

# Setting up your device for work

This could take a while and your device may need to reboot.



## Device preparation [Hide details](#)

Working on it...

Securing your hardware (Complete)  
Joining your organization's network (Complete)  
Registering your device for mobile management (Complete)  
Preparing your device for mobile management (Working on it...)



## Device setup

Waiting for previous step to finish



## Account setup

Waiting for previous step to finish

## How to deploy hybrid Azure AD-joined devices by using Intune and Windows Autopilot

OCTOBER 4, 2019 | DAN DJURASOVIC | NO COMMENTS

When deploying new Windows devices, Windows Autopilot leverages the OEM-optimized version of Windows 10 that is preinstalled on the device, saving organizations the effort of having to maintain custom images and drivers for every model of device being used.

Instead of re-imaging the device, your existing Windows 10 installation can be converted into a “ready” state, applying settings and policies and installing apps. After deployment, Windows 10 devices can be managed by **Microsoft Intune**.

This is a perfect tool for small and medium-sized business which do not have SCCM or MDT to automate the deployment of computers in their organization.

Windows **Autopilot** and **Intune** enables you to:

- Automatically join devices to Azure Active Directory (Azure AD) and Active Directory (via Hybrid Azure AD Join) at the same time.
- Auto-enroll devices into Microsoft Intune.
- Install all company applications from Intune Portal.
- Silently encrypt the local drive with BitLocker and store recovery key in Azure AD.
- Enroll Device in Windows Update for Business and keep all Windows 10 workstation updated.
- Apply some of Groups Settings from Intune instead from Local AD

### Software and OS requirements

- Windows 10 v1809 or greater.
- The following editions are supported:
  - Windows 10 Pro
  - Windows 10 Pro Education
  - Windows 10 Pro for Workstations
  - Windows 10 Enterprise
  - Windows 10 Education
  - Windows 10 Enterprise 2019 LTSC

Licensing requirements

One of the following is required:

- Microsoft 365 Business subscriptions
- Microsoft 365 F1 subscriptions
- Microsoft 365 Academic A1, A3, or A5 subscriptions
- **Microsoft 365 Enterprise E3** or E5 subscriptions, which include all Windows 10, Office 365, and EM+S features (Azure AD and Intune).
- Enterprise Mobility + Security E3 or E5 subscriptions, which include all needed Azure AD and Intune features.
- Intune for Education subscriptions, which include all needed Azure AD and Intune features.
- Azure Active Directory Premium P1 or P2 and Microsoft Intune subscriptions (or an alternative MDM service).

Local AD Requirement

AD Connect (the most recent version)

Windows Server 2016 to install Intune Connector

An overview of deployment steps

1. Create **new OU** and new GPO to configure SCP entry in the registry of your devices.
2. Configure Delegation to new OU for computer object which is going to have Azure Intune Connector
3. Reconfigure AD Connect to include new OU in syncing scope
4. Install Intune Connector on windows 201q6 server hosted on-premises.
5. Configure a couple Groups in Azure AD
6. Configure Device Settings to allow users to join devices to Azure AD
7. Configure automatic MDM enrollment
8. Create and assign an Autopilot deployment profile
9. Create and assign a Domain Join profile
10. Load Hardware Hashes from workstation to Azure AD
11. Boot up workstation to start deployment.

Let’s review the steps that this goes through:

1. The workstation boots up and connects to the network.
2. Autopilot profile is downloaded to workstation.
3. Workstation is asking for Azure AD credentials , which are used to **enroll** the device in Intune. The workstation does not join Azure AD.
4. The device enrolls in Intune, using the **“Domain Join”** device configuration profile settings, the device will request an **Offline Domain Join** blob from Intune. Intune passes this request to the **Offline Domain Join connector service** and gets back the blob. That blob is passed back to the client PC.  
The client PC applies the Offline Join Blob blob and then restarts to complete the **Active Directory join process**.
5. The workstation won’t reboot if it can’t find a domain controller.The most common erros on this steps is **“Something went wrong” with error 0x80070774**.
6. After the reboot, the enrollment status page (ESP) will be shown to process the device configuration .
7. Now, the user will be asked to sign in again , but this time using their Active Directory credentials.  
The AD account signs on, goes through the first sign-on experience and then desktop is presented.

Create new OU and new GPO to configure SCP entry in the registry of your devices.

Create new OU where provisioned Computers will be created.

