Troubleshooting the Modern Managed Client

Ronni Pedersen

Cloud Architect, APENTO

@RonniPedersen

Workplace Ninja Virtual Edition 2020

V-Platin Sponsor

V-Gold Sponsor

Event Sponsors

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

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

Scenarios

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

Userless enrollment (Bulk enrollment)

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?
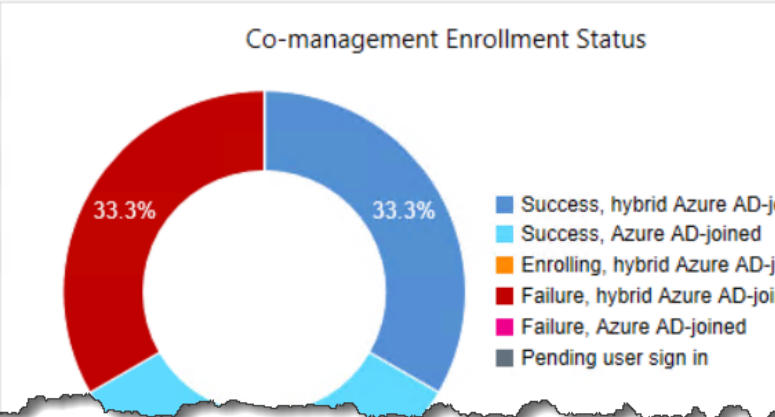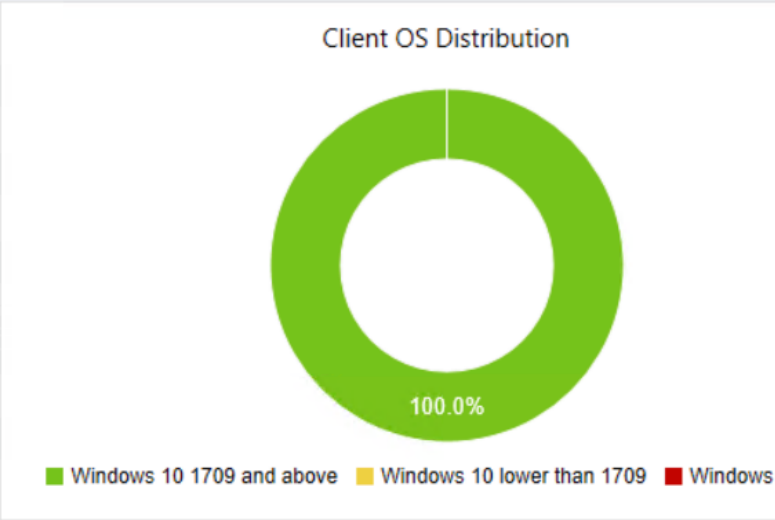- How many devices are affected? Are all devices affected or just some?

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

Co-Management

Co-management

Client OS Distribution

9.4%

25.0%

65.7%

■ Windows 10 1709 and above   ■ Windows 10 lower than 1709   ■ Windows 7 & 8.x
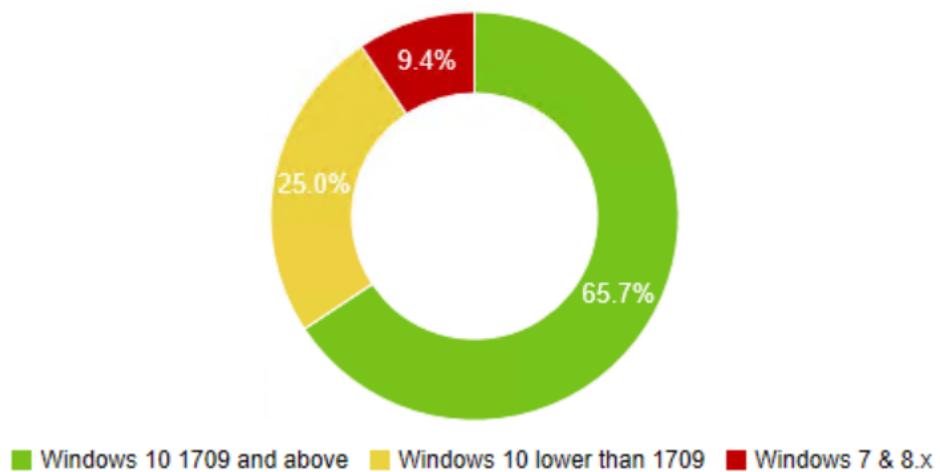
Co-management Status

