**Microsoft Intune Autopilot Hybrid Entra ID (Azure AD) Join – The Complete Guide**

[Hybrid Entra ID: Unlock Your Potential with Intune](https://intunestuff.com/2025/01/28/microsoft-intune-autopilot-hybrid-entra-id-azure-ad-join-the-complete-guide/)

Here is a full guide on Microsoft Intune Autopilot Hybrid Entra ID. I know that Microsoft no longer recommends the use of Hybrid EntraID joined devices as stated in this article:

[Overview for Windows Autopilot user-driven Microsoft Entra hybrid join in Intune | Microsoft Learn](https://learn.microsoft.com/en-us/autopilot/tutorial/user-driven/hybrid-azure-ad-join-workflow)

However we still get a lot of questions to configure this. Also from customers that don’t have any Intune setup. This mainly because they still have legacy stuff on-premise, and that it is still a lot of work for sysadmins to change over to full cloud. I know that there are workarounds for these legacy things and I always try to convince the customers to go full cloud but sometimes you need to go the not recommended way.

As a result of this i’m writing this blog post for you to get all the necessary things to configure and to watch out for during the setup in 1 place. If you are reading this and you feel this guide is still incomplete or you have other solutions to the things that can go wrong please leave me a comment so i can add it. When browsing the internet i came across a lot of contradictory information around this topic so my goal was to give the community a better view on how to configure things.

This will be a long guide, trust me, and there are some strange quirks to overcome, so get your coffee(s) ready and clear your mind and let me take you on a rather strange trip.

Happy Reading!

In the time i was writing this guide some great news came from Microsoft. Next generation Autopilot!! Read all about it [here](https://techcommunity.microsoft.com/t5/microsoft-intune-blog/windows-deployment-with-the-next-generation-of-windows-autopilot/ba-p/4148169).

**UPDATE:** Entra ID Cloud Sync does **NOT**yet support hybrid joins.

**Prerequisites**

* Windows 10 1809 or later enduser devices having access to both intranet and internet.
* Server 2016 or later joined to local domain to install the Intune ODJ connector with access to internet.
* A Domain Controller
* Hybrid Entra ID join configured via Azure AD Connect tool.
* If behind a firewall, the device must meet the Windows Auto Pilot network requirements, see: [Windows Autopilot software requirements | Microsoft Learn](https://learn.microsoft.com/en-us/autopilot/software-requirements#networking-requirements)
* Device has to be in the direct line of sight with the DC on the local network or with a pre configure always on VPN, for VPN see: [Windows Autopilot User-Driven Mode | Microsoft Learn](https://learn.microsoft.com/en-us/autopilot/user-driven#user-driven-mode-for-microsoft-entra-hybrid-join-with-vpn-support) I will not cover the use of the always on VPN, in this guide i have line of sight to the DC
* Not a mandate – the recommendation is to have a DHCP running in on-prem infra as well.
* Intune licenses
* A global admin account for your Entra ID
* An enterprise admin account for your on-premise environment

**Configure the server stuff for Microsoft Intune Autopilot Hybrid Entra ID**

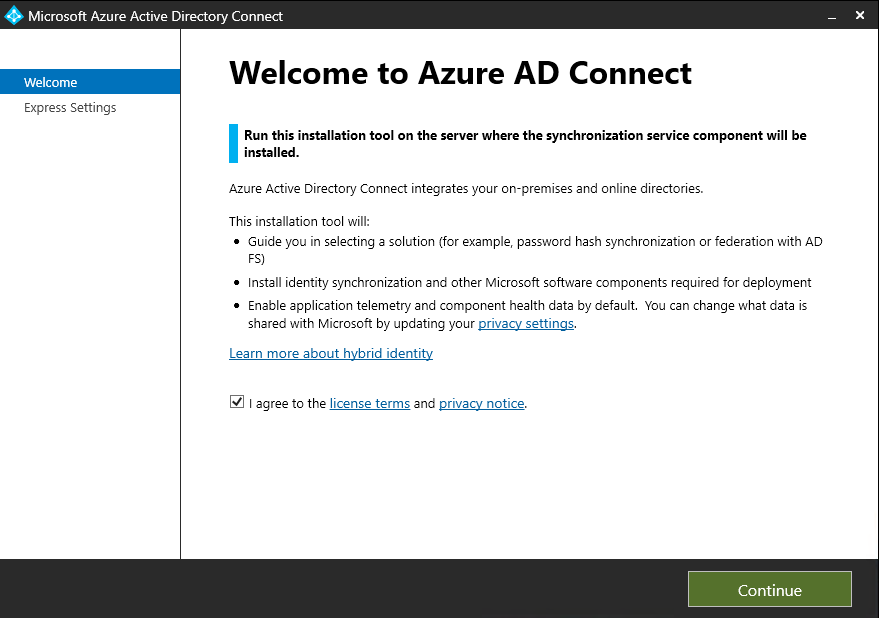
**Setup and Configure AD Connect**

**Setup AD Connect**

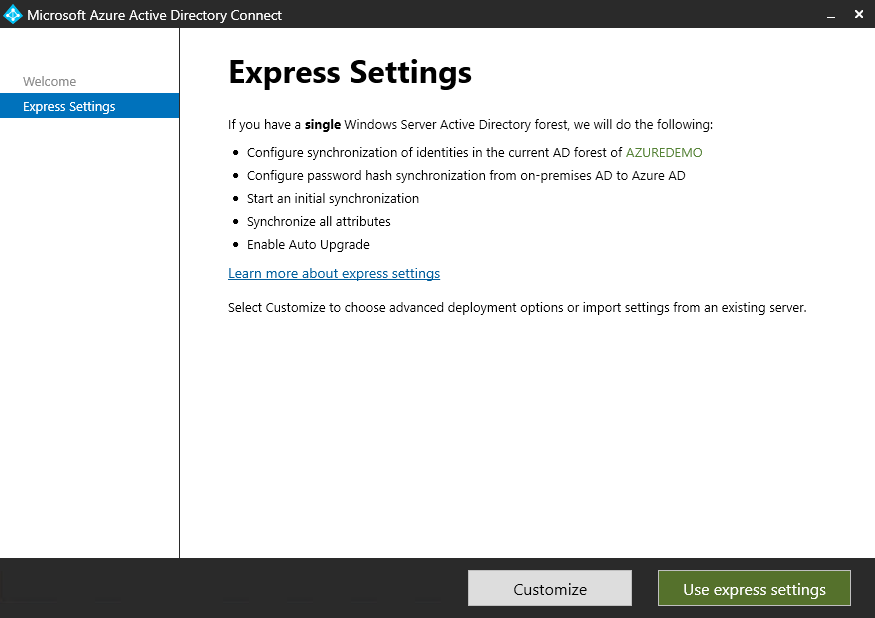
If you already have AD Connect installed you can skip to the configure part. If you don’t have AD Connect you can download the latest version [here](https://download.microsoft.com/download/B/0/0/B00291D0-5A83-4DE7-86F5-980BC00DE05A/AzureADConnect.msi).

If you have an older version of AD Connect installed, I highly recommend to upgrade it to the latest version.

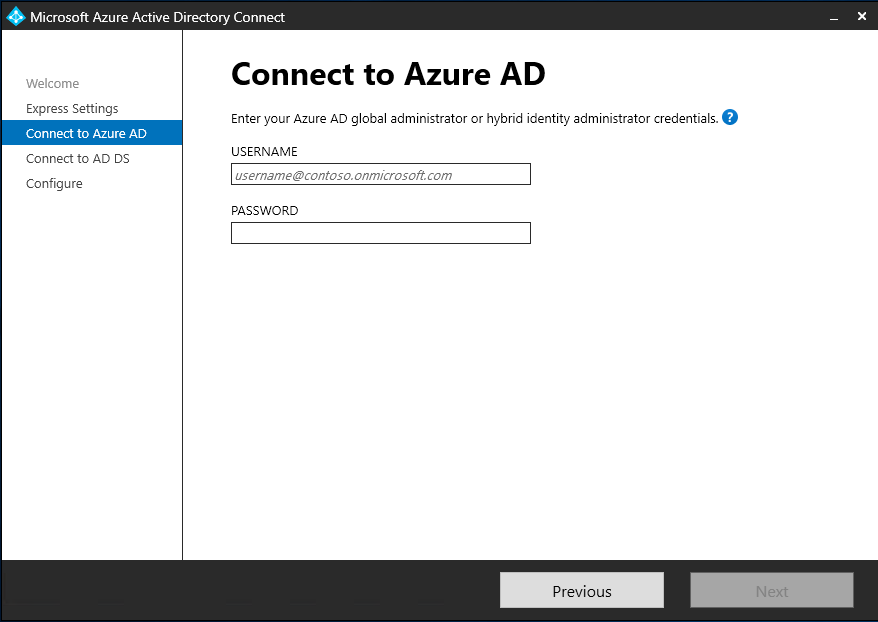
Run the installer and agree to the license terms and privacy notice and then click Continue.



Select Use Express Settings

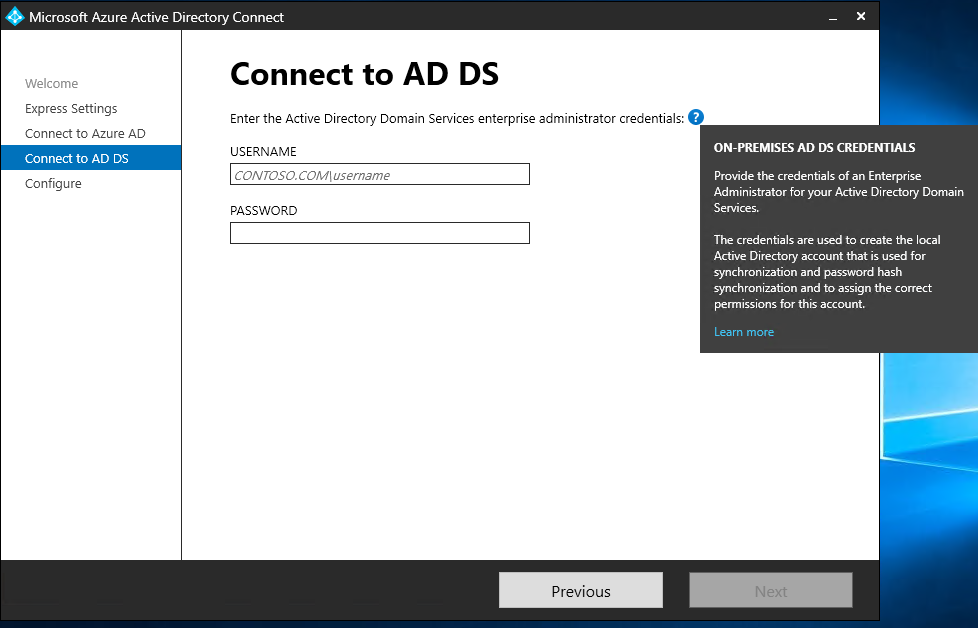


Enter your Global Administrator credentials to connect to Azure AD

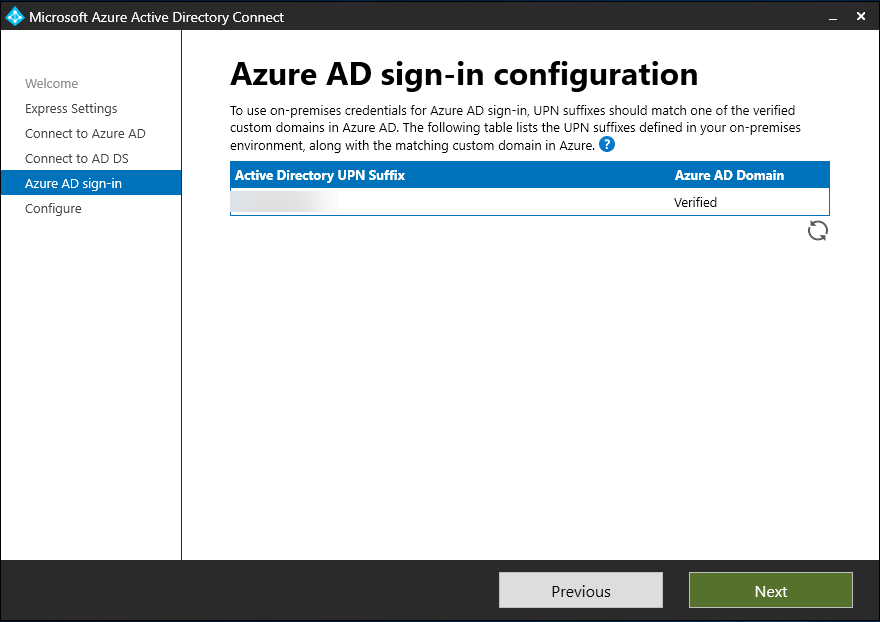


Enter credentials to connect to AD DS. The account must be a **Enterprise Administrator**

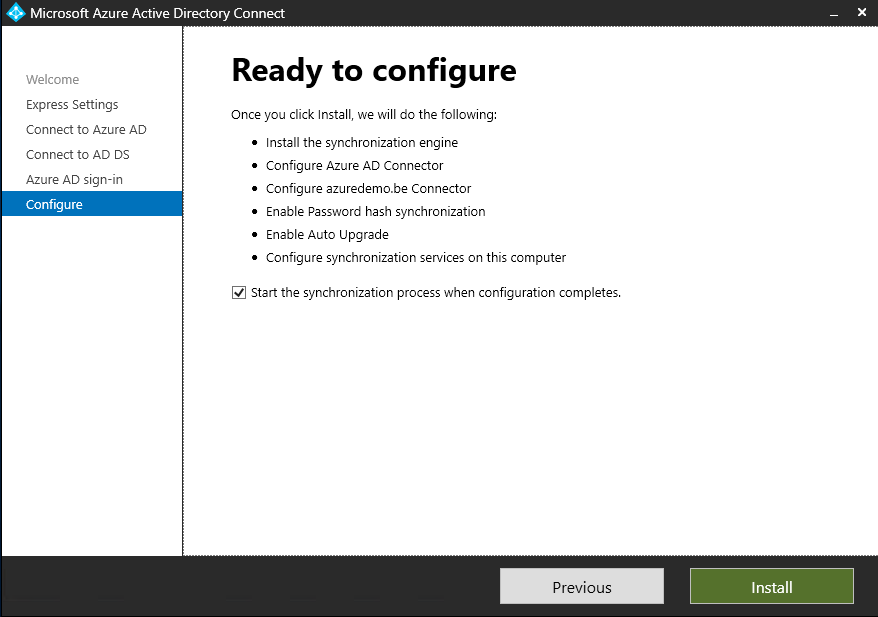
The user to be specified here for the SCP (Service Connection Point) configuration must be a member of the Enterprise Administrators group. These permissions can be revoked after successful SCP configuration.



Select install



Select Install and when ready select exit

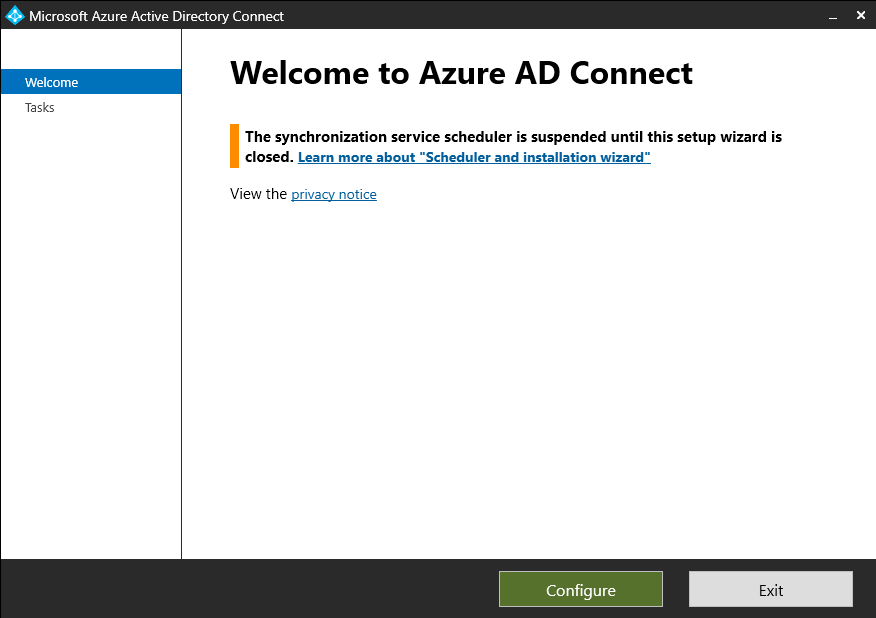


**Configure AD Connect for Microsoft Intune Autopilot Hybrid Entra ID**

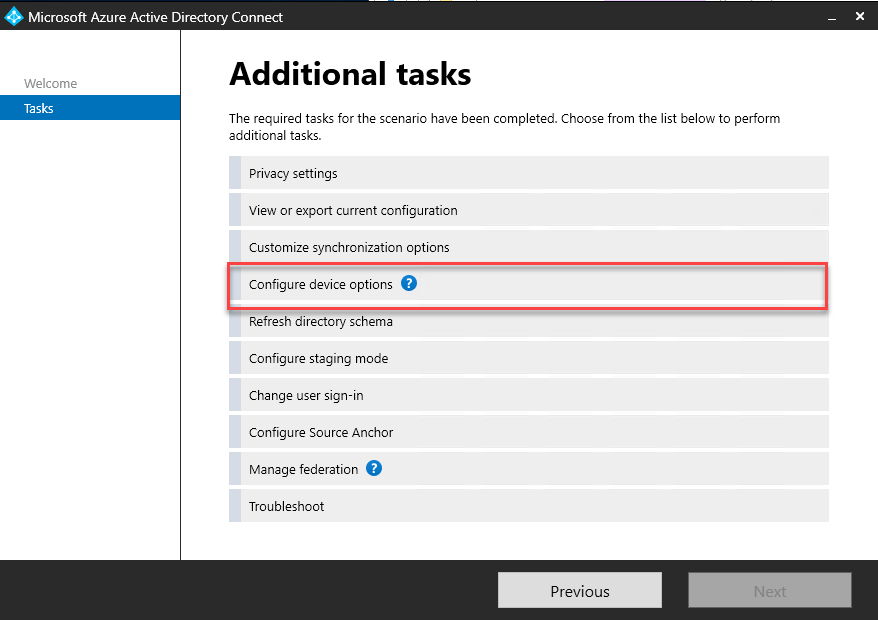
You will now see an Azure AD Connect icon on your Desktop. Double click the icon as we need to configure Device sync.



