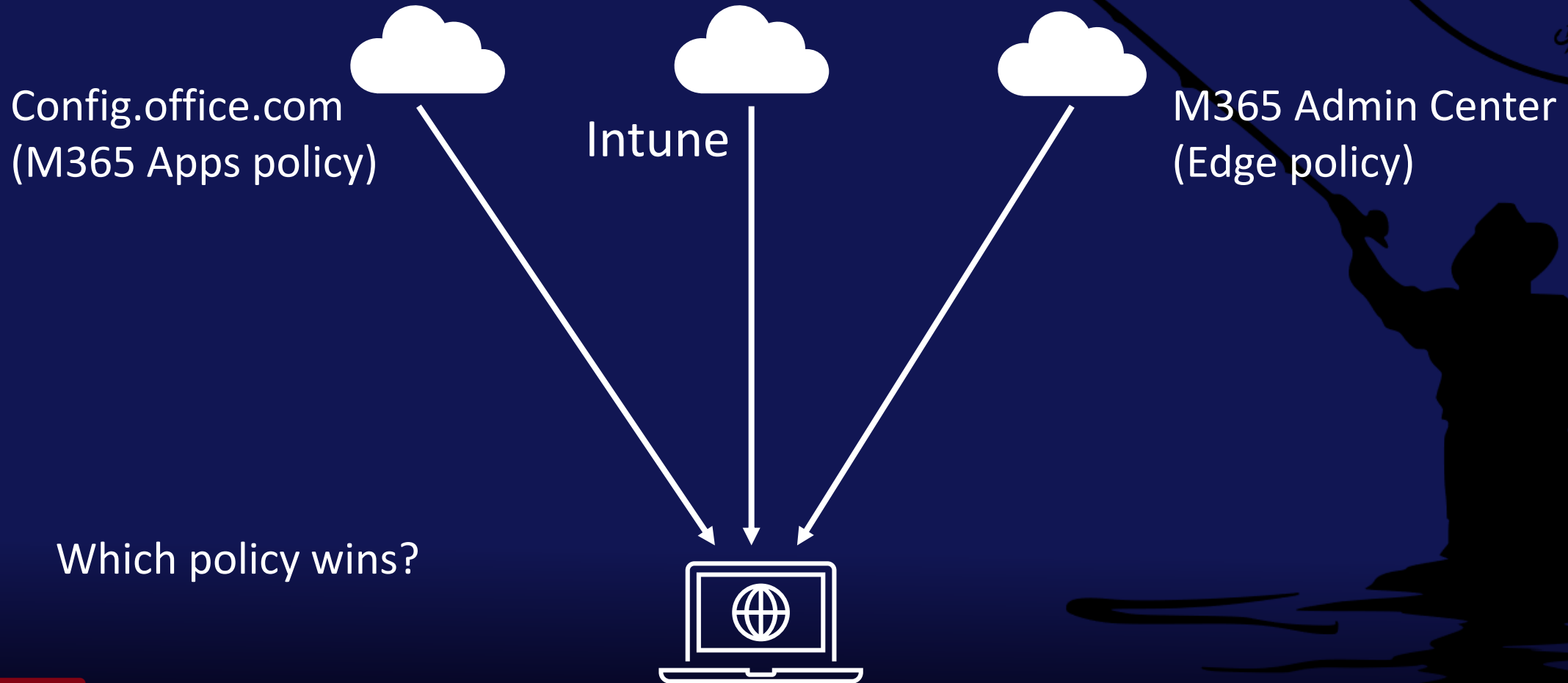
<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#existing-enterprise-deployments>

Subscription based activation

- ◆ Important: Devices will automatically “migrate” from MAK, KMS and AD-based activation to Subscription when a user with an assigned license logs on.
- ◆ Blocked by the “Work or school account problem”
- ◆ Exclude **Windows Store for business: AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f** from your Conditional Access framework.

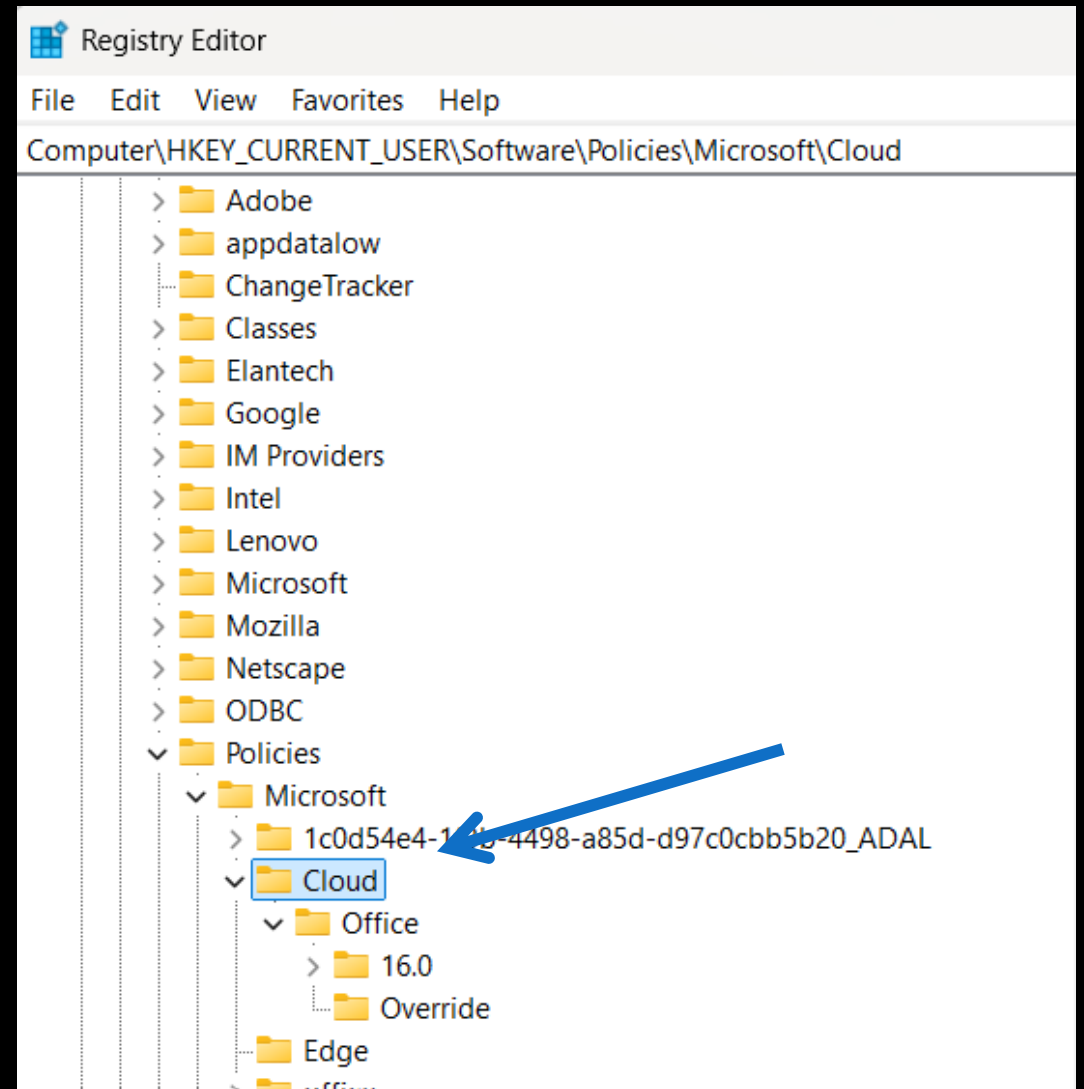


More than Intune policies



M365 cloud policy <https://config.office.com/>

- Let you enforce policy settings for Microsoft 365 Apps for enterprise on a user's device, even if the device isn't domain joined or otherwise managed
- Policies from Cloud Policy are applied only when the Office app is restarted
- Cloud Policy includes many of the same **user-based** policy settings that are available in Group Policy
- Policy settings implemented by using Cloud Policy **take precedence** over Group Policy on Windows Server, and taking precedence over preference settings or locally applied policy settings



M365 cloud policy vs. Intune policies

- Our test result:
 - It get messy when using Intune configure **computer-based** settings conflict with Cloud policy **user-based** settings. Unexpected result
 - Intune **user-based** settings vs Cloud policy **user-based** settings: Cloud Policy wins.
 - Don't do conflict, manage your settings from one place!!!

