EPM, The Chocolate Intune Version 2 Factory

Start 13:00

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

EPM, The Chocolate Intune Version 2 Factory

Rudy Ooms / Joost Gelijsteen

Experts Live Netherlands

Sprekers

Joost Gelijsteen

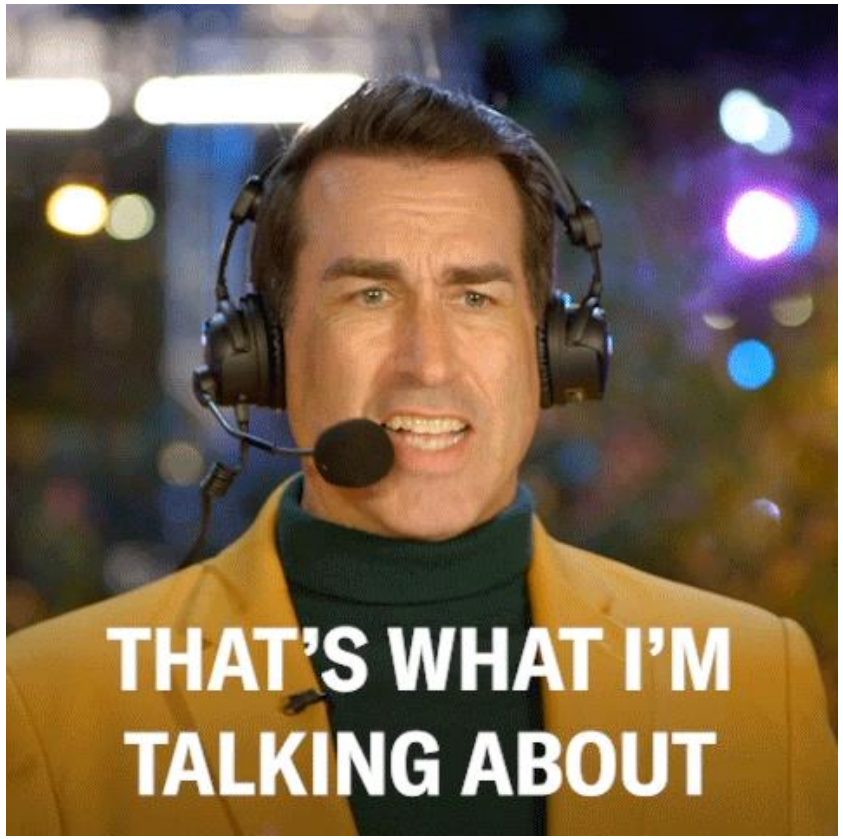
Sneakers
Deepdiving Intune
Job: Pink Elephant
Blog: JoostGelijsteen.com
@jgelijsteen

Rudy Ooms

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

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

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

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

1. Introduction

Security vs Productivity

Removing Admin Permissions **VS** **Installing apps and peripherals**

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

1. Introduction

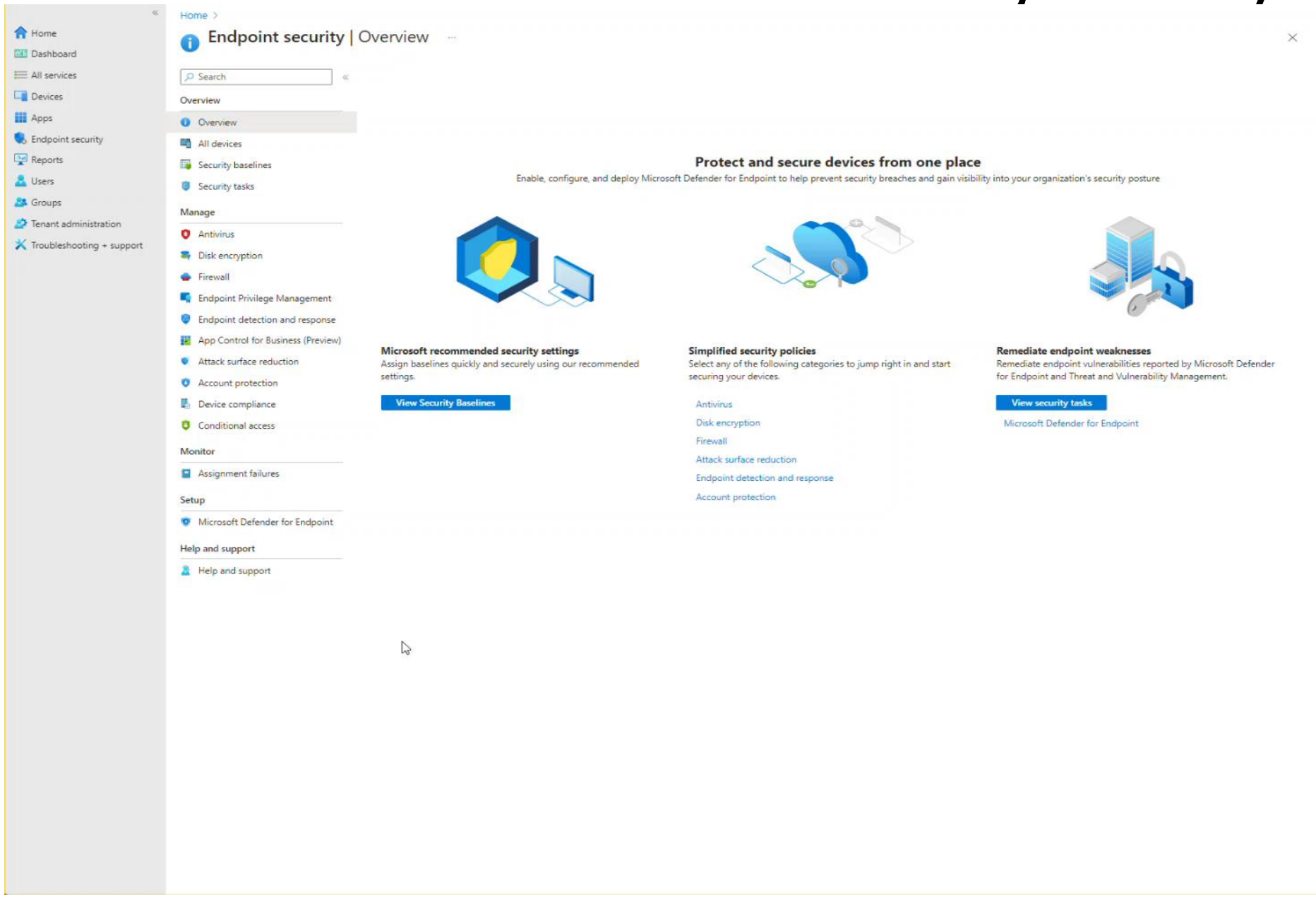
Enforce least privilege access
- Reduce attack surface of local admins
- Protect corporate data by enabling least privilege access
- Support Zero Trust model

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

Insights
- Elevation reporting

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

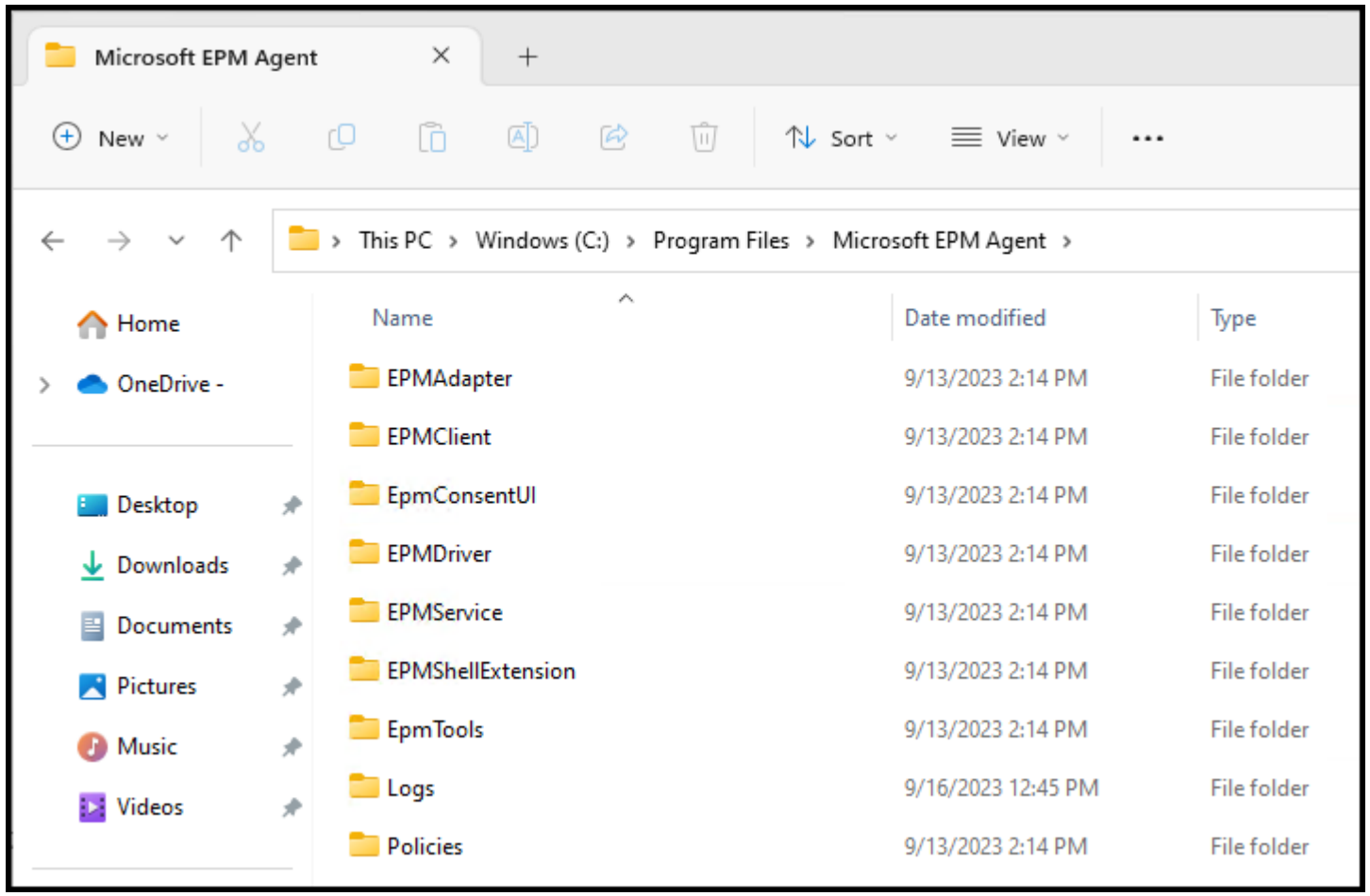
2. EPM Elevation settings Policy

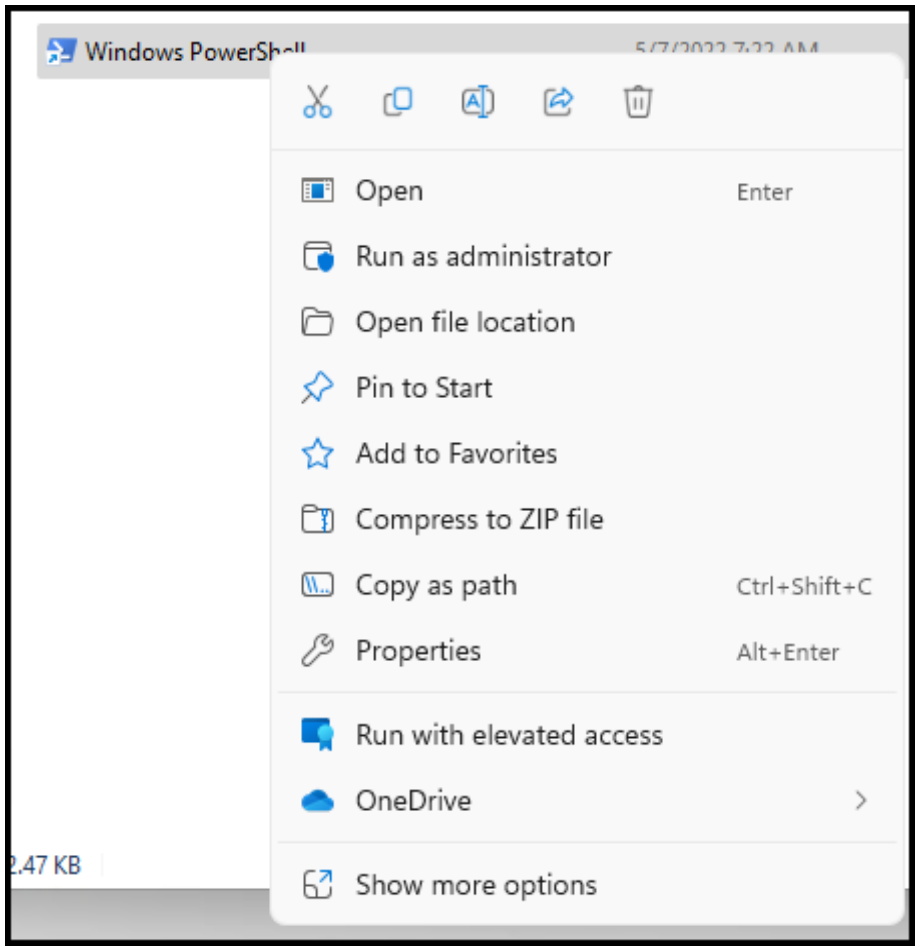


rubrik

cegeka

EPM Agent magically appears!





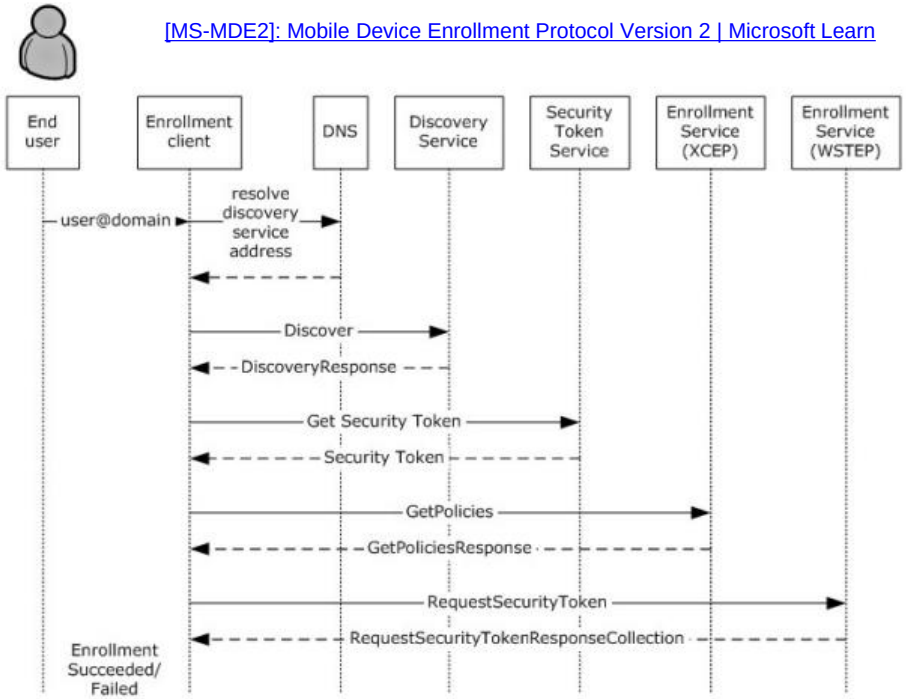
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

But…how does EPM got installed?

