



WORKPLACEDUDES

*Meetup*

**Dr Intune, how I  
stopped syncing and  
loved the enrollments**



# Who is that guy?

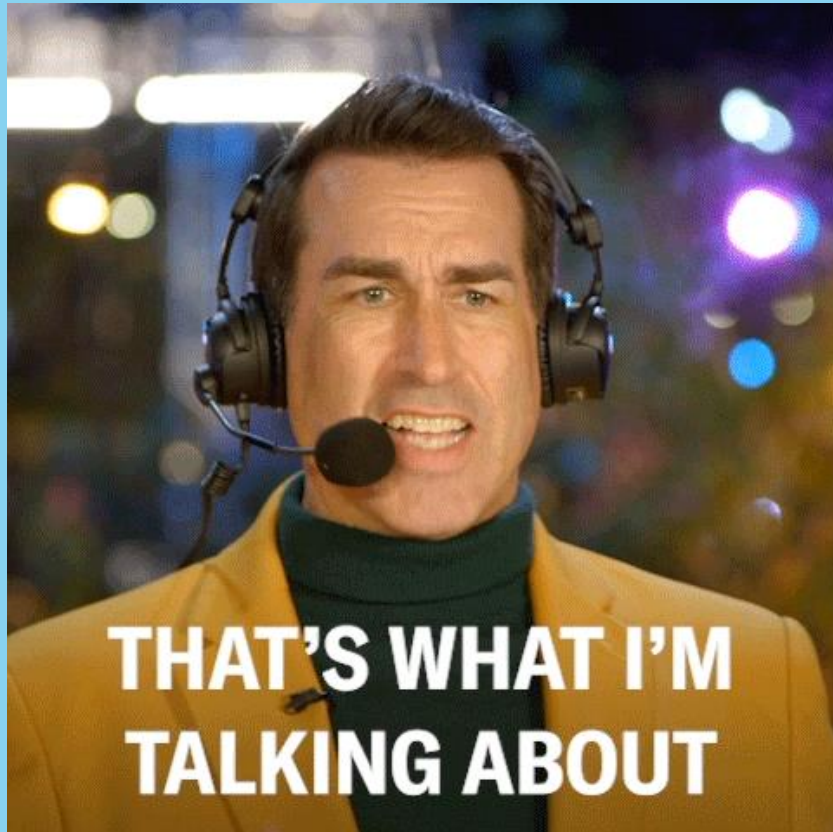
- Microsoft MVP
- Cloud Architect | Deltacom
- Blogger | Call4Cloud
- Twitter: @Mister\_MDM
- Email: [info@call4cloud.nl](mailto:info@call4cloud.nl)



- What do I love? Good Beer!!







