Enroll Windows Device using PPKG.

Contents

Summary

In this post I'm covering how to import device hash into Windows Autopilot devices using a provisioning package (PPKG)

There are 2 ways to get hardware imported into Windows Autopilot devices

- Using the manual (importing hash in Intune Admin Portal or Online) or automated method (covered in this post)
- Enabling "Convert all targeted devices to Autopilot" into Windows Autopilot deployment profiles for Hybrid Azure AD joined and Azure AD joined devices.

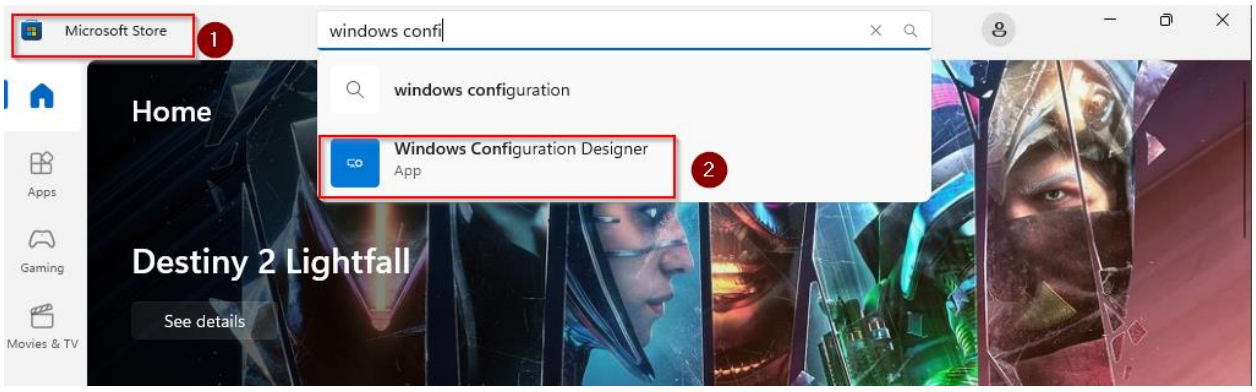
More info here https://learn.microsoft.com/en-us/mem/autopilot/profiles

Notes

Converting all targeted devices to Autopilot isn't supported for transforming a hybrid Azure AD device into an Azure AD Autopilot device.

Step 1

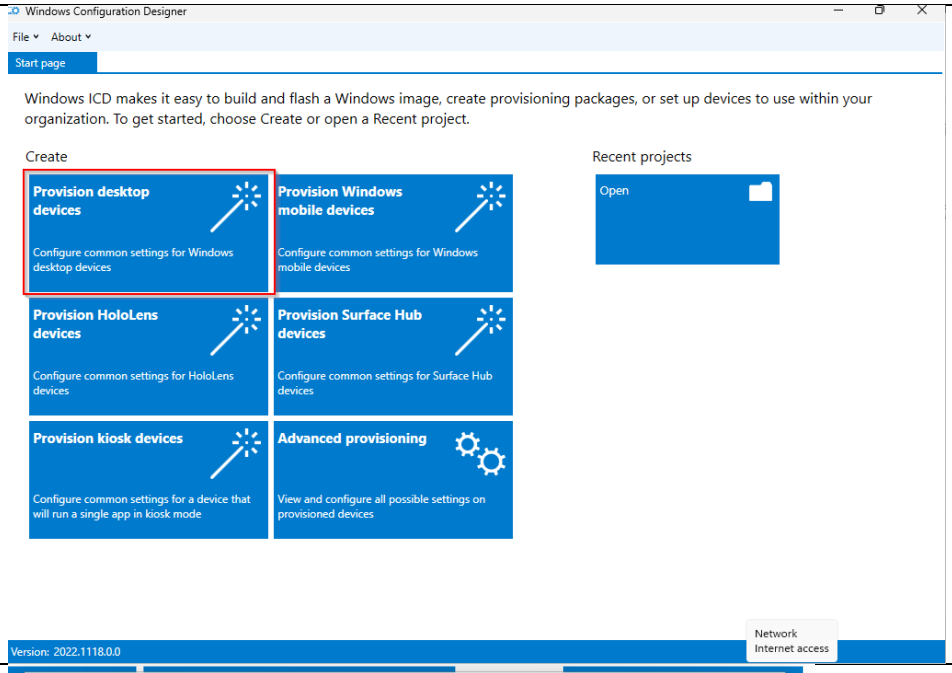
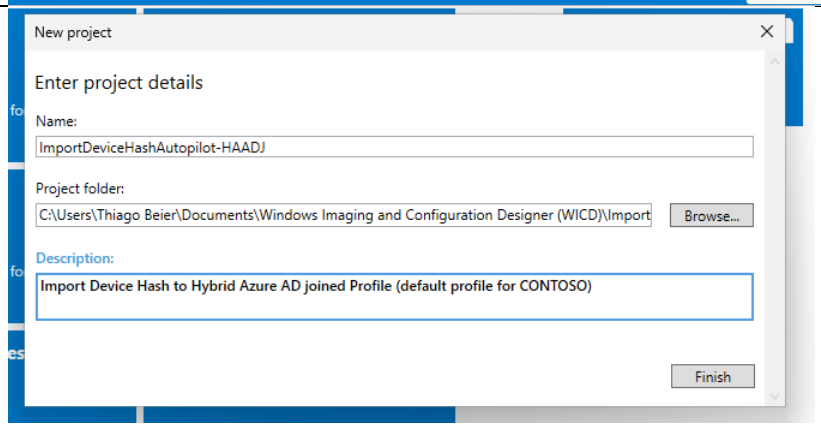
1. Create your PowerShell Script to import device hash into Windows Autopilot
    a. This requires
        i. **Azure AD application #1** registered using secret to be used by "Get-WindowsAutoPilotInfo" to upload the device hash to the default Group Tag "empty", in our scenario Hybrid Azure AD joined. – post to be published
        ii. **Azure AD application #2** registered using certificate to be used by SharePoint online PowerShell module to send out the device information to SharePoint online Lists – post to be published.
2. Open Microsoft Store on windows 10 or 11
3. Search for "" and click on it
4. Proceed with its installation – clicking on Get
5. Click open when installation is finished

