



EPM, The Chocolate Intune + Version 2 Factory

Start 13:00



SquaredUp



infinity



kpn
Partner Network



INSPARK



cegeka



EPM, The Chocolate Intune Version 2 Factory

Rudy Ooms / Joost Glijsteen



Sprekers



Joost Glijsteen

Sneakers
Deepdiving Intune
Job: Pink Elephant
Blog: JoostGlijsteen.com
@jgelijsteen



Rudy Ooms

Opening DLLs
Deepdiving Intune
Job: Patch My Pc
Blog: Call4cloud.nl
@Mister_mdm

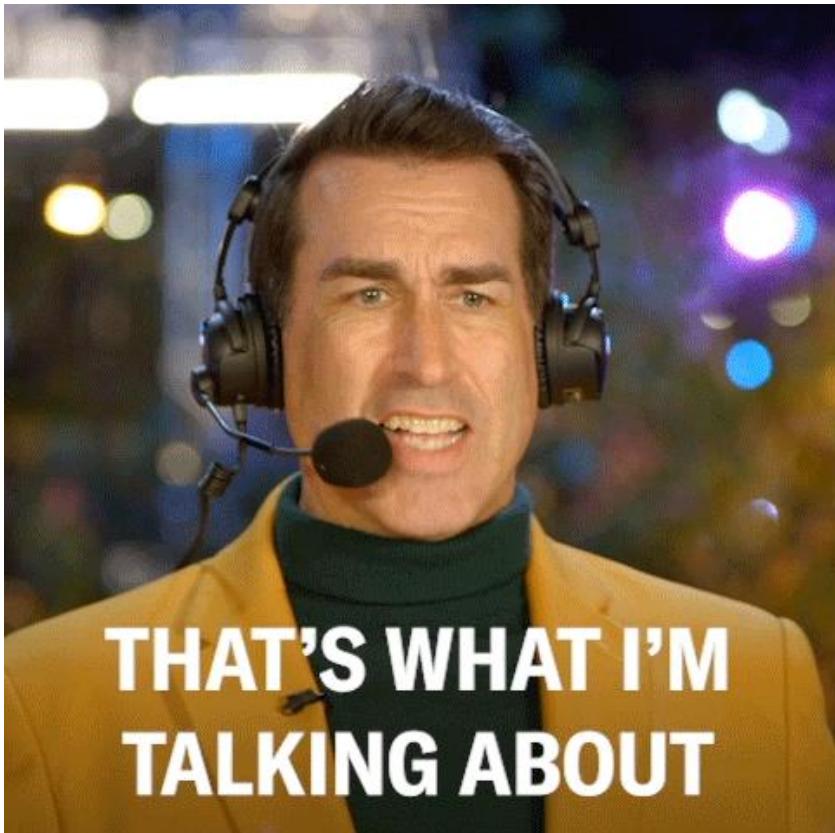


SquaredUp infinity





Agenda



- 1. Introduction to EPM**
- 2. Configuring EPM**
- 3. The EPM Enrollment?**
- 4. Deepdiving the Enrollment**
- 5. A quick recap**
- 6. Support Approved**
- 7. The elevation rules**
- 8. The Future is Bright!**
- 9. Recap**



DELL
Technologies



SquaredUp



infinity



1. Introduction

Security vs Productivity



Removing Admin Permissions

VS

Installing apps and peripherals



DELL
Technologies



SquaredUp





1. Introduction

Enforce least privilege access

- Reduce attack surface of local admins
- Protect corporate data by enabling least privilege access
- Support Zero Trust model

Enable productivity

- Use policy-based elevation management
- Flexibility to support standard users
- Ability to run approved processes as an admin

Insights

- Elevation reporting



DELL
Technologies



SquaredUp



infinity

INTERSTELLAR



kpn
Partner Network



INSPARK



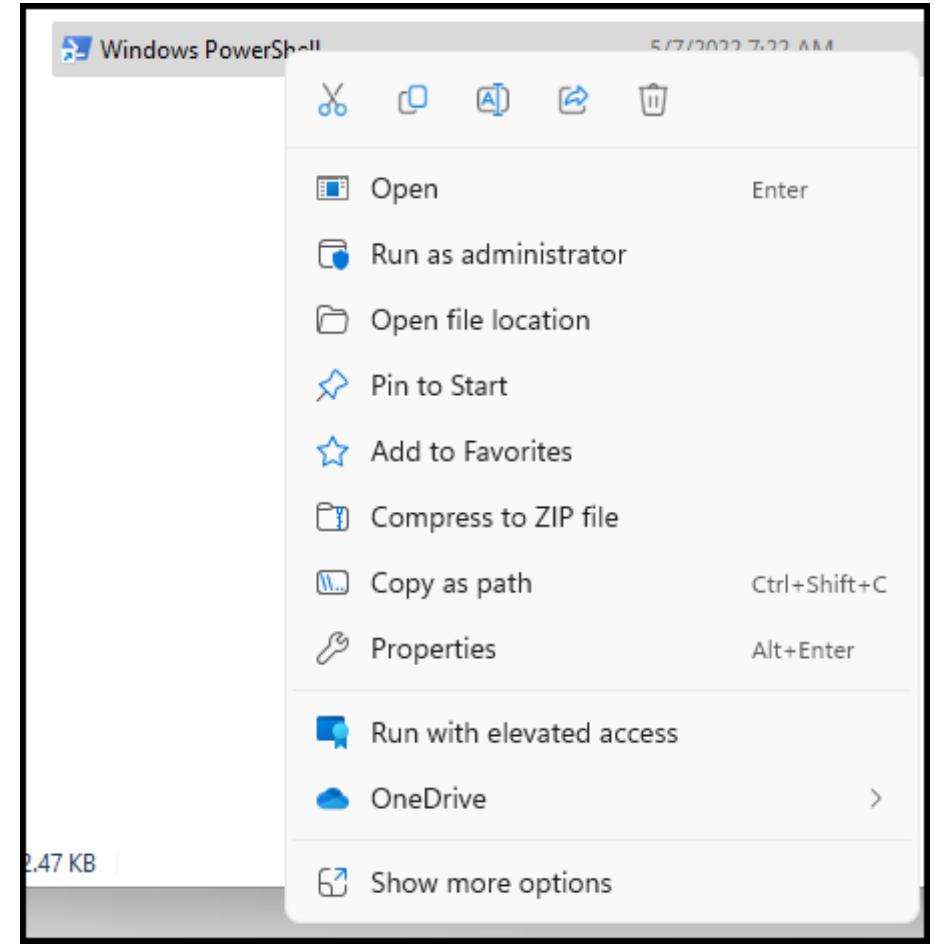
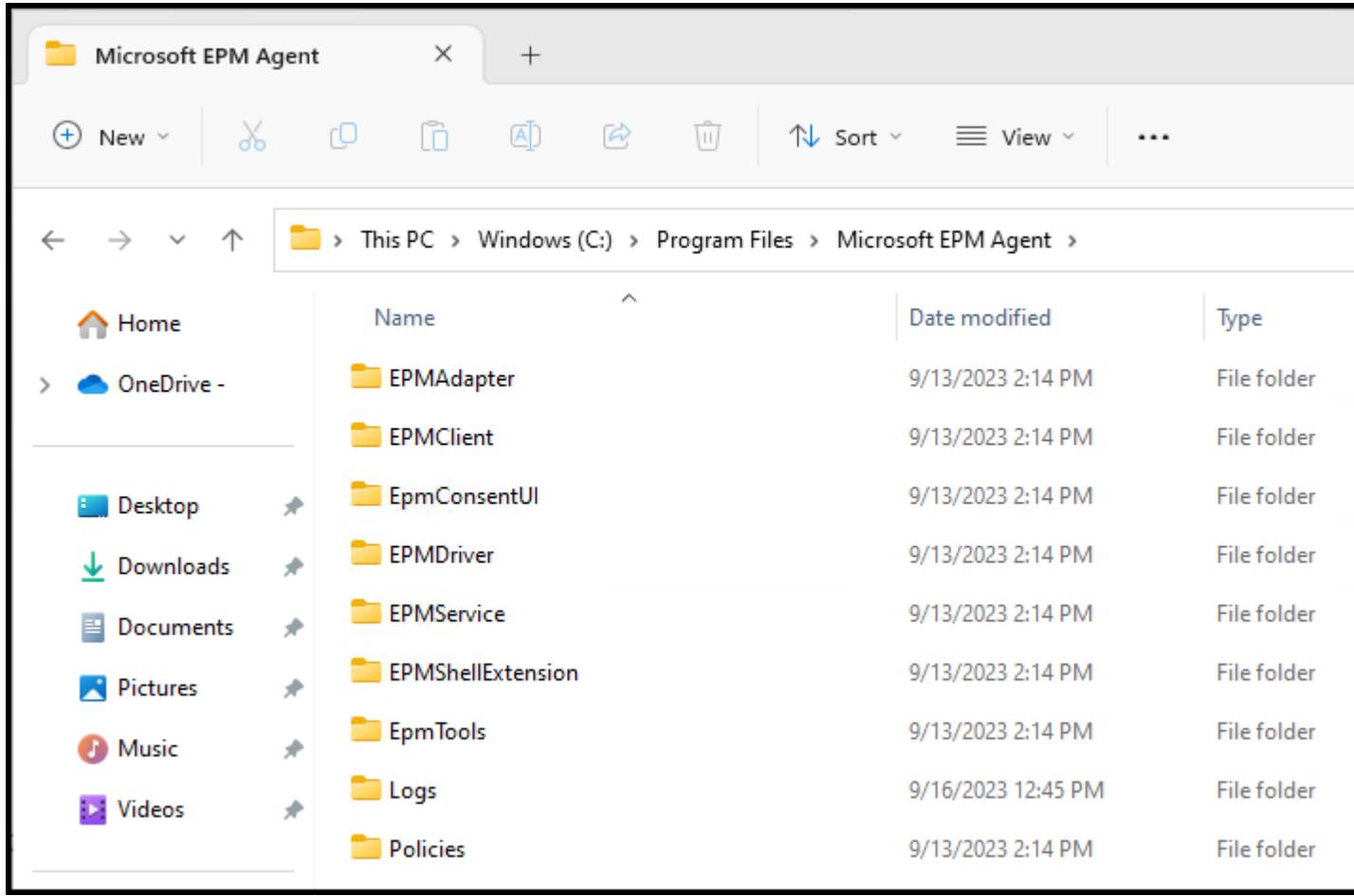
cegeka

2. EPM Elevation settings Policy

The screenshot shows the Microsoft Endpoint Security Overview page. The left sidebar includes links for Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area features a search bar and navigation links for Overview, All devices, Security baselines, and Security tasks. A central heading "Protect and secure devices from one place" is followed by a subtext: "Enable, configure, and deploy Microsoft Defender for Endpoint to help prevent security breaches and gain visibility into your organization's security posture." Three main sections are displayed:

- Microsoft recommended security settings**: Describes assigning baselines quickly and securely using recommended settings. Includes a "View Security Baselines" button.
- Simplified security policies**: Allows selecting categories to jump right in and start securing devices. Options include Antivirus, Disk encryption, Firewall, Attack surface reduction, Endpoint detection and response, and Account protection.
- Remediate endpoint weaknesses**: Lists vulnerabilities reported by Microsoft Defender for Endpoint and Threat and Vulnerability Management. Includes a "View security tasks" button and a link to Microsoft Defender for Endpoint.

