HOW TO MANAGE DEVICES

#htmdcommunity

@htmdcommunity

HTMD Community Conference - 2024

Microsoft

PATCH MY PC

ZERO TOUCH

nerdio

Thank You Sponsors!

Microsoft

PATCH MY PC

ZERO TOUCH

nerdio

Speaker

Saurabh Sarkar

Microsoft Intune CAT Product Manager

▶ aka.ms/intunevideos

Approaches for Transitioning Intune managed Hybrid devices to Cloud Native

HOW TO MANAGE DEVICES

#htmdcommunity

@htmdcommunity

AGENDA

Background

Benefits of going Cloud Native

Options for Transitioning hybrid to cloud

Tips on when to use

Conclusion

Background

Cloud native endpoints are devices which can be deployed and used from anywhere over the internet without any dependency on the on-premises.

Cloud-native endpoints are Windows devices that are deployed using Windows Autopilot, joined to Microsoft Entra ID and are automatically enrolled in a Mobile Device Management (MDM) solution

Benefits

Don't worry about connecting to the VPN

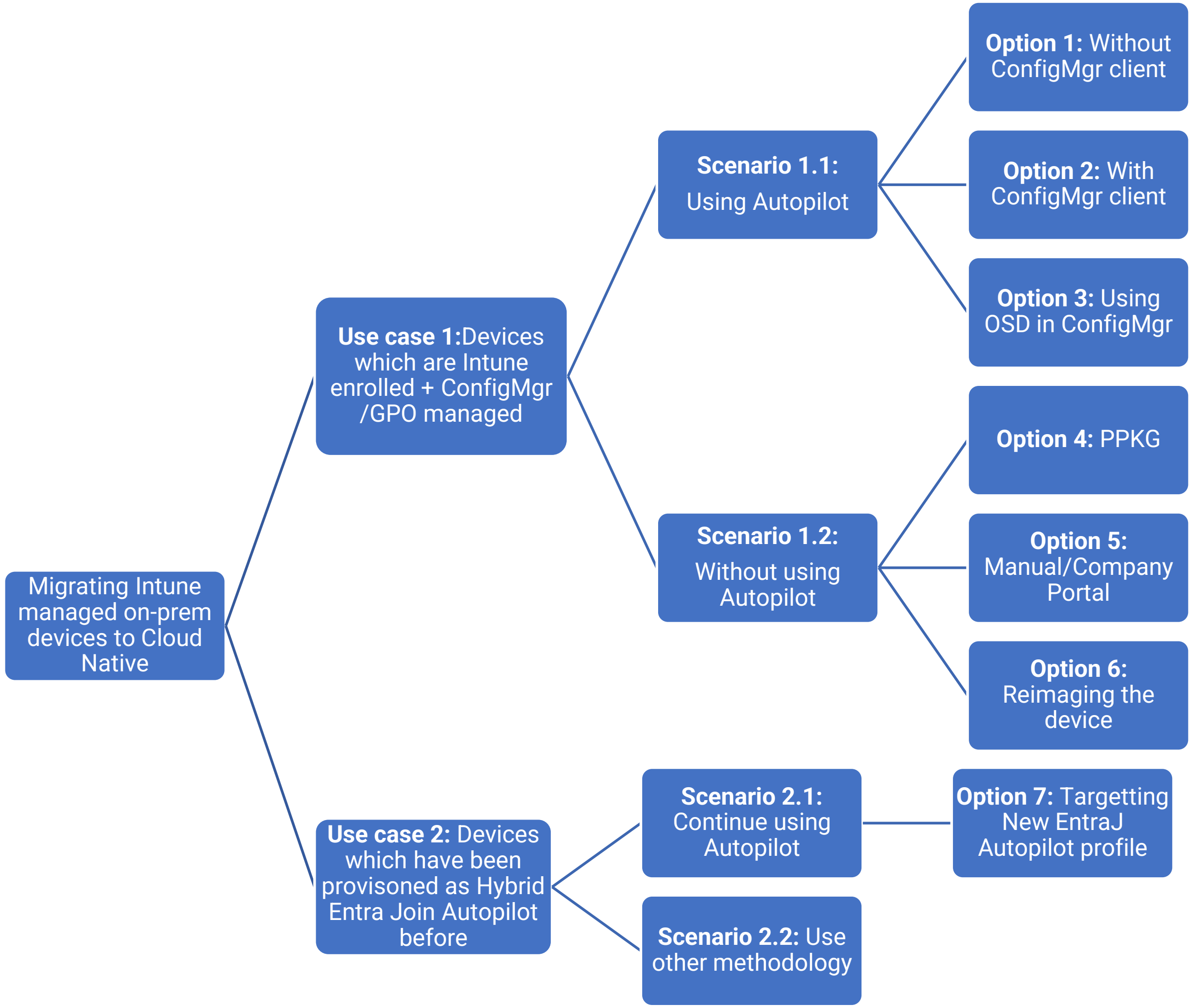
Deploy from anywhere

Simplified management for all platforms

Provide a secure Single-Sign-On (SSO) experience to cloud and on-premises apps

Secure access without passwords

Transitioning Hybrid to Cloud:



Migrating Intune managed on-prem devices to Cloud Native

Use case 1: Devices which are Intune enrolled + ConfigMgr /GPO managed

Scenario 1.1: Using Autopilot

Option 1: Without ConfigMgr client

Option 2: With ConfigMgr client

Option 3: Using OSD in ConfigMgr

Scenario 1.2: Without using Autopilot

Option 4: PPKG

Option 5: Manual/Company Portal

Option 6: Reimaging the device

Use case 2: Devices which have been provisoned as Hybrid Entra Join Autopilot before

