Log Detective: Uncovering Clues in Windows and Intune

Petri Paavola

Panu Saukko

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

robopack

numecent

Microsoft

eido

Rimo3

Panu Saukko

Panu Saukko
Microsoft MVP · Intune/Security Copilot

Role
Consultant/Trainer

Focus
Intune · Windows Workstation/Server · Security

Blog, Hobbies and more
Panu Saukko (@panusaukko) / X
Panu Saukko | LinkedIn

Petri Paavola

Petri Paavola
Microsoft MVP · Intune & Windows

Role
Senior Modern Management Principal

Focus
Intune · Windows · PowerShell · Community Tools

Blog, Hobbies and more
Intune.ninja
PowerShell.ninja

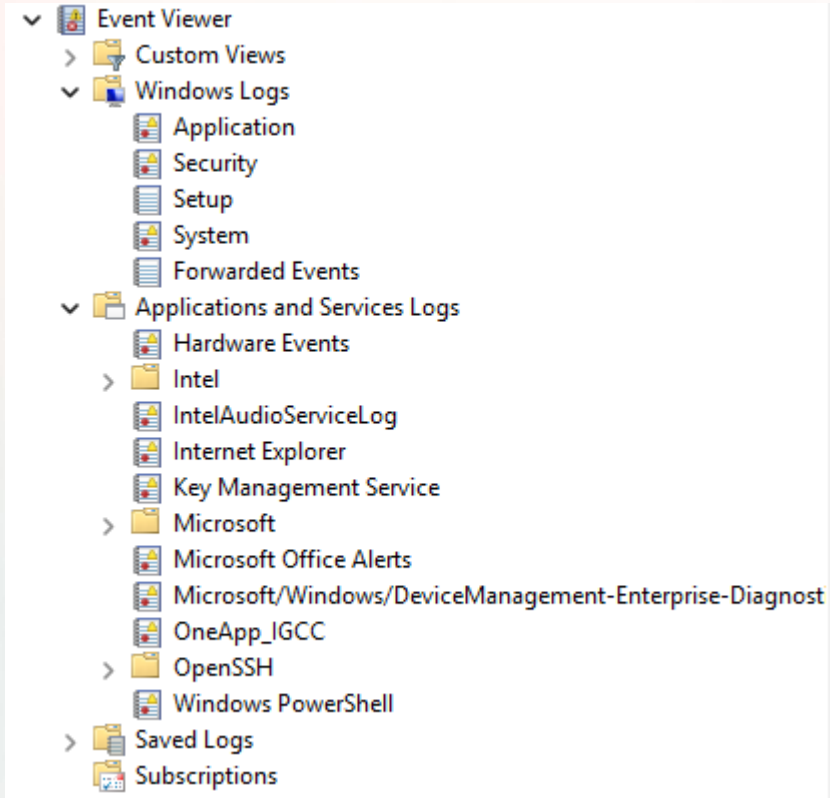
Agenda

- Logs: What are they? ☺
- Collecting logs from a remote device
- How to parse logs?
- Different tools to help with troubleshooting

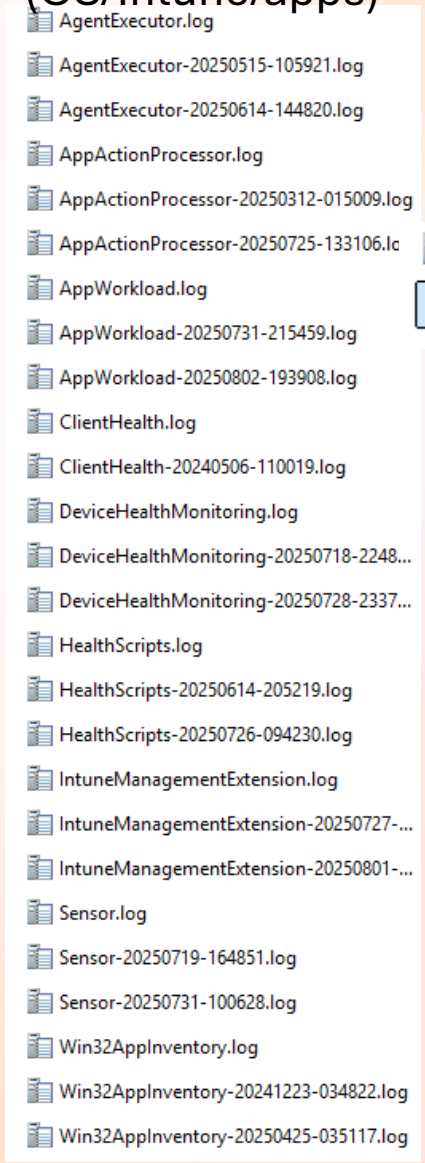
What we mean by "Logs"

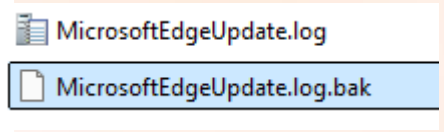
Troubleshooting information from Windows devices

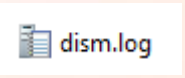
Windows Event Viewer events

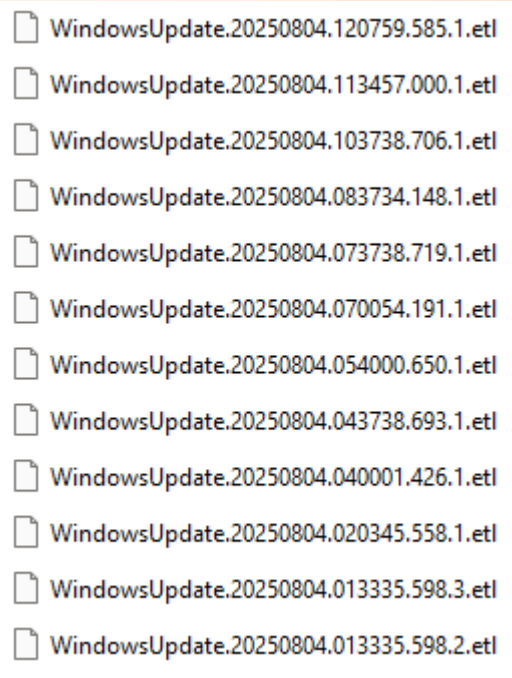


Text based log files (OS/Intune/apps)





