

Troubleshooting the Modern Managed Client

Ronni Pedersen

Cloud Architect, APENTO

@RonniPedersen



Workplace Ninja Virtual Edition 2020



V-Platin Sponsor



Patch My PC
PATCH MANAGEMENT MADE EASY



RECAST SOFTWARE

V-Gold Sponsor

liquidwareTM

baseVISION
SECURE & MODERN WORKPLACE

2Pint
Software

PolicyPakTM
SECURING YOUR STANDARDS

Event Sponsors

SmartIT

make it noble

RealStuff
Informatik AG

baggenstos.

Computerworld

SD:>_
[swissdevjobs.ch]



Ronni Pedersen

Cloud Architect

- APENTO ApS
- Microsoft MVP: Enterprise Mobility (13 years)
- MCSE/MCSA/MCITP/MCTS (+75 certifications)
- ITIL Foundation Certified
- Microsoft Certified Trainer since 2007 (MCT)

Contact Me

- Twitter: @ronnipedersen
- Website: <https://www.apento.com/>
- Blog: <https://www.ronnipedersen.com/>
- Mail: rop@apento.com
- Phone: +45 2085 9452





Agenda

During this session we will cover how to troubleshoot:

- Intune Enrollment (Standalone and Hybrid)
- Intune Profiles and Device Compliance
- Intune Management Extension
- PowerShell Scripts
- Win32 Apps



Intune Enrollment





- Existing PC
- New PC – AAD Join (Auto Enrollment)
- Existing PC – Hybrid AAD Joined
- New PC – Hybrid AAD Joined (Auto Enrollment)

Userless enrollment (Bulk enrollment)



Before you start troubleshooting...

Check the following first:

- Is a valid Intune license assigned to the user?
- Is the user allowed to enroll a device (MDM User scope)?
- Is the latest update installed on the Windows device?
- Is automatic MDM enrollment enabled?

Collect the following information about the problem:

- What is the exact error message/ error code?
- Where/When does the error message appears?
- When did the problem start? Has enrollment ever worked?
- How many users are affected? Are all users affected or just some?
- How many devices are affected? Are all devices affected or just some?





Something went wrong.

This user is not authorized to enroll. You can try to do this again or contact your system administrator with the error code 801c0003.

Additional problem information:

Server error code: 801c0003

Correlation ID: 3cf8d9b5-a749-43f7-97e4-9b315ffe97fd

Timestamp: 08-16-2019 9:14:01Z

Server message: User '538156d0-c028-429c-90ec-be15074f379f' is not eligible to enroll a device of type 'Windows'. Reason 'DeviceCapReached'.

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



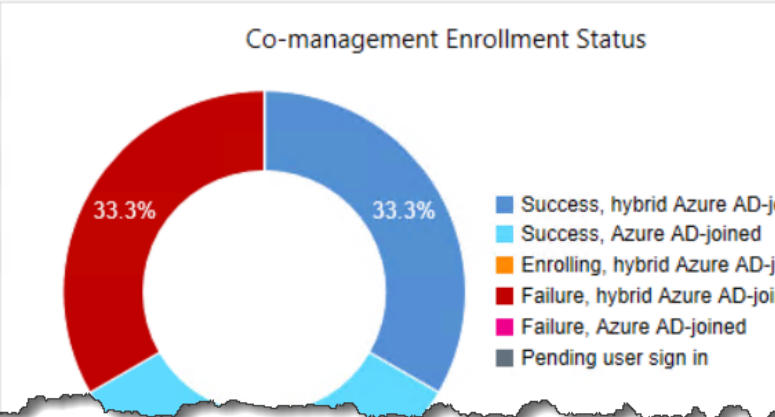
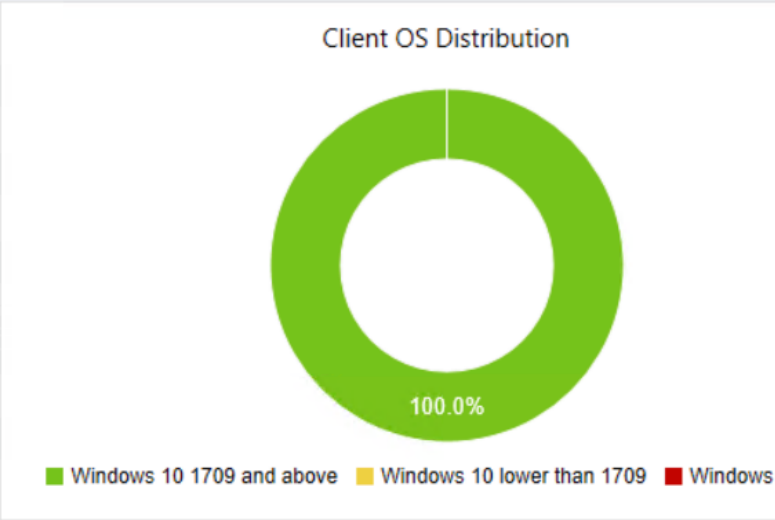
Troubleshoot enrollment issues

- Always check error codes if the description is not right
- <https://docs.microsoft.com/en-us/intune/enrollment/troubleshoot-windows-enrollment-errors>
- Check enrollment errors in the MEM Intune console.
- Also if using SCCM co-management
 - <https://docs.microsoft.com/en-us/configmgr/comanage/how-to-monitor#enrollment-errors>





Co-management



Home > Microsoft Intune > Device enrollment - Enrollment failures

Device enrollment - Enrollment failures

Microsoft Intune

Search (Ctrl+J)

Filter Refresh Export

Quick start

Manage

Monitor

Help and support

Apple enrollment

Android enrollment

Windows enrollment

Terms and conditions

Enrollment restrictions

Device categories

Corporate device identifiers

Device enrollment managers

Enrollment failures

Audit logs

Incomplete user enrollments

Get help

For a graphical view of enrollment failures [see here.](#)