In our case, we created the following OU

**OU=AutoPilot Domain Join,DC=9tech,DC=ca**

For a computer to be able joined in Azure AD, we will need to configure SCP entry settings using the following GPO

Create a Computer-based GPO with the following names and settings.

| OU                                      | Policy Name          |
|---|----------------------|
| OU=AutoPilot Domain Join,DC=9tech,DC=ca | Hybrid Azure AD join |

## Configure client-side registry setting for SCP

Use the following example to create a Group Policy Object (GPO) to deploy a registry setting

Create new GPO (**Hybrid Azure AD join**) and locate the following path: **Computer Configuration > Preferences > Windows Settings > Registry**

Right-click on the Registry and select **New > Registry Item**

1. On the **General** tab, configure the following

- Action: **Update**
- Hive: **HKEY\_LOCAL\_MACHINE**
- Key Path: **SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD**
- Value name: **TenantId**
- Value type: **REG\_SZ**
- Value data: The GUID or **Directory ID** of your Azure AD instance (This value can be found in the **Azure portal > Azure Active Directory > Properties > Directory ID**)

Click **OK**

2. Right-click on the Registry and select **New > Registry Item**

1. On the **General** tab, configure the following

- .Action: **Update**
- Hive: **HKEY\_LOCAL\_MACHINE**
- Key Path: **SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD**
- Value name: **TenantName**
- Value type: **REG\_SZ**
- Value data: Your verified **domain name** if you are using federated environment such as AD FS. Your verified **domain name** or your onmicrosoft.com domain name, for example, contoso.onmicrosoft.com if you are using managed environment

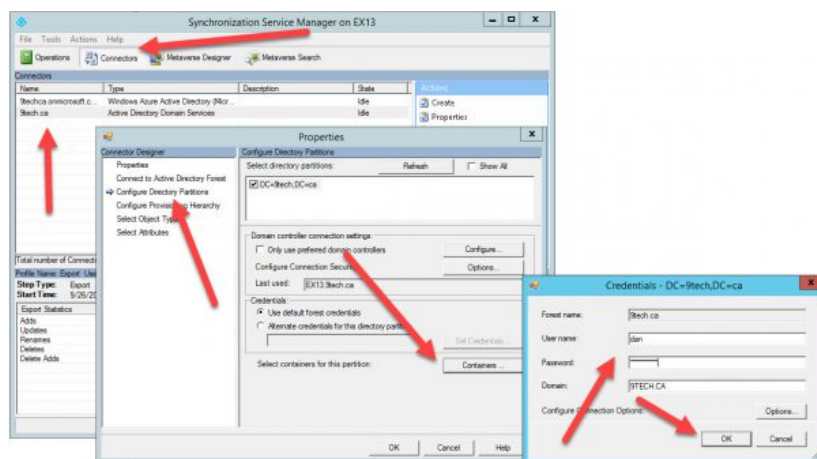
Click **OK**

2. Close the editor for the newly created GPO

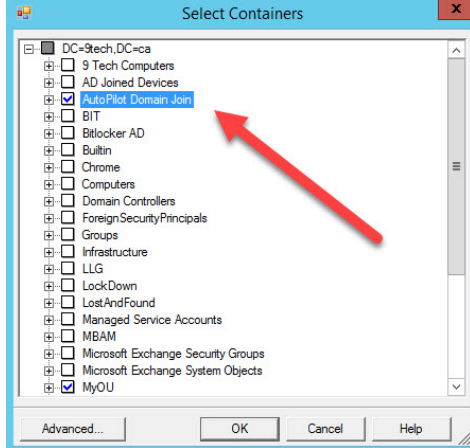
3. Link the newly created GPO (**Hybrid Azure AD join**) to the desired OU (OU=AutoPilot Domain Join,DC=9tech,DC=ca) containing domain-joined computers that belong to your controlled rollout population

Login to **AD Connect Server** and run **Synchronization Service Manager**

Navigate to containers using the following figure



Select your OU, Save, and Exit



Open Powershell on AD Connect Server and run the following Powershell Command.

```
Start-ADSyncSyncCycle -PolicyType initial
```

We need to run this command each time we make modification in OU Scope

You can run this script on AD Connect server during deployment to speed up domain join operation to Azure AD.

Script will run sync process every 300 sec.

```
$i=1
for(;$i -le 10;$i++)
{
Start-ADSyncSyncCycle -PolicyType delta
Write-Host $i
start-sleep -seconds 300
}
```

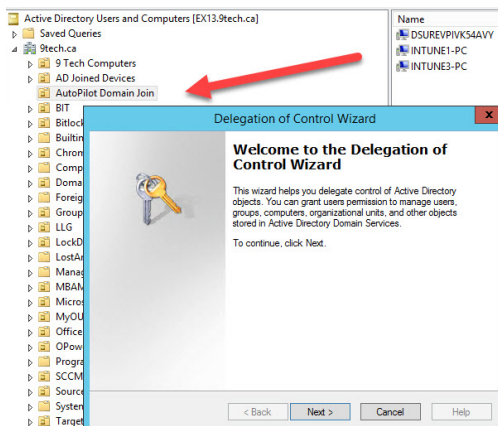
## Configure Delegation to new OU for computer object which is going to have Azure Intune Connector

The Intune Connector for your Active Directory creates autopilot-enrolled computers in the on-premises Active Directory domain.

