
# How to debug Intune Settings/Features When they break

*Which they will?... ?*

# Sponsors


onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Microsoft MVP 4 years
Secure at Work
Hobbys Sneaker, Sport

# Rudy Ooms

Microsoft MVP 5 years
Patch My PC
Multiple Nicknames
-TroubleMaker
-Mister MDM
-The guy that reverse Code for fun

Hobbys? → The Above

# Session Overview


- It will be a fun Session!!
- Securing Intune with and without breaking your devices!
- If somehow it still breaks (which it will), we will show you how to troubleshoot it
- After this session, you know why PROD / TEST should not be the same and why Yeeting features to prod is not smart... well it depends...

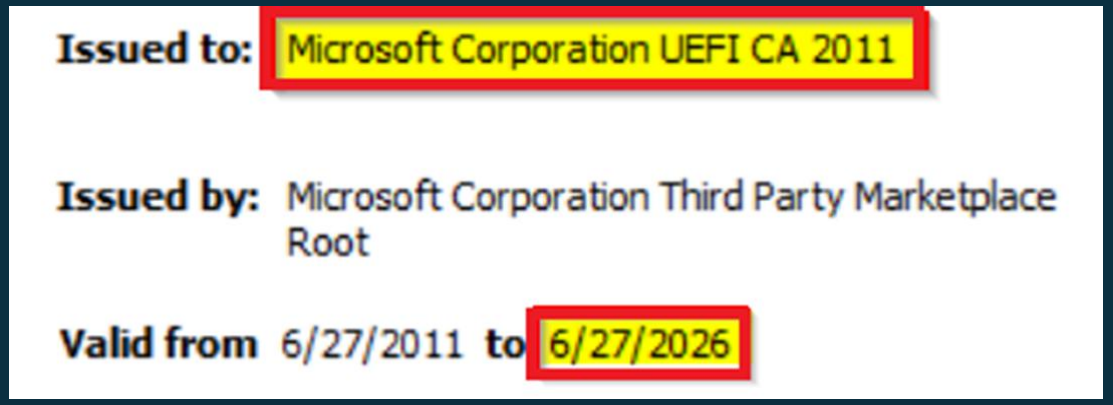
# Security vs  Productivity



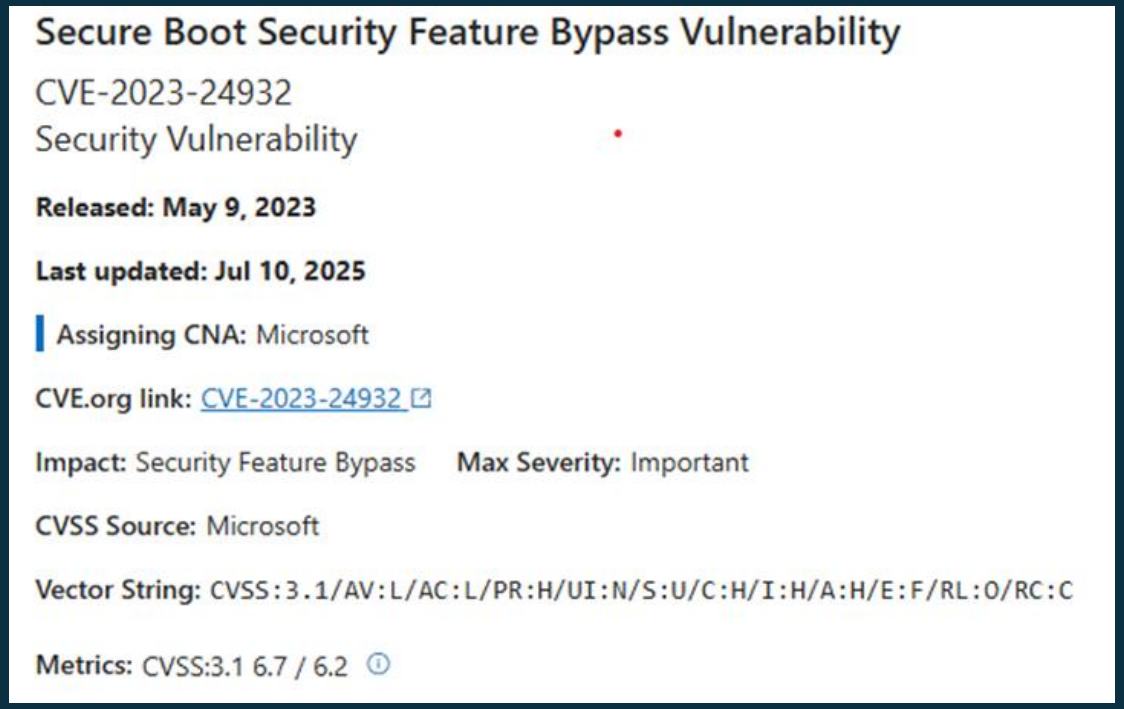
**Implementing (Security) Features  VS  Users not able to do their work**


# Secure Boot Policy

# Secure Boot Policy



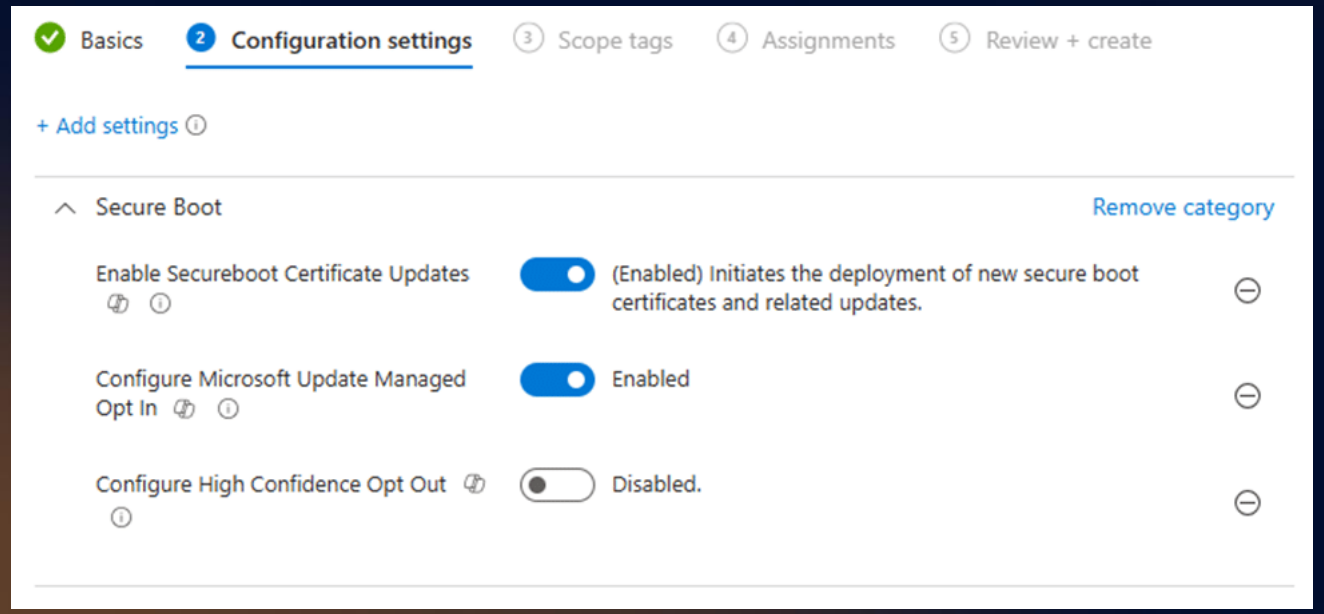

The 2011 Windows Production CA, 2011 UEFI CA and 2011 Microsoft KEK are expiring in 2026.



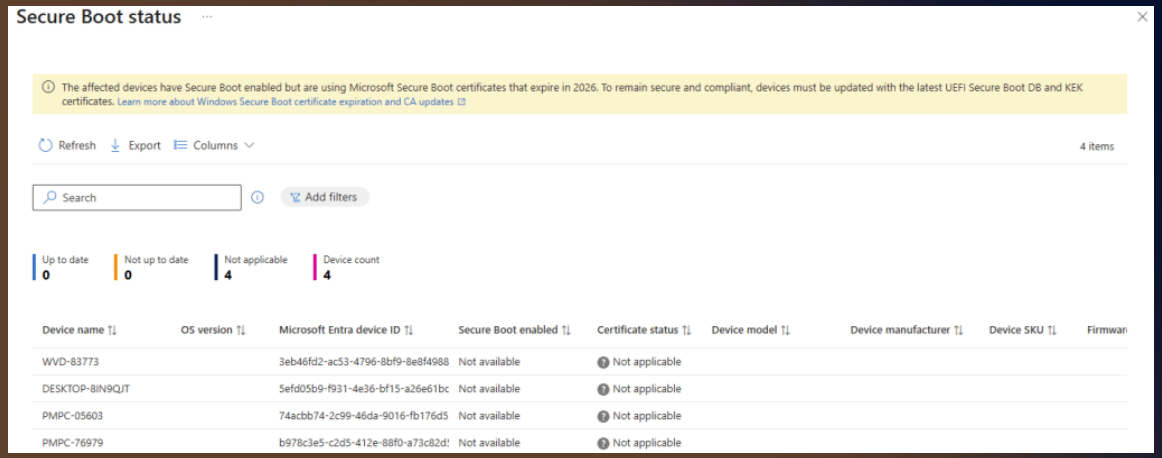

To stay protected against BlackLotus/ Exploits CVE-2023-24932 – we need to keep Secure Boot Patched

# Secure Boot Policy

The Idea was easy..



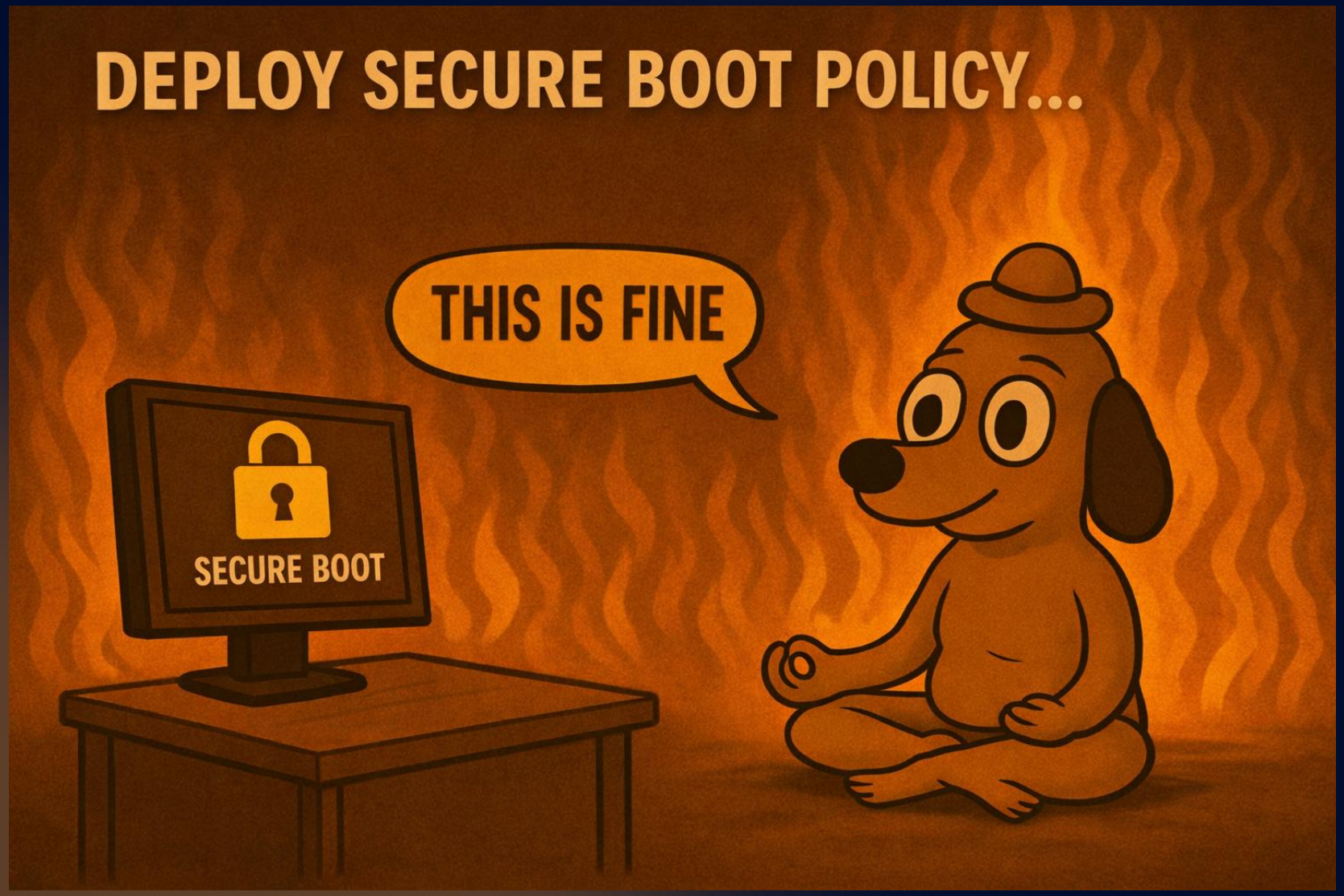

*Deploy this simple policy to ensure the certificate would be getting updated




The Reporting… ? That is a different challenge…

*Before the policy can be applied, we need to Ensure the firmware/bios is also up to date