Select user

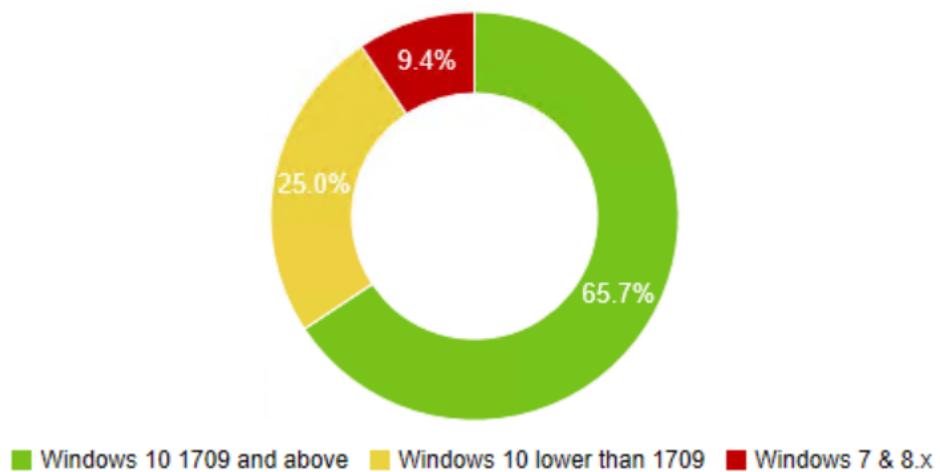
All users

Date	Failure	OS	OS version
Select a user or all users.			



Co-management

Client OS Distribution



Co-management Status

Eligible devices

Scheduled

Enrollment

Initiated

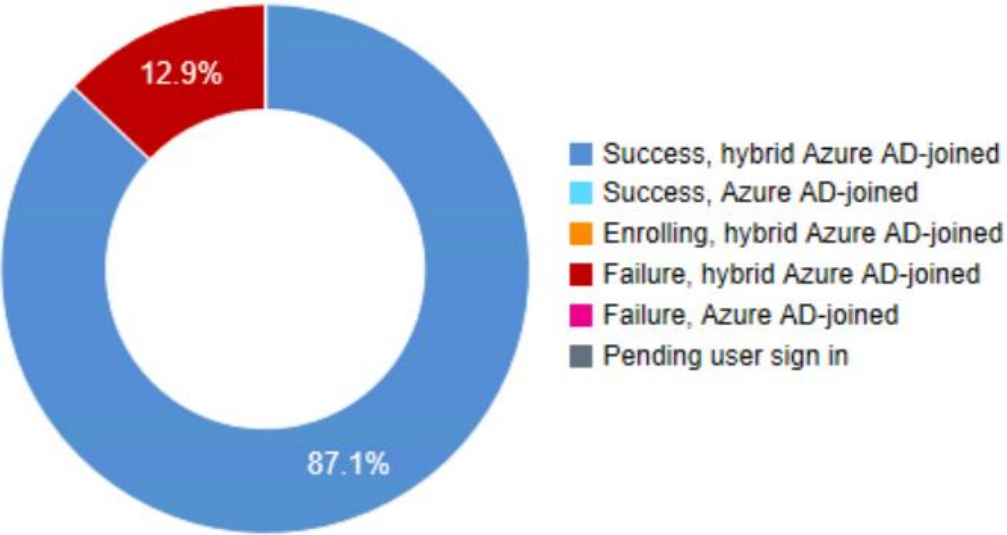
Enrolled





Co-Management Enrollment Status

Co-management Enrollment Status



Count	Enrollment Error
706	License of user is in bad state blocking enrollment
382	Undefined
6	Element not found.
5	Catastrophic failure
4	The Internet connection has timed out
2	MDM enrollment hasn't been configured yet on AAD, or the enrollment url isn't expected.
1	The user canceled the operation



Hybrid Azure AD Join

www.wpninjas.eu

- Group Policy (No Offset)
- Co-Management (Offset)
 - Schedules enrollment with an offset
 - If the enrollment fails, SCCM will retry 2 times every 15 mins
- Common issues
 - The users is not in AAD
 - The device is not Synced (Hybrid Azure AD Join)
- Will be flagged as Corporate

<https://www.imab.dk/auto-mdm-enrollment-fails-with-error-code-0x8018002a-troubleshooting-mdm-enrollment-errors-co-management-with-sccm-and-intune/>



Client Health

- How do you verify that a client is working as expected ?
- Co-management to the rescue!
- In Intune we can see:
 - Configuration Manager agent state
 - Last Configuration Manager agent check in time
 - Workloads managed by Intune
- Intune-enrolled devices connect to the cloud service 3 times a day, (approximately every 8 hours).





Search (Ctrl+*/*)

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Recovery keys

Managed Apps

RetireWipeDeleteRemote lockSyncReset passcodeRestartFresh StartAutopilot ResetQuick scan

Device name : APENTO-Bndfil1Z

Management name : mail_Windows_5/26/2019_6:52 PM

Ownership : Corporate

Serial number : 7987-3600-6266-3074-4536-7994-21

Phone number : ---

See more

Primary User : Ronni Pedersen

Enrolled by : Ronni Pedersen

Compliance : Not Compliant

Operating system : Windows

Device model : Virtual Machine

Device actions status

Action	Status	Date/Time
No results		

Co-management

Ronni Pedersen's Windows PC is being co-managed between Intune and Configuration Manager. Configuration Manager agent state is shown below, if the state is a there are a few steps that help with this. [Learn more](#)

Configuration Manager agent state

Unknown

Details

Details about the client's state are only reported for Configuration Manager version 1806 and later. Make sure that the Configuration Manager client is present on your running a supported version.

Last Configuration Manager agent check in time

05-06-2019 15:10:12

Intune managed workloads

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

Intune Profiles





Recommended Order

- Security Baselines
- Device Configuration Profiles
- Built-In Administrative Templates
- Custom ADMX ingestion (3rd. Party apps)
- PowerShell Scripts
- OMA-URI (Custom CSP)





Profile Tattooing

- Prior to 1909 removing the assignment of the policy from the user or device does not revert the setting.
- The setting remains until configured to a different value
- Even after removing the assignment of the policy
- A few profiles are removed after the assignment is removed or the profile is deleted:
 - Wi-Fi profiles
 - VPN profiles
 - Certificate profiles
 - Email profiles
- All other profile types are not removed.



