



# How to debug Intune Settings/Features When they break

*Which they will?... ?*

# Sponsors





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

**Issued to:** Microsoft Corporation UEFI CA 2011

**Issued by:** Microsoft Corporation Third Party Marketplace Root

**Valid from** 6/27/2011 to 6/27/2026

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

## Secure Boot Security Feature Bypass Vulnerability

CVE-2023-24932  
Security Vulnerability

**Released:** May 9, 2023

**Last updated:** Jul 10, 2025

Assigning CNA: Microsoft

CVE.org link: [CVE-2023-24932](https://cve.org/CVE-2023-24932)

**Impact:** Security Feature Bypass    **Max Severity:** Important

**CVSS Source:** Microsoft

**Vector String:** CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

**Metrics:** CVSS:3.1 6.7 / 6.2

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

# Secure Boot Policy

The Idea was easy..



✓ Basics
**2 Configuration settings**
3 Scope tags
4 Assignments
5 Review + create

+ Add settings ⓘ

---

^ Secure Boot
Remove category

Enable Secureboot Certificate Updates  (Enabled) Initiates the deployment of new secure boot certificates and related updates. ⓘ

Configure Microsoft Update Managed Opt In  Enabled ⓘ

Configure High Confidence Opt Out ⓘ  Disabled. ⓘ

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



Secure Boot status ⓘ

ⓘ The affected devices have Secure Boot enabled but are using Microsoft Secure Boot certificates that expire in 2026. To remain secure and compliant, devices must be updated with the latest UEFI Secure Boot DB and KEK certificates. [Learn more about Windows Secure Boot certificate expiration and CA updates](#) ⓘ

Refresh Export Columns 4 items

Search ⓘ Add filters

Up to date: 0 | Not up to date: 0 | Not applicable: 4 | Device count: 4

Device name ⓘ	OS version ⓘ	Microsoft Entra device ID ⓘ	Secure Boot enabled ⓘ	Certificate status ⓘ	Device model ⓘ	Device manufacturer ⓘ	Device SKU ⓘ	Firmware
WVD-83773		3eb46fd2-ac53-4796-8bf9-8e8f4988	Not available	ⓘ Not applicable				
DESKTOP-8IN9QJT		5efd05b9-f931-4e36-bf15-a26e61bc	Not available	ⓘ Not applicable				
PMPC-05603		74acbb74-2c99-46da-9016-fb176d5	Not available	ⓘ Not applicable				
PMPC-76979		b978c3e5-c2d5-412e-88f0-a73c82d	Not available	ⓘ Not applicable				

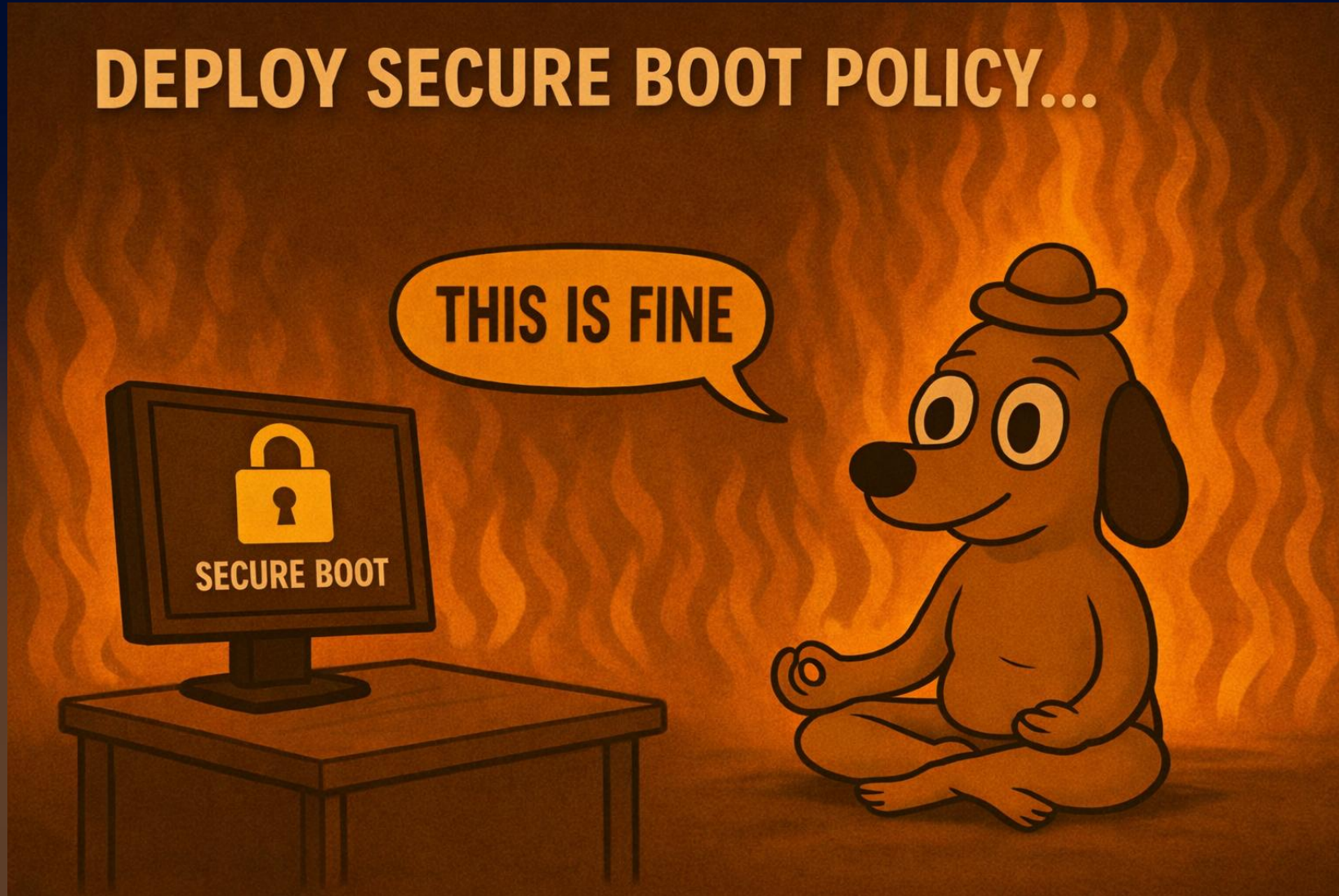
The Reporting... ? That is a different challenge..