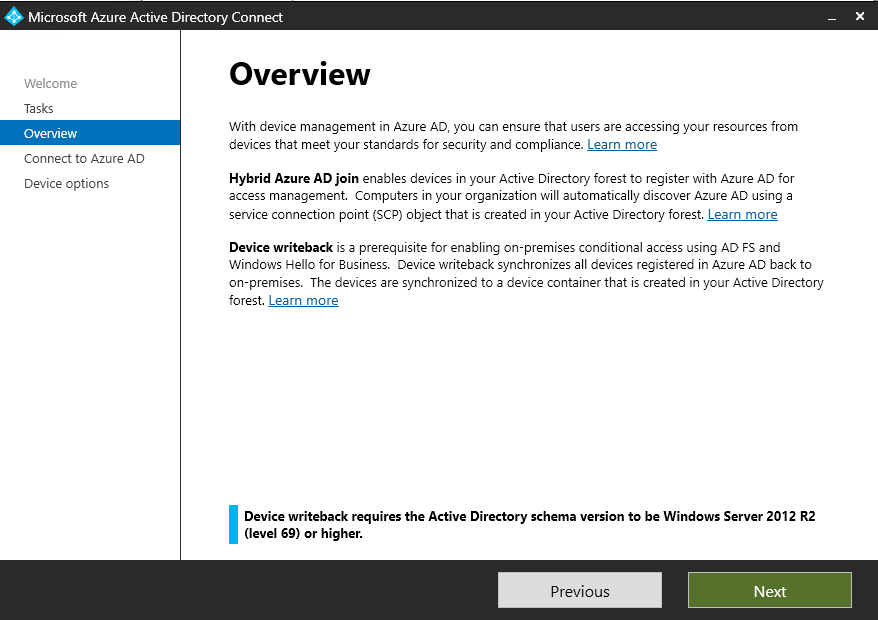
Click the green Configure button to configure AD Connect



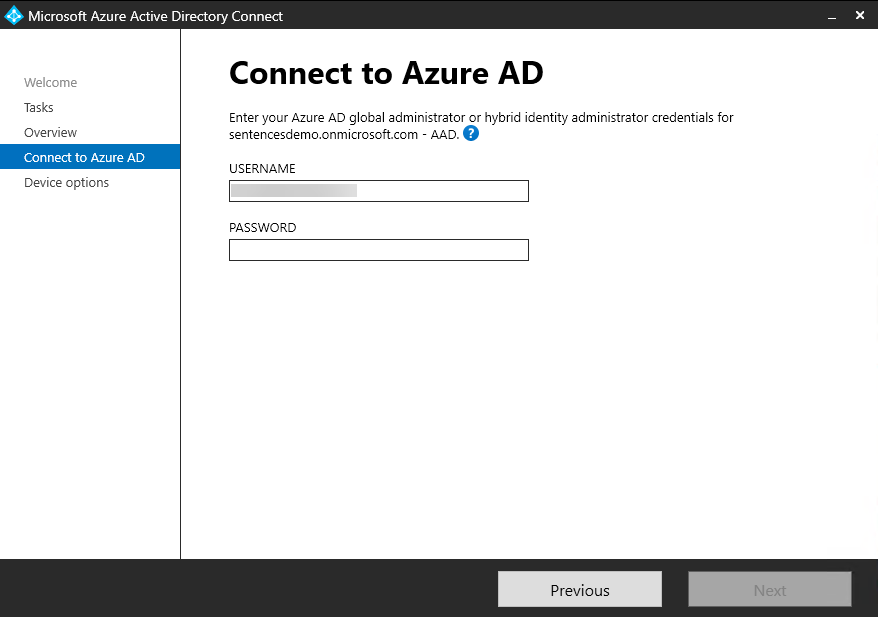
Select Configure Device Options and then click Next



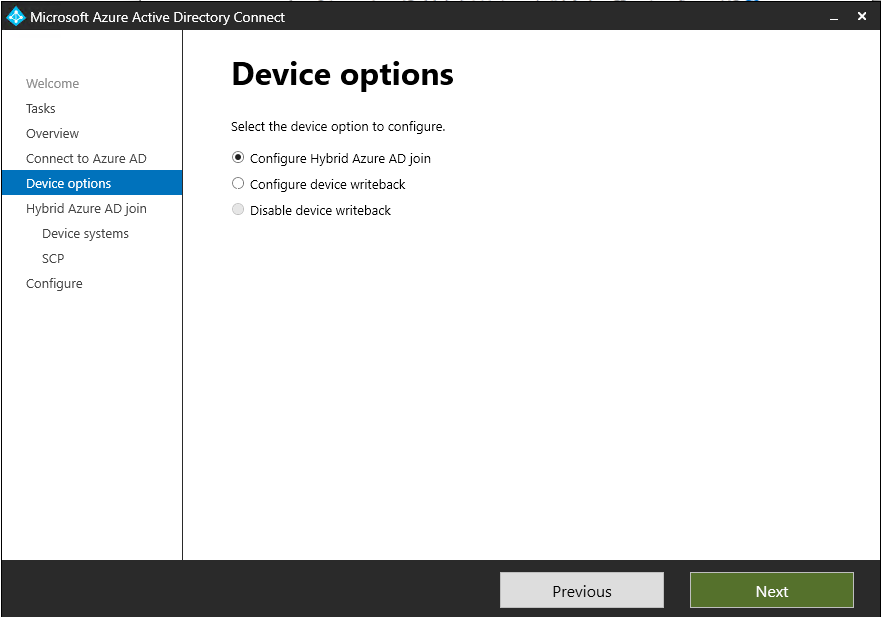
Click next



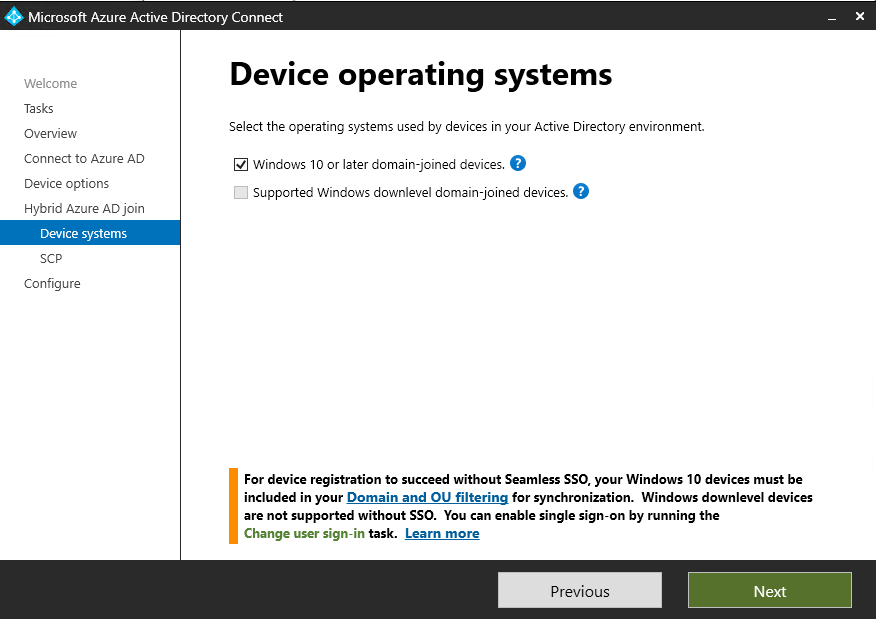
Enter your global administrator credentials to connect to Azure AD and then click Next



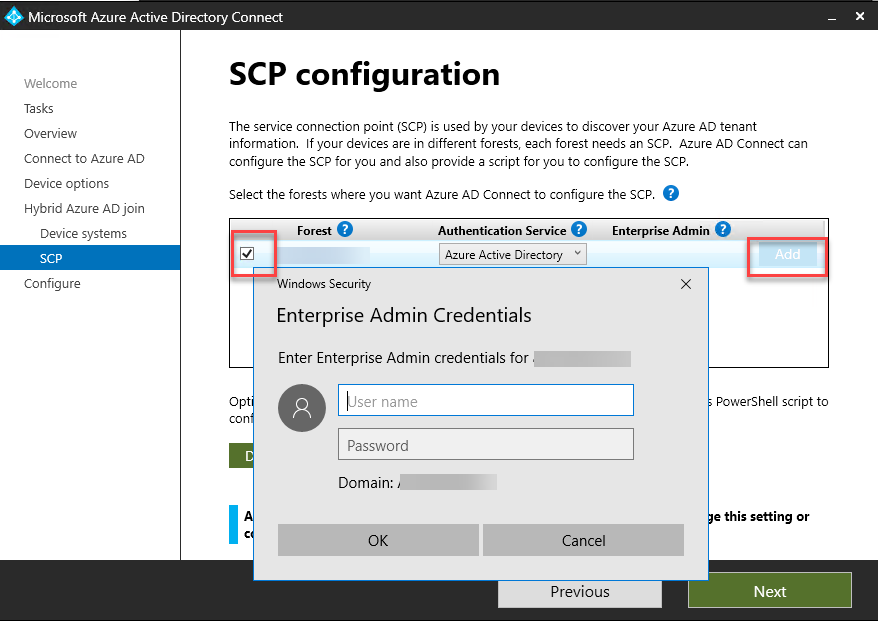
Click the Configure Hybrid Azure AD Join and then click Next



Select Windows 10 or later domain-joined devices and then select Next



Select your ADDS forest, authentication service click add and then provide a enterprise administrator



Once you are ready to configure, select Configure

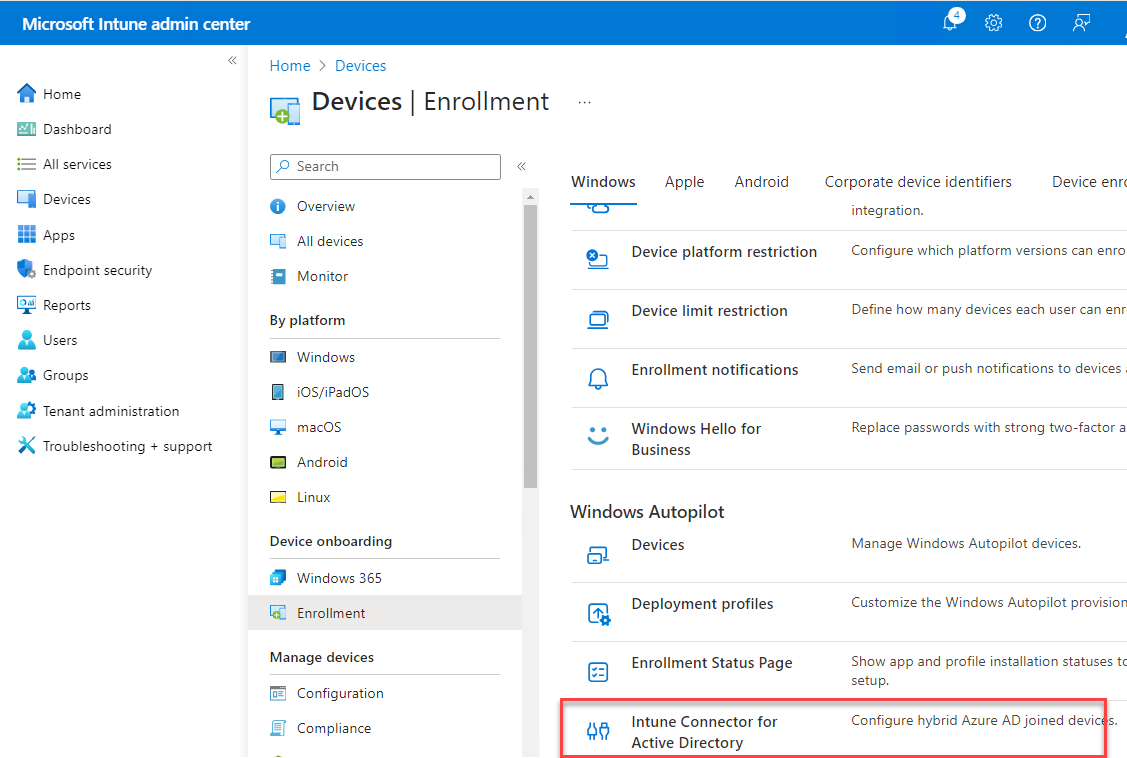


This concludes the setup and configuration of AD Connect. Now we continue to the installation of the Intune connector.

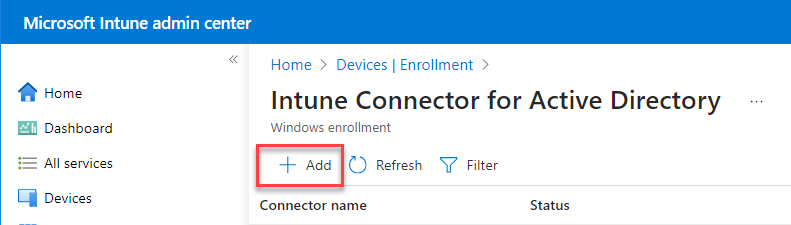
**Setup and Configure the Intune Connector**

If your server is a newly setup machine switch off IE Enhanced Security Configuration in the server manager. Also download the Edge browser because IE will not work when you sign in with the Intune Connector.

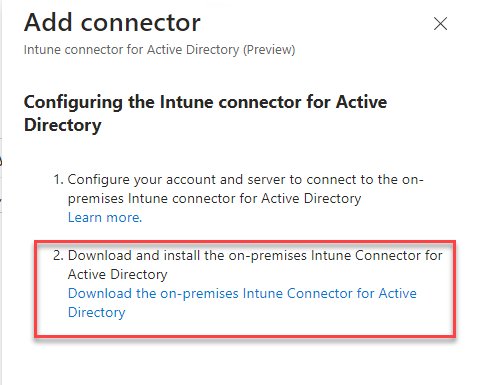
First, download the Intune connector from your Intune portal by going to Devices – Enrollment – Windows – Intune Connect for Active directory. Log in to the portal with either global admin or Intune administrator rights.



Click Add



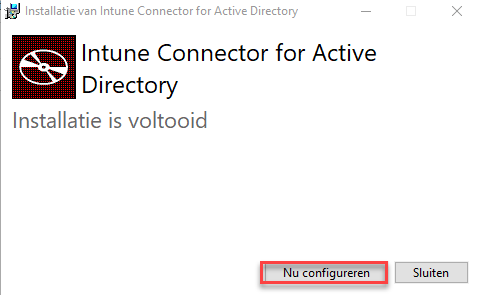
Download the connector



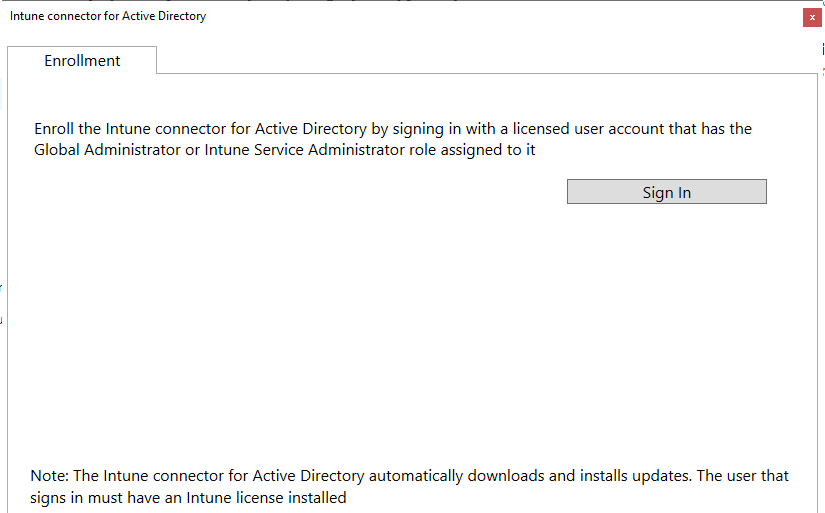
Accept the license terms and conditions and then select Install, you can change the install location if you want. The installer of mine comes in Dutch because I’m in this region but I assume you will know what to do 😉



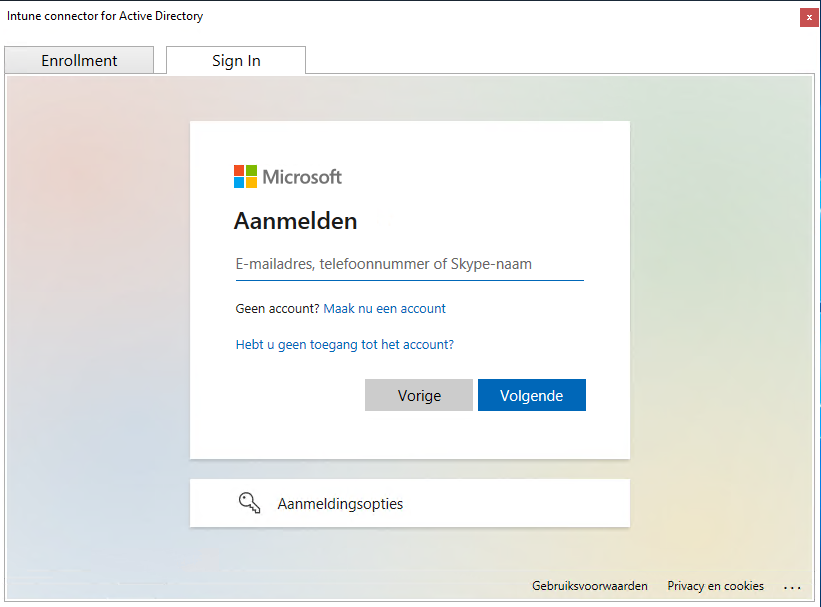
Once it has finished select Configure Now



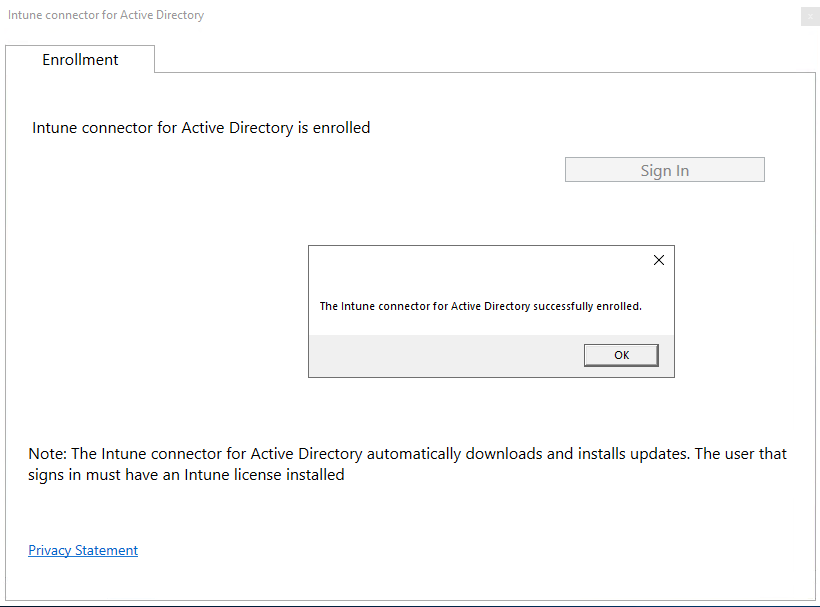
Next, select Sign In



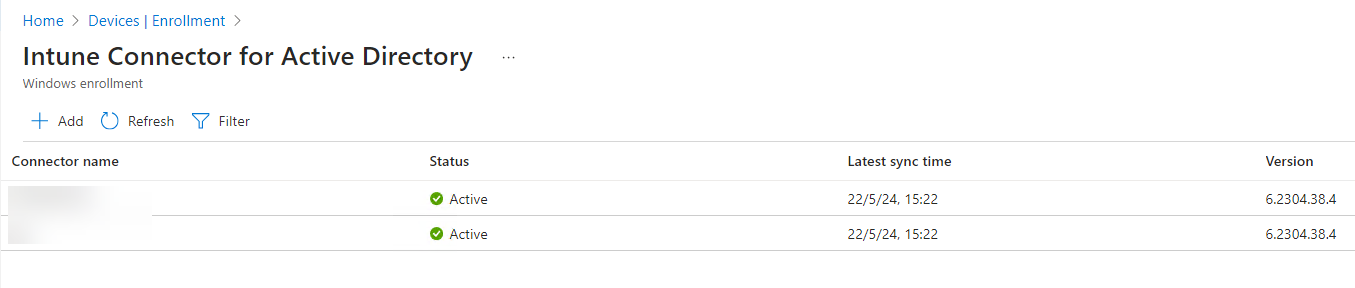
Sign in with an account that has at least an Intune license (a Microsoft 365 bundle license with the Intune feature enabled is also OK but a license overkill)  and a Global Administrator or Intune Administrator role.