Scenario 2.1: Continue using Autopilot

Option 7: Targetting New EntraJ Autopilot profile

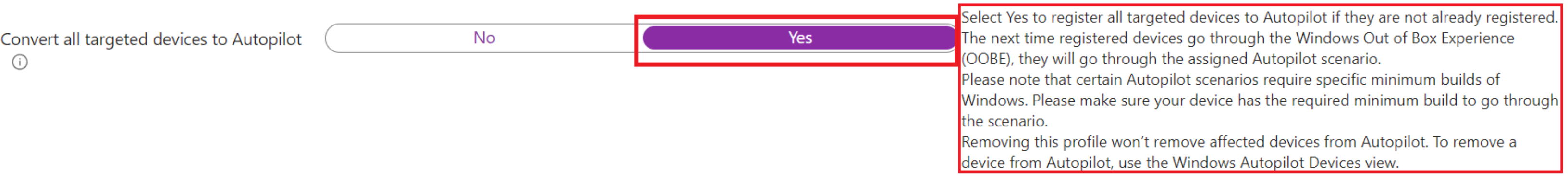
Scenario 2.2: Use other methodology

Use case 1: Entra Hybrid joined and Intune enrolled devices (ConfigMgr managed/GPO managed) to Cloud Native

Scenario 1.1: Options Using Autopilot:

Option 1: If we want to remove the dependency on ConfigMgr:

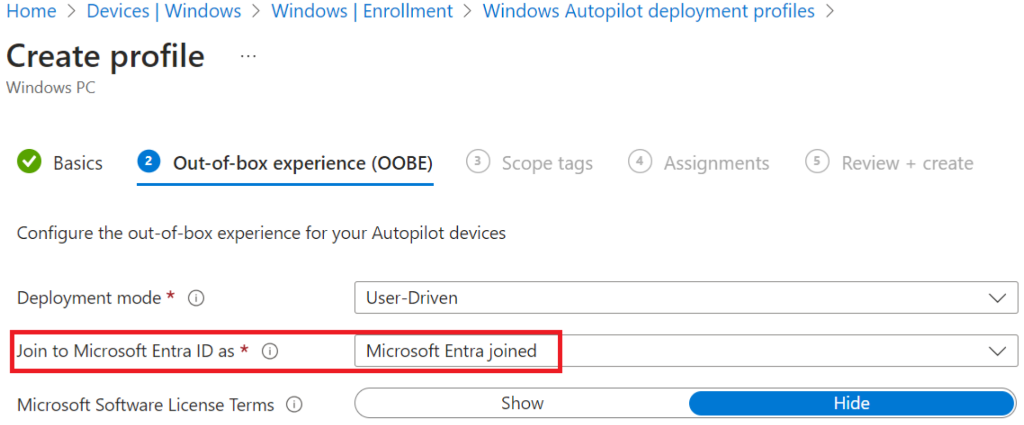
- Since the device records are already present in Entra (as the device is Entra Hybrid Joined), All we must do is first create a Device group containing the devices
- Now Create an Autopilot profile and select 'Convert all targeted devices to Autopilot'> Set the Autopilot profile as Microsoft Entra Joined>Deploy.
- Now the devices will get registered with Autopilot service automatically as per Automatic registration of existing devices | Microsoft Learn. Since these devices are already targeted via Autopilot profile, it will take effect when the devices undergo provisioning the next time
- Now we just need to go to the Intune portal>Do a 'Wipe' of the device
- Device will come back to the out of the box (OOBE)   screen and receive the Autopilot profile thereby undergoing Entra Join + Intune enrollment.



Convert all targeted devices to Autopilot ⓘ

No | **Yes**

Select Yes to register all targeted devices to Autopilot if they are not already registered. The next time registered devices go through the Windows Out of Box Experience (OOBE), they will go through the assigned Autopilot scenario.
Please note that certain Autopilot scenarios require specific minimum builds of Windows. Please make sure your device has the required minimum build to go through the scenario.
Removing this profile won't remove affected devices from Autopilot. To remove a device from Autopilot, use the Windows Autopilot Devices view.



Home > Devices | Windows > Windows | Enrollment > Windows Autopilot deployment profiles >

