Troubleshooting the modern managed client

Ronni Pedersen
Microsoft MVP
@RonniPedersen

Jörgen Nilsson
Microsoft MVP
@ccmexec

BitHawk

Configuration Manager Community Event CMCE

Agenda

During this session we will cover how you troubleshoot:

- Intune Enrollment (Standalone and Hybrid)
- Intune Profiles
- Device Compliance
- Application Deployment (incl. PowerShell Scripts)
- Windows Autopilot

Intune Enrollment

Scenarios

- Existing PC
- New PC – AAD Join (auto enrollment)
- Existing PC – Hybrid joined
- NEW PC – Hybrid

Userless 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?
- 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 description is not right

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

Hybrid Azure AD Join

- Group Policy (No Offset)
- Co-Management (Offset)
  - Schedules enrollment with an offset
  - If the enrollment fails, **SCCM** will retry 2 times every 15 mins
  - Most common issue, the users is not in AAD

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/

Options

- Hybrid SCCM-Co-managed

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 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 eight hours.

Intune Profiles

Troubleshooting

Device Profiles in Microsoft Intune

Recommended Order

1. Security Baselines
2. Device Configuration Profiles
3. Built-In Administrative Templates
4. Custom (CSP)
5. Custom (ADMX)

Policy and Profile refresh cycles

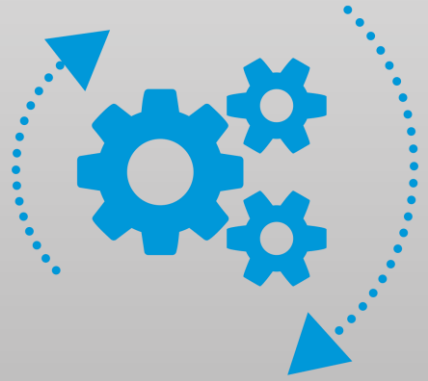
Existing Devices

- 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

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

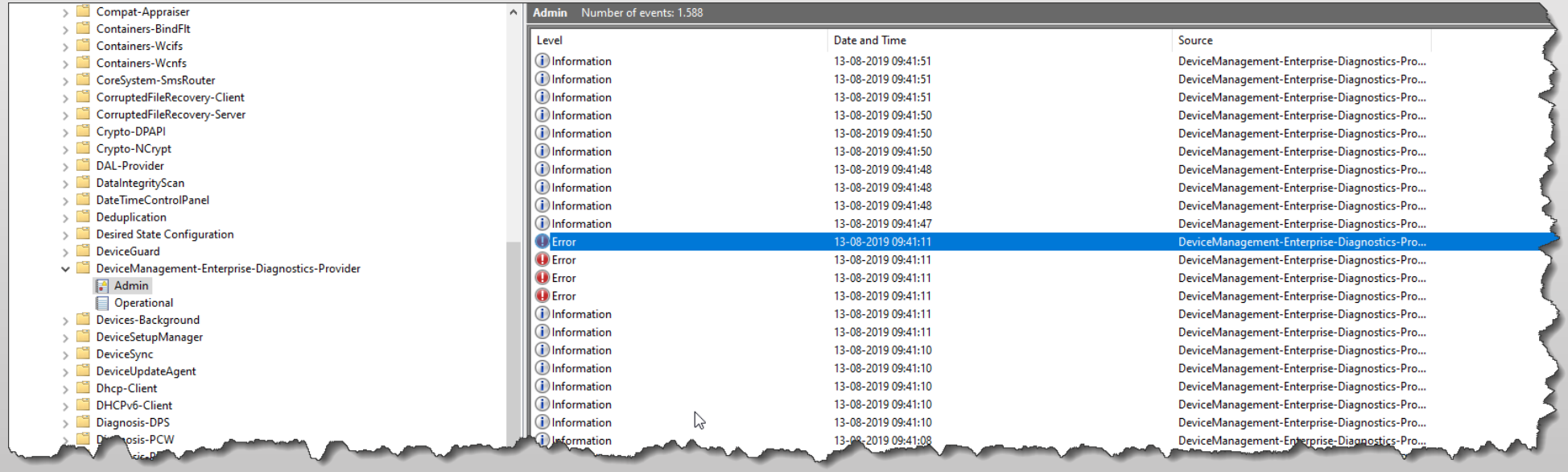
Current Limitation:

- 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

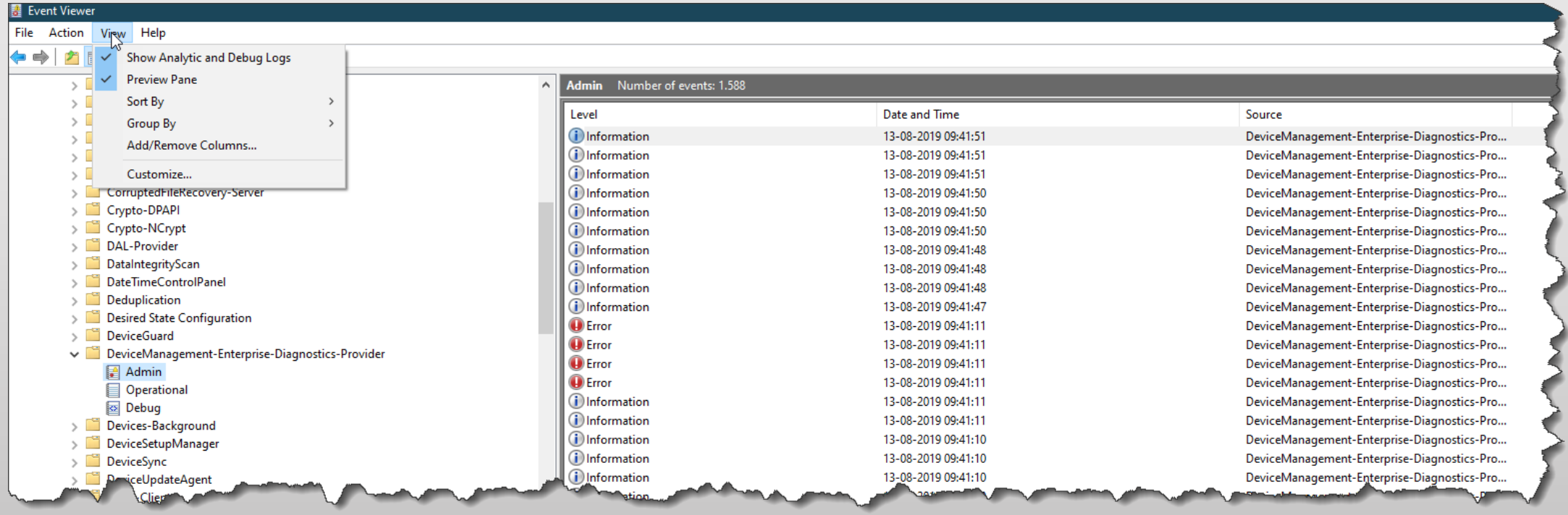
Device Profiles
- Where is my logs ?

Event viewer is your new best friend

- Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider



Enable debug mode



mdmdiagnosticstool.exe

Collect files for troubleshooting:

mdmdiagnosticstool.exe -area Autopilot -cab c:\autopilot.cab

```
Command Prompt
Microsoft Windows [Version 10.0.18362.295]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\RonniPedersen>mdmdiagnosticstool.exe -area Autopilot -cab c:\demo\autopilot.cab
Collecting licensing information.  This may take up to one minute...
Collecting hardware hash information.

Succeeded to CollectLog at: c:\demo\autopilot.cab

C:\Users\RonniPedersen>_
```

Policy Conflicts

- Compliance policy settings always have precedence over configuration profile settings.
- Compliance policy conflicts: The **most restrictive** compliance policy setting applies.
- Conflicts with conflict is shown in Intune. Manually resolve these conflicts.
  - By default the first created policy will “win”

Deleting Profiles or no longer applicable

Delete a profile or remove a device from a group:

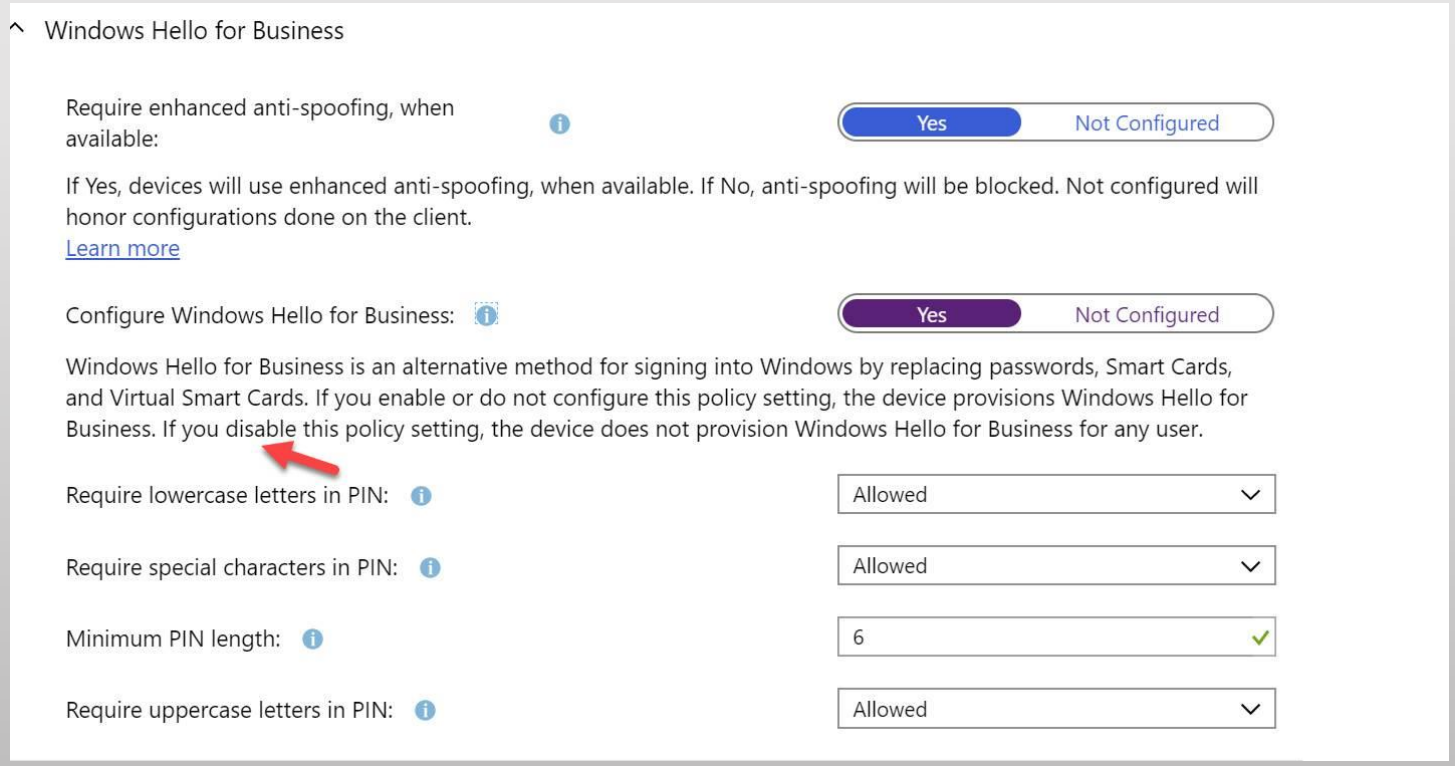
- **Windows** and **Android** devices: Settings aren't removed from the device

- More info:
  - https://docs.microsoft.com/en-us/intune/device-profile-troubleshoot#what-happens-when-a-profile-is-deleted-or-no-longer-applicable

Security Baseline: Disable settings

Can’t be done for most settings in the UI

- Only Configure or Not Configured is available



Monitor Security Baselines

Matches baseline

- All settings in the baseline match

Does not match baseline

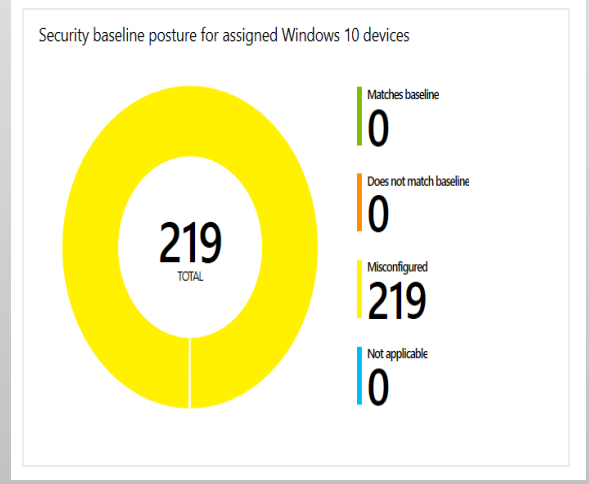
- Setting in the baseline doesn't match

Misconfigured

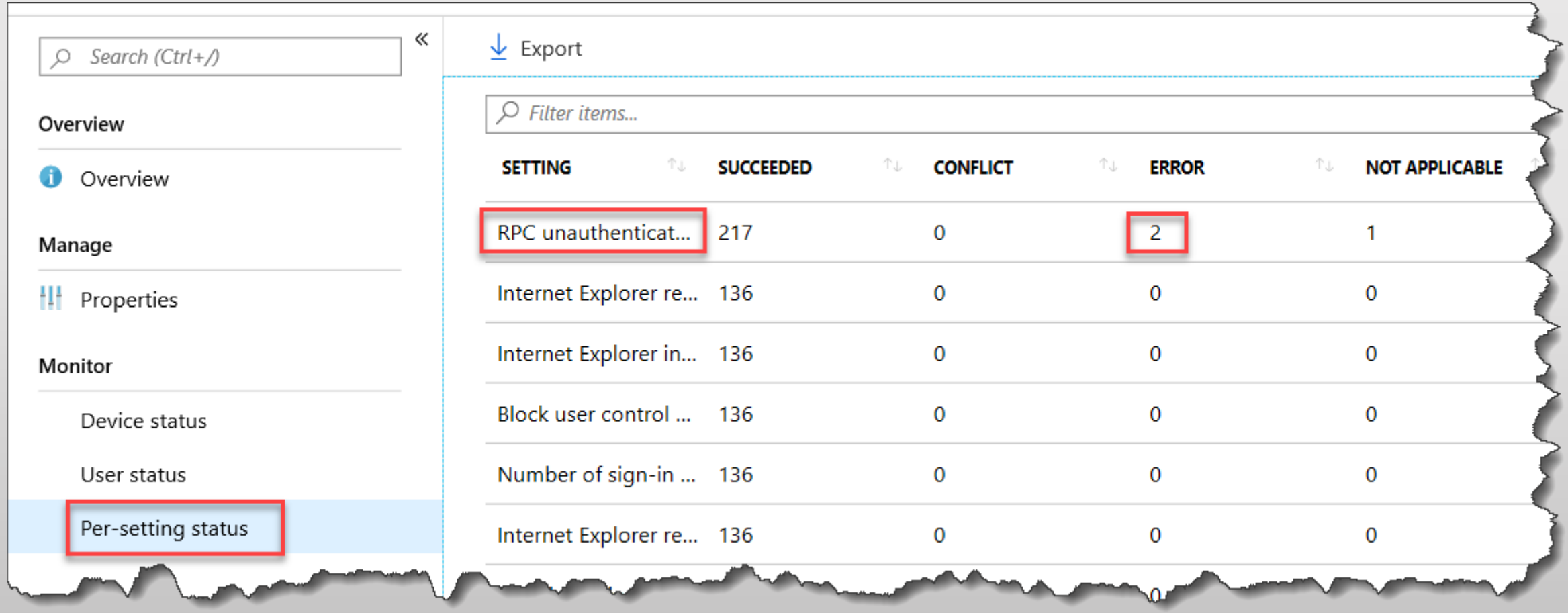
- Setting isn't properly configured. This status means the setting is in a conflict, error, or a pending state.

