



Forget Hybrid;  
Go Entra Joined!

# Agenda

- **What is Entra Hybrid Join?**
  - Signing into multiple domains at once
- **When is Entra Hybrid Join a good thing?**
  - Transitioning to cloud-based management
- **Entra Hybrid Join and Windows Autopilot**
  - Here is where the complexity starts
- **Entra Joined devices will never work for us**
  - We have a highly complex environment with on-premises apps and printing requirements
- **Strong Auth Methods – Windows Hello for Business**
  - Considerations when implementing password less solutions
- **Entra Hybrid Join to Entra Join**
  - Are migrations possible?

# Presented By

## Maurice Daly

Microsoft Enterprise Mobility MVP since 2017,  
25+ years experience in the IT industry, in both in-house and consultancy roles

Running user group events and webinars and sharing content on the MSEndpointMgr.com blog with an annual subscription of 1.5m readers

X @modaly\_it





# Presented By

## Gerry Hampson

Microsoft Enterprise Mobility MVP since 2015

Years and years and years 😊 experience in the IT industry

Helping the community where I can with blog posts and speaking at events



X @GerryHampson

# Hybrid Entra Joined

The “easy” option





# Hybrid Entra Joined

- **What is Entra Hybrid Joined?**

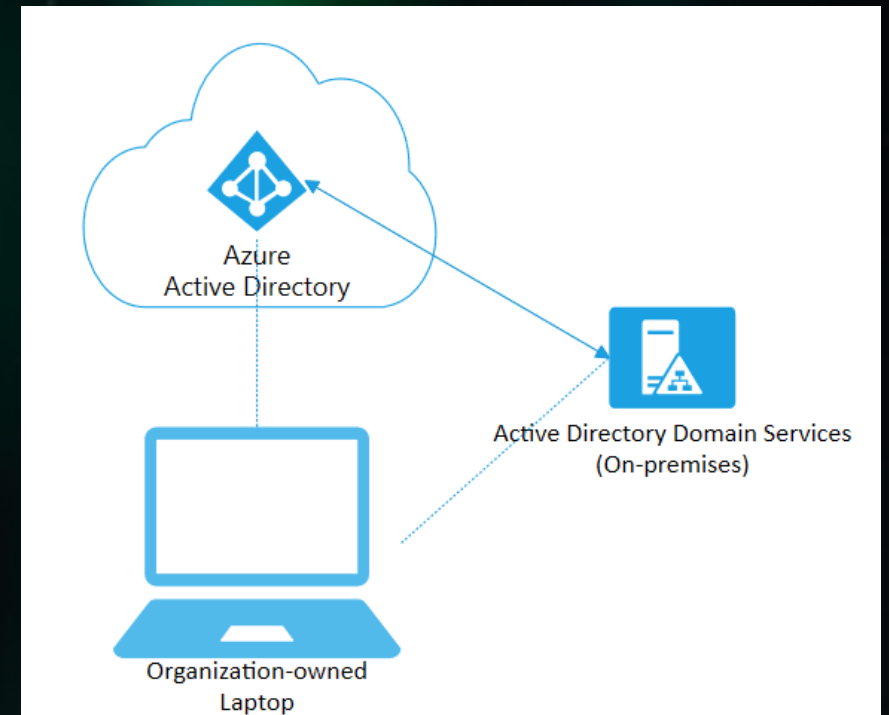
Hybrid Entra Joined is a term used for devices which are joined to an on-premises Active Directory, and also joined to a Microsoft Entra tenant

- **Supported Operating Systems?**

- Windows 8.1, 10 & 11
- Windows Server 2008R2 – 2022

- **Benefits?**

- Single Sign On (SSO) to both cloud and on-premises resources / applications
- Additional auditing in the form of Windows Sign-In events in Entra
- Leverage join states



# Hybrid Entra Joined - Benefits

☒ Grant access

- ☐ Require multifactor authentication ⓘ
- ☐ Require authentication strength ⓘ
- ☐ Require device to be marked as compliant ⓘ
- ☒ Require Microsoft Entra hybrid joined device ⓘ

⚠ Don't lock yourself out! Make sure that your device is Microsoft Entra hybrid joined. [Learn more](#) ↗

## Create filter ...

✓ Basics **2 Rules** ⓘ Scope tags ⓘ Review + create

You can use the rule builder or rule syntax text box to create or edit the filter rule. [Learn more about creating filters](#) ↗

And/Or	Property	Operator	Value
<input type="text"/>	deviceTrustTyp... ⓘ	Equals ⓘ	Hybrid Azure AD j... ⓘ

[+ Add expression](#)

Rule syntax [Edit](#)

```
(device.deviceTrustType -eq "Hybrid Azure AD joined")
```

# Hybrid Entra Joined – Other Benefits

- Additional benefits for initially going Hybrid;
  - Allows you to co-manage domain-joined Configuration Manager managed clients (Hybrid is a pre-requisite)
  - Automatic Intune enrollment through Group Policy delivered settings (Hybrid is a pre-requisite)
  - Entra Self Service Password Reset (SSPR), providing self-service password reset to end users\*
    - Password initially written to Entra ID
    - Password written back down to Active Directory where password write-back is enabled within Azure AD Connect