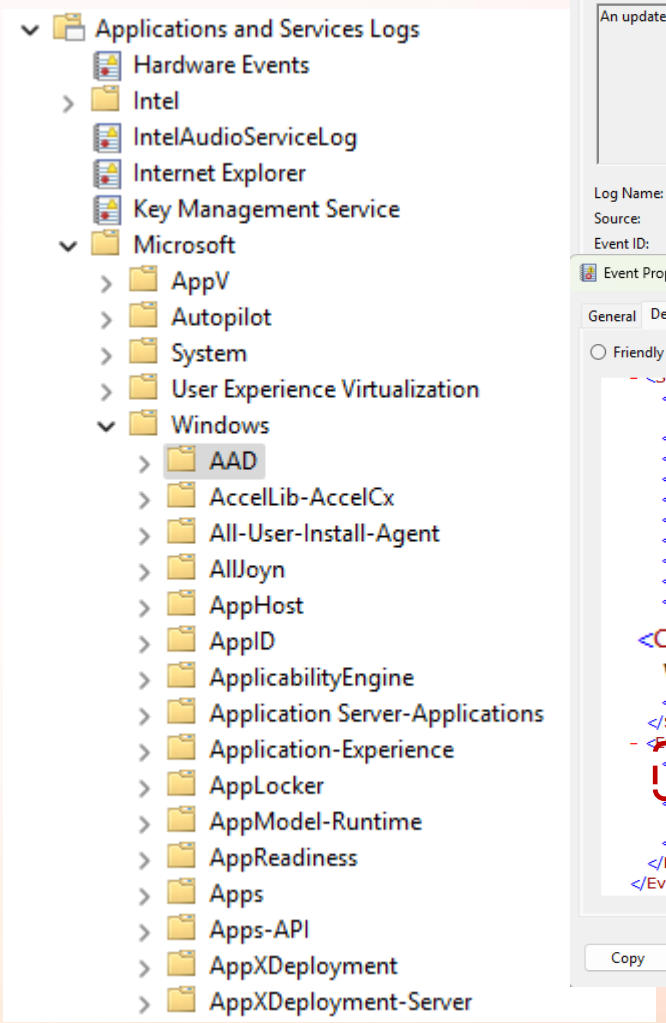


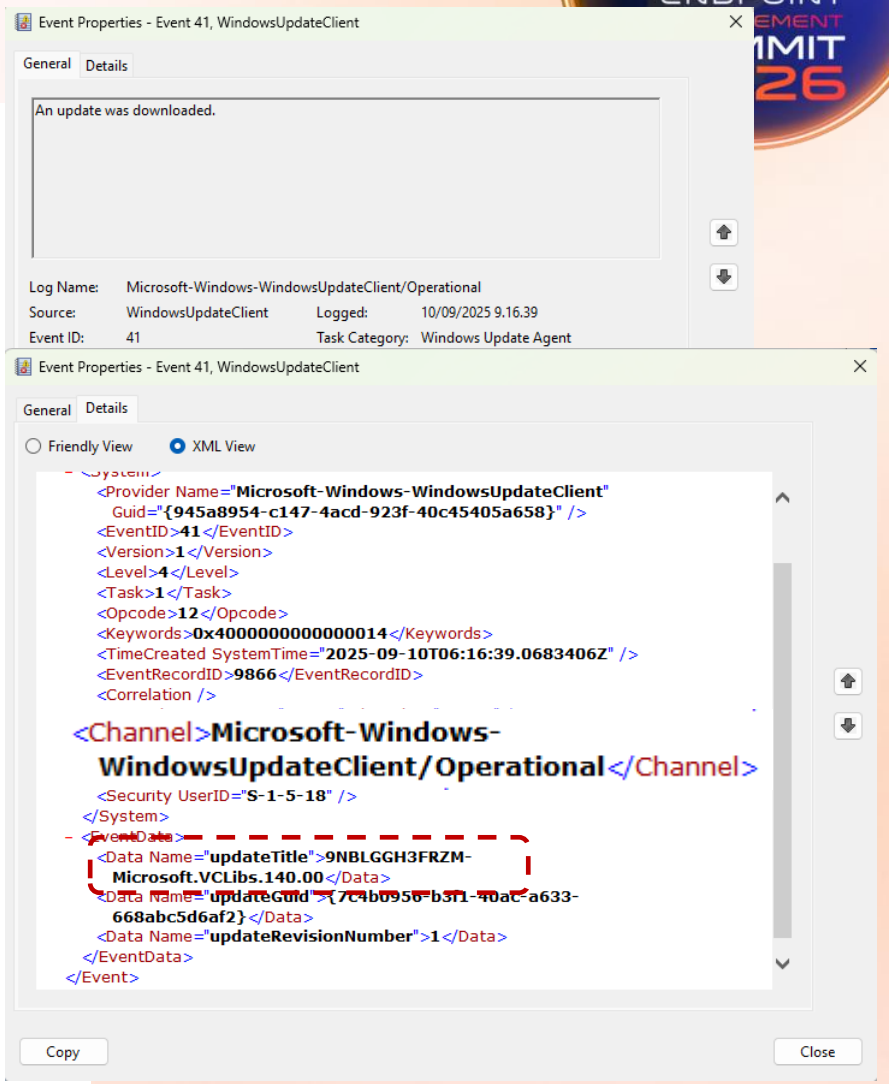


EventViewer

"Classical" Windows logs

Application specific logs





Different log files

- Normally standard text files
    - File size can be anything…

```
<![LOG[[datasensor](EventManager) No refresh is needed.]LOG]!><time="13:25:12.0230078" date="8-20-2025" component="IntuneManagementExtension" cont
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query '2ef6314a-cc15-487d-abfc-24a02cc9180f' 0]LOG]!><time="13:25:12.0390816" date="8-
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query '488bf6dd-6375-434b-ba35-4faefbfb8c41' 2]LOG]!><time="13:25:12.0390816" date="8-
<![LOG[Current collector endpoint = https://eu-mobile.events.data.microsoft.com/OneCollector/1.0/]LOG]!><time="13:25:12.0390816" date="8-20-2025"
<![LOG[[datasensor](EventManager) endpoint = [https://eu-mobile.events.data.microsoft.com/OneCollector/1.0/], IsReady = True, expired = False, IsT
<![LOG[[datasensor](EventManager) No refresh is needed.]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension" cont
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query 'd8900422-33e5-4f4c-847c-1c1d374d3697' 0]LOG]!><time="13:25:12.0390816" date="8-
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query 'e7eee33f-a719-49e4-91e6-e37
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query 'a887147e-94ea-48e8-a961-e1e
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" d
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" d
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" d
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" d
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" d
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" d
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" d
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" d
```

```
[08/17/25 03:11:48.891][MicrosoftEdgeUpdate:msedgeupdate][67780:65996][CheckForUpdate][Latest][app_id {F
[08/17/25 03:11:48.891][MicrosoftEdgeUpdate:msedgeupdate][67780:65996][CheckForUpdate][app_id {F3017226-
[08/17/25 03:11:48.891][MicrosoftEdgeUpdate:msedgeupdate][67780:65996][CdpServicesClient::SendInternal][
[08/17/25 03:11:48.891][MicrosoftEdgeUpdate:msedgeupdate][67780:65996][CdpServicesClient::LegacySendInte
[08/17/25 03:11:48.891][MicrosoftEdgeUpdate:msedgeupdate][67780:65996][CdpServicesClient::Send][finished
[08/17/25 03:11:48.891][MicrosoftEdgeUpdate:msedgeupdate][67780:65996][edge_preview::DoEdgePreviewRollba
[08/17/25 03:11:49.006][MicrosoftEdgeUpdate:msedgeupdate][67780:65996][IsManaged][Group Policy][1]
[08/17/25 03:11:49.006][MicrosoftEdgeUpdate:msedgeupdate][67780:65996][IsManaged][Group Policy][1]
[08/17/25 03:11:49.012][MicrosoftEdgeUpdate:msedgeupdate][66708:51320][DoInstallApps returning][0x000000
[08/17/25 03:11:49.021][MicrosoftEdgeUpdate:msedgeupdate][67780:41052][Started process][26180]
[08/17/25 03:11:49.035][MicrosoftEdgeUpdate:msedgeupdate][66708:51320][Update all apps process finished]
[08/17/25 03:11:49.057][MicrosoftEdgeUpdate:msedgeupdate][26180:68272][OmahaPolicyManager::set_policy][
[08/17/25 03:11:49.063][MicrosoftEdgeUpdate:msedgeupdate][26180:68272][DllEntry]["C:\Program Files (x86)
```

```
MSI (s) (B4:7C) [13:52:25:104]: Windows Installer installed the product. Product Name: Vernier Graphical Analysis
6.2.1-3963. Product Version: 6.2.1.0. Product Language: 1033. Manufacturer: Vernier Software & Technology. Installation
success or error status: 0.

MSI (s) (B4:7C) [13:52:25:142]: Deferring clean up of packages/files, if any exist
MSI (s) (B4:7C) [13:52:25:142]: MainEngineThread is returning 0
MSI (s) (B4:50) [13:52:25:146]: RESTART MANAGER: Session closed.