Eligible devices — 9881

Scheduled — 7375

Enrollment Initiated — 7375

Enrolled — 7374

Co-management Enrollment Status

- Success, hybrid Azure AD-joined
- Success, Azure AD-joined
- Enrolling, hybrid Azure AD-joined
- Failure, hybrid Azure AD-joined
- Failure, Azure AD-joined
- Pending user sign in

12.9%

87.1%
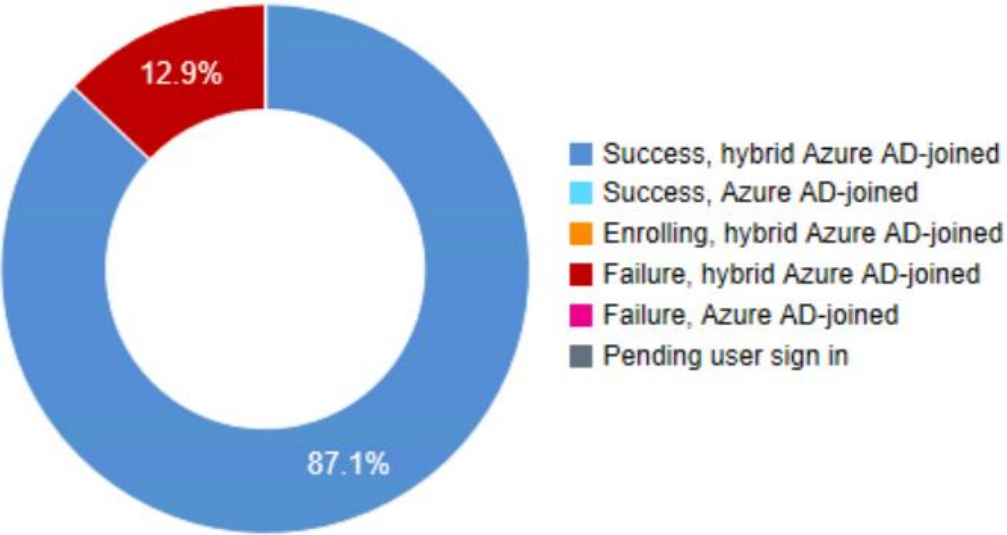
Count	Enrollment Error
706	License of user is in bad state blocking enrollment
382	Undefined
6	Element not found.
5	Catastrophic failure
4	The Internet connection has timed out
2	MDM enrollment hasn't been configured yet on AAD, or the enrollment url isn't expected.
1	The user canceled the operation

- 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).

✕ Retire   ↩ Wipe   🗑 Delete   🔒 Remote lock   ↻ Sync   🔑 Reset passcode   ⏻ Restart   ↩ Fresh Start   ⏻ Autopilot Reset   ⟳ Quick scan

Device name	: APENTO-Bndfil1Z	Primary User	: Ronni Pedersen
Management name	: mail_Windows_5/26/2019_6:52 PM	Enrolled by	: Ronni Pedersen
Ownership	: Corporate	Compliance	: Not Compliant
Serial number	: 7987-3600-6266-3074-4536-7994-21	Operating system	: Windows
Phone number	: ---	Device model	: Virtual Machine

See more

⌃

Left navigation:

🔍 Search (Ctrl+/)

ⓘ Overview

Manage

⫼ Properties

Monitor

🖥 Hardware

🔲 Discovered apps

📱 Device compliance

🖳 Device configuration

🔳 App configuration

🗄 Security baselines

🔑 Recovery keys

👥 Managed Apps

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 you 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.