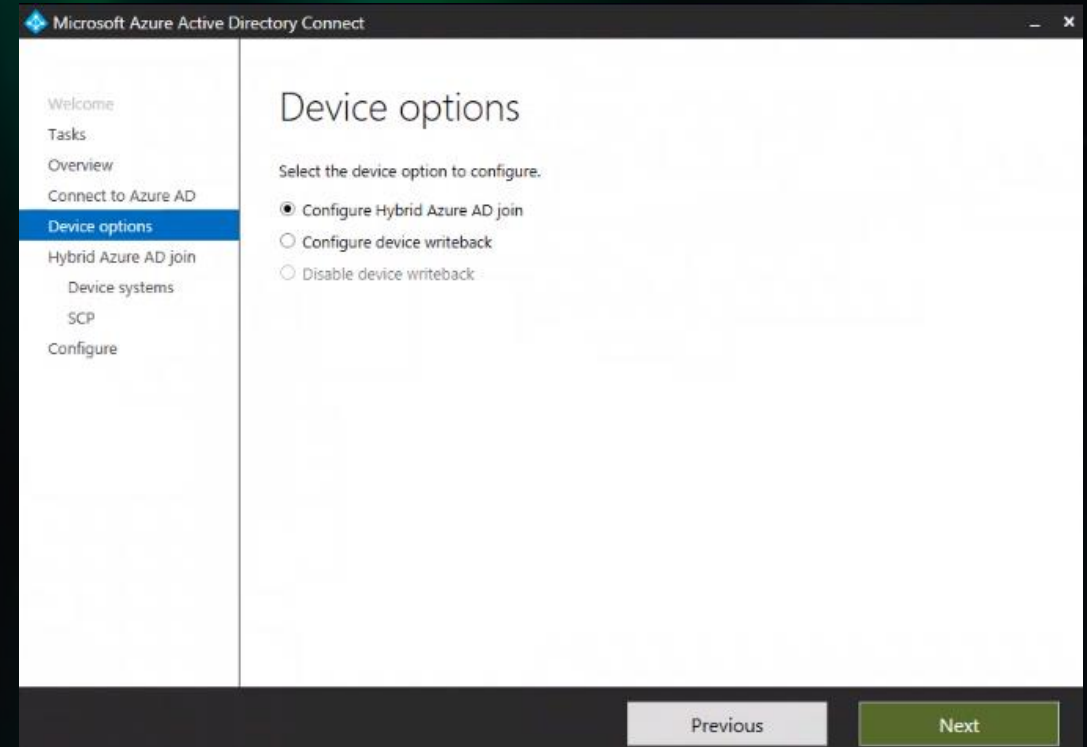




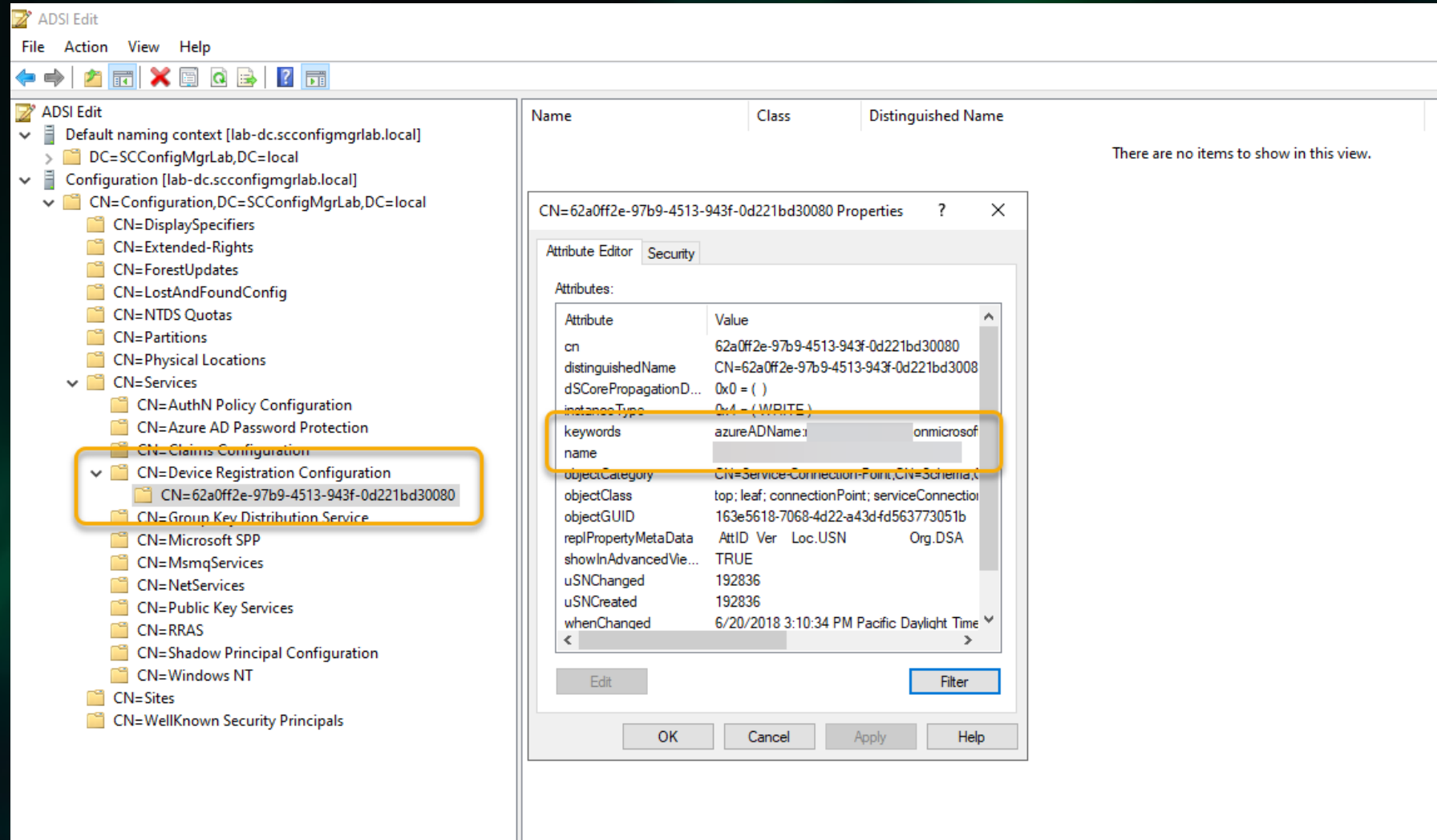
# Hybrid Entra Joined – Configuration

- Hybrid Join is simple

- Open Entra ID Azure AD Connect
- Click on “Configure device options”
- Sign into your Entra ID environment using either a Global or Hybrid Identity Admin role enabled account
- Select “Configure Hybrid Azure AD join”
- Select the OU’s where devices are located, to sync through to Entra ID
- Using an account with “Enterprise Admin” membership, create the required Service Connection Point (SCP) in Active Directory
- Force a sync and wait..



# Hybrid Entra Joined – Configuration



The screenshot shows the ADSI Edit application. The left pane displays the directory tree with the following structure:

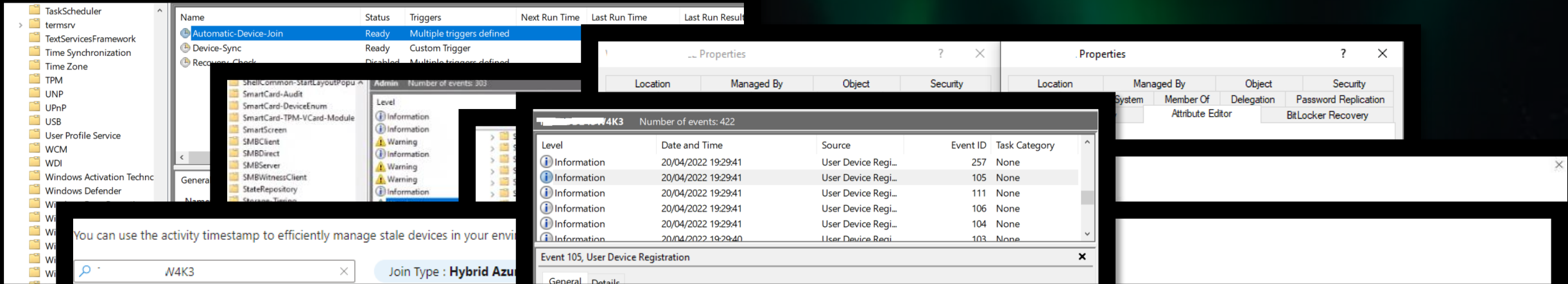
- Default naming context [lab-dc.scconfigmgrlab.local]
  - DC=SCConfigMgrLab,DC=local
  - Configuration [lab-dc.scconfigmgrlab.local]
    - CN=Configuration,DC=SCConfigMgrLab,DC=local
      - CN=DisplaySpecifiers
      - CN=Extended-Rights
      - CN=ForestUpdates
      - CN=LostAndFoundConfig
      - CN=NTDS Quotas
      - CN=Partitions
      - CN=Physical Locations
      - CN=Services
        - CN=AuthN Policy Configuration
        - CN=Azure AD Password Protection
        - CN=Claims Configuration