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

# Secure Boot Policy



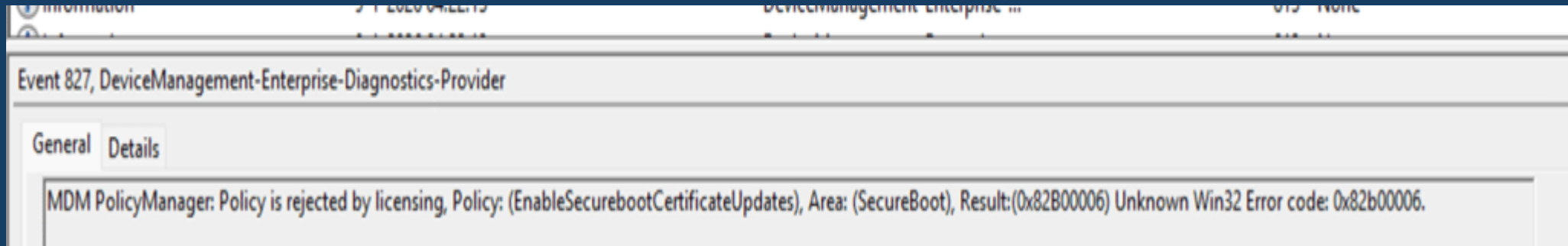
**DEPLOY SECURE BOOT POLICY...**



# 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

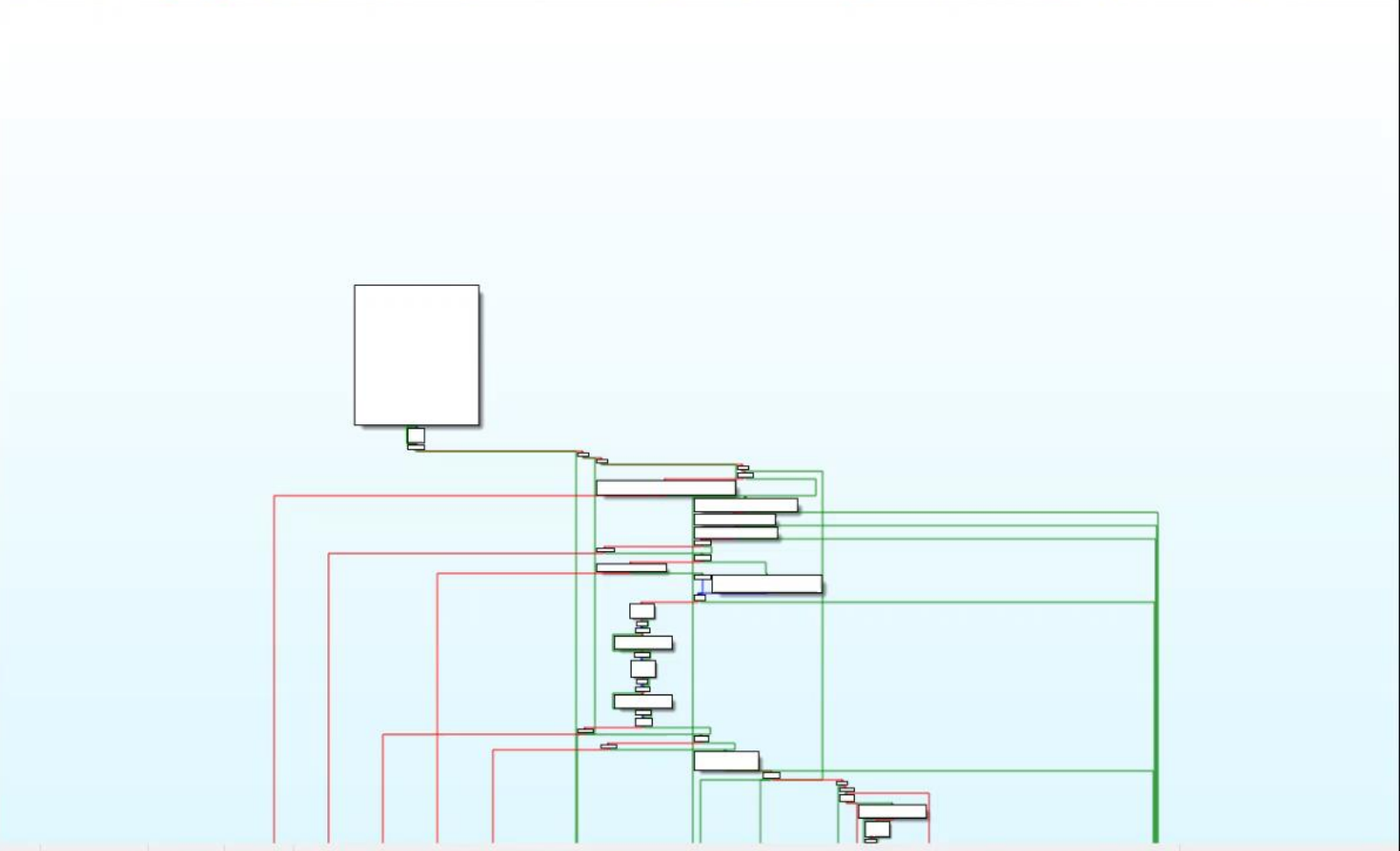
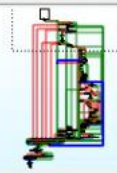


To find out what happened... I opened the Policymanager.dll

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
_ExtractValueElement_GetNewClassToParse___1___dtor\$14	.text	000000018008C1D

Line 2034 of 2061

Graph overview



6.87% (-1949, -3781) (768, 510) 0005BFF9 000000018005BFF9: EnterprisePolicyManagerStore\_SetProviderContextSidAreaPolicyValue (PolicyManagerScopeData \*, usho) (Synchronized with Hex View)

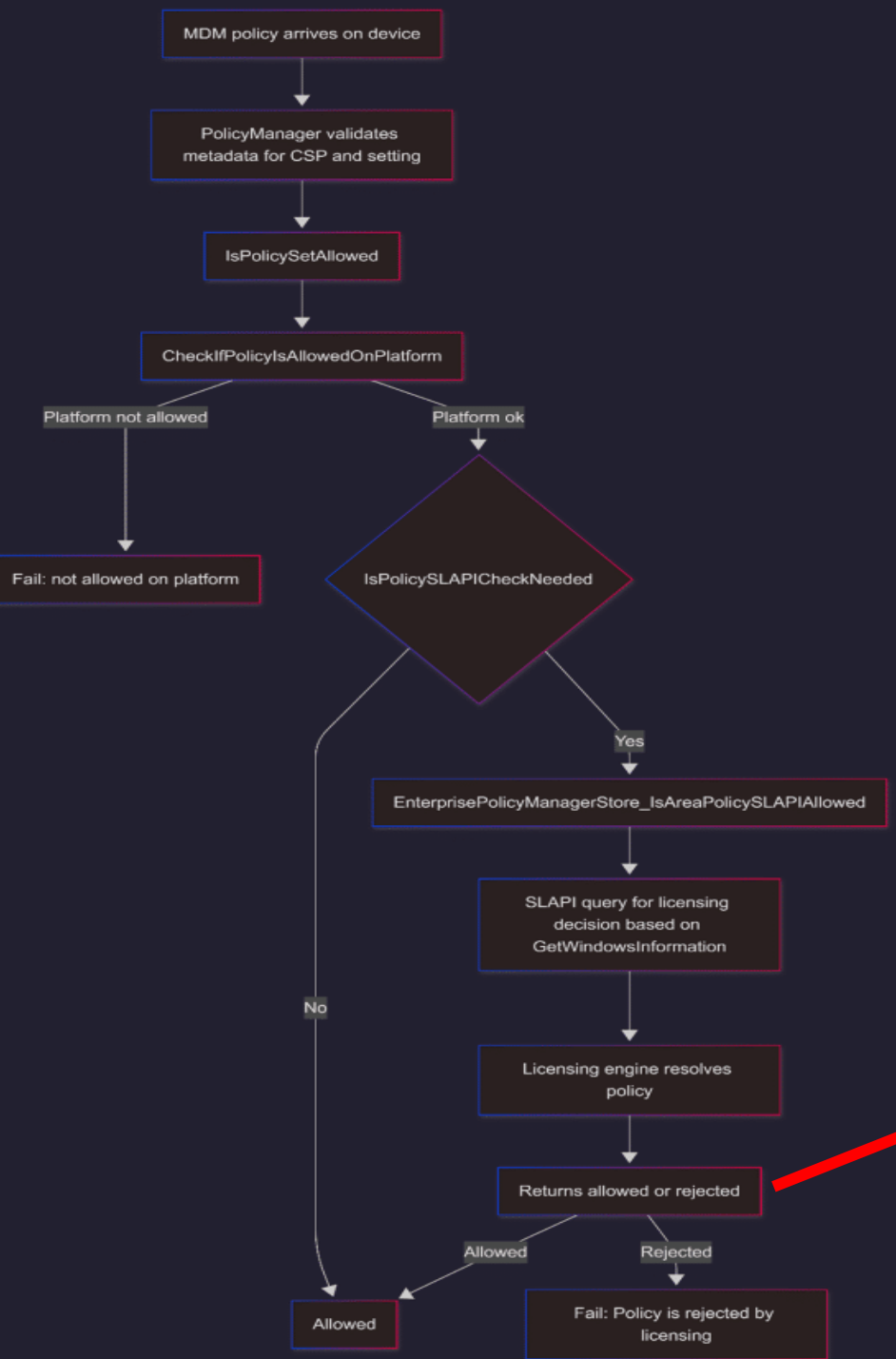
Output

License: 55-BK3-0K04-55 ChinaR10; 2022 happy new year (99 users)  
 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.

# The PolicyManager code told me where to look

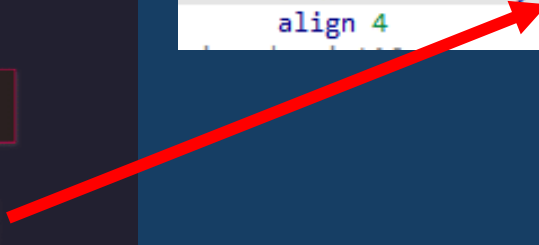


```
C:\Users\RudyOoms>licensingdiag -cab c:\temp\123.cab  
<policy name="dmenrollment-Mobile-Business" type="DWORD">0</policy>  
<policy name="enterprisemgmt_policymanager-License-MDMPolicyAllowList"  
type="string">AboveLock|Accounts|ActiveXControls|ADMXIngest|AllowMessageSync|AppDeviceInventory|AppHVSI|Application  
<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↑to  
; IsPolicySLAPICheckNeeded(void)+13A5↑to ...  
text "UTF-16LE", 'enterprisemgmt_policymanager-License-CheckMDMPolicy'  
text "UTF-16LE", 'AllowList',0  
align 4
```



# Secure Boot Policy



The screenshot shows a Microsoft 365 subscription list for the user 'Rudy Oöms' (email: rudyoöms@wvdcloud.nl). The list includes the following subscriptions:

- Skype for Business Online (Plan 2)**  
Microsoft 365 E5 EEA (no Teams)
- Sway**  
Microsoft 365 E5 EEA (no Teams)
- To-Do (Plan 3)**  
Microsoft 365 E5 EEA (no Teams)
- Universal Print**  
Microsoft 365 E5 EEA (no Teams)
- Viva Engage Core**  
Microsoft 365 E5 EEA (no Teams)
- Viva Learning Seeded**  
Microsoft 365 E5 EEA (no Teams)
- Whiteboard (Plan 3)**  
Microsoft 365 E5 EEA (no Teams)
- Windows 10/11 Enterprise (Original)**  
Microsoft 365 E5 EEA (no Teams)

A red arrow points from the center of the screenshot towards the 'Windows 10/11 Enterprise (Original)' subscription, which is the only one with an unchecked checkbox.