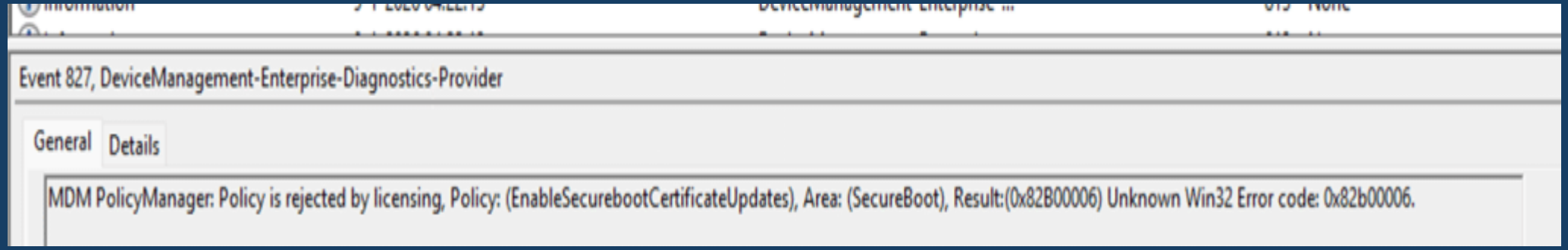
# Secure Boot Policy



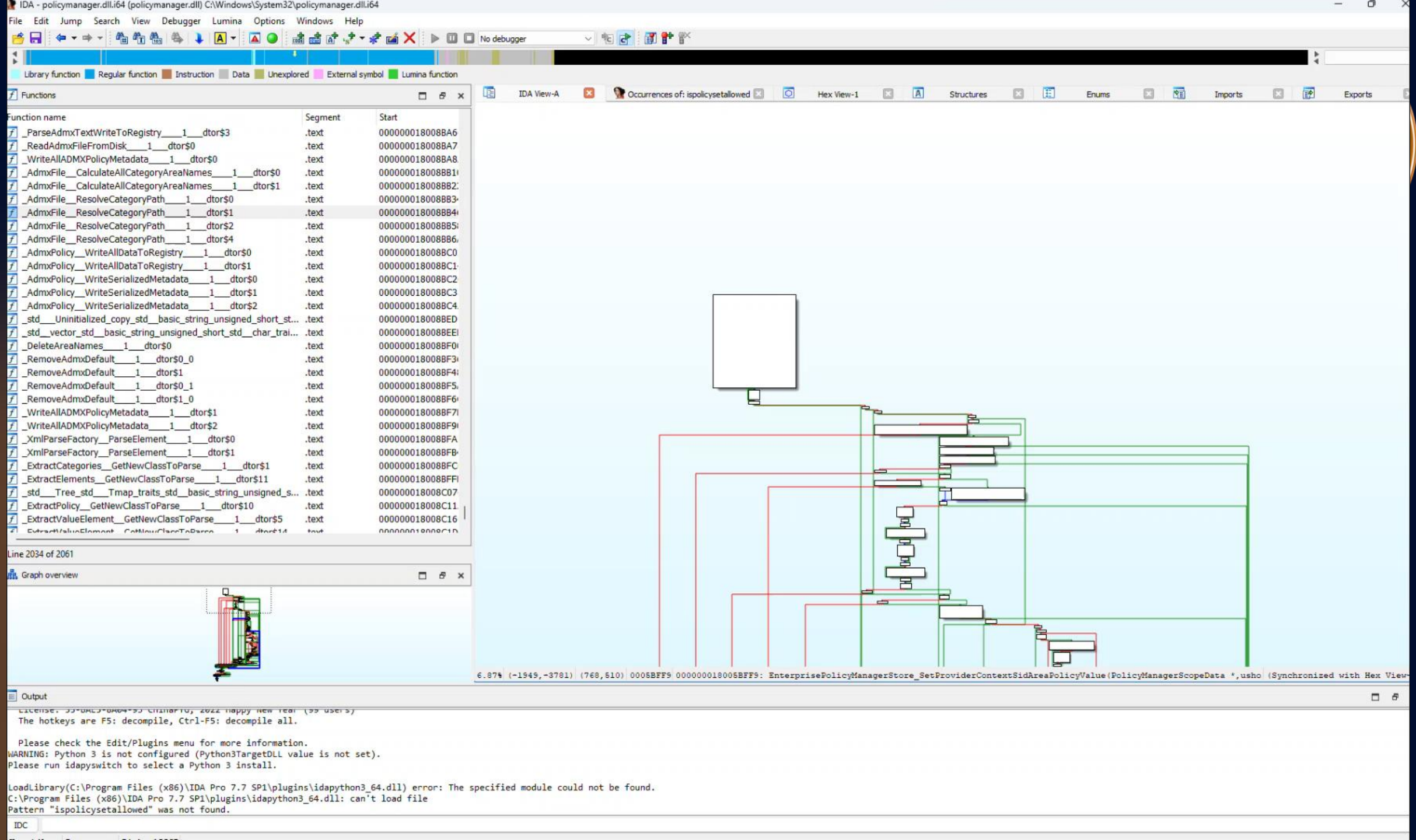
# Secure Boot Policy

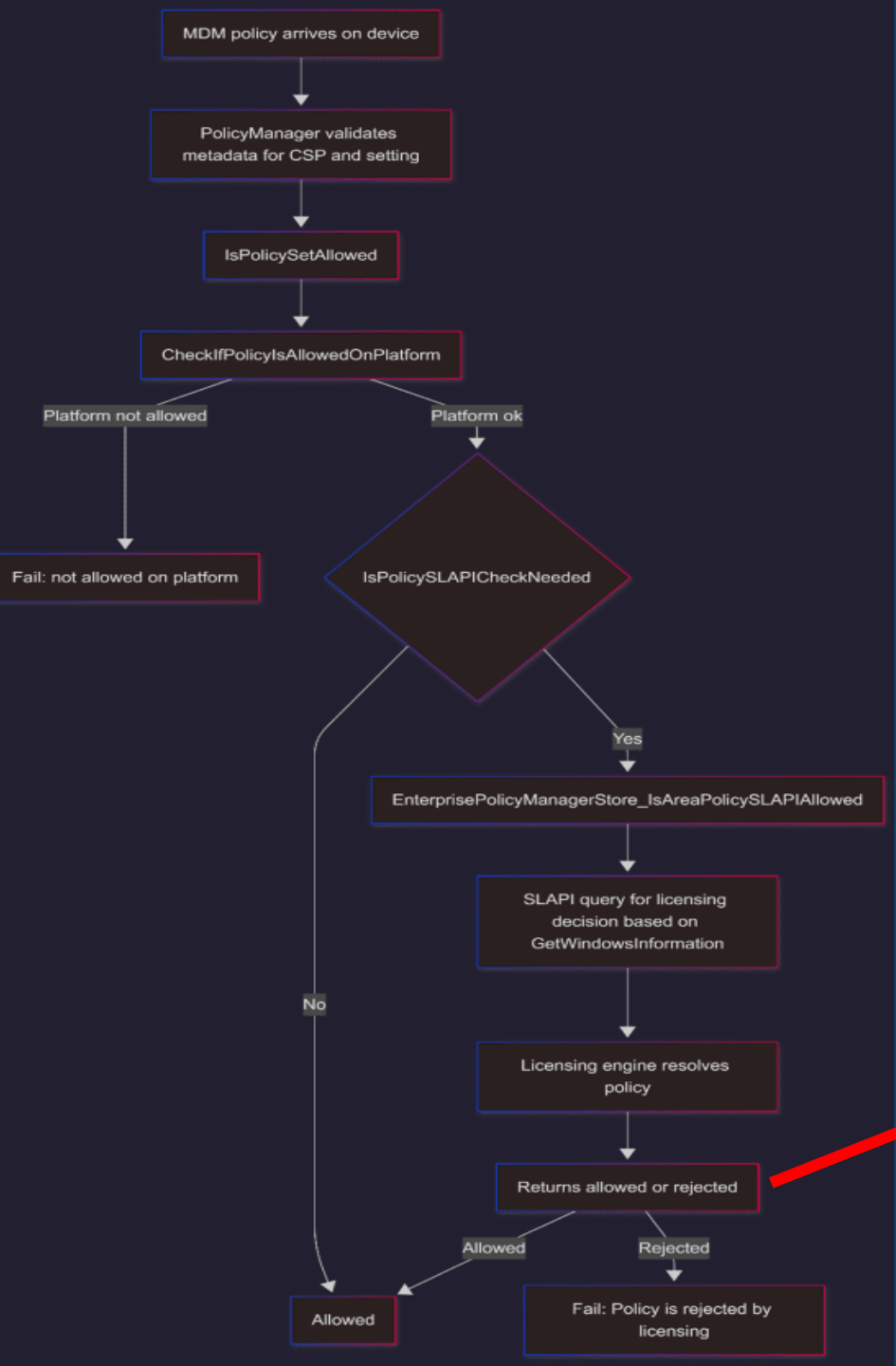
| Name | Status | Error code |
|---|---|---|
| Configure High Confidence Opt Out | Error | 65000 |
| Configure Microsoft Update Managed Opt In | Error | 65000 |
| Enable Secureboot Certificate Updates | Error | 65000 |

Until it errors out on all devices with the error code 65000....
which means we really don't know what happened




To find out what happened... I opened the Policymanager.dll


IDA - policymanager.dll.i64 (policymanager.dll) C:\Windows\System32\policymanager.dll.i64
File Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name Segment Start
_ParseAdmxTextWriteToRegistry____1___dtor$3 .text 000000018008BA6
_ReadAdmxFileFromDisk____1___dtor$0 .text 000000018008BA7
_WriteAllADMXPolicyMetadata____1___dtor$0 .text 000000018008BA8
_AdmxFile__CalculateAllCategoryAreaNames____1___dtor$0 .text 000000018008BB1
_AdmxFile__CalculateAllCategoryAreaNames____1___dtor$1 .text 000000018008BB2
_AdmxFile__ResolveCategoryPath____1___dtor$0 .text 000000018008BB3
_AdmxFile__ResolveCategoryPath____1___dtor$1 .text 000000018008BB4
_AdmxFile__ResolveCategoryPath____1___dtor$2 .text 000000018008BB5
_AdmxFile__ResolveCategoryPath____1___dtor$4 .text 000000018008BB6
_AdmxPolicy__WriteAllDataToRegistry____1___dtor$0 .text 000000018008BC0
_AdmxPolicy__WriteAllDataToRegistry____1___dtor$1 .text 000000018008BC1
_AdmxPolicy__WriteSerializedMetadata____1___dtor$0 .text 000000018008BC2
_AdmxPolicy__WriteSerializedMetadata____1___dtor$1 .text 000000018008BC3
_AdmxPolicy__WriteSerializedMetadata____1___dtor$2 .text 000000018008BC4
_std___Uninitialized_copy_std__basic_string_unsigned_short_st... .text 000000018008BED
_std__vector_std__basic_string_unsigned_short_std__char_trai... .text 000000018008BEE
_DeleteAreaNames____1___dtor$0 .text 000000018008BF0
_RemoveAdmxDefault____1___dtor$0_0 .text 000000018008BF3
_RemoveAdmxDefault____1___dtor$1 .text 000000018008BF4
_RemoveAdmxDefault____1___dtor$0_1 .text 000000018008BF5
_RemoveAdmxDefault____1___dtor$1_0 .text 000000018008BF6
_WriteAllADMXPolicyMetadata____1___dtor$1 .text 000000018008BF7
_WriteAllADMXPolicyMetadata____1___dtor$2 .text 000000018008BF9
_XmlParseFactory__ParseElement____1___dtor$0 .text 000000018008BFA
_XmlParseFactory__ParseElement____1___dtor$1 .text 000000018008BFB
_ExtractCategories__GetNewClassToParse____1___dtor$1 .text 000000018008BFC
_ExtractElements__GetNewClassToParse____1___dtor$11 .text 000000018008BFF
_std___Tree_std___Tmap_traits_std__basic_string_unsigned_s... .text 000000018008C07
_ExtractPolicy__GetNewClassToParse____1___dtor$10 .text 000000018008C11
_ExtractValueElement__GetNewClassToParse____1___dtor$5 .text 000000018008C16
Line 2034 of 2061
Graph overview
IDA View-A
Occurrences of: ispolicysetallowed
Hex View-1
Structures
Enums
Imports
Exports
6.87% (-1949,-3781) (768,510) 0005BFF9 000000018005BFF9: EnterprisePolicyManagerStore_SetProviderContextSidAreaPolicyValue(PolicyManagerScopeData *,usho (Synchronized with Hex View
Output
The hotkeys are F5: decompile, Ctrl-F5: decompile all.
Please check the Edit/Plugins menu for more information.
WARNING: Python 3 is not configured (Python3TargetDLL value is not set).
Please run idapyswitch to select a Python 3 install.
LoadLibrary(C:\Program Files (x86)\IDA Pro 7.7 SP1\plugins\idapython3_64.dll) error: The specified module could not be found.
C:\Program Files (x86)\IDA Pro 7.7 SP1\plugins\idapython3_64.dll: can't load file
Pattern "ispolicysetallowed" was not found.
IDC




The PolicyManager code told me where to look

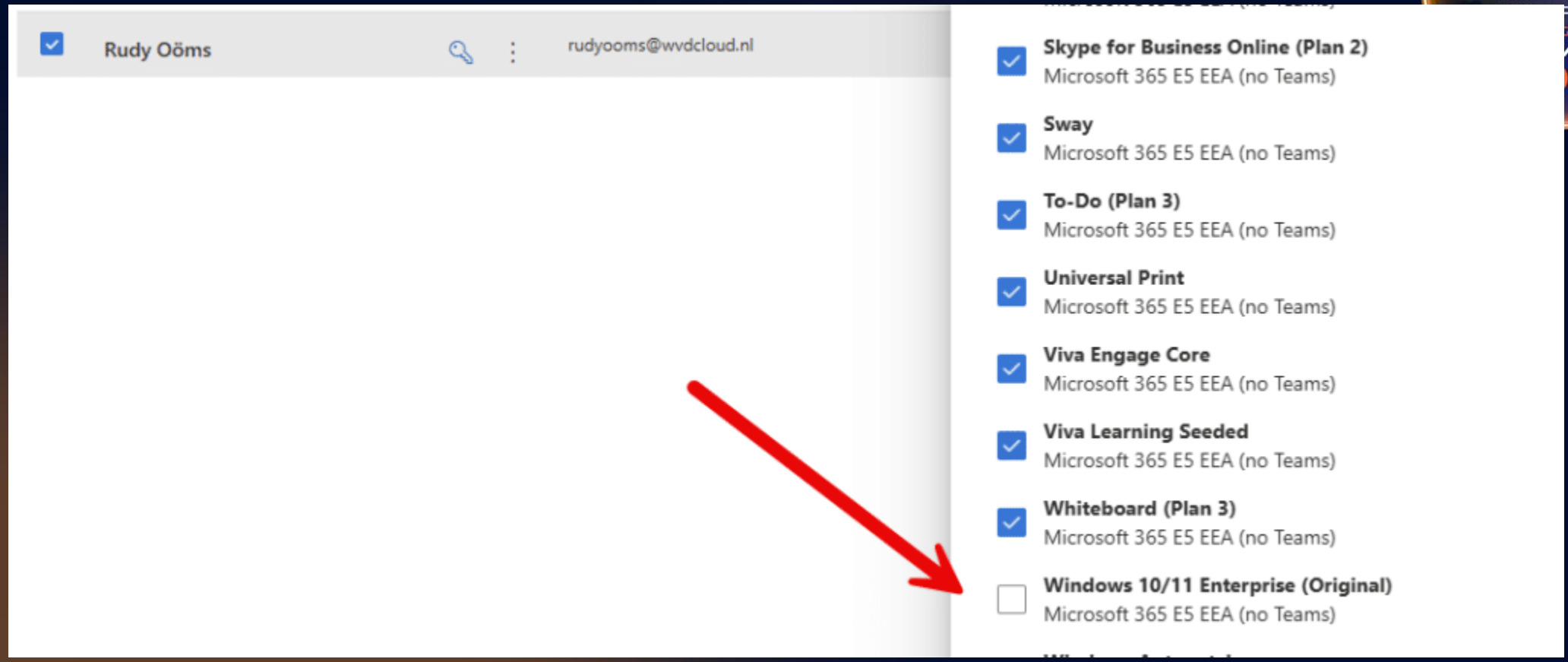
```
C:\Users\RudyOoms>licensingdiag -cab c:\temp\123.cab
    <policy name="dmenrollengine-Mobile-Business" type="DWORD">0</policy>
    <policy name="enterprisemgmt_policymanager-License-MDMPolicyAllowList"
    type="string">AboveLock|Accounts|ActiveXControls|ADMXIngest|AllowMessageSync|AppDeviceInventory|AppHVSI|Application
    <policy name="enterprisemgmt_policymanager-License-ADMXIngestionAllowList" type="DWORD">0</policy>
```

In the licensingdiag, Secure Boot was **NOT** in the MDM Policy AllowList.

This caused the policy to be getting rejected

```
emgmt_1:                                ; DATA XREF: IsPolicySLAPICheckNeeded(void)+C4F↑o
                                        ; IsPolicySLAPICheckNeeded(void)+13A5↑o ...
        text "UTF-16LE", 'enterprisemgmt_policymanager-License-CheckMDMPolicy'
        text "UTF-16LE", 'AllowList',0
        align 4
```

# Secure Boot Policy




**Subscription activation was “one” the culprits!!!**

# Secure Boot Policy

## Licenses

The following policies apply to acquisition and renewal of licenses on devices:

- Upgraded devices attempt to renew licenses about every 30 days. They must be connected to the internet to successfully acquire or renew a license.

Microsoft fixed it “service side” but we needed to renew the subscription activation license…. (happens each 30 days)

- ClipDLS.exe removesubscription
- ClipRenew.exe

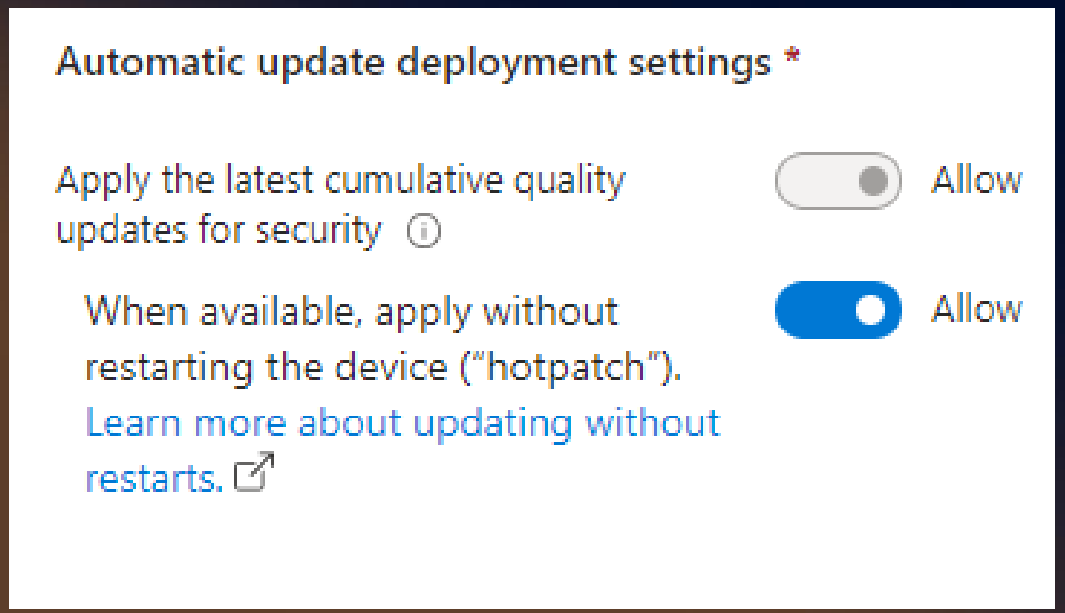
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | 200 | HTTPS | licensing.mp.micros… | /v7.0/licenses/content | 8.491 | application/… | svchos… |
| 41 | 200 | HTTPS | licensing.mp.micros… | /v7.0/licenses/leases/renew | 4.911 | application/… | svchos… |