        - CN=Device Registration Configuration
          - CN=62a0ff2e-97b9-4513-943f-0d221bd30080
          - CN=Group Key Distribution Service
        - CN=Microsoft SPP
        - CN=MsmqServices
        - CN=NetServices
        - CN=Public Key Services
        - CN=RRAS
        - CN=Shadow Principal Configuration
        - CN=Windows NT
      - CN=Sites
      - CN=WellKnown Security Principals

The right pane shows the properties of the selected object, CN=62a0ff2e-97b9-4513-943f-0d221bd30080. The 'Attributes' tab is active, displaying the following table:

Attribute	Value
cn	62a0ff2e-97b9-4513-943f-0d221bd30080
distinguishedName	CN=62a0ff2e-97b9-4513-943f-0d221bd30080
dSCorePropagationD...	0x0 = ( )
instanceType	0x4 = (WRITE)
keywords	azureADName: onmicrosoft
name	
objectCategory	CN=Service-Connection-Point,CN=Schema,CN=Configuration,DC=SCConfigMgrLab,DC=local
objectClass	top; leaf; connectionPoint; serviceConnection
objectGUID	163e5618-7068-4d22-a43d-fd563773051b
replPropertyMetaData	AttID Ver Loc:USN Org:DSA
showInAdvancedVie...	TRUE
uSNChanged	192836
uSNCreated	192836
whenChanged	6/20/2018 3:10:34 PM Pacific Daylight Time

The 'keywords' attribute is highlighted with an orange box. The 'Filter' button is visible at the bottom right of the properties window.

