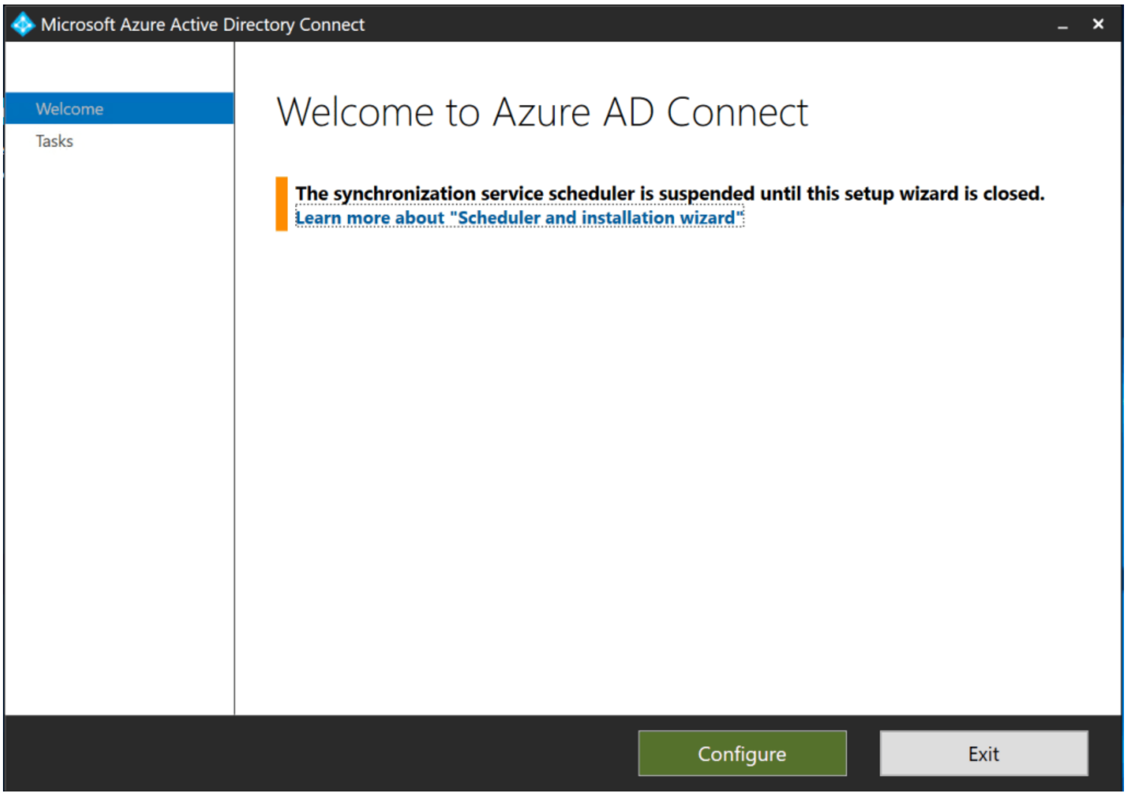
1. Configure Hybrid AD Join

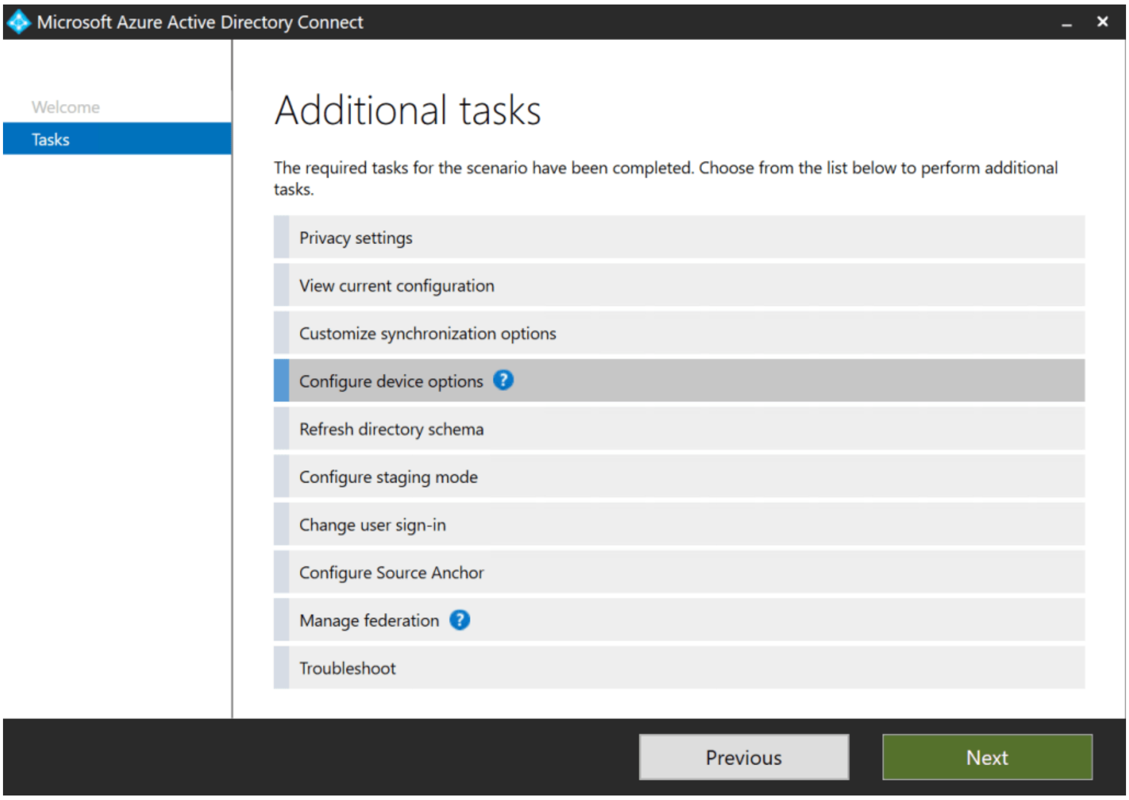
From the Azure AD Connect server, launch **Configuration Wizard** and click on **Configure**.



Welcome to Azure AD Connect

The synchronization service scheduler is suspended until this setup wizard is closed.
Learn more about "Scheduler and installation wizard"

Click on **Configure device options** then on **Next**.

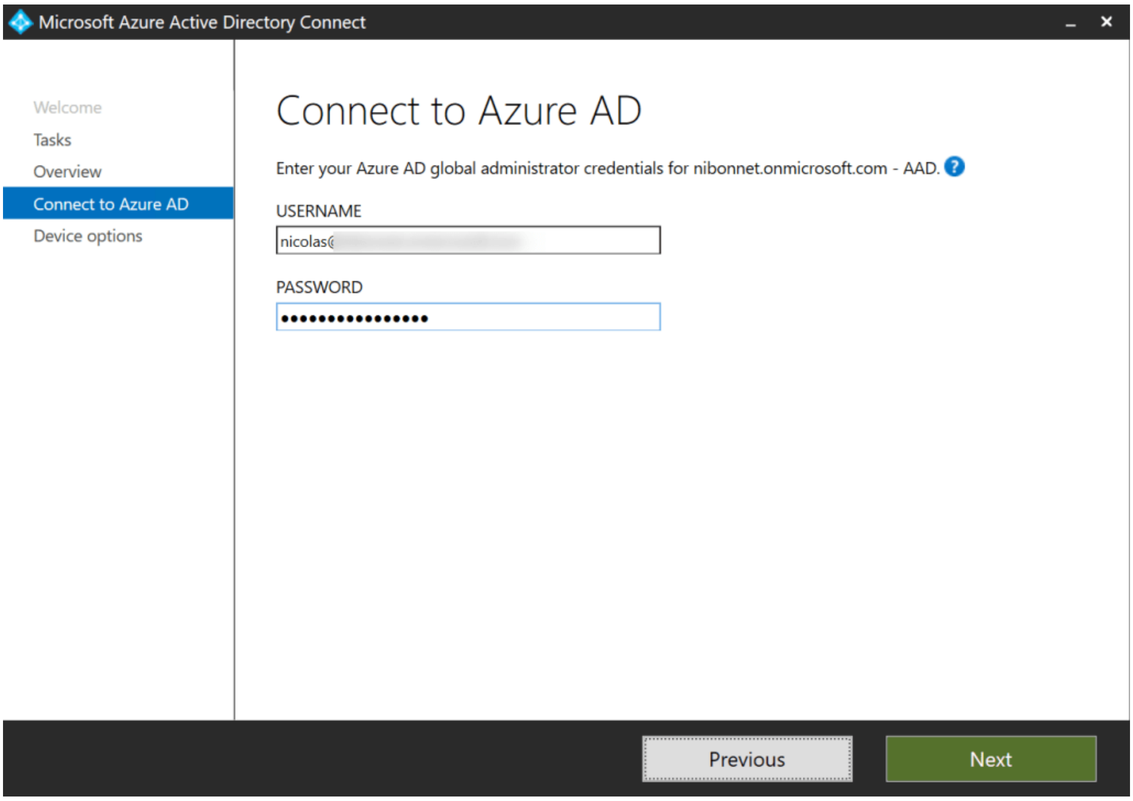


Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

- Privacy settings
- View current configuration
- Customize synchronization options
- Configure device options
- Refresh directory schema
- Configure staging mode
- Change user sign-in
- Configure Source Anchor
- Manage federation
- Troubleshoot

Enter credential of **Global Admin account** and click on **Next**.



Connect to Azure AD

Enter your Azure AD global administrator credentials for nibonnet.onmicrosoft.com - AAD.

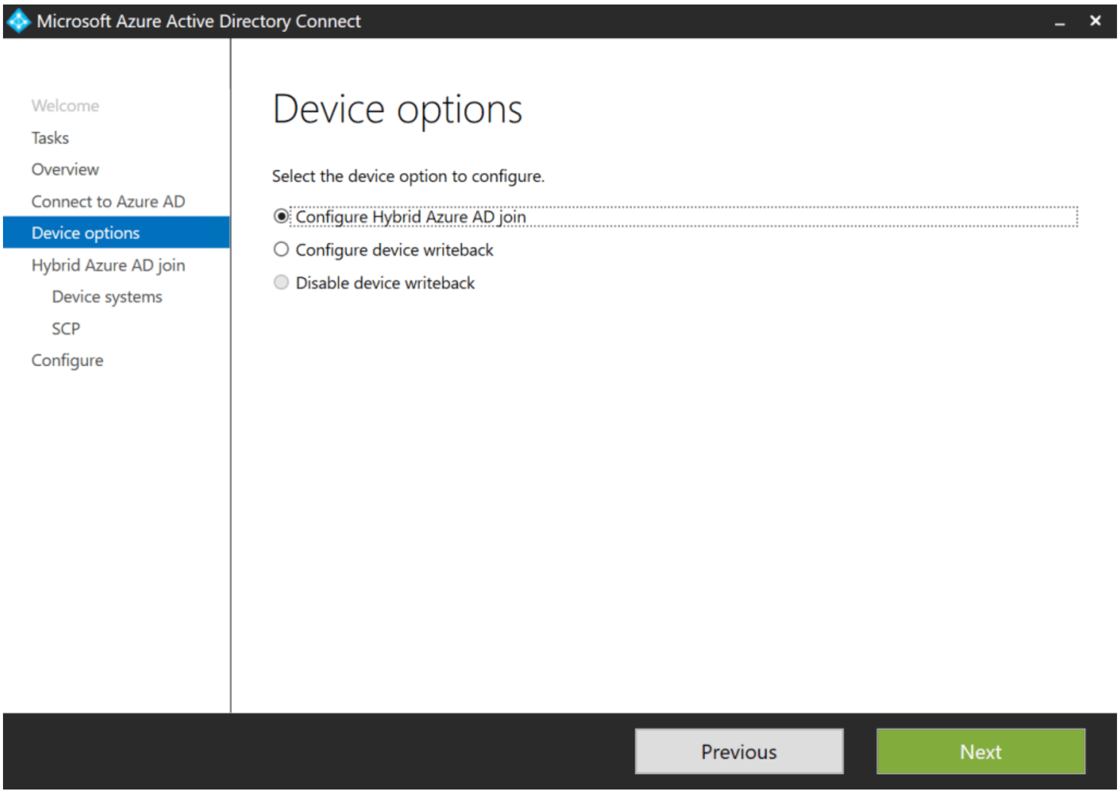
USERNAME

nicolas@[redacted]

PASSWORD

••••••••••••••••

Select **Configure Hybrid Azure AD Join** and click on **Next**.



Device options

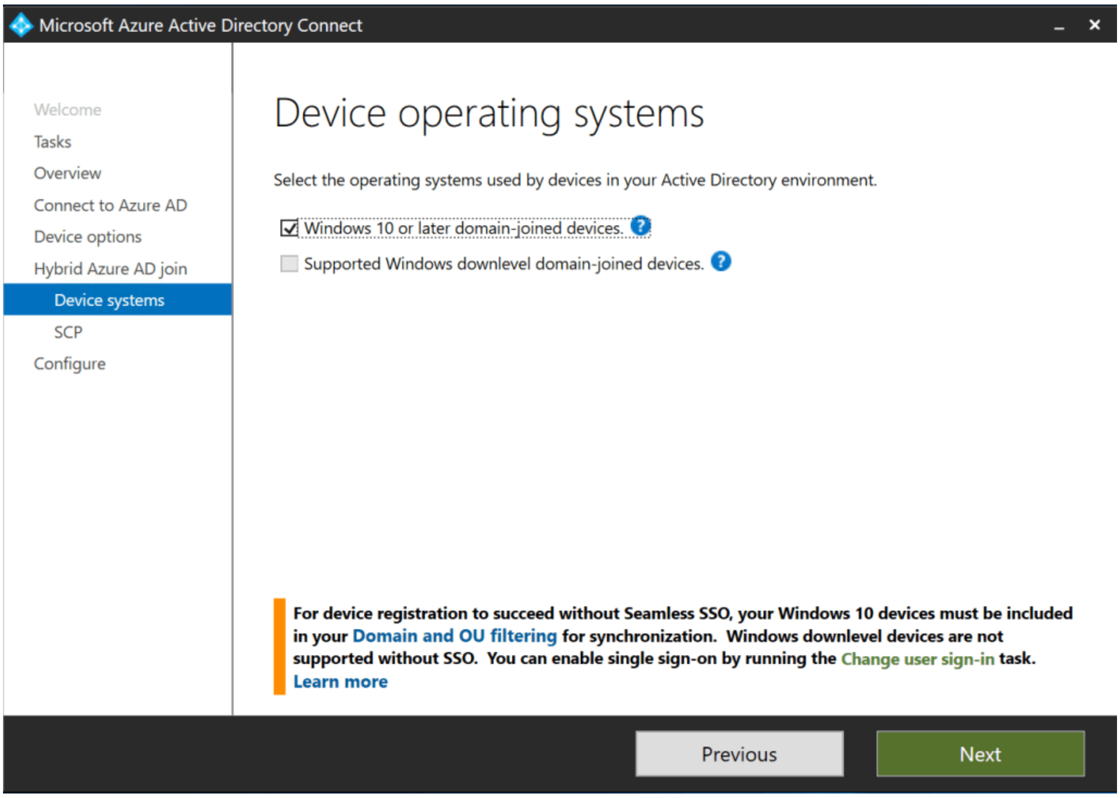
Select the device option to configure.

● Configure Hybrid Azure AD join

○ Configure device writeback

○ Disable device writeback

Check **Windows 10 or later domain-joined devices** and click on **Next**.



Device operating systems

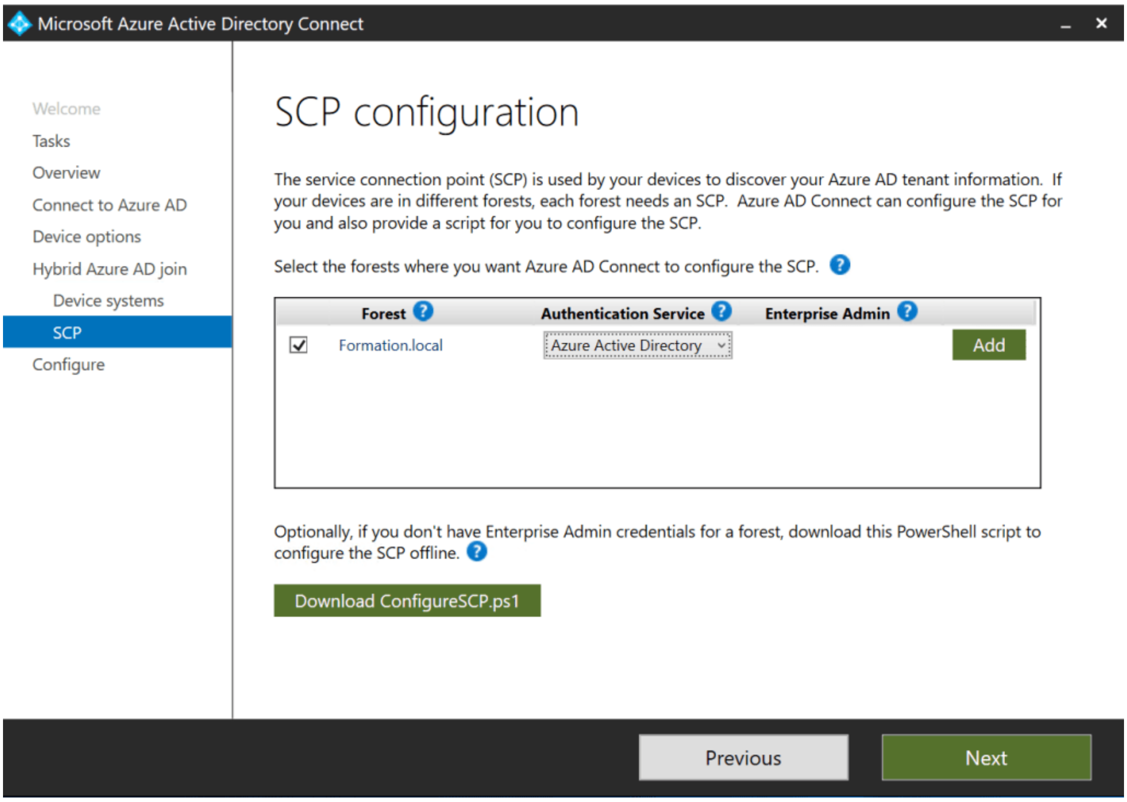
Select the operating systems used by devices in your Active Directory environment.

☑ Windows 10 or later domain-joined devices.

□ Supported Windows downlevel domain-joined devices.