EPM Agent magically appears!





But...how does EPM got installed?



3. The "EPM" Enrollment?

Tunnel to discovery.dm.microsoft.com:443		
discovery.dm.microsoft.com	/EnrollmentConfiguration?api-version=1.0	590
enrollment.dm.microsoft.com	/deviceenrollment/getpolicies?client-request-id=d8...	2,439
enrollment.dm.microsoft.com	/deviceenrollment/enroll?client-request-id=d884dc...	12,371

[MS-MDE2]: Mobile Device Enrollment Protocol Version 2 | Microsoft Learn

The sequence diagram illustrates the protocol flow:

- End user** sends a **user@domain** message to the **Discovery Service**.
- Discovery Service** sends a **Discover** message to the **Enrollment client**.
- Enrollment client** sends a **Get Security Token** message to the **Security Token Service**.
- Security Token Service** returns a **Security Token** message to the **Enrollment client**.
- Enrollment client** sends a **GetPolicies** message to the **Enrollment Service (XCEP)**.
- Enrollment Service (XCEP)** returns a **GetPoliciesResponse** message to the **Enrollment client**.
- Enrollment client** sends a **RequestSecurityToken** message to the **Enrollment Service (WSTEP)**.
- Enrollment Service (WSTEP)** returns a **RequestSecurityTokenResponseCollection** message to the **Enrollment client**.
- The **Enrollment client** then performs an **Enrollment Succeeded/ Failed** action.

RequestSecurityTokenResponseCollection XML structure:

```
XML View
<?xml version="1.0"?>
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RSTRC/wstep</a:Action>
    <a:RelatesTo>urn:uuid:urn:uuid:0d5a1441-5891-453b-becf-a2e5f6ea3749</a:RelatesTo>
  </s:Header>
  <s:Body>
    <RequestSecurityTokenResponseCollection xmlns="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
      <RequestSecurityTokenResponse>
        <TokenType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3PKIPathCert</TokenType>
        <RequestedSecurityToken>
          <BinarySecurityToken ValueType="http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RequestSecurityTokenResponseCollection">PHdhcC1wcm92aNpb25pbmdkb2MgdmVyc2lvbj0IMS4xIj48Y2hhcmFjdGVyaXN0aWMgdH...</BinarySecurityToken>
        </RequestedSecurityToken>
        <RequestID>http://schemas.microsoft.com/windows/pki/2009/01/enrollment</RequestID>
      </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
  </s:Body>
</s:Envelope>
```

Microsoft Intune Suite

A collection of premium, cloud based endpoint management and security capabilities unified in Microsoft Intune



What does EPM enroll into?



TAKE A WILD GUESS



It will enroll into....

When activating the “Intune Suite” a CSP will be pushed to trigger...?

```
Device Copy
./Device/Vendor/MSFT/DMClient/Provider/{ProviderID}/LinkedEnrollment/Enroll
```

Trigger to enroll for the Linked Enrollment.

This is an execution node and will trigger a silent MMP-C enrollment, using the Azure Active Directory device token pulled from the Azure AD-joined device. There is no user interaction needed.

What does MMP-C Stand for?



DELL
Technologies



SquaredUp



infinity

INTERSTELLAR



kpn
Partner Network



INSPARK



cegeka

Microsoft Malware Protection Center

The Microsoft Malware Protection Center website is shown with a large red 'X' drawn across the entire page. The site features a blue header with the Microsoft logo and the text "Malware Protection Center Threat Research and Response". It includes a search bar, social media links for Twitter and Facebook, and a "Sign In" button. Below the header is a navigation bar with links for "Get the latest definitions", "Learn more about malware", "Submit a sample" (which is highlighted in white), and "Learn about us". The main content area shows the "Submit a sample" form and a "Submission list" section. A red "rubri" watermark is visible in the bottom left corner.

Malware Protection Center
Threat Research and Response

Search the Encyclopedia

Having trouble signing in?

Sign In

Get the latest definitions

Learn more about malware

Submit a sample

Learn about us

Home > Submit a sample

Submit a sample

Please submit files that are suspected of containing malware or potentially unwanted software to Microsoft using this form.

Please refrain from using personal information when naming your submission and when entering comments.

* Indicates a required field

Name:

Email:

Submission list

No submissions to display.

To view and track a detailed view of your submission online, please [sign in](#).

rubri



Microsoft Docs??

Long live Google

This is Google's cache of <https://learn.microsoft.com/es-es/graph/api/resources/intune-deviceconfig-endpointprivilegemanagementprovisioningstatus?view=graph-rest-beta>. It is a snapshot of the page as it appeared on 11 Mar 2023 17:14:52 GMT.

[Full version](#) [Text-only version](#) [View source](#)

Properties

Property	Guy	Description
Id	Chain	A unique identifier represents Intune account ID.
licenseType	licenseType	Indicates whether the tenant has a valid Intune endpoint privilege management license. The possible value is : 0 - not paid, 1 - paid, 2 - test. See LicenseType enumeration for details. Unpaid default. The possible values are: , , and .notPaid paid trial unknownFutureValue
onboardedToMicrosoftManagedPlatform	Boolean	Indicates whether the tenant is onboarded to Microsoft Managed Platform - Cloud (MMPC). When set to true, it implies that the tenant is incorporated, and when set to false, it implies that the tenant is not incorporated. Default value set to false.



SquaredUp



kpn
Partner Network



INSPARK



cegeka



Microsoft Docs??

Things change?????

```
2435 2435 <!-- Add any additional information about this policy here. Anything outside this section will get overwritten. -->
2436 - This is an execution node and will trigger a silent MMP-C enrollment, using the Azure Active Directory device token pulled from the Azure AD-joined
      device. There is no user interaction needed.
2436 + This is an execution node and will trigger a silent Declared Configuration enrollment, using the AAD device token pulled from the Azure AD-joined
      device. There is no user interaction needed. When the **DiscoveryEndpoint** is not set, the Enroll node will fail with `ERROR_FILE_NOT_FOUND
      (0x80070002)` and there is no scheduled task created for dual enrollment.
2437 2437 <!-- Device_Provider_{ProviderID}.linkedEnrollment_Enroll_Editable_End -->
```



DELL
Technologies



SquaredUp



infinity



kpn
Partner Network



cegeka



MMP-C



A close-up photograph of actor Mark Wahlberg. He has dark hair and is wearing a dark jacket over a white shirt. He is looking slightly downwards and to his left with a thoughtful expression. A pink microphone with the "Absolute Radio" logo is positioned in front of him, partially obscuring his chest. The background is a plain, light-colored wall.

WHAT IS THIS MAGIC?





MMP-C is the “Next Gen” MS Infra



DELL
Technologies



SquaredUp



infinity



kpn
Partner Network



cegeka

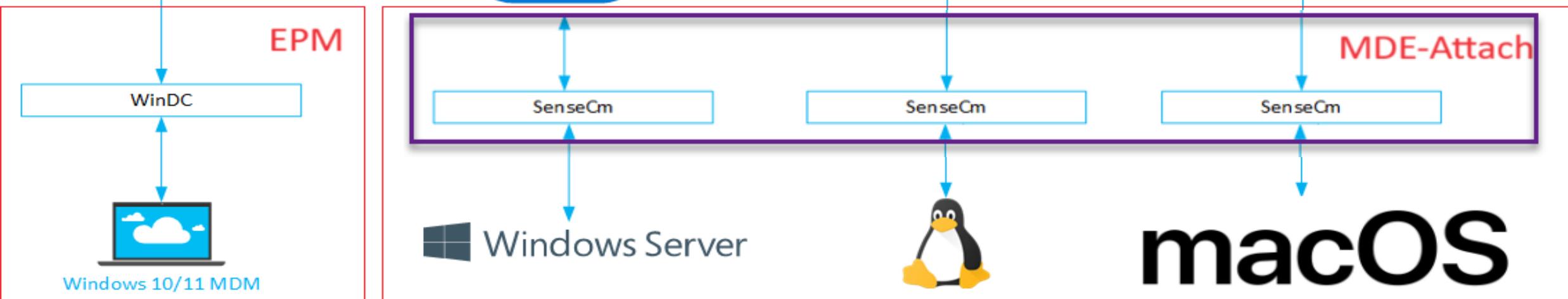
Intune + Entra



MMP-C

URLs:
*discovery.dm.microsoft.com
*Enrollment.dm.microsoft.com
*Checkin.dm.microsoft.com

The “Next Gen” Infra



MMP-C = Microsoft Managed Platform - Cloud

WinDc = Declared Configuration Service / Declarative Device Management

SenseCm = Defender Advanced Threat Protection Security Configuration Module



4. Deepdiving the Enrollment

You will need to know these details, when you need to troubleshoot MMP-C enrollments in the future!

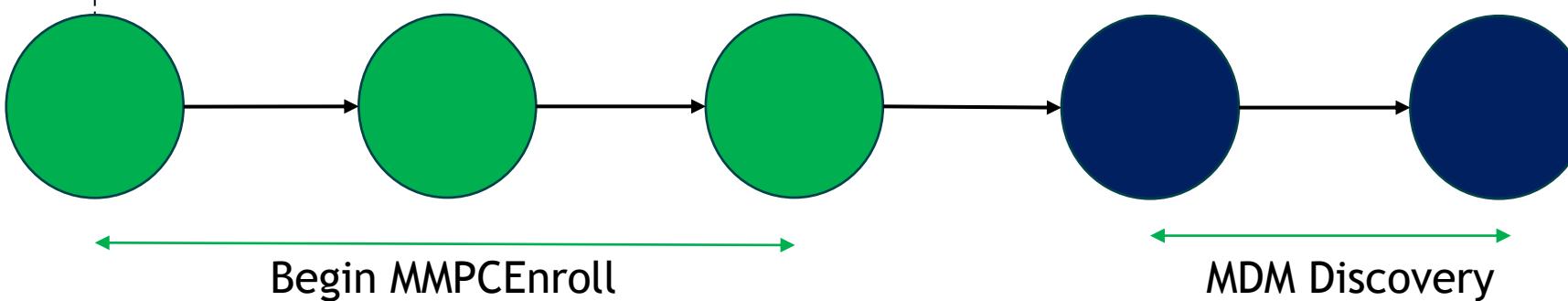


Deepdive Activation policy

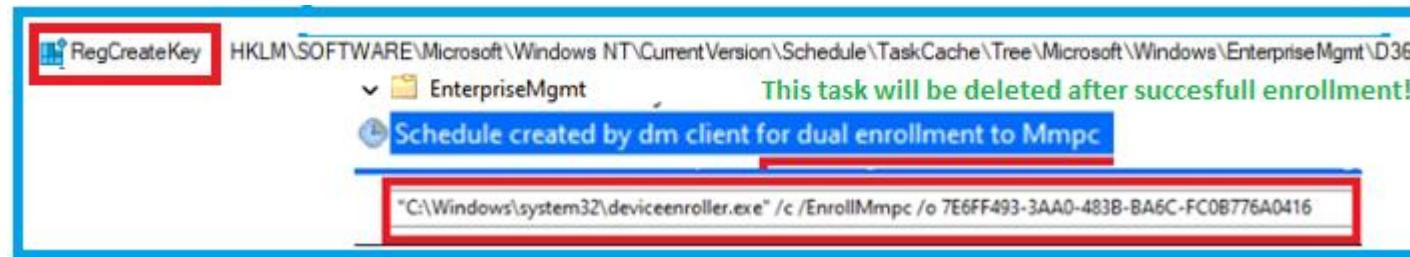
Triggering The Linked Enrollment

When we activate the Intune Suite, the **LinkedEnrollment policy (CSP)** will be sent to the device when applicable*