# Hybrid Entra Joined – Flow



The screenshot shows the Windows Task Scheduler and Event Viewer. The Task Scheduler lists several tasks, including 'Automatic-Device-Join', 'Device-Sync', and 'Recovery-Check'. The Event Viewer shows a list of events, including 'Event 105, User Device Registration'.

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
Automatic-Device-Join	Ready	Multiple triggers defined			
Device-Sync	Ready	Custom Trigger			
Recovery-Check	Disabled	Multiple triggers defined			

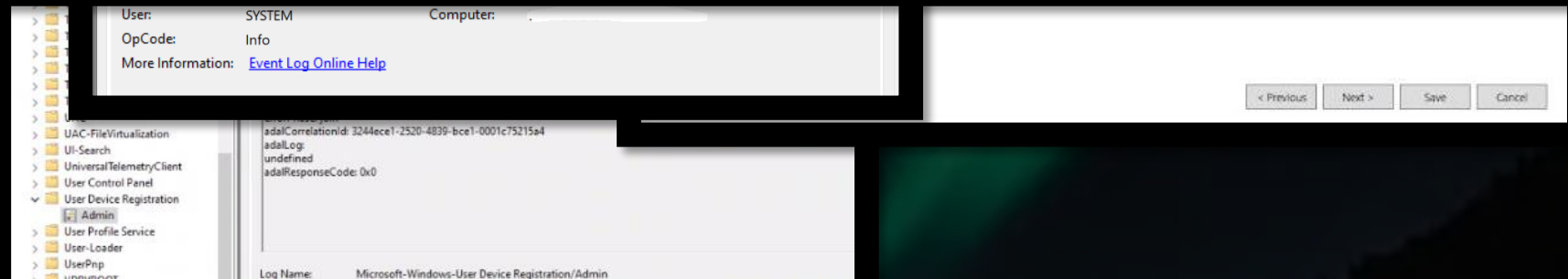
Level	Date and Time	Source	Event ID	Task Category
Information	20/04/2022 19:29:41	User Device Regi...	257	None
Information	20/04/2022 19:29:41	User Device Regi...	105	None
Information	20/04/2022 19:29:41	User Device Regi...	111	None
Information	20/04/2022 19:29:41	User Device Regi...	106	None
Information	20/04/2022 19:29:41	User Device Regi...	104	None
Information	20/04/2022 19:29:40	User Device Regi...	103	None

You can use the activity timestamp to efficiently manage stale devices in your environment. [Learn more](#)

Search: . . . W4K3 Join Type: Hybrid Azure AD joined Add filters

1 devices found

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant	Registered	Activity
W4K3	Yes	Windows	10.0.19044.1766	Hybrid Azure AD join...	N/A	None	N/A	6/24/2022, 7:26:41 PM	6/24/2022, 7:26:44 PM



The screenshot shows the Windows Event Viewer with the 'User Device Registration' log selected. The log entry shows the following details:

- User: SYSTEM
- OpCode: Info
- More Information: [Event Log Online Help](#)
- Log Name: Microsoft-Windows-User Device Registration/Admin



# Verifying Hybrid Entra Join

## Verifying Hybrid Azure AD Join

- Device join state is available in Entra ID
- Locally you can run DSRegCMD /status
- Troubleshoot with DSRegCMD /debug/join



```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\administrator>dsregcmd /status

+-----+
| Device State |
+-----+

AzureAdJoined : YES
EnterpriseJoined : NO
DomainJoined : YES
DomainName : SCCONFIGMGRLAB
Virtual Desktop : NOT SET
Device Name : DESKTOP-1MKCI1U.SCConfigMgrLab.local
```

You can use the activity timestamp to efficiently manage stale devices in your environment. [Learn more](#)

. . . .W4K3						
Join Type : Hybrid Azure AD joined						
Add filters						
1 devices found						
Name	Enabled	OS	Version	Join Type	Owner	
 .W4K3	 Yes	Windows	10.0.19044.1766	Hybrid Azure AD join...	N/A	

```
Administrator: Windows PowerShell

PreReqResult : WillNotProvision

PS C:\WINDOWS\system32> dsregcmd /debug /join
dsregcmd::wmain logging initialized.
dsregcmd::wmain logging initialized.
DsrCmdJoinHelper::Join: ClientRequestId: 4650531f-6c62-454d-945d-c7f8d01ca5fdDsrCmdAccountMgr::IsDomainControllerAvailable: DsGetDcName success { domain: . forest: . domainController: \. }
Iness.ie isDcAvailable:true }
DsrCmdAccountMgr::IsDrsJoined: DsrCmdCertHelper::PrivateKeyAcquireTest Passed 0x00000000.
DsrCmdAccountMgr::IsDrsJoined: DsrCmdCertHelper::PrivateKeyAcquireTest Passed 0x00000000.
PreJoinChecks Complete.
preCheckResult: DoNotJoin
deviceKeysHealthy: YES
isJoined: YES
isDcAvailable: YES
isSystem: YES
keyProvider: Microsoft Platform Crypto Provider
keyContainer: 86244f90-dff3-4094-bb7d-3f8e41af5bb1
dsrInstance: AzureDrs
elapsedSeconds: 1
resultCode: 0x1
The device is already joined.
PS C:\WINDOWS\system32>
```

# Hybrid Entra Joined – Makes Sense?

- **Hybrid is the way to go for me!**

- Continued non disruptive sign in processes for users and existing devices
- The best of “both” worlds for access to applications
- A gateway to a more secure environment, with the added bonus of conditional access
- My application developers don’t need to be contacted
- I don’t have to convert my GPO’s to MDM profiles

I’m **“comfortable”** with this...



