

|  |
| --- |
| **Windows Autopilot Cookbook: Surface Edition** |

Windows Autopilot with Surface

Proof of Concept Setup Guide

© 2018 Microsoft. All rights reserved.

Table of Contents

[About this Document 4](#_Toc5059147)

[Windows Autopilot with Surface 4](#_Toc5059148)

[Prerequisites & Setup 5](#_Toc5059149)

[Proof of Concept Prerequisites 5](#_Toc5059150)

[One Time AAD and Intune Configurations 6](#_Toc5059151)

[User Configuration 7](#_Toc5059152)

[Setting up Surface Devices 8](#_Toc5059153)

[Autopilot Configuration 10](#_Toc5059154)

[Network Connectivity Requirements 10](#_Toc5059155)

[Intune 10](#_Toc5059156)

[Intune Device Configuration 18](#_Toc5059157)

[Device Profiles 18](#_Toc5059158)

[Enable the Enrollment Status Page 19](#_Toc5059159)

[Deploy Software – Office ProPlus 20](#_Toc5059160)

[Windows 10 Edition Upgrade 22](#_Toc5059161)

[Assign a User to a Device (Optional) 23](#_Toc5059162)

[End User Experience - Autopilot with Surface (User-Driven) 25](#_Toc5059163)

[Optional: Partner Center registration process 28](#_Toc5059164)

[Requesting a Customer Relationship 28](#_Toc5059165)

[Registering Devices for Windows AutoPilot 29](#_Toc5059166)

[Creating and Managing AutoPilot Profiles 35](#_Toc5059167)

[Applying an AutoPilot Profile to Devices 36](#_Toc5059168)

[How to remove a device from Windows AutoPilot Enrollment 36](#_Toc5059169)

[Microsoft Intune, Azure Active Directory, and Windows AutoPilot 37](#_Toc5059170)

[Managing Devices Not Supported for OEM Enrollment 37](#_Toc5059171)

[Pegging Orders for Windows AutoPilot 37](#_Toc5059172)

[Harvesting Hardware Hashes for Partner Center import 38](#_Toc5059173)

[Resources 40](#_Toc5059174)

[Troubleshooting Autopilot 40](#_Toc5059175)

[Appendix: Additional Capabilities 41](#_Toc5059176)

|  |  |
| --- | --- |
| **Version Notes** | |
| 12032018-1 | Added section called “About this Document”; edited the wording in the Windows Autopilot with Surface section; additional editing to align formatting that impacted the page #’s |
| 11272018-1 | Added info on extracting Device ID from “NEW” Surface devices to simplify guidance |
| 11012018-1 | Initial draft based on Windows 10 1803 |
| 11072018-1 | Added section: Assign a User to a Device (Optional) |
|  |  |

# About this Document

About This Document

This document is a "cookbook" designed to help walk you through the set up and execution of your own Windows Autopilot with Surface Proof of Concept (POC). It contains everything you need for a successful POC and includes step-by-step instructions for each activity along with screen shots.

There is also a companion document called the "***Autopilot for Surface POC Punch List***" to help you apply structure to your project, assign roles and responsibilities and track progress.

# Windows Autopilot with Surface

Traditionally, IT pros spend a lot of time building and customizing images that will later be deployed to devices that already come with a perfectly good OS already installed on them. Windows Autopilot introduces a new zero-touch deployment approach using a collection of technologies to set up and configure Surface devices. This enables an IT department to achieve this with little to no infrastructure to manage and a process that's easy and simple. From the users' perspective, it only takes a few simple steps to get Surface to a productive state. In fact, the only interaction required from the end user is to connect to a network and to verify their credentials.

Everything after that is fully automated.

Windows Autopilot allows you to:

* Automatically join devices to Azure Active Directory (Azure AD)
* Auto-enroll devices into MDM services, such as Microsoft Intune (Requires an Azure AD Premium subscription)
* Restrict the Administrator account creation (Autopilot is the only way to have the first person who logs into Windows enter as a standard user.)
* Create and auto-assign devices to configuration groups based on a device's profile
* Customize OOBE content/branding specific to the organization
* Enable the complete configuration of the device using Microsoft Intune

# Prerequisites & Setup

## Proof of Concept Prerequisites

|  |
| --- |
| **✪** Important |
| You can use your existing Azure Tenant/Intune environment for this Proof of Concept or you can set up an **Office 365 Trial Tenant** (valid for 30 days).  Microsoft 365 E5 30 Day Trial Tenant – <https://go.microsoft.com/fwlink/p/?LinkID=698279> |

For this Surface Modern Management Proof of Concept (POC), you will need to create a Microsoft 365 Enterprise environment in Intune.

|  |  |
| --- | --- |
| Azure Active Directory Premium | Required to enroll your devices in your organization and to automatically enroll devices in your organization’s MDM solution.  *(Users must be allowed to join devices into Azure AD)* |
| Mobile Device Management (MDM) | Required to remotely deploy applications, configure, and manage your enrolled devices. |
| Office 365 Pro Plus (Optional) | Required to if you wish to include Microsoft Office in your deployment to your enrolled devices. |
| Windows RS3 1709 or higher | Surface devices must leave the factory with a minimum version of Windows RS3/1709. Devices manufactured after January 2018 should meet this requirement.  *(Documentation states Windows 10 1703 as minimum version supported but we strongly recommend at least 1709)* |

These requirements are also met by one of the following solutions:

|  |  |
| --- | --- |
| Microsoft 365 E3 or E5 | Includes Azure Active Directory Premium, Microsoft Intune, and Office 365 ProPlus |
| Enterprise Mobility+Security E3 / E5 | Includes Azure Active Directory Premium and Microsoft Intune |
| Office 365 ProPlus E3 or E5 | Includes Office 365 ProPlus |

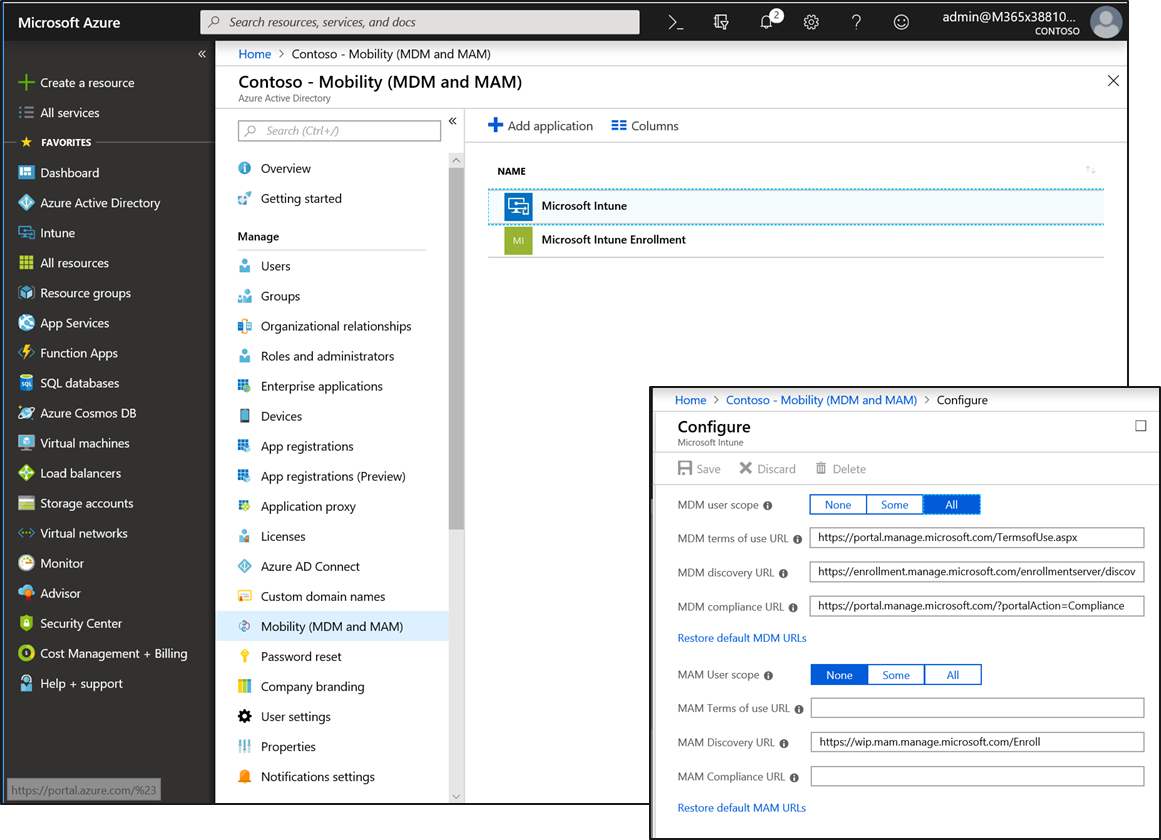
## One Time AAD and Intune Configurations

Before Windows Autopilot can be used, some configuration tasks are required to support the common Autopilot scenarios.

Configure Azure Active Directory

Sign in to <https://portal.azure.com> using the admin credentials provided for the tenant.

* + Configure automatic MDM enrollment.
  + Enable MDM for all POC users – navigate to **Azure Active Directory**>**Mobility (MDM and MAM)** ->> select **Microsoft Intune** and make sure that under **MDM user scope** ALL is selected. Do this for **Microsoft Intune Enrollment** as well.
  + See [https://docs.microsoft.com/en-us/intune/windows-enroll#enable-windows-10-automatic-enrollment](https://docs.microsoft.com/en-us/intune/windows-enroll).



|  |
| --- |
| **✪** Important |
| If both MAM user scope and automatic MDM enrollment (MDM user scope) are enabled for a group, only MAM is enabled. Only MAM is added for users in that group when they workplace join personal device. Devices are not automatically MDM enrolled. |

* + Configure company branding.
    - For your company branding to appear during the OOBE, you'll need to configure it in Azure Active Directory first.
    - To configure these settings. Add your own custom branding by navigating to **Azure Active Directory -> Company branding**. Click **Edit** and make the changes required.
    - See [Add company branding to your directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/customize-branding.)
* [As needed] Adjust the tenant name that will be displayed during OOBE by navigating to **Azure Active Directory -> Properties** and set the **Name** field as needed, then click **Save**.
* Enable [Windows Subscription Activation](https://docs.microsoft.com/windows/deployment/windows-10-enterprise-subscription-activation) if desired, in order to automatically step up from Windows 10 Pro to Windows 10 Enterprise.

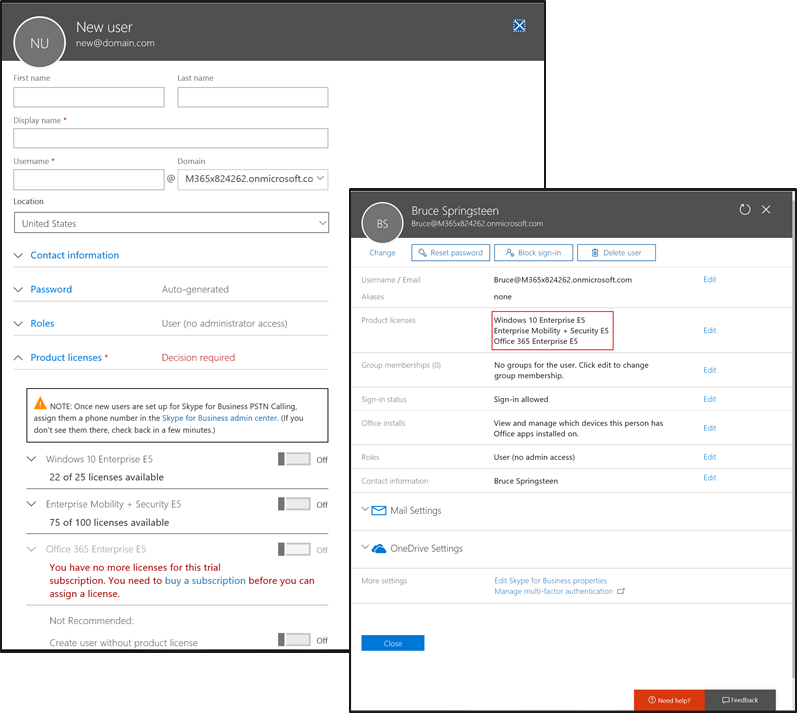
Configure Intune

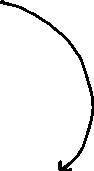
* + [Enable the enrollment status page](#Enrollment) (Windows 10, version 1803 or higher)
  + Ensure users can enroll devices in Intune
  + (Optional) New! Set up enrollment restrictions so only Autopilot-registered devices can enroll

## User Configuration

Assign EMS or Microsoft 365 License to new or existing users. Navigate to [portal.office.com](https://portal.office.com/) and go to the **Admin Center**.

* Click **Add a user** to add a new user and configure. Add details as you wish.
* Click **Edit a user to edit an existing** user’s details.
* Make sure you assign the following licenses to the user.





## Setting up Surface Devices

Once the environment has been created, the following one-time configuration steps need to be performed:

|  |
| --- |
| **✪** Important |
| 1. For purposes of this POC, it is strongly recommended you use Surface devices that were **manufactured with Windows 10 1709 or higher**. This will ensure that you will be able to add them to the Autopilot service directly from Intune. If you are unsure of the version or are using devices manufactured with 1703 or lower engage your partner or Microsoft resource to assist. |
| 1. Following these steps will **erase all data** on the device. Ensure proper backup of all data prior to resetting the device. |

* To demonstrate the client-side experience of Windows Autopilot, a device is needed. Windows 10 Pro, Enterprise, or Education SKUs can be used. Windows 10 Home does not support Autopilot.
* Before the Surface device can be deployed using Windows Autopilot, you must gather the hardware information from the device.

New Surface Devices

* For purposes of the POC, you will need to manually upload Device ID information into Autopilot. In a production environment, this step will be automatically performed as part of the ordering process via a partner.
* To accomplish this manually, you need to generate a CSV file containing the hardware ID’s of the POC Surface devices. Note: Do not open the CSV file in Excel as reformatting of the information can occur and corrupt the file. Instead use Notepad to open the CSV. Once you have a CSV file with the device details, you will be able to add the devices into the Autopilot Deployment Service via Intune.
* To simplify this step, simply send a list of the POC device serial numbers to the Microsoft Surface Global Black Belt you are working with. He/she will be able to generate a CSV file that you can upload for the POC.

