#NVSummit2021

Troubleshooting the modern managed client

- Jörgen Nilsson
- Principal Consultant, Onevinn
- Twitter @ccmexec
- MVP / MCT

- Ronni Pedersen
- Cloud Architect, APENTO
- Twitter @ronnipedersen
- MVP / MCT

NORDIC — VIRTUAL SUMMIT —

NORDIC
– VIRTUAL SUMMIT –

Ronni Pedersen

- Cloud Architect, APENTO
- Microsoft MVP: Enterprise Mobility
- MCSE/MCSA/MCITP/MCTS
- ITIL Foundation Certified
- Microsoft Certified Trainer (MCT)

Contact Info

- Mail: rop@apento.com
- Twitter: @ronnipedersen

APENTO

Jörgen Nilsson

- Principal Consultant
- Microsoft MVP: Enterprise Mobility
- MCSE/MCSA/MCITP/MCTS
- ITIL Foundation Certified
- Microsoft Certified Trainer (MCT)

Contact Info

- Mail: Jorgen.nilsson@onevinn.se
- Twitter: @ccmexec

Takeaways

- Tools
- The Log Files
- Configuration Policy Process
- Subscription Based activation
- Troubleshooting Enrollment
- Troubleshooting Policies
- Intune Management Extension

Remote Control

NORDIC
– VIRTUAL SUMMIT –

- TeamViewer integrates in the Endpoint Management Portal
- Quick Assist is built-in
  - Lacks UAC support
  - No Logging
  - Maybe OK for smaller organizations
  - Can be used during AutoPilot

https://oliverkieselbach.com/2020/03/03/quick-assist-the-built-in-remote-control-in-windows-10/

Let's set things up for your work or school

You'll use this info to sign in to your devices.

CCMEXEC

Sign in

e-mail

Can't access your account?

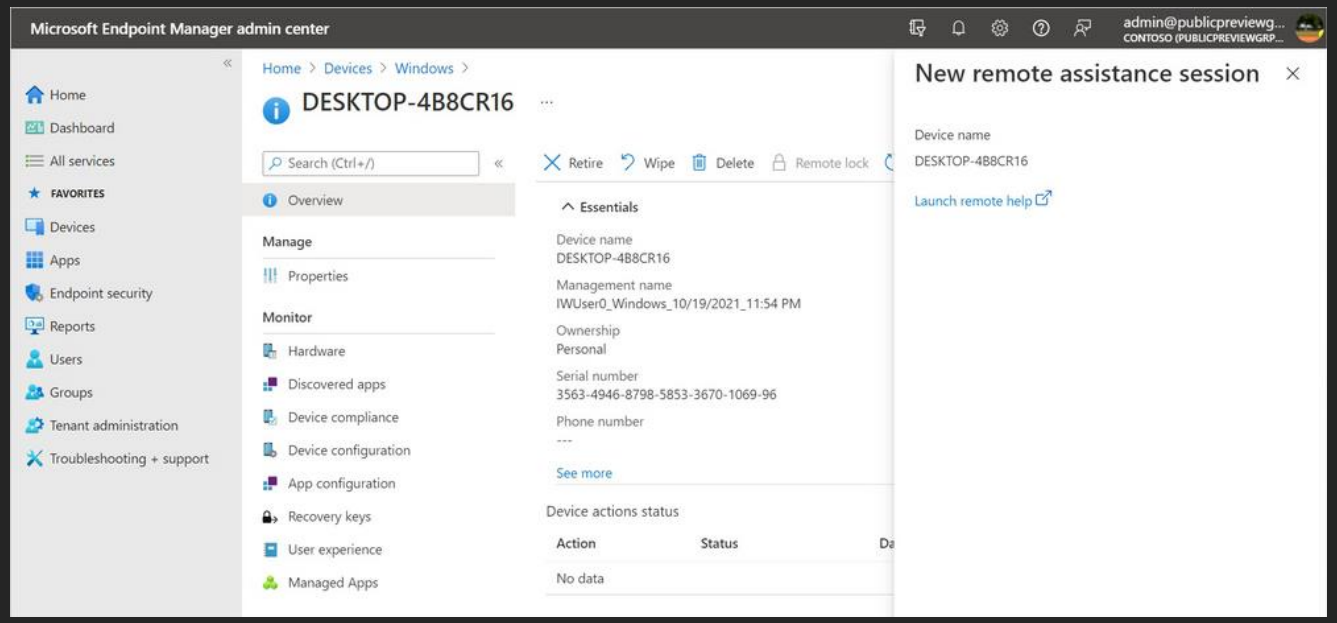
Choosing **Next** means that you agree to the Microsoft Services Agreement and privacy and cookies statement.

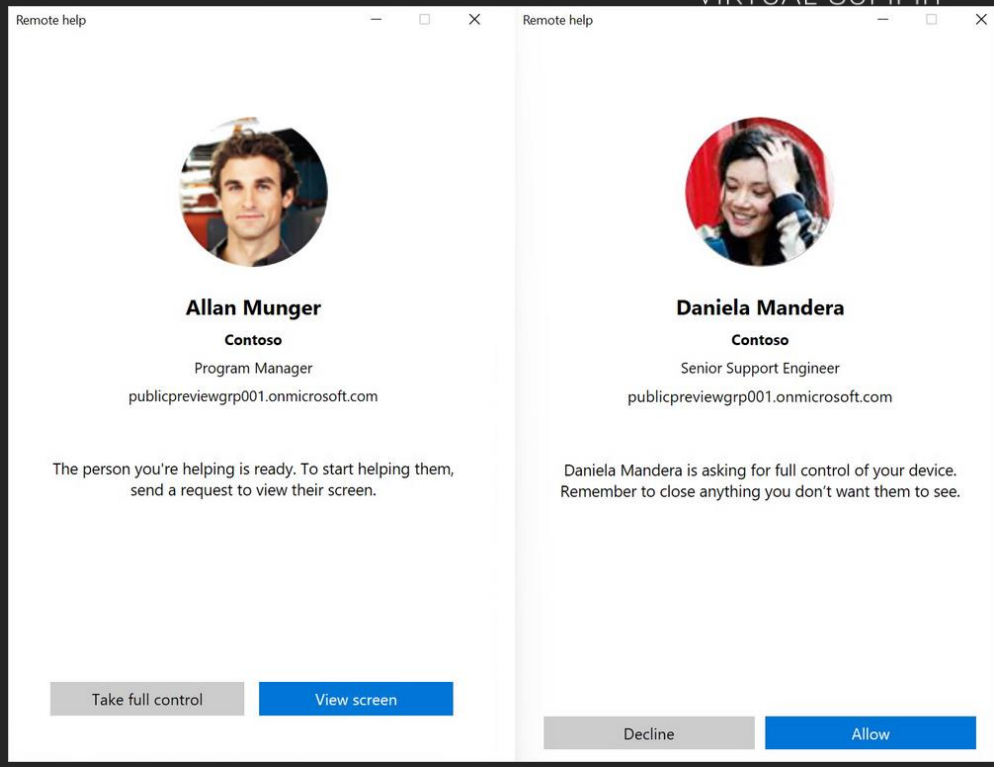
Next

Remote Help (Announced at Ignite)

- Support UAC
- RBAC
- Logging/Tracking

Note: Comes with an additional cost





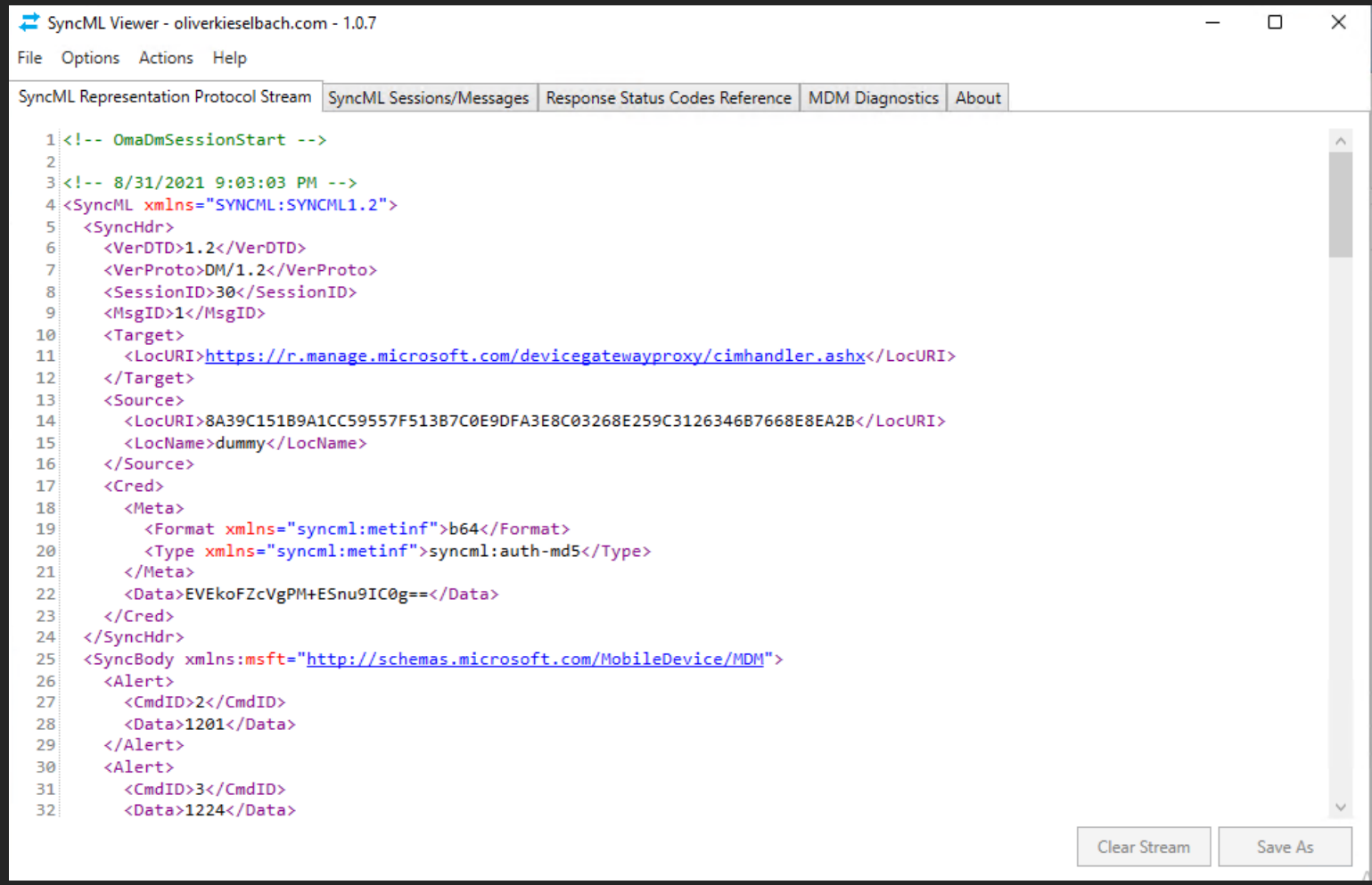
CMtrace

- Great log reader
- Not free but included in the Intune/MEM license
- Deploy it to all clients

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

More Tools – advanced troubleshooting

- Wireshark
- Fiddler
- Netmon
- **SyncMLViewer**



[SyncMLViewer/SyncMLViewer/dist at master · okieselbach/SyncMLViewer · GitHub]