Click OK



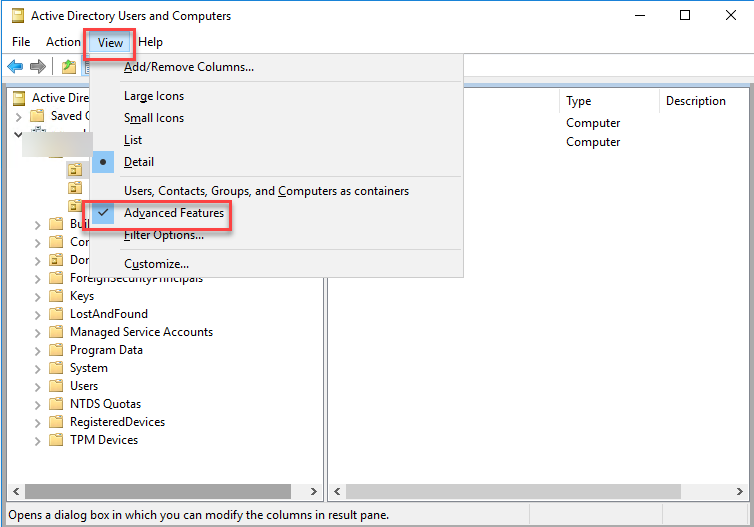
You can install multiple Intune Connectors on your environment of you want to. It will take 10 minutes to show the connector in your Intune portal.



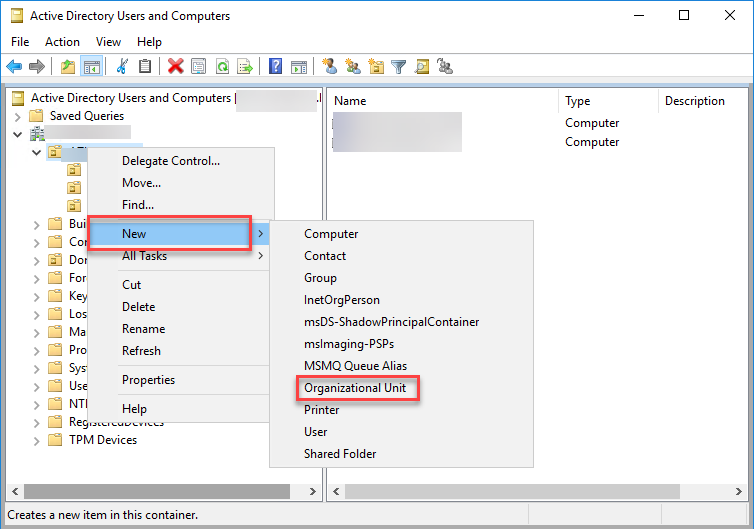
Now that your Intune Connector is up and running we can configure Delegate control on your local AD, let’s go!

**Configure Local AD OU Delegate Control for Microsoft Intune Autopilot Hybrid Entra ID**

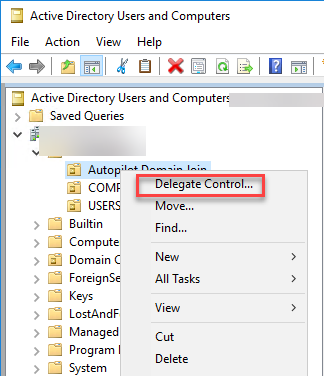
In this step we will need to configure a new Organizational Unit for out hybrid devices, You do not need a separate OU for your hybrid devices but you will need to configure delegate control, a seperate OU is recommended for this. 1st enable your Active Directory Users and Computers’ view in Advanced Features mode.



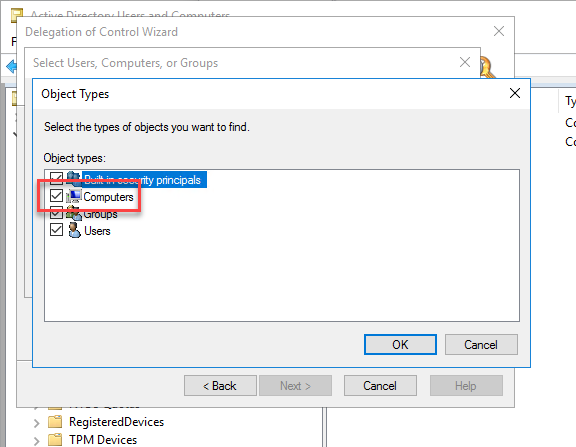
Create a new OU (If you use an existing one, you can skip this step)



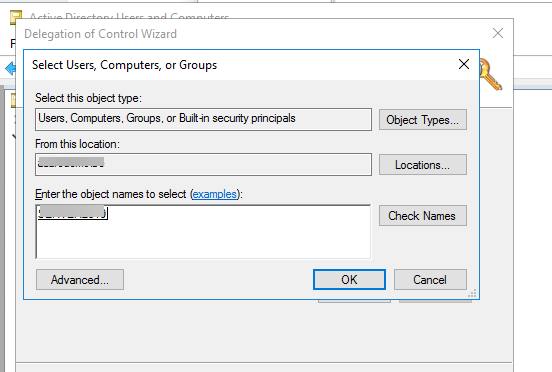
Right Click the OU and select Delegate Control



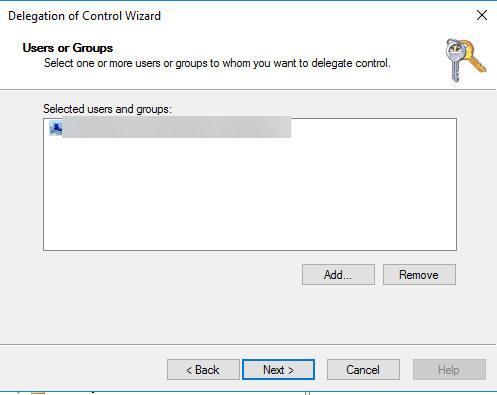
Select Computers



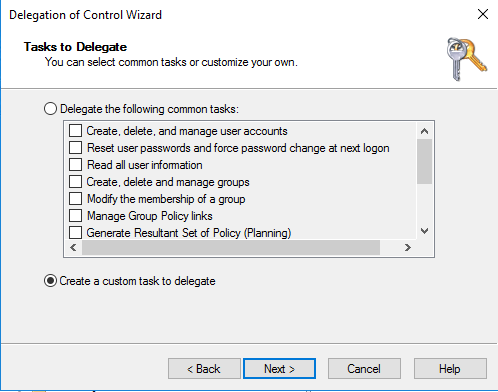
Add the server(s) that holds your Intune Hybrid Connector(s) and then click OK



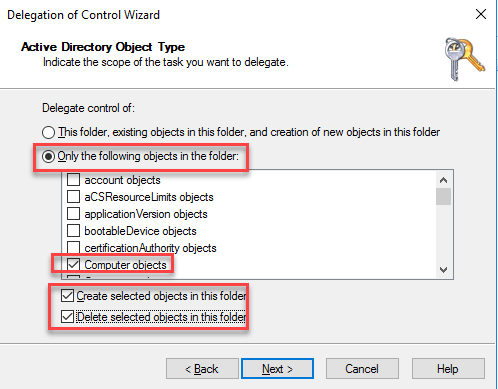
Click Next



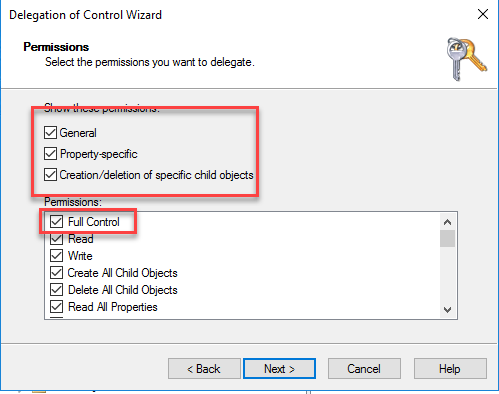
Select Create a custom task to delegate and then click Next



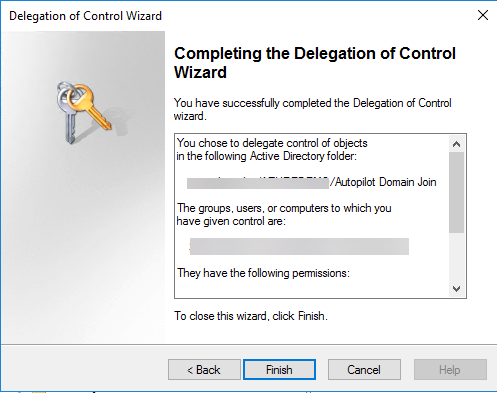
In the next pane, select Computer Object under Only the following objects in the folder, then select the Create selected objects in this folder and Delete selected objects in this folder checkboxes.



Check General, Property-Specific, Creation/deletion of specific child objects and Full Control



Finally select Finish



Now you have set the needed permissions on you local AD, now let’s go to the Intune part of the configuration.

**Hybrid join without Autopilot**

For Hybrid joins we have 2 options, from on-prem to Entra or from Entra to on-prem. The 2nd option is with Autopilot, the 1st option is done with GPO’s.

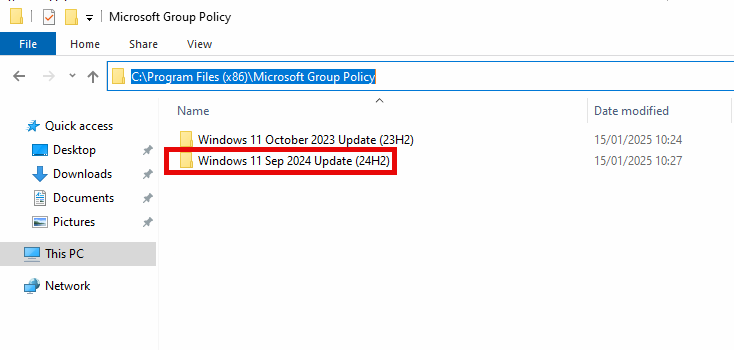
**Download and install the ADMX (Administrative templates) files**

[Here](https://www.microsoft.com/en-us/download/details.aspx?id=106254?wt.mc_id=MVP_377186) you can download the ADMX files.

Administrative Templates (.admx) for Windows 11 2024 Update (24H2)

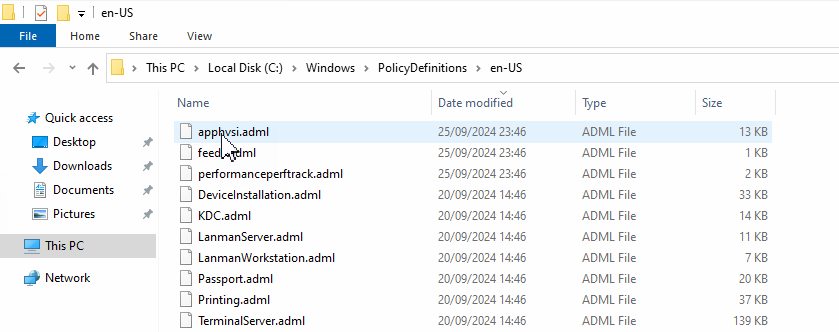
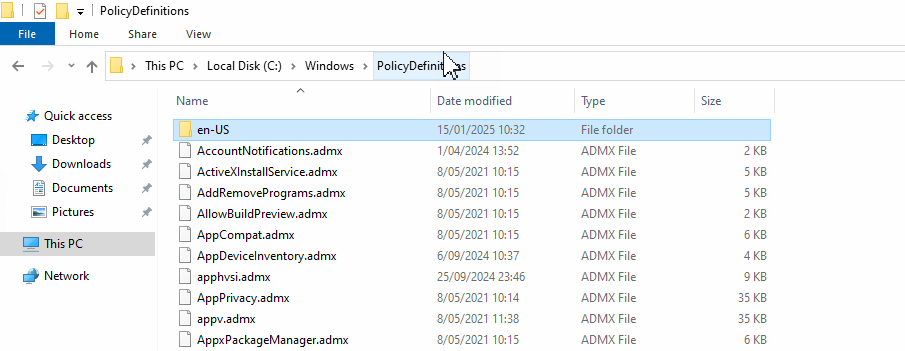
To download the .msi file that contains the .admx files:  
Click the download button.  
In the File Download dialog box, click Save .  
In the Save As dialog box, browse to the directory on your computer to which you want to save the .msi file.  
To start downloading the .msi file, click Save .

The files will be installed in C:\Program Files (x86)\Microsoft Group Policy.



The ADMX files are backwards compatible with older Windows versions

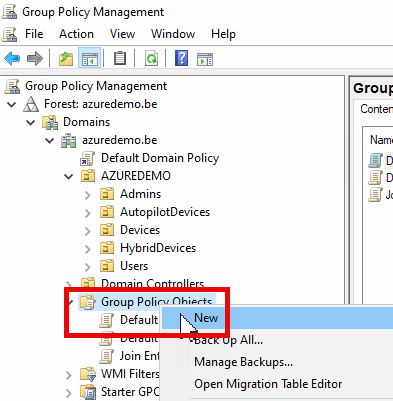
Now copy the ADMX files to C:\Windows\PolicyDefinitions and the correct language files ADML to C:\Windows\PolicyDefinitions\en-US



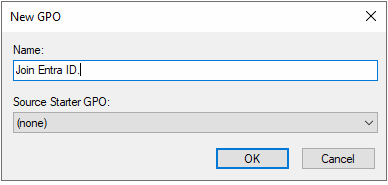
Now the ADMX files are in place.

**Create the GPO**

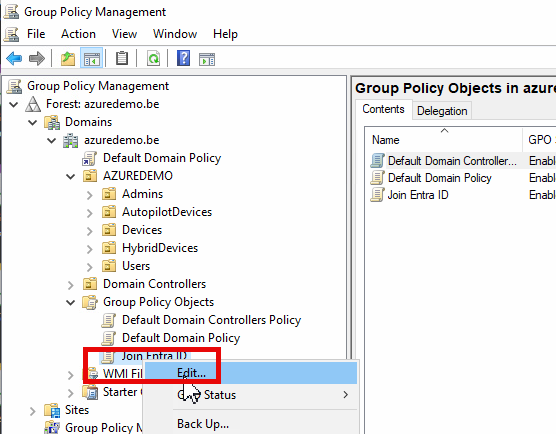
Open the Group Policy editor to create the GPO we need and click Group Policy Objects, right click and click new.



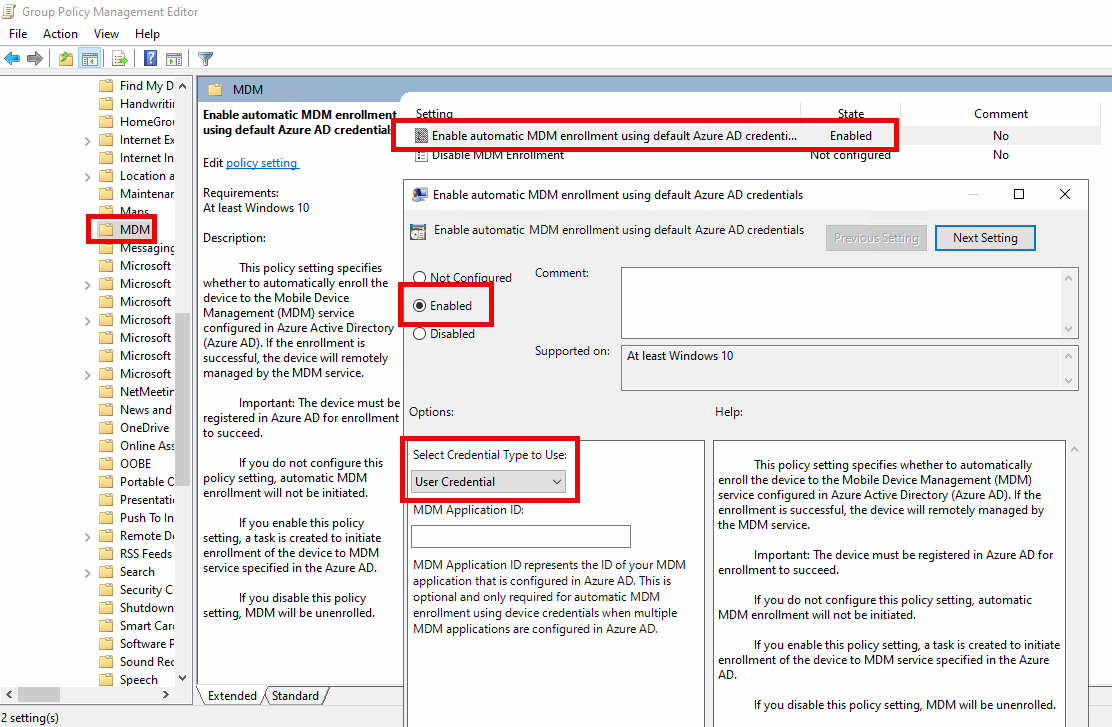
Name your policy e.g. Join Entra ID adn click OK.



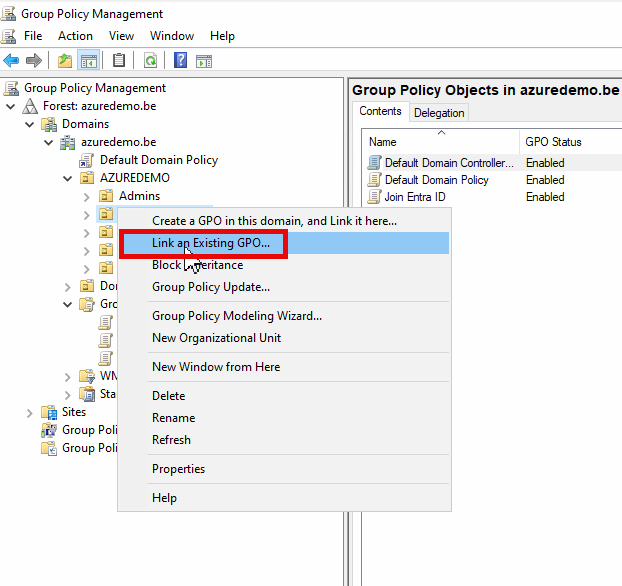
Now right click your created GPO and click edit.