For device registration to succeed without Seamless SSO, your Windows 10 devices must be included in your Domain and OU filtering for synchronization. Windows downlevel devices are not supported without SSO. You can enable single sign-on by running the Change user sign-in task. Learn more

The SCP configuration's must be set up. Check the Active Directory domain name and Azure Active Directory for the **Authentification Service.** Click on **Add** for add Enterprise Admin Account. Enter credential of Enterprise Admin Account and click on **Next**.



SCP configuration

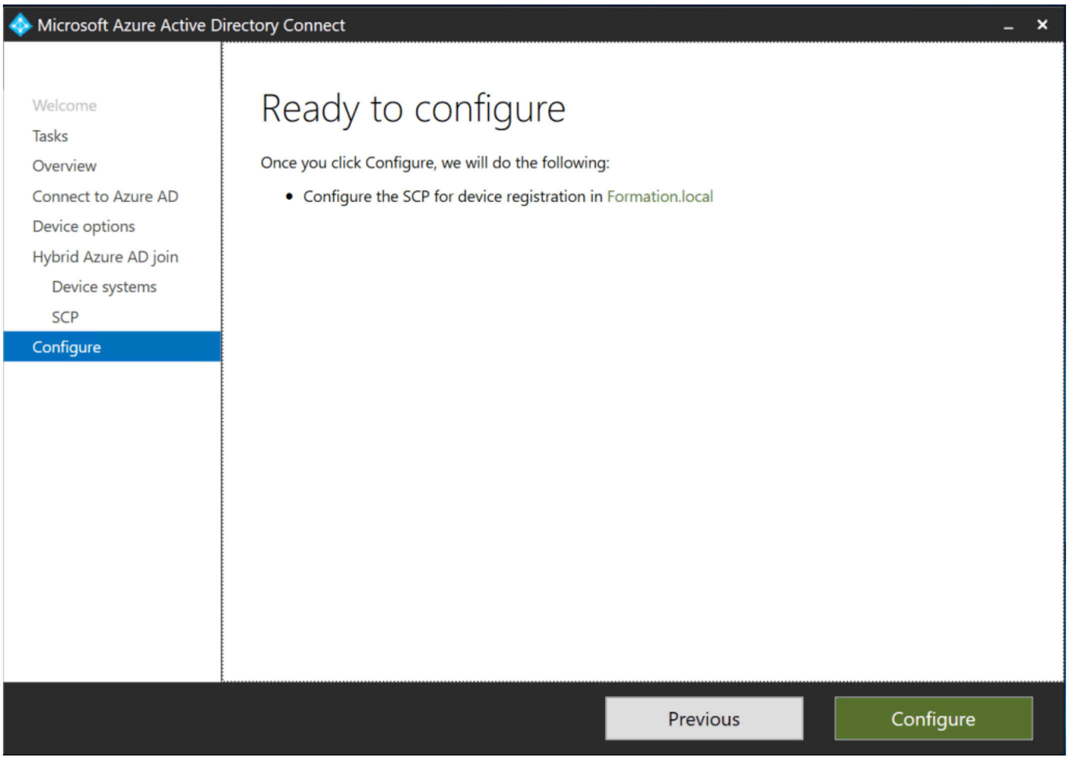
The service connection point (SCP) is used by your devices to discover your Azure AD tenant information. If your devices are in different forests, each forest needs an SCP. Azure AD Connect can configure the SCP for you and also provide a script for you to configure the SCP.

Select the forests where you want Azure AD Connect to configure the SCP.

	Forest	Authentication Service	Enterprise Admin
☑	Formation.local	Azure Active Directory	Add

Optionally, if you don't have Enterprise Admin credentials for a forest, download this PowerShell script to configure the SCP offline.

Click on **Configure** to launch configuration. Click on **Exit** when it's finished.



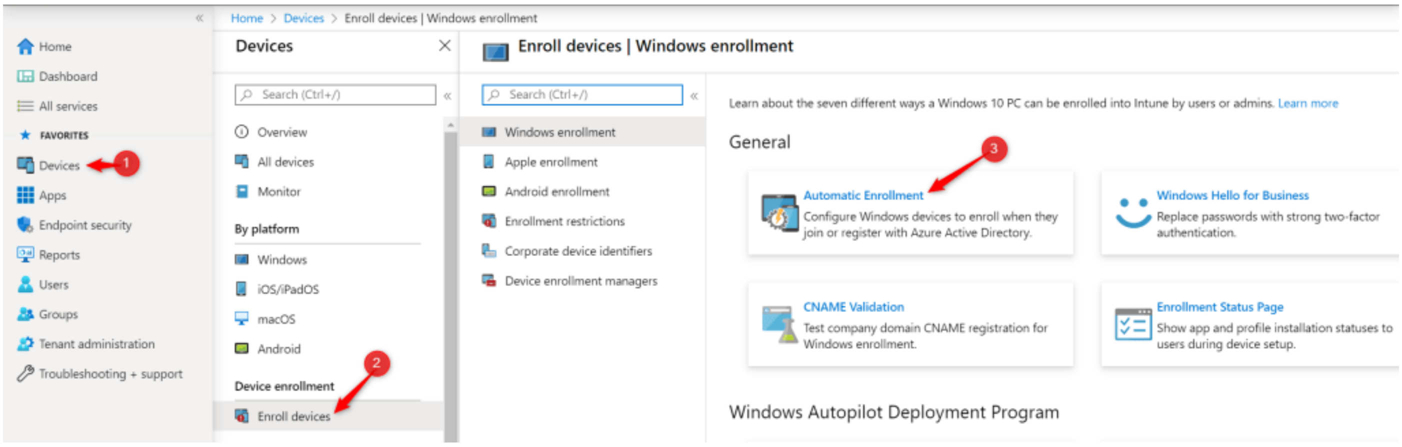
Ready to configure

Once you click Configure, we will do the following:

- Configure the SCP for device registration in Formation.local

1.1 Configure Automatic Enrollment

From the intune portal, click on **Devices**, on **Enroll devices** then on **Automatic Enrollment**.



Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

General

Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory.

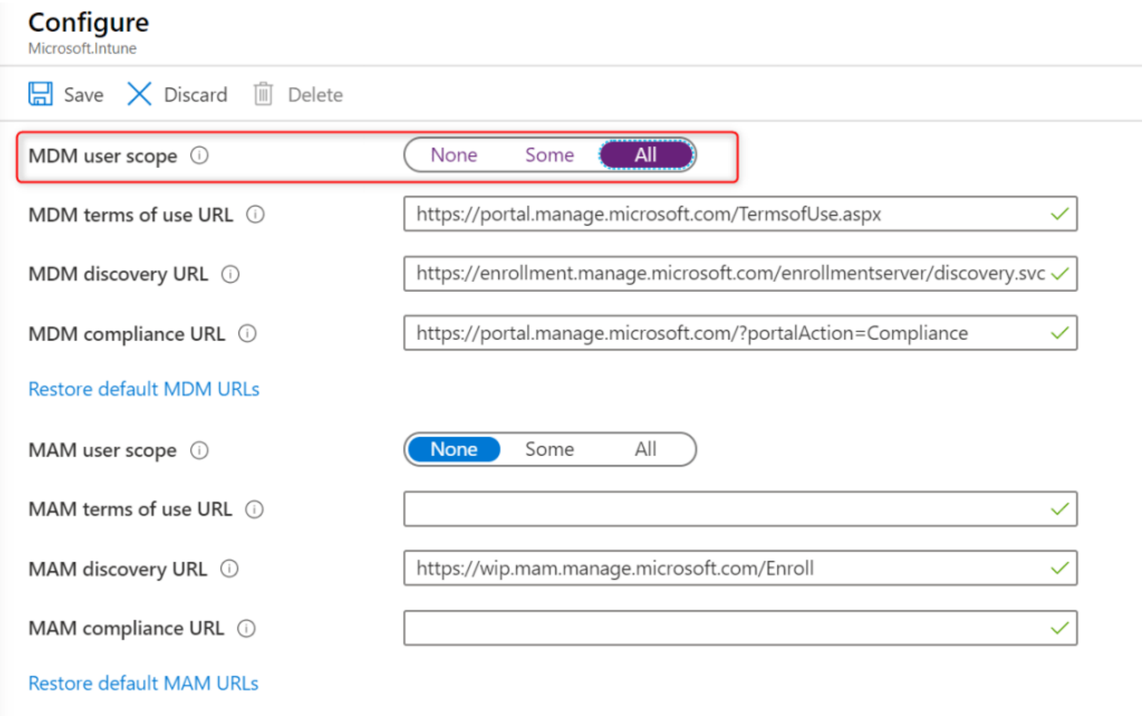
Windows Hello for Business
Replace passwords with strong two-factor authentication.

CNAME Validation
Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page
Show app and profile installation statuses to users during device setup.

Windows Autopilot Deployment Program

Configure **MDM user scope** and click on **Save**.



Configure

Microsoft.Intune

MDM user scope: None Some [✓ All]

MDM terms of use URL: https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL: https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc

MDM compliance URL: https://portal.manage.microsoft.com/?portalAction=Compliance

Restore default MDM URLs

MAM user scope: [✓ None] Some All

MAM terms of use URL:

MAM discovery URL: https://wip.mam.manage.microsoft.com/Enroll

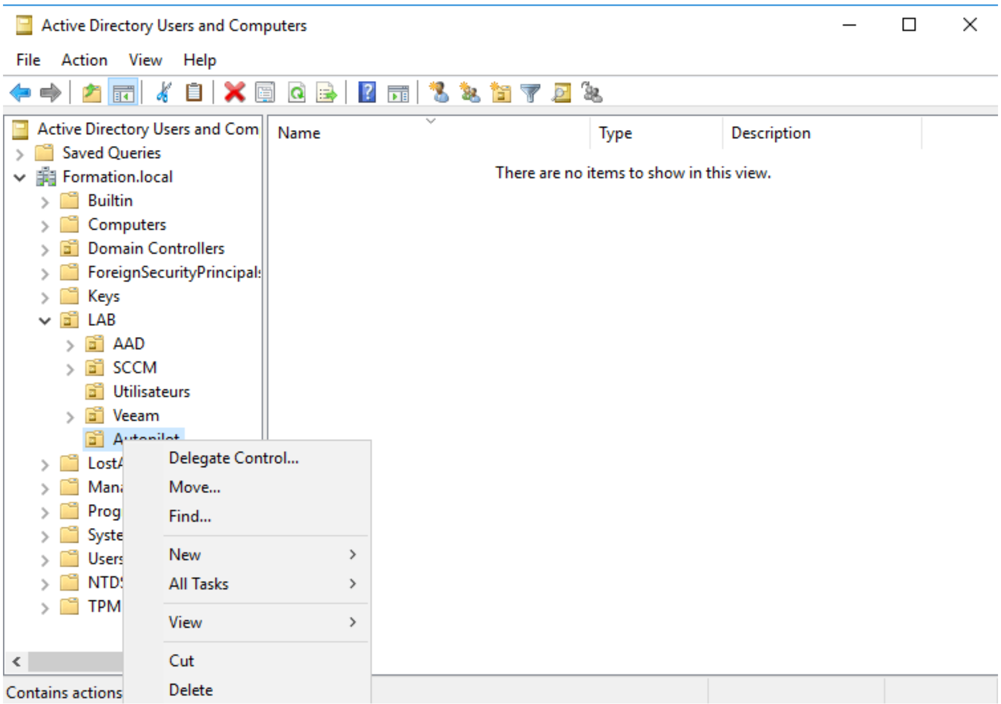
MAM compliance URL:

Restore default MAM URLs

1.2 Increase the computer account limit

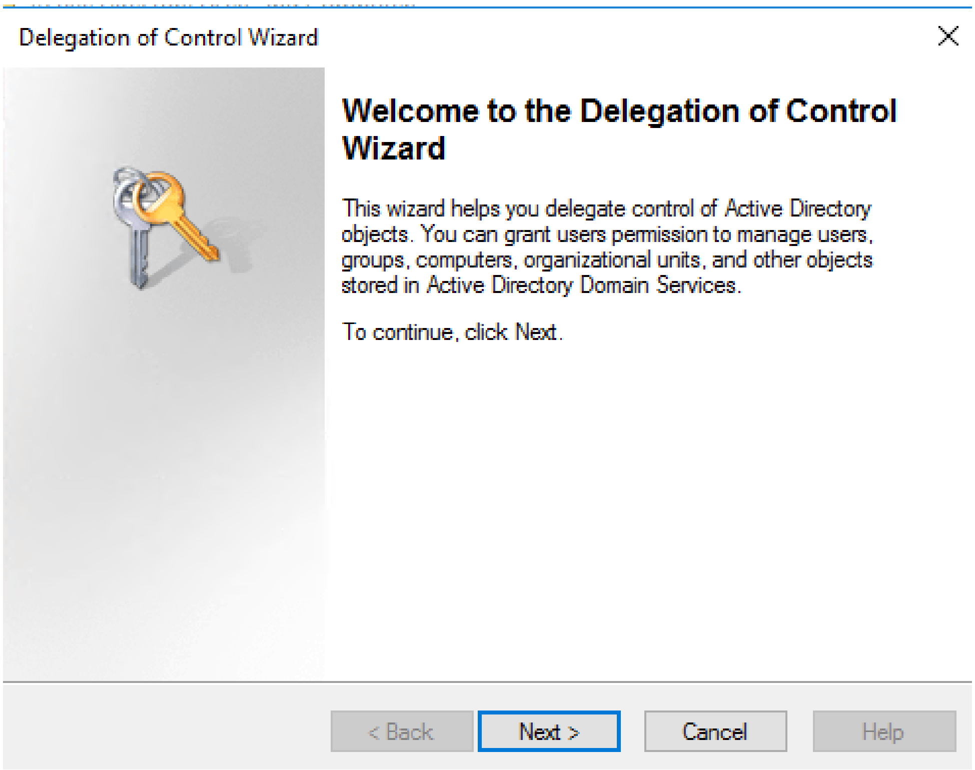
The computers account of the autopilot-enrolled computers has created by the Intune Connector in Active Directory. The computer that hosts the Intune Connector must have the rights to create the computer objects. Additionally a limit is configured on Active Directory. Each computer object can be create 10 computer object by default. So it's important to delegated to computer that host the intune connector the necessary right. I will positioned the permission on a Organization Unit. Nevertheless, it is possible to position the delegation on the root of the domain.

From the domain controller, open **Active Directory Users and Computers** and right click on the container who the delegation must be positioned and click on **Delegate Control**.



There are no items to show in this view.

A wizard appear, click on **Next**.



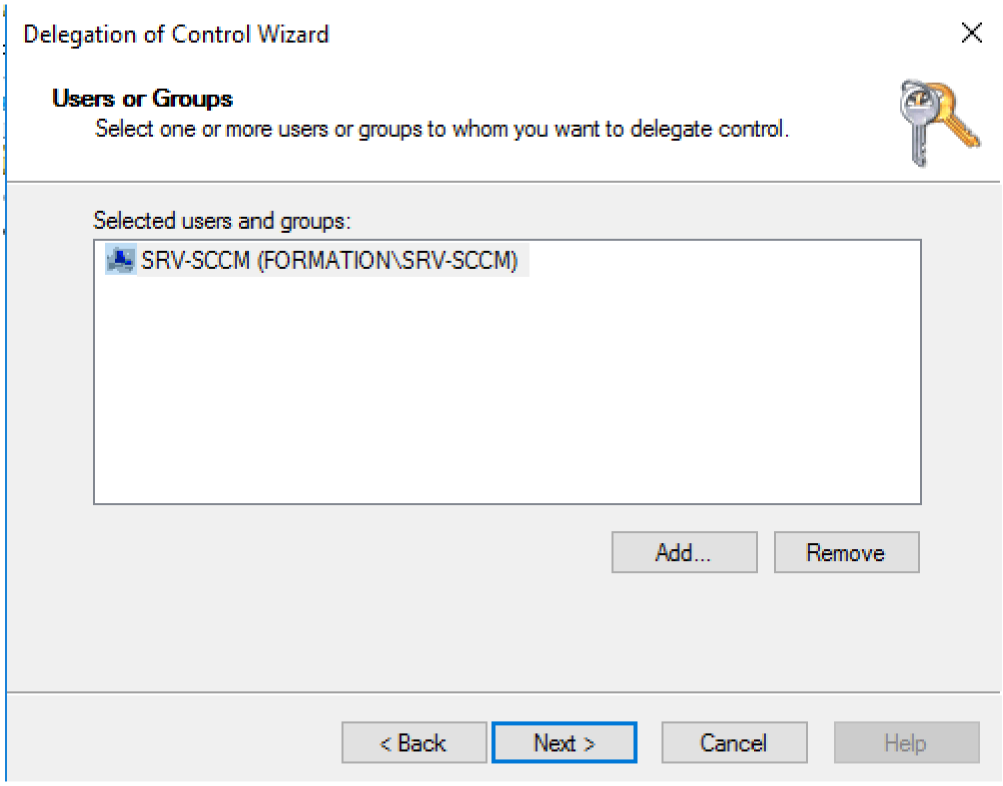
Delegation of Control Wizard

Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

Click on **Add** and select the desired computer account.



Delegation of Control Wizard

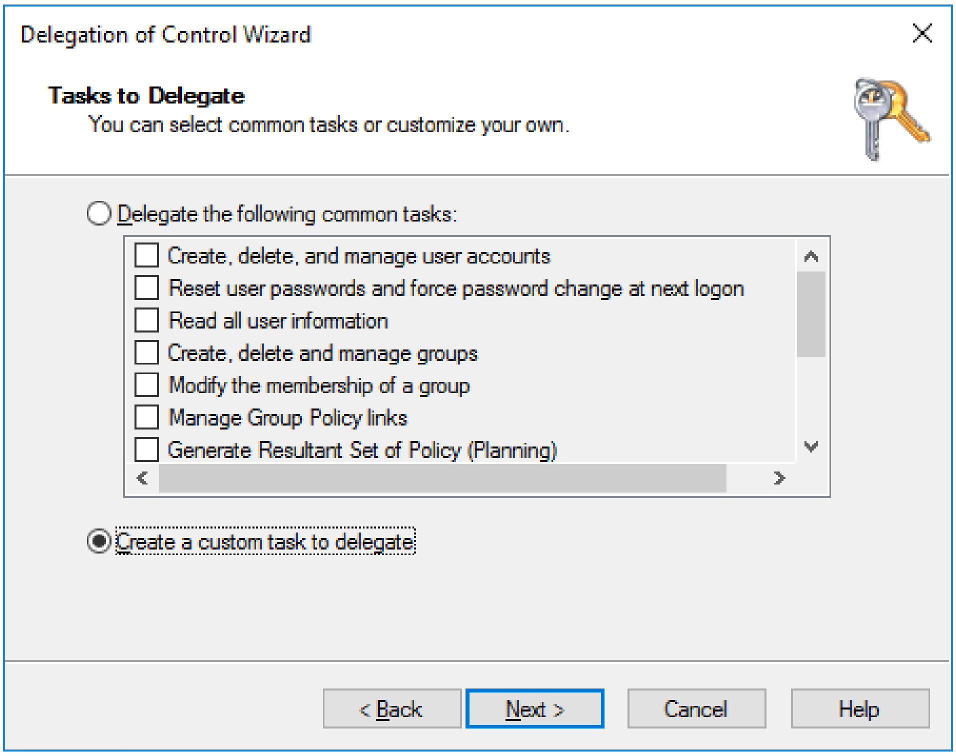
Users or Groups

Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

SRV-SCCM (FORMATION\SRV-SCCM)

Check **Create a custom task to delegate** then click on **Next**.