Edge Management Service vs. Intune

[ShowHomeButton](#)

false

Platform

Current user

Mandatory

Warning, Conflict



Value false

Warning More than one source with conflicting values is present for this policy!

Conflict true

Cloud

Current user

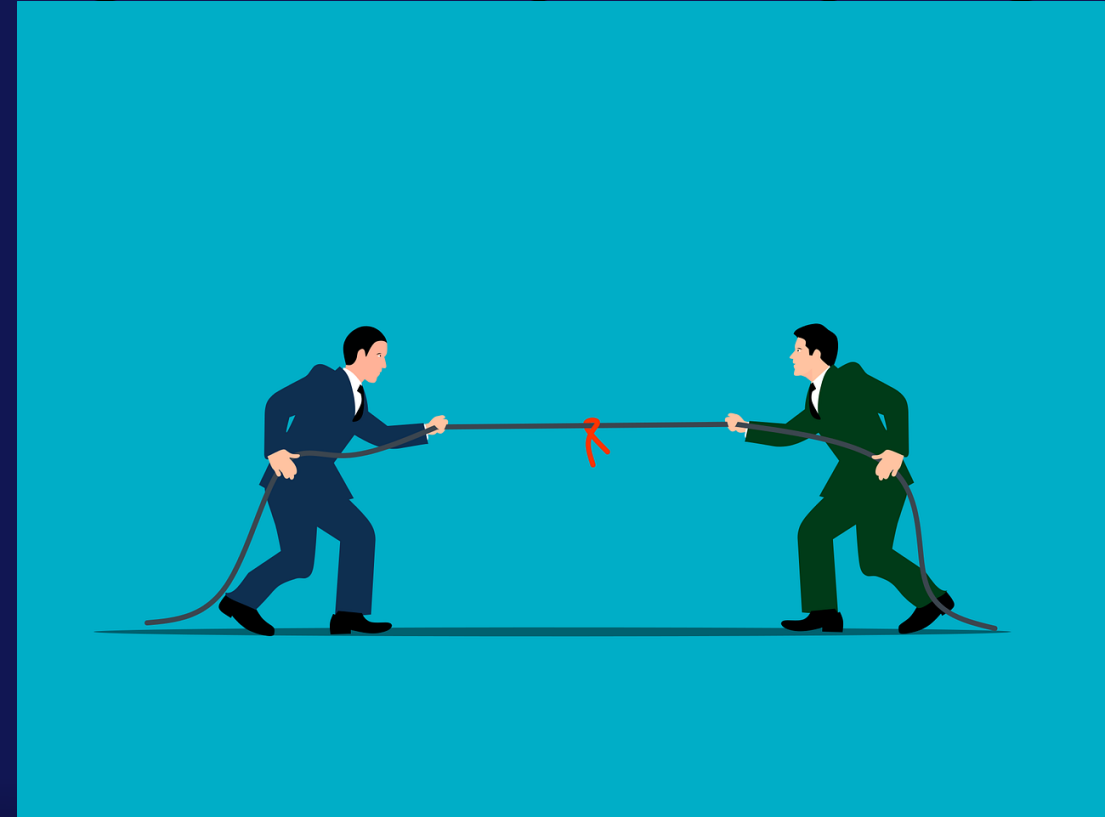
Mandatory

Two policies can be used to change this:

- ◆ EdgeManagementPolicyOverridesPlatformPolicy
- ◆ EdgeManagementUserPolicyOverridesCloudMachinePolicy

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.

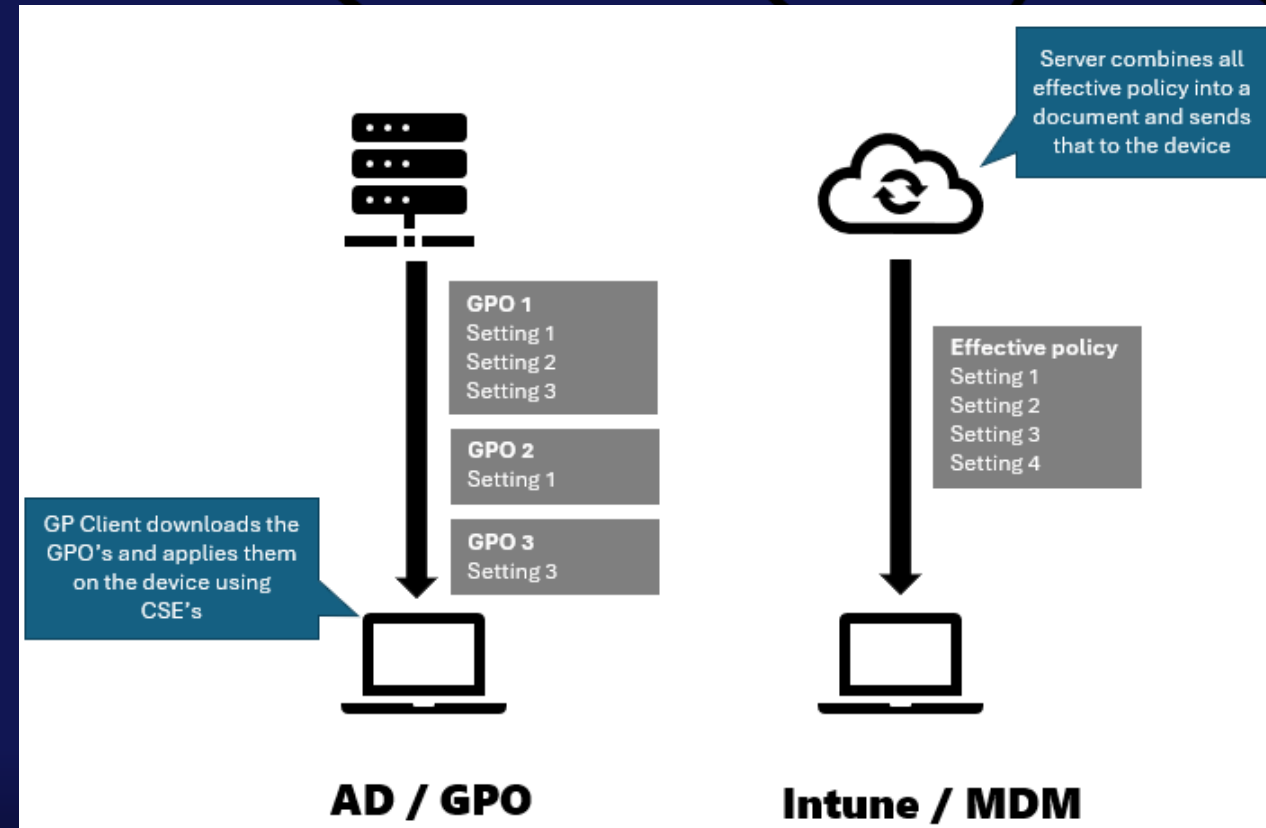


Intune policy

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



Policy - Sync

Scheduled check-in	Interval	Duration
New enrollment	3 minutes	15 minutes
New enrollment	15 minutes	2 hours
	8 hours	∞

- ◆ **Admin check-in** = Intune Portal, Sync, remote lock...
- ◆ **End user driven check-ins** = Manual sync – Company Portal, settings
- ◆ **Notification-based check-ins** = policy, profile, or app change...
(available apps deployed to user does not trigger a check-in)

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)

