



# TunedIn:London





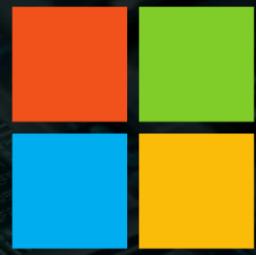
## Intune Management Extension Deep Dive

# TunedIn: London

Microsoft Reactor, Paddington, London  
8th December 2023



# Thank you to our Sponsors & Host



Microsoft



TunedIn:London

8<sup>th</sup> December 2023

# Agenda

- What is the IME?
- How is the IME installed?
- How does the IME process app policy?
- How does the IME process scripts?
- Digging into win32app policy event state messages
- Try again, how the IME handles failures and retries
- Invoke IME actions remotely like a boss
- Inventory
- Q&A



# What is the IME

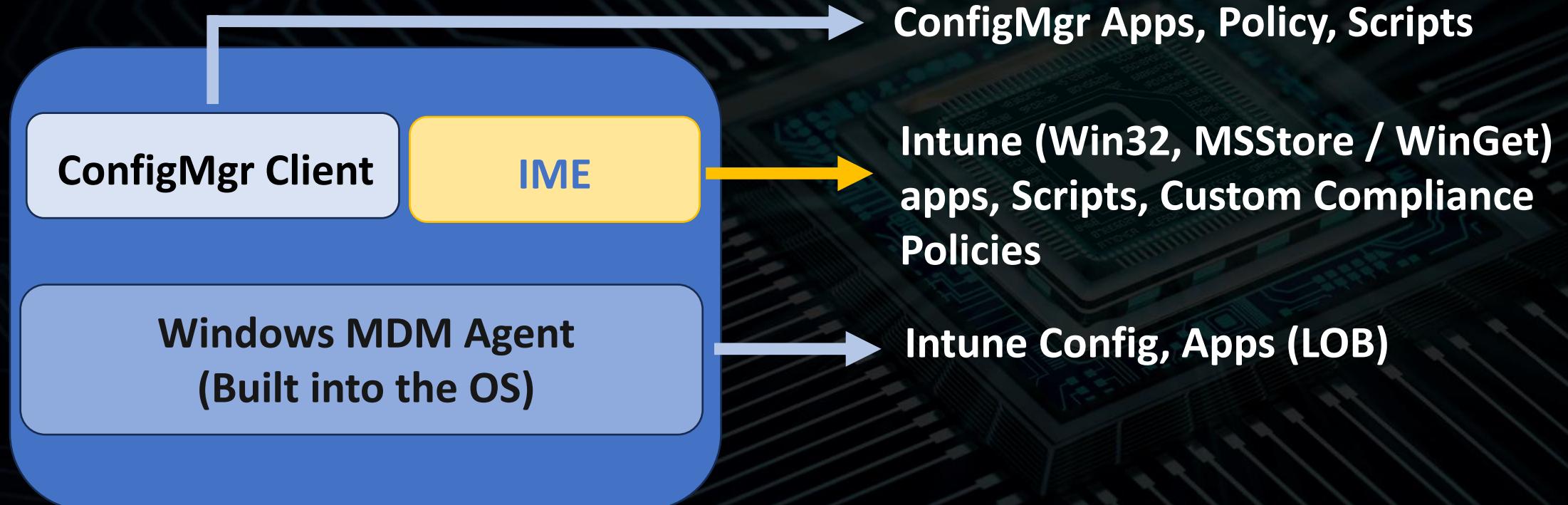
- A component installed by Intune and leveraged by Intune
- Used to deploy and execute PowerShell scripts and install Win32 applications on Windows devices that are enrolled in Intune

Microsoft 365 Apps for enterprise - en-us	Microsoft Corporation
Microsoft ASP.NET Core 6.0.23 - Shared Framework (x...)	Microsoft Corporation
Microsoft Azure Storage Explorer version 1.31.2	Microsoft Corporation
Microsoft Edge WebView2 Runtime	Microsoft Corporation
Microsoft Intune Management Extension	Microsoft Corporation
Microsoft OneDrive	Microsoft Corporation
Microsoft PowerBI Desktop (x64)	Microsoft Corporation
Microsoft System CLR Types for SQL Server 2019	Microsoft Corporation
Microsoft Teams	Microsoft Corporation



# What is the IME?

Where does the IME sit in the Microsoft RMM agent stack?



# What is the IME?

## IntuneManagementExtension.log

- Activities and processes related to the execution of scripts
- Installation of apps deployed through Microsoft Intune
- Provides insights into how the IME is functioning

## AgentExecutor.log

- Execution of scripts deployed through Microsoft Intune

## HealthScripts.log

- Proactive remediation scripts deployed through Microsoft Intune

## ClientHealth.log

- Client health activities for the IME i.e. Is the service is running

Win32ApplInventory.log is back!

Name	Date mod
AgentExecutor.log	24/10/20
AgentExecutor-20231019-100024.log	19/10/20
AgentExecutor-20231021-103159.log	21/10/20
AgentExecutor-20231023-090233.log	23/10/20
AgentExecutor-20231024-091855.log	24/10/20
ClientHealth.log	24/10/20
IntuneManagementExtension.log	18/10/20
IntuneManagementExtension-20231018-100254.log	18/10/20
IntuneManagementExtension-20231018-125702.log	18/10/20
IntuneManagementExtension-20231018-155712.log	18/10/20
IntuneManagementExtension-20231018-171225.log	18/10/20
Reset-Appx.log	01/07/20
Sensor.log	24/10/20
Sensor-20231020-173931.log	20/10/20
Sensor-20231022-152148.log	22/10/20
Sensor-20231023-172424.log	23/10/20
Sensor-20231024-110054.log	24/10/20

C:\ProgramData\Microsoft\IntuneManagementExtension\Logs

# What is the IME?

Increase IME Logging

HKLM\SOFTWARE\Microsoft\IntuneWindowsAgent\Logging

LogMaxHistory – Default is 3

LogMaxSize – Default is 3145728

(Used to be 2 x 2MB logs)



<https://github.com/okieselbach>



TunedIn:London



# How is the IME installed?

The IME is installed when a managed device is targeted with either a:-

1. PowerShell Script or Proactive Remediation
2. Win32 app or Microsoft Store app
3. Custom compliance settings

The screenshot shows the Microsoft Intune admin center interface. On the left, there's a navigation sidebar with links like Home, Dashboard, All services, Devices (which is highlighted with an orange box), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Windows | Scripts". It has a search bar and a table of remediations. The table has two tabs at the top: "Remediations" (which is selected and highlighted with an orange box) and "Platform scripts". The table lists several script packages with columns for "Script package name", "Author", and "Status". Some entries include "Restart stopped Office C2R svc" by Microsoft, "WU Device Settings Inventory" by Ben Whitmore, "Ninja Basic" by Ben Whitmore, "Update stale Group Policies" by Microsoft, "UnSupported Apps" by Ben Whitmore, "Update Compliance" by Ben Whitmore, "Ninja Detect Java Apps" by Ben Whitmore, and "WU Reminder 24-5-21" by Ben Whitmore.

Script package name	Author
Restart stopped Office C2R svc	Microsoft
WU Device Settings Inventory	Ben Whitmore
Ninja Basic	Ben Whitmore
Update stale Group Policies	Microsoft
UnSupported Apps	Ben Whitmore
Update Compliance	Ben Whitmore
Ninja Detect Java Apps	Ben Whitmore
WU Reminder 24-5-21	Ben Whitmore

# How is the IME installed?

The IME is installed, from an MSI, via the OMA-DM channel using the:-

***EnterpriseDesktopAppManagement***  
Configuration Service Provider (CSP)

This CSP is used to handle enterprise desktop application management tasks, such as querying installed enterprise applications, installing applications, or removing applications.

**Device/MSI/{ProductID}**

Scope	Editions	Applicable OS
<input checked="" type="checkbox"/> Device	<input checked="" type="checkbox"/> Pro	<input checked="" type="checkbox"/> Windows 10, version 1511 [10.0.10586] and later
<input checked="" type="checkbox"/> User	<input checked="" type="checkbox"/> Enterprise	
	<input checked="" type="checkbox"/> Education	
	<input checked="" type="checkbox"/> Windows SE	
	<input checked="" type="checkbox"/> IoT Enterprise / IoT Enterprise LTSC	

Device Copy

./Device/Vendor/MSFT/EnterpriseDesktopAppManagement/MSI/{ProductID}

The MSI product code for the application.

Description framework properties:

Property name	Property value
Format	node
Access Type	Add, Delete, Get
Atomic Required	True
Dynamic Node Naming	UniqueName: The MSI product code for the application.

<https://learn.microsoft.com/en-us/windows/client-management/mdm/enterprisedesktopappmanagement-csp>

# How is the IME installed?

You can track the install via the local registry

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\EnterpriseDesktopAppManagement\  
S-0-0-00-0000000000-0000000000-0000000000-000\MSI

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActionType	REG_DWORD	0x00000001 (1)
AssignmentType	REG_DWORD	0x00000001 (1)
BITSJobId	REG_SZ	440beb44-75f5-4bf2-8d9f-e802a75e3b0c
CommandLine	REG_SZ	
CreationTime	REG_QWORD	0x1d9d1f1154f1a06 (133368497358969350)
CurrentDownloadUrl	REG_SZ	https://euprodimedatapri.azureedge.net/IntuneWindowsAgent.msi
CurrentDownloadUrlList	REG_DWORD	0x00000001 (1)
DownloadInstall	REG_SZ	InProgress
DownloadLocation	REG_SZ	
DownloadUrlList	REG_MULTI_SZ	https://euprodimedatapri.azureedge.net/IntuneWindowsAgent.msi
EnforcementRetries	REG_DWORD	0x00000005 (5)
EnforcementRetries	REG_DWORD	0x00000001 (1)
EnforcementRetries	REG_DWORD	0x00000003 (3)
EnforcementStartTime	REG_QWORD	0x1d9d1f11ce3d06d (133368497486155885)
EnforcementTimeLeft	REG_DWORD	0x0000001e (30)
FileHash	REG_SZ	f16d46502cc24d5c48f53df8de3587ab01038b5edfdc8e104b24fb36de99f15
JobStatusReport	REG_DWORD	0x00000001 (1)
LastError	REG_DWORD	0x00000000 (0)