3. The "EPM" Enrollment?

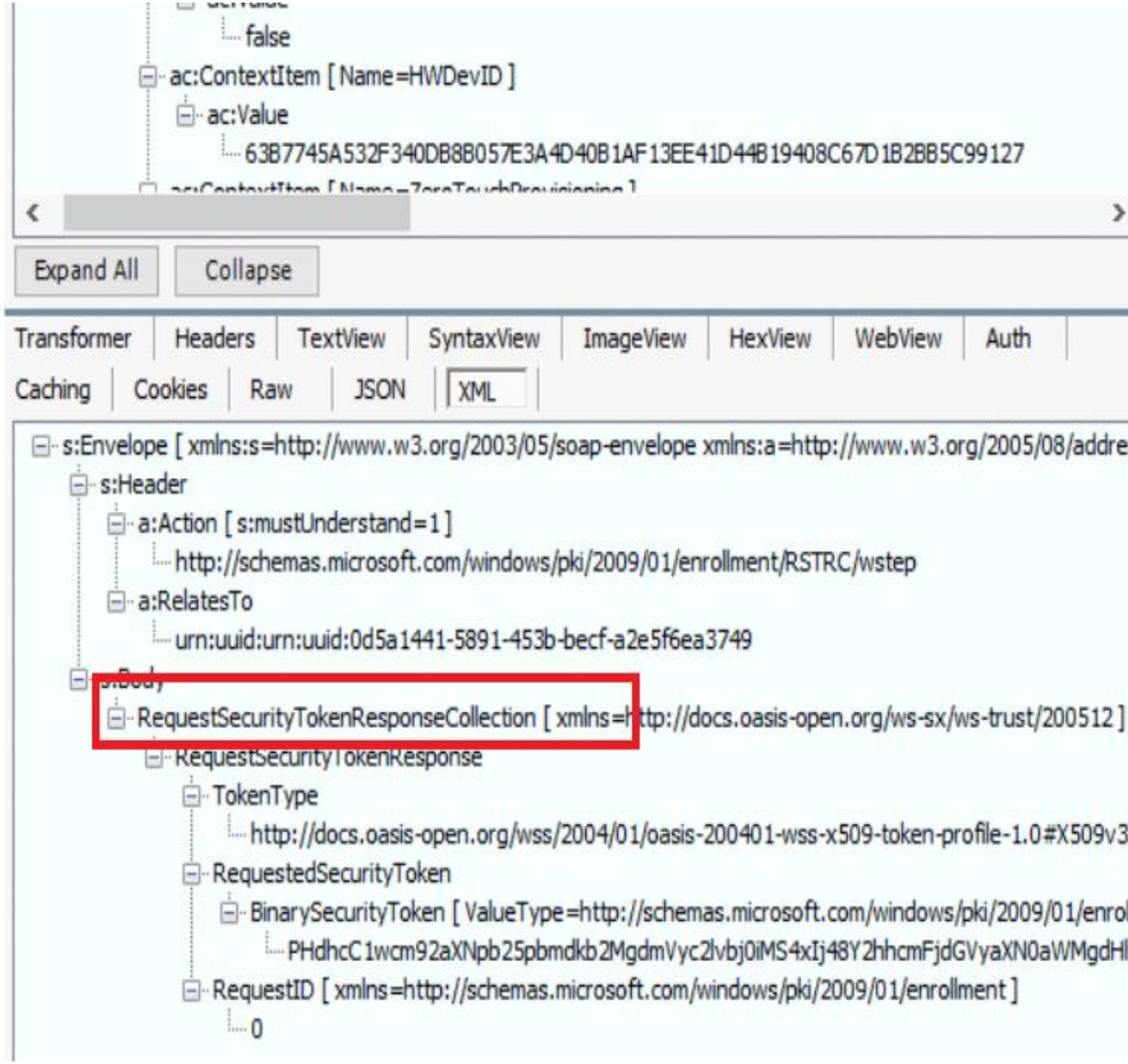
discovery.dm.microsoft.com	/EnrollmentConfiguration?api-version=1.0	590
enrollment.dm.microsoft.com	/deviceenrollment/getpolicies?client-request-id=d8...	2,439
enrollment.dm.microsoft.com	/deviceenrollment/enroll?client-request-id=d884dc...	12,371

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



Microsoft Intune Suite

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



What does EPM enroll into?

It will enroll into….

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

Device Copy

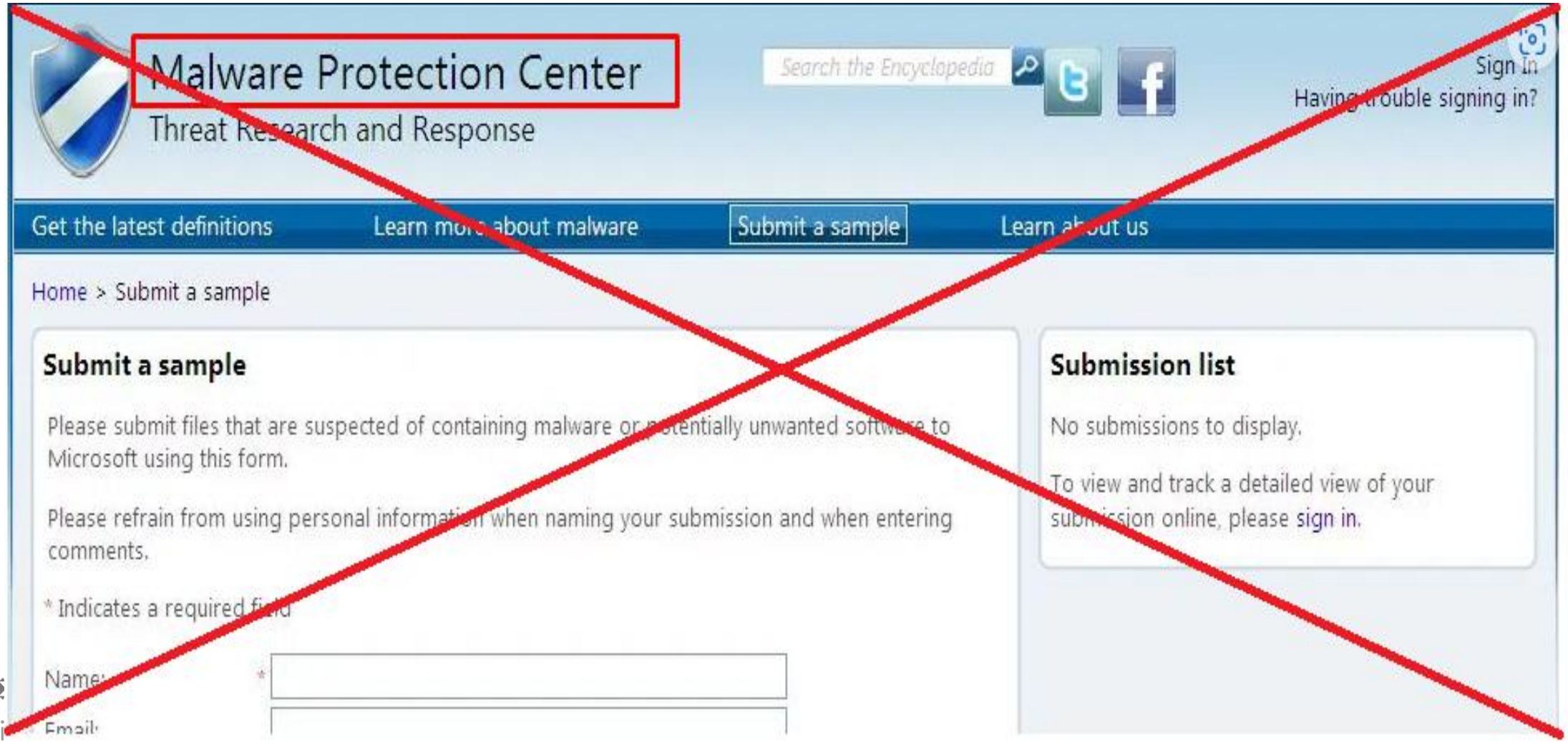
```
./Device/Vendor/MSFT/DMClient/Provider/{ProviderID}/LinkedEnrollment/Enroll
```

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?

Microsoft Malware Protection Center



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.

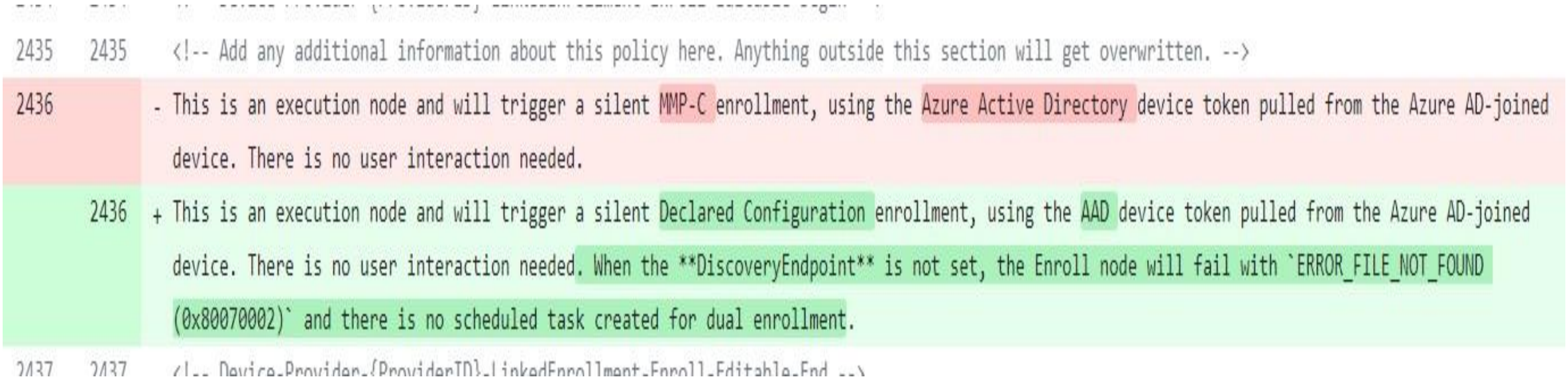
Full version Text-only version View source

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.

Microsoft Docs??

Things change?????

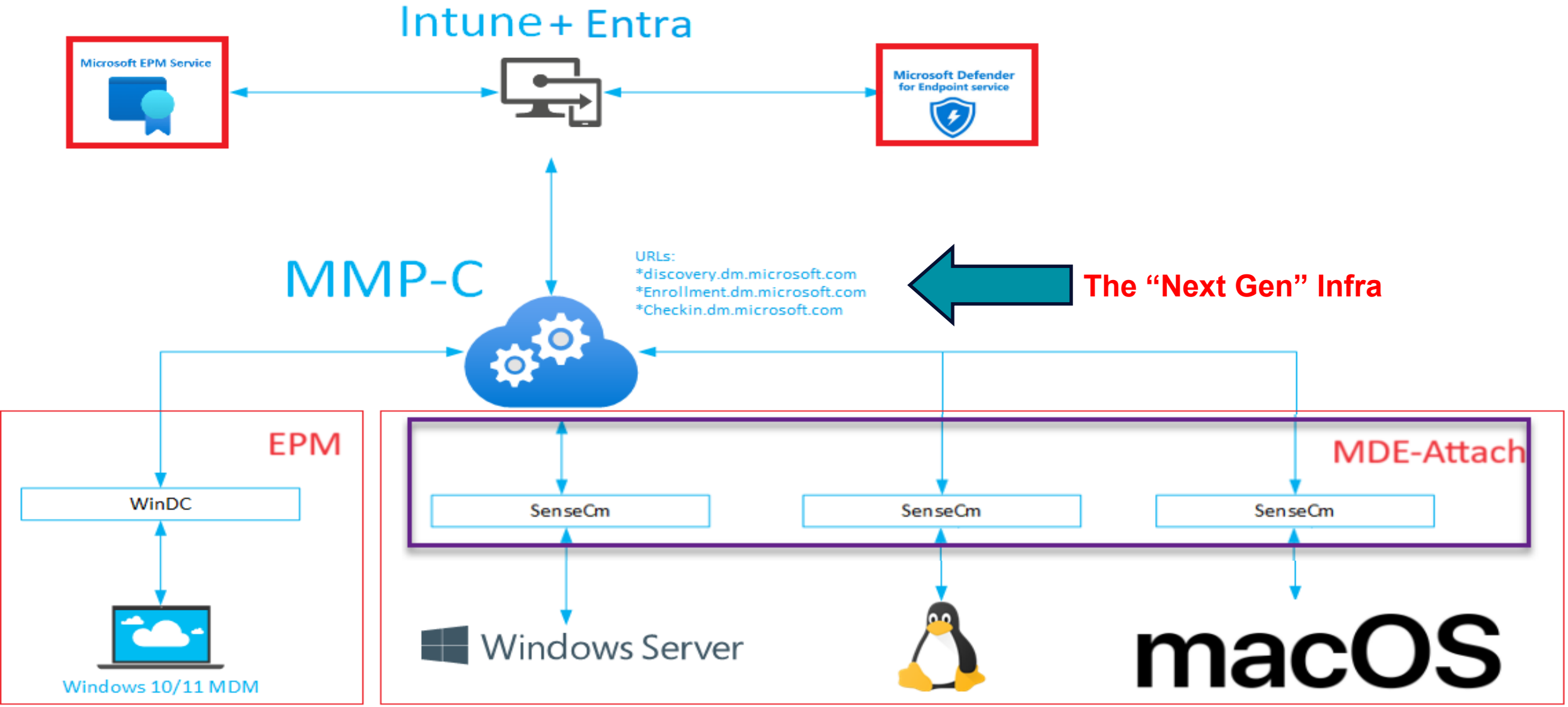


2435	2435	<!-- Add any additional information about this policy here. Anything outside this section will get overwritten. -->
2436		- This is an execution node and will trigger a silent MMP-C enrollment, using the Azure Active Directory device token pulled from the Azure AD-joined device. There is no 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 -->

cegeka

MMP-C is the “Next Gen” MS Infra

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka



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!