Removing a policy

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

ⓘ Note

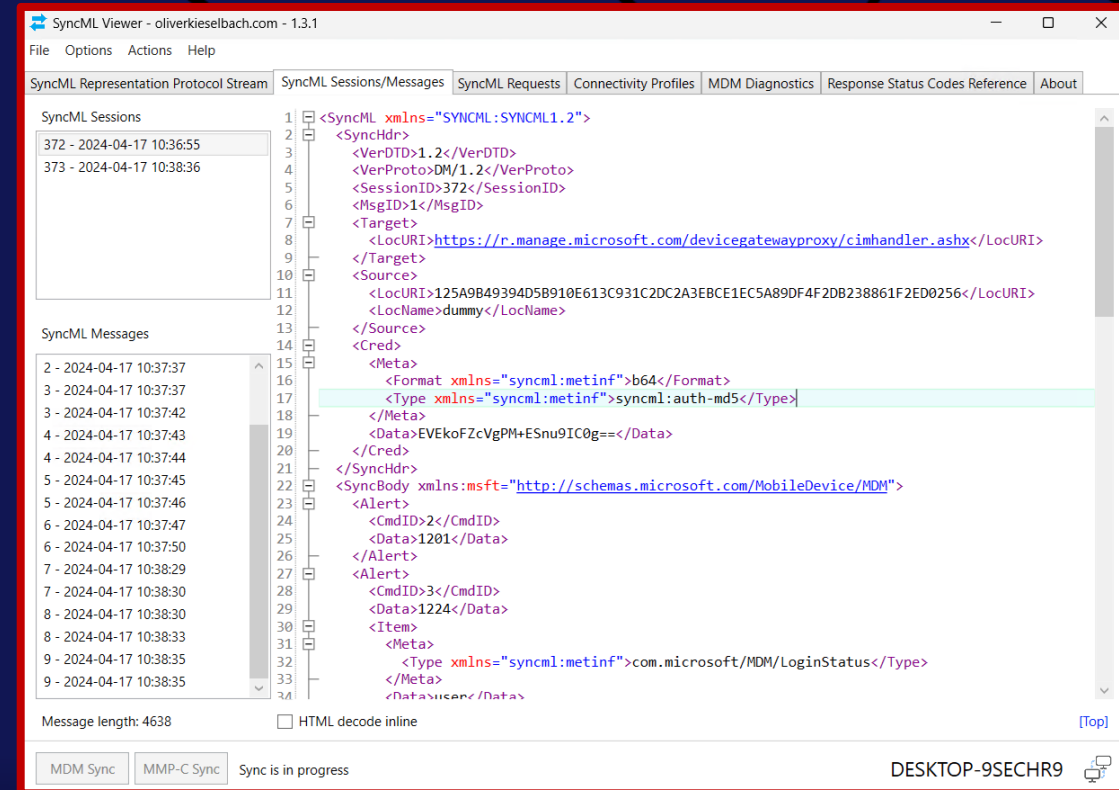
When a profile is removed or no longer assigned to a device, different things can happen, depending on the settings in the profile. The settings are based on CSPs, and each CSP can handle the profile removal differently. For example, a setting might keep the existing value, and not revert back to a default 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](#).

SyncMLViewer

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



The screenshot shows the SyncML Viewer application interface. The main window displays an XML stream for a SyncML session. The XML content is as follows:

```
<SyncML xmlns="SYNCHML:1.2">
  <SyncHdr>
    <VerDTD>1.2</VerDTD>
    <VerProto>DM/1.2</VerProto>
    <SessionID>372</SessionID>
    <MsgID>1</MsgID>
    <Target>
      <LocURI>https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx</LocURI>
    </Target>
    <Source>
      <LocURI>125A9B49394D5B910E613C931C2DC2A3EBCE1EC5A89DF4F2DB238861F2ED0256</LocURI>
      <LocName>dummy</LocName>
    </Source>
    <Cred>
      <Meta>
        <Format xmlns="syncml:metinf">b64</Format>
        <Type xmlns="syncml:metinf">syncml:auth-md5</Type>
      </Meta>
      <Data>EVEkoFzCvgPM+ESnu9IC0g==</Data>
    </Cred>
  </SyncHdr>
  <SyncBody xmlns:mft="http://schemas.microsoft.com/MobileDevice/MDM">
    <Alert>
      <CmdID>2</CmdID>
      <Data>1201</Data>
    </Alert>
    <Alert>
      <CmdID>3</CmdID>
      <Data>1224</Data>
    </Alert>
    <Item>
      <Meta>
        <Type xmlns="syncml:metinf">com.microsoft/MDM/LoginStatus</Type>
      </Meta>
      <Data>user</Data>
    </Item>
  </SyncBody>
</SyncML>
```

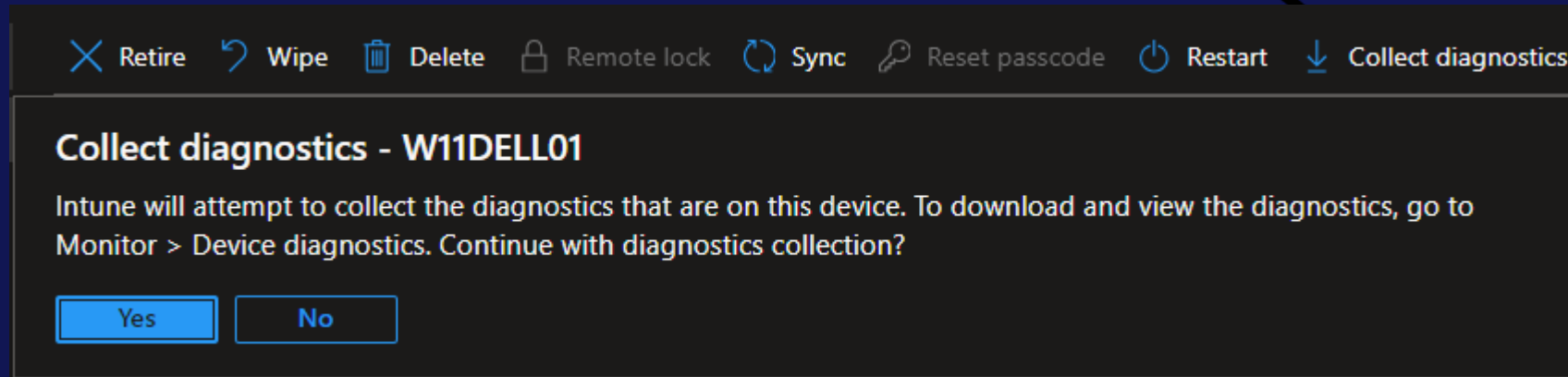
The interface includes a menu bar (File, Options, Actions, Help), a tabbed view (SyncML Sessions/Messages, SyncML Requests, Connectivity Profiles, MDM Diagnostics, Response Status Codes, Reference, About), and a status bar at the bottom showing "MDM Sync", "MMP-C Sync", and "Sync is in progress". The system tray shows "DESKTOP-9SECHR9".

Troubleshooting collect client logs



Manually collect diagnostic logs

- ◆ “Collect diagnostics” button from Intune

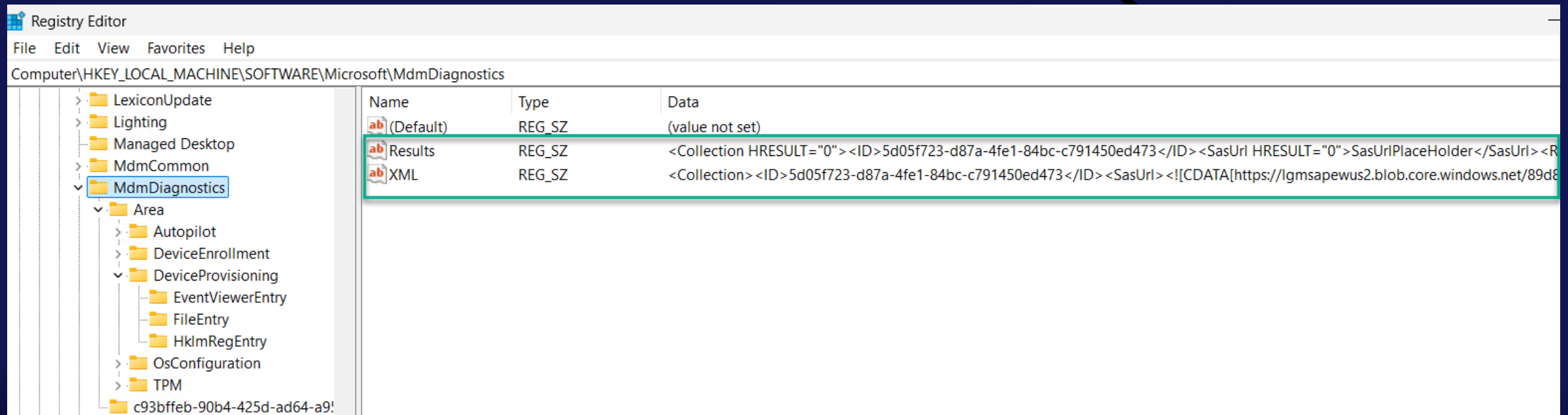


- ◆ Run command locally in the device
 - ◆ `mdmdiagnosticstool.exe -area`

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

Intune triggered collect diagnostics results

- Check from the device registry:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MdmDiagnostics



Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MdmDiagnostics

Name	Type	Data
(Default)	REG_SZ	(value not set)
Results	REG_SZ	<Collection HRESULT="0"><ID>5d05f723-d87a-4fe1-84bc-c791450ed473</ID><SasUrl HRESULT="0">SasUrlPlaceholder</SasUrl><R
XML	REG_SZ	<Collection><ID>5d05f723-d87a-4fe1-84bc-c791450ed473</ID><SasUrl><![CDATA[https://lgmsapewus2.blob.core.windows.net/89d8

- Download the logs
- The diagnostic collection is stored for 28 days

Home > Devices | Windows > Windows | Windows devices > ZIT-H-001

ZIT-H-001 | Device diagnostics

Search: diga

Refresh Columns

Monitor

- Device diagnostics
- Remediations (preview)

Requested by	Status	Request initiated	Diagnostics uploaded	
admin@mvp24.onmicrosoft.com	Complete	4/14/2025, 10:28:46 AM	4/15/2025, 2:11:38 AM	...

Download

- Don't forgot network requirement

ⓘ Note

For diagnostics to be able to upload successfully from the client, make sure that the URL for your region isn't blocked on the network:

- Europe - `lgmsapeweu.blob.core.windows.net`
- Americas - `lgmsapewus2.blob.core.windows.net`
- East Asia - `lgmsapesea.blob.core.windows.net`
- Australia - `lgmsapeaus.blob.core.windows.net`
- India - `lgmsapeind.blob.core.windows.net`

How to add more logs or events

From the XML result, we see it triggers command:
mdmdiagnosticstool.exe

```
<Command>%windir%\system32\mdmdiagnosticstool.exe -area  
Autopilot;deviceprovisioning;deviceenrollment;tpm;HololensFallbackDeviceOwner -cab  
%temp%\MDMDiagnostics\mdmlogs-xxxx-xx-xx.cab</Command>
```

Add more logs to collect in registry

Registry Editor

File Edit View Favorites Help

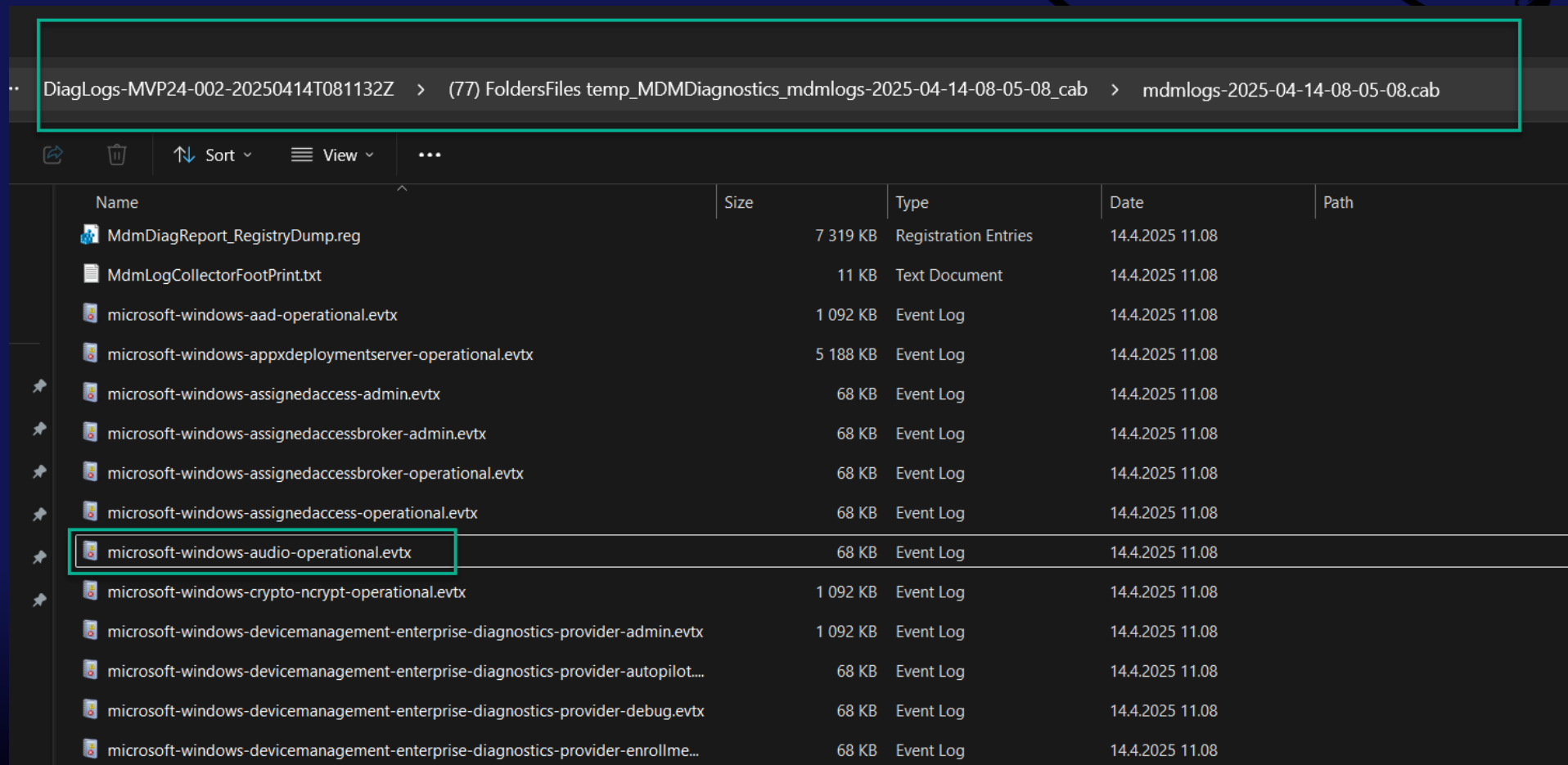
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MdmDiagnostics\Area\DeviceEnrollment\EventViewerEntry

Name	Type	Data
(Default)	REG_SZ	(value not set)
Application	REG_DWORD	0x000000ff (255)
Microsoft-Windows-AAD/Operational	REG_DWORD	0x000000ff (255)
Microsoft-Windows-AppXDeploymentServer/Operational	REG_DWORD	0x000000ff (255)
Microsoft-Windows-Audio/Operational	REG_DWORD	0x000000ff (255)
Microsoft-Windows-Crypto-NCrypt/Operational	REG_DWORD	0x000000ff (255)
Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin	REG_DWORD	0x000000ff (255)
Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Autopilot	REG_DWORD	0x000000ff (255)
Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Debug	REG_DWORD	0x000000ff (255)
Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Enrollment	REG_DWORD	0x000000ff (255)
Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Operational	REG_DWORD	0x000000ff (255)
Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Sync	REG_DWORD	0x000000ff (255)
Microsoft-Windows-LAPS/Operational	REG_DWORD	0x000000ff (255)
Microsoft-Windows-ModernDeployment-Diagnostics-Provider/AutoPilot	REG_DWORD	0x000000ff (255)

Add more logs or events

Check what logs, registry or events are supported

<https://learn.microsoft.com/en-us/windows/client-management/mdm/diagnosticlog-csp>