Existing Surface Devices

* If the existing machine has a functional and qualified operating system on it, it can be prepared for POC use by resetting the device back to OOBE (out of box experience) by following these steps:
* Fully update the device using Windows Update. Reboot the device. To take advantage of all the latest Autopilot features, updating the device to the latest version of Windows 10 is recommended.
* Sign in with an account that has admin rights.
* Open the Settings app and navigate to **Update & Security -> Recovery**. Under “Reset this PC” click “Get started” and choose “Remove everything.” This process can take 30 minutes or longer.
* Once the reset process completes and the language selection screen is presented, continue with the POC Device Autopilot Configuration section below.

For Surface devices such as Surface Book or Surface Pro, reapplying the available recovery image is also an option. These recovery images can be downloaded via <https://support.microsoft.com/en-us/surfacerecoveryimage>. After restoring the image using the provided instructions, the device will boot to the language selection screen. At that point, continue with the POC Device Autopilot Configuration section.

If the recovery image or existing OS is not running at least Windows 10 1709, upgrade the OS to Windows 10 1709 via Windows Update, and then reset the OS.

* Extracting the Device ID from existing devices can be accomplished in the same manner as with new devices outlined above or you can do this on your own by running a PowerShell script.

PowerShell Script Method:

For devices that have wired network connections, or when using a USB key, the following steps can be used:

* Boot the devices into Windows 10 1709+.
* On the first OOBE screen, press Shift-F10 to open a command prompt.
* Run PowerShell.exe. Run command Set-ExecutionPolicy Bypass to enable scripts. Then run command Install-Script Get-WindowsAutopilotInfo and answer Y to any prompts.
* Execute command Get-WindowsAutopilotInfo.ps1 -OutputFile POC.csv and copy the CSV file to a USB key, or map a drive to a network location and copy the file to that location.
* Exit from PowerShell.exe and the command prompt to remain at the OOBE language selection screen.

If this device only has Wi-fi networking and no USB key is available, the steps will need to be modified:

* Boot the devices into Windows 10 1709+.
* On the first OOBE screen, press Control-Shift-F3 to reboot the device into audit mode.
* Once the desktop appears, connect to a Wi-fi network.
* Open an elevated command prompt.
* Run PowerShell.exe. Run command Set-ExecutionPolicy Bypass to enable scripts. Then run command Install-Script Get-WindowsAutopilotInfo and answer Y to any prompts.
* Execute command Get-WindowsAutopilotInfo.ps1 -OutputFile POC.csv then map a drive to a network location and copy the file **POC.csv** to that location.
* Click OK in the Sysprep dialog to reseal the OS and reboot the computer (ready for the POC).

|  |
| --- |
| **✪** Important |
| Note that the above instructions do not work for devices running Windows 10 S since Windows 10 S will not run PowerShell scripts. In this case, you can remotely gather the hardware information, then reset the computer to get back to the start of the process. |

Any of these methods will result in the creation of a CSV file containing the hardware ID’s of the POC Surface devices. Note: Do not open the CSV file in Excel as reformatting of the information can occur and corrupt the file. Instead use Notepad to open the CSV. Once you have a CSV file with the device details, you will be able to add the devices into the Autopilot Deployment Service via Intune.

# Autopilot Configuration

## Network Connectivity Requirements

The Windows Autopilot Deployment Program uses several cloud services to get your devices to a productive state. This means those services need to be accessible from devices registered as Windows Autopilot devices.

To manage devices behind firewalls and proxy servers, the following URLs need to be accessible:

* https://go.microsoft.com
* https://login.microsoftonline.com
* https://login.live.com
* https://account.live.com
* https://signup.live.com
* https://licensing.mp.microsoft.com
* https://licensing.md.mp.microsoft.com
* ctldl.windowsupdate.com
* download.windowsupdate.com

|  |
| --- |
| **✪** Important |
| Where not explicitly specified, both HTTPS (443) and HTTP (80) need to be accessible.  If you're auto-enrolling your devices into Microsoft Intune, or deploying Microsoft Office, make sure you follow the networking guidelines for [**Microsoft Intune**](https://docs.microsoft.com/intune/network-bandwidth-use#network-communication-requirements) and [**Office 365**](https://support.office.com/en-us/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2). |

## Intune

Sign in to <https://portal.azure.com> using the admin credentials provided for the tenant.

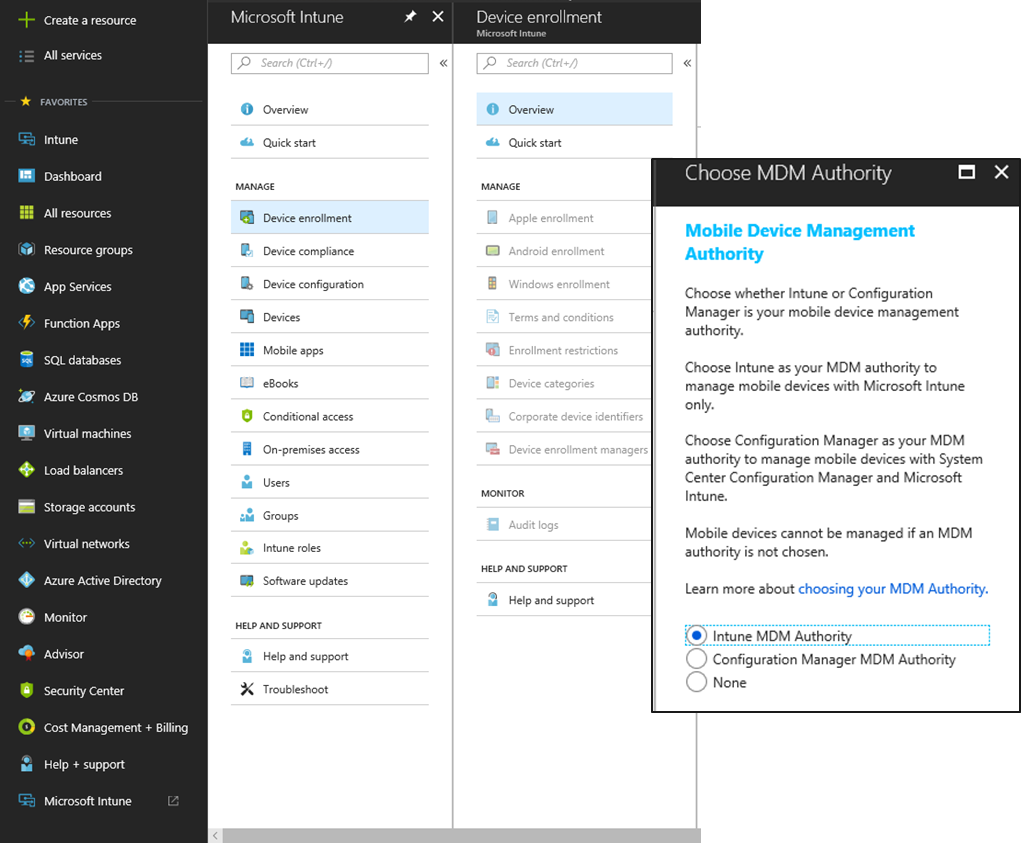
Go to Intune -> **Device enrollment**

The first thing you’ll be asked to do is choose the **MDM Authority**.

MDM Authority must be chosen, and you’ll be offered two options:

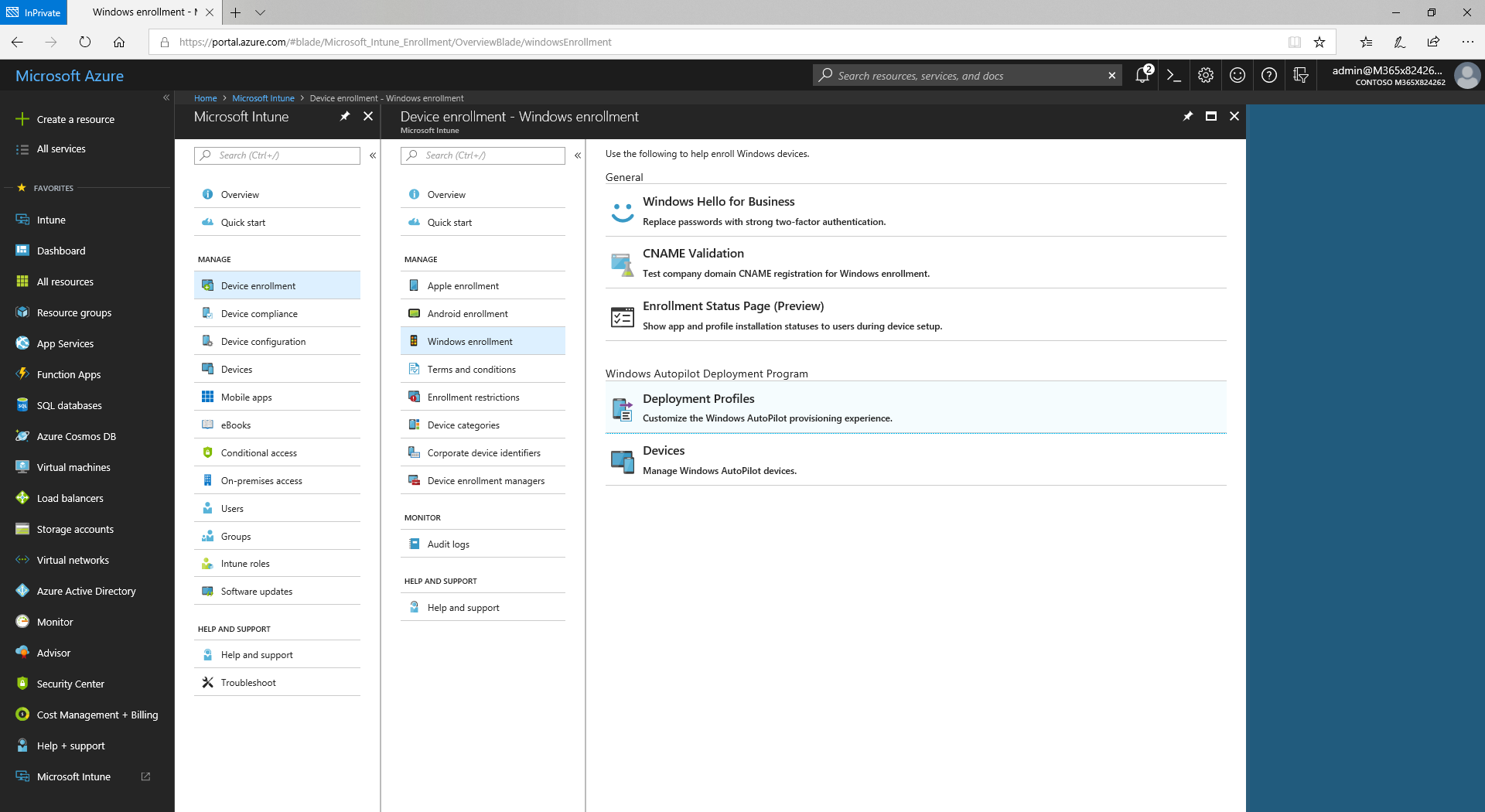
1. Intune MDM Authority – When Intune is the only place you use to manage your devices.
2. Configuration Manager MDM Authority – When you have SCCM in your organization set up in a hybrid configuration with Intune.

For this POC we’ll be using Intune MDM Authority:



Next, when people in your organization run the out-of-box experience on the device, the profile configures Windows based on the Autopilot deployment profile you applied to the device. You can create and apply Autopilot deployment profiles to these devices.

Under **Device enrollment**, go to **Windows enrollment**, and choose **Deployment Profiles**.



In the **Create profile** box, name the profile you’re creating and add a description if you want.

In **Deployment mode** choose “**User-Driven**”, and in **Join to Azure AD**select “**Azure AD joined**”.

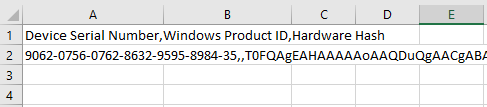


Under **Out-of-box (OOBE)**, confirm that all defaults are selected, then save and create the profile.



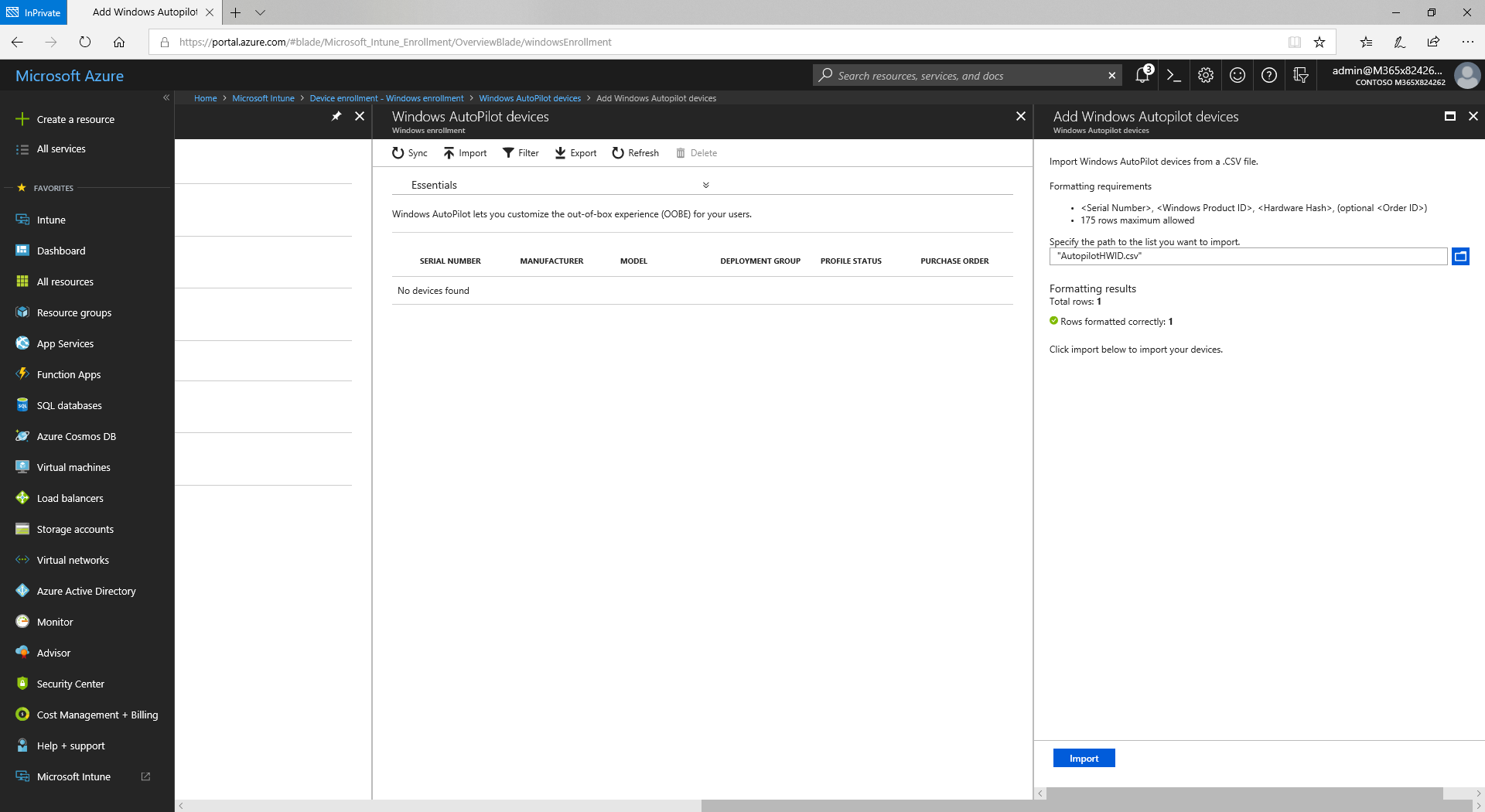
Next, go to **Windows enrollment** -> **Devices**. This is where you need to import the CSV file you created in preparation for this POC. The CSV file contains the following information on the device you’re about to enroll:

1. The Device’s Serial Number
2. The Windows Product ID (Optional in this case).
3. The Hardware Hash

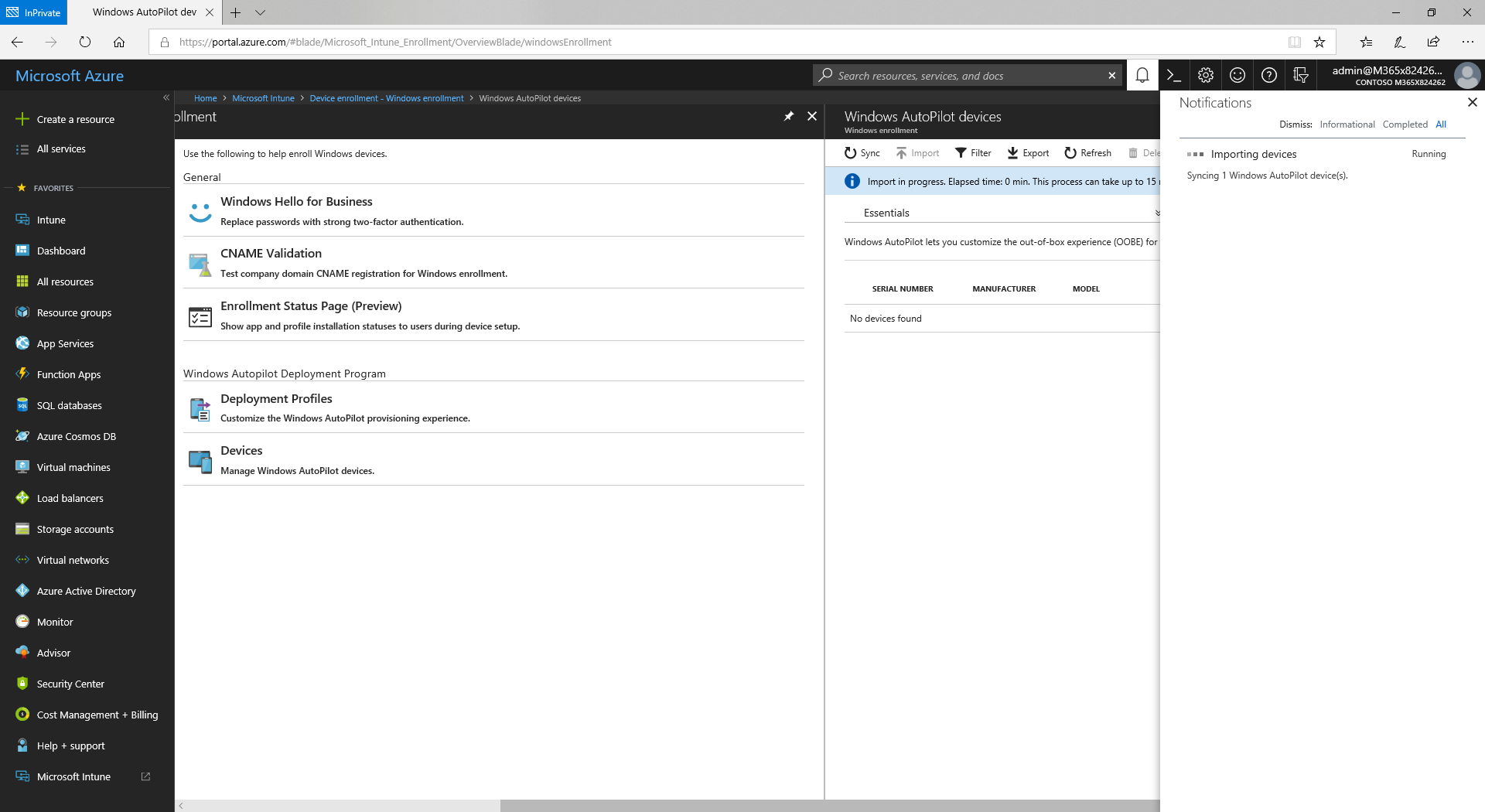


It is recommended not to open these files with Excel, as it might destroy the structure of the data.

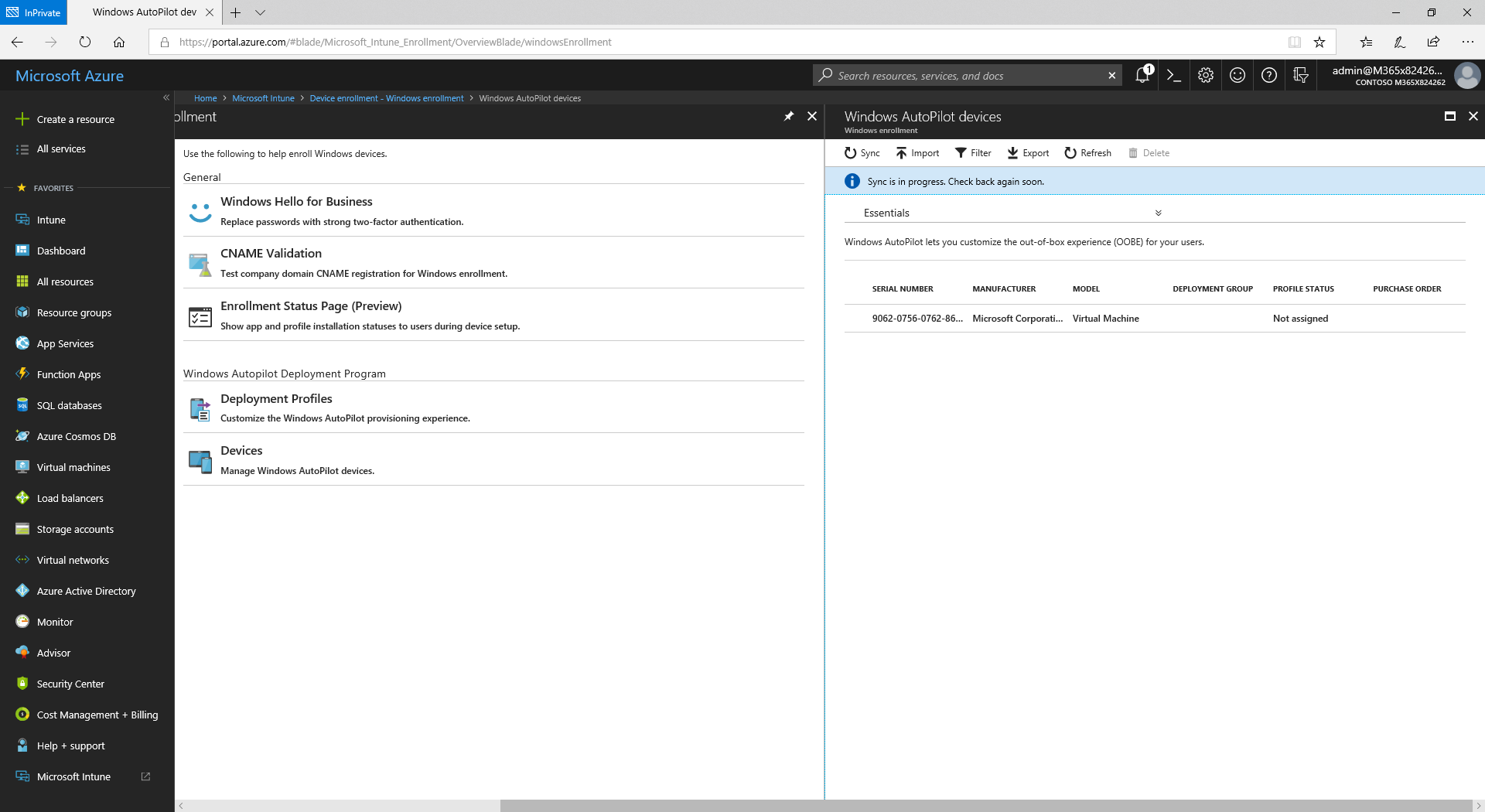
Click the **Import** icon and browse to the location of the CSV file.



You’ll notice how many rows are in the file and how many are correctly formatted. If all is well, click the **Import** button.

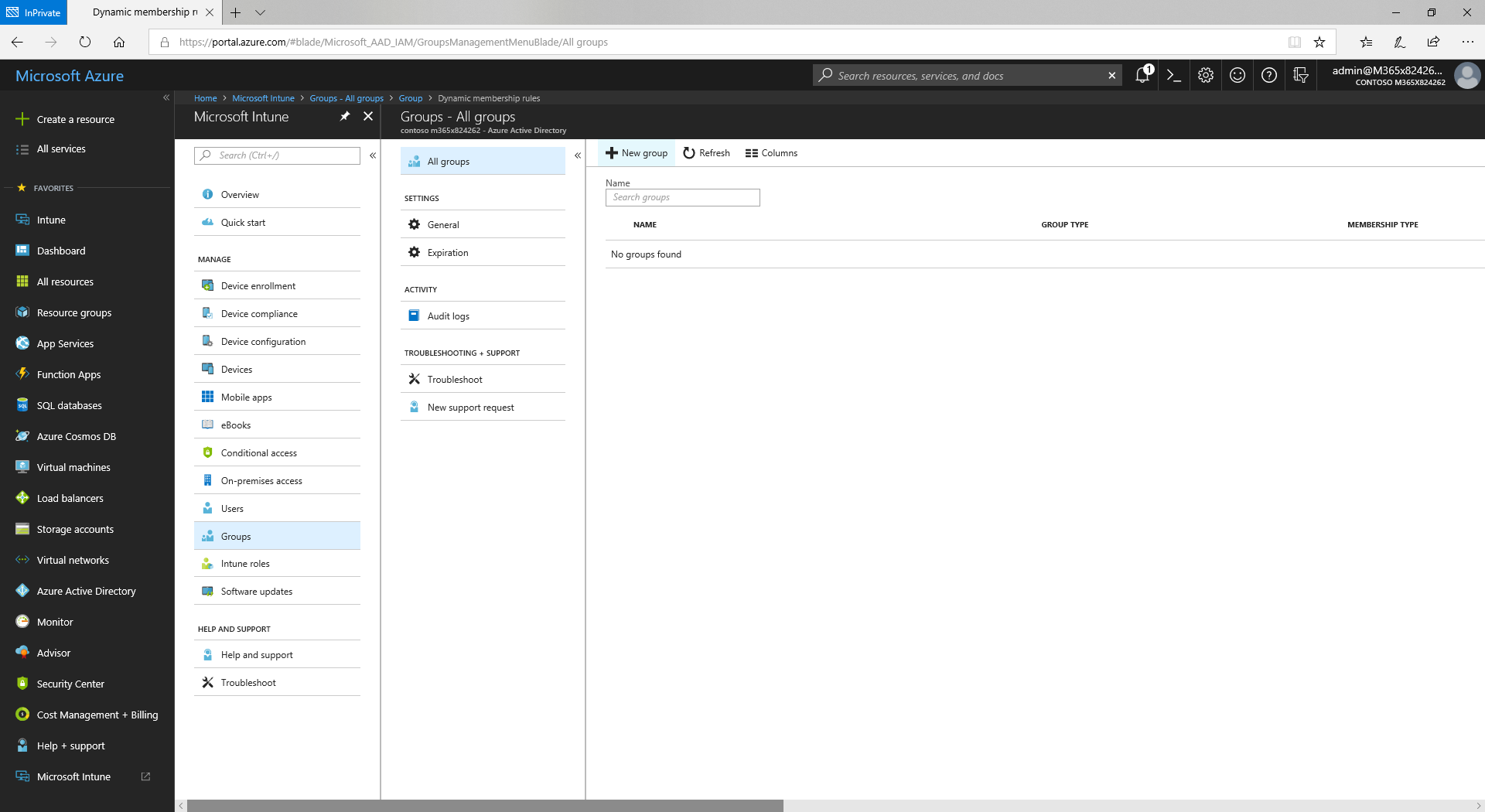


Import might take a while, and Intune will notify you once it’s complete. When completed, you’ll be able to see the device’s serial number, manufacturer and model. Click the Sync button, and then the Refresh button once the Sync is completed.



Next, let’s create an Azure AD group that all new devices will automatically join to use Autopilot.