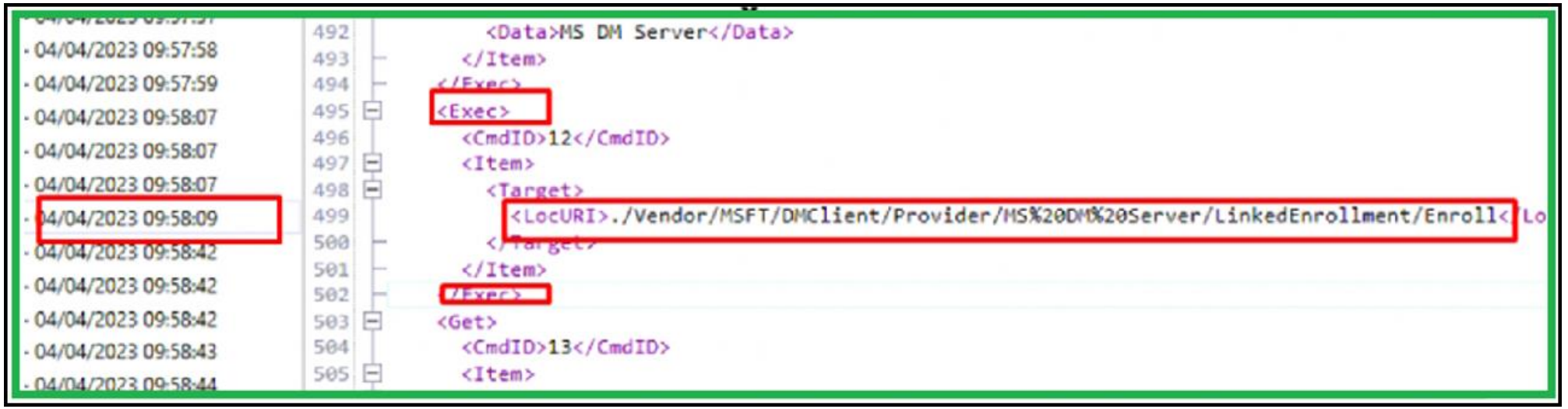
rubrik

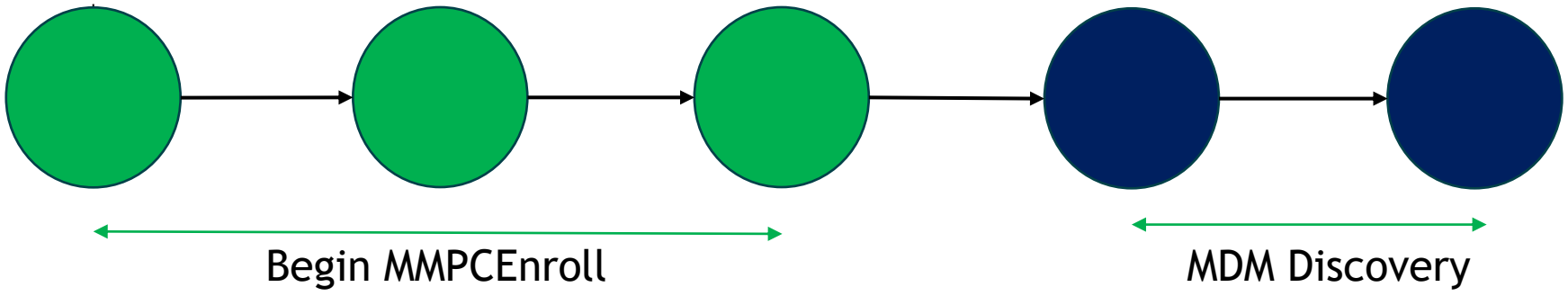
cegeka

Deepdive Activation policy

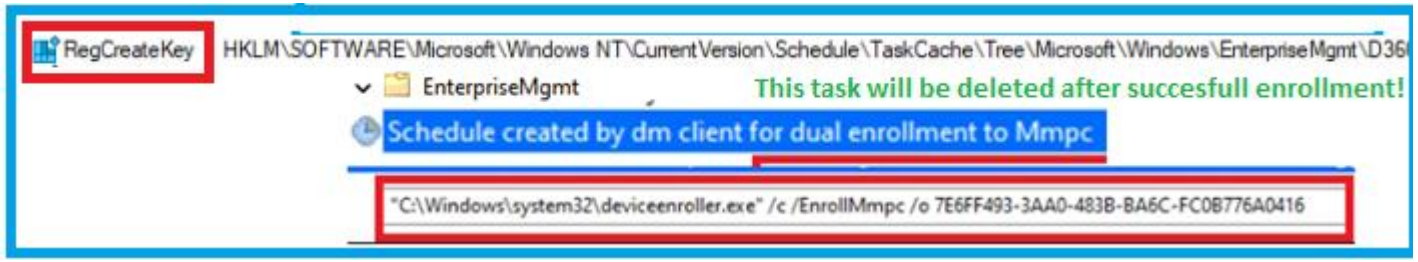
Triggering The Linked Enrollment

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

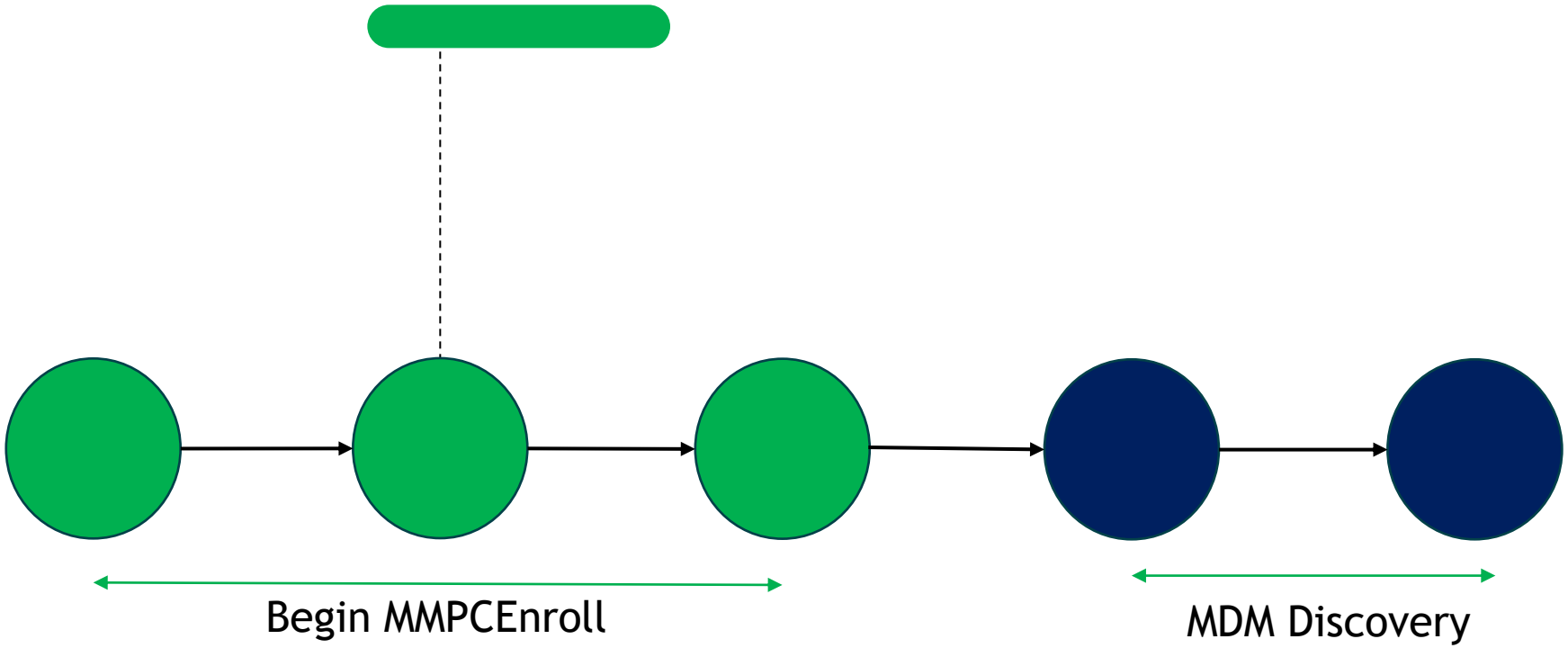




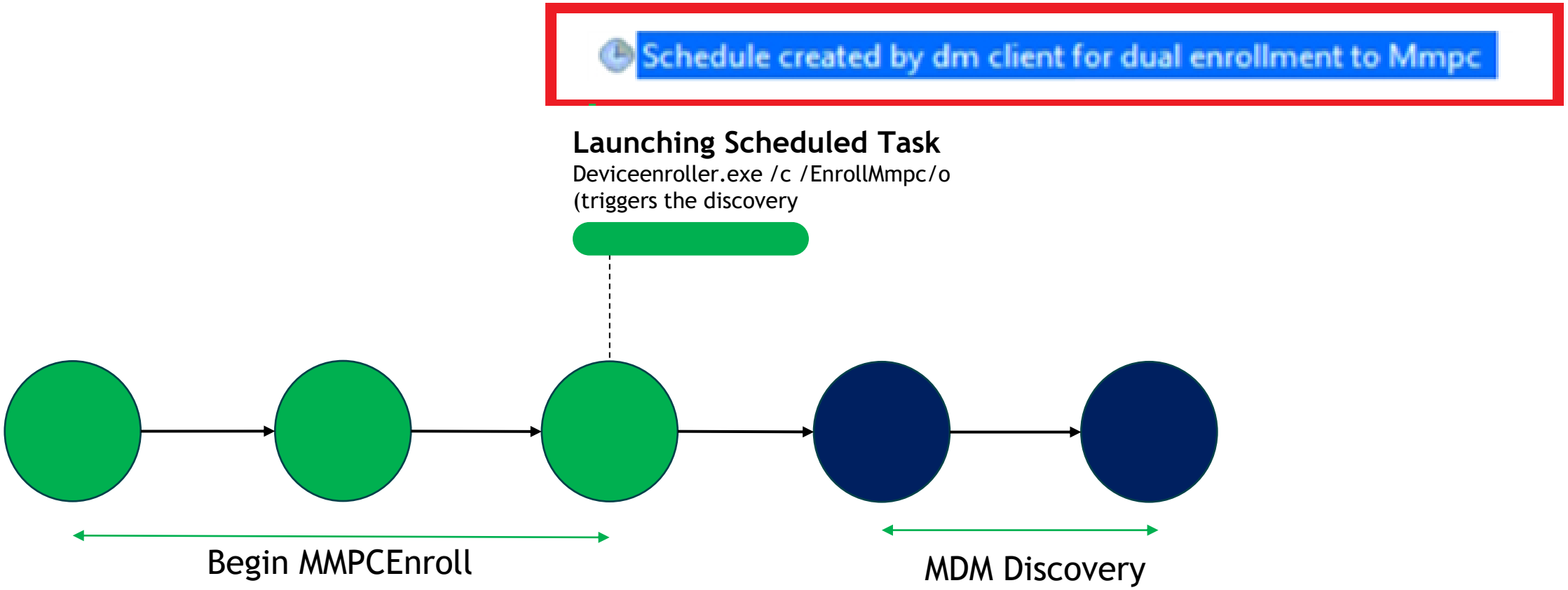
Triggering the Enrollment



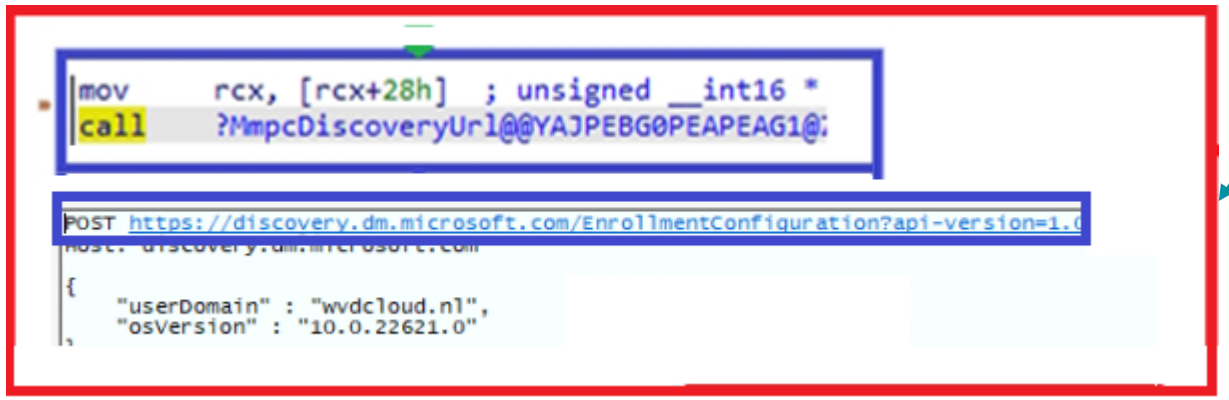
The required scheduled task
For dual enrollment to MMPC will be created