<https://euprodimedatasec.azureedge.net/IntuneWindowsAgent.msi>

New versions are rolled out automatically

Snapshots are a curse

# How is the IME installed?

View the SyncML message where OMA-DM initiates the MSI install for the IME



<https://github.com/okieselbach/SyncMLViewer>

SyncML Viewer - oliverkieselbach.com - 1.0.8

File Options Actions Help

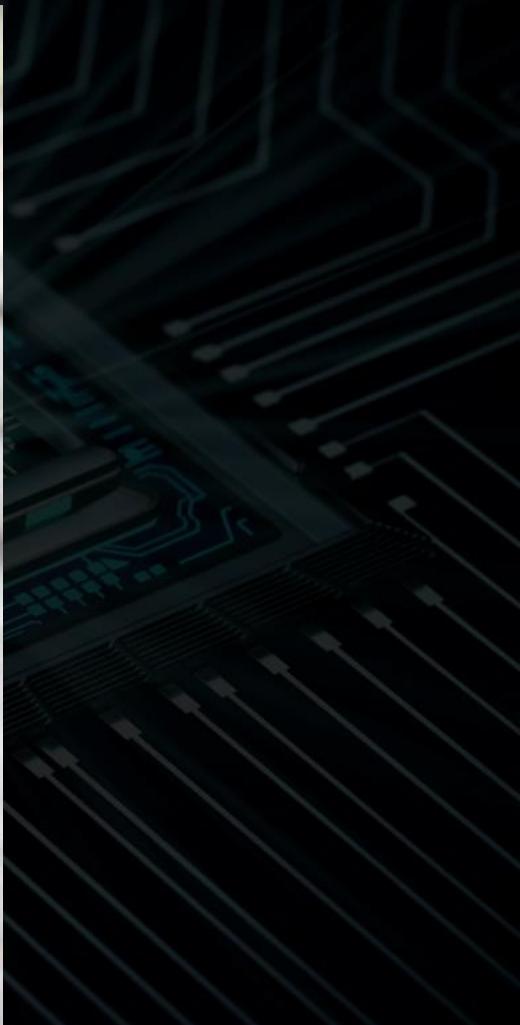
SyncML Representation Protocol Stream SyncML Sessions/Messages Response Status Codes Reference MDM Diagnostics About

```
<CmdID>29</CmdID>
<Item>
  <Target>
    <LocURI>./Device/Vendor/MSFT/Policy/Config/ADMX_DataCollection/CommercialIdPolicy</LocURI>
  </Target>
</Item>
</Get>
<Get>
<CmdID>30</CmdID>
<Item>
  <Target>
    <LocURI>./Device/Vendor/MSFT/EnterpriseDesktopAppManagement/MSI/%7B%7Bd395abfb-4f6a-46e6-b766-4cd9addf7331%7D%7D</LocURI>
  </Target>
</Item>
</Get>
<Get>
<CmdID>31</CmdID>
<Item>
  <Target>
    <LocURI>./Device/Vendor/MSFT/EnterpriseDesktopAppManagement/MSI/%7B%7Bd395abfb-4f6a-46e6-b766-4cd9addf7331%7D%7D/</LocURI>
  </Target>
</Item>
</Get>
<Get>
<CmdID>32</CmdID>
<Item>
  <Target>
    <LocURI>./Device/Vendor/MSFT/EnterpriseDesktopAppManagement/MSI/%7B%7Bd395abfb-4f6a-46e6-b766-4cd9addf7331%7D%7D/</LocURI>
  </Target>
</Item>
</Get>
```

MDM Sync Sync is in progress DESKTOP-B2DLNOJ

```
2753
2754
2755
2756
2757 <It;ContentURL>https://euprodimedatapri.azureedge.net/IntuneWindowsAgent.msi</ContentURL>&lt;/ContentURLList&gt;&lt;
2758
2759
```

# How is the IME installed?



Is this the right country or region?

United States

Afghanistan

Åland Islands

Albania

Algeria

American Samoa

Andorra

Yes



# How does the IME process app policy?

Policy is deployed

Assignments [Edit](#)

Group mode	Group	Filter mode	Filter	End user notifications	Availability	Inst
Required						
Available for enrolled devices						
<a href="#">Included</a>	All users	None	None	Show all toast notificat...	As soon as possible	

Policy reaches the device

```
[SendWebRequestInternal] Sending network request... Current proxy is https://fef.amsub0502.manage.microsoft.com/TrafficGateway/TrafficRoutingService/SideC...
[SendWebRequestInternal] Succeeded
[Win32App] Got result with session id 1b7e0964-1664-4485-bfce-8ea9c7f2f7d4
[Win32App] Got 2 Win32App(s) for user ddc3cf6e-3b3b-461c-a823-53196902d067 in session 2
<![LOG(Get policies = [{"Id":"85a3f281-933d-4c72-90eb-66253787efb3","Name":"7-Zip 23.01 (MSI-x64)","Version":2,"Intent":1,"TargetType":1,"AppApplicabilitySt...
[Win32App] espSupportForSupersedenceEnabled : False, v2AppProcessorDisabled : True
```

Dependencies checked

Detection rule checked

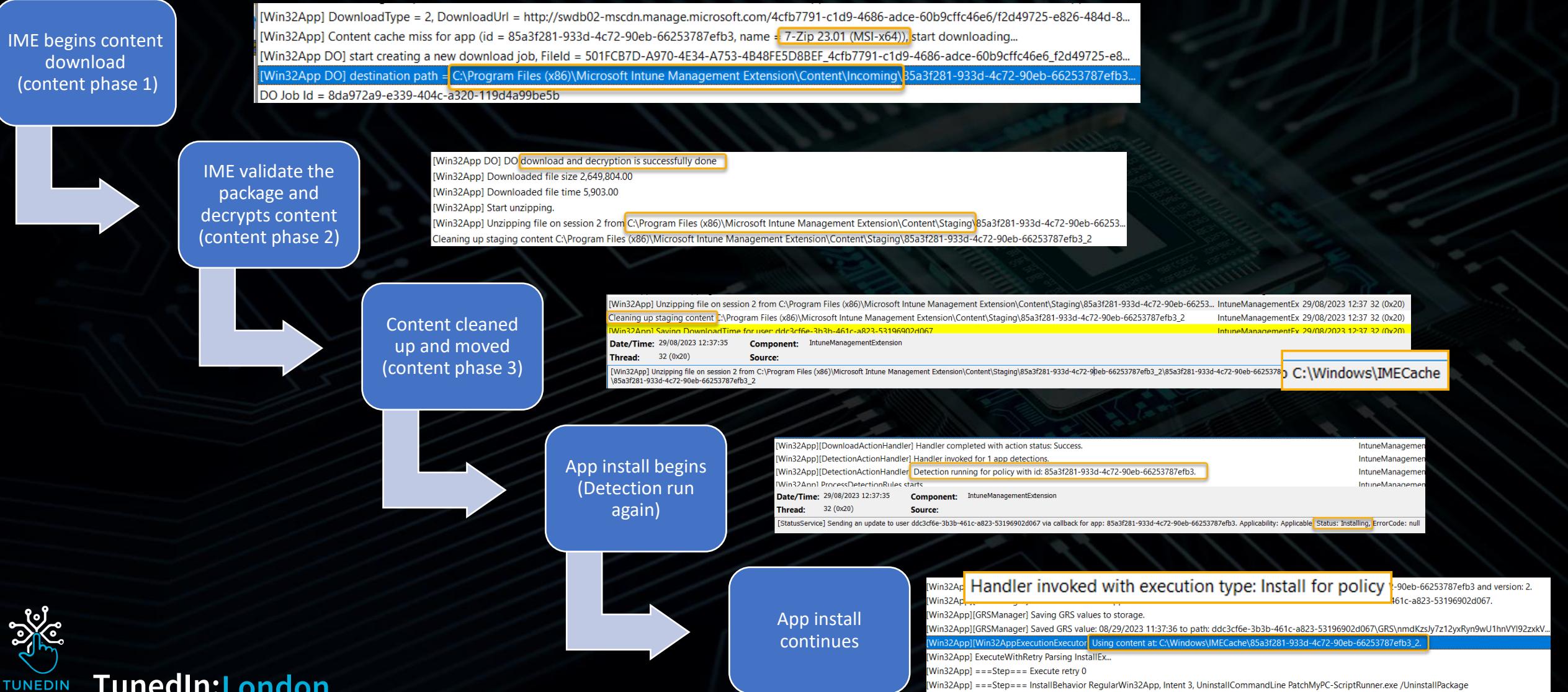
Applicability and requirements checked

```
graph reevaluation interval is not expired.Hash = xP8RetQTWNJ2yuVMOvEb5osh3DKsSoSLcOXW+I3R3lw=
graph TD
    A[IntuneManagementExtension]
    A --> B[{"b4cde7","Name":"Company
abilityStateDueToAssignmentFir...
":false,"InstallProgramVisibility":0,"InstallCommandLine":null,"UninstallCommand":null,"TimeInMinutes":0,"DeviceRestartBehavior":1,"Intent":1,"FlatDependencies":null,"M...
":1,"RelationVersion":0,"RebootEx":0,"StartTime":VDate(-621355,"2018-01-01T00:00:00Z"),"StopTime":VDate(1000000000000000000,"2106-06-21T23:59:59Z")}]
```

```
[Win32App] SideCarScriptDetectionManager Powershell ExitCode: 0
[Win32App] Detection script file C:\Program Files (x86)\Microsoft Intune Management Extension\Content\DetectionScripts\85a3f281-933d-4c72-90eb-66253787efb3.ps1
[Win32App] Checked Powershell script result:
[Win32App] Checked Powershell script exitCode: 0 EnforceSignatureCheck: 0 RunAs32Bit: 0 InstallExRunAs: , result of applicationDetected: False
```

```
[Win32App][DetectionActionHandler] Handler completed.
[Win32App][ApplicabilityActionHandler] Handler invoked for 1 app applicability checks
[Win32App] RequiredOSArchitecture: 2, is64BitOperatingSystem: True, isArm64: False, applicability: ApplicableBuild: 19044.
[Win32App] applicationRequirementMetadata expected version: 10.0.14393, client version: 10.0.19044, applicability: Applicable.
[Win32App] applicationRequirementMetadata.RequiredFreespace is , skip check.
[Win32App] applicationRequirementMetadata.RequiredMemory is , skip check.
[Win32App] applicationRequirementMetadata.RequiredCPUSpeed is , skip check.
[Win32App] applicationRequirementMetadata.MinimumNumberOfProcessors is , skip check.
```

# How does the IME process app policy?



# How does the IME process app policy?

Reboot Manager checks exit code for reboot requirement and content cleaned up

Cleaning up staged content C:\Windows\IMECache\85a3f281-933d-4c72-90eb-66253787efb3\_2  
[Win32App][RebootManager] Removing user with id: ddc3cf6e-3b3b-461c-a823-53196902d067 from the available check-in schedule.

Detection reevaluated

Compliance state set in registry and sent to the Intune service

Toast Success or Company Portal update

Drink Coffee

[Win32App] Detection script file C:\Program Files (x86)\Microsoft Intune Management Extension\Content\DetectionScripts\85a3f281-933d-4c72-90eb-66253787efb3\_2  
[Win32App] Checked Powershell script result: Detected  
[Win32App] Checked Powershell script exitCode: 0  
[Win32App] Detection script file C:\Program Files (x86)\Microsoft Intune Management Extension\Content\DetectionScripts\85a3f281-933d-4c72-90eb-66253787efb3\_2  
if applicationDetected: True

[Win32App][ReportingManager] Detection state for app with id: 85a3f281-933d-4c72-90eb-66253787efb3 has been updated. Report delta: {"DetectionState": "...  
[Win32App][ReportingManager] Sending status to company portal based on report: {"ApplicationId": "85a3f281-933d-4c72-90eb-66253787efb3", "ResultantApp...  
[Win32App][StatusServiceReportsStore] Saved ApplInstallStatusReport for user ddc3cf6e-3b3b-461c-a823-53196902d067 for app 85a3f281-933d-4c72-90eb-66253787efb3  
[StatusService] Sending update from StatusServicePublisher.

Microsoft Intune Management Extension

Byteben Lab software distribution  
7-Zip 23.01 (MSI-x64) was installed successfully.  
12:37



Installed



7-Zip 23.01 (MSI-x64)

Igor Pavlov

Reinstall

...