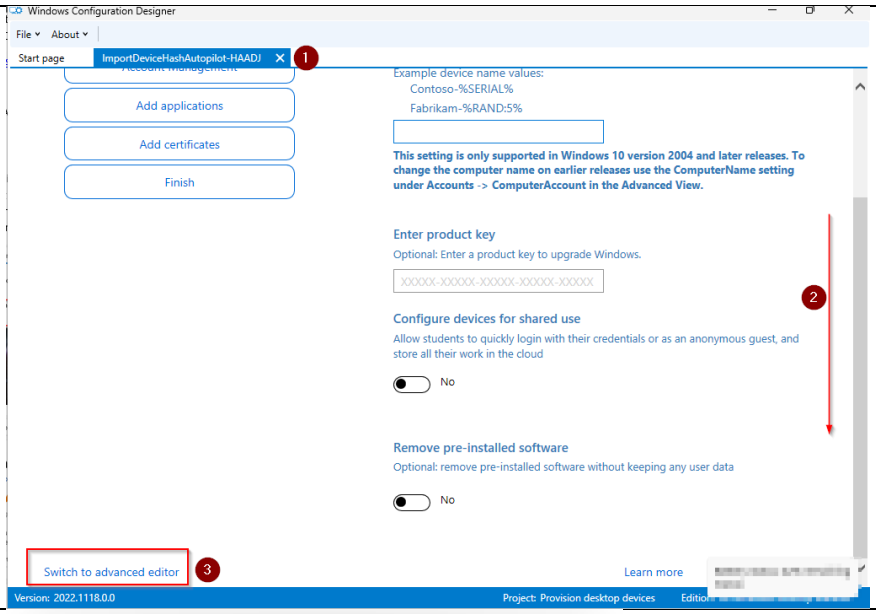
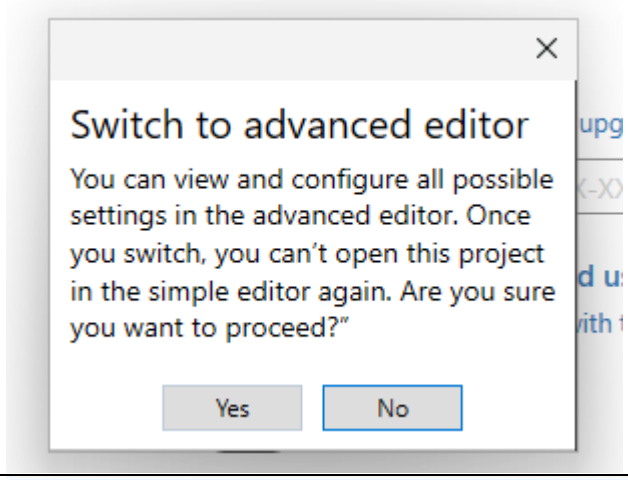
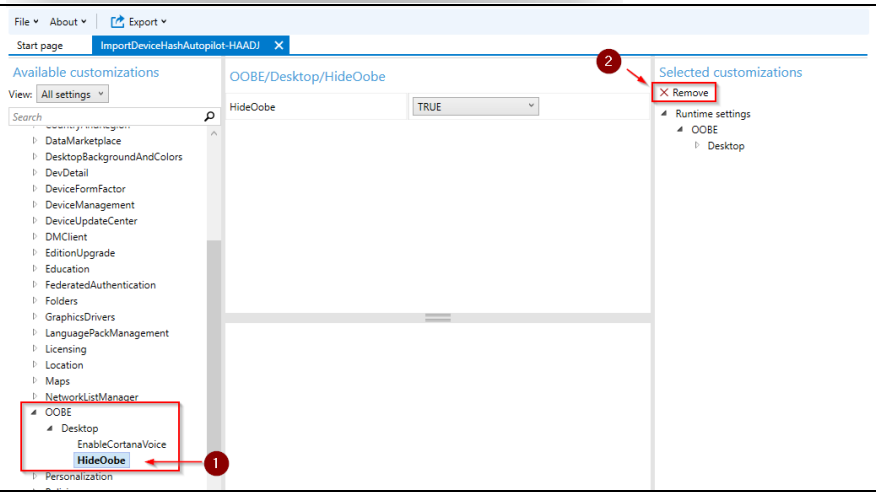

