

TROUBLESHOOTING A MEM MANAGED WINDOWS 10/11

RONNI PEDERSEN

CoLABORA – JANUARY 2022

SPEAKER



RONNI PEDERSEN

CLOUD ARCHITECT

- MICROSOFT MVP: ENTERPRISE MOBILITY (14 YEARS)
- MCSE/MCSA/MCITP/MCTS (+75 CERTIFICATIONS)
- ITIL FOUNDATION CERTIFIED
- MICROSOFT CERTIFIED TRAINER (MCT)

CONTACT INFO

- MAIL: ROP@APENTO.COM
- PHONE: +45 20 85 94 52
- TWITTER: [@RONNIPEDERSEN](https://twitter.com/ronnipederesen)



TAKEAWAYS

- TOOLS
- THE LOG FILES
- CONFIGURATION POLICY PROCESS
- SUBSCRIPTION BASED ACTIVATION
- TROUBLESHOOTING POLICIES

REMOTE CONTROL

- 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.



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](#).

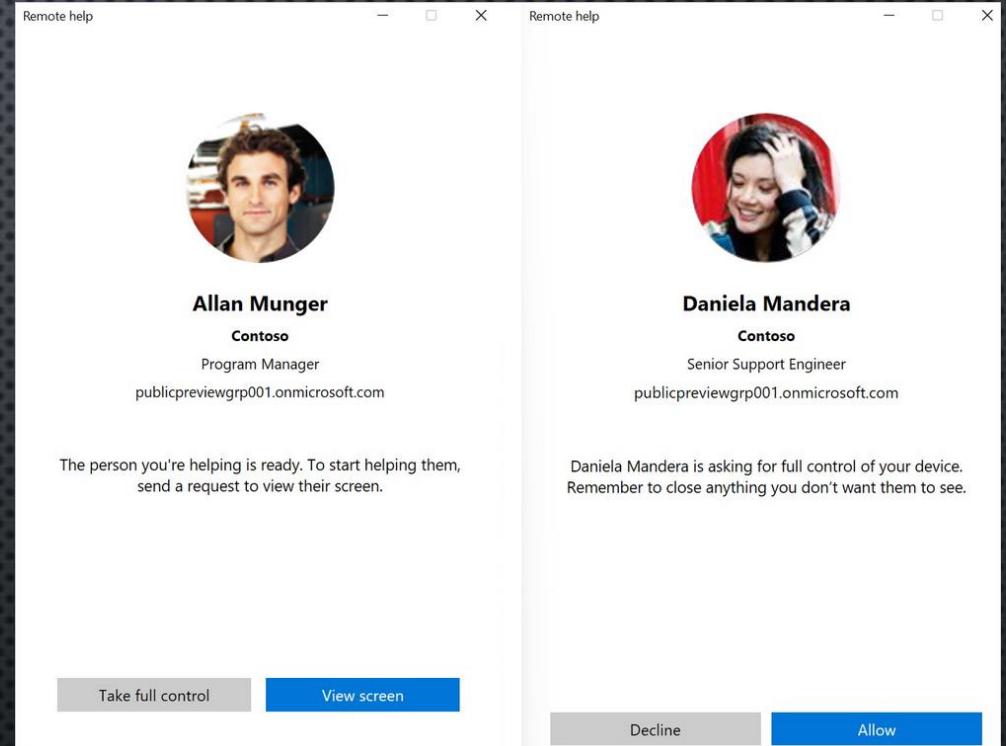
Next



REMOTE HELP (ANNOUNCED AT IGNITE)

- SUPPORT UAC
- RBAC
- LOGGING/TRACKING

The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left, there's a navigation sidebar with options like Home, Dashboard, All services, Favorites (Devices selected), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area shows a device named 'DESKTOP-4B8CR16'. The 'Overview' tab is selected. A 'New remote assistance session' dialog box is open, prompting the user to 'Launch remote help'. The device details shown include Device name (DESKTOP-4B8CR16), Management name (IWUser0_Windows_10/19/2021_11:54 PM), Ownership (Personal), Serial number (3563-4946-8798-5853-3670-1069-96), Phone number (---), and a 'See more' link. Below this, there's a 'Device actions status' table with columns for Action, Status, and Data, showing 'No data'.



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

LOG FILES

COLLECT DIAGNOSTICS FROM A WINDOWS DEVICE

- 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](https://docs.microsoft.com/en-us/mem/intune/remote-actions/collect-diagnostics)



COLLECTING DIAGNOSTIC LOGS

The screenshot shows the Microsoft Intune Device Overview page for a device named "DESKTOP-NIIRT6B". The page includes a navigation bar with links like Home, Windows, Overview, and a search bar. The main content area displays device details such as Device name, Management name, Ownership, Serial number, Phone number, Primary user, Enrolled by, Compliance, Operating system, and Device model. Below this, there's a "Device actions status" table and a "Device diagnostics (preview)" section.

1 The "Collect diagnostics" button in the top navigation bar is highlighted with a red box.

2 In the "Device actions status" table, the row for "Collect diagnostics" is highlighted with a red box. The table has columns for Action, Status, Date/Time, and Error. The entry is: Action: Collect diagnostics, Status: Complete, Date/Time: 5/16/2021, 8:18:21 AM, Error: None.

3 The "Device diagnostics (preview)" link in the left sidebar is highlighted with a red box.

Device diagnostics (preview)

Requested by	Status ↑↓	Request initiated ↑↓	Diagnostics uploaded ↑↓	Diagnostics
rop@apento.com	Complete	5/16/2021, 8:18:07 AM	5/16/2021, 8:28:57 AM	Download