MSI (s) (B4:50) [13:52:25:146]: No System Restore sequence number for this installation.
=== Logging stopped: 7/29/2025  13:52:25 ===
MSI (s) (B4:50) [13:52:25:147]: User policy value 'DisableRollback' is 0
MSI (s) (B4:50) [13:52:25:147]: Machine policy value 'DisableRollback' is 0
MSI (s) (B4:50) [13:52:25:147]: Incrementing counter to disable shutdown. Counter after increment: 0
MSI (s) (B4:50) [13:52:25:149]: Note: 1: 1402 2: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer
\Rollback\Scripts 3: 2
MSI (s) (B4:50) [13:52:25:151]: Note: 1: 2265 2:  3: -2147287035
MSI (s) (B4:50) [13:52:25:151]: Note: 1: 1402 2: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer
\Rollback\Scripts 3: 2
MSI (s) (B4:50) [13:52:25:151]: Decrementing counter to disable shutdown. If counter >= 0, shutdown will be denied.  Counter
after decrement: -1
MSI (s) (B4:50) [13:52:25:161]: Destroying RemoteAPI object.
MSI (s) (B4:20) [13:52:25:161]: Custom Action Manager thread ending.
MSI (c) (4C:C0) [13:52:25:163]: Decrementing counter to disable shutdown. If counter >= 0, shutdown will be denied.  Counter
after decrement: -1
MSI (c) (4C:C0) [13:52:25:165]: MainEngineThread is returning 0
=== Verbose logging stopped: 7/29/2025  13:52:25 ===
```

Know what information is where

How do you know?

It might be difficult for the first 10 years, but after that it is pretty easy…

Or use AI!

Intune client log file location

Main log files:
C:\ProgramData\Microsoft\IntuneManagementExtension\Logs

Enhanced inventory
C:\Program Files\Microsoft Device Inventory Agent\Logs

Enterprise Privilege Manager
C:\Program Files\Microsoft EPM Agent\Logs

Users have permissions to read log files

AgentExecutor.log	13/04/2026 16.01	Text Document	1 635 KB
AppActionProcessor.log	13/04/2026 9.01	Text Document	709 KB
AppWorkload.log	13/04/2026 15.06	Text Document	2 969 KB
AppWorkload-20260322-161244.log	22/03/2026 16.12	Text Document	3 073 KB
AppWorkload-20260330-075937.log	30/03/2026 17.59	Text Document	3 073 KB
ClientCertCheck.log	13/04/2026 15.42	Text Document	108 KB
ClientHealth.log	13/04/2026 15.43	Text Document	552 KB
DeviceHealthMonitoring.log	13/04/2026 15.43	Text Document	906 KB
DeviceHealthMonitoring-20260317-113345.l...	17/03/2026 11.33	Text Document	3 073 KB
DeviceHealthMonitoring-20260401-035548.l...	01/04/2026 13.55	Text Document	3 073 KB
HealthScripts.log	13/04/2026 15.06	Text Document	1 867 KB
IntuneManagementExtension.log	13/04/2026 16.01	Text Document	1 737 KB
IntuneManagementExtension-20260322-20...	22/03/2026 20.21	Text Document	3 080 KB
IntuneManagementExtension-20260401-00...	01/04/2026 10.49	Text Document	3 073 KB
NotificationInfraLogs.log	13/04/2026 16.01	Text Document	66 KB
Sensor.log	13/04/2026 16.04	Text Document	1 514 KB
Sensor-20260318-191126.log	18/03/2026 19.11	Text Document	3 073 KB
Sensor-20260331-230624.log	01/04/2026 9.06	Text Document	3 073 KB
Win32AppInventory.log	09/04/2026 17.19	Text Document	255 KB

Windows log files

Main log files:
C:\Windows\logs
- Dism
- CBS

Windows Update Log files
- .etl files by default
- Get-WindowsUpdateLog

Get-WindowsUpdateLog -ETLPath '.\(82) FoldersFiles windir_Logs_WindowsUpdate_etl\' -LogPath .\windowsupdate.log

C:\Windows\temp
- WinGet
- Users have no permission to read

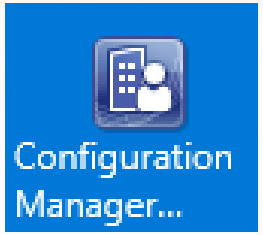
C:\ProgramData\Microsoft
- EdgeUpdate
- Windows Defender\support

C:\Windows\Panther
- Need anymore?

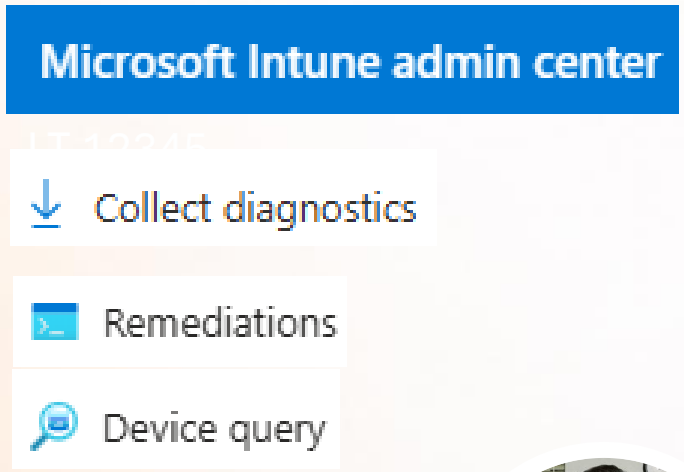
Application installation log files

- Enabling MSI log files
  - msiexec.exe /i app.msi /qn **/L*v C:\Windows\Temp\install-app.log**
- PSAppDeployToolkit log files: C:\Windows\Logs\Software
- Other applications
  - Browser updates?
- Finding errors from MSI log files remotely
  - Different ways?
  - Intune Remediation scripts
  - CMPivot