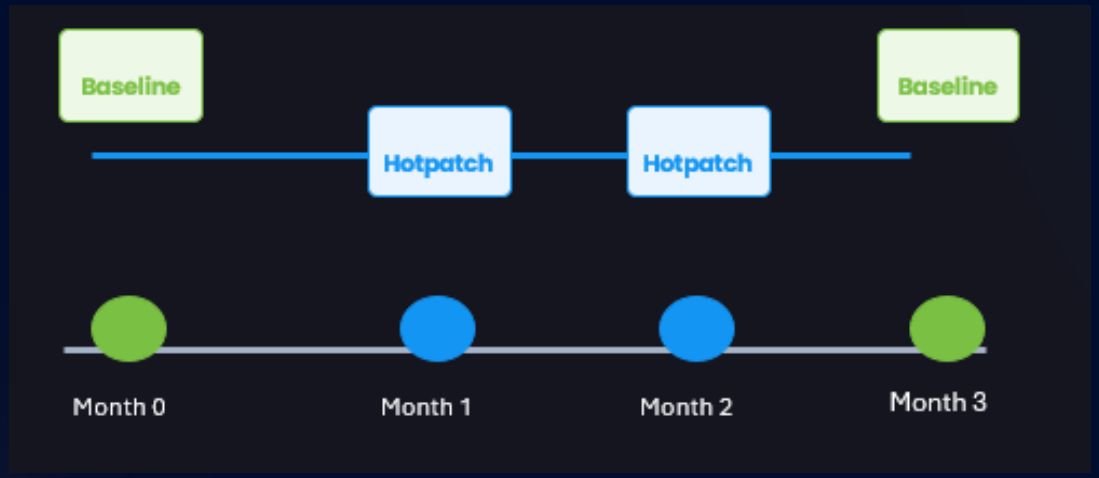
| Name | Status |
|---|---|
| Configure High Confidence Opt Out | Succeeded |
| Configure Microsoft Update Managed Opt In | Succeeded |
| Enable Secureboot Certificate Updates | Succeeded |


# Hotpatch

# Hotpatch

We could enable Hotpatch to ensure our devices won't reboot every month

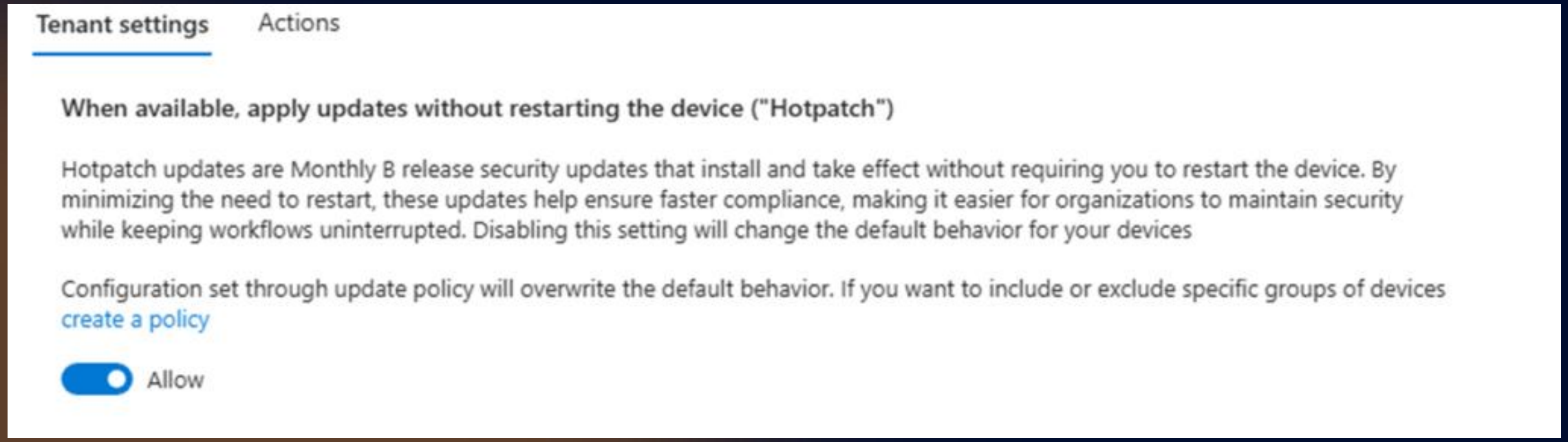



It will only reboot during the "Baseline" Months
Which is excellent for your security posture!

# Hotpatch

Or we just wait untill Hotpach becomes the default.... (12 May)

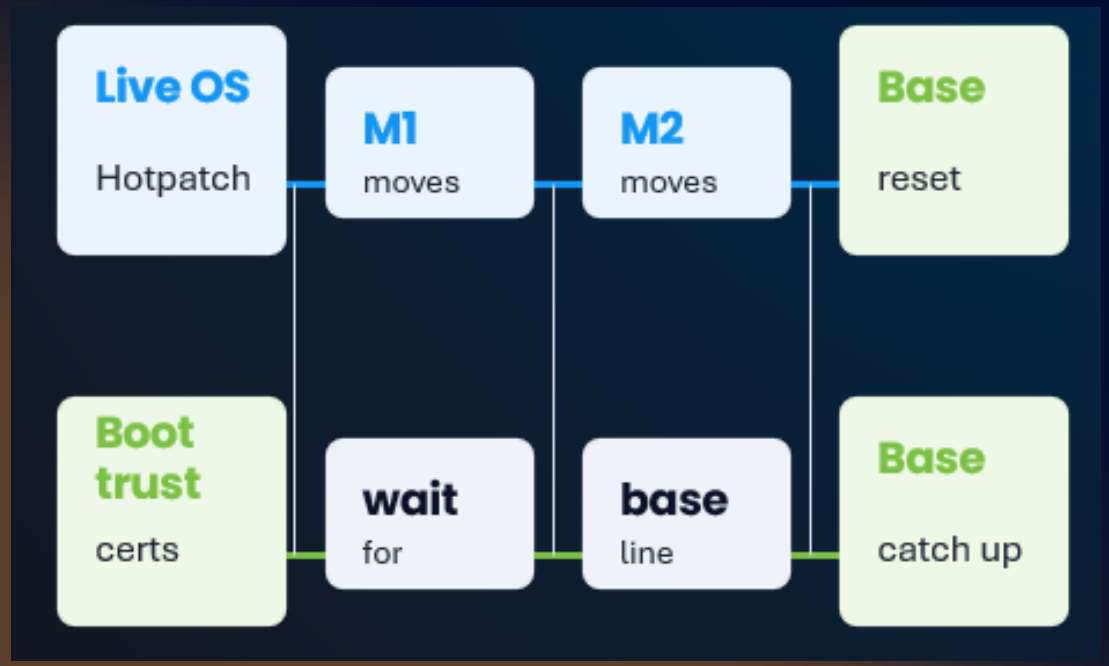



We can opt out if we want...

# Hotpatch

# Hotpatch

| Name | Status | Error code |
|---|---|---|
| Configure High Confidence Opt Out | Error | 65000 |
| Configure Microsoft Update Managed Opt In | Error | 65000 |
| Enable Secureboot Certificate Updates | Error | 65000 |




Hotpatch + Secure Boot Cert

The Secure Boot Certificate Update will Only be applied in the baseline update… Which Is April. Hotpatch updates ONLY contain security updates!

This Hotpatch update includes security and quality improvements.

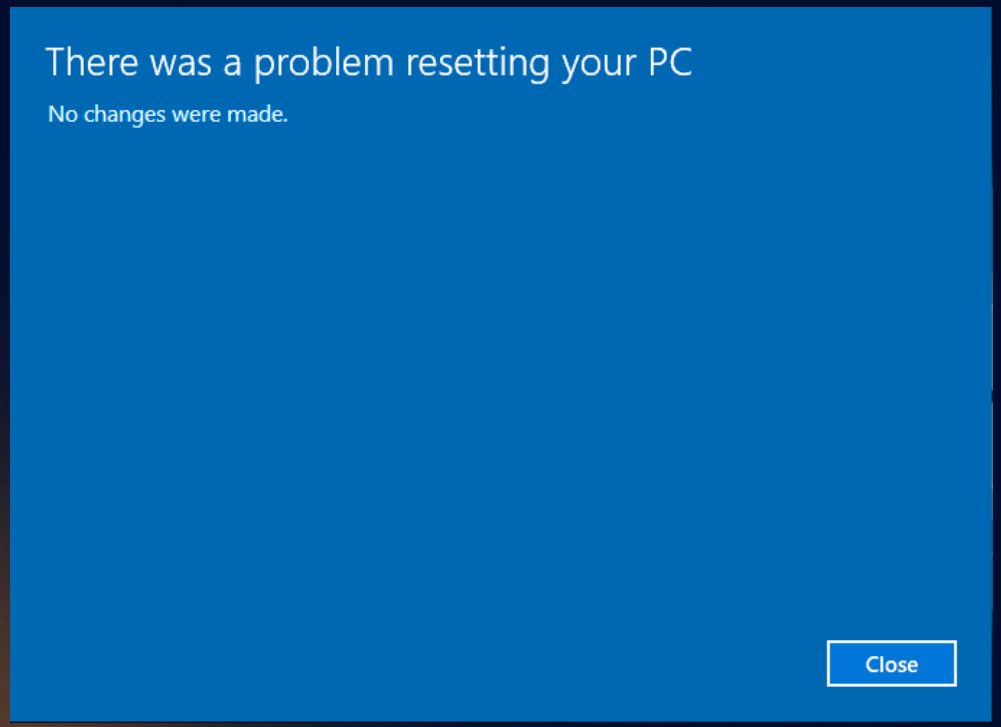
**Note:** Secure Boot certificate updates will be delivered with the next baseline Windows update in April 2026.

# Hotpatch

Hotpatch updates only contains security updates!

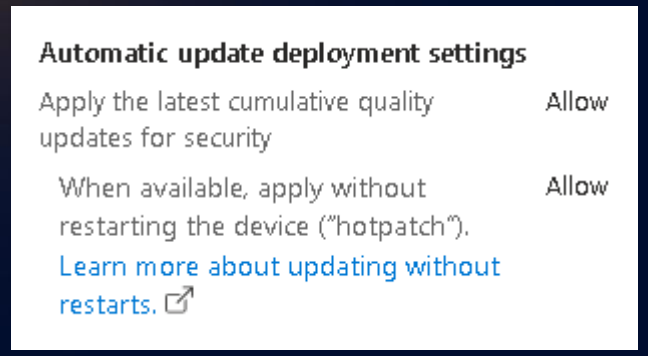

If hotpatch is enabled... it also interferes with the WinRE. With it resetting your pc will fail

**Please Note:**
Fixed With April Release
For now

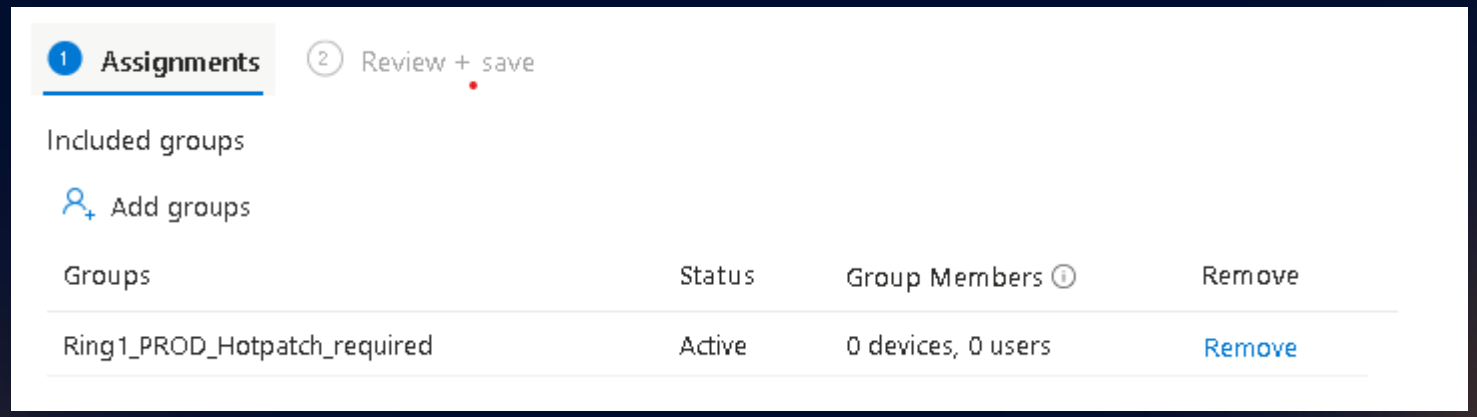



```
I    00000005 Perf: LRU Cache Initialize @0x182b816d360; Maximum Size: 628 MiB; Initial Elements: 6430
S    Initialized store, arch=amd64, style=Desktop, compact=true, windir=C:\Windows\, sandbox=
S        Session: 1852_27015 initialized by client Push Button Reset - Enumerate
S        Appl:Hotpatch package Package_for_HotpatchFix_7985~31bf3856ad364e35~amd64~~26100.7985.1.1 found and opRevisionCompare set to 1
S        Package Format: PSFX
S        Delta Format: ForwardOnly
S        Package Format: PSFX
S        Delta Format: ForwardOnly
S        Package Format: PSFX
```

# Advise



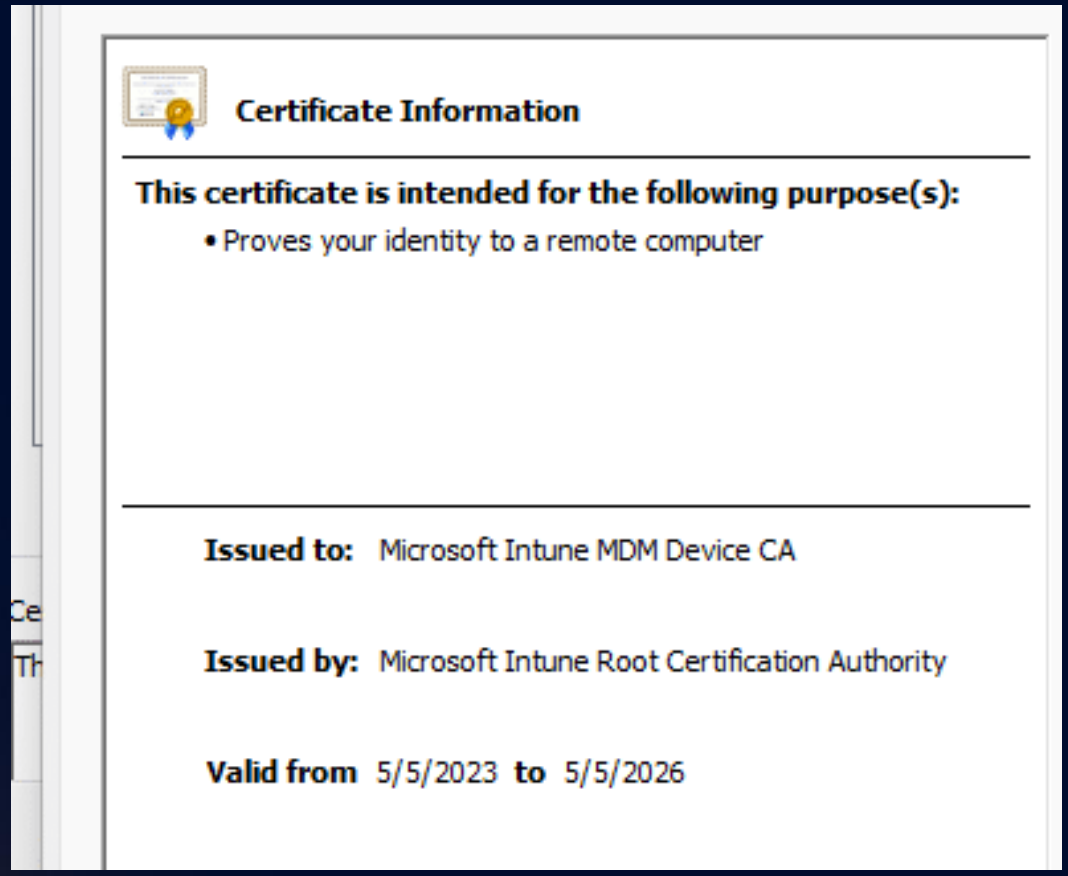

Deploy it only to the devices that really really need it. AKA device that are not allowed to reboot often




# Intune Certificate

# Intune MDM Device CA

The Intune MDM certificate is also going to expire.