Not applicable

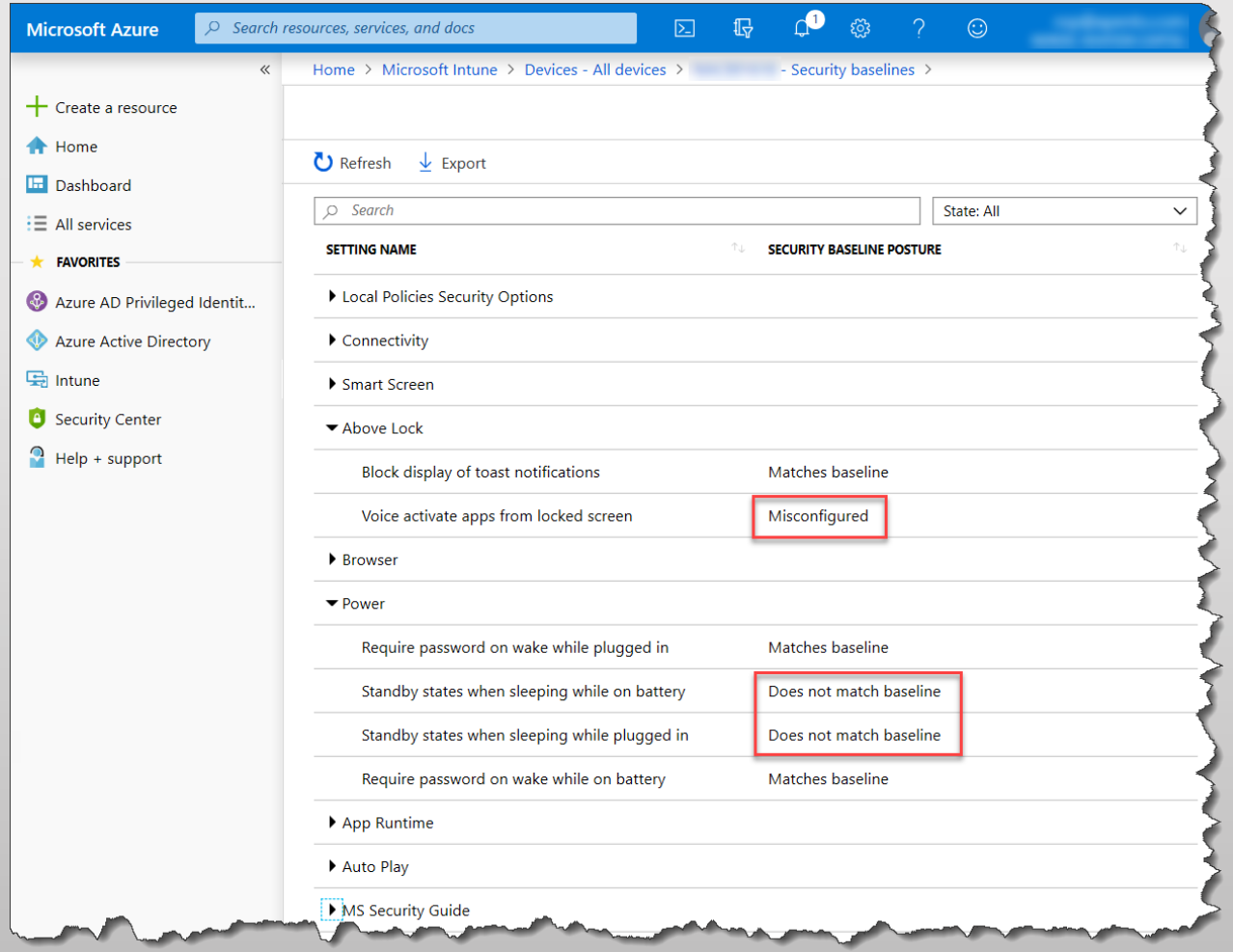
- At least one setting isn't applicable, and isn't applied.



Troubleshoot using per-setting



Troubbleshooting Security Baselines



Application Deployment

Intune Management Extension

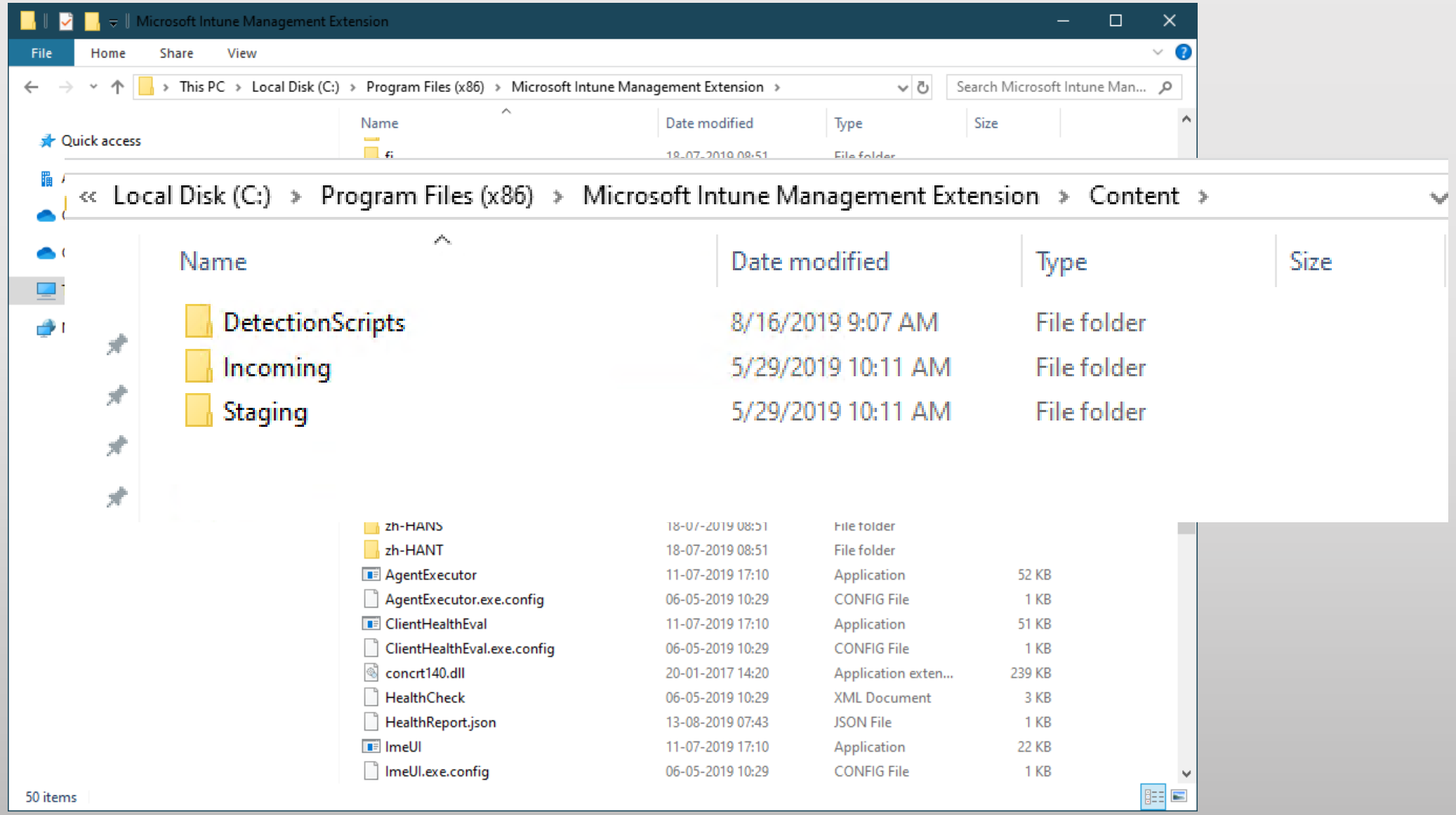
- Installed only on "Corporate owned devices"
- Not installed automatically, installed when needed first time.

