



Troubleshooting Windows Autopilot and Modern Deployment

RONNI PEDERSEN

MICROSOFT MVP: ENTERPRISE MOBILITY

@RONNIPEDERSEN



Ronni Pedersen

Freelance Cloud Architect



- APENTO ApS
- Microsoft MVP: Enterprise Mobility (12 years)
- MCSE/MCSA/MCITP/MCTS (+50 certifications)
- ITIL Foundation Certified
- Microsoft Certified Trainer (MCT)

Contact Me

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



About me...

Agenda

During this session we will cover how you troubleshoot:

- Troubleshooting overview
- Intune Enrollment
- Intune Profiles
- Device Compliance
- Win32 Applications
- Windows Autopilot



Troubleshooting overview

WINDOWS AUTOPILOT AND MICROSOFT INTUNE

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?
 - 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?



Intune Enrollment

Troubleshoot enrollment issues

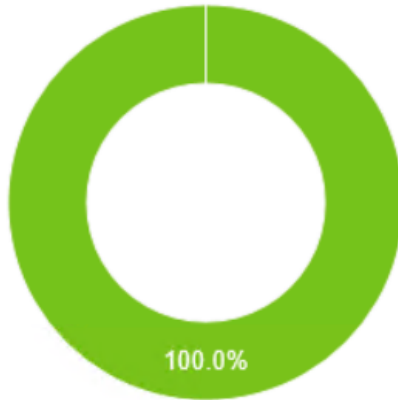
- Always check error codes if description is not right

<https://support.microsoft.com/en-us/help/4469913/troubleshooting-windows-device-enrollment-problems-in-microsoft-intune>

- Check enrollment errors in the Intune console.
 - Also if using SCCM co-management

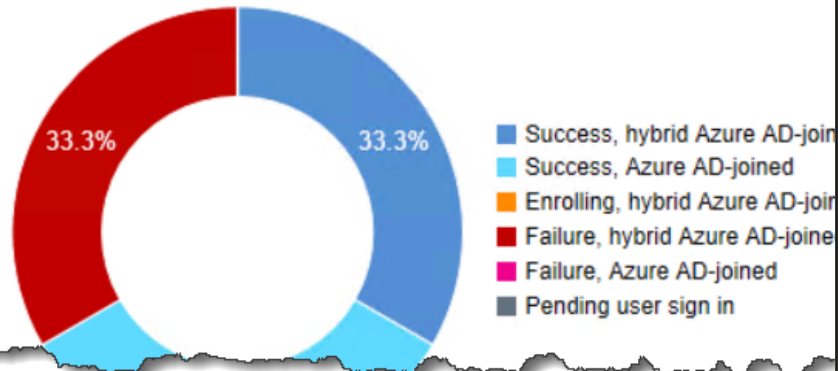


Client OS Distribution



■ Windows 10 1709 and above
 ■ Windows 10 lower than 1709
 ■ Windows 7

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

[Home](#) > [Microsoft Intune](#) > [Device enrollment - Enrollment failures](#)

Device enrollment - Enrollment failures
 Microsoft Intune

Filter Refresh Export

Quick start

Manage

- Apple enrollment
- Android enrollment
- Windows enrollment
- Terms and conditions
- Enrollment restrictions
- Device categories
- Corporate device identifiers
- Device enrollment managers

Monitor

- Enrollment failures**
- Audit logs
- Incomplete user enrollments

Help and support

- Get help and support

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

Select user
All users

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

Client Health

- How do you verify that a client are working as expected ?
- Co-management to the rescue!
- In Intune we can now see:
 - Configuration Manager agent state
 - Last Configuration Manager agent check in time
- Intune-enrolled devices connect to the cloud service three 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

