#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 -





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



- 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







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





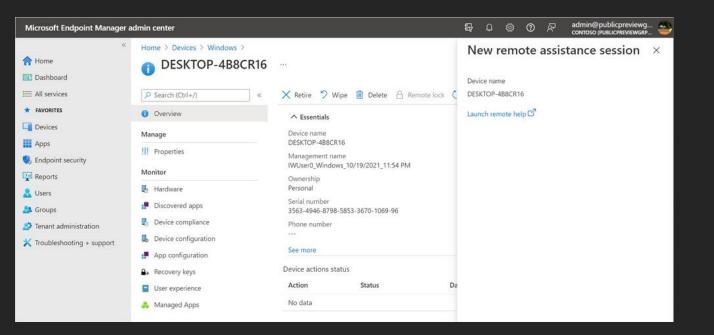


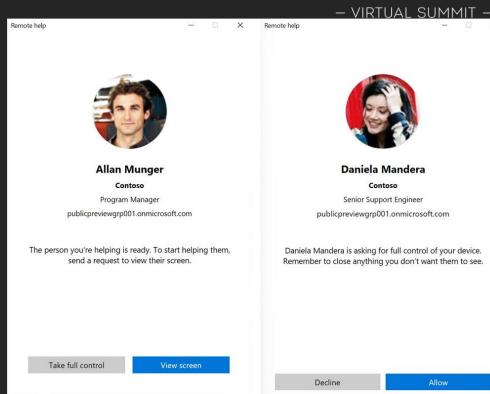
Remote Help (Announced at Ignite)

NORDIC - VIRTUAL SUMMIT -

- 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

NORDIC - VIRTUAL SUMMIT -

- Wireshark
- Fiddler
- Netmon
- SyncMLViewer

```
SyncML Viewer - oliverkieselbach.com - 1.0.7
                                                                                                                                File Options Actions Help
SyncML Representation Protocol Stream SyncML Sessions/Messages Response Status Codes Reference MDM Diagnostics About
      -- OmaDmSessionStart -->
  3 <!-- 8/31/2021 9:03:03 PM -->
  4 <SyncML xmlns="SYNCML:SYNCML1.2">
      <SvncHdr>
        <VerDTD>1.2</VerDTD>
        <VerProto>DM/1.2</VerProto>
        <SessionID>30</SessionID>
        <MsgID>1</MsgID>
 11
          <LocURI>https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx</LocURI>
 12
        </Target>
 13
        <Source>
          <LocURI>8A39C151B9A1CC59557F513B7C0E9DFA3E8C03268E259C3126346B7668E8EA2B/LocURI>
 15
          <LocName>dummy</LocName>
 16
        </Source>
 17
        <Cred>
 18
            <Format xmlns="syncml:metinf">b64</Format>
 19
 20
            <Type xmlns="syncml:metinf">syncml:auth-md5</Type>
 21
 22
           <Data>EVEkoFZcVgPM+ESnu9IC0g==
 23
        </Cred>
      </SyncHdr>
       <SyncBody xmlns:msft="http://schemas.microsoft.com/MobileDevice/MDM">
 26
        <Alert>
 27
          <CmdID>2</CmdID>
 28
          <Data>1201</Data>
 29
        </Alert>
 30
        <Alert>
 31
          <CmdID>3</CmdID>
          <Data>1224</Data>
                                                                                                               Clear Stream
                                                                                                                               Save As
```



```
1533
      <Status>
1534
       <CmdID>32</CmdID>
1535
       <MsgRef>2</MsgRef>
1536
       <CmdRef>25</CmdRef>
1537
       <Cmd>Get</Cmd>
1538
        <Data>200</Data>
1539
      </Status>
1540
      <Results>
       <CmdID>33</CmdID>
1541
       <MsgRef>2</MsgRef>
1542
       <CmdRef>25</CmdRef>
1543
1544
        <Item>
1545
         <Source>
          <LocURI>./DevDetail/Ext/DeviceHardwareData</LocURI>
1546
1547
         </Source>
         1548
1549
       </Item>
      </Results>
1550
      <Status>
1551
       <CmdID>34</CmdID>
1552
       <MsgRef>2</MsgRef>
1553
       <CmdRef>26</CmdRef>
1554
```

```
SyncML xmlns="SYNCML:SYNCML1.2" xmlns:A="syncml:metinf">
   <SyncHdr>
     <VerDTD>1.2</VerDTD>
     <VerProto>DM/1.2</VerProto>
     <SessionID>120</SessionID>
     <MsgID>6</MsgID>
     <Target>
       <LocURI>8A39C151B9A1CC59557F513B7C0E9DFA3E8C03268E259C3126346B7668E8EA2B/LocURI>
     </Target>
     <Source>
       <LocURI>https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx</LocURI>
     </Source>
     <Meta>
       <A:MaxMsgSize>524288</A:MaxMsgSize>
     </Meta>
   </SyncHdr>
   <SyncBody>
     <Status>
       <CmdID>1</CmdID>
       <MsgRef>6</MsgRef>
       <CmdRef>0</CmdRef>
       <Cmd>SyncHdr</Cmd>
       <Data>200</Data>
     </Status>
     <Replace>
       <CmdID>2</CmdID>
       <Item>
         <Target>
           <LocURI>./Vendor/MSFT/NodeCache/MS%20DM%20Server/Nodes/4929/NodeUri</LocURI>
         <Data>./cimv2/MDM_WebApplication/MDM_WebApplication.PackageName=CCMEXEC%20-%20Not%20Managed/PackageUrl</Data>
       </Item>
     </Replace>
     <Replace>
       <CmdID>3</CmdID>
       <Item>
         <Target>
           <LocURI>./Vendor/MSFT/NodeCache/MS%20DM%20Server/Nodes/4929/ExpectedValue</LocURI>
         </Target>
         <Data>https://ccmexec.com/</Data>
```