1. The Two  
Enrollments

2. Taking a first  
look at  
Enrollment 2

3. Enrollment 2  
Overview and  
maybe a Demo

4. The "Unknown  
Service"

5. Summary



# A Small Warning!!! Or maybe not





# 1. The Two Enrollments





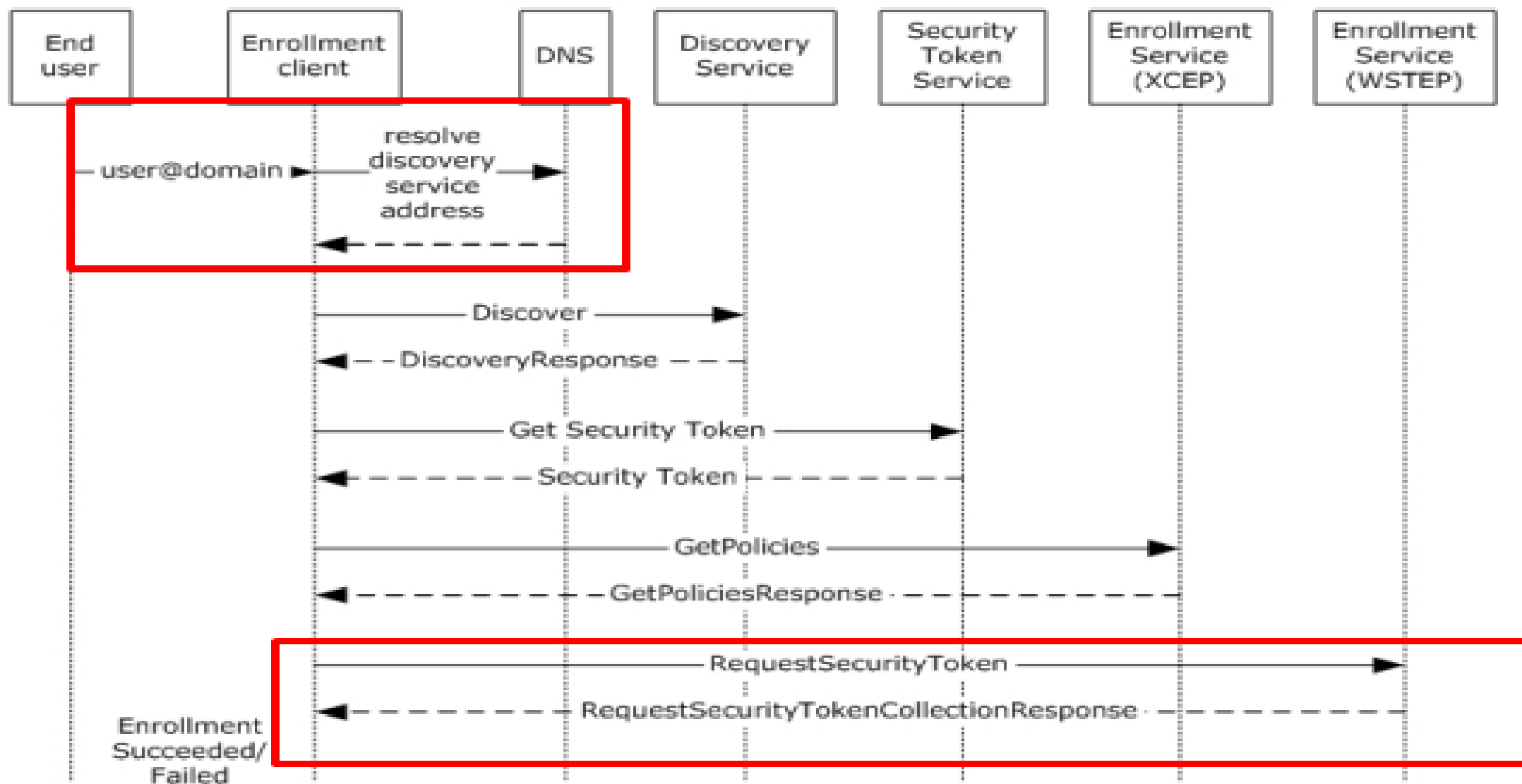
# First Enrollment: Intune







# The MDE Basics





## 2. Second Enrollment: EPM

### Activate Endpoint Privilege Management (preview) for your tenant now

Manage how your organization handles requests for privileged access to apps and files on devices by creating rules for standard users to get just-in-time elevation.

You must activate this feature for your tenant during public preview. Once activated, it can't be undone. No changes to devices will occur until you update your Intune policy.

**Activate**

#### ^ Privilege Management Elevation Client Settings

Endpoint Privilege Management Enabled

Send elevation data for reporting Yes

Reporting scope Diagnostic data and all endpoint elevations

Default elevation response Deny all requests



# EPM Enrollment Flow

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



XML View of SOAP Response:

```
<?xml version='1.0' encoding='utf-8'>
  <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#X509v3</TokenType>
          <RequestedSecurityToken>
            <BinarySecurityToken [ValueType='http://schemas.microsoft.com/windows/pki/2009/01/enrollment/BinarySecurityToken']>PHdhcC1wcm92aXNpb25pbmdkb2MgdmVyc2lvbj0iMS4xIj48Y2hhcmFjdGVyaXN0aWwMgdHl</BinarySecurityToken>
          </RequestedSecurityToken>
          <RequestID [xmlns='http://schemas.microsoft.com/windows/pki/2009/01/enrollment']>0</RequestID>
        </RequestSecurityTokenResponse>
      </RequestSecurityTokenResponseCollection>
    </s:Body>
  </s:Envelope>
```



# What does it enroll to?





# It will enroll into....

When activating EPM a CSP will be pushed to trigger...?

Device	Copy
<code>./Device/Vendor/MSFT/DMClient/Provider/{ProviderID}/LinkedEnrollment/Enroll</code>	

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.

**Okay... but what is MMP-C?**







# Microsoft Malware Protection Center



## Malware Protection Center

Threat Research and Response

*Search the Encyclopedia*  

[Sign In](#)  
Having trouble signing 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](#).



# Microsoft Docs??



**And long live LinkedIn!**

## - Principal Engineering Manager - Microsoft

Greater Seattle Area · Principal Engineering Manager · Microsoft

Overall Eng Leader (GC) for v1 product **MMPC** across multiple organizations. Owned... Worked on multiple high-scale, high-impact product areas for Microsoft:

### - Microsoft Managed Platform Cloud

Overall Eng Leader (GC) for v1 product **MMPC** across multiple organizations. Owned design/architecture/engineering/release/security/perf for AP, **WCOS check-in** and reporting services. Developed algorithms & protocols to deliver pre-computed payload to a group of devices making check-in reliable and scalable. Managed MMPC team for check-in/reporting and drove project with 10-20 people across MMPC and Windows division.