**Subscription activation was "one" the culprits!!!**

# Secure Boot Policy



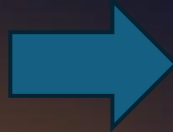
## Licenses

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 removes subscription
- 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



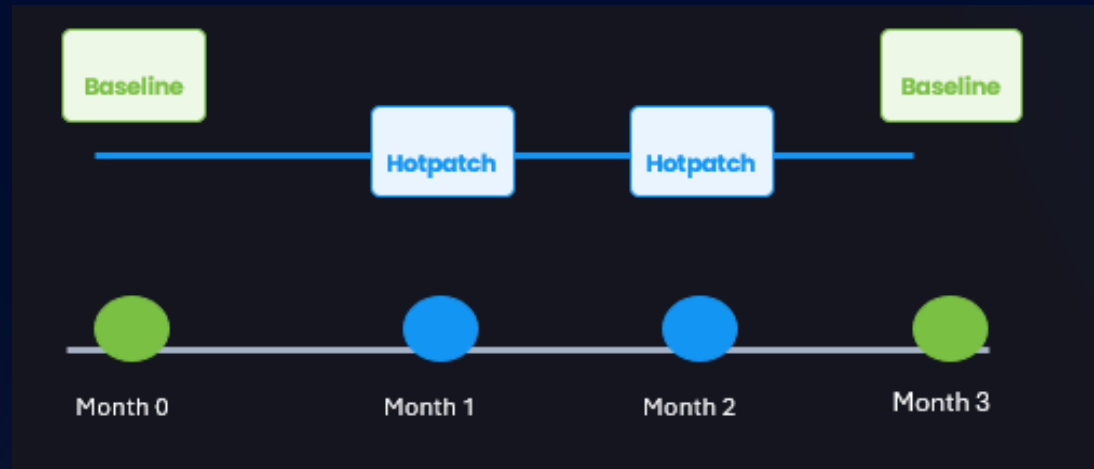
We could enable Hotpatch to ensure our devices won't reboot every month

Automatic update deployment settings \*

Apply the latest cumulative quality updates for security  Allow  ⓘ

When available, apply without restarting the device ("hotpatch").  Allow

[Learn more about updating without restarts.](#)



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

# Hotpatch



Or we just wait until Hotpatch becomes the default... (12 May)

Tenant settings    Actions

---

**When available, apply updates without restarting the device ("Hotpatch")**

Hotpatch updates are Monthly B release security updates that install and take effect without requiring you to restart the device. By minimizing the need to restart, these updates help ensure faster compliance, making it easier for organizations to maintain security while keeping workflows uninterrupted. Disabling this setting will change the default behavior for your devices

Configuration set through update policy will overwrite the default behavior. If you want to include or exclude specific groups of devices [create a policy](#)

Allow

We can opt out if we want...

# Hotpatch



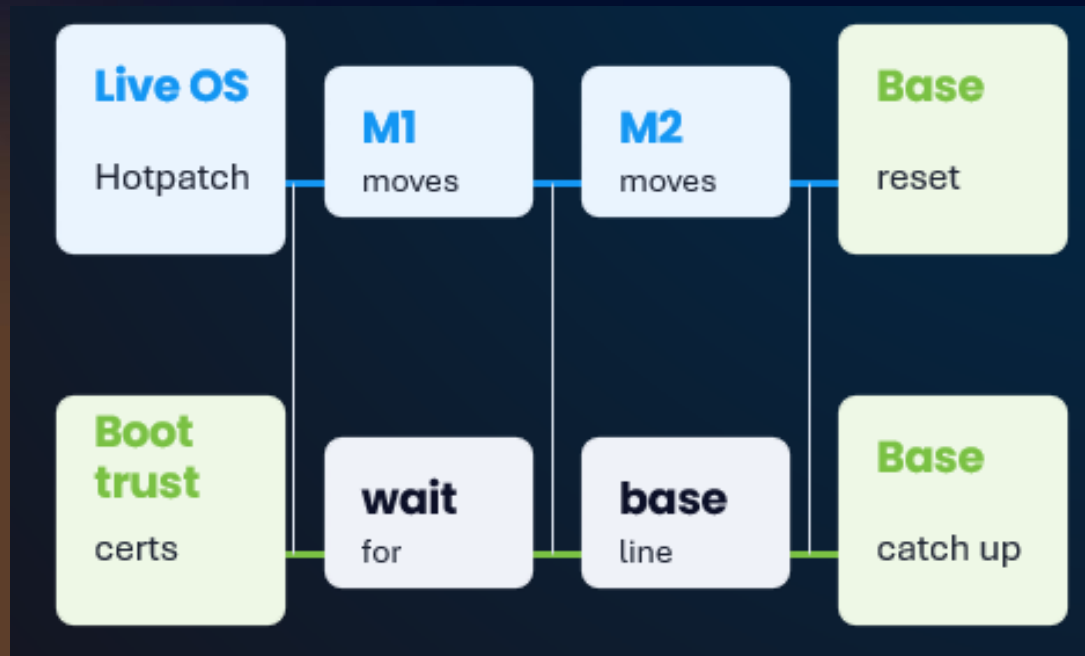
# Hotpatch



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.

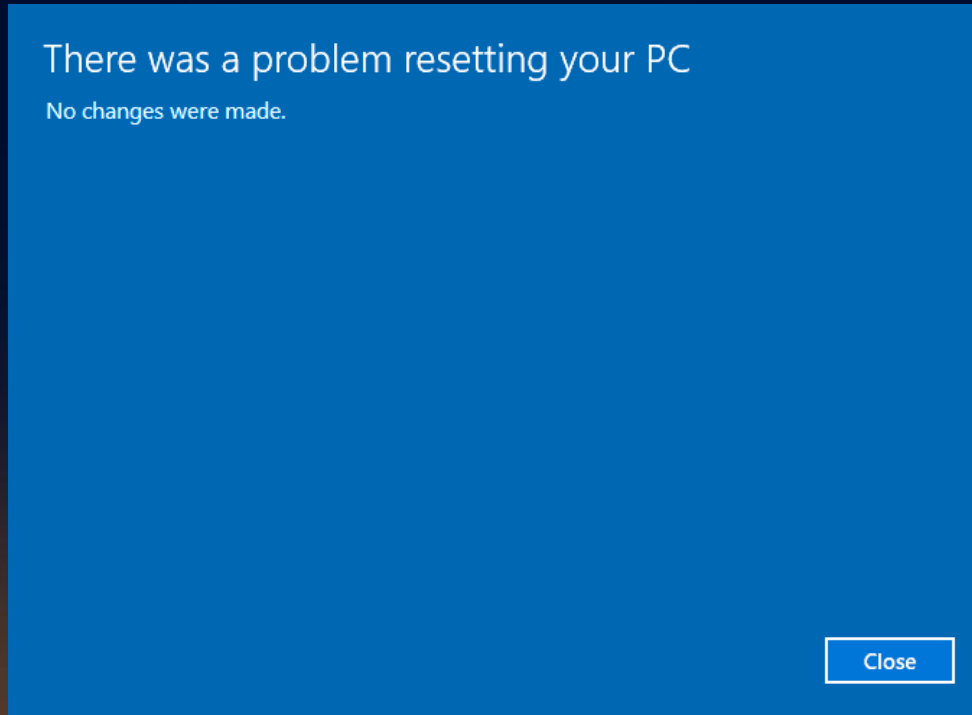
# Hotpatch

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: PSEFX
```



# Advise

**Automatic update deployment settings**

Apply the latest cumulative quality updates for security Allow

When available, apply without restarting the device ("hotpatch"). Allow

[Learn more about updating without restarts.](#)

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

**1 Assignments** 2 Review + save

Included groups

Add groups

Groups	Status	Group Members	Remove
Ring1_PROD_Hotpatch_required	Active	0 devices, 0 users	<a href="#">Remove</a>




# Intune Certificate

# Intune MDM Device CA



The Intune MDM certificate is also going to expire.

 **Certificate Information**

---

**This certificate is intended for the following purpose(s):**

- Proves your identity to a remote computer

---

**Issued to:** Microsoft Intune MDM Device CA

**Issued by:** Microsoft Intune Root Certification Authority

**Valid from** 5/5/2023 **to** 5/5/2026



# 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 CERTIFICATE EXPIRE!**

**Intune**  
**! CERTIFICATE EXPIRE!**

**THIS IS FINE**

# Intune MDM Device CA



Error	10/24/2025 7:28:28 AM	DeviceManagement-Enterpri...	1
Error	10/24/2025 7:28:28 AM	DeviceManagement-Enterpri...	5
Error	10/24/2025 7:28:28 AM	DeviceManagement-Enterpri...	5
Information	10/24/2025 7:28:28 AM	DeviceManagement-Enterpri...	
Information	10/24/2025 7:28:17 AM	DeviceManagement-Enterpri...	

---

Event 52, DeviceManagement-Enterprise-Diagnostics-Provider

General Details

MDM Enroll: Server Returned Fault/Code/Subcode/Value=(UserLicense) Fault/Reason/Text=(Failed to issue token: UserValidation).

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



**Aliases**

Username

Domains

OLD DOMAIN

NEW DOMAIN

---

rudy@wvdcloud.nl

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-78C7-460F-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



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

```
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);
    }
}
```

```
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/enrollmentserver/discovery.svc</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@o1domain.com</E
<RequestVersion>7.0</RequestVersion><DeviceType>CIMClient_Windows</DeviceType><ApplicationVersion>10.0.26200.7171</ApplicationVersion></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 Device CA Issue 2



```
Provider Name: Bit4id UKC Service Provider
Provider Name: Bit4id Universal Middleware Provider
Provider Name: Microsoft Base Cryptographic Provider v1.0
Provider Name: Microsoft Base DSS and Diffie-Hellman Cryptographic Pr
Provider Name: Microsoft Base DSS Cryptographic Provider
Provider Name: Microsoft Base Smart Card Crypto Provider
Provider Name: Microsoft DH SChannel Cryptographic Provider
Provider Name: Microsoft Enhanced Cryptographic Provider v1.0
Provider Name: Microsoft Enhanced DSS and Diffie-Hellman Cryptographi
Provider Name: Microsoft Enhanced RSA and AES Cryptographic Provider
Provider Name: Microsoft RSA SChannel Cryptographic Provider
Provider Name: Microsoft Strong Cryptographic Provider
Provider Name: Microsoft Software Key Storage Provider
Provider Name: Bit4id Key Storage Provider
Provider Name: Microsoft Passport Key Storage Provider
Provider Name: Microsoft Platform Crypto Provider
```

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
```

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?