Log Files

Collect diagnostics from a Windows Device

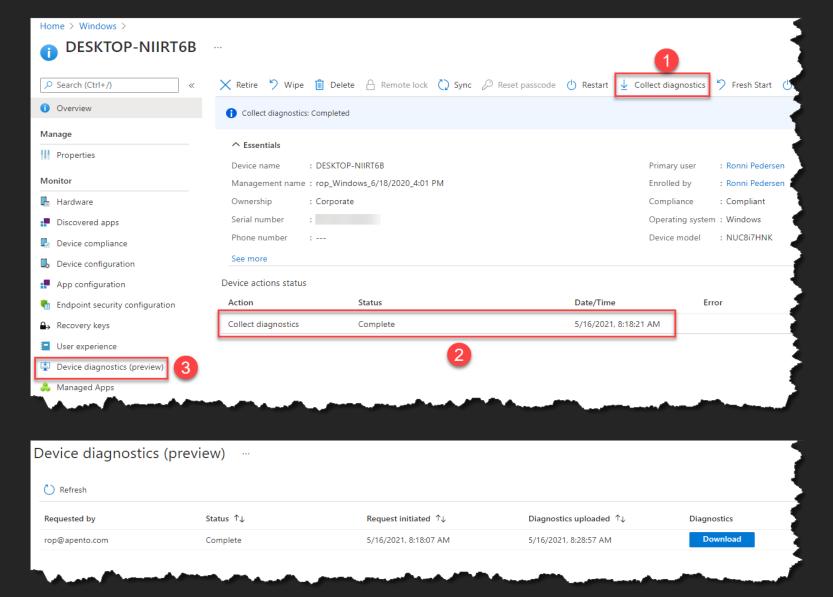
- VIRTUAL SUMMIT

- 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/collectdiagnostics

Collecting Diagnostic Logs







Configuration Policy Process

Microsoft 365 Apps Policy

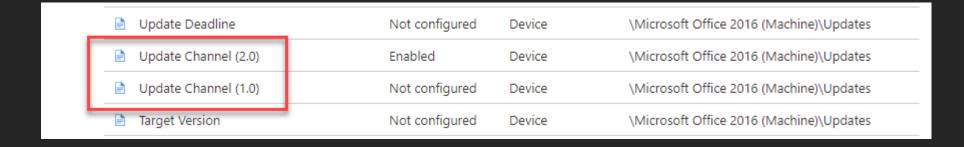


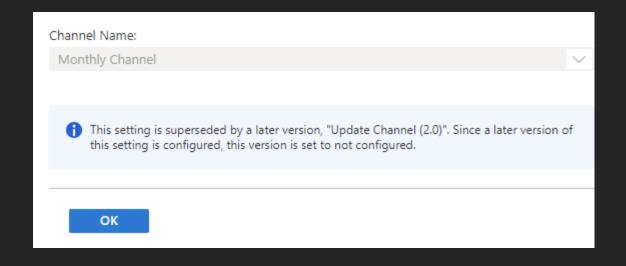
- Endpoint Manager Configuration:
 - Policy 1: Enable Microsoft 365 Apps Automatic Updates
 - Policy 2: Set the Update Channel
- Client-Side debugging:
 - #1 Check the Intune registry keys
 - #2 Check the Office registry keys
 - #3 Force Office automatic updates to run
 - #4 Force the Office synchronization to update account information

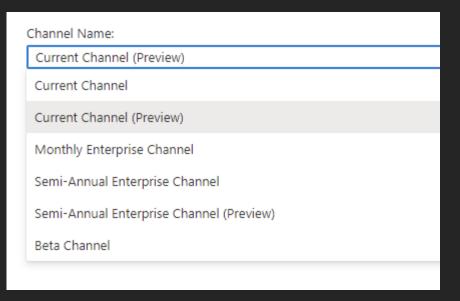
Administrative Templates



Example using Administrative Templates



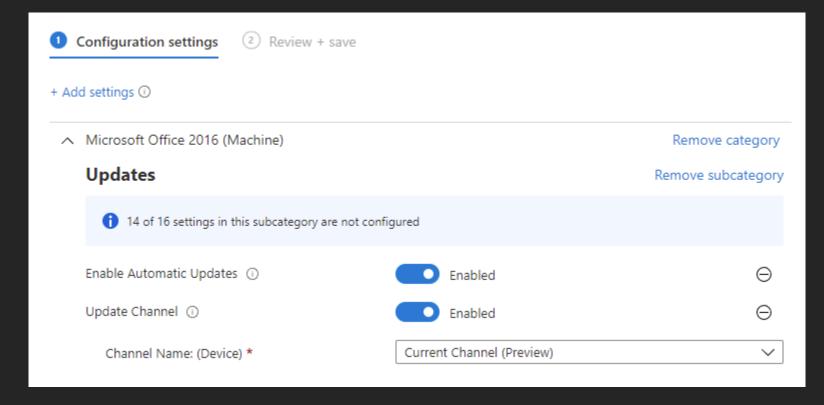




Using Settings Catalog (Preview)