Retire

Wipe

Delete

Remote lock

Sync

Reset passcode

Restart

Fresh Start

Autopilot Reset

Quick 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

TROUBLESHOOTING

Device Settings in Microsoft Intune

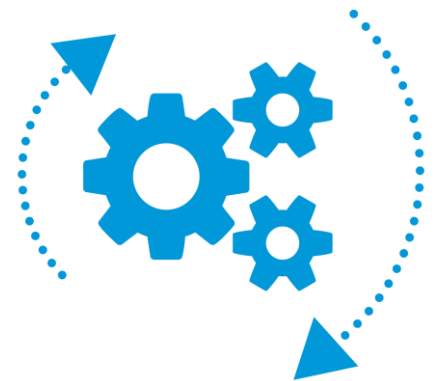
Recommended Order

- Security Baselines
- Device Configuration Profiles
- Built-In Administrative Templates
- Custom (CSP)
- Custom (ADMX)
- PowerShell Scripts



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
 - Every 3 minutes for 30 minutes
 - And then around every 8 hours
- Manuel
 - Open the Company Portal app, and sync the device to immediately check for policy or profile updates.



Intune notifications

- Sync immediately

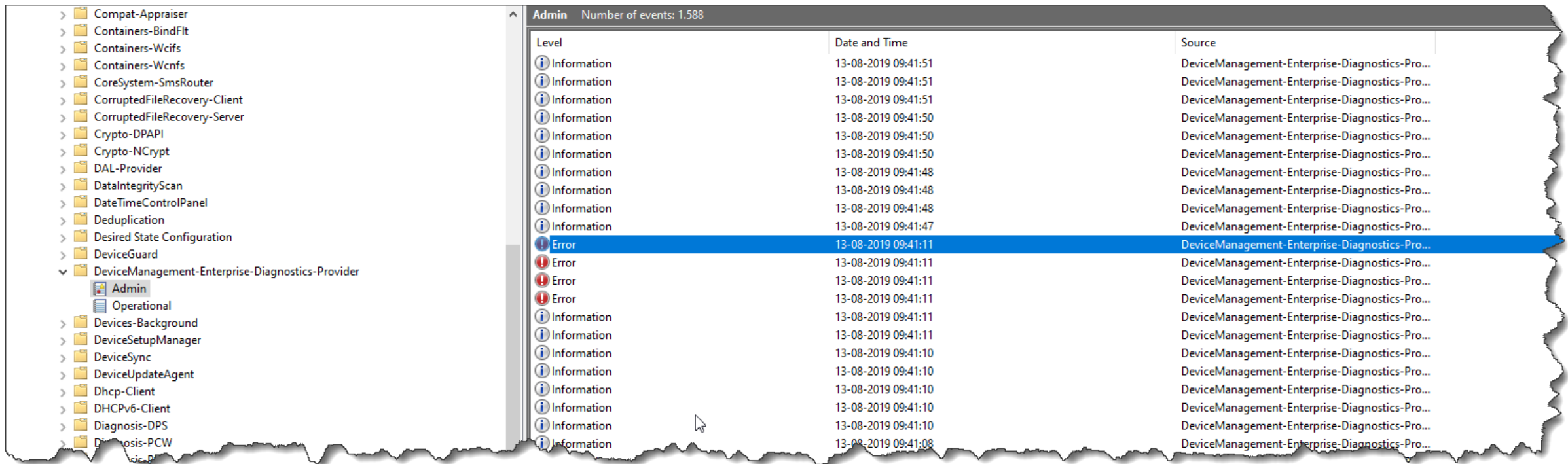
- Some actions will trigger a sync notification to the device
- When a Policy, Profile, or App is:
 - Assigned (or unassigned)
 - Updated
 - Deleted
- Current Limitation:
 - Only the first 200 devices will be updated !
 - By Design (to avoid denial of service)
 - Workaround: Use script to connect to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