CONFIGURATION POLICY PROCESS

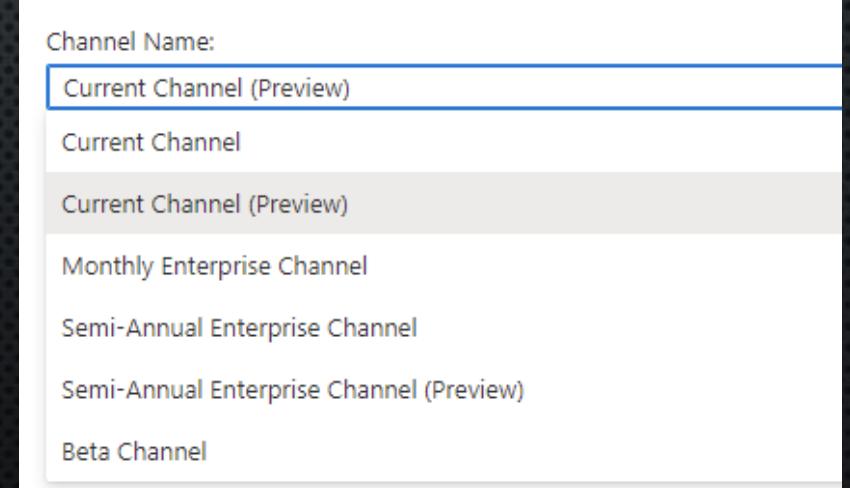
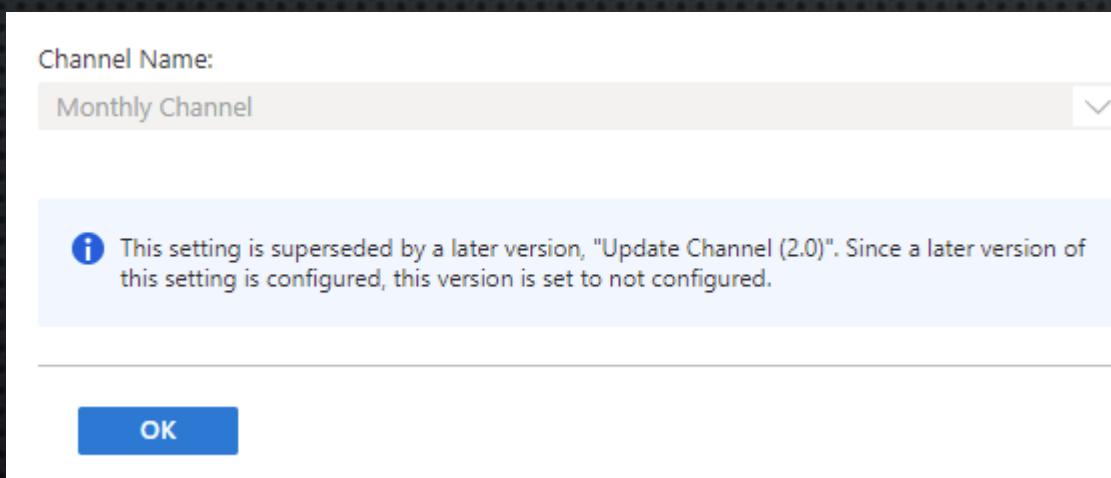
MICROSOFT 365 APPS POLICY

- 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

Update Deadline	Not configured	Device	\Microsoft Office 2016 (Machine)\Updates
Update Channel (2.0)	Enabled	Device	\Microsoft Office 2016 (Machine)\Updates
Update Channel (1.0)	Not configured	Device	\Microsoft Office 2016 (Machine)\Updates
Target Version	Not configured	Device	\Microsoft Office 2016 (Machine)\Updates



USING SETTINGS CATALOG (PREVIEW)

- POLICY CONFIGURATION:
 - ENABLE MICROSOFT 365 APPS AUTOMATIC UPDATES
 - SET THE UPDATE CHANNEL

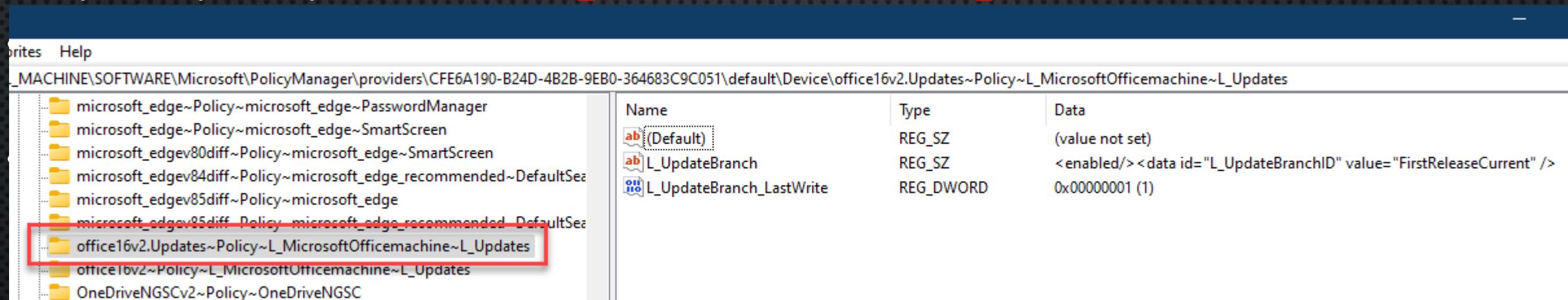
The screenshot shows the 'Configuration settings' step of the Settings Catalog wizard. It displays a list of settings under the 'Updates' category for 'Microsoft Office 2016 (Machine)'. The 'Enable Automatic Updates' setting is enabled, and the 'Update Channel' setting is also enabled. A note indicates that 14 of 16 settings in the 'Updates' subcategory are not configured.

Setting	Status	Action
Enable Automatic Updates	Enabled	Remove
Update Channel	Enabled	Remove
Channel Name: (Device) *	Current Channel (Preview)	Remove