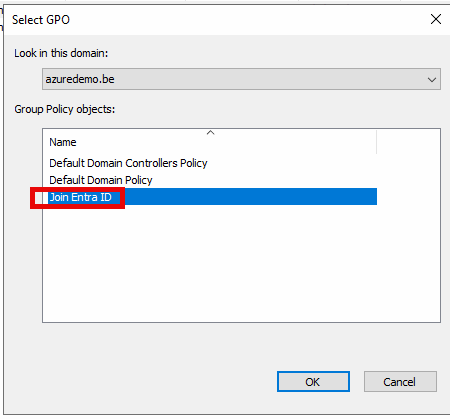
Navigate to **Computer Configuration – Policies – Administrative Templates – Windows Components – MDM**. Here configure the **Enable automatic MDM Emrollment using default Azure AD credentials.** Set the policy to **enable** and set the **Select Credential Type to Use to User Credential**.



Now close the editor, we now need to scope this GPO to the OU we created. To do this right click the OU and select Link an Existing GPO.



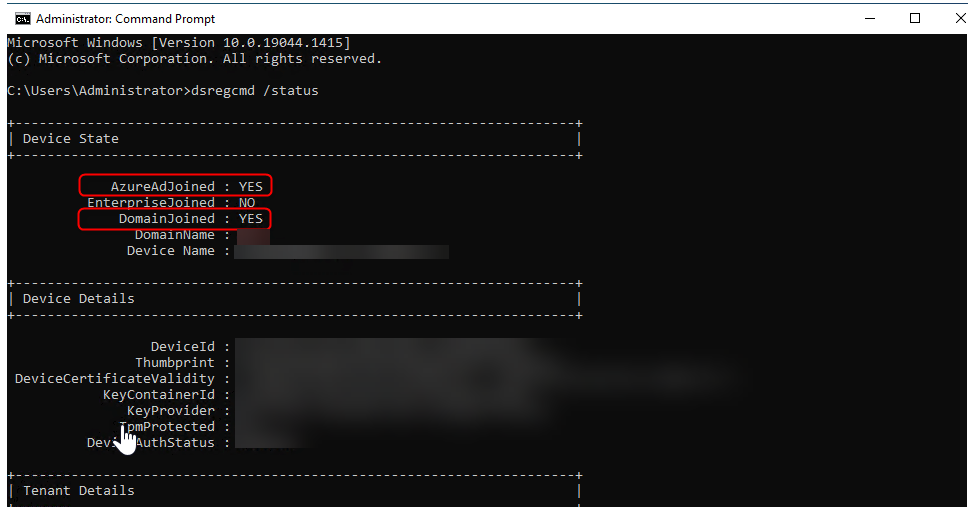
Now select your newly created GPO and click OK



From now on all devices that reside in this OU will get the GPO and will also join Entra ID.

It can take around 10 minutes before you will see the device in Entra ID, a reboot of the device can always kickstart the process. You can also use **gpupdate /force** in an elevated command prompt. To check this use this command in an elevated command prompt on the device: **dsregcmd /status**

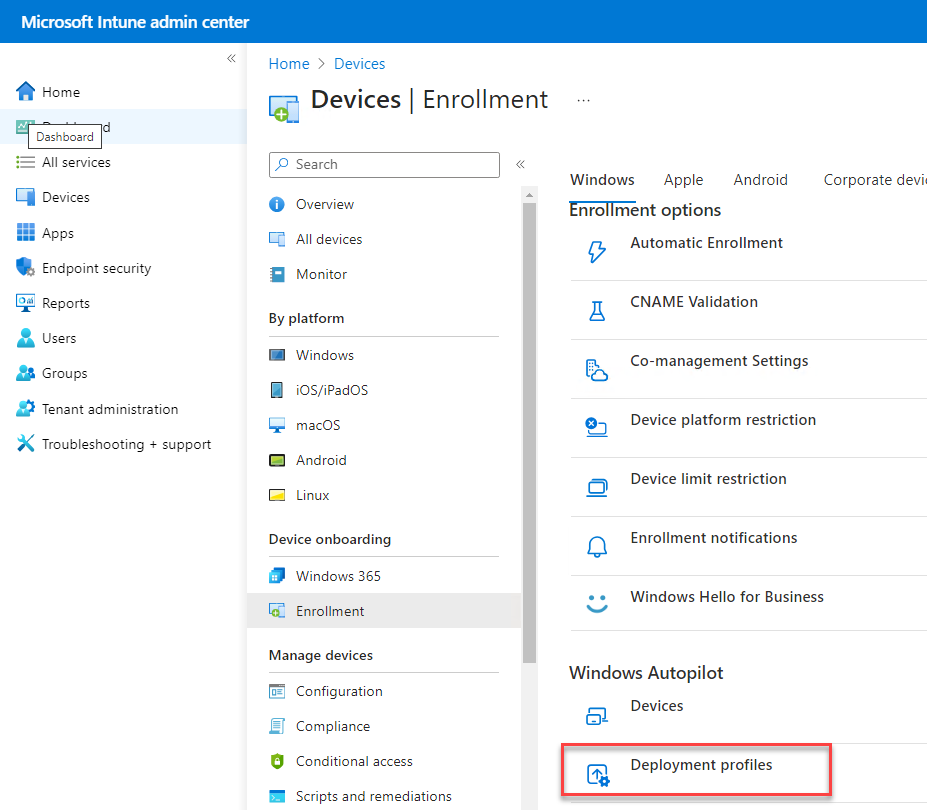
You will get this result:



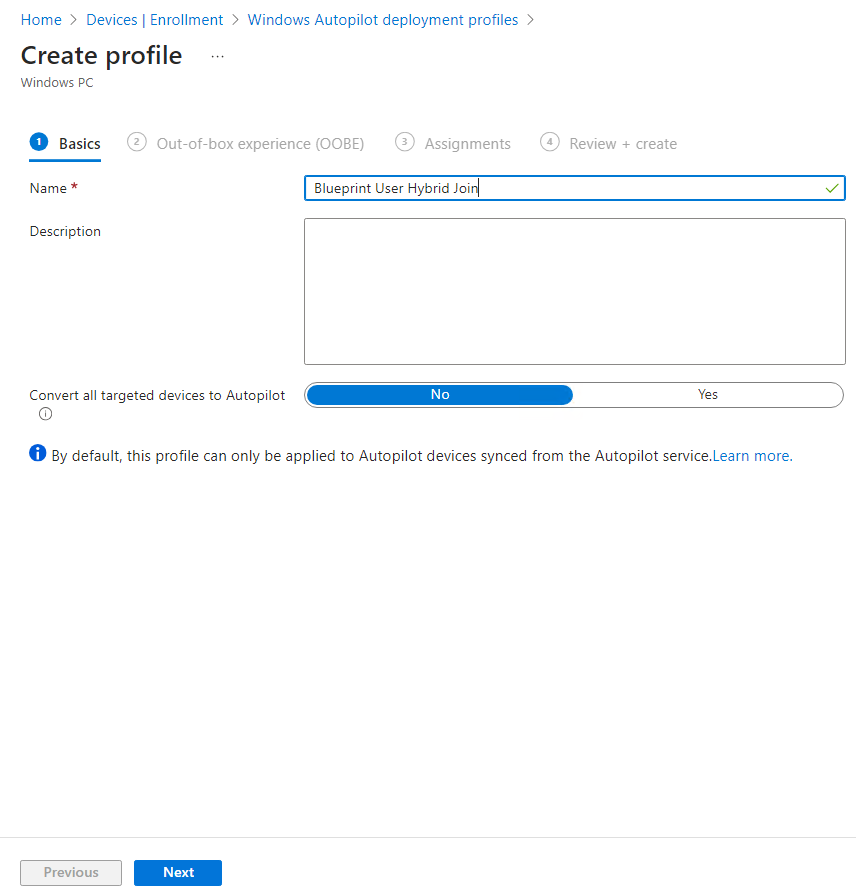
**Configure the Intune Stuff**

**Create an Autopilot Hybrid Deployment Profile**

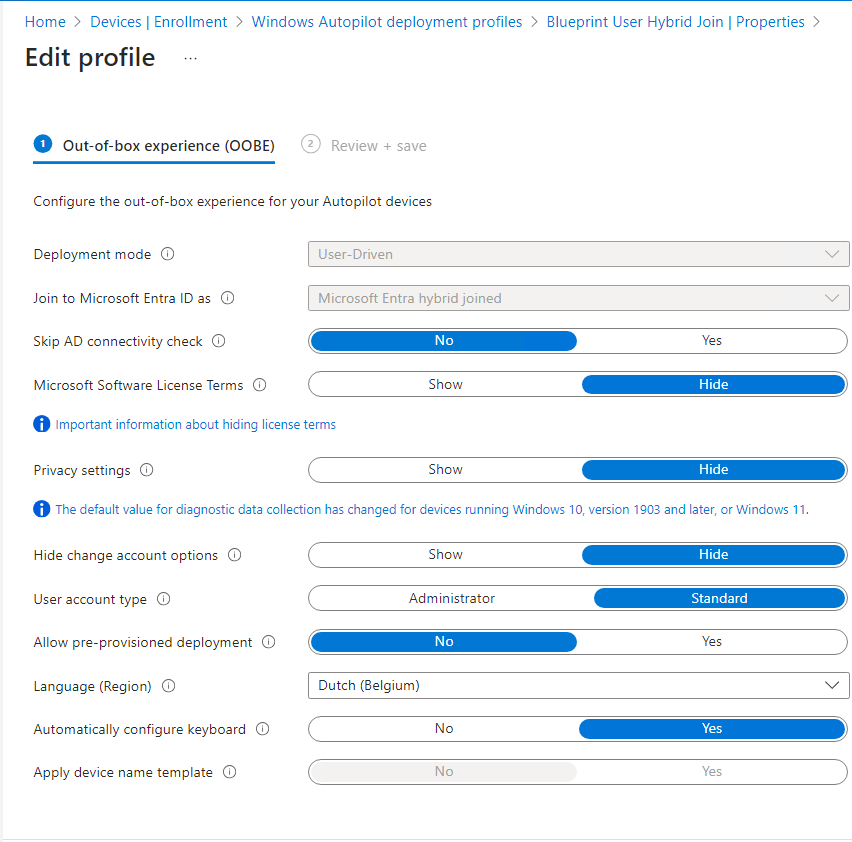
Now we must create an Auto Pilot Hybrid deployment profile. In the intune portal go to Intune – Device Enrollment – Windows – Deployment Profiles



Give your new deployment profile a name and description then press Next



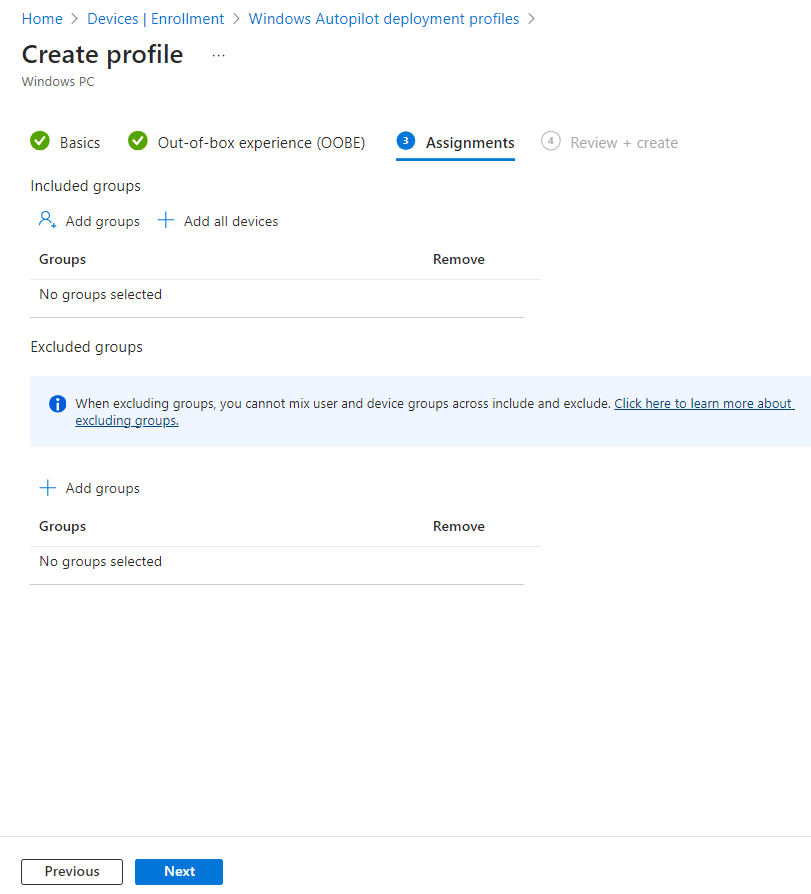
We will create a deployment profile for a standard user with no local admin rights on the device. Fill in the options a stated in the screenshot. You can change the region and keyboard selection if you want according to your specific needs. Click next when your are done



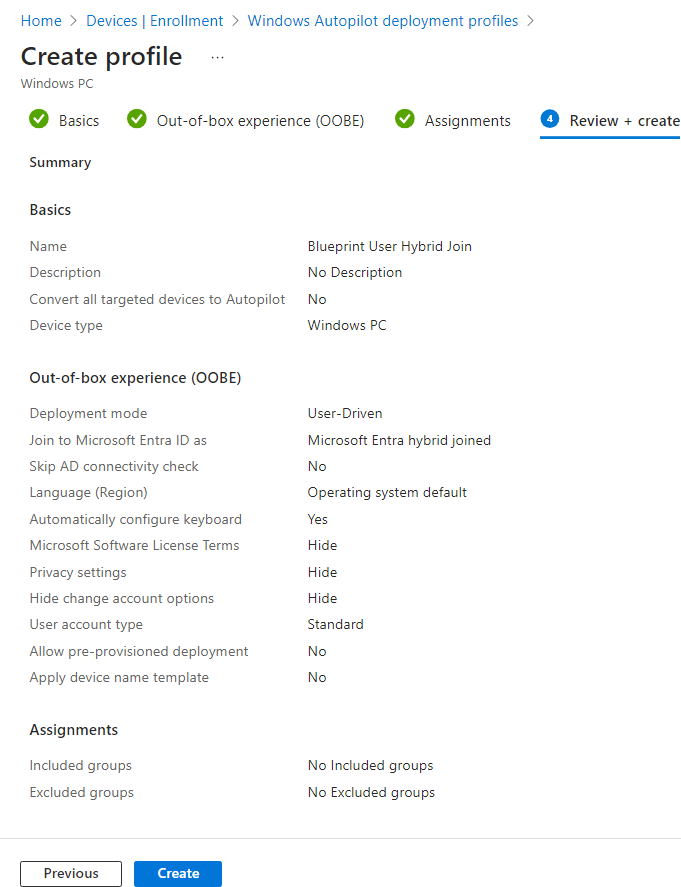
You can also set the Allow pre-provisioned Deployment to yes. If you do so you can use this deployment profile also for pre-provisioned Autopilot. More info on pre-provisioning (formerly know as the OOBE Experience) check this Microsoft article: [https://learn.microsoft.com/en-us/autopilot/pre-provision](https://learn.microsoft.com/en-us/autopilot/pre-provision?wt.mc_id=MVP_377186) Pre-provisioning is started by pressing the Windows key 5 times at the company sign in screen. Also you will notice that you cannot apply a device name template, this is by design and needs to be configured in the Domain Join profile later on in this guide

Windows Autopilot for pre-provisioned deployment

Now for the assignments, at this point i will not assign this deployment profile just yet, more info later in this guide. Click next.



On the Review and Create screen click create.

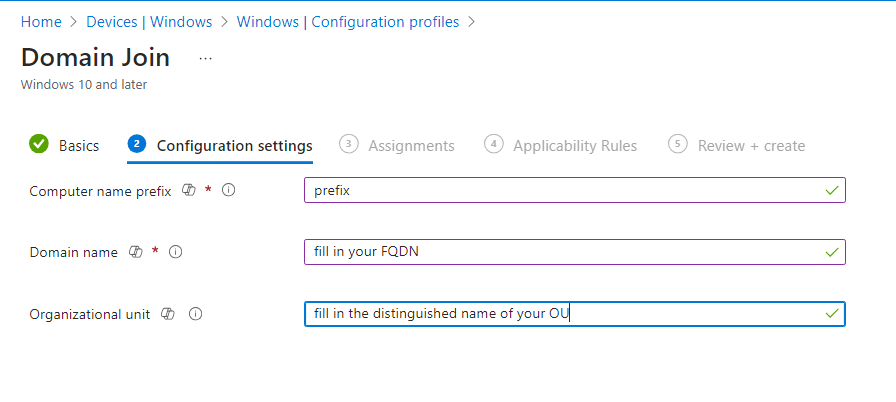


Now you have created a Hybrid Join enabled deployment profile, let’s head over to the creation of the Domain Join profile in Intune.

**Create an Intune Hybrid Domain Join Configuration Profile**

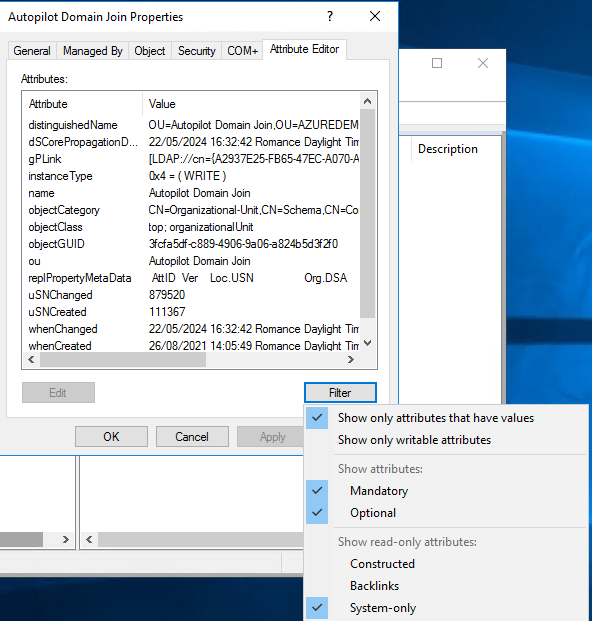
Next, we must create a Intune Configuration profile to tell our devices to hybrid domain join.

In Intune go to Devices – Windows – Configuration Profiles – Create – New Policy – select the platform as Windows 10 or later and the profile type Templates and choose Domain Join and give you profile a name.