# How does the IME process scripts?

Microsoft Intune admin center

Home > Devices | Scripts > Test Script

## Test Script | Properties

Windows 10 and later

GitHub > byteben > Private > Intune > TestScript.ps1 > ...

```
1 Try {  
2     $folderContent = Get-ChildItem - Path 'C:\IDontExist' -ErrorAction SilentlyContinue  
3 }  
4 Catch {  
5     #Dont tell a soul  
6 }  
7 If (-not $folderContent) {  
8     Try {  
9         New-Item -Path 'C:\IDontExist' -ItemType 'Directory' -Force  
10    }  
11    Catch {  
12        #I failed miserably  
13    }  
14 }
```

Enforce script signature check Yes

Run script in 64 bit PowerShell Host No



TunedIn:London





Log Text

[PowerShell] After filter, get 1 policies for user ddc3cf6e-3b3b-461c-a823-53196902d067 in session 2  
Powershell policies are detected, but device is not Mode S or E, skipping unlock.  
[PowerShell] Processing policy with id = 2ee1c561-3e1e-495b-8a6d-06cca4a08bc2 for user ddc3cf6e-3b3b-461c-a823-53196902d067

Component	Date/Time	Thread
IntuneManagementEx	29/08/2023 12:20	9 (0x9)
IntuneManagementEx	29/08/2023 12:20	9 (0x9)
IntuneManagementEx	29/08/2023 12:20	9 (0x9)
IntuneManagementEx	29/08/2023 12:20	9 (0x9)

[PowerShell] Policy body = Try {\$FolderContent = Get-ChildItem - Path "C:\IDontExist" -ErrorAction SilentlyContinue}Catch {#Dont tell a soul}If (-not \$FolderContent){  
[PowerShell] policy hash = pP/qoivrgcNmBUnDt1f7MiQoXYWkc4FBsgyw+TKtQzc=  
The calculated old hash is c/jQkZVq8n9aPYeQF0b05IzqpTyeHmQOvlBCCjDDyUs=, new hash is 7lajfBel4OvnENW0BfWpnGEzhZr8h5UWgM3ocpYMDU= for polic...  
The incoming hash is pP/qoivrgcNmBUnDt1f7MiQoXYWkc4FBsgyw+TKtQzc=  
[PowerShell] Hash validation pass.  
[TamperProtection] Enforcement mode = Enforcement2. PolicyType = 1. Running checks.  
[TamperProtection] Blob embedded certs:DigiCert Global Root G2:DigiCert Global Root G2|08/01/2013 13:00:00|01/15/2038 12:00:00|DF3C24F9BFD666761B268...  
[TamperProtection] Pass.  
[PowerShell] Tamper validation pass.  
Script file C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\ddc3cf6e-3b3b-461c-a823-53196902d067\_2ee1c561-3e1e-495b-8a6d...  
[PowerShell] The policy needs be run as System  
PowerShell: Enforce signature check = True  
PowerShell: Running mode = 0

'C:\Program Files (x86)\Microsoft Intune Management Extension\agentexecutor.exe" -powershell "C:\Program Files (x86)\Microsoft Intune Management Extensi...  
Launch powershell executor in machine session  
Create proxy process successfully.  
process id = 8936  
Execution is done collecting result

**Date/Time:** 29/08/2023 12:20:45    **Component:** IntuneManagementExtension

**Thread:** 9 (0x9)

**Source:**

```
[PowerShell] Policy body = Try {
$FolderContent = Get-ChildItem - Path "C:\IDontExist" -ErrorAction SilentlyContinue
}
Catch {
#Dont tell a soul
}
If (-not $FolderContent){
Try {
New-Item -Path 'C:\IDontExist' -ItemType 'Directory' -Force
}
```



Log Text	Component	Date/Time	Thread
write output done. output = OK, error =	AgentExecutor	29/08/2023 12:14	1 (0x1)
ExecutorLog AgentExecutor gets invoked	AgentExecutor	29/08/2023 12:20	1 (0x1)
Creating command line parser, name delimiter is - and value separator is .	AgentExecutor	29/08/2023 12:20	1 (0x1)
Getting Ordered Parameters	AgentExecutor	29/08/2023 12:20	1 (0x1)
Parsing Ordered Parameters.	AgentExecutor	29/08/2023 12:20	1 (0x1)
Adding argument powershell with value C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\ddc3cf6e-3b3b-461c-a823-53196902d0...	AgentExecutor	29/08/2023 12:20	1 (0x1)
Powershell option gets invoked	AgentExecutor	29/08/2023 12:20	1 (0x1)
C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\ddc3cf6e-3b3b-461c-a823-53196902d067_2ee1c561-3e1e-495b-8a6d-06cca4a0...	AgentExecutor	29/08/2023 12:20	1 (0x1)
C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\ddc3cf6e-3b3b-461c-a823-53196902d067_2ee1c561-3e1e-495b-8a6d-06cca4a...	AgentExecutor	29/08/2023 12:20	1 (0x1)
C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\ddc3cf6e-3b3b-461c-a823-53196902d067_2ee1c561-3e1e-495b-8a6d-06cca4a...	AgentExecutor	29/08/2023 12:20	1 (0x1)
C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\ddc3cf6e-3b3b-461c-a823-53196902d067_2ee1c561-3e1e-495b-8a6d-06cca4a...	AgentExecutor	29/08/2023 12:20	1 (0x1)
Prepare to run Powershell Script ..	AgentExecutor	29/08/2023 12:20	1 (0x1)
scriptParams is	AgentExecutor	29/08/2023 12:20	1 (0x1)
cmd line for running powershell is -NoProfile -executionPolicy allsigned -file "C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\d...	AgentExecutor	29/08/2023 12:20	1 (0x1)
PowerShell path is C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	AgentExecutor	29/08/2023 12:20	1 (0x1)
[Executor] created powershell with process id 8888	AgentExecutor	29/08/2023 12:20	1 (0x1)
Powershell exit code is 1	AgentExecutor	29/08/2023 12:20	1 (0x1)
lenth of out=2	AgentExecutor	29/08/2023 12:20	1 (0x1)
lenth of error=723	AgentExecutor	29/08/2023 12:20	1 (0x1)
error from script =File C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\ddc3cf6e-3b3b-461c-a823-53196902d067_2ee1c561-3e1...	AgentExecutor	29/08/2023 12:20	1 (0x1)
Powershell script is failed to execute	AgentExecutor	29/08/2023 12:20	1 (0x1)
write output done. output = , error = File C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\ddc3cf6e-3b3b-461c-a823-53196902d...	AgentExecutor	29/08/2023 12:20	1 (0x1)
Agent executor completed.	AgentExecutor	29/08/2023 12:20	1 (0x1)

Date/Time: 29/08/2023 12:20:50

Component: AgentExecutor

Thread: 1 (0x1)

Source:

```
write output done. output =
, error = File C:\Program Files (x86)\Microsoft Intune Management
Extension\Policies\Scripts\ddc3cf6e-3b3b-461c-a823-53196902d067_2ee1c561-3e1e-495b-8a6d-06cca4a08bc2.ps1 cannot be
runned. The file C:\Program Files (x86)\Microsoft Intune Management
Extension\Policies\Scripts\ddc3cf6e-3b3b-461c-a823-53196902d067_2ee1c561-3e1e-495b-8a6d-06cca4a08bc2.ps1 is not
digitally signed. You cannot run this script on the current system. For more information about running scripts and
setting execution policy, see about_Execution_Policies at https://go.microsoft.com/fwlink/?LinkId=135170.
+ CategoryInfo          : SecurityError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : UnauthorizedAccess
```

# How does the IME process scripts?

Enforce script signature is now enabled by default

The screenshot shows a user interface for managing scripts. At the top, there are five tabs: Basics (green checkmark), Script settings (blue circle with 2), Scope tags (grey circle with 3), Assignments (grey circle with 4), and Review + add (grey circle with 5). The 'Script settings' tab is selected.

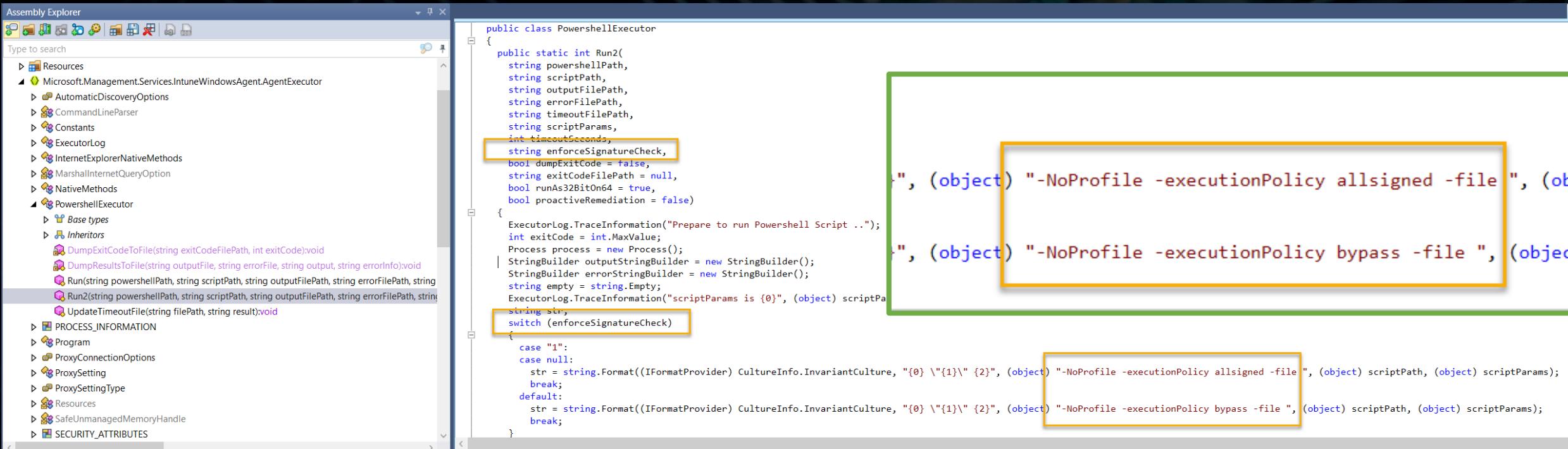
The main area contains several configuration options:

- Script location \***: A file input field labeled "Select a file" with a blue folder icon.
- Run this script using the logged on credentials**: A toggle switch with "Yes" and "No" buttons.
- Enforce script signature check**: A toggle switch with "Yes" and "No" buttons. This option is highlighted with a yellow rectangular border.
- Run script in 64 bit PowerShell Host**: A toggle switch with "Yes" and "No" buttons.