#1 CHECK THE INTUNE REGISTRY KEYS

- 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

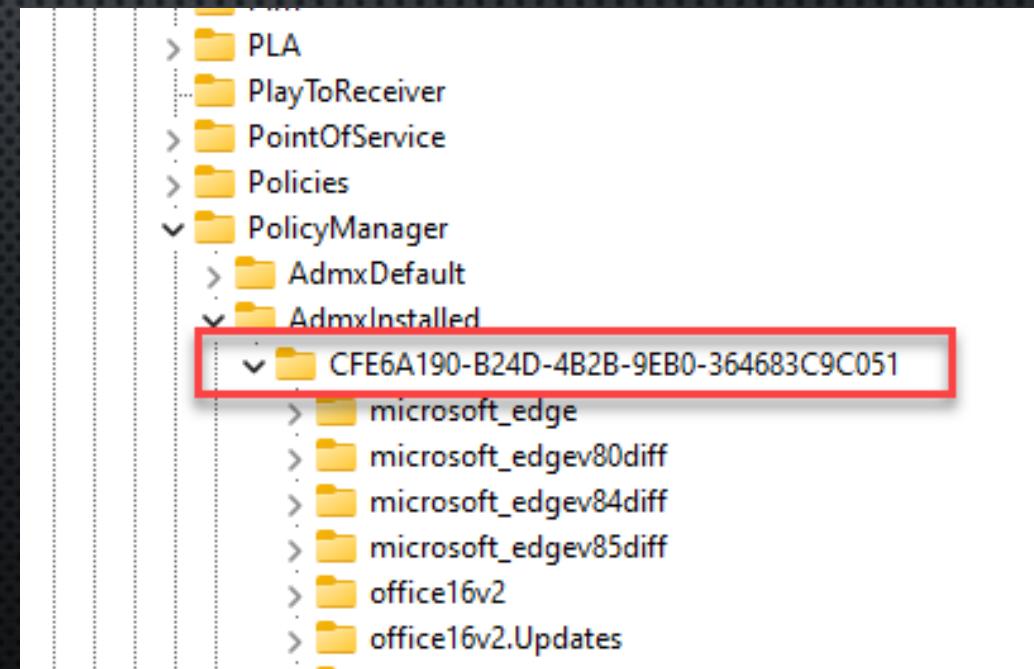


#TIP: FIND THE PROVIDER ID

FIND THE PROVIDER ID FOR YOUR DEVICE

- OPEN THE REGISTRY EDITOR, AND GO TO:

COMPUTER\HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\POLICYMANAGER\ADMXINSTALLED



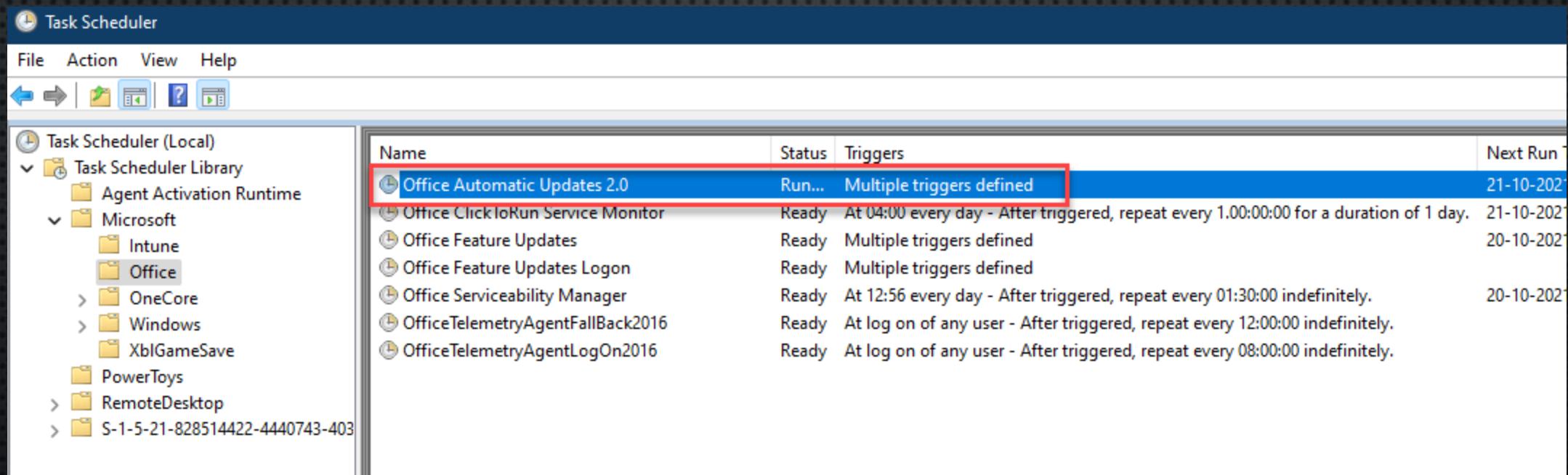
#2 CHECK THE OFFICE REGISTRY KEYS

- 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

<code>ab_SCLCacheOverride</code>	<code>REG_SZ</code>	0
<code>ab_SharedComputerLicensing</code>	<code>REG_SZ</code>	0
<code>ab_StreamingFinished</code>	<code>REG_SZ</code>	True
<code>ab_StreamPackageUrlChanged</code>	<code>REG_SZ</code>	True
<code>ab_TearnsUpdate</code>	<code>REG_SZ</code>	INSTALLED
<code>ab_UpdateChannel</code>	<code>REG_SZ</code>	http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-8936-8840a6a4f5be
<code>ab_UpdateChannelChanged</code>	<code>REG_SZ</code>	False
<code>ab_UpdatesEnabled</code>	<code>REG_SZ</code>	True
<code>ab_VersionToReport</code>	<code>REG_SZ</code>	16.0.14527.20268
<code>ab_VisioProRetail.ExcludedApps</code>	<code>REG_SZ</code>	groove
<code>ab_Win32_PatchInstallTime</code>	<code>REG_SZ</code>	SPN

#3 FORCE OFFICE AUTOMATIC UPDATES TO RUN

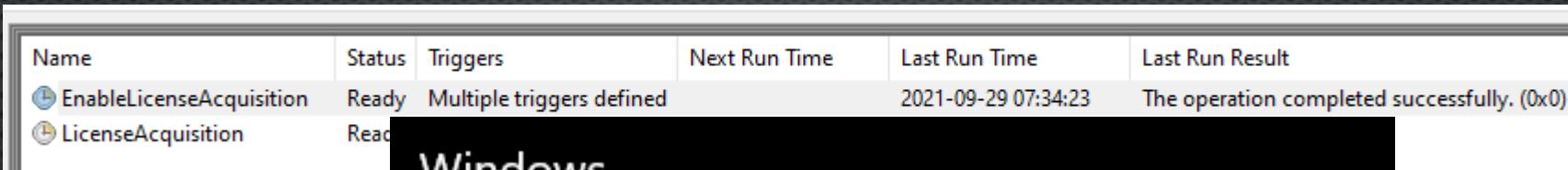
- TO TEST THE POLICY, WE CAN FORCE THE POLICY SETTINGS ON THE DEVICE
 - Go to HKLM\SOFTWARE\MICROSOFT\OFFICE\CLICKTORUN\UPDATES
 - EDIT THE UPDATEDETECTIONLASTRUNTIME KEY > DELETE THE VALUE DATA.
 - LAUNCH TASK SCHEDULER > MICROSOFT > OFFICE
 - RUN “OFFICE AUTOMATIC UPDATES 2.0”



