[**MICROSOFT ENDPOINT MANAGER**](https://niklasrast.com/tag/microsoft-endpoint-manager/)**,**[**WINDOWS**](https://niklasrast.com/tag/windows/)

A Guide to setting up Windows Autopilot with Hybrid Azure AD join capabilities in Microsoft Intune

A diagram of a software application

Description automatically generated with medium confidence

**Date:**[**August 22, 2023**](https://niklasrast.com/2023/08/22/a-guide-to-setting-up-windows-autopilot-with-hybrid-azure-ad-join-capabilities-in-microsoft-intune/)**Author:**[**Niklas Rast**](https://niklasrast.com/author/niklasrast/)[**0 Comments**](https://niklasrast.com/2023/08/22/a-guide-to-setting-up-windows-autopilot-with-hybrid-azure-ad-join-capabilities-in-microsoft-intune/#respond)

Windows Autopilot has revolutionized the way organizations deploy and manage Windows devices. It’s a powerful tool that simplifies the initial setup of Windows 10 and Windows 11 devices, reducing the need for manual configuration. In this blog post, we will explore the setup process for Hybrid Azure AD join, which allows devices to be joined to both on-premises Active Directory and Azure AD. While Hybrid Azure AD join is a valuable step in transitioning to the cloud, we’ll also discuss why you might consider moving to Azure AD-only join in the long run.

**What is Windows Autopilot?**

Windows Autopilot is a modern deployment technology introduced by Microsoft to streamline the process of setting up Windows devices for end-users. With Autopilot, administrators can pre-configure devices, making them ready to use right out of the box. It simplifies and automates the traditional setup processes by allowing devices to join Azure Active Directory (AAD) and enroll in Microsoft Intune, all without the need for IT intervention.

**How does Windows Autopilot with Hybrid Azure AD join works?**

During the Windows Autopilot phase there are some things in the background. Specially with an Hybrid Azure AD join there are some more tasks than in an Azure AD only join. Lets see what those are and what they do.

A diagram of a cloud computing process

Description automatically generated

1. Device contacts the Windows Autopilot during the OOBE and asks if it knows the devices hardware hash.
2. Windows Autopilot detects the hardware hash in its database and connects to the Microsoft Intune instance of the customer from which the hardware hash has been uploaded and assigned to its organization. Intune sends the Autopilot profile to the Autopilot service.
3. The Autopilot service forwards the Autopilot profile which will be downloaded and applied from the client.
4. Intune uses the Intune AD Connector to ask the onprem Active Directory to create an Computer account object.
5. The Intune AD Connector forwards the request to the domain controller and waits for an response.
6. The domain controller uses the authentication from the Intune AD Connector to create an computer account object in its directory and sends back an “Offline domain join blob (ODJB)” to the Intune AD Connector.
7. The Intune AD Connector forwards the ODJB object to the Intune service in the Cloud.
8. Intune sends the ODJB to the client who has asked it for.
9. The client connects to the onprem domain controller to apply the ODJB. At this point the client needs an direct or VPN connection to the domain controller. Now the client is Active Directory joined. In the background Azure AD Connect synchronizes the computer account object to Azure AD. This task will make the client Hybrid Azure AD joined as it now has an computer account object both in onprem and cloud directories.
10. Microsoft Intune sends configuration profiles, deployed apps and more to the client. The client installs those assignments and finishes the OOBE.

After this process, the client is enrolled to the customers Microsoft Intune instance and ready to be used by an user.

**Requirements**

Before diving into the setup process, it’s essential to ensure you meet the following requirements:

1. **Azure AD and Intune Subscription**: You need an Azure AD subscription and an Intune subscription.
2. **Azure AD Connect**: Install and configure Azure AD Connect to synchronize on-premises Active Directory with Azure AD. If you have not setup this yet, check out my post on that [HERE](https://niklasrast.com/2023/05/17/setup-azure-ad-cloud-sync-to-sync-your-onprem-active-directory-identities-to-azure/).
3. **Active Directory**: Maintain an on-premises Active Directory infrastructure.
4. **Windows 10/11 Devices**: Devices should be running Windows 10 version 1703 or later, or Windows 11.
5. **Azure AD Company branding:** It looks company branded in Autopilot if you have setup Company branding in Azure AD. Highly recommending you this.