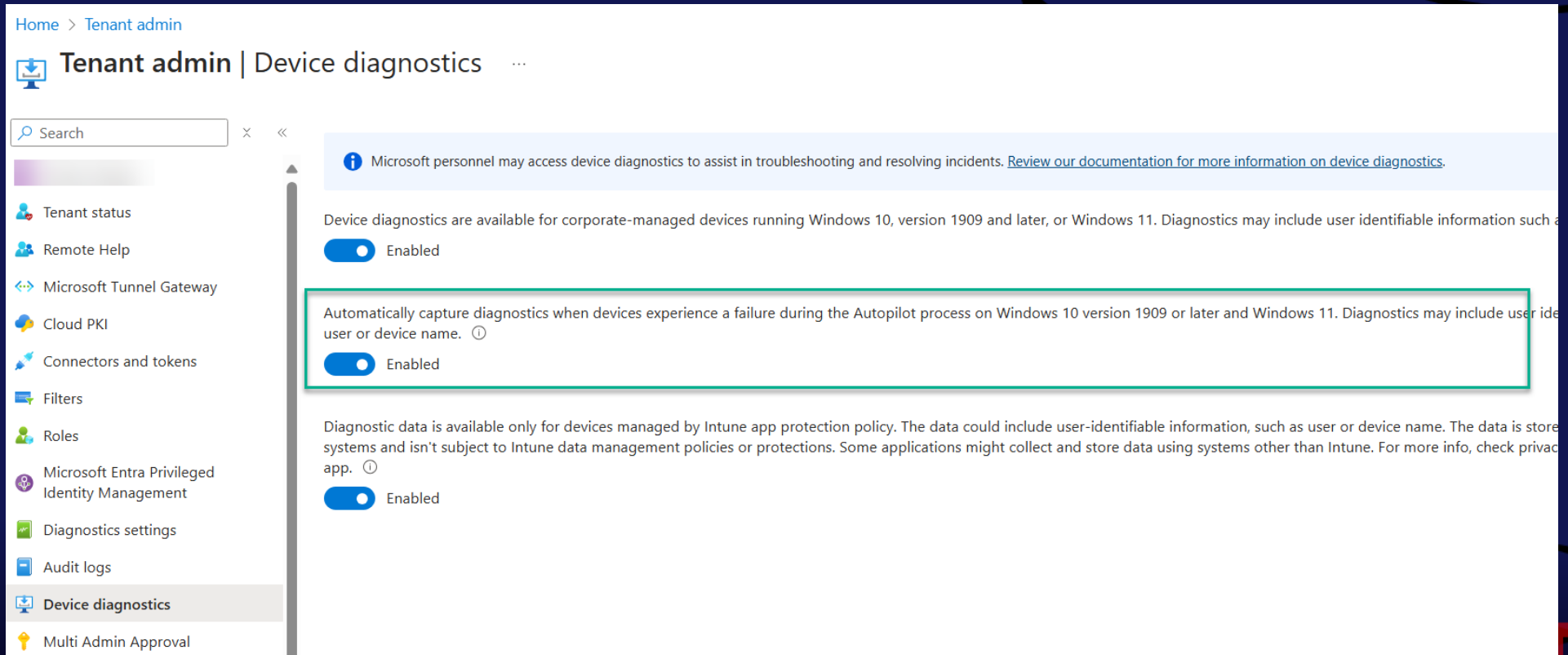


DiagLogs-MVP24-002-20250414T081132Z > (77) FoldersFiles temp_MDMDiagnostics_mdmlogs-2025-04-14-08-05-08_cab > mdmlogs-2025-04-14-08-05-08.cab

Name	Size	Type	Date	Path
MdmDiagReport_RegistryDump.reg	7 319 KB	Registration Entries	14.4.2025 11.08	
MdmLogCollectorFootPrint.txt	11 KB	Text Document	14.4.2025 11.08	
microsoft-windows-aad-operational.evtx	1 092 KB	Event Log	14.4.2025 11.08	
microsoft-windows-appxdeploymentserver-operational.evtx	5 188 KB	Event Log	14.4.2025 11.08	
microsoft-windows-assignedaccess-admin.evtx	68 KB	Event Log	14.4.2025 11.08	
microsoft-windows-assignedaccessbroker-admin.evtx	68 KB	Event Log	14.4.2025 11.08	
microsoft-windows-assignedaccessbroker-operational.evtx	68 KB	Event Log	14.4.2025 11.08	
microsoft-windows-assignedaccess-operational.evtx	68 KB	Event Log	14.4.2025 11.08	
microsoft-windows-audio-operational.evtx	68 KB	Event Log	14.4.2025 11.08	
microsoft-windows-crypto-ncrypt-operational.evtx	1 092 KB	Event Log	14.4.2025 11.08	
microsoft-windows-devicemanagement-enterprise-diagnostics-provider-admin.evtx	1 092 KB	Event Log	14.4.2025 11.08	
microsoft-windows-devicemanagement-enterprise-diagnostics-provider-autopilot....	68 KB	Event Log	14.4.2025 11.08	
microsoft-windows-devicemanagement-enterprise-diagnostics-provider-debug.evtx	68 KB	Event Log	14.4.2025 11.08	
microsoft-windows-devicemanagement-enterprise-diagnostics-provider-enrollme...	68 KB	Event Log	14.4.2025 11.08	

Automatic upload logs

◆ When Autopilot failed



Home > Tenant admin

Tenant admin | Device diagnostics

Search

- Tenant status
- Remote Help
- Microsoft Tunnel Gateway
- Cloud PKI
- Connectors and tokens
- Filters
- Roles
- Microsoft Entra Privileged Identity Management
- Diagnostics settings**
- Audit logs
- Device diagnostics
- Multi Admin Approval

Microsoft personnel may access device diagnostics to assist in troubleshooting and resolving incidents. [Review our documentation for more information on device diagnostics.](#)

Device diagnostics are available for corporate-managed devices running Windows 10, version 1909 and later, or Windows 11. Diagnostics may include user identifiable information such as user or device name.

Enabled

Automatically capture diagnostics when devices experience a failure during the Autopilot process on Windows 10 version 1909 or later and Windows 11. Diagnostics may include user identifiable information such as user or device name. ⓘ

Enabled

Diagnostics data is available only for devices managed by Intune app protection policy. The data could include user-identifiable information, such as user or device name. The data is stored in Intune systems and isn't subject to Intune data management policies or protections. Some applications might collect and store data using systems other than Intune. For more info, check privacy settings in the app. ⓘ

Enabled

Intune debug tools

A silhouette of a fisherman standing in water, holding a large net that is draped over the top of the slide. The fisherman is wearing a hat and a jacket, and the net is a large, dark, curved shape that spans across the top and right side of the slide.

- <https://github.com/MSEndpointMgr/IntuneDebugToolkit>
- <https://github.com/markstan/IntuneOneDataCollector>

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
- ◆ And much more

The screenshot displays the Intune Device Details GUI for device W10AAD1. The interface is divided into several sections:

- Header:** Shows the user connected as 'w10' and a search filter. It includes buttons for '1. Search devices' and '2. Create report'.
- Device Information:** A table showing details for device W10AAD1, including Manufacturer (Microsoft Corporation), OS/Version (Windows 11 21H2 Ent), Language (en-US), Storage (34GB / 79GB), Ethernet MAC (00155D104127), Primary User (Jane@demiranda.nu), and Compliance (compliant).
- Recent check-ins:** Shows a check-in for Jane@demiranda.nu on 2022-05-18 at 17:38:25.
- Device Group Memberships:** A table listing group memberships with columns for DisplayName and Group.
- Application Assignments:** A table listing assigned applications with columns for context, Application type, displayName, and Version.
- Configurations Assignments:** A table listing assigned configuration profiles with columns for context, Configuration type, and displayName.
- Overview:** A detailed JSON view of the device's configuration, including userPrincipalName, operatingSystem, osVersion, skuFamily, manufacturer, model, and enrollment details.
- Primary User:** A table showing user details for Jane@demiranda.nu, including accountEnabled, displayName, userPrincipalName, email, userType, and other attributes.

At the bottom, it states 'Device details updated 2022-05-29 19:47:37' and provides the author's contact information: Petri Paavola (@yodamiitti) - Microsoft MVP, with a GitHub link to the project.