Policy and Profile refresh cycles

- **Existing Devices**

- Windows 10 devices will scheduled check-in with the Intune service, which is estimated at: About every 8 hours

- **Recently Enrolled Devices**

- #1 - Every 3 minutes for 15 minutes
- #2 - Every 15 minutes for 2 hours
- #3 - Every 8 hours

- **Manual refresh**

- Open the Company Portal app, and sync the device to immediately check for policy or profile updates.
 - This device check-in will **not** refresh the already applied Policy CSP settings.
- Trigger Task Scheduler (Recommended for troubleshooting)
- Scripted methods





Computer Management

File Action View Help

Computer Management (Local)

- System Tools
 - Task Scheduler
 - Task Scheduler Library
 - Intel
 - Lenovo
 - Microsoft
 - Intune
 - Office
 - OneCore
 - Windows
 - .NET Framework
 - Active Directory Rights Management S
 - AppID
 - Application Experience
 - ApplicationData
 - AppxDeploymentClient
 - Autochk
 - BitLocker
 - Bluetooth
 - BrokerInfrastructure
 - CertificateServicesClient
 - Chkdsk
 - Clip
 - CloudExperienceHost
 - Customer Experience Improvement Pr
 - Data Integrity Scan
 - Defrag
 - Device Information
 - Device Setup
 - DeviceDirectoryClient
 - Diagnosis
 - DirectX
 - DiskCleanup
 - DiskDiagnostic
 - DiskFootprint
 - DUSM
 - EDP
 - EnterpriseMgmt
 - BF34185C-4364-40CF-A364-98DBD
 - VirtulizationBasedIsolation
 - ExploitGuard
 - Feedback

Name	Status	Triggers
Login Schedule created by enrollment client	Ready	At log on of any user
OS Edition Upgrade event listener created by enrollment client	Ready	Custom Trigger
Passport for Work alert created by enrollment client	Ready	On event - Log: Microsoft-Windows-User Device Registration/Admin, Source: Microsoft-Windows-User Device Registration
Provisioning initiated session	Ready	
PushLaunch	Ready	Custom Trigger
PushRenewal	Ready	Multiple triggers defined
PushUpgrade	Ready	At 16:15 on 18-01-2020
Schedule #1 created by enrollment client	Ready	At 23:24 on 16-05-2019 - After triggered, repeat every 00:03:00 for a duration of 15 minutes.
Schedule #2 created by enrollment client	Ready	At 23:39 on 16-05-2019 - After triggered, repeat every 15 minutes for a duration of 02:00:00.
Schedule #3 created by enrollment client	Ready	At 01:39 on 17-05-2019 - After triggered, repeat every 08:00:00 indefinitely.
Schedule created by enrollment client for renewal of certificate warning	Ready	At 23:21 on 04-04-2020 - After triggered, repeat every 7:00:00:00 for a duration of 49:00:00:00.
Schedule to run OMADMClient by client	Ready	
Schedule to run OMADMClient by server	Ready	
Win10 S Mode event listener created by enrollment client	Ready	Custom Trigger

General Triggers Actions Conditions Settings History (disabled)

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

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

Intune Profiles





Intune notifications // Sync immediately

www.wpninjas.eu

- Some actions will trigger a sync notification to the device
- When a Policy, Profile, or App is:
 - Assigned (or unassigned)
 - Updated
 - Deleted
- Current Limitation:
 - Only the first 200 devices will be updated !
 - By design (to avoid denial of service)
 - Workaround: Use script to connect to all clients and force a sync





Policy/Profile Conflicts

- 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.
 - By default the first created policy will “win”