```
if (StringCchPrintfW(a7, 0x100, L"%s%d", L"ConfigMgrEnrollment", index);
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 = OMARegistryGetString(v28, 0i64, L"DMPCertThumbPrint", psz, 0x2Au);
v37 = SysAllocString(psz);
```

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



# Last Check-In

# Last Check-In



Windows | Windows devices

Search

Refresh Export Columns Bulk device actions

Windows devices

Monitor

Device onboarding

- Windows 365
- Enrollment

Manage devices

- Configuration
- Compliance
- Scripts and remediations
- Group Policy analytics
- eSIM cellular profiles (preview)

Manage updates

Search OS: Windows, Windows Mobile, Windows Holographic Add filters

Device name	Ownership	Primary user UPN	Last check-in
P-5CD13263WD	Corporate		11/20/2025, 10:13 AM
P-5CD147L79C	Corporate		11/03/2025, 03:21 PM
P-5CD9397SM7	Corporate		11/07/2025, 12:42 PM
P-5CD127B80T	Corporate		11/20/2025, 01:19 PM
P-5CD2288D0C	Corporate		11/20/2025, 10:12 AM
P-5CD127B84Q	Corporate		11/20/2025, 11:24 AM
P-5CD24972ST	Corporate		11/18/2025, 05:01 PM
P-5CD211FN22	Corporate		11/19/2025, 01:57 PM

**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
[blurred]	11/20/2025, 10:13 AM	04/29/2025, 11:43 PM
[blurred]	11/03/2025, 03:21 PM	05/10/2025, 11:12 PM
[blurred]	11/07/2025, 12:42 PM	07/14/2025, 08:50 AM
[blurred]	11/20/2025, 01:19 PM	07/16/2025, 01:12 AM
[blurred]	11/20/2025, 10:12 AM	07/19/2025, 09:35 PM
[blurred]	11/20/2025, 11:24 AM	07/20/2025, 03:15 AM
[blurred]	11/18/2025, 05:01 PM	07/20/2025, 05:31 PM
[blurred]	11/19/2025, 01:57 PM	07/22/2025, 06:08 PM
[blurred]	10/01/2025, 09:21 AM	07/23/2025, 04:55 PM
[blurred]	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
  "BackCompatRetrvDisabled"=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

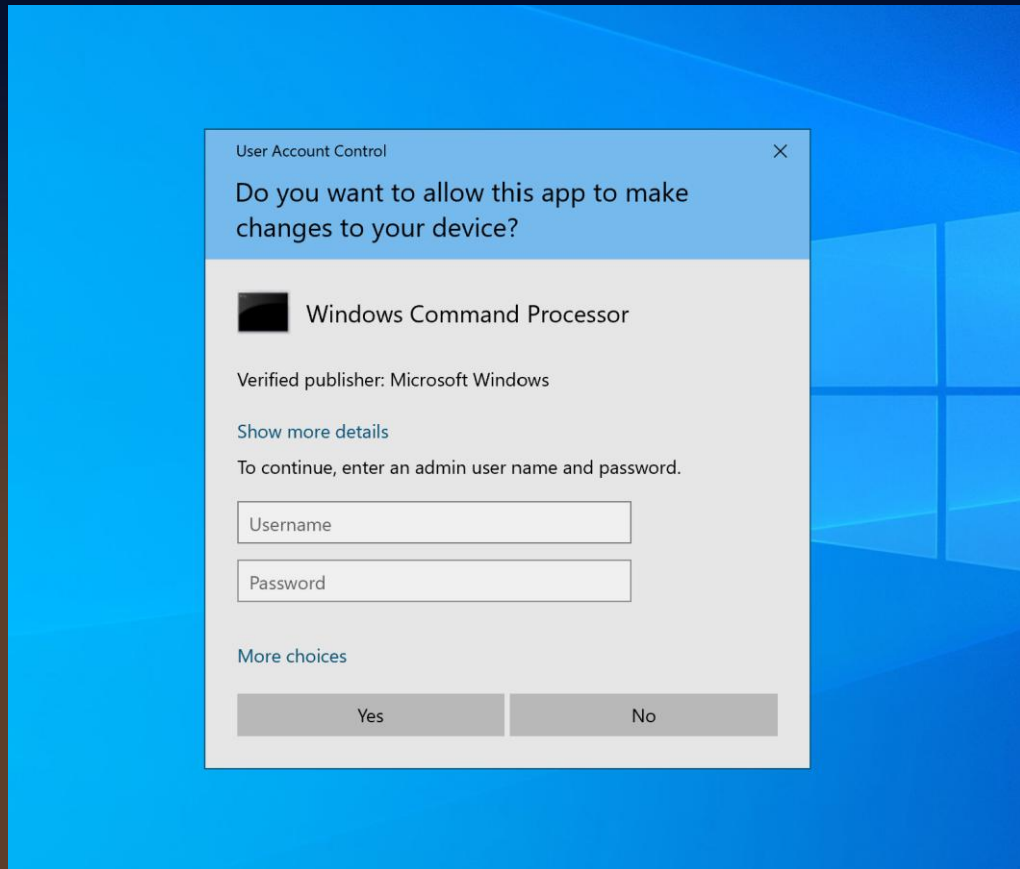


# Local Administrator Protection

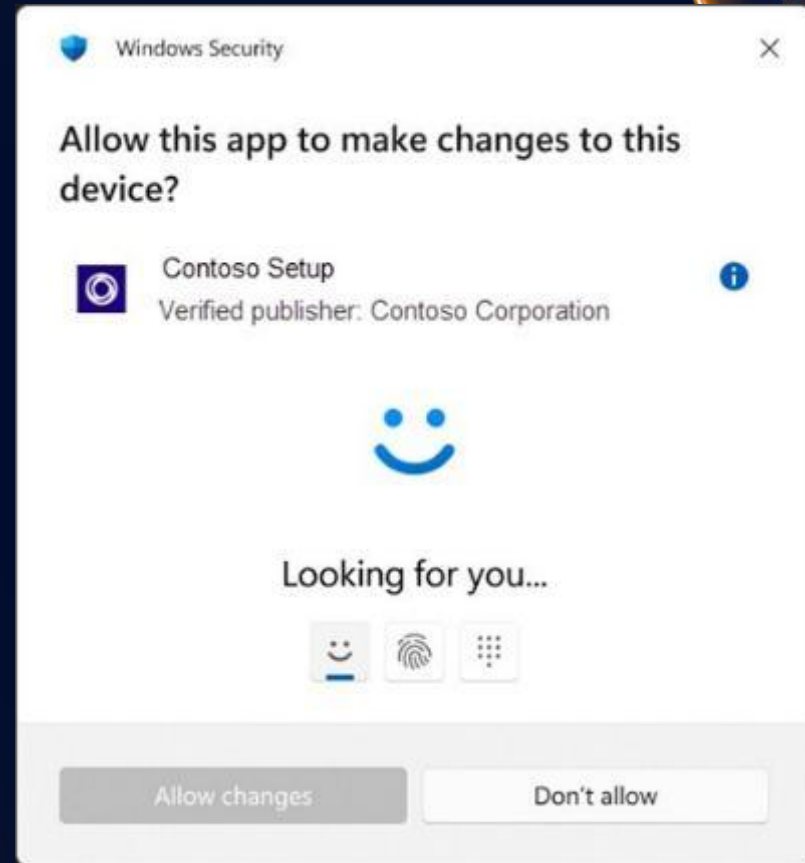
# Local Administrator Protection



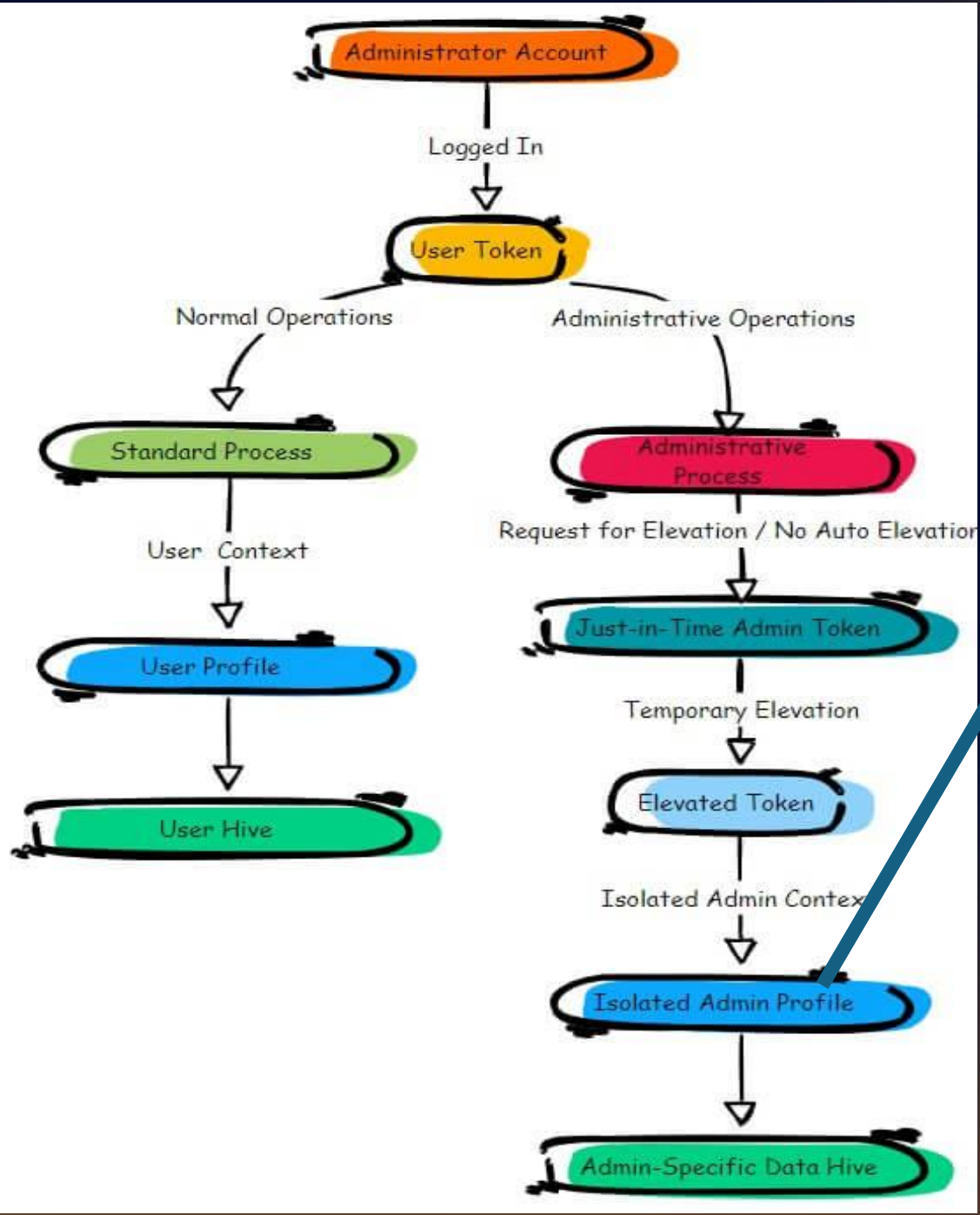
**In the Past: UAC (CLARK KENT MODE)**



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

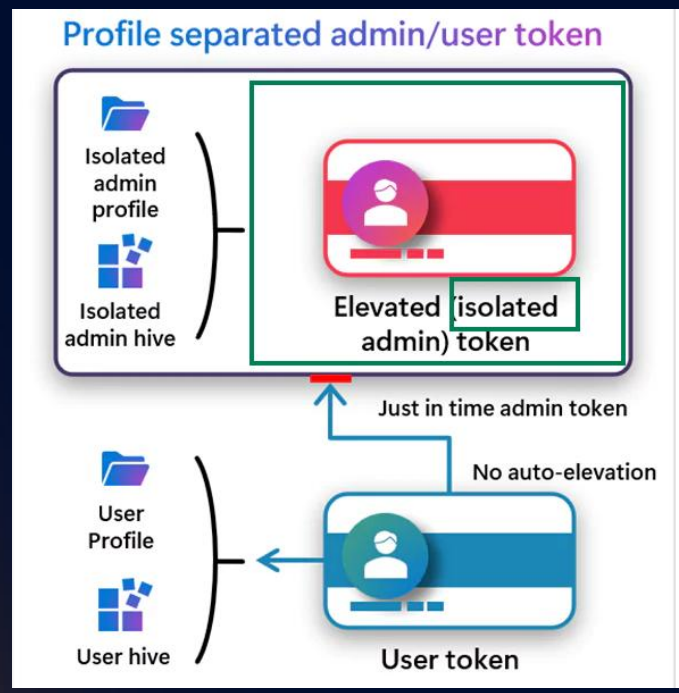


**Now!: Administrator Protection  
(to secure your local admin)**