Launching Scheduled Task



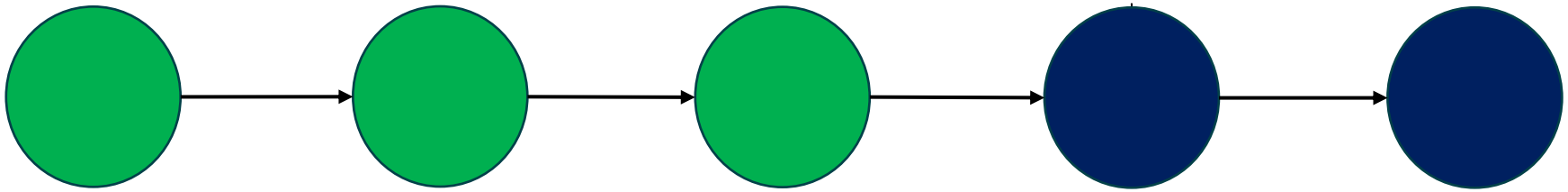
MMP-C Start Discovery



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

MMP-C Start Discovery

Discovery of the Enrollment URLs with:Discovery.dm.microsoft.com



Begin MMPCEnroll

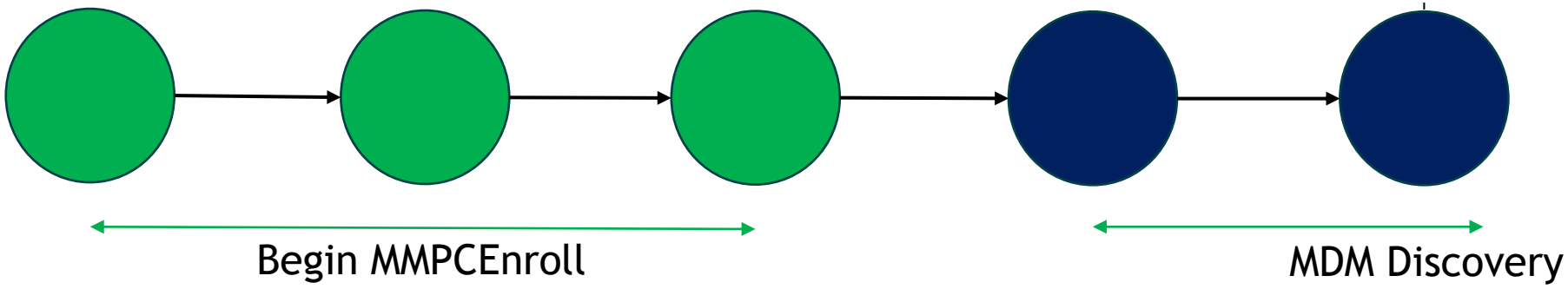
MDM Discovery

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

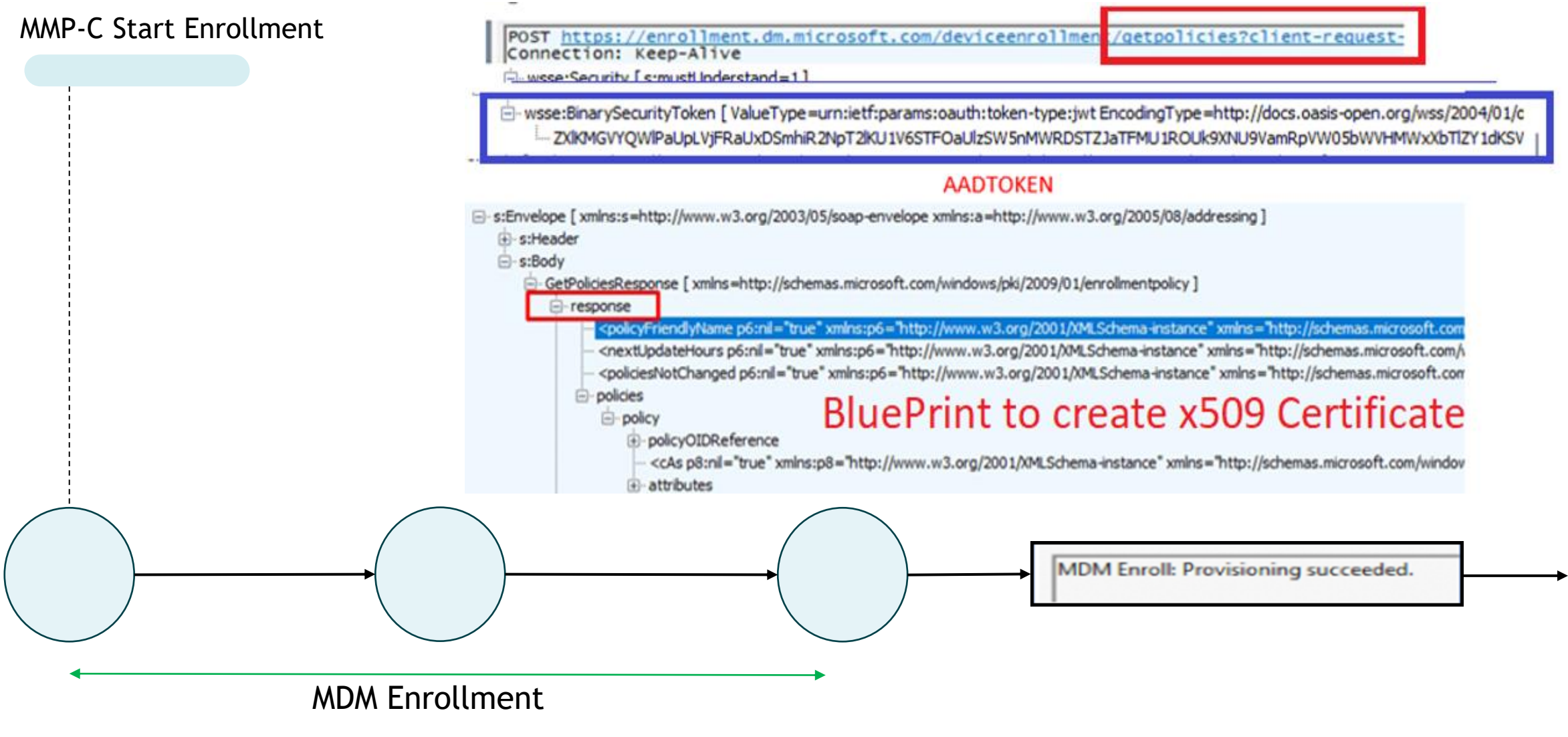
```
AuthenticationServiceUrl=https://enrollment.dm.microsoft.com/enrollmentserver/loginredirect/87f7e2bb-4e07-4f27-93bd-2dab63ee12c7
AuthPolicy=Federated
EnrollmentPolicyServiceUrl=https://enrollment.dm.microsoft.com/deviceenrollment/getpolicies?client-request-id=87f7e2bb-4e07-4f27-93bd-2dab63ee12c7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