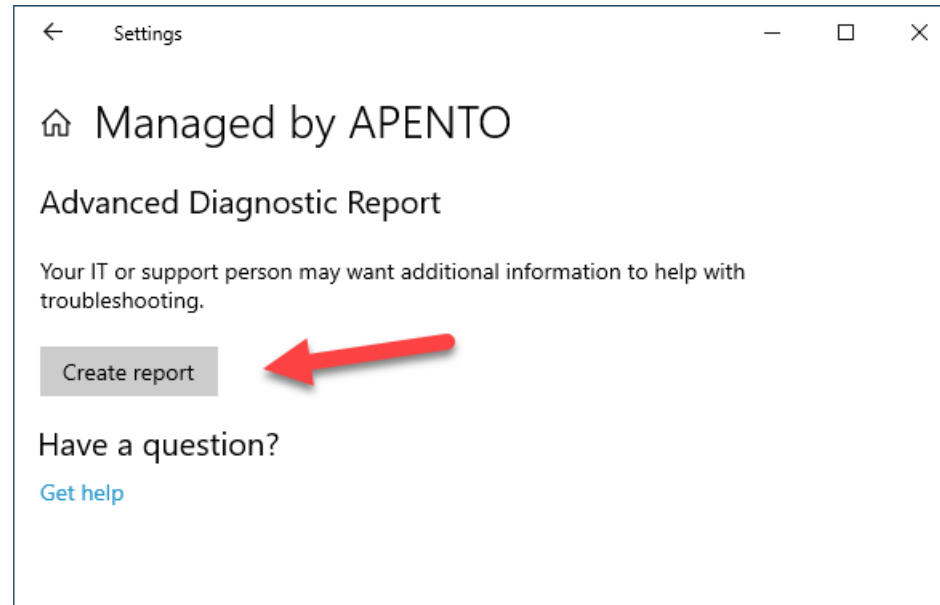




Troubleshooting MDM Policies

www.wpninjas.eu

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





Managed policies

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

Area	Policy	Default Value	Current Value	Target	Dynamic	Config Source
Authentication	EnableWebSignIn	0	1	device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
BitLocker	EncryptionMethodByDriveType			device		BF34185C-4364-40CF-A364-98DBD5B8ECB7= <enable d/> <data id="EncryptionMethodWithXtsOsDropDown_Name" value="7"/> <data id="EncryptionMethodWithXtsFdvDropDown_Name" value="7"/> <data id="EncryptionMethodWithXtsRdvDropDown_Name" value="7"/>
BitLocker	SystemDrivesRecoveryOptions			device		BF34185C-4364-40CF-A364-98DBD5B8ECB7= <enable d/> <data id="OSAllowDRA_Name" value="true"/> <data id="OSRecoveryPasswordUsageDropDown_Name" value="2"/> <data id="OSRecoveryKeyUsageDropDown_Name" value="2"/> <data id="OSHideRecoveryPage_Name" value="false"/> <data id="OSActiveDirectoryBackup_Name" value="true"/> <data id="OSActiveDirectoryBackupDropDropDown_Name" value="1"/> <data id="OSRequireActiveDirectoryBackup_Name" value="true"/>
BitLocker	RequireDeviceEncryption	0	1	device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	AllowArchiveScanning	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	RealTimeScanDirection	0		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	AllowEmailScanning	0		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	AllowOnAccessProtection	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	AllowIntrusionPreventionSystem	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1
Defender	PUAProtection	0		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=2
Defender	AVGCPULoadFactor	50		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=50
Defender	AllowCloudProtection	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1



- Intune portal page
 - <https://aka.ms/intunetroubleshooting>
- Displays information focused around a particular user
 - See info about assignments, devices, enrollment failures, etc.
- For more info:
<https://docs.microsoft.com/en-us/intune/help-desk-operators>

Dashboard > Microsoft Intune - Troubleshoot

Microsoft Intune - Troubleshoot

Search (Ctrl+/)

Account status: Active

Display name: **Anna Anderson**
Principal name: anna@contosocm.com
Email: anna@contosocm.com
[Change](#)

Intune license: ✓
99 devices non compliant

GROUP MEMBERSHIP
AutoPilot Users

ASSIGNMENTS
Client apps

ASSIGNME...	NAME	OS	TYPE	LAST MODIFIED
Included	AutopilotBranding	Windows P...	required	4/20/2019 12:27:31 AM
Included	Chrome		required	3/10/2019 7:20:55 AM
Included	Office 365 ProPlus (cu...	Windows 10...	required	3/28/2019 6:23:43 PM
Included	paint.net		required	2/1/2019 10:01:20 AM
Included	VPNSetup	Windows P...	required	11/27/2018 7:03:40 AM

DEVICES
Showing 110 of 110

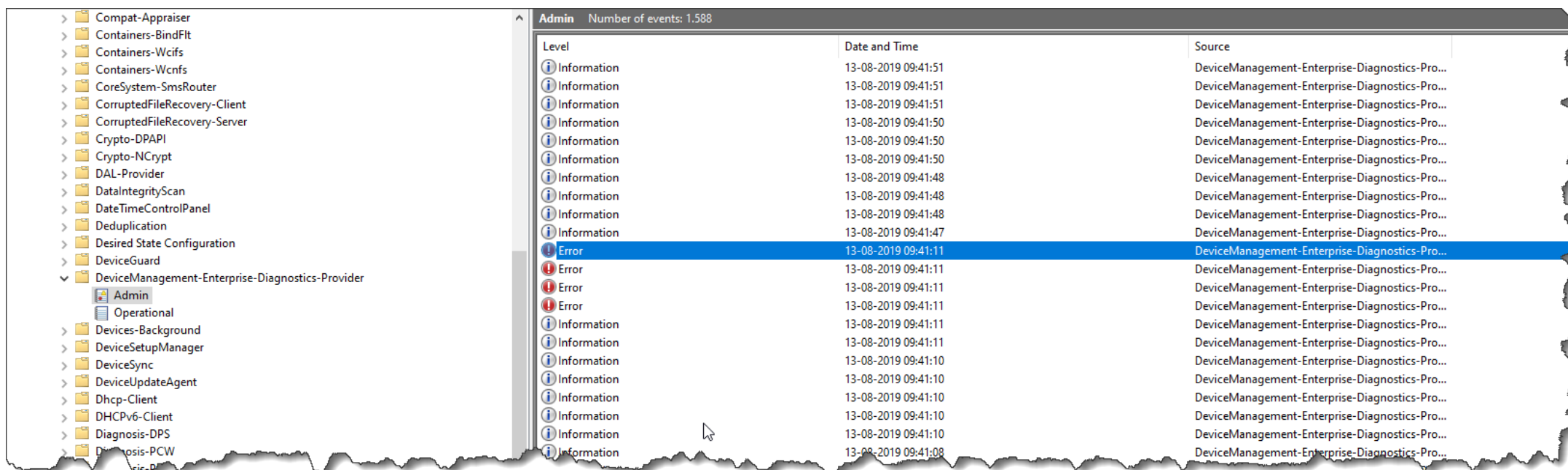
DEVIC...	...	A...	O...	INTU...	AZURE ...	A...	OS	...	LAST ...
AAD-573...	MDM	Not ...	Corp...	✓ Yes	NA	✓	Win...	10.0...	4/12/201...