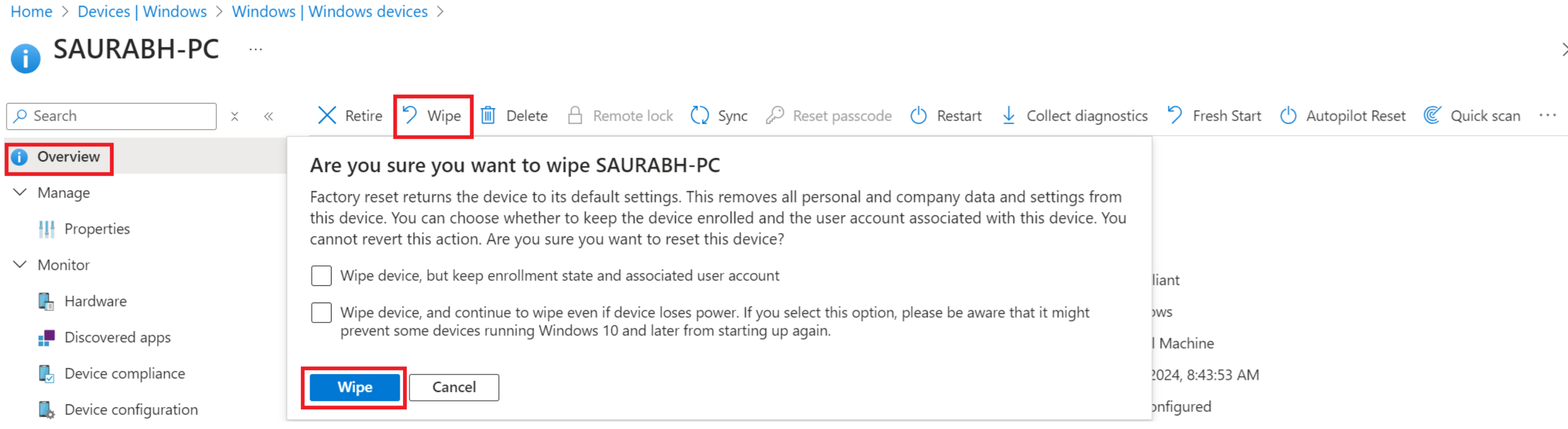
Create profile ···
Windows PC

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ: User-Driven

Join to Microsoft Entra ID as * ⓘ: Microsoft Entra joined

Microsoft Software License Terms ⓘ: Show | **Hide**



Home > Devices | Windows > Windows | Windows devices >

SAURABH-PC ···

Are you sure you want to wipe SAURABH-PC

Factory reset returns the device to its default settings. This removes all personal and company data and settings from this device. You can choose whether to keep the device enrolled and the user account associated with this device. You cannot revert this action. Are you sure you want to reset this device?

☐ Wipe device, but keep enrollment state and associated user account

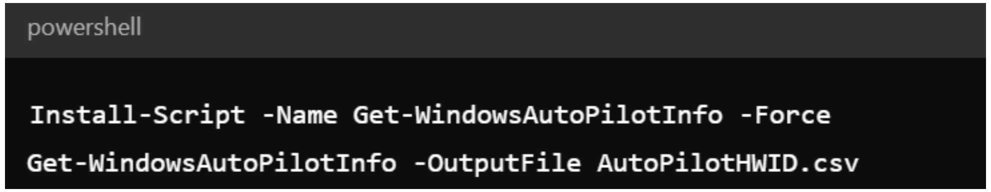
☐ Wipe device, and continue to wipe even if device loses power. If you select this option, please be aware that it might prevent some devices running Windows 10 and later from starting up again.

Wipe | Cancel

HOW TO MANAGE DEVICES #htmdcommunity @htmdcommunity

TIP: When to use

- This is the recommended approach.
- Migrating a device from Entra Hybrid to Cloud Native with Intune enrollment is best achieved using Autopilot.
- This is seamless and the device gets provisioned automatically as a part of the OOBE experience after the reset.
- Make sure the users either back up their data manually to OneDrive before initiating the wipe from Intune Or deploy a policy from Intune portal to configure the Known Folder Move for OneDrive
- It's also possible to generate the hardware IDs of the devices by running the below PowerShell script in them.
  - This script will generate a CSV file with the hardware IDs of the devices.



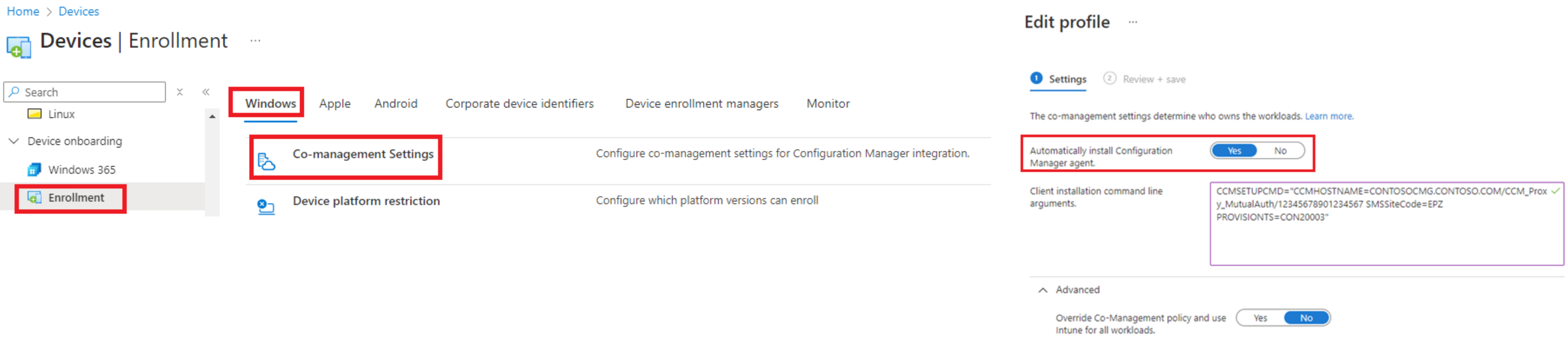
powershell

```
Install-Script -Name Get-WindowsAutoPilotInfo -Force
Get-WindowsAutoPilotInfo -OutputFile AutoPilotHWID.csv
```

Option 2: If we want to continue to utilize SCCM:

- We encourage our customers to go with a cloud only approach to reduce total cost of ownership, however if you want to continue to utilize your existing investment you can configure devices to become co-managed after they enroll into Intune.
    - We can achieve that automatically, by setting the “Automatically Install the Configuration Manager agent’.
        - This will automatically install the Configuration Manager client as a first-party app and the device gets the client content from the Configuration Manager cloud management gateway (CMG)
        - If we don’t wish to use the above setting, we always have the option of pushing the ConfigMgr client from Intune as a Win32 app/ lob app

- After getting wiped, the device would receive the Autopilot profile and become Entra Joined + Intune enrolled.
    - Now the ConfigMgr client will come down to the device (either automatically via the policy or as Win32 app/.msi) making the device Co-managed eventually



Co-management Settings — Configure co-management settings for Configuration Manager integration.