- Used by:
  - PowerShell scripts
  - Win32 apps
  - Win32 app Inventory

What is a corporate device

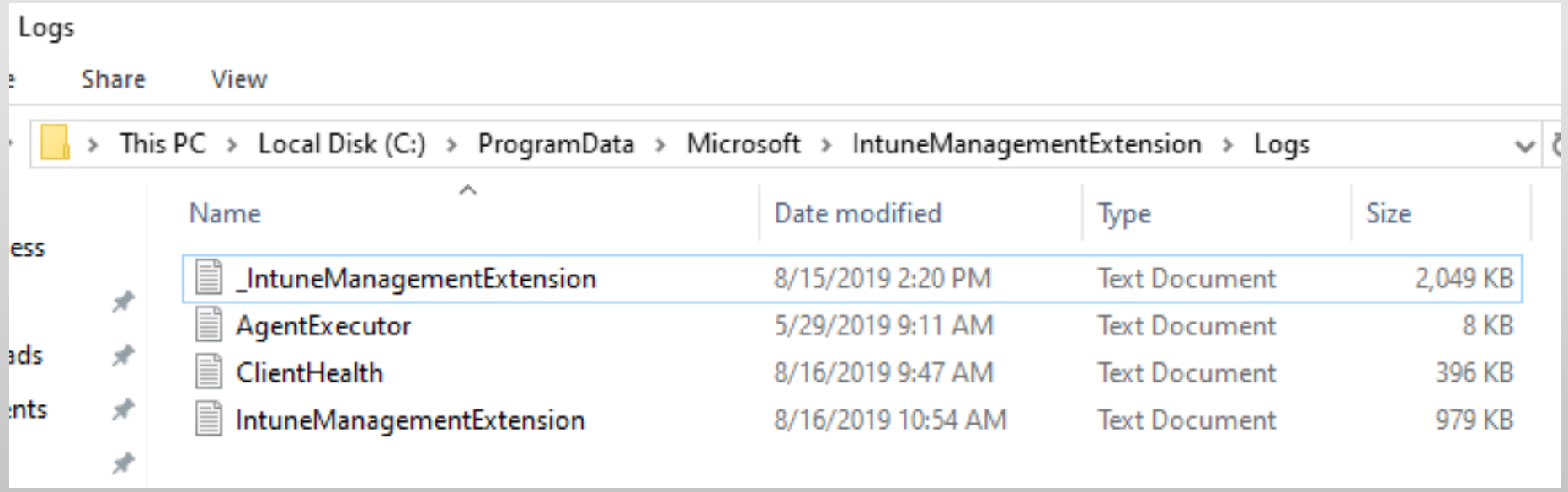
- The enrolling user is using a device enrollment manager account.
- The device enrolls through Windows Autopilot.
- The device is registered with Windows Autopilot but isn't an MDM enrollment only option from Windows Settings.
- The device's IMEI number is listed in Device enrollment > Corporate device 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



Troubleshooting

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



Read log files = CMTrace

Use our favorite log reader!

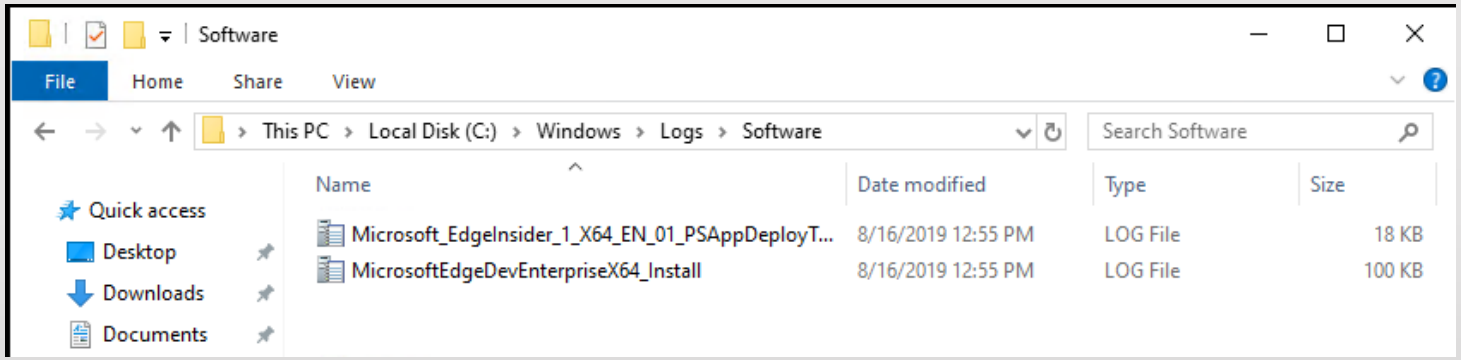
License for SCCM is included in Intune = CMTrace can be used

Deploy it using Intune Win32 App

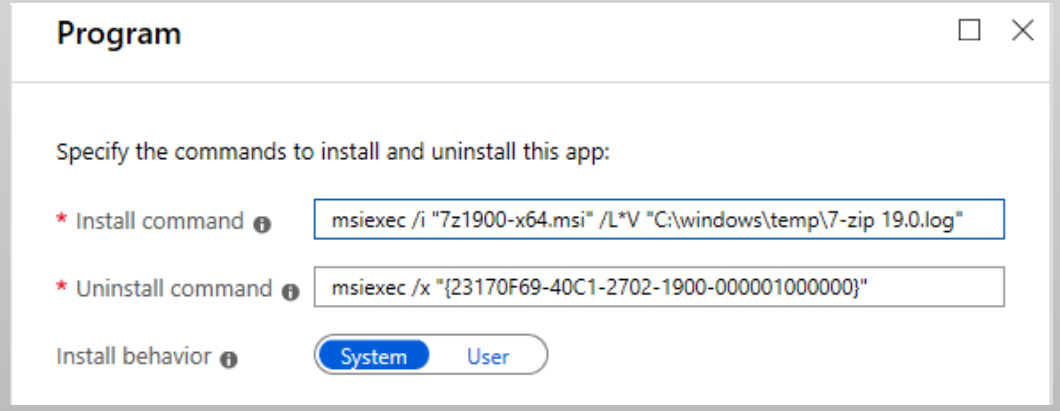
https://ccmexec.com/2018/12/copy-and-associate-cmtrace-using-intune-win32app-and-powershell/

Use the tools you know

- PsAppDeploymentToolkit – get logging for example



- Use /L*V for MSiexec command lines so we have log files



Windows Autopilot

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.

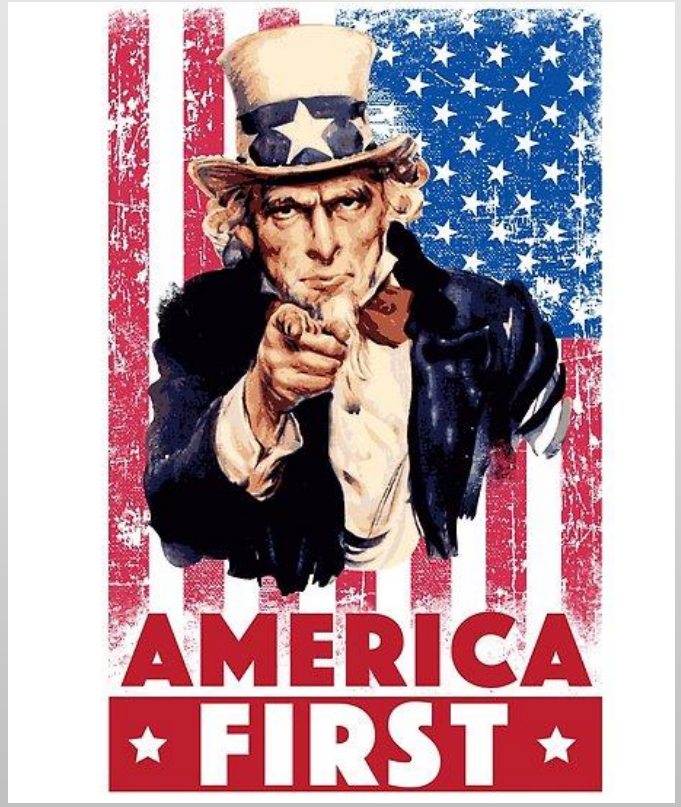
That's all I can think of right at this moment, but I'm sure there are more...

Install the latest update!

- Make sure you've installed a recent cumulative update
- Using the original unpatched Windows 10 1903 media might fail

Use English OS for your POC

- Windows Autopilot white glove does not work for non-English OSes.
- If you've seen a red screen from Windows Autopilot that says "Success" and you were using a non-English OS, you now know why.