The computer that hosts the Intune Connector must have the rights to create the computer objects within the domain.

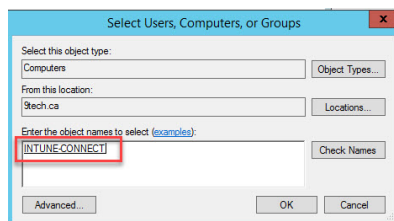
Open Active Directory Users and Computers (DSA.msc).

Right-click the organizational unit that you'll use to create hybrid Azure AD-joined computers, and then select Delegate Control.



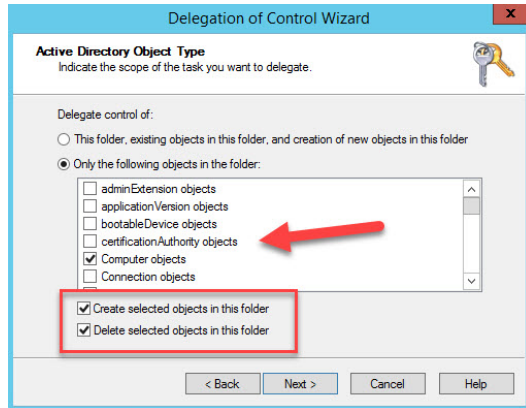
In the Delegation of Control wizard, select Next > Add > Object Types. In the Object Types pane, select the Computers check box, and then select OK.

In the Select Users, Computers, or Groups pane, in the Enter the object names to select box, enter the name of the computer where the Connector is installed.



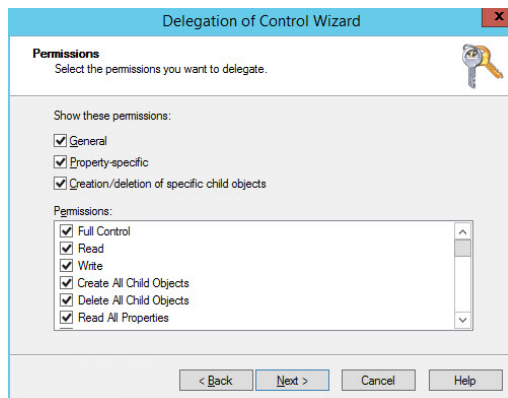
Select **Create a custom task to delegate** >

Next. Select the Only the following objects in the folder checkbox, and then select the **Computer objects**, **Create selected objects** in this folder, and **Delete selected objects** in this folder checkboxes.



Under Permissions, select the Full Control checkbox.

This action selects all the other options.



Select Next, and then select Finish.

## Install the Intune Connector

The Intune Connector for Active Directory must be installed on a computer that's running Windows Server 2016 or later. The computer must also have access to the internet and your Active Directory.

1. In Intune, select **Device enrollment** > **Windows enrollment** > **Intune Connector for Active Directory (Preview)** > **Add connector**.
2. Follow the instructions to download the Connector.
3. Open the downloaded Connector setup file, **ODJConnectorBootstrapper.exe**, to install the Connector.
4. At the end of the setup, select Configure.
5. Select Sign In
6. Enter the user Global Administrator or Intune Administrator role credentials.
7. The user account must have an assigned Intune license.

8. Go to **Device enrollment > Windows enrollment > Intune Connector for Active Directory (Preview)**, and then confirm that the connection status is Active.

## Create Azure AD Group for AutoPilot Devices

Navigate to **Home>9 Tech>Groups – All groups**

**Group Name**=All Autopilot Devices

**MemberShip Type** = Dynamic

Home > 9 Tech > Groups - All groups > New Group

### New Group

---

\* Group type  
Security

\* Group name ⓘ  
All Autopilot Devices

Group description ⓘ  
All Autopilot Devices

\* Membership type ⓘ  
Dynamic Device

Owners

\* Dynamic device members ⓘ  
Add dynamic query

Go to **Advanced rule box**, do one of the following:

To create a group that includes all your Autopilot devices, enter

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

Home > 9 Tech > Groups - All groups > New Group > Dynamic membership rules

### Dynamic membership rules

Save Discard Got feedback?

Configure 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 |
|--------|----------------|----------|
|        | accountEnabled | All      |

+ Add expression

Rule syntax ⓘ

**Edit rule syntax**

You can create or edit rules directly by editing the syntax builder.