Delegation of Control Wizard

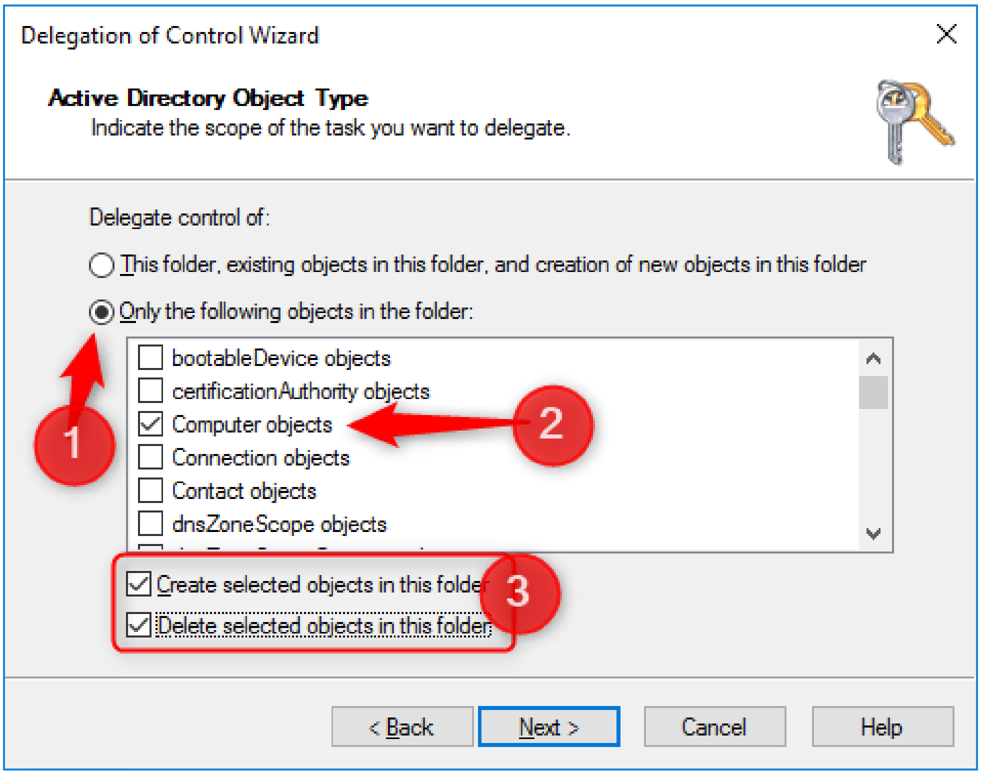
Tasks to Delegate
You can select common tasks or customize your own.

○ Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

● Create a custom task to delegate

Check **Only the following objects in the folder** and select Computer objects. Enable **Create selected objects in this folder** and **Delete selected objects in this folder options** then click on **Next**.



Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

○ This folder, existing objects in this folder, and creation of new objects in this folder

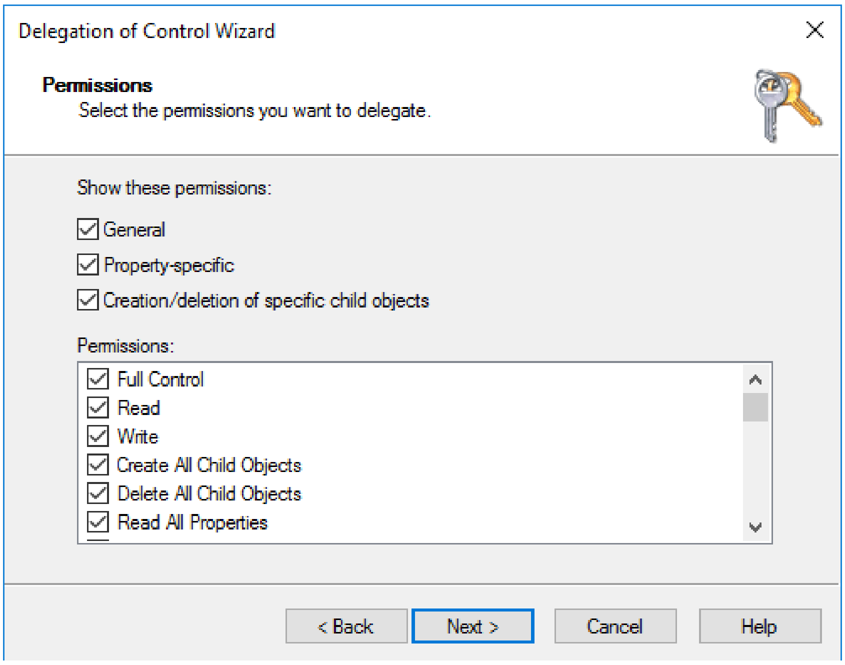
● Only the following objects in the folder:

- □ bootableDevice objects
- □ certificationAuthority objects
- ☑ Computer objects
- □ Connection objects
- □ Contact objects
- □ dnsZoneScope objects

☑ Create selected objects in this folde

☑ Delete selected objects in this folder

Select **Full Control** and click on **Next**.



Delegation of Control Wizard

Permissions
Select the permissions you want to delegate.

Show these permissions:

☑ General
☑ Property-specific
☑ Creation/deletion of specific child objects

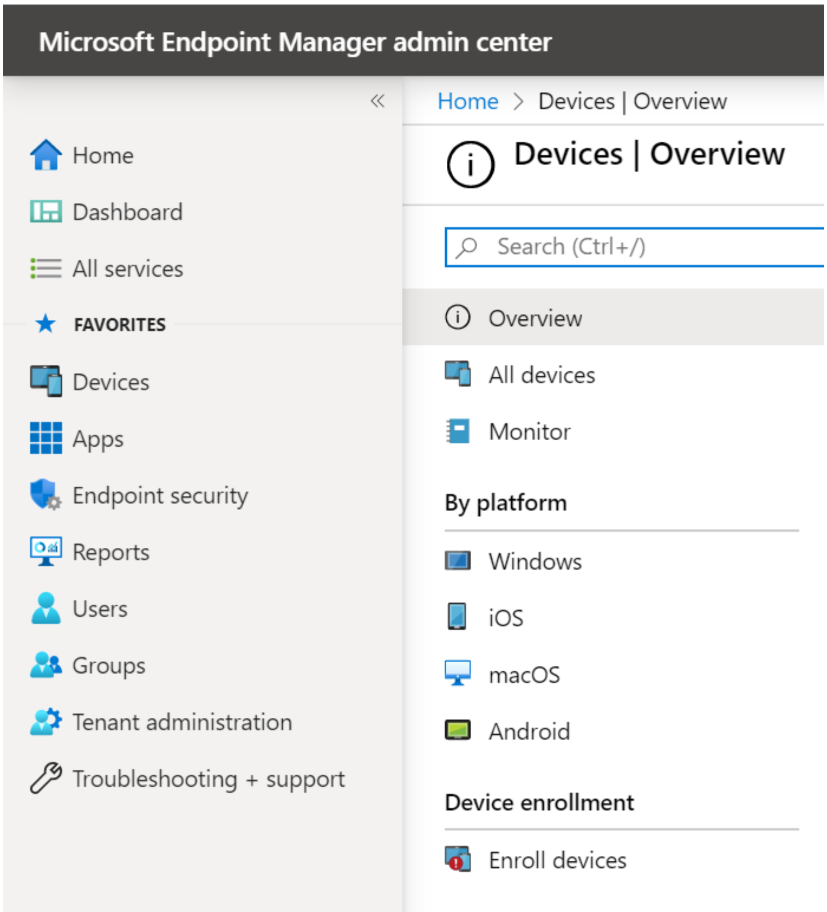
Permissions:

☑ Full Control
☑ Read
☑ Write
☑ Create All Child Objects
☑ Delete All Child Objects
☑ Read All Properties

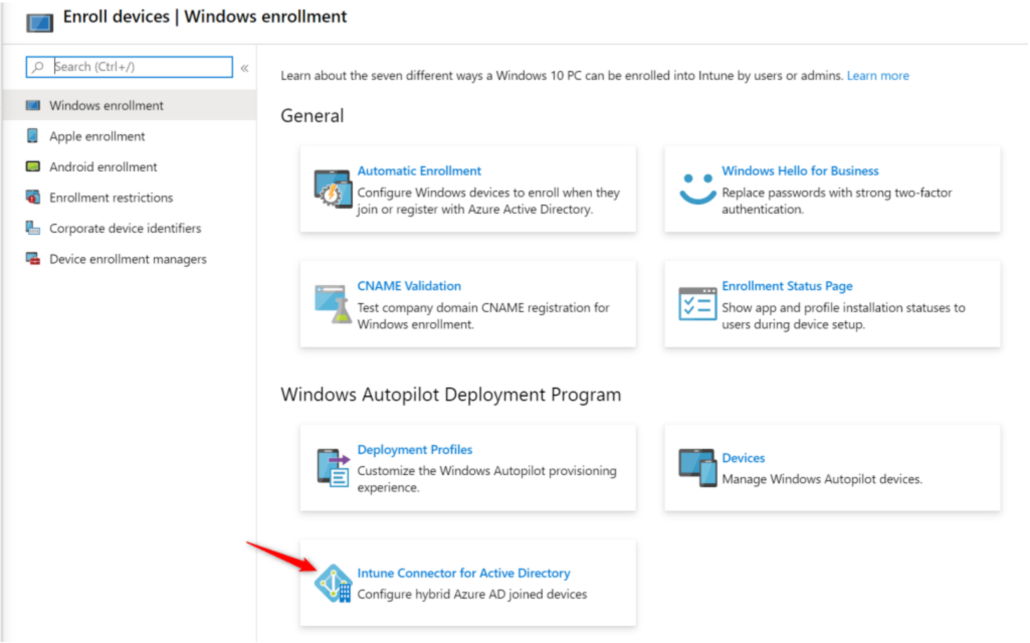
Click on **Next** and **Finish**.

1.3 Install Intune Hybrid Connector

From the Intune portal (endpoint.microsoft.com), click on **Devices** then on **Enroll devices**.



A new windows appear, click on **Intune Connector for Active Directory**.


Enroll devices | Windows enrollment

Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

General

Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business
Replace passwords with strong two-factor authentication.

CNAME Validation
Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page
Show app and profile installation statuses to users during device setup.

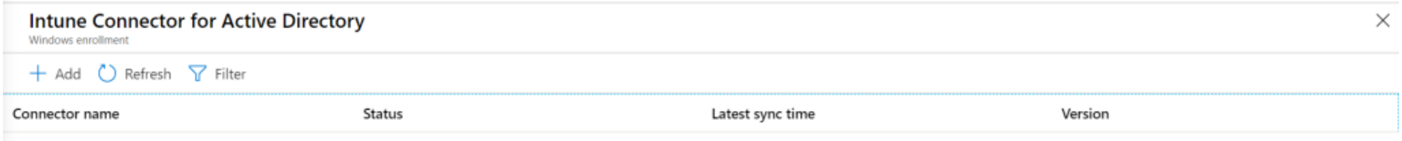
Windows Autopilot Deployment Program

Deployment Profiles
Customize the Windows Autopilot provisioning experience.

Devices
Manage Windows Autopilot devices.

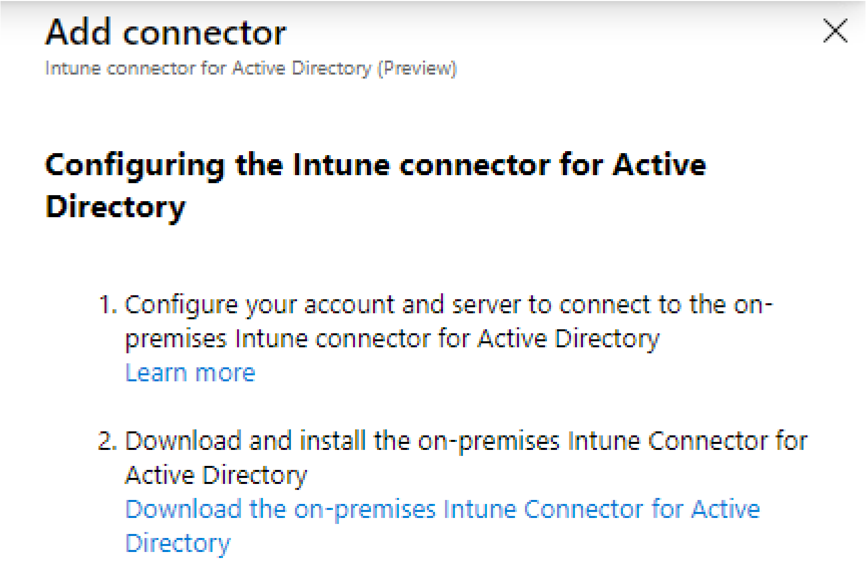
Intune Connector for Active Directory
Configure hybrid Azure AD joined devices

Click on **Add** for add new connector.


Intune Connector for Active Directory
Windows enrollment

Connector name	Status	Latest sync time	Version

Click on **Download** the on-premises Intune Connector for Active Directory for download the connector.


Add connector
Intune connector for Active Directory (Preview)

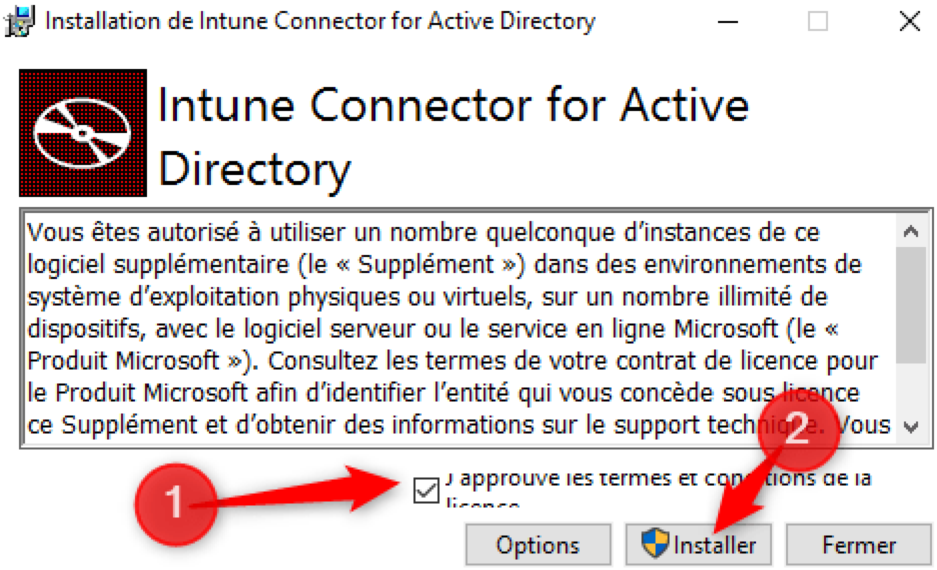
Configuring the Intune connector for Active Directory

1. Configure your account and server to connect to the on-premises Intune connector for Active Directory
   Learn more

2. Download and install the on-premises Intune Connector for Active Directory
   Download the on-premises Intune Connector for Active Directory

1.4 Install the Intune connector

From the server cho you want to install the connector, run the installation file. A new windows appear, Accept the terms of the licence and click on **Install**.

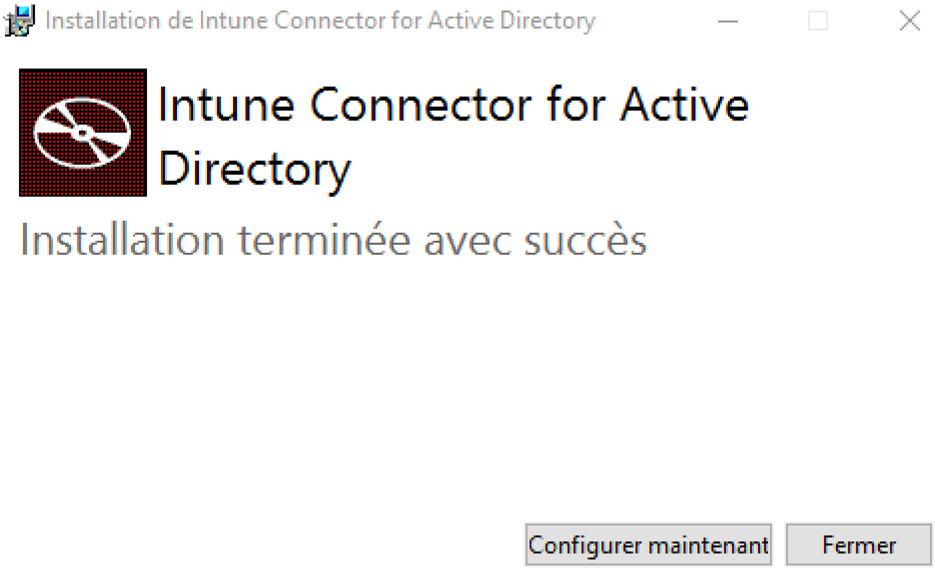


Installation de Intune Connector for Active Directory
Intune Connector for Active Directory
1
2
Options
Installer
Fermer

Vous êtes autorisé à utiliser un nombre quelconque d'instances de ce logiciel supplémentaire (le « Supplément ») dans des environnements de système d'exploitation physiques ou virtuels, sur un nombre illimité de dispositifs, avec le logiciel serveur ou le service en ligne Microsoft (le « Produit Microsoft »). Consultez les termes de votre contrat de licence pour le Produit Microsoft afin d'identifier l'entité qui vous concède sous licence ce Supplément et d'obtenir des informations sur le support technique. Vous

☑ J'approuve les termes et conditions de la licence

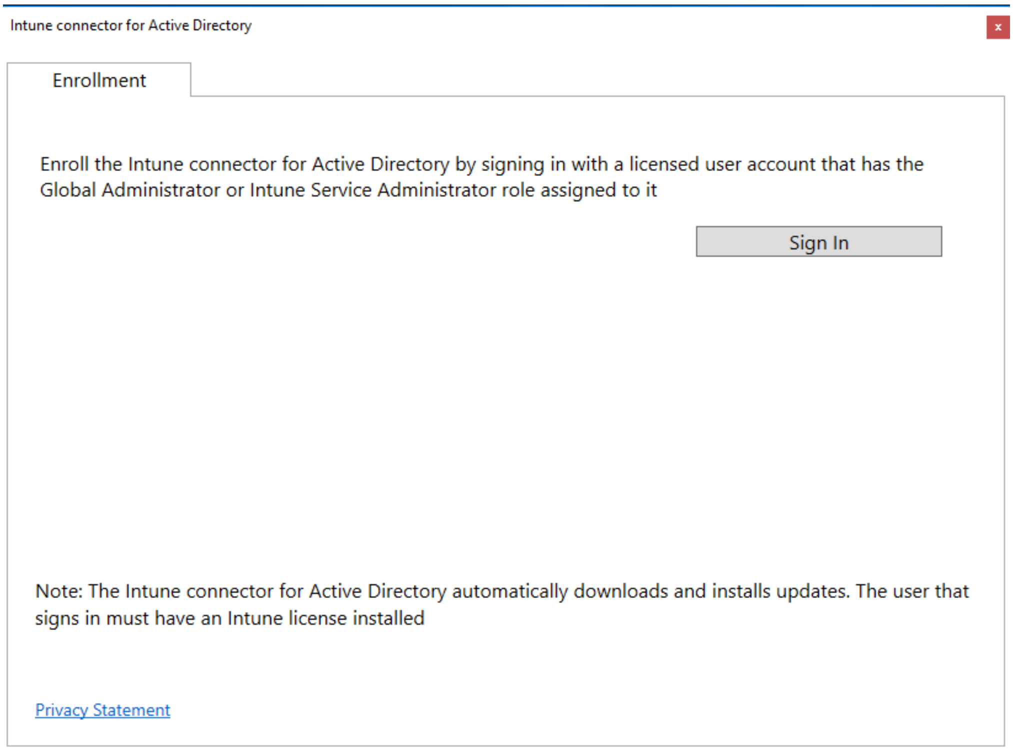
When the installation is finished, click on **Configure now**.