- **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

Intune Profiles

- 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

- C:\Users\Public\Documents\MDMDiagnostics\MDMDiagReport.html
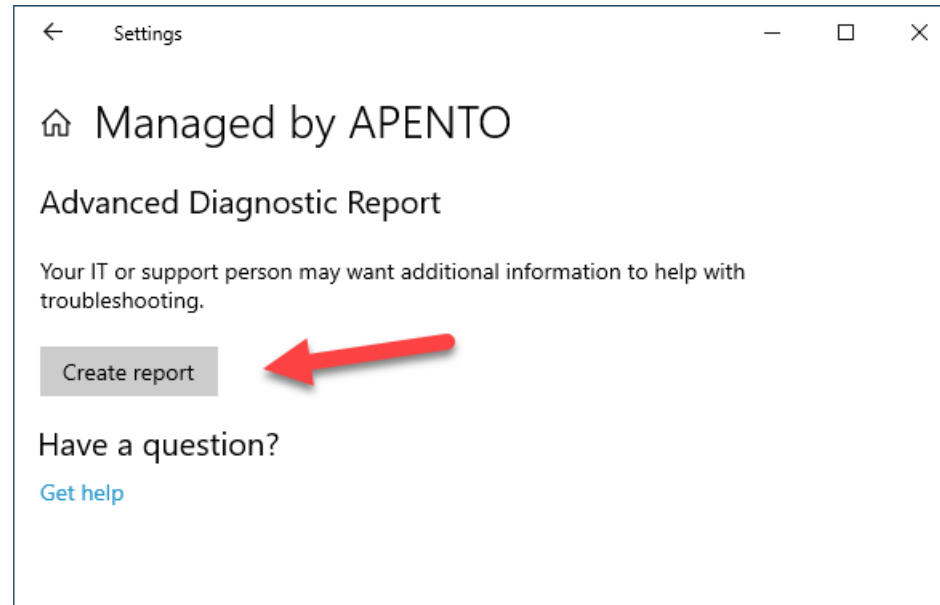
Managed policies ^

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=<enabled/><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=<enabled/><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="OSActiveDirectoryBackupDropDown_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
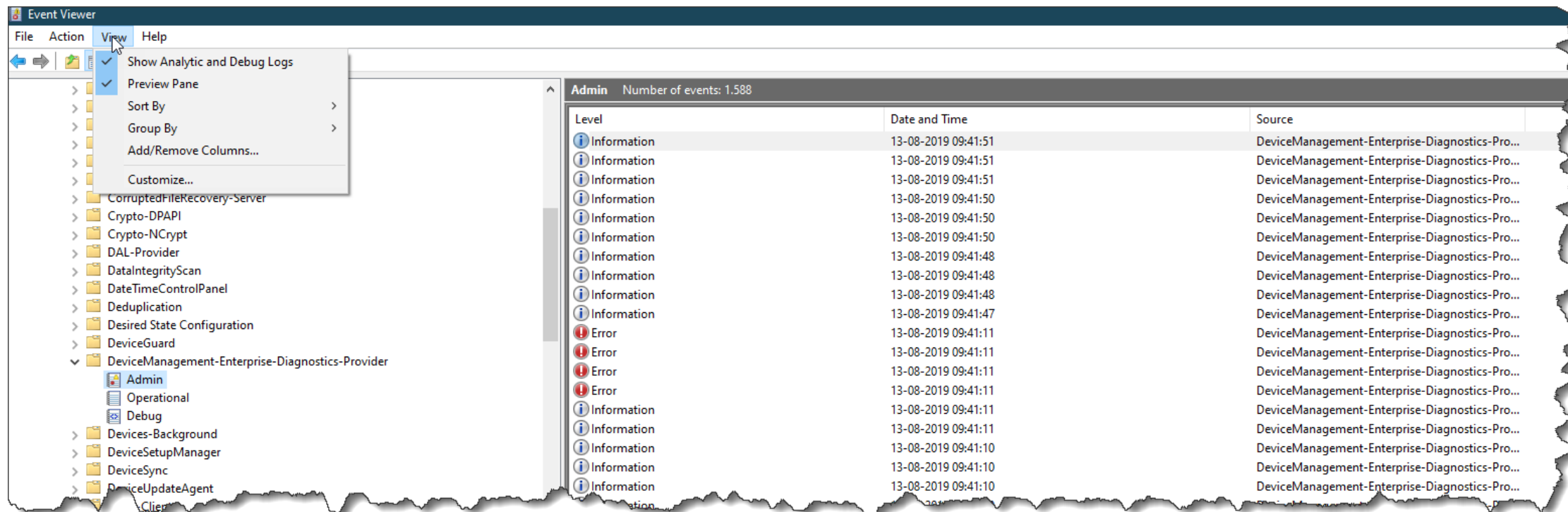
Device Profiles // Where is my logs ?