# Microsoft Managed Platform - Cloud



# Microsoft Intune v2



# Something to think about!

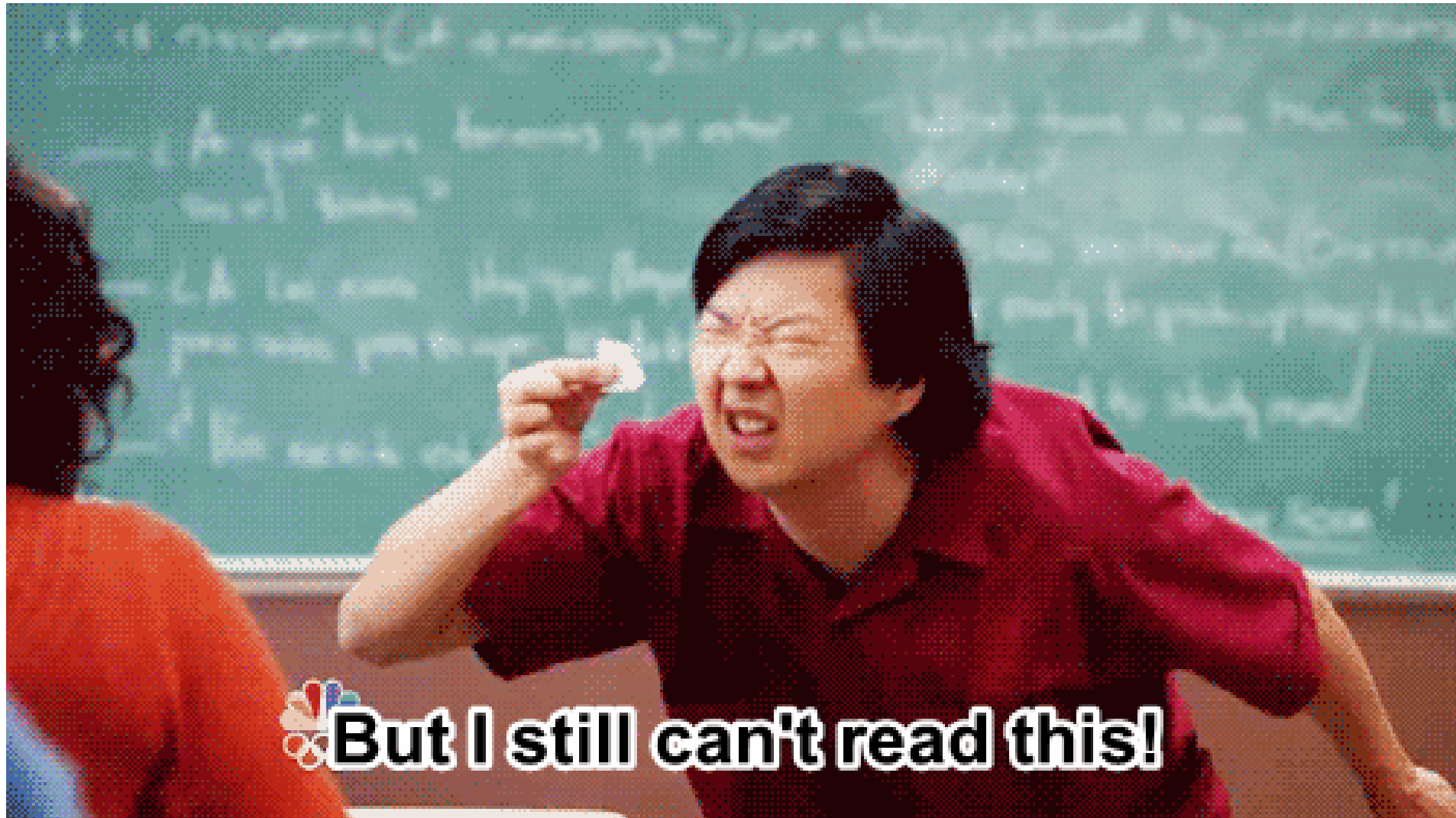
MDMRegistration.dll from 2020 contains functions of MMPC

The screenshot displays the Windows File Explorer interface for the file `mdmregistration.dll`. The left pane shows the file's location within a directory structure. The right pane shows the file's properties, including its type, size, and creation/modification dates. The 'Details' tab is active, and the 'Gemaakt' and 'Gewijzigd' fields are highlighted with a red box.