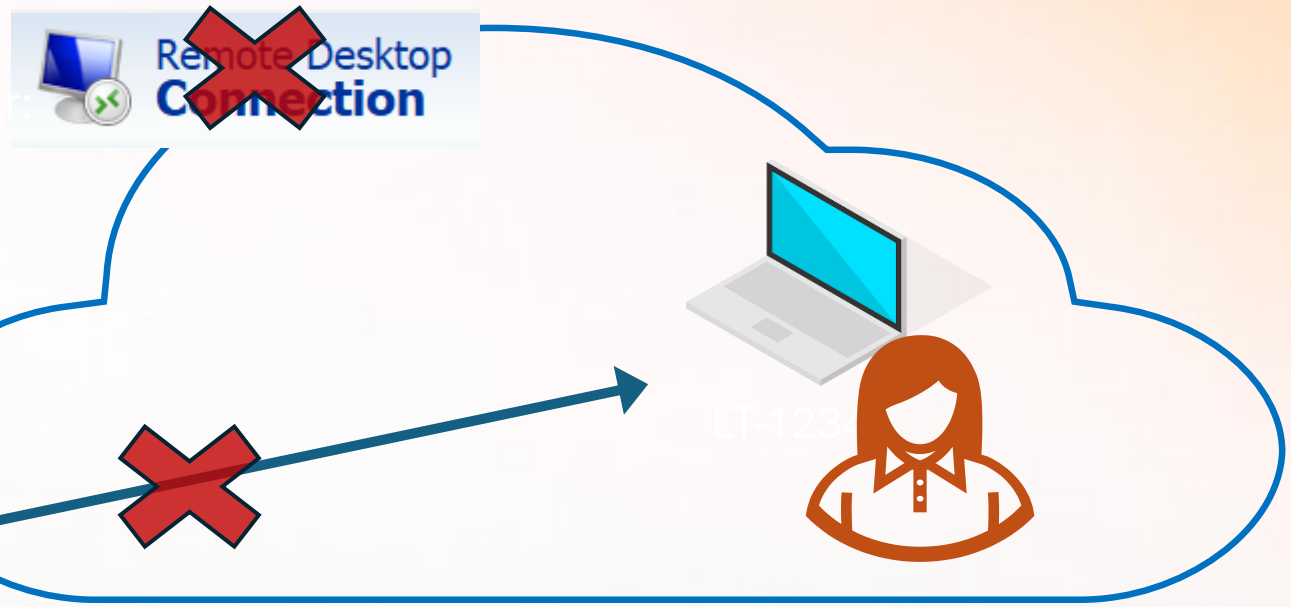
Get events/logs from a remote device



?

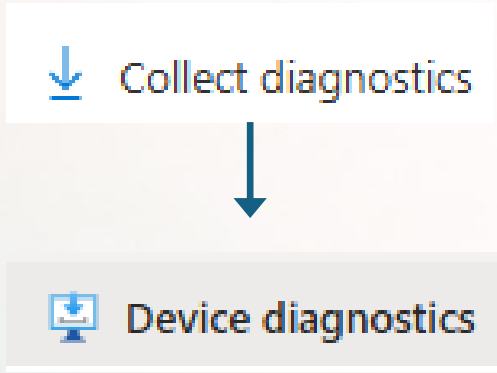


Advanced analytics/
Intune Suite

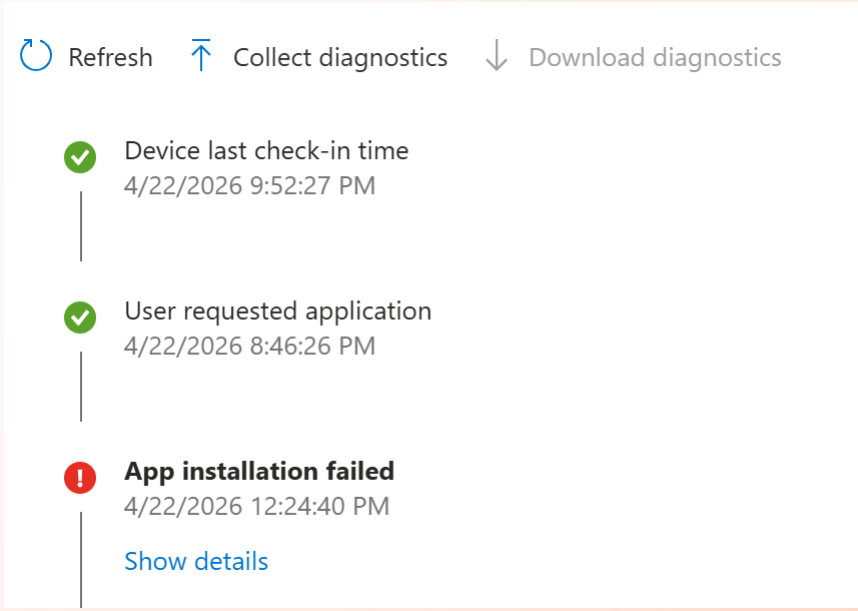


Collect Diagnostics

- Manually/Bulk
- Automatically if Autopilot fails
- Win32 applications
- "Cannot" modify what to collect (Wait for a demo)



Request initiated	Diagnostics uploaded
4/13/2026, 2:45:13 PM	4/13/2026, 2:56:56 PM



Demo

Device Diagnostics

Diagnostics file content

1. Registry keys

(1) RegistryKey HKLM_SOFTWARE_Microsoft_CloudMan
(2) RegistryKey HKLM_Software_Microsoft_DeclaredCont
(3) RegistryKey HKLM_Software_Microsoft_DeviceInvent
(4) RegistryKey HKLM_Software_Microsoft_Enrollments
(5) RegistryKey HKLM_SOFTWARE_Microsoft_EPMAgent
(6) RegistryKey HKLM_Software_Microsoft_IntuneManag
(7) RegistryKey HKLM_SOFTWARE_Microsoft_PolicyMan
(8) RegistryKey HKLM_SOFTWARE_Microsoft_SystemCer
(9) RegistryKey HKLM_SOFTWARE_Microsoft_Windows_
(10) RegistryKey HKLM_SOFTWARE_Microsoft_Windows
(11) RegistryKey HKLM_SOFTWARE_Microsoft_Windows
(12) RegistryKey HKLM_SOFTWARE_Microsoft_Windows
(13) RegistryKey HKLM_SOFTWARE_Microsoft_Windows
(14) RegistryKey HKLM_SOFTWARE_Microsoft_Windows
(15) No Results - Error [0x80070001] RegistryKey HKLM_S
(16) RegistryKey HKLM_SOFTWARE_Microsoft_Windows
(17) RegistryKey HKLM_SOFTWARE_Microsoft_Windows
(18) RegistryKey HKLM_Software_Microsoft_Windows_C
(19) RegistryKey HKLM_SOFTWARE_Microsoft_Windows
(20) RegistryKey HKLM_SOFTWARE_Policies_Microsoft_C
(21) RegistryKey HKLM_SOFTWARE_WOW6432Node_Microsoft_Windows_CurrentVersion_Uninstall export.reg
(22) RegistryKey HKLM_SYSTEM_CurrentControlSet_Control_SecurityProviders_SCHANNEL export.reg
(23) RegistryKey HKLM_SYSTEM_CurrentControlSet_Services_SharedAccess_Parameters_FirewallPolicy_MD expo...
(24) RegistryKey HKLM_SYSTEM_Setup export.reg