Installation de Intune Connector for Active Directory
Intune Connector for Active Directory
Configurer maintenant
Fermer

Installation terminée avec succès

A wizard appear, click on **Sign In**.



Intune connector for Active Directory

Enrollment

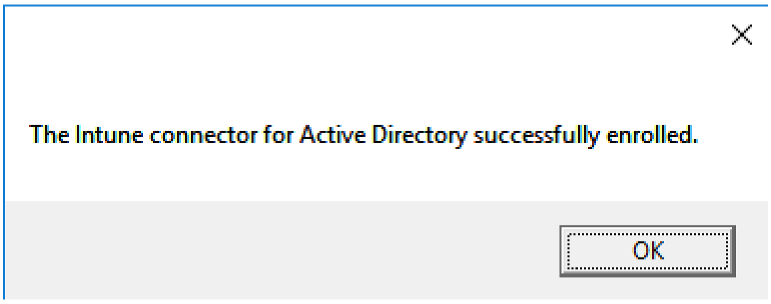
Enroll the Intune connector for Active Directory by signing in with a licensed user account that has the Global Administrator or Intune Service Administrator role assigned to it

Sign In

Note: The Intune connector for Active Directory automatically downloads and installs updates. The user that signs in must have an Intune license installed

Privacy Statement

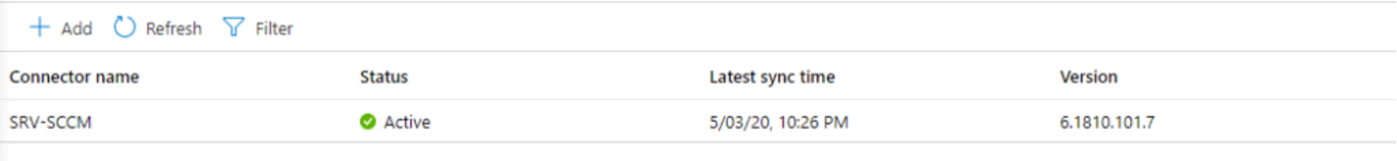
Enter username and password of Admin account. The Intune Connector for Active Directory is successfully enrolled, click **OK** and close the wizard.



The Intune connector for Active Directory successfully enrolled.

OK

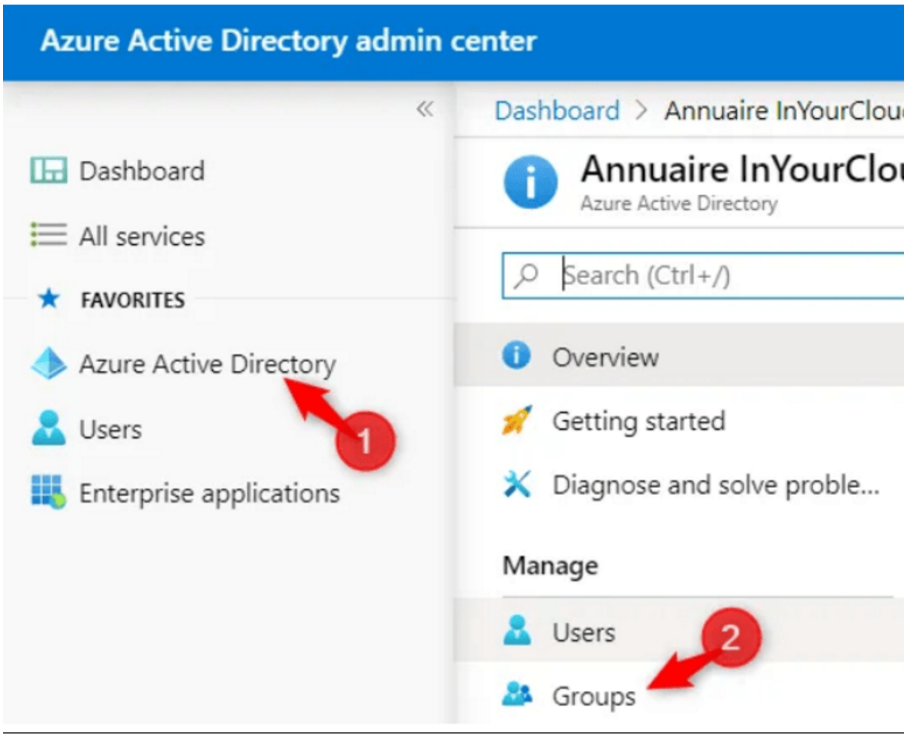
On the Intune portal, Click to **Devices**, **Windows**, **Windows enrollment** and **Intune Connector for Active Directory**. The statut of the connector is Active.



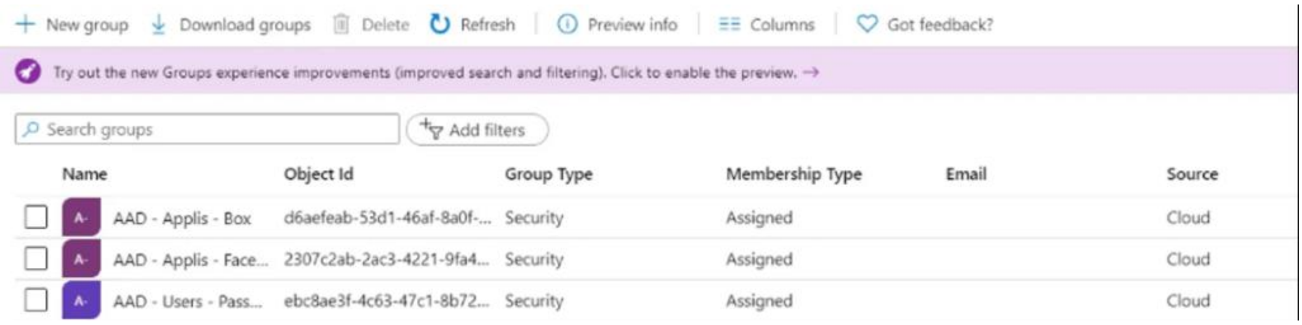
Connector name	Status	Latest sync time	Version
SRV-SCCM	✓ Active	5/03/20, 10:26 PM	6.1810.101.7

1.5 Create dynamic group

From the **Azure AD portal**, click on Azure Active Directory then on Groups.



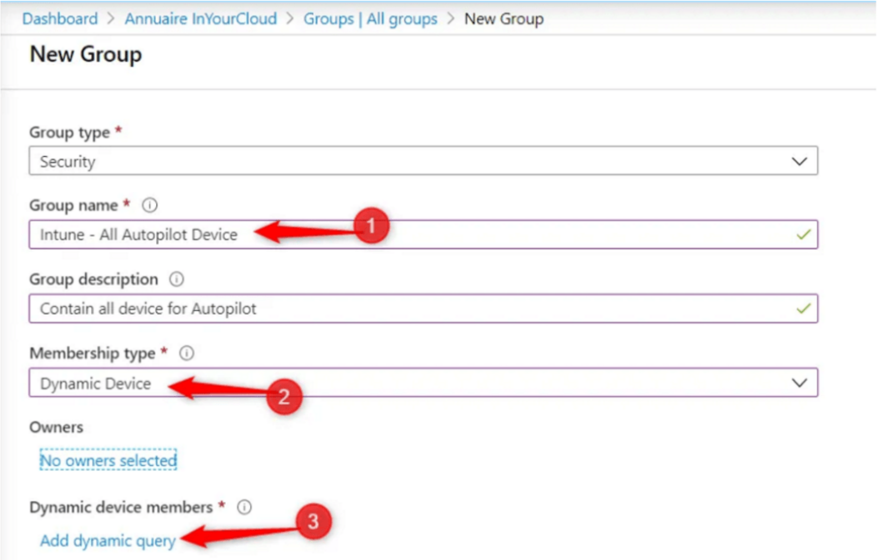
Click on **New Group** for create new group.



Try out the new Groups experience improvements (improved search and filtering). Click to enable the preview. →

	Name	Object Id	Group Type	Membership Type	Email	Source
□	A- AAD - Applis - Box	d6aefeab-53d1-46af-8a0f-...	Security	Assigned		Cloud
□	A- AAD - Applis - Face...	2307c2ab-2ac3-4221-9fa4...	Security	Assigned		Cloud
□	A- AAD - Users - Pass...	ebc8ae3f-4c63-47c1-8b72...	Security	Assigned		Cloud

Enter the name of the group and select **Dynamic Device** on **Membership type**. Click on **Add dynamic query** for add query.



Dashboard > Annuaire InYourCloud > Groups | All groups > New Group

New Group

Group type *

Security

Group name *

Intune - All Autopilot Device

Group description

Contain all device for Autopilot

Membership type *

Dynamic Device

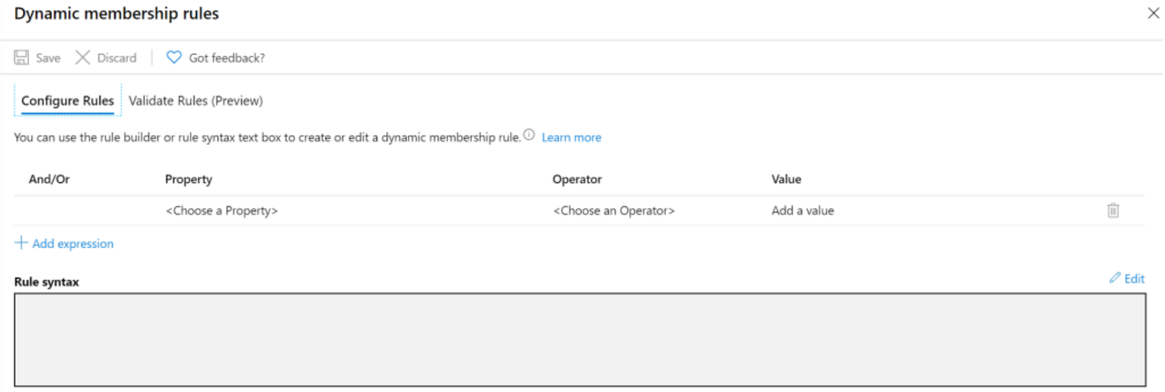
Owners

No owners selected

Dynamic device members *

Add dynamic query

Click on **Edit** then on **Rule Syntax**.



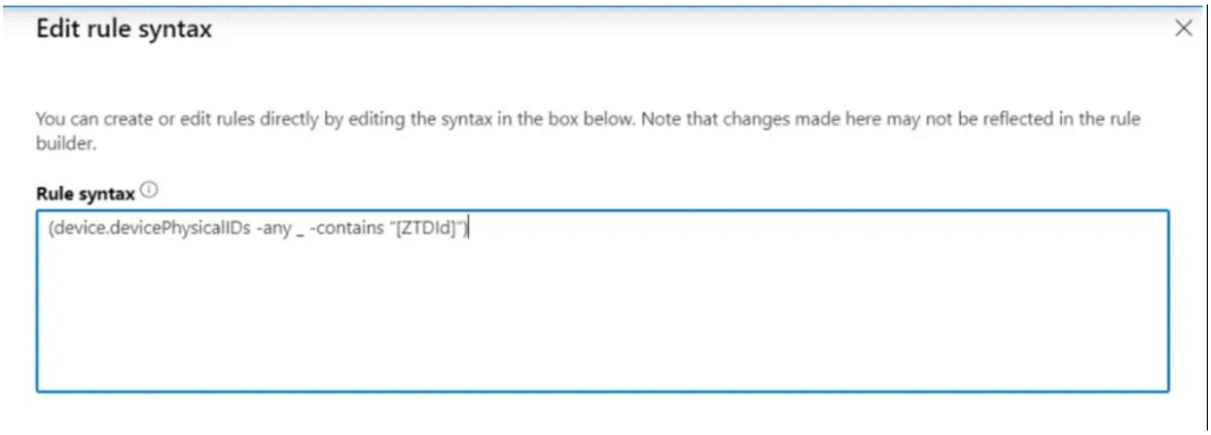
Dynamic membership rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. Learn more

And/Or	Property	Operator	Value
	<Choose a Property>	<Choose an Operator>	Add a value

Rule syntax

Enter the query (**device.devicePhysicalIDs -any _ -contains "[ZTDId]"**) and click on **OK**.



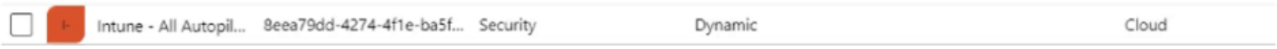
Edit rule syntax

You can create or edit rules directly by editing the syntax in the box below. Note that changes made here may not be reflected in the rule builder.

Rule syntax

```
(device.devicePhysicalIDs -any _ -contains "[ZTDId]")
```

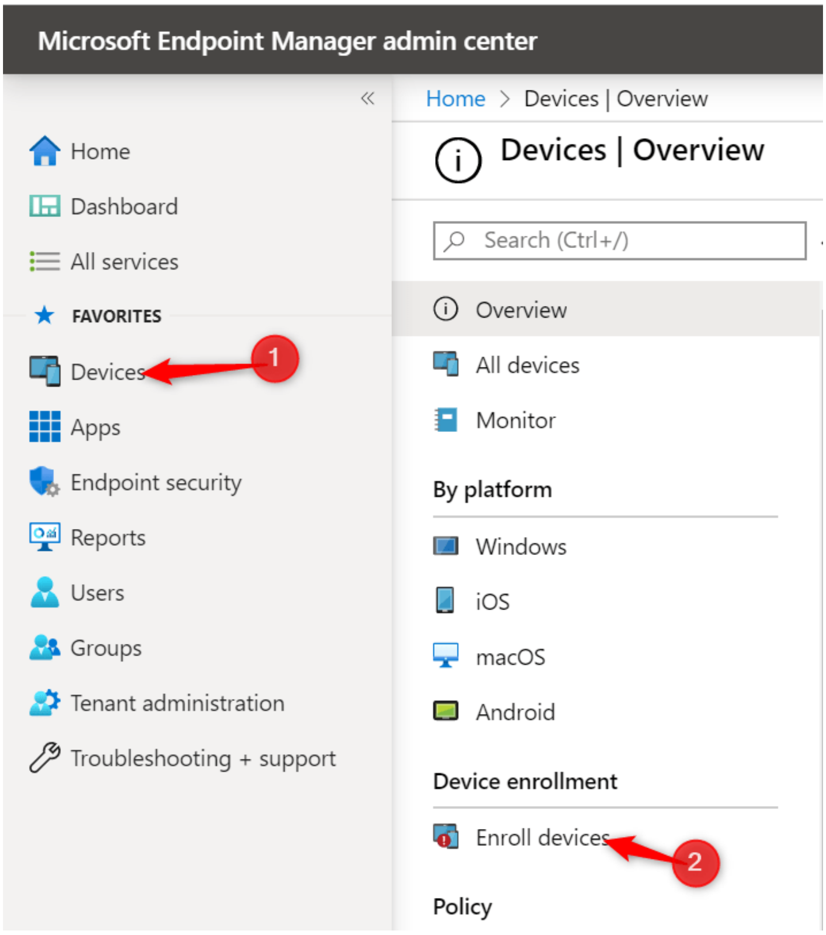
Click on **Save** then on **Create**.



□	Intune - All Autopil...	8eea79dd-4274-4f1e-ba5f...	Security	Dynamic	Cloud

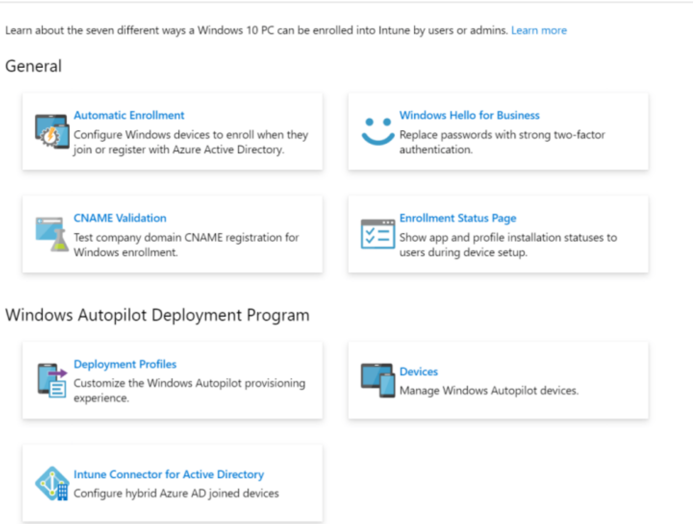
1.6 CreateDeployment Profiles

From the intune portal, click on **Devices** then on **Enroll devices**.



Microsoft Endpoint Manager admin center

Click on **Deployment Profiles**.



Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

General

Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business
Replace passwords with strong two-factor authentication.

CNAME Validation
Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page
Show app and profile installation statuses to users during device setup.