Property	Value
Bestandstype	Toepassingsuitbreiding (.dll)
Openen met	TraceView Plus
Locatie	C:\install\mdmdregistration 2020
Grootte	317 kB (325.120 bytes)
Grootte op schijf	320 kB (327.680 bytes)
Gemaakt	zaterdag 8 augustus 2020, 10:19:44
Gewijzigd	zaterdag 8 augustus 2020, 10:19:44



### 3. MMP-C Overview







# MMP-C Overview

The screenshot shows a Windows File Explorer window with the address bar set to "This PC > Local Disk (C:) > Program Files > Microsoft EPM Agent >". The main pane displays a list of folders and files. The left sidebar shows the navigation pane with "This PC" selected. The bottom status bar shows "1 item selected" and "1 KB of space used".

Name	Date modified	Type
EPMAAdapter	6/16/2023 6:55 PM	File folder
EPMClient	6/16/2023 6:55 PM	File folder
EpmConsentUI	6/16/2023 6:55 PM	File folder
EPMDriver	6/16/2023 6:55 PM	File folder
EPMService	6/16/2023 6:55 PM	File folder



# MMP-C Enrollment on the fly!





# Intune Vs MMP-C







# Intune has the IME

Deze pc > Lokale schijf (C:) > Program Files (x86) > Microsoft Intune Management Extension

Microsoft.Management.Services.IntuneWindowsAgent.AgentCommon.ServiceContracts.dll	8-5-2023 21:07
Microsoft.Management.Services.IntuneWindowsAgent.exe	8-5-2023 21:07
Microsoft.Management.Services.IntuneWindowsAgent.exe.config	16-9-2022 20:32

 Microsoft Edge Update Service (edgeupdate.m...)	Hiermee blijft de software van Microsoft u...	
 Microsoft Intune Management Extension	Microsoft Intune Management Extension	Wordt uitgevoerd
 Microsoft iSCSI Initiator Service	Hiermee worden iSCSI (Internet SCSI)-recci	



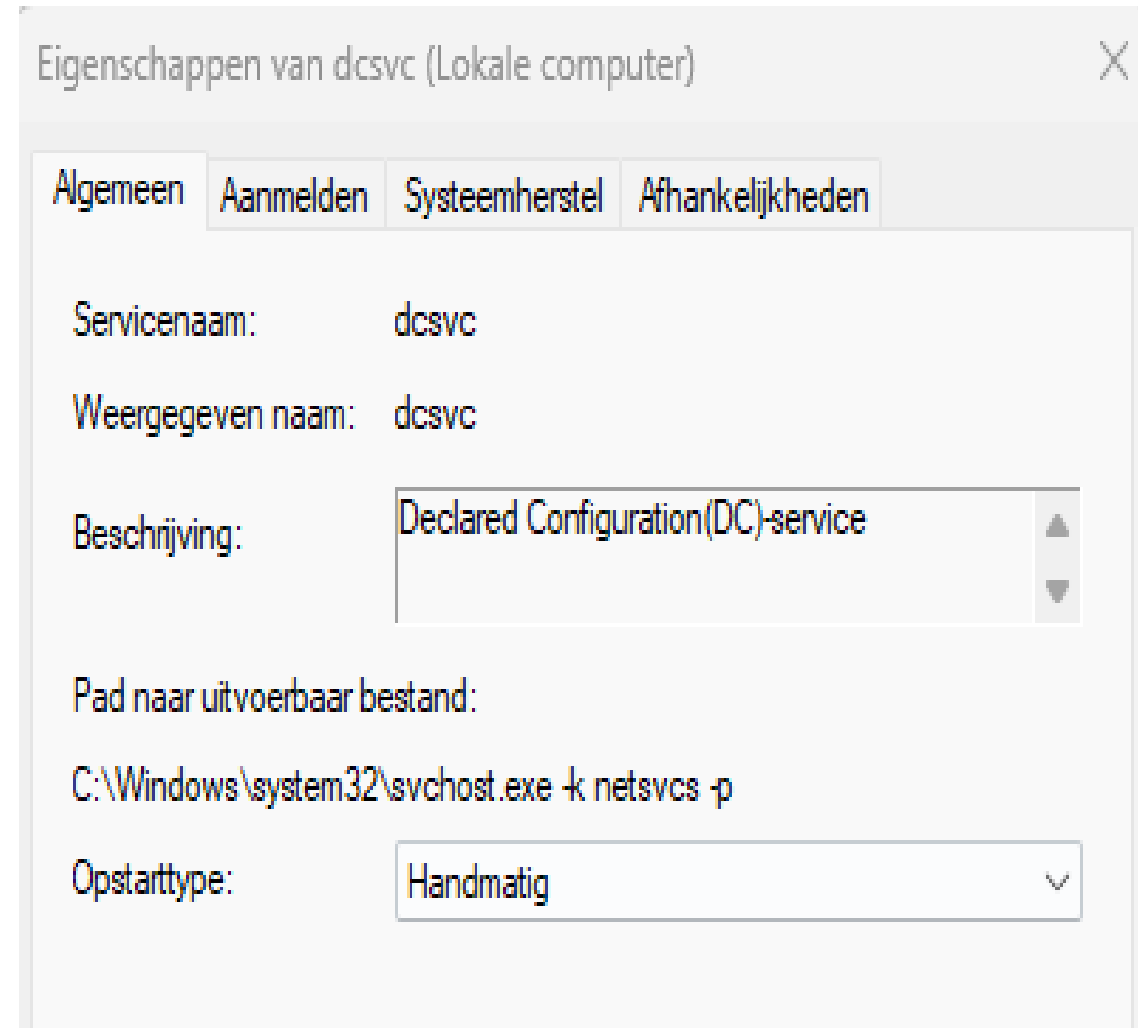
# MMP-C has the??