Log Files

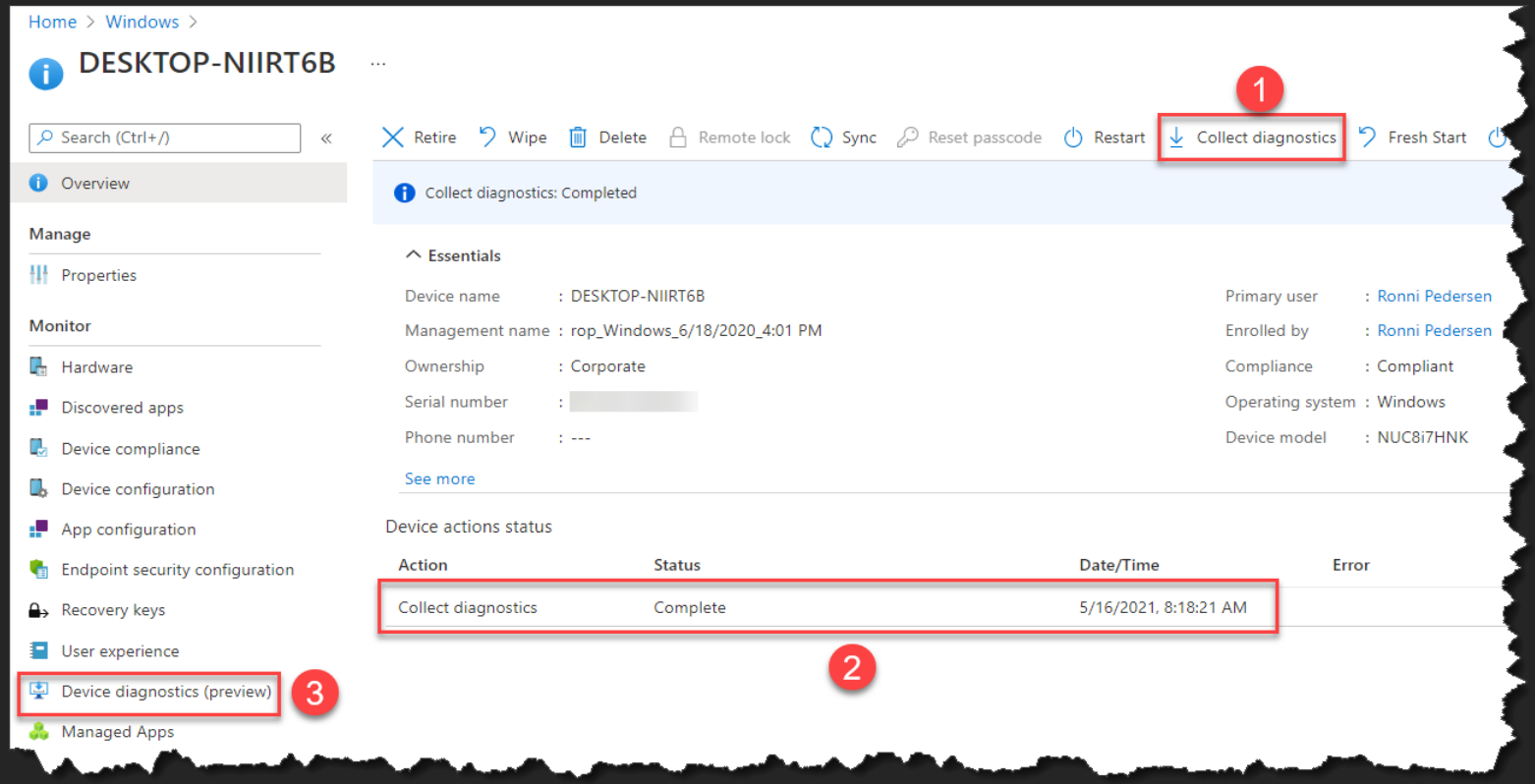
Collect diagnostics from a Windows Device

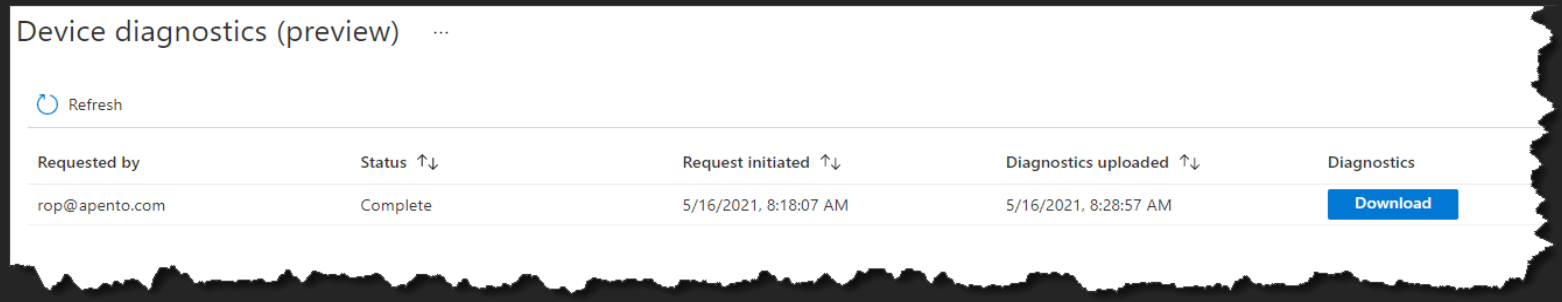
NORDIC
– VIRTUAL SUMMIT –

- Collecting Diagnostic Logs from Windows Devices
  - All supported versions of Windows 10/11
  - Both Intune and Co-Managed devices
  - Corporate-owned devices only

- More information:
  - https://docs.microsoft.com/en-us/mem/intune/remote-actions/collect-diagnostics

Collecting Diagnostic Logs





NORDIC
– VIRTUAL SUMMIT –

Configuration Policy Process

Microsoft 365 Apps Policy

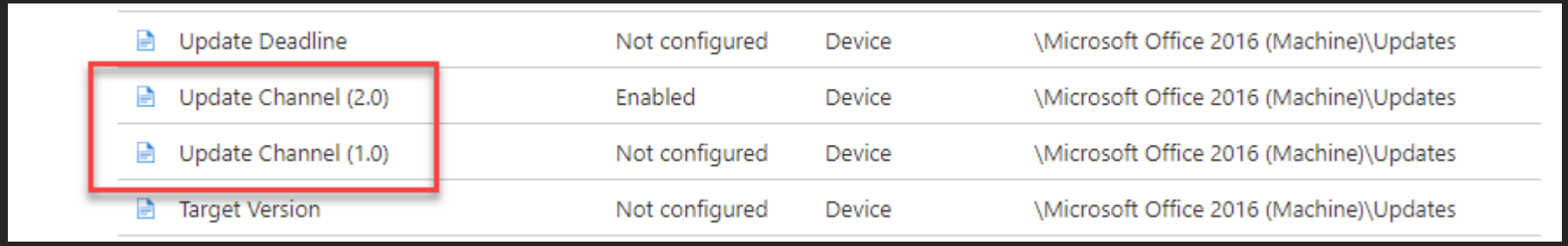
NORDIC
– VIRTUAL SUMMIT –

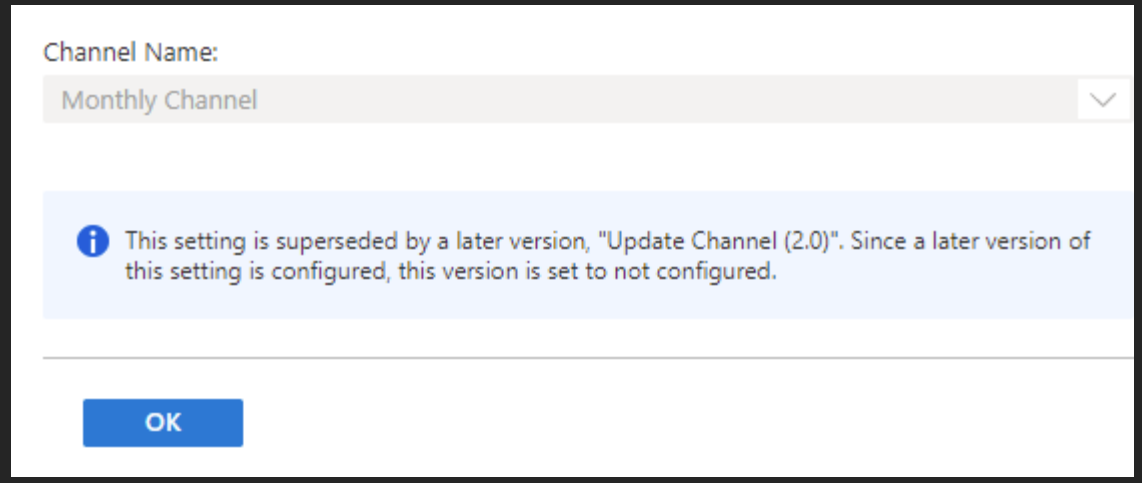
- Endpoint Manager Configuration:
  - Policy 1: Enable Microsoft 365 Apps Automatic Updates
  - Policy 2: Set the Update Channel

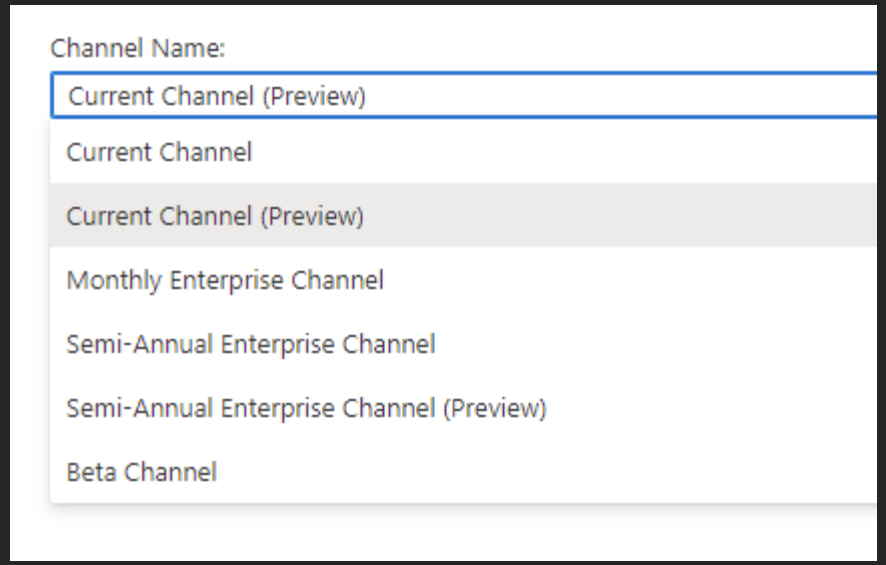
- Client-Side debugging:
  - #1 Check the Intune registry keys
  - #2 Check the Office registry keys
  - #3 Force Office automatic updates to run
  - #4 Force the Office synchronization to update account information

Administrative Templates

- Example using Administrative Templates



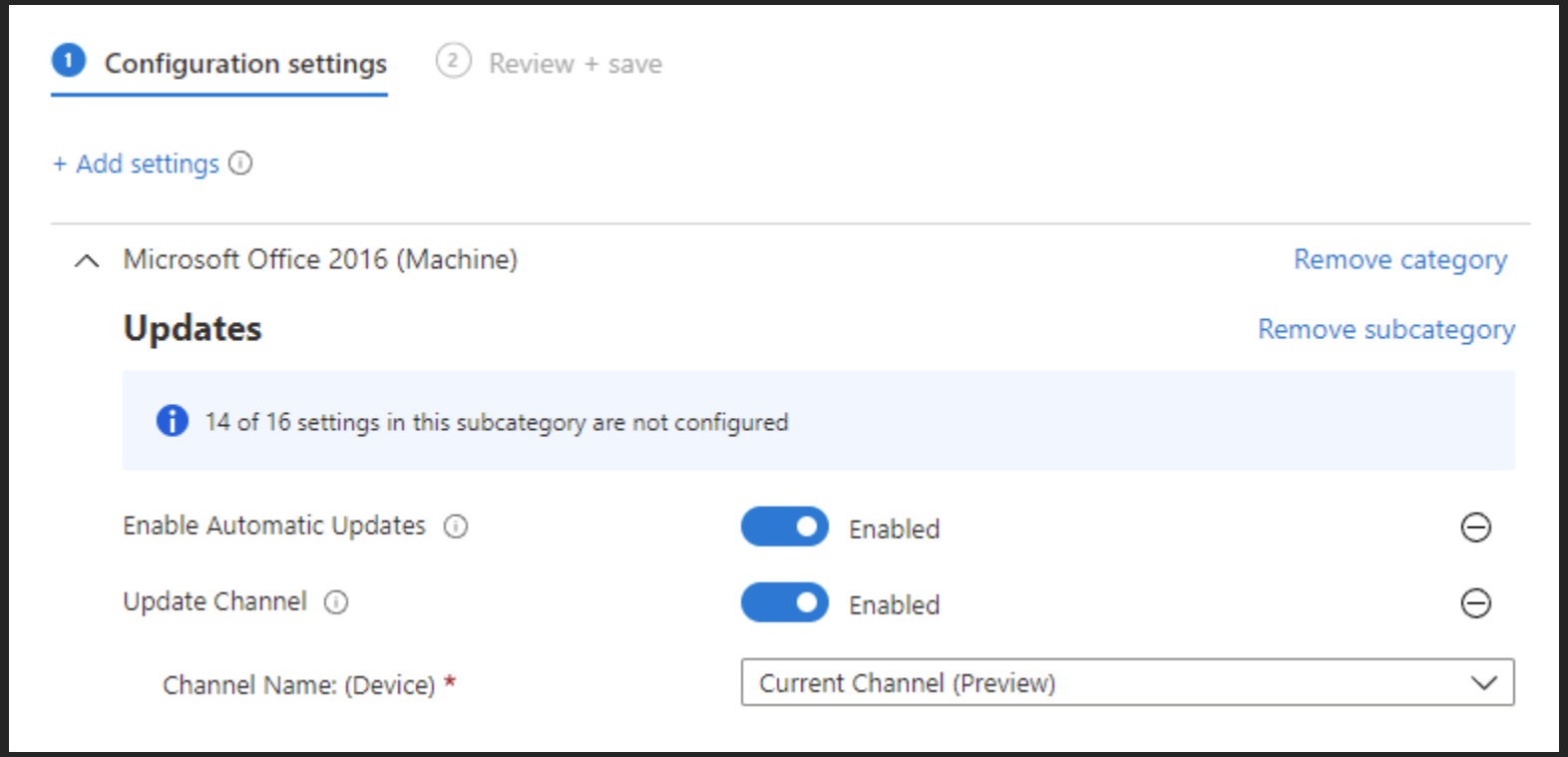




Using Settings Catalog (Preview)

NORDIC
– VIRTUAL SUMMIT –

- Policy Configuration:
  - Enable Microsoft 365 Apps Automatic Updates
  - Set the Update Channel



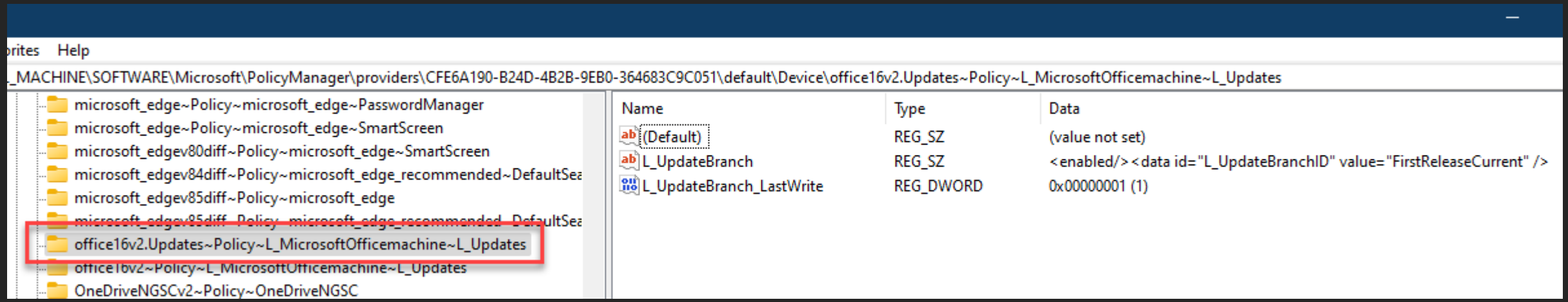
#1 Check the Intune registry keys

NORDIC
– VIRTUAL SUMMIT –

- Open the Registry Editor, and go to the Intune policy path:

HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\<Provider ID>
\default\Device\office16~Policy~L_MicrosoftOfficemachine~L_Updates

- When the policy is applied, you see the following registry keys:
  - L_UpdateBranch
- At this point, the Intune policy is successfully applied to the device.