Device platform restriction — Configure which platform versions can enroll

The co-management settings determine who owns the workloads. Learn more.

Automatically install Configuration Manager agent. [✓ Yes] No

Client installation command line arguments.

```
CCMSETUPCMD="CCMHOSTNAME=CONTOSOCMG.CONTOSO.COM/CCM_Prox
y_MutualAuth/12345678901234567 SMSSiteCode=EPZ
PROVISIONTS=CON20003"
```

Advanced

Override Co-Management policy and use Intune for all workloads. Yes [✓ No]

TIP: When to use

- If we have a strong dependency on ConfigMgr and workloads still managed via ConfigMgr then we can consider getting the device co-managed after going cloud native.
- Our aim should be trying to remove our on-prem dependencies for Client management in the longer run, however in the interim we can have our cloud native devices comanaged as well if needed.

Option 3: Using ConfigMgr Task Sequence

- By using Task Sequence in ConfigMgr, we can do reimaging and provisioning of a Windows device for Autopilot user driven mode and get the device Entra Joined and Co-managed.
- This process involves creating an Autopilot profile in the Intune portal and exporting it as JSON. Then we need to create a package in the ConfigMgr console (containing the JSON), and a task sequence which would be targeted to a collection of devices.
    - More details on the entire workflow can be found doc Windows Autopilot for existing devices | Microsoft Learn.

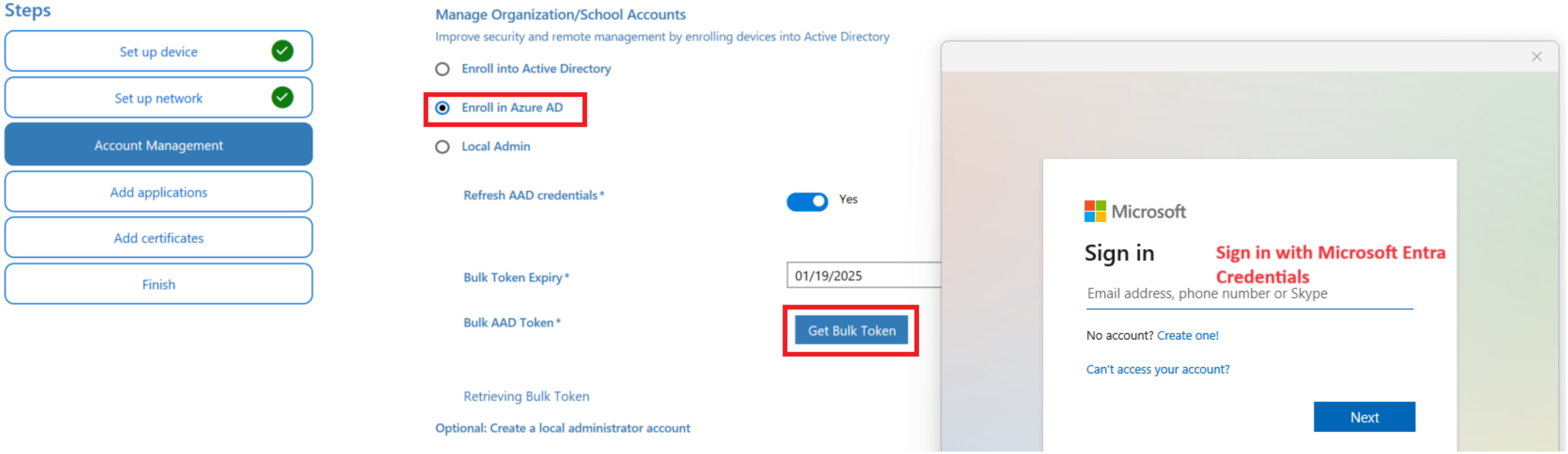
TIP: When to use

- If we have a strong dependency on ConfigMgr (leading to the device being comanaged) and a use case where we want the provisioning of the device to happen by the IT admin, then this methodology can be chosen.
- This method involves the over ahead of manual IT intervention for each device.
    - This can be a possible method if provisioning a device via Autopilot is not an option (due to network restrictions).

Scenario 1.2: Options without Using Autopilot:

Option 4: Using Provisioning Package:

- If for some reason we don’t want to use Windows Autopilot/want the IT admin to do the enrollment and provisioning of the devices manually, then we can follow this approach.
- We would first have to Create a Provisioning package using Windows Configuration Designer which will get the device Entra Id Joined + Intune enrolled.
  - While creating the .ppkg, we must provide Microsoft Entra creds which is used to fetch the Bulk PRT (used for doing the Entra Id Join and Intune enrollment. The .ppkg has to be saved in a USB drive)
- Now we just need to go to the Intune portal> Do a ‘Wipe’ of the device.
- Device comes to oobe screen>Now we need to insert the USB stick with .ppkg .
- The package will be installed which would do an Entra Id join and Intune enrollment. The same has been documented in: Bulk enrollment for Windows devices - Microsoft Intune | Microsoft Learn



Steps

- Set up device ✓
- Set up network ✓
- Account Management
- Add applications
- Add certificates
- Finish

Manage Organization/School Accounts

Improve security and remote management by enrolling devices into Active Directory