```

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



# Local Administrator Protection



Basics Configuration settings Scope tags Assignments Review + create

+ Add settings

Local Policies Security Options Remove category

50 of 52 settings in this category are not configured

User Account Control Type Of Admin Approval Mode (Windows Insiders only) Admin Approval Mode with Administrator protection

User Account Control Behavior Of The Elevation Prompt For Administrator Protection (Windows Insiders only) Prompt for credentials on the secure desktop

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...

Windows Security

- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control
- Device security
- Device performance & health
- Family options
- Protection history

Account protection

Security for your account and sign-in.

Windows Hello

Windows Hello is set up for faster and more secure sign-in.

Dynamic lock

Dynamic lock is not set up, and is available on your device.

**Administrator protection**

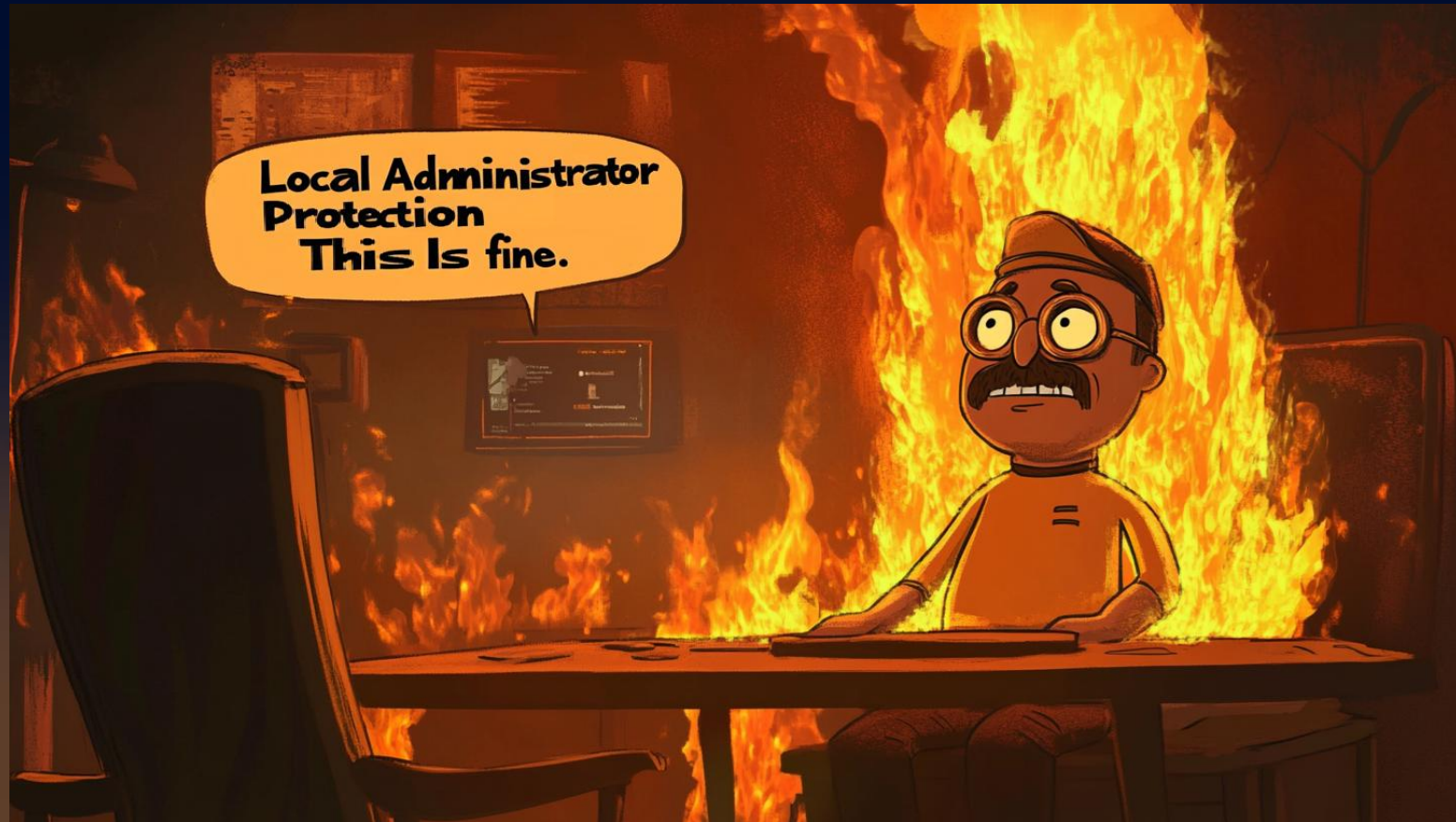
Administrator protection is on. Keep it on to safeguard privileged access.