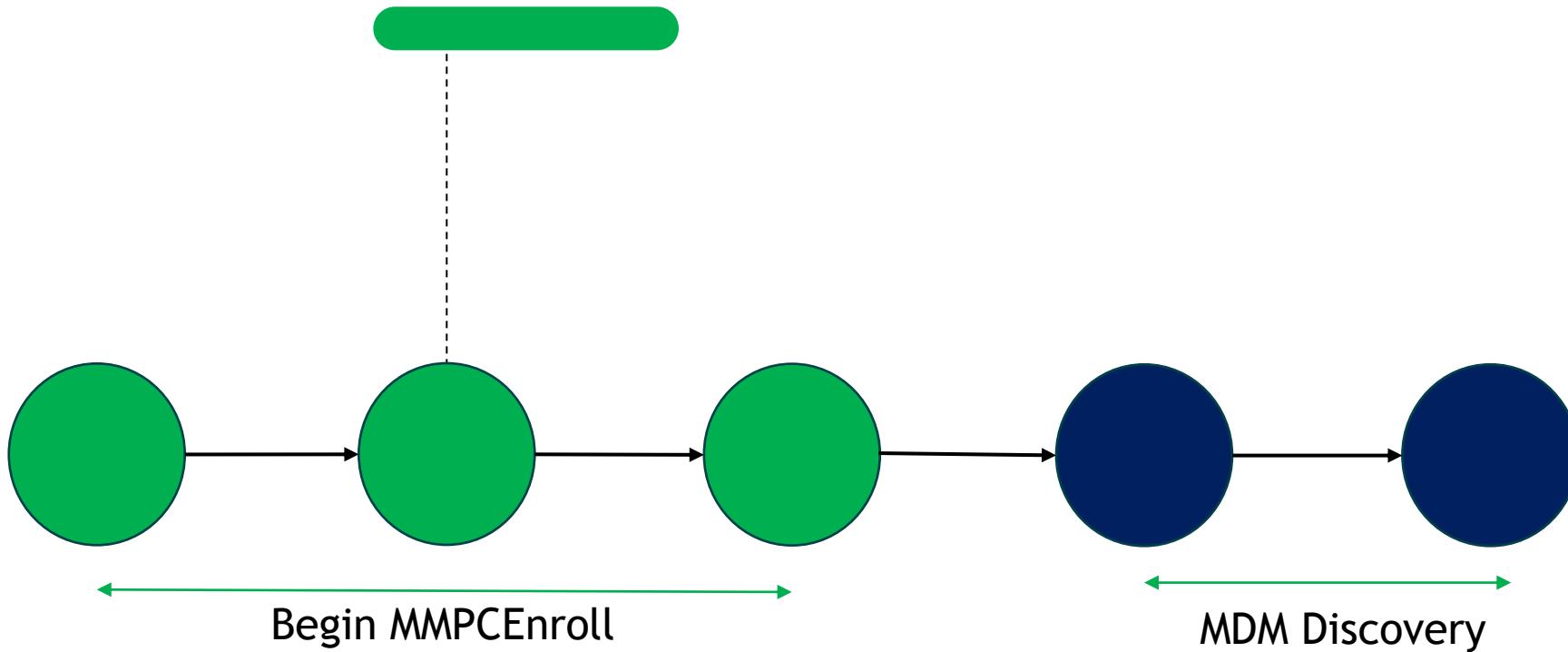
```
04/04/2023 09:57:57
- 04/04/2023 09:57:58
- 04/04/2023 09:57:59
- 04/04/2023 09:58:07
- 04/04/2023 09:58:07
- 04/04/2023 09:58:07
- 04/04/2023 09:58:07
- 04/04/2023 09:58:09
- 04/04/2023 09:58:42
- 04/04/2023 09:58:42
- 04/04/2023 09:58:42
- 04/04/2023 09:58:43
- 04/04/2023 09:58:44
492      <Data>MS DM Server</Data>
493    </Item>
494  </Exec>
495  <Exec>
496    <CmdID>12</CmdID>
497    <Item>
498      <Target>
499        <LocURI>./Vendor/MSFT/DMClient/Provider/MS%20DM%20Server/LinkedEnrollment/Enroll</LocURI>
500      </Target>
501    </Item>
502  </Exec>
503  <Get>
504    <CmdID>13</CmdID>
505    <Item>
```



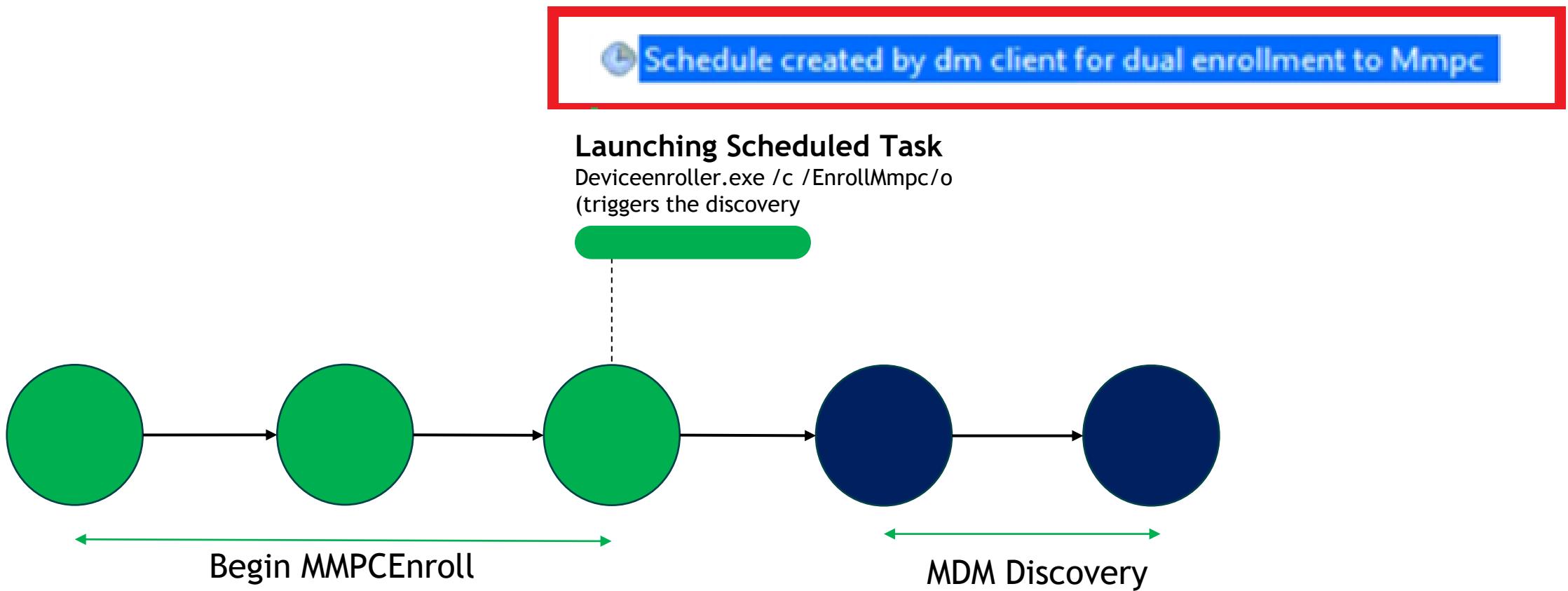
Triggering the Enrollment



**The required scheduled task
For dual enrollment to MMPC will be created**



Launching Scheduled Task

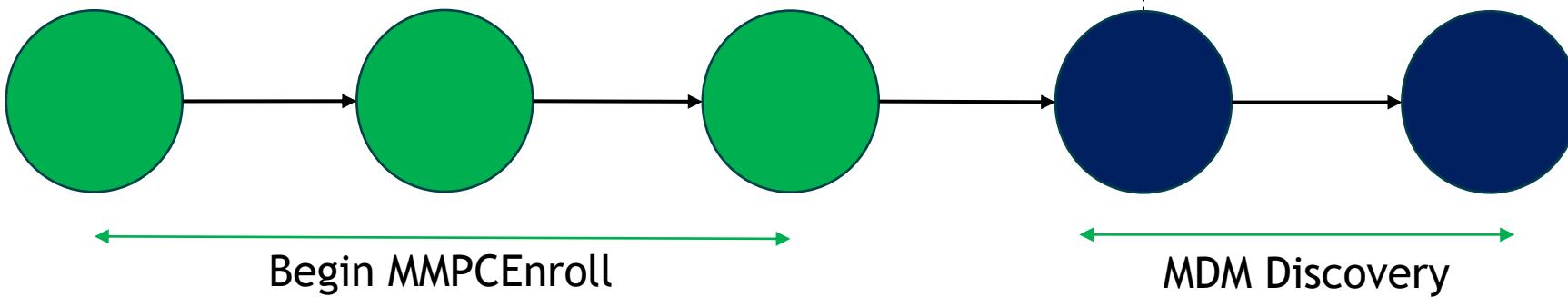


MMP-C Start Discovery

MMP-C Start Discovery
Discovery of the Enrollment URLs
with:Discovery.dm.microsoft.com

```
mov rcx, [rcx+28h] ; unsigned __int16 *  
call ?MmpcDiscoveryUrl@@YAJPEBG0PEAPEAG1@;  
  
POST https://discovery.dm.microsoft.com/EnrollmentConfiguration?api-version=1.0  
Host: discovery.dm.microsoft.com  
{  
    "userDomain": "wvdcloud.nl",  
    "osVersion": "10.0.22621.0"  
}
```

This Discovery URL will be used to find the enrollment URLs (Fiddler)