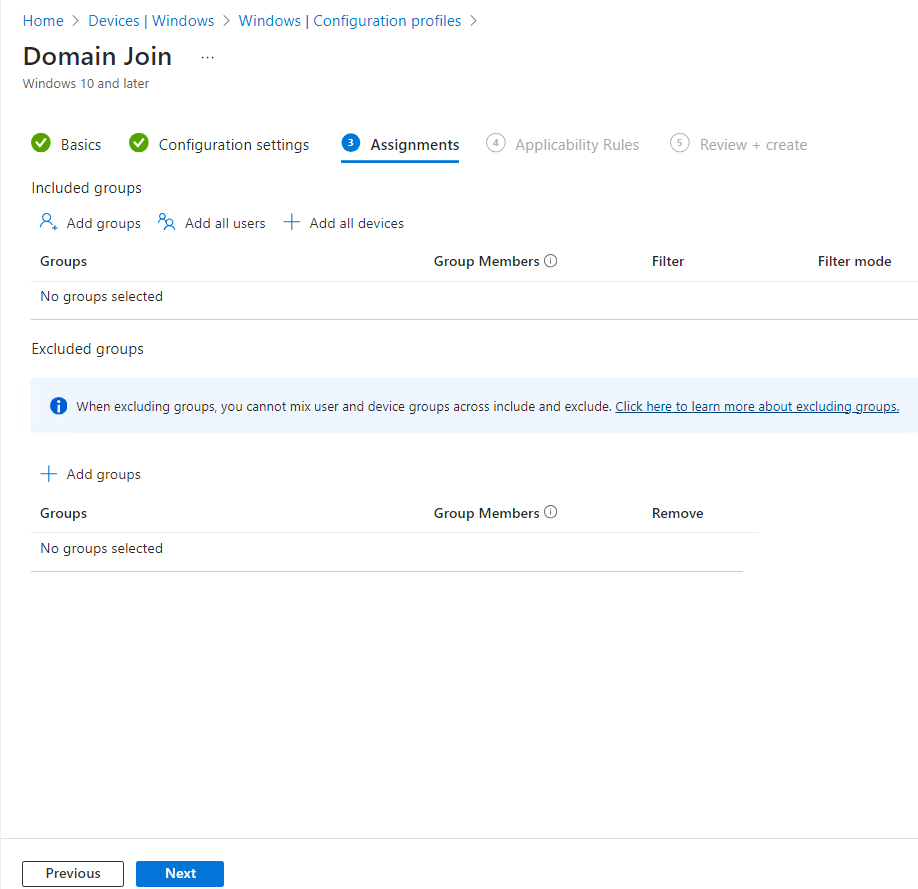


As describes in the previous info box, here is the place where you can specify a name for your device. You cannot use the %SERIAL% or %RAND:X% macro’s here. I find this very inconvenient because you can set a prefix and Intune will fill in the rest of the characters randomly. You are obliged to specify a prefix!

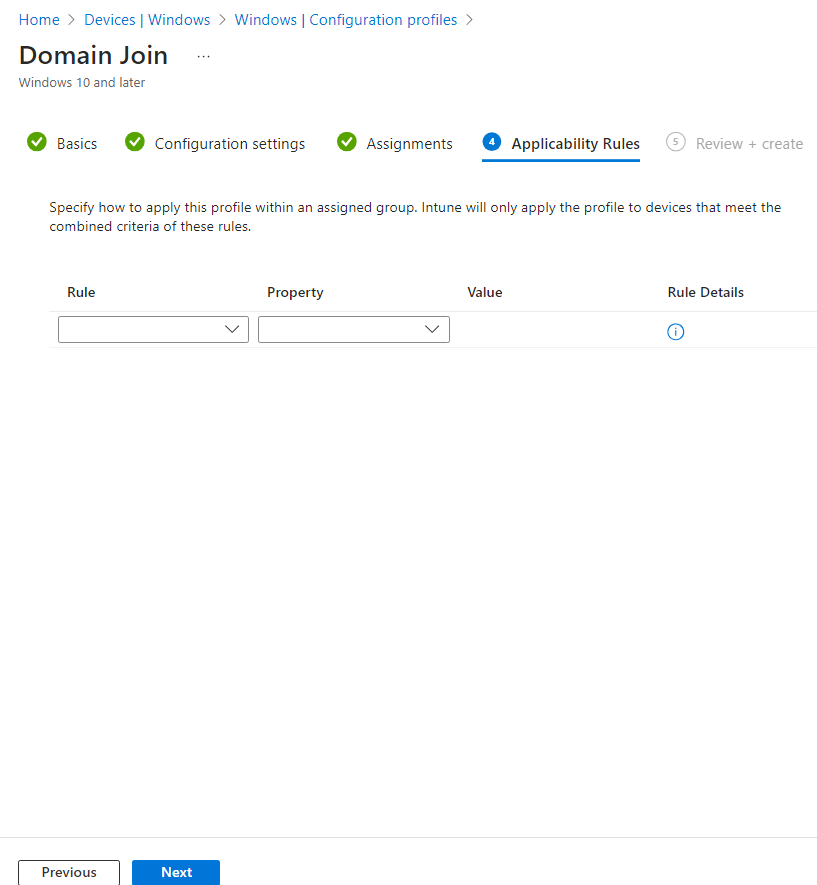
To get the OU in distinguished name format go to your Active Directory Users and Computers (we have enabled the Advanced Features view before), right click your OU where you have set the delegated control to, select properties – Attribute Editor and look for distinguishedName. If it is not visible you will need to set the filters correctly. Take note of the distinguishedName attribute.



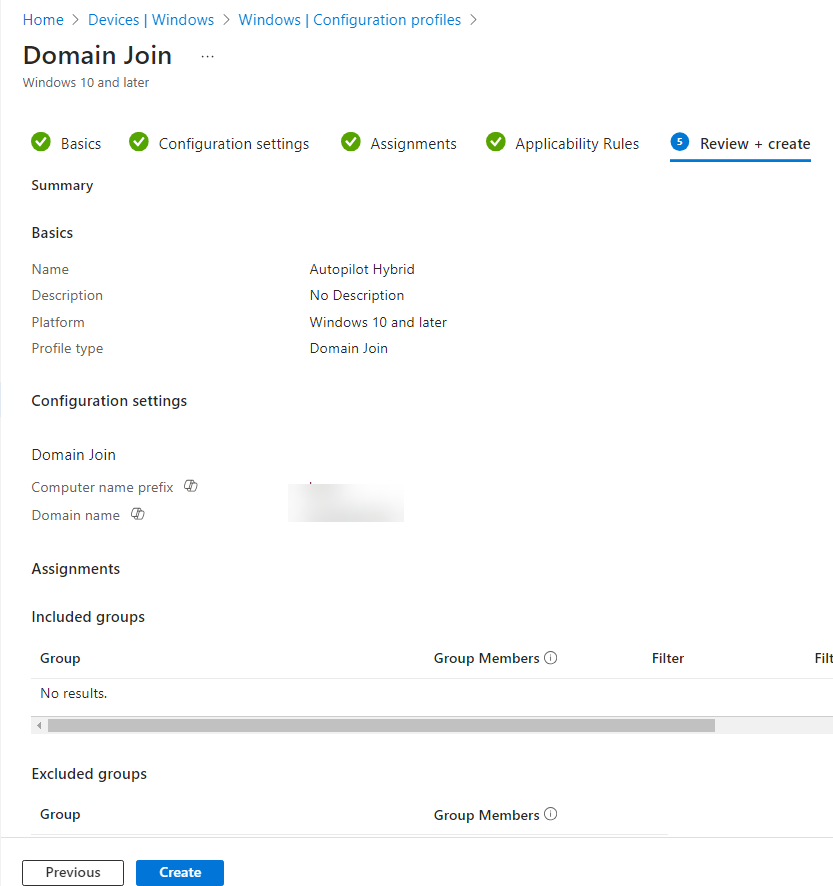
For the deployment profile go to Devices – Enrollment – Deployment profiles – click on your created deployment profile – properties. Click Edit next to assignments and select your Dynamic group.



At the applicability rules page, click next



at the Review and Create screen click create.



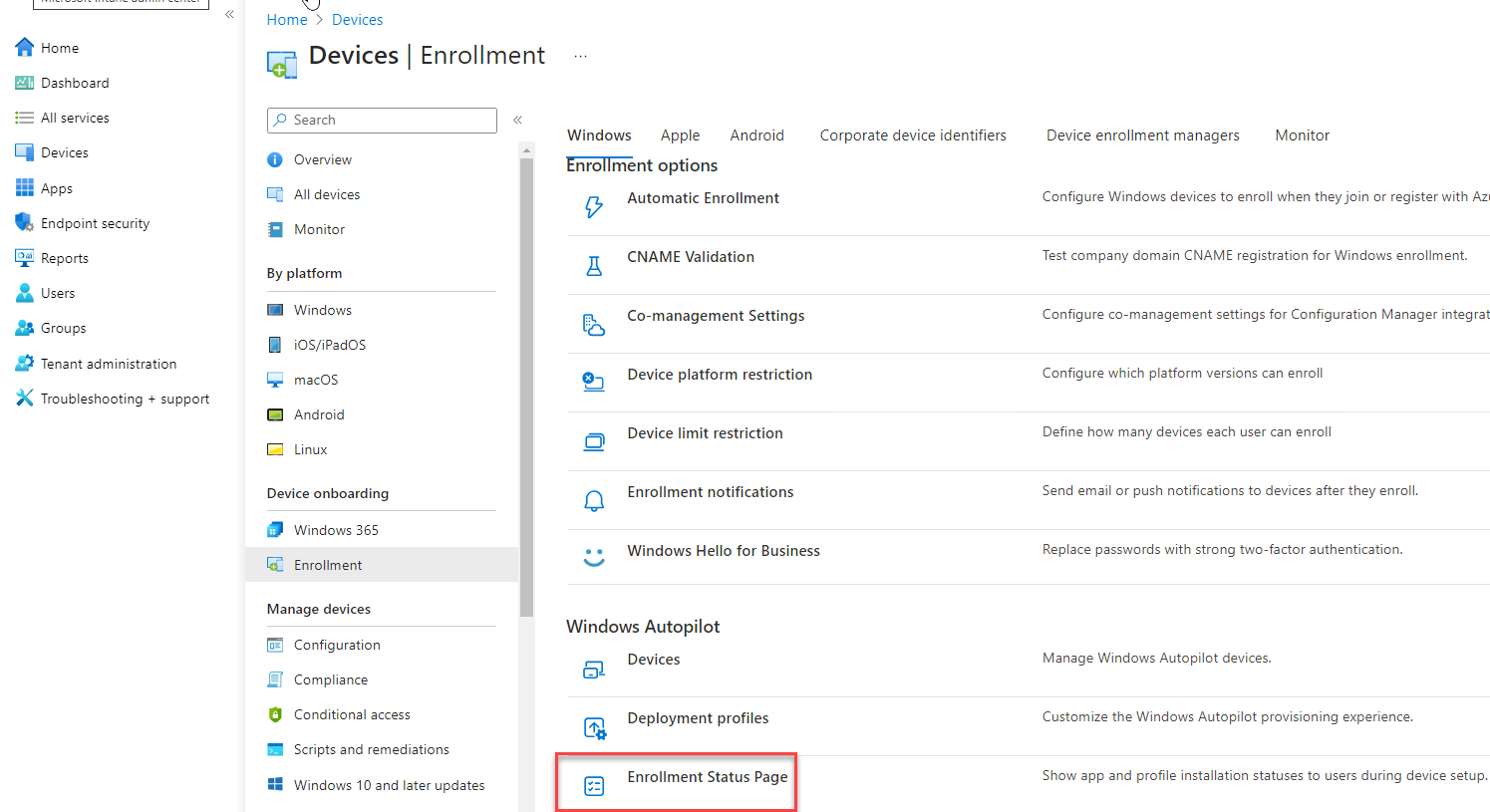
**Create the ESP (Enrollment Status Page) – Not to be used in an Autopilot Hybrid Entra ID join!**[**See Breakpoint 5**](https://intunestuff.com/2024/05/23/microsoft-intune-autopilot-hybrid-entra-id-azure-ad-join-the-complete-guide/#Breakpoint_5_%E2%80%93_The_device_wont_fetch_the_required_user_token_Azure_AD_PRT)

When a user signs into a device for the first time, the Enrollment Status Page (ESP) displays the device’s configuration progress. The ESP also makes sure the device is in the expected state before the user can access the desktop for the first time. The ESP tracks the installation of applications, security policies, certificates, and network connections.

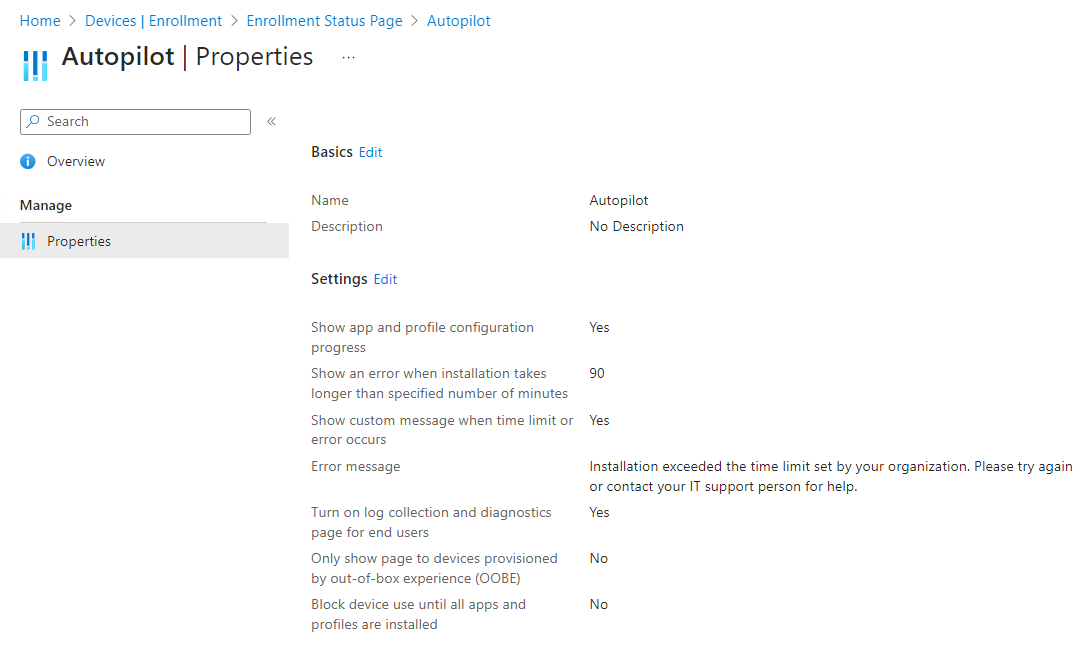
An administrator can deploy ESP profiles to a licensed Intune user and configure specific settings within the ESP profile. A few of these settings are:

* Force the installation of specified applications.
* Allow users to collect troubleshooting logs.
* Specify what a user can do if device setup fails.

The enrollment status page is created by going to the Intune portal – Devices – Enrollment – Enrollment Status Page



Click Create – Give the ESP a name e.g Autopilot and configure as in the screenshot.



These settings work for me, if you have a lot of apps configured to install in your deployment you can consider to increase the time on the show an error when installations takes longer than specified number of minutes. In [this article](https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status#create-new-profile) all settings are being explained individually.

Now you have everything in place to perform Autopilot Hybrid Entra ID joins. Let’s dive into the creation and assigning of groups for your configured profiles.

**Create Dynamic Device Groups Based on Group Tags**

**Clarifying**

Now to get al your configured policies assigned to specific groups we will need to create groups, i will create these groups in Entra ID because here we can create dynamic groups which will be filled up automatically with a dynamic query. You cannot create a dynamic group on your local AD. This will minimize your admin work instead of using assigned groups. With assigned groups you will have to put in the devices manually in these groups, dynamic groups will automate this for you.

You may ask yourself why dynamic device groups? I have written an article on assignments in Intune, read this [here](https://intunestuff.com/2023/12/15/intune-assignments-user-groups-vs-device-groups-a-short-blog/). Check out the matrix at the bottom of that page.

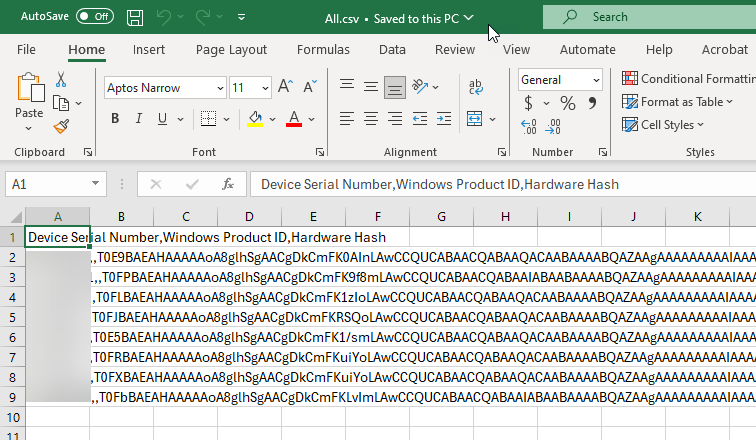
For Autopilot i always use dynamic groups based on the group tag of the autopilot devices, this group tag will be filled in in the dynamic query of that specific group. To get your devices into autopilot check out this article [here](https://intunestuff.com/2024/01/08/how-to-get-the-hardware-hash-imported-into-intune-without-going-through-the-full-oobe/). You will need to get the hardware hash of the device(s) imported into Intune. You can do this by following the steps in the guide.

These manual steps to get your devices into Autopilot are only for existing devices already in your possession

You can also use the setting in the deployment profile convert all targeted devices to Autopilot. This means that all devices this specific deployment profile is assigned to will be converted to Autopilot. (This is an option a rarely use)

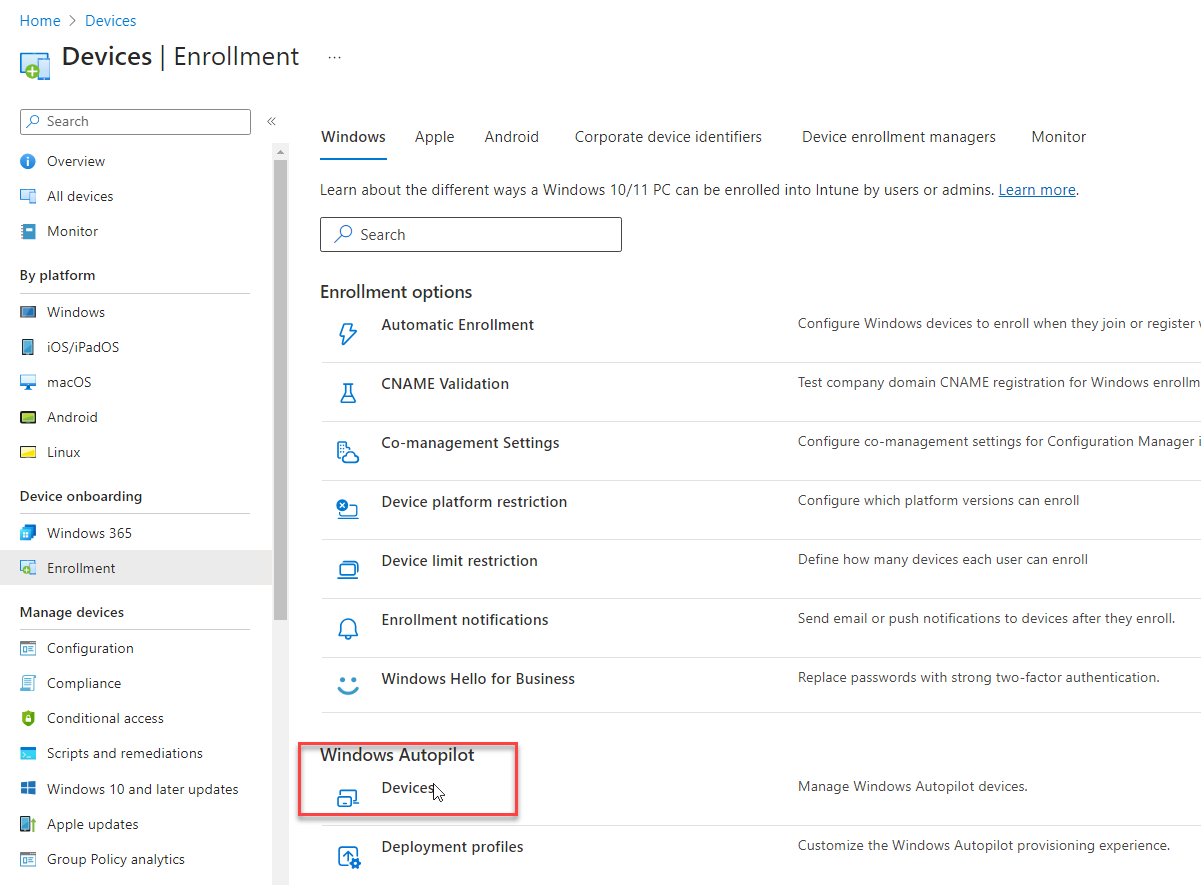
Also if you are ordering **new devices** you can ask your reseller to order the devices Autopilot ready, if you do this your reseller will sent you a csv file with the hardware hashes of your ordered devices. You can also give your reseller access to your environment and he will upload the devices for you.