NORDIC - VIRTUAL SUMMIT -

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



#1 Check the Intune registry keys

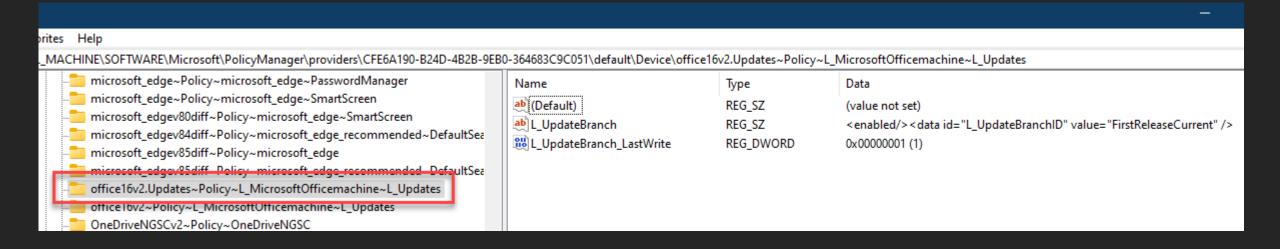


Open the Registry Editor, and go to the Intune policy path:

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.



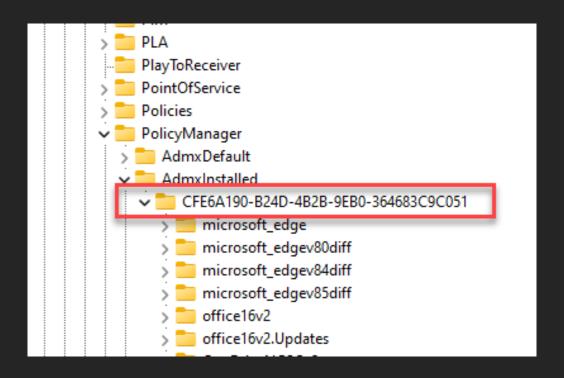
#TIP: Find the Provider ID



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



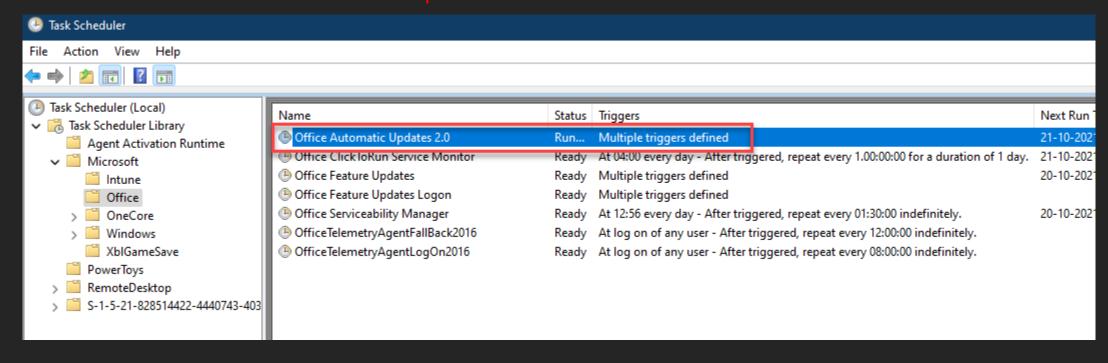
- Go to the Office policy path: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\Configuration
- Check the UpdateChannel value:
 - Monthly Enterprise Channel = 55336b82-a18d-4dd6-b5f6-9e5095c314a6
 - Current Channel = 492350f6-3a01-4f97-b9c0-c7c6ddf67d60
 - Current Channel (Preview) = 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

SCLCacheOverride	REG_SZ	0
ab SharedComputerLicensing	REG_SZ	0
ab StreamingFinished	REG_SZ	True
a Stream Package Url Changed	REG_SZ	True
TeamsAddon	REG_3Z	IIVSTALLED
ab UpdateChannel	REG_SZ	http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-8936-8840a6a4f5be
ab UpdateChannelChanged	PEG_SZ	Falco
ab UpdatesEnabled	REG_SZ	True
ab VersionToReport	REG_SZ	16.0.14527.20268
ab VisioProRetail.ExcludedApps	REG_SZ	groove
abluc : D. D. HAA C T	DEC CZ	CDN

#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 Secheduler > Microsoft > Office
 - Run "Office Automatic Updates 2.0"