# Hybrid Entra Joined – Configuration

## Connectivity Problems?

To become hybrid joined, devices need to reach out to the internet

Test Device Registration Connectivity - Code Samples | Microsoft Learn

```
=====
Test Device Registration Connectivity
=====

Test-DeviceRegConnectivity log file has been created.

Testing Internet Connectivity...
Checking winHTTP proxy settings...
    Access Type : DIRECT

Checking winInet proxy settings...
    Proxy Enabled : No
    Proxy Server List :
    Proxy Bypass List :
    AutoConfigURL :

Testing Device Registration Endpoints...
Testing connection via winInet...

Connection to login.microsoftonline.com ..... Succeeded.
Connection to device.login.microsoftonline.com ..... Succeeded.
Connection to enterpriseregistration.windows.net ..... Succeeded.

Test passed: Device is able to communicate with MS endpoints successfully under system context

Script completed successfully.
```

```
Checking winHTTP proxy settings...
Access Type : DIRECT

Checking Internet Connectivity...
Connection to login.microsoftonline.com ..... Succeeded.
Connection to device.login.microsoftonline.com ..... Succeeded.
Connection to enterpriseregistration.windows.net ..... Failed.

Test failed: device is not able to communicate with MS endpoints under system account

Recommended actions:
- Make sure that the device is able to communicate with the above MS endpoints successfully under the system account.
- If the organization requires access to the internet via an outbound proxy, it is recommended to implement Web Proxy Auto-Discovery (WPAD).
- If you don't use WPAD, you can configure proxy settings with GPO by deploying WinHTTP Proxy Settings on your computers beginning with Windows 10 1709.
- If the organization requires access to the internet via an authenticated outbound proxy, make sure that Windows 10 computers can successfully authenticate to the outbound proxy using the machine context.

Script completed successfully.
```



# Hybrid Entra Joined – Configuration

```
Checking winHTTP proxy settings...
```

```
Access Type : DIRECT
```

```
Checking Internet Connectivity...
```

```
Connection to login.microsoftonline.com ..... Succeeded.
```

```
Connection to device.login.microsoftonline.com ..... Succeeded.
```

```
Connection to enterpriseregistration.windows.net ..... failed.
```

```
Test failed: device is not able to communicate with MS endpoints under system account
```

```
Recommended actions:
```

- Make sure that the device is able to communicate with the above MS endpoints successfully under the system account.
- If the organization requires access to the internet via an outbound proxy, it is recommended to implement Web Proxy Auto-Discovery (WPAD).
- If you don't use WPAD, you can configure proxy settings with GPO by deploying WinHTTP Proxy Settings on your computers beginning with Windows 10.
- If the organization requires access to the internet via an authenticated outbound proxy, make sure that Windows 10 computers can successfully aut

```
Script completed successfully.
```



# Hybrid Entra Joined & Windows Autopilot

Hold my beer...