# How does the IME process scripts?

Agent Executor invokes PowerShell to run platform scripts and sets the PowerShell policy to **allsigned** or **bypass** according to the policy received



The screenshot shows the Microsoft Visual Studio IDE with the Assembly Explorer and the code editor open. The code editor displays the `PowershellExecutor` class from the `Microsoft.Management.Services.IntuneWindowsAgent.AgentExecutor` namespace. The code implements methods for running PowerShell scripts with specific execution policies based on a configuration parameter `enforceSignatureCheck`.

```
public class PowershellExecutor
{
    public static int Run2(
        string powershellPath,
        string scriptPath,
        string outputPath,
        string errorFilePath,
        string timeoutFilePath,
        string scriptParams,
        int timeoutSeconds,
        string enforceSignatureCheck,
        bool dumpExitCode = false,
        string exitCodefilePath = null,
        bool runAs32BitOn64 = true,
        bool proactiveRemediation = false)
    {
        ExecutorLog.TraceInformation("Prepare to run Powershell Script ..");
        int exitCode = int.MaxValue;
        Process process = new Process();
        StringBuilder outputStringBuilder = new StringBuilder();
        StringBuilder errorStringBuilder = new StringBuilder();
        string empty = string.Empty;
        ExecutorLog.TraceInformation("scriptParams is {0}", (object) scriptParams);
        string str;
        switch (enforceSignatureCheck)
        {
            case "1":
            case null:
                str = string.Format((IFormatProvider) CultureInfo.InvariantCulture, "{0} \\{1}\\ {2}", (object) "-NoProfile -executionPolicy allsigned -file ", (object) scriptPath, (object) scriptParams);
                break;
            default:
                str = string.Format((IFormatProvider) CultureInfo.InvariantCulture, "{0} \\{1}\\ {2}", (object) "-NoProfile -executionPolicy bypass -file ", (object) scriptPath, (object) scriptParams);
                break;
        }
        ...
    }
}
```

# How does the IME process scripts?

- Platform scripts are executed before Win32 apps
- Platform scripts will try 3 times. Will not retry unless script is modified
- IME deployed even if Client Apps workload is not set to Intune
- Script size must be less than 200kb
- Platform scripts time out after 30 minutes

Tip: Use PSEXEC to simulate a script running as SYSTEM

# Digging into win32 app policy event state messages

Win32 app policy events are stored in the registry

Registry Editor

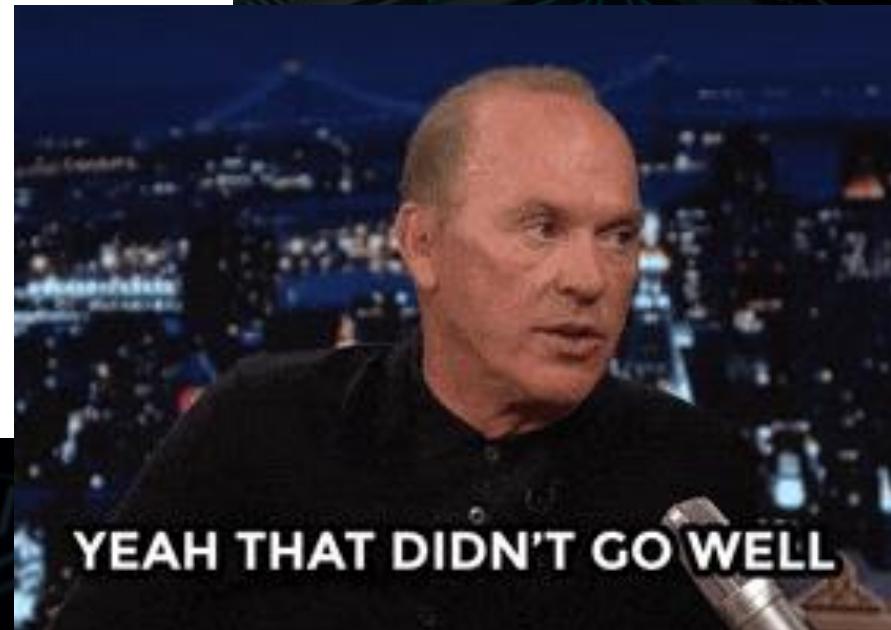
File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\Win32Apps\ddc3cf6e-3b3b-461c-a823-53196902d067\0066fcca-4102-4ea7-9ea5-a78144b1ed50\_1\ComplianceStateMessage

Name	Type	Data
(Default)	REG_SZ	(value not set)
ComplianceState...	REG_SZ	{"Applicability":1008,"ComplianceState":1,"DesiredState":2,"ErrorCo...

Notification  
Proxies  
RebootSettings  
sensor  
Settings  
SideCarPolicies  
Win32Apps  
00000000-0000-0000-000000000000  
85a3f281-933d-4c72-90eb-66253787efb3\_2  
GRS  
ddc3cf6e-3b3b-461c-a823-53196902d067  
0066fcca-4102-4ea7-9ea5-a78144b1ed50\_1  
ComplianceStateMessage  
18bec66c-6ebf-4061-8b36-350ca1ae6e6a\_1  
6af49084-14ce-4ed4-8fb-2a2b23f25da9\_1  
72d81252-f66d-4a6f-8e18-0af64e438fd7\_1  
85a3f281-933d-4c72-90eb-66253787efb3\_2  
aca02ed5-b575-4b6c-95e9-6ba13b60589d\_1  
ba93598d-d703-43dc-a119-6f91b19c9355\_1  
c159a5e0-00d4-4d4e-9f6e-0507f0b4cd7\_1  
d1df03a6-cfd5-407e-a337-b095dd7bdcec\_1  
e316127d-a9a4-4193-8f04-b07c37d1130f\_1  
fe38a779-a875-4c0f-a9ff-46ded4e79753\_1  
GRS  
OperationalState  
Reporting  
Win32AppSettings

Apps deployed to the device



HKLM:SOFTWARE\Microsoft\IntuneManagementExtension\Win32Apps

# Digging into win32 app policy event state messages

Win32 app policy events are stored in the registry

Registry Editor

File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\Win32Apps\ddc3cf6e-3b3b-461c-a823-53196902d067\ComplianceStateMessage

Notification  
Proxies  
RebootSettings  
sensor  
Settings  
SideCarPolicies  
Win32Apps  
00000000-0000-0000-0000-000000000000  
ddc3cf6e-3b3b-461c-a823-53196902d067  
0066fcc4-4102-4ea7-9ea5-a78144b1ed50\_1  
18bec66c-6ebf-4061-8b36-350ca1ae6e6a\_1  
6af49084-14ce-4ed4-8fbf-2a2b23f25da9\_1  
72d81252-f66d-4a6f-8e18-0af64e438fd7\_1  
85a3f281-933d-4c72-90eb-66253787efb3\_2  
aca02ed5-b575-4b6c-95e9-6ba13b60589d\_1  
ba93598d-d703-43dc-a119-6f91b19c9355\_1  
c159a5e0-00d4-4d4e-9f6e-0507f0b4cde7\_1  
d1df03a6-cfd5-407e-a337-b095dd7bdcec\_1  
e316127d-a9a4-4193-8f04-b07c37d1130f\_1  
ComplianceStateMessage  
EnforcementStateMessage  
fe38a779-a875-4c0f-a9ff-46ded4e79753\_1

Name Type Data

(Default) REG\_SZ (value not set)

ComplianceStateMessage REG\_SZ {"Applicability":0,"ComplianceState":2,"DesiredState":2,"ErrorCode":null,"Target...

Edit String

Value name: ComplianceStateMessage

Value data: {"Applicability":0,"ComplianceState":2,"DesiredState":2,"ErrorCode":null,"Target...

OK Cancel

# Digging into win32 app policy event state messages

The screenshot shows the Windows Registry Editor with a focus on a registry key. The key path is visible at the top: `AppExtension\Win32Apps\ddc3cf6e-3b3b-461c-a823-53196902d067\e316127d-a9a4-4193-8f04-b07c37d1130f_1\ComplianceStateMessage`. Inside this key, there are two entries:

- (Default)**: Type `REG_SZ`, Data: `(value not set)`
- ComplianceStateMessage**: Type `REG_SZ`, Data: `{"Applicability":0,"ComplianceState":2,"DesiredState":2,"ErrorCode":null,"Target":null}`

A yellow arrow points from the `ComplianceStateMessage` entry to the **Compliance State:** table on the right.

App deployment Type (Intent):

Values	Description
1	Available
3	Required
4	Uninstall

Compliance State:

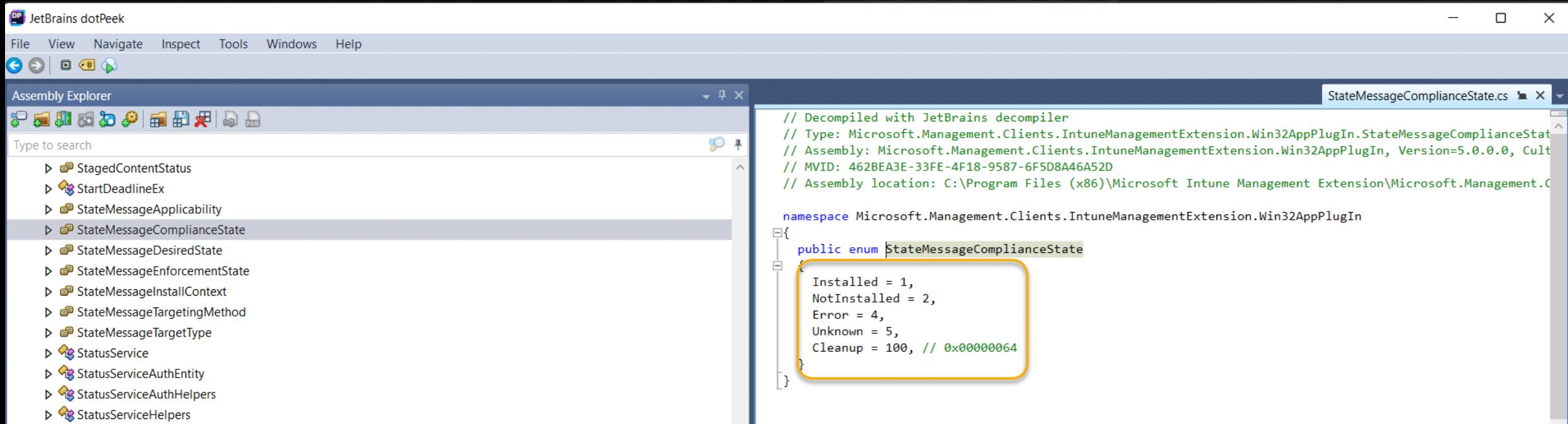
Values	Description
0	Unknown
1	Compliant
2	Not compliant
3	Conflict (Not applicable for app deployment)
4	Error

Desired State:

Values	Description
0	None
1	NotPresent
2	Present
3	Unknown
4	Available

# Digging into win32 app policy event state messages

## State Message Magic



The screenshot shows the JetBrains dotPeek decompiler interface. The Assembly Explorer window on the left lists various types, with `StateMessageComplianceState` selected. The main code editor window displays the C# code for the `StateMessageComplianceState` enum:

```
// Decompiled with JetBrains decompiler
// Type: Microsoft.Management.Clients.IntuneManagementExtension.Win32AppPlugIn.StateMessageComplianceState
// Assembly: Microsoft.Management.Clients.IntuneManagementExtension.Win32AppPlugIn, Version=5.0.0.0, Culture=neutral, PublicKeyToken=null
// MVID: 462BEA3E-33FE-4F18-9587-6F5D8A46A52D
// Assembly location: C:\Program Files (x86)\Microsoft Intune Management Extension\Microsoft.Management.Clients.IntuneManagementExtension.Win32AppPlugIn.dll

namespace Microsoft.Management.Clients.IntuneManagementExtension.Win32AppPlugIn
{
    public enum StateMessageComplianceState
    {
        Installed = 1,
        NotInstalled = 2,
        Error = 4,
        Unknown = 5,
        Cleanup = 100, // 0x00000064
    }
}
```

A yellow box highlights the list of enum values: `Installed`, `NotInstalled`, `Error`, `Unknown`, and `Cleanup`.

```
$stateMessageComplianceState = @{
    1   = "Installed"
    2   = "NotInstalled"
    4   = "Error"
    5   = "Unknown"
    100 = "Cleanup"
}
```

# Digging into win32 app policy event state messages

## State Message Magic



The screenshot shows a blog post titled "Win32 app State Messages Demystified" by Ben Whitmore. The post is dated 2023-08-28 and has a 6-minute read time. The content discusses Win32 app state messages and their storage in the local registry for policies processed by the client, including how to convert state values into readable formats. A bulleted list of topics is provided at the bottom.