# Intune MDM Device CA

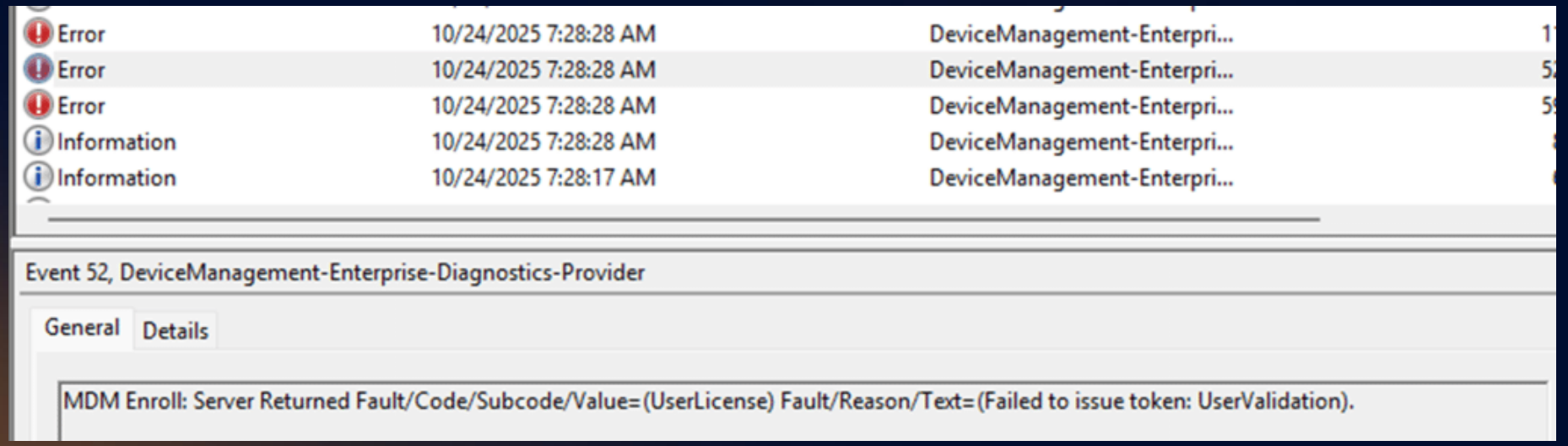
Which wouldn't cause any issue...


in 99% of all cases, Microsoft would send out the RenewNow CSP ... which would renew the root and Intune certificate on the fly (old scheduled task is obsolete)

| Device |
| --- |
| ./Device/Vendor/MSFT/CertificateStore/MY/WSTEP/Renew/RenewNow |

# Intune MDM Device CA

# Intune MDM Device CA

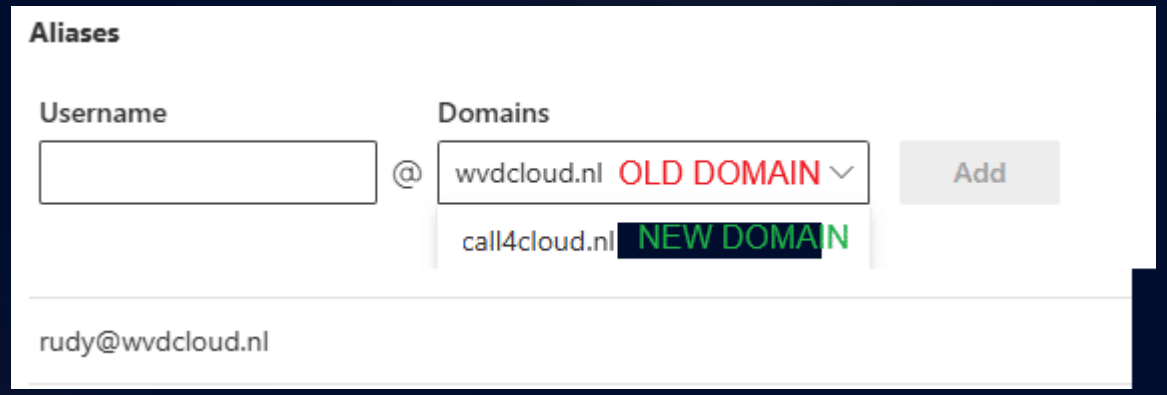



Somehow renewal failed on on a subset of devices.. Because of a license??

| | | | |
|---|---|---|---|
| UserLicense | MENROLL_E_USERLICENSE | License of user is in bad state and blocking the enrollment. The user needs to call the admin. | 80180018 |

Which is weird because all users have an Intune license???

# Intune MDM Device CA




The company had a merger... and changed the domain name

And eventually removed the domainname from the accepted domain names

```
[HKEY_LOCAL_MACHINE\software\microsoft\enrollments\DF14030C-7BC7-460F-A17E-E0B7C6D6B1D9]
    "EnrollmentState"=DWORD:00000001
    "EnrollmentType"=DWORD:00000006
    "UPN"="testuser@olddomain.com
    "DiscoveryServiceFullURL"="enrollment.manage.microsoft.com"
    "PartnerOpaqueID"=""
    "AADResourceID"="https://manage.microsoft.com/"
    "AADOpaqueID"=""
    "AADTenantID"="97759401-0ff9-42fb-8eae-9163e29d19bf"
    "CorrelationID"="{05E01937-5196-0006-9F23-E0059651D901}"
```

That old domain name is configured as the UPN in the enrollment registry when the device is enrolled

# Intune MDM Device CA

```
EEDBManager::GetEnrollmentString(&v28, L"AADTenantID", &v36);
if ( *((char *)a2 + 72) < 0 )
{
  ActivityContext::set_EnrollmentServiceFullURL(a2, v33);
  IsLockedToMmpc = 1;
  goto LABEL_62;
}
v28 = *(struct _GUID *)((char *)a2 + 8);
EnrollmentString = EEDBManager::GetEnrollmentAuthPolicy(&v28, (enum MDMAuthPolicy *)&v26);
if ( EnrollmentString >= 0 )
{
  if ( (unsigned int)(v26 - 1) > 1
    && (v28 = *(struct _GUID *)((char *)a2 + 8), EEDBManager::GetEnrollmentString(&v28, L"DomainUsername", &v32) >= 0)
    || (v28 = *(struct _GUID *)((char *)a2 + 8),
        EnrollmentString = EEDBManager::GetEnrollmentString(&v28, L"UPN", &v32),
        EnrollmentString >= 0) )
  {
    v25 = 0i64;
    v28 = *(struct _GUID *)((char *)a2 + 8);
    EEDBManager::GetEnrollmentString(&v28, L"SID", &v25);
```

That same UPN will be sent over to the enrollment service when renewing the certificate

```
POST https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc HTTP/1.1
Connection: Keep-Alive
Content-Type: application/soap+xml; charset=utf-8
User-Agent: ENROLLClient
Content-Length: 1039
Host: enrollment.manage.microsoft.com

<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:s="http://www.w3.org/2003/05/soap-envelope"><s:Header><a:Action s:mustUnderstand="1">
http://schemas.microsoft.com/windows/management/2012/01/enrollment/IDiscoveryService/Discover</a:Action><a:MessageID>urn:uuid:748132ec-a575-4329-b01b-6171a9cf8478</a:MessageID><a:ReplyTo><a:Address>
http://www.w3.org/2005/08/addressing/anonymous</a:Address></a:ReplyTo><a:To s:mustUnderstand="1">https://enrollment.manage.microsoft.com/...</a:To></s:Header><s:Body><Discover
xmlns="http://schemas.microsoft.com/windows/management/2012/01/enrollment"><request xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><EmailAddress>rudyooms@oldomain.com</EmailAddress>
<RequestVersion>7.0</RequestVersion><DeviceType>CIMClient_Windows</DeviceType><ApplicationVersion>10.0.26200.7171</ApplicationVersion><...AuthPolicy>OnPremise</AuthPolicy>
<AuthPolicy>Federated</AuthPolicy></AuthPolicies></request></Discover></s:Body></s:Envelope>
```

**Figure 1: Typical sequence for enrolling a message using MDE**

The enrollment process consists of the following steps.

1. The user's email name is entered via the **enrollment client**.
2. The enrollment client extracts the domain suffix from the email address, prepends the domain name with a well-known label, and resolves the address to the **Discovery Service (DS)**. The administrator configures the network name resolution service (that is, the **Domain Name System (DNS)**) appropriately.

Guess what happens if the domainname is gone....
User is not licensed!!!

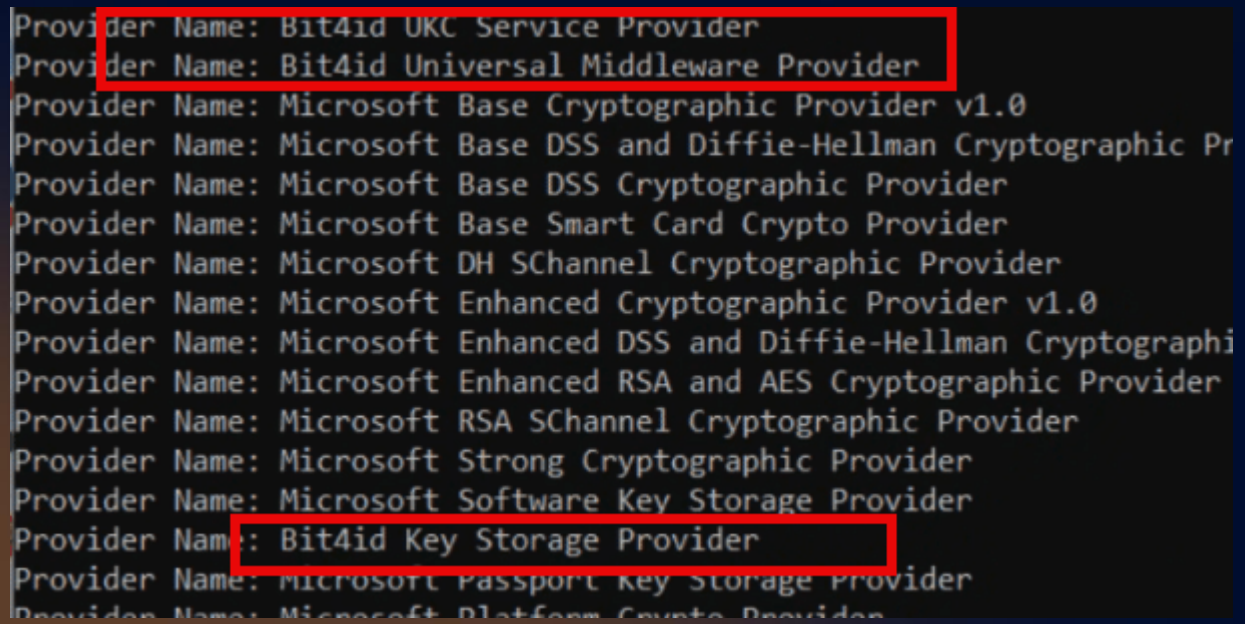
# Intune MDM Device CA

```
<#
REMEDIATION SCRIPT
Fixes Intune MDM enrollment entries where the UPN domain does not match $targetDomain.
Creates a one time backup in UPN_OldBackup and UPN_OldBackupTimestamp.
#>

[CmdletBinding()]
param()

$targetDomain = 'patchmypc.com'     # change if needed
$baseKey      = 'HKLM:\SOFTWARE\Microsoft\Enrollments'
$now          = Get-Date

$changes = @()

Get-ChildItem -Path $baseKey -ErrorAction SilentlyContinue | ForEach-Object {
    $keyPath = $_.PsPath
    $props   = Get-ItemProperty -Path $keyPath -ErrorAction SilentlyContinue

    if ($props.ProviderID -ne 'MS DM Server') {
        return
```

If you had a company merger....
Check the UPN!!
Change it / Fix it to ensure the certificate gets renewed

Intune MDM Certificate Renewal Failure: The Hidden UPN Issue

# Intune MDM Device CA Issue 2




If you were using the Bit4ID smartcard driver…. (Italy)

You will also end up with a certificate that wasn't getting renewed….

# Intune MDM Device CA Issue 2


```
do
{
    StringCchPrintfW(a7, 0x100, L"%s%d", L"ConfigMgrEnrollment", index);
    result = CreateKey(psz, a2, a3, a4, a5, a7, a8);
    ...
} while (result == -2146893809); // NTE_EXISTS
```

```
  goto LABEL_82;
v36 = a8;
if ( a7 && (a8 & 0x20) == 0 )
{
  if ( (unsigned __int8)wil::details::FeatureImpl<__WilFeatureTraits_Feature_Bypass3rdPartyKspsInRenew>::__private_IsEnabled(&`wil::Feature<__WilFeatureTraits_Feat
  {
    v34 = ProcessRenewalRequestWithRetry(v28, a8, a20);
    String = v34;
    if ( v34 < 0 )
    {
      v39 = L"ProcessRenewalRequestWithRetry";
      goto LABEL_82;
    }
    goto LABEL_8;
  }
  psz[0] = 0;
  String = OmaDmRegistryGetString(v28, 0i64, L"DMPCertThumbPrint", psz, 0x2Au);
  v37 = SysAllocString(psz);
```

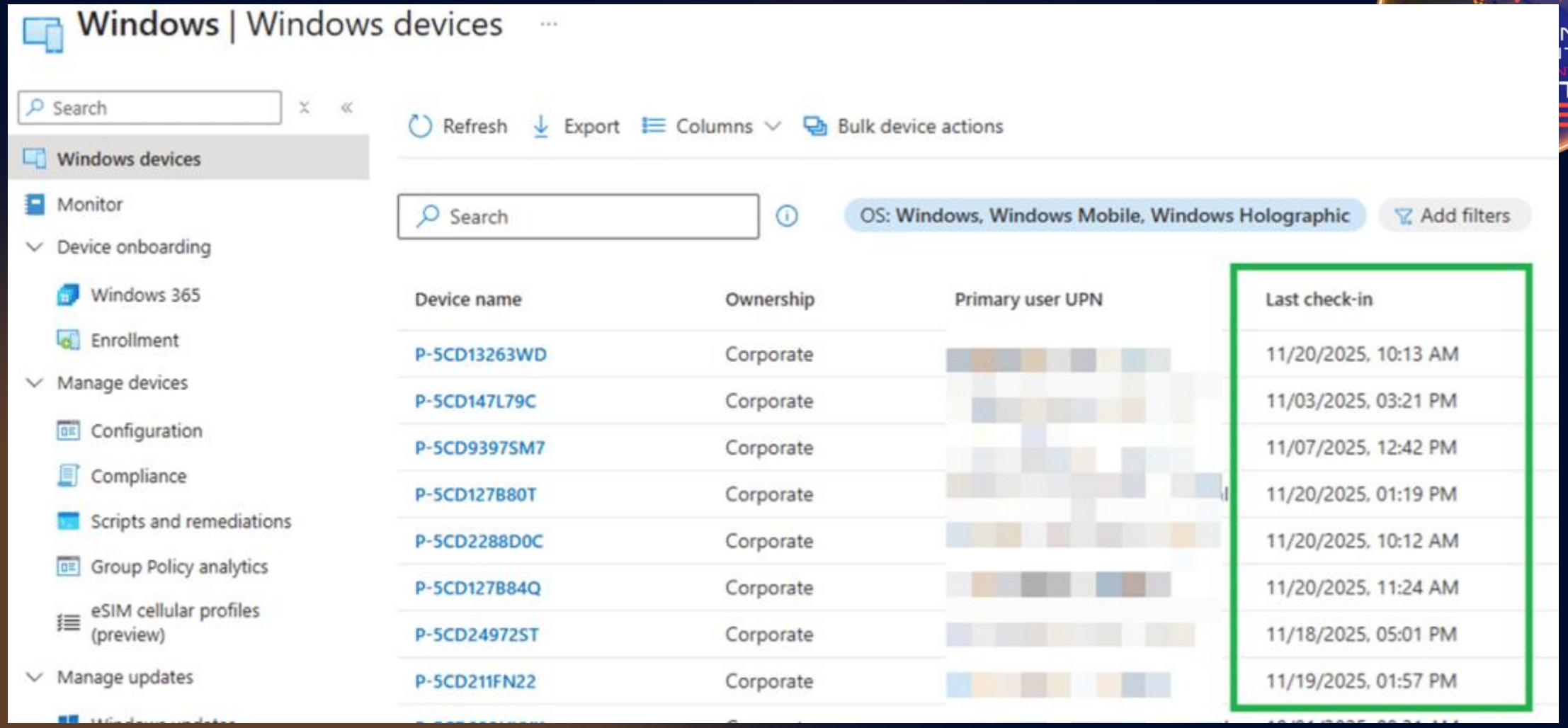
Before the CertEnroll could build a renewal request, the system initialized *ALL* available Key Storage Providers (PSZ in the picture).

Guess on which smartcard the certificate renewal flow broke?