## 4. The “Unknown” Service





# KB5016691 “activated” DCSVC

August 25, 2022—KB5016691 (OS Build 22000.918) Preview

## File information

For a list of the files that are provided in this update, download the [file information for cumulative update 5016691](#).

dcsvc.dll	10.0.22000.918	"23-Aug-2022"	"16:24"	"937,472"
-----------	----------------	---------------	---------	-----------



# Declared Configuration Service (DCSVC)

```
1 <Get>
2   <CmdID>9</CmdID>
3   <Item>
4     <Target>
5       <LocURI>./Device/Vendor/MSFT/DeclaredConfiguration/Host/Inventory/Results/622feab7-cf26-5846-dc0e-d21dbb13972e/Document</LocURI>
6     </Target>
7   </Item>
8 </Get>
9 <Get>
10  <CmdID>10</CmdID>
11  <Item>
12    <Target>
13      <LocURI>./User/Vendor/MSFT/DeclaredConfiguration/Host/Inventory/Results/6c8d296c-327c-a39d-78d4-6c29ad639920/Document</LocURI>
14    </Target>
15  </Item>
16 </Get>
17 <Replace>
18   <CmdID>11</CmdID>
19   <Item>
```

File Edit Format View Help

```
<DeclaredConfiguration context="User" schema="1.0" id="3c6f254c-965d-3fd7-9111-ff5f945976e4" scenario="EPMPAYLOAD">
  <DSC namespace="root/MicrosoftDeviceManagement_EpmExtensibility" className="EPMElevationRulesAdapter">
    <Key name="MeID">8122a726-fd81-447a-873d-ccd4fd0b2cdf</Key>
    <Key name="DocumentID">3c6f254c-965d-3fd7-9111-ff5f945976e4</Key>
    <Key name="Version">322E734D1C271CCBE22B3693F50781DB33BEE61BF5EB676D266DCB68EFACB04D</Key>
    <Value name="ExtendedProperties">{"Signatures":["MIIRLgYJKoZIhvcNAQcCoIIRHzCCERsCAQExDzANBgIghkgBZQMEAgMFAlZRNfZsAAAGFnO6gngAABAMARzBFAiEAwwac5LrXszChvk2E5MkbZacBtTLt53H4N99XzsaLH0oCIDwR3dkHcYAeWqp3ngun0iAkb15p+twq7
```