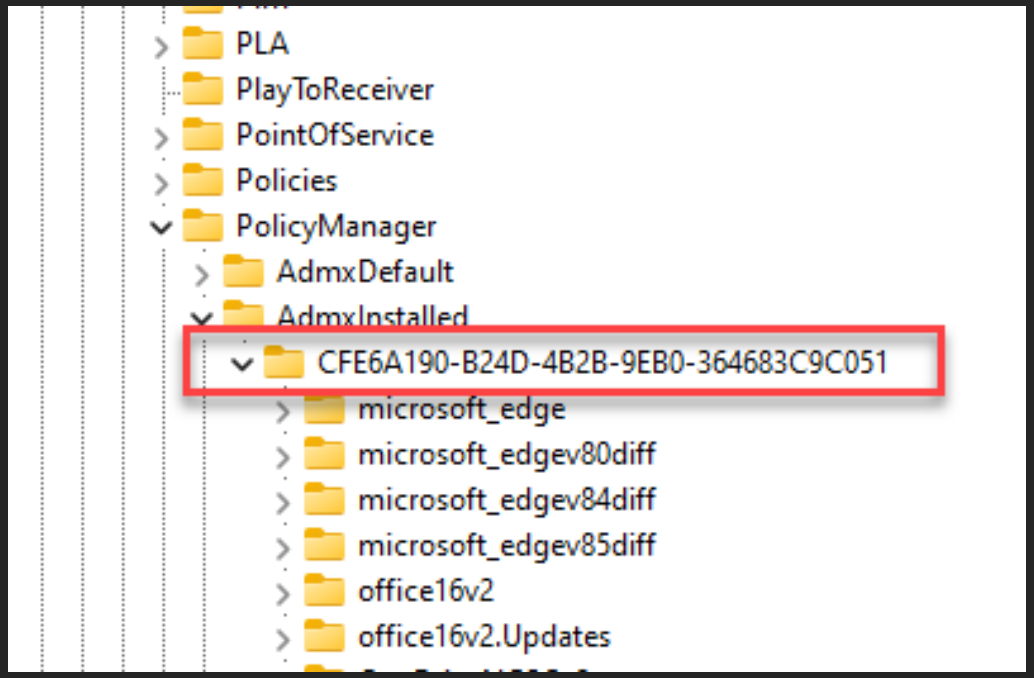
#TIP: Find the Provider ID

NORDIC
– VIRTUAL SUMMIT –

Find the provider ID for your device

- Open the Registry Editor, and go to:

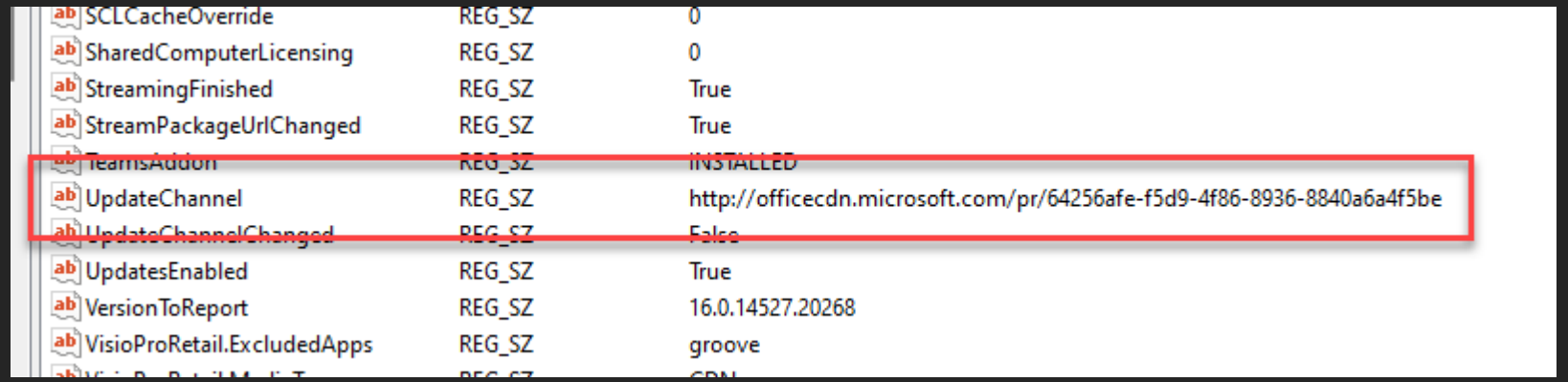
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\AdmxInstalled



#2 Check the Office registry keys

NORDIC
– VIRTUAL SUMMIT –

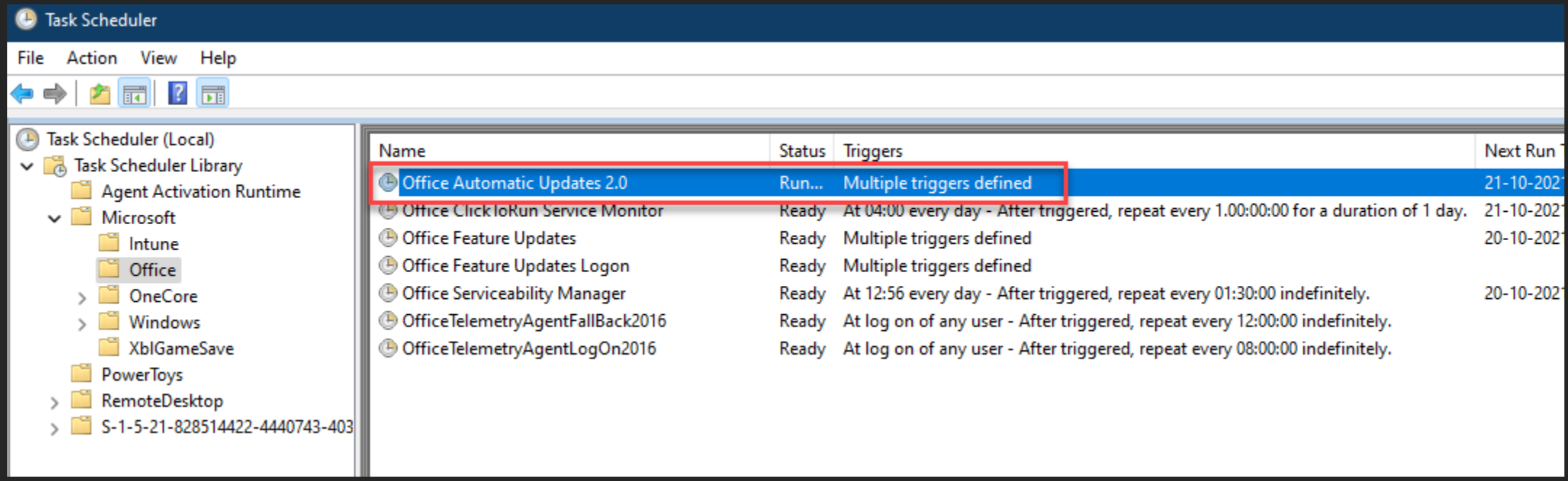
- Go to the Office policy path:
  Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\Configuration
- Check the UpdateChannel value:
  - Monthly Enterprise Channel = 55336b82-a18d-4dd6-b5f6-9e5095c314a6
  - Current Channel = 492350f6-3a01-4f97-b9c0-c7c6ddf67d60
  - Current Channel (Preview) = 64256afe-f5d9-4f86-8936-8840a6a4f5be
  - Semi-Annual Enterprise Channel = 7ffbc6bf-bc32-4f92-8982-f9dd17fd3114
  - Semi-Annual Enterprise Channel (Preview) = b8f9b850-328d-4355-9145-c59439a0c4cf
  - Beta Channel = 5440fd1f-7ecb-4221-8110-145efaa6372f



#3 Force Office automatic updates to run

NORDIC
– VIRTUAL SUMMIT –

- To test the policy, we can force the policy settings on the device
  - Go to HKLM\SOFTWARE\Microsoft\Office\ClickToRun\Updates
  - Edit the UpdateDetectionLastRunTime key > delete the value data.
  - Launch Task Secheduler > Microsoft > Office
    - Run "Office Automatic Updates 2.0"

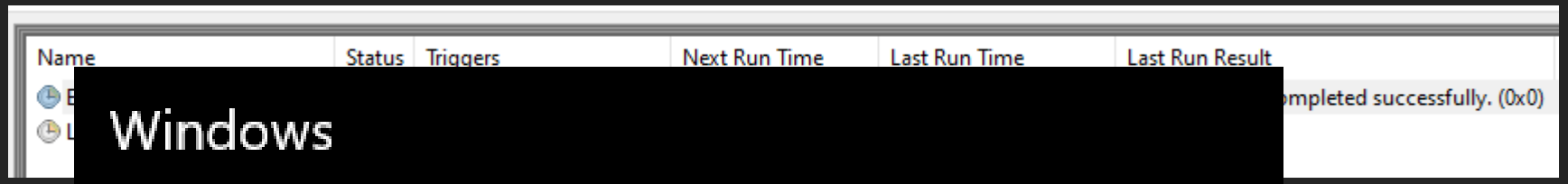


NORDIC
– VIRTUAL SUMMIT –

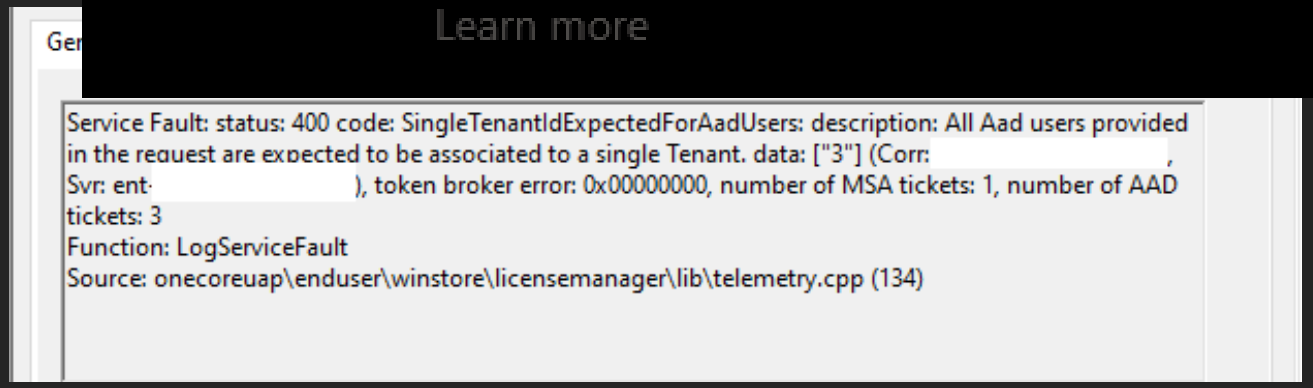
Troubleshooting Subscription based activation