An Autopilot csv file will look like this:

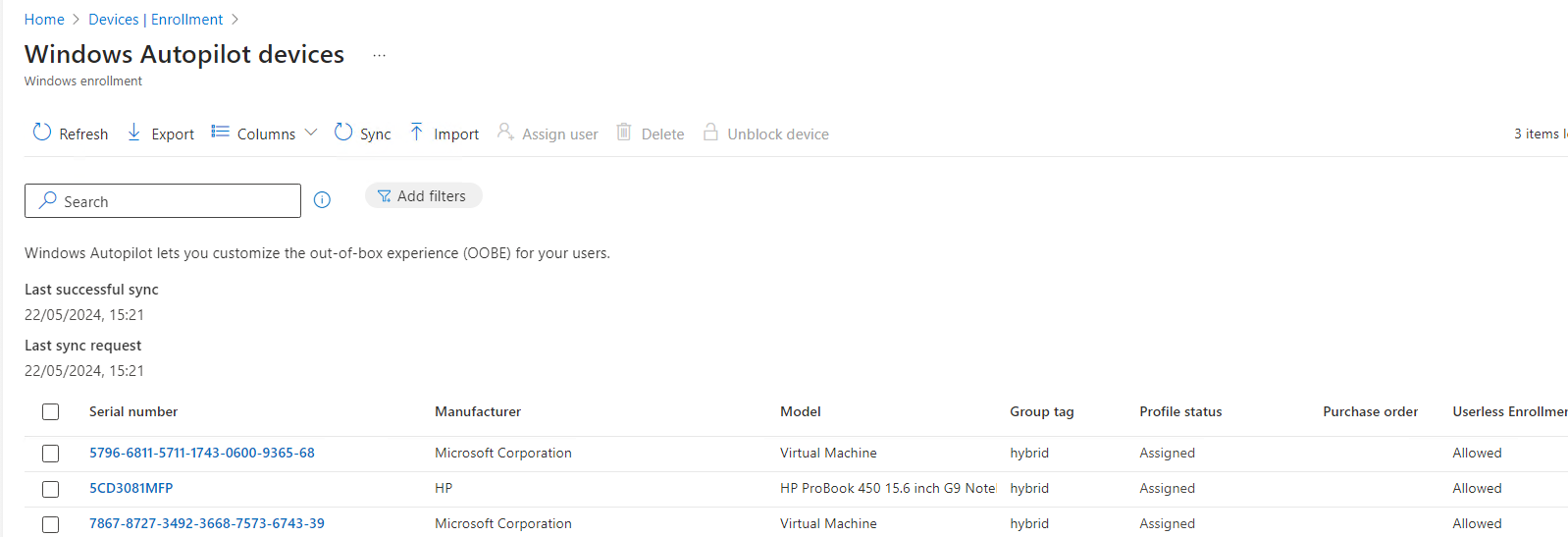


**Group tags**

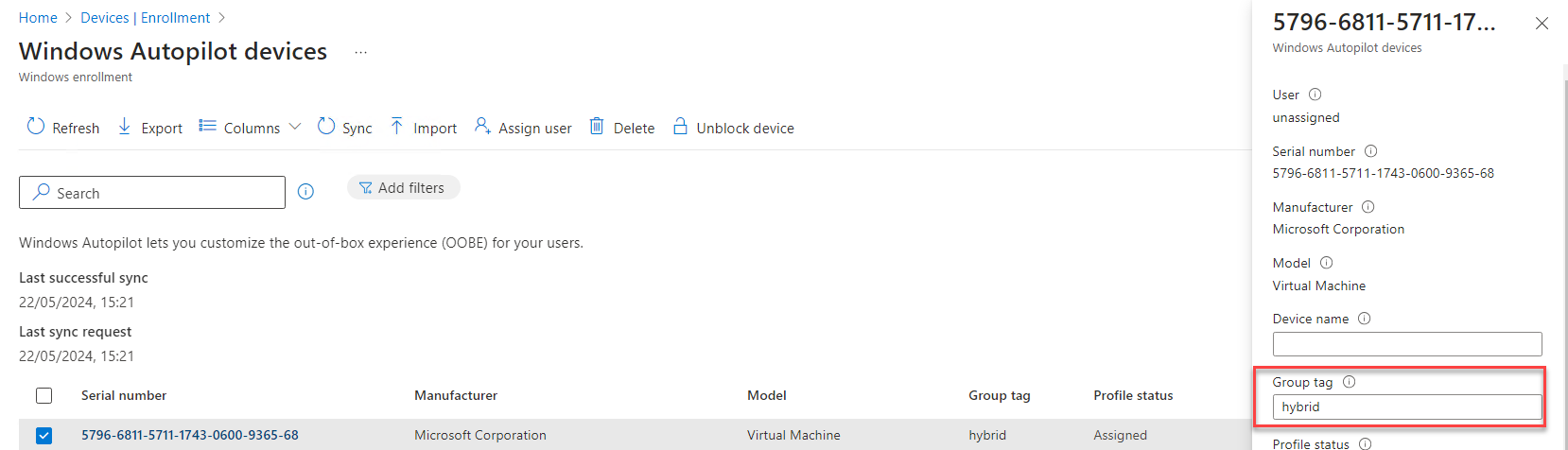
Let’s say you have uploaded a device in Autopilot by following the manual process or you have devices uploaded with the csv file from your reseller or your reseller has added a list of devices. Go to the Intune portal – Devices – Enrollment – Devices.



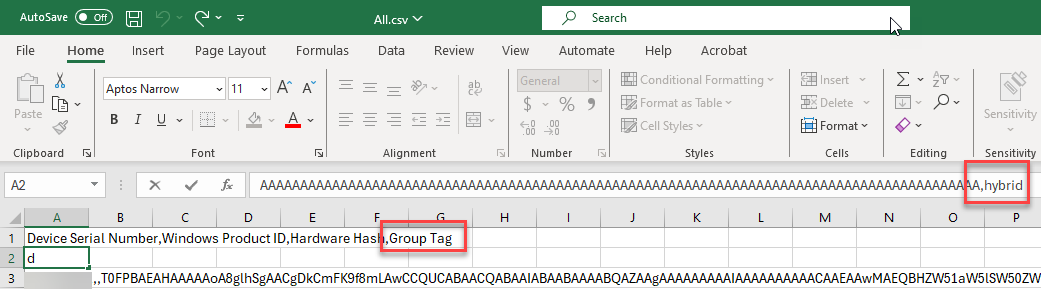
Here you will see your uploaded devices with their serial number.



Now if you click on a device a new pane will open on the right hand side, in this pane you can fill in your group tag. In this case i have chosen for **hybrid**



You can also enter the group tag in the csv file before you upload the csv file. Open the csv file and add Group Tag to line 1 (no space and use capitals like in the screenshot). At the device lines completely at the back of the line add the group tag that you want, in this case hybrid. You can create different group tags according to the deployment profiles you have created of course.



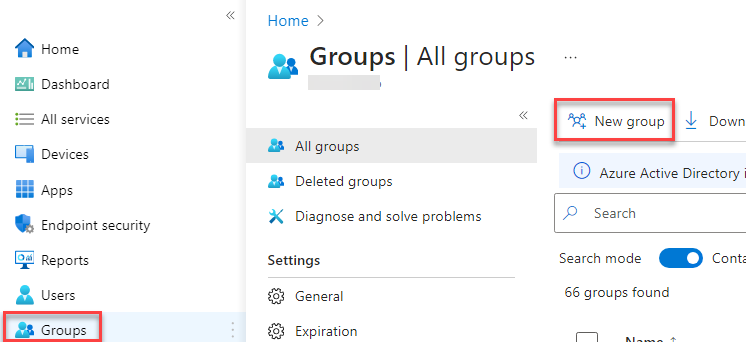
Now that the group tag is in place we can continue to create dynamic groups based on this group tag.

**Creating Dynamic Groups**

To create the dynamic group based on the group tag follow these simple steps.

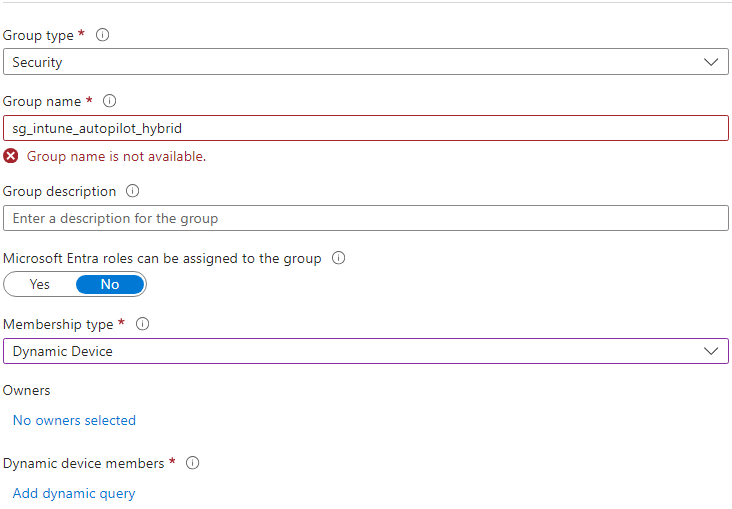
Go to either the Intune Portal or the Entra ID portal, I will create the group from the Intune portal.

Click on groups – New Group

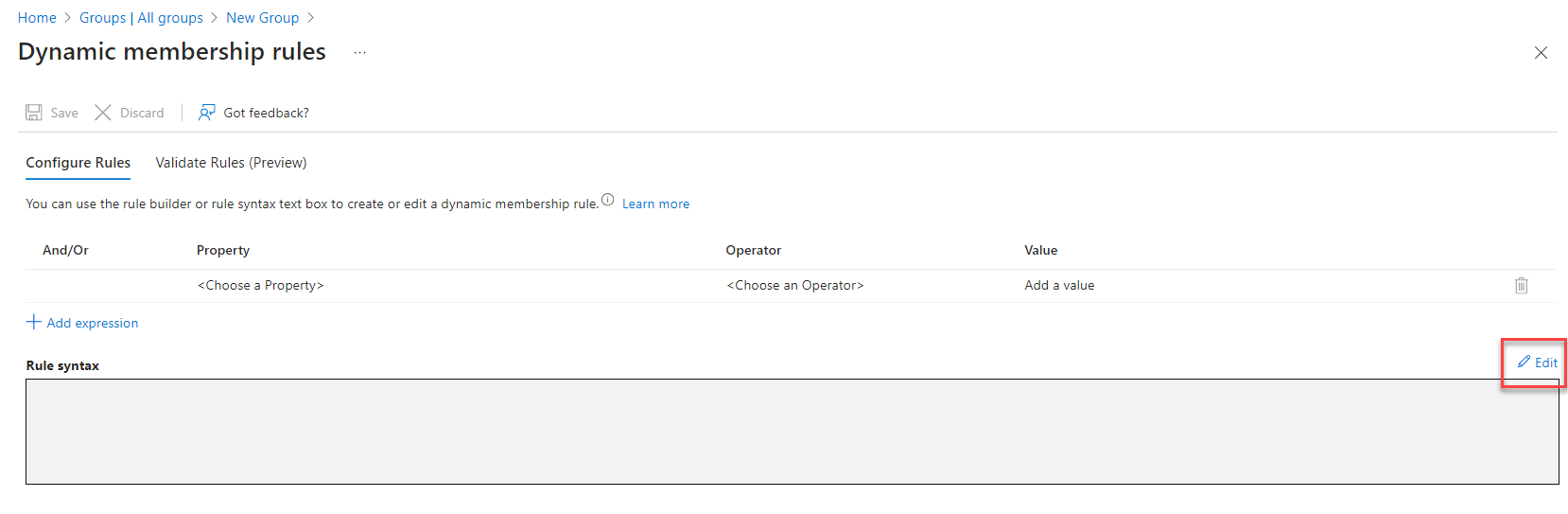


As group type select security, enter a group name, enter a description if you want. If you want to assign Entra ID roles in the future set this to yes (you cannot change this after the creation of the group), membership type is Dynamic Device, select an owner if you want.

I have already created this group so that is why the group name is not available. Please ignore this.

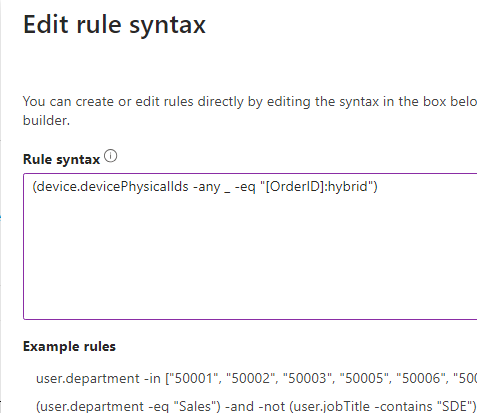


Now for the dynamic query, click on add dynamic query and click edit on the far right side.

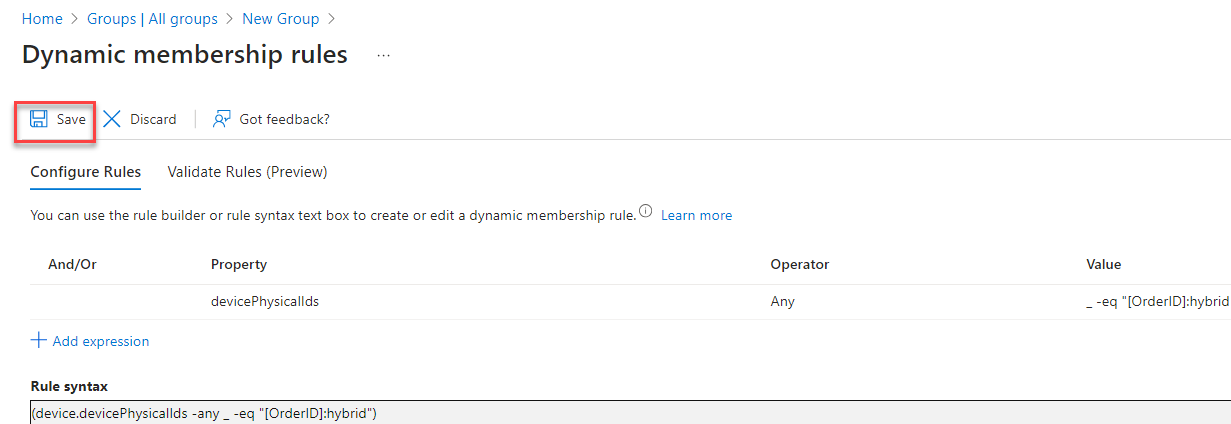


In the Edit rule syntax enter this code

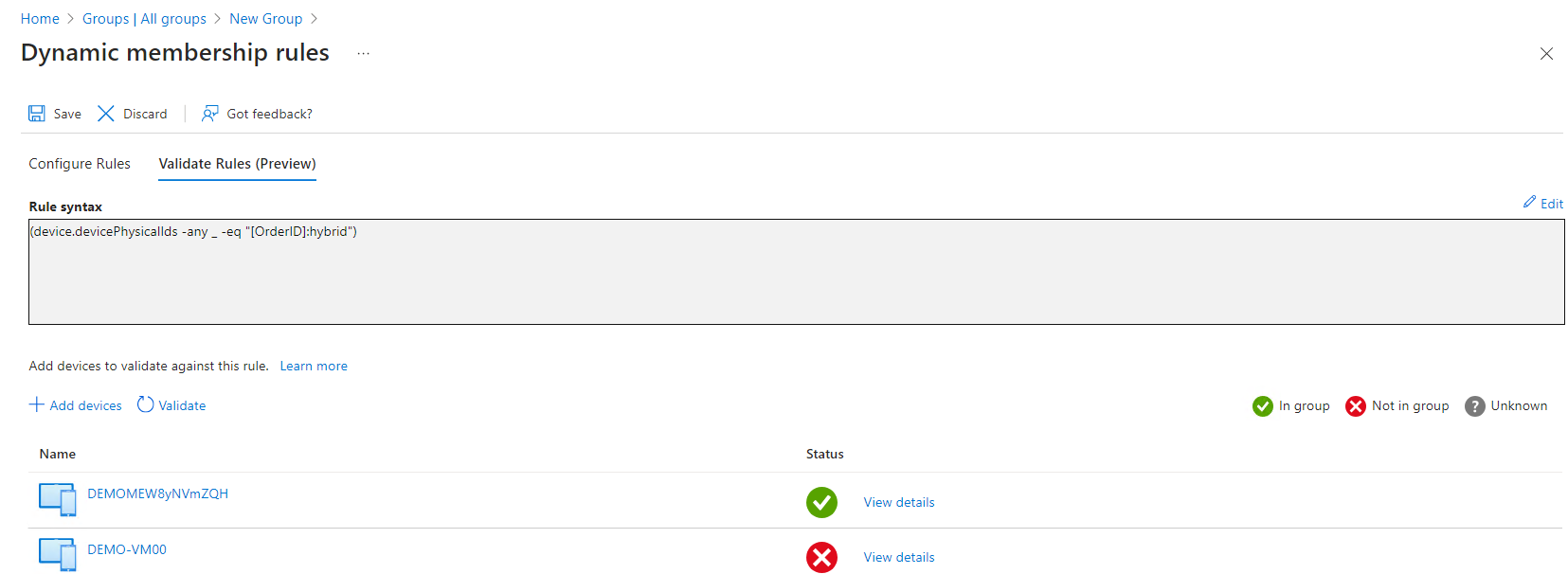
(device.devicePhysicalIds -any \_ -eq "[OrderID]:hybrid")



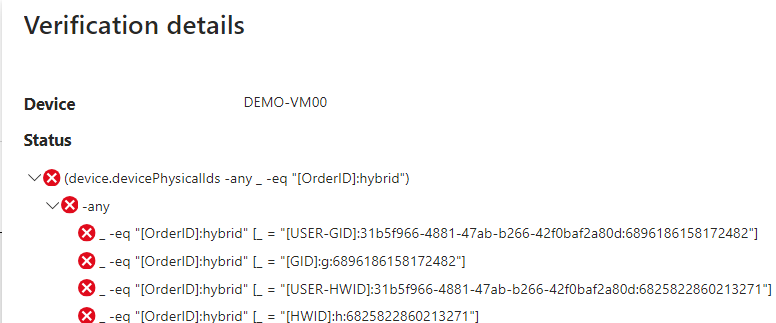
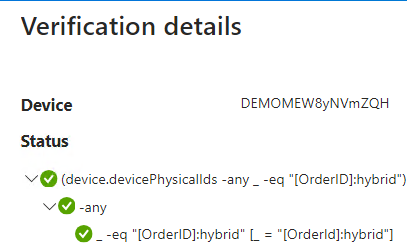
Now click OK and save your group



You can also validate your group to see if your device is eligible. To do this click on the Validate rules button – Add Devices – choose your device(s) from the list. In this example i will show you a device that is eligible and not.