Microsoft Store
1
windows confi
windows configuration
Windows Configuration Designer
App
2
Home
Apps
Gaming
Movies & TV
Destiny 2 Lightfall
See details

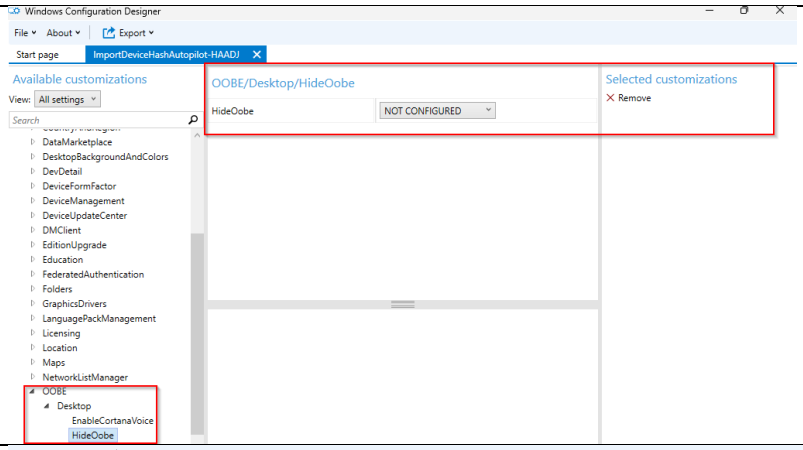
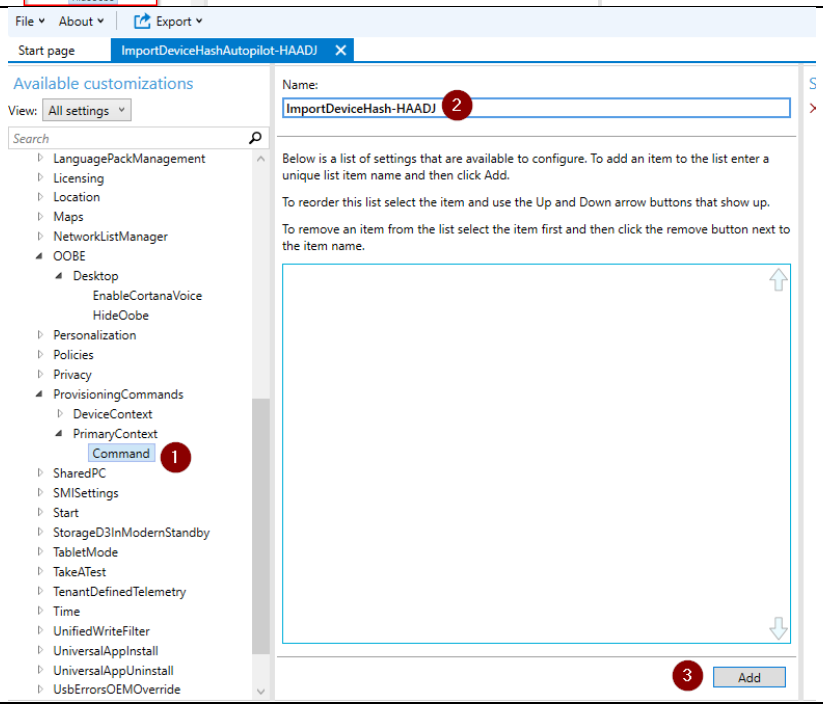

Microsoft Store
windows confi
Windows Configuration Designer
Microsoft Corporation
Get
4.4
Average
10
Ratings
EVERYONE
Configure Windows devices without imaging. Use the Windows Configuration Designer App to simplify deployment of Windows devices at your...
Utilities & tools
Apps
Gaming
Movies & TV


Microsoft Store
windows confi
Windows Configuration Designer
Microsoft Corporation
Open
4.4
Average
10
Ratings
EVERYONE
Configure Windows devices without imaging. Use the Windows Configuration Designer App to simplify deployment of Windows devices at your...
Utilities & tools
Apps
Gaming
Movies & TV

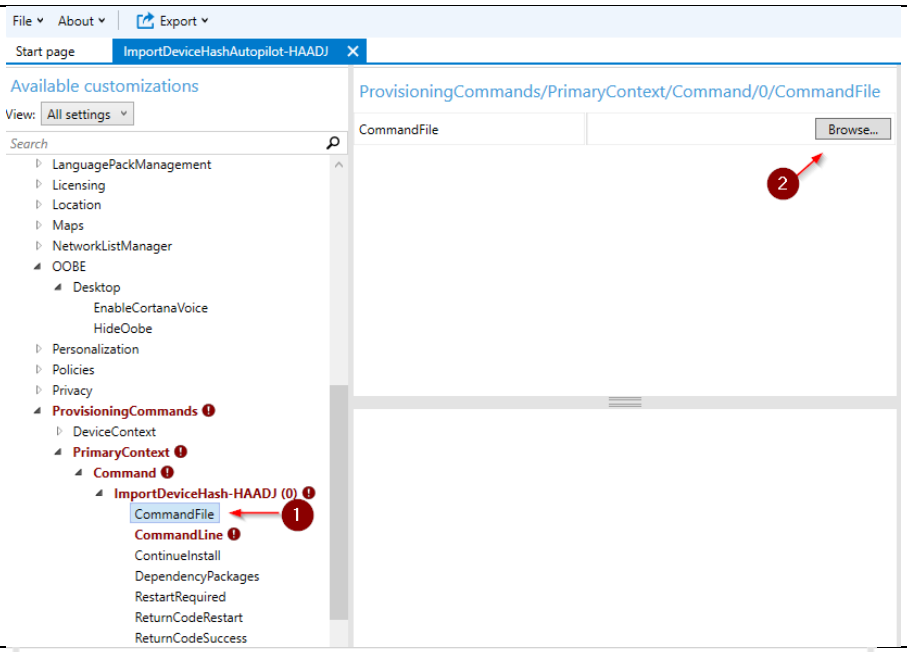
You're now on Windows Configuration Designer main screen.