TROUBLESHOOTING SUBSCRIPTION BASED ACTIVATION

SUBSCRIPTION BASED ACTIVATION

- RE-ACTIVATED EVERY 30 DAYS
- TWO SCHEDULED TASKS TRIGGERS LICENSE ACQUISITION



The screenshot shows the Windows Task Scheduler interface. It lists two tasks:

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
EnableLicenseAcquisition	Ready	Multiple triggers defined		2021-09-29 07:34:23	The operation completed successfully. (0x0)
LicenseAcquisition	Ready				

Below the task list, a modal window titled "Windows" displays system information:

Edition	Windows 10 Pro
Subscription	Windows 10 Enterprise subscription is not valid.
Activation	Windows is activated with a digital license

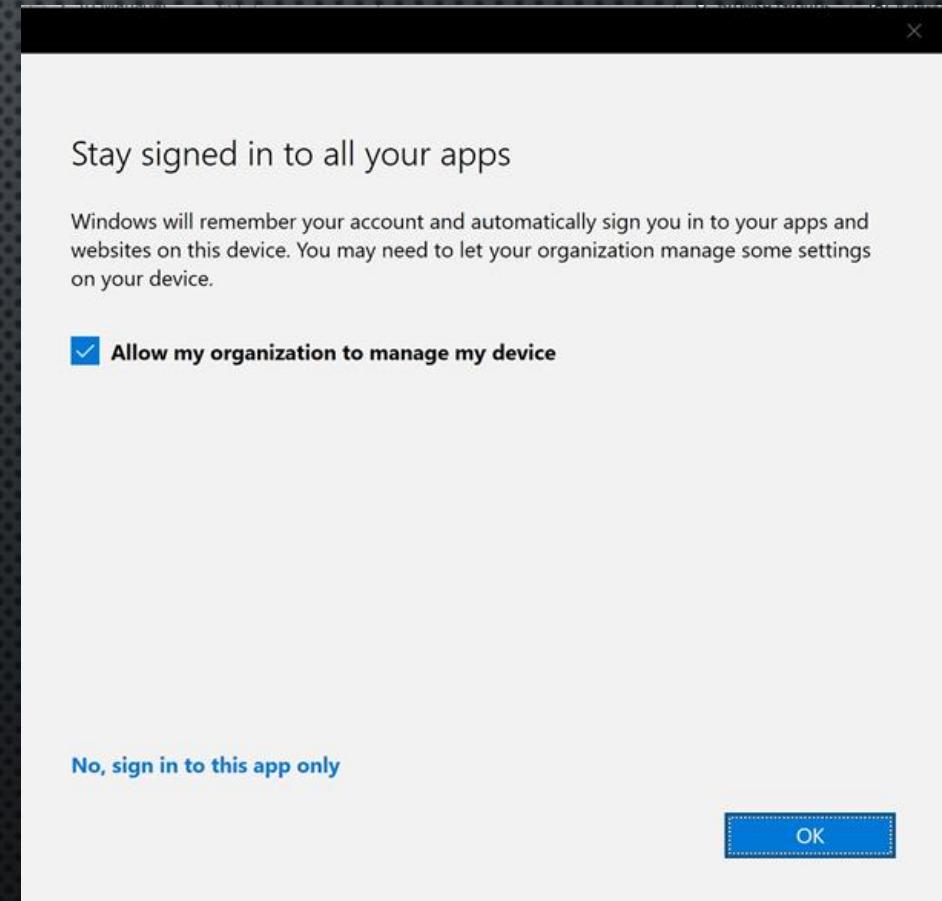
A "Learn more" link is present under Activation.

At the bottom of the modal, a detailed error message is shown:

```
Service Fault: status: 400 conflict
in the request are expected to be associated to a single tenant. data[{"$": "com
Svr: ent: ), token broker error: 0x00000000, number of MSA tickets: 1, number of AAD
tickets: 3
Function: LogServiceFault
Source: onecoreuap\enduser\winstore\licensemanager\lib\telemetry.cpp (134)
```

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

Create profile ...

Windows 10 and later - Settings catalog (preview)