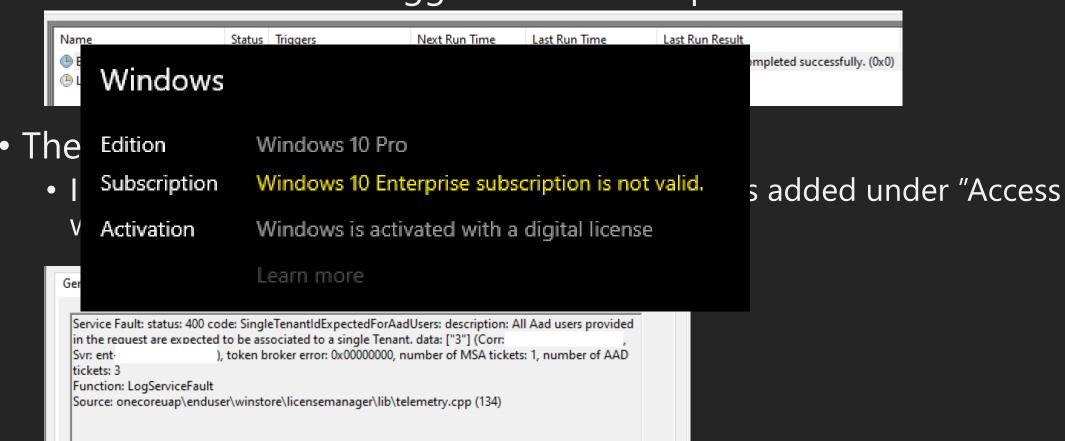


Troubleshooting Subscription based activation

Subscription based activation



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



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

Stay signed in to all your apps

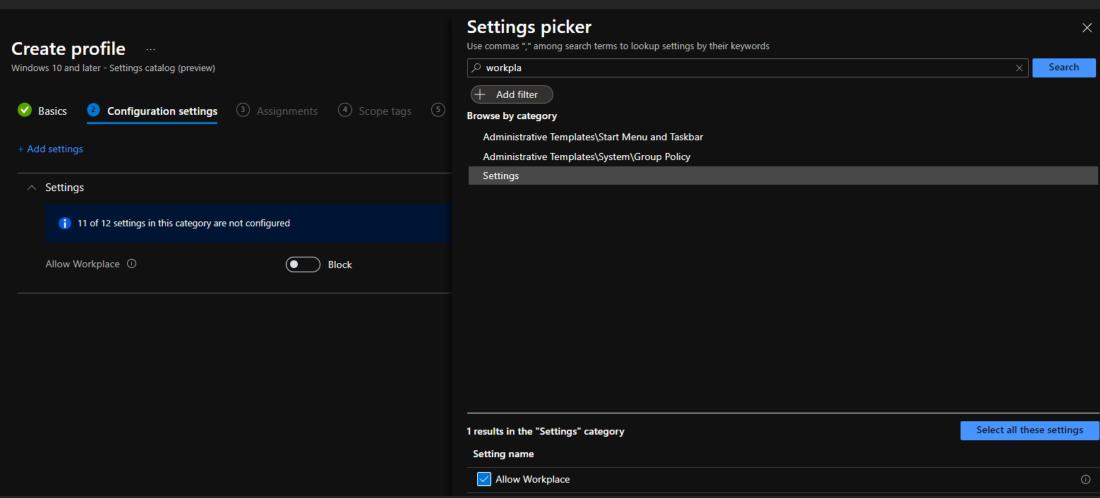
Windows will remember your account and automatically sign you in to your apps and websites on this device. You may need to let your organization manage some settings on your device.

Allow my organization to manage my device

No, sign in to this app only

Blocking Workplace join







Troubleshoot enrollment

Troubleshooting Windows enrollemnt in Intune

NORDIC
- VIRTUAL SUMMIT -

- 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



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

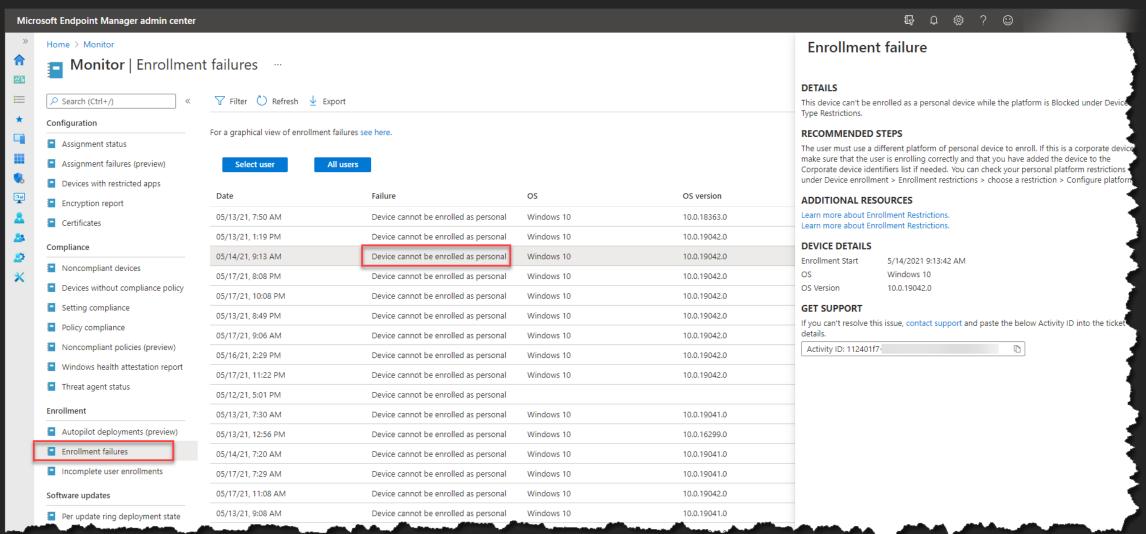
Server message: User '538156d0-c028-429c-90ecbe15074f379f' is not eligible to enroll a device of type