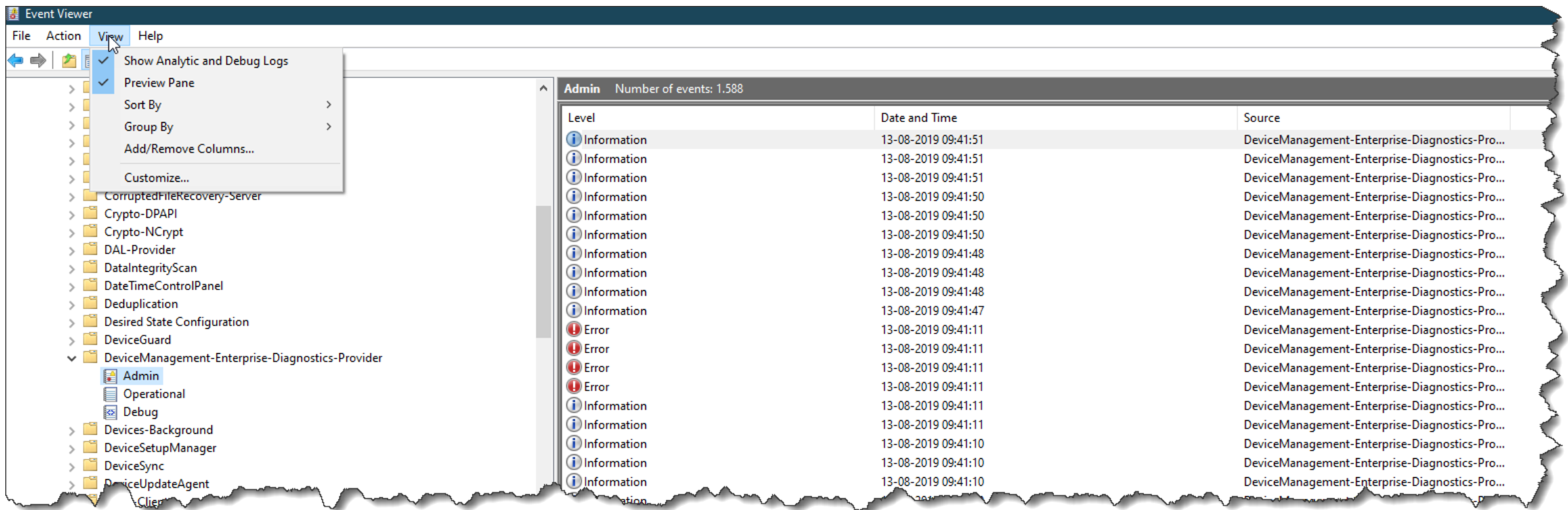
Device Profiles

- Where is my logs ?

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



Enable debug mode



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”



Security Baselines

TROUBLESHOOTING

Security Baseline: Disable settings

- Can't be done for many settings in the UI
- Only Configure or Not Configured is available

^ Windows Hello for Business

Require enhanced anti-spoofing, when available: i

Yes

Not Configured

If Yes, devices will use enhanced anti-spoofing, when available. If No, anti-spoofing will be blocked. Not configured will honor configurations done on the client.

[Learn more](#)

Configure Windows Hello for Business: i

Yes

Not Configured

Windows Hello for Business is an alternative method for signing into Windows by replacing passwords, Smart Cards, and Virtual Smart Cards. If you enable or do not configure this policy setting, the device provisions Windows Hello for Business. If you **disable** this policy setting, the device does not provision Windows Hello for Business for any user.

Require lowercase letters in PIN: i

Allowed



Require special characters in PIN: i

Allowed



Minimum PIN length: i

6



Require uppercase letters in PIN: i

Allowed



Monitor Security Baselines

Matches baseline

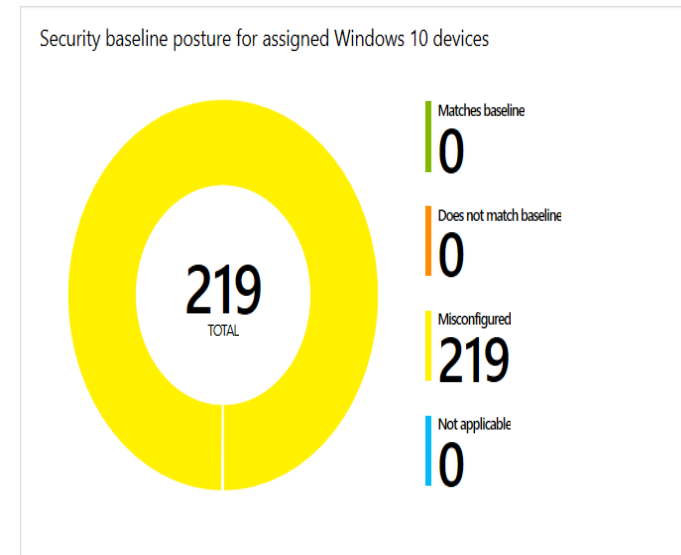
- All settings in the baseline match
- Does not match baseline
- Setting in the baseline doesn't match