Click on Provision desktop devices	
Give it a **Name** and a **Description** **Note**: this scenario all Hybrid Azure AD Joined devices will have Group Tag as "**blank**" in our Tenant. Then click Finish All Azure AD Joined devices will have **AADJ** as Group Tag	

You're now under the Project (1) Scroll down (2) until you find the option Switch to advanced editor (3) Click on it.	
Select YES for the warning. After you select YES there's no way to switch back to in the simple editor.	
After you have all Runtime settings expanded Scroll down Find OOBE Expand it Select **HideOOBE** on the left Then click on Remove	

Expected result	
Scroll down Find “ProvisioningCommands” Expand Primary Context and click on Command (1) On the Center, give it a name (2) Then click Add (3)	

Expand the "ImportDeviceHash-HAADJ"
Select CommandFile (1)
Click Browse (2)

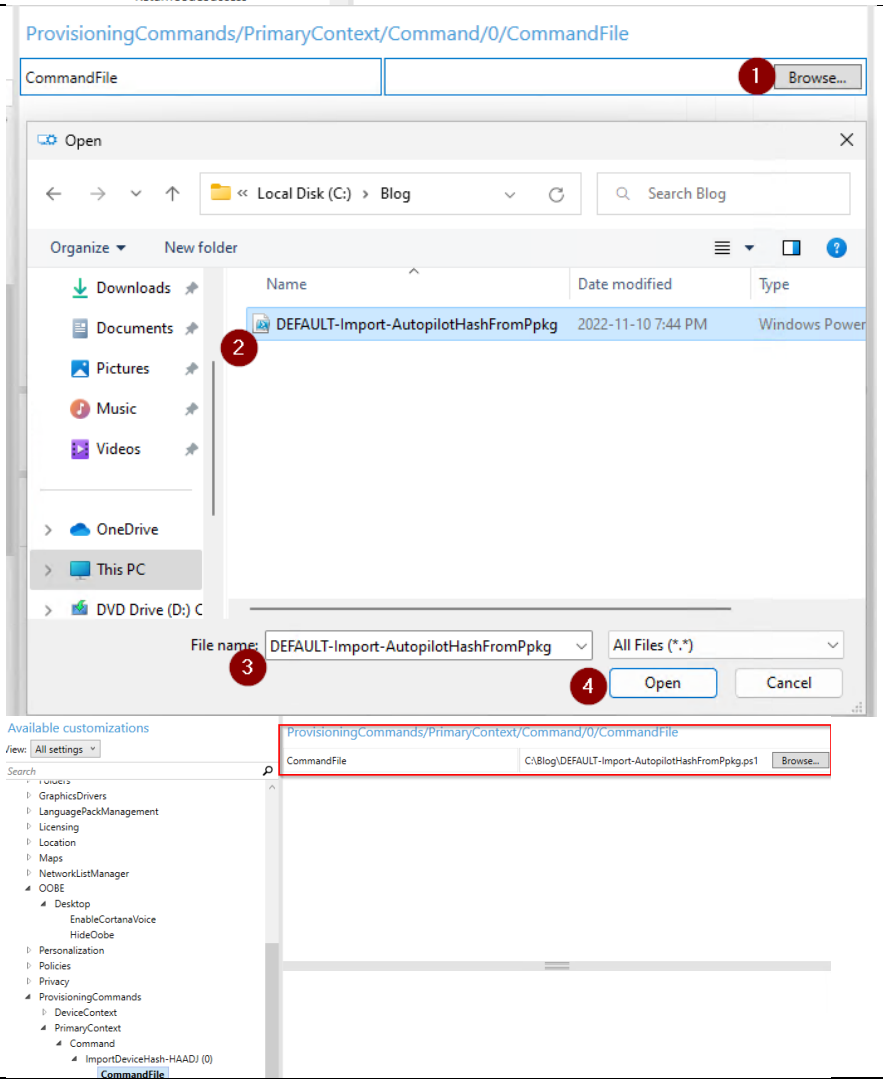


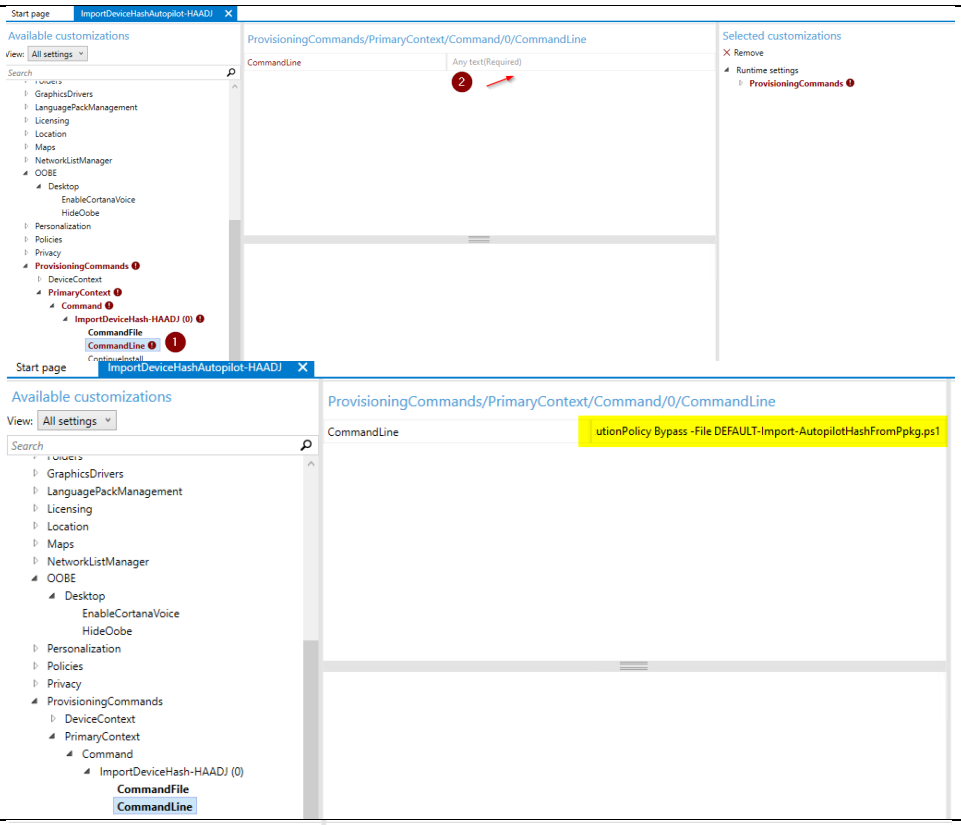
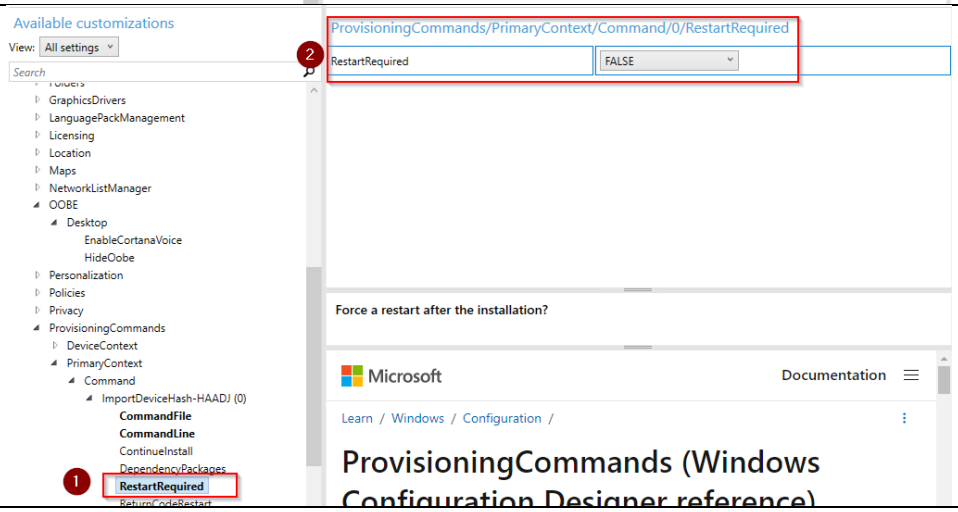
Go the folder where your PowerShell is located. (1)