Microsoft introduced a “bypass” to only select the regular key storage providers (TPM/Software)


# Last Check-In

# Last Check-In

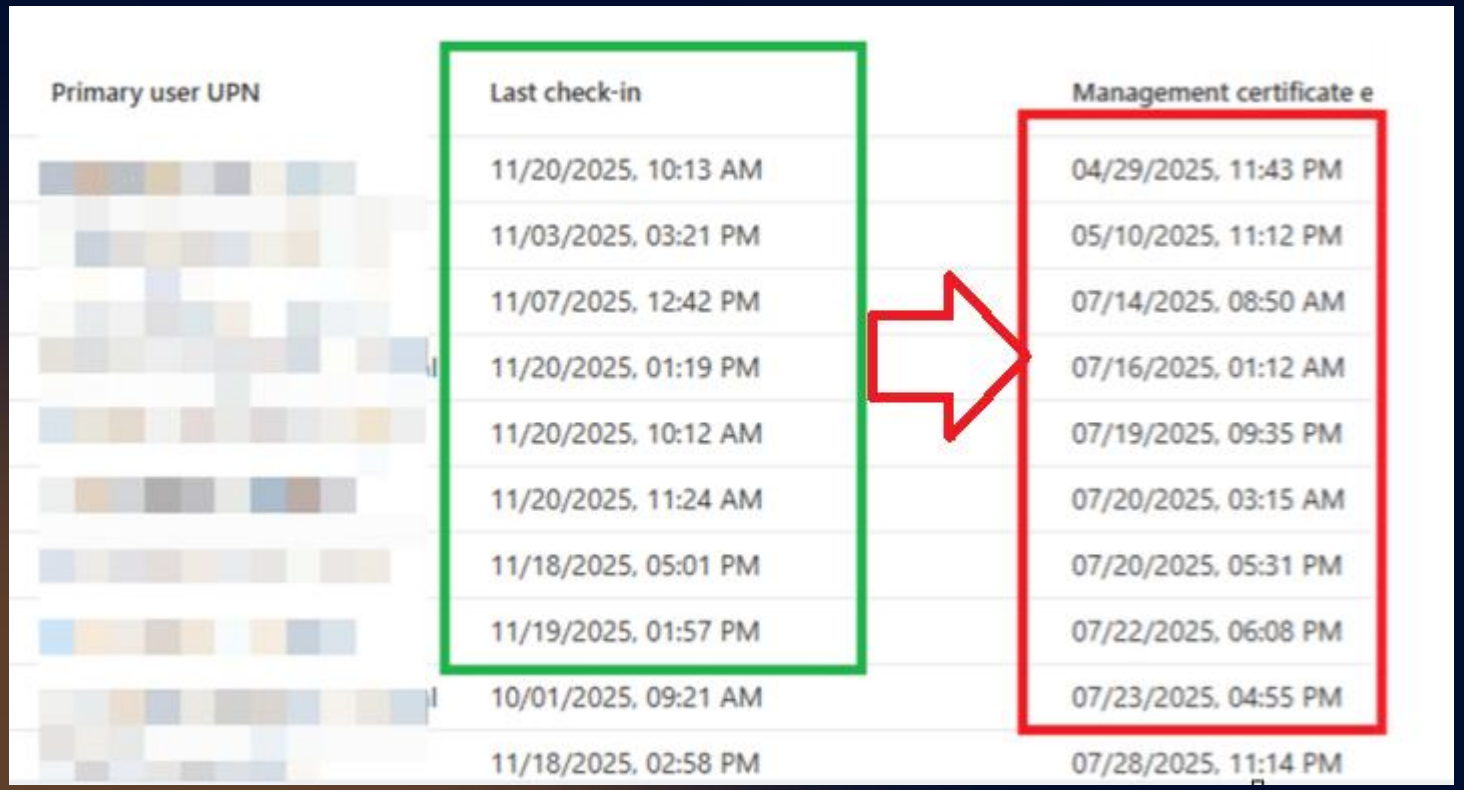



**Who is "trusting" the last check-in to find out if the device is still checking in to Intune??**

# Trusting the Last Check-In

# Trusting the Last Check-In

The device certificate was expired but the last check-in was still getting updated....



| Primary user UPN | Last check-in | Management certificate e |
|---|---|---|
| [redacted] | 11/20/2025, 10:13 AM | 04/29/2025, 11:43 PM |
| [redacted] | 11/03/2025, 03:21 PM | 05/10/2025, 11:12 PM |
| [redacted] | 11/07/2025, 12:42 PM | 07/14/2025, 08:50 AM |
| [redacted] | 11/20/2025, 01:19 PM | 07/16/2025, 01:12 AM |
| [redacted] | 11/20/2025, 10:12 AM | 07/19/2025, 09:35 PM |
| [redacted] | 11/20/2025, 11:24 AM | 07/20/2025, 03:15 AM |
| [redacted] | 11/18/2025, 05:01 PM | 07/20/2025, 05:31 PM |
| [redacted] | 11/19/2025, 01:57 PM | 07/22/2025, 06:08 PM |
| [redacted] | 10/01/2025, 09:21 AM | 07/23/2025, 04:55 PM |
| [redacted] | 11/18/2025, 02:58 PM | 07/28/2025, 11:14 PM |

If the certificate is expired → NO communication.. No Policies.. No Apps.. Nothing..

# Trusting the Last Check-In

The device will ALWAYS be able to reach out (say hi) to the service….
With it the last check in is updated….

```
[HKEY_LOCAL_MACHINE\software\microsoft\provisioning\OMADM\Accounts\B3CAED05-09
    "Flags"=DWORD:0000036f
    "ConnRetryFreq"=DWORD:00000006
    "InitialBackOffTime"=DWORD:00007530
    "MaxBackOffTime"=DWORD:0001d4c0
    "BackCompatRetryDisabled"=DWORD:0000ffff
    "ServerLastAccessTime"="20251114T123200Z"
    "LastSessionResult"=DWORD:00000000
    "ServerLastSuccessTime"="20251114T123346Z"
```

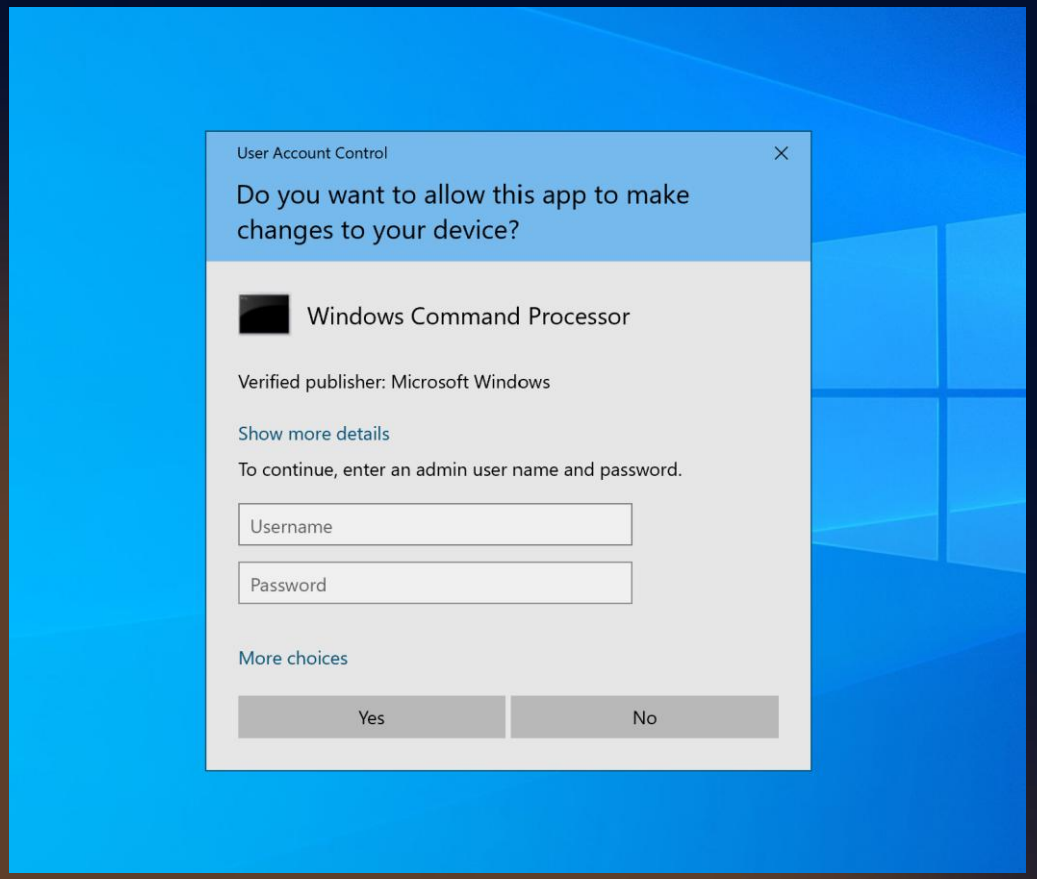
But it does **NOT** mean the device is able to communicate with the service successfully!!!

So please don't trust the last check-in

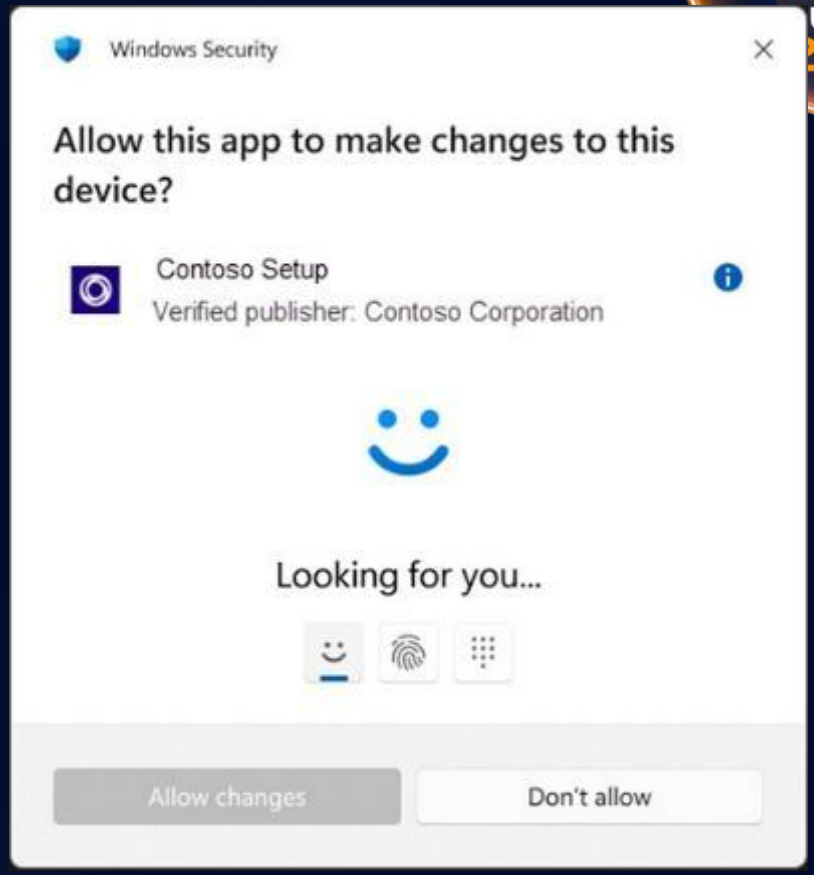

# Local Administrator Protection

# Local Administrator Protection

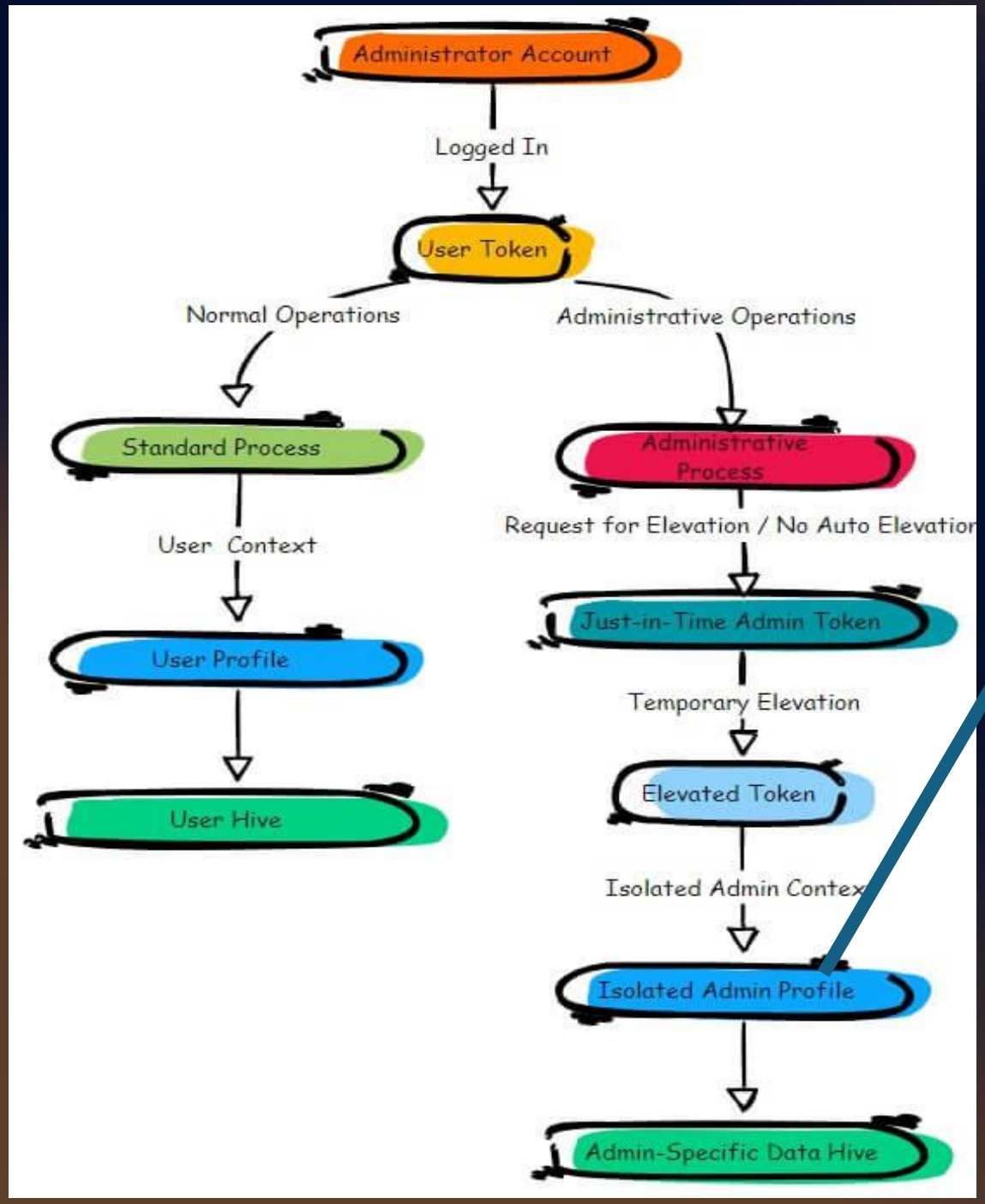
## In the Past: UAC (CLARK KENT MODE)



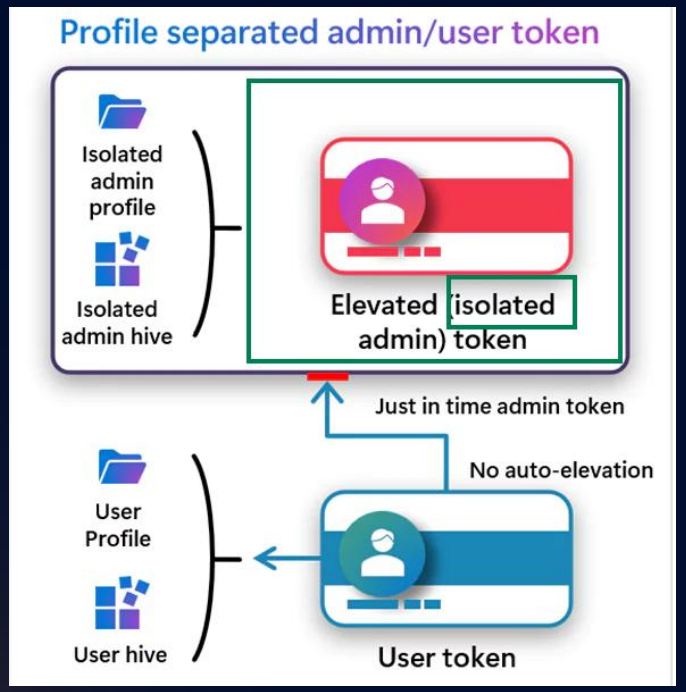

After Elevation it becomes superman...
But still the same person




**Now!: Administrator Protection**
**(to secure your local admin)**

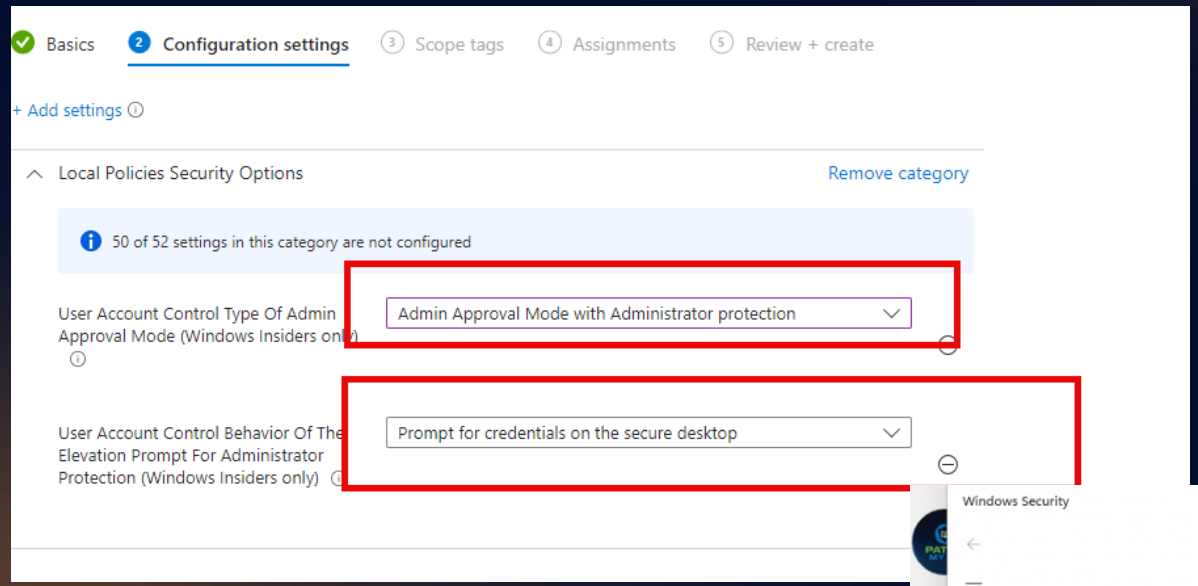



```
c:\temp>whoami
desktop-fekstb7\admin_rudy
```