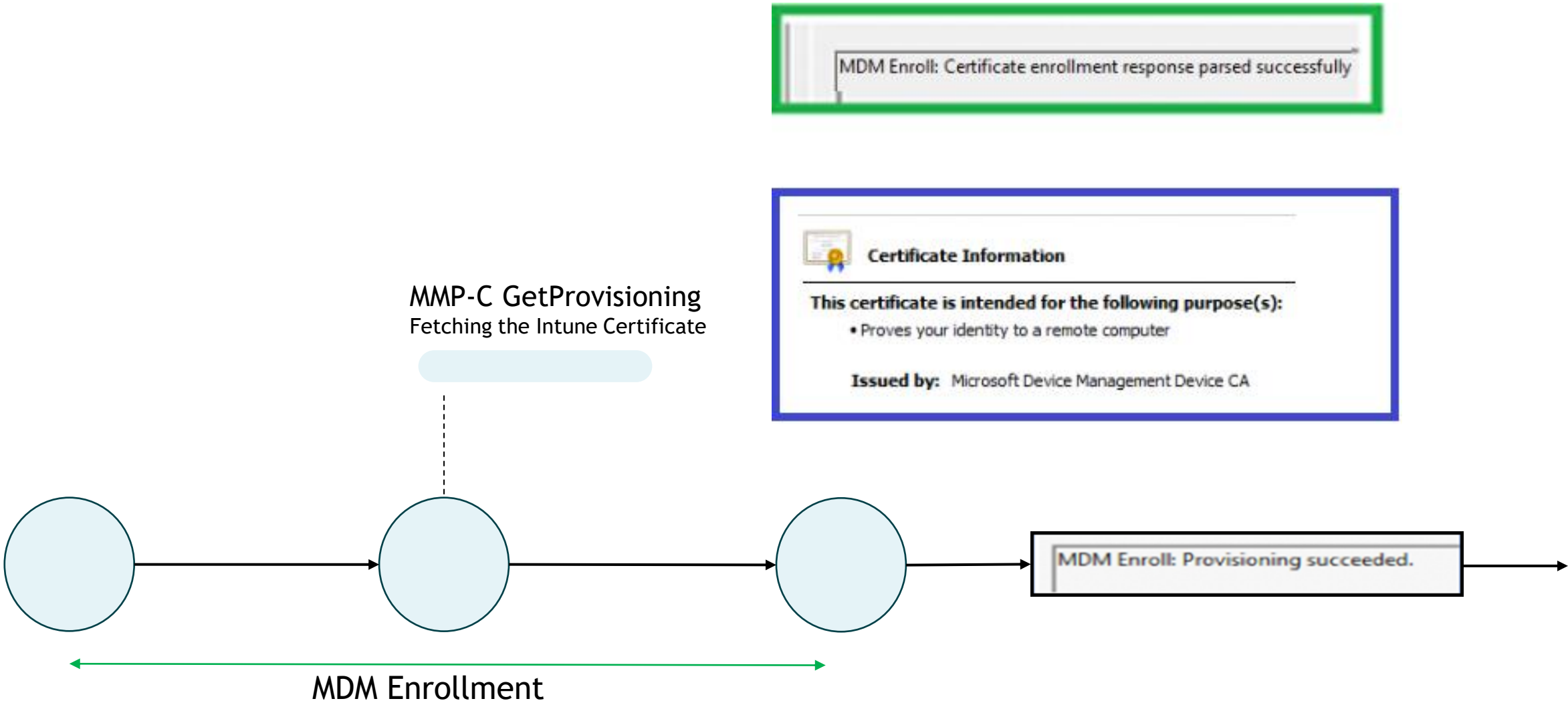


MMP-C Start Enrollment

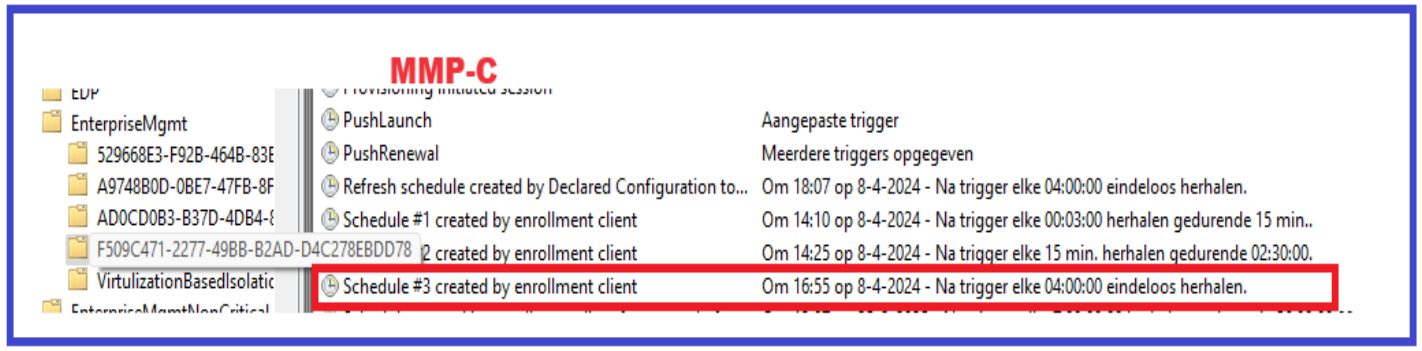
Getting the “Certificate Policies / blueprint”

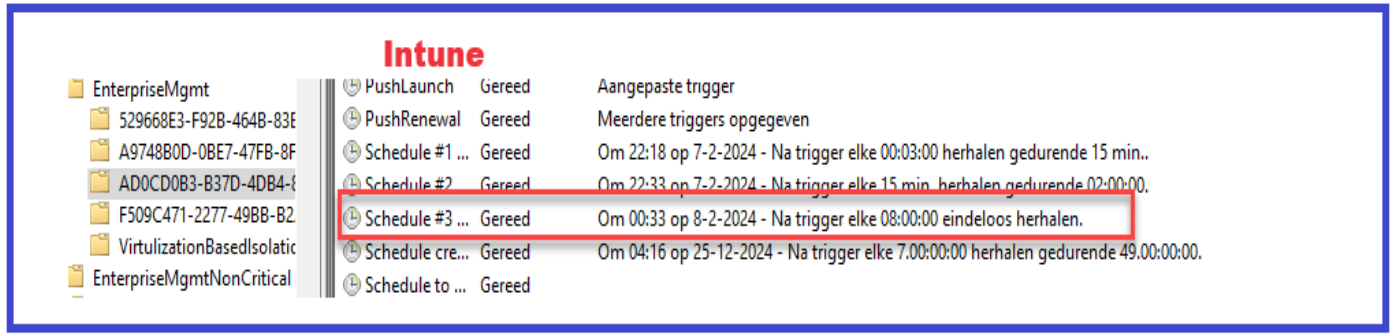


MMP-C Certificate



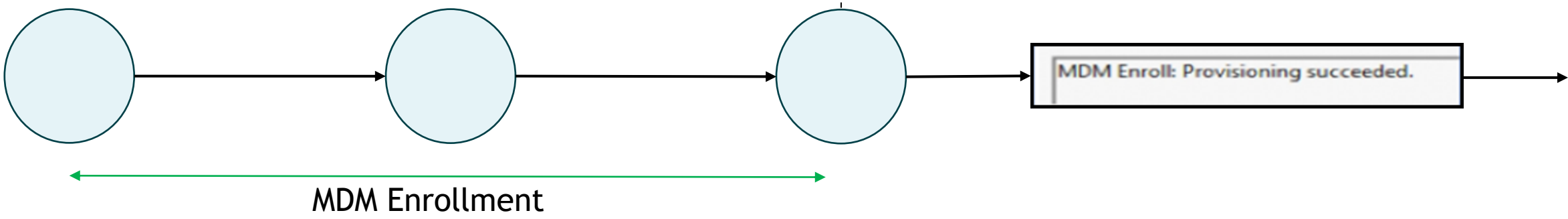
MMP-C Creating the Scheduled Sync Tasks





MMP-C ApplyProvisioning

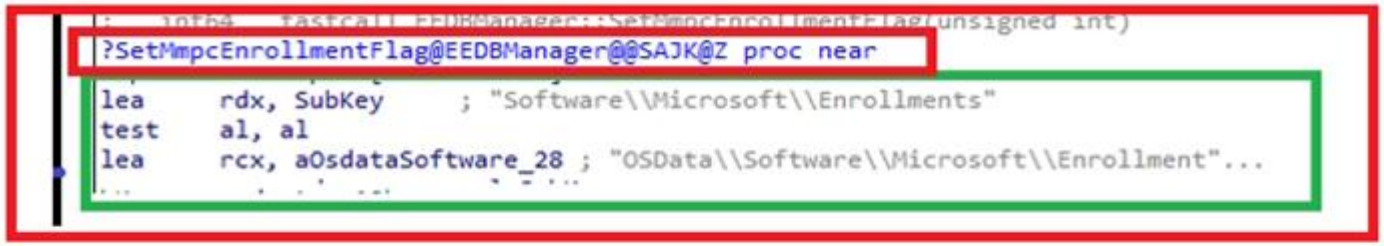
Creating Enrollment Task Schedules

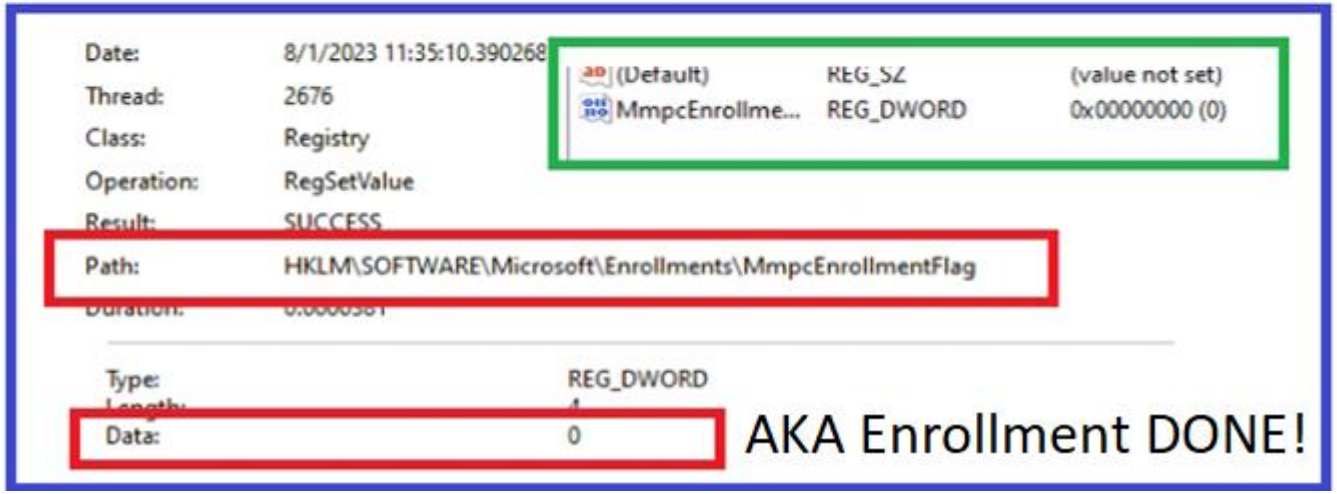


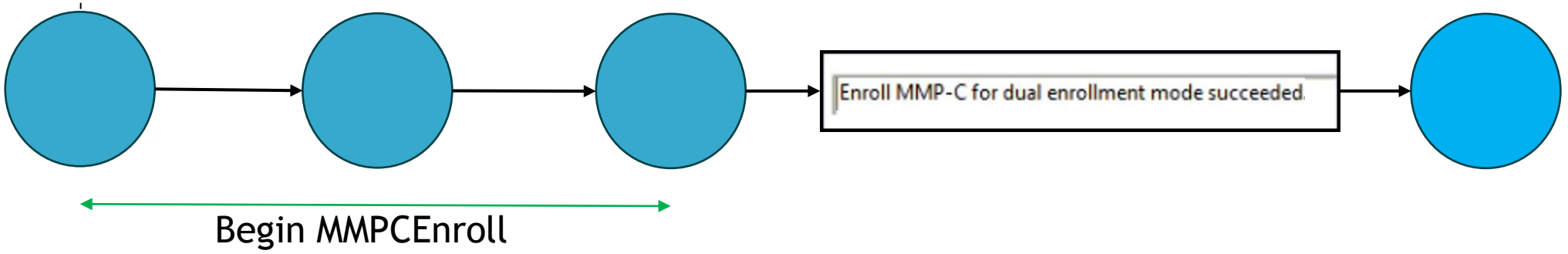
Set MmpcEnrollment Flag

Setting Enrollment Flag

Setting the MMP-C EnrollmentFlag (0)







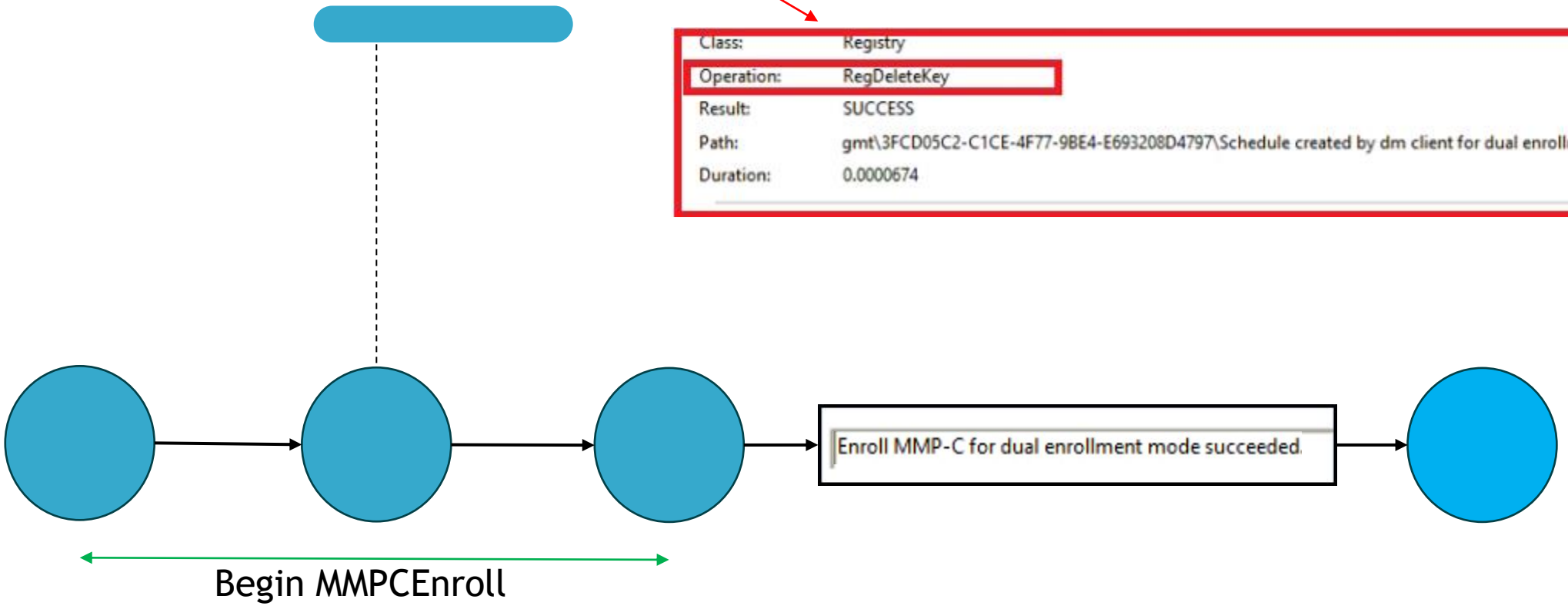
Cleaning Up