**Enabling and Setting Up Windows Autopilot in an Hybrid Scenario**

To enable and set up Windows Autopilot with Hybrid Azure AD join follow these steps, but ensure that you have the requirements correctly setup:

**Azure AD Configuration**

Make sure your organization has Azure Active Directory Premium licenses or an Enterprise Mobility + Security (EMS) license to access Autopilot capabilities.

A screenshot of a computer

Description automatically generated

**Azure AD dynamic device group Setup**

First of all we need to create a Azure AD group with a dynamic membership type. So we do nat have to add devices manually later on. In this example we are going to create a group called “MDM-WIN-HYBRID” which automatically collects all devices that have been flagged with a tag named “hybrid” at the hardware hash in the Autopilot service.

A screenshot of a group

Description automatically generated

Under “Add dynamic query” click on “Edit”:

A screenshot of a computer

Description automatically generated

Paste the following rule to collect devices with the tag “hybrid”:

(device.devicePhysicalIds -any \_ -eq "[OrderID]:hybrid")

A screenshot of a computer program

Description automatically generated

If you want to use another tag, for example based on locations which you use as a tag than simply replace that with hybrid in the rule from this example. Then click on Save. This will add the rule to our group:

A screenshot of a computer

Description automatically generated

Save the group to finish the group creation process.

**Intune Enrollment**

In Intune we need to have the Automatic enrollment to be enabled. Check if it is enabled at Devices -> Enroll devices -> Windows enrollment -> Automatic enrollment. Make sure that the “MDM user scope” is set to All or a defined Azure AD group of users who should be able to enroll new devices:

A screenshot of a computer

Description automatically generated

**Intune AD Connector Setup**

Now we are at the most complex but also most important step to setup for an Hybrid Azure AD joined experience within Autopilot – the Intune AD Connector. This is a little tool which connects both to Intune in the Cloud and to the Domain Controller onprem. This tool will accept reqests from Intune to ask the domain controller onprem to create computer account objects in the Active Directory and send an Offline Domain Join blob to Intune which will forward this to the device it was requested for. You need to install this Connector on an server in your onprem network infrastructure where it can reach the domain controller (similar to the Azure AD Connector).

So lets start. Firstly we need to navigate to [https://endpoint.microsoft.com](https://endpoint.microsoft.com/) on this server onprem and click on “Enroll devices” under the “Devices” blade:

A screenshot of a computer

Description automatically generated

Now click on the “Intune Connector for Active Directory” button:

A screenshot of a computer program

Description automatically generated

In the opened menu from the right side click on “+ Add”:

A screenshot of a computer

Description automatically generated

Now click on “Download the on-premises Intune Connector for Active Directory”:

A screenshot of a computer

Description automatically generated

NOTE: The Server containing the Intune AD Connector **must**have access to the internet. If you have a proxy in your environment, please follow the [proxy recommendations](https://docs.microsoft.com/en-en/azure/active-directory/manage-apps/application-proxy-configure-connectors-with-proxy-servers).