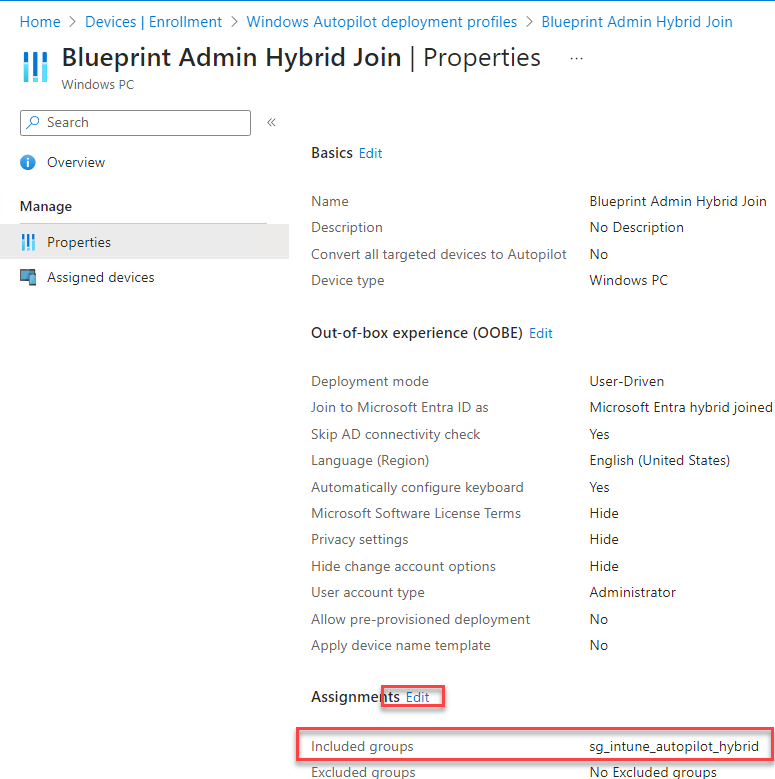


If you click on view details you can see the different outcomes

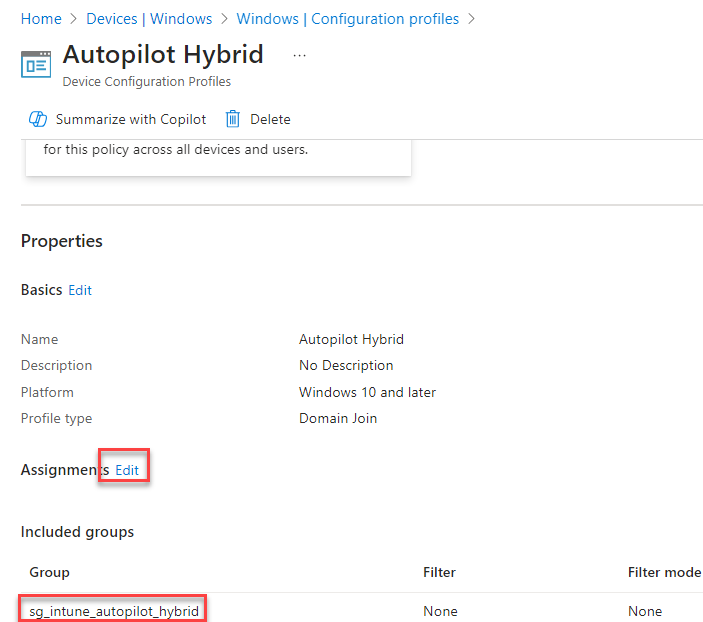


Ok, so now we have also our dynamic device group. This group needs to be assigned to the deployment profile and our domain join profile. To do this go to the Intune portal.

For the deployment profile go to Devices – Enrollment – Deployment profiles – click on your created deployment profile – properties. Click Edit next to assignments and select your Dynamic group.

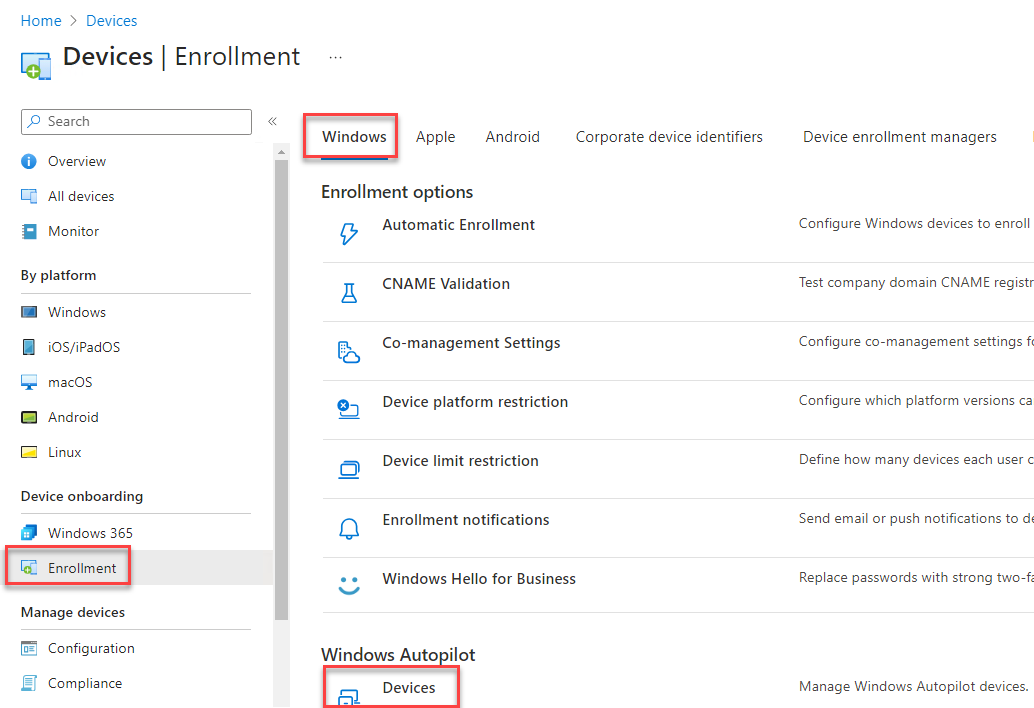


For the deployment profile go to Devices – Windows – Configuration profiles – click on your created configuration profile. Click Edit next to assignments and select your Dynamic group.

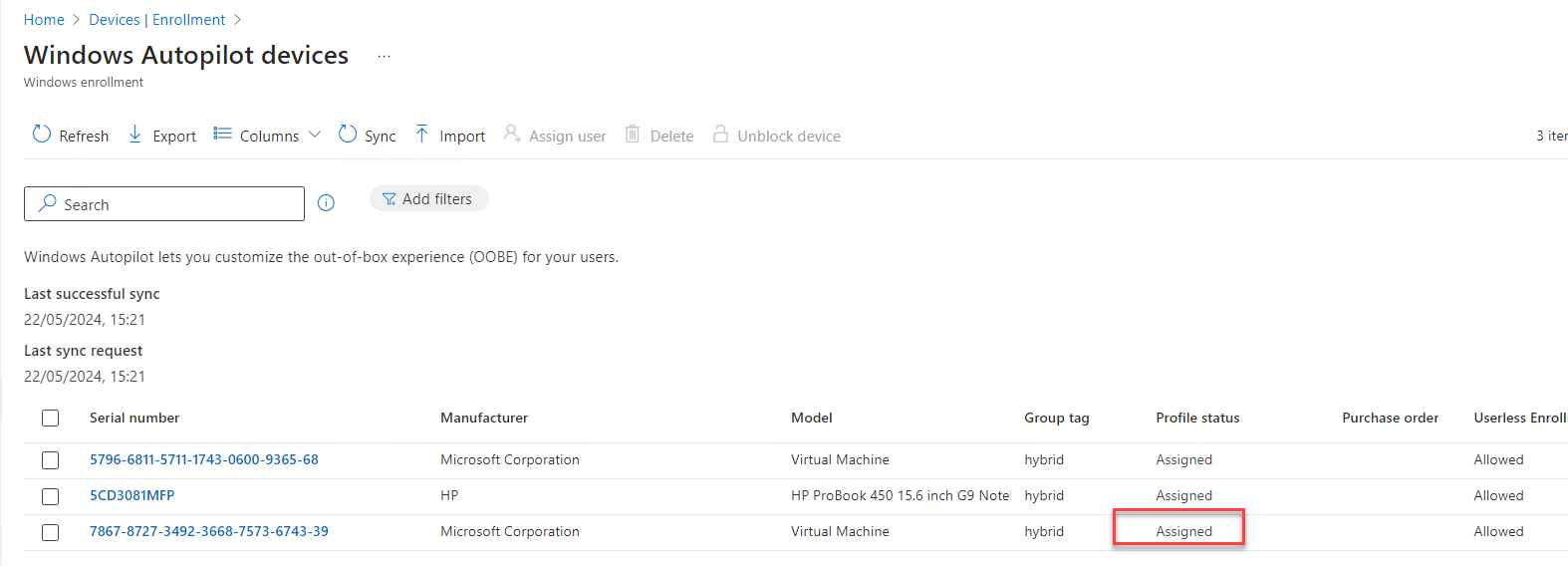


Ok good job! Now we got everything in place to get started with our enrollment you say? Well not quite to be honest. For those who are working with Intune already you know that you need a bit (a lot) of patience.

Now that we have assigned the group to the deployment profile and domain join profile we need to go back to the Intune portal – Devices – Enrollment – Windows – Devices

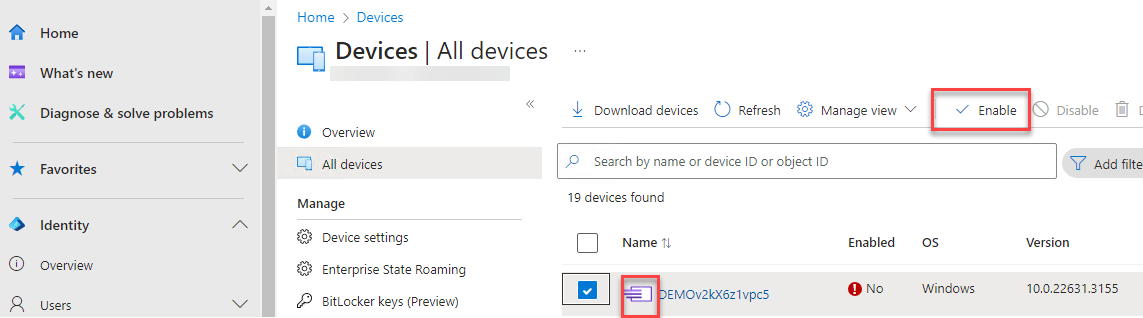


Here we need to make sure that the deployment profile is assigned to our device. We want to see assigned next to our device.



The time from when you add the group tag until the device status says assigned here can take up to 30 minutes. So please be patient. Also if you upload a device to the Autopilot devices it can take up to 15 minutes to sync.

If your device says assigned, also take a look in the Entra ID portal in the device section. You will notice that your autopilot device has another icon then all other devices. Select the device and click enable.



You cannot delete an autopilot device from Entra ID, if you want to delete is you first delete it from the devices at the enrollment section in Intune, after that you can go back to Entra ID, the icon of your autopilot device has been changed back to a regular device icon and now you can delete it.

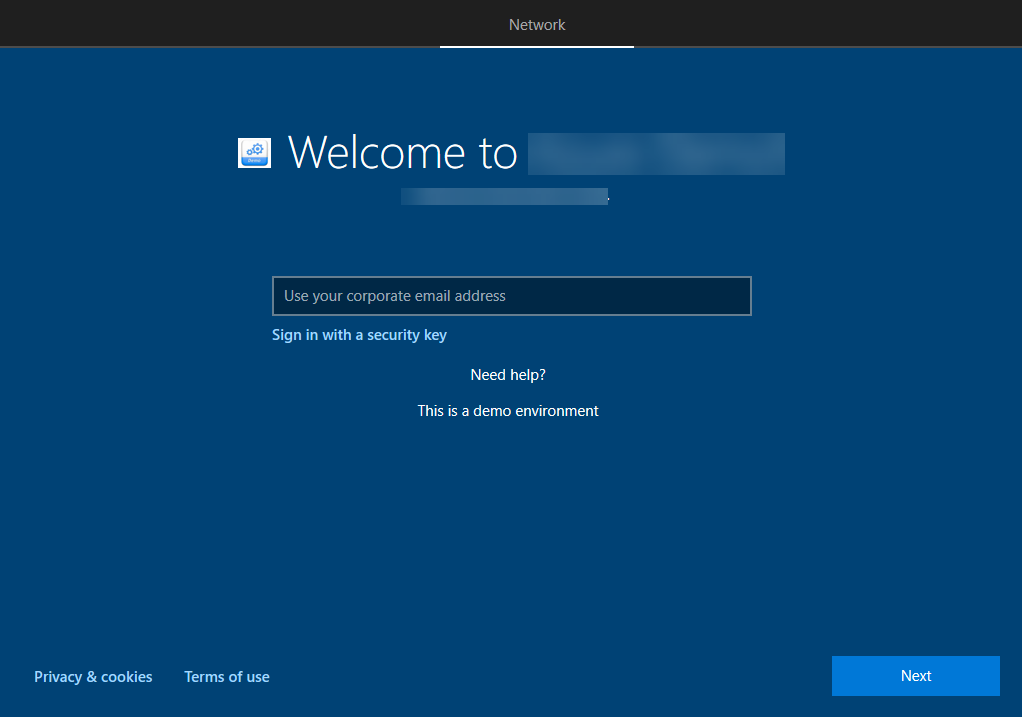
Alright, now we have everything in place (finally ;-)) to begin enrolling our device. However….

**Things that can go wrong**

Obviously we are only sure of one thing, and that is that the sun rises everyday, and in these times this is also not true unfortunately. There are some things that could go wrong. Here are some things that i have encountered during the enrollment of devices. Let’s call them breakpoints.

**Breakpoint 1 – No branded sign-in screen**

If the user does not get the company-branded sign-in screen, then the device has failed the autopilot check.

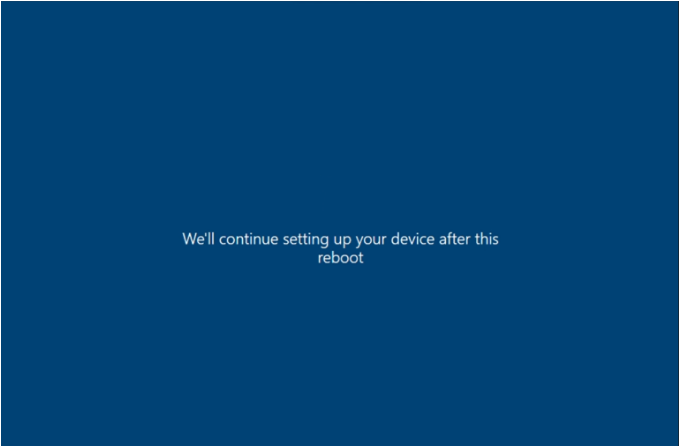


For a successful autopilot profile download, the user gets the company-branded sign-in screen. This failure or breakpoint is more related to the Windows Autopilot service and as such is common for both Azure AD Join as well as Hybrid Azure AD Join. If the network requirements are not met, irrespective of the join state configured/desired, the device can fail the Autopilot activation check, or if there is no deployment profile assigned to the device.

Post successful user authentication, the provisioning is taken over by the Hybrid Azure AD join mechanism. The OOBE setup process briefly displays the screen as shown below. This is the time when the device requests an ODJ blob (Offline Domain Join Blob) from Intune and waits for the same.

**Breakpoint 2 – Windows Autopilot Hybrid Azure AD Join**

If Intune cannot find a domain join profile targeted to the device, the device provisioning process will time-out here at this stage, waiting for the ODJ blob. Make sure you have the Domain Join profile deployed correctly. Intune gets the ODJ blob created for the device from the domain controller via the Intune ODJ Connector (officially named the “Intune Connector for Active Directory”) and sends it to the device. As the device receives the ODJ blob and applies it, if the applied Autopilot profile has “skip connectivity check” setting enabled, the device will immediately reboot.

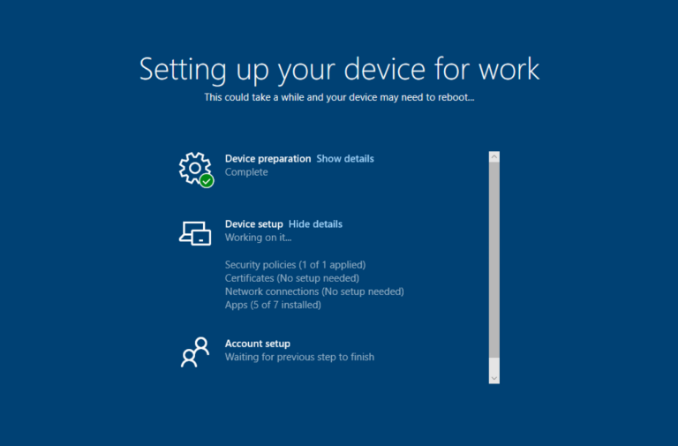


**Breakpoint 3 – Skip Connectivity Check**

If the “skip connectivity check” setting is not enabled in the Autopilot profile, the device starts to ping the connected network to check the existence for a domain controller. As the device receives the ODJ blob from Intune and applies it, before rebooting to complete the process, it will try to ping the domain to ensure connectivity. The device provisioning process will time out here at this stage if the device ping test does not succeeds.

Ensure the “Skip Connectivity Check” is enabled in the assigned Autopilot profile.