Device Profiles // Where is my logs ?

www.wpninjas.eu

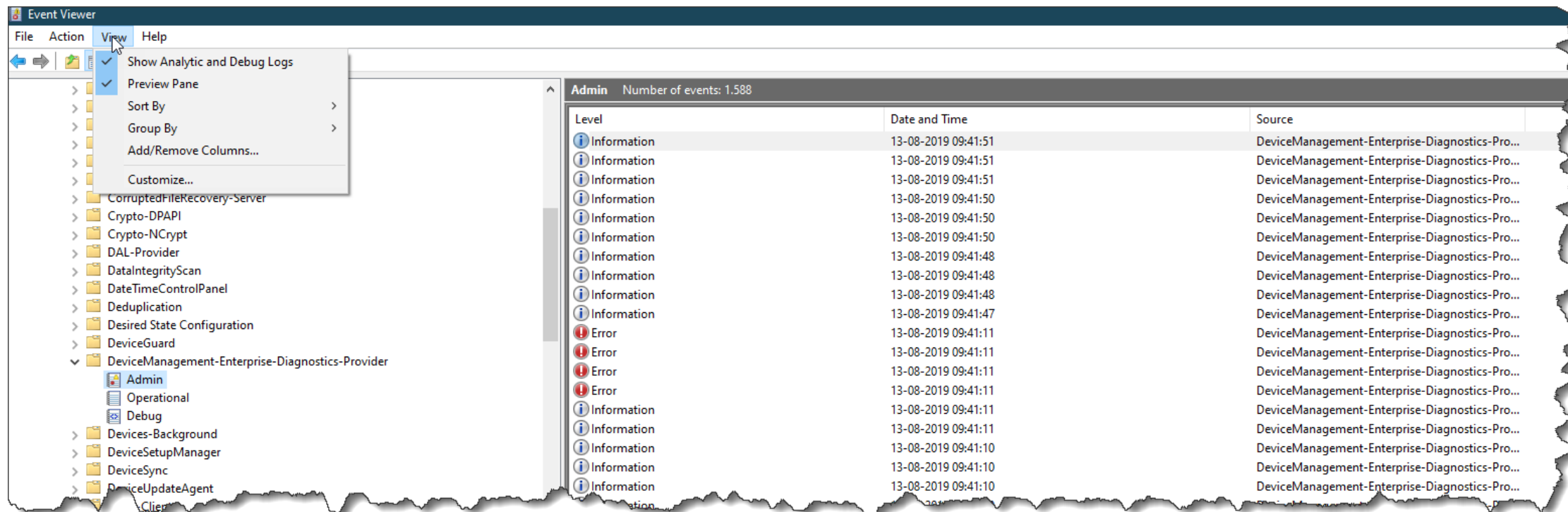
- Event viewer is your new best friend
 - Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider





Enable debug mode

www.wpninjas.eu



Intune Management Extension





Intune Management Extension

www.wpninjas.eu

- An Introduction...
 - Know it
 - Plan it
 - Own it!





Management Extension // Pre-requisites

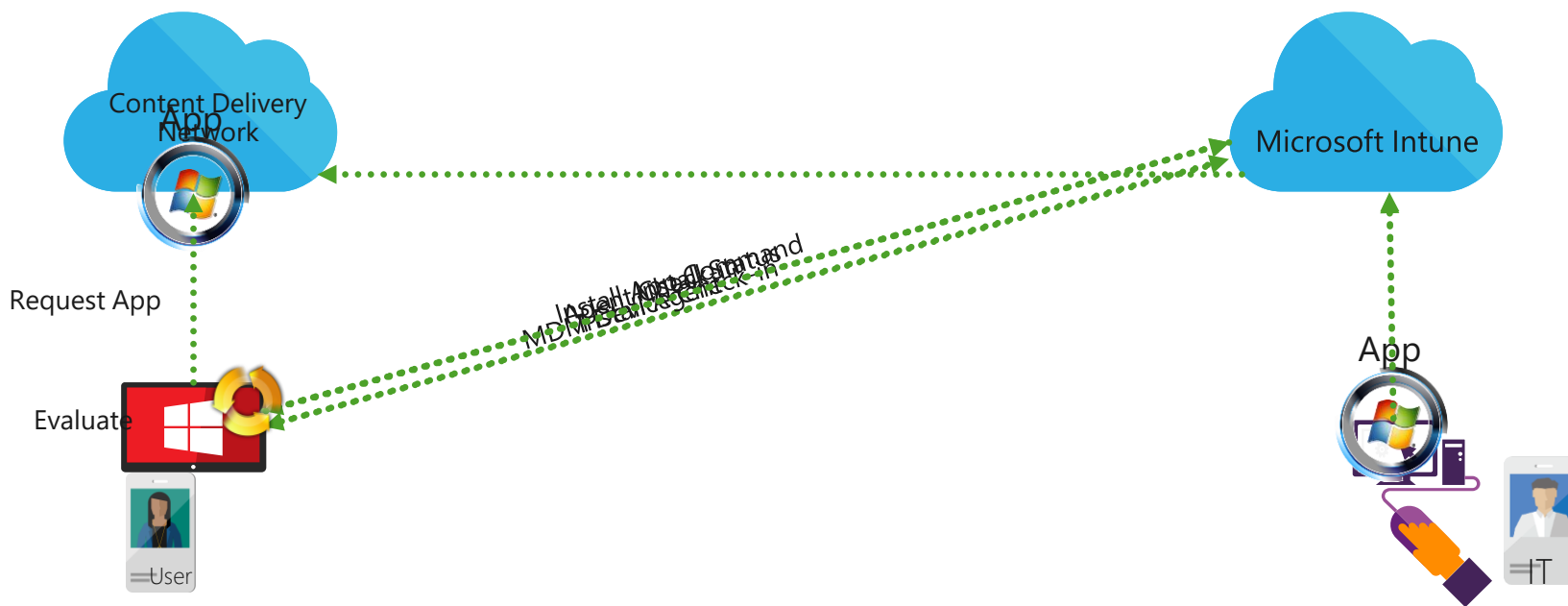
www.wpninjas.eu

- Installed only on "Corporate owned devices"
- Not installed automatically - installed when needed!
 - Triggered by:
 - PowerShell scripts
 - Win32 apps
- <https://docs.microsoft.com/en-us/intune/apps/intune-management-extension#prerequisites>





Win32 App Install





What is a Corporate Device?

- The enrolling user is using a device enrollment manager account.
- The device enrolls through Windows Autopilot.
- The device enrolls through a bulk provisioning package.
- The device enrolls through GPO
 - or automatic enrollment from SCCM for co-management.