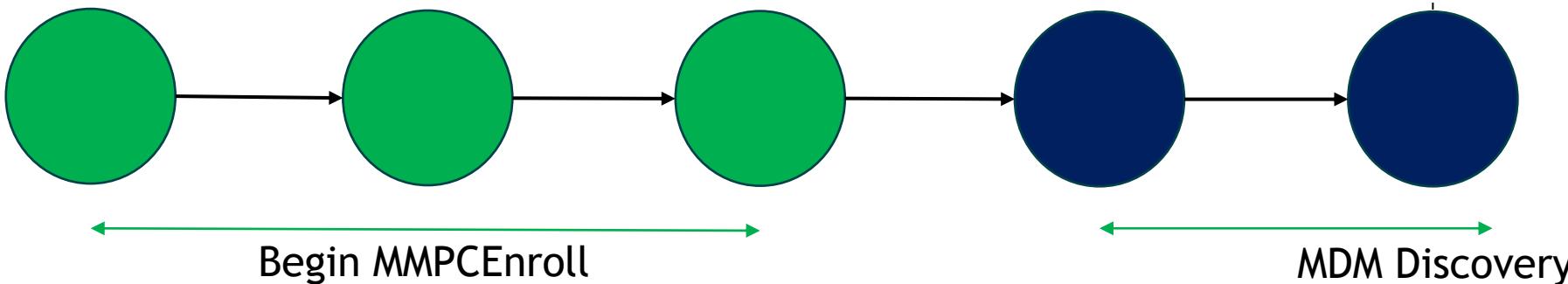


MMP-C Discovery Response

In the Discovery response we received (Fiddler) we will find the enrollment URLs
These URLs are used to start the true MMP-C enrollment

```
AuthenticationServiceUrl=https://enrollment.dm.microsoft.com/enrollmentserver/loginredirect/87f7e2bb-4e07-4f27-93bd-2dab63ee12c7
AuthPolicy=Federated
EnrollmentPolicyServiceUrl=https://enrollment.dm.microsoft.com/deviceenrollment/getpolicies?client-request-id=87f7e2bb-4e07-4f27-93bd-2dab63ee12c7
EnrollmentServiceUrl=https://enrollment.dm.microsoft.com/deviceenrollment/enroll?client-request-id=87f7e2bb-4e07-4f27-93bd-2dab63ee12c7
ManagementResource=https://enrollment.dm.microsoft.com/
TouUrl=https://enrollment.dm.microsoft.com/deviceenrollment/termsofuse.aspx
```

MMP-C Discovery Response
Enrollment URLs:
Enrollment.dm.Microsoft.com

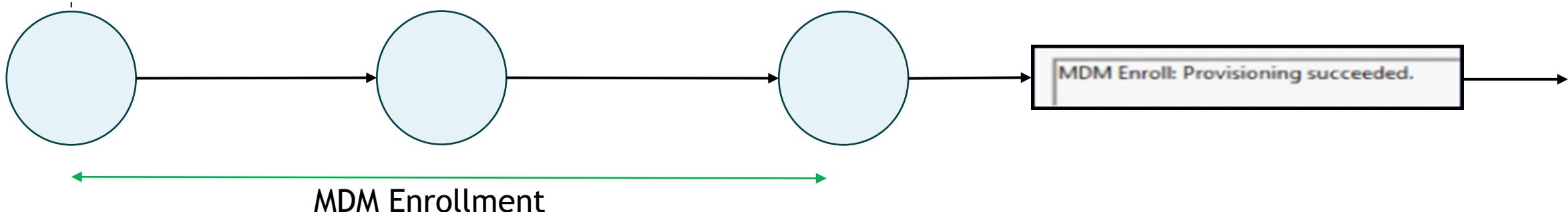


MMP-C Start Enrollment

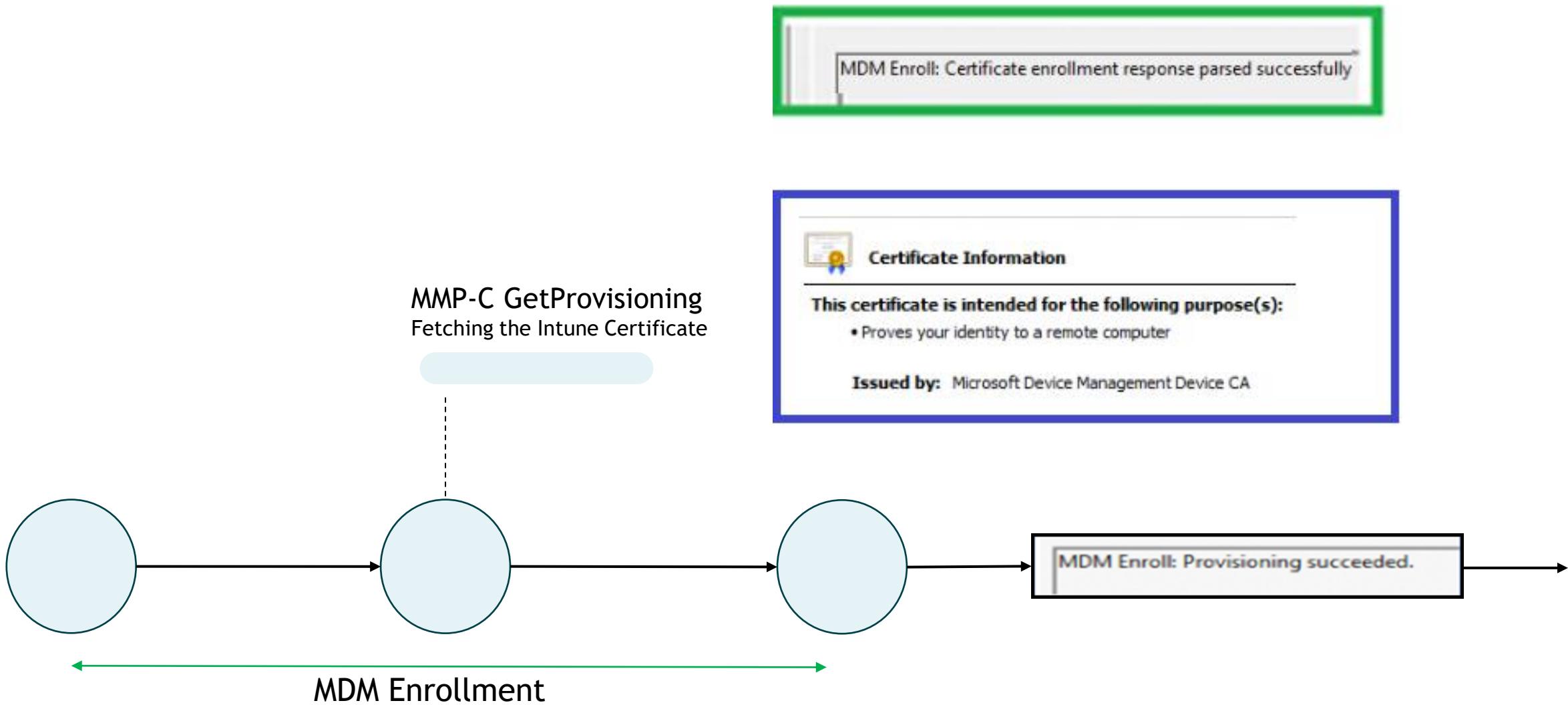
Getting the “Certificate Policies / blueprint”

MMP-C Start Enrollment

```
POST https://enrollment.dm.microsoft.com/deviceenrollment/getpolicies?client-request-  
Connection: Keep-Alive  
...wsse:SecurityToken mustUnderstand=11  
...wsse:BinarySecurityToken [ValueType=urn:ietf:params:oauth:token-type:jwt EncodingType=http://docs.oasis-open.org/wss/2004/01/c  
ZXIKMGVYQWIPaUpLVjFRaUxDShiR2NpT2lKU1V6STFOaUlzSW5nMWRDSTZJaTFMU1ROUk9XNU9VamRpVW05bWVHMWx0bTlZY1dKSV |  
  
AADTOKEN  
...s:Envelope [ xmlns:s=http://www.w3.org/2003/05/soap-envelope xmlns:a=http://www.w3.org/2005/08/addressing ]  
...s:Header  
...s:Body  
...GetPoliciesResponse [ xmlns=http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy ]  
...response  
...<policyFriendlyName p6:nil="true" xmlns:p6="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/  
...<nextUpdateHours p6:nil="true" xmlns:p6="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/  
...<policiesNotChanged p6:nil="true" xmlns:p6="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/  
...polices  
...policy  
...policyOIDReference  
...<cAs p8:nil="true" xmlns:p8="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/window  
BluePrint to create x509 Certificate
```



MMP-C Certificate



MMP-C Creating the Scheduled Sync Tasks

MMP-C

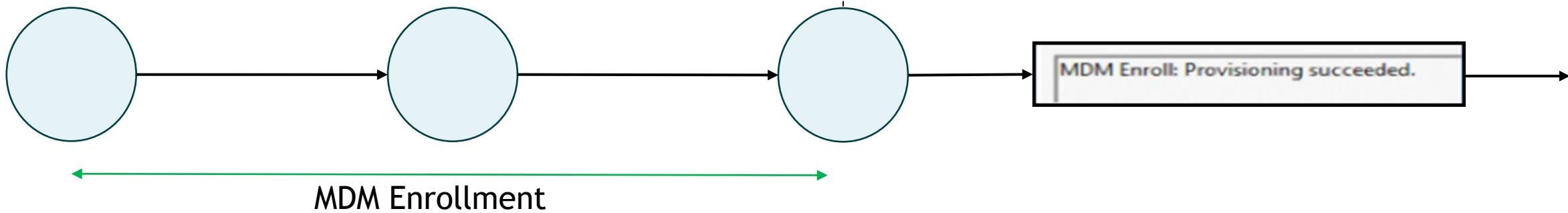
Category	Task	Description
Provisioning initiated session	PushLaunch	Aangepaste trigger
	PushRenewal	Meerdere triggers opgegeven
	Refresh schedule created by Declared Configuration to...	Om 18:07 op 8-4-2024 - Na trigger elke 04:00:00 eindeloos herhalen.
	Schedule #1 created by enrollment client	Om 14:10 op 8-4-2024 - Na trigger elke 00:03:00 herhalen gedurende 15 min..
	F509C471-2277-49BB-B2AD-D4C278EBDD78	2 created by enrollment client
	VirtulizationBasedIsolatc	Schedule #3 created by enrollment client
EnterpriseMgmtNonCritical	Schedule #3 created by enrollment client	Om 16:55 op 8-4-2024 - Na trigger elke 04:00:00 eindeloos herhalen.