'Windows'. Reason 'DeviceCapReached'.

More information: https://www.microsoft.com/aadjerrors

Enrollment Failures

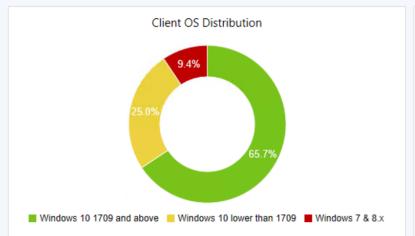


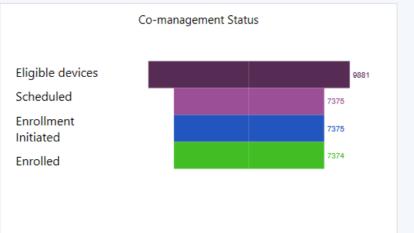


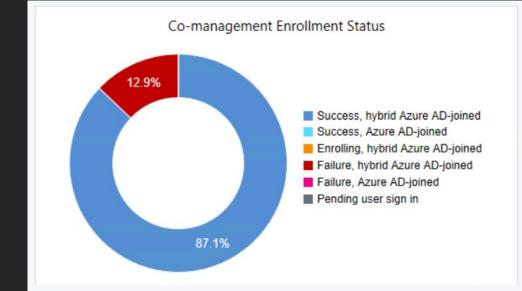
Co-Management Enrollment Status











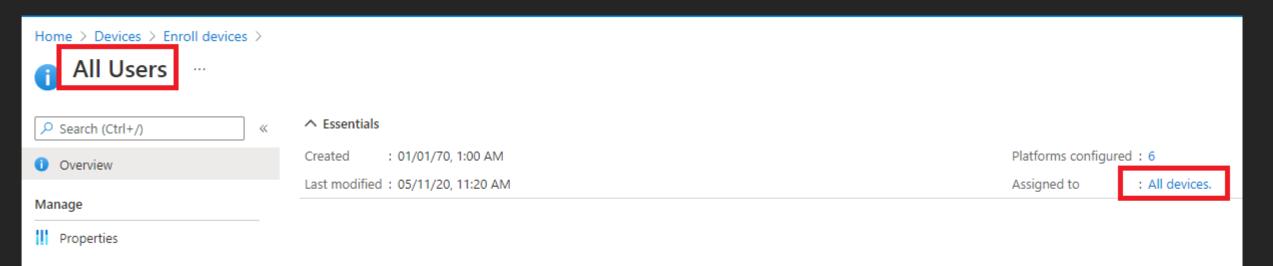
Count	Enrollment Error	
706	License of user is in bad state blocking enrollment	
382	Undefined	
6	Element not found.	
5	Catastrophic failure	
4	The Internet connection has timed out	
2	MDM enrollment hasn't been configured yet on AAD, or the enrollment url isn't expected.	
1	The user canceled the operation	

Co-Managed device enrollment



- 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.

<u>Important:</u> the default enrollment restriction policy "All Users" is applied to "All Devices"





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

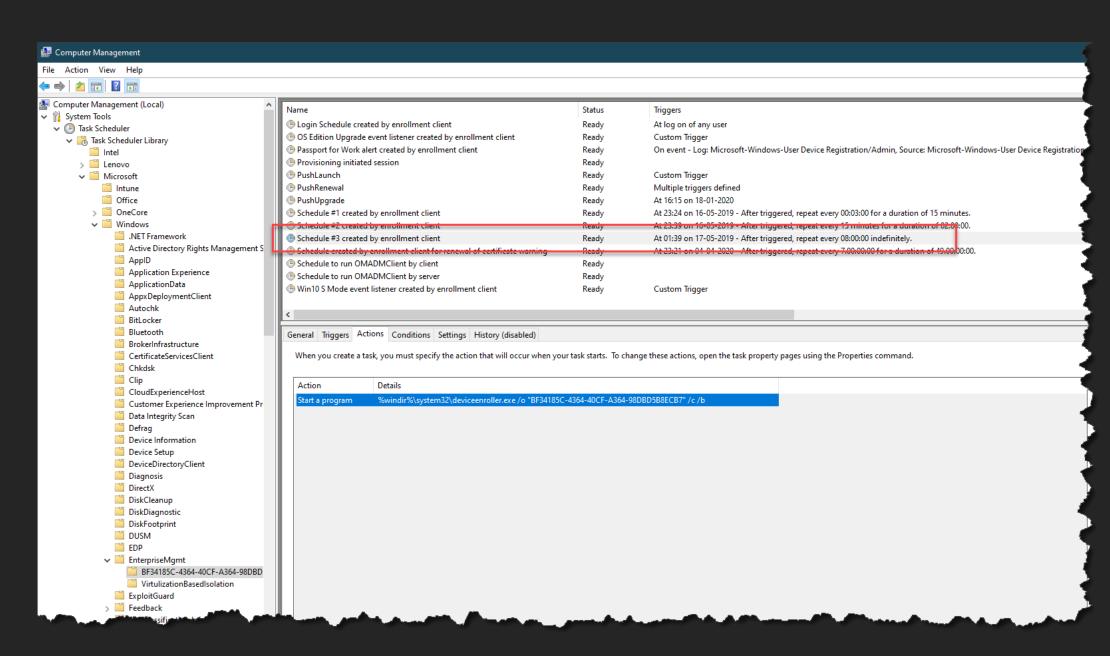
 Windows 10/11 devices will schedule check-in with the Intune service, which is estimated at: About every 8 hours