You should find a “ODJConnectorBootstrapper.exe” shortly afterwards in your Downloads. Please open this file with administrative permissions:

A screenshot of a computer

Description automatically generated

Accept the license terms and click in Install:

A screenshot of a computer

Description automatically generated

The installation should only take a few seconds. Now click on “Configure Now”:

A screenshot of a computer

Description automatically generated

In the configuration wizard click on “Sign In”:

A screenshot of a computer

Description automatically generated

Now enter the Azure AD credentials for an Global administrator account with an assigned Intune license:

A screenshot of a computer

Description automatically generated

Once you are authenticated wait a few seconds until you see the message box telling you that the connector has been successfully enrolled:

A screenshot of a computer error

Description automatically generated

If this process fails you need to check the logs at C:\Users\**USERNAME**\AppData\Local\Temp\Intune\_connector\_for\_Active\_Directory\_<Year>

Now you can see an registered connector in the Intune portal:

A screenshot of a computer

Description automatically generated

**Delegating permissions for the Intune AD Connector for Active Directory**

Sadly we are not done yet. We need to grant the Intune AD Connector permissions in the organizational unit (OU) within our Active Directory where we want to create the computer accounts. As shown in the following screenshot of the local services, the Connector service (IntuneODJConnector Service) works with the local system account. So the server computer object (SERVERNAME$) must have permission to create the computer objects in AD at the right OU.

A screenshot of a computer

Description automatically generated

I have this “HybridClients” OU in my onprem Active Directory where I am going to delegate the permissions and want to store the computer account objects. By default every domain account can join up to 10 devices to Active Directory, but we want our Intune AD Connector to be able to join more than 10 devices so we need to delegate it the right permissions.

Launch the Active Directory Users and Computers console in your Active Directory. Right-Click on the OU that you want to keep the computer objects in and click on Delegate Control:

A screenshot of a computer

Description automatically generated

Click on Next:

A screenshot of a computer

Description automatically generated

Click on “Add”. In the Object Types check Computers and then search for the computer name of your server. In my lab I had the Connector on the DC directly – but in an production environment you need to install the Connector on another server. You can install the Connector on any other server or for example on the same server as the one hosting your Azure AD Connector.

A screenshot of a computer

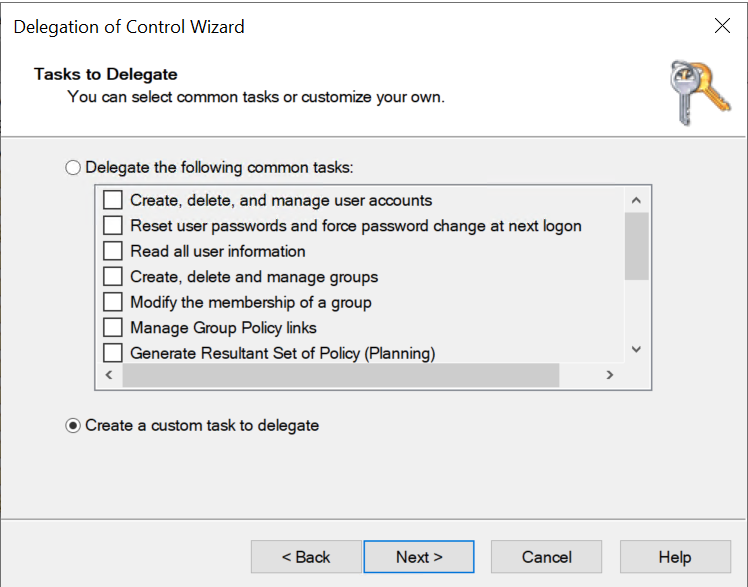
Description automatically generated

Now the computer account of your server should be added to the list:

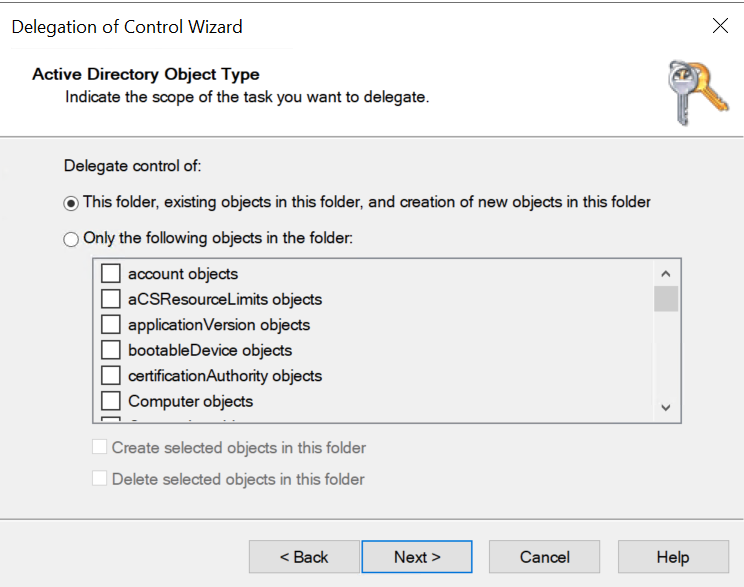
A screenshot of a computer

Description automatically generated

We need to check “Create a custom task to delegate” now:



Check “Delegate folder, existing objects in this folder, and creation on new objects in this folder” because we want to manage existing and create new computer account objects in this OU by the Connector service:



Click on “Full control” this will check all other options automatically:

A screenshot of a computer

Description automatically generated

Finish the wizard:

A screenshot of a computer

Description automatically generated

**Intune Autopilot Profile Setup**

Now that the hard part of the work is done we can continue with the creation of an Windows Autopilot profile for the Hybrid Azure AD join. Lets continue in the Intune portal at Devices -> Enroll Devices -> Deployment profiles at the Windows Autopilot Deployment Program section:

A screenshot of a computer program

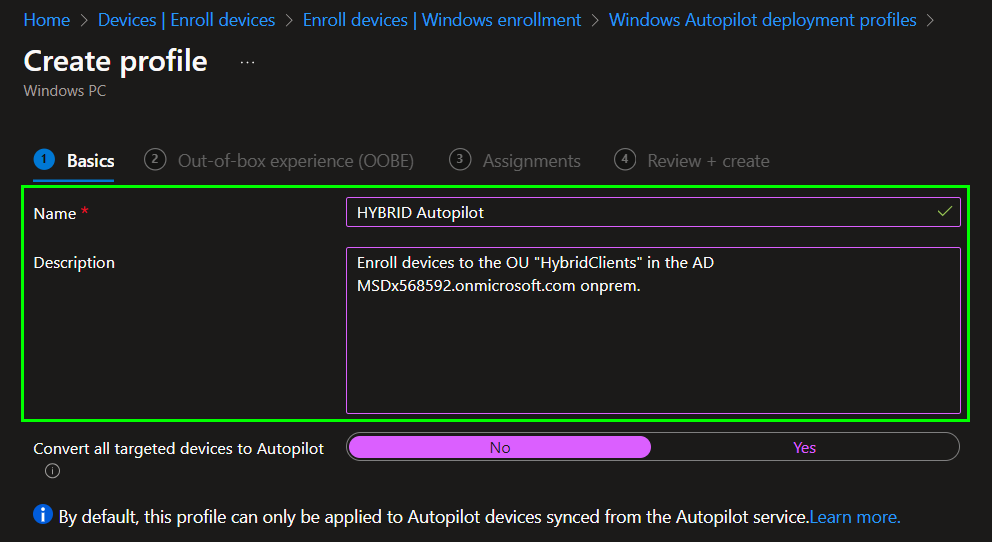
Description automatically generated

Click on “+ Create profile” and choose “Windows PC”:

A screenshot of a computer

Description automatically generated

Set a name and description:



Next configure the profile to have an Join type of “Hybrid Azure AD joined”, disable the AD Connectivity skip.

Optionally you might want to check that users will become a Standard user (No Admin rights) and you can enable that “Pre-Provisioning” can be used. Read more about Pre-Provisioning [HERE](https://niklasrast.com/2023/03/20/pre-stage-windows-devices-with-autopilot-pre-provisioning/).

A screenshot of a computer

Description automatically generated

As you can see in the yellow box there is no support for a device name template here. We will cover this in the next step where we create a Intune Domain Join profile.