Intune Management Extension Event log

www.wpninjas.eu

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

Event Viewer

File Action View Help

CodeIntegrity
Compat-Appraiser
Containers-BindFlt
Containers-Wcifs
Containers-Wcnfs
CoreSystem-SmsRouter
CorruptedFileRecovery-Client
CorruptedFileRecovery-Server
Crypto-DPAPI
Crypto-NCrypt
DAL-Provider
DataIntegrityScan
DateTimeControlPanel
Deduplication
Desired State Configuration
DeviceGuard
DeviceManagement-Enterprise-Diagnostics-Provider
Admin
Operational
Devices-Background
DeviceSetupManager
DeviceSync
DeviceUpdateAgent
Dhcp-Client
DHCPv6-Client
Diagnosis-DPS
Diagnosis-PCW
Diagnosis-PLA
Diagnosis-Scheduled
Diagnosis-Scripted

Admin Number of events: 1.792

Filtered: Log: Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin; Levels: Critical, Error,

Level	Date and Time	Source	Event ID	Task Ca...
Error	04/02/2020 17.02.45	Device...	404	None
Error	04/02/2020 09.38.12	Device...	404	None
Error	04/02/2020 09.36.49	Device...	404	None
Error	04/02/2020 04.45.16	Device...	404	None
Error	04/02/2020 01.02.38	Device...	404	None
Error	03/02/2020 17.02.42	Device...	404	None
Error	03/02/2020 16.04.37	Device...	1903	None
Error	03/02/2020 16.04.32	Device...	1903	None
Error	03/02/2020 12.25.21	Device...	404	None
Error	03/02/2020 12.22.39	Device...	404	Nor
Error	03/02/2020 12.02.23	Device...	404	Nor
Error	03/02/2020 12.00.37	Device...	404	None
Error	03/02/2020 11.59.50	Device...	454	None
Error	03/02/2020 11.59.43	Device...	1924	None

Look for event id 1924

Event 1924, DeviceManagement-Enterprise-Diagnostics-Provider

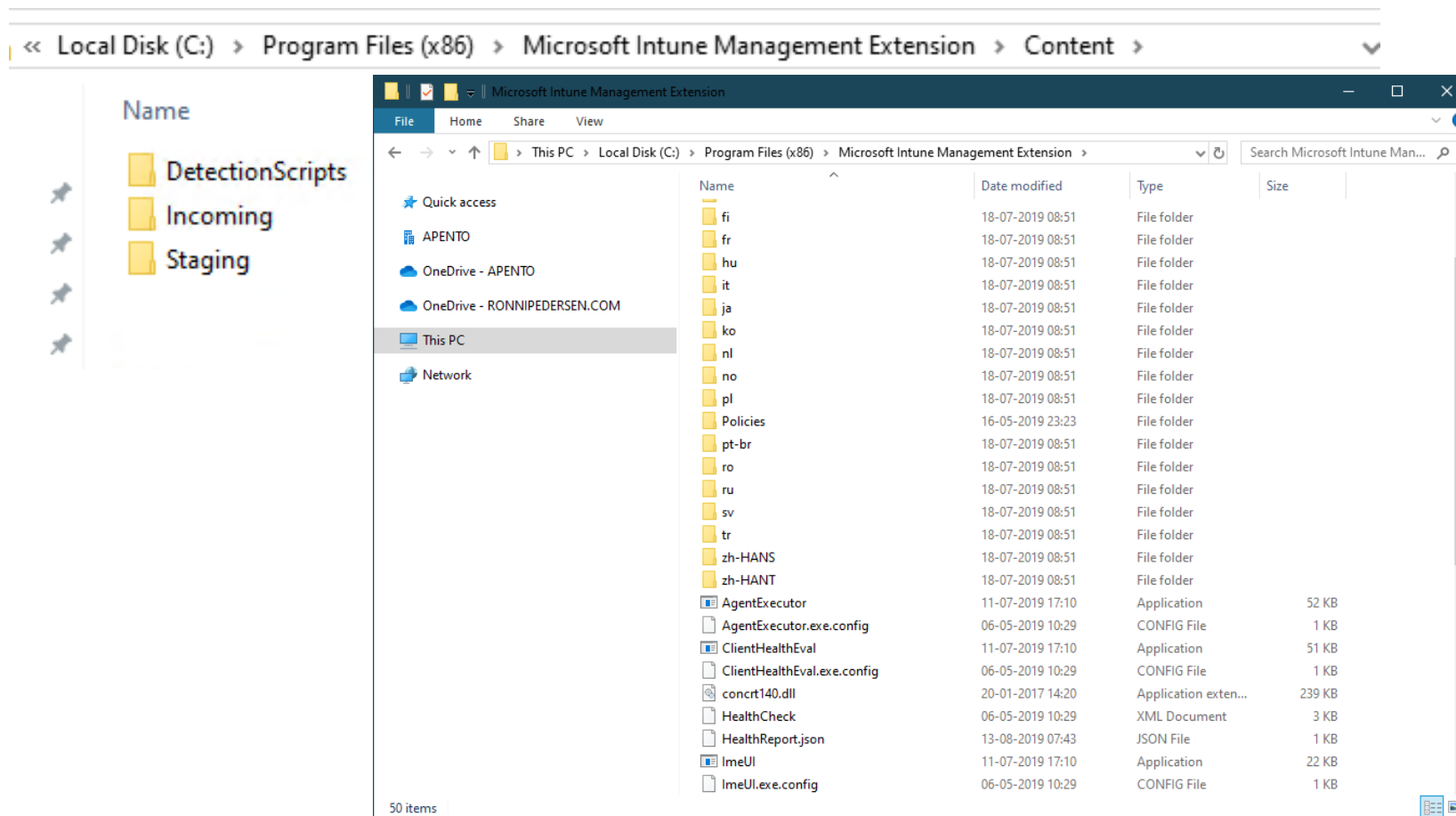
General Details

EnterpriseDesktopAppManagement CSP: An application install has failed. Examine the MSI log (C:\WINDOWS\system32\config\systemprofile\AppData\Local\mdm\093ea47b-ef2c-4f46-a022-6f57a50e39a2.log) for more details. Install command: ("C:\WINDOWS\system32\msiexec.exe" /quiet /I*v "C:\WINDOWS\system32\config\systemprofile\AppData\Local\mdm\093ea47b-ef2c-4f46-a022-6f57a50e39a2.log" /qn /i "C:\WINDOWS\system32\config\systemprofile\AppData\Local\mdm\{B9BDE5CE-DD33-4D55-A992-A874F601627D}.msi"), MSI ProductCode: 093ea47b-ef2c-4f46-a022-6f57a50e39a2, User SID: (S-0-0-00-0000000000-0000000000-0000000000), Result: (Fatal error during installation.).