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



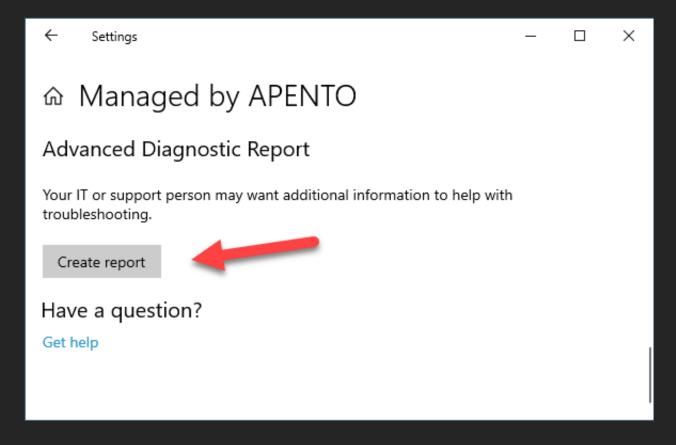
- Compliance policy settings always have precedence over configuration profile settings.
- Compliance policy conflicts: The most restrictive compliance policy setting applies.
- Configuration Profile Conflicts: Shown in Intune.
 - Manually resolve these conflicts



Troubleshooting MDM Policies



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





Managed policies

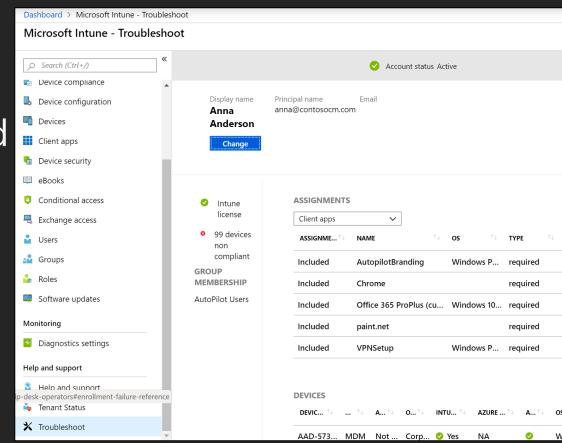
Policies that are not set to the default value or have a configuration source applied

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=""></enable> <data id="EncryptionMethodWithXtsOsDropDown_Name" value="7"></data> <data id="EncryptionMethodWithXtsFdvDropDown_Name" value="7"></data> <data id="EncryptionMethodWithXtsRdvDropDown_Name" value="7"></data>
BitLocker	System Drives Recovery Options			device		BF34185C-4364-40CF-A364-98DBD5B8ECB7= <enable d=""></enable> <data id="OSAllowDRA_Name" value="true"></data> <data id="OSRecoveryPasswordUsageDropDown_Name" value="2"></data> <data id="OSRecoveryKeyUsageDropDown_Name" value="2"></data> <data id="OSHideRecoveryPage_Name" value="false"></data> <data id="OSActiveDirectoryBackup_Name" value="true"></data> <data id="OSActiveDirectoryBackup_DropDown_Name" value="1"></data> <data id="OSRequire ActiveDirectoryBackup_Name" value="true"></data>
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	wClaud Drotection	a1 area #		device		BE34185C-4364-10CF-4264-98DBDE88ECB7=1