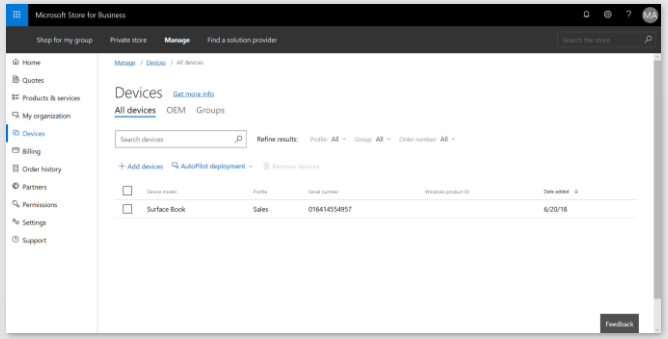


Hybrid Join: Administrator Rights

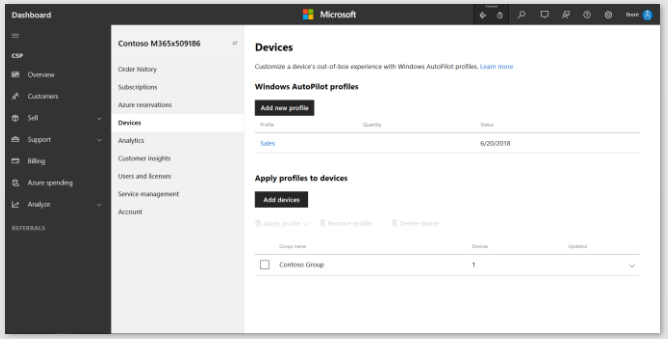
Error: User is not granted administrator rights after Windows Autopilot user-driven Hybrid Azure AD join scenario.