# Entra Hybrid Join – Hang on a sec..

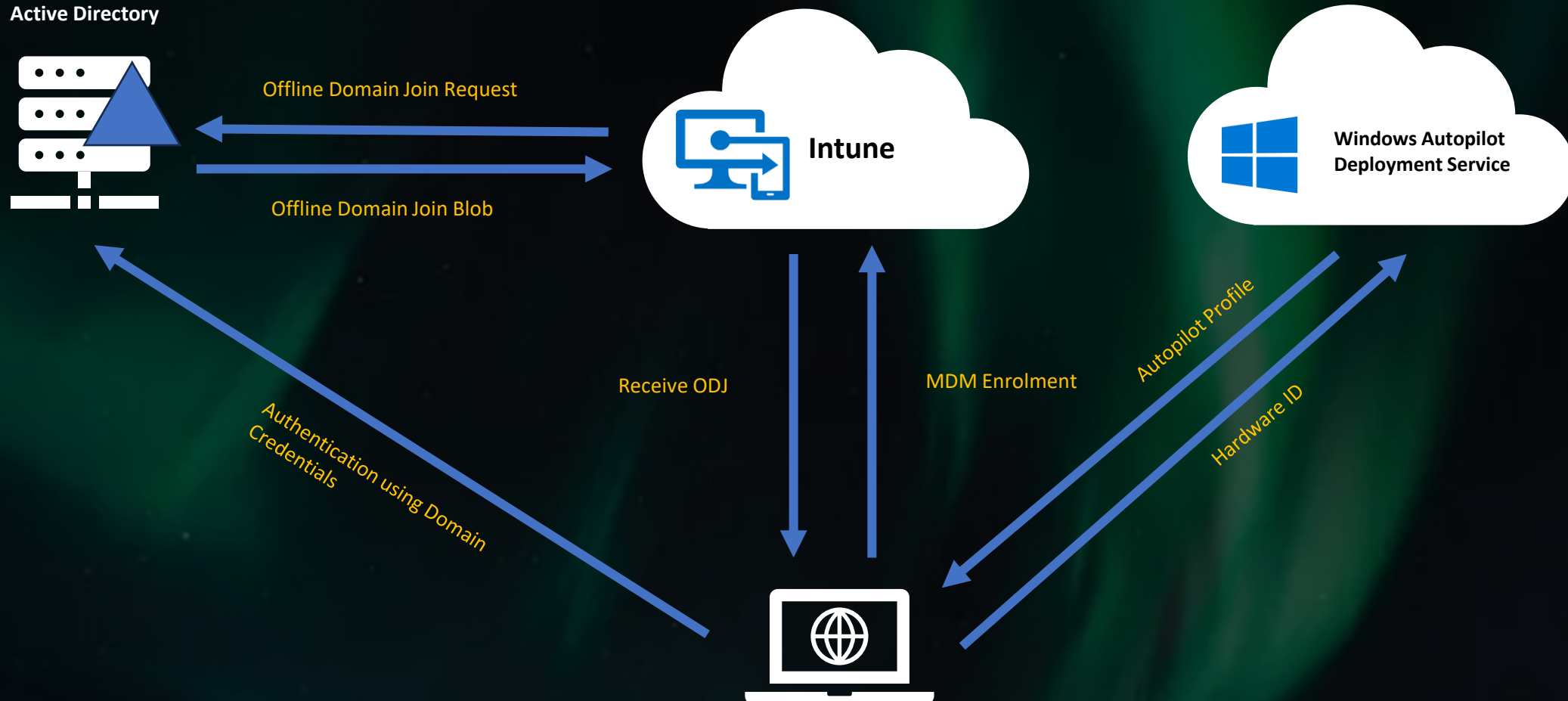
Entra Hybrid Join when combined with Windows Autopilot brings challenges.

Let us understand the “**WHY**” first

- **Hybrid requires an Intune Connector for Active Directory**
  - The connector is used to obtain / issue an offline domain join token during Windows Autopilot
- **OU configuration is required in the form of an Intune profile**
- **Line of sight to the domain controller is required upon reboot**
  - In the office, no problem
  - Outside of the office.. Ah..
- **Device / certificate-based VPN solution required for line of sight to the DC**



# Therefore, I need the following...

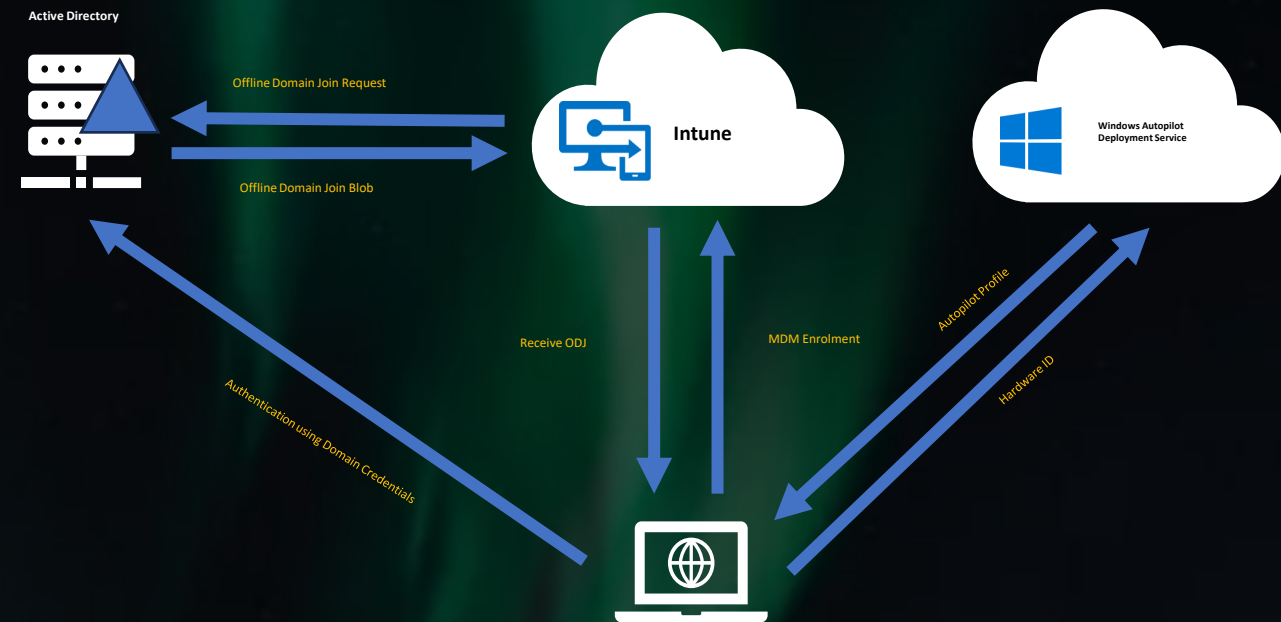


# Reminder.. You need to manage this

- **Intune Connector for Active Directory**
  - Another agent to manage
- **Certificate-Based VPN**
  - Line of site is required for the initial log on
- **Intune Active Directory OU Configuration**
  - OU placement during domain join

**Increased Complexity..**

**More things to break..**



# The Hybrid Entra Joined Challenge

Now ask yourself “What benefits do we get in this process?”