Intune Troubleshooting Pane



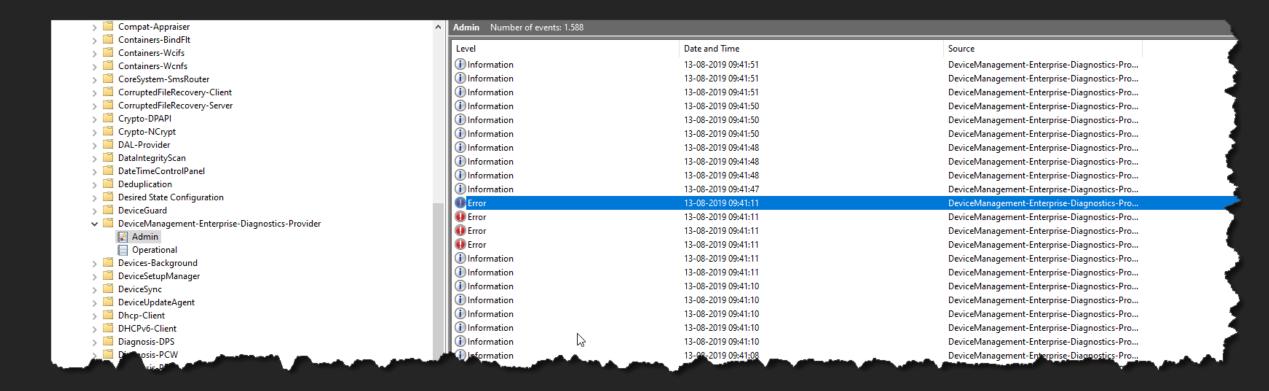
- Intune portal page
 - https://aka.ms/intunetroubleshooting
- Displays information focused around a particular user
 - See info about assignments, devices, enrollment failures, etc.
- For more info: https://docs.microsoft.com/enus/intune/help-desk-operators



Device Profiles - Where is my logs?

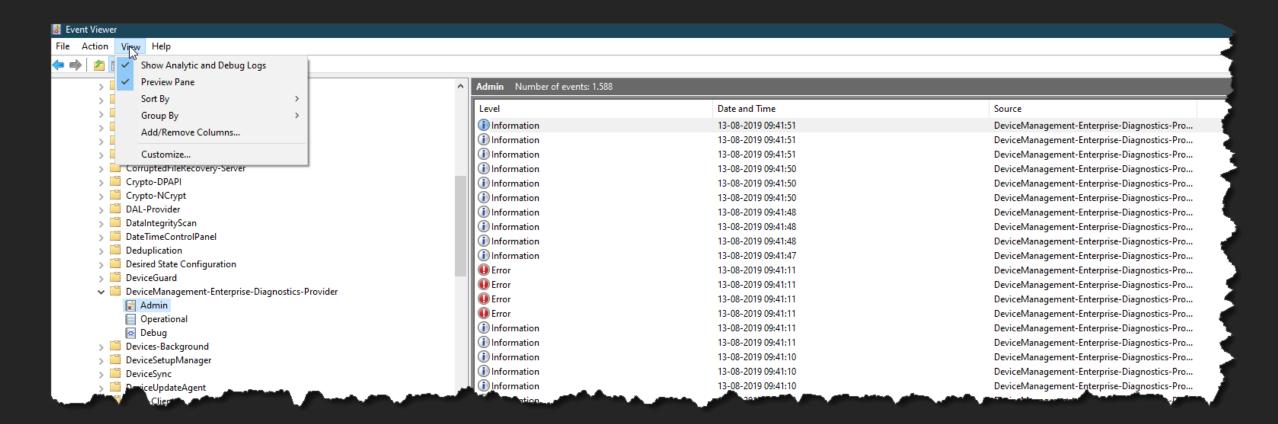


- Event viewer is your new best friend
 - Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider



Enable debug mode







Intune Management Extension

Intune Management Extension Prerequisites



- 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?!...)

① 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?



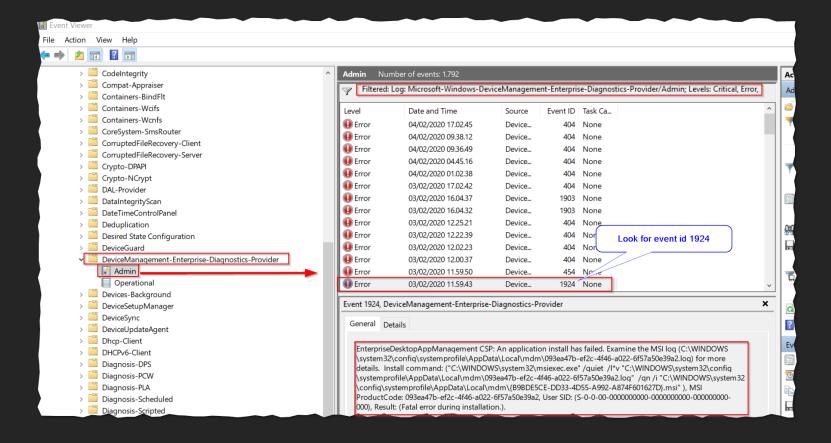
- The enrolling user is using a device enrollment manager account.
- The device enrolls through Windows Autopilot.
- The device enrolls through a bulk provisioning package.
- The device enrolls through GPO
 - or automatic enrollment from SCCM for co-management.