Go to Intune -> **Groups** and click **+New group.**



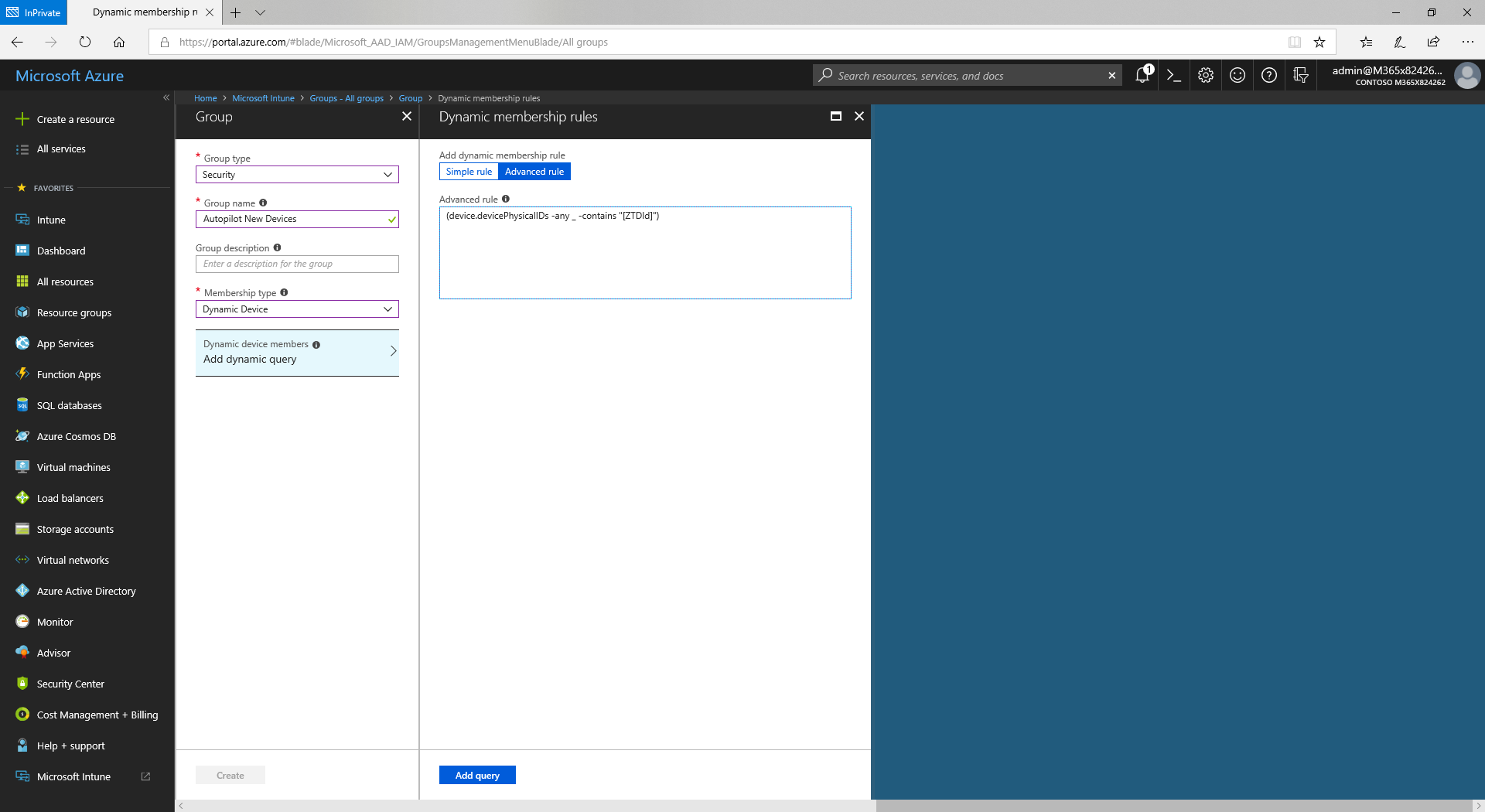
Make this a **Security Group** and give it the name “**Autopilot New Devices”**. You can add a description if you like.

Under **Membership type** choose “**Dynamic Device**” and choose “**Advanced rule**” for the dynamic query.

In the **advanced rule** box, type the following:

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

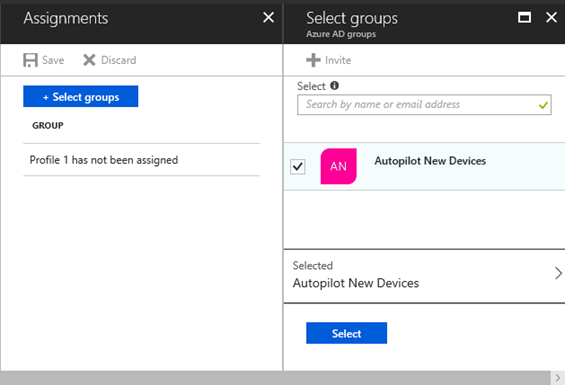
Then, click **Add query** and **Create**.



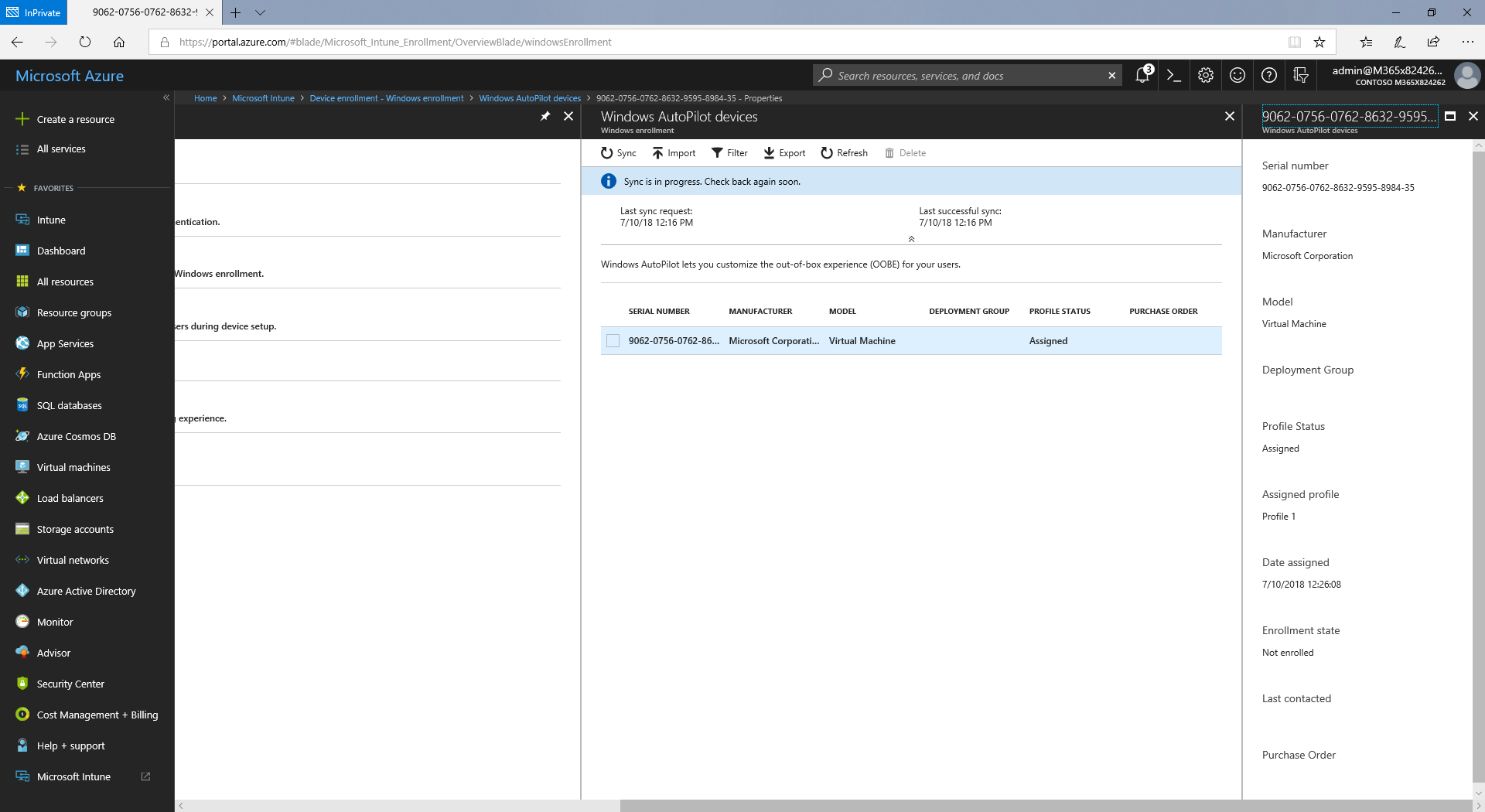
Go back to **Windows enrollment** -> **Deployment profiles** and choose the profile you created earlier.

Click **Assignments**, then click **+Select groups**.

Add the dynamic group you created earlier and save the configuration.



Wait for the profile to sync – you’ll then see that it assigned to the dynamic group.



# Intune Device Configuration

What good is a deployment if you can’t configure the devices the way you want them? Let’s use the power of Intune to set some basic settings for your devices:

## Device Profiles

Microsoft Intune includes settings and features that you can enable or disable on different devices within your organization. These settings and features are managed using profiles.

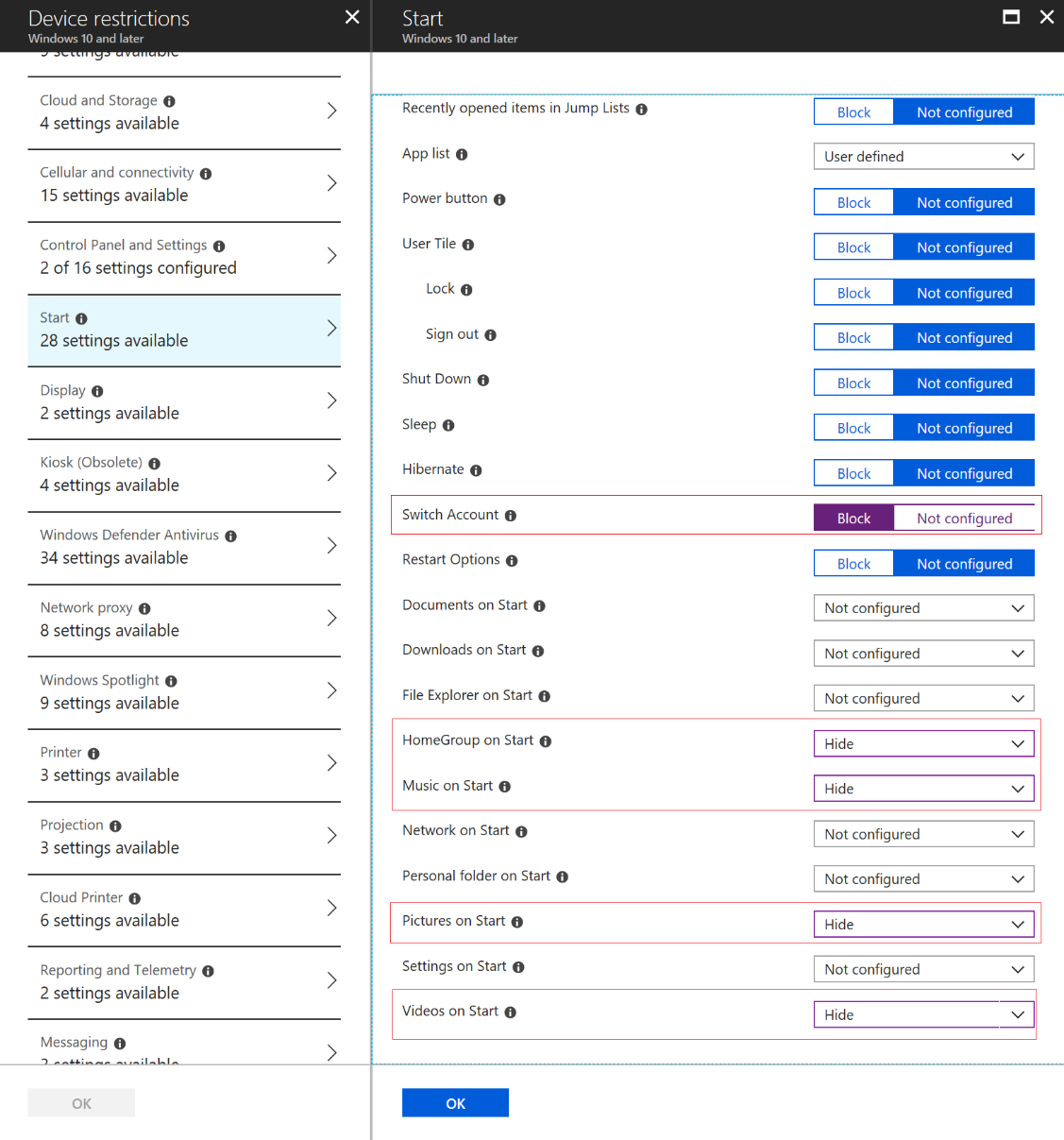
Navigate to **Intune** -> **Device configuration** -> **Profiles** and choose **+Create profile.**

Name the profile “**Initial Configuration**”.

For the Platform choose **Windows 10 and later**.

Under Profile type choose **Device restrictions**.

From the **Device restrictions** pane navigate to **Start** and scroll down to apply the following



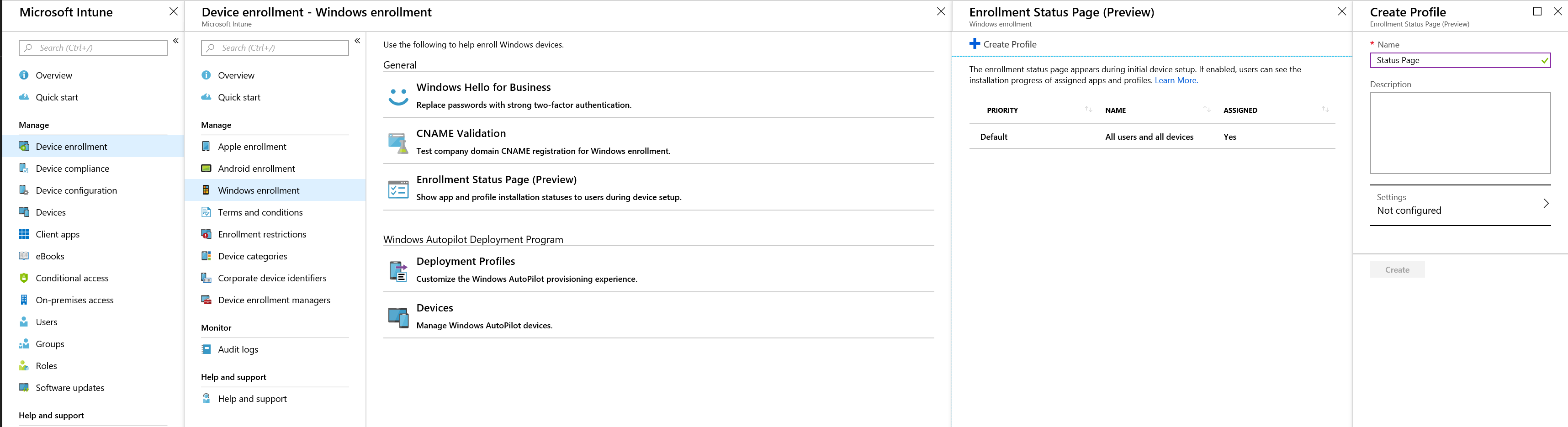
Next, navigate to **Control Panel and Settings** and block **Gaming**.

Last, navigate to **Microsoft Edge Browser** and set the **Start page** to your favorite website.