Rule syntax ⓘ  
(device.devicePhysicalIDs -any \_ -contains "[ZTDId]")

OK

## Create Intune Users Group

To limit who can join devices in Intune, create the following group

**Group Name**=Intune Users

**Membership type** = Assigned

**Members** = Add all users which will be using Intune and AutoPilot

## New Group

\* Group type ⓘ  
Security

\* Group name ⓘ  
Intunes Users

Group description ⓘ  
Intunes Users

\* Membership type ⓘ  
Assigned

Owners

Members

## Configure MDM Global Settings

Navigate to

Home\9 Tech – Mobility (MDM and MAM)\Configure

**MDM User scope** = Some= ADD Intune Users (Group created in the previous step )

**MDM User scope** = Some = ADD Intune Users (Group created in the previous step )

Home > 9 Tech - Mobility (MDM and MAM) > Configure

**Configure**  
Microsoft Intune

Save Discard Delete

MDM user scope ⓘ None **Some** All

Groups Select groups Intunes Users >

MDM terms of use URL ⓘ <https://portal.manage.microsoft.com/TermsOfUse.aspx>

MDM discovery URL ⓘ <https://enrollment.manage.microsoft.com/enrollmentserver/disco...>

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

Restore default MDM URLs

MAM User scope ⓘ None **Some** All

Groups Select groups Intunes Users >

MAM Terms of use URL ⓘ

MAM Discovery URL ⓘ <https://wip.mam.manage.microsoft.com/Enroll>

MAM Compliance URL ⓘ

Restore default MAM URLs

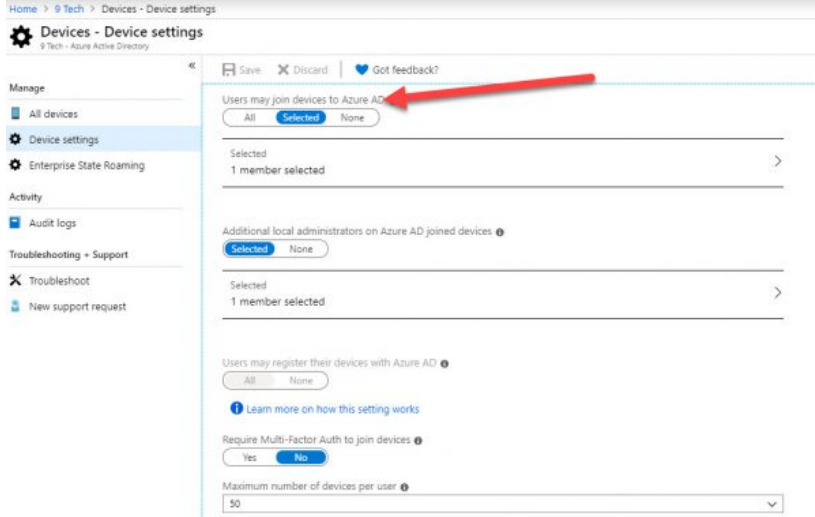
## Configure Device Settings

This setting will allow only members of Intune Users groups to join a workstation to Azure AD

Navigate to

Home\Azure Active Directory\Devices\Device setting

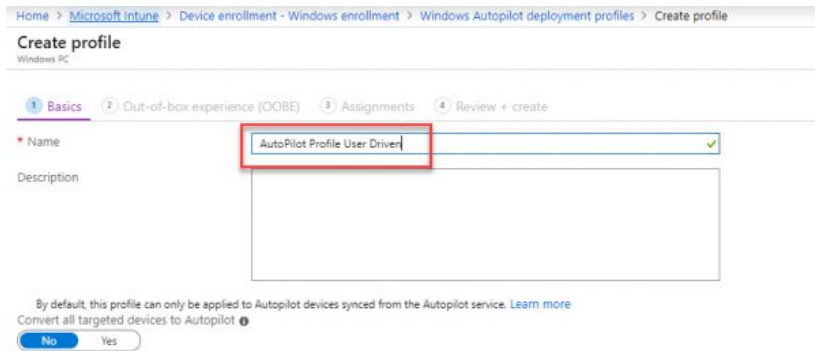
Select the users and groups that are allowed to join devices to Azure AD= Selected = Intune Users



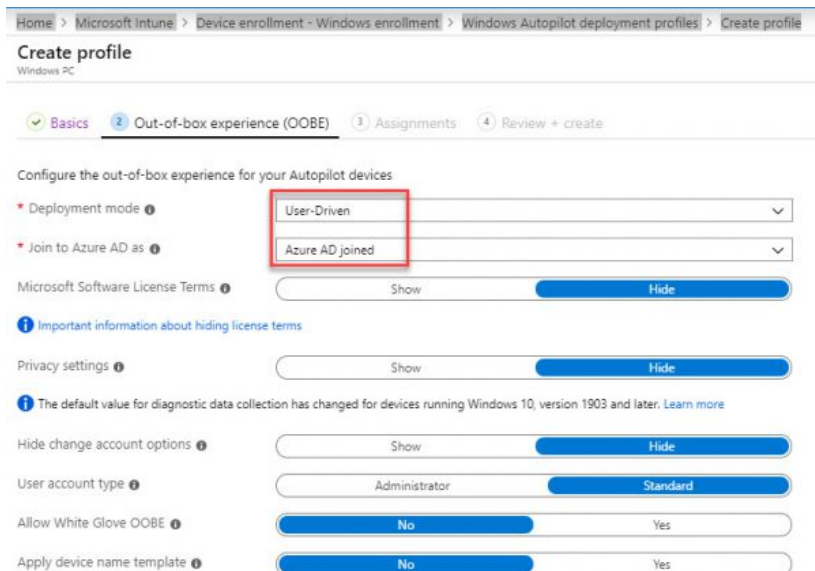
## Create and assign an Autopilot deployment profile

Autopilot deployment profiles are used to configure the Autopilot devices.