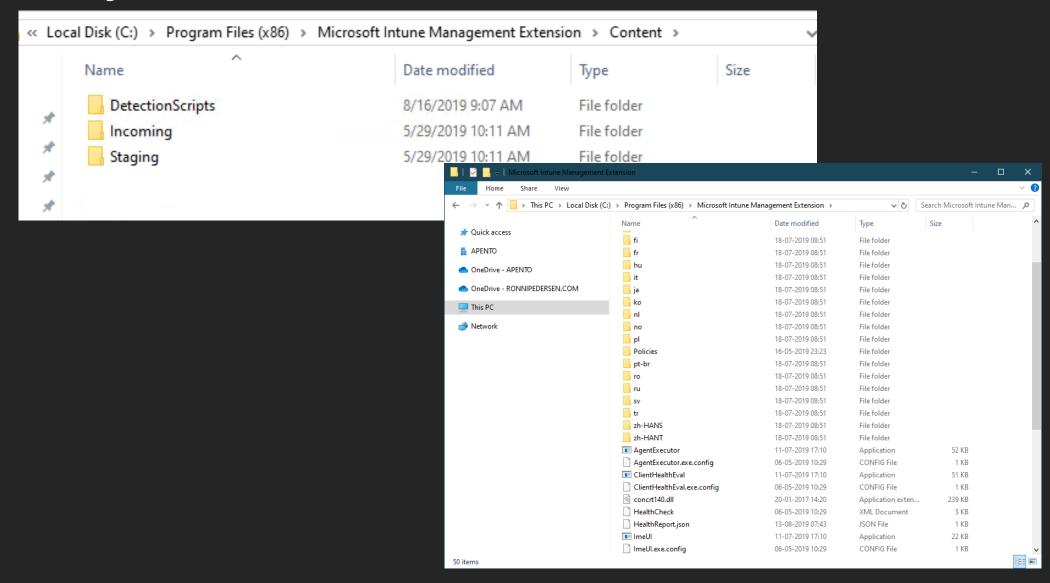
Intune Management Extension Event log



 Applications and services logs\Microsoft\Windows\DeviceManage...



Intune Management Extension File System

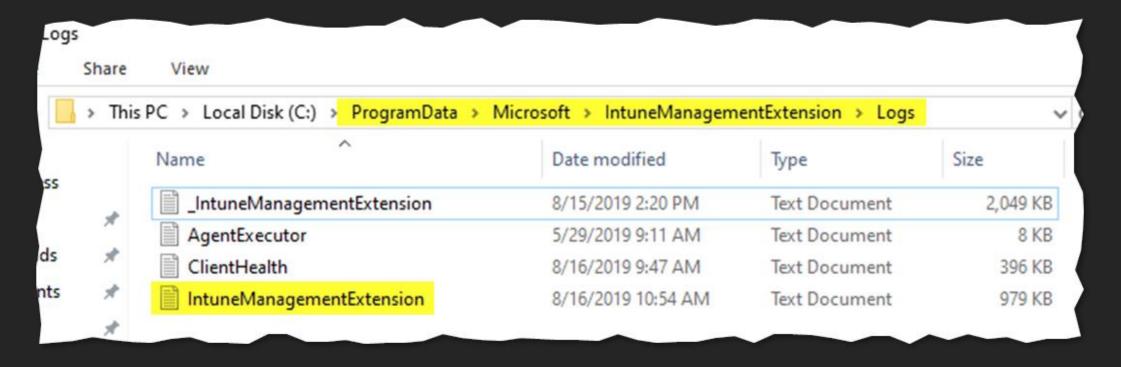




Intune Management Extension Log files



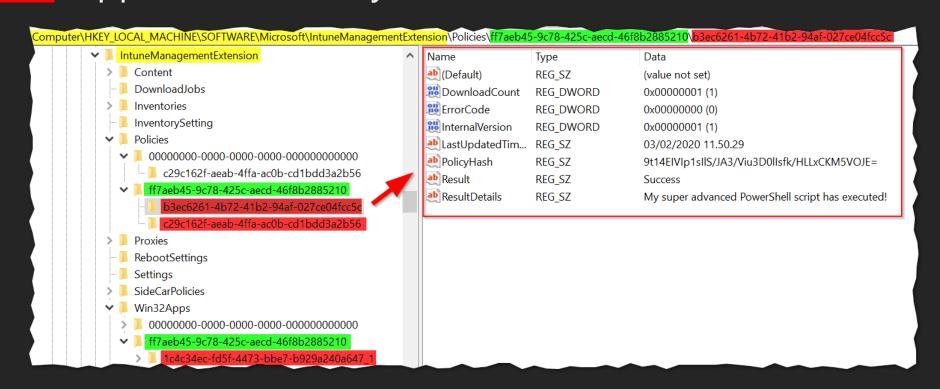
 Log files: "C:\ProgramData\Microsoft\IntuneManagementExtension\logs"



Intune Management Extension The Registry

NORDIC - VIRTUAL SUMMIT -

- 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?

Microsoft Intune Management Extension Properties (Local Comput... Log On Recovery Dependencies IntuneManagementExtension Service name: Microsoft Intune Management Extension Display name: Microsoft Intune Management Extension Description: Path to executable: ement Extension\Microsoft.Management.Services.IntuneWindowsAgent.exe" Startup type: Automatic (Delayed Start) Service status: Running Resume Start Pause You can specify the start parameters that apply when you start the service from here. Start parameters: OK Cancel Apply

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



Thank You!!