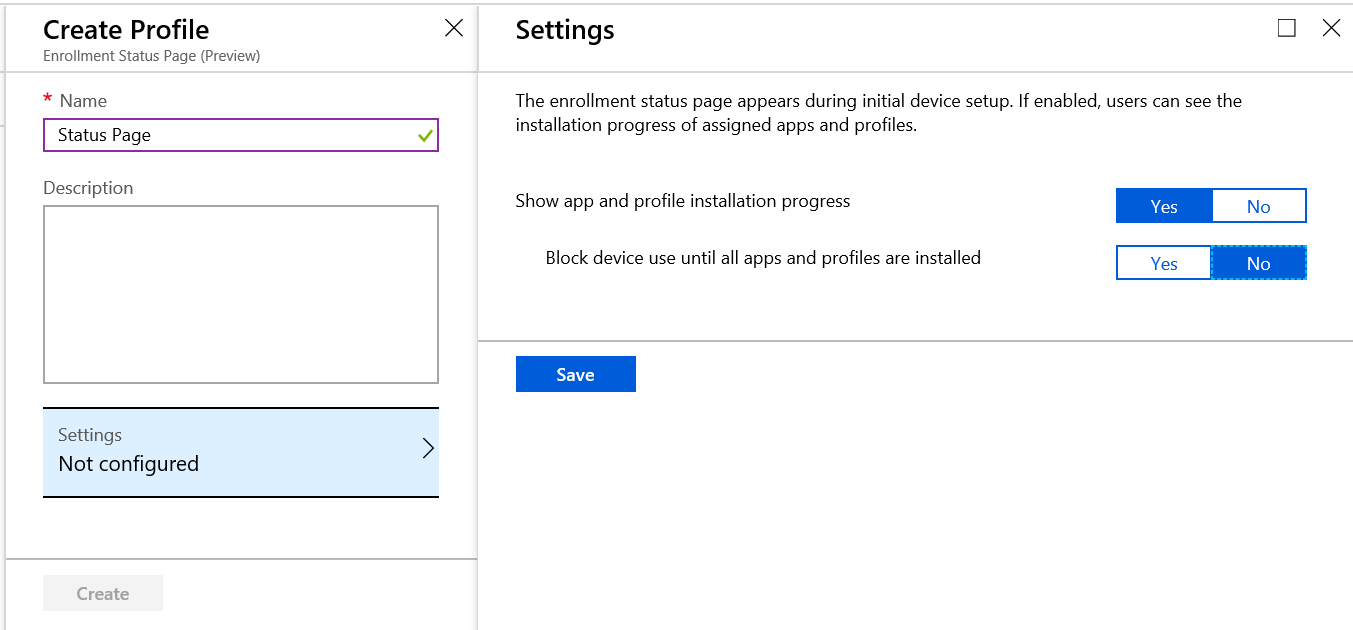
Save the configuration and assign it to **All Users & All Devices.**

## Enable the Enrollment Status Page

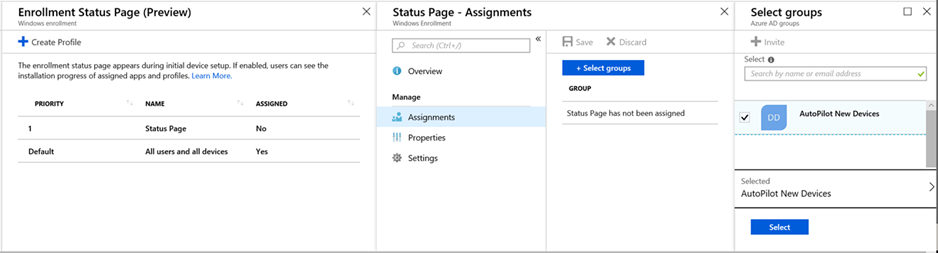
Navigate to **Device Enrollment** ->**Windows Enrollment**->**Enrollment Status Page (Preview)**. Create a new profile called “Status Page”



Select **YES** to **Show app and profile installation progress**. For POC purposes you can leave the others at the default setting. Click Save and Create.



From there, you’ll see the new profile but notice it has not yet been assigned. Here you will assign the profile to the Azure AD Group that was created earlier called “**Autopilot New Devices**”. To do this, click on the profile you just created. Select **Assignments**->**Select groups**.



## Deploy Software – Office ProPlus

Navigate to **Intune** -> **Mobile apps** (may appear as **Client apps**) -> **Apps** and click **+Add**.

In the **Add app** pane choose **Office 365 Suite: Windows 10**. Remove ***Publisher*** and ***Access*** from the app list, click **OK.**

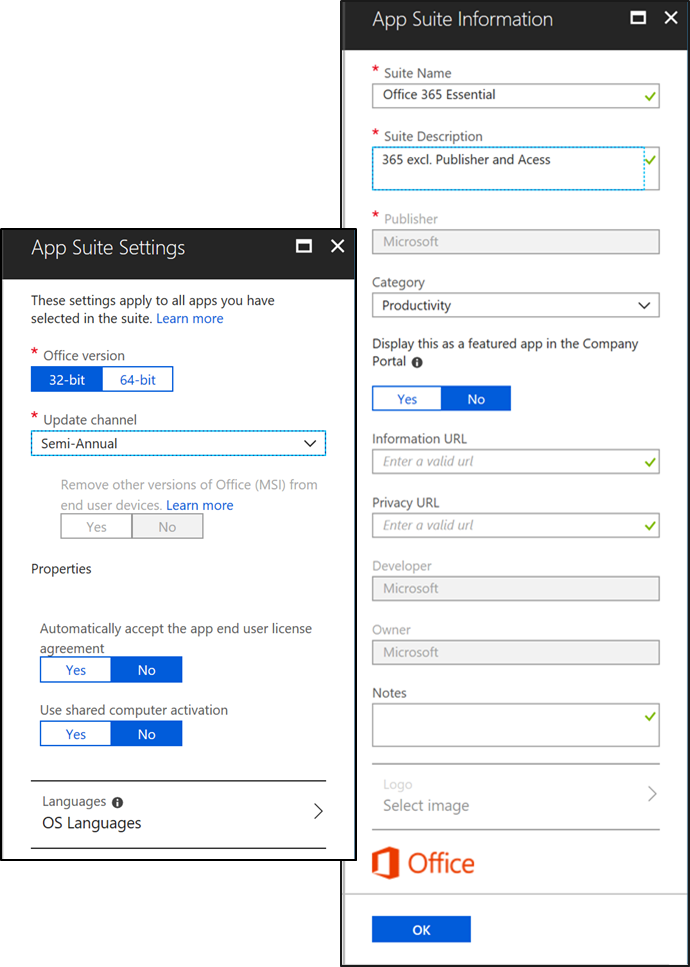


Navigate to “***App Suite Information***”.

Enter “**Office 365 Essential**” under **Suite Name**.

Enter a description under **Suite Description**, then click **OK**.

Under “**App Suite Settings**”, change the version to 64 bit and choose **Semi-Annual** for the Update channel, then click **OK**.



Click **Add** when finished and confirm it shows in the Apps list.

Click the profile in the apps list and click **Assignments**.

In the ***Add group*** pane, choose **Required** for Assignment type and then choose “**Make this app required for all users**”.

Click **OK** twice and then **Save**.

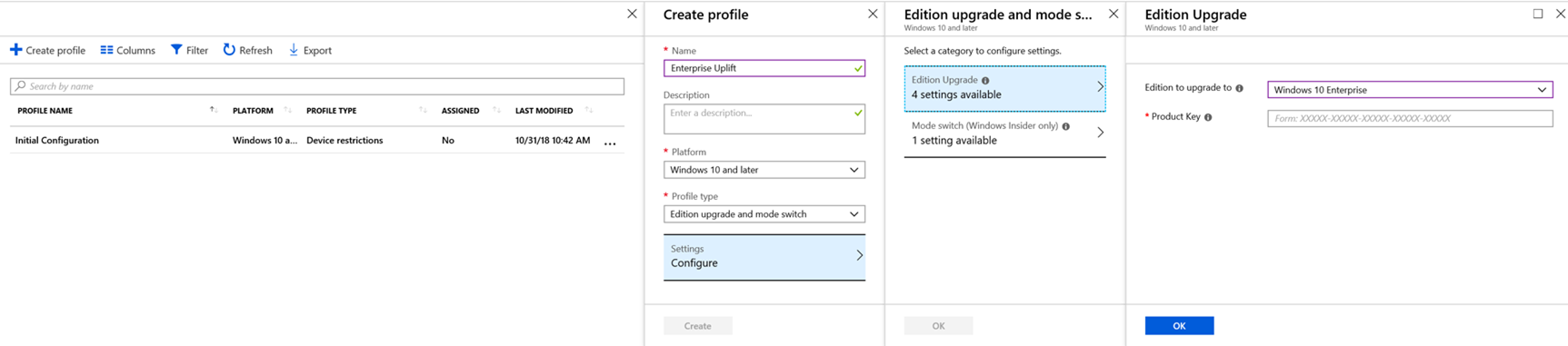


## Windows 10 Edition Upgrade

As part of the automated provisioning process you can choose to upgrade the factory installed operating systems from Windows 10 Pro to Windows 10 Enterprise (assuming own the rights to do so). To do this we will create a new profile and assign it to all users.

|  |
| --- |
| **✪** Important |
| If you have M365 E3 or E5 licensing the following is not needed and will happen automatically the first time the user [with the license assigned] logs in. |

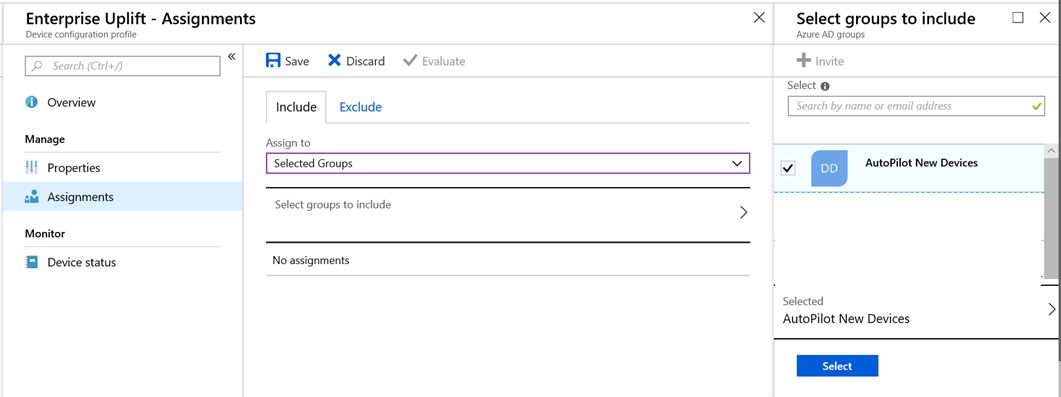
To begin, In Intune navigate to **Device configuration** –> **Profiles** -> **Create profile** -> **Edition upgrade and mode switch** ->**Edition Upgrade**



Name the new profile “**Enterprise Uplift**”. Under Platform select **Windows 10 and later**. Profile type select **Edition upgrade and mode switch**. Select to configure **Settings**. From there click on **Edition Upgrade (4 settings available)** and then choose Windows 10 Enterprise and fill in the required Product Key information.

Click **OK** -> **OK** -> **Create**.

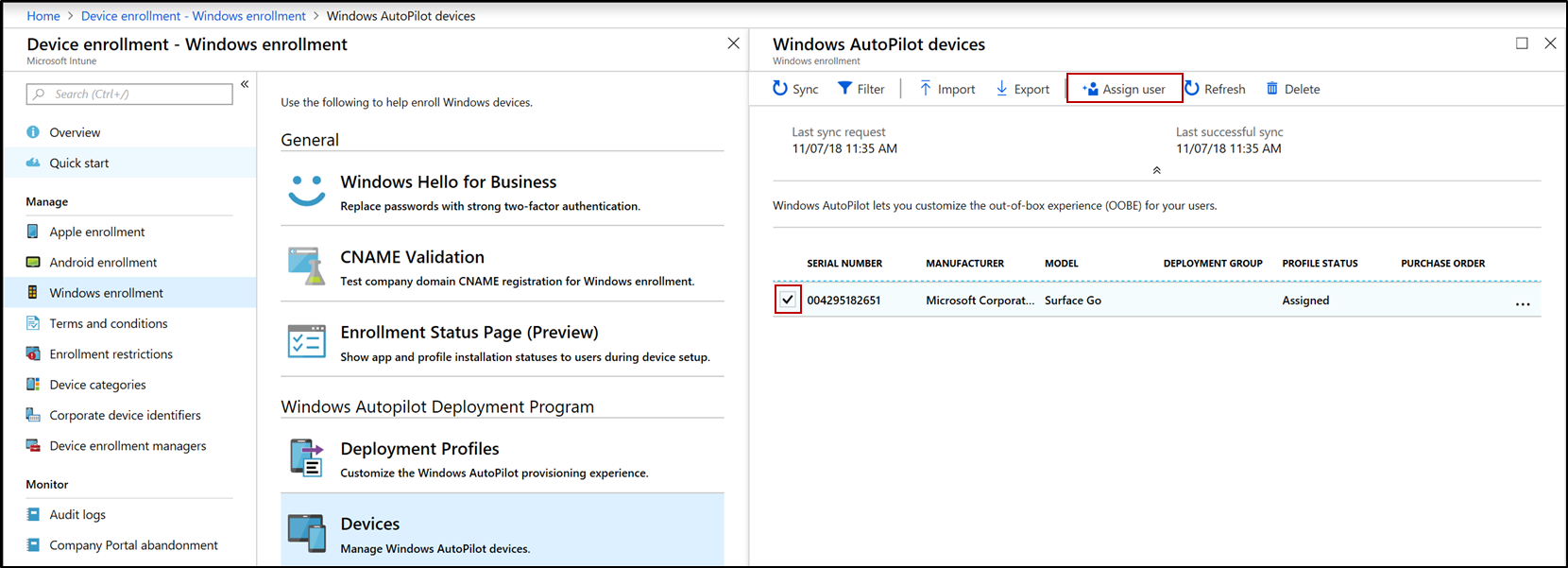
After the profile has been created you need to assign it. Click on **Assignments**. Under **Assign to** choose **Selected Groups** from the drop down and once again select the Azure AD group you created called “**Autopilot New Devices**”. Finish by clicking **Select** -> **Save.**

****

## Assign a User to a Device (Optional)

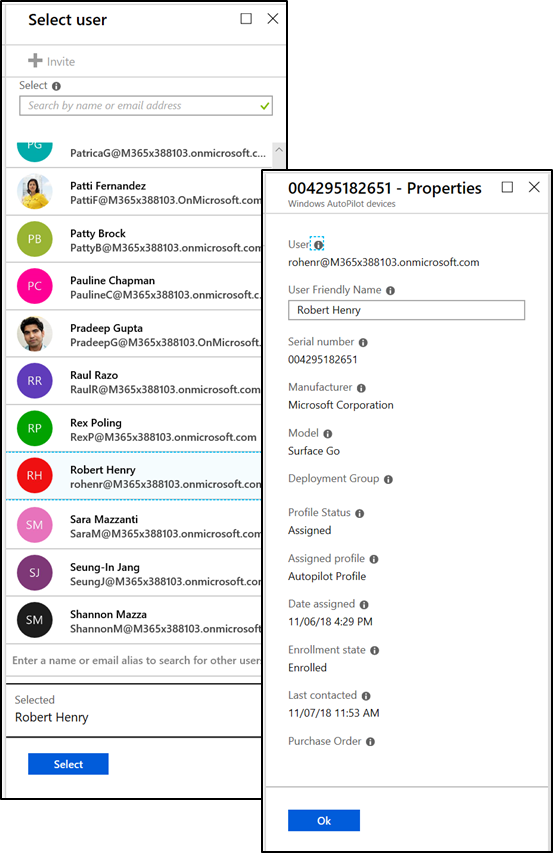
Optionally, you can assign a specific user to a device. This can be helpful in creating a customized experience for your users as well as removing the need for them to input their corporate user name (as it is captured automatically during the setup process). This capability can be initiated once the device is registered to your tenant as part of the Windows Autopilot service. To do this:

In Intune, navigate to **Device enrollment** –> **Windows enrollment** -> **Devices** and select the device you wish to assign to a specific user.