Subscription based activation

- Re-activated every 30 days
- Two scheduled tasks triggers License Acquisition

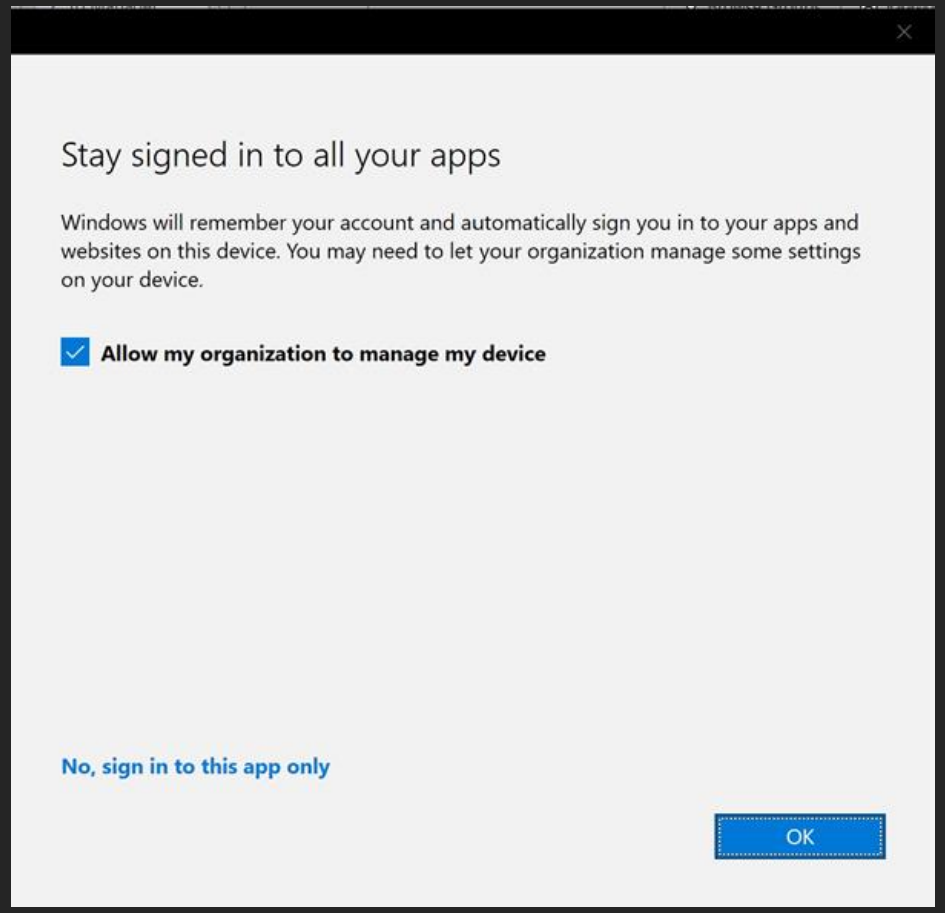


- The
  - I s added under "Access
    V

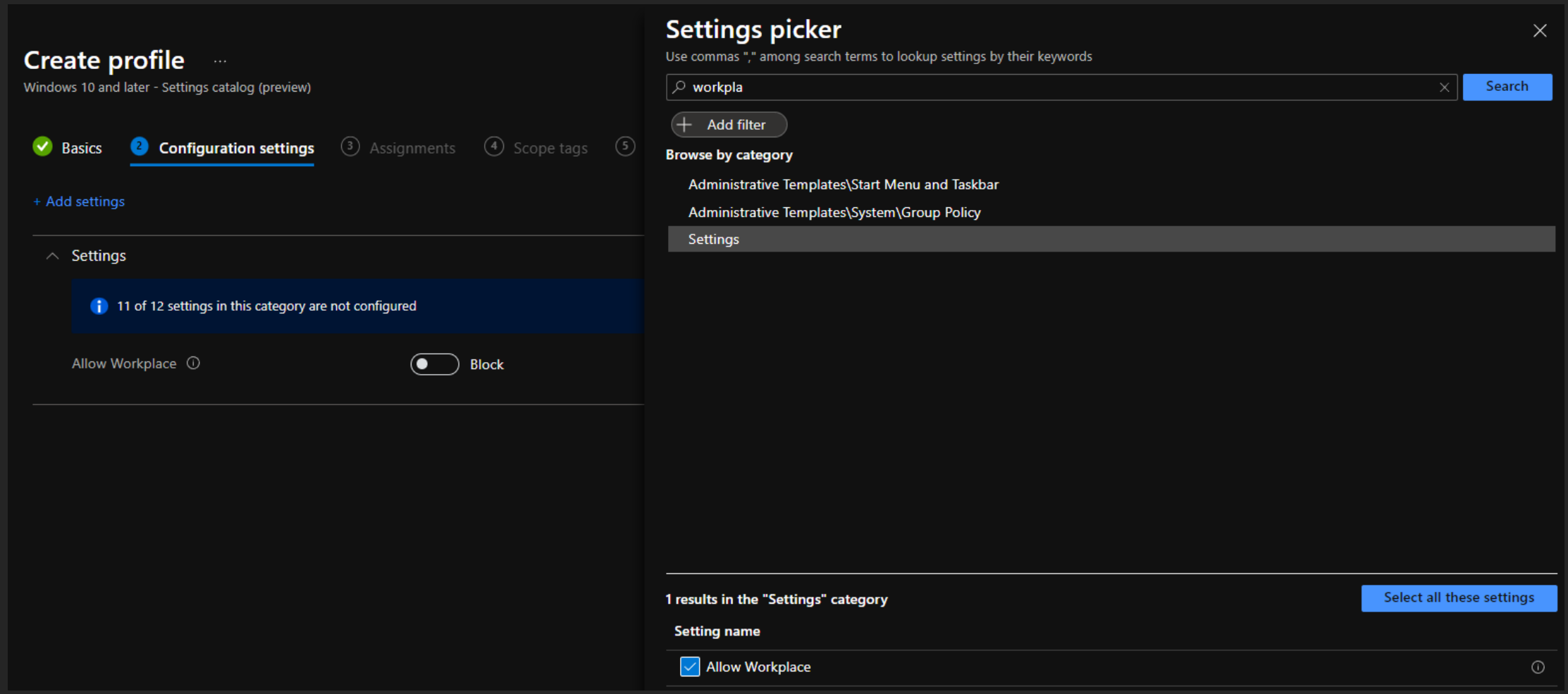


Stay signed in to all your apps = Evil

- “Stay signed in to all your apps” dialog in Microsoft Apps (outlook, Powerpoint, excel….)
- Recommended to block on Hybrid Join
- Needs to be blocked on all modern managed Windows 10!
  - Personal devices: Intune sync will fail
  - AzureAD Joined devices: Windows Activation will fail



Blocking Workplace join



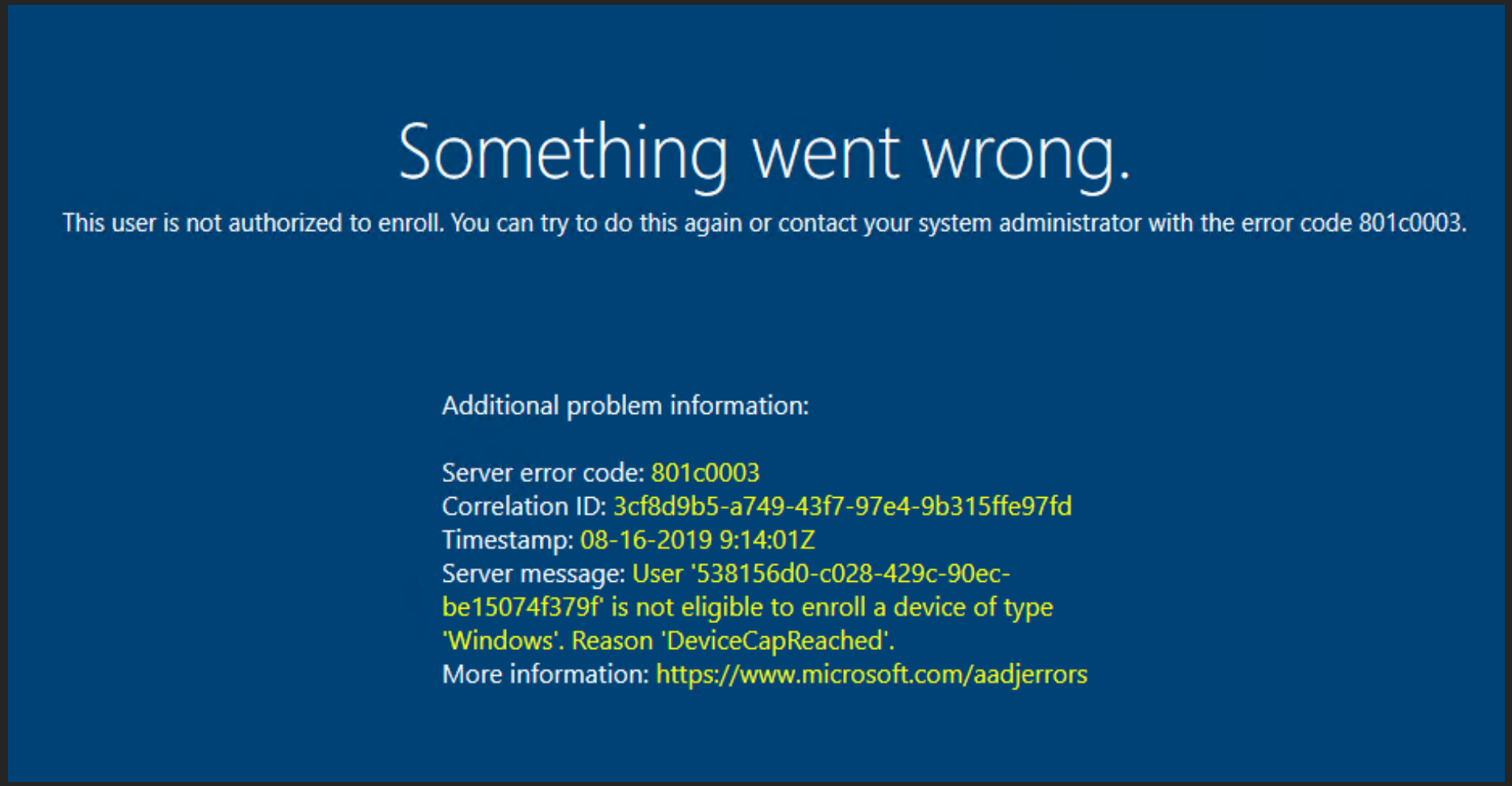
NORDIC
– VIRTUAL SUMMIT –

Troubleshoot enrollment

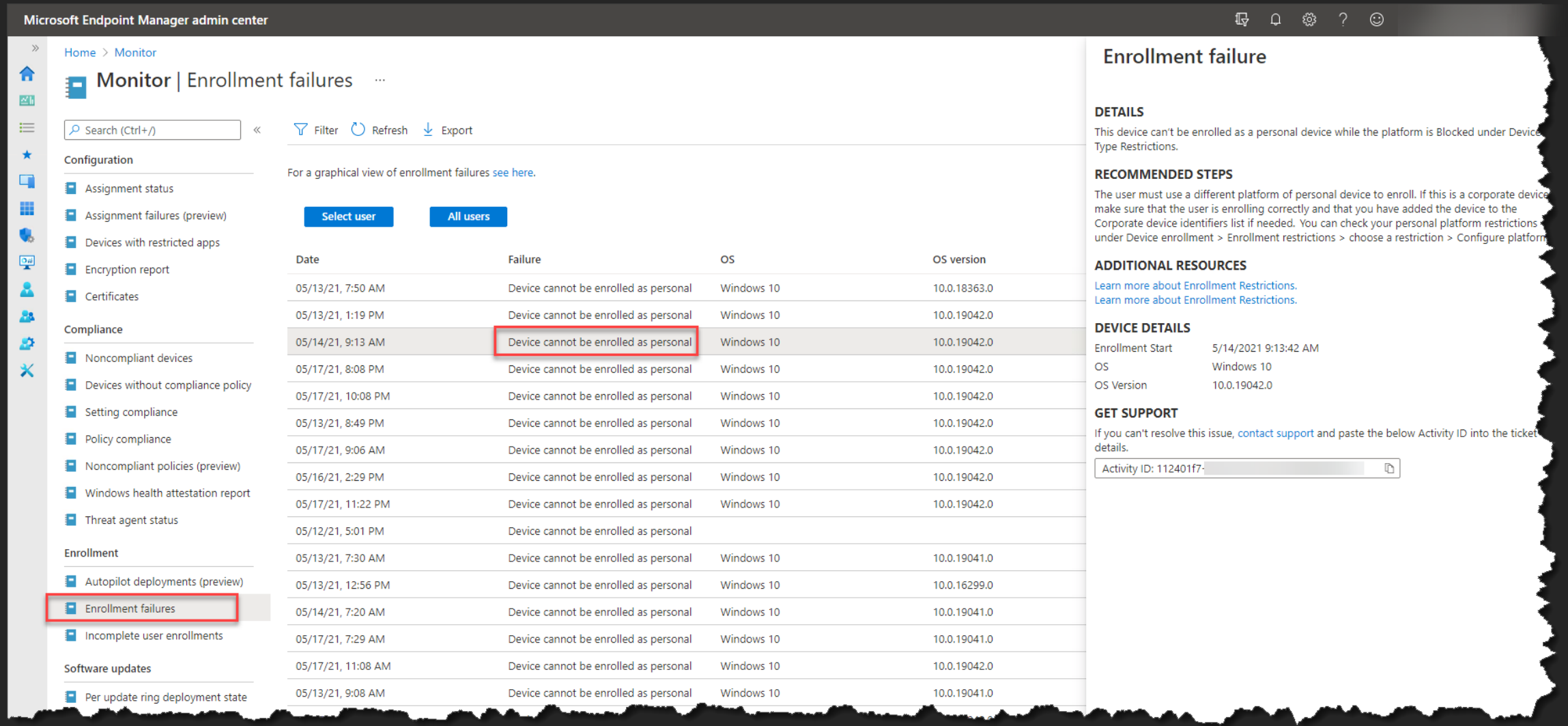
Troubleshooting Windows enrollemnt in Intune