- **Group Policy Objects**
  - Let's party like we are running Windows XP..as if..
- **Domain Access**
  - OK, that sounds like it is “needed”, we have a domain..
- **Access to SMB File Shares**
  - Granted, everyone needs files on servers, right?
- **Print Server Access**
  - Sometimes I need to print, entire manuals
- **Application Access**
  - Of course, we need access to applications, and therefore we need to be domain joined, right?





# Social Media Storm

Don't say the word "Legacy"



# Go Entra Joined.. Social Media Storm

Except where an existing "on-prem" product does a thing simply by nature of being on-prem, and the cloud version can't because of fundamental difference in the architecture, but the MS "investment" isn't worth fixing it because it doesn't affect enough people

Entra hybrid joined devices  
by using Intune and Windows

Then allow us the ability to integrate any system we want, including custom ones, to the compliance checks so that we can use compliance policies in conditional access? Seems easy. Gives flexibility.

Don't take this the wrong way, but it feels very much like Microsoft engineers do \*not\* have a vision. In fact, it feels from the outside that's half the problem.

## 📌 Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. For more information, see

I am a Microsoft evangelist, but I strongly dislike the direction the company is taking - seemingly in pursuit of monthly subscriptions for everything that once would have had a perpetual license and basically abandoning on-premise based products for half baked substitutes

It's a poor relative of cm still. Just today co portal wouldn't install, error code in intune. Now what. It's draining.

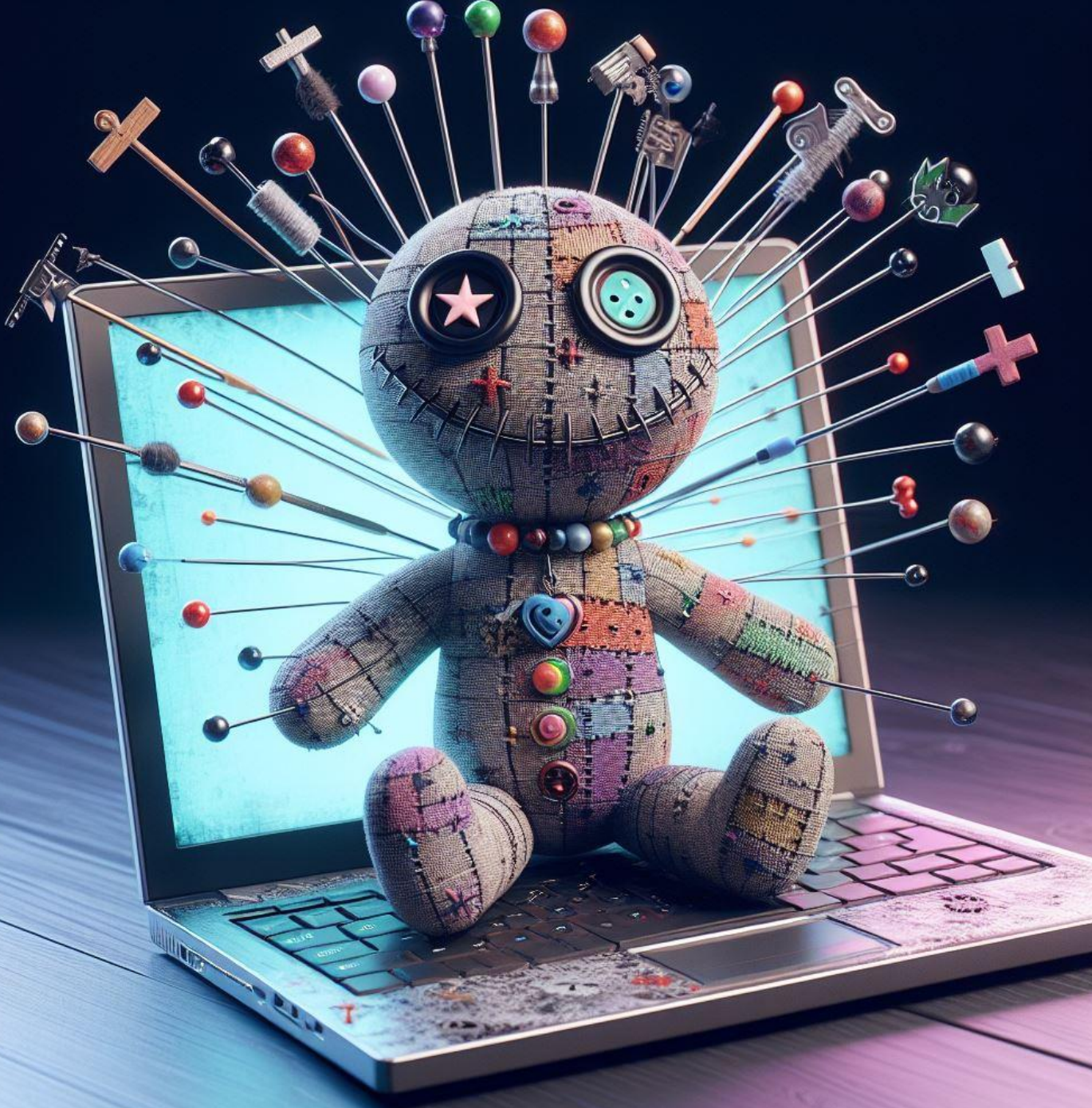
Entra joined in cloud-native endpoints: Which option is right for your

The whole hybrid/cloud debate is highly personal for some people.