****

Select “**Assign user**” from the top menu. This will open the **Select user** menu. From there click on the user you want to assign to that device.

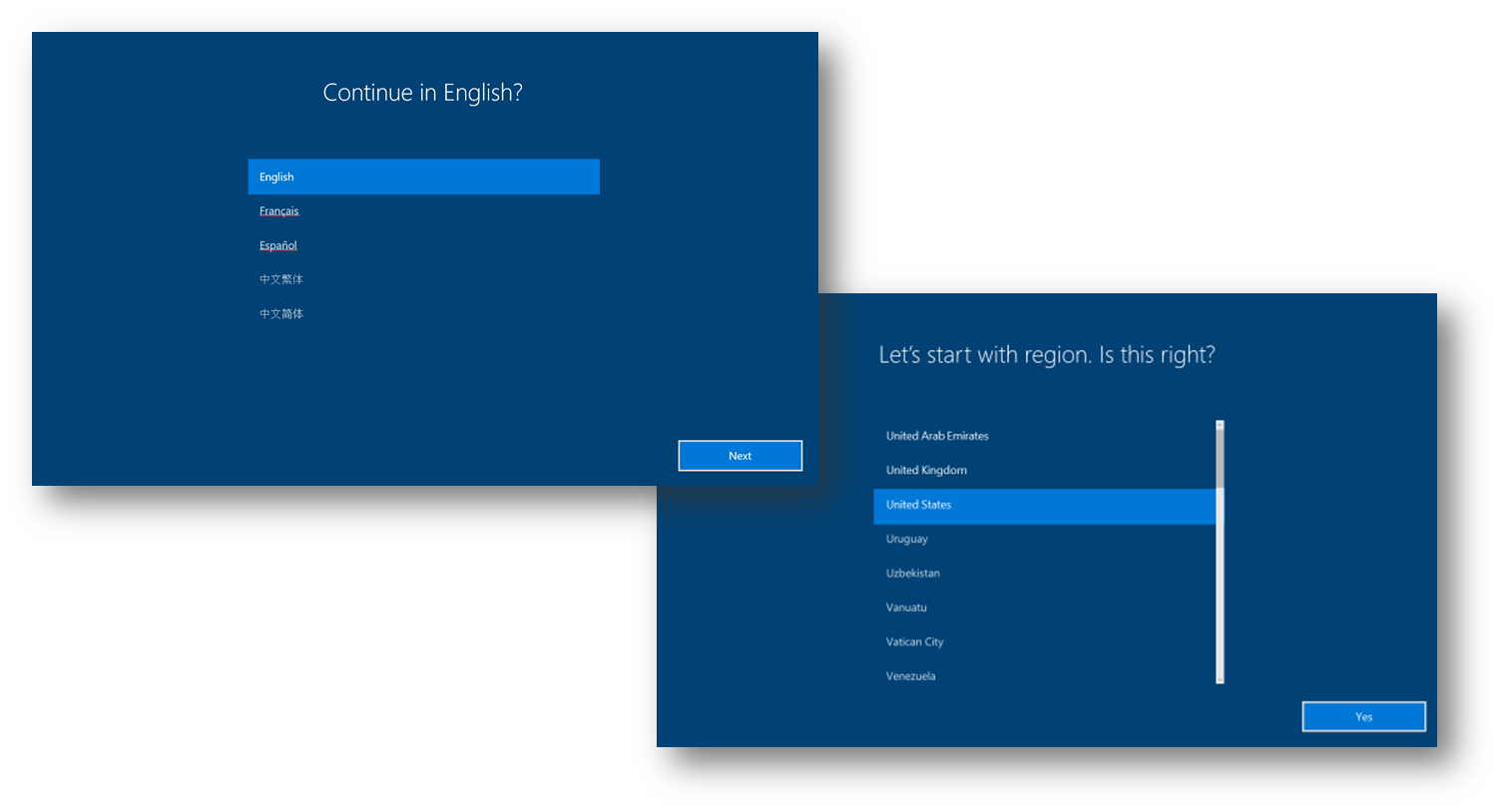
Click **Select** (bottom of the page) then click **OK** on the **Properties** page that appears.

****

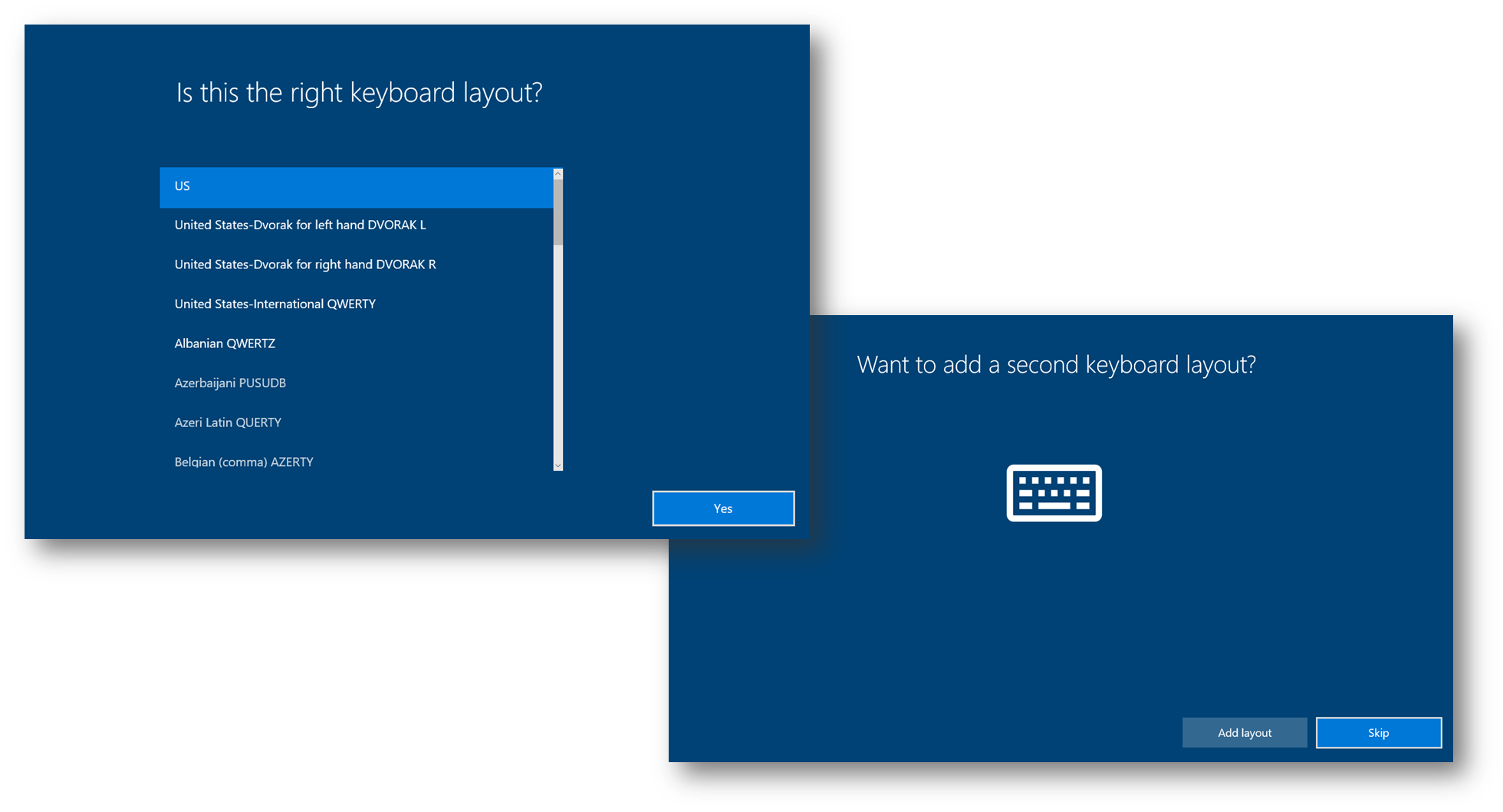
# End User Experience - Autopilot with Surface (User-Driven)

Not only does Windows Autopilot with Surface make life easier for IT, your users also benefit from the automation and simplicity. When using the device for the first time, users will experience the Windows Out-of-box experience (OOBE). With Autopilot the OOBE experience has been great simplified with the number of screens the user has to go through reduced by 75% from the traditional OOBE experience. In fact, users only need their work account credentials. No local admin permissions required.

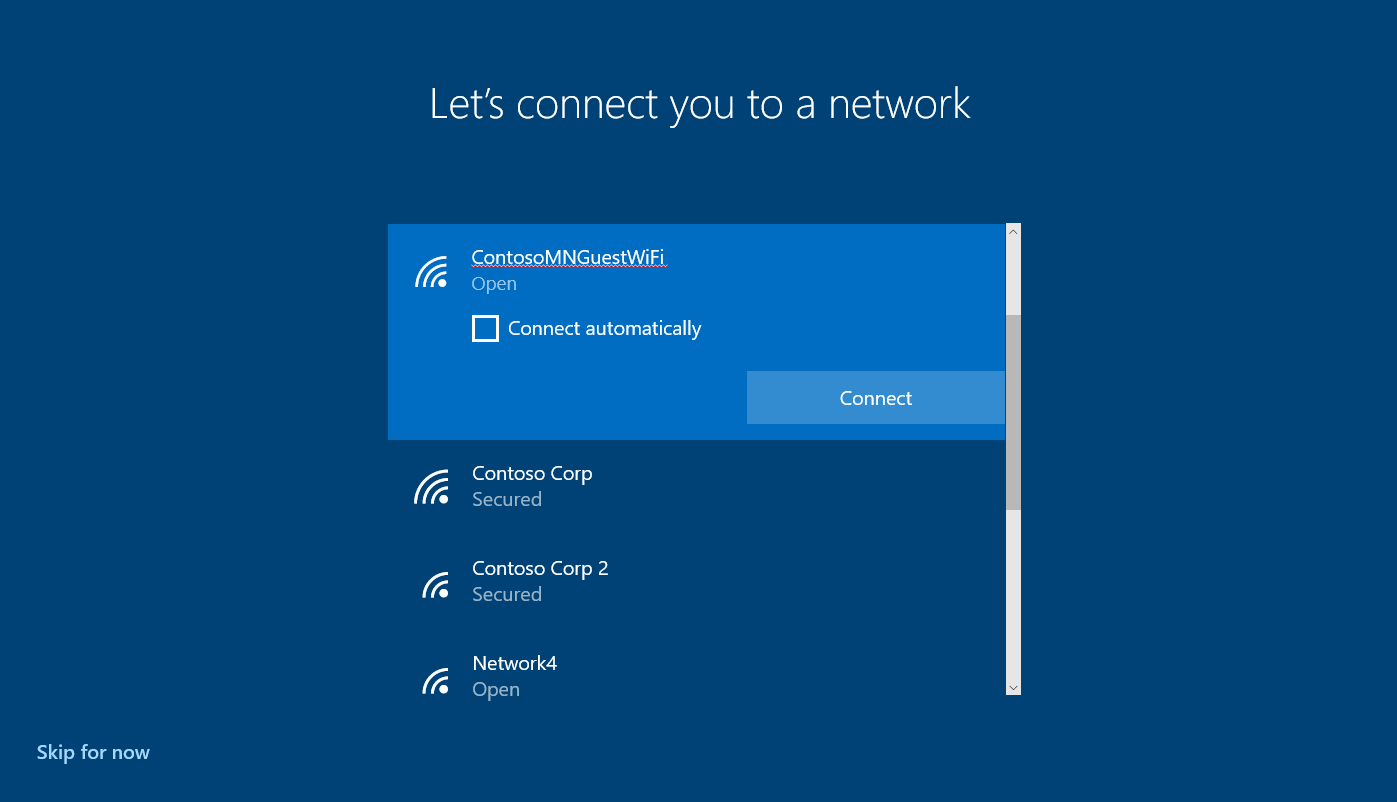
When the Windows 10 device is turned on for the first time, this user is asked to identify their language and region.