Basics Configuration settings Assignments Scope tags

+ Add settings

Settings

11 of 12 settings in this category are not configured

Allow Workplace ⓘ Block

Settings picker

Use commas "," among search terms to lookup settings by their keywords

Search

workpla

+ Add filter

Browse by category

Administrative Templates\Start Menu and Taskbar

Administrative Templates\System\Group Policy

Settings

1 results in the "Settings" category

Select all these settings

Setting name

Allow Workplace ⓘ

TROUBLESHOOTING POLICIES

DEVICE SETTINGS IN MICROSOFT INTUNE

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

EXISTING DEVICES

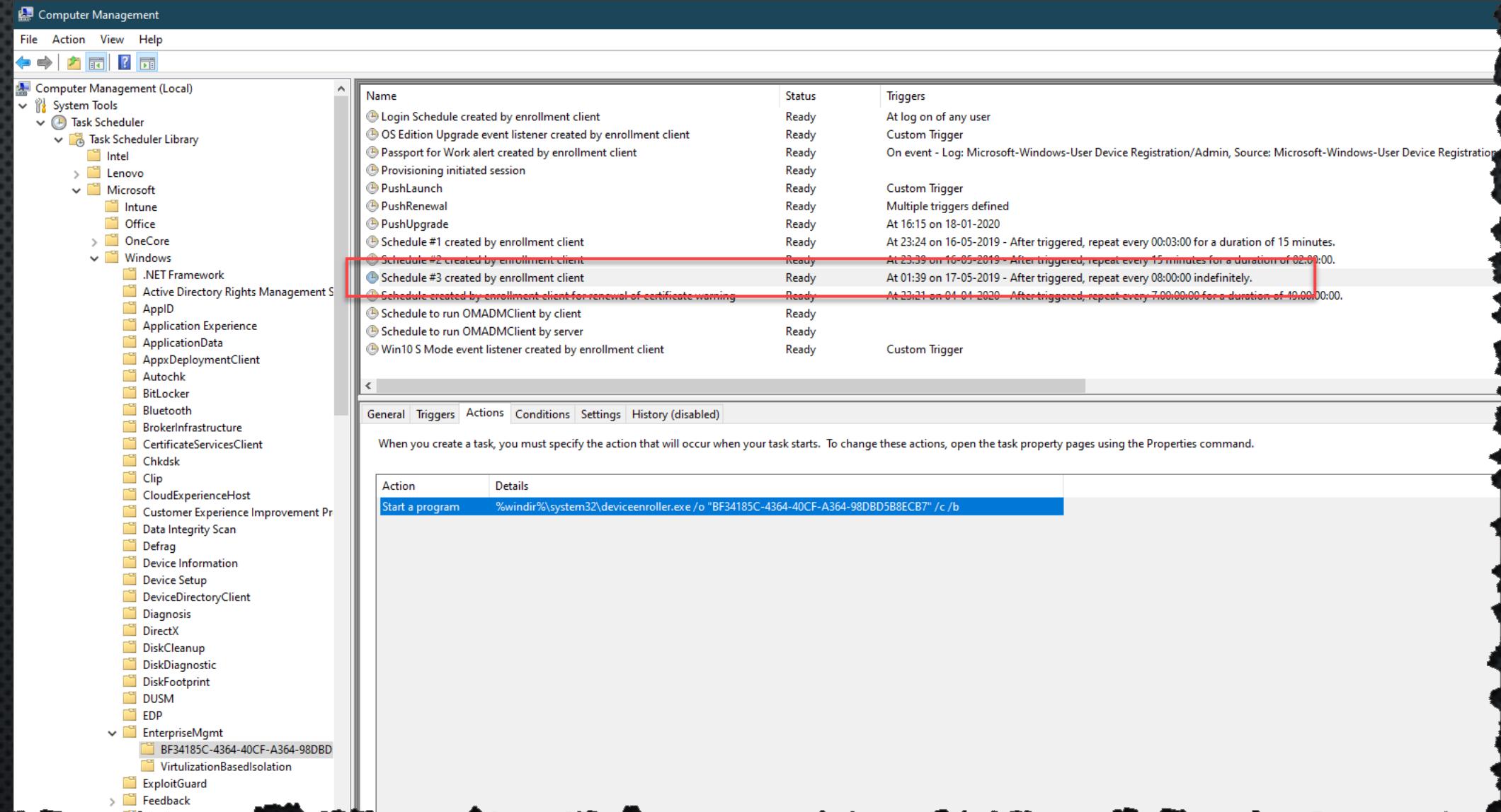
- WINDOWS 10/11 DEVICES WILL SCHEDULE CHECK-IN WITH THE INTUNE SERVICE, WHICH IS ESTIMATED AT: ABOUT EVERY 8 HOURS

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



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 “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