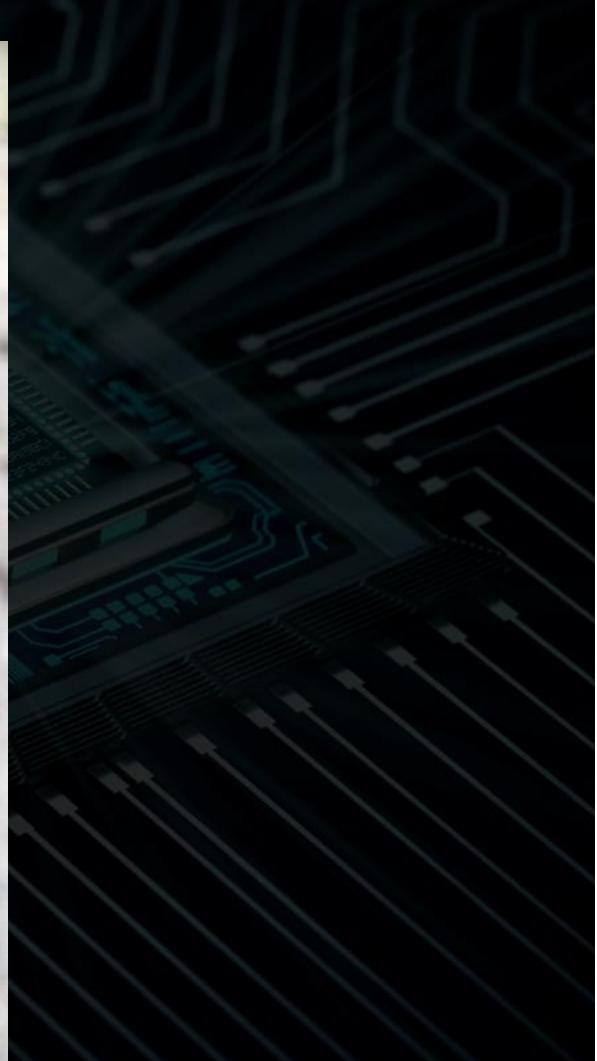
## Win32 app State Messages Demystified

Ben Whitmore | 2023-08-28 | Add comment | 6 min read

In this post we will do some digging on Win32 app state messages and look at the compliance state and enforcement state messages stored in the local registry for win32 app policies processed by the client. We will also take the state values and convert them into a readable format to help you understand if a Win32 app was processed successfully

- [Where are Win32 app policy results stored on the client?](#)
  - [Compliance State Messages](#)
  - [Enforcement State Messages](#)
- [Understanding State Messages](#)
  - [Applicability](#)
  - [ComplianceState](#)
  - [DesiredState](#)
  - [TargetingMethod](#)
  - [InstallContext](#)

# Digging into win32 app policy event state messages



# How the IME handles failures and retries

Failed apps retry 3 times every 5 minutes and then every 24 hours if they are required and the installer exits with a known retry code

Failed apps retry every 24 hours if they are required, and the installer exits with a failure or unknown exit code

Home > Apps | Windows > Windows | Windows apps > PMPC Update Notepad++ 8.5.8 (x64)

## PMPC Update Notepad++ 8.5.8 (x64) | Properties

Client Apps

Search

Overview

Manage

Properties

Monitor

Allow available uninstall

No

Install behavior

System

Device restart behavior

Determine behavior based on return codes

Return codes

0 Success

1707 Success

3010 Soft reboot

1641 Hard reboot

1618 Retry

1 Failed

# How the IME handles failures and retries

- When a new app is assigned, it is evaluated
- Time Column is local | Time in the lower row is UTC
- Two components:
  - Reevaluation Schedule Manager (subgraph) – expires and is evaluated every 8 hours
  - Global Retry Schedule (GRS) - expires every 24 hours; it controls when a failed app install is retried

[i]	IntuneManagementEx...	Get policies = [{"Id": "5cf8e28-25a4-44f1-86d0-a0d107dd0a5d", "Name": "Update for Notepad++ 8.5.8 (x64)", "Version": 1, "Intent": 3, "TargetType": 2, "AppApplicabilityStateDueToAssgini": 10/20/2023 3:47:51.916}	
[i]	IntuneManagementEx...	[Win32App][V3Processor] Processing 1 subgraphs.	10/20/2023 3:47:51.947
⚠	IntuneManagementEx...	[Win32App][ReevaluationScheduleManager] Did not find any previous reevaluation check-in time.	10/20/2023 3:47:52.009
⚠	IntuneManagementEx...	[Win32App][ReevaluationScheduleManager] Did not find any previous subgraph reevaluation time at key RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfitQI=.	10/20/2023 3:47:52.009
[i]	IntuneManagementEx...	[Win32App][ReportingManager] App with id: 5cf8e28-25a4-44f1-86d0-a0d107dd0a5d and prior AppAuthority: V2 could not be loaded from store. Reporting state initialized with in:	10/20/2023 3:47:57.916
[i]	IntuneManagementEx...	[Win32App][ReportingManager] Not sending status update for user with id: 807efa31-c262-4f9c-9372-c22189e33964 and app: 5cf8e28-25a4-44f1-86d0-a0d107dd0a5d because there is n	10/20/2023 3:47:57.931
[i]	IntuneManagementEx...	[Win32App][ReportingManager] Real time status is not reportable for user: 807efa31-c262-4f9c-9372-c22189e33964 and app: 5cf8e28-25a4-44f1-86d0-a0d107dd0a5d after switch to '	10/20/2023 3:47:57.931
[i]	IntuneManagementEx...	[Win32App][ReportingCacheManager] No full sync time found for user: 807efa31-c262-4f9c-9372-c22189e33964, which is treated as expired. All targeted apps will be evaluated and	10/20/2023 3:47:57.947
[i]	IntuneManagementEx...	[Win32App][V3Processor] Processing subgraph with app ids: 5cf8e28-25a4-44f1-86d0-a0d107dd0a5d	10/20/2023 3:47:57.947
[i]	IntuneManagementEx...	[Win32App][GRSManager] Reading GRS values from storage path: 807efa31-c262-4f9c-9372-c22189e33964\GRS\RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfitQI=\.	10/20/2023 3:47:57.963
[i]	IntuneManagementEx...	[Win32App][GRSManager] App with id: 5cf8e28-25a4-44f1-86d0-a0d107dd0a5d has no recorded GRS value which will be treated as expired.Hash = RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGI	10/20/2023 3:47:57.963
[i]	IntuneManagementEx...	[Win32App][ReevaluationScheduleManager] Subgraph has no recorded reevaluation info which will be treated as expired.Hash = RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfitQI=	10/20/2023 3:47:57.963
[i]	IntuneManagementEx...	[Win32App][ReevaluationScheduleManager] Setting subgraph reevaluation time with value: 10/20/2023 9:47:57 AM for subgraph with hash RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfitQI=	10/20/2023 3:47:57.963



# How the IME handles failures and retries

Policy is processed and GRS key is set

Win32Apps	
35c0db33-eb75-406a-bf13-746962020e71	
> 504de8c0-599b-4221-aed4-b7c9f1ce6d9f 1	
> 69f3c293-fc66-4e23-aacc-21f05573c230_1	
GRS	
93MnyvQHZgt0ipIF+ +GN6iS1X+VN+FO5zDecFEC13pk=	
9UknF1kYjt6jXX0IAidS6GgOvVQmiscSMgiSLf37T3g=	
kmCrDCSam3VSIHXltIUNRGSXQgbM0ybycCcQgBDrl4w=	

Name	Type	Data
ab(Default)	REG_SZ	(value not set)
ab69f3c293-fc66-4e23-aacc-21f05573c230	REG_SZ	12/07/2023 11:15:27
abSubgraphEvaluationTimeUTC	REG_SZ	12/07/2023 11:14:25

# How the IME handles failures and retries

In this example, the app installer terminated with a known retry code and tried 3 more times to attempt the installation (5 minute intervals)

[Win32App] ===Step== Execute retry 0	10/20/2023 3:48:
[Win32App] ===Step== InstallBehavior Regul	10/20/2023 3:48:
PatchMyPC-ScriptRunner.exe /UpdatePackage	
[Win32App] SetCurrentDirectory: C:\WINDOWS\	
[Win32App] Launch Win32AppInstaller in mach	
[Win32App] Installer process timeout millis	
[Win32App] process id = 3064	
[Win32App] lastWin32Error 0 after CreatePro	
[Win32App] lastHRESULT -2147024896 after Cr	
[Win32App] Create installer process success	
[Win32App] Create installer process success	
[Win32App] lpExitCode is defined as Retry	
[Win32App] SetCurrentDirectory back to C:\W	
[Win32App] Close handle	
[Win32App] DeviceRestartBehavior: 0	
[Win32App] Sleep 5 minute(s) before retry	
[Win32App] hResultFromWin32 -2147023278	
[Win32App] lpExitCode 1618	
<b>Initial Install</b>	
1	
[Win32App] ===Step== Execute retry 1	10/20/2023 3:53:
[Win32App] ===Step== InstallBehavior Regul	10/20/2023 3:53:
PatchMyPC-ScriptRunner.exe /UpdatePackage	
[Win32App] lastWin32Error 0 after CreatePro	
[Win32App] lastHRESULT -2147024896 after Cr	
[Win32App] Create installer process success	
[Win32App] process id = 8816	
[Win32App] Installer process timeout millis	
[Win32App] process id = 10636	
[Win32App] Create installer process success	
[Win32App] process id = 11004	
[Win32App] Installer process timeout millis	
[Win32App] lastWin32Error 0 after CreatePro	
[Win32App] App with id: 5cf8e28-25a4-44f1-	
[Win32App] SetCurrentDirectory back to C:\W	
[Win32App] lastHRESULT -2147024896 after Cr	
[Win32App] lastWin32Error 0 after WaitForSi	
[Win32App] lpExitCode is defined as Retry	
[Win32App] Installation is done, collecting	
[Win32App] Close handle	
[Win32App] DeviceRestartBehavior: 0	
[Win32App] Sleep 5 minute(s) before retry	
[Win32App] hResultFromWin32 -2147023278	
[Win32App] lpExitCode 1618	
2	
[Win32App] ===Step== Execute retry 2	10/20/2023 3:58:
[Win32App] ===Step== InstallBehavior Regul	10/20/2023 3:58:
PatchMyPC-ScriptRunner.exe /UpdatePackage	
[Win32App] lastWin32Error 0 after CreatePro	
[Win32App] lastHRESULT -2147024896 after Cr	
[Win32App] Create installer process success	
[Win32App] process id = 11004	
[Win32App] Installer process timeout millis	
[Win32App] lastWin32Error 0 after CreatePro	
[Win32App] App with id: 5cf8e28-25a4-44f1-	
[Win32App] SetCurrentDirectory back to C:\W	
[Win32App] lastHRESULT -2147024896 after Cr	
[Win32App] lastWin32Error 0 after WaitForSi	
[Win32App] lpExitCode is defined as Retry	
[Win32App] Installation is done, collecting	
[Win32App] Close handle	
[Win32App] DeviceRestartBehavior: 0	
[Win32App] Sleep 5 minute(s) before retry	
[Win32App] hResultFromWin32 -2147023278	
[Win32App] lpExitCode 1618	
3	
[Win32App] ===Step== Execute retry 3	10/20/2023 4:03:
[Win32App] ===Step== InstallBehavior Regul	10/20/2023 4:03:
PatchMyPC-ScriptRunner.exe /UpdatePackage	
[Win32App] lastWin32Error 0 after CreatePro	
[Win32App] lastHRESULT -2147024896 after Cr	
[Win32App] Create installer process success	
[Win32App] process id = 11004	
[Win32App] Installer process timeout millis	
[Win32App] lastWin32Error 0 after CreatePro	
[Win32App] App with id: 5cf8e28-25a4-44f1-	
[Win32App] SetCurrentDirectory back to C:\W	
[Win32App] lastHRESULT -2147024896 after Cr	
[Win32App] lastWin32Error 0 after WaitForSi	
[Win32App] lpExitCode is defined as Retry	
[Win32App] Installation is done, collecting	
[Win32App] Close handle	
[Win32App] DeviceRestartBehavior: 0	
[Win32App] Sleep 5 minute(s) before retry	
[Win32App] hResultFromWin32 -2147023278	
[Win32App] lpExitCode 1618	