○ Enroll into Active Directory

● Enroll in Azure AD

○ Local Admin

Refresh AAD credentials * Yes

Bulk Token Expiry * 01/19/2025

Bulk AAD Token * Get Bulk Token

Retrieving Bulk Token

Optional: Create a local administrator account

Microsoft

Sign in

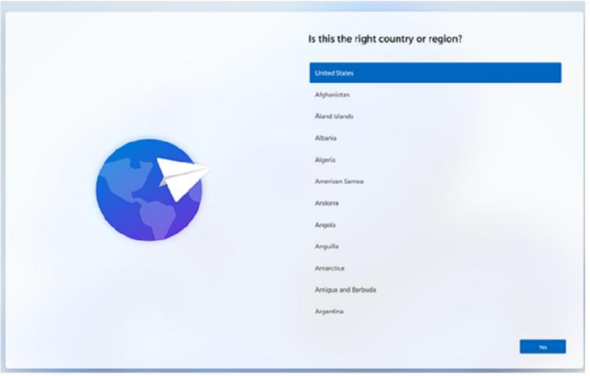
Sign in with Microsoft Entra Credentials

Email address, phone number or Skype

No account? Create one!

Can't access your account?

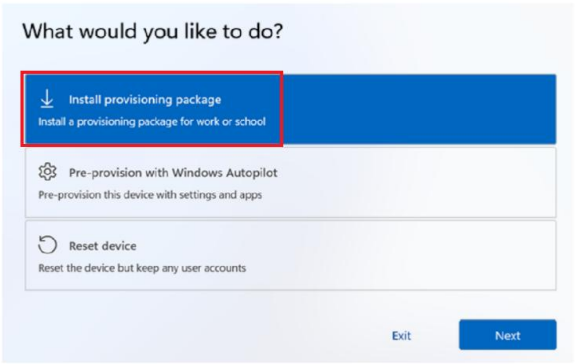
Next



Is this the right country or region?

- United States
- Afghanistan
- Aland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina

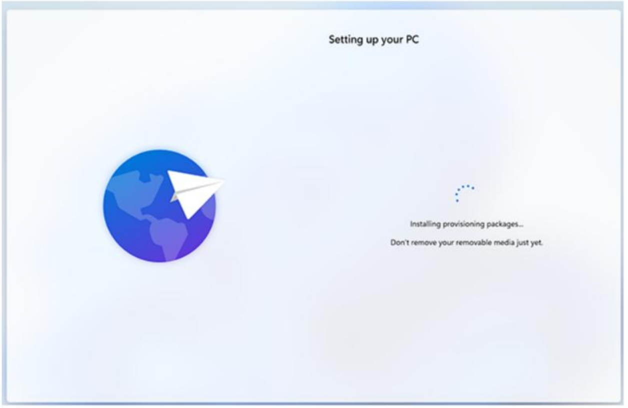
Yes



What would you like to do?

- Install provisioning package
  Install a provisioning package for work or school
- Pre-provision with Windows Autopilot
  Pre-provision this device with settings and apps
- Reset device
  Reset the device but keep any user accounts

Exit Next



Setting up your PC

Installing provisioning packages...

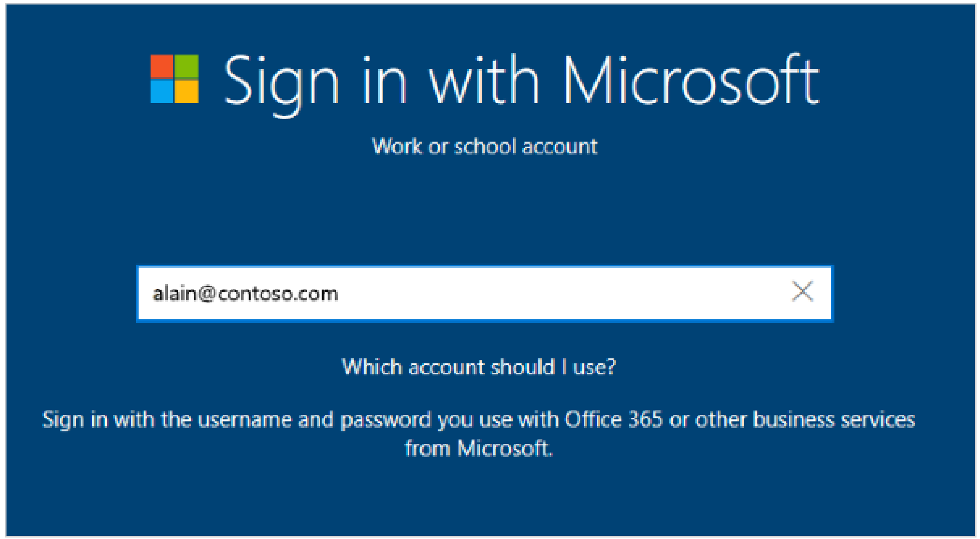
Don't remove your removable media just yet.

TIP: When to use

- This is also a very efficient method of enrolling a device in cases where Autopilot cannot be used for network related reasons.
- This also requires IT intervention (to plug in the USB containing the .ppkg)
- The provisioning of the device is fast as the .ppkg is installed during the out of the box (OOBE) phase.
- This method of provisioning a device is ideal when we want the device to be setup by the IT admin and then handed over.
- Make sure that user’s data is backed up in OneDrive as explained earlier in the blog, before initiating a Wipe.