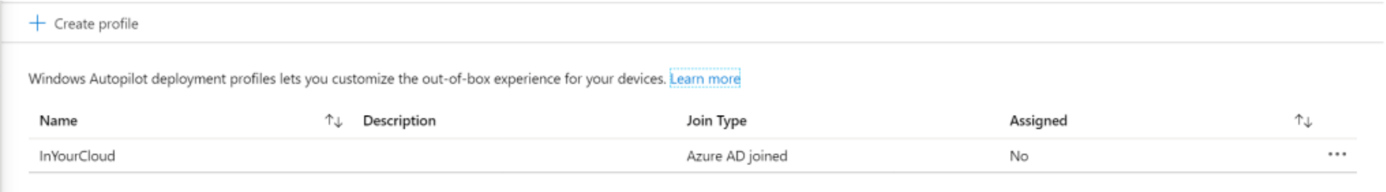
Windows Autopilot Deployment Program

Deployment Profiles
Customize the Windows Autopilot provisioning experience.

Devices
Manage Windows Autopilot devices.

Intune Connector for Active Directory
Configure hybrid Azure AD joined devices

Click on **Create profile** for create new deployment profile.

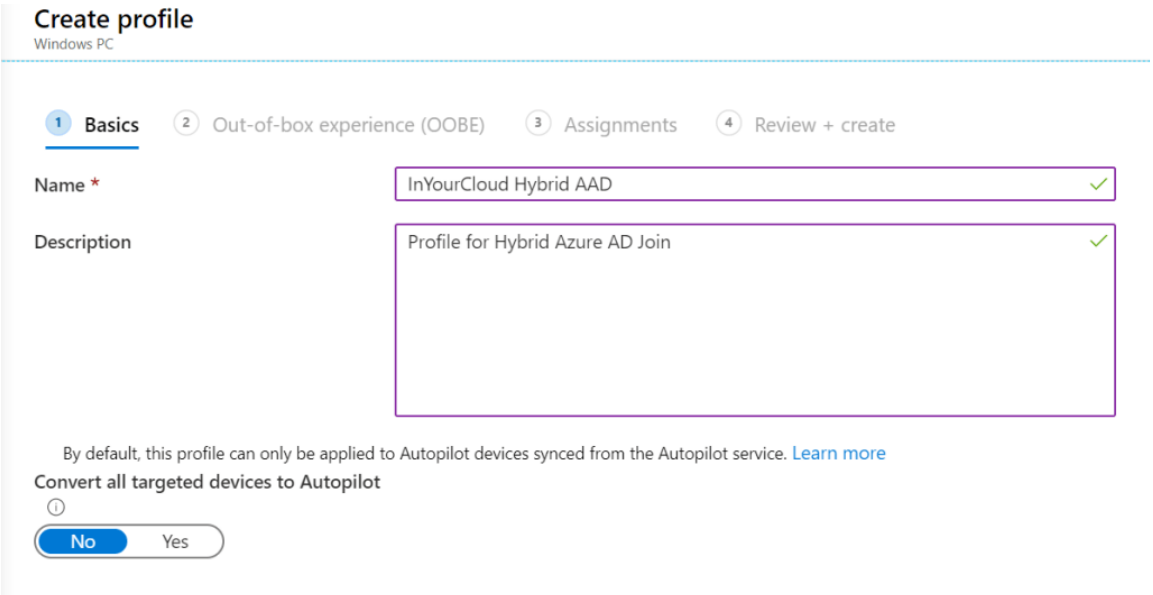


+ Create profile

Windows Autopilot deployment profiles lets you customize the out-of-box experience for your devices. Learn more

Name ↑↓	Description	Join Type	Assigned ↑↓
InYourCloud		Azure AD joined	No

Enter the name of the profile, the description and click on **Next**.



Create profile

Windows PC

1 Basics   2 Out-of-box experience (OOBE)   3 Assignments   4 Review + create

Name * InYourCloud Hybrid AAD ✓

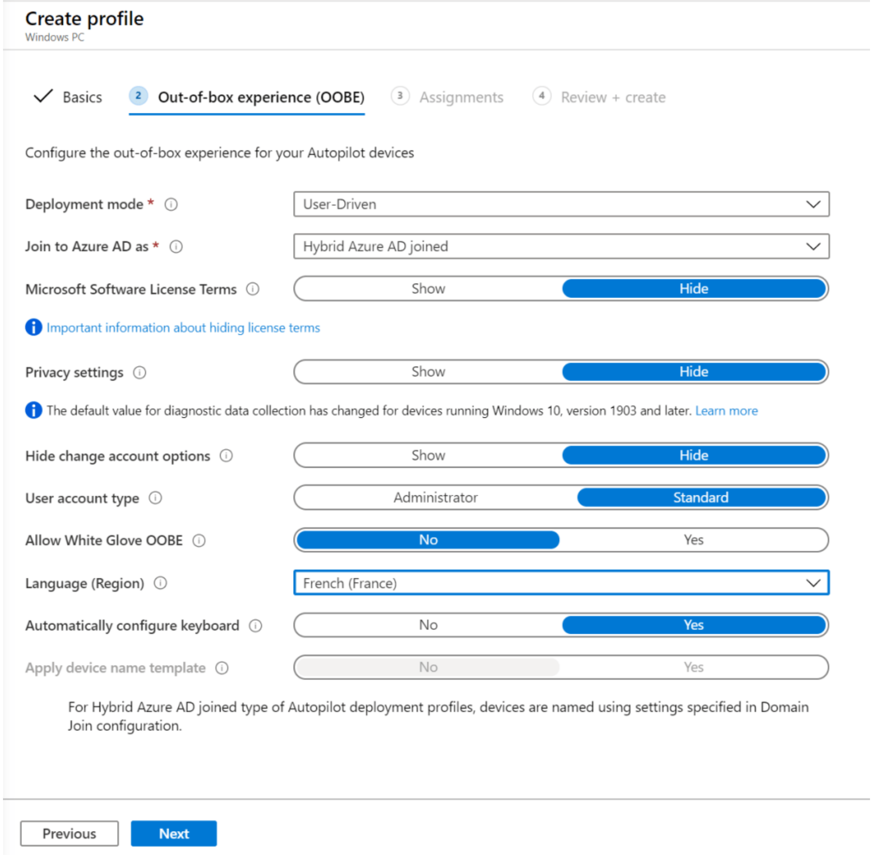
Description Profile for Hybrid Azure AD Join ✓

By default, this profile can only be applied to Autopilot devices synced from the Autopilot service. Learn more

Convert all targeted devices to Autopilot ⓘ

[✓ No] Yes

Select **Hybrid Azure AD joined** configure other option.



Create profile

Windows PC

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

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

Deployment mode * ⓘ User-Driven

Join to Azure AD as * ⓘ Hybrid Azure AD joined

Microsoft Software License Terms ⓘ Show [✓ Hide]

ⓘ 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. Learn more

Hide change account options ⓘ Show [✓ Hide]

User account type ⓘ Administrator [✓ Standard]

Allow White Glove OOBE ⓘ [✓ No] Yes

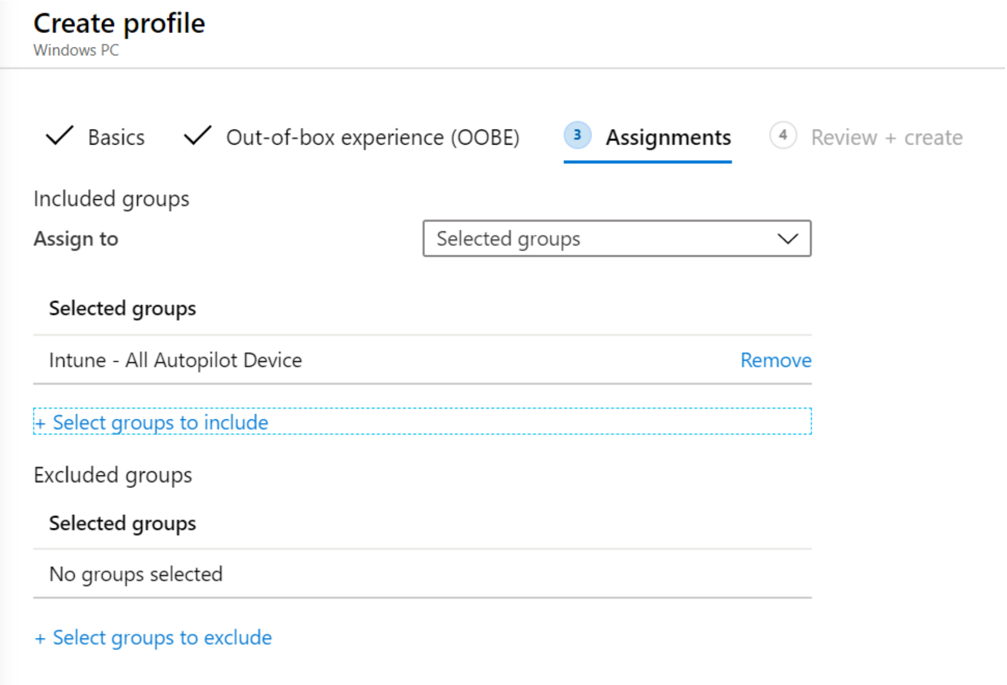
Language (Region) ⓘ French (France)

Automatically configure keyboard ⓘ No [✓ Yes]

Apply device name template ⓘ No Yes

For Hybrid Azure AD joined type of Autopilot deployment profiles, devices are named using settings specified in Domain Join configuration.

Assign to the desired groups and create profile.



Create profile

Windows PC

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

Included groups

Assign to: Selected groups

Selected groups

Intune - All Autopilot Device — Remove

+ Select groups to include

Excluded groups

Selected groups

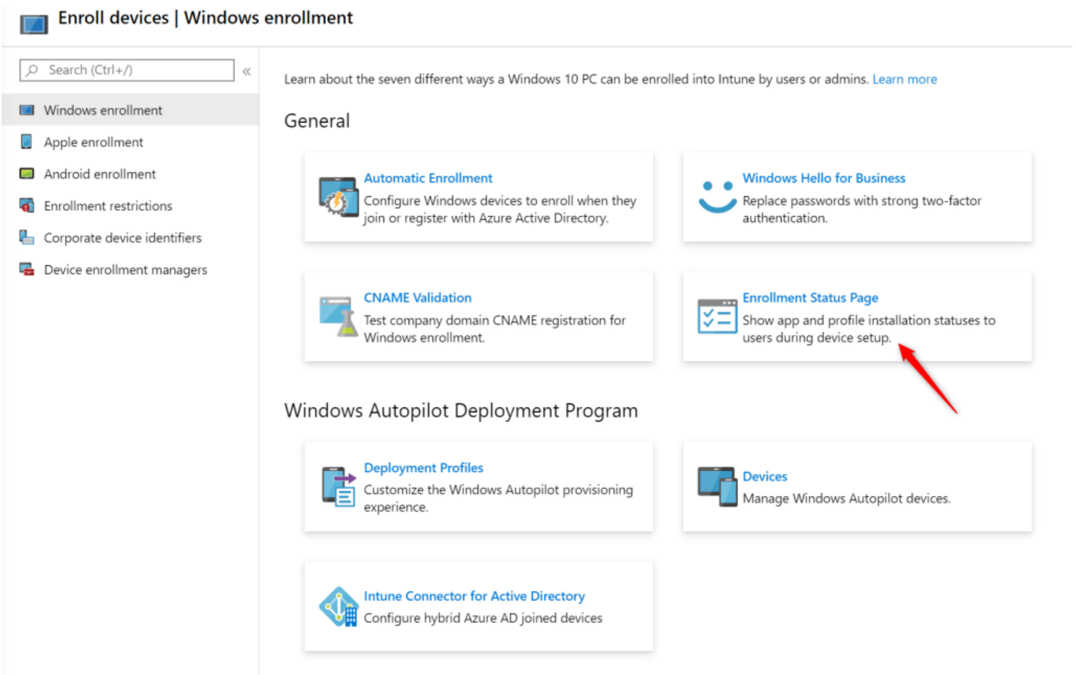
No groups selected

+ Select groups to exclude

The deployment profiles is now correctly created.

1.7 Configure Enrollment Status Page

From the Intune portal, click on **Devices**, **Enroll devices** and click on **Enrollment Status Page**.



Enroll devices | Windows enrollment

Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

General

Automatic Enrollment: Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business: Replace passwords with strong two-factor authentication.

CNAME Validation: Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page: Show app and profile installation statuses to users during device setup.

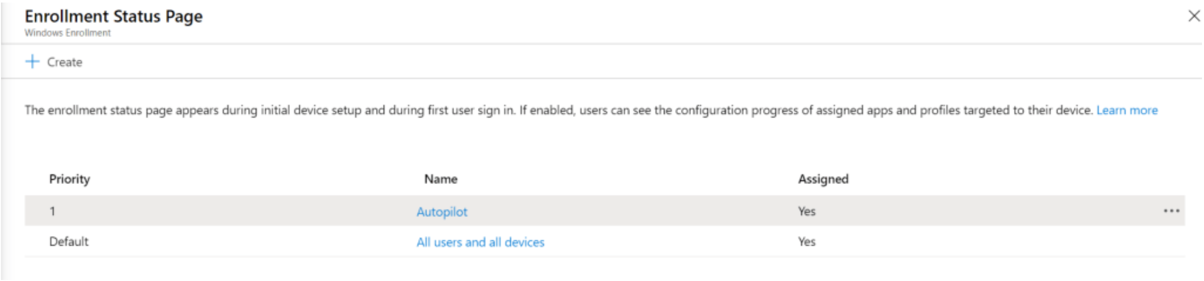
Windows Autopilot Deployment Program

Deployment Profiles: Customize the Windows Autopilot provisioning experience.

Devices: Manage Windows Autopilot devices.

Intune Connector for Active Directory: Configure hybrid Azure AD joined devices

Click on **Create** for create new Enrollment Status Page.



Enrollment Status Page

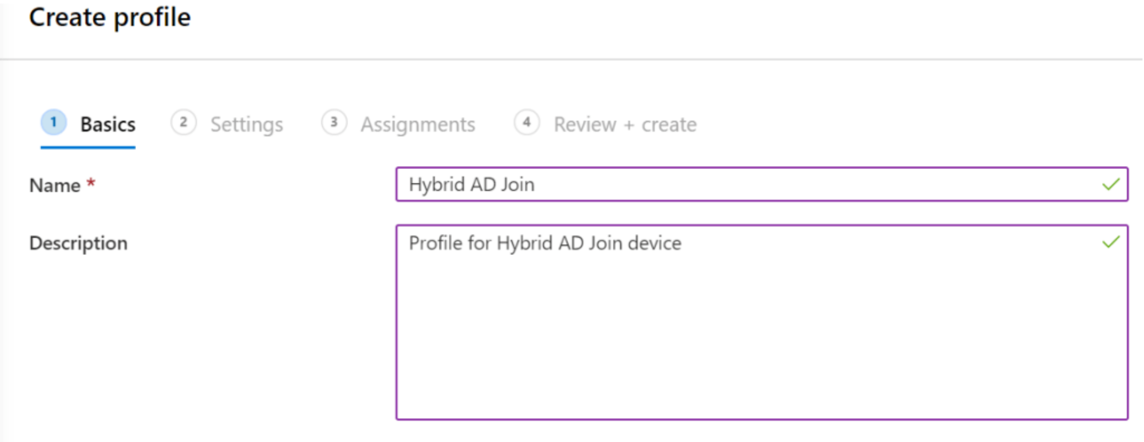
Windows Enrollment

+ Create

The enrollment status page appears during initial device setup and during first user sign in. If enabled, users can see the configuration progress of assigned apps and profiles targeted to their device. Learn more

Priority	Name	Assigned
1	Autopilot	Yes
Default	All users and all devices	Yes

Enter the name and click on **Next**.



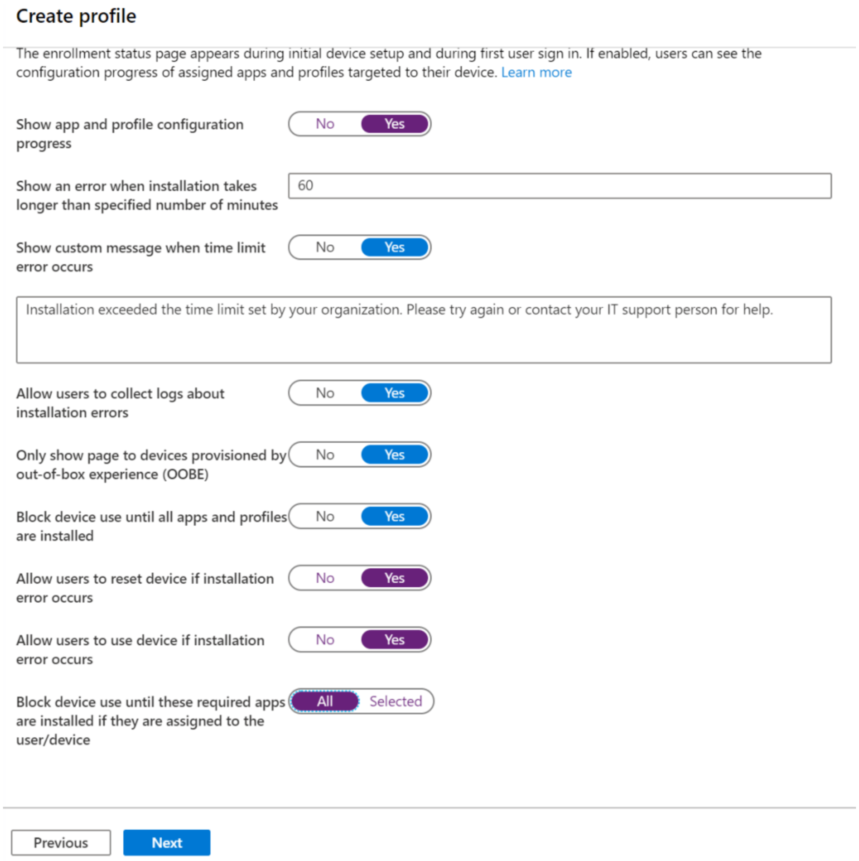
Create profile

1 Basics 2 Settings 3 Assignments 4 Review + create

Name * : Hybrid AD Join ✓

Description: Profile for Hybrid AD Join device ✓

Configure **Settings** as needed.



Create profile

The enrollment status page appears during initial device setup and during first user sign in. If enabled, users can see the configuration progress of assigned apps and profiles targeted to their device. Learn more

Show app and profile configuration progress: No [✓ Yes]

Show an error when installation takes longer than specified number of minutes: 60

Show custom message when time limit error occurs: No [✓ Yes]

Installation exceeded the time limit set by your organization. Please try again or contact your IT support person for help.