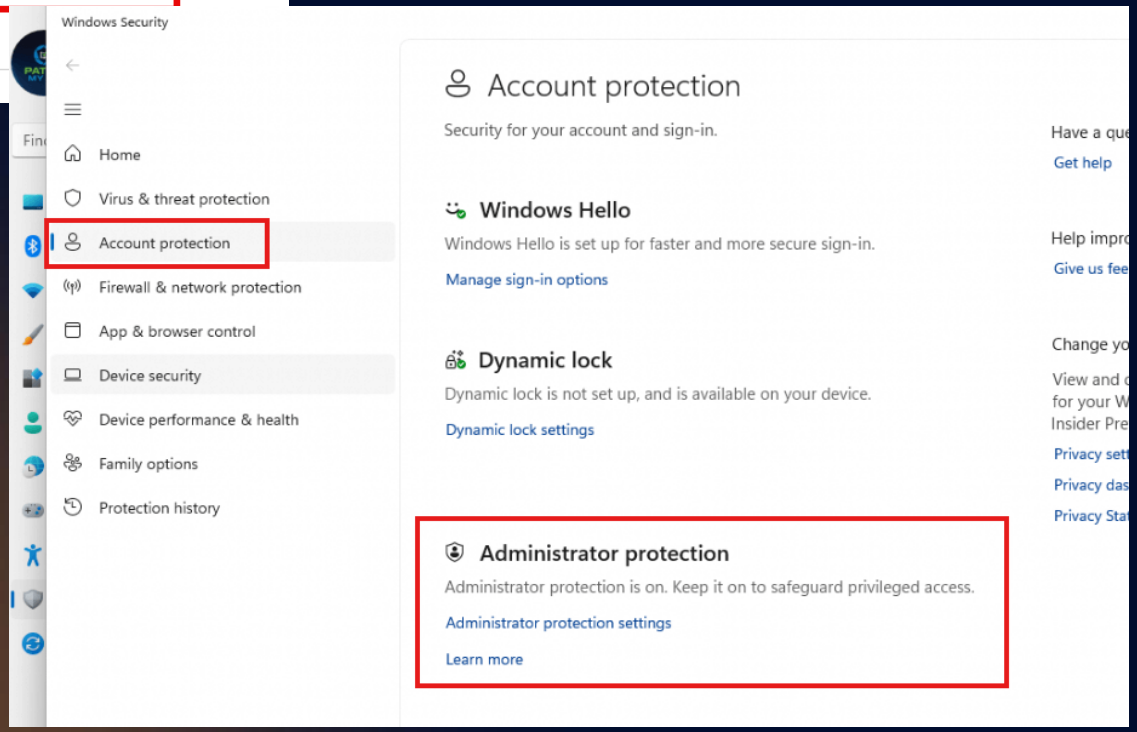

Patch My PC Blog: Administrator Protection on Windows 11:

# Local Administrator Protection




**For now we need to enable it manually..**
**(which is a good thing)**

**Will be turned on by default in the (near.....or not) future...**



# Enable Local Admin protection

This is fine


What if it broke all your NON-US devices (not able to login anymore?)

# Local Administrator Protection


**So… using a NON-US OS … is called rare?**

## [Administrator Protection]

**Luckily Microsoft fixed it with the next Windows Update**

- Fixed a rare issue when Administrator Protection was enabled, which could cause you to see a resource loader cache error loading the MUI file on sign in.
- Removed extraneous space between Dynamic Lock and Administrator Protection under Account Protection in Windows Security.
- Fixed an issue where Administrator Protection wasn't showing in the results if you searched from the taskbar.

# Local Administrator Protection


Announcing Windows 11 Insider Preview Build 26300.7965 (Dev Channel)

Looks like more stuff was broken when you enabled administrator protection

So please… don't implement features the day they are released

## New features gradually being rolled out with toggle on*

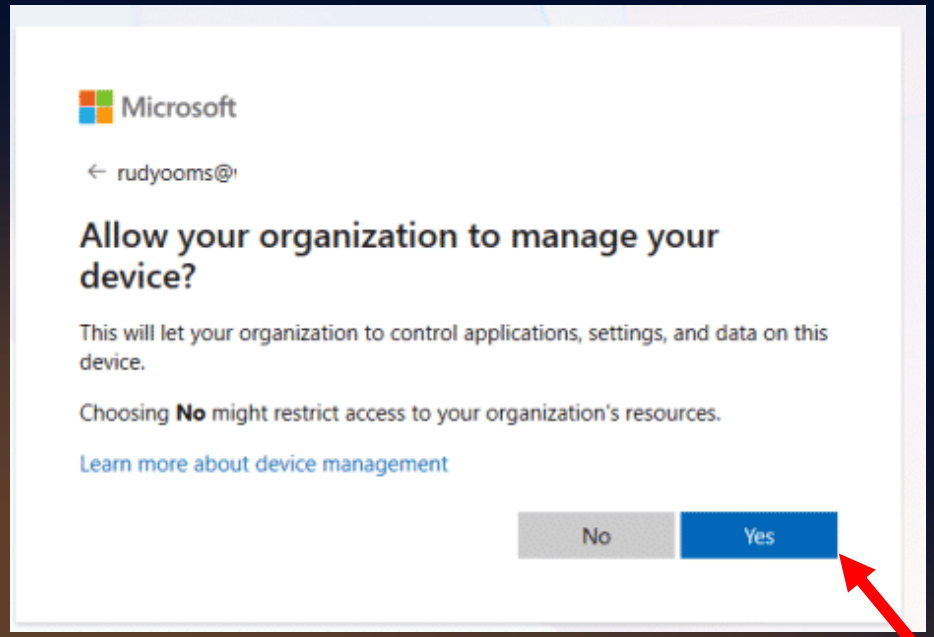
### [Administrator Protection]

Administrator protection is being re-enabled and aims to protect free floating admin rights for administrator users, allowing them to still perform all admin functions with just-in-time admin privileges. This feature is OFF by default and can be enabled via OMA-URI in Intune or via group policy.

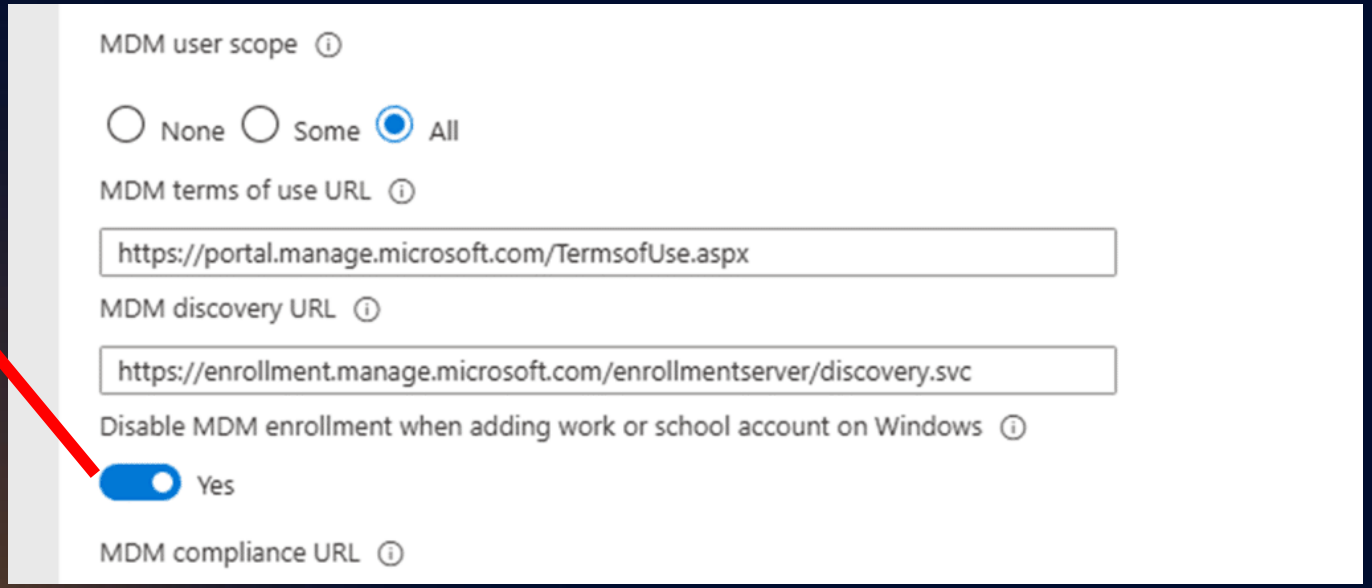

# Disable MDM Enrollment When Adding a Work or School Account on Windows

# Disable MDM Enrollment


**We all hate this prompt, right?**



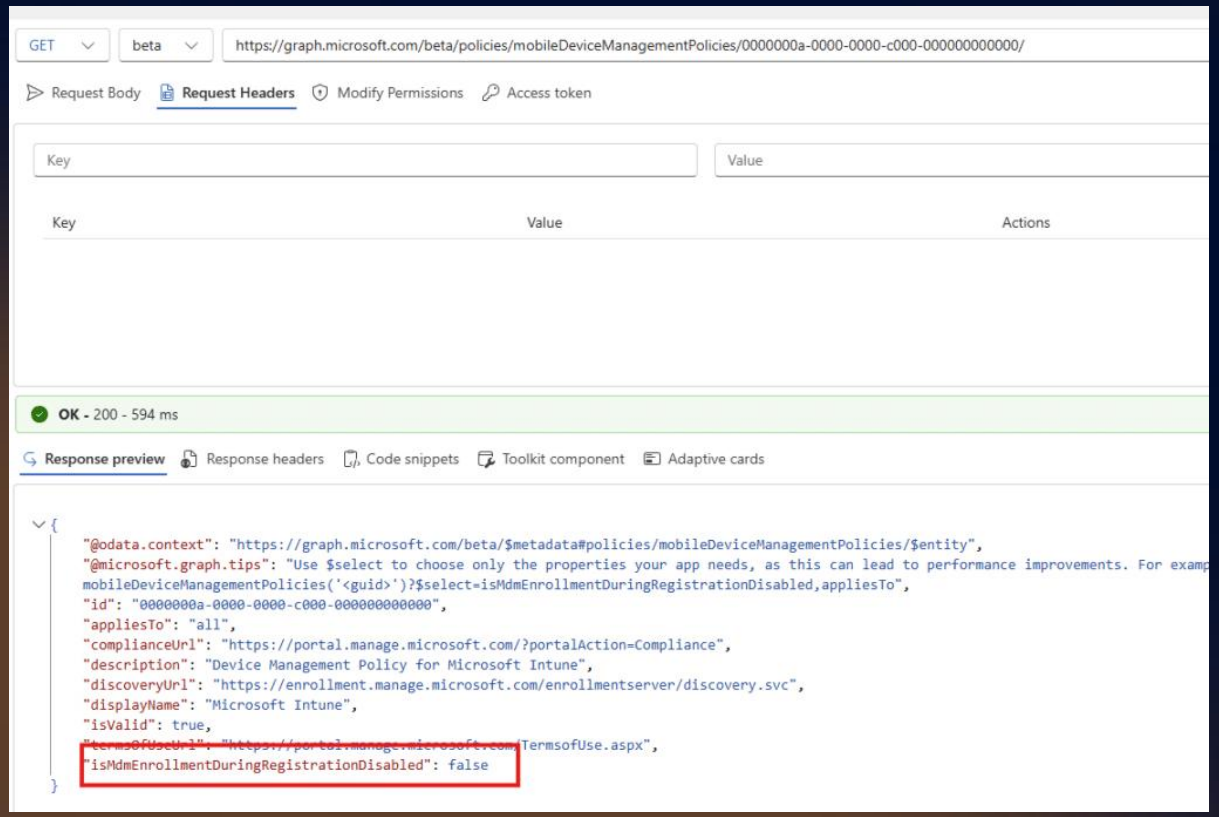

Microsoft (Entra team?) came up with a *solution to disable MDM enrollment when adding a work/school account from teams/office




*Of course blocking personal devices in general is always better

# Disable MDM Enrollment

## IsMDMENrolmentDuringRegistrationDisabled

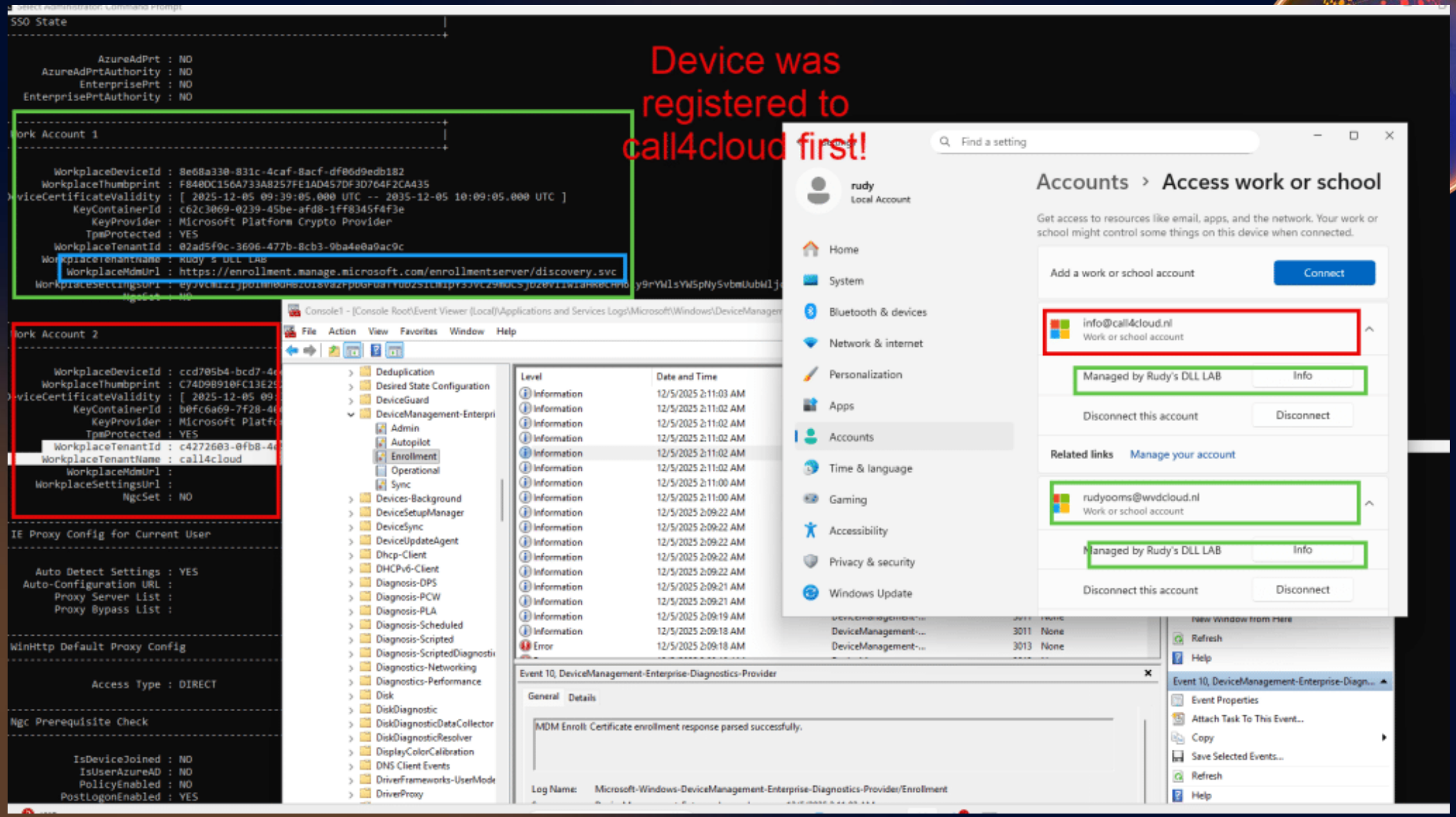



Before the feature went GA, we could already enable it with Graph


Is this smart to do in Prod???