Option 5: Manual Entra ID join and enrollment :

- Even though this method involves manual action steps which are needed to be taken on each device, however this is also an option. We need to go to the Intune portal and do a ‘Wipe’>Device comes to OOBE screen.
- Now the user has the option of doing Entra ID join and Intune enrollment
- Or the end user can go to the Windows client screen and do Entra ID join from Access Work or School account or via Company Portal application



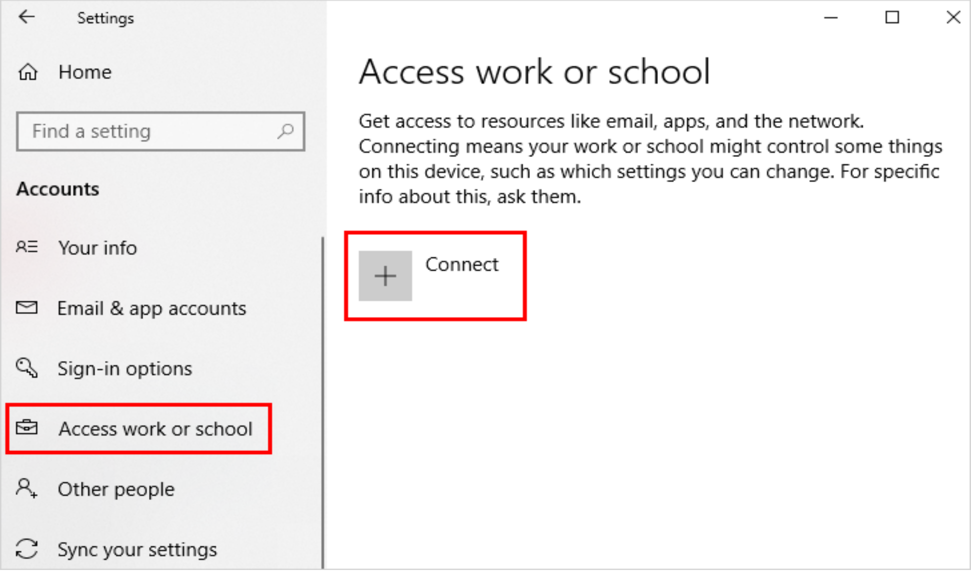
Sign in with Microsoft

Work or school account

alain@contoso.com

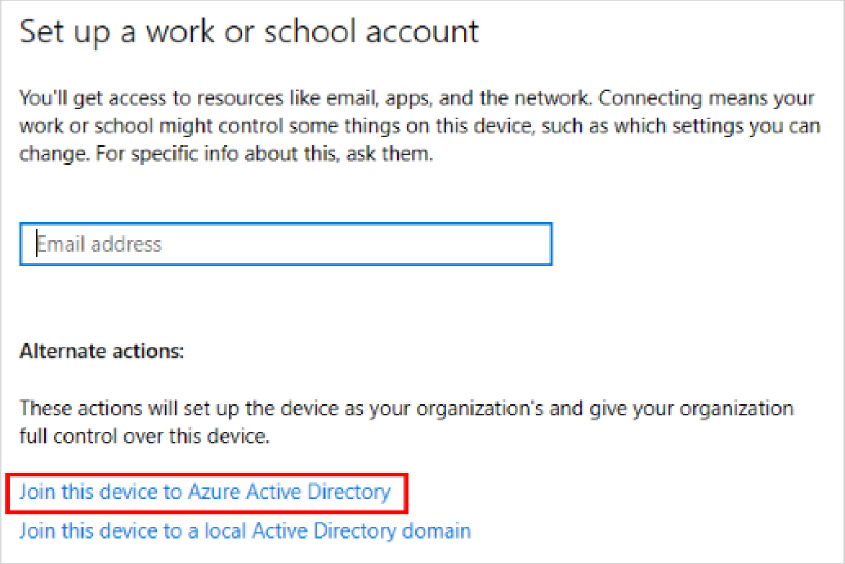
Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.



Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.



Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

Join this device to Azure Active Directory

Join this device to a local Active Directory domain

TIP: When to use

- Manually enrolling the device can be used in scenarios where we don’t have any IT admin staff to manage/create profiles/packages on end user's behalf.
- This process is time taking and needs to be repeated in each device manually hence not scalable
- This methodology ideal if we just must enrol a couple of devices for testing purpose.
- Devices enrolled by this methodology are treated as Personal devices, hence “Personal’ enrollment needs to be allowed under the **enrollment restrictions** in the Intune portal.

Option 6: Reimaging/Reinstallaing the Operating System

- User always has the option of reimaging the device and start fresh while transitioning to Cloud Native.
- This option can also be used if we want to upgrade from Windows 10 to Windows 11 and don't want to go via the Autopilot way. Once the device is reimaged, it will be removed from the on-prem domain.
- Once the device is re-imaged, the device can be then joined to Entra and Intune enrolled by using any of the methodology mentioned above (i.e. Autopilot/Manual Enrollment from Settings or Company Portal App /using provisioning package.

TIP: When to use

- This method is most intrusive and time taking as it involves installing a fresh Operating System
- This method would also require IT admin intervention to re-image the device. This can be chosen as a possible method if we want to start fresh on the existing device, possibly with a new Operating System Version or Edition.