- In Intune, select **Device enrollment > Windows enrollment > Deployment Profiles > Create Profile**.
- Type a Name= **AutoPilot Profile User Driven**



- For Deployment mode, select **User-driven**.
- In the Join to Azure AD as box, select **Hybrid Azure AD joined (Preview)**.
- Do not select Out-of-box experience (OOBE) and then select Save.
- Select Create to create the profile.



- In the profile pane, select Assignments.

- Select Select groups.
- In the Select groups pane, select the AutoPilot **All Autopilot Devices** device group, and then click Select.

Home > Microsoft Intune > Device enrollment - Windows enrollment > Windows Autopilot deployment profiles > Create profile

### Create profile

Windows PC

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

Included groups

**SELECTED GROUPS**

All Autopilot Devices Remove

+ Select groups to include

Excluded groups

**SELECTED GROUPS**

No groups selected

+ Select groups to exclude

It takes about 15 minutes for the device profile status to change from Not assigned to Assigning and, finally, to Assigned.

## Turn on the enrollment status page

1. In Intune, select **Device enrollment > Windows enrollment > Enrollment Status Page**.
2. In the **Enrollment Status Page** pane, select Default > Settings.
3. In the Show app and profile installation progress box, select Yes.
4. Configure the other options as needed.
5. Select Save.

Home > Microsoft Intune > Device configuration - Profiles > Create profile > Domain Join

### Create profile

Domain Join

Windows 10 and later

\* Name  
AutoPilot Hybrid Profile ✓

Description  
AutoPilot Hybrid Profile ✓

\* Platform  
Windows 10 and later ✓

\* Profile type  
Domain Join (preview) ✓

Settings  
Configure

Scope (Tags)  
0 scope(s) selected

Applicability Rules  
0 Rule(s) Configured

\* Computer name prefix  
PC ✓

\* Domain name  
9tech.ca ✓

Organizational unit  
OU=AutoPilot Domain Join,DC=9tech,DC=ca ✓

## Create and assign a Domain Join profile

1. In Intune, select **Device configuration > Profiles > Create Profile**.
2. Enter the following properties:
3. **Name:** AutoPilot Hybrid Profile
4. Description: Enter a description for the profile.
5. **Platform:** Select Windows 10 and later.
6. **Profile type:** Select Domain Join (Preview).
7. Select Settings, and then provide a

Computer name prefix = PC

Domain name = 9tech.ca

Organizational unit in DN format **OU=AutoPilot Domain Join,DC=9tech,DC=ca**

Do not experiment with computer prefix putting %serial% variable. It will fail on Offline Domain Join Process.

Home > Microsoft Intune > Device configuration - Profiles > Create profile > Domain Join

Create profile

Name

AutoPilot Hybrid Profile ✓

Description

AutoPilot Hybrid Profile ✓

Platform

Windows 10 and later

Profile type

Domain Join (preview)

Settings

Configure

Scope (Tags)

0 scope(s) selected

Applicability Rules

0 Rule(s) Configured

Domain Join

Windows 10 and later

Computer name prefix

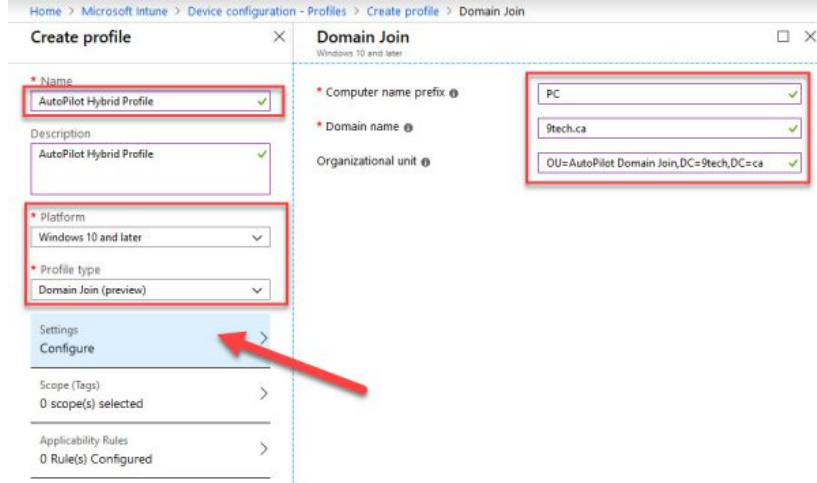
PC ✓

Domain name

9tech.ca ✓

Organizational unit

OU=AutoPilot Domain Join,DC=9tech,DC=ca ✓



Select OK > Create

The profile is created and displayed in the list.