Administrator protection settings

Learn more

# 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.

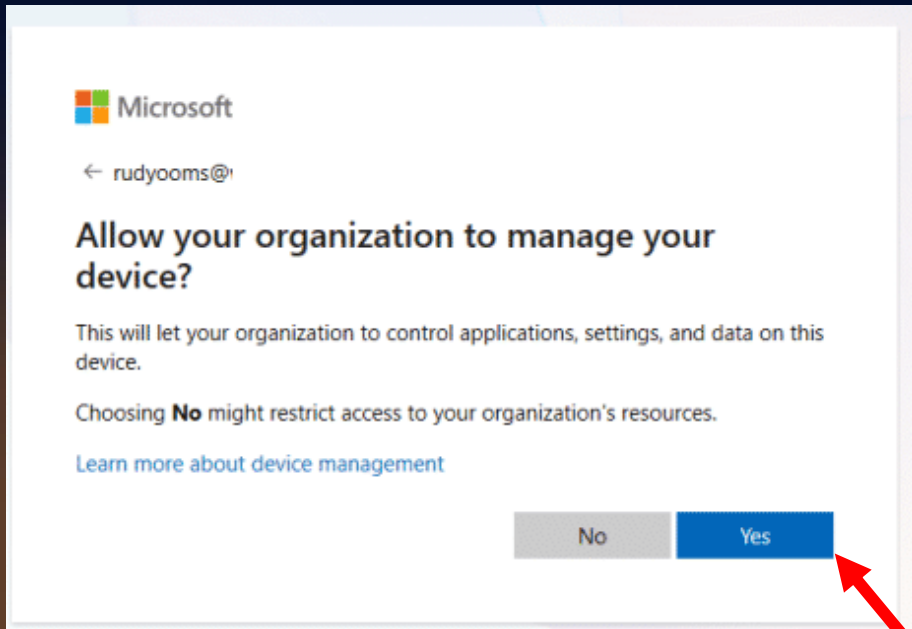


# Disable MDM Enrollment When Adding a Work or School Account on Windows

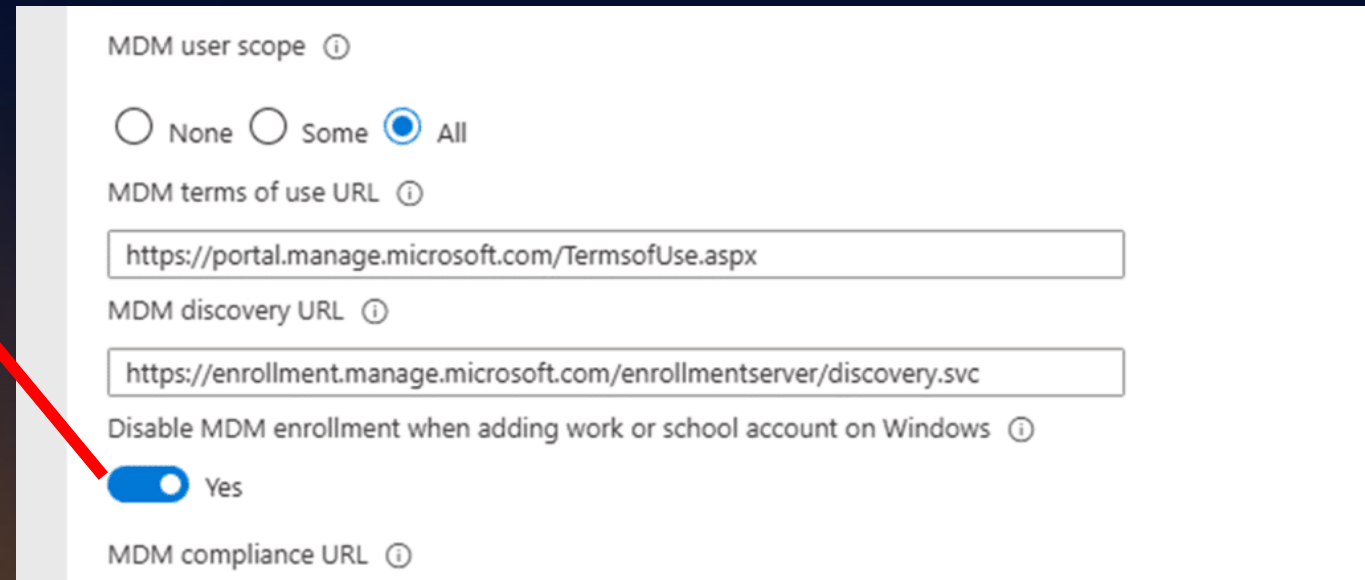
# Disable MDM Enrollment



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



## IsMDMEnrollmentDuringRegistrationDisabled

GET beta https://graph.microsoft.com/beta/policies/mobileDeviceManagementPolicies/0000000a-0000-0000-c000-000000000000/

Request Body Request Headers Modify Permissions Access token

Key	Value	Actions
-----	-------	---------

OK - 200 - 594 ms

Response preview Response headers Code snippets Toolkit component Adaptive cards

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#policies/mobileDeviceManagementPolicies/$entity",
  "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For example, mobileDeviceManagementPolicies('<guid>)?$select=isMdmEnrollmentDuringRegistrationDisabled,appliesTo",
  "id": "0000000a-0000-0000-c000-000000000000",
  "appliesTo": "all",
  "complianceUrl": "https://portal.manage.microsoft.com/?portalAction=Compliance",
  "description": "Device Management Policy for Microsoft Intune",
  "discoveryUrl": "https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc",
  "displayName": "Microsoft Intune",
  "isValid": true,
  "termsOfUseUrl": "https://portal.manage.microsoft.com/TermsOfUse.aspx",
  "isMdmEnrollmentDuringRegistrationDisabled": false
}
```

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

PATCH beta https://graph.microsoft.com/beta/policies/mobileDeviceManagementPolicies/0000000a-0000-0000-c000-000000000000/

Request Body Request Headers Modify Permissions Access token

```
{"isMdmEnrollmentDuringRegistrationDisabled": true}
```

Is this smart to do in Prod???

# Disable MDM Enrollment



# Disable MDM Enrollment

Device was registered to call4cloud first!

The screenshot displays a Windows environment with several windows open. On the left, a console window shows the configuration for two work accounts. The first account, 'Work Account 1', is highlighted with a green box and has its 'WorkplaceMdmUrl' set to 'https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc'. The second account, 'Work Account 2', is highlighted with a red box and has its 'WorkplaceMdmUrl' set to 'call4cloud'. In the center, the Windows Settings app is open to 'Accounts > Access work or school', showing two work accounts: 'info@call4cloud.nl' (highlighted with a red box) and 'rudyooms@vwdcloud.nl' (highlighted with a green box). Both accounts show 'Managed by Rudy's DLL LAB'. On the right, the Windows Event Viewer is open, showing a log of events. An event titled 'MDM Enroll: Certificate enrollment response parsed successfully.' is visible, with a log name of 'Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Enrollment'. A context menu is open over this event, showing options like 'Event Properties' and 'Attach Task To This Event...'. A small 'DLL' logo is visible in the top right corner of the overall image.

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

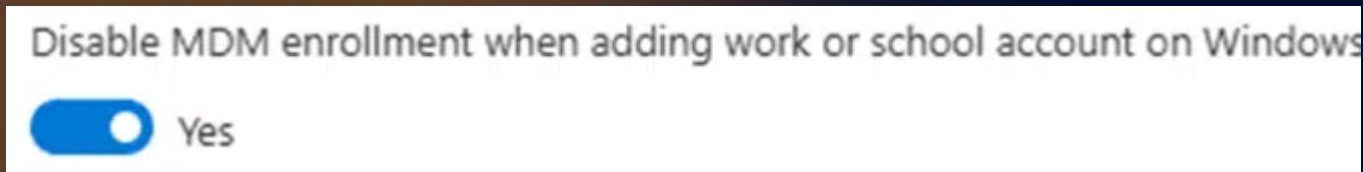
# Disable MDM Enrollment



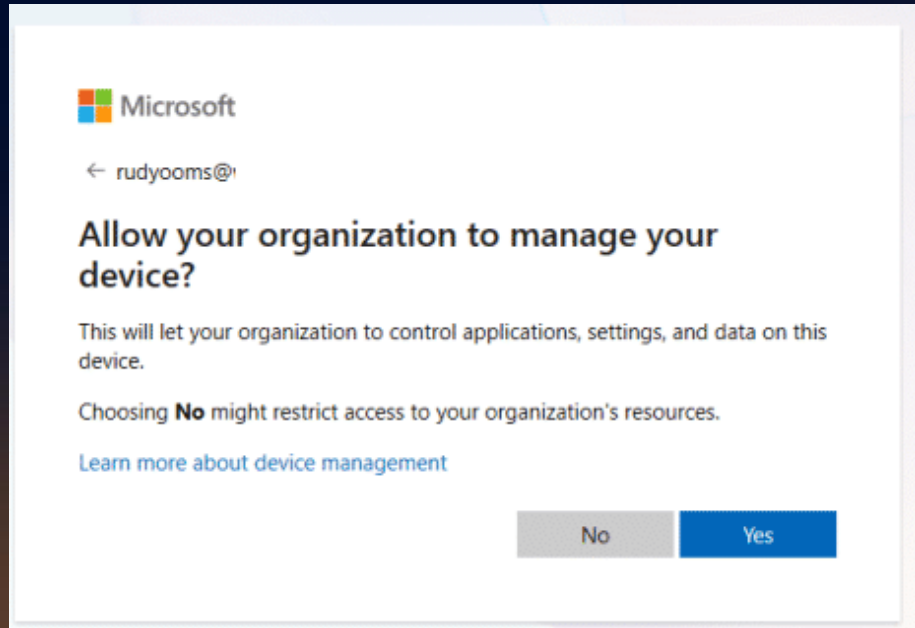
```
/common/SAS/EndAuth?authMethodId=PhoneAppNotificatio... no-stor... application/json; charset=utf-8
/OneCollector/1.0/?cors=true&content-type=application/x-j... public, ... application/json
/OneCollector/1.0/?cors=true&content-type=application/x-j... application/json
tsfe.trafficshaping.dsp.mp.microsoft.com:443
/TrafficShaping/ContentRegulationV2.asmx private text/xml; charset=utf-8
/common/SAS/EndAuth?authMethodId=PhoneAppNotificatio... no-stor... application/json; charset=utf-8
/common/SAS/EndAuth?authMethodId=PhoneAppNotificatio... no-stor... application/json; charset=utf-8
tsfe.trafficshaping.dsp.mp.microsoft.com:443
/TrafficShaping/ContentRegulationV2.asmx private text/xml; charset=utf-8
/common/SAS/EndAuth?authMethodId=PhoneAppNotificatio... no-stor... application/json; charset=utf-8
/common/SAS/EndAuth?authMethodId=PhoneAppNotificatio... no-stor... application/json; charset=utf-8
tsfe.trafficshaping.dsp.mp.microsoft.com:443
/IsMdmEnrollmentRequired? IsMdmEnrollmentRequired: true
/common/SAS/ProcessAuth?cxhflow=TB&cxhplatformversio... no-stor... text/html; charset=utf-8
tsfe.trafficshaping.dsp.mp.microsoft.com:443
/TrafficShaping/ContentRegulationV2.asmx private text/xml; charset=utf-8
/OneCollector/1.0/?cors=true&content-type=application/x-j... application/json
tsfe.trafficshaping.dsp.mp.microsoft.com:443
```

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

Home > Devices | Enrollment >

### Microsoft Intune

MDM user scope ⓘ

None  Some  All

MDM terms of use URL ⓘ

MDM discovery URL ⓘ

MDM compliance URL ⓘ

[Restore default MDM URLs](#)

## Preferred?

Home > Devices | Enrollment >

### Microsoft Intune

MDM user scope ⓘ

None  Some  All

Groups

2 groups selected

MDM terms of use URL ⓘ

MDM discovery URL ⓘ

MDM compliance URL ⓘ

[Restore default MDM URLs](#)

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