Assign the Autopilot profile to the Azure AD group that we created at the beginning of this article.

**Intune Domain Join profile Setup**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Here we can define a computer name prefix. The name will be 15 characters long and automatically filled if your prefix is less than 15 characters:

WIN-HYBRID-0000

The domain name needs to be in FQDN:

msdx568592.onmicrosoft.com

You need to write the OU in the fully qualified name:

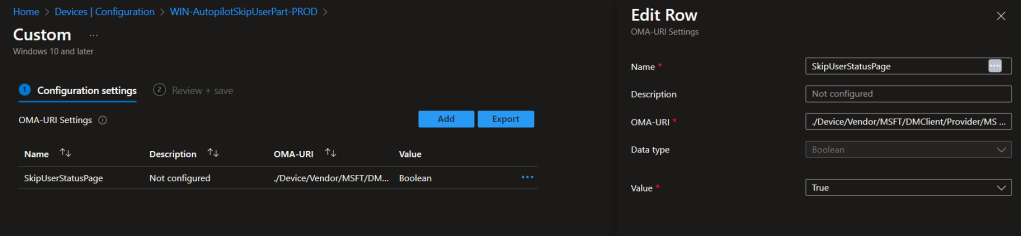
OU=HybridClients,DC=msdx568592,DC=onmicrosoft,DC=com

TIPP: Do not copy values. There can be issues with “.” or “,” and then the Autopilot will fail at the domain join part. I highly recommend you to manually type domain an OU from your keyboard.

Finish the wizard and assign the profile to the Azure AD group that we created earlier.

**Create a Custom configuration to disable User Setting during Autopilot**

It is highly recommended to skip the user setup part in an Hybrid Azure AD join scenario as this is a point which mostly fails. So you need to create a configuration profile from the CUSOTM type with the following OMA-URI setting:



**Name:** SkipUserStatusPage

**OMA-URI:** ./Device/Vendor/MSFT/DMClient/Provider/MS DM Server/FirstSyncStatus/SkipUserStatusPage

**Data type:** Boolean

**Value:** True

Finish the wizard and assign the profile to the Azure AD group that we created earlier.

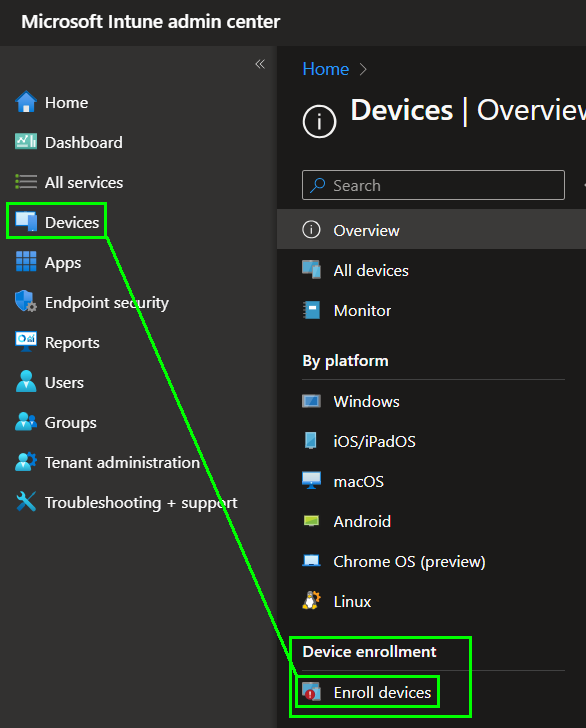
**Enabling the Enrollment Status Page (ESP)**

The Enrollment Status Page (ESP) is a crucial component of the Windows Autopilot deployment process managed through Microsoft Intune. It’s designed to provide users with a clear and informative experience during the device setup phase, ensuring that the device is correctly configured and policies are applied before the user can access the desktop.