Misconfigured

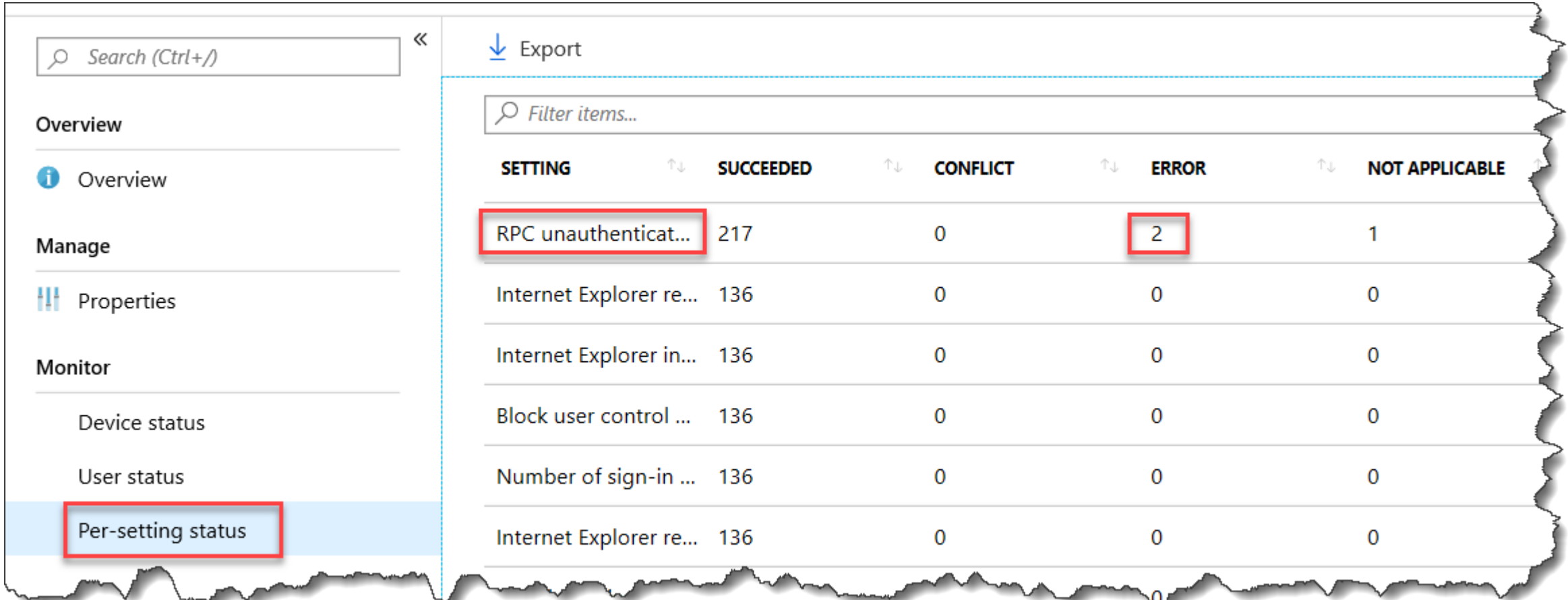
- Setting isn't properly configured. This status means the setting is in a conflict, error, or a pending state.

Not applicable

- At least one setting isn't applicable, and isn't applied.