2. Command outputs

(25) No Results - Error [0x80070001] RegistryKey HKLM_SYSTEM_Setu
(26) Command programfiles_windows_defender_mpcmdrun_exe_-G
(27) Command windir_system32_certutil_exe_-store output.log
(28) Command windir_system32_certutil_exe_-store_-user_my outpu
(29) No Results - Error [0x8000ffff] Command windir_system32_dism
(30) No Results - Error [0x8000ffff] Command windir_system32_dism
(31) Command windir_system32_Dsregcmd_exe_status output.log
(32) Command windir_system32_ipconfig_exe_all output.log
(33) Command windir_system32_mdmdiagnosticstool_exe_-area_Au
(34) Command windir_system32_msinfo32_exe_report_temp_MDMD
(35) Command windir_system32_netsh_exe_advfirewall_show_allprof
(36) Command windir_system32_netsh_exe_advfirewall_show_global
(37) Command windir_system32_netsh_exe_lan_show_profiles outpu
(38) Command windir_system32_netsh_exe_winhttp_show_proxy out
(39) Command windir_system32_netsh_exe_wlan_show_profiles outp
(40) Command windir_system32_netsh_exe_wlan_show_wlanreport o
(41) Command windir_system32_ping_exe_-n_50_localhost output.lo
(42) Command windir_system32_pnputil_exe_enum-drivers output.lo
(43) Command windir_system32_powercfg_exe_batteryreport_output_temp_MDMDiagnostics_battery-re output...
(44) Command windir_system32_powercfg_exe_energy_output_temp_MDMDiagnostics_energy-report_htm out...

3. EventViewer events

(45) Events Application Events.evtx
(46) Events Microsoft-Windows-AppLocker_EXE_and_DLL Eve
(47) Events Microsoft-Windows-AppLocker_MSI_and_Script E
(48) Events Microsoft-Windows-AppLocker_Packaged_app-D
(49) Events Microsoft-Windows-AppLocker_Packaged_app-E
(50) Events Microsoft-Windows-AppXDeployment_Operation
(51) Events Microsoft-Windows-AppXDeploymentServer_Ope
(52) Events Microsoft-Windows-AppxPackaging_Operational
(53) Events Microsoft-Windows-Bitlocker_Bitlocker_Manager
(54) Events Microsoft-Windows-HelloForBusiness_Operationa
(55) Events Microsoft-Windows-SENSE_Operational Events.ev
(56) Events Microsoft-Windows-SenseIR_Operational Events.e
(57) Events Microsoft-Windows-Shell-Core_Operational Even
(58) Events Microsoft-Windows-Windows_Firewall_With_Adv
(59) Events Microsoft-Windows-WinRM_Operational Events.e
(60) Events Microsoft-Windows-WMI-Activity_Operational Ev
(61) Events Setup Events.evtx
(62) Events System Events.evtx

4. Files from specific folders

(63) FoldersFiles ProgramData_Microsoft_DiagnosticLogCSP_Collectors_etl
(64) FoldersFiles ProgramData_Microsoft_IntuneManagementExtension_Logs
(65) FoldersFiles ProgramData_Microsoft_Windows_Defender_Support_MpSupportFiles_cab
(66) FoldersFiles ProgramData_Microsoft_Windows_WlanReport_wlan-report-latest_html
(67) FoldersFiles programdata_usoshared_logs_System
(68) FoldersFiles ProgramFiles_Microsoft_Device_Inventory_Agent_Logs
(69) FoldersFiles ProgramFiles_Microsoft_EPM_Agent_Logs
(70) FoldersFiles ProgramFiles_Microsoft_Update_Health_Tools_Logs_etl
(72) FoldersFiles temp_MDMDiagnostics_battery-report_html
(73) FoldersFiles temp_MDMDiagnostics_energy-report_html
(74) FoldersFiles temp_MDMDiagnostics_mdmlogs-2026-04-16-11-48-51_cab
(75) FoldersFiles temp_MDMDiagnostics_msinfo32_log
(77) FoldersFiles windir_ccm_logs_log
(78) FoldersFiles windir_ccmsetup_logs_log
(79) FoldersFiles windir_logs_CBS_cbs_log
(80) FoldersFiles windir_logs_measuredboot
(82) FoldersFiles windir_Logs_WindowsUpdate_etl
(83) FoldersFiles windir_panther_setupact_log
(84) FoldersFiles windir_panther_unattendgc_setupact_log
(85) FoldersFiles windir_SensorFramework_etl
(86) FoldersFiles windir_SoftwareDistribution_ReportingEvents_log
(87) FoldersFiles windir_system32_config_systemprofile_AppData_Local_mdm_log
(88) FoldersFiles windir_temp_computername_log

5. Individual files

(71) No Results - Error [0x80070003] FoldersFiles temp_CloudDesktop_log
(76) No Results - Error [0x80070003] FoldersFiles temp_winget_defaultstate_log
(81) No Results - Error [0x80070003] FoldersFiles windir_Logs_SetupDiag_SetupDiagResults_xml