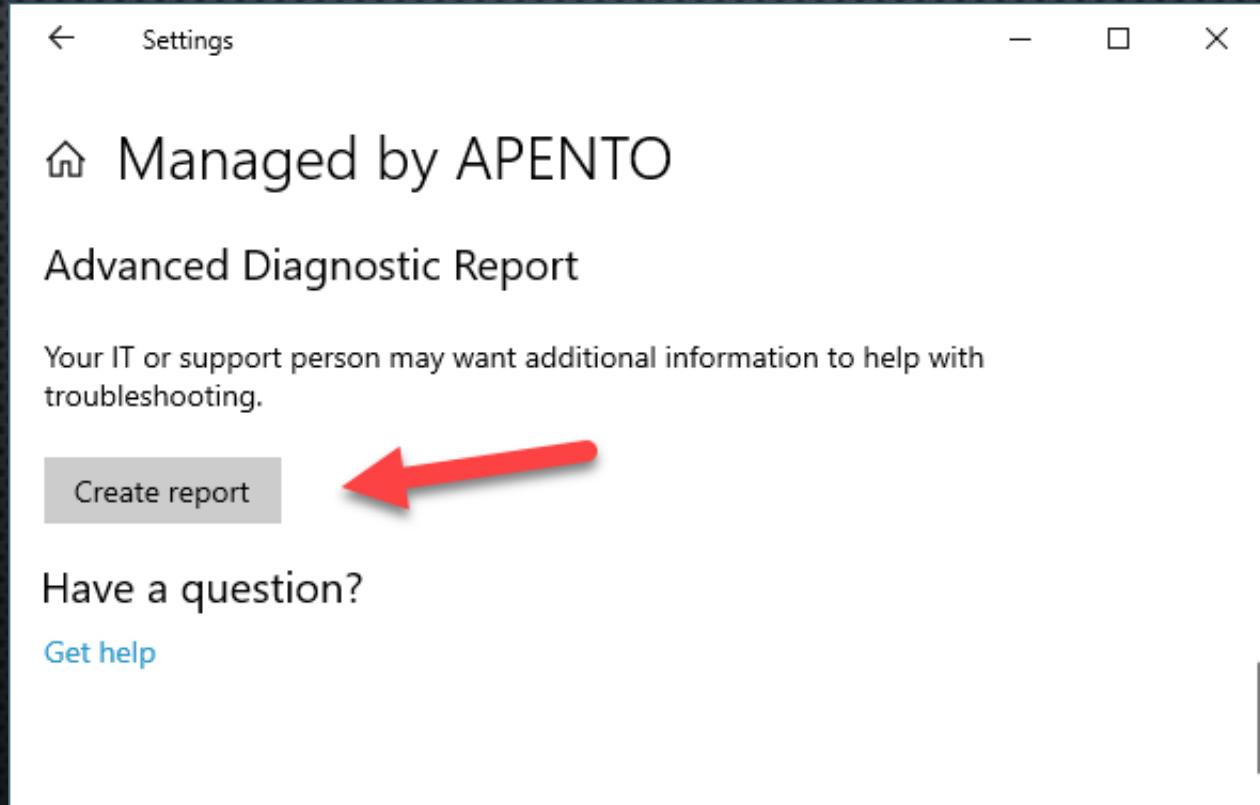
POLICY/PROFILE CONFLICTS

- 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=<enable d/><data id="EncryptionMethodWithXtsOsDropDown_Name" value="7"/><data id="EncryptionMethodWithXt sFdvDropDown_Name" value="7"/><data id="Encrypti onMethodWithXtsRdvDropDown_Name" value="7"/>
BitLocker	SystemDrivesRecoveryOptions			device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=<enable d/><data id="OSAllowDRA_Name" value="true"/><dat a id="OSRecoveryPasswordUsageDropDown_Name" val ue="2"/><data id="OSRecoveryKeyUsageDropDown_N ame" value="2"/><data id="OSHideRecoveryPage_N ame" value="false"/><data id="OSActiveDirectoryBackup_ Name" value="true"/><data id="OSActiveDirectoryBack upDropDown_Name" value="1"/><data id="OSRequire ActiveDirectoryBackup_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	LowClipboardProtection	1		device		BF34185C-4364-40CF-A364-98DBD5B8ECB7=1

INTUNE TROUBLESHOOTING PANE

- INTUNE PORTAL PAGE
 - [HTTPS://AKA.MS/INTUNETROUBLESHOOTING](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](https://docs.microsoft.com/en-us/intune/help-desk-operators)

The screenshot shows the Microsoft Intune - Troubleshoot pane. At the top, it displays the user's account status as "Active". Below that, it shows the user's display name, principal name, and email. There is a "Change" button for the display name. On the left, there is a sidebar with various navigation links: Device compliance, Device configuration, Devices, Client apps, Device security, eBooks, Conditional access, Exchange access, Users, Groups, Roles, Software updates, Monitoring, Diagnostics settings, Help and support (with a link to "ip-desk-operators#enrollment-failure-reference"), Tenant Status, and Troubleshoot (which is currently selected). The main area is divided into two sections: "ASSIGNMENTS" and "DEVICES". The "ASSIGNMENTS" section shows a table of client app assignments, including columns for Assignment ID, Name, OS, Type, and Last Modified. The "DEVICES" section shows a table of devices, including columns for Device ID, MDM, OS, Corp..., and Last Sync.

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

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

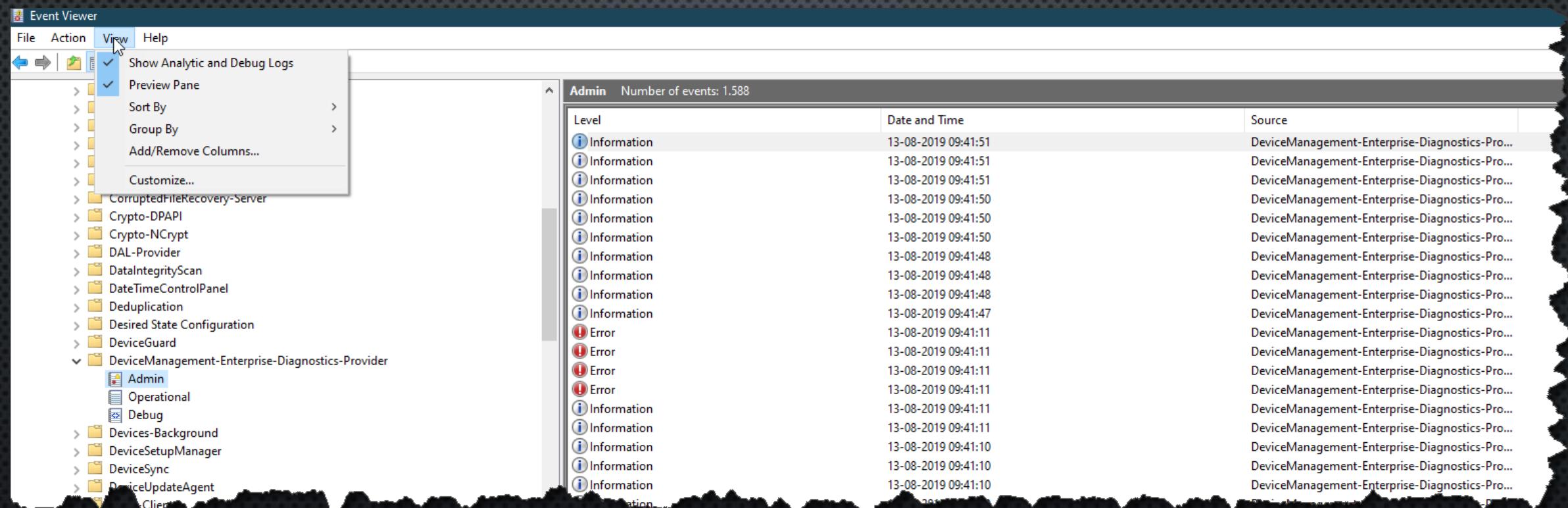
DEVICE PROFILES - WHERE IS MY LOGS?

- EVENT VIEWER IS YOUR NEW BEST FRIEND
 - MICROSOFT-WINDOWS-DEVICEMANAGEMENT-ENTERPRISE-DIAGNOSTICS-PROVIDER

The screenshot shows the Windows Event Viewer interface. On the left, there is a navigation pane with a tree view of event sources. The 'DeviceManagement-Enterprise-Diagnostics-Provider' source is expanded, showing its 'Admin' and 'Operational' log levels. On the right, the main pane displays a table of events. The table has three columns: 'Level', 'Date and Time', and 'Source'. The 'Level' column uses icons to represent event types: blue for Information and red for Error. The 'Source' column lists 'DeviceManagement-Enterprise-Diagnostics-Pro...' repeated multiple times. The table shows approximately 1588 events. A single error event from the 'Admin' log is highlighted with a blue selection bar, and its details are visible in the bottom pane.