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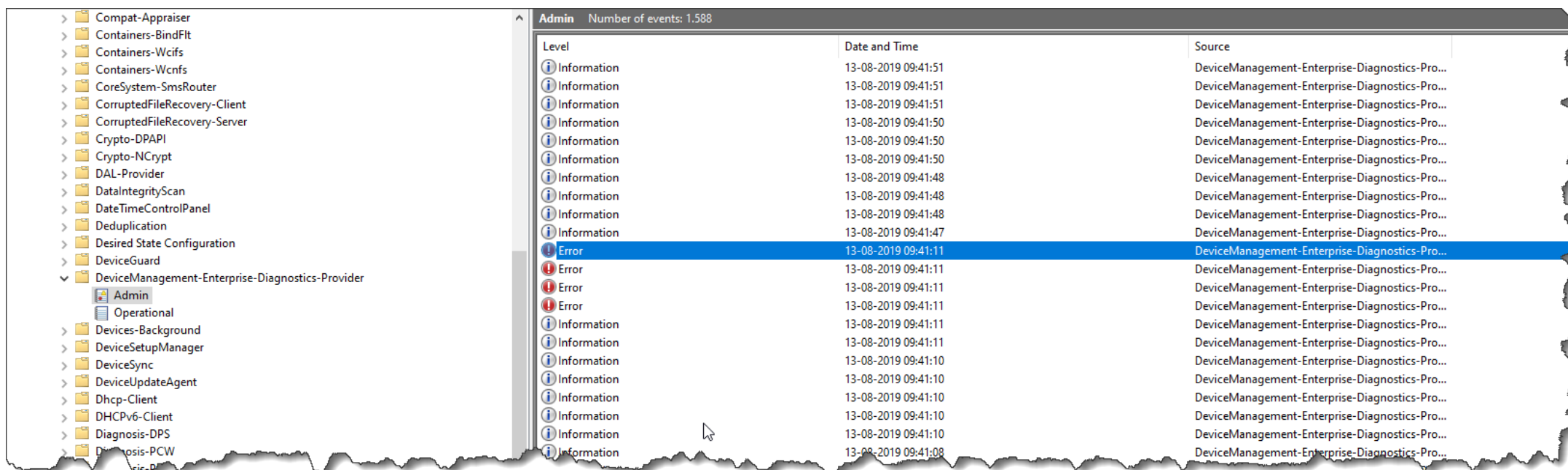
Enable debug mode