- Valid License assigned to the user?
- Is the user allowed to enroll a device?
- Network issues, proxy etc.?
- Enrollment restrictions that blocks enrollment?
- Number of devices already enrolled (Device Limit)
- MDM Terms of use not correct

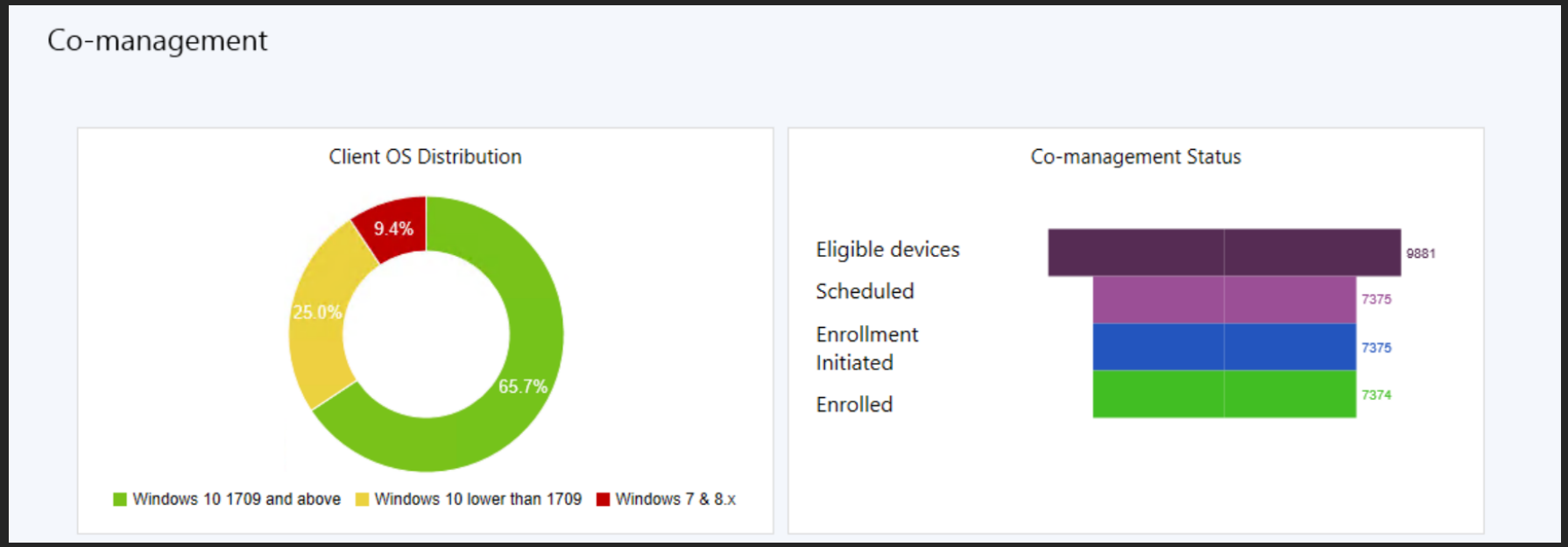
DeviceCapReached = Device Limits

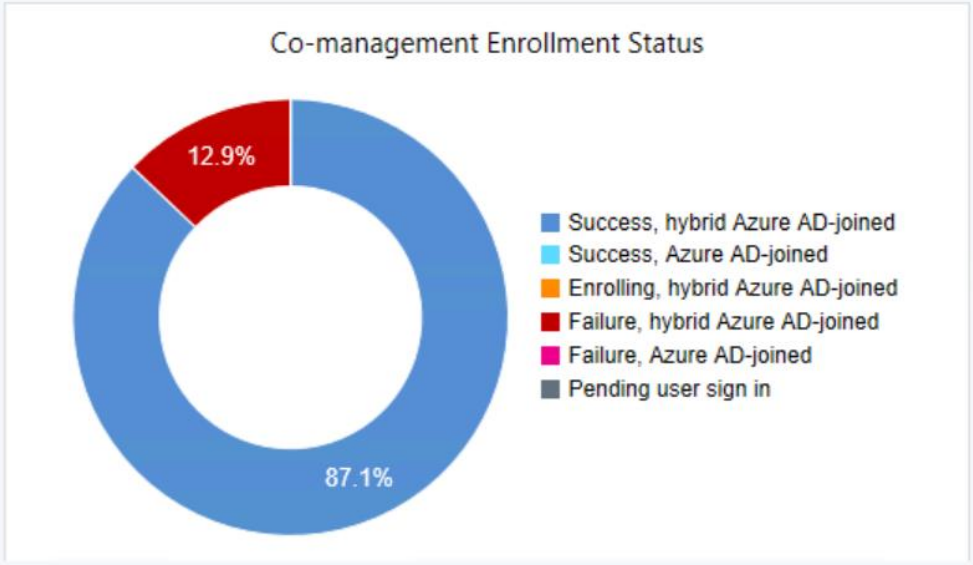


Enrollment Failures



Co-Management Enrollment Status





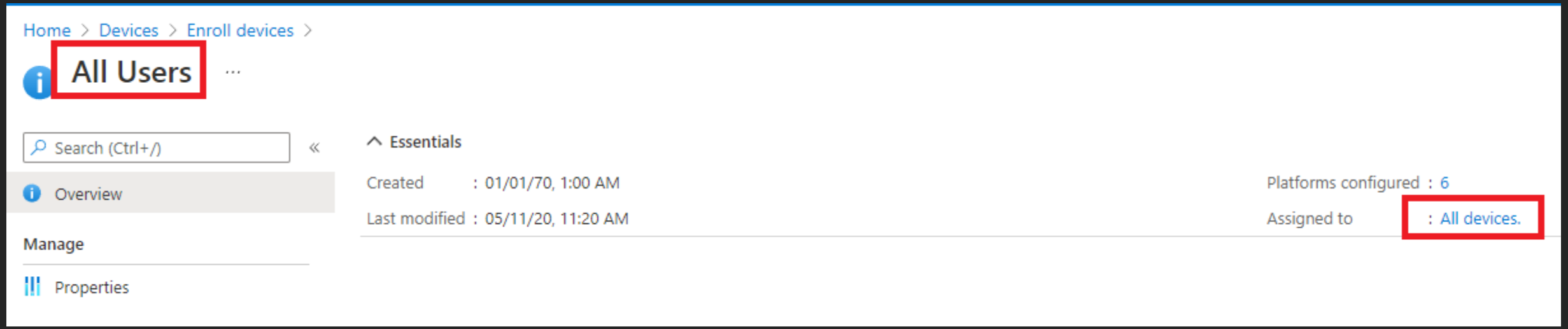
Count	Enrollment Error
706	License of user is in bad state blocking enrollment
382	Undefined
6	Element not found.
5	Catastrophic failure
4	The Internet connection has timed out
2	MDM enrollment hasn't been configured yet on AAD, or the enrollment url isn't expected.
1	The user canceled the operation

Co-Managed device enrollment

NORDIC
– VIRTUAL SUMMIT –

- Co-managed devices will always try to enroll using a Device token
- If it fails it will try using the user token, depending on MFA settings this can fail as well.

Important: the default enrollment restriction policy “All Users” is applied to “All Devices”



Troubleshooting Policies

Device Settings in Microsoft Intune

NORDIC
– VIRTUAL SUMMIT –

Recommended order for Windows devices

- Endpoint Security
- Settings Catalog (Preview)
- Templates
  - Configuration Policies
  - Built-In Administrative Templates
  - OMA-URI (Custom CSP)
- Custom ADMX ingestion (3rd. Party apps)
- PowerShell Scripts

Optional:

- Proactive Remediation (Requires a Windows Enterprise E3 license)

Profile Tattooing

- Removing the assignment of the profile does not always revert the setting.
  - The behavior depends on the CSP.
  - Some setting remains until configured to a different value
  - Some CSPs remove the setting, and some CSPs keep the setting.

- Profiles applies to a **User Group** and a user is removed from the group.
  - Note: It can take up to **7 hours + the platform-specific policy refresh cycle**.

- Wi-Fi, VPN, Certificate, and Email Profiles
  - These profiles are removed from all supported enrolled devices

Policy and Profile refresh cycles

NORDIC
– VIRTUAL SUMMIT –

Existing Devices

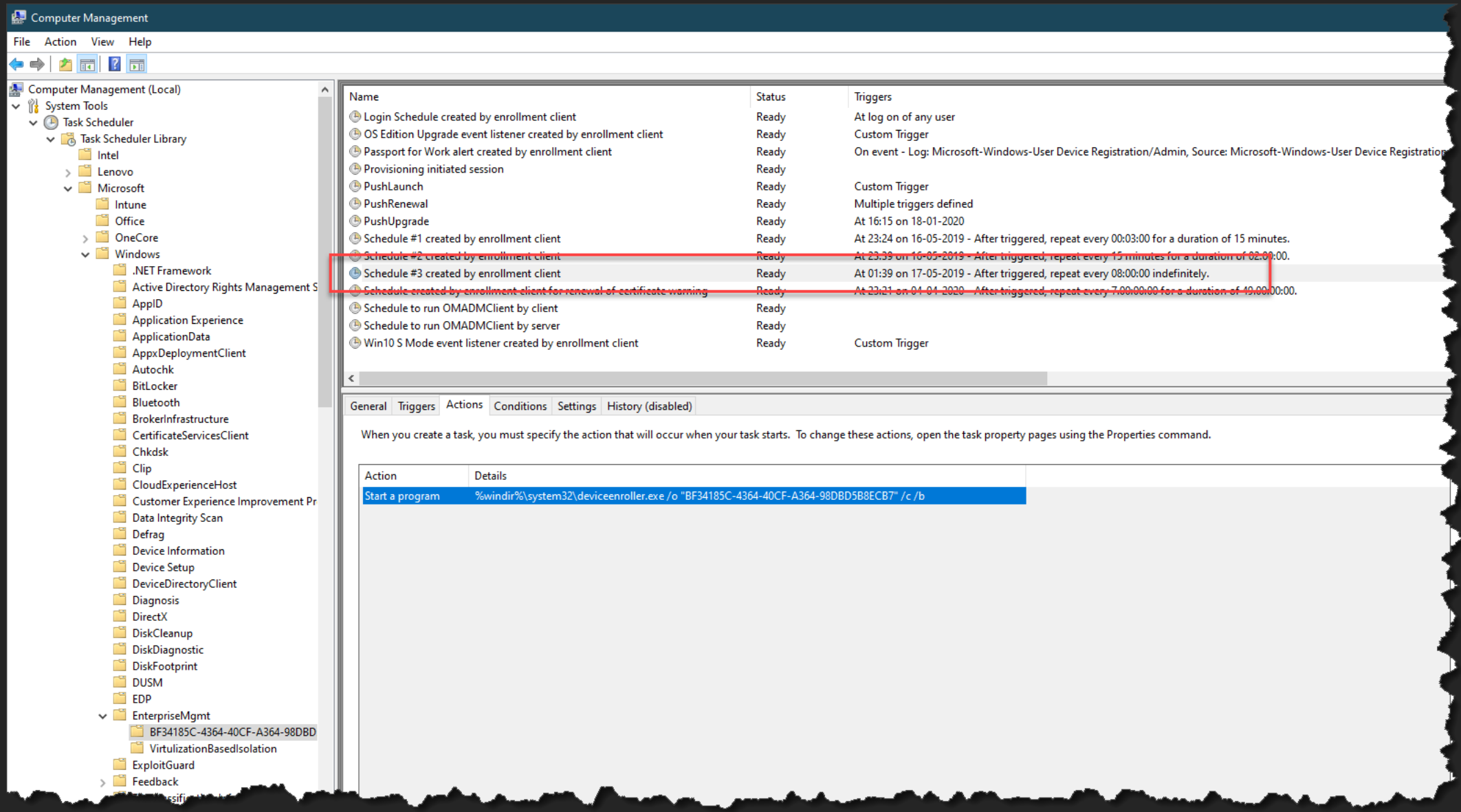
- Windows 10/11 devices will schedule check-in with the Intune service, which is estimated at: About every 8 hours

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



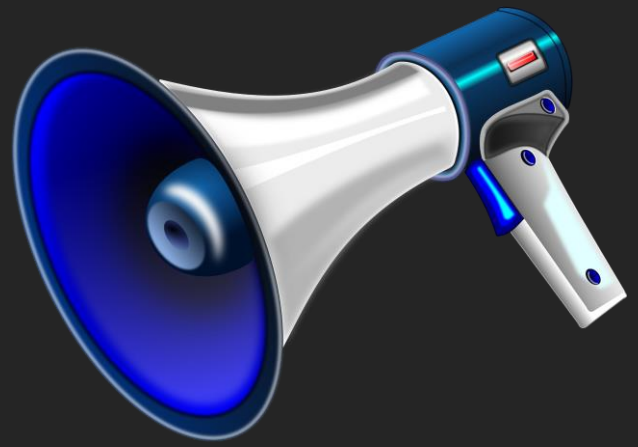
NORDIC
— VIRTUAL SUMMIT —

Intune notifications / Sync immediately

NORDIC
– VIRTUAL SUMMIT –

- 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 “XXX” devices will be updated !
  - By design (to avoid denial of service)
  - Not the same for all platforms
  - Workaround: Use script to connect to all clients and force a sync