# Disable MDM Enrollment

# Disable MDM Enrollment

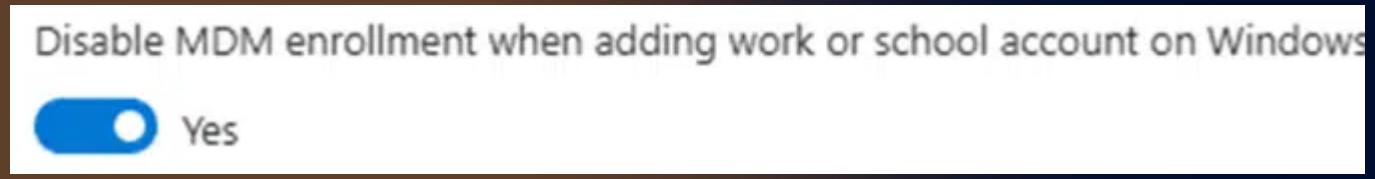



The prompt was gone... but the device still was MDM enrolled!!!

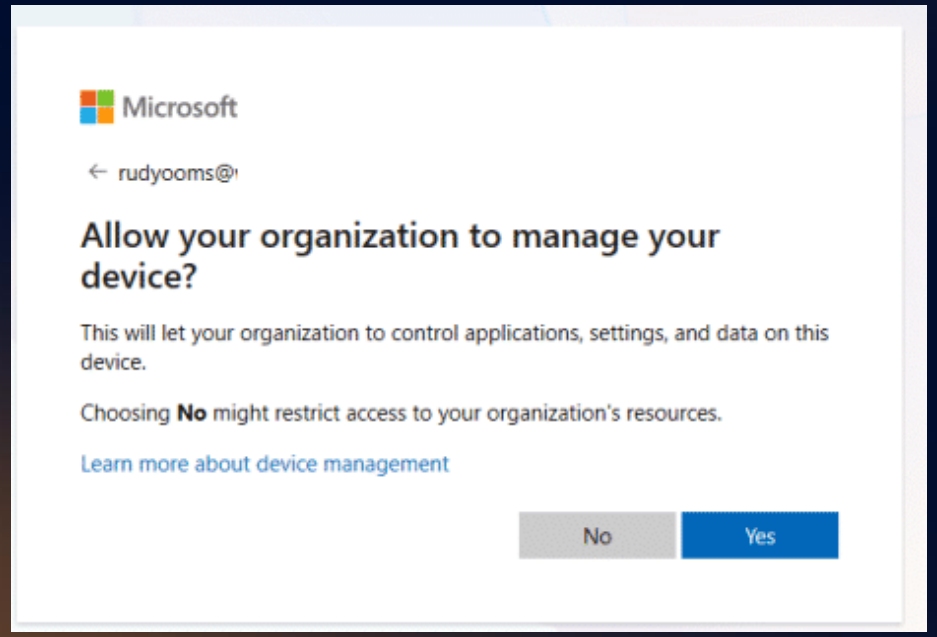
# Disable MDM Enrollment


When the feature was first activated, the **IsMDMEnrollmentRequired** config was **ALWAYS** send over to the device...

Even when the MDM enrollment was disabled



# Disable MDM Enrollment




Luckily, this issue was fixed before the feature Really went GA

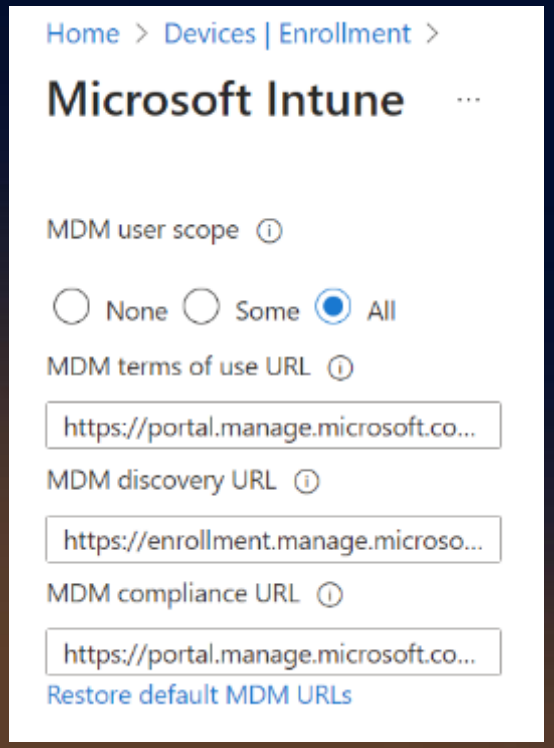
**Impact across common Windows enrollment scenarios**

| Scenario | Default behavior | Opt-in recommended behavior |
|---|---|---|
| BYOD / personal devices | High risk of accidental enrollment | App access without device takeover |
| Microsoft Office / Teams sign in | May initiate MDM enrollment | No MDM enrollment unless user chooses |
| Microsoft Entra hybrid join (corporate) | Microsoft Entra joined | Microsoft Entra joined |
| Windows settings enrollment | MDM enrollment | MDM enrollment |
| Windows Autopilot / provisioning | MDM enrollment | MDM enrollment |

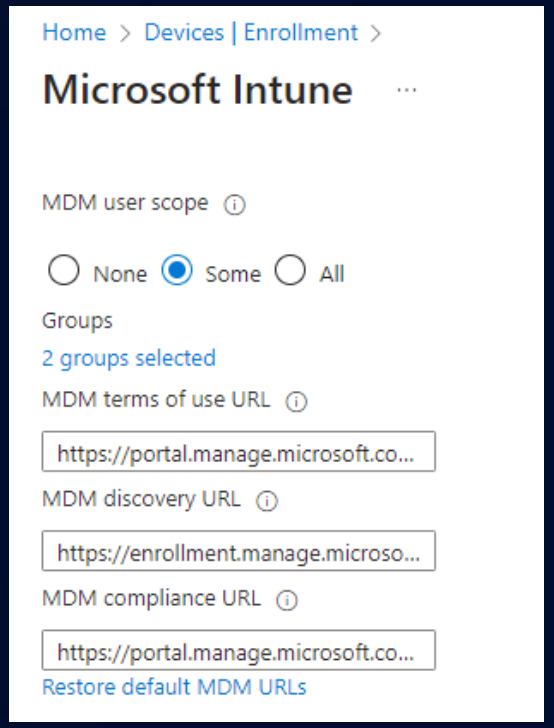

# MDM Scope
# &
# Automatic Enrollment

# MDM Scope / Automatic Enrollment


Default




Preferred?




We need to define the MDM scope if we want to automatically enroll our devices with Intune

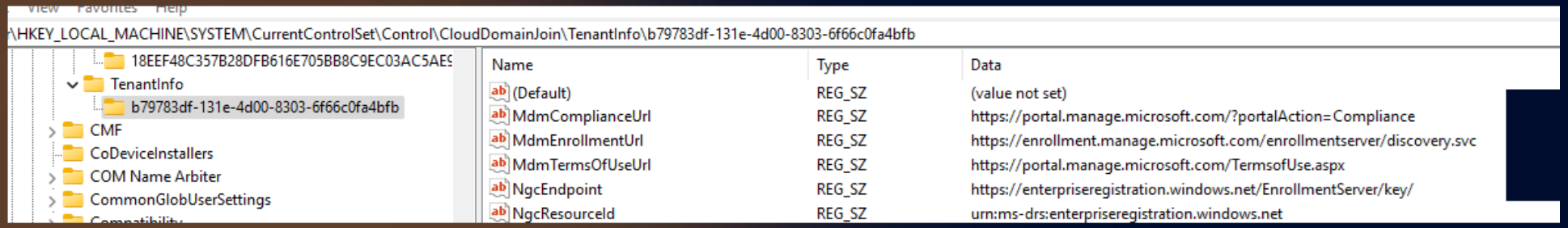
Automatic MDM enrollment is a premium Microsoft Entra feature available for Microsoft Entra ID Premium subscribers. If you can't see the automatic enrollment settings, select **Automatic MDM enrollment is available only for Microsoft Entra ID Premium subscribers** to activate a free trial.

# The Automatic MDM Enrollment


DSREGCMD /status

```
+----------------------------------------------------------------------+
| Tenant Details                                                       |
+----------------------------------------------------------------------+

                TenantName : Patch My PC
                  TenantId : [redacted]
               AuthCodeUrl : https://login.microsoftonline.com/
           AccessTokenUrl  : https://login.microsoftonline.com/
                    MdmUrl : https://enrollment.manage.microsoft.com/enrollmentserver/discovery.s
                 MdmTouUrl : https://portal.manage.microsoft.com/TermsofUse.aspx
          MdmComplianceUrl : https://portal.manage.microsoft.com/?portalAction=Compliance
              SettingsUrl  : eyJVcmlzIjpbImh0dHBzOi8va2FpbGFuaS5vbmUubWljcm9zb2Z0LmNvbS8
caWNyb3Nv[redacted]
              JoinSrvVersion : 2.0
```

**The moment the MDM scope is configured it should show up using DSREG**
**DSREG fetches the data from the TenantInfo registry key**



# Configure the MDM Scope: This is Fine!


**What if Automatic Enrollment doesn't kick in on new enrolled AP devices after configuring the MDM scope???**

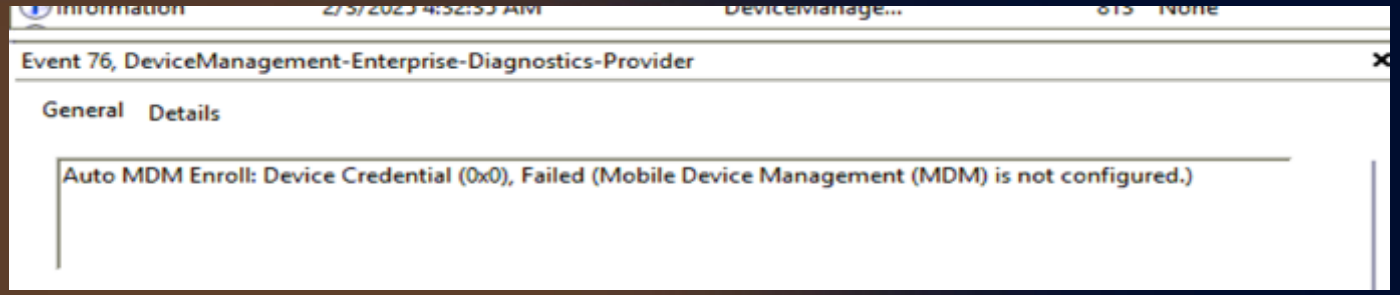
# Troubleshooting Automatic Enrollment


**Autopilot skipping the ESP… because Automatic MDM Enrollment didn't work!**
**And…. Somehow the MDM urls are empty?**

```
            TenantName :
              TenantId : [redacted]
          AuthCodeUrl : https://login.microsoftonline.com/[redacted]/oauth2/authorize
       AccessTokenUrl : https://login.microsoftonline.com/[redacted]/oauth2/token
                MdmUrl :
             MdmTouUrl :
       MdmComplianceUrl :
           SettingsUrl :
        JoinSrvVersion : 2.0
```

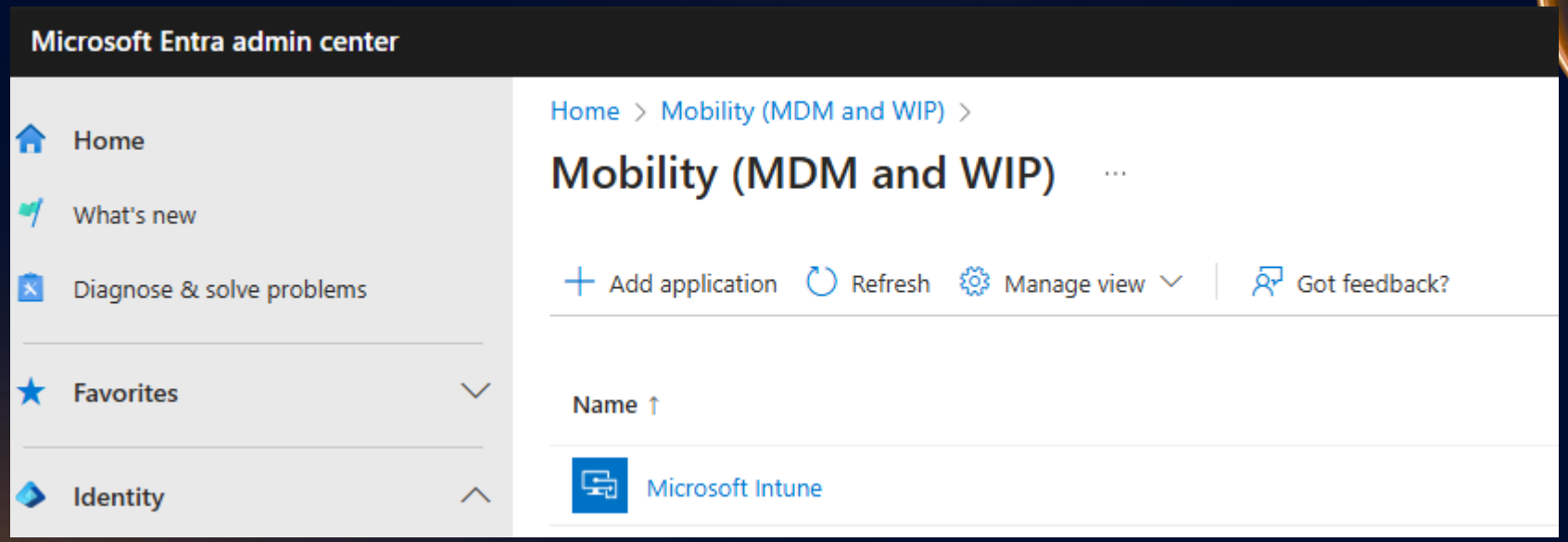
```
# Trigger AutoEnroll
C:\Windows\system32\deviceenroller.exe /c /AutoEnrollMDM
```

**Manually Enrolling the device also fails….**

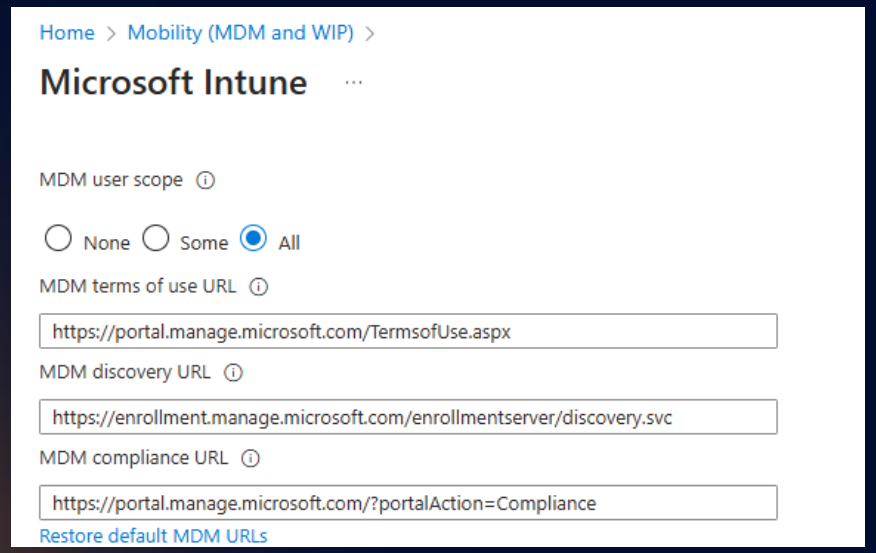



- **User is licensed for P1**
- **User is in the MDM Scope and has an Intune License**