MMP-C ApplyProvisioning

Creating Enrollment Task Schedules

Intune

Category	Task	Description
Provisioning initiated session	PushLaunch	Gereed
	PushRenewal	Gereed
	Schedule #1 ...	Gereed
	Schedule #2 ...	Gereed
	Schedule #3 ...	Gereed
	Schedule cre...	Gereed
	Schedule to ...	Gereed



Set MmpcEnrollment Flag

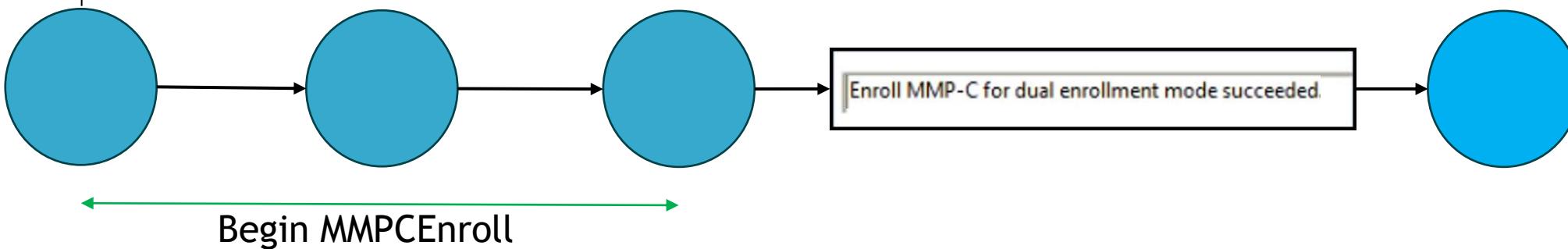
Setting Enrollment Flag

Setting the MMP-C EnrollmentFlag (0)

The screenshot shows two windows. The top window is a debugger's assembly view with a red box highlighting the function name `?SetMmpcEnrollmentFlag@EEDBManager@@SAJK@Z`. Below it, green boxes highlight the registry key path `Software\Microsoft\Enrollments` and the value name `aOsdataSoftware_28`. The bottom window is a Windows Registry details view for the key `HKEY_LOCAL_MACHINE\Software\Microsoft\Enrollments\0x00000000`. It shows the following information:

Date:	8/1/2023 11:35:10.390268
Thread:	2676
Class:	Registry
Operation:	RegSetValue
Result:	SUCCESS
Path:	HKLM\SOFTWARE\Microsoft\Enrollments\0x00000000
Type:	REG_DWORD
Length:	4
Data:	0

A red box highlights the path `HKLM\SOFTWARE\Microsoft\Enrollments\0x00000000`. A large red box surrounds the entire bottom window, and the text "AKA Enrollment DONE!" is displayed to its right.



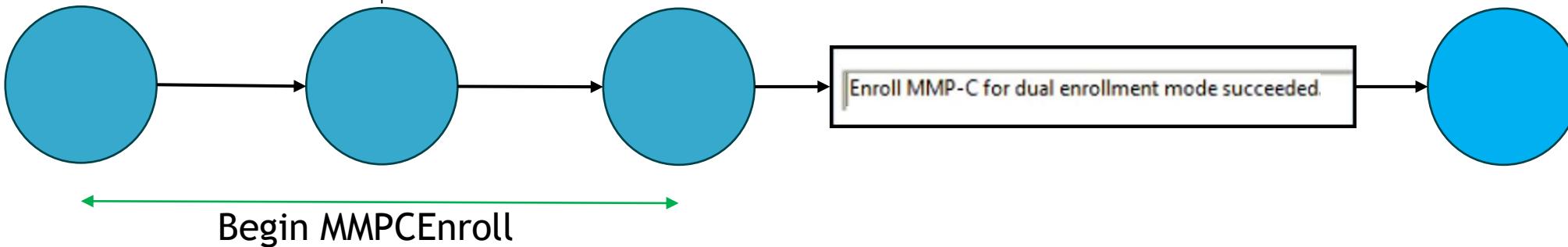
Cleaning Up

```
loc_140013E07:  
lea    r8, aScheduleCreate ; "Schedule created by dm client for dual "...  
mov    rdx, [rsp+1210h+var_11C0]  
lea    rcx, aMicrosoftWindo_1 : "\\\'Microsoft\\\Windows\\\EnterciseMemt"  
call   cs:_imp_?DmDeleteTask@@YAJPEBG00@Z ; DmDeleteTask(ushort const *, ushort const *, ushort const *)  
nop    dword ptr [r8+r8+40h]
```

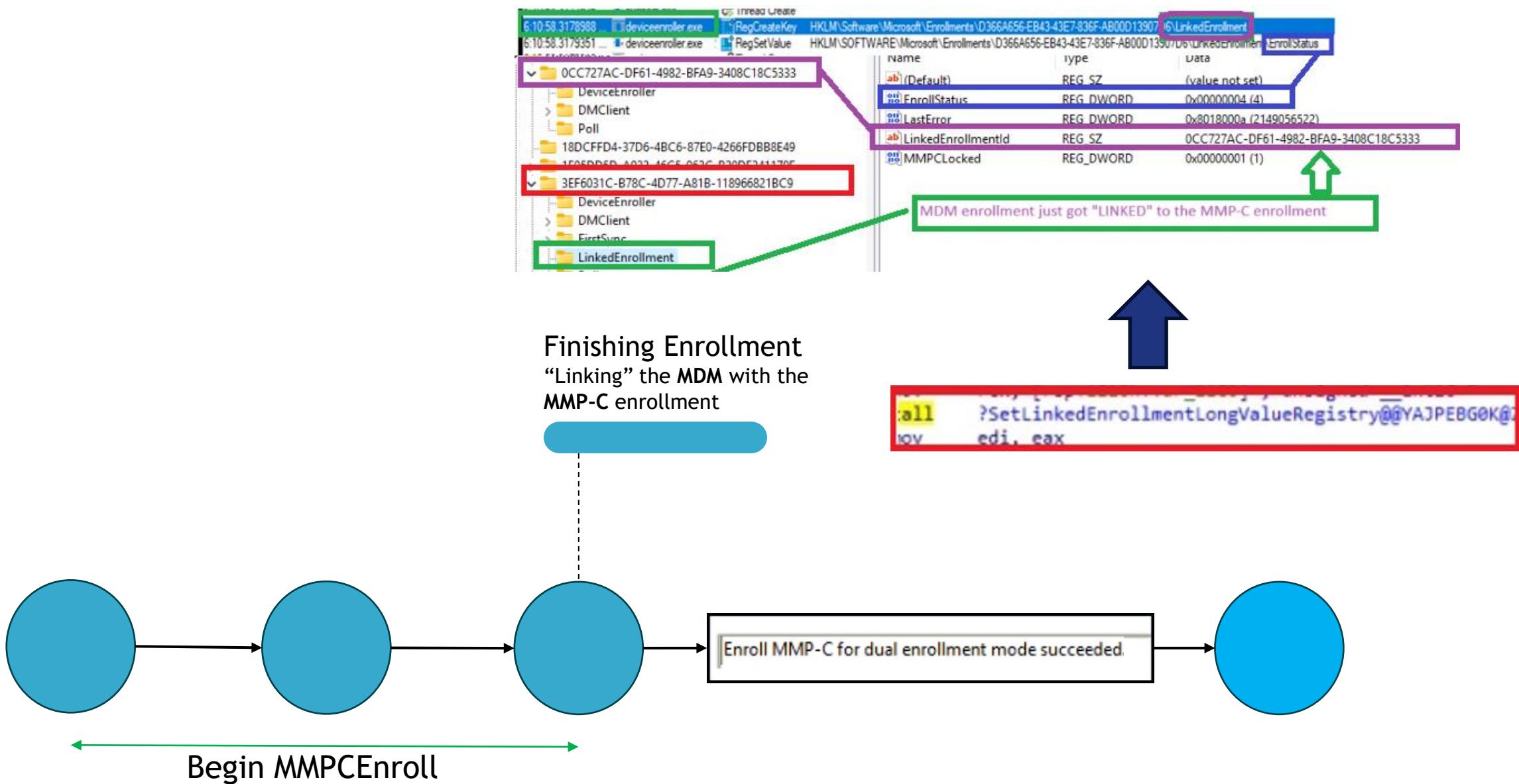
Cleaning up

- Deleting the previous created Scheduled Task to kick off enrollment

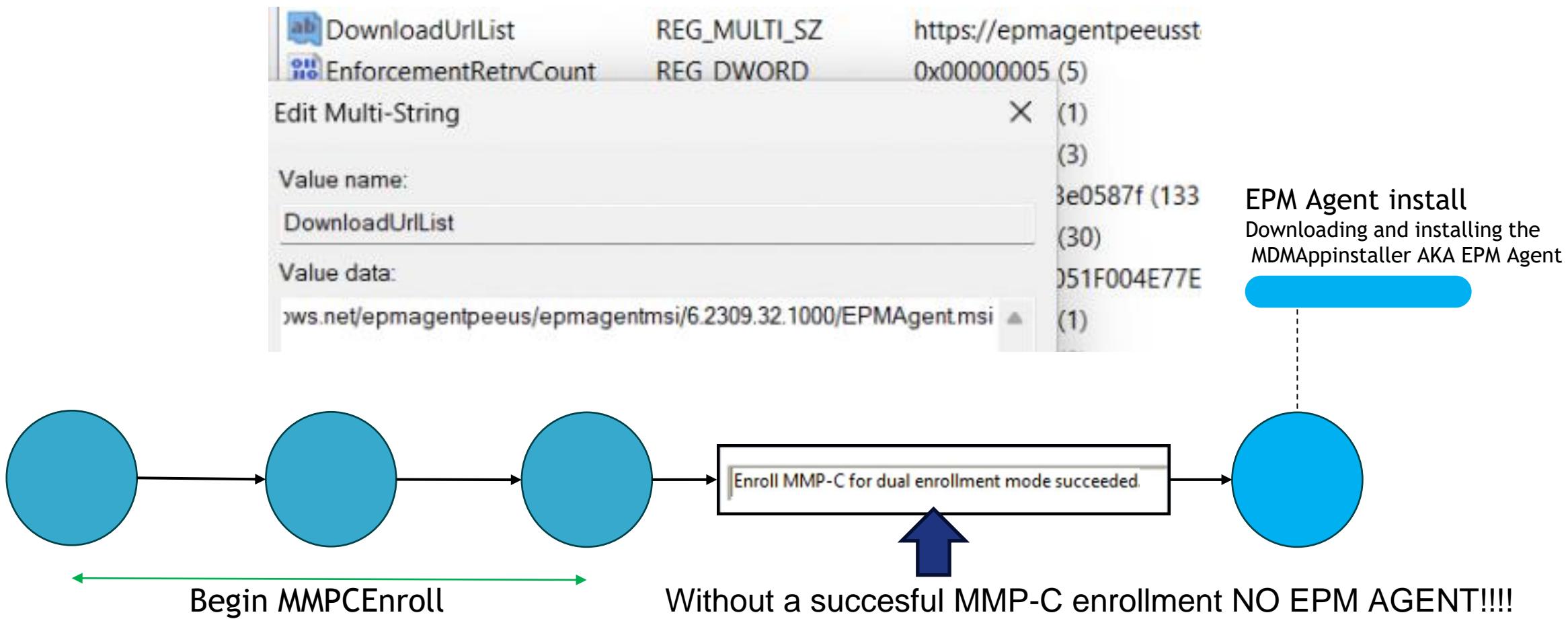
Class:	Registry
Operation:	RegDeleteKey
Result:	SUCCESS
Path:	gmt\3FCD05C2-C1CE-4F77-9BE4-E693208D4797\Schedule created by dm client for dual enrollment to Mmpc
Duration:	0.0000674



Linking Enrollments



Installing EPM Agent





5. A quick recap

- We activated the Intune Suite and configured EPM
- This will push a CSP to kick off a Linked/Dual enrollment
- The CSP would trigger the device to enroll into MMP-C
- This “enrollment” looks the same as the well known Intune enrollment
- Without the MMP-C Enrollment NO Epm Agent!