Compliance Policy in error state

- ◆ Hardcoded behaviour
- ◆ 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.

Compliance setting in error state for more than 7 days.

[Less](#) ^

Intune couldn't determine your device's compliance with one or more settings for at least 7 days. Sometimes these errors are resolved by restarting your device and selecting Check compliance. If you do this and get this message again, contact your organization's support.

Sync

Setting

State

State details

Firewall

⊗ Error

2016345612(Syncm1(500): The recipient encountered an unexpected condition which prevented it from fulfilling the request)

Forcing the Co-managed client to re-enroll in Intune

Removes the detection method and initiates a new enrollment:

```
$guid = Get-ChildItem HKLM:\Software\Microsoft\Enrollments |  
ForEach-Object {Get-ItemProperty $_.pspath} | where-object  
{$_ .DiscoveryServiceFullURL} | ForEach-Object  
{$_ .PSChildName}
```

```
Remove-Item -Path "HKLM:\Software\Microsoft\Enrollments\$guid"  
-recurse
```

```
Restart-Service -Name ccmexec
```

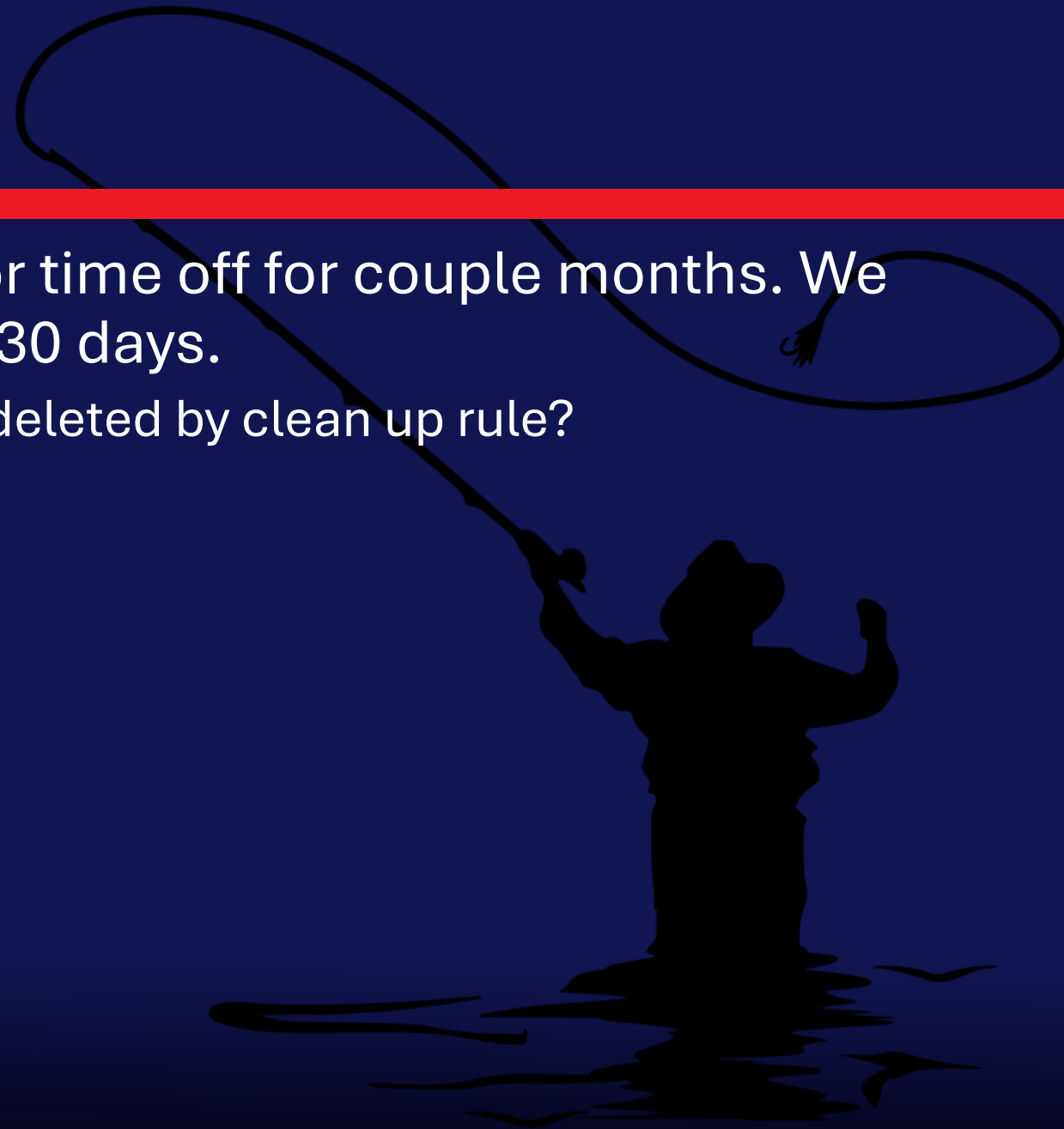

Forcing client to re-join

- ◆ `dsregcmd.exe /leave /debug`
- ◆ Sync Entra AD connect
- ◆ `dsregcmd.exe /join /debug`



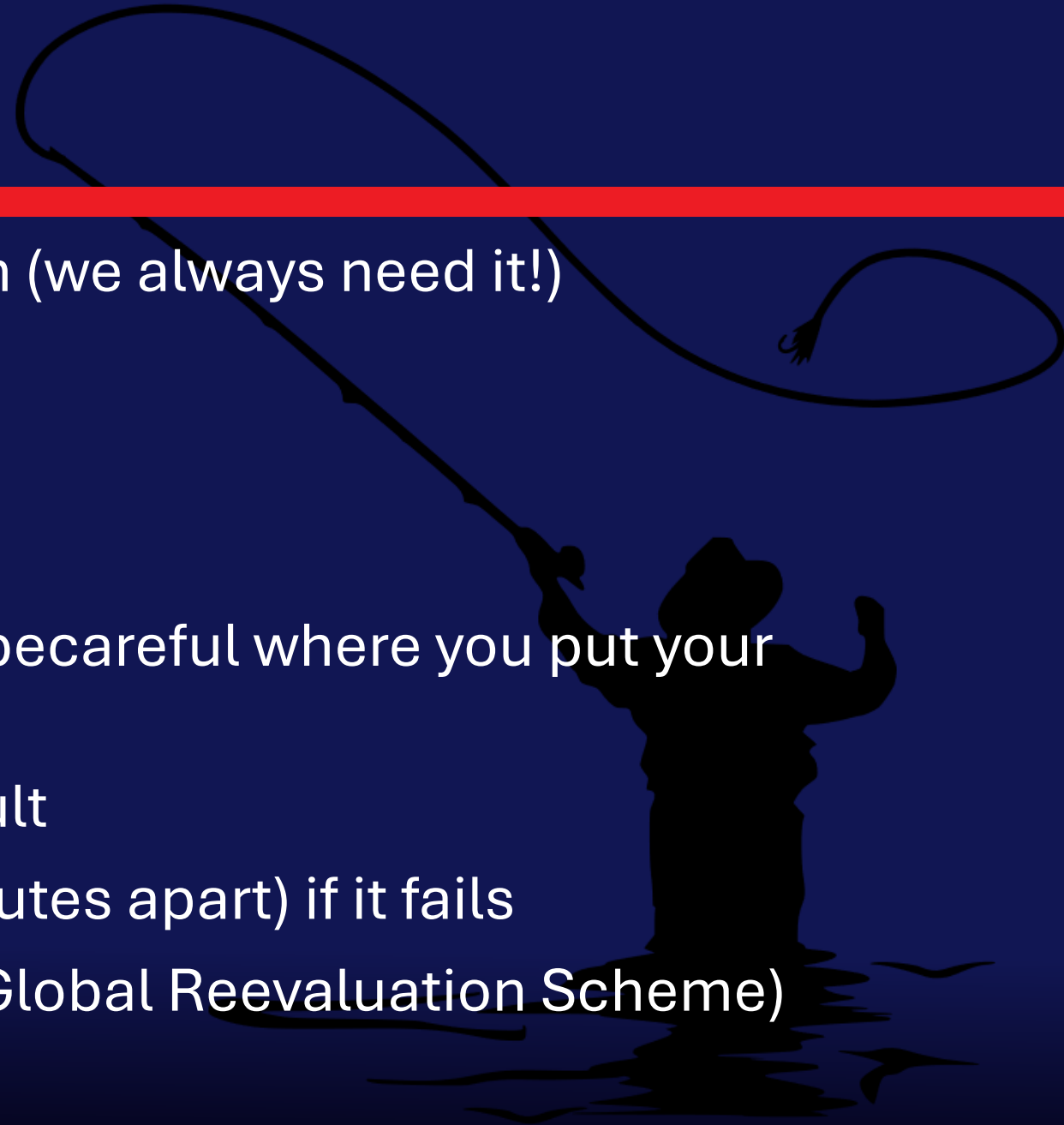
Cloud-native client

- ◆ Challenge: User has been away or time off for couple months. We have Intune device clean up rule 30 days.
 - What if the Intune device object is deleted by clean up rule?
- ◆ Force the client to reenroll
 - ◆ `dsregcmd.exe /forcerecover`