Another non-English issue

Administering Windows Autopilot

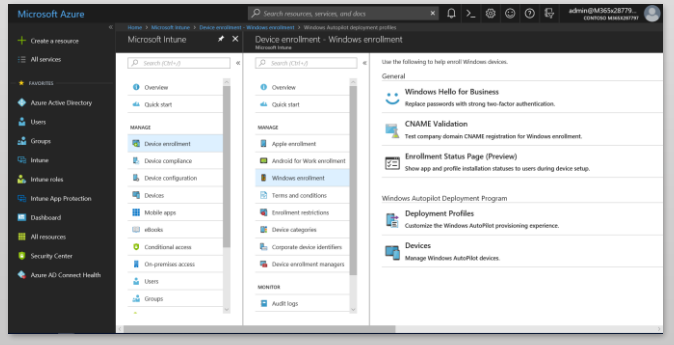


Microsoft Store for Business

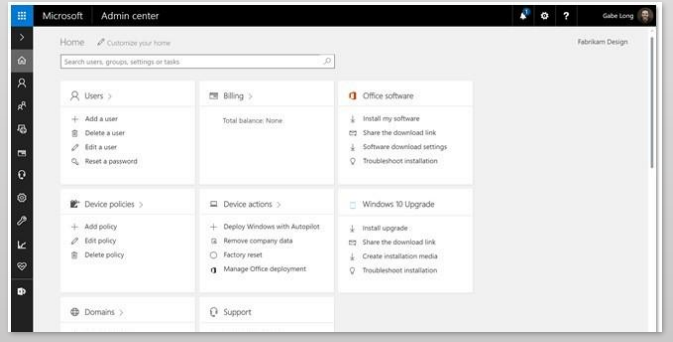


Partner Center

The only portal enterprises should use

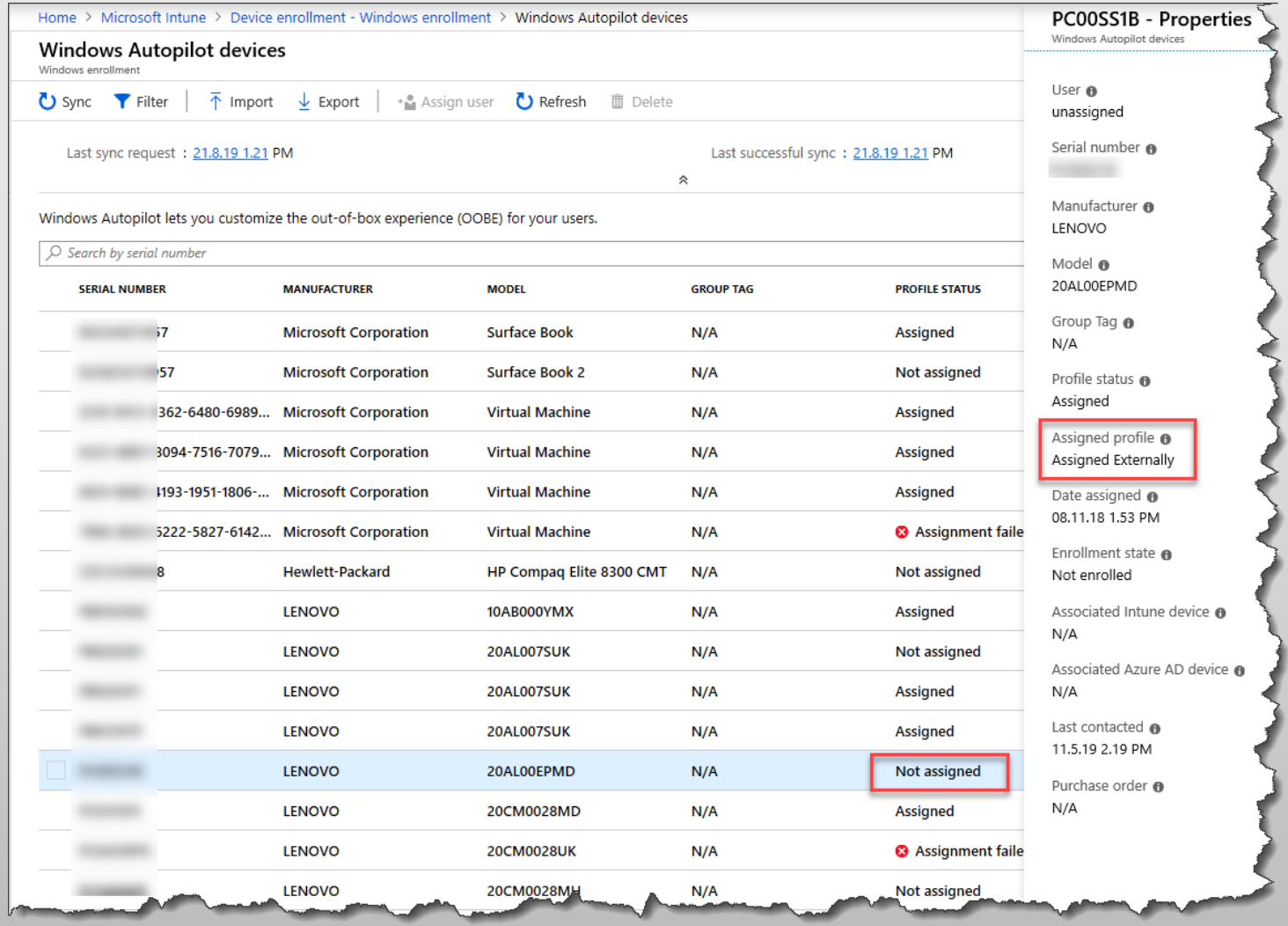


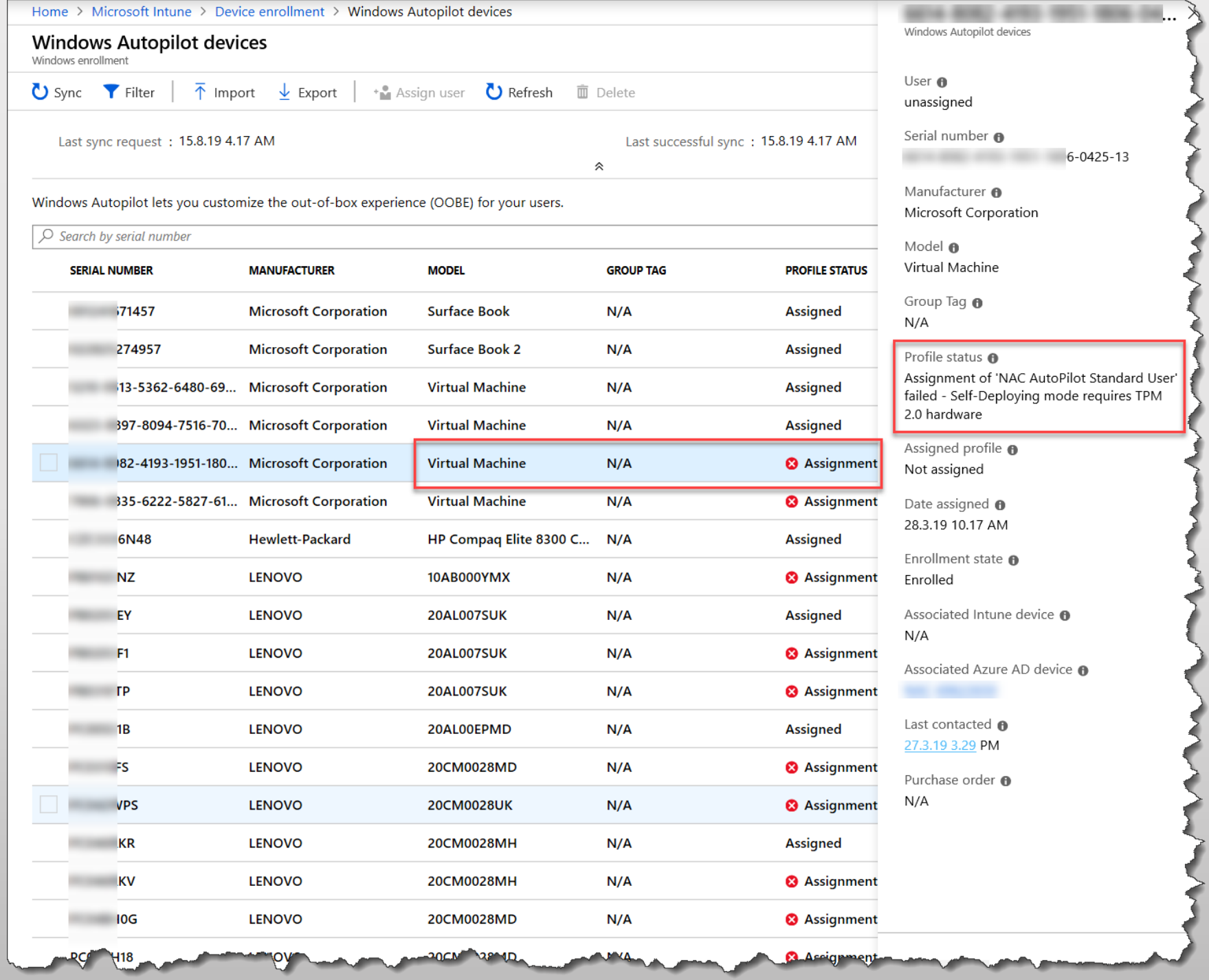
Microsoft Intune



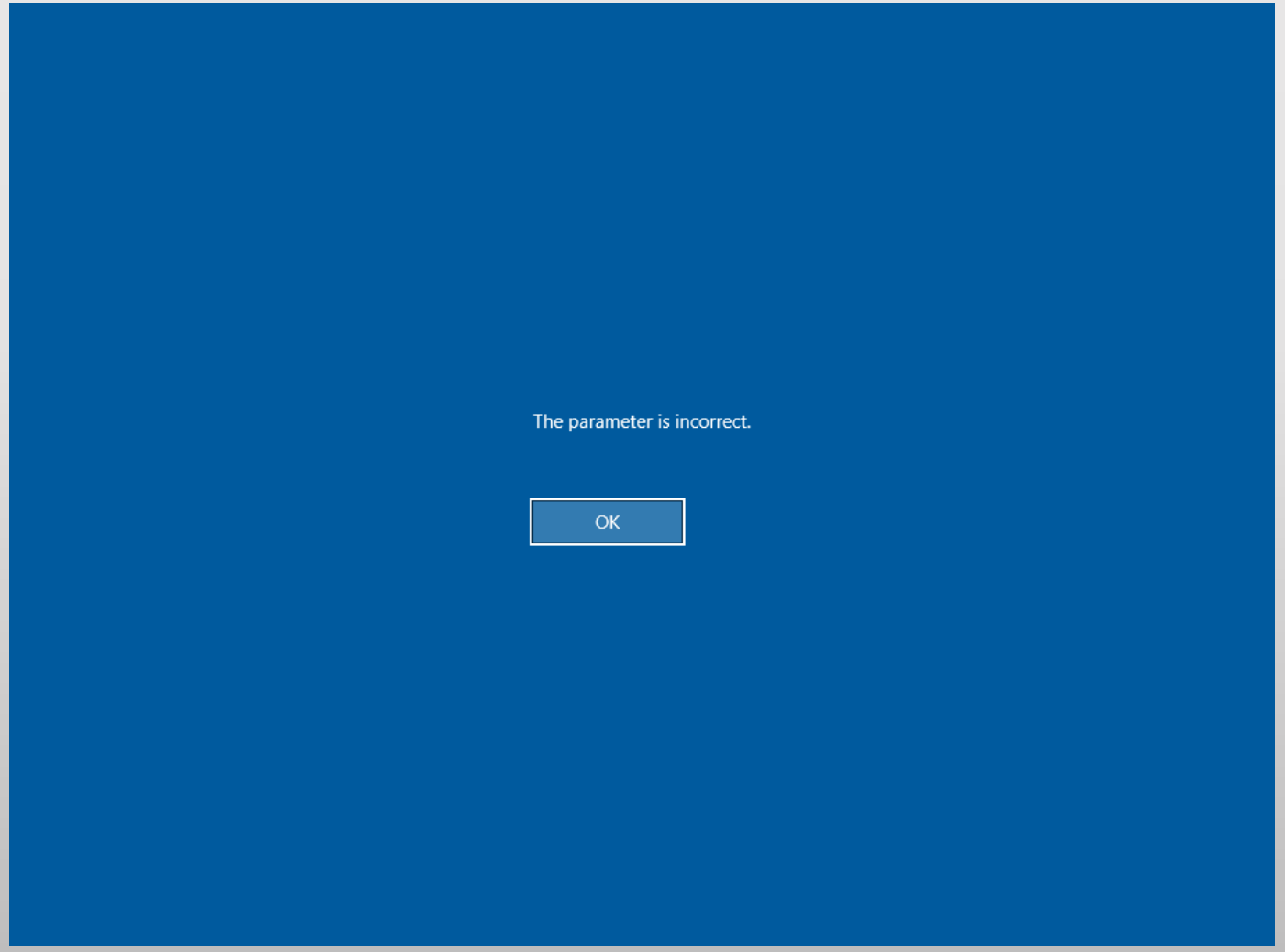
Microsoft 365 Business

Assigned Profile: Assigned Externally




Home > Microsoft Intune > Device enrollment > Windows Autopilot devices
Windows Autopilot devices
Windows enrollment
Sync
Filter
Import
Export
Assign user
Refresh
Delete
Last sync request : 15.8.19 4.17 AM
Last successful sync : 15.8.19 4.17 AM
Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.
Search by serial number
SERIAL NUMBER
MANUFACTURER
MODEL
GROUP TAG
PROFILE STATUS
71457 Microsoft Corporation Surface Book N/A Assigned
274957 Microsoft Corporation Surface Book 2 N/A Assigned
13-5362-6480-69... Microsoft Corporation Virtual Machine N/A Assigned
397-8094-7516-70... Microsoft Corporation Virtual Machine N/A Assigned
82-4193-1951-180... Microsoft Corporation Virtual Machine N/A Assignment
335-6222-5827-61... Microsoft Corporation Virtual Machine N/A Assignment
6N48 Hewlett-Packard HP Compaq Elite 8300 C... N/A Assigned
NZ LENOVO 10AB000YMX N/A Assignment
EY LENOVO 20AL007SUK N/A Assigned
F1 LENOVO 20AL007SUK N/A Assignment
TP LENOVO 20AL007SUK N/A Assignment
1B LENOVO 20AL00EPMD N/A Assigned
FS LENOVO 20CM0028MD N/A Assignment
VPS LENOVO 20CM0028UK N/A Assignment
KR LENOVO 20CM0028MH N/A Assigned
KV LENOVO 20CM0028MH N/A Assignment
I0G LENOVO 20CM0028MD N/A Assignment
H18
Windows Autopilot devices
User
unassigned
Serial number
6-0425-13
Manufacturer
Microsoft Corporation
Model
Virtual Machine
Group Tag
N/A
Profile status
Assignment of 'NAC AutoPilot Standard User' failed - Self-Deploying mode requires TPM 2.0 hardware
Assigned profile
Not assigned
Date assigned
28.3.19 10.17 AM
Enrollment state
Enrolled
Associated Intune device
N/A
Associated Azure AD device
Last contacted
27.3.19 3.29 PM
Purchase order
N/A