Level	Date and Time	Source
Information	13-08-2019 09:41:51	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:51	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:51	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:50	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:50	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:50	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:48	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:48	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:48	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:47	DeviceManagement-Enterprise-Diagnostics-Pro...
Error	13-08-2019 09:41:11	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:11	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:11	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:10	DeviceManagement-Enterprise-Diagnostics-Pro...
Information	13-08-2019 09:41:08	DeviceManagement-Enterprise-Diagnostics-Pro...

ENABLE DEBUG MODE



INTUNE MANAGEMENT EXTENSION

INTUNE MANAGEMENT EXTENSION PRE-REQUISITES

- 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?

- 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

- APPLICATIONS AND SERVICES LOGS\MICROSOFT\WINDOWS\DEVICEMANAGE...

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists various logs under 'File and Services Logs'. A red box highlights the 'DeviceManagement-Enterprise-Diagnostics-Provider' log, and a red arrow points from it to the main pane. The main pane displays a table of events for the 'Admin' category. A red box surrounds the entire table header and the first few rows. A blue callout bubble with the text 'Look for event id 1924' points to the last event in the list, which is also highlighted with a red box. The event details show an error message about an application install failing.

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	None
Error	03/02/2020 12.02.23	Device...	404	None
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

Event 1924, DeviceManagement-Enterprise-Diagnostics-Provider

General Details

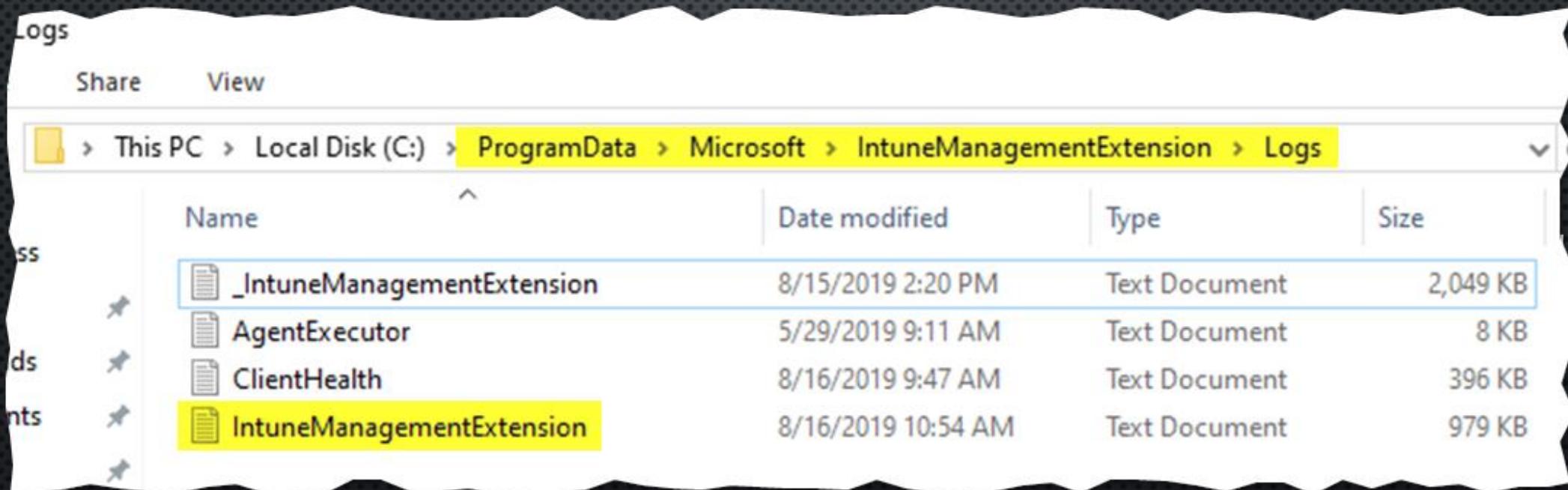
EnterpriseDesktopAppManagement CSP: An application install has failed. Examine the MSI log (C:\WINDOWS\system32\config\systemprofile\AppData\Local\mdm\093ea47b-ef2c-4f46-a022-6f57a50e39a2.log) for more details. Install command: ("C:\WINDOWS\system32\msiexec.exe" /quiet /l*v "C:\WINDOWS\system32\config\systemprofile\AppData\Local\mdm\093ea47b-ef2c-4f46-a022-6f57a50e39a2.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-0-0-0-000000000-000000000-000000000-000), Result: (Fatal error during installation.).

INTUNE MANAGEMENT EXTENSION FILE SYSTEM

The screenshot shows the Windows File Explorer interface displaying the contents of the Microsoft Intune Management Extension folder. The left pane shows a navigation tree: Local Disk (C:) > Program Files (x86) > Microsoft Intune Management Extension > Content. The right pane is a detailed list view with columns: Name, Date modified, Type, and Size. The list includes several folders and files, such as DetectionScripts, Incoming, Staging, and various language sub-folders (fi, fr, hu, it, ja, ko, nl, no, pl, pt-br, ro, ru, sv, tr, zh-HANS, zh-HANT). It also lists AgentExecutor, ClientHealthEval, and other configuration files.