```
Tenant Details
-----+
TenantName : Patch My PC          DSREGCMD /status
TenantId   : 179783df-131e-4d00-8303-6f66c0fa4bfb
AuthCodeUrl : https://login.microsoftonline.com/
AccessTokenUrl : https://login.microsoftonline.com/
MdmUrl      : https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc
MdmTouUrl   : https://portal.manage.microsoft.com/TermsOfUse.aspx
MdmComplianceUrl : https://portal.manage.microsoft.com/?portalAction=Compliance
SettingsUrl : eyJVcmIzIjpbImh0dHBzOi8va2FpbGFuaS5vbmUubWljcm9zb2Z0LmNvbS8
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

A screenshot of the Windows Registry Editor showing the path HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\CloudDomainJoin\TenantInfo\b79783df-131e-4d00-8303-6f66c0fa4bfb. The right pane displays a list of registry values for the selected key.

Name	Type	Data
(Default)	REG_SZ	(value not set)
MdmComplianceUrl	REG_SZ	https://portal.manage.microsoft.com/?portalAction=Compliance
MdmEnrollmentUrl	REG_SZ	https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc
MdmTermsOfUseUrl	REG_SZ	https://portal.manage.microsoft.com/TermsOfUse.aspx
NgcEndpoint	REG_SZ	https://enterpriseregistration.windows.net/EnrollmentServer/key/
NgcResourceId	REG_SZ	urn:ms-drs:enterpriseregistration.windows.net

# 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

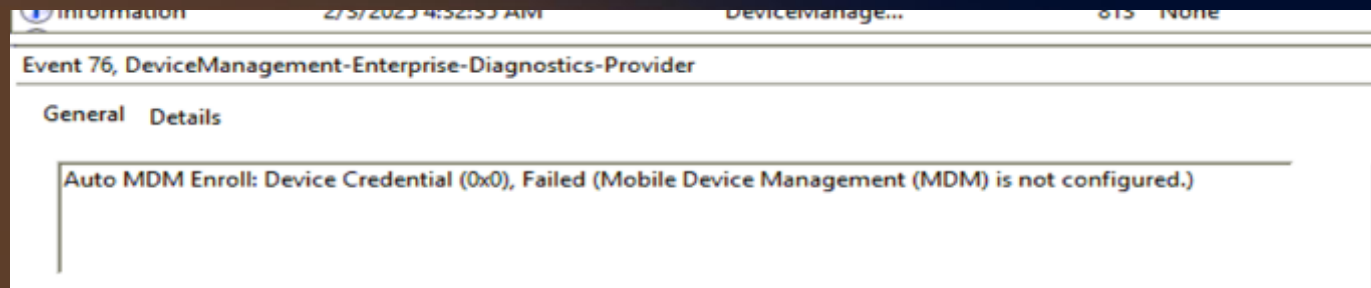


**Autopilot skipping the ESP... because Automatic MDM Enrollment didn't work!  
And.... Somehow the MDM urls are empty?**

```
TenantName :  
TenantId :  
AuthCodeUrl : https://login.microsoftonline.com/ /oauth2/authorize  
AccessTokenUrl : https://login.microsoftonline.com/ /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




Microsoft Entra admin center

Home > Mobility (MDM and WIP) >

## Mobility (MDM and WIP) ...

+ Add application   Refresh   Manage view ▾   Got feedback?

Name ↑

 Microsoft Intune
------------------------------------------------------------------------------------------------------

  
**Checking the MDM Policies in Entra**

Home > Mobility (MDM and WIP) >

## Microsoft Intune ...

MDM user scope ⓘ  
 None    Some    All

MDM terms of use URL ⓘ

MDM discovery URL ⓘ

MDM compliance URL ⓘ

[Restore default MDM URLs](#)

# Troubleshooting Automatic Enrollment

Let's use Fiddler to Troubleshoot!

The screenshot shows the Fiddler Web Debugger interface. On the left, a list of intercepted requests is displayed with columns for #, Result, Protocol, Host, and URL. Request 13 is selected. The main pane shows the details for this request, including the request count (1), bytes sent (174), and bytes received (1,127). It also displays the actual performance metrics and response bytes.

#	Result	Protocol	Host	URL
1	200	HTTPS	www.fiddler2.com	/UpdateCheck.aspx?is
2	200	HTTP	Tunnel to	dtzbdy9anri2p.cloudfr
3	200	HTTP	Tunnel to	d6vtbcy3ong79.cloud
4	200	HTTP	Tunnel to	www.telerik.com:443
5	200	HTTP	Tunnel to	www.googleadservice
6	200	HTTP	Tunnel to	static.hotjar.com:443
7	200	HTTP	Tunnel to	cdn.bizible.com:443
8	200	HTTP	Tunnel to	img.en25.com:443
9	200	HTTP	Tunnel to	www.google-analytics
10	200	HTTP	Tunnel to	bat.bing.com:443
11	200	HTTP	Tunnel to	px.ads.linkedin.com:4
12	200	HTTP	Tunnel to	connect.facebook.net
13	200	HTTP	fiddler2.com	/content/GetArticles?c
14	200	HTTP	fiddler2.com	/content/GetBanner?c
15	200	HTTPS	d6vtbcy3ong79.do...	/fonts/2.0.0/faktslabp
16	200	HTTPS	dtzbdy9anri2p.dou...	/cache/ef8f4cb3abbb:
17	200	HTTPS	www.telerik.com	/RestApi/personalitati
18	304	HTTPS	www.googleadservi...	/pagead/conversion_
19	304	HTTPS	cdn.bizible.com	/scripts/bizible.js
20	200	HTTPS	connect.facebook.net	/signals/config/14440:
21	204	HTTPS	bat.bing.com	/action/0?ti=5614127
22	200	HTTPS	www.google-analyti...	/gtm/js?id=GTM-PQP6
23	200	HTTPS	static.hotjar.com	/c/hotjar-66905.js?sv
24	200	HTTP	Tunnel to	googleads.g.doublecl

```
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..)

The screenshot shows the 'AppContainer Loopback Exemption Utility' dialog box. It contains a message about Windows security restrictions and three buttons: 'Refresh', 'Exempt All', and 'Save Changes'. The 'Exempt All' button is highlighted with a red box.

The screenshot shows the 'Options' dialog box in Fiddler, with the 'HTTPS' tab selected. The 'Capture HTTPS CONNECTS' checkbox is checked. The 'Decrypt HTTPS traffic' checkbox is also checked, and the dropdown menu below it is set to '...from all processes'. Other options like 'Ignore server certificate errors (unsafe)' and 'Check for certificate revocation' are unchecked.