# Faster and more Secure!

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

SyncML Sessions

92 - 4/29/2023 5:50:30 AM

SyncML Messages

1 - 4/29/2023 5:50:30 AM  
1 - 4/29/2023 5:50:30 AM  
2 - 4/29/2023 5:50:30 AM  
2 - 4/29/2023 5:50:30 AM

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Results>
  <Item>
    <Status>
      <CmdID>4</CmdID>
      <MsgRef>1</MsgRef>
      <CmdRef>10</CmdRef>
      <Cmd>Get</Cmd>
      <Data>200</Data>
    </Status>
    <Results>
      <CmdID>5</CmdID>
      <MsgRef>1</MsgRef>
      <CmdRef>10</CmdRef>
      <Item>
        <Source>
          <LocURI>./Device/Vendor/MSFT/DeclaredConf
        </Source>
        <Data>&lt;DeclaredConfigurationResult contex
          b20vb2NzcDAdBgNVHQ4EFgQUEpvLeuRVC2uT2n5nX2a1
          9AFcAQQAsACAAQwA9AFUAUwAiACwAIgBDAG8AbQ8tAG8
```

\*Way more faster sync  
\*Way more Secure

Company Portal

Search for apps

Home  
Apps  
App categories  
Downloads & updates  
Devices  
Help & support

Settings

Sync

Sync your device to get the latest organization.

Sync

Last sync on 4/29/2023 5:50:29 AM

App mode

Personalize your app with a color

Light  
Dark  
Windows default

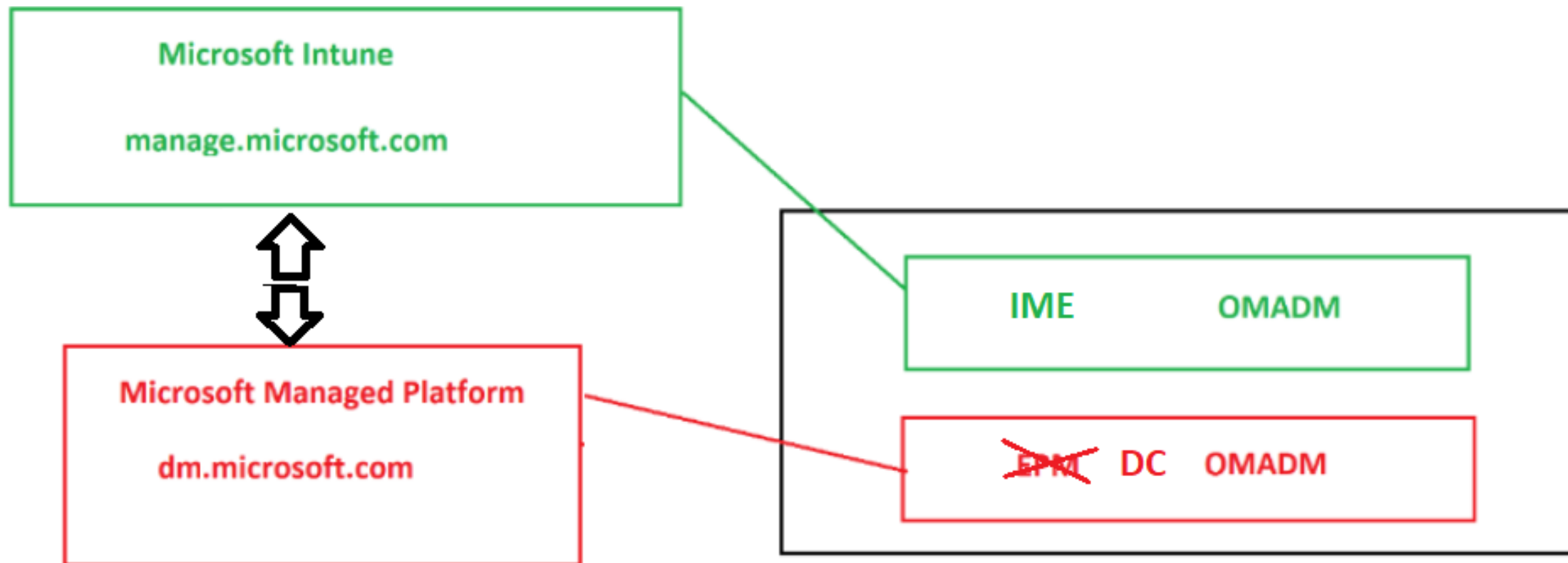
\*Untitled - Notepad

File Edit Format View Help