# How the IME handles failures and retries

After 3 failed retries, the policy will be tried again in 24 hours time when the GRS value expires

Get policies = [{"Id": "5cf8e28-25a4-44f1-86d0-a0d107dd0a5d", "Name": "Update for Notepad++ 8.5.8 (x64)", "Version": 1, "Intent": 3, "TargetType": 2, "AppApplicabilityStateDueToAssig...},	10/21/2023 4:57:35.
[Win32App] Got 1 Win32App(s) for user 807efa31-c262-4f9c-9372-c22189e33964 in session 2	10/21/2023 4:57:35.
[Win32App] Got result with session id 60f6aa80-8671-428d-8bc4-bde8f8a3c186	10/21/2023 4:57:35.
[Win32App] espSupportForSupersedenceEnabled : False, v2AppPrococesorDisabled : True	10/21/2023 4:57:35.
[Win32App][DetectionActionHandler] Detection running for policy with id: 5cf8e28-25a4-44f1-86d0-a0d107dd0a5d.	10/21/2023 4:57:35.
"C:\Program Files (x86)\Microsoft Intune Management Extension\agentexecutor.exe" -powershellDetection "C:\Program Files (x86)\Microsoft Intune Management Extension\Content\DetectionScript... 10/21/2023 4:57:35.	10/21/2023 4:57:35.
[Win32App] Detection script file C:\Program Files (x86)\Microsoft Intune Management Extension\Content\DetectionScripts\5cf8e28-25a4-44f1-86d0-a0d107dd0a5d_1.ps1 is saved.	10/21/2023 4:57:35.
[Win32App] SideCarScriptDetectionManager create files for outputs	10/21/2023 4:57:35.
[Win32App] Start detectionManager SideCarScriptDetectionManager	10/21/2023 4:57:35.
[Win32App] DetectionType 3	10/21/2023 4:57:35.
[Win32App] ProcessDetectionRules Parsing InstallEx...	10/21/2023 4:57:35.
[Win32App] ProcessDetectionRules starts	10/21/2023 4:57:35.
[Win32App][DetectionActionHandler] Handler invoked for 1 app detections.	10/21/2023 4:57:35.
[Win32App][V3Processor] Processing subgraph with app ids: 5cf8e28-25a4-44f1-86d0-a0d107dd0a5d	10/21/2023 4:57:35.
[Win32App][ReevaluationScheduleManager] Setting subgraph reevaluation time with value: 10/21/2023 10:57:35 AM for subgraph with hash RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfi 10/21/2023 4:57:35.	10/21/2023 4:57:35.
[Win32App][ReevaluationScheduleManager] Subgraph reevaluation interval is expired.Hash = RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfitQI=	10/21/2023 4:57:35.
[Win32App][GRSManager] App with id: 5cf8e28-25a4-44f1-86d0-a0d107dd0a5d is expired Hash = RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfitQI=GRSTimeUTC = 10/20/2023 9:48:16 AM ...	10/21/2023 4:57:35.
[Win32App][GRSManager] Found GRS value: 10/20/2023 09:48:16 at key 807efa31-c262-4f9c-9372-c22189e33964\GRS\RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfitQI=\5cf8e28-25a4-44f1-8	10/21/2023 4:57:35.
[Win32App][GRSManager] Reading GRS values from storage path: 807efa31-c262-4f9c-9372-c22189e33964\GRS\RaBK4Zlza1ZC19uOMmgh0I+TgBdDX3vPGIcPpFfitQI=.	10/21/2023 4:57:35.



# How the IME handles failures and retries

## Summary

1. If the install fails, does the exit code indicate “Retry”? If so, retry 3 more times every 5 minutes
2. If the installation is failed (still), add the app to the GRS
3. Evaluate a sub graph every 8 hours to check when 24 hours have passed since the app was added to GRS
4. After 24 hours, retry the installation. If failed, update GRS check-in time value
5. Repeat forever until successful



# Inventory

The IME will inventory installed applications.

The screenshot shows the Microsoft Intune interface for managing devices. On the left, a navigation sidebar lists various management categories like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. Under the 'Devices' section, there's a 'Discover apps' link, which is highlighted with a yellow box. The main content area displays the 'BB-W10-5 | Discovered apps' page. At the top, there's a search bar, a refresh button, an export button, and a 'Columns' dropdown. A callout box highlights '50 detected apps'. Below this, a table lists the installed applications with their names and versions. The table has two columns: 'Application name' and 'Application version'.

Application name ↑	Application version
7-Zip 23.01 (x64 edition)	23.01.00.0
Adobe Acrobat (64-bit)	22.003.20258
Google Chrome	111.0.5563.111
Microsoft Edge	116.0.1938.62
Microsoft Edge Update	13.177.11
Microsoft Edge WebView2 Runtime	116.0.1938.62
Microsoft Intune Management Extension	1.68.204.0
Microsoft OneDrive	23.169.0813.0001
Microsoft Update Health Tools	3.72.0.0

# Inventory

The screenshot shows a web-based application interface for monitoring discovered applications. The left sidebar contains navigation links for Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area has a breadcrumb navigation path: Home > Apps | Monitor > Monitor. The title is "Monitor | Discovered apps". On the left, there is a sidebar with "App licenses" and "Discovered apps" selected, both highlighted with orange boxes. Below the sidebar is a search bar labeled "Search by application name". The main table displays 192 records, showing 1 to 20 of them. The columns are Application name, Application version, and Device count. The data includes:

Application name	Application version	Device count
7-Zip 22.00 (x64 edition)	22.00.00.0	1
7-Zip 22.01 (x64 edition)	22.01.00.0	1
7-Zip 23.01 (x64 edition)	23.01.00.0	1
AVG AntiVirus Free	23.6.3290	1
Adobe Acrobat (64-bit)	22.003.20258	1
Adobe Acrobat Reader DC MUI	21.005.20060	2
Apple Application Support (64-bit)	8.7	1
Bonjour	3.1.0.1	1
CCleaner	6.13	1
Citrix Workspace 2203	22.3.1000.1054	1



# Inventory

The IME performs a delta inventory every 24hrs and/or when the IME service starts. A full inventory is taken every 7 days and the first time the IME is installed

Configuration Manager Trace Log Tool - [C:\ProgramData\Microsoft\IntuneManagementExtension\Logs\IntuneManagementExtension.log]

File Tools Window Help

Log Text

```
[Win32AppInventory] Collected app inventory details: 000017b8ad1c79f2b7e3a44b100e9bf1aac40000ffff, Npcap, 1.31, Nmap Project, 65535, 1/1/0001 12:00:00 ... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Collected app inventory details: 0000ad178200ccce1314ccb24a37fbcef41e0000ffff, Wireshark 3.4.9 64-bit, 3.4.9, The Wireshark developer c... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Collected app inventory details: 0000236d849f9ec02013f257a9e72a9ece3a0000ffff, Microsoft Visual C++ 2015-2019 Redistributable (x64) ... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Collected app inventory details: 0000d4675245654010a4a989f2d3a6f765ba00000904, Microsoft Intune Management Extension, 1.68.204.0, ... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Collected app inventory details: 00007579bd23827d79e1a234460072cf68690000ffff, Microsoft OneDrive, 23.169.0813.0001, Microsoft Corp... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Printing out saved inventory
[Win32AppInventory] Saved app inventory details: 000007475bf0297ef8f5849629a1f8c1e5810000ffff, Microsoft Edge WebView2 Runtime, 116.0.1938.62, , , 1/1/0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 000017b8ad1c79f2b7e3a44b100e9bf1aac40000ffff, Npcap, 1.31, , , 1/1/0001 12:00:00 AM IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 0000236d849f9ec02013f257a9e72a9ece3a0000ffff, Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 000030e6c08fd7828e0e5e532186cd1949e50000ffff, Microsoft Edge, 116.0.1938.62, , , 1/1/0001 12:00:00 AM IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 0000423d7ac1aa1c6dd2408775f90d66d83000000904, 7-Zip 23.01 (x64 edition), 23.01.00.0, , , 1/1/0001 12:00:0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 00004a8798691c8a793c950b8cfa1449110a0000ffff, Microsoft Visual Studio Code, 1.72.2, , , 1/1/0001 12:00:0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 000069ce0ebb5be18a86c7b8ccaa87c5ff900000000, Microsoft Update Health Tools, 3.72.0.0, , , 1/1/0001 12:0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 000075065b14bde73e32cf51a78e9f29750e00000904, Adobe Acrobat (64-bit), 22.003.20258, , , 1/1/0001 12:00:... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 00007579bd23827d79e1a234460072cf68690000ffff, Microsoft OneDrive, 23.169.0813.0001, , , 1/1/0001 12:00:0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 0000a668ea4b3e2f722eea3eac6289b4f8680000ffff, Microsoft Edge Update, 1.3.177.11, , , 1/1/0001 12:00:0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 0000ad178200ccce1314ccb24a37fbcef41e0000ffff, Wireshark 3.4.9 64-bit, 3.4.9, , , 1/1/0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 0000b12c1ab721091a0752f94712d19b213300000904, Google Chrome, 111.0.5563.111, , , 1/1/0001 12:00:0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 0000b6934951a9dacb4399be4bebdee2a82700000904, PutTY release 0.77 (64-bit), 0.77, , , 1/1/0001 12:00:0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 0000bbd452451e42617d4489f9ac9a7637d70000ffff, Notepad++ (64-bit x64), 8.4.6, , , 1/1/0001 12:00:0... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Saved app inventory details: 0000d4675245654010a4a989f2d3a6f765ba00000904, Microsoft Intune Management Extension, 1.68.204.0, ... IntuneManagementEx 31/08/2023 10:53 4 (0x4)
[Win32AppInventory] Computing delta inventory... newly collected inventory count = 15, loaded from registry count = 15
[Win32AppInventory] Computing delta inventory...Done. Add count = 0, Modify count = 0, Delete count = 0
[Win32AppInventory] report type is 0
[Win32AppInventory] No change detected in win32 app inventory delta update and hence not uploading data to SideCarGatewayService.
[Win32AppInventory] Inventory collector thread stopped.
[OnStart](OnStart) {"Message":"Agent StartWork Ends","Colmetadata":"DeviceId;AccountId;ScaleUnit;Exception;","Col1":"6fbf5c2c-8ce4-49
[Win32AppInventory] No change detected in win32 app inventory delta update and hence not uploading data to SideCarGatewayService.
```

Date/Time: 31/08/2023 10:53:01 Component: IntuneManagementExtension  
Thread: 4 (0x4) Source:

Scan full every 7 days

```
private bool IsFullInventoryDue()
{
    if (!RegistryHelper.FirstTimeFlagExists())
    {
        RegistryHelper.SaveFirstTimeFlag();
        return true;
    }
    return RegistryHelper.GetLastInventoryFullSyncTimeUtc() < DateTime.UtcNow.AddDays(-7.0);
}
```

Remember .NET  
disassemblers!