To assign the profile, navigate to **Assignments** and select **AutoPilot User Driven** Group.

Home > Microsoft Intune > Device configuration - Profiles > AutoPilot Hybrid Profile - Assignments

AutoPilot Hybrid Profile - Assignments

Device configuration profile

Search (Ctrl+F)

Save Discard Evaluate

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

Per-setting status

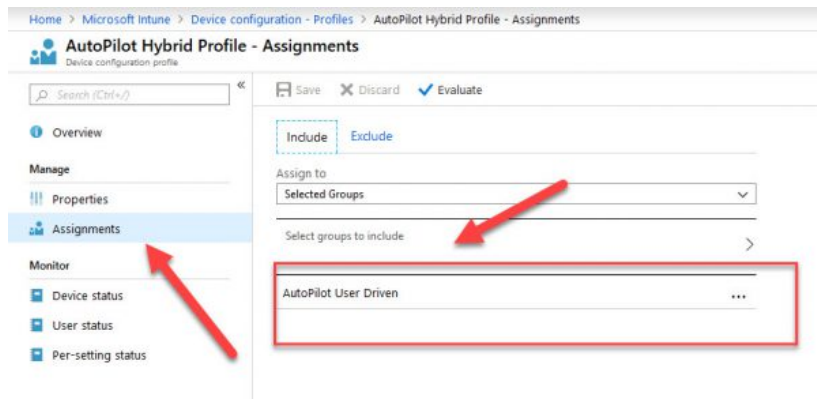
Include Exclude

Assign to

Selected Groups

Select groups to include

AutoPilot User Driven



## Turn on default enrollment status page for all users

To turn on the enrollment status page, follow the steps below.

1. In Intune choose Device enrollment > Windows enrollment > Enrollment Status Page.
2. In the Enrollment Status Page blade, choose Default > Settings.
3. For Show app and profile installation progress, choose Yes.
4. Choose the other settings that you want to turn on and then choose Save.

**All users and all devices - Settings**

Windows Enrollment

Search (Ctrl+J)

Save Discard

**Overview**

Manage

Properties

**Settings**

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress ☒ Yes ☐ No

Show time limit error when installation takes longer than specified number of minutes 60

Show custom message when time limit error occurs ☒ Yes ☐ No

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 ☒ Yes ☐ No

Block device use until all apps and profiles are installed ☒ Yes ☐ No

Allow users to reset device if installation error occurs ☒ Yes ☐ No

Allow users to use device if installation error occurs ☒ Yes ☐ No

Block device use until these required apps are installed if they are assigned to the user/device Selected ☒ All

## Registering Devices

### Register devices from an OEM

If you're buying new devices, some OEMs can register the devices for you.

If you are using existing devices, you will need to pull out a unique hardware ID for the device that needs to be captured and uploaded to the service.

This harvesting process will collect ID from a device running **Windows 10 version 1703** or later installation.

Yes, you will need to install Windows 10 to an old device to get the hardware key.

#### Extract Hardware Hashes from existing devices

I created the following three files which will automate all the processes.

Put all these three files on a USB drive.

#### DisableST.reg

Windows Registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore] "AutoDownload"=dword:00000002

#### Export Key and Sysprep to USB.bat

```
@echo off
color 06
ECHO -----
ECHO Collecting Hardware Key
Powershell.exe -ExecutionPolicy Bypass -File "%~dp0\Get-WindowsAutoPilotInfo.ps1" -OutputFile %~dp0\%computername%.csv
ECHO -----
Echo Hardware Keys has been uploaded to USB DRIVE
reg import "%~dp0\disableST.reg"
ECHO -----
ECHO Microsoft Store updates have been disabled.
```

```
powershell -executionpolicy Bypass -Command "Get-AppxPackage -AllUsers | Remove-AppxPackage"
```

```
ECHO -----  
ECHO All Microsoft Store Applications have been removed.  
ECHO -----  
ECHO Press any key to sysprep computer and shutdown.  
ECHO -----  
pause  
Echo -----  
ECHO Executing SYSPREP...System will go down shortly. DO  
ECHO DO NOT SHUTDOWN SYSTEM  
C:\Windows\System32\Sysprep\Sysprep.exe /generalize /oobe /shutdown /quiet  
  
TIMEOUT 5
```

### Get-WindowsAutoPilotInfo.ps1

Download Get-WindowsAutoPilotInfo.ps1 from the following location

<https://www.powershellgallery.com/packages/Get-WindowsAutoPilotInfo/1.6>

### Run a file to export key

To run process, navigate to a USB drive to **Export Key and Sysprep to USB.bat** file.