Here’s a description of the Enrollment Status Page:

1. **Purpose**: The ESP helps to streamline the out-of-box experience for users when setting up a new Windows device. It ensures that essential configuration and app installations occur before the user can start using the device, reducing the need for post-setup configurations.
2. **Customization**: Administrators can customize the ESP to display specific branding, messages, and progress information. This customization helps reinforce your organization’s branding and provides clear instructions to users.
3. **Status Updates**: The ESP provides real-time status updates to users about the progress of the device configuration. Users can see which stage of the setup process is currently in progress and how much longer it is expected to take.
4. **Predefined Checks**: ESP checks various conditions, such as network connectivity and app installations, to ensure that the device meets your organization’s requirements before allowing the user to proceed.
5. **Blocking Access**: Until the ESP completes its tasks and confirms that the device is compliant with your organization’s policies, users are prevented from accessing the desktop. This ensures that devices are properly configured and secure before use.
6. **Recovery Options**: In case of any issues or failures during the ESP process, there are recovery options available. These options allow administrators to troubleshoot and remediate problems without needing to reimage the device.
7. **User Experience**: The ESP is designed to provide a user-friendly experience. It keeps users informed about what’s happening, reducing frustration during the initial setup process.
8. **Device Compliance**: The ESP ensures that the device is compliant with your organization’s policies, which can include installing necessary applications, configuring security settings, and verifying network connectivity.
9. **Completion Notification**: Once the ESP successfully finishes its tasks, it provides a completion notification to the user, indicating that the device is ready for use.

In my mind this is an very useful feature and I would recommend you to enable it. Do to so navigate from the Intune portal to Devices -> Enroll devices.



Here click on “Enrollment Status Page” at Windows enrollment:

A screenshot of a computer program

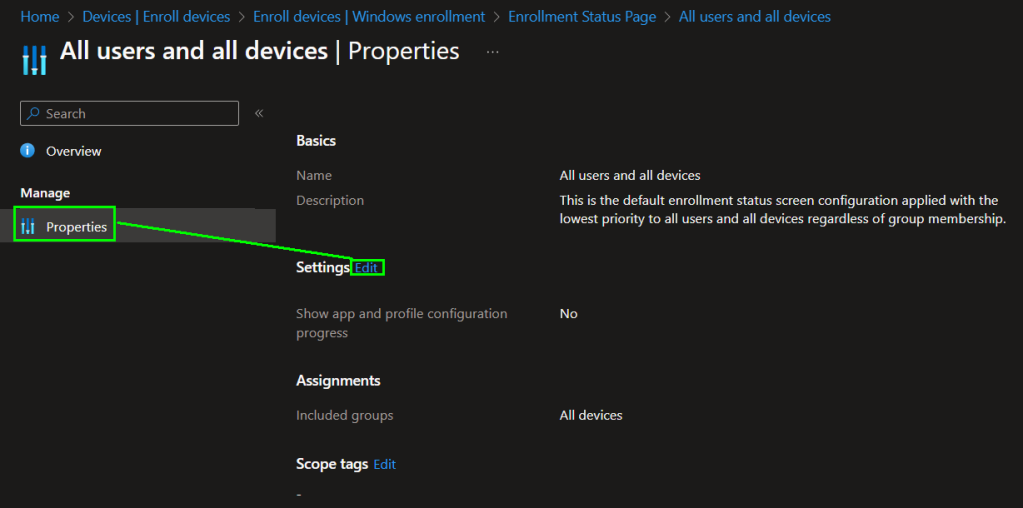
Description automatically generated

You could create more than one ESPs but in this example we are simply enabling one ESP config for all devices an so for all different Autopilot profiles with the same ESP experience:

A screenshot of a computer

Description automatically generated

Click on “Edit” at the settings:



Enable the app and profile configuration progress. The other options can be set as you need them:

A screenshot of a computer

Description automatically generated

Finish the wizard and assign the profile to the Azure AD group that we created earlier.