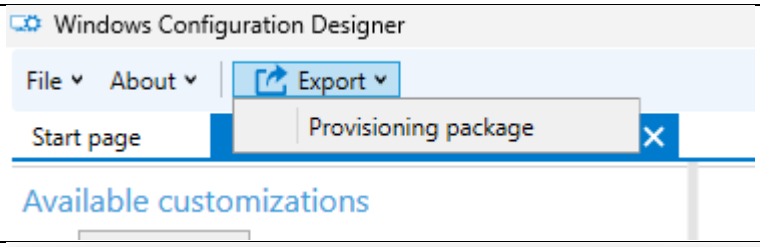
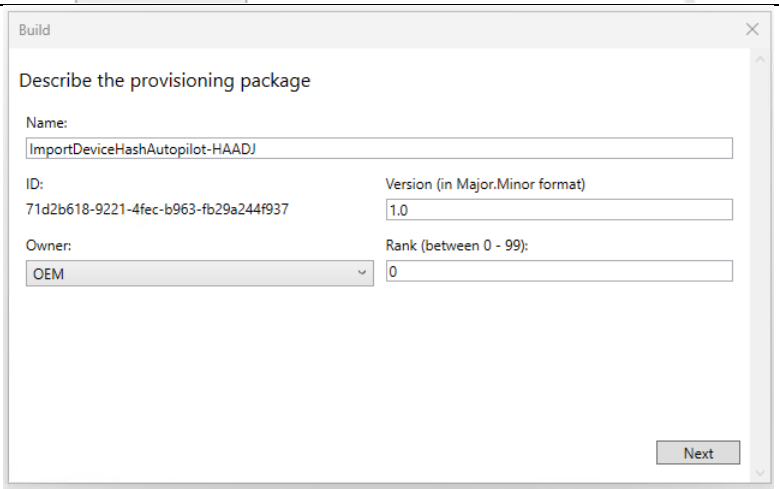
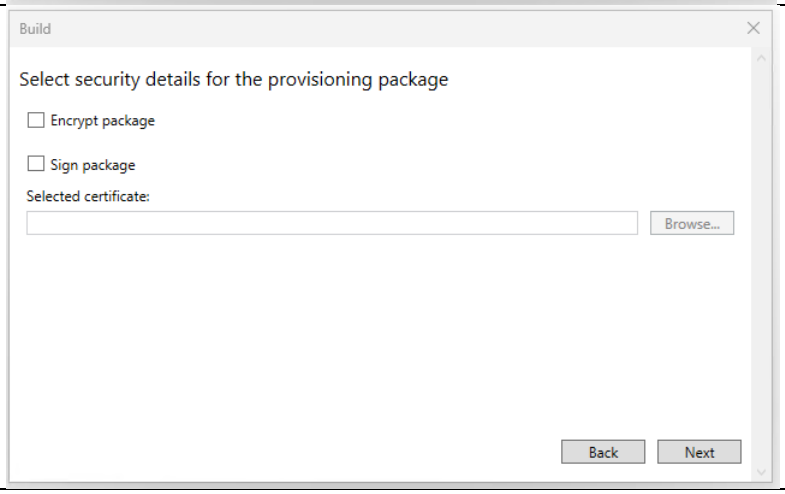
(2) select the PowerShell file

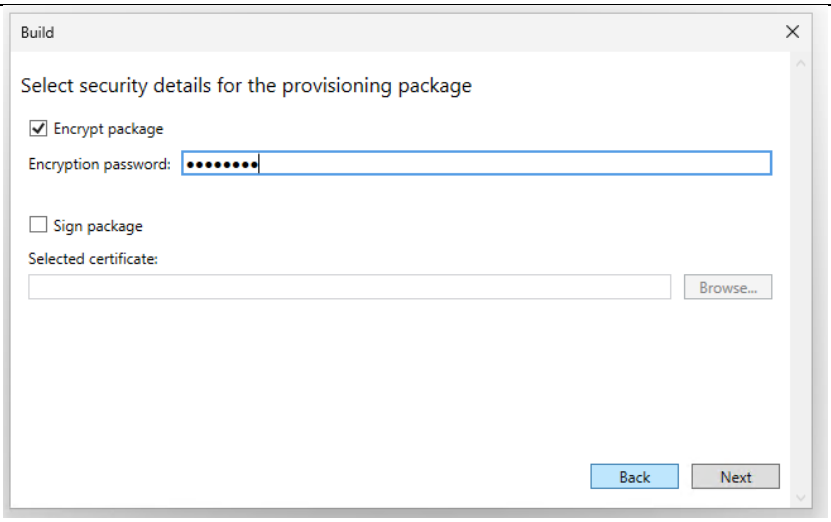
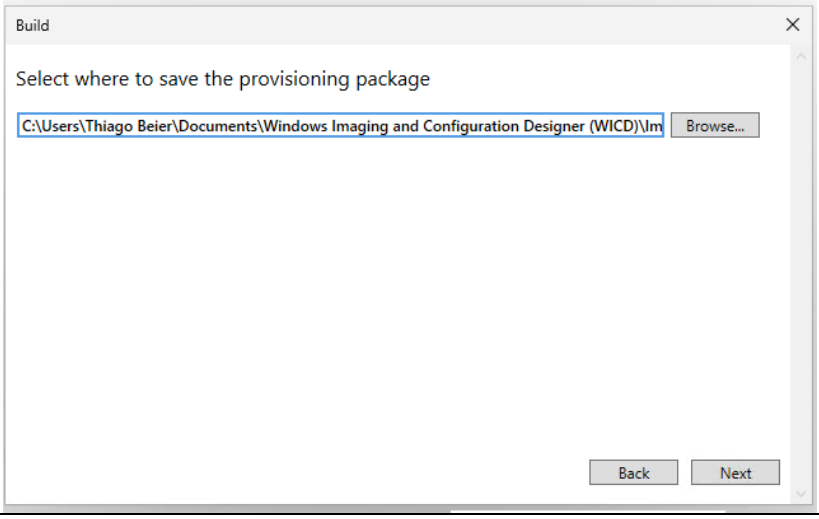
(3) make sure that's the correct file