# Inventory

The IME uses a specific WMI class to query installed software

```
{  
    List<WindowsApplication> savedInventory = RegistryHelper.LoadApplicationInventoryFromRegistr  
    reportToSend.ApplicationInventory = this.ComputeDeltaInventoryList(windowsApplicationList, s  
    reportToSend.InventoryReportType = 0;  
}  
Win32AppInventoryLog.TraceInformation(string.Format("[Win32AppInventory] report type is {0}",  
if (reportToSend.InventoryReportType == 1 || reportToSend.InventoryReportType == 0 && ((IEnumera  
    this.uploader.UploadInventory(reportToSend, sessionId);  
else  
    Win32AppInventoryLog.TraceInformation("[Win32AppInventory] No change detected in win32 app i  
}  
  
public IEnumerable<WindowsApplication> GetWin32AppInventoryExpanded()  
{  
    string queryString = "select * from Win32_InstalledWin32Program";  
    List<WindowsApplication> inventoryExpanded = new List<WindowsApplication>();  
    Dictionary<string, WindowsApplication> dictionary = new Dictionary<string, WindowsApplication>;  
    try  
    {  
        using (ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher(quer  
        {  
            foreach (ManagementObject managementObject in managementObjectSearcher.Get())  
            {  
                WindowsApplication windowsApplication = new WindowsApplication()  
                {  
                    ApplicationId = (string) managementObject["ProgramID"],  
                    ApplicationName = (string) managementObject["Name"],  
                    ApplicationPublisher = (string) managementObject["Vendor"],  
                    ApplicationVersion = (string) managementObject["Version"],  
                    ApplicationLanguage = (string) managementObject["Language"]  
                };  
                inventoryExpanded.Add(windowsApplication);  
                if (!dictionary.ContainsKey(windowsApplication.ApplicationName))  
                    dictionary.Add(windowsApplication.ApplicationName, windowsApplication);  
            }  
        }  
    }  
}
```



# Inventory

WMI Explorer 2.0.0.2 (Administrator)

File Launch Help

Computer: BB-W10-5 Connect

Mode: Asynchronous Filter: %

Class Enumeration Options: Include System Classes, Include Perf Classes, Include CIM Classes, Include MSFT Classes Refresh Classes

Namespaces: \\BB-W10-5\ROOT

- ROOT\Appv
- ROOT\CIMV2
  - ROOT\CIMV2\mdm
  - ROOT\CIMV2\ms\_409
  - ROOT\CIMV2\power
  - ROOT\CIMV2\Security
  - ROOT\CIMV2\TerminalServices
- ROOT\Cli
- ROOT\DEFAULT
- ROOT\directory
- ROOT\Hardware
- ROOT\Interop
- ROOT\MEM
- ROOT\Microsoft
- ROOT\msdtc
- ROOT\PEH
- ROOT\Policy
- ROOT\RSOP
- ROOT\SECURITY
- ROOT\SecurityCenter
- ROOT\SecurityCenter2
- ROOT\ServiceModel
- ROOT\StandardCimv2
- ROOT\subscription
- ROOT\WMI

Classes (418) Search Quick Filter:

Name	Lazy...	Description	Path
Win32_DMACHannel	False	The Win32_DMACH...	\BB-W10-5\ROC
Win32_DriverForDevice	False	A generic association...	\BB-W10-5\ROC
Win32_DuplicateFileAction	False	The DuplicateFileActi...	\BB-W10-5\ROC
Win32_Environment	False	The Win32_Environm...	\BB-W10-5\ROC
Win32_EnvironmentSpecification	False	Instances of this class...	\BB-W10-5\ROC
Win32_ExtensionInfoAction	False	The ExtensionInfoActi...	\BB-W10-5\ROC
Win32_Fan	False	The Win32_Fan class...	\BB-W10-5\ROC
Win32_FileSpecification	False	Each instance of this ...	\BB-W10-5\ROC
Win32_FolderRedirection	False		\BB-W10-5\ROC
Win32_FolderRedirectionHealth	False		\BB-W10-5\ROC
Win32_FolderRedirectionHealthC...	False		\BB-W10-5\ROC
Win32_FolderRedirectionUserCon...	False		\BB-W10-5\ROC
Win32_FontInfoAction	False	The RegisterFonts ac...	\BB-W10-5\ROC
Win32_Group	False	The Win32_Group cla...	\BB-W10-5\ROC
Win32_GroupInDomain	False	The Win32_GroupInD...	\BB-W10-5\ROC
Win32_GroupUser	False	The Win32_GroupUs...	\BB-W10-5\ROC
Win32_HeatPipe	False	The Win32_HeatPipe...	\BB-W10-5\ROC
Win32_IDEController	False	The Win32_IDEContr...	\BB-W10-5\ROC
Win32_IDEControllerDevice	False	The Win32_IDEContr...	\BB-W10-5\ROC
Win32ImplementedCategory	False	The Win32_Implemen...	\BB-W10-5\ROC
Win32_InfraredDevice	False	The Win32_InfraredD...	\BB-W10-5\ROC
Win32_IniFileSpecification	False	This class contains th...	\BB-W10-5\ROC
Win32_InstalledProgramFramework	False	The Win32_Installed...	\BB-W10-5\ROC
Win32_InstalledSoftwareElement	False	The InstalledSoftwar...	\BB-W10-5\ROC
Win32_InstalledStoreProgram	False	The Win32_Installed...	\BB-W10-5\ROC
Win32_InstalledWin32Program	False	The Win32_Installed...	\BB-W10-5\ROC
Win32_IP4PersistedRouteTable	False	The IP4PersistedRou...	\BB-W10-5\ROC
Win32_IP6PersistedRouteTable	False	The IP6PersistedRou...	\BB-W10-5\ROC

Instances (15) Properties (7) Methods (0) Query Script Logging

Instance Options: Quick Filter, Show Null Values, Show System Properties, Refresh Instances, Refresh Object

Instances: Win32\_InstalledWin32Program.ProgramId, Win32\_InstalledWin32Program.ProgramId

Properties:

Name	Type	Description
*ProgramId	String	000007475bf0297ef8f5849629a1f8c1e581000ffff
Language	String	65535
MsiPackageCode	String	
MsiProductCode	String	
Name	String	Microsoft Edge WebView2 Runtime
Vendor	String	Microsoft Corporation
Version	String	116.0.1938.62

Name: Type - String  
Program name

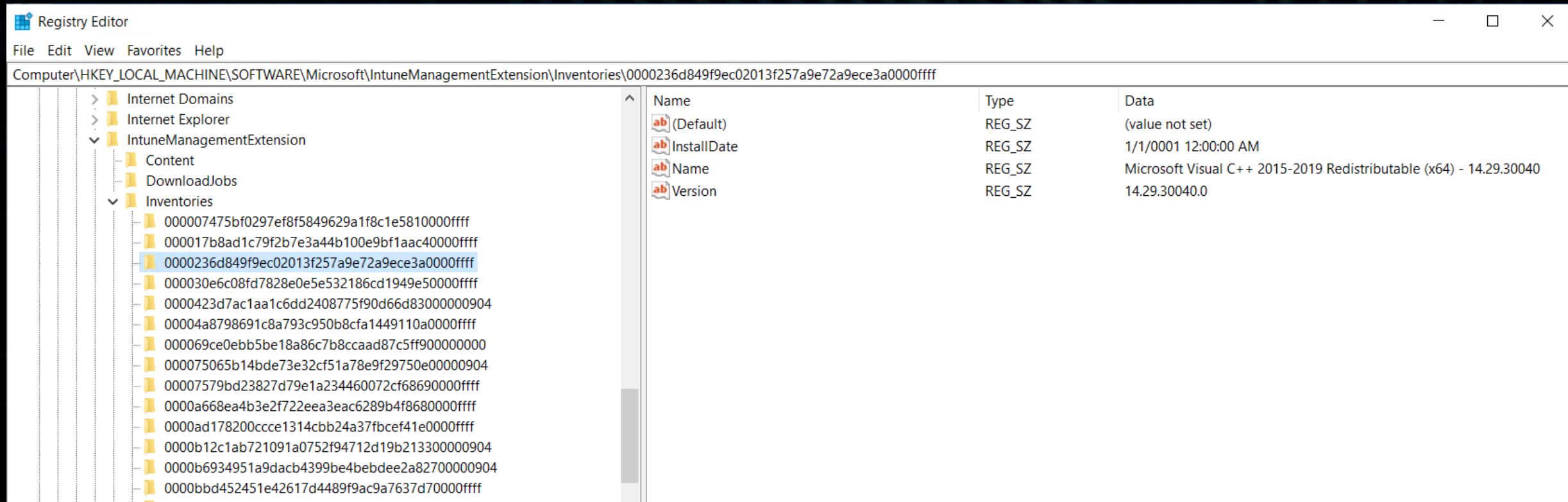
WQL Query (Selected Object): SELECT \* FROM Win32\_InstalledWin32Program WHERE ProgramId='000007475bf0297ef8f5849629a1f8c1e581000ffff'

Query: SELECT \* FROM Win32\_InstalledWin32Program WHERE ProgramId='000007475bf0297ef8f5849629a1f8c1e581000ffff' Execute

Retrieved 418 classes from ROOT\CIMV2 that match specified criteria. Retrieved 15 instances from Win32\_InstalledWin32Program.

Time to Enumerate Instances: 00:03.640

# Inventory



HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\Inventories



TunedIn:London



# Inventory

1. New apps appear in Intune reports fairly quickly
2. It can take up to 7 days for delta changes (removes) to be reflected in Intune reports
3. Inventory is run every 24 hours
4. A full inventory is run the first time and every 7 days, a delta inventory occurs subsequent runs
5. Delete FirstTimeRun key to force a full inventory

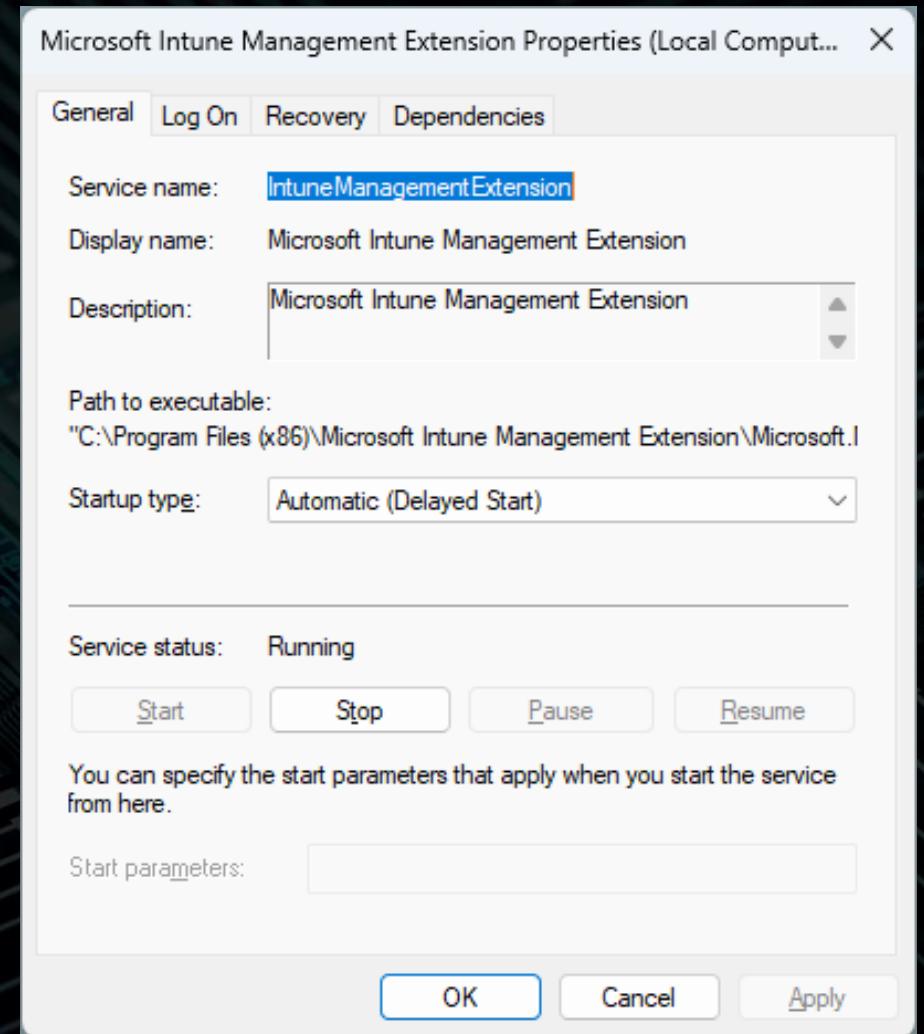
# Invoking the IME

When does the IME process policy?