Diagnostics Log: results.xml

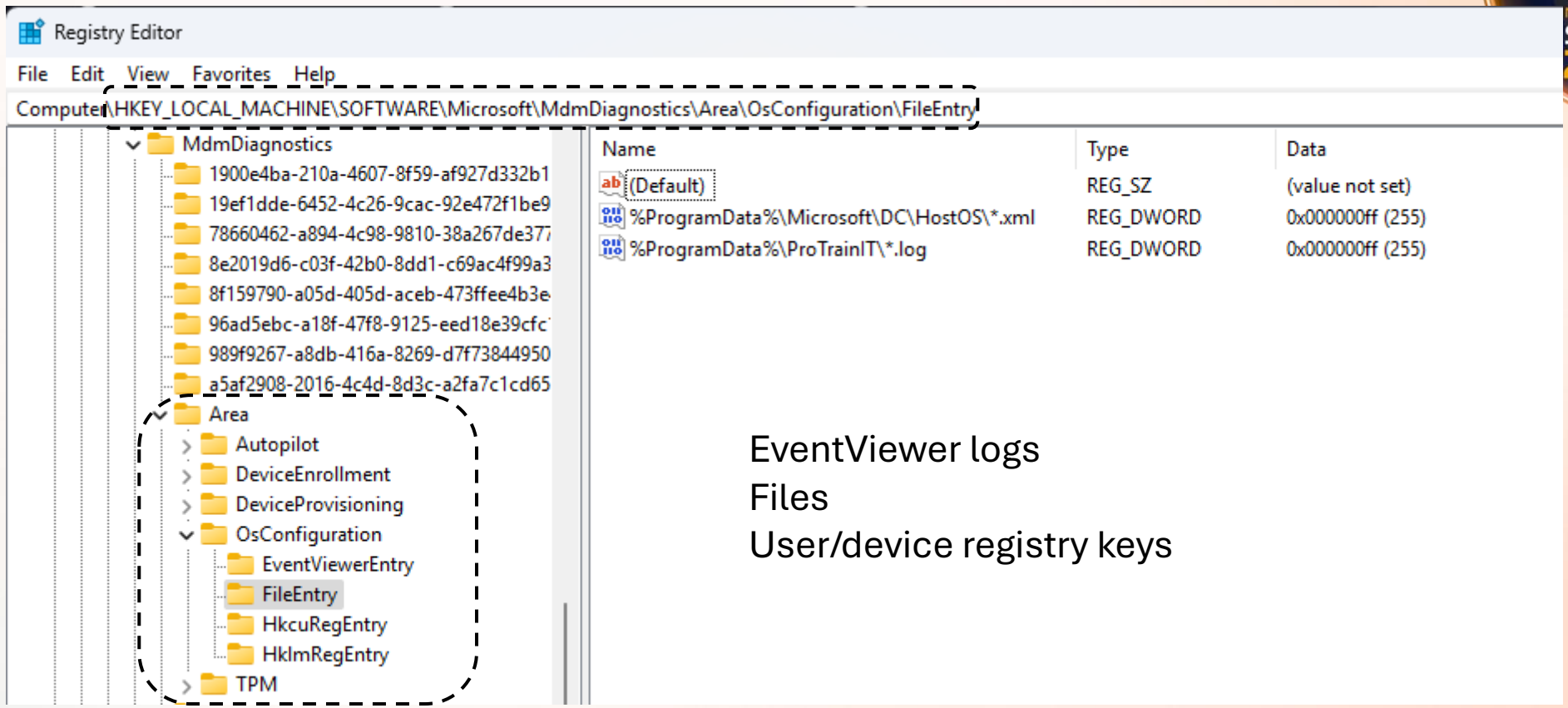
Exact commands used in diagnostics process. Don't trust the error codes! ☺

```
<RegistryKey HRESULT="-2147024895">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\NDUP</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OOBE</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Orchestrator</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\MDM</RegistryKey>
<RegistryKey HRESULT="-2147024893">HKLM\SYSTEM\Setup</RegistryKey>
<RegistryKey HRESULT="-2147024895">HKLM\SYSTEM\Setup\SetupDiag\Results</RegistryKey>
<Command HRESULT="0">%programfiles%\windows defender\mpcmdrun.exe -GetFiles</Command>
<Command HRESULT="0">%windir%\system32\certutil.exe -store</Command>
<Command HRESULT="0">%windir%\system32\certutil.exe -store -user my</Command>
<Command HRESULT="-2147418113">%windir%\system32\dism.exe /online /get-packages</Command>
<Command HRESULT="-2147418113">%windir%\system32\dism.exe /online /get-ProvisionedAppxPackages</Command>
<Command HRESULT="0">%windir%\system32\Dsregcmd.exe /status</Command>
<Command HRESULT="0">%windir%\system32\ipconfig.exe /all</Command>
<Command HRESULT="0">%windir%\system32\mdmdiagnosticstool.exe -area Autopilot;deviceprovisioning;deviceenrollment;tpm;HololensFallbackDeviceOwner -cab
%temp%\MDMDiagnostics\mdmlogs-2026-04-16-11-48-51.cab</Command>
<Command HRESULT="-2147024895">%windir%\system32\netsh.exe lan show profiles</Command>
<Command HRESULT="0">%windir%\system32\netsh.exe winhttp show proxy</Command>
<Command HRESULT="0">%windir%\system32\netsh.exe wlan show profiles</Command>
<Command HRESULT="0">%windir%\system32\netsh.exe wlan show wlanreport</Command>
<FoldersFiles HRESULT="0">%temp%\MDMDiagnostics\msinfo32.log</FoldersFiles>
<FoldersFiles HRESULT="-2147024893">%temp%\winget\defaultstate\*.log</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\ccm\logs\*.log</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\ccmsetup\logs\*.log</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\logs\CBS\cbs.log</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\logs\measuredboot\*.*</FoldersFiles>
<FoldersFiles HRESULT="-2147024893">%windir%\Logs\SetupDiag\SetupDiagResults.xml</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\Logs\WindowsUpdate\*.etl</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\panther\setupact.log</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\panther\unattendgc\setupact.log</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\SensorFramework\*.etl</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\SoftwareDistribution\ReportingEvents.log</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\system32\config\systemprofile\AppData\Local\mdm\*.log</FoldersFiles>
<FoldersFiles HRESULT="0">%windir%\temp\%computername%*.log</FoldersFiles>
<FoldersFiles HRESULT="-2147024894">%windir%\temp\officeclicktorun*.log</FoldersFiles>
```

MDMDiagnosticsTool


```
PS C:\> MdmDiagnosticsTool.exe /?

  Usage1: C:\WINDOWS\system32\MdmDiagnosticsTool.exe -out <output folder path>
      * Output MDM diagnostics info only to given folder path specified in -out parameter.
      eg: C:\WINDOWS\system32\MdmDiagnosticsTool.exe -out c:\temp\outputfolder

  Usage2: C:\WINDOWS\system32\MdmDiagnosticsTool.exe -area <area name(s)> -cab <output cab file path>
      * Collect predefined area logs and create a log cab to given cab file.
      * Supported area name example:
          Autopilot
          DeviceProvisioning
          Tpm
      * It also supports multiple areas, separated by ';', example:
          Autopilot;DeviceEnrollment;Tpm
      * Please find all possible areas in registry under:
          HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MdmDiagnostics\Area
      eg: C:\WINDOWS\system32\MdmDiagnosticsTool.exe -area Autopilot;Tpm -cab c:\temp\AutopilotDiag.cab

  Usage3: C:\WINDOWS\system32\MdmDiagnosticsTool.exe -area <area name(s)> -zip <output zip file path>
      * Collect predefined area logs and create a log zip to given zip file. Areas supported are the same as Usage2 for
creating cab

  Usage4: C:\WINDOWS\system32\MdmDiagnosticsTool.exe -xml <xml file of information to gather> -zip <output zip file path
> -server <MDM Server to alert>
      * Collect information specified in the xml and create a log zip to given zip file.

  Usage5: C:\WINDOWS\system32\MdmDiagnosticsTool.exe -clean
      * Cleans up all the diagnostic log files collected.
```