So what's next? → Taking a look at the Support Approved and the policies!!

32



DELL
Technologies



SquaredUp



infinity



kpn
Partner Network

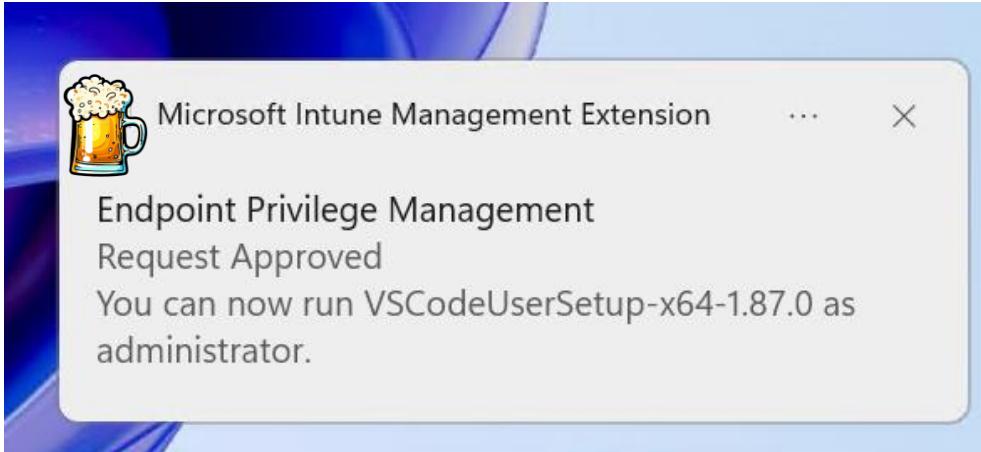


INSPARK



cegeka

6. New Feature: Support Approved



- New Feature to EPM (Require Support Approval)
- Allow users to request temporary administrative privileges for specific applications or tasks
- Intune administrators can approve or deny

A screenshot of the Intune Settings Catalog titled "Edit profile - BL-WIN-USR-P-EPM-Elevation setting-v1.0". It shows the "Configuration settings" tab selected. Under "Privilege Management Elevation Client Settings", there is a note about elevation settings establishing default behaviors. A red arrow points to the "Default elevation response" dropdown, which is set to "Require support approval". Other settings shown include "Send elevation data for reporting" (Yes) and "Reporting scope" (Diagnostic data and all endpoint elevations). The "Review + save" tab is also visible.



DELL
Technologies



SquaredUp infinity

INTERSTELLAR

 **kpn**
Partner Network

 **INSPIRK**

 cegeka



Story line EPM SA



- John needs the Visual Studio application and creates a EPM request



DELL
Technologies



SquaredUp



infinity

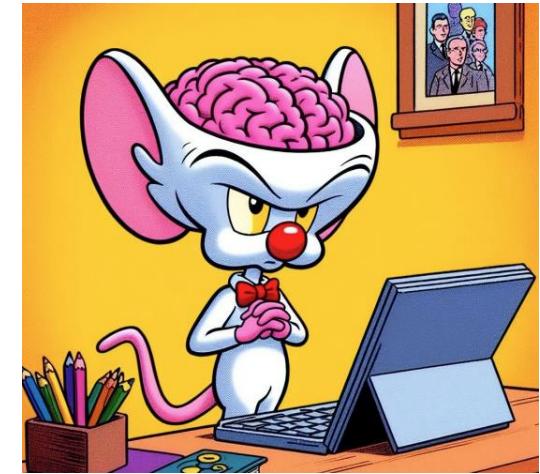
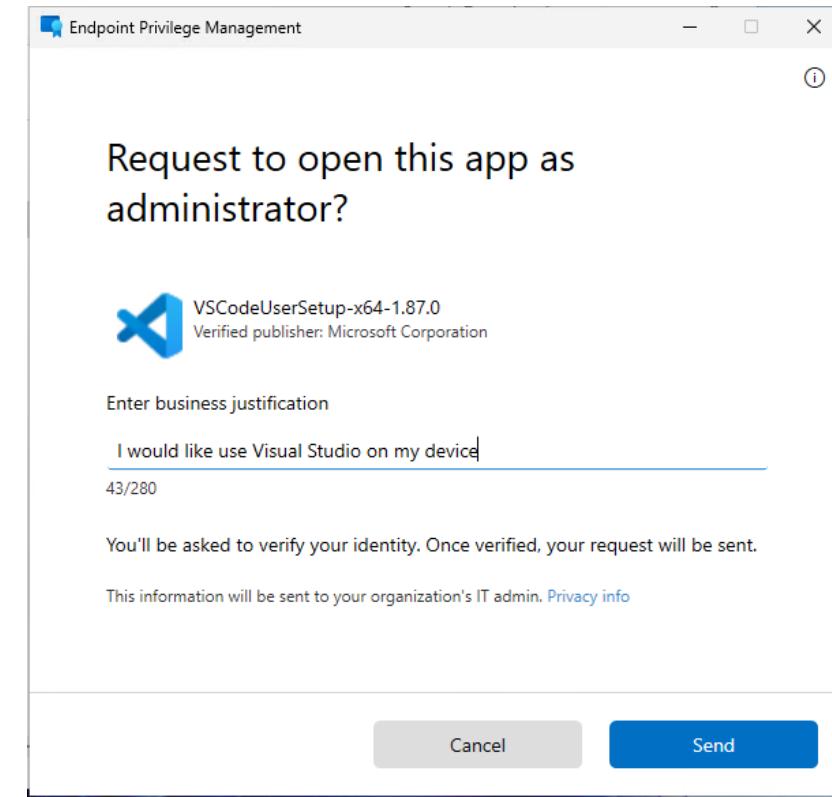
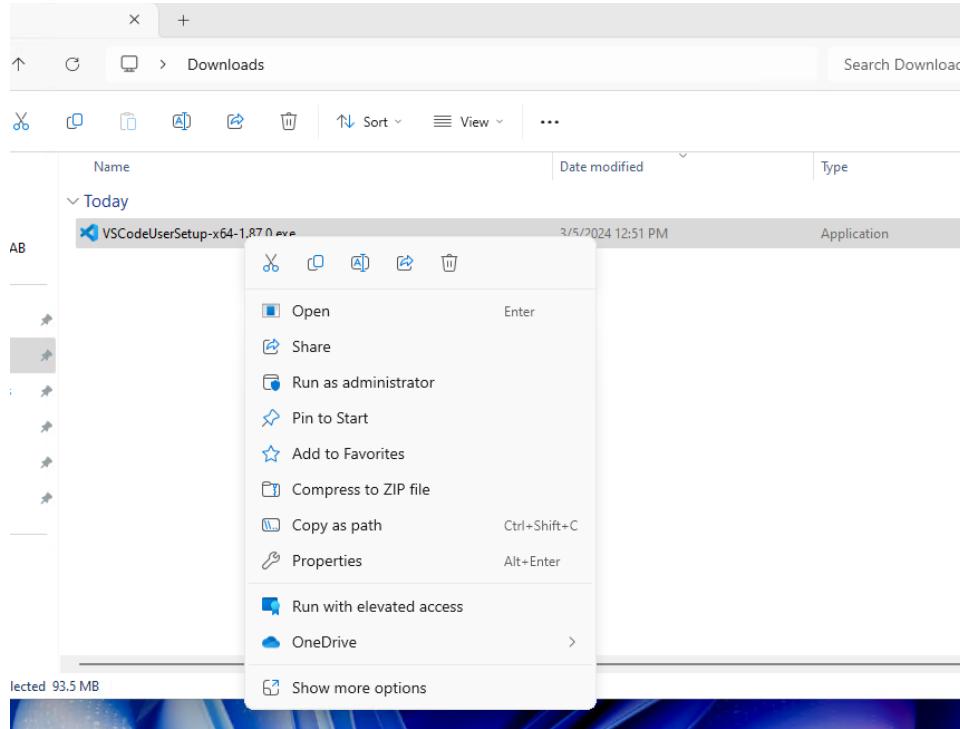


kpn
Partner Network



cegeka

John perspective

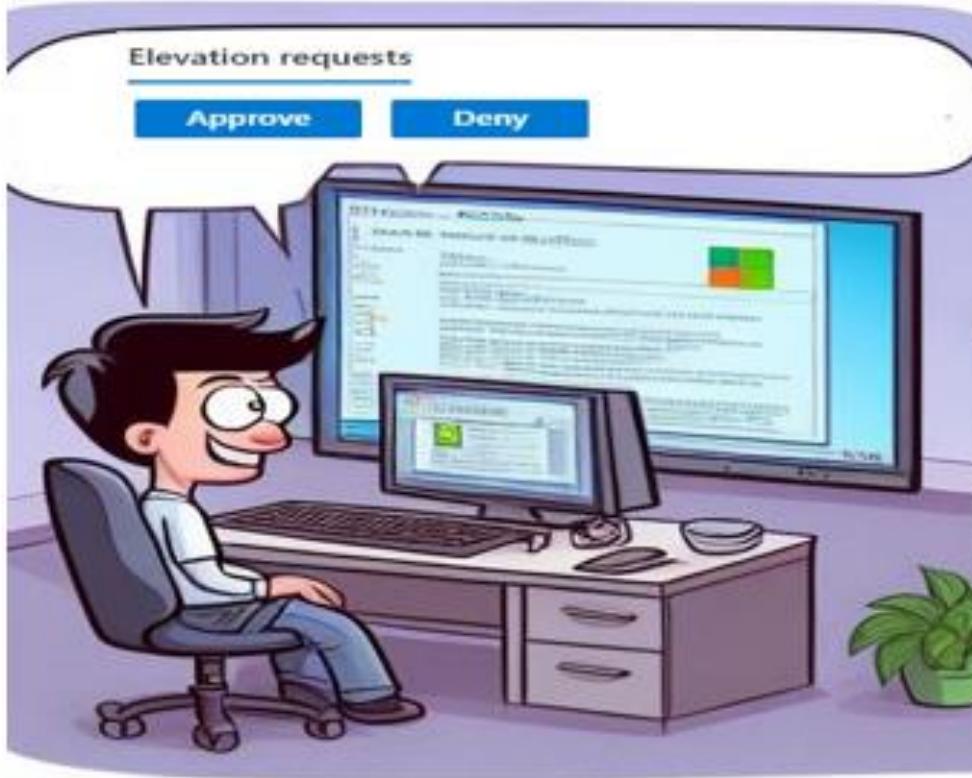


SquaredUp infinity





Story line EPM SA



- Support Engineer notices the request in Intune
- The Admin approves or denies request



DELL
Technologies



SquaredUp



infinity

INTERSTELLAR



kpn
Partner Network



INSPARK



cegeka

Support Engineer perspective

Home > Endpoint security

Endpoint security | Endpoint Privilege Management ...