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

Log files:

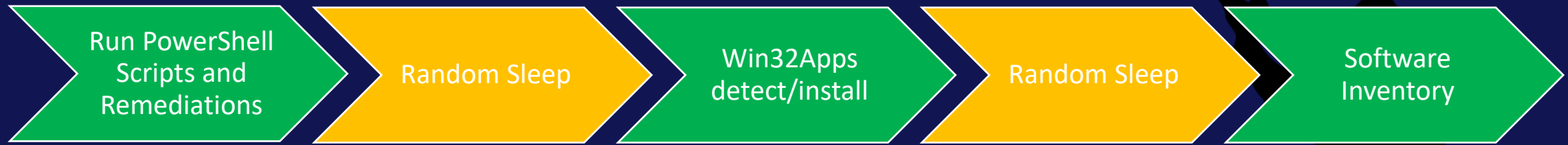
- ◆ C:\ProgramData\Microsoft\IntuneManagementExtension\Logs
 - ◆ AgentExecution.log – Log file for PowerShell detection methods
 - ◆ ClientHealth.log – Log file for IME health and remediation actions
 - ◆ DeviceHealthMonitoring – Log file for Appcrash, app events
 - ◆ HealthScripts – Log file for remediation 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

IME flow

```
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
```

Disable User ESP – Kiosk scenarios

- ◆ IME checks that USER ESP completed otherwise it will NEVER install a Win32 App anymore.

```
[Win32App] GetLogonIdFromFirstSyncReg check subkey: S-1-12-1-3972641916-1128363478-2181379757-4105040
[Win32App] GetLogonIdFromFirstSyncReg Found userSIDFromFirstSync: S-1-12-1-3972641916-1128363478-21813
[Win32App] GetLogonIdFromFirstSyncReg Got isSyncDoneForUserStr: 1 under: SOFTWARE\Microsoft\Enrollments\
[Win32App] Checking ESP status and found isSyncDoneForUser: True
Finished ESP phase check before kicking off PowerShell script. ESP phase NotInEsp
Delaying PS and Win32 app workload checkins by seconds = 118 in the first check in on start/restart.
[GenericWorkload] Initiating GenericWorkload Checkin
```

Registry

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension

Name	Type	Data
(Default)	REG_SZ	(value not set)

https://intune.microsoft.com/#view/Microsoft_Intune_Apps/SettingsMenu/~/?appId/2043db9d-f484-4b49-9709-fd79f0555a78

Intune admin center

Home > Apps | Windows > Windows | Windows apps > Remote Help

Remote Help | Properties

Client Apps

Search

Overview

App information Edit

Manage

Name

Remote Help

Reinstalling app remotely

- ◆ Uninstall the app if installed
- ◆ Remove the AppID in the registry
- ◆ Remove the GRS association
- ◆ Launch a new PowerShell process that restarts IME agent



Troubelshoot - Reinstall Remote Help

Remediations on demand = RBAC

- ◆ Remediations on demand is a great
- ◆ Perfect in a Zero-trust scenario
- ◆ Requires RBAC to filter script

Run remediation (preview) ...

DESKTOP-9SECHR9

Deploy a remediation script package to this device using both a detection and remediation script. [Learn more about the remediation script packages.](#) To manage the script packages available on this device, go to [Proactive remediations](#).

Search ⓘ

Script package name	Description
<input type="checkbox"/> Troubleshoot - Reset Windows Update	
<input type="checkbox"/> Troubleshoot - Cleanup Profiles	
<input type="checkbox"/> Troubleshoot - Fix VPN Profile	
<input type="checkbox"/> Troubleshoot - Clear DNS Cache	
<input type="checkbox"/> Troubleshoot - Clean all download folders	
<input type="checkbox"/> Troubleshoot - Cleanup and restart - Win...	

<https://github.com/JayRHa/EndpointAnalyticsRemediationScripts>



Troubleshoot WufBDS registration

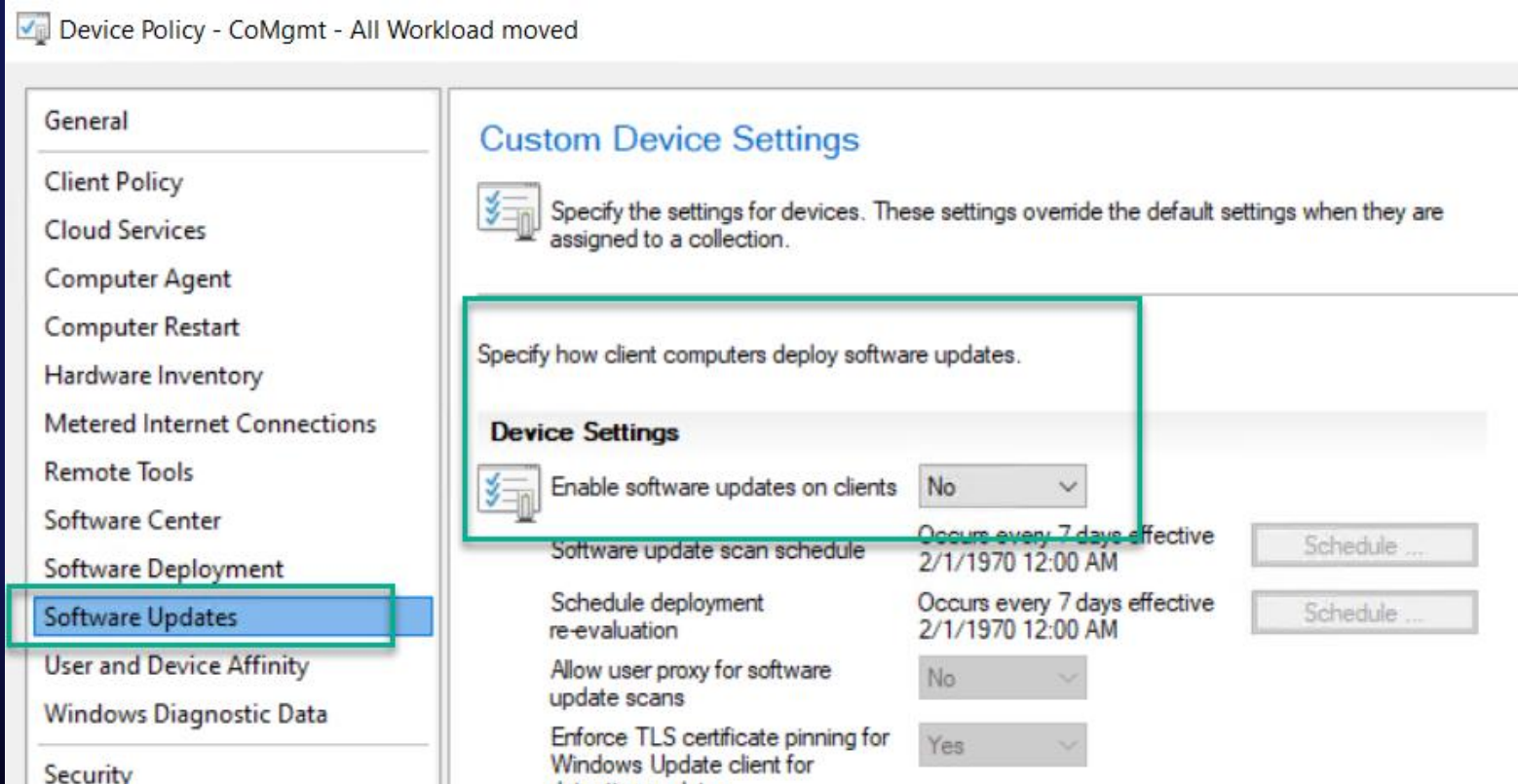
- ◆ <https://patchmypc.com/troubleshooting-windows-feature-updates-with-graph>