I've tried to be fair in this conversation and call out both sides when I thought they were in the wrong so I hope this isn't seen as just more "piling on".....as you know I work in a cloud only environment. Fix the problems caused by cloud only users if you want to be cloud first.

Free to decide... until microsoft deprecate onprem functions that are heavily used? Cloud is not the be all and end all technology. I have nothing against cloud, but in its place. You cant call something "legacy tools" when the replacement isn't even close to being ready 🙄





Entra Joined  
Devices will never  
work for us!

Access to on-premises  
Voodoo



# Entra Joined Devices will never work for us!

## Word: Misconception

**Definition:** “An idea that is wrong because it has been based on a failure to understand a situation”

Source:

- **Group Policy Objects**
  - Replace these with Intune MDM profiles. Yes, we know.. No group policy preferences, looking at you Intune product group
- **Domain Access**
  - Have you tried this? Synced identities.. You might be surprised
- **Access to SMB File Shares**
  - Refer to the previous point
- **Print Server Access**
  - Refer to the previous, previous point
- **Application Access**
  - You get the picture..but this area does need testing of course



# DEMO

Seeing is believing.. Local resource access

# Entra Join will never work for us!

## Other real-world challenges include:

- **Certificates**
  - Delivery of certificates from internal PKI for things like 802.1x
- **Mapped Drives**
  - Organisations are not fully ready for SharePoint, and users are not ready to let go of mapped drives
- **Hardware IDs**
  - Smaller organisations do not have resources for obtaining hardware hashes
- **Autopilot Stability**
  - I have a “friend” who requires every single potential app ever to be installed
- **Group Policy Analytics**
  - It doesn't migrate all of my settings, and I have a baseline to adhere to



# Strong Authentication

**Passwords = BAD**

**Strong Auth Tokens = Good**

- **Windows Hello for Business FTW!**

- **ISSUE:** We tried it on our Entra joined devices, everything worked except access to file/print. The users had to sign in using their password, so we disabled it!
- **SOLUTION:** Without Cloud Kerberos trust, there is no ability to use this for **on-premises access**

[Windows Hello for Business cloud Kerberos trust deployment guide - Windows Security | Microsoft Learn](#)



# DEMO

Seeing is believing.. Part 2.. Cloud Kerberos Trust





# The Joy of “Unsupported”

Migration you say?..  
You’re on your own there..  
(Also.. AI still can’t spell)



# “Cause for Concern?”

## Migrating from Entra Hybrid Join to Entra Join

- **Microsoft**
  - No supported method of migration
- **Third Parties**
  - This is where things get a bit “shady”

Migrating from EHJ(HAADJ) to EJ(AADJ) is very similar to migration of on-premises domains in the past. User profiles will be impacted. Security settings will be impacted.. Can it be done.. Yes.

Is it a better idea to start fresh? Typically.

# Third Party Methods

## Edit Your Device ReACL Profile

PROFILE NAME

Testlabs Workstation Re-ACL Profile

LOGGING LEVEL

☒ INFORMATIONAL  
☐ DEBUGGING

COMPONENTS TO PROCESS

<input checked="" type="checkbox"/> LOCAL FILES/FOLDERS	<input type="checkbox"/> ROAMING PROFILES
<input checked="" type="checkbox"/> REGISTRY PERMISSIONS	<input checked="" type="checkbox"/> WINDOWS SERVICES
<input checked="" type="checkbox"/> USER PROFILES	<input type="checkbox"/> WINDOWS SERVICE ACCOUNTS
<input checked="" type="checkbox"/> <b>LOCAL GROUP MEMBERSHIP</b>	<input checked="" type="checkbox"/> USER RIGHTS ASSIGNMENTS
<input checked="" type="checkbox"/> LOCAL PRINTER PERMISSIONS	<input checked="" type="checkbox"/> SYSTEM ACLS
<input checked="" type="checkbox"/> NETWORK SHARE PERMISSIONS	<input type="checkbox"/> PRESERVE THE "ARCHIVE" BIT
<input checked="" type="checkbox"/> PRINTER SHARE PERMISSIONS	

CLEAR NEXT

# Final Thoughts..Moral of this session

## Going Entra Joined / Cloud Native

- Doesn't have to be a monumental effort in the vast majority of cases
- Group policy migration is easier than ever
- All about testing, but don't let that put you off
- Devices that don't have internet access... Keep them locally joined / managed
- If applications are holding you back, deliver them in another way
  - AppProxy
  - Azure Virtual Desktop / Citrix / Windows365
- Invest in a web-driven Printing Solution

**End Result = It makes it easier and less complex for everyone. Win/Win**



# Session Feedback



**Thank you for attending our session!**

**Please provide feedback by scanning the QR code**