Search < Reports Policies Reusable settings Elevation requests

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint Privilege Management
- Endpoint detection and response



Elevation request properties

File	VSCodeUserSetup-x64-1.87.0.exe
Publisher	Microsoft Corporation
Username	Luke Skywalker
Device	CPC-Luke-PLDZQ
Intune compliant	true

Request details

Status	Pending
By	
Last modified	03/06/24, 1:12 PM
User's justification	Need it for my daily work
Approval expiration	03/07/24, 1:12 PM
Admin's reason	

File information

File path	C:\Users\LukeSkywalker\Downloads
Hash value	02F972362910FCDA3AB0D4AE4DC339B68F1BF6EA77
File version	1.87.0
File description	Visual Studio Code Setup
Product name	Visual Studio Code
Internal name	

Approve

Deny



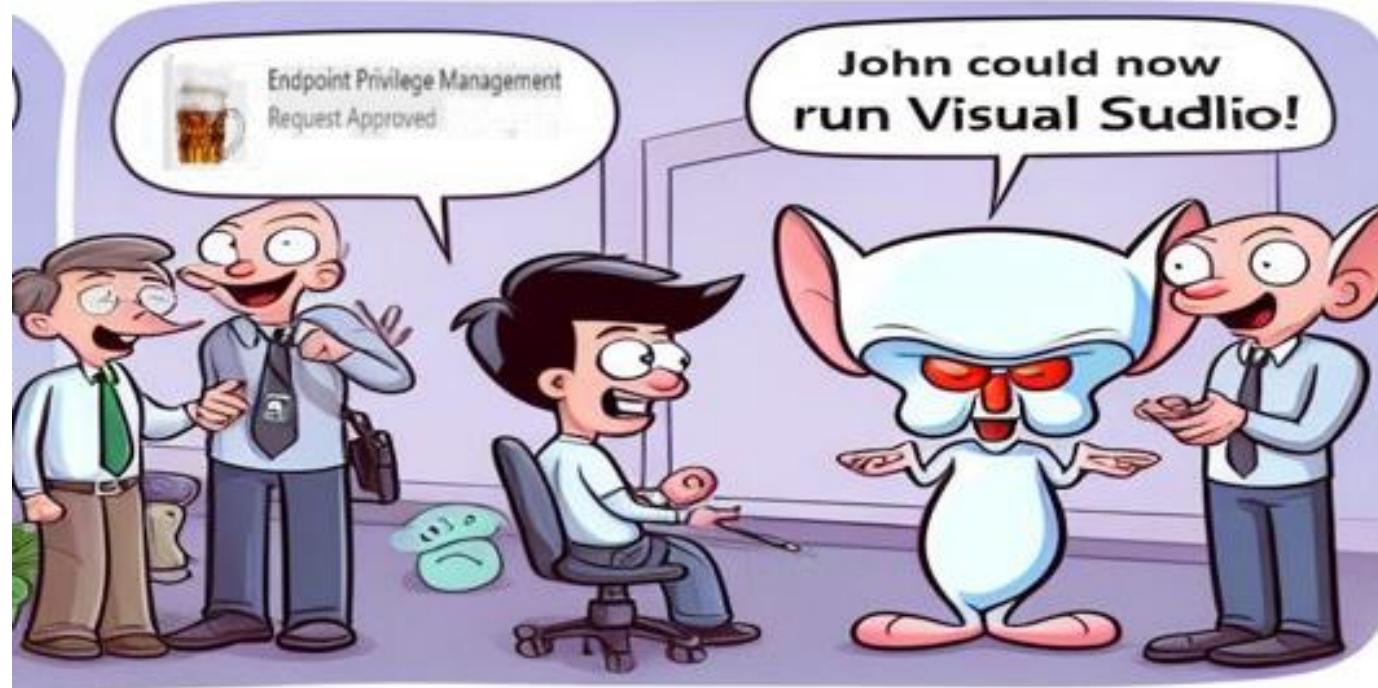
DELL
Technologies



SquaredUp infinity

INTERSTELLAR

Story line EPM SA



- The temporary Elevation Rules/Policy will arrive on the device with 5 minutes delay
- John can elevate the installation.
- The Process Will be executed in a **weird virtual Account**



The “weird Virtual Account”

The Virtual Account that rocks the EPM!

by: rudyooms - May 31, 2023

Last Updated on April 3, 2024 by [rudyooms](#)

Are you using Intune Endpoint Privilege Management (EPM) and wondering what is “needed” when you launch a process with elevated access?

In this blog, I will have a little peek at the “virtual account” which is created during the EPM installation. The process you elevated will be run in the context of this virtual account.

I need to warn you.... This is **NOT** going to be a level **100 blog** or an introduction to Endpoint Privilege Management but more like **level 400+**.

[Virtual Account | EPM | Endpoint Privilege Management \(call4cloud.nl\)](#)



DELL
Technologies



SquaredUp



infinity

 **INTERSTELLAR**



kpn
Partner Network



INSPARK



cegeka



7. The Elevation rules

```
PS C:\Program Files\Microsoft EPM Agent\EpmTools> Import-Module .\EpmCmdlets.dll
2PS C:\Program Files\Microsoft EPM Agent\EpmTools> Get-Policies -PolicyType ElevationRules -Verbose | Format-Tab
2e -AutoSize
2VERBOSE: Retrieving EPM Agent policies information for policy type 'ElevationRules'.
2VERBOSE: Policies processed by the ElevationRules adapter, count=1
2
2ExeFileNames
2-----  
2Powershell.exe,PowerShell.exe,PowerShell.exe,powershell.exe 8122a726-fd81-447a-873d-cccd4fd0b2cdf DEA4A693F42...
```