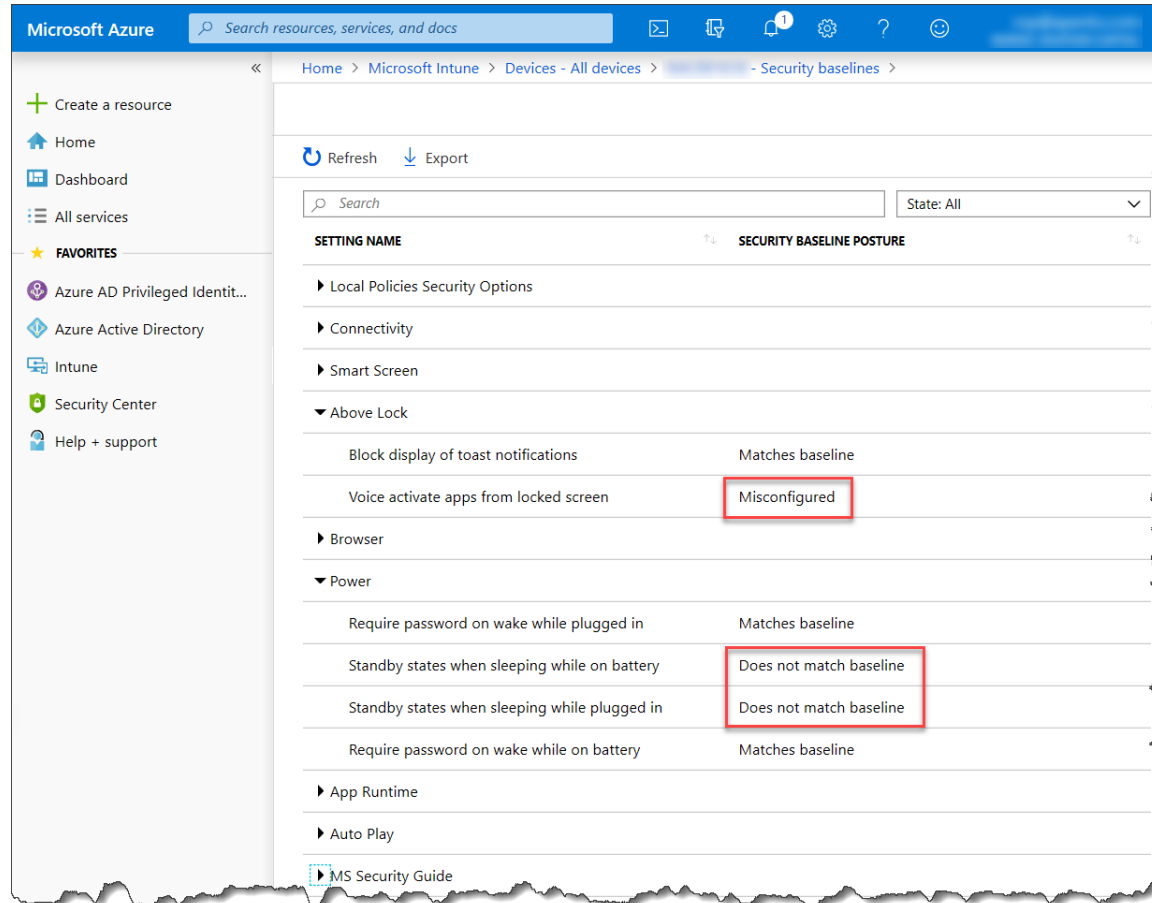


Troubleshoot Security Baselines



| SETTING | SUCCEEDED | CONFLICT | ERROR | NOT APPLICABLE |
|-------------------------|-----------|----------|-------|----------------|
| RPC unauthenticated... | 217 | 0 | 2 | 1 |
| Internet Explorer re... | 136 | 0 | 0 | 0 |
| Internet Explorer in... | 136 | 0 | 0 | 0 |
| Block user control ... | 136 | 0 | 0 | 0 |
| Number of sign-in ... | 136 | 0 | 0 | 0 |
| Internet Explorer re... | 136 | 0 | 0 | 0 |