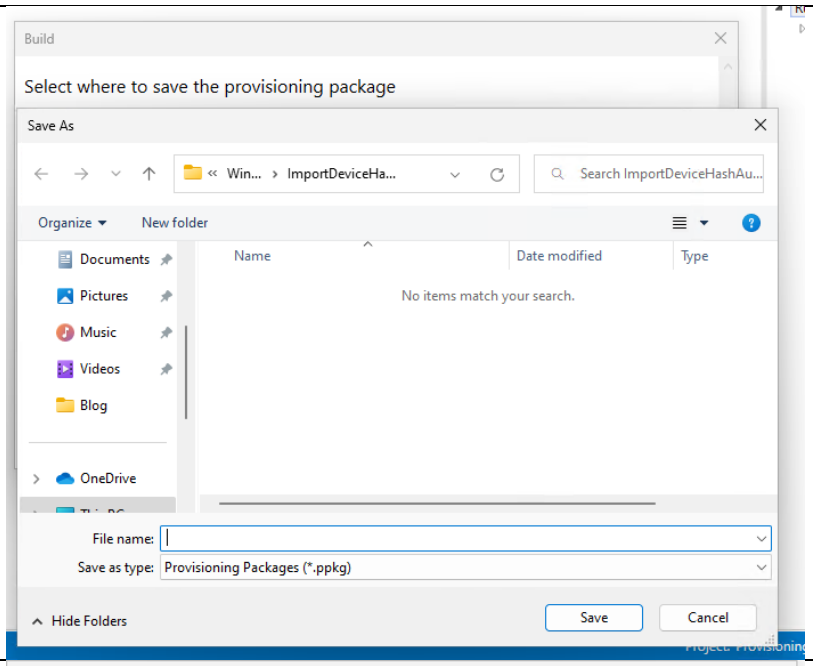
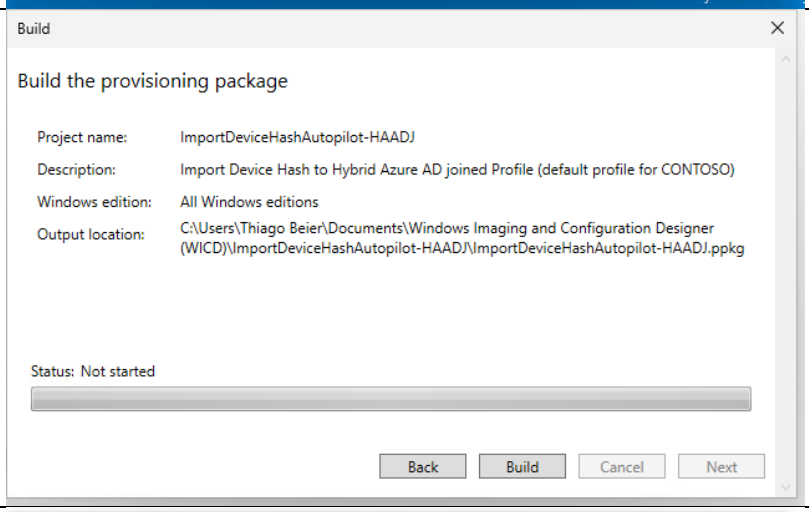
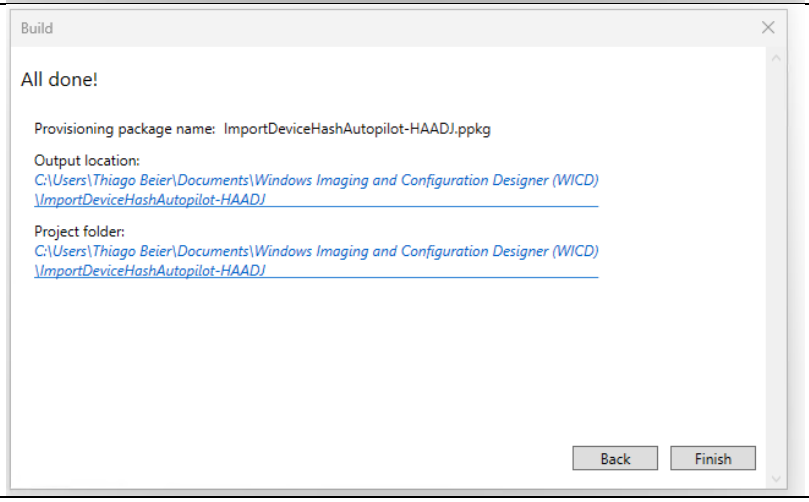
(4) click open