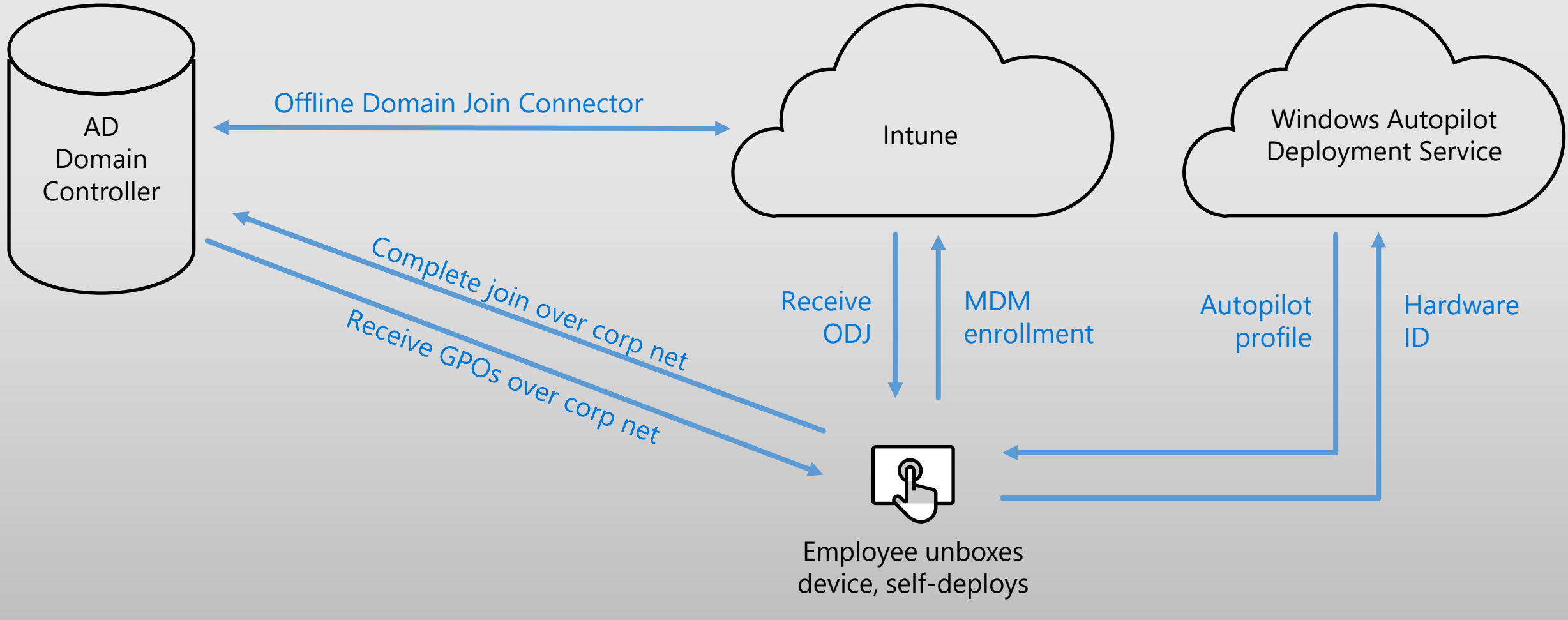
Windows 10 1809 Pro
“The parameter is incorrect”



Lesson learned

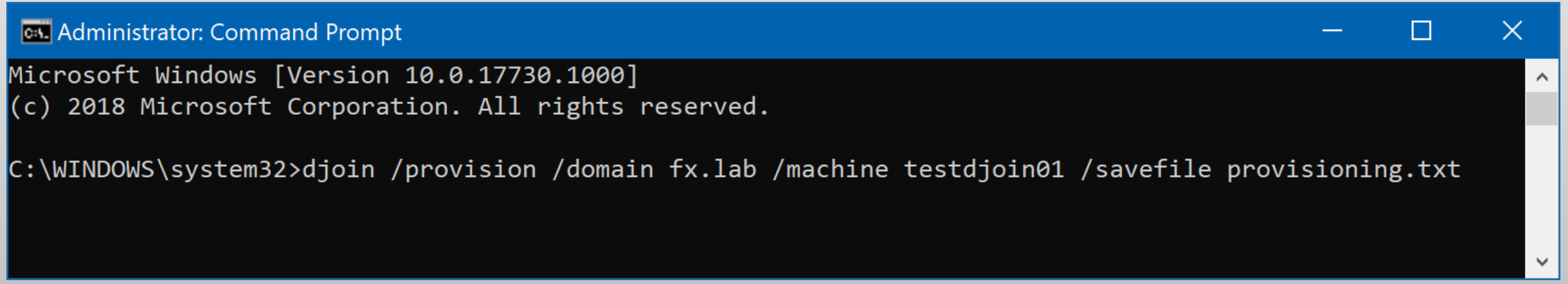
- “ChangeProductKey“ for Windows 10 1809 Pro requires a reboot
  - (Pro OEM to Pro MAK)
  - This causes issues with the credentials during the ESP and gives the parameter is incorrect error
- Fix:
  - Continue on with the error
  - Use subscription based license
  - Use Windows 10 1903

Hybrid Azure AD Join through Windows Autopilot



Let’s talk about ODJ blobs

- Stands for an **O**ffline **D**omain **J**oin blob
- At the center of the Hybrid Autopilot flow
- You can generate your own blob from any domain joined machine if you have rights to join