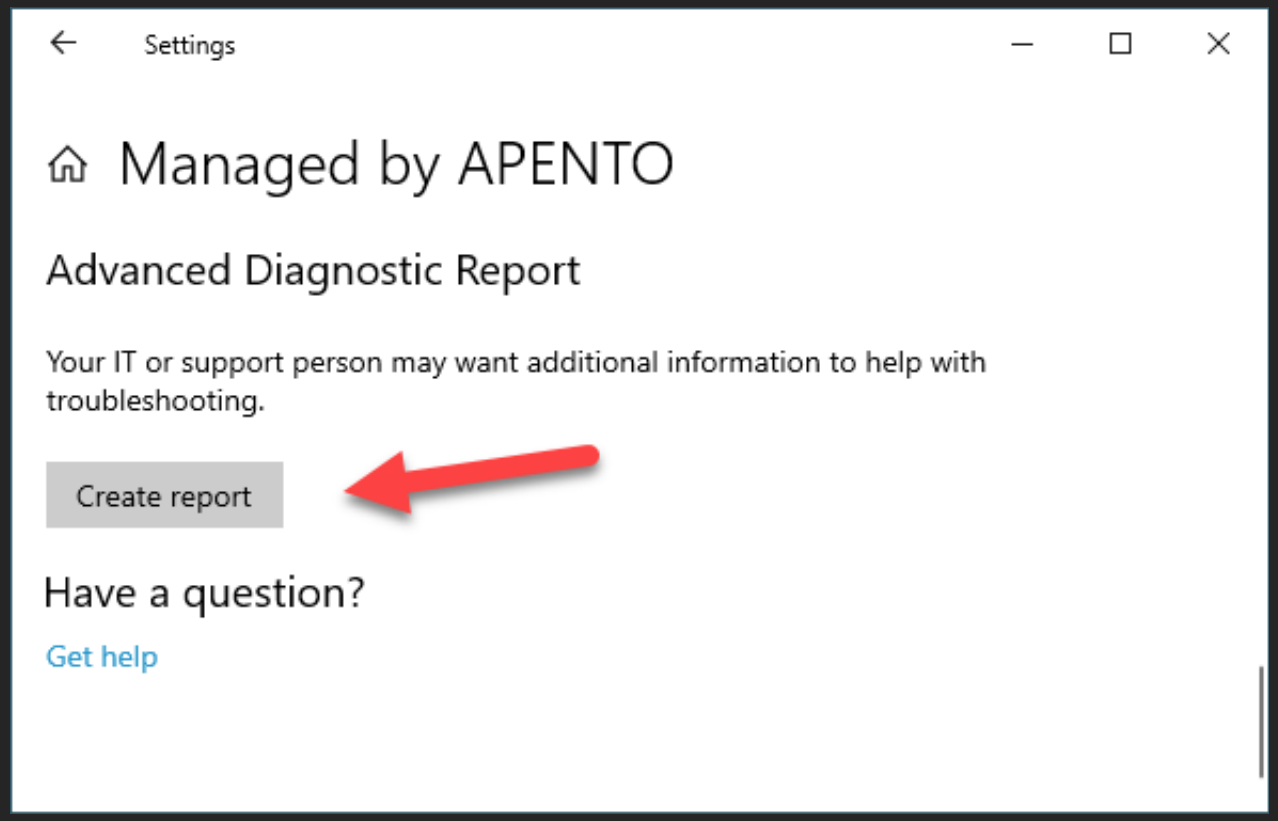
Policy/Profile Conflicts

NORDIC
– VIRTUAL SUMMIT –

- Compliance policy settings always have precedence over configuration profile settings.
- Compliance policy conflicts: The most restrictive compliance policy setting applies.
- Configuration Profile Conflicts: Shown in Intune.
  - Manually resolve these conflicts

Troubleshooting MDM Policies

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



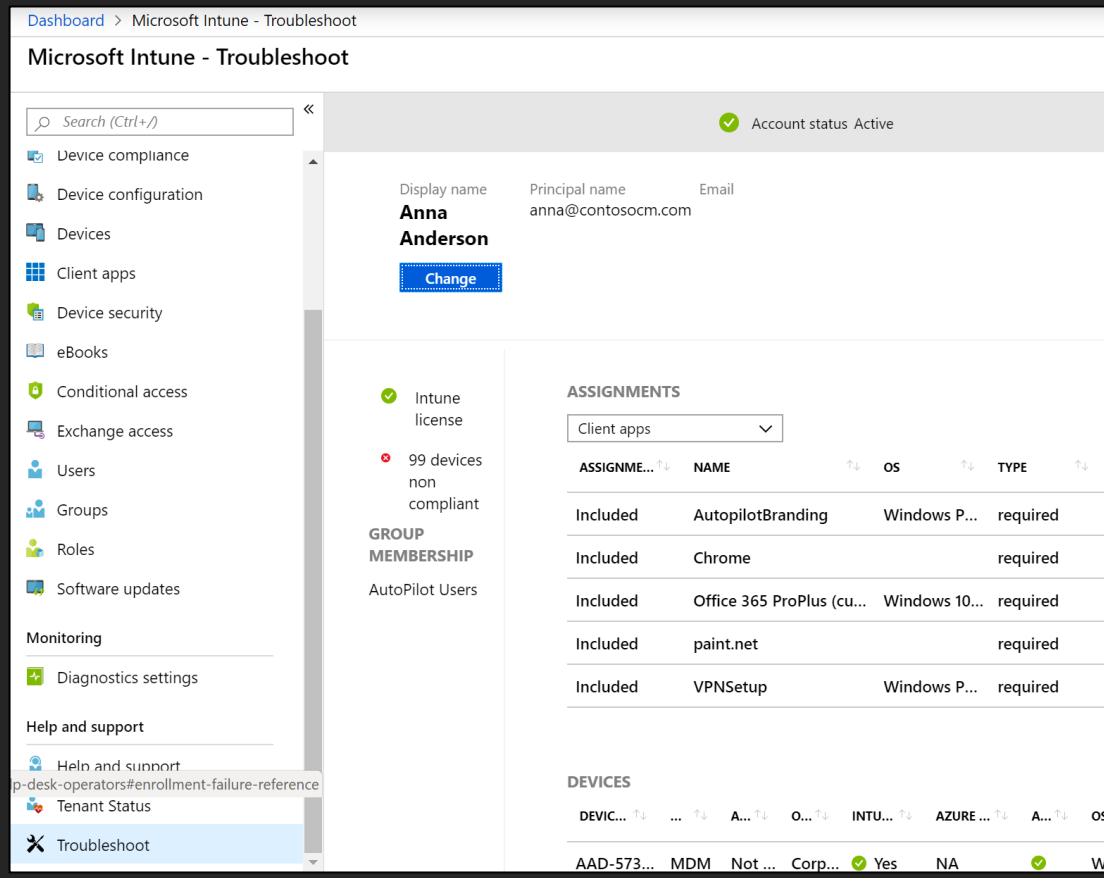
Managed policies

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	[illegible]	1		device		[illegible]

Intune Troubleshooting Pane

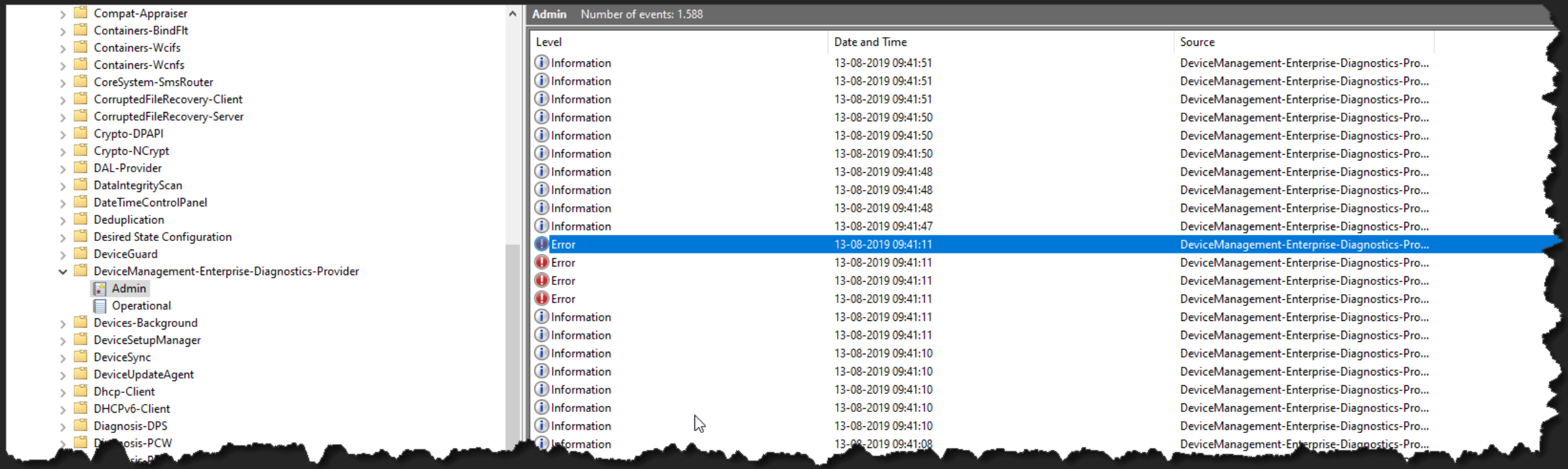
- Intune portal page
  - https://aka.ms/intunetroubleshooting
- Displays information focused around a particular user
  - See info about assignments, devices, enrollment failures, etc.
- For more info: https://docs.microsoft.com/en-us/intune/help-desk-operators



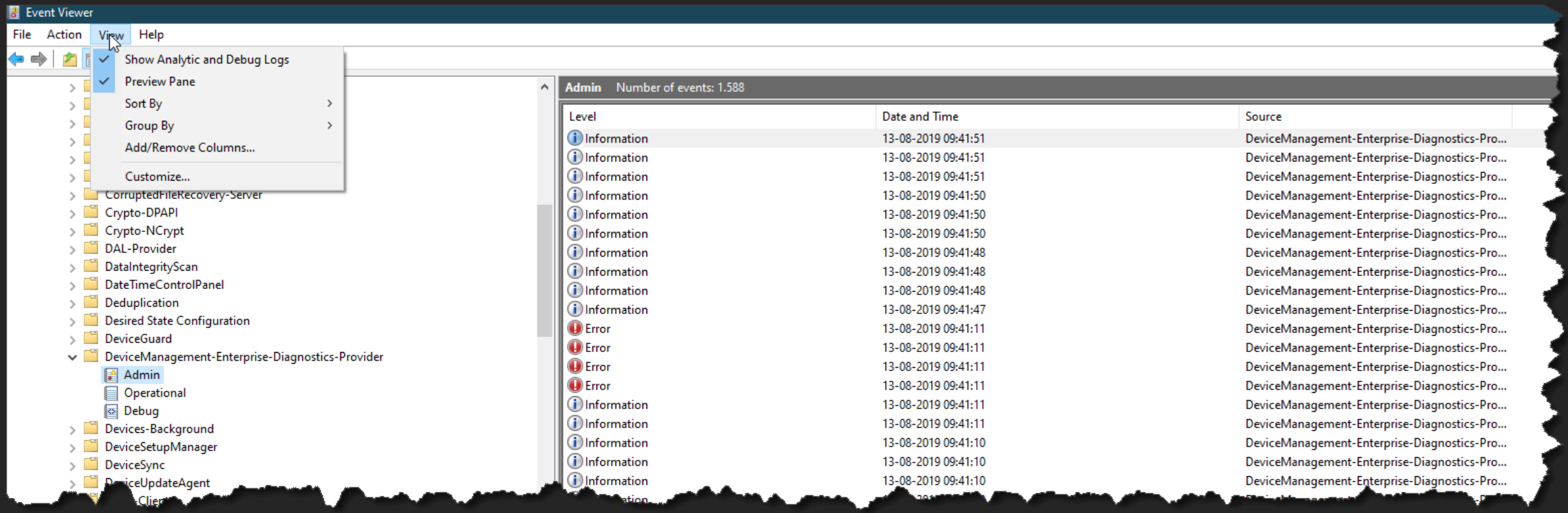
Device Profiles - Where is my logs?

NORDIC
— VIRTUAL SUMMIT —

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



Enable debug mode



NORDIC
– VIRTUAL SUMMIT –

Intune Management Extension

Intune Management Extension Pre-requisites

NORDIC
– VIRTUAL SUMMIT –

- Installed when first needed by Win32App or PowerShell script.
- Installed only on “Corporate” and “personal” devices (personal device context only, added in late 2020-but not supported?!…)

> **Note**
>
> Once the Intune management extension prerequisites are met, the Intune management extension is installed automatically when a PowerShell script or Win32 app is assigned to the user or device. For more information, see Intune Management Extensions **prerequisites**.
>
> PowerShell scripts, which are not officially supported on Workplace join (WPJ) devices, can be deployed to WPJ devices. Specifically, device context PowerShell scripts work on WPJ devices, but user context PowerShell scripts are ignored by design. User context scripts will be ignored on WPJ devices and will not be reported to the Microsoft Endpoint Manager console.

https://docs.microsoft.com/en-us/intune/apps/intune-management-extension#prerequisites

What is a Corporate Device?