```
loc_140013E07:
lea     r8, aScheduleCreate ; "Schedule created by dm client for dual "...
mov     rdx, [rsp+1210h+var_11C0]
lea     rcx, aMicrosoftWindo_1 ; "\\Microsoft\\Windows\\EnterpriseMgmt"
call    cs:__imp_?DmDeleteTask@@YAJPEBG00@Z ; DmDeleteTask(ushort const *,ushort const *,ushort const *)
nop     dword ptr [rax+rax+00h]
```

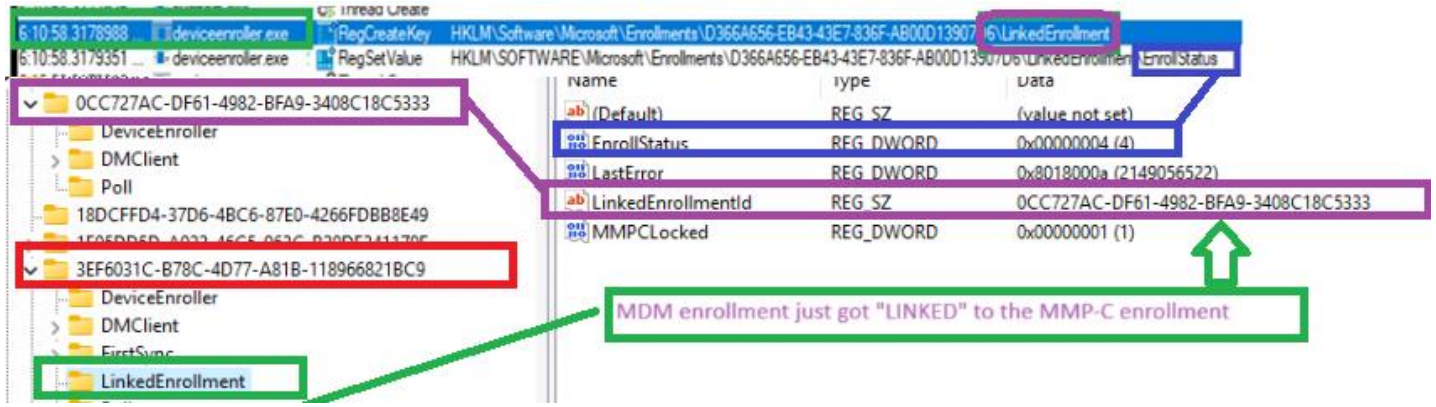
Cleaning up

-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

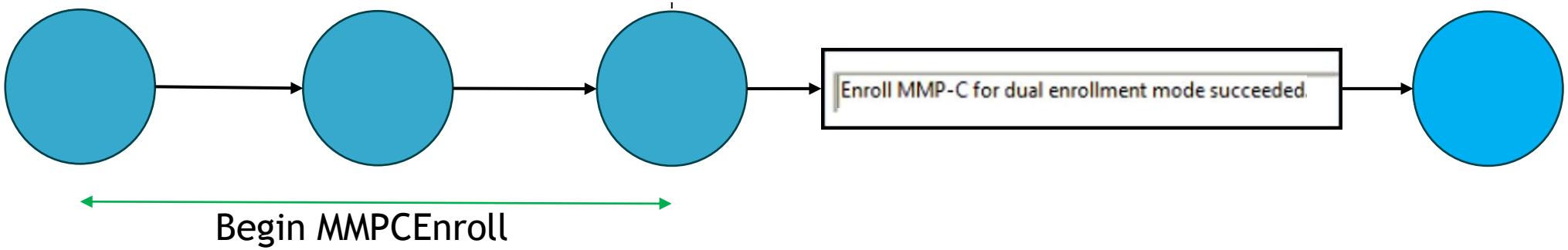


Linking Enrollments

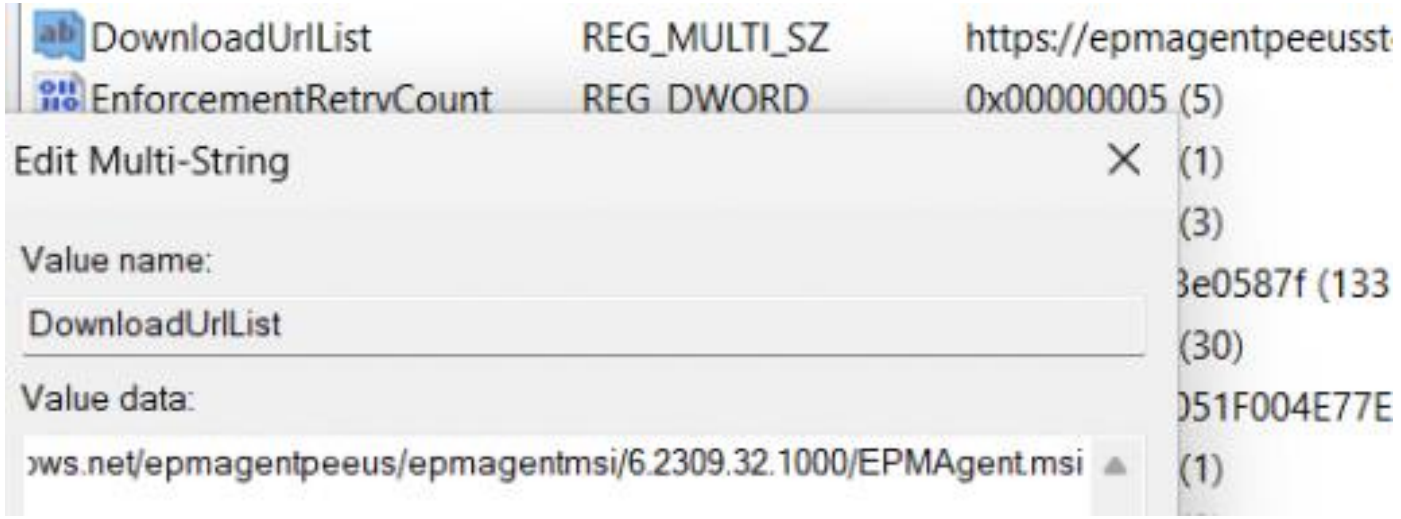


Finishing Enrollment

"Linking" the **MDM** with the **MMP-C** enrollment

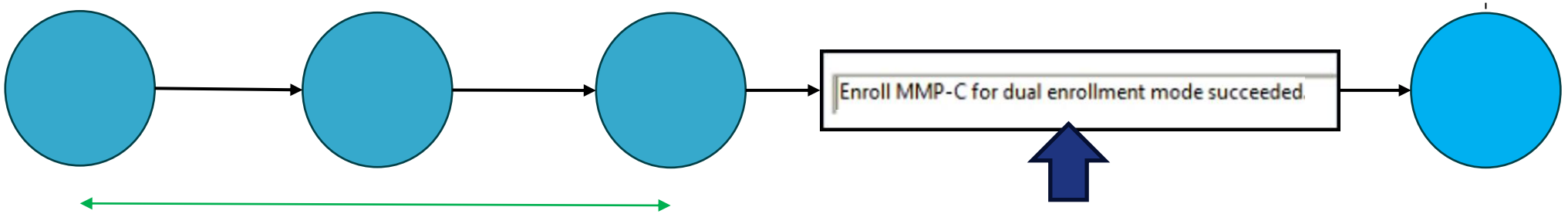


Installing EPM Agent



EPM Agent install

Downloading and installing the MDMAppinstaller AKA EPM Agent



Begin MMPCEnroll

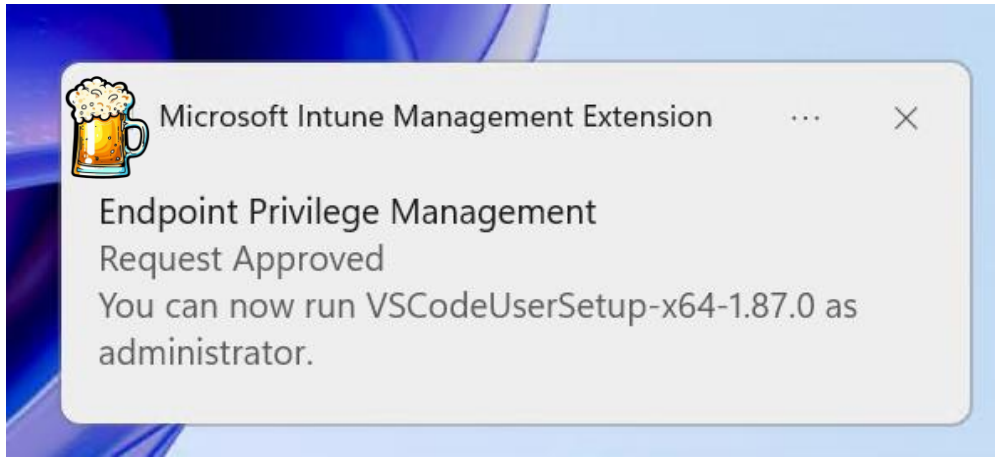
Without a succesful MMP-C enrollment NO EPM AGENT!!!!

5. A quick recap

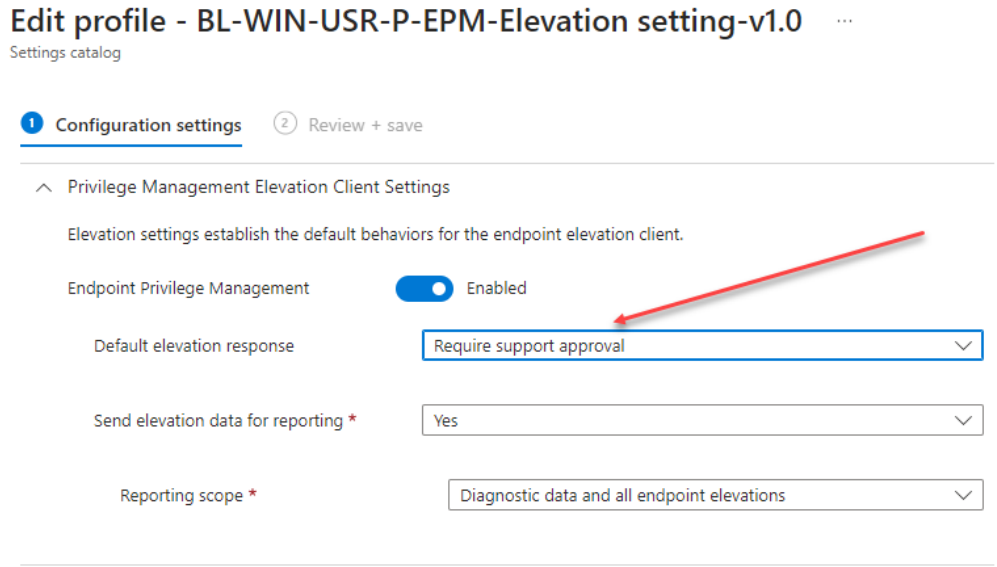
- **We activated the Intune Suite and configured EPM**
- **This will push a CSP to kick off a Linked/Dual enrollment**
- **The CSP would trigger the device to enroll into MMP-C**
- **This “enrollment” looks the same as the well known Intune enrollment**
- **Without the MMP-C Enrollment NO Epm Agent!**