Modifying what MDMDiagnosticsTool collects



EventViewer logs
Files
User/device registry keys

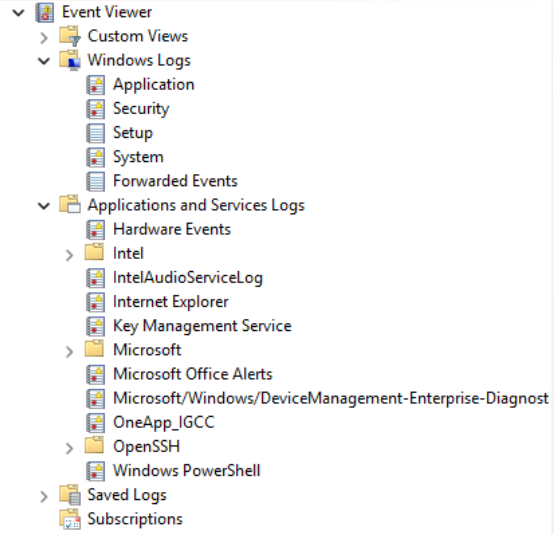
Device diagnostics mdmdiagnosticstool command line:
<Command HRESULT="0">%windir%\system32\mdmdiagnosticstool.exe -area Autopilot;deviceprovisioning;deviceenrollment;tpm;HololensFallbackDeviceOwner -cab %temp%\MDMDiagnostics\mdmlogs-2026-04-13-10-43-26.cab</Command>

Max diagnostics log size

How to parse logs?

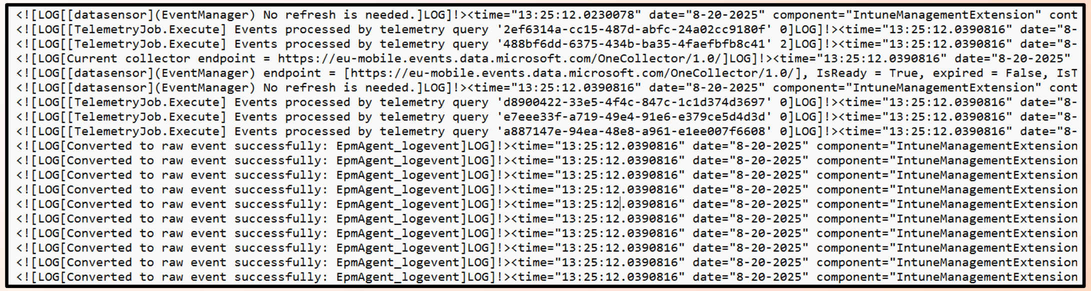
Windows Event Logs

- Event Viewer
- Single device query
- CMPivot (if still using ConfigMgr)
- Remediations
- Community Tools



Log files

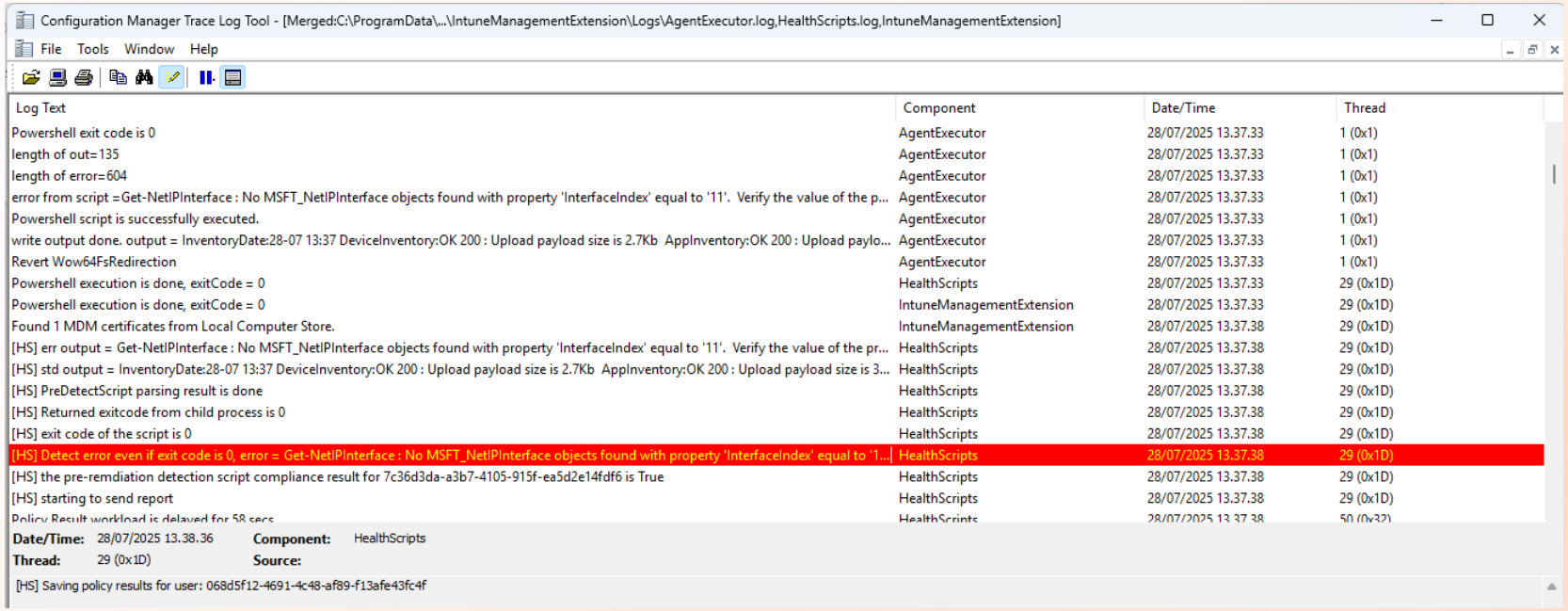
- CMTrace/CMTrace Open
- Notepad ++
- CMPivot (if still using ConfigMgr)
- Remediations
- Community Tools



```
<![LOG[[datasensor](EventManager) No refresh is needed.]LOG]!><time="13:25:12.0230078" date="8-20-2025" component="IntuneManagementExtension" cont
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query '2ef6314a-cc15-487d-abfc-24a02cc9180f' 0]LOG]!><time="13:25:12.0390816" date="8-
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query '488bf6dd-6375-434b-ba35-4faefbfb8c41' 2]LOG]!><time="13:25:12.0390816" date="8-
<![LOG[Current collector endpoint = https://eu-mobile.events.data.microsoft.com/OneCollector/1.0/]LOG]!><time="13:25:12.0390816" date="8-20-2025"
<![LOG[[datasensor](EventManager) endpoint = [https://eu-mobile.events.data.microsoft.com/OneCollector/1.0/], IsReady = True, expired = False, IsT
<![LOG[[datasensor](EventManager) No refresh is needed.]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension" cont
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query 'd8900422-33e5-4f4c-847c-1c1d374d3697' 0]LOG]!><time="13:25:12.0390816" date="8-
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query 'e7eee33f-a719-49e4-91e6-e379ce5d4d3d' 0]LOG]!><time="13:25:12.0390816" date="8-
<![LOG[[TelemetryJob.Execute] Events processed by telemetry query 'a887147e-94ea-48e8-a961-e1ee007f6608' 0]LOG]!><time="13:25:12.0390816" date="8-
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
<![LOG[Converted to raw event successfully: EpmAgent_logevent]LOG]!><time="13:25:12.0390816" date="8-20-2025" component="IntuneManagementExtension
```

CMTrace

- De-facto standard for log file reading
- Part of ConfigMgr client
  - Licensed also to use with Intune only environments
  - How to get?