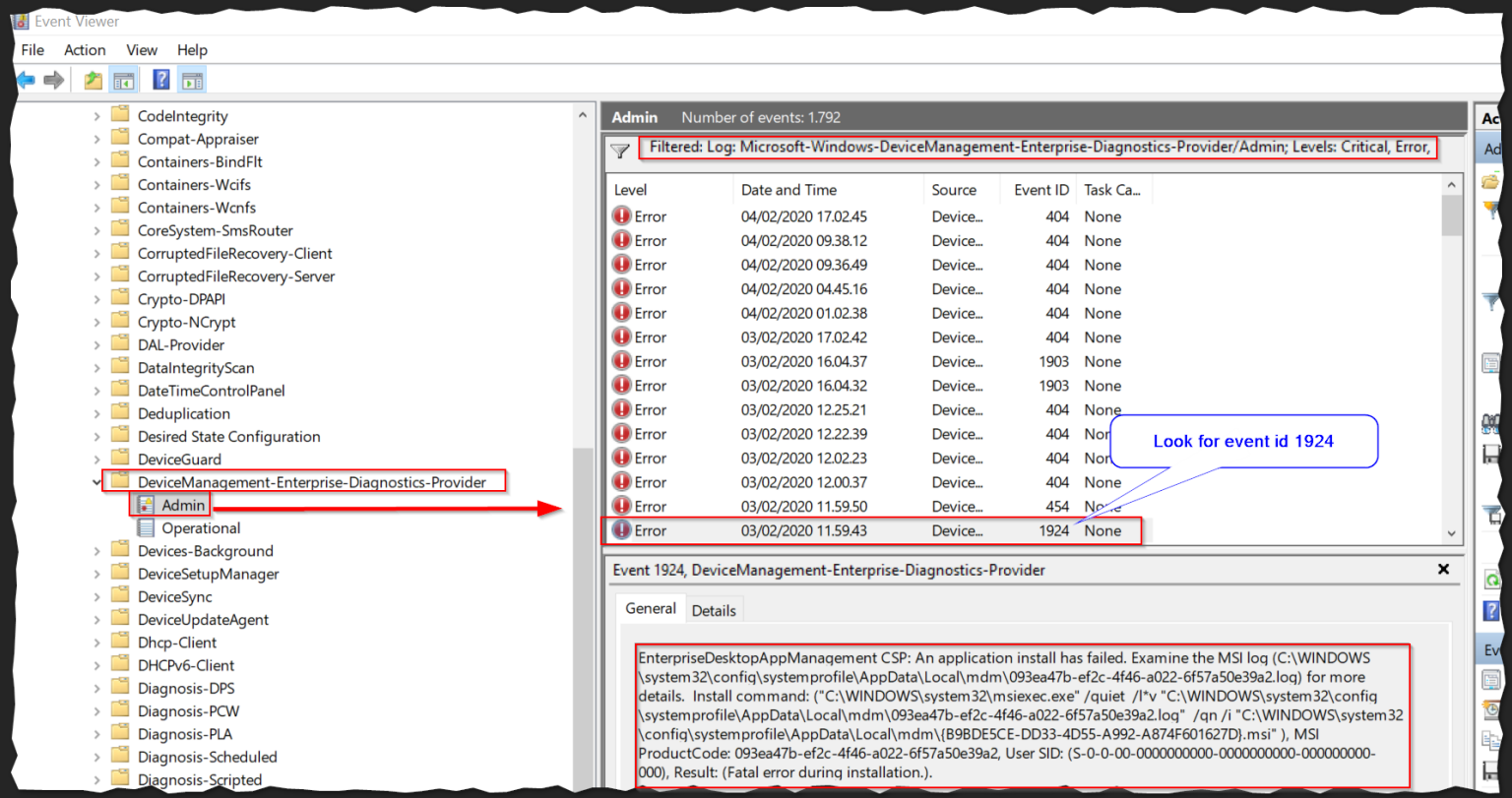
NORDIC
– VIRTUAL SUMMIT –

- 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.