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

6.New Feature: Support Approved



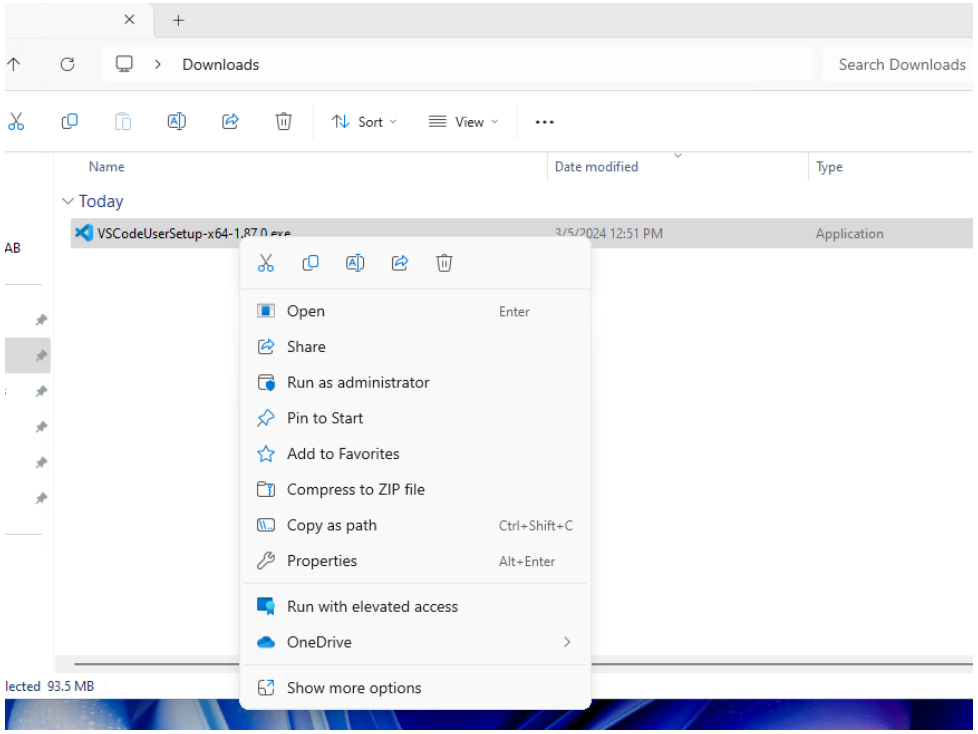
- New Feature to EPM (Require Support Approval)
- Allow users to request temporary administrative privileges for specific applications or tasks
- Intune administrators can approve or deny

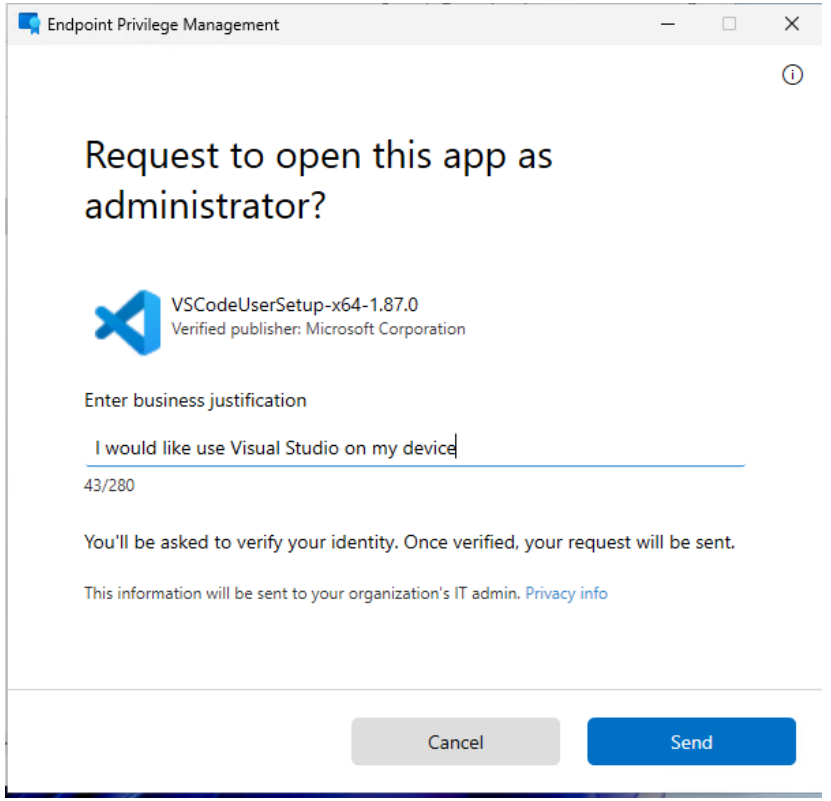


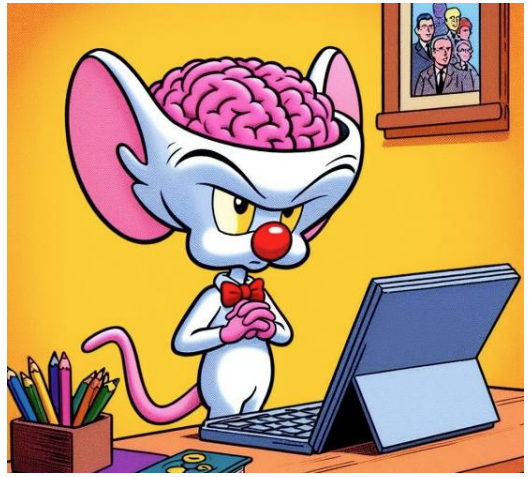
Story line EPM SA

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

John perspective

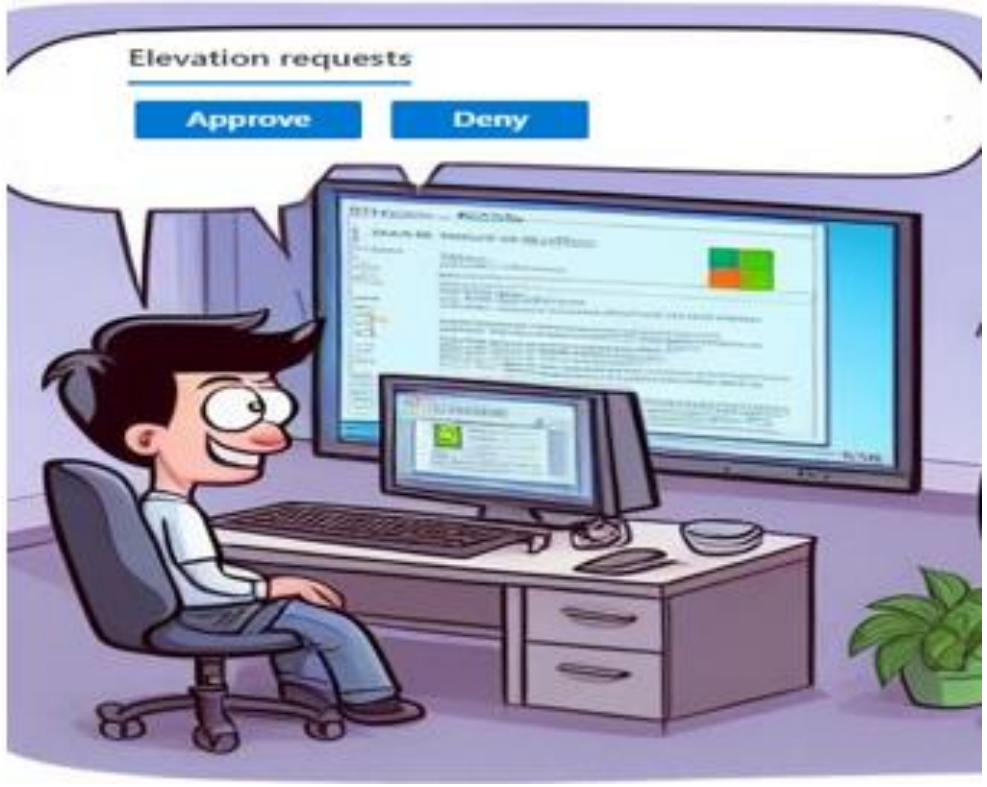






rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

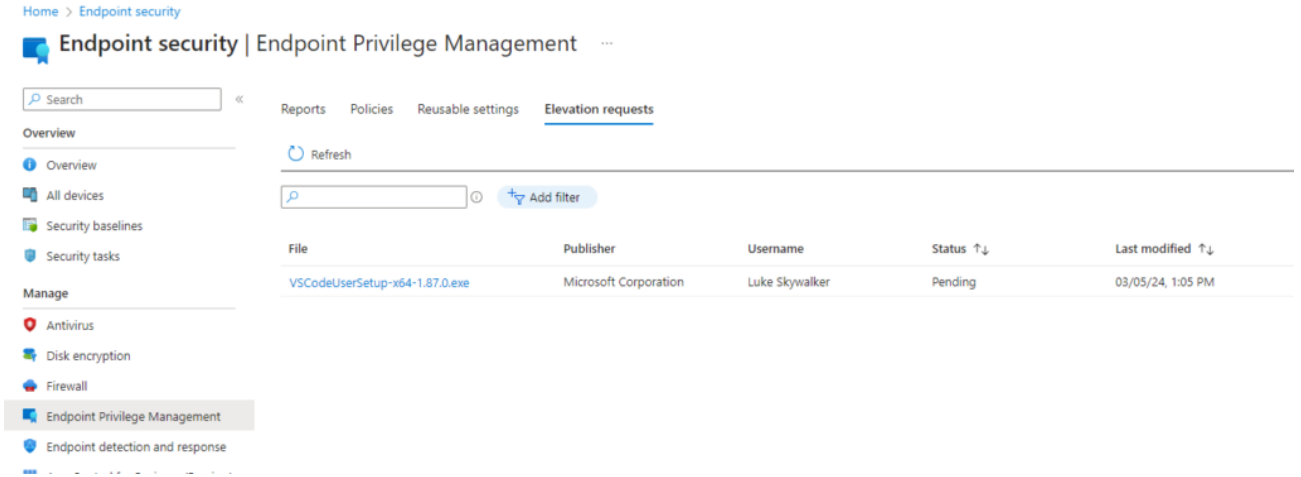
Story line EPM SA

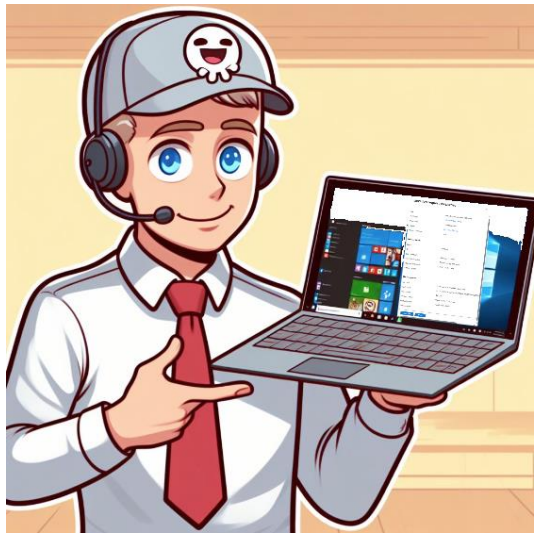


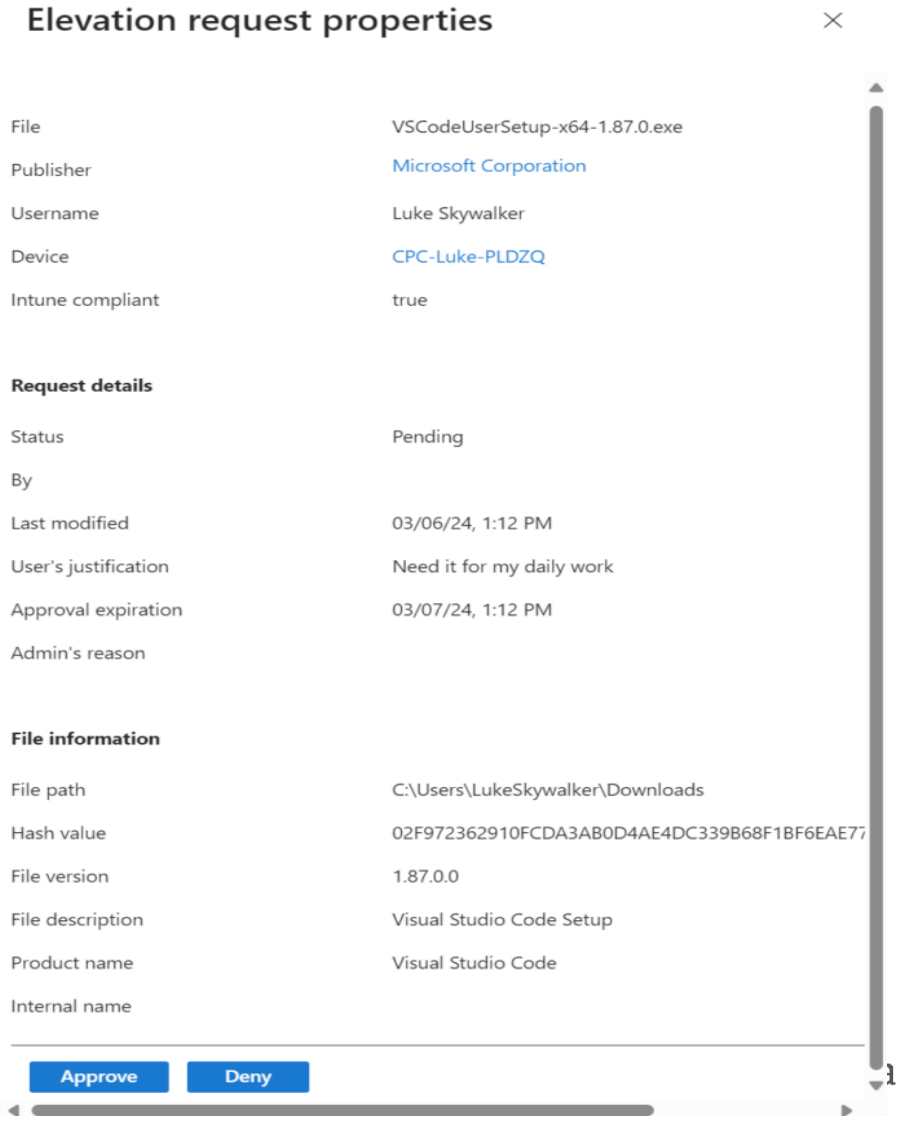
- Support Engineer notices the request in Intune
- The Admin approves or denies request

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

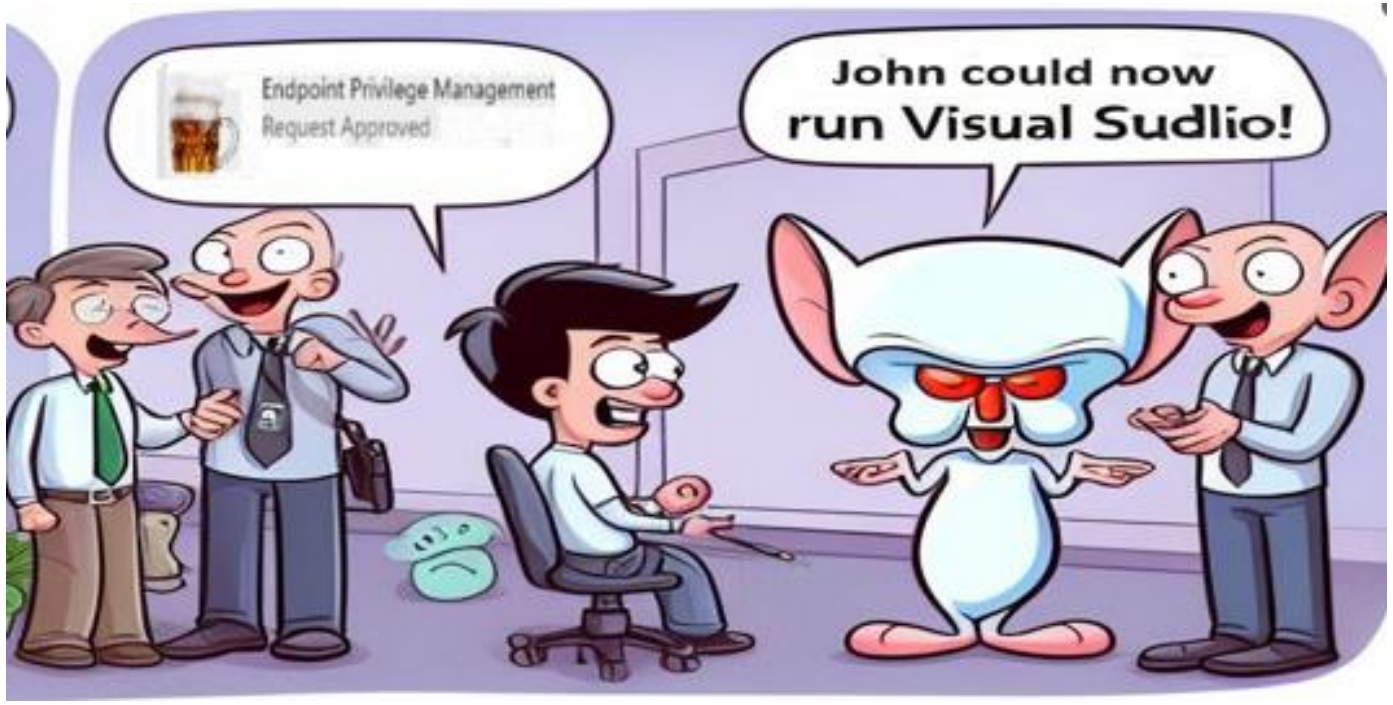
Support Engineer perspective







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**

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

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)

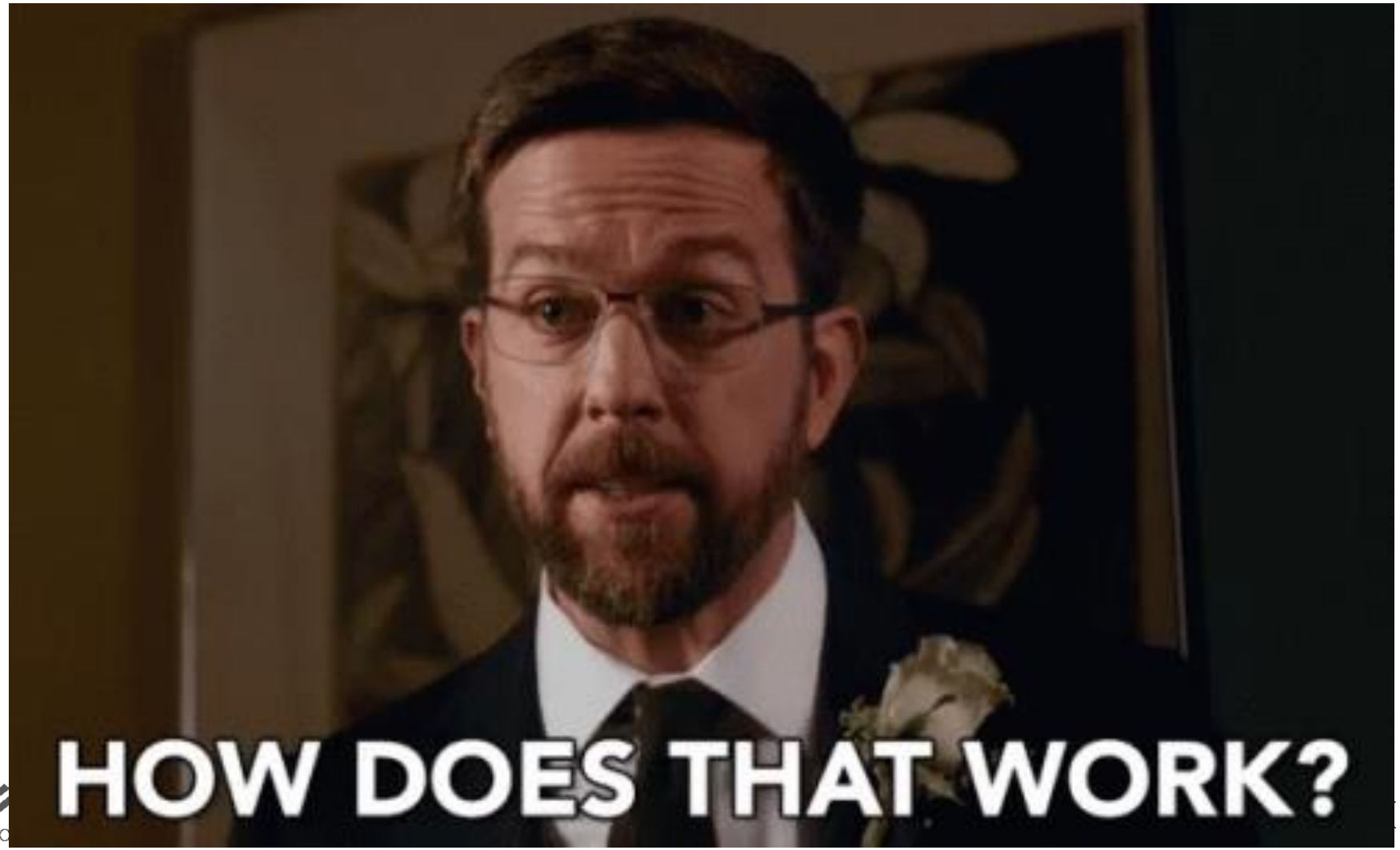
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

7. The Elevation rules