Demo

CMTrace

Notepad++

- Very flexible text editor
- Free!
- Some cool features for log reading
  - Advanced search
  - Comparison

Demo

Notepad++

Intune Single Device Query

- Part of Intune Suite
  - Included in Microsoft 365 E3 & E5 license Q3 timeframe
- Easy way to access events from a remote device
- Not possible to read log files... ☹

CMPivot

- For customers still using ConfigMgr
- Possible to access events and log files
  - Any event
  - ConfigMgr log files are parsed nicely
  - Also possible to get any text based log files
- One or more devices as a target

Demo

Single-device query/CMPivot

Remediations

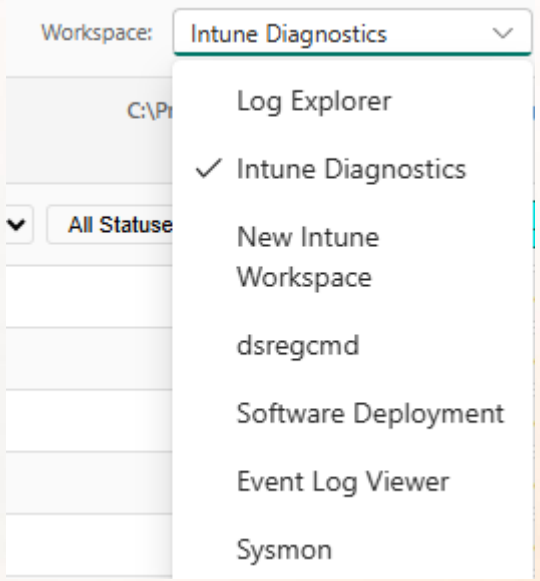
- Flexible method to get *anything* from devices
- On-demand remediation especially useful
- Only way to show custom information from devices to Intune portal
- Main scenarios:
  - To see how many other devices have the same issue (**When you know what you are looking for)**
  - Upload custom logs to some cloud storage for further debugging

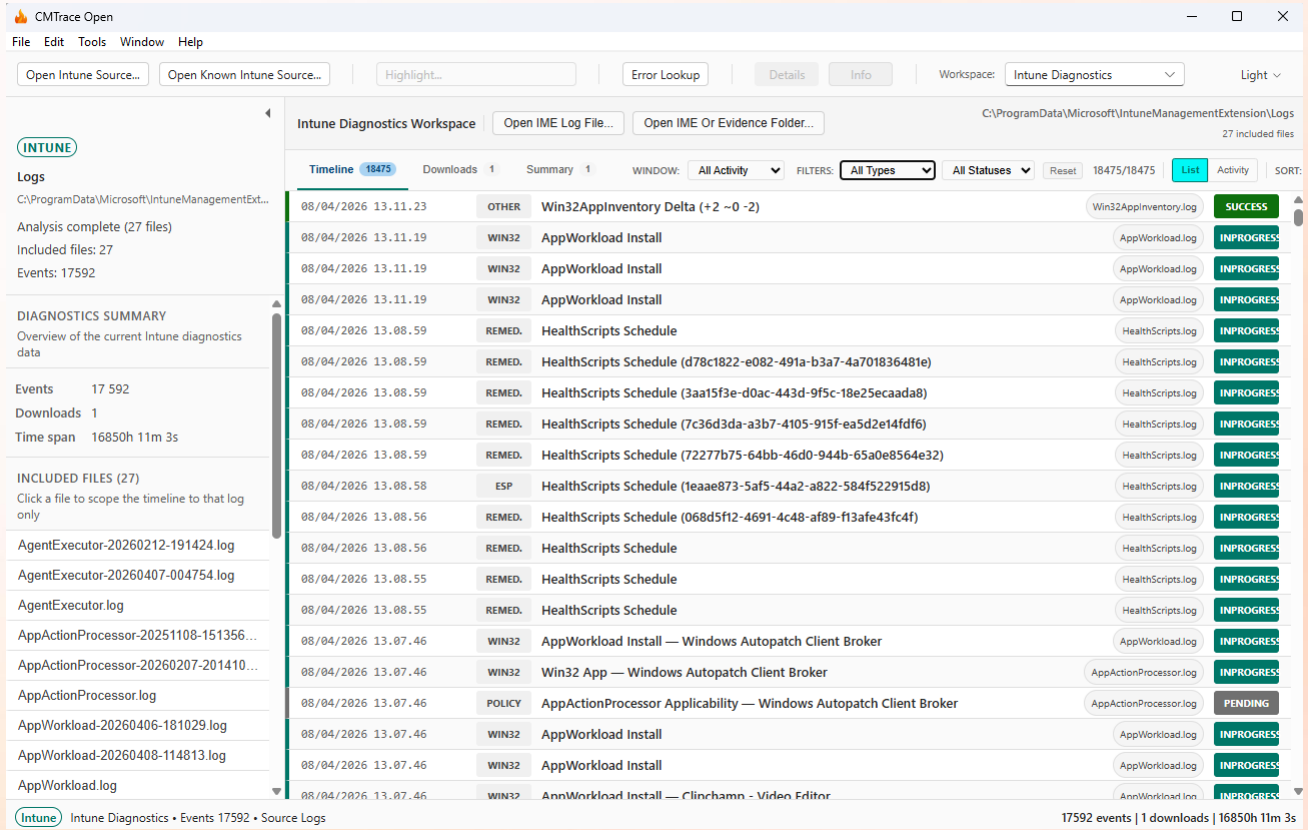
Demo

Remediations

CMTrace Open

- Open-source CMTrace like log viewer
  - https://github.com/adamgell/cmtraceopen
- Log files/Events…





Community tools

- Multiple community tools to help troubleshooting
- Autopilot
  - Get-AutopilotDiagnosticsCommunity
- Intune logs
  - Get-IntuneManagementExtensionDiagnostics
- General troubleshooting
  - Get-WindowsTroubleshootingReportCommunity
- What tools are missing?
  - Check the additional sessions

Community tools

- Multiple community tools to help troubleshooting

DEMO

Summary

- Intune Device Diagnostics gives you all the logs
  - Can be customized
- CMTrace is still a valuable tool
  - Can be used with Intune-only environments
- CMTrace-Open FTW ?!?
- Remediations very helpful with custom logs
- Single device query useful for events
  - CMPivot for text-based logs/events if using ConfigMgr
- Community tools fill many gaps!

Links

- All the example PowerShell scripts and KQL queries:
  - WP Ninjas FI Github
  - Get-IntuneManagementExtensionDiagnostics
  - Get-WindowsTroubleshootingReportCommunity

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!