Allow users to collect logs about installation errors: No [✓ Yes]

Only show page to devices provisioned by out-of-box experience (OOBE): No [✓ Yes]

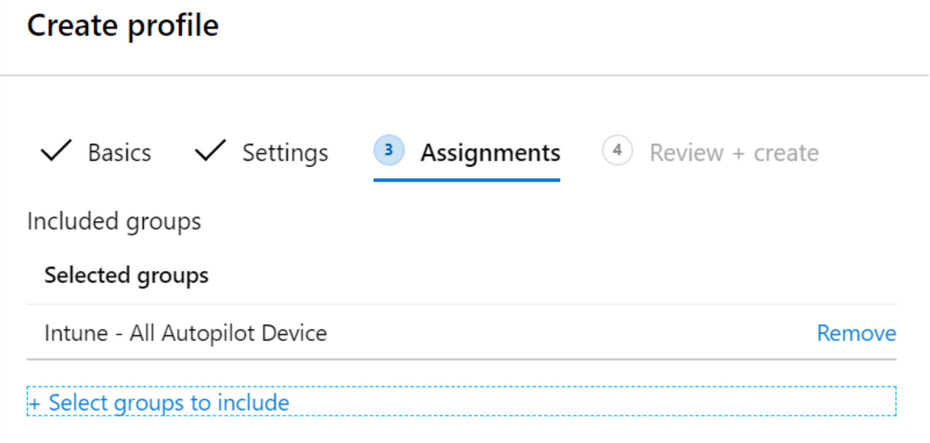
Block device use until all apps and profiles are installed: No [✓ Yes]

Allow users to reset device if installation error occurs: No [✓ Yes]

Allow users to use device if installation error occurs: No [✓ Yes]

Block device use until these required apps are installed if they are assigned to the user/device: [✓ All] Selected

Assign the profile to the dynamic group created previously.



Create profile

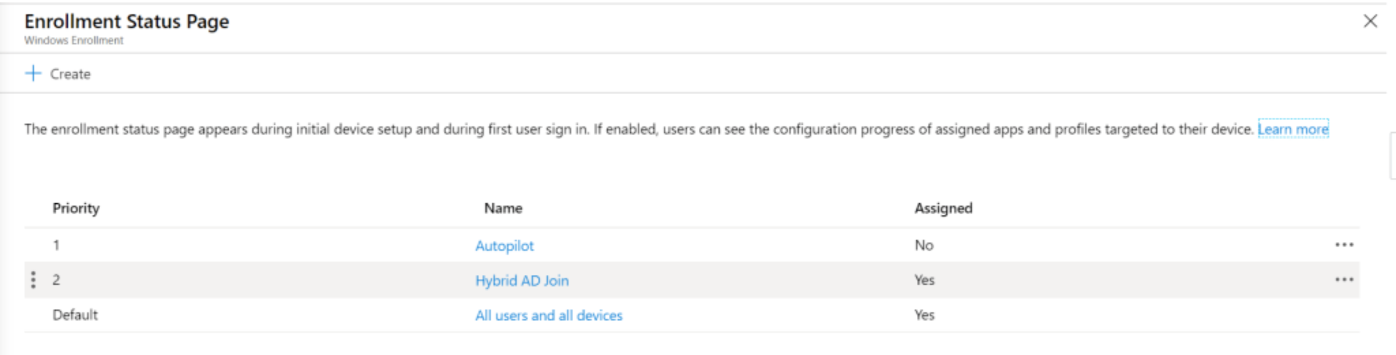
✓ Basics ✓ Settings ③ Assignments ④ Review + create

Included groups

Selected groups	
Intune - All Autopilot Device	Remove

+ Select groups to include

Click on **Next** then on **Create**. The profile has been created.



Enrollment Status Page

Windows Enrollment

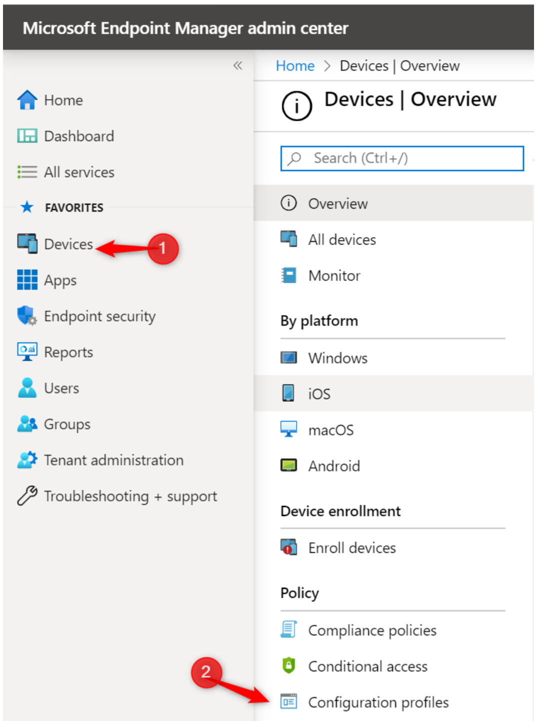
+ Create

The enrollment status page appears during initial device setup and during first user sign in. If enabled, users can see the configuration progress of assigned apps and profiles targeted to their device. Learn more

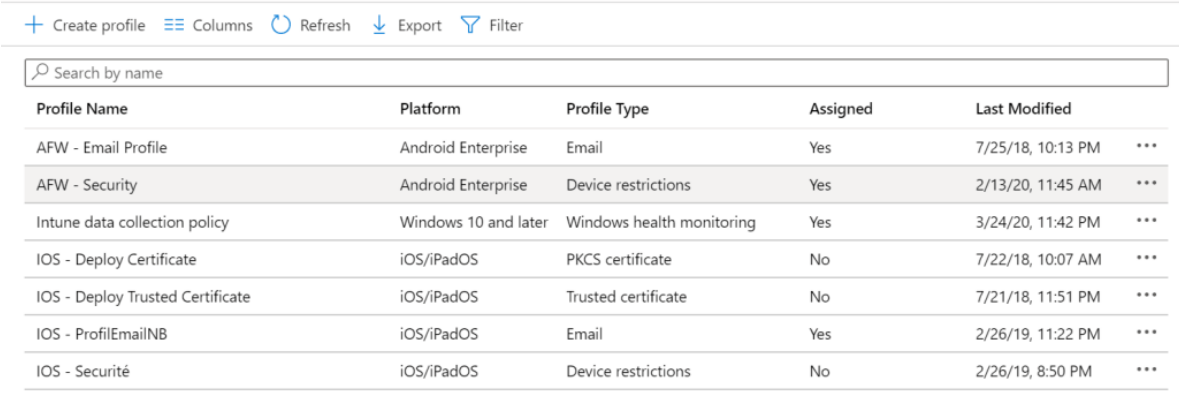
Priority	Name	Assigned
1	Autopilot	No
2	Hybrid AD Join	Yes
Default	All users and all devices	Yes

1.8 Create Domain Join profile

From the intune portal, click on **Devices** the on **Configuration Profiles**.

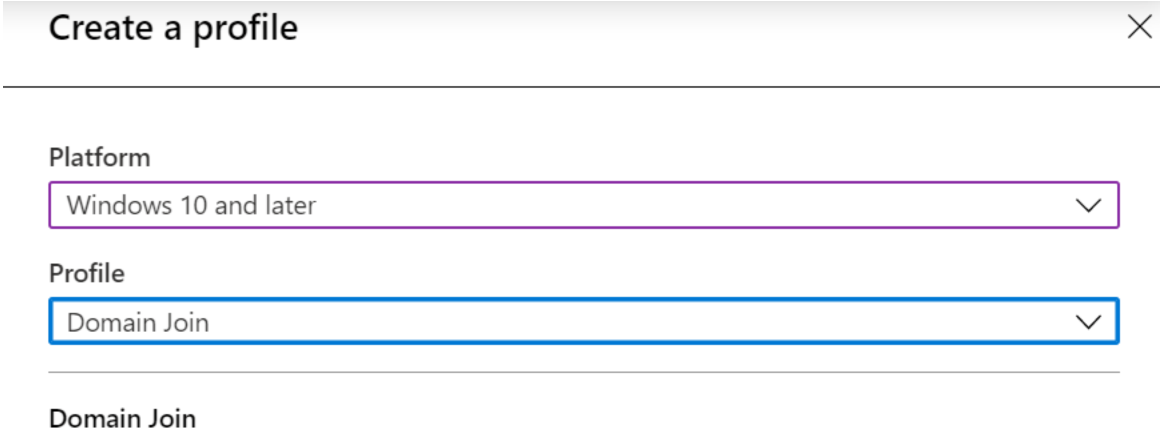


Click on **Create profile** for create new policy.



Profile Name	Platform	Profile Type	Assigned	Last Modified	
AFW - Email Profile	Android Enterprise	Email	Yes	7/25/18, 10:13 PM	···
AFW - Security	Android Enterprise	Device restrictions	Yes	2/13/20, 11:45 AM	···
Intune data collection policy	Windows 10 and later	Windows health monitoring	Yes	3/24/20, 11:42 PM	···
IOS - Deploy Certificate	iOS/iPadOS	PKCS certificate	No	7/22/18, 10:07 AM	···
IOS - Deploy Trusted Certificate	iOS/iPadOS	Trusted certificate	No	7/21/18, 11:51 PM	···
IOS - ProfilEmailNB	iOS/iPadOS	Email	Yes	2/26/19, 11:22 PM	···
IOS - Securité	iOS/iPadOS	Device restrictions	No	2/26/19, 8:50 PM	···

Select **Windows 10 and later** on **Platform** drop-down and **Domain Join** on **Profile** drop-down. Click on **Create**.



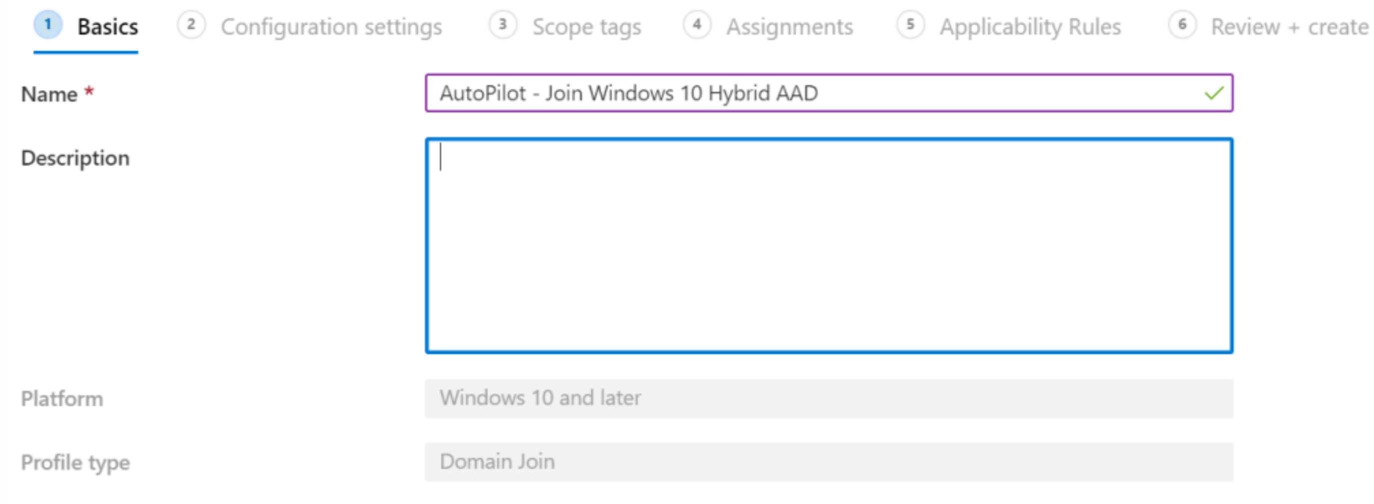
Create a profile

Platform: Windows 10 and later

Profile: Domain Join

Domain Join

Enter the name of the description and click on **Next**.



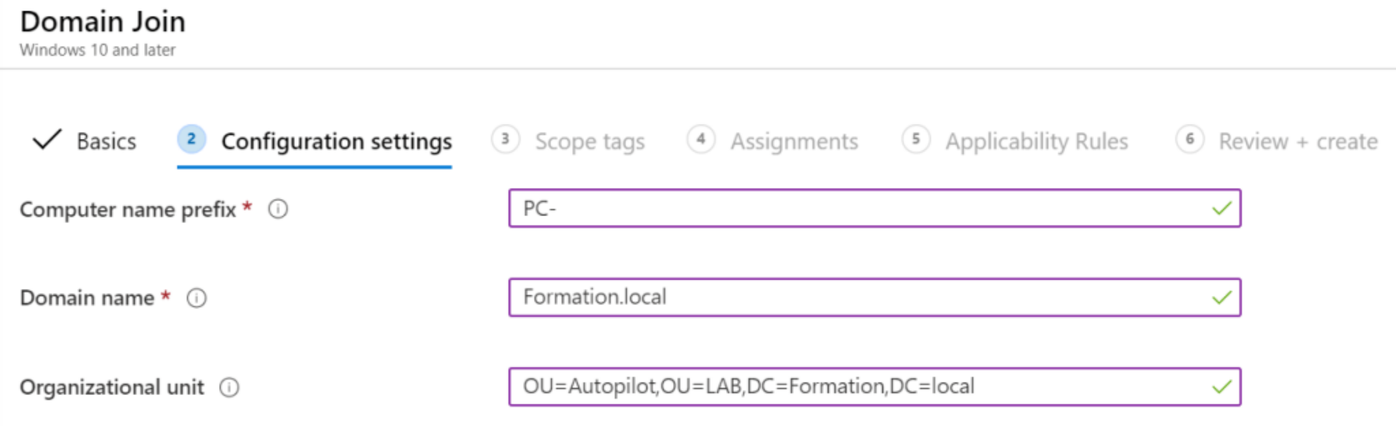
Name *: AutoPilot - Join Windows 10 Hybrid AAD

Description:

Platform: Windows 10 and later

Profile type: Domain Join

Enter the prefix for the computer name and the domain name. For the Organizational Unit, you need enter the value of the **distinguishedName** attribut ldap of the Organizational Unit.



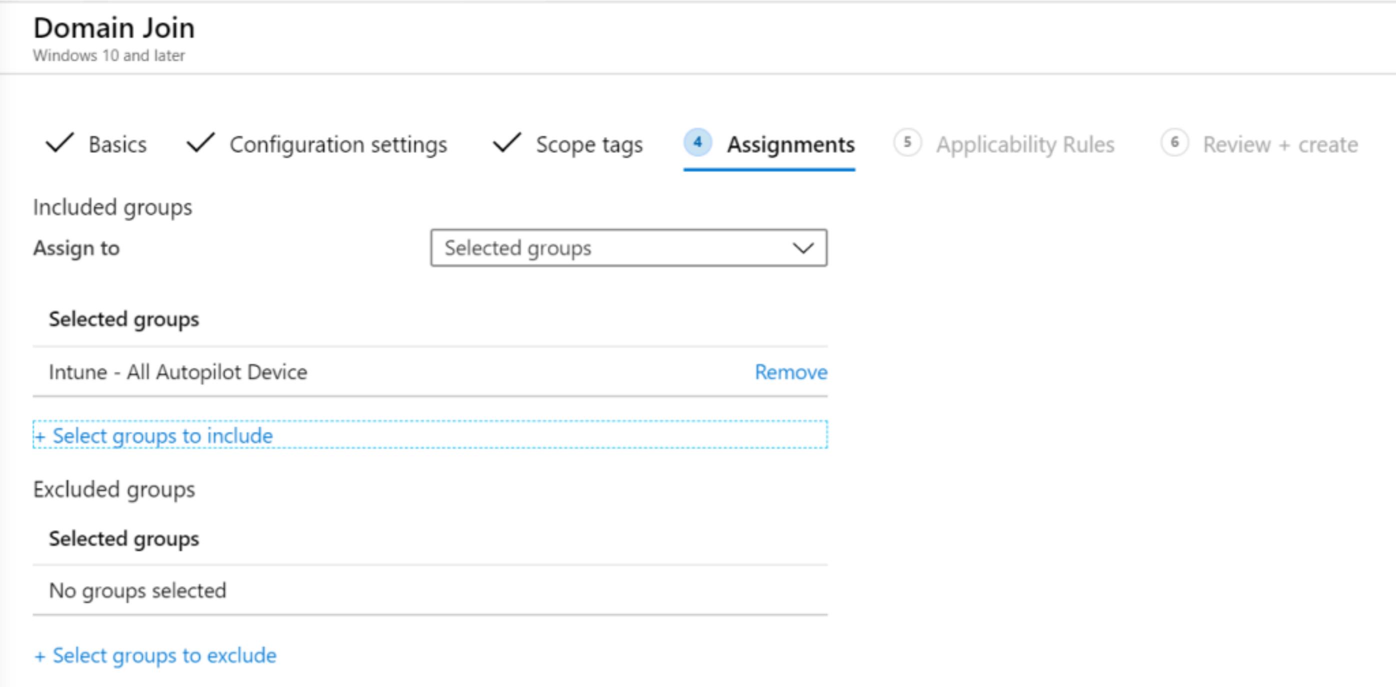
Domain Join
Windows 10 and later

Computer name prefix * : PC-

Domain name * : Formation.local

Organizational unit : OU=Autopilot,OU=LAB,DC=Formation,DC=local

Assign the profile at the previously created group and create profile.



Domain Join
Windows 10 and later

Included groups

Assign to: Selected groups

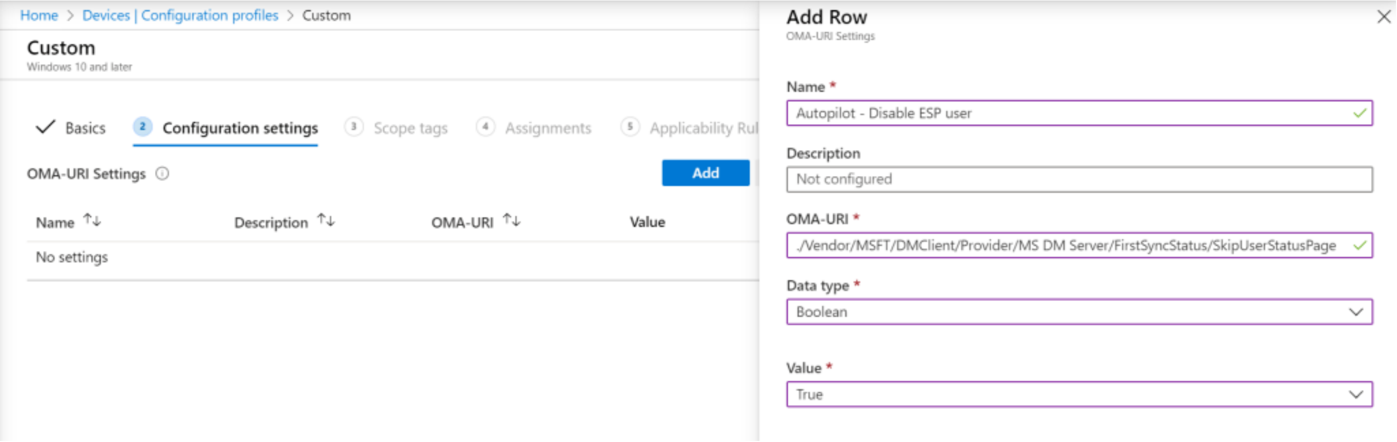
Selected groups	
Intune - All Autopilot Device	Remove

Excluded groups

Selected groups
No groups selected

Repeat the same operation for disable user ESP. If you don’t disable ESP user, a timeout is present on Enrollment Status Page. Use the following information for create the Intune profile.