Troubleshooting Security Baselines



Microsoft Azure Search resources, services, and docs

Home > Microsoft Intune > Devices - All devices > - Security baselines >

Refresh Export

Search State: All

| SETTING NAME | SECURITY BASELINE POSTURE |
|---|---------------------------|
| Local Policies Security Options | |
| Connectivity | |
| Smart Screen | |
| Above Lock | |
| Block display of toast notifications | Matches baseline |
| Voice activate apps from locked screen | Misconfigured |
| Browser | |
| Power | |
| Require password on wake while plugged in | Matches baseline |
| Standby states when sleeping while on battery | Does not match baseline |
| Standby states when sleeping while plugged in | Does not match baseline |
| Require password on wake while on battery | Matches baseline |
| App Runtime | |
| Auto Play | |
| MS Security Guide | |

Win32 Applications

TROUBLESHOOTING

Intune Management Extension

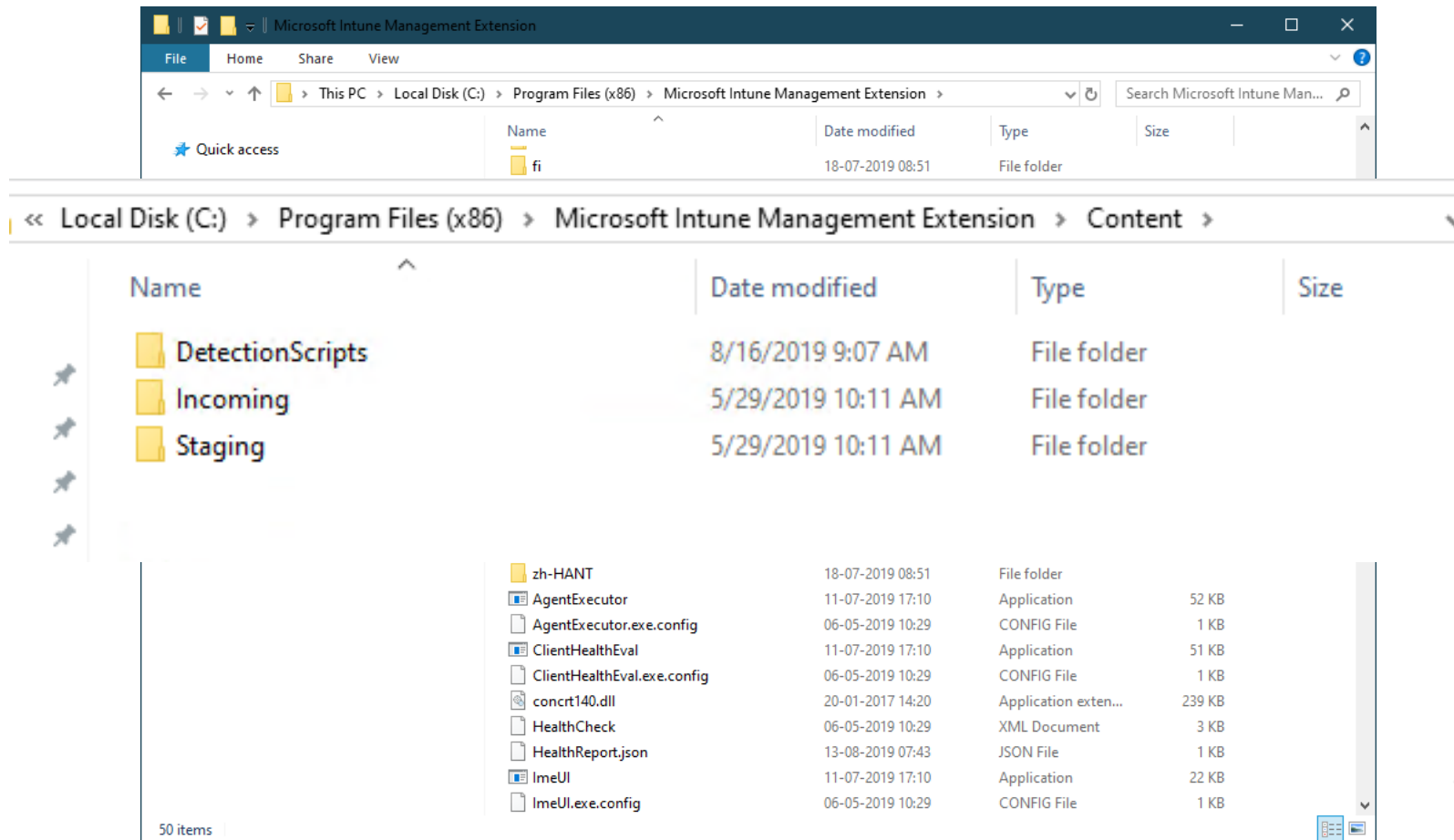
- Installed only on "Corporate owned devices"
- Not installed automatically, installed when needed first time.
- Used by:
 - PowerShell scripts
 - Win32 apps
 - Win32 app Inventory