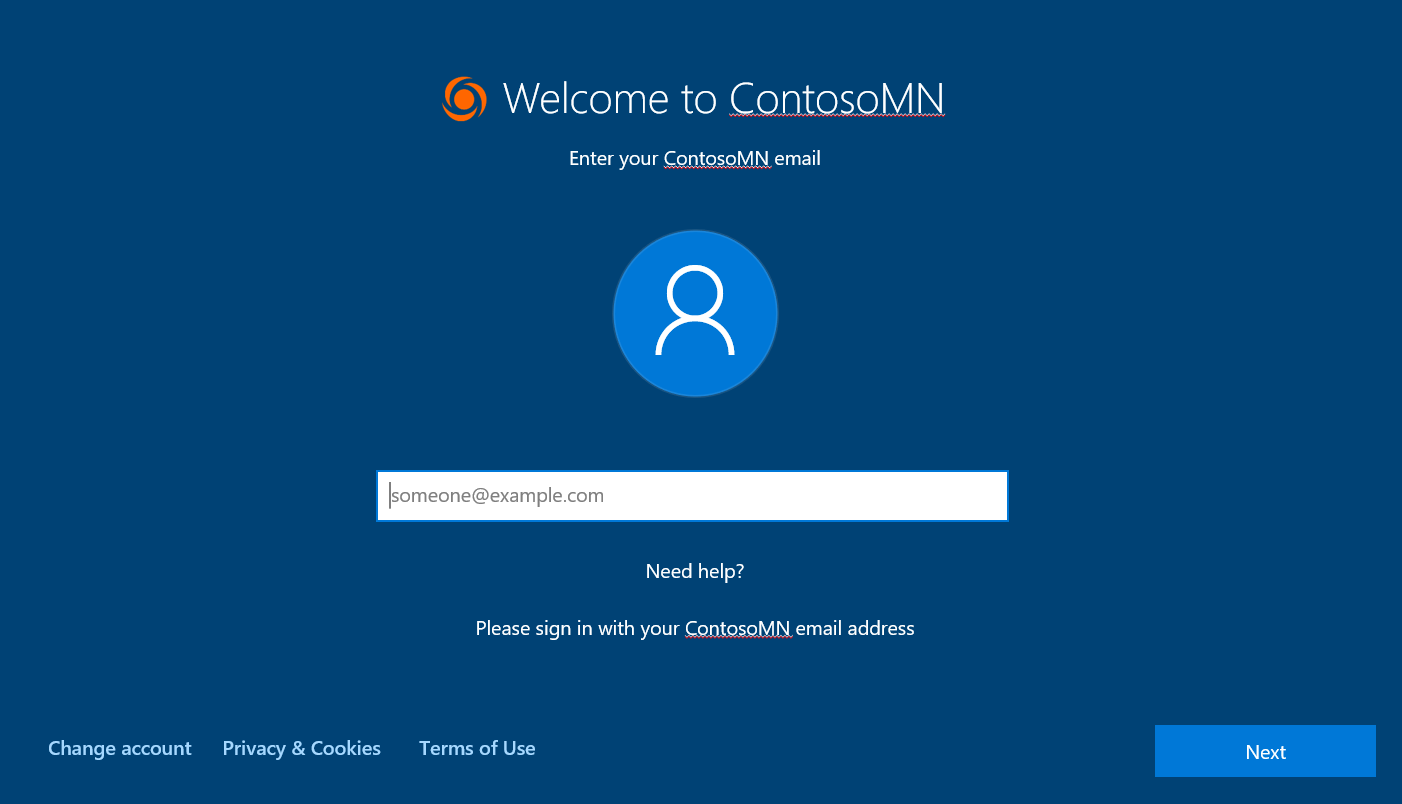
Next, user selects keyboard layout and is given the option for second keyboard layout.



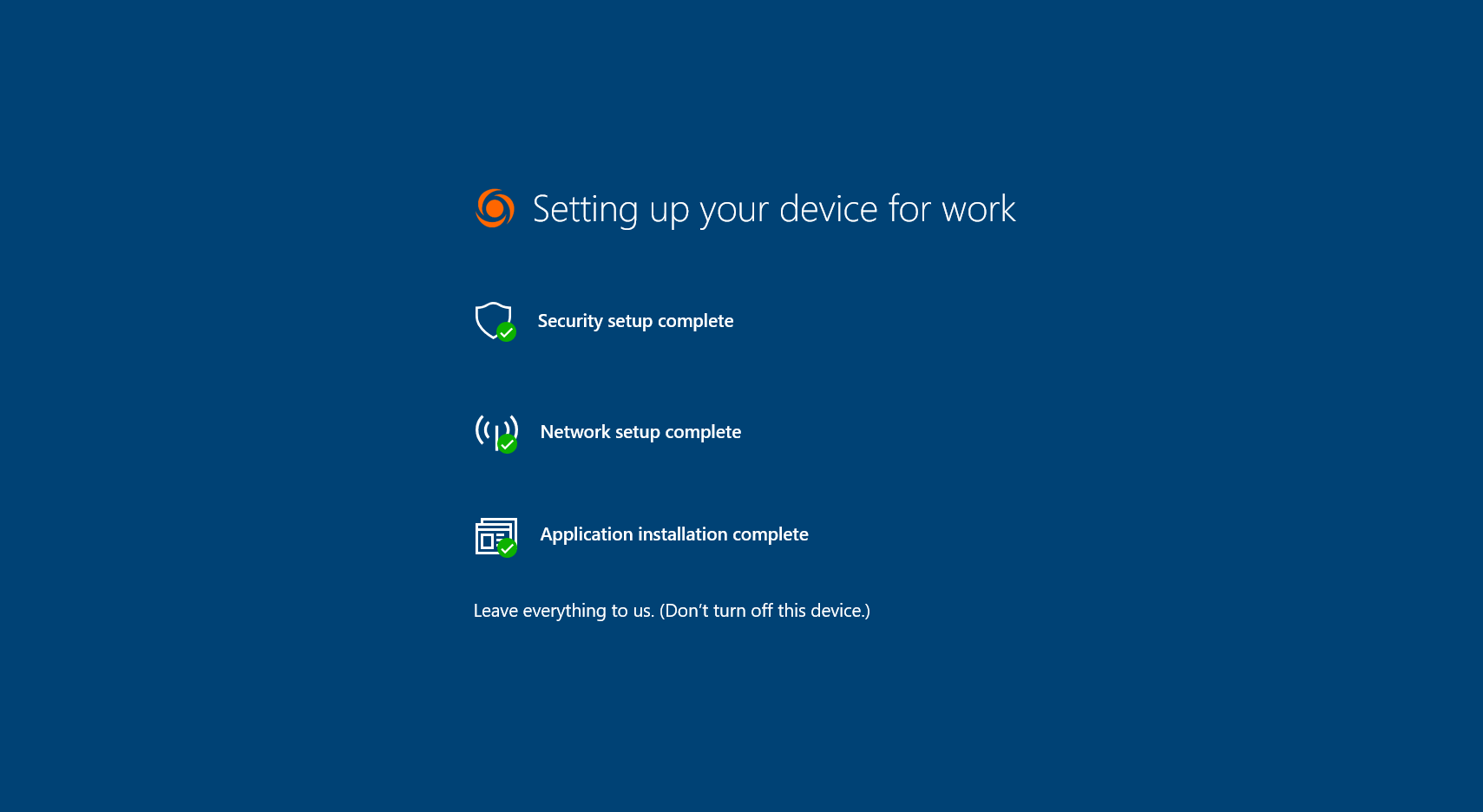
The next step, Windows will verify network connectivity to the internet. If connecting via Wi-Fi, the user will be prompted to connect to a wireless network. If the Surface device is connected via an ethernet cable, Windows will skip this step.



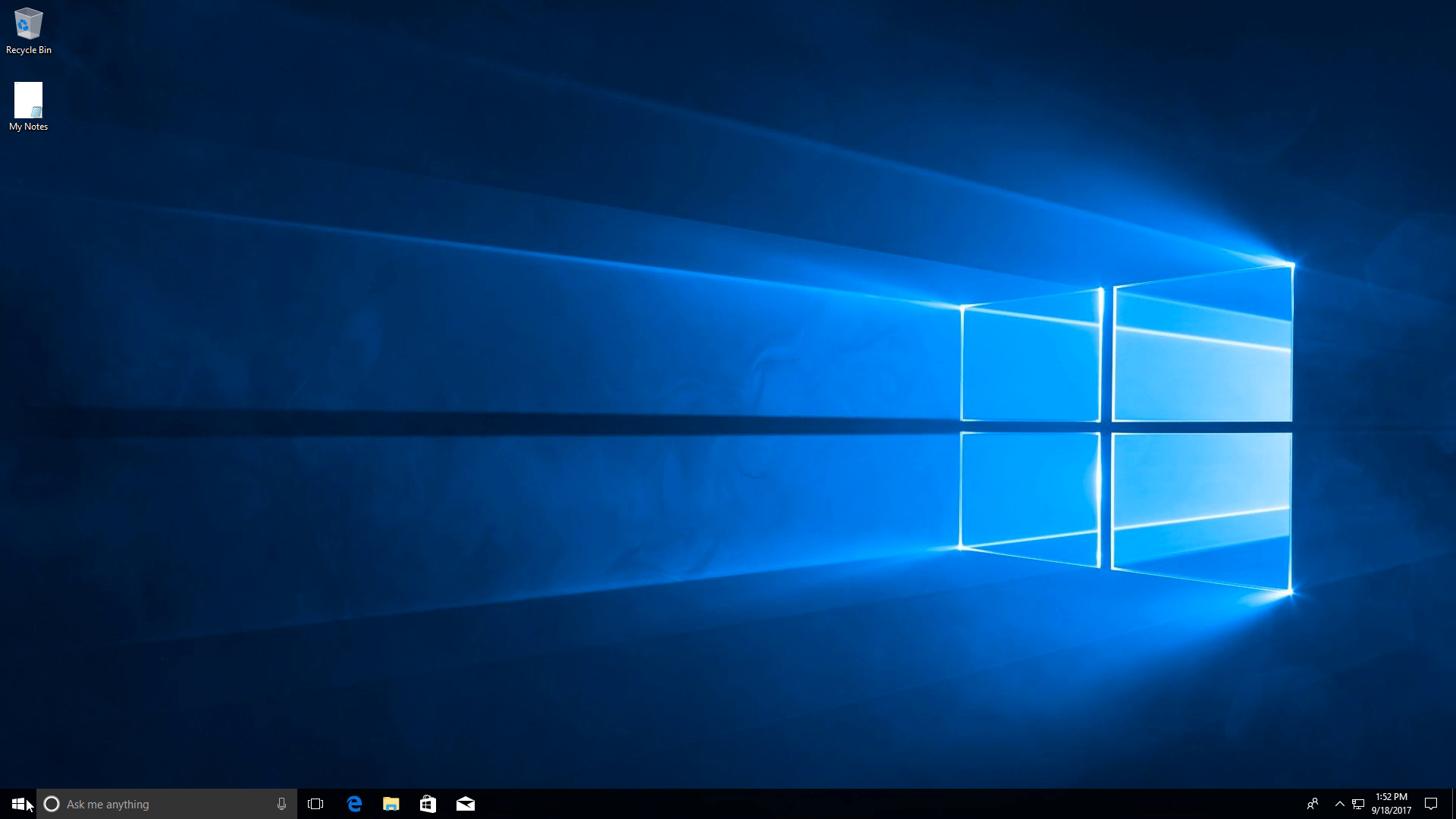
Once connected, Windows will look for, and apply, any required updates. Once completed, the user will be presented with a corporate branded welcome screen. Here they will be prompted to log in with their corporate user name and password.



After logging in, Windows will finish setting up the device. The Enrollment Status Page is used as a place to “park” the user during set up as well as provide visual cues.



The provisioning process takes as little as 4-5 minutes to complete though it could be longer depending on the number of applications, policies, etc. that are being deployed as part of the Autopilot process. Once complete, the device is ready for productive use.



# Optional: Partner Center registration process

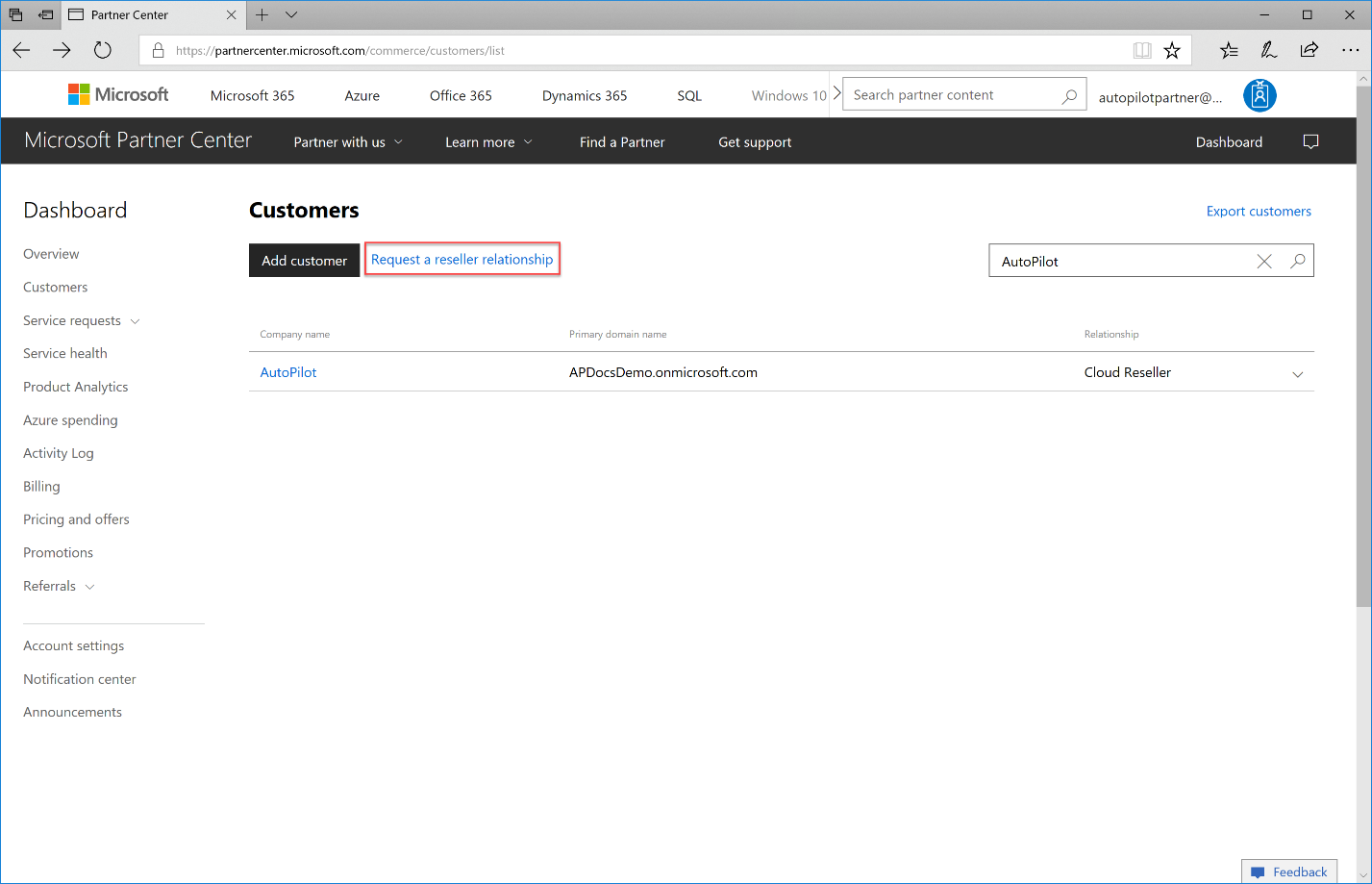
First and foremost, we recommend every partner that is interested in offering modern manageability services of Microsoft 365 such as Windows AutoPilot investigate the steps needed to become a Microsoft CSP. Information can be gained at the [Microsoft Cloud Solution Provider landing page](https://partner.microsoft.com/en-us/cloud-solution-provider). There are simple steps to become an Indirect Reseller and work with your Indirect Provider to sell licenses and services.