Use case 2: Migrating Entra Hybrid devices which are already registered with Autopilot

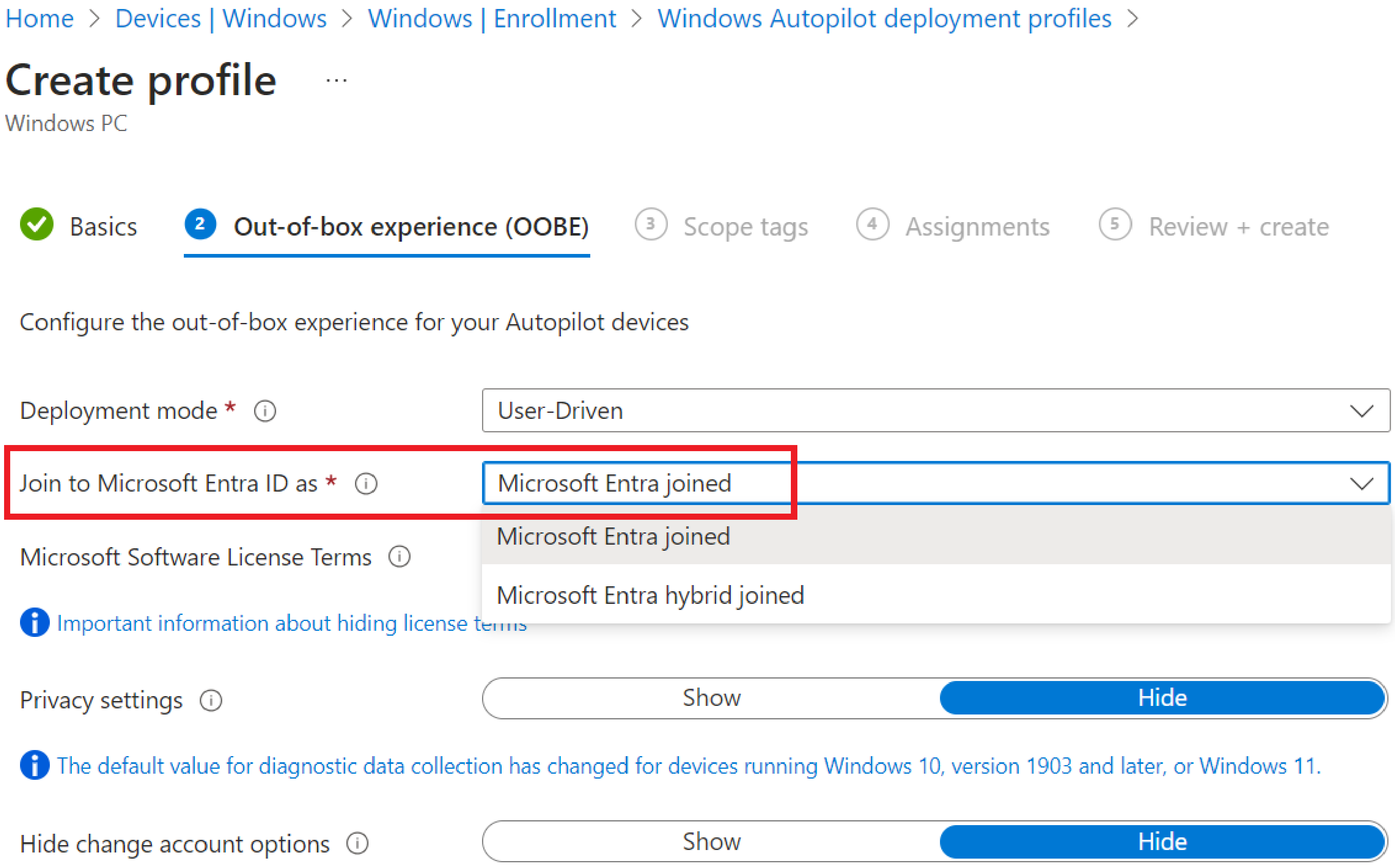
Scenario 2.1: Continue Using Autopilot:

Option 7: Targeting new Autopilot Profile

- If we had provisioned our existing device using Autopilot as Entra Hybrid join, then the devices would be already registered with the Autopilot service.
- To move them to cloud native, we just need to create a new Autopilot profile (with Entra Id join).
- For the new Autopilot profile to take effect, we would have to do a reset of the device which the Intune admin can initiate from the portal, or the end user can initiate manually.
- In this case we no longer need the Offline Domian Join (ODJ) connector which can later be deleted from the Intune portal.

TIP: When to use

- This is the easiest and fastest option if we wish to move our existing devices which were previously provisioned using Autopilot to cloud native.
- By using this option, we don’t need to recall the device back to IT admin workstation from end user as there is no manual IT intervention needed.
  - Once the configuration is done by the admin (i.e. Creation and assignation of the new Autopilot profile), after device resets, the device becomes Entra Joined and business ready over the internet, at any location.



Home > Devices | Windows > Windows | Enrollment > Windows Autopilot deployment profiles >

Create profile ...

Windows PC

✓ Basics ② Out-of-box experience (OOBE) ③ Scope tags ④ Assignments ⑤ Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ User-Driven

Join to Microsoft Entra ID as * ⓘ Microsoft Entra joined

- Microsoft Entra joined
- Microsoft Entra hybrid joined

Microsoft Software License Terms ⓘ

ⓘ Important information about hiding license terms

Privacy settings ⓘ Show [✓ Hide]

ⓘ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11.