Right-click and run file as **Administrator**

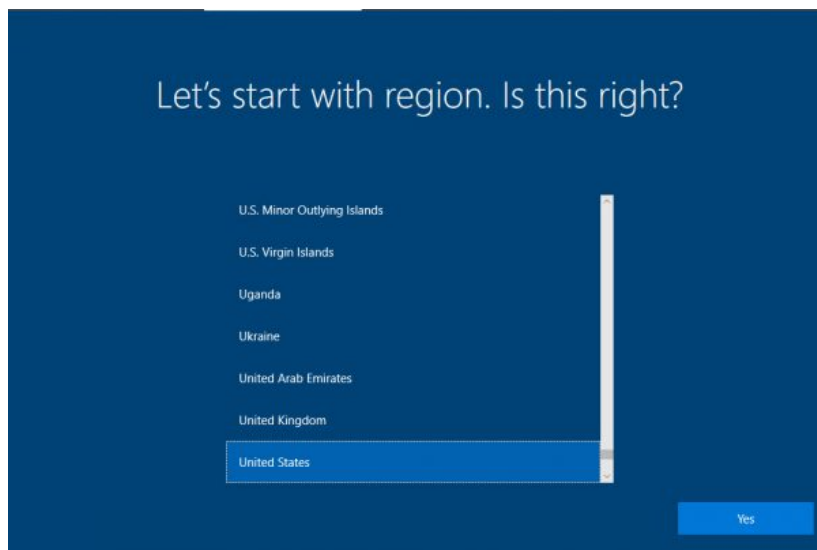
This is what will happen after you run a file.

1. Get-WindowsAutoPilotInfo.ps1 will export hardware ID to a USB drive
2. Microsoft Store updates will be disabled
3. All Microsoft apps will be removed from PC
4. Sysprep will be run and the system will be shut down.

## Deploying Workstation

Boot up workstation.

Pick up region



Pick up Keyboard

# Is this the right keyboard layout?

If you also use another keyboard layout, you can add that next.

US

Canadian Multilingual Standard

English (India)

Irish

Scottish Gaelic

United Kingdom

United States-Dvorak

Yes

Skip keyboard layout

## Want to add a second keyboard layout?



Add layout

Skip

On next screen, you will get customized message welcoming you to your domain

This is a sign that workstation got Auto Pilot Profile from Azure.

Type your Office 365 ID.

## Welcome to 9 Tech!

Enter your 9 Tech email.

intune1@9tech.ca

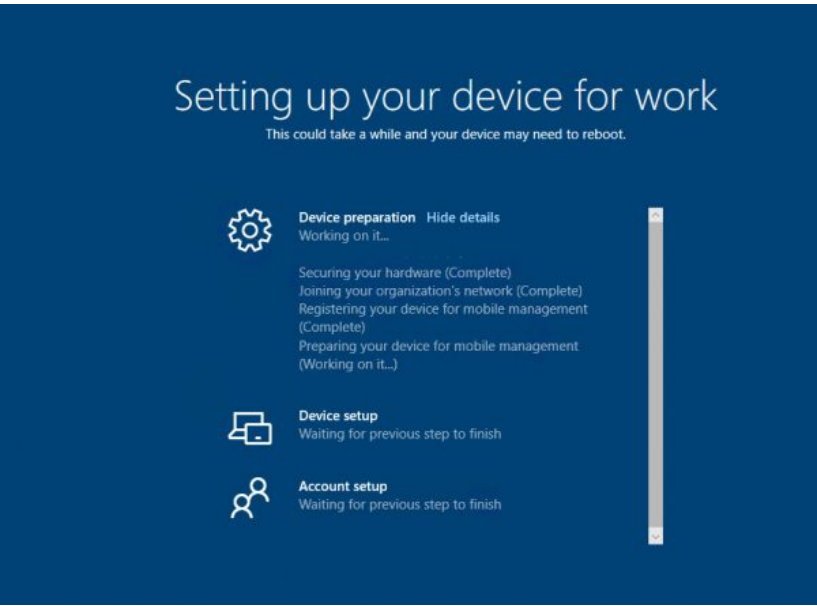
Which account should I use?