What is a corporate device?

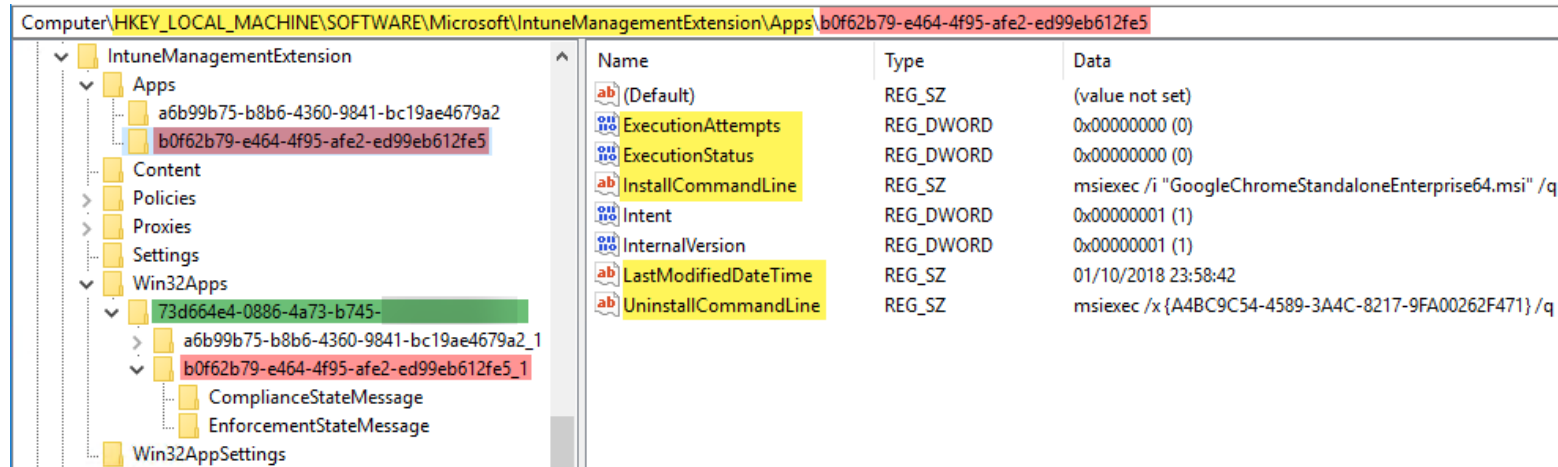
- The enrolling user is using a [device enrollment manager account](#).
- The device enrolls through [Windows Autopilot](#).
- The device is registered with Windows Autopilot but isn't an MDM enrollment only option from Windows Settings.
- The device's IMEI number is listed in Device enrollment > [Corporate device identifiers](#).
- The device enrolls through a [bulk provisioning package](#).
- The device enrolls through GPO, or [automatic enrollment from SCCM for co-management](#).