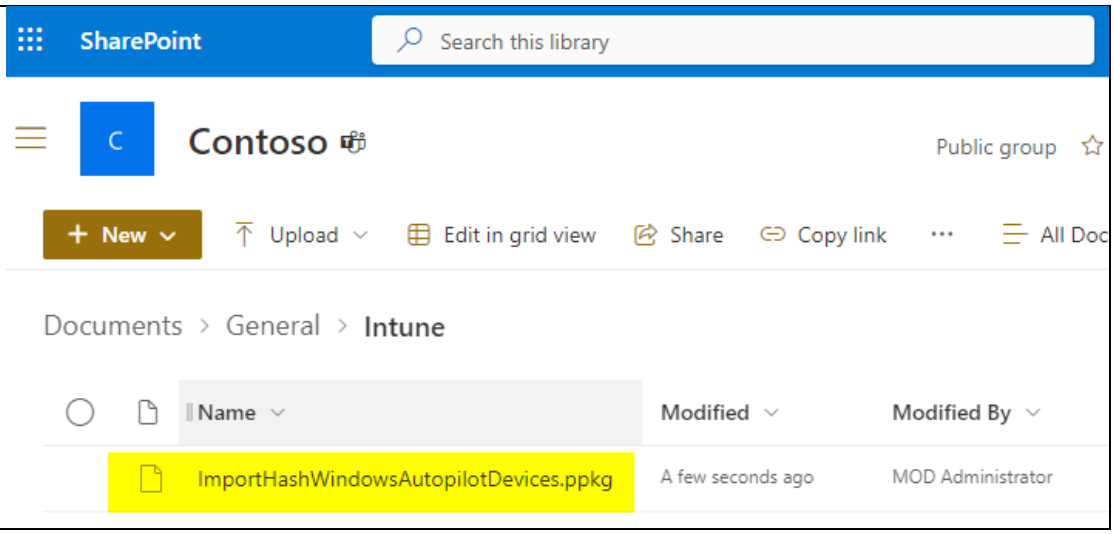


Now proceed to “CommandLine” (1) Select it (2) Add the PowerShell command to be executed “PowerShell.exe -ExecutionPolicy Bypass -File DEFAULT-Import-AutopilotHashFromPpkg.ps1 ”	
Under RestartRequired (1) Select FALSE (2) Then click anywhere on the screen (blank area)	
Now click on DependencyPackages Then select Browse Go to source folder (C:\blog\) Select the following files at the same time then click Open Cmtrace.exe, companyPortal.ico, PnPPowerShell.cer and	All cmtrace.exe, companyPortal.ico, PnPPowershell.cer and PNPowershell.pfx files are part of this deployment that you can check other blog posts at https://thebeier.com to learn more about it.

PNPPowerShell.pfx	
Exporting the package Click on the Export option (1) Then select Provisioning package (2)	
Keep the Name (1) Select “IT Admin” at Owner (2) Click Next (3)	
Under Build Click next (1)	

If you want to encrypt the password (request a user a Password to run it) Select Encrypt package and give a password Note: there's no way to recover the password. However, a new build can be done (Export) and update its password (new package version) Select Encrypt package Give it a password = M365@123 (1) Click Next (2) to proceed	
You can change the package output folder – not required for this scenario Clicking on browse (1) Then click next (2) to proceed	

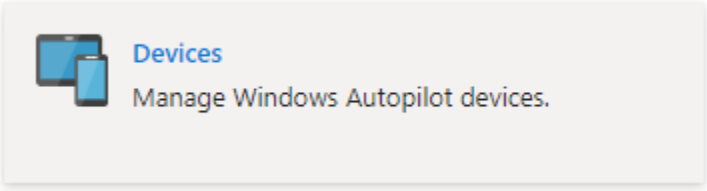
TIP: click on the UNC path , CTRL + A (select ALL), paste on (windows key + R) to see the directory (remove the last part – that's the file name DefaultImport - Onboarding.ppkg) Or past in notepad C:\Users\THiago\Documents \Windows Imaging and Configuration Designer (WICD)\DefaultImport-Onboarding Click on Build to finish the process (1)	
Check the output location (1) Check the project folder (2) Finish this process (3)	
On windows explorer Click view (1) Check "file name extensions" checkbox (2) Validate the file name (3) - .ppkg The PPKG file will be given to help desk or end-user to initiate its DEVICE Enrollment in YOURTENANT tenant.	

Upload the PPKG to SharePoint site where you have access using first.last@domain.com	

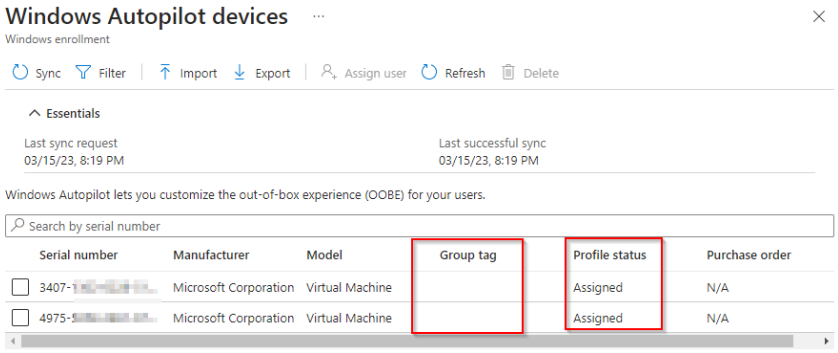
Step 2

Go to the Device you want to enroll and run the following steps:

- During OOBE (New device to intune or Existing Device that's being imported)
- Run Shift + F10
- You now have access to CMD.exe
- Press Windows key + R
- Type: msedge
- After Edge is open follow its wizard and do not cache any logon information neither synchronization options
- Go to your SharePoint site
- Go to your document library
- Download the PPKG file.
- Run it from the browser
    - It won't show any notification if that's being executed on a brand new device
    - It will show a notification when executed on existing devices (devices in use that only need to be imported to autopilot)
- Go back to Microsoft Intune Admin center \ Devices \ Enroll Devices \ Devices (Windows Autopilot Devices)



    - Check if imported device has its Profile status as "assigned"



Enjoy it.

A video recording will be uploaded In a few weeks to help you with this deployment.

Cheers,

Thiago Beier
Toronto, ON

https://thebeier.com