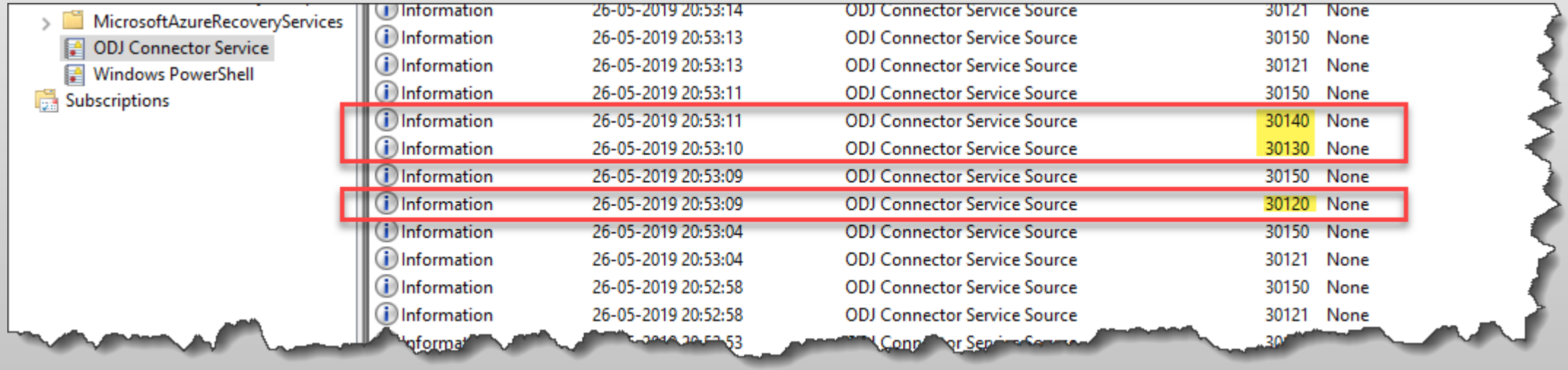


Event Log ODJ Connector Service

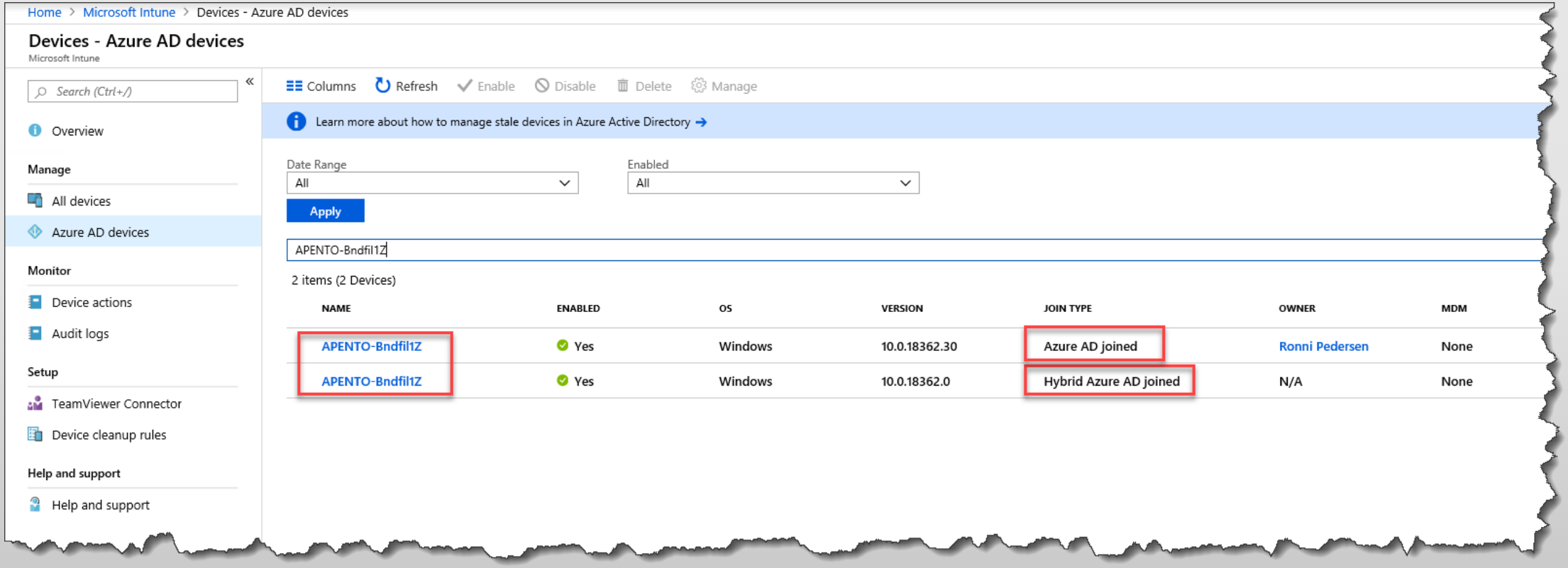
30120 = Offline Domain Join Blob download success (policy)

30130 = Offline Domain Join Blob request success

30140 = Offline Domain Join Blob upload success



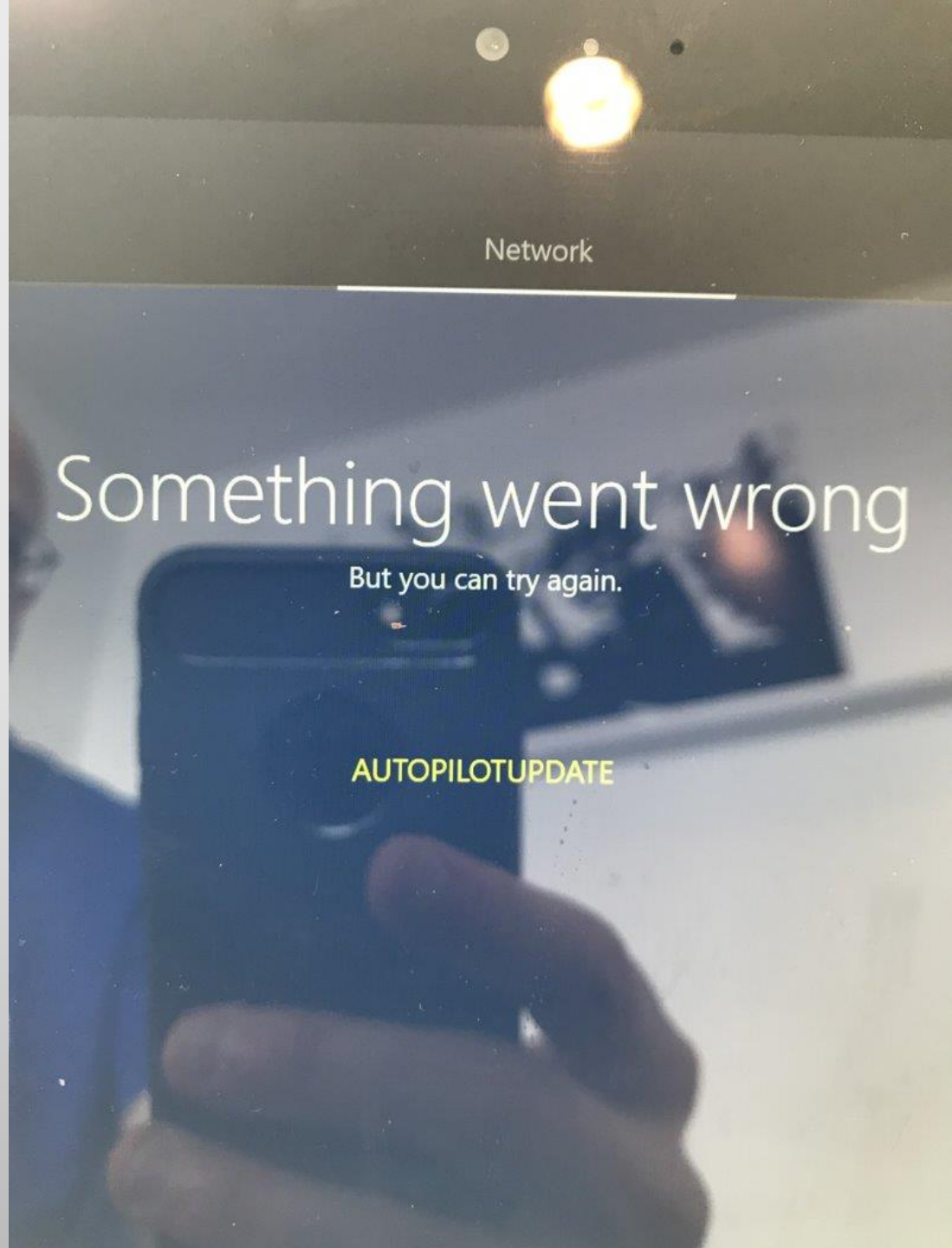
Duplicate Records



Firewall rules!

If only opening the ports needed always check the Docs article, they change!

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-requirements



Windows Autopilot Configuration

Organization:	apento.com
Deployment profile:	APENTO White Glove
Assigned user:	Not assigned
Elapsed time:	1677 h 43 min

Provisioning information could not be located. Contact the customer IT admin to troubleshoot.

View diagnostics

Retry

Reset

Setting up your device for work

This could take a while and your device may need to reboot.

Device preparation Show details
Complete

Device setup
Complete

Account setup Hide details
Failed

Joining your organization's network (Complete)
Security policies (1 of 1 applied)
Certificates (No setup needed)
Network connections (4 of 4 added)
Apps (Failed)

Please contact IT for help with this issue. +45 [redacted] or itsupport@[redacted]

Continue anyway

Reset Device

Try again

Share your ideas

- Share your voice / ideas!
  - http://microsoftintune.uservoice.com/
  - http://configurationmanager.uservoice.com/

Questions?

Thank You

Danke

Herzlichen Dank

Jörgen Nilsson, @ccmexec, https://www.ccmexec.com

Ronni Pedersen, @RonniPedersen, https://www.ronnipedersen.com

Bewertung der Session: Configmgr.ch / azureems.ch

Xing: https://www.xing.com/net/cmce

Facebook: https://www.facebook.com/groups/411231535670608/

Linkedin: http://www.linkedin.com

Twitter: https://twitter.com/configmgr_ch

baseVISION

BitHawk

RealStuff Informatik AG

digicomp

Digital Competence. Made of People.