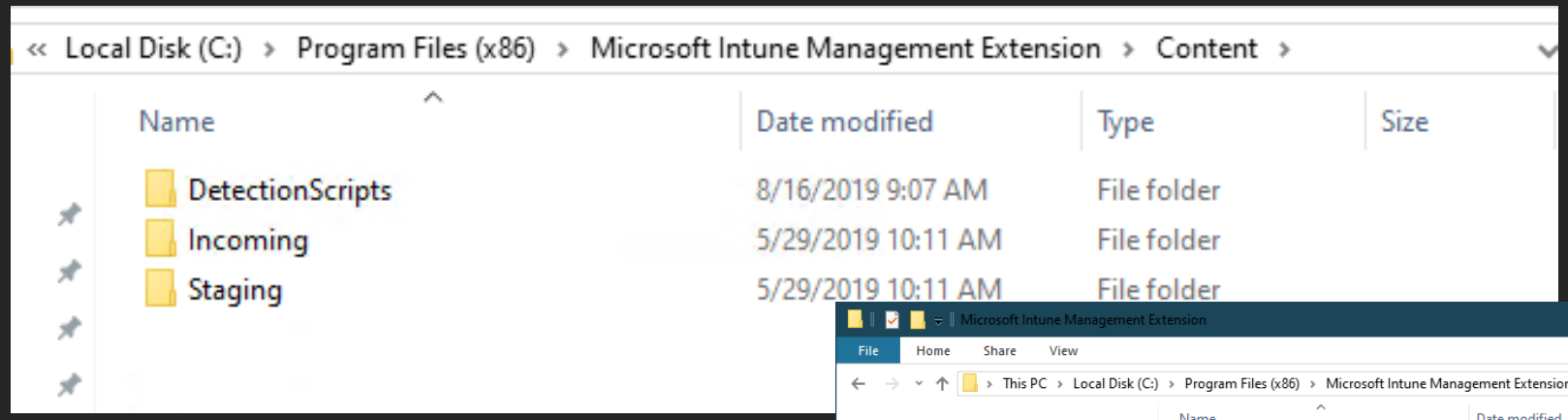
Intune Management Extension Event log

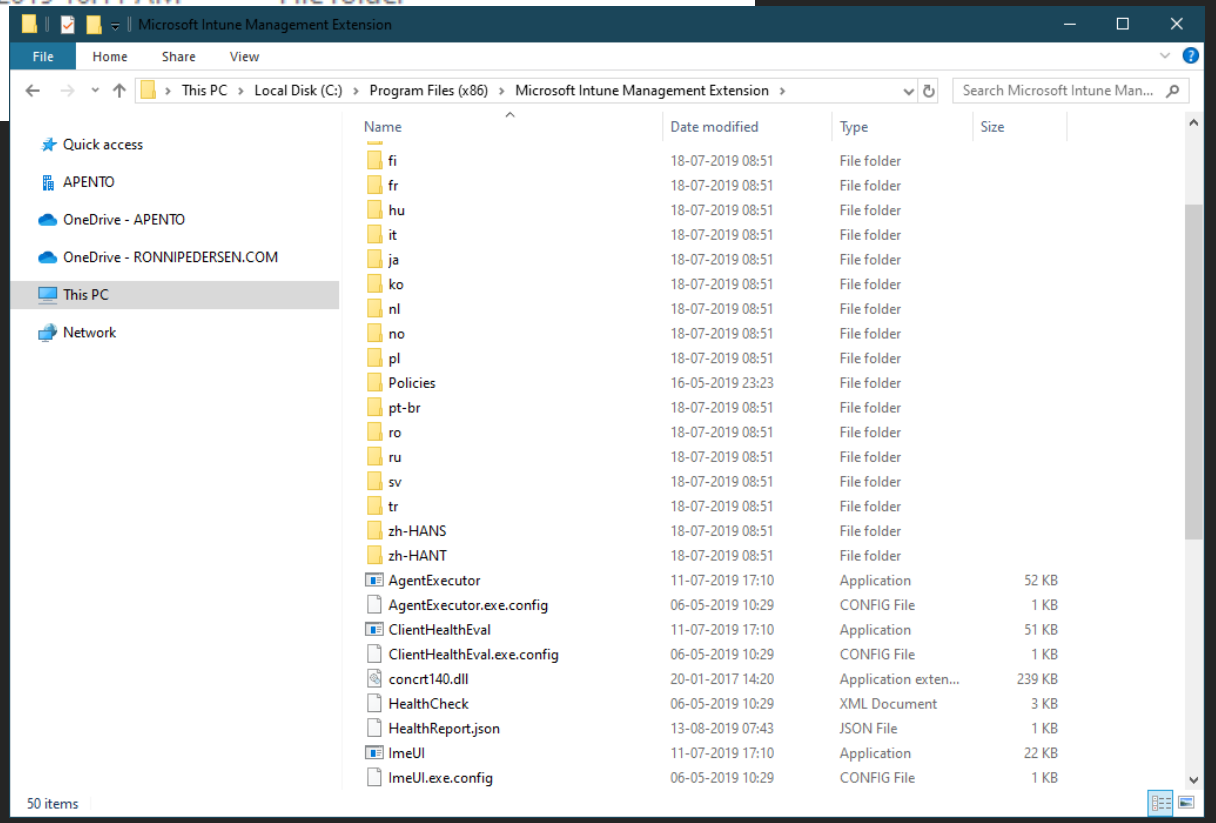
NORDIC
– VIRTUAL SUMMIT –

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



Intune Management Extension File System

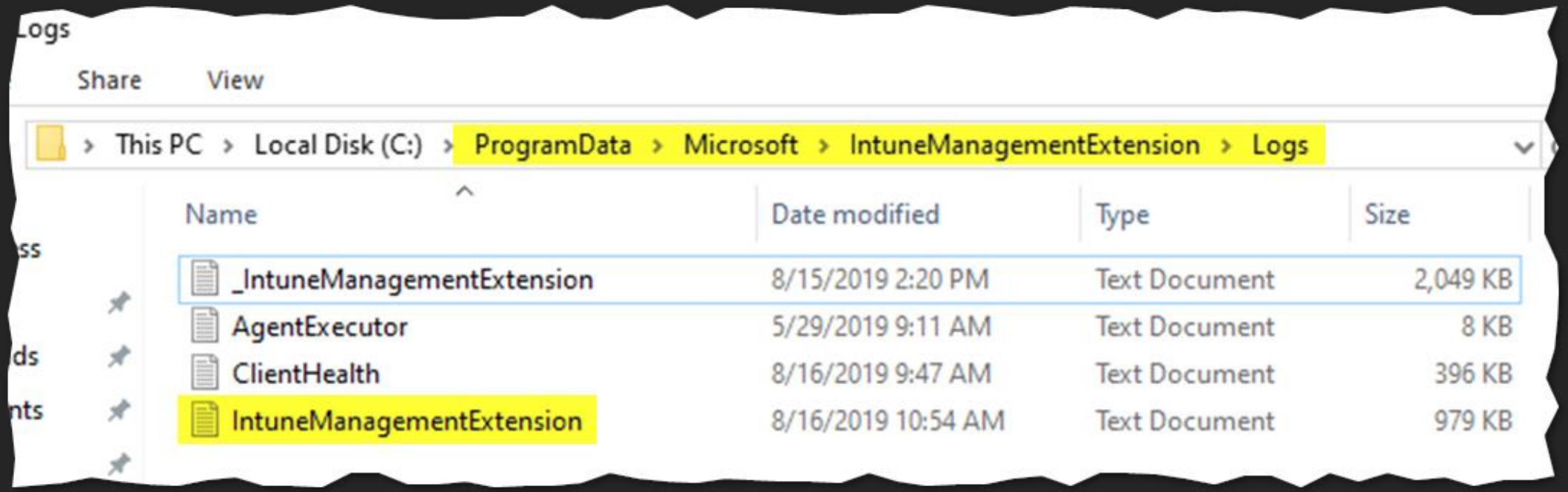




Intune Management Extension Log files

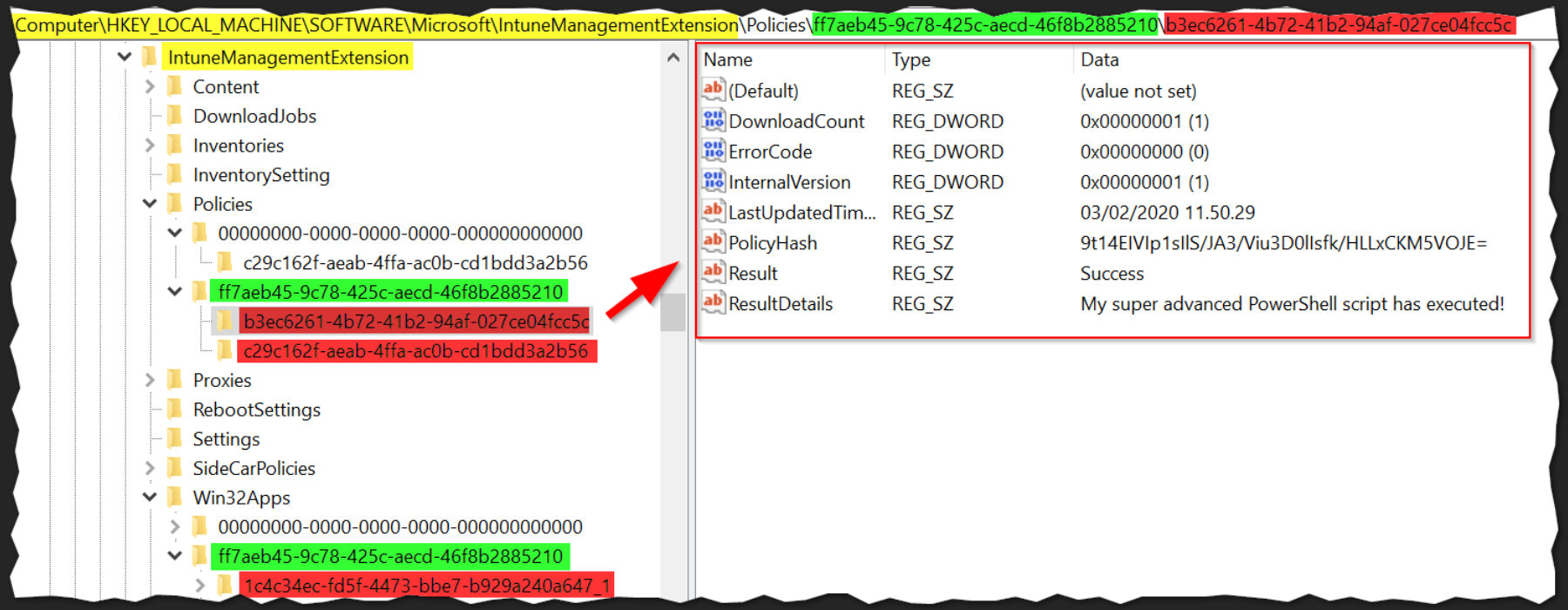
NORDIC
– VIRTUAL SUMMIT –

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



Intune Management Extension The Registry

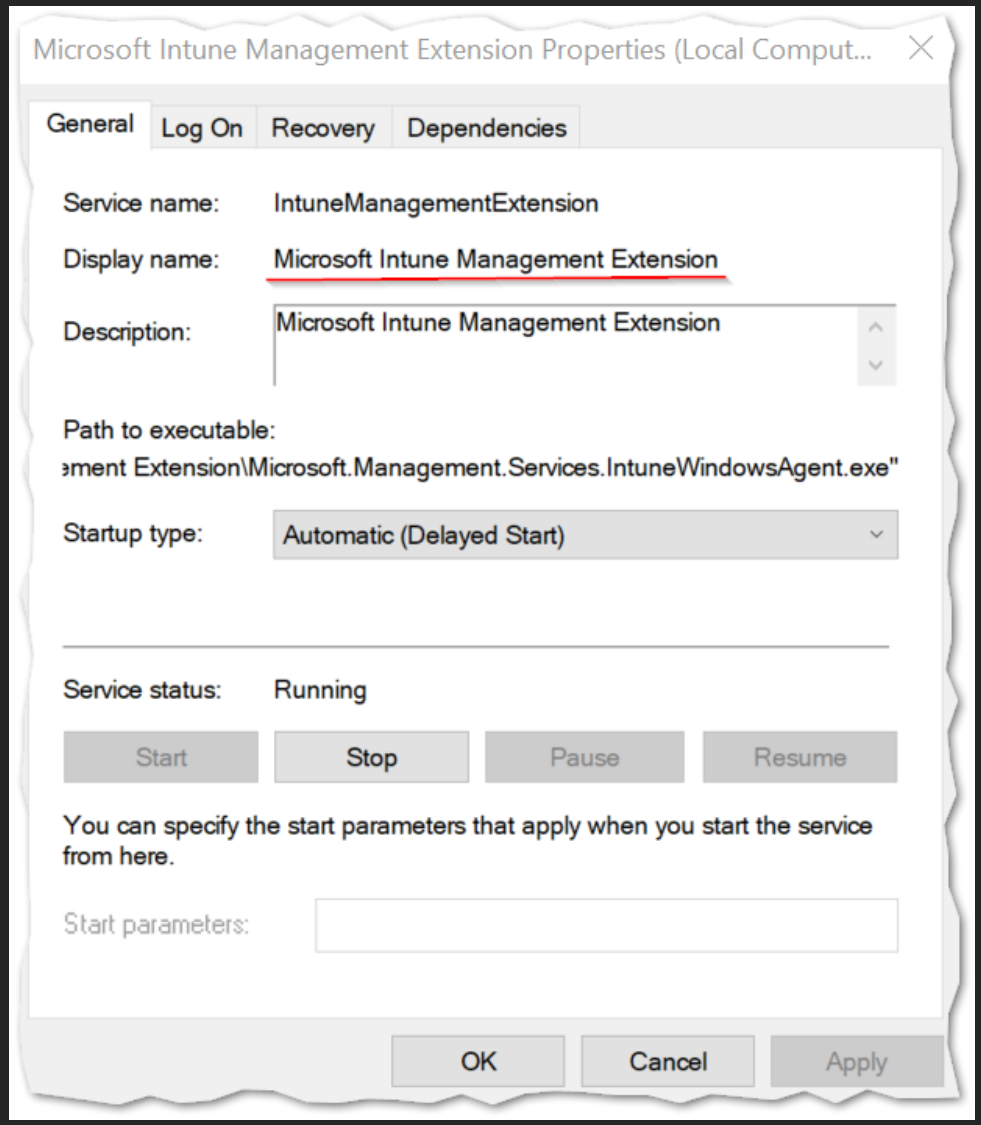
- Yellow: IME Root Registry Key
- Green: Azure AD Object ID of the User
- Red: Application / Policy GUID



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



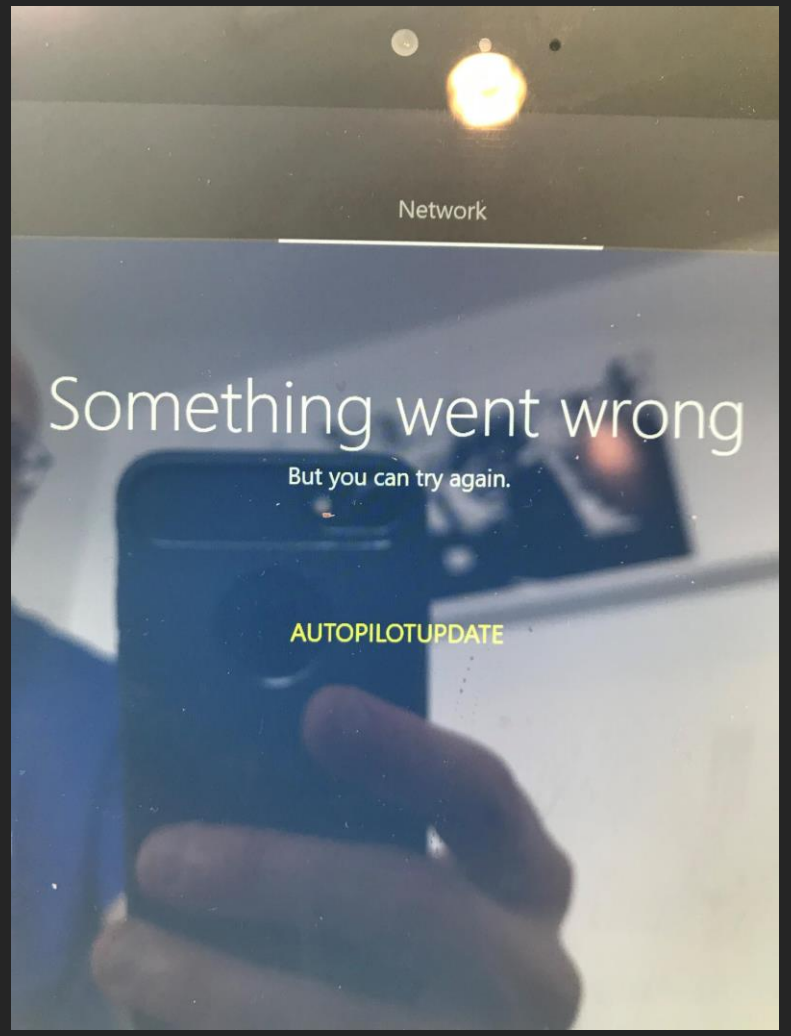
Thank You!!

NORDIC
— VIRTUAL SUMMIT —

Windows AutoPilot

Network

- A network for enrollment is needed
- Guest network, open network
- All ports, URL required and must be open



Network issues

- Pie-Hole blocking all traffic to Microsoft URLs used.
- Home routers/Wi-Fi with IPS.

“My son setup our home network, no idea what he did”.

“It is a different organization name showing up when I start my computer”.

Shift+F10

- Great for troubleshooting
  - Can be a security concern for some customers

- Disable by placing **DisableCMDRequest.TAG** in the **C:\Windows\Setup\Scripts** folder.
  - Needs to be there when the computer starts up. Must be added by OEM.

Licensing

NORDIC
– VIRTUAL SUMMIT –

- User must have the appropriate license assigned
  - Microsoft Intune + Azure AD Premium
  - Enterprise Mobility + Security (EMS) E3/E5
  - Microsoft 365 Business Premium
  - Microsoft 365 E3 / E5

- Azure AD Premium P1/P2 is required for Automatic enrollment

NORDIC
– VIRTUAL SUMMIT –

Troubelshooting

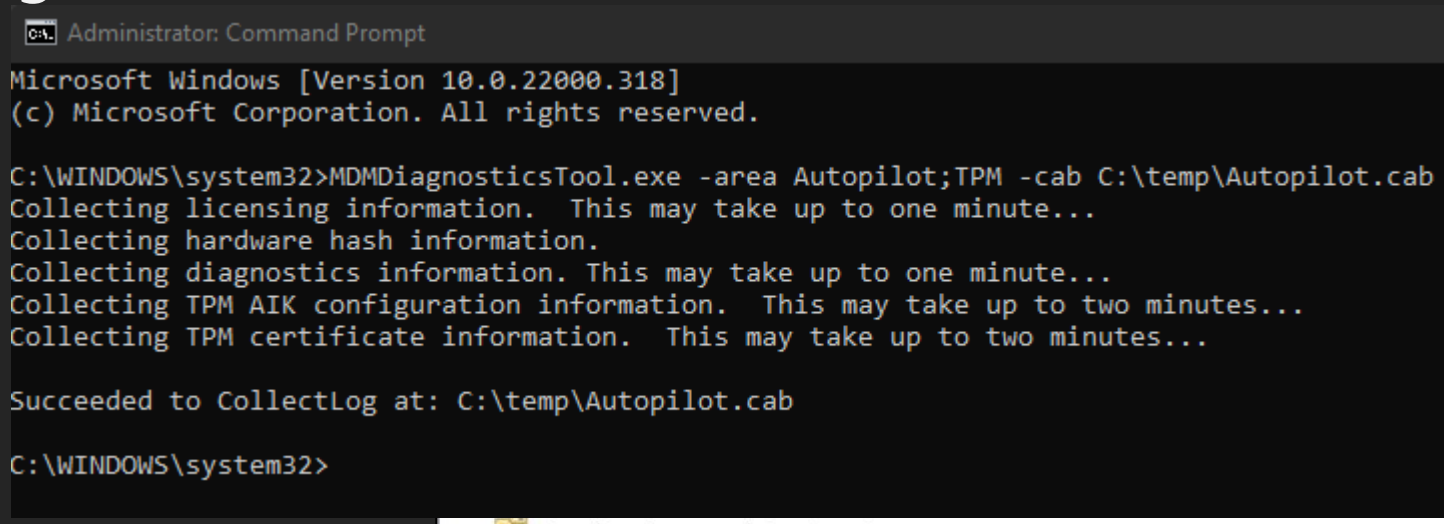
Troubleshooting on Windows 10

NORDIC
– VIRTUAL SUMMIT –

- Grab all potentially-interesting information:
  - Event logs
  - Registry, configuration data
  - TPM details (1809+)
  - ETL trace files

- Windows 10/11
  - MDMDiagnosticsTool.exe -area Autopilot;TPM -cab C:\temp\Autopilot.cab

- Analyze offline



Windows Autopilot Win32 Error Codes

- 8007 : Win32 errors (network, etc.)
  - 0x800705B4 = timeout
  - 0x80070774 = domain controller not found
- 801C : Azure AD join / device registration
  - 0x801C0003 = device authorization error (not authorized to join AAD, exceeded device limit)
- 8018 : MDM enrollment
  - 0x80180003 = authorization error (user not authorized to enroll)
  - 0x80180005 = server error (enrollment rejected, scenario not enabled, etc.)
  - 0x80180014 = device not supported (enrollment restriction)
  - 0x80180018 = no user license (AAD Premium or Intune)
- 8000: Windows errors
  - 0x80004005 = generic error (fail)

Account

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.

Offline account

Try again

Account

Something went wrong.

There was an error with your license. You can try to do this again or contact your system administrator with the error code 80180018.

Offline account

Try again

NORDIC
– VIRTUAL SUMMIT –

- Still have problems?

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...