- When the service starts
- Every 60 minutes

Can you invoke the policy on-demand?

- Can emu's fly?



# Invoking the IME

er

Home > Devices | Windows > Windows | Windows devices >

## DEMO1INTUNE

Search Retire Wipe Delete Remote lock Sync Reset passcode Restart Collect diagnostics Fresh Start

Overview

Manage Properties

Monitor

Hardware

Discovered apps

Device compliance

Essentials

Device name	: DEMO1INTUNE	Primary user	: MOD A
Management name	: admin_Windows_12/30/2022_11:31 PM	Enrolled by	: MOD A
Ownership	: Corporate	Compliance	: Compliant
Serial number	: [REDACTED]	Operating system	: Windows
Phone number	: ---	Device model	: Virtual I

See more

Device actions status

Sync initiated

# Invoking the IME

The screenshot shows the Microsoft Settings application interface. On the left is a navigation sidebar with the following items:

- Home
- Apps
- App categories
- Downloads & updates
- Devices
- Help & support
- My profile
- Settings** (highlighted with a red box)

The main content area is titled "Settings" and contains the following sections:

- Sync**: A button labeled "Sync" is highlighted with a red box. A large red arrow points from the "Settings" button in the sidebar to this button.
- App mode**: Personalize your app with a color mode.
  - Light
  - Dark
  - Windows default

Windows color settings
- Usage data**: Allow Microsoft to collect performance and usage data to help improve Microsoft products and services.

# Invoking the IME

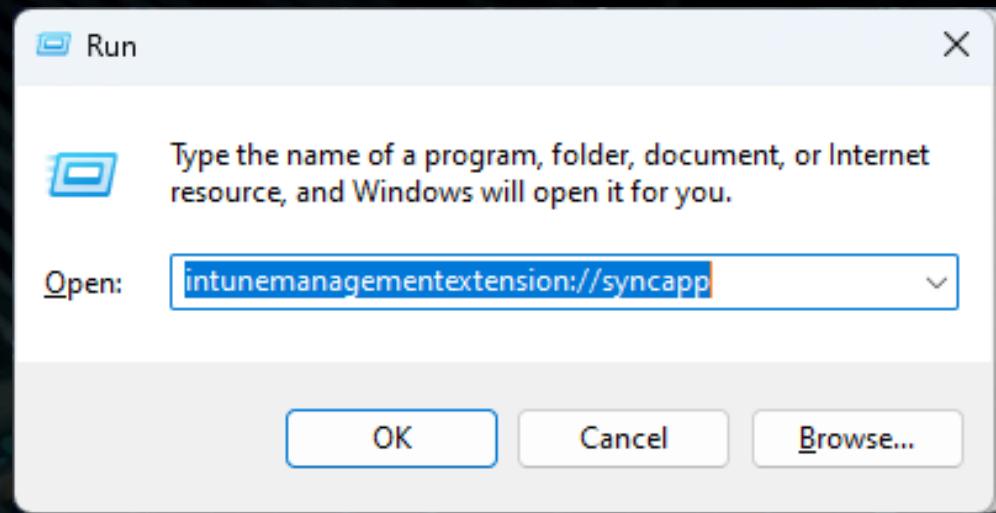
The screenshot shows the Windows Services snap-in window. On the left, there is a tree view under 'Microsoft Intune Management Extension' with options to 'Stop the service' and 'Restart the service'. Below this, a 'Description:' label is followed by the text 'Microsoft Intune Management Extension'. A red arrow points from the bottom of this section towards the list of services on the right. The main pane displays a table of services with columns: Name, Description, Status, Startup Type, and Log On As. The 'Microsoft Intune Management Extension' service is highlighted with a red border. The table data is as follows:

Name	Description	Status	Startup Type	Log On As
McpManagementService	<Failed to Read Description. Error Code: 1...	Running	Manual	Local System
MessagingService_42535c	Service supporting text messaging and rel...	Running	Manual (Trigger Start)	Local System
Microsoft (R) Diagnostics Hub Standard Collector Se...	Diagnostics Hub Standard Collector Servic...	Running	Manual	Local System
Microsoft Account Sign-in Assistant	Enables user sign-in through Microsoft ac...	Running	Manual (Trigger Start)	Local System
Microsoft App-V Client	Manages App-V users and virtual applicati...	Disabled	Disabled	Local System
Microsoft Cloud Identity Service	Supports integrations with Microsoft clou...	Running	Manual	Network Service
Microsoft Defender Antivirus Network Inspection Ser...	Helps guard against intrusion attempts tar...	Running	Manual	Local Service
Microsoft Defender Antivirus Service	Helps protect users from malware and othe...	Running	Automatic	Local System
Microsoft Edge Elevation Service (MicrosoftEdgeElev...	Keeps Microsoft Edge up to update. If this ...	Running	Manual	Local System
Microsoft Edge Update Service (edgeupdate)	Keeps your Microsoft software up to date. ...	Running	Automatic (Trigger Start)	Local System
Microsoft Edge Update Service (edgeupdate)	Keeps your Microsoft software up to date. ...	Running	Manual (Trigger Start)	Local System
Microsoft Intune Management Extension	Microsoft Intune Management Extension	Running	Automatic (Delayed Start)	Local System
Microsoft IIS SSL Initializer Service	Manages Internet SSL (SSCI) sessions from...	Running	Manual	Local System
Microsoft Keyboard Filter	Controls keystroke filtering and mapping	Disabled	Disabled	Local System
Microsoft Office Click-to-Run Service	Manages resource coordination, background...	Running	Automatic	Local System
Microsoft Passport	Provides process isolation for cryptograph...	Running	Manual (Trigger Start)	Local System
Microsoft Passport Container	Manages local user identity keys used to a...	Running	Manual (Trigger Start)	Local Service
Microsoft Software Shadow Copy Provider	Manages software-based volume shadow ...	Running	Manual	Local System
Microsoft Storage Spaces SMP	Host service for the Microsoft Storage Spa...	Running	Manual	Network Service
Microsoft Store Install Service	Provides infrastructure support for the Mi...	Running	Manual	Local System
Microsoft Update Health Service	Maintains Update Health	Running	Automatic (Delayed Start)	Local System

# Invoking the IME

URL Moniker FTW

Thanks to Oliver Kieselbach (MVP)



A screenshot of the Windows Registry Editor. The title bar says "Registry Editor". The left pane shows a tree view of registry keys under "Computer\HKEY\_CLASSES\_ROOT\intunemanagementextension\shell\open\command". One key is expanded, showing sub-keys "shell" and "open", with "open" further expanded to show "command". The right pane displays a table with columns "Name", "Type", and "Data". There is one entry: "Name" is "ab (Default)", "Type" is "REG\_SZ", and "Data" is "C:\Program Files (x86)\Microsoft Intune Management Extension\Microsoft.Management.Services.IntuneWindowsAgent.exe" %1.

```
$newShell = New-Object -ComObject Shell.Application  
$newShell.open("intunemanagementextension://syncapp")
```

<https://oliverkieselbach.com/2020/11/03/triggering-intune-management-extension-ime-sync/>

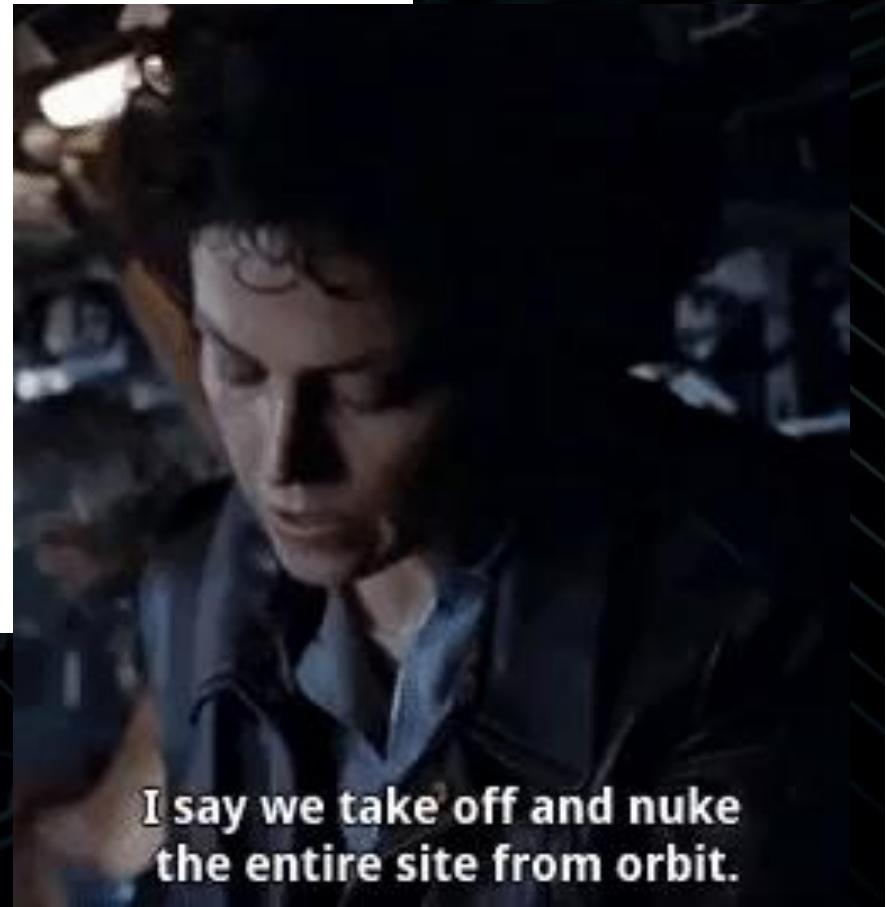
# Invoking the IME

Registry Editor

File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\Win32Apps\1301314b-c3e8-443d-9d69-6659e5ad1d08\GRS\xlzGRXP8f4sEuPxrf+37/deV4j\lorXQDF2hun35Hg=

Name	Type	Data
(Default)	REG_SZ	(value not set)
42f0a7c5-684e-449c-b230-6ca6b53bda75	REG_SZ	10/24/2023 19:26:34
SubgraphEvaluationTimeUTC	REG_SZ	10/24/2023 19:26:23

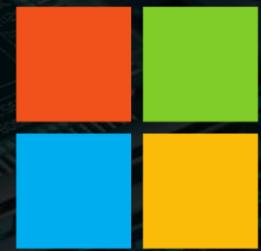


# Q&A

Thank you again to our Sponsors



TunedIn: London



Microsoft

8<sup>th</sup> December 2023