- **Platform :** Windows 10 and later
- **Profile :** Custom
- **OMA-URI :** ./Vendor/MSFT/DMClient/Provider/MS DM Server/FirstSyncStatus/SkipUserStatusPage
- **Data Type :** Boolean
- **Value :** True



OMA-URI Settings

Name	Description	OMA-URI	Value
No settings			

Add Row

OMA-URI Settings

Name *: Autopilot - Disable ESP user

Description: Not configured

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

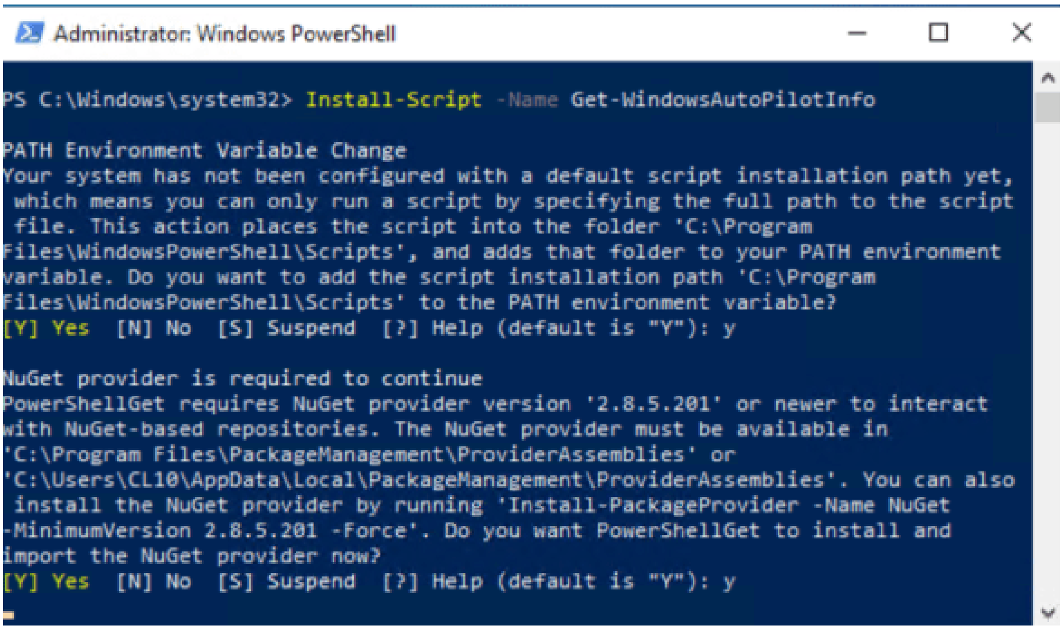
Data type *: Boolean

Value *: True

Assign the profile at the same group that the previously profile and create profile.

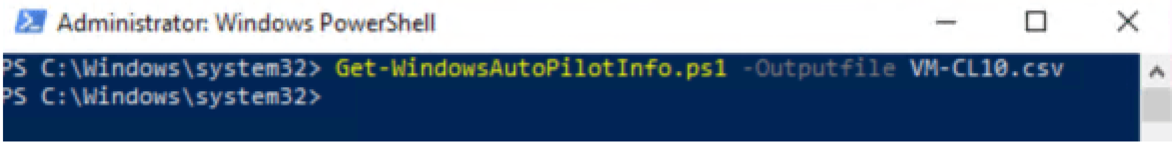
1.9 Add device on Autopilot

I test Autopilot on my virtual machine. So before to use Autopilot, I need add device on autopilot platform. From the Windows 10 device, open a **Windows Powershell prompt** and run the command **Install-Script -Name Get-WindowsAutoPilotInfo**.

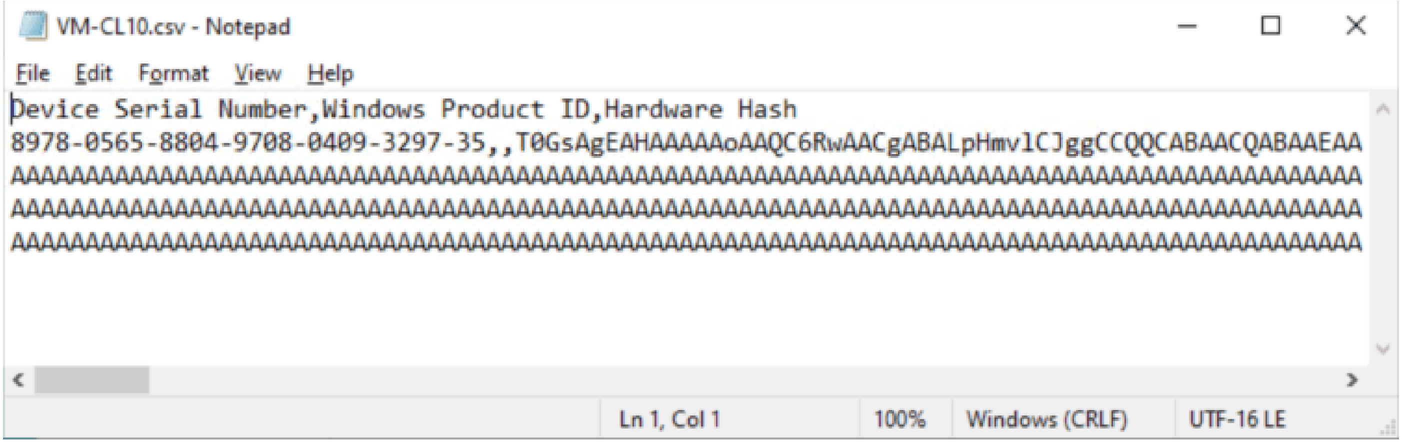


```
PS C:\Windows\system32> Install-Script -Name Get-WindowsAutoPilotInfo

PATH Environment Variable Change
Your system has not been configured with a default script installation path yet,
 which means you can only run a script by specifying the full path to the script
 file. This action places the script into the folder 'C:\Program
Files\WindowsPowerShell\Scripts', and adds that folder to your PATH environment
variable. Do you want to add the script installation path 'C:\Program
Files\WindowsPowerShell\Scripts' to the PATH environment variable?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact
with NuGet-based repositories. The NuGet provider must be available in
'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\CL10\AppData\Local\PackageManagement\ProviderAssemblies'. You can also
 install the NuGet provider by running 'Install-PackageProvider -Name NuGet
-MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
```

Create a CSV file with ID of the device. This ID must be added on Autopilot. On the Windows 10 computer, run the command **Get-WindowsAutoPilotInfo.ps1 -Outputfile VM-CL10.csv**.