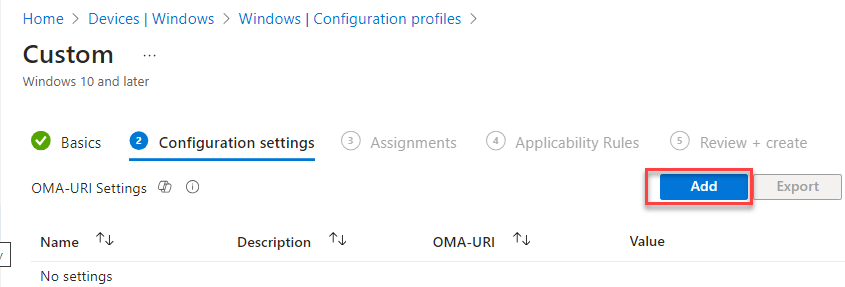
Post restart the device comes up to the Windows ESP screen to show the device provisioning progress. On completion of the ESP device setup phase, the end-user gets prompted for a Windows sign-in.



**Breakpoint 4 – Enrollment Status Page Issue**

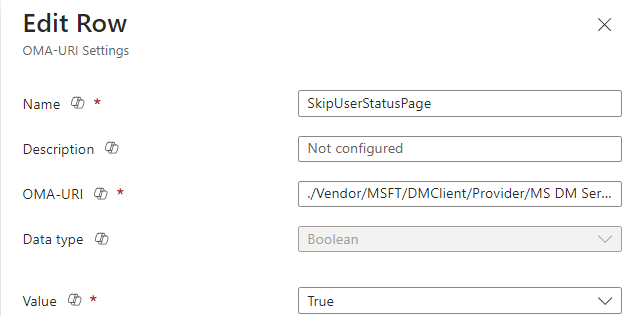
In an Autopilot Hybrid Domain Join scenario, you may observe an error in enrollment status page (ESP). This error is because of the timeout as mentioned in the post by Michael Niehaus, check it out [here](https://learn.microsoft.com/en-us/archive/blogs/mniehaus/trying-out-windows-autopilot-user-driven-hybrid-azure-ad-join).

To solve this you can create a new device configuration profile by going to the Intune portal – Devices – Windows – Configuration profiles. Click create – New policy – Platform is Windows 10 and later – profile type is Templates – Template name is custom. Name your profile e.g. Autopilot Hybrid SkipUserState. Click Add



Fill in these settings

Name: SkipUserStatusPage (or whatever you want)  
OMA-URI: ./Vendor/MSFT/DMClient/Provider/MS DM Server/FirstSyncStatus/SkipUserStatusPage  
Data type: Boolean  
Value: True

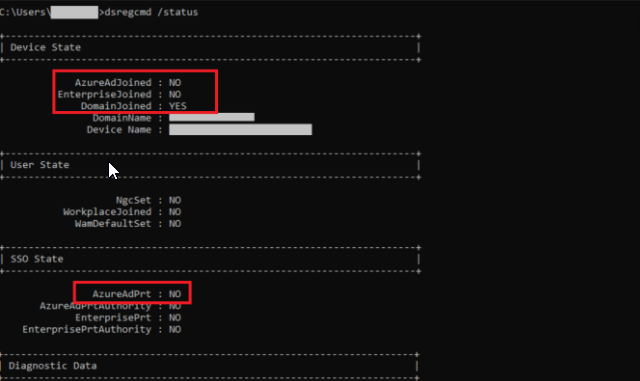


Click save and assign this policy to your dynamic device group.

**Breakpoint 5 – The device wont fetch the required user token (Azure AD PRT)**

If the device does not stay locked in the device ESP phase for long enough to buffer this backend sync delay, then the user sign-in event (login to Windows post completing device ESP) won’t fetch the device the required user token (Azure AD PRT).

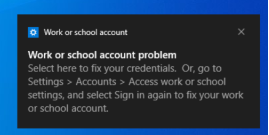
If you run dsregcmd /status on the device you can check if your device is correctly enrolled in both Entra ID and your local domain.



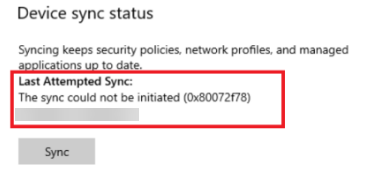
Considering the fact that the device is yet to complete that backend AAD sync process, which is generally true (unless you have enough apps to install during the device ESP to mask the sync delay), the device at this stage is not yet in a production-ready state, even though the user is presented with the Desktop.

And this is where things start getting inconsistent from the end-user experience perspective.

* At this point, the device will not receive the policies targeted to the user.
* OneDrive sync does not gets automatically configured, even if you have the related Intune policies in place.
* None of the Office apps get automatically signed-in with the user account on start.
* Bitlocker encryption wont kick off, even if you have Intune policy targeted to the device.
* End-user gets this annoying Work or school account problem notification.

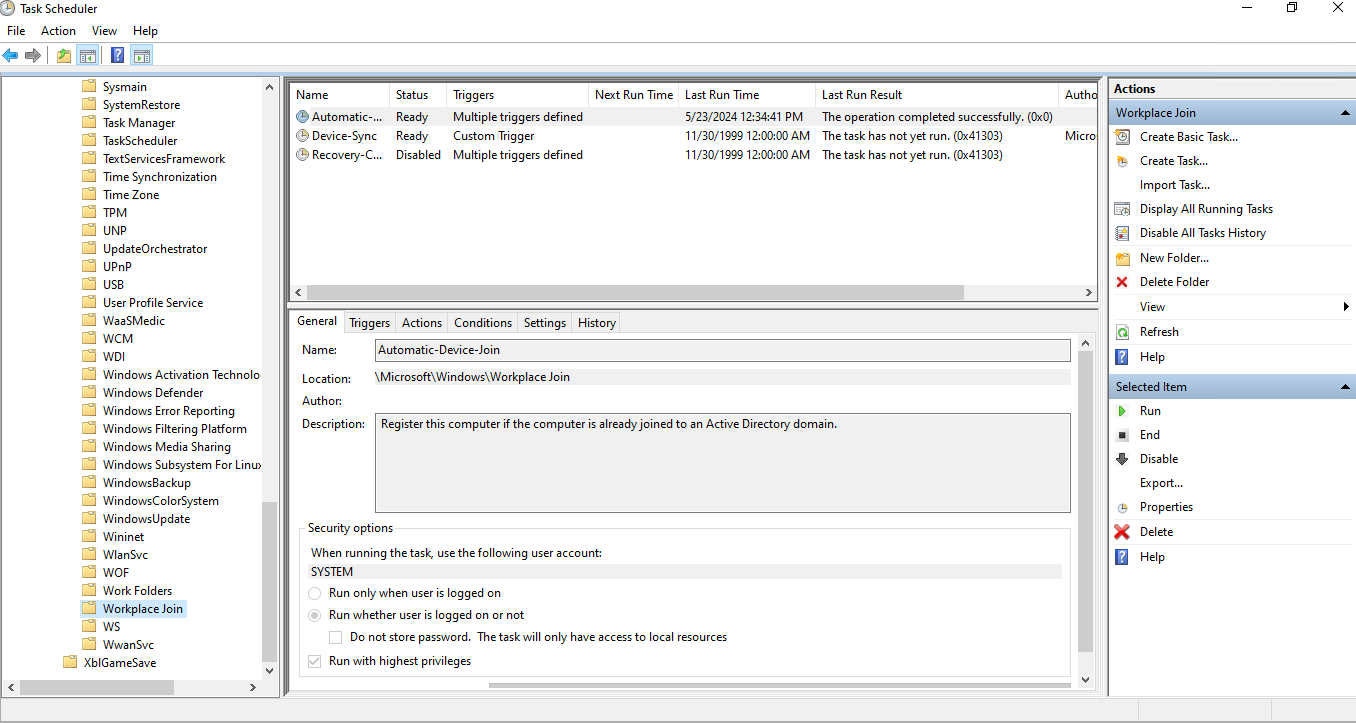


Further if you try to sync device, the sync action will not succeed.



All of the behavior as mentioned above is only due to the fact that the device HAS NOT received the user token (Azure AD PRT) that IS REQUIRED for the device to start communicating with Intune and the rest of the M365 services. The Windows Autopilot service and Microsoft Intune only take care of getting the device joined to Active Directory and enrolled in Intune. The Hybrid Azure AD Join in itself is a separate process that happens in the background, and for a managed domain environment, is dependent on the sync schedule of AAD Connect. Till the time AAD connect syncs this device to Azure, the device fails the Azure AD DRS process. The Azure AD DRS process gives the device an identity vide the Azure AD device certificate.

There is a scheduled task created on the device to register the the device when it is domain joined, you can find this task under Windows – Workplace join



It is after the AAD Connect syncs the on-prem device object to Azure, is when the Azure DRS process of automatic registration succeeds, thereby fetching the device its much-needed Azure AD device certificate. Only after this, when the user does a fresh sign-in to the device, is when the device receives the Azure AD PRT and can start communicating with the Microsoft cloud services for proper functioning.

**So this is why we will NOT assign an ESP page for Intune Autopilot Hybrid Entra ID Joined setups**

**Breakpoint 6 – Duplicate devices with different enrollment status (not really a breakpoint)**

In Entra ID you can have 3 join types:

* Microsoft Entra Registered
* Microsoft Entra joined
* Microsoft Entra Hybrid joined

Registered: This column will display one of the following values:

* This state confirms that AD Connect has synced the computer object to AAD, but that the hybrid join is not complete yet. As such, the machine is not considered hybrid joined meaning the benefits shown above are not available yet.
* The date/time the device completed the hybrid join.

If there are a lot of devices listed a filter can be set to show inly hybrid joined machines: Join type – hybrid Azure AD joined. At this point the computer object should be displayed with the Registered value set to pending.

If the Windows machine was previously Azure AD registered there may be duplicate entries for the computer object. Duplicate entries will also exist if multiple users share the same machine. In this scenario the machine showing the Azure AD Registered state will be removed after the same user logs into the machine once the hybrid join has completed. The removal for additional users will occur after they log in. Automatic device cleanup requires Windows 10 version 1803 and higher. For previous versions, cleanup the Azure AD registered state before initiating the hybrid join process.

You can prevent your domain joined device from being Azure AD registered by adding the following registry value to HKLM\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin: “BlockAADWorkplaceJoin” = dword:00000001.

Once ADConnect has done its job and the computer object is showing a pending state in Azure AD, the next step is for a user to log into the machine. For the hybrid join to complete, the machine must have line-of-site to a domain controller. If it does not, the registered state will continue to show pending.

According to Microsoft [this is their explanation](https://learn.microsoft.com/en-us/answers/questions/1339674/duplicated-ad-computer-in-the-azure-ad-entra-devic):

***When the same device ends up with two different identities in Azure AD, it is known as a Dual state in AAD terminology. This usually happens when your users add their accounts to apps on a domain-joined device, they might be prompted with Add account to Windows, and if they enter Yes on the prompt, the device registers with Azure AD. The trust type is marked as Azure AD registered. After you enable hybrid Azure AD Join in your organization, the device also gets hybrid Azure AD joined. Then two device states show up for the same device.***

***Note: Hybrid Azure AD join takes precedence over the Azure AD registered state. So, your device is considered hybrid Azure AD joined for any authentication and Conditional Access evaluation. You can safely delete the Azure AD registered device record from the Azure AD portal. If the duplicate devices are very old and stale you can also check out steps mentioned on following document to clear those device entries: How To:***[***Manage stale devices in Azure AD***](https://learn.microsoft.com/en-us/azure/active-directory/devices/manage-stale-devices)

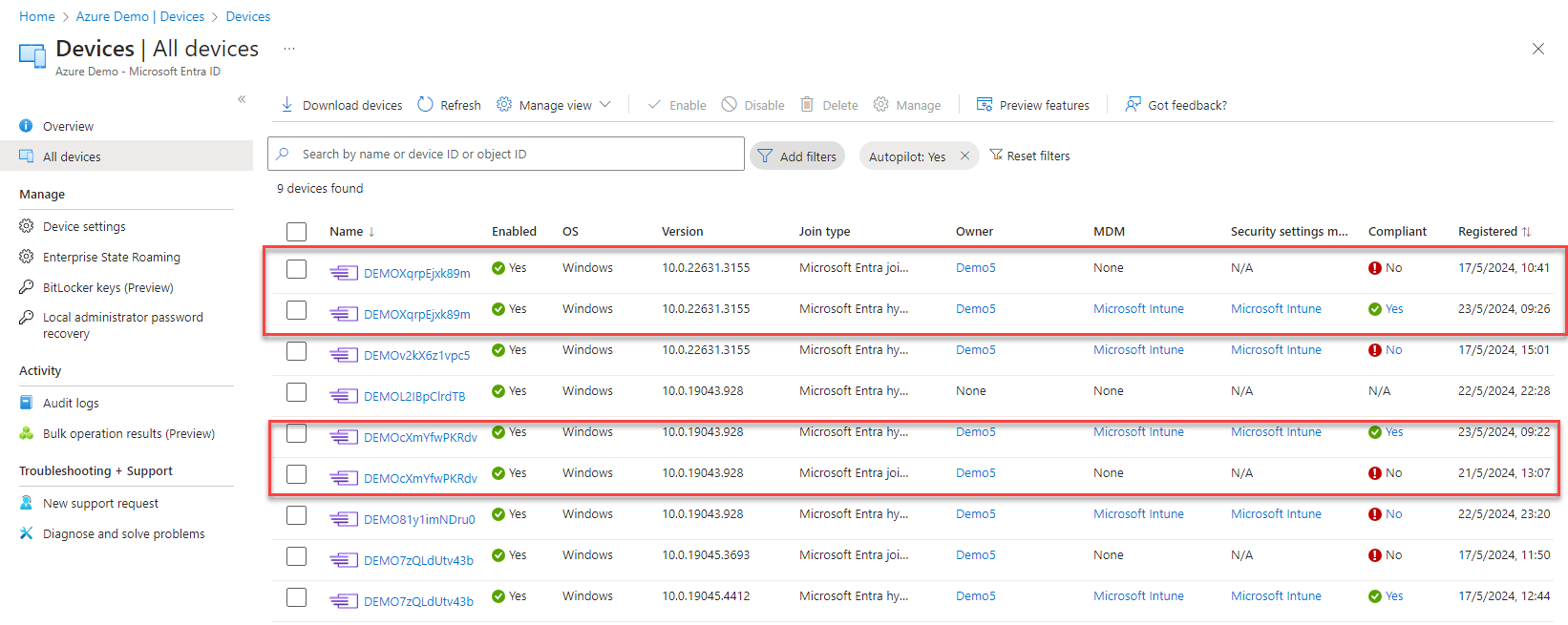
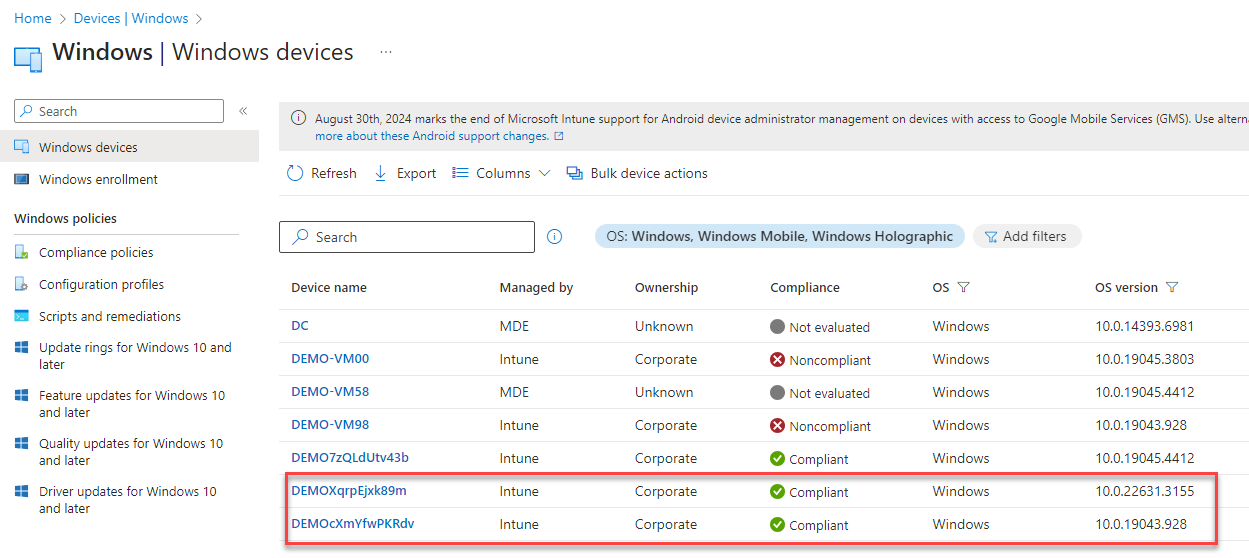
***Additionally, you can check out the instructions provided under***[***Handling devices with Azure AD registered state***](https://learn.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan#handling-devices-with-azure-ad-registered-state)***, if you want to avoid such a scenario.***

And also this

***Duplicate device objects with hybrid Microsoft Entra deployments***  
*A device object is pre-created in Microsoft Entra ID once a device is registered in Autopilot. If a device goes through a hybrid Microsoft Entra deployment, by design, another device object is created resulting in duplicate entries.*

[Windows Autopilot known issues | Microsoft Learn](https://learn.microsoft.com/en-us/autopilot/known-issues#duplicate-device-objects-with-hybrid-microsoft-entra-deployments)

Some screenshots of my Intune portal devices and Entra ID joined devices, i have 1 VM running Windows 10 and 1 physical HP Device running Windows 11



These where some of the issues i encountered, these are not the only ones but from my personal point of view and experience the most common.

**Enrolling a device**

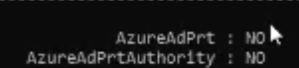
Now i will show you the experience of enrolling an autopilot hybrid Entra ID joined device. Here we go.

You see that after the 1st reboot the device is not yet Entra ID joined but domain joined. Run this command in an elevated command prompt.

dsregcmd /status



And also no Entra ID PRT yet

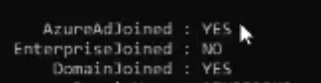


At this point in time normally you should wait for AD Connect to sync, i did a force sync on my AD Connect server by running this command in an elevated powershell.

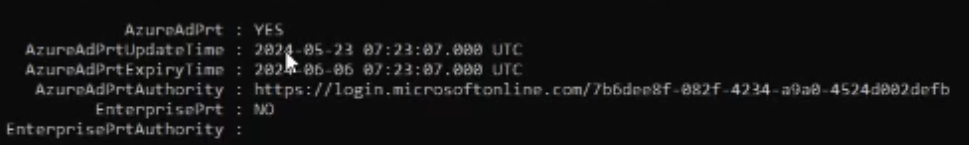
Start-ADSyncSyncCycle -PolicyType Initial

After running the sync and a reboot of the device you will get these results when doing the dsregcmd /status again.

Now the device is Entra ID joined and domain joined.



And also the Entra ID PRT is ok



**Conclusion**

You see this is very tricky material and it seems that this is something that is not quite finished, however some of the weird stuff is by design. It can be a challenge and somewhat frustrating to setup and get it working. I hope this guide will makes you feel more at ease when customers or your company asks you to implement this. For all you techies out there reading this guide, if you feel like there is something in error or if you would like to contribute, don’t hesitate to contact me!

Good luck!