```
PS C:\Program Files\Microsoft EPM Agent\EpmTools> Import-Module .\EpmCmdlets.dll
PS C:\Program Files\Microsoft EPM Agent\EpmTools> Get-Policies -PolicyType ElevationRules -Verbose | Format-Table -AutoSize
VERBOSE: Retrieving EPM Agent policies information for policy type 'ElevationRules'.
VERBOSE: Policies processed by the ElevationRules adapter, count=1

ExeFileNames                                                PolicyId                             Version
------------                                                --------                             -------
Powershell.exe,PowerShell.exe,PowerShell.exe,powershell.exe 8122a726-fd81-447a-873d-ccd4fd0b2cdf DEA4A693F42...
```

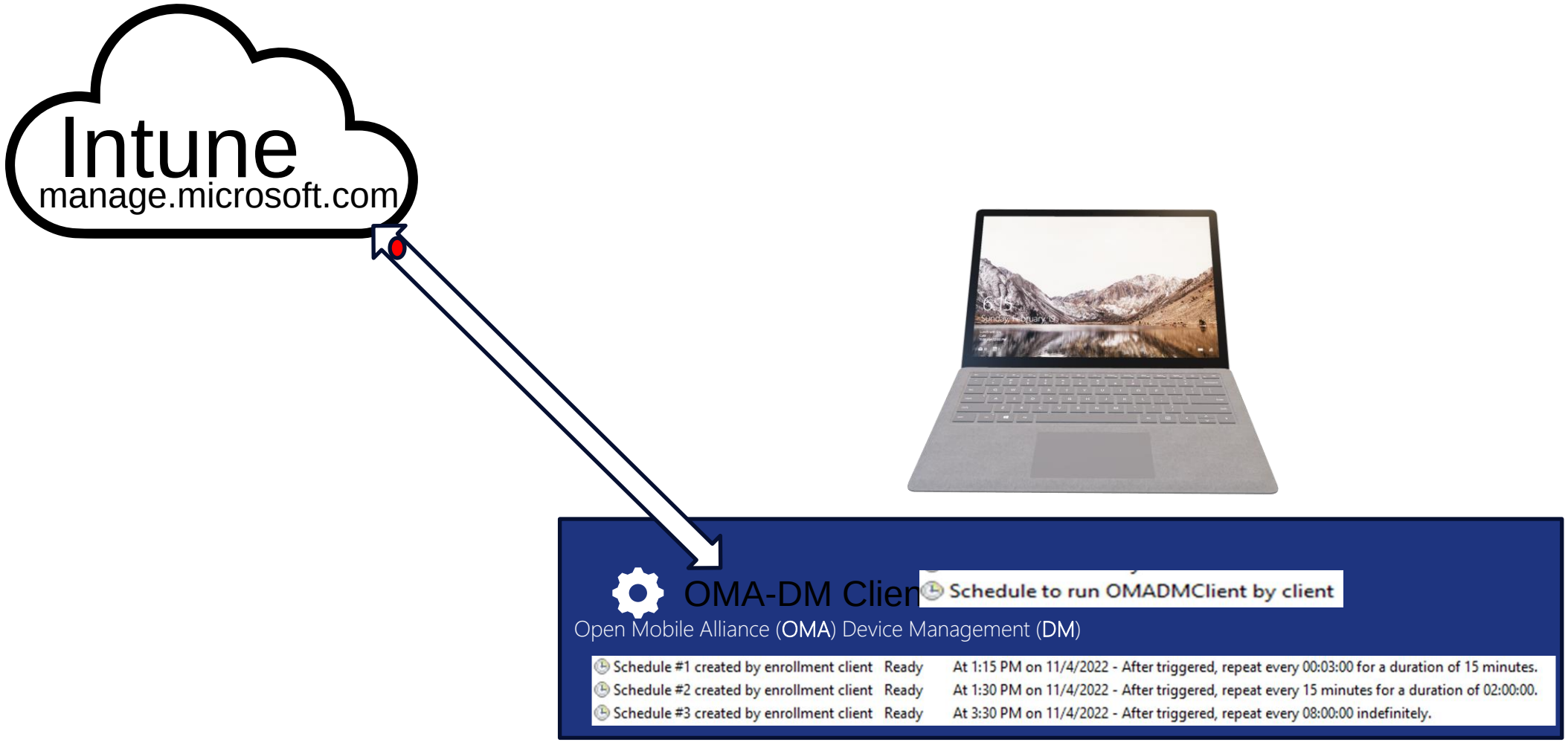
How did they arrive on the device?



rubrik

cegeka

Intune only enrolled Device

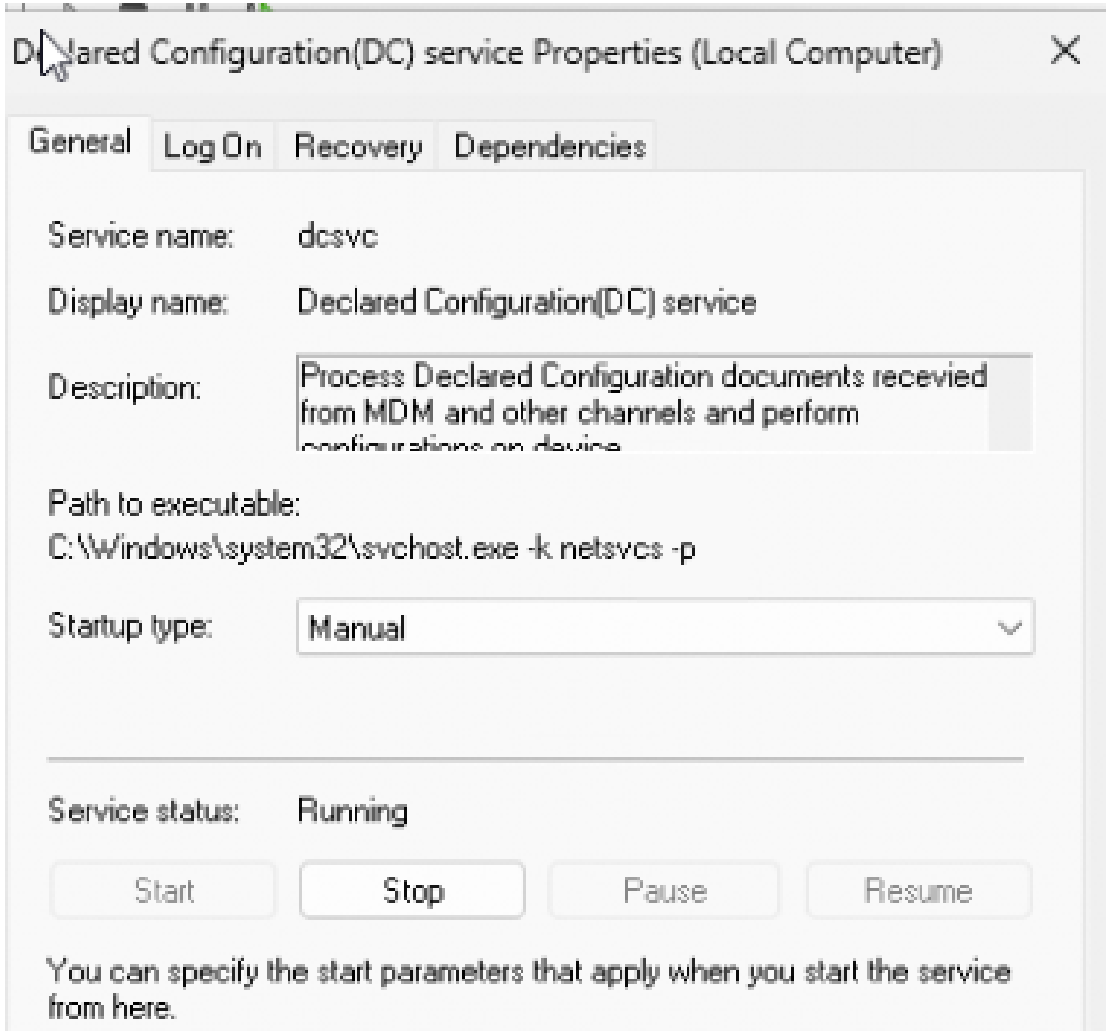


MMP-C has??

The “Unknown” Service

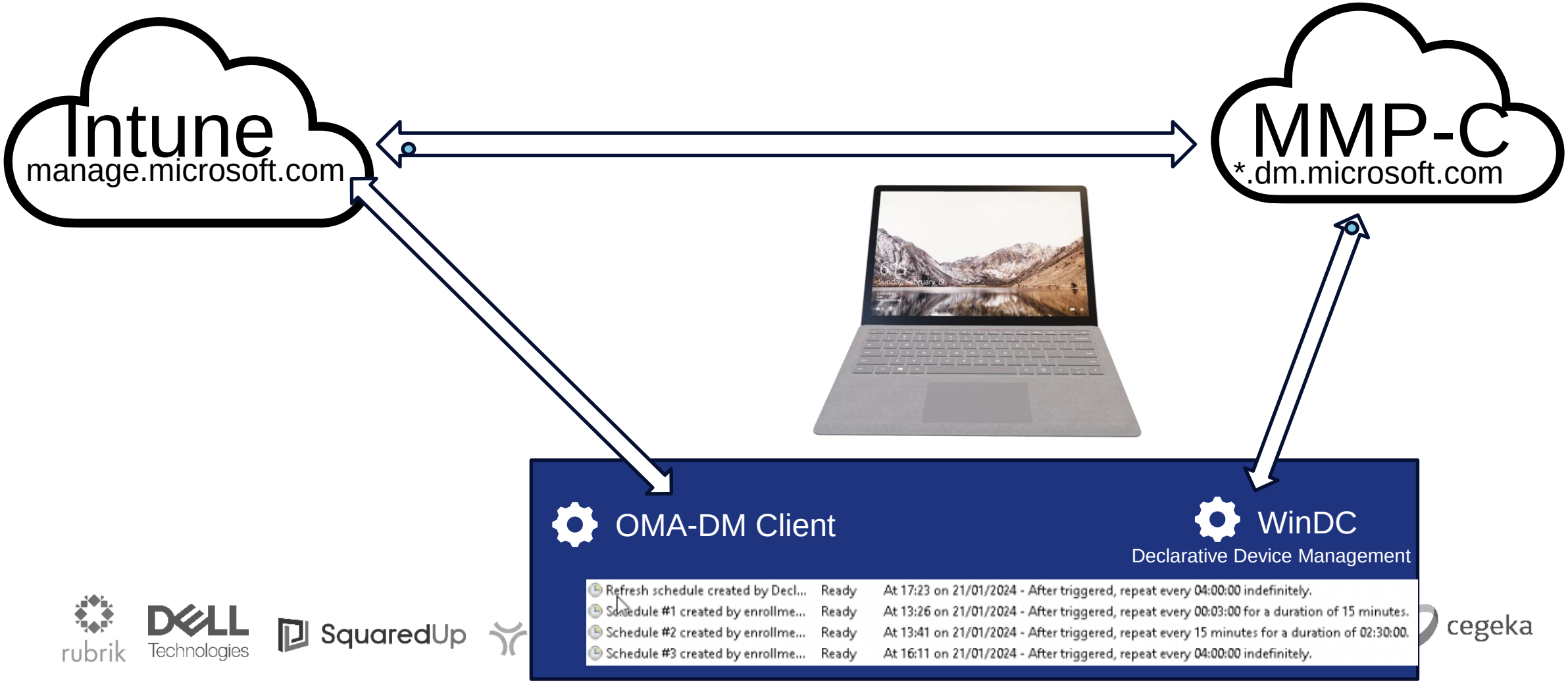
“enabled/Activated” with this update:

August 25, 2022—KB5016691



Intune + MMP-C enrolled Device

(Dual Enrolled State)



rubrik DELL Technologies SquaredUp cegeka

8. The Future is bright!

DeclaredConfiguration CSP - Windows Client Management | Microsoft Learn

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

The future is indeed bright!

rubrik DELL Technologies Squ twork INSPARK cegeka

Let me show you!!!

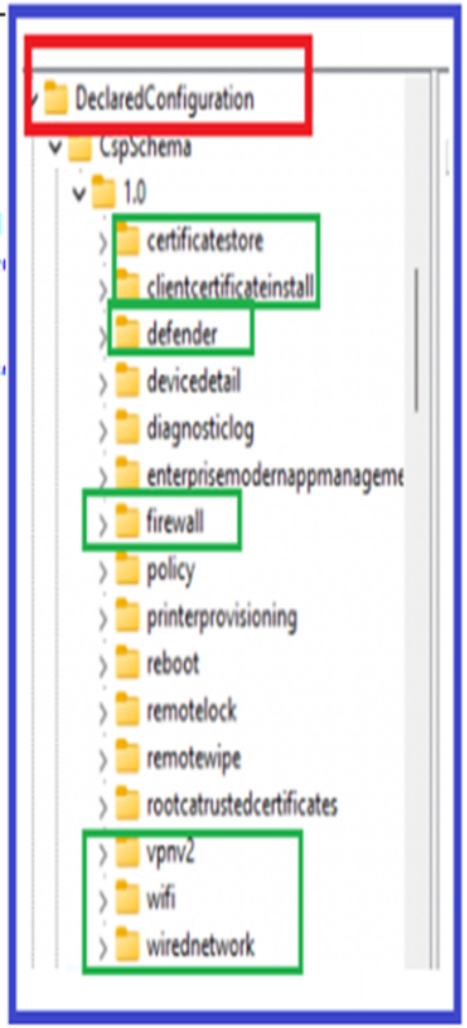
rubrik

cegeka

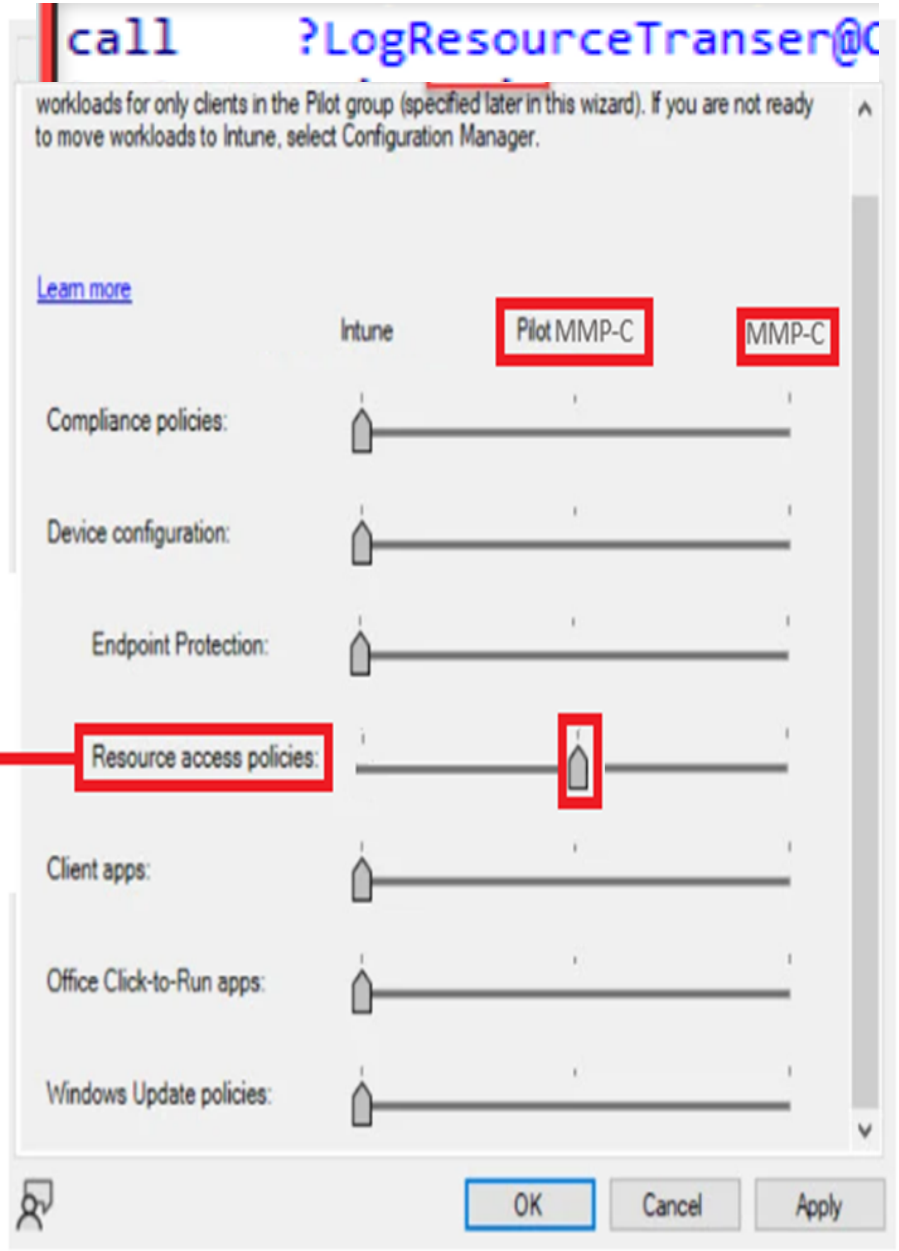
8. Moving the ~~SCCM~~ MDMworkloads

DeclaredConfiguration\HostOS\Config\Enrollments\F509(

csp	REG_SZ	./Vendor/MSFT/CertificateStore



- Certificate profiles,
- VPN profiles
- Wi-Fi profiles



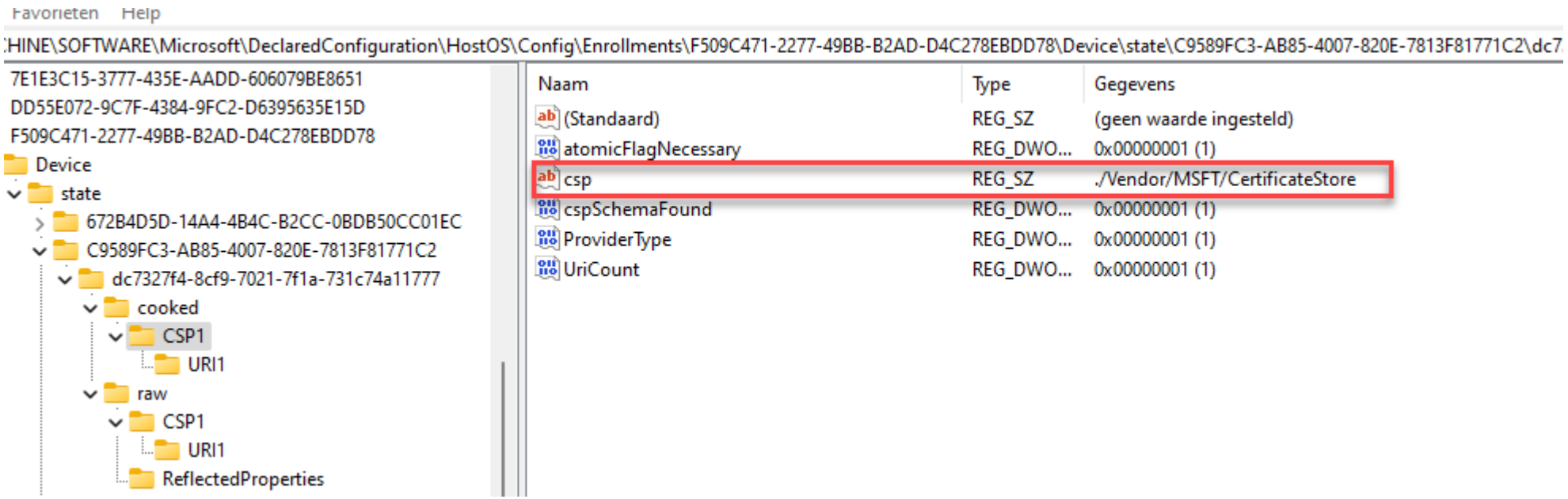
- dcsvc.dll.i64 (dcsvc.dll) C:\install\insider 03-2024\dcsvc.dll.i64

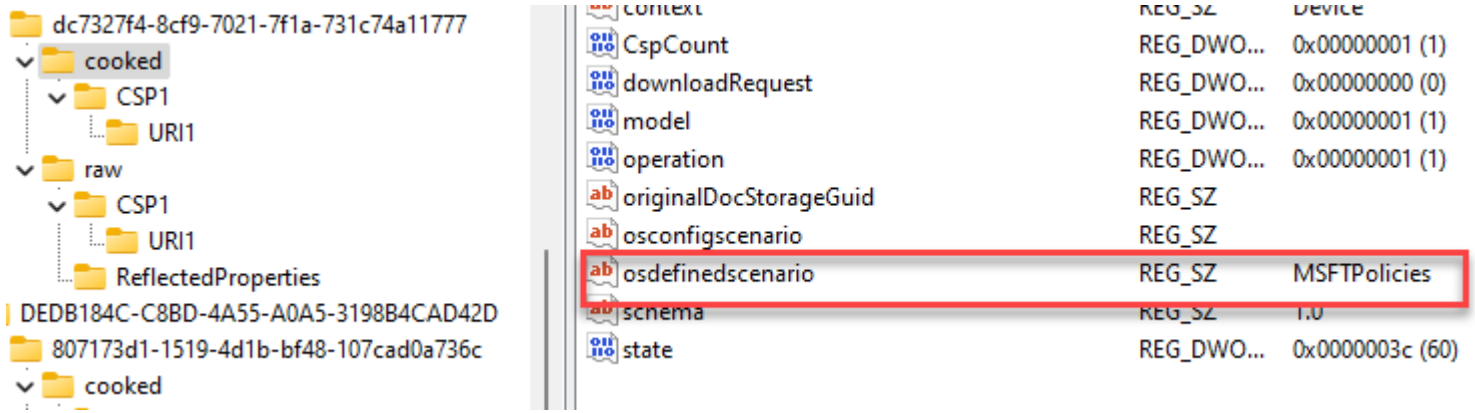
```
?DeclaredConfiguration_CreateCookedSettings@

; __int64 __fastcall CSPProviderCo
?CSPProviderConfiguration@@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") )
{
```

8. Certificate Resource Policies being “moved”





rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

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 revolutonize device management**

Please evaluate this session in the App.

THANK YOU

Are there any questions?