```
/ checksum="b557ad1e182e74556f30f4b1568d152ad5ffa348104d62cc6b7d0316e5cfc9a0" result
:10FD74F5DE54E2&lt;/Key&gt;&lt;Value name="ExtendedProperties"&gt;{"Signatures":["MI
&lt;Bs7FXLedtM0tojKHRny87N7DUUhZRnEftZsAAAGFnO6gngAABAMARzBFAiEAwac5LrXszChvk2E5Mkb7ac
ngV6BVh1NodHRwO18vd3d3Ln1pY3Jvc29mdC5jb20vcGtpb3BzL2Nybc9NaWwNybnVzZnQ1MjBBenVyzSUyMFF
TFAU...&lt;/Value>
```



# IME VS DCSVC







# But who controls the DC?





# DMOrchestrator

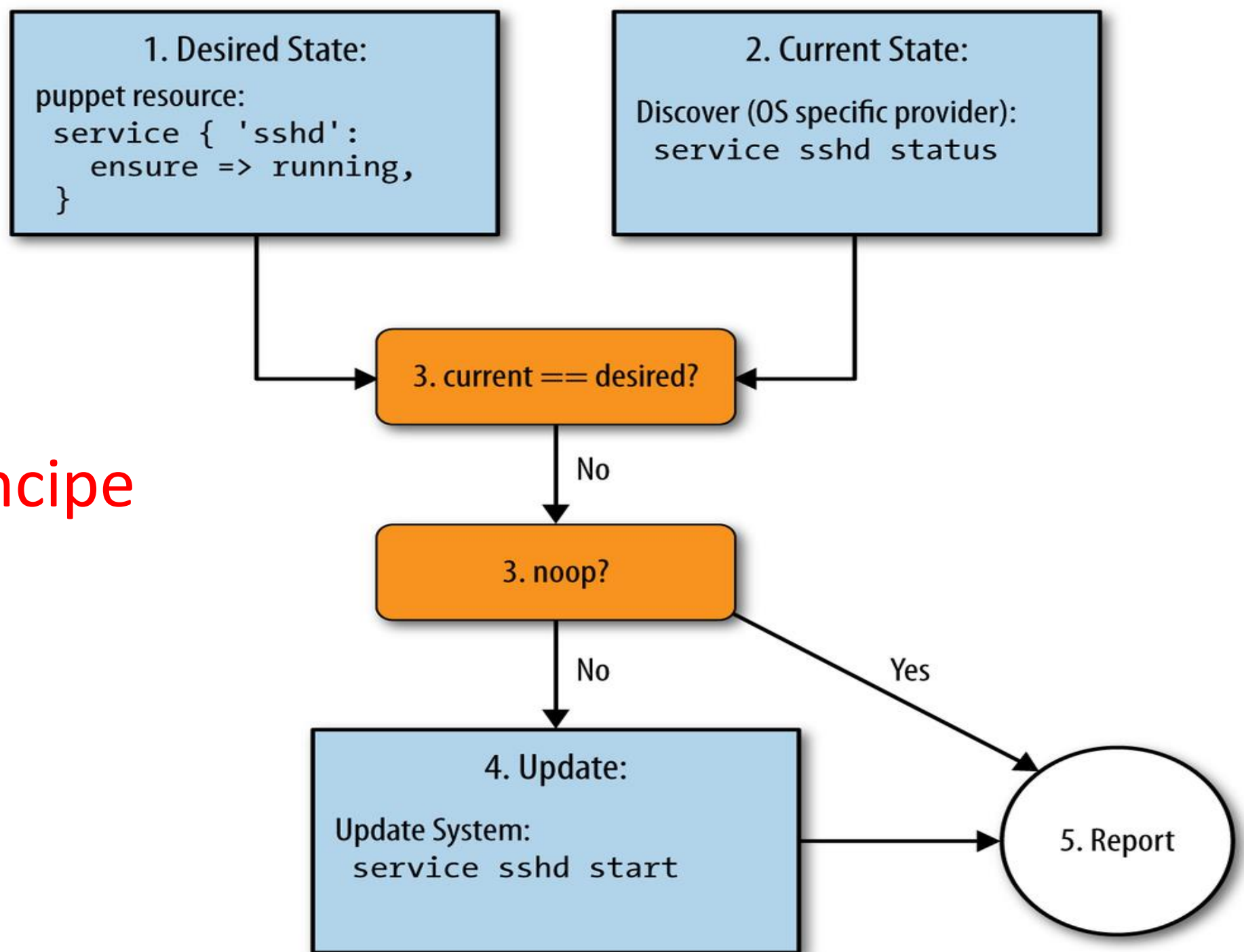
Y\_LOCAL\_MACHINE\SOFTWARE\Microsoft\DMOrchestrator\055C05BD-8C8F-46B7-88E2-76E31EEA3E99

	Name	Type	Data
DirectX	(Default)	REG_SZ	(value not set)
DMOrchestrator	DocId	REG_SZ	98a58f01-7d0a-d256-3963-54790c95f6f9 --> PolicyId
055C05BD-8C8F-46B7-88E2-76E31EEA3E99	DocVersion	REG_SZ	57b743587119cbb4949df139ec216f01f5c9c5df3e7d...
10706B08-5FAC-4D5A-8AA2-3AD40A4ADB2D	EnrollmentId	REG_SZ	33625E68-3BC3-4851-B92D-20F80C52D6C1 --> MMP-C EnrollmentId
64974B52-C55A-49B8-99EC-0A0EDF8495D8	LifecycleNotific...	REG_DWORD	0x00000001 (1)
78A61BD6-4552-43F5-8AE5-7512186DAED3	LifecycleNotific...	REG_DWORD	0x00000000 (0)
C49F1D25-BC09-42BC-8709-DF9BD21D1A54	LifecycleNotific...	REG_DWORD	0x00000001 (1)
EB3BB9A6-8BA8-4915-BECB-3205B1766A03			