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WufbDS

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

Installing machine from ConfigMgr

Managing update with Windows Update for Business in Intune



The screenshot displays the 'Device Policy - CoMgmt - All Workload moved' interface in the Intune console. The left-hand navigation pane lists various policy categories, with 'Software Updates' highlighted in blue. The main content area is titled 'Custom Device Settings' and includes a descriptive icon and text: 'Specify the settings for devices. These settings override the default settings when they are assigned to a collection.' Below this, a section titled 'Specify how client computers deploy software updates.' contains a 'Device Settings' table. The table lists several settings, with the first one, 'Enable software updates on clients', set to 'No'. The other settings include 'Software update scan schedule', 'Schedule deployment re-evaluation', 'Allow user proxy for software update scans', and 'Enforce TLS certificate pinning for Windows Update client for detection data'. Each setting has a corresponding 'Schedule ...' button.

Device Settings	
Enable software updates on clients	No
Software update scan schedule	Occurs every 7 days effective 2/1/1970 12:00 AM
Schedule deployment re-evaluation	Occurs every 7 days effective 2/1/1970 12:00 AM
Allow user proxy for software update scans	No
Enforce TLS certificate pinning for Windows Update client for detection data	Yes

Did you notice?

Autopatch changes from message center

Update to Windows Autopatch diagnostic d... ×

 Translate

MC996580, Published date: 02/04/2025, 02:04:49 AM

Updated February 4, 2025: We have updated the content.

Windows Diagnostics data settings must be configured for Windows Autopatch reports to accurately include devices and update status. The minimum necessary [Windows diagnostic data](#) collection level to be configured on devices registered to Autopatch with the following diagnostic data settings: Windows 10 and Windows 11 - [Required](#)

With this change:

- Windows Autopatch will cease to deploy and configure the Windows Data Diagnostics policy. Previously, as part of the Autopatch feature activation process, Windows Autopatch deployed a policy named **Windows Autopatch - Data collection** which set the Windows diagnostics data collection level to Optional (previously labeled as Full) for managed devices. You will be able to configure and maintain the Windows Diagnostics Data level policy in your environment.
- As part of the ongoing service maintenance Windows Autopatch will remove the **Windows Autopatch - Data collection** policy from tenants starting **March 03, 2025**, Pacific Standard Time. This change will be completed in 2 weeks.

Action required:

Create and deploy a Windows Diagnostic data collection policy with at least the recommended minimum setting to all Autopatch devices prior to this change. You may see missing Client State and Client Substate values if your devices are not configured with the recommended Windows Diagnostics settings and level. Alternatively, you may already be covered with existing data collection policies in your environment.

TIP: You may want to consider using the **Windows Autopatch - Devices All** group which contains all of the active, registered devices presently in your Autopatch implementation across any and all Autopatch Groups. This is a service-managed group (subject to changes at any time). **Not Registered** devices will not appear in this Entra group.



No Drivers are deployed anymore?

- ◆ We have seen this in the wild
- ◆ Users authenticate to Intune Update Service using Entra Enterprise application

Microsoft Azure

Home > Onevinn | Enterprise applications > Enterprise applications | All applications > Intune Update Service

Intune Update Service | Properties

Enterprise Application

« Save Discard Delete Got feedback?

View and manage application settings for your organization. Editing properties settings, and user visibility settings requires Global Administrator, Cloud Application Administrator roles. [Learn more.](#)

Some of the displayed properties that are not editable are managed on the app home tenant.

i You can't delete this application because it's a Microsoft first party application

Enabled for users to sign-in? Yes No

Name

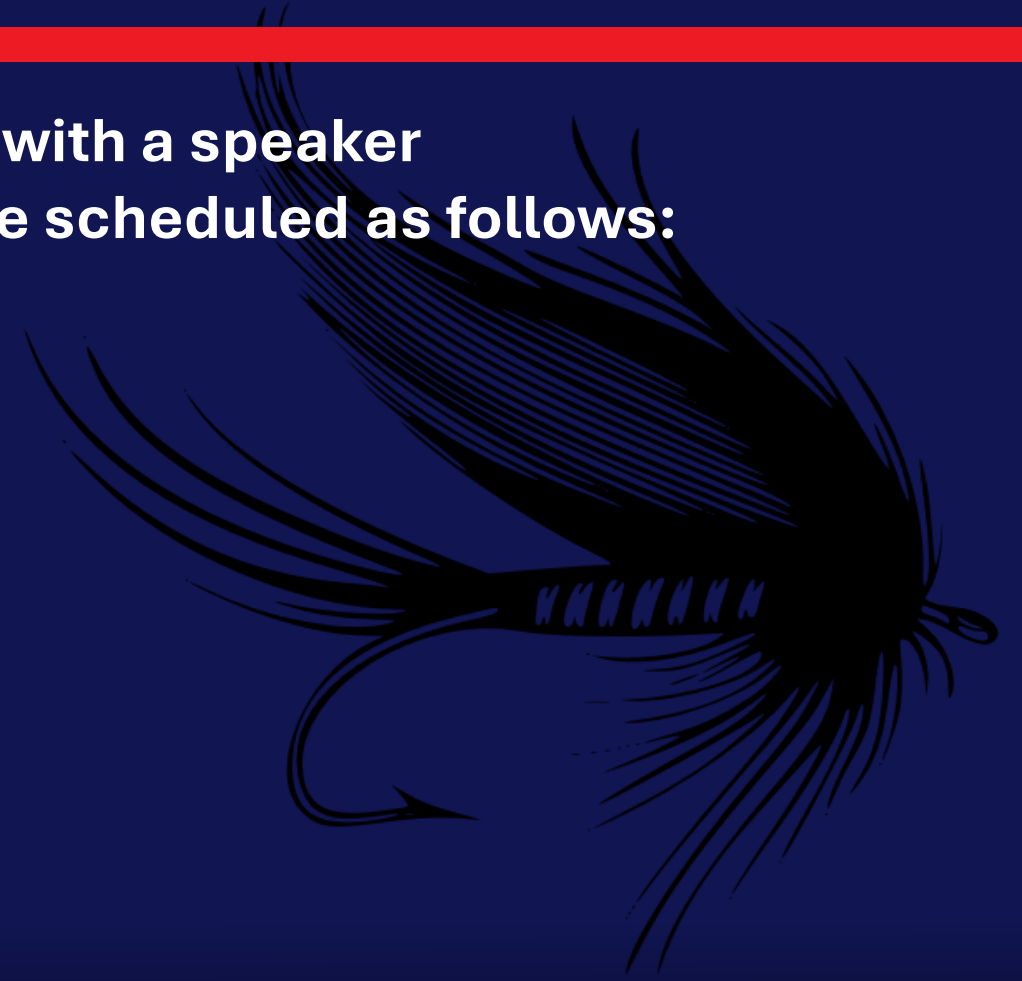
Useful blog post

- ◆ <https://techcommunity.microsoft.com/blog/intunecustomersuccess/troubleshooting-windows-feature-updates-in-microsoft-intune/4401828>



Fishing Sessions

Be sure to find Wally and sign up for 1:1 time with a speaker
If you'd like to "catch" us for a session, we are scheduled as follows:



Don't forget to leave feedback for your speakers!

Save the Dates

12-15 Oct. 2025



May 3-7, 2026



Oct 25-28, 2026