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

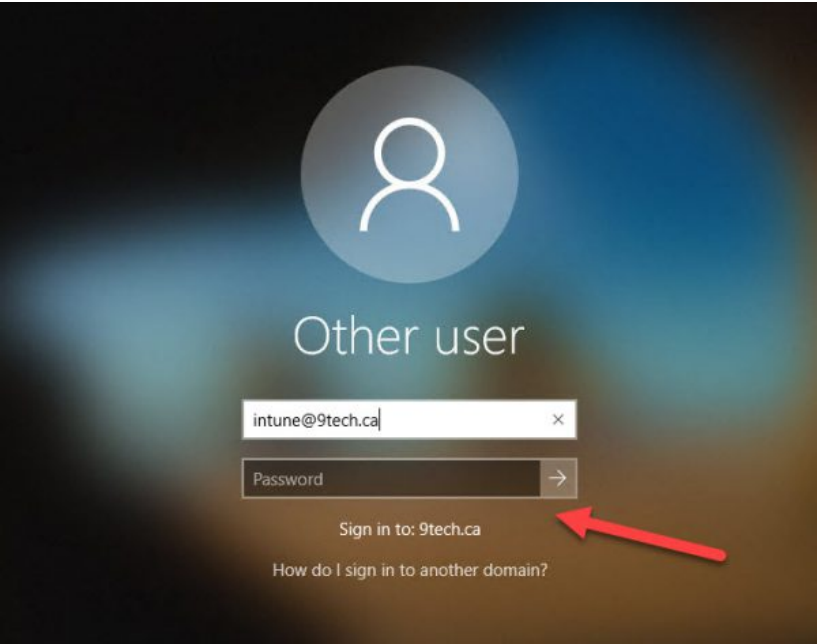
[Change account](#) [Privacy & cookies](#) [Terms of use](#)

Next

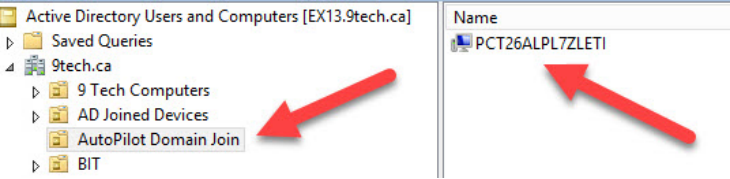
After you authenticate, you will receive **Enrollment page** with status of enrollment.



As you can see , workstation has been joined to **local AD Domain**.



Computer object is created in local AD and AD connect created AD Joined Device in Azure AD



Here is a properties of Device in Azure AD.

| NAME            | ENROLLED | OS      | VERSION       | JOIN TYPE              | OWNER | NAME             | COMPANY | REGISTERED             | ACTIVITY               |
|-----------------|----------|---------|---------------|------------------------|-------|------------------|---------|------------------------|------------------------|
| PCT26ALPL7ZLETI | Yes      | Windows | 1809.15253.33 | Hybrid Azure AD joined | N/A   | Microsoft Intune | Yes     | 10/4/2019, 12:20:17 PM | 10/4/2019, 12:20:17 PM |
| DESKTOP-0000000 | Yes      | Windows |               | Hybrid Azure AD joined | N/A   | None             | N/A     | Pending                | N/A                    |
| PC0022y00000000 | Yes      | Windows |               | Hybrid Azure AD joined | N/A   | None             | N/A     | Pending                | N/A                    |
| INTUNE0000000   | Yes      | Windows |               | Hybrid Azure AD joined | N/A   | None             | N/A     | Pending                | N/A                    |
| DESKTOP-0000000 | Yes      | Windows |               | Hybrid Azure AD joined | N/A   | None             | N/A     | Pending                | N/A                    |

When your Autopilot devices are **registered**, before they're enrolled into Intune, they're displayed in **three places** (with names set to their serial numbers):

1. The Autopilot Devices pane in the Intune in the Azure portal. Select **Device enrollment > Windows enrollment > Devices**.
2. The Azure AD devices pane in the Intune in the Azure portal. Select **Devices > Azure AD Devices**.
3. The Azure AD All Devices pane in **Azure Active Directory in the Azure portal by selecting Devices > All Devices**.

After your Autopilot devices are **enrolled**, they're displayed in four places:

1. The Autopilot Devices pane in the Intune in the Azure portal. Select **Device enrollment > Windows enrollment > Devices**.
2. The Azure AD devices pane in the Intune in the Azure portal. Select **Devices > Azure AD Devices**.
3. The Azure AD All Devices pane in Azure Active Directory in the Azure portal. Select **Devices > All Devices**.
4. The All Devices pane in the Intune in the Azure portal. Select **Devices > All Devices**.

After your Autopilot devices are enrolled, their names become the hostname of the device. By default, the hostname begins with DESKTOP-.

I hope this blog will help you with your depymnet.

/Dan Djurasovic

4 Oct 2019

**in** LinkedIn    E-Mail



#### ABOUT THE AUTHOR

Dan is a Senior IT Consultant with over a dozen years of IT experience, specializing in Microsoft Office 365, Exchange Server Azure IaaS and Active Directory.  
Dan is Currently employed with <https://www.tuor.ca>