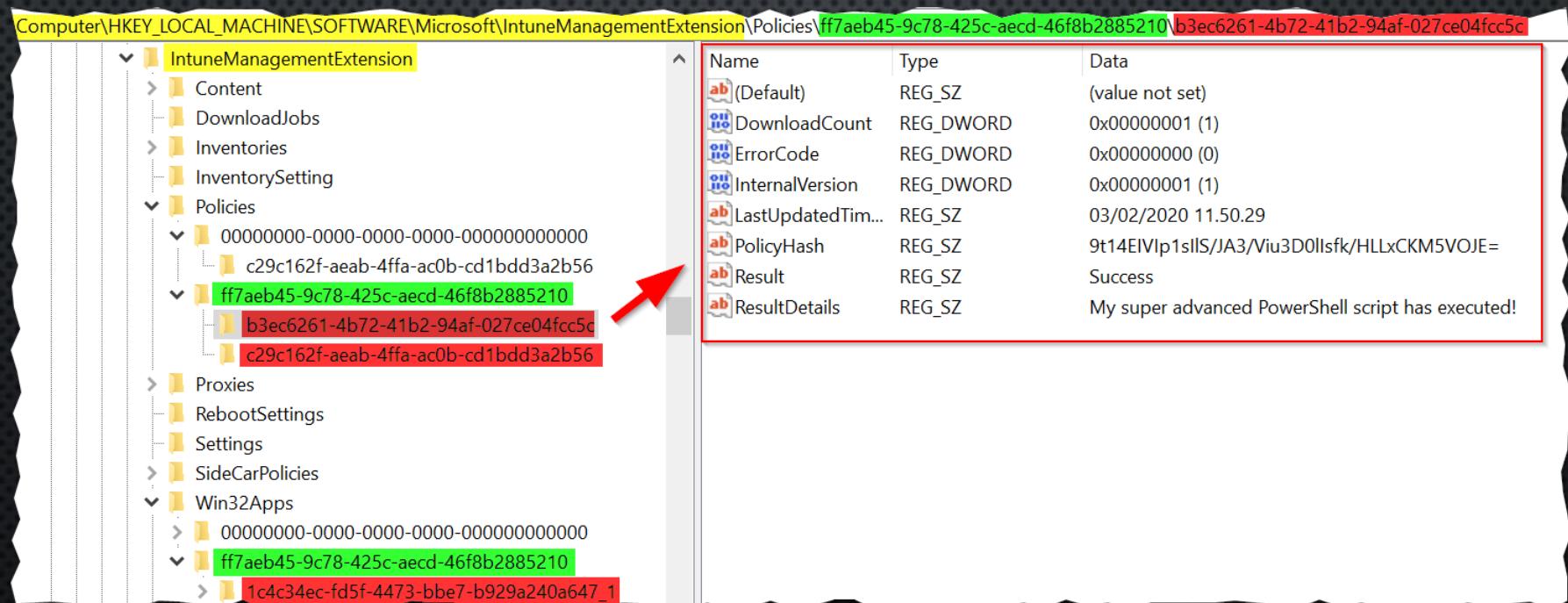
Name	Date modified	Type	Size
DetectionScripts	8/16/2019 9:07 AM	File	
Incoming	5/29/2019 10:11 AM	File	
Staging	5/29/2019 10:11 AM	File	
fi	18-07-2019 08:51	File folder	
fr	18-07-2019 08:51	File folder	
hu	18-07-2019 08:51	File folder	
it	18-07-2019 08:51	File folder	
ja	18-07-2019 08:51	File folder	
ko	18-07-2019 08:51	File folder	
nl	18-07-2019 08:51	File folder	
no	18-07-2019 08:51	File folder	
pl	18-07-2019 08:51	File folder	
Policies	16-05-2019 23:23	File folder	
pt-br	18-07-2019 08:51	File folder	
ro	18-07-2019 08:51	File folder	
ru	18-07-2019 08:51	File folder	
sv	18-07-2019 08:51	File folder	
tr	18-07-2019 08:51	File folder	
zh-HANS	18-07-2019 08:51	File folder	
zh-HANT	18-07-2019 08:51	File folder	
AgentExecutor	11-07-2019 17:10	Application	52 KB
AgentExecutor.exe.config	06-05-2019 10:29	CONFIG File	1 KB
ClientHealthEval	11-07-2019 17:10	Application	51 KB
ClientHealthEval.exe.config	06-05-2019 10:29	CONFIG File	1 KB
concrt140.dll	20-01-2017 14:20	Application exten...	239 KB
HealthCheck	06-05-2019 10:29	XML Document	3 KB
HealthReport.json	13-08-2019 07:43	JSON File	1 KB
ImeUI	11-07-2019 17:10	Application	22 KB
ImeUI.exe.config	06-05-2019 10:29	CONFIG File	1 KB

INTUNE MANAGEMENT EXTENSION LOG FILES



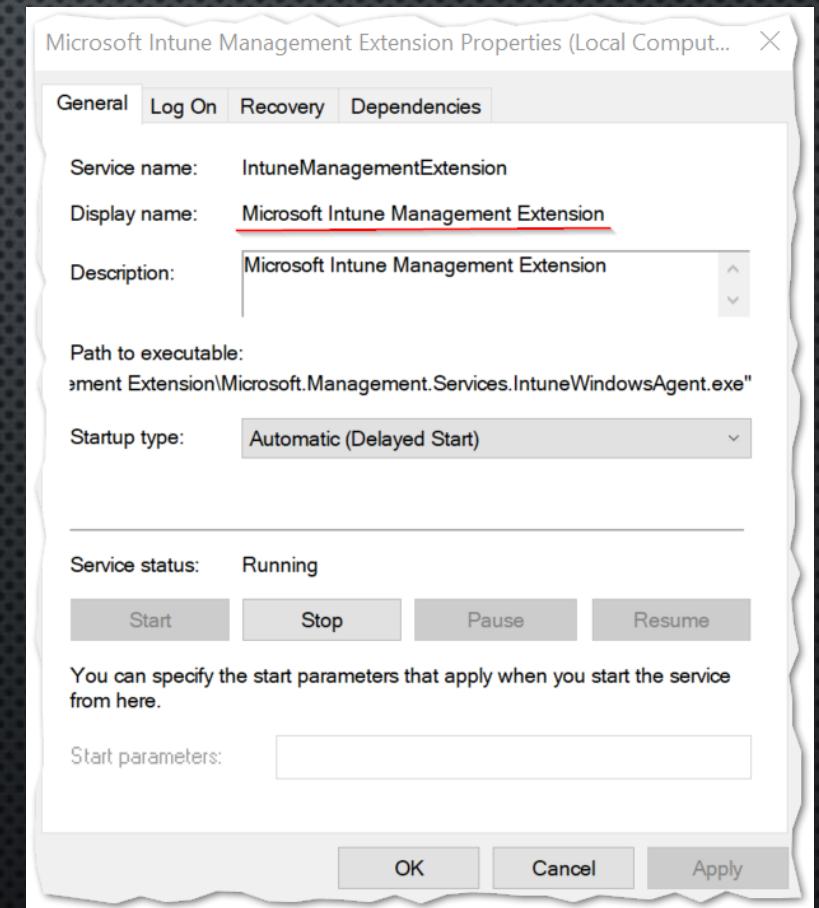
INTUNE MANAGEMENT EXTENSION THE REGISTRY

- **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>

QUESTIONS ?