# Troubleshooting Automatic Enrollment

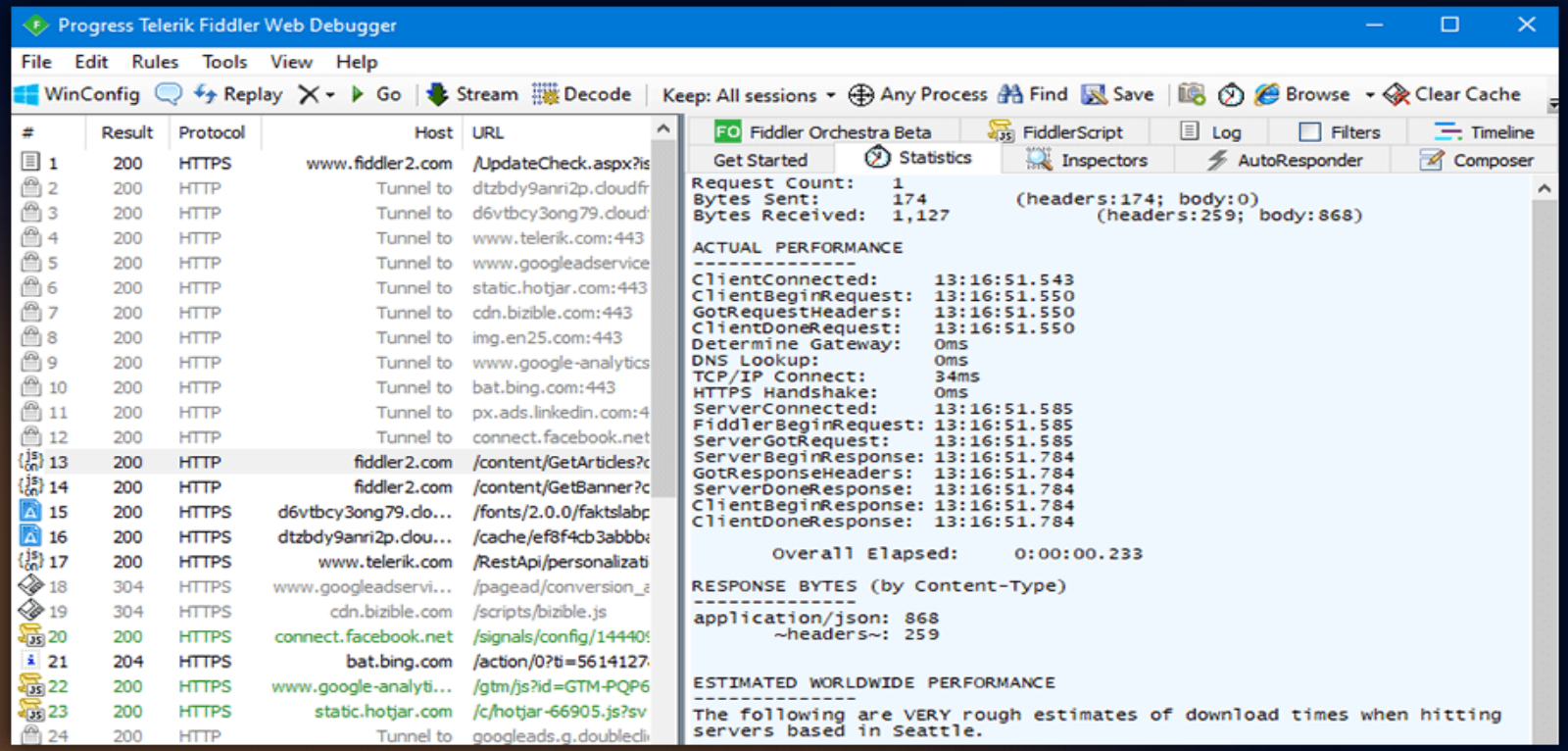



**Checking the MDM Policies in Entra**



# Troubleshooting Automatic Enrollment

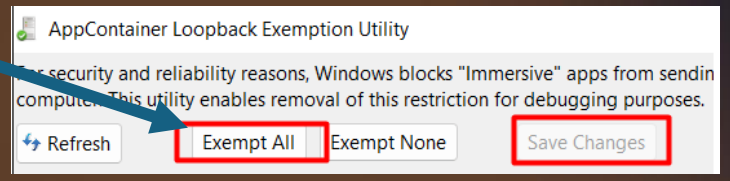
## Let's use Fiddler to Troubleshoot!

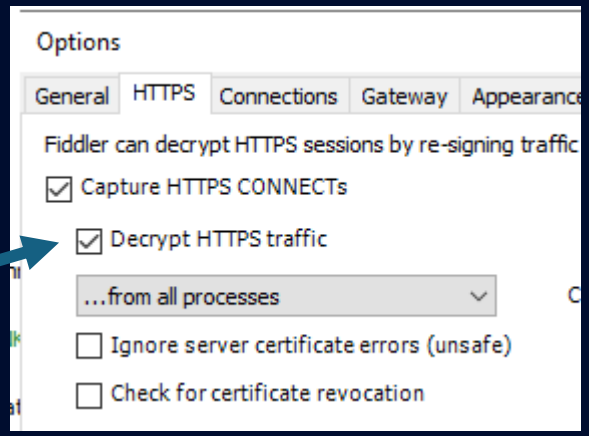



```
if (oSession.HostnameIs("r.manage.microsoft.com")) {
        oSession["https-Client-Certificate"] = "C:\\test\\Intune.cer";
    }
    if (oSession.HostnameIs("manage.microsoft.com")) {
        oSession["https-Client-Certificate"] = "C:\\test\\Intune.cer";
    }
    if (oSession.HostnameIs("fef.amsub0302.manage.microsoft.com")) {
        oSession["https-Client-Certificate"] = "C:\\test\\Intune.cer";
    }
    if (oSession.HostnameIs("checkin.dm.microsoft.com")) {
        oSession["https-Client-Certificate"] = "C:\\test\\MDM.cer";
    }
    if (oSession.HostnameIs("discovery.dm.microsoft.com")) {
        oSession["https-Client-Certificate"] = "C:\\test\\MDM.cer";
    }
    if (oSession.HostnameIs("enrollment.dm.microsoft.com")) {
        oSession["https-Client-Certificate"] = "C:\\test\\MDM.cer";
    }
    if (oSession.HostnameIs("enterpriseregistration.windows.net")) {
        oSession["https-Client-Certificate"] = "C:\\test\\Azure.cer";
    }
```

**We can even attach the Intune and Entra Certificate to it!**

**With Fiddler we can intercept HTTPS Traffic / Decode it and use it for troubleshooting** (or other things..)



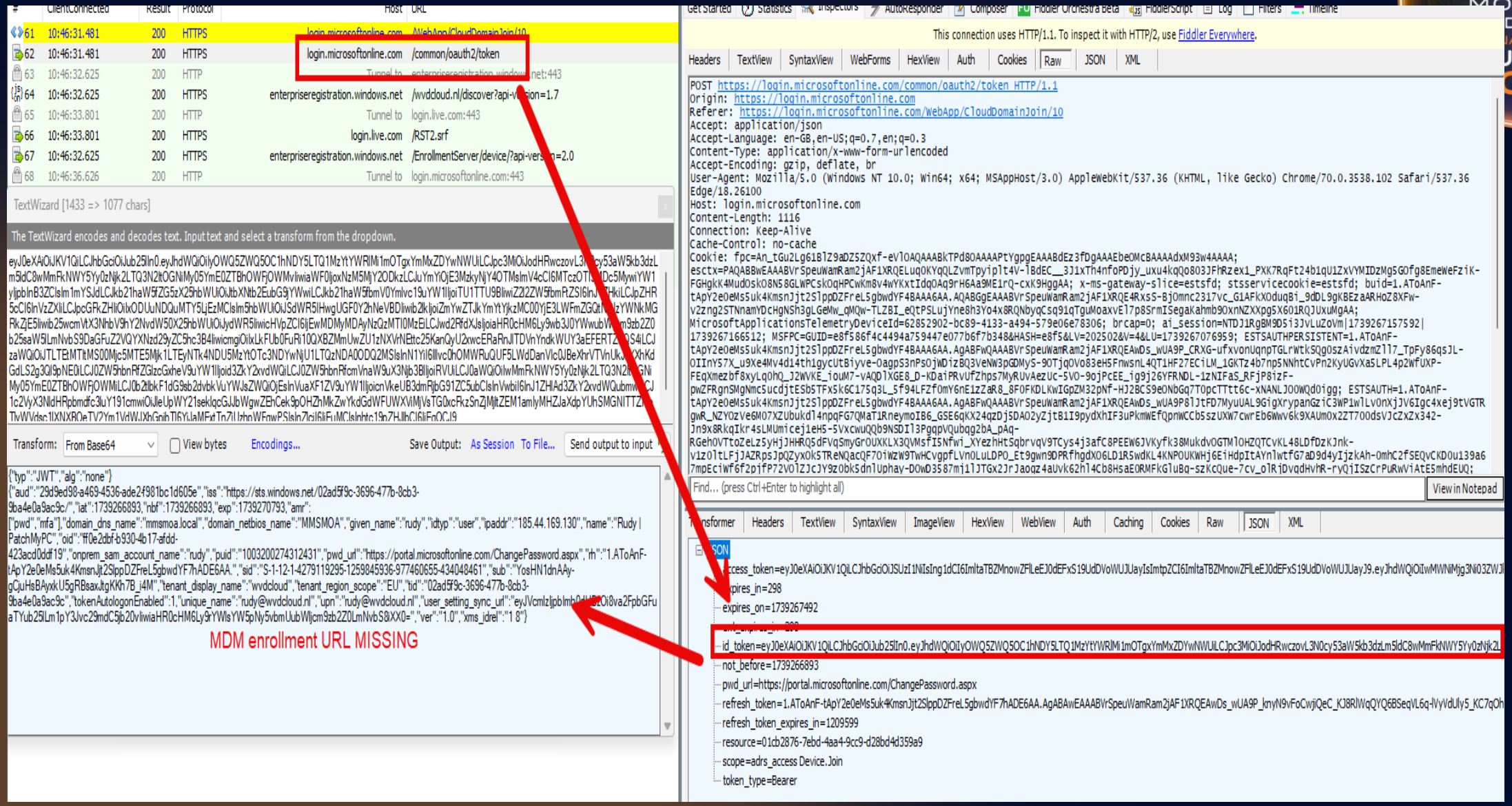

https://call4cloud.nl/fiddler-decrypt-capture-intune-traffic/

# Troubleshooting Automatic Enrollment

**On a working device:**
**When joining Entra, The ID Token should be there holding the MDM enrollment URL**

# Troubleshooting Automatic Enrollment

## This how it looked like on the BROKEN devices

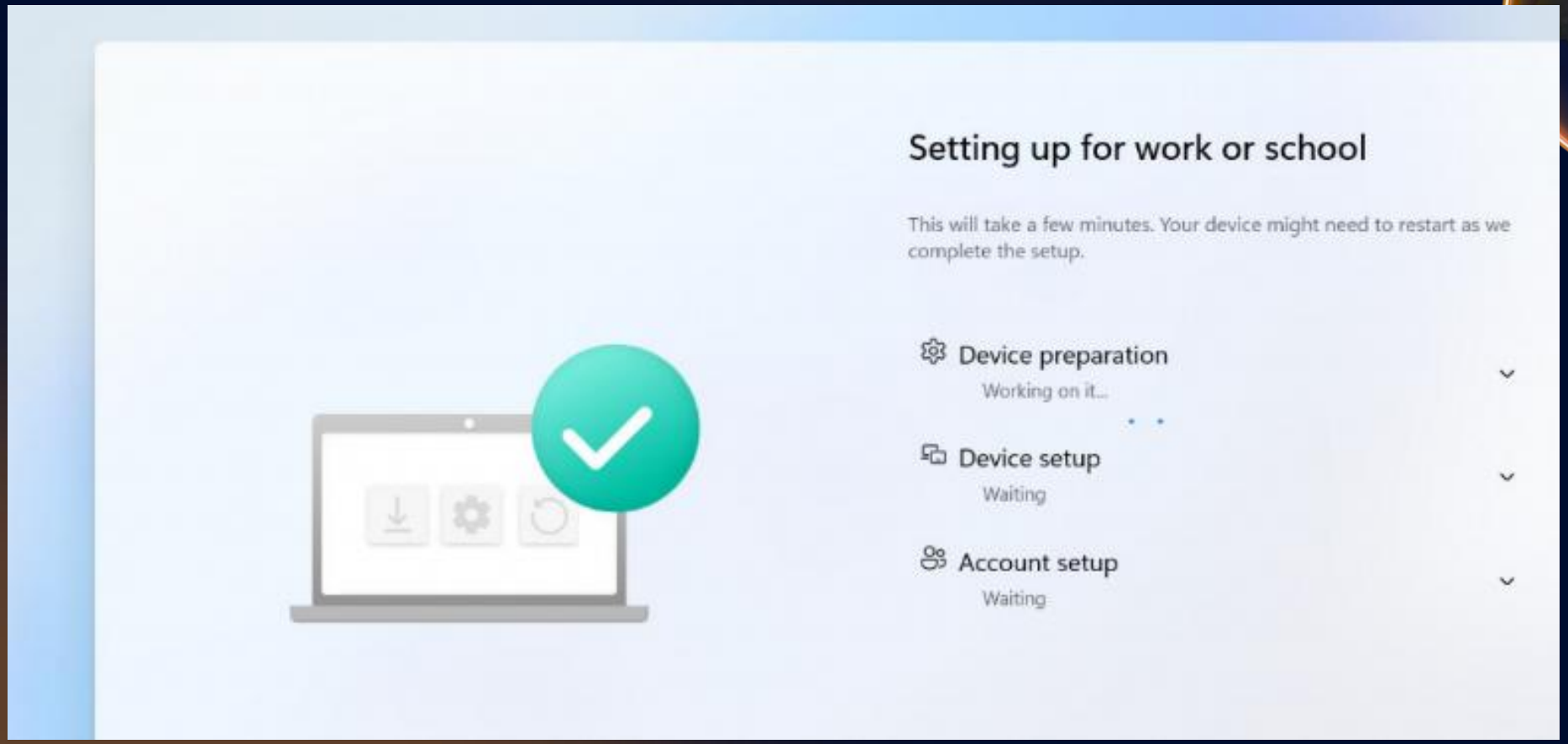


# Troubleshooting Automatic Enrollment

## Using Graph to find the MDM Policies

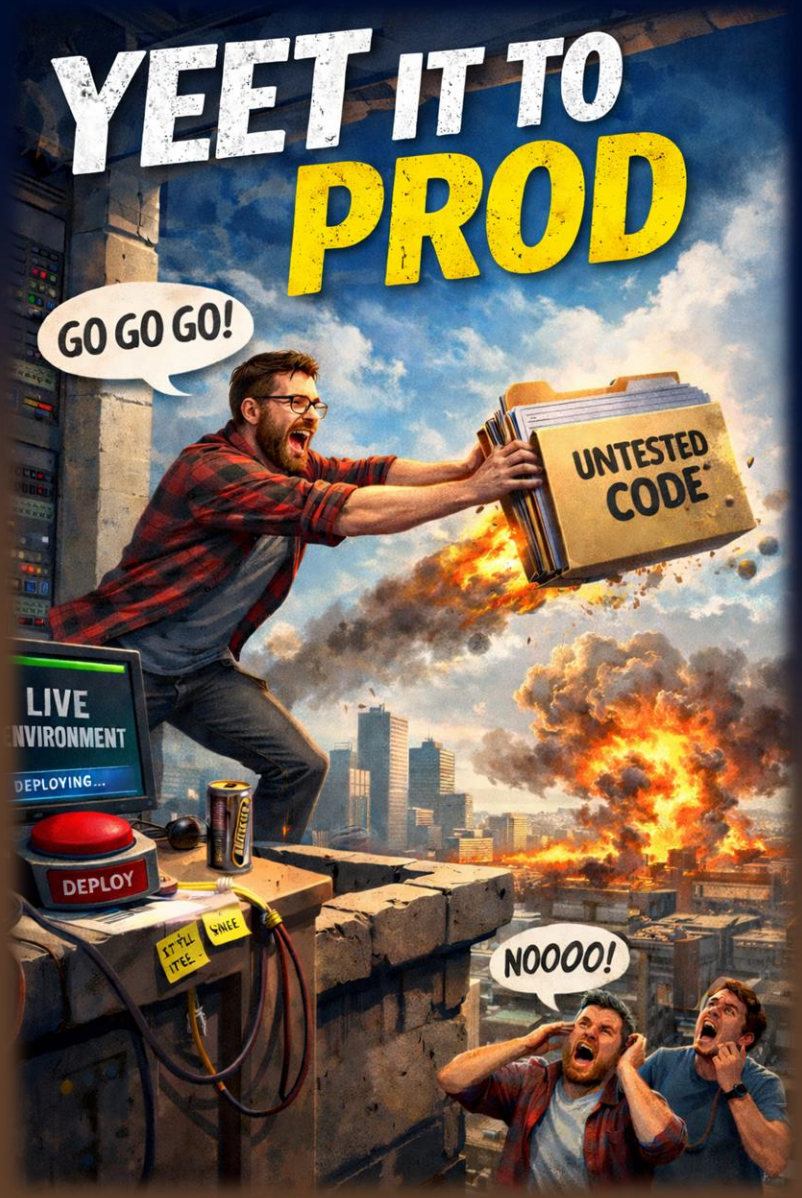

They had a different MDM provider before moving to Intune... but the removal of the MDM policy in the portal failed to delete it from the backend

# Troubleshooting Automatic Enrollment




- **After deleting the broken enrollment policy…. It worked within seconds**

# Lesson Learned:




We need to test every single feature before implementing it and yeeting it to prod

# Wrapping Up


- **We implemented some funny Security Features**

- **Potential Issues**: Misconfigurations leading to enrollment failures, compliance problems, policy enforcement issues, admin privilege complications.

- **Best Practices**: Don’t deploy stuff to prod and all devices! Use Deployment Rings! And wait until the feature goes GA!