Hide change account options ⓘ Show [✓ Hide]

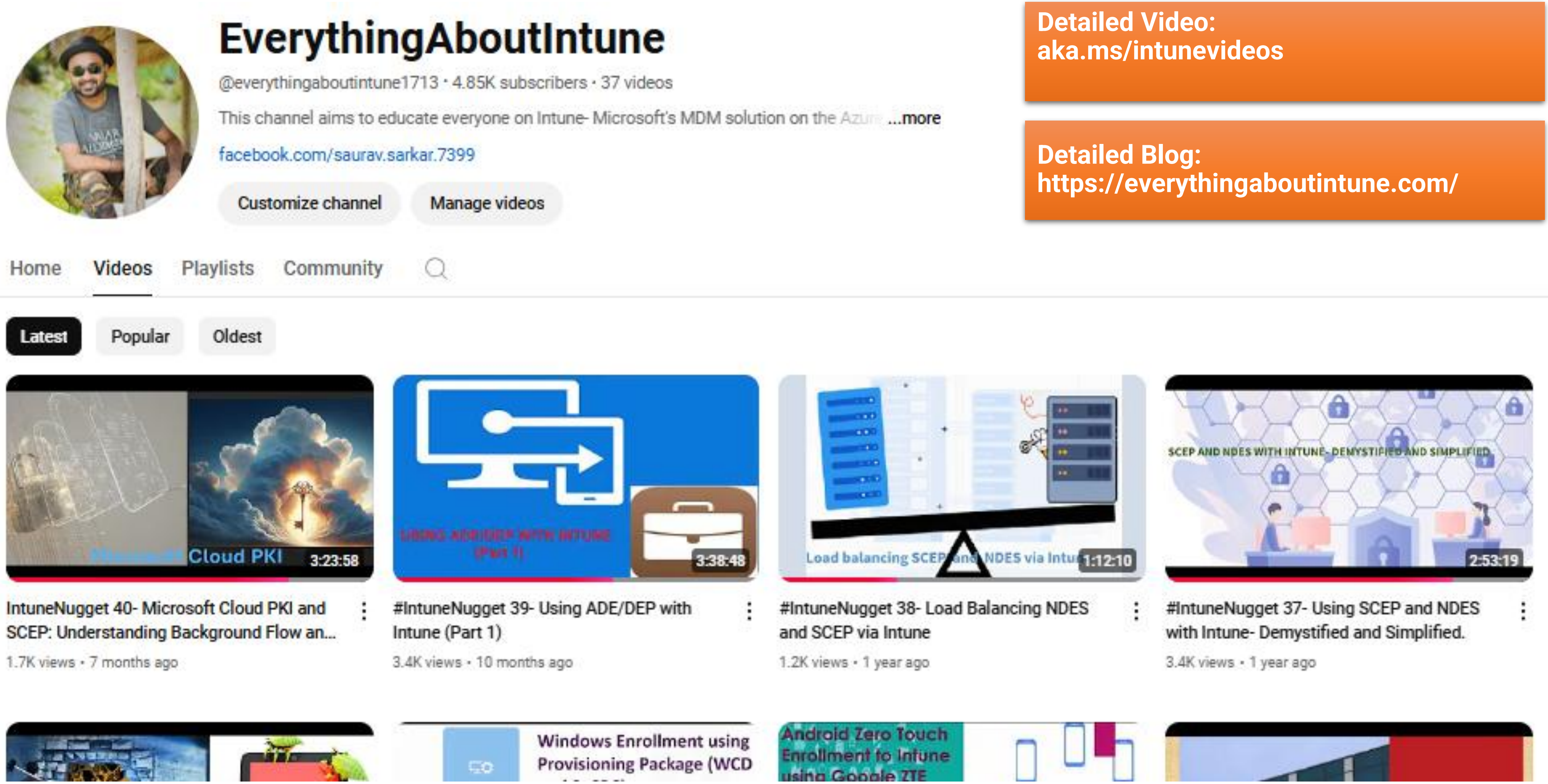
HOW TO MANAGE DEVICES #htmdcommunity @htmdcommunity

Conclusion

- Just to re-iterate, Microsoft recommendation is to provision new devices as Cloud Native using Entra ID join Autopilot while the existing Entra Hybrid Joined devices are removed as a part of device refresh cycle.

- Factors which we should keep in mind while choosing the best option for our organization includes:

  - Availability of IT admins to provision devices like for using Operating System Deployment (OSD) via ConfigMgr or Creating Profiles for Autopilot or Creating packages for using Windows Configuration Designer (WCD)
  - If we wish to ship devices directly to the end user and remove the IT admin intervention.
  - If we want to persist with on-prem management i.e. ConfigMgr
  - Network bandwidth availability and the URLs allowed in the client's network etc.



EverythingAboutIntune

@everythingaboutintune1713 · 4.85K subscribers · 37 videos

This channel aims to educate everyone on Intune- Microsoft's MDM solution on the Azure ...more

facebook.com/saurav.sarkar.7399

Customize channel
Manage videos
Home
Videos
Playlists
Community
Latest
Popular
Oldest
Cloud PKI
3:23:58
USING ADE/DEP WITH INTUNE (Part 1)
3:38:48
Load balancing SCEP and NDES via Intune
1:12:10
SCEP AND NDES WITH INTUNE- DEMYSTIFIED AND SIMPLIFIED
2:53:19
Windows Enrollment using Provisioning Package (WCD
Android Zero Touch Enrollment to Intune using Google ZTE

IntuneNugget 40- Microsoft Cloud PKI and SCEP: Understanding Background Flow an...
1.7K views • 7 months ago

#IntuneNugget 39- Using ADE/DEP with Intune (Part 1)
3.4K views • 10 months ago

#IntuneNugget 38- Load Balancing NDES and SCEP via Intune
1.2K views • 1 year ago

#IntuneNugget 37- Using SCEP and NDES with Intune- Demystified and Simplified.
3.4K views • 1 year ago

Detailed Video:
aka.ms/intunevideos

Detailed Blog:
https://everythingaboutintune.com/

THANK
YOU