Intune Management Extension File System

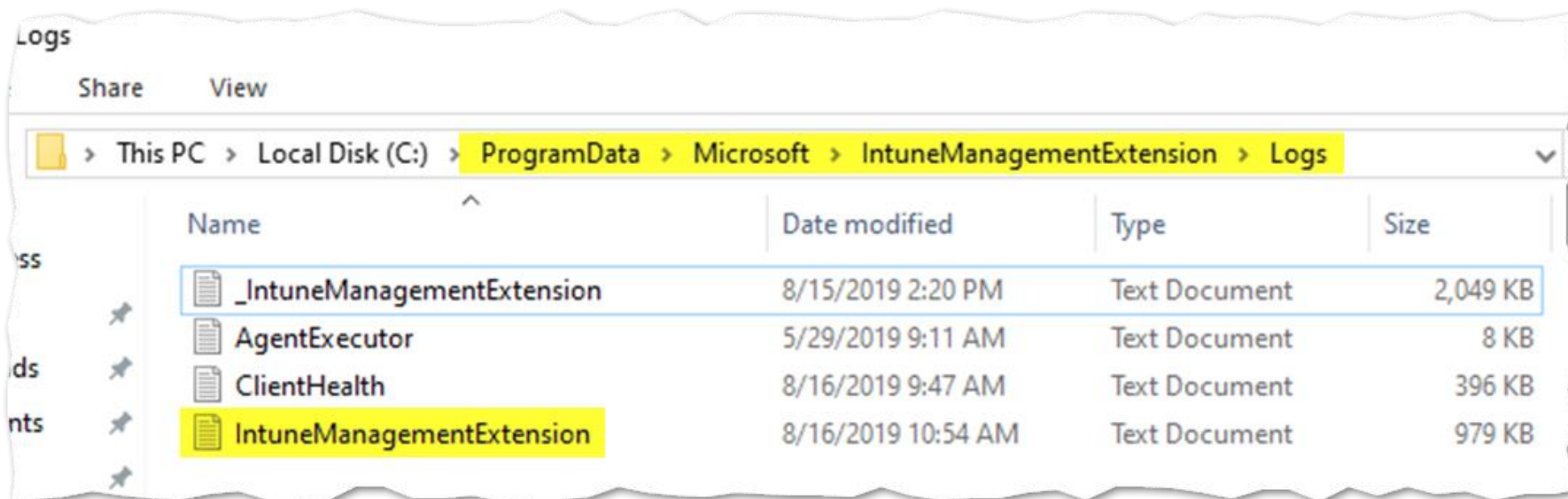
www.wpninjas.eu





Intune Management Extension Log files

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



The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Local Disk (C:) > ProgramData > Microsoft > IntuneManagementExtension > Logs'. The file list contains four text documents: '_IntuneManagementExtension' (2,049 KB), 'AgentExecutor' (8 KB), 'ClientHealth' (396 KB), and 'IntuneManagementExtension' (979 KB). The last file is highlighted in yellow.

Name	Date modified	Type	Size
_IntuneManagementExtension	8/15/2019 2:20 PM	Text Document	2,049 KB
AgentExecutor	5/29/2019 9:11 AM	Text Document	8 KB
ClientHealth	8/16/2019 9:47 AM	Text Document	396 KB
IntuneManagementExtension	8/16/2019 10:54 AM	Text Document	979 KB



Intune Management Extension The Registry

www.wpninjas.eu

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

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\Policies\ff7aeb45-9c78-425c-aecd-46f8b2885210\b3ec6261-4b72-41b2-94af-027ce04fcc5c

Name	Type	Data
(Default)	REG_SZ	(value not set)
DownloadCount	REG_DWORD	0x00000001 (1)
ErrorCode	REG_DWORD	0x00000000 (0)
InternalVersion	REG_DWORD	0x00000001 (1)
LastUpdatedTim...	REG_SZ	03/02/2020 11.50.29
PolicyHash	REG_SZ	9t14EIVlp1sllS/JA3/Viu3D0llsfk/HLLxCKM5VOJE=
Result	REG_SZ	Success
ResultDetails	REG_SZ	My super advanced PowerShell script has executed!



Intune Management Extension

- Troubleshooting

- Check that the service is installed and running
- Verify deployment in MDMDiagReport.html
- Are you meeting the Prerequisites?
<https://docs.microsoft.com/en-us/intune/apps/intune-management-extension#prerequisites>

A screenshot of the 'Microsoft Intune Management Extension Properties (Local Comput...)' dialog box. The 'General' tab is selected. It shows the service name as 'IntuneManagementExtension', the display name as 'Microsoft Intune Management Extension' (underlined), and the description as 'Microsoft Intune Management Extension'. The path to the executable is 'ment Extension\Microsoft.Management.Services.IntuneWindowsAgent.exe'. The startup type is set to 'Automatic (Delayed Start)'. The service status is 'Running'. There are buttons for 'Start', 'Stop', 'Pause', and 'Resume'. A section for 'Start parameters' is also visible, with a text box for specifying parameters.

Microsoft Intune Management Extension Properties (Local Comput...)

General Log On Recovery Dependencies

Service name: IntuneManagementExtension

Display name: Microsoft Intune Management Extension

Description: Microsoft Intune Management Extension

Path to executable: ment Extension\Microsoft.Management.Services.IntuneWindowsAgent.exe"

Startup type: Automatic (Delayed Start)

Service status: Running

Start Stop Pause Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK Cancel Apply

PowerShell Scripts





PowerShell Scripts // Not applying

www.wpninjas.eu

- Verify Intune Management Extension is installed.
- Check your assignments (don't mix devices and users)
- Decide on 32 or 64 bit from the start, don't change afterwards (recreate instead)
- Take a deep breath and start from scratch...