Intune Management Extension

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

Management Extension // Pre-requisites

- 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
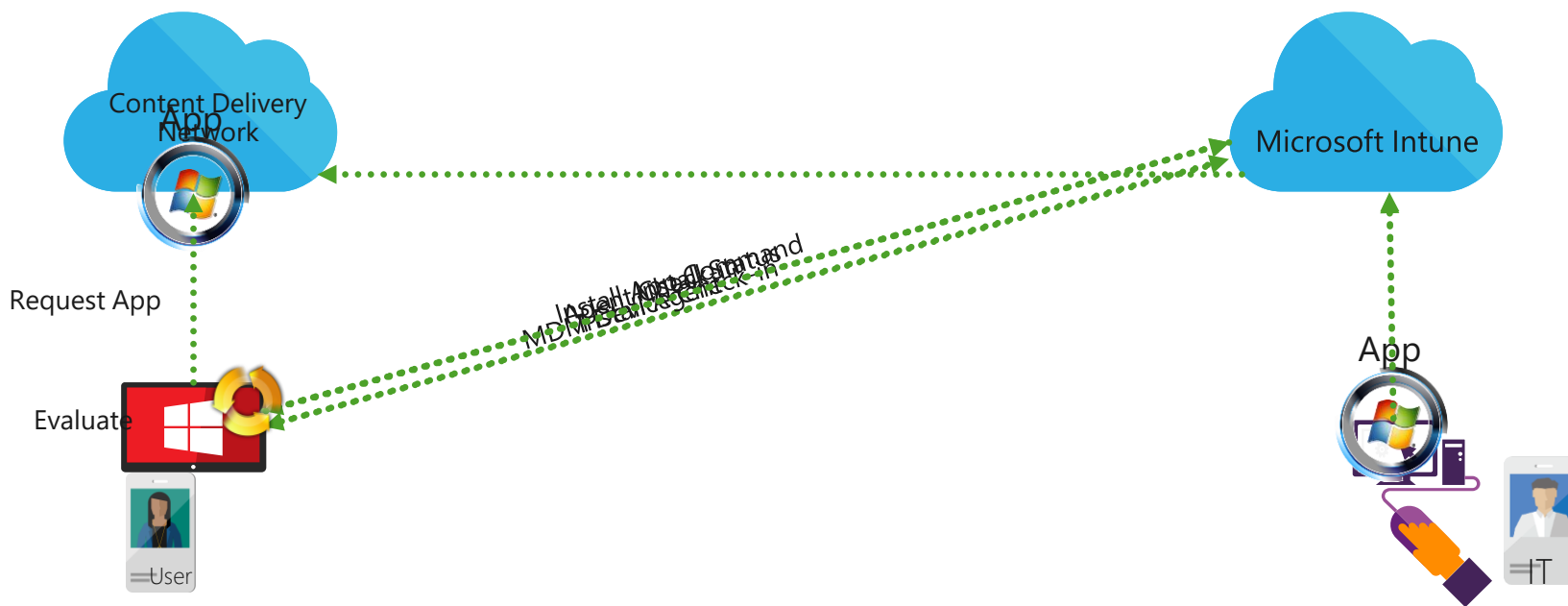
What is a Corporate Device?

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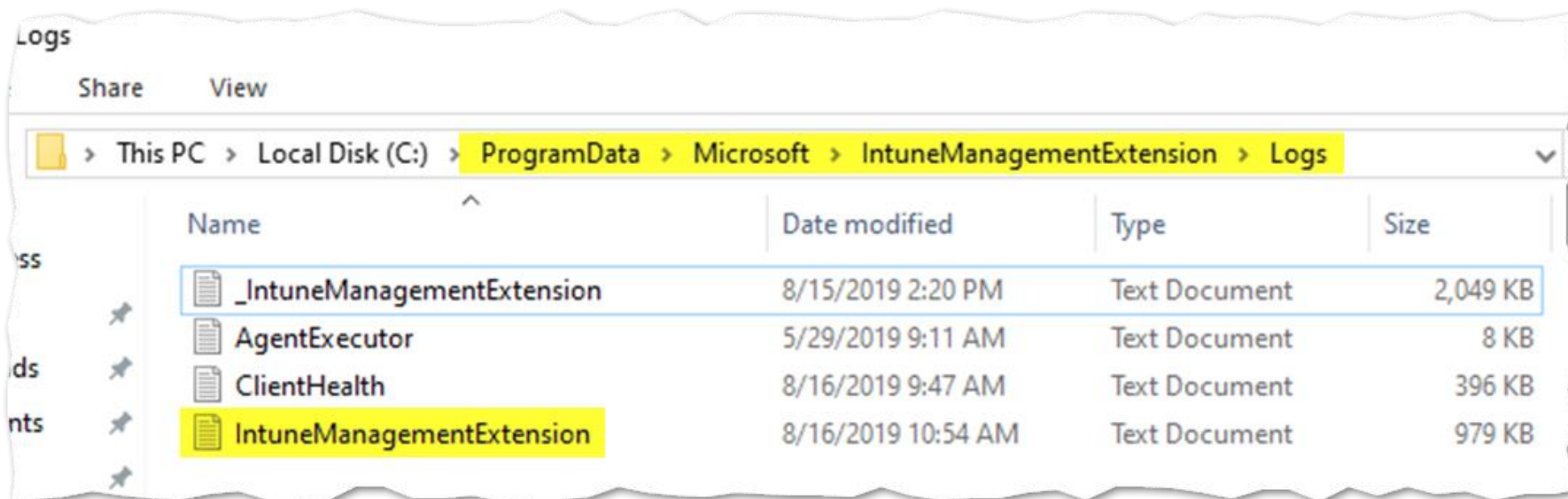
• Applications and services logs\Microsoft\Windows\DeviceManage…