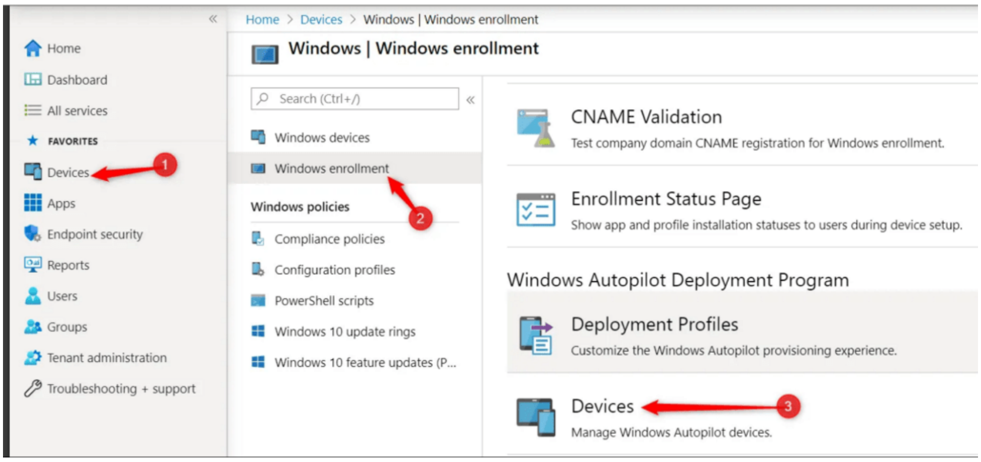


```
PS C:\Windows\system32> Get-WindowsAutoPilotInfo.ps1 -Outputfile VM-CL10.csv
PS C:\Windows\system32>
```



```
Device Serial Number,Windows Product ID,Hardware Hash
8978-0565-8804-9708-0409-3297-35,,T0GsAgEAHAAAAAoAAQC6RwAACgABALpHmv1CJggCCQQCABAACQABAAEAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

From the Intune portal, click on **Devices**, **Windows Enrollment** and **Devices**.



CNAME Validation
Test company domain CNAME registration for Windows enrollment.

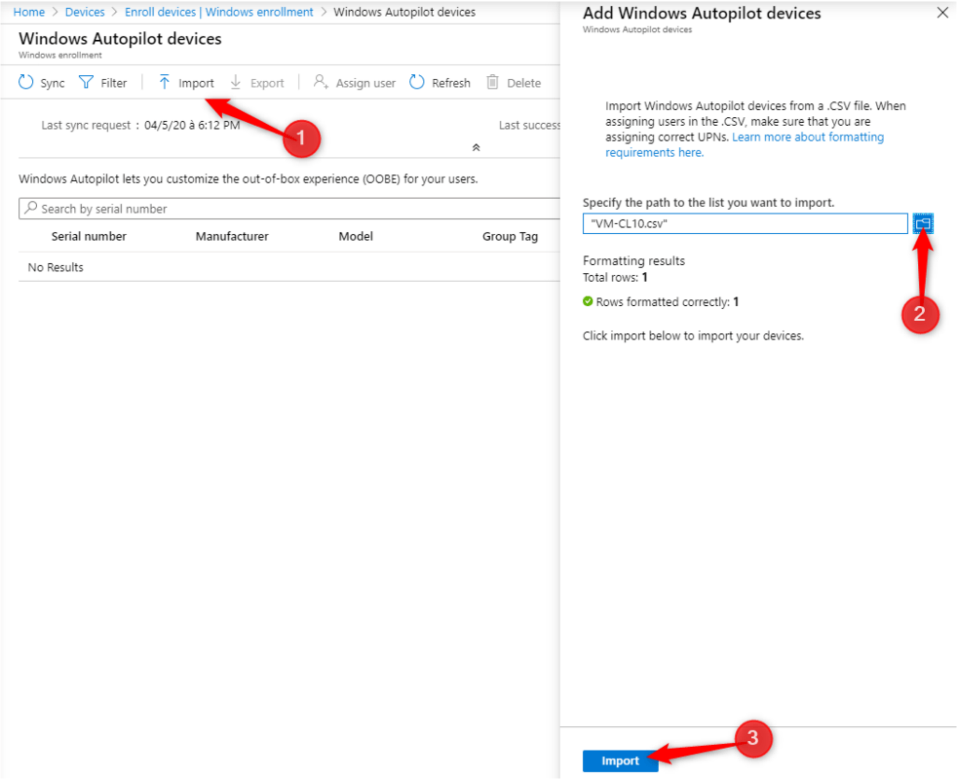
Enrollment Status Page
Show app and profile installation statuses to users during device setup.

Windows Autopilot Deployment Program

Deployment Profiles
Customize the Windows Autopilot provisioning experience.

Devices
Manage Windows Autopilot devices.

Cliquez on **Import** and select the CSV file previously created. Click on **Import** for import file.


Home > Devices > Enroll devices | Windows enrollment > Windows Autopilot devices
Windows Autopilot devices
Windows enrollment
Sync
Filter
Import
Export
Assign user
Refresh
Delete
1
Last success
Search by serial number
Add Windows Autopilot devices
Windows Autopilot devices
2
Import
3

Last sync request : 04/5/20 à 6:12 PM

Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.

Serial number	Manufacturer	Model	Group Tag
No Results			

Import Windows Autopilot devices from a .CSV file. When assigning users in the .CSV, make sure that you are assigning correct UPNs. Learn more about formatting requirements here.

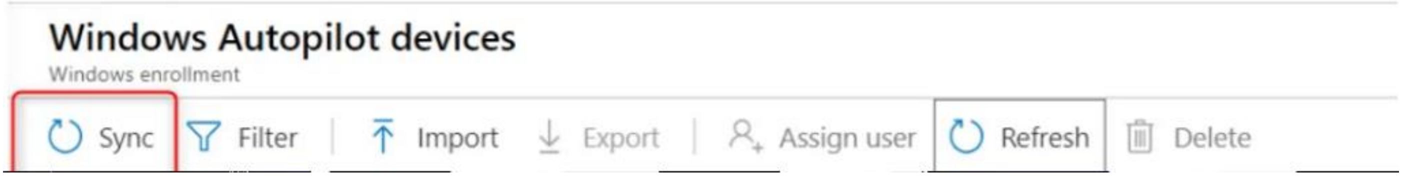
Specify the path to the list you want to import.
"VM-CL10.csv"

Formatting results
Total rows: **1**

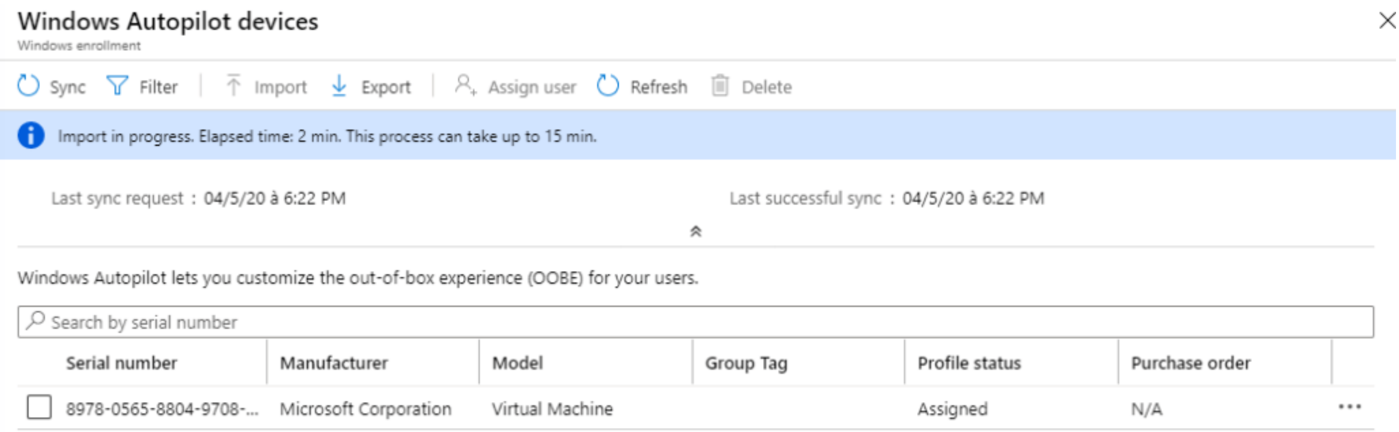
Rows formatted correctly: **1**

Click import below to import your devices.

Click on **Sync** when import is finished.



Device appear in the Intune portal.



Import in progress. Elapsed time: 2 min. This process can take up to 15 min.

Last sync request : 04/5/20 à 6:22 PM

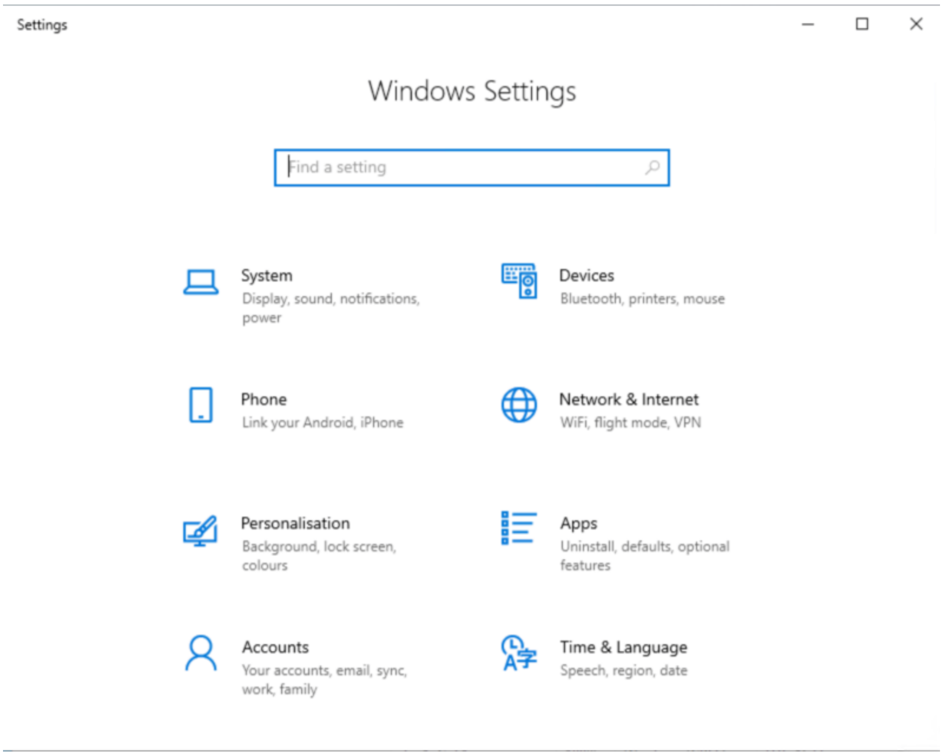
Last successful sync : 04/5/20 à 6:22 PM

Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.

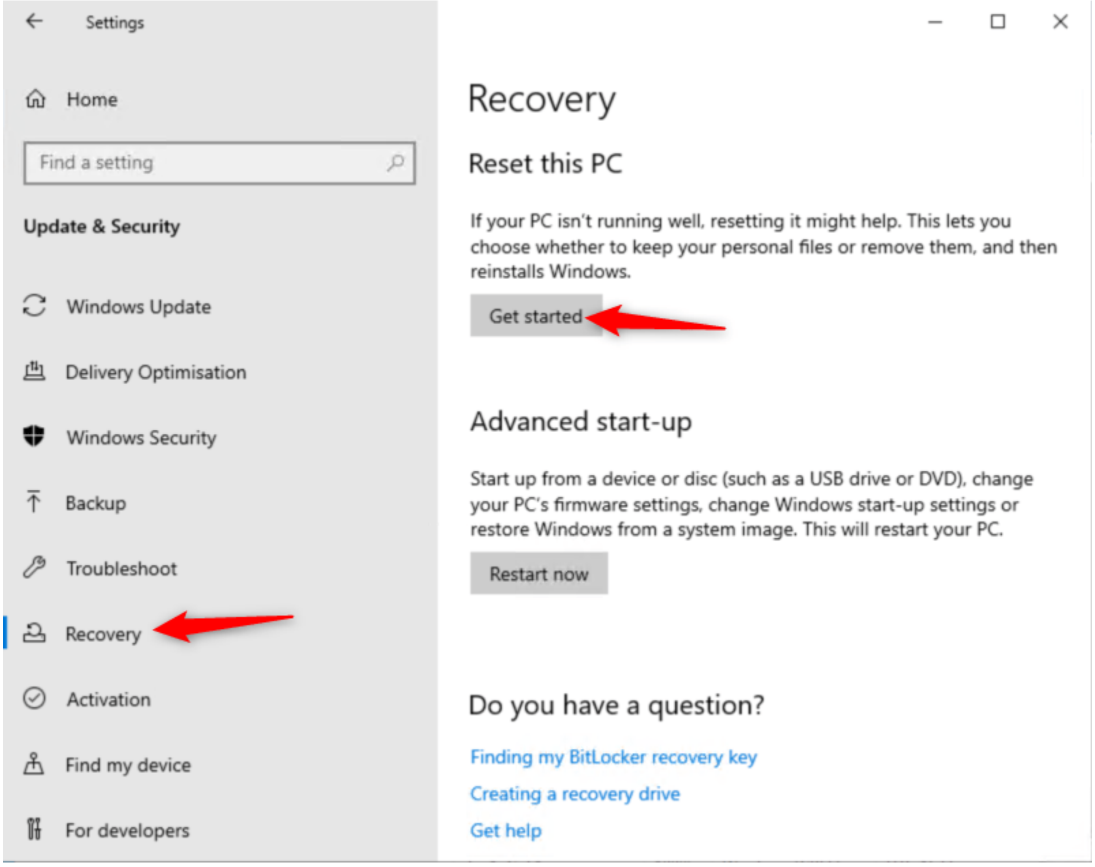
Search by serial number

	Serial number	Manufacturer	Model	Group Tag	Profile status	Purchase order	
□	8978-0565-8804-9708-...	Microsoft Corporation	Virtual Machine		Assigned	N/A	•••

Device appear in the Intune portal. You can reset the computer and use the professionnal account for enroll device on Microsoft intune. From the Windows 10 computer, open Windows Settings and click on Update & Security.


Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
WiFi, flight mode, VPN
Personalisation
Background, lock screen, colours
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date

Click on **Recovery** then on **Get Started**.



Recovery

Reset this PC

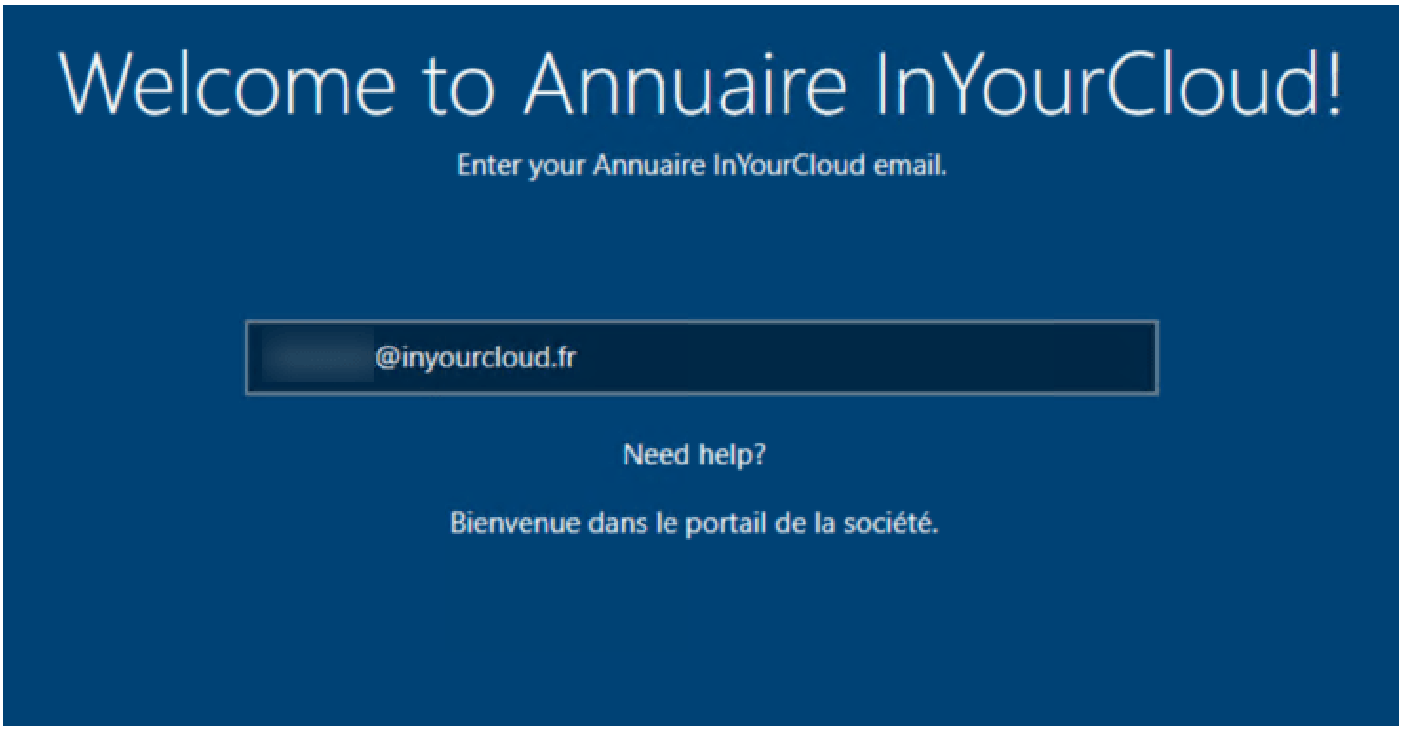
If your PC isn't running well, resetting it might help. This lets you choose whether to keep your personal files or remove them, and then reinstalls Windows.

Advanced start-up

Start up from a device or disc (such as a USB drive or DVD), change your PC's firmware settings, change Windows start-up settings or restore Windows from a system image. This will restart your PC.

Do you have a question?

Click on **Remove everything** for remove all files, apps, etc. Click on **Next** then on **Reset** to launch reset. Enter the username of your account and click on **Next**.



Welcome to Annuaire InYourCloud!

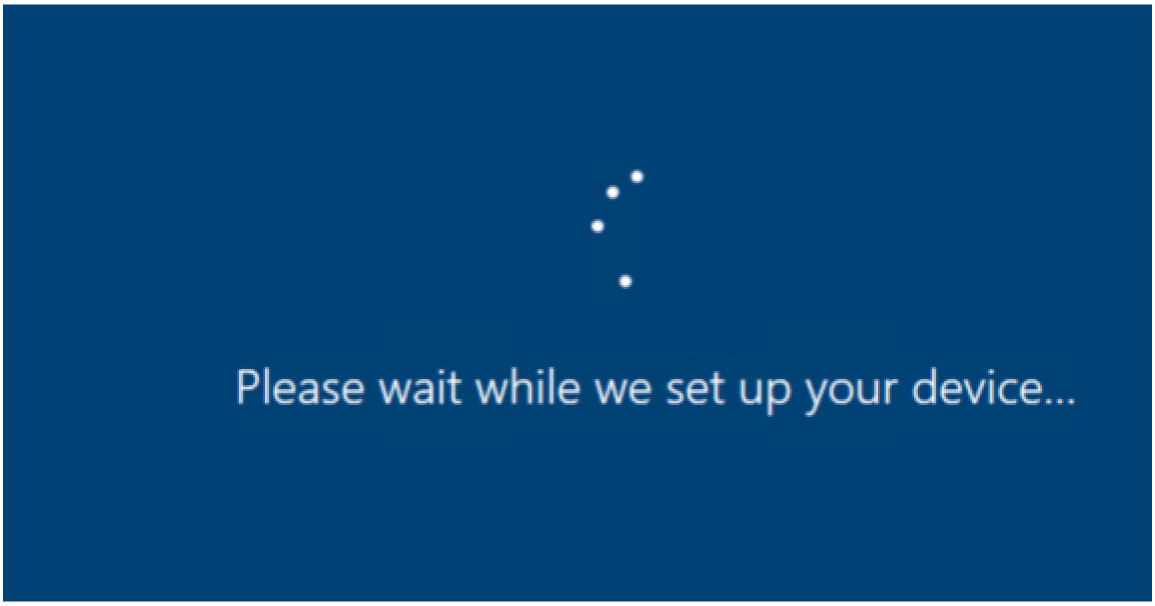
Enter your Annuaire InYourCloud email.

[redacted]@inyourcloud.fr

Need help?

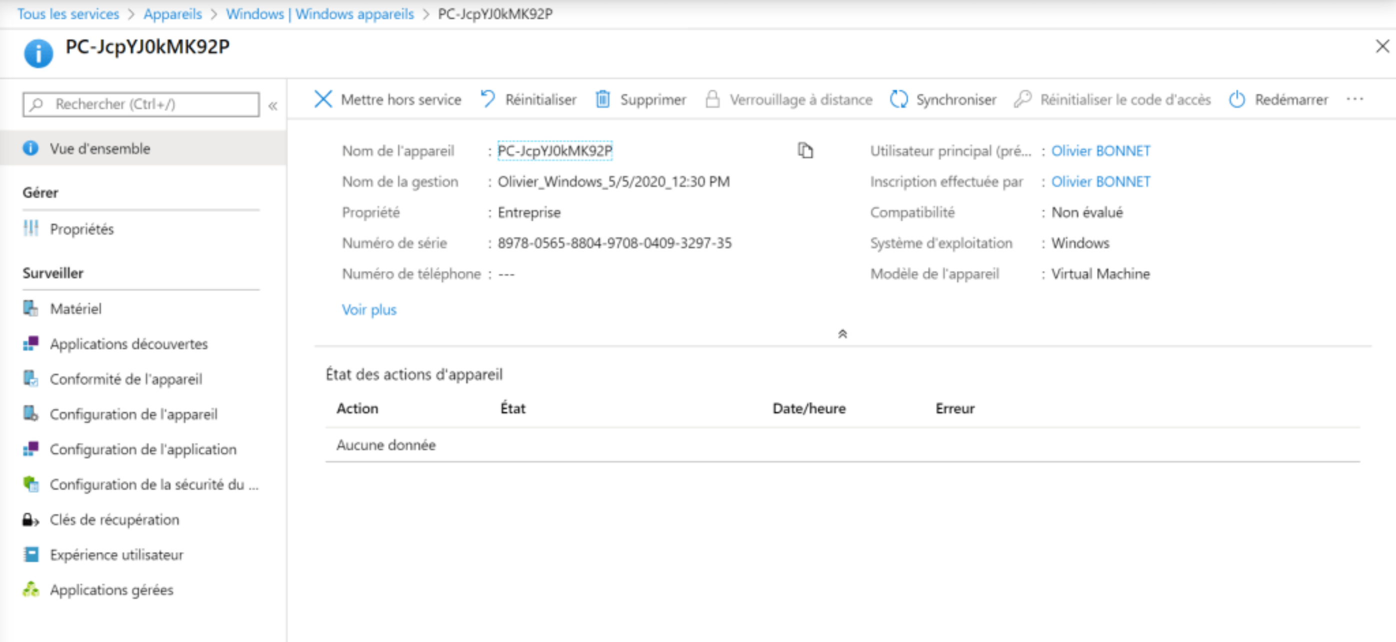
Bienvenue dans le portail de la société.

Set up is on progress



Please wait while we set up your device...

The computer account is added to Microsoft Intune



Tous les services > Appareils > Windows | Windows appareils > PC-JcpYJ0kMK92P

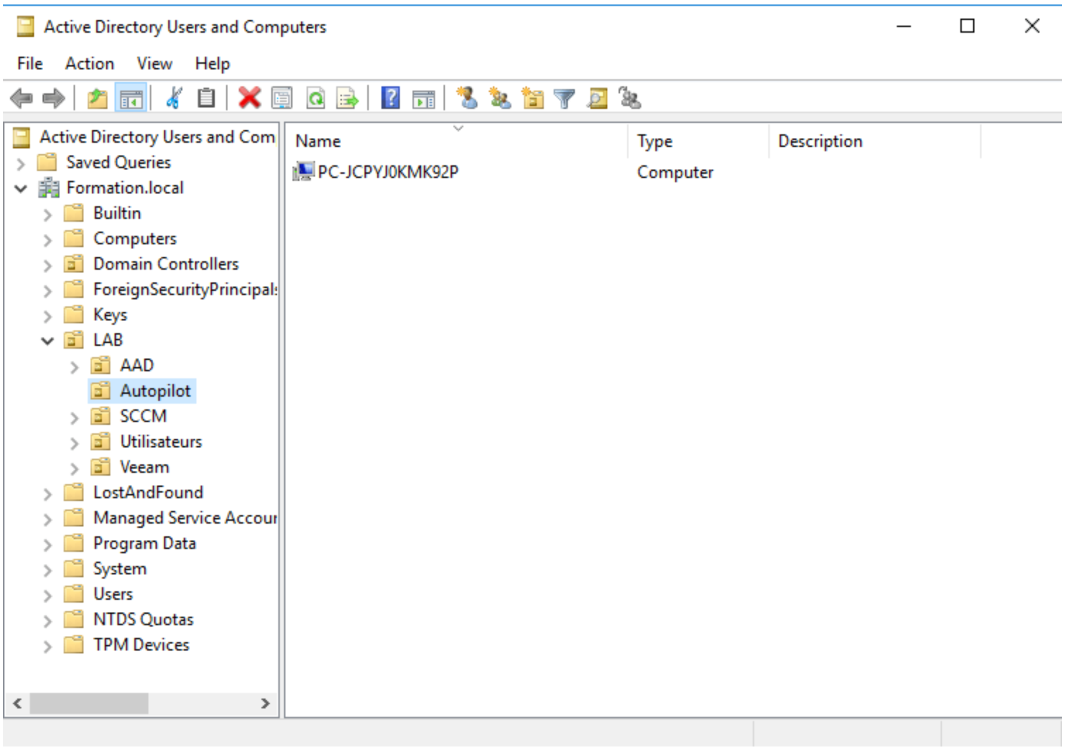
PC-JcpYJ0kMK92P

Nom de l'appareil	: PC-JcpYJ0kMK92P	Utilisateur principal (pré...	: Olivier BONNET
Nom de la gestion	: Olivier_Windows_5/5/2020_12:30 PM	Inscription effectuée par	: Olivier BONNET
Propriété	: Entreprise	Compatibilité	: Non évalué
Numéro de série	: 8978-0565-8804-9708-0409-3297-35	Système d'exploitation	: Windows
Numéro de téléphone	: ---	Modèle de l'appareil	: Virtual Machine

État des actions d'appareil

Action	État	Date/heure	Erreur
Aucune donnée			

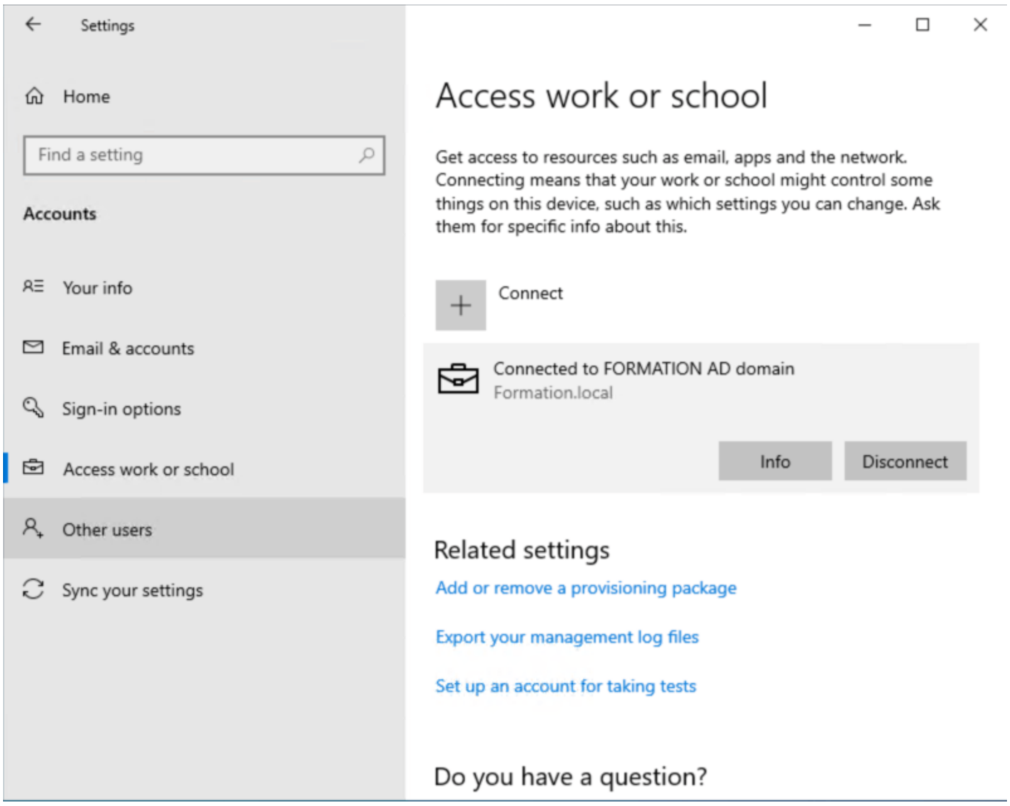
The account is present in Active Directory.



- Active Directory Users and Com
  - Saved Queries
  - Formation.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Keys
    - LAB
      - AAD
      - Autopilot
      - SCCM
      - Utilisateurs
      - Veeam
    - LostAndFound
    - Managed Service Accour
    - Program Data
    - System
    - Users
    - NTDS Quotas
    - TPM Devices

Name	Type	Description
PC-JCPYJ0KMK92P	Computer	

The computer is been join to AD and Azure AD.



Access work or school

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

Connected to FORMATION AD domain
Formation.local

Related settings

Add or remove a provisioning package

Export your management log files

Set up an account for taking tests

Do you have a question?