**Optionally: Registering devices in Windows Autopilot and assigning them to your organization**

Now that the environment is ready we need to add devices to Windows Autopilot. Therefore we have 2 options. The first one is to buy new devices and tell the vendor to directly upload the hardware hashes of the devices to Autopilot and assign them to our tenant. The second option can be used for existing devices and you need to extract the hardware hash as an CSV file which you can then upload manually to Autopilot. If you need help here just follow my post on that.

**Optionally: Pre-Logon VPN**

A Pre-Logon VPN solution is an indispensable component when implementing Windows Autopilot in conjunction with Hybrid Azure AD join. This necessity arises from the inherent requirements of the Hybrid Azure AD join process. In this scenario, a device needs to establish connectivity with the on-premises domain controller for several crucial operations. Firstly, it is essential for the device to access the on-premises domain controller to apply the offline domain join blob. This blob contains critical domain configuration information that is essential for integrating the device seamlessly into the corporate network. Secondly, authentication plays a pivotal role in ensuring the security and access control of the device. To accomplish this, the device needs to communicate with the on-premises domain controller, which holds user account information and security policies. The Pre-Logon VPN solution serves as the bridge that enables these vital interactions to occur, ensuring that Windows Autopilot can effectively perform Hybrid Azure AD join, granting the device the necessary access and functionality to seamlessly blend the benefits of cloud and on-premises resources. Without this Pre-Logon VPN solution, the device might encounter authentication and connectivity issues, compromising the overall success and security of the Hybrid Azure AD join process.

*Once you have successfully set up everything, you will be able to effortlessly create multiple configuration profiles for client design and easily deploy software packages on your clients. Furthermore, you can seamlessly enroll new devices using Windows Autopilot in a Hybrid Azure AD join scenario, and efficiently manage these clients with Microsoft Intune directly from the cloud. Exciting times await as you harness the power of these seamless solutions!*

**OOBE Troubleshooting for Hybrid Azure AD Join enrollment issues**

With an Hybrid Windows Autopilot setup there can be some more points which can fail. So you need an troubleshooting strategy. When I configure an Hybrid Azure AD join with Windows Autopilot I am always using the *Get-AutopilotDiagnostics* script from the PowerShell gallery. This script tells you in which part of the enrollment Windows Autopilot currently is and how its return code is. For example when the request or download for the ODJB fails you wont get it until you use this script to see where and why it failed. This script is absolute my favorite for Autopilot troubleshooting. Read more on how to get it and how to use it in my other post about Troubleshooting Windows Autopilot.

**Transition to Azure AD-Only Join**

While Hybrid Azure AD join is a valuable intermediate step in transitioning to the cloud, it’s important to note that it’s not the final destination. Azure AD-only join offers numerous advantages, including simplified management, capability to use Kerberos on Intune managed devices and enhanced security compared to onprem only as you can use MFA and other Entra ID security features. But as part of your long-term strategy, consider migrating from Hybrid Azure AD join to Azure AD-only join. This transition involves decommissioning your on-premises Active Directory infrastructure, which can be a complex process but offers significant benefits in terms of agility and cost savings. To archive this goal you need to rebuild legacy apps in the cloud environment but on an long time view this will help you to optimize your environment, enhance security and also review your environment to start clean in the cloud. So my recommendation is absolute to directly go with the Azure AD join only and rebuild apps to support modern authentication and move fileshares to online services like SharePoint online.

I have this post where I show you how to setup Windows Autopilot with an Azure AD join. Check it out if you want to directly go with the preferred way:

**Conclusion**

In conclusion, Windows Autopilot with Hybrid Azure AD join is a powerful tool for streamlining device deployment and management in a hybrid environment. It provides a bridge between on-premises and cloud-based identity services. However, as you plan for the future, seriously consider moving towards Azure AD-only join to fully leverage the capabilities of the cloud and simplify device management even further. Embracing Azure AD-only join is a step towards a more modern and efficient IT ecosystem.

**Share this:**