Intune Management Extension



Intune Management Extension

The Registry



| Name | Type | Data |
|----------------------|-----------|--|
| (Default) | REG_SZ | (value not set) |
| ExecutionAttempts | REG_DWORD | 0x00000000 (0) |
| ExecutionStatus | REG_DWORD | 0x00000000 (0) |
| InstallCommandLine | REG_SZ | msiexec /i "GoogleChromeStandaloneEnterprise64.msi" /q |
| Intent | REG_DWORD | 0x00000001 (1) |
| InternalVersion | REG_DWORD | 0x00000001 (1) |
| LastModifiedDateTime | REG_SZ | 01/10/2018 23:58:42 |
| UninstallCommandLine | REG_SZ | msiexec /x {A4BC9C54-4589-3A4C-8217-9FA00262F471} /q |

- Yellow: Execution commands for install and uninstall
- Green: Azure AD user object ID
- Red: Application GUID
 - Can be easily traced by looking at the graph data with the Graph Explorer from Microsoft: <https://developer.microsoft.com/en-us/graph/graph-explorer>

Troubleshooting

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

Logs

Share View

This PC > Local Disk (C:) > ProgramData > Microsoft > IntuneManagementExtension > Logs

| 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 |



APENTO-0001 - Managed Apps

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Recovery keys

Managed Apps

Refresh

| Application | Resolved intent |
|------------------------------|------------------|
| Microsoft Edge Beta | Available |
| Office 365 ProPlus - da-DK | Available |
| Microsoft Authenticator | Required install |
| Microsoft To Do | Available |
| Microsoft Kaizala | Available |
| Corporate Phonebook | Available |
| Microsoft Planner | Available |
| Spotify | Available |
| Dansk lokal grænsefladepakke | Available |
| Trello | Available |
| GitHub Desktop | Available |
| Putty | Available |
| OneNote | Available |

Microsoft Edge Beta - Installation details

Refresh

Collect logs

Download logs



App installation failed

10/24/2019 9:13:38 AM

[Hide details](#)

Error code: 0x87D30067
Error unzipping downloaded content.



User requested application

10/24/2019 9:13:19 AM



Device last check-in time

10/24/2019 9:12:08 AM



Agent installed

10/23/2019 2:13:38 AM



Application created

9/19/2019 3:45:41 PM

Read log files = CMTrace

- Use your favorite log reader!
- License for SCCM is included in Intune = CMTrace can be used
- Deploy it using Intune Win32 App
- <https://ccmexec.com/2018/12/copy-and-associate-cmtrace-using-intune-win32app-and-powershell/>

Still have problems?

- 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.**

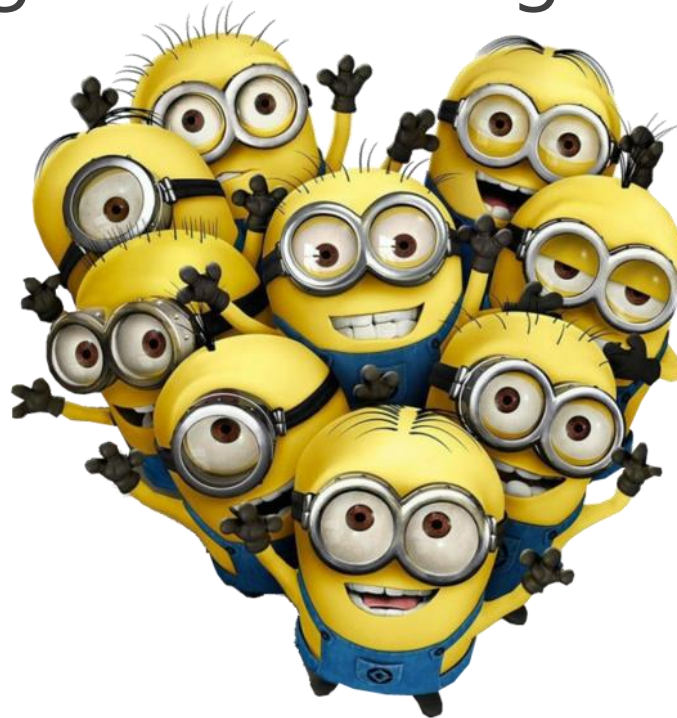
That's all I can think of right at this moment, but I'm sure there are more...



Share your ideas

<http://microsoftintune.uservoice.com/>

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



Questions



Thank you!