<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



```
Transform: From Base64 [x] View bytes Encodings... Save Output: As Session To File... Send output to input [x]
{"typ":"JWT","alg":"none"}
{"aud":"29d9ed98-a469-4536-ade2f981bc1d605e","iss":"https://sts.windows.net/02ad5f9c-3696-477b-8cb3-
bba4e0a9ac9c/","iat":1678373194,"nbf":1678373194,"exp":1678377094,"amr":
["pwd"],"domain_dns_name":"mmsmoa.local","domain_netbios_name":"MMSMOA","given_name":"rudy","ipaddr":"185.44.169.130","mdm_compliance_url":"https://portal.mana
ge.microsoft.com/portalAction=Compliance","mdm_enrollment_url":"https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc","mdm_terms_of_use_url":"https://portal.manage.micr
osoft.com/TermsOfUse.aspx","name":"rudy","oid":"f8c2d8f1-9988-4b17-afdd-429ced8dd1f9","onprem_sam_account_name":"rudy","onprem_sid":"S-1-5-21-2607092747-
1301076339-1591193098-1103","puid":"1003200274312431","pwd_url":"https://portal.microsoftonline.com/ChangePassword.aspx","rh":"0.AToAnF-
ApY2e0eMs5uk4KmsnJt2SlppDZFreL5gbwdYF46ADE","sid":"S-1-12-1-4279119295-1259845936-977460655-434048461","sub":"YoshH11daAAy-
gCjuHsBAyxkU5gRBsaxJtgKKh7B_i4M","tenant_display_name":"wvdcloud","tenant_region_scope":"EU","tid":"02ad5f9c-3696-477b-8cb3-
bba4e0a9ac9c","tokenAutologonEnabled":1,"unique_name":"rudy@wvdcloud.nl","upn":"rudy@wvdcloud.nl","user_setting_sync_url":"eyJVcm1zIjpbImh0dHBzOi8va2FpbGFuaT
Yub25iLm1pY3Jvc29mdC5jb20vliwiaHR0cHM6Ly9rYW5pNy5vbmUubWljcm9zb2Z0LmNvbS8iXX0=","ver":"1.0"}
token_type=bearer
```



# Troubleshooting Automatic Enrollment

## Using Graph to find the MDM Policies

GET beta https://graph.microsoft.com/beta/policies/mobileDeviceManagementPolicies Run query

OK - 200 - 991 ms

Response preview Response headers Code snippets Toolkit component Adaptive cards Expand

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#mobilityManagementPolicies",
  "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For more information, see https://aka.ms/odata-select",
  "value": [
    {
      "id": "0000000a-0000-0000-c000-000000000000",
      "appliesTo": "all",
      "complianceUrl": "https://portal.manage.microsoft.com/?portalAction=Compliance",
      "description": "Device Management Policy for Microsoft.Intune",
      "discoveryUrl": "https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc",
      "displayName": "Microsoft.Intune",
      "isValid": true,
    },
    {
      "id": "f6ddc682-c885-45e3-beba-67f8eb99de56",
      "appliesTo": "all",
      "complianceUrl": null,
      "description": null,
      "discoveryUrl": null,
      "isValid": false,
    }
  ]
}
```

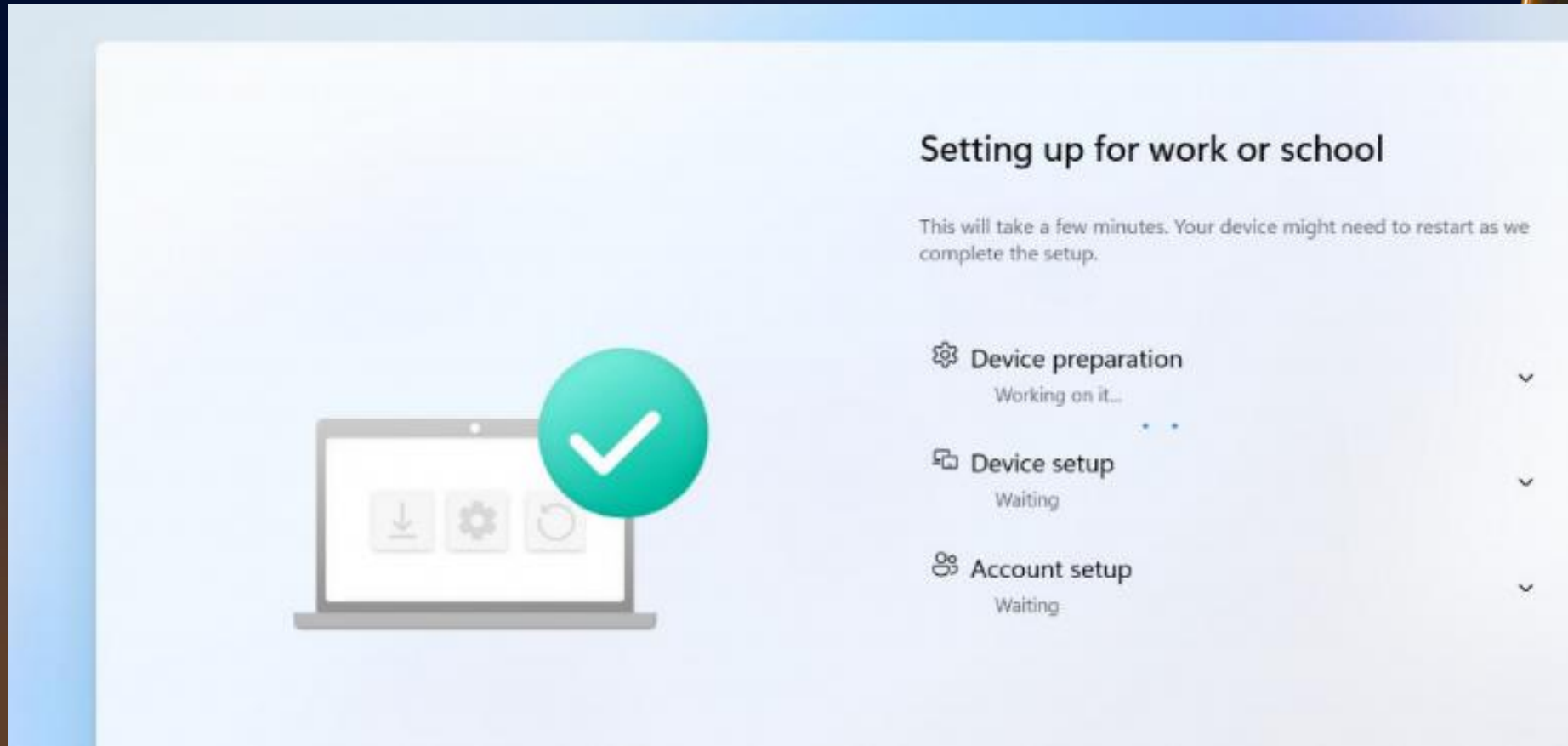
**The MDM Policy**

**The Broken one**

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

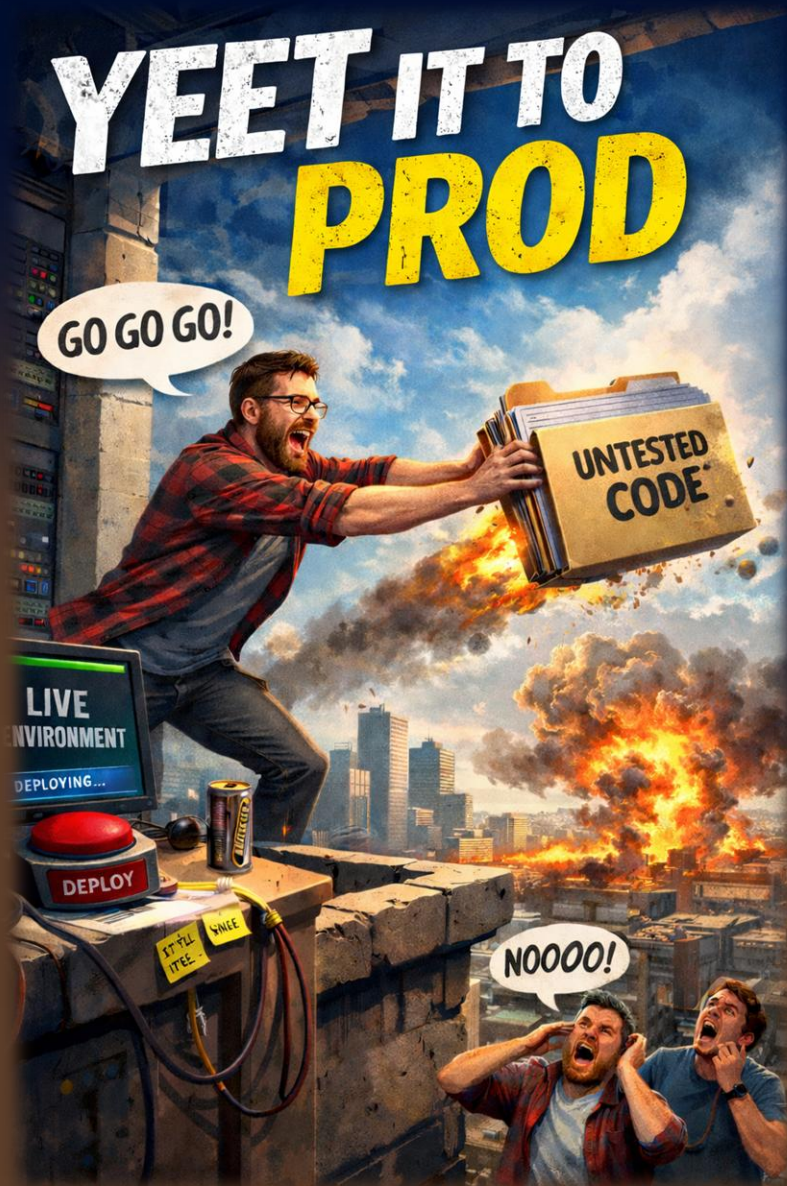


# Troubleshooting Automatic Enrollment



- 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!