Intune Management Extension Log files

- Log files:

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

Intune Management Extension The Registry

- <mark>Yellow</mark>: IME Root Registry Key

- <mark>Green</mark>: Azure AD Object ID of the User

- <mark>Red</mark>: Application / Policy GUID

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

PowerShell Scripts

PowerShell Scripts // Not applying

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

- Always consider context!
  - In "User context" mode PS executes with users permissions.
  - In "System context" has no knowledge of the user.
    - Execution will happen regardsless 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 throught 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"

Applied once - then never again?

- This is by design

- PowerShell execution manifest states:
  - Execute once and never revist 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 you way around this behaviour?
  https://www.iphase.dk/hacking-intune-management-extension/

- Workaround: Use remediation script

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…

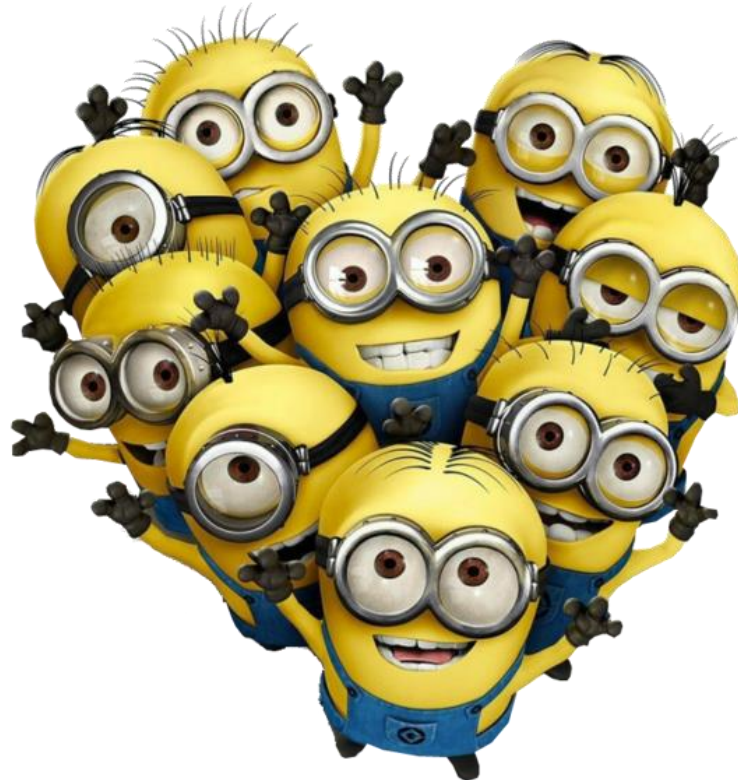# Share your ideas

http://microsoftintune.uservoice.com/

http://configurationmanager.uservoice.com/

Thank You