```
; int64 fastcall OrchestratorDBManager::GetDMOrchestratorRootKey(HKEY *)
?GetDMOrchestratorRootKey@OrchestratorDBManager@@SAJPEAPEAUHKEY_@@@Z proc near
push    rbx
sub     rsp, 20h
mov     rbx, rcx
call    cs:__imp_RtlIsStateSeparationEnabled
nop     dword ptr [rbx+0x100h]
test    al, al
lea     rdx, a0sdataSoftware_15 ; "OSData\\Software\\Microsoft\\DMOrchestr..."
lea     rcx, aSoftwareMicros_22 ; "Software\\Microsoft\\DMOrchestrator"
cmovnz  rcx, rdx ; lpSubKey
xor     r8d, r8d ; int
mov     rdx, rbx ; HKEY *
add     rsp, 20h
pop     rbx
jmp     ?GetHKey@OrchestratorDBManager@@SAJPEBGPEAPEAUHKEY_@@H@Z ; OrchestratorDBManager::GetHKey(ushc
?GetDMOrchestratorRootKey@OrchestratorDBManager@@SAJPEAPEAUHKEY_@@@Z endp
```



# Puppet Principle





Current State

Name	Type	Data
(Default)	REG_SZ	(value not set)
behavior	REG_DWORD	0x00000000 (0)
context	REG_SZ	Device
CspCount	REG_DWORD	0x00000003 (3)
downloadDestin...	REG_SZ	C:\ProgramData\Microsoft\DC\HostOS\33625E68-
downloadGUID	REG_SZ	70F5E47E-98FD-4F68-8D7A-8408B99489F3
downloadRequest	REG_DWORD	0x00000000 (0)
downloadUrl	REG_SZ	https://checkin.dm.microsoft.com/WinDCFE/doc...
LastRunTimeSta...	REG_SZ	2023-06-24T20:49:00Z
LatestRunTickC...	REG_QWORD	0x07892e8b (126430859)

DMOrchestrator --> The One that does all the lifting and manage/coordinates the processing of the raw documents to create a desired state (cooked)

DMOrchestrator

- 27C36663-DADF-4221-8C27-FA954DB9452C
- 2B7B59D5-A25C-4FDF-B842-D5A1BAFBD8D
- 46D81B38-BBC7-4C5C-82A5-722622C1AAC1
- 9B1CFC7F-E731-424A-BCCF-CCC6CFACD036

Key gets created the moment EPM got installed

MDM Declared Configuration: Exit function: (CreateCookedDocumentActivity::Execute) with Result: (The operation completed successfully.)

```
<DeclaredConfiguration context="User" schema="1.0" id="3c6f254c-965d-3fd7-9111-ff5f945976e4"
  <DSC namespace="root/MicrosoftDeviceManagement_EpmExtensibility" className="EPMElevationR
    <Key name="MeID">8122a726-fd81-447a-873d-ccd4fd0b2cdf</Key>
    <Key name="DocumentID">3c6f254c-965d-3fd7-9111-ff5f945976e4</Key>
```

EPMPAYLOAD

Desired State

Name	Type	Data
(Default)	REG_SZ	(value not set)
behavior	REG_DWORD	0x00000000 (0)
context	REG_SZ	User
CspCount	REG_DWORD	0x00000001 (1)
downloadRequest	REG_DWORD	0x00000000 (0)
model	REG_DWORD	0x00000001 (1)
operation	REG_DWORD	0x00000001 (1)



# Summary

1. EPM will trigger an enrollment into MMP-C
2. This enrollment is also called a Dual or Linked Enrollment
3. Intune uses the Sidecar Agent/IME → MMP-C uses DCSVC
4. The DMOrchestrator is the main operator!
5. MMP-C Sync is way faster and way more secure
6. MMP-C is Intune v2! (In my humble opinion)
7. MMP-C is NOT something new!!

The image features a classic Looney Tunes-style graphic. It consists of a series of concentric circles. The outermost ring is a dark red color. Inside this is a lighter red ring, followed by a dark blue ring, and then a lighter blue ring. The text "That's all Folks!" is written in a white, elegant script font, slanted slightly to the right. The text is positioned across the middle of the concentric circles, with the words "That's all" on the left and "Folks!" on the right. The background of the entire image is white.

*That's all Folks!*





DANKE!  
THANK YOU!  
MERCI!  
GRAZIE!  
GRACIAS!  
DANK JE WEL!

.....