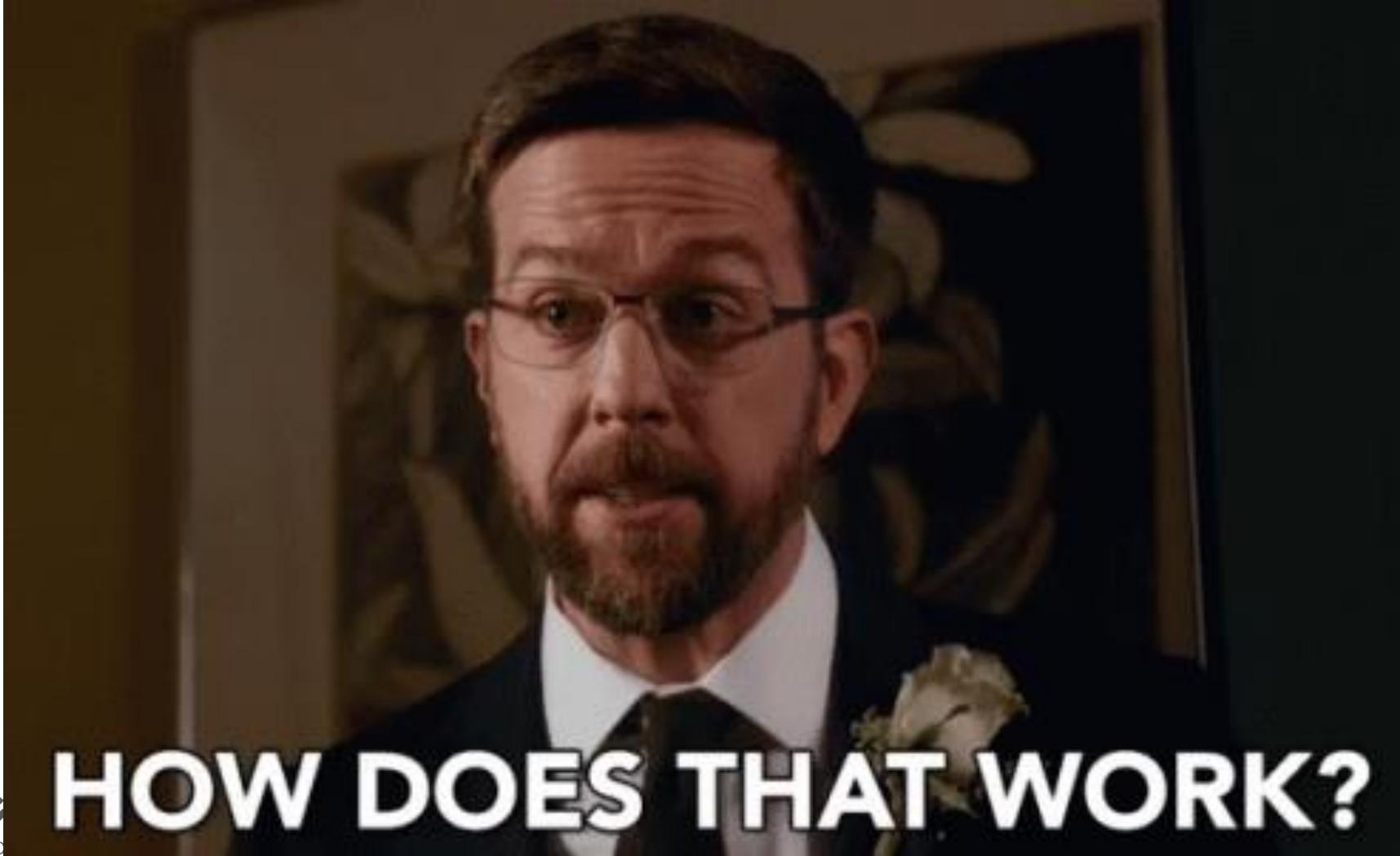


SquaredUp

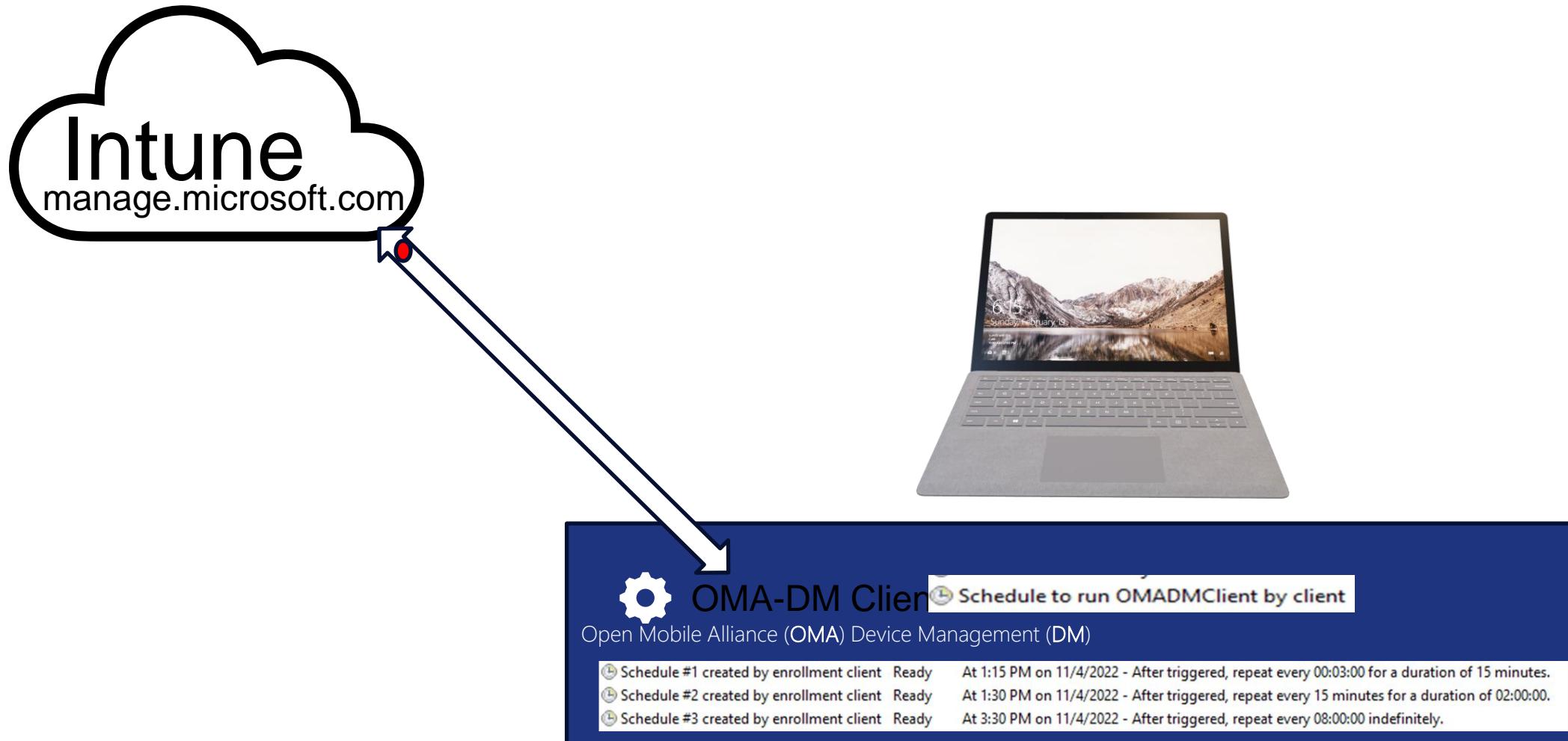




How did they arrive on the device?



Intune only enrolled Device





MMP-C has??



INTERSTELLAR

Farmer Network

INSTAPARK



The “Unknown” Service



“enabled/Activated” with this update:

August 25, 2022—KB5016691

D**clared Configuration(DC) service Properties (Local Computer)** X

General Log On Recovery Dependencies

Service name: dcsvc
Display name: Declared Configuration(DC) service
Description: Process Declared Configuration documents received from MDM and other channels and perform configuration on devices
Path to executable: C:\Windows\system32\svchost.exe -k netsvcs -p
Startup type: Manual ▾

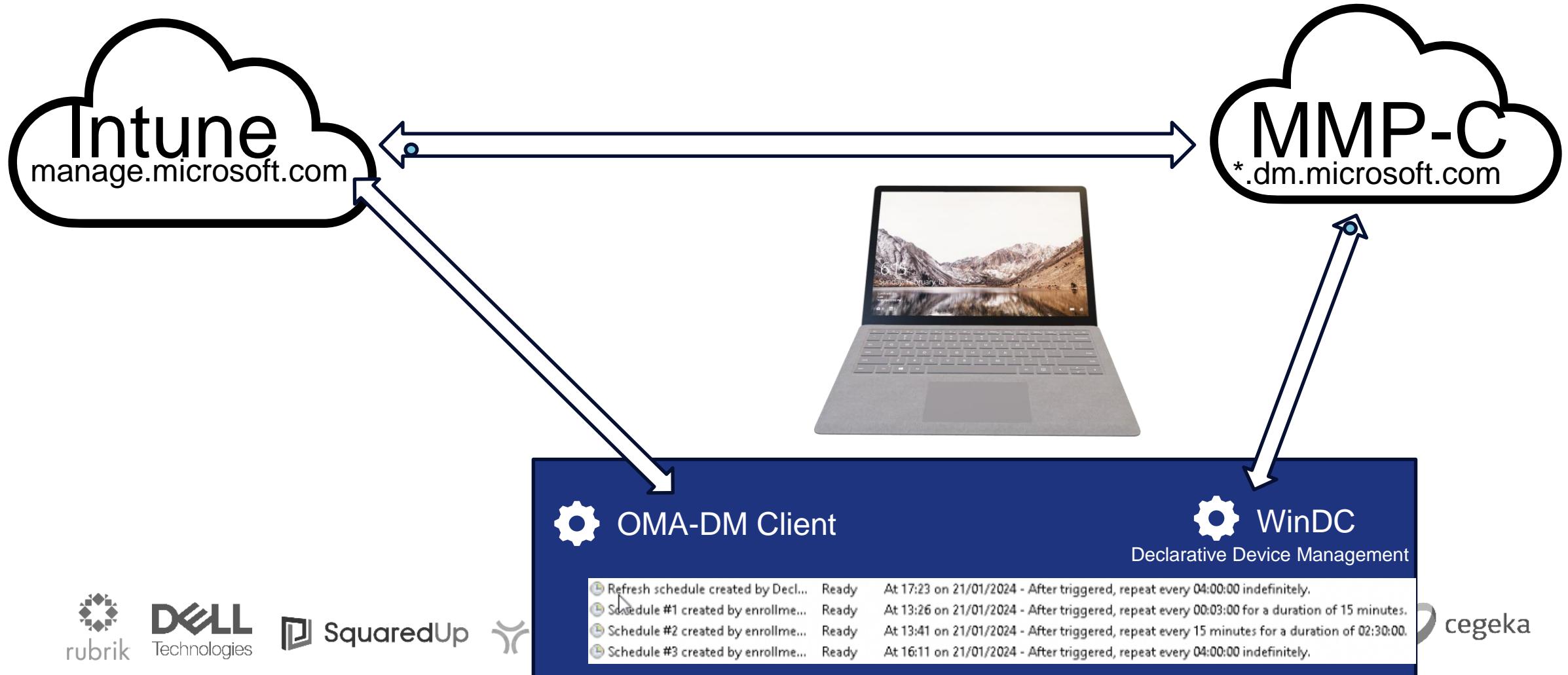
Service status: Running

Start Stop Pause Resume

You can specify the start parameters that apply when you start the service from here.

Intune + MMP-C enrolled Device

(Dual Enrolled State)



8. The Future is bright!



MikeDano

@MikeDanoski

...

The future is bright



[DeclaredConfiguration CSP - Windows Client Management | Microsoft Learn](#)



DELL
Technologies



SquaredUp



infinity

INTERSTELLAR



kpn

Partner Network



INSPARK



cegeka



The future is indeed bright!



DELL
Technologies



network  **INSPIRK**

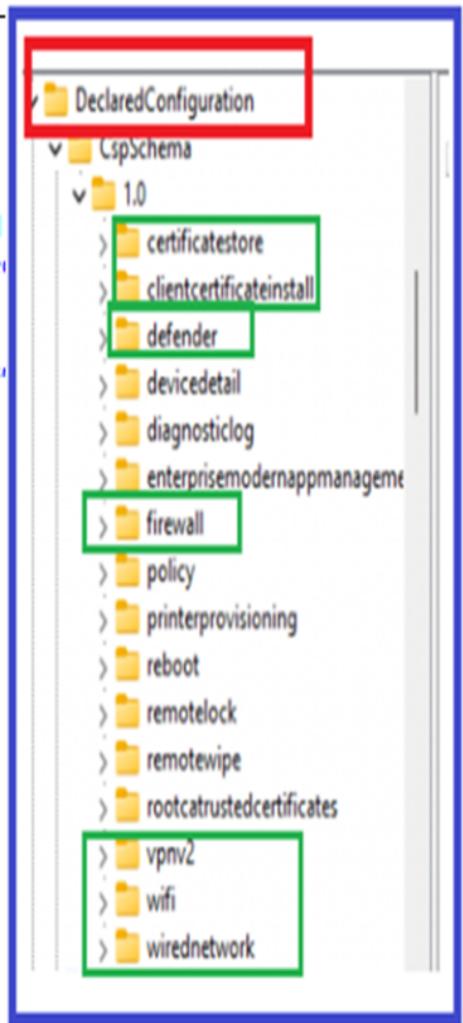


Let me show you!!!



8. Moving the SCCM MDM workloads

DeclaredConfiguration\HostOS\Config\Enrollments\F5090
csp REG_SZ ./Vendor/MSFT/CertificateStore



- dcsvc.dll.i64 (dcsvc.dll) C:\install\insider 03-2024\dcsvc.dll.i64

```
?DeclaredConfiguration_CreateCookedSettings@  
; __int64 __fastcall CSPPProviderCor  
?CSPPProviderConfiguration@@YAJPEAU  
  
if ( v199 >= 8 )  
    v100 = v198[0];  
if ( !_wcsicmp(v10, L"wifi") )  
{  
    if ( wcsstr(v73, L"vpnv2") )  
        goto LABEL_11;  
    if ( *((_QWORD *)v66 + 3) >= 8ui64 )  
        v66 = *(wchar_t ***)v66;  
    v74 = _wcslwr(v66);  
    if ( wcsstr(v74, L"clientcertificateinstall") )  
    {  
        LABEL_11:  
    }  
}
```

8. Certificate Resource Policies being "moved"

The screenshot shows the Windows Registry Editor with two main panes. The left pane displays a tree view of registry keys under `HKEY_CURRENT_USER\Software\Microsoft\DeclaredConfiguration\HostOS\Config\Enrollments\F509C471-2277-49BB-B2AD-D4C278EBDD78\Device\state\C9589FC3-AB85-4007-820E-7813F81771C2\dc7327f4-8cf9-7021-7f1a-731c74a11777`. The right pane shows a table of registry values with their names, types, and data.

Top Registry View:

Naam	Type	Gegevens
ab (Standaard)	REG_SZ	(geen waarde ingesteld)
atomicFlagNecessary	REG_DWORD	0x00000001 (1)
csp	REG_SZ	./Vendor/MSFT/CertificateStore
cspSchemaFound	REG_DWORD	0x00000001 (1)
ProviderType	REG_DWORD	0x00000001 (1)
UriCount	REG_DWORD	0x00000001 (1)

Bottom Registry View:

Naam	Type	Gegevens
context	REG_SZ	DEVICE
CspCount	REG_DWORD	0x00000001 (1)
downloadRequest	REG_DWORD	0x00000000 (0)
model	REG_DWORD	0x00000001 (1)
operation	REG_DWORD	0x00000001 (1)
originalDocStorageGuid	REG_SZ	
osconfigscenario	REG_SZ	
osdefinedscenario	REG_SZ	MSFTPolicies
schema	REG_SZ	1.0
state	REG_DWORD	0x0000003c (60)



9.The Final Recap

- **MMP-C is the infra that ties it all together**
- **MMP-C is used by EPM and MDE-Attach..**
- **WinDC (Declared Configurations) is the next gen OMADMClient**
- **WinDC is all about Desired State Config (DSC)**
- **It looks like policies are going to get moved over from MDM to MMPC**
- **MMP-C will revolutionize device management**



DELL
Technologies



SquaredUp



infinity





Please evaluate this session in the App.

THANK YOU
Are there any questions?