Applying but not working as expected

- Always consider context!
 - In "User context" mode PS executes with users permissions.
 - In "System context" has no knowledge of the user.
 - Execution will happen regardless of the user being logged in.
- Verify script contents as seen by IME
 - `\ProgramData\Microsoft\IntuneManagementExtension\Logs\IntuneManagementExtension.log`
 - Put keywords in script to easily find it through a search.
 - `#MyAwesomeScriptVersion4`



Applying but status is failed

- Your script is returning a terminating error
 - Consider logging with "start-transcript / stop-transcript"
 - Worst case, force "exit 0"

Home > Device configuration - Scripts > Solidworks2019 Configuration - Device status

Solidworks2019 Configuration - Device status

Windows 10 and later

Search (Ctrl+/) << Export

OS Version	Status	Last Updated
10.0.18363.592	❌ Failed	1/29/20, 12:41 PM

Overview

Manage

Properties

Monitor

Device status

User status



Applied once - then never again?

- This is by design
- PowerShell execution manifest states:
 - Execute once and never revisit after success.
 - Retry 3 times if failed (once an hour), then fail permanently.
 - Execute once more if script contents or configuration changes (resets failed attempts).
- Don't mind hacking your way around this behaviour?
<https://www.iphase.dk/hacking-intune-management-extension/>
- Workaround: Use remediation script



Still have problems?

www.wpninjas.eu

You are not alone... But we'll get there...

MICROSOFT INTUNE

Windows Autopilot oddities

BY MICHAEL NIEHAUS ON AUGUST 15, 2019 • ([LEAVE A COMMENT](#))

Sometimes **I can't explain them**, but I can at least pass them on so that you don't tear your hair out trying to figure out what's going on.

- The enrollment status page **doesn't track PowerShell scripts** executed via Intune Management Extensions. They will be sent to the machine along with all the other policies, and if you are installing a bunch of apps it's quite **possible** that the PowerShell scripts will install. **But it's not guaranteed**; **they may** continue running after ESP has completed.
- The enrollment status page **doesn't actually track** device configuration policies. You **might** notice that it shows "0 of 1" for security policies, and that quickly changes to "1 of 1." But if you have created multiple device configuration policies in Intune, as well as security baselines, they aren't explicitly tracked. Again, if you install any apps it's **quite likely that they will be processed** and applied before ESP completes.
- Win32 app install failures cause ESP timeout errors. If you install a Win32 app via Intune Management Extensions and that app install fails, typically with an unexpected return code, that **error isn't reported by the ESP**. (You will see it in the Intune Management Extensions log and in the Intune portal.) Instead, the ESP will always wait until it times out.
- Win32 app install detection rule errors cause an ESP timeout error. If you install a Win32 app via Intune Management Extensions but you don't have the detection rules right, Intune Management Extensions **will assume the app failed** to install and will try to install it again – over and over again. (I've had a number of people say "but it works fine when not using ESP. Well sure, but Intune is still installing it over and over again, you just don't notice. Make sure you get your detection rules right.)
- ESP settings can be complicated. Currently Intune targets ESP settings to users, not to devices. But there are some scenarios (e.g. white glove, self-deploying mode) where there isn't a user. In those cases, ESP will use a default set of policies. So you might expect to see longer timeouts or a list of filtered apps, but that doesn't actually happen. (There's more to it, but **it gives me a headache trying to reason it all out**, so I'll stick with the simple explanation.)
- Some Windows Autopilot scenarios (e.g. self-deploying mode, user-driven Hybrid Azure AD Join) will fail with an enrollment error (80180005) if you assign the Autopilot profile via Microsoft Store for Business instead of through Intune. **So don't assign profiles via Microsoft Store for Business.**

That's all I can think of right at this moment, but I'm sure there are more...

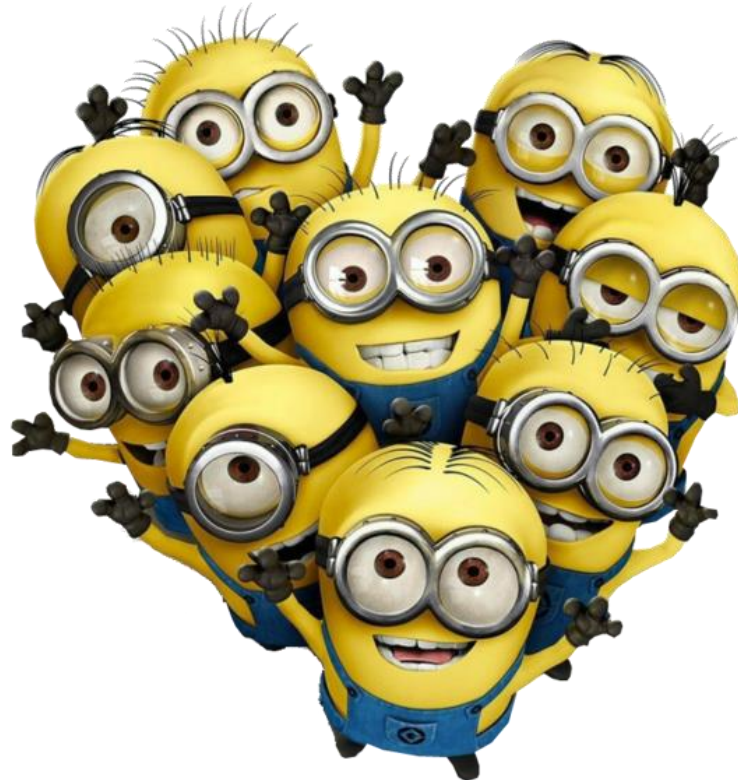




Share your ideas

www.wpninjas.eu

<http://microsofttintune.uservoice.com/>
<http://configurationmanager.uservoice.com/>





Thank You



Workplace Ninja Virtual Edition 2020