[Since October 2018](https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/registration-auth) Indirect CSP Reseller can get direct authorization from the customer to register devices. At the same time, their indirect CSP Provider partner (distributor) also gets authorization, which mean that either the Indirect Provider or the Indirect Reseller can register devices for the customer.

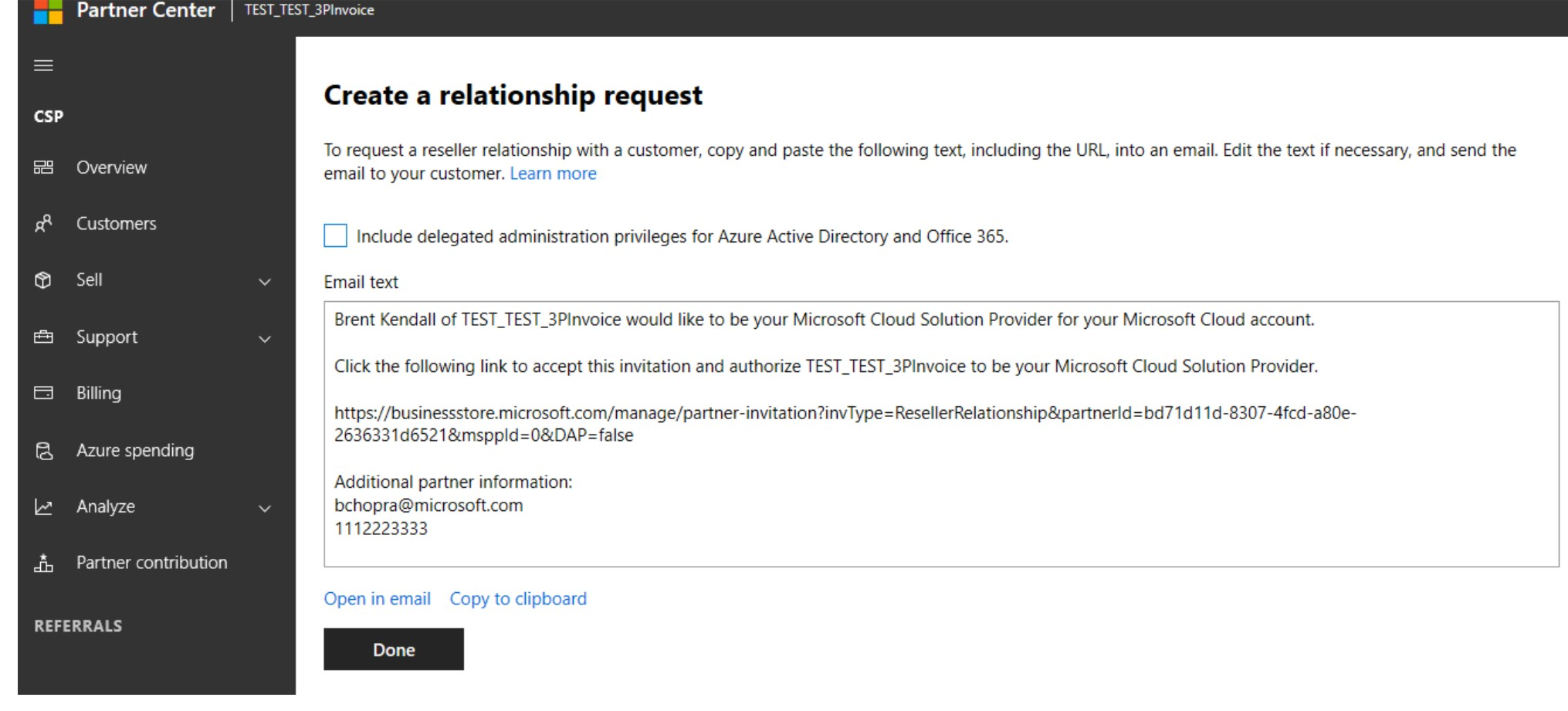
However, the Indirect CSP Reseller must register devices through the Partner Center UI (manually uploading CSV file), whereas the Indirect CSP Provider has the option to register devices using the [Partner Center APIs](https://msdn.Microsoft.com/en-US/Library/Partnercenter/mt842824.aspx).

## Requesting a Customer Relationship

In order to enroll devices as a CSP on behalf of it’s customer, a partner must have a relationship with that customer in Partner Center. If you do not already have an existing relationship with the customer, for example to permit you to manage their AAD or MDM environments, you will need to [request a relationship with that customer](https://msdn.microsoft.com/en-us/partner-center/request-a-relationship-with-a-customer) before you can enroll devices in Windows AutoPilot for them:



To request a relationship, you will need to copy and paste the provided text (outlined in the red box in the following figure) into an email. This text includes a link (highlighted in the following figure) that they can follow to authorize you as a reseller for their accounts. Once they click this link and establish a relationship with you as their reseller, you will be able to manage their account from the Partner Center and register and enroll devices for Windows AutoPilot.

**



Please also note that a CSP partner only get minimum privileges needed to register/de-register devices on the customer AAD tenant.

If more privileges would be needed ( for example: if a customer would ask you to also manage AAD, Office 365 and Intune ) the partner can request this by checking the checkbox “*Include delegated administrator privileges for Azure Active Directory and Office365*”.

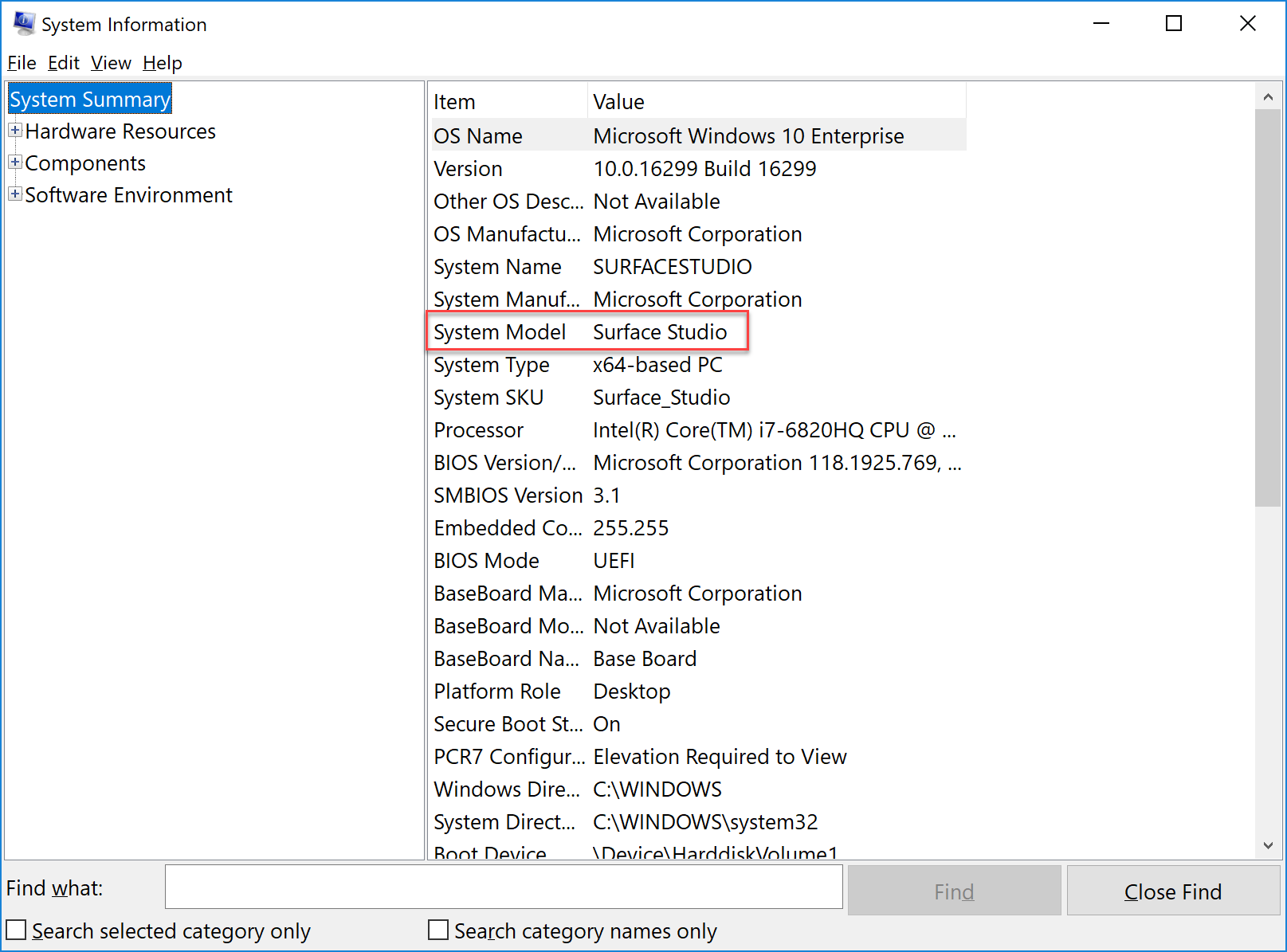
## Registering Devices for Windows AutoPilot

Before an AutoPilot profile can be applied to a device, the device must first be known to Azure Active Directory and the AutoPilot service. Devices that are already enrolled in AAD or Intune can be configured with an AutoPilot profile without being added separately, but new devices that are otherwise unknown to AAD or MDM must first be added.

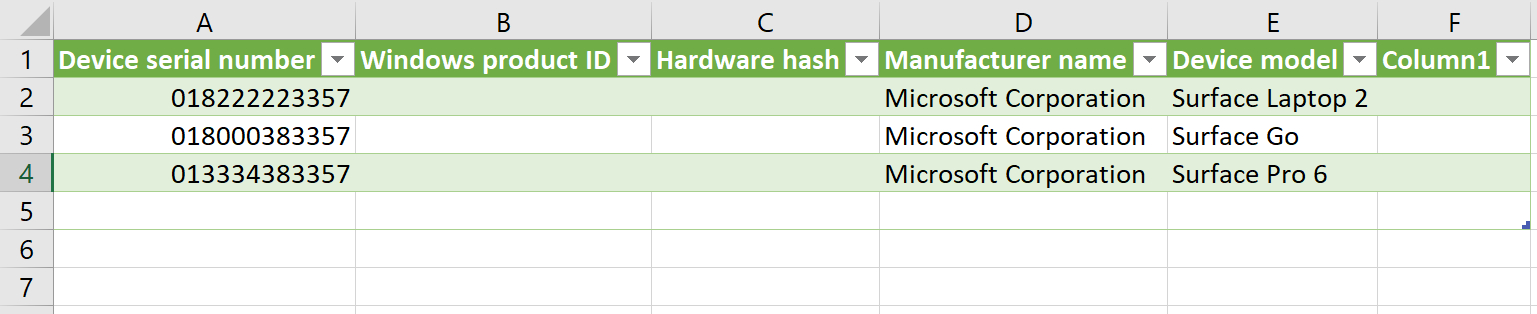
Through the Partner Center, adding devices by serial number, without the need to open the box or run a script on the device, is supported where the device manufacturer provides this capability, such as Surface devices manufactured with Windows 10 Version 1709 or above.

**Note:** Registration of new devices by serial number requires that you have access to a list of the serial numbers for the devices being registered. This step can often occur early in the device order process, sometimes as early as devices arrive at the partner location and often before the order is assembled for shipping to the customer. It is recommended to establish practices to allocate and isolate Windows AutoPilot orders, allowing the collection of serial numbers prior to their registration and enrollment in Windows AutoPilot.

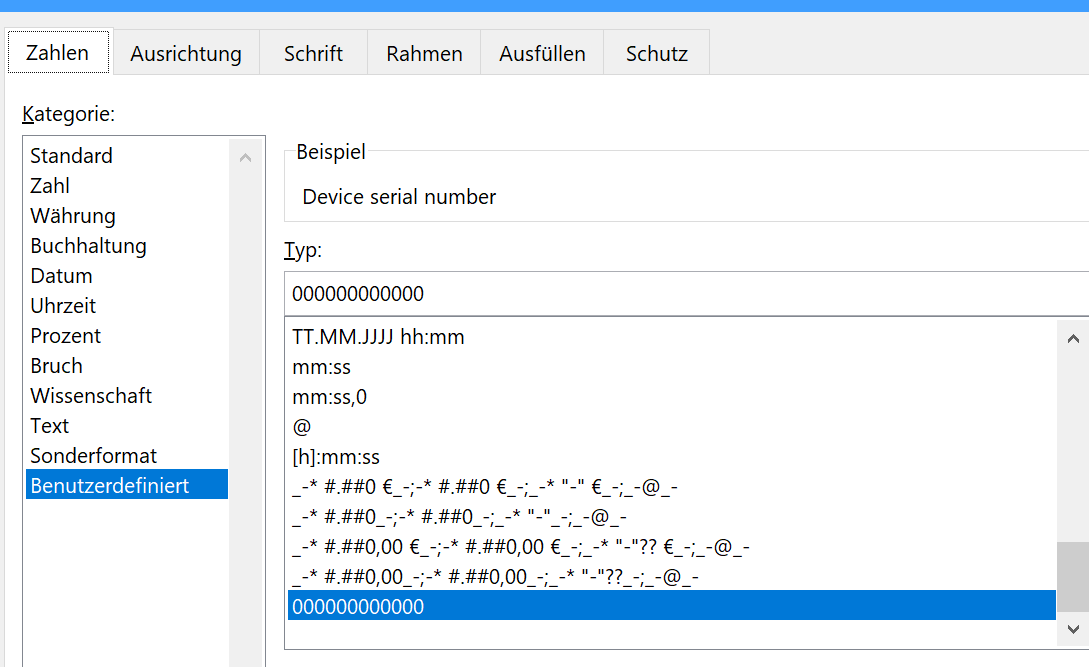
To register devices as owned by the organization and to enable configuration through the Partner Center, you can upload a CSV file with the necessary information. The CSV file must contain the following to register devices via serial number:

* The CSV file should have the following columns with each device on a separate line, comma separated: Device Serial Number, Windows Product ID, Hardware Hash, Manufacturer Name, Device Model
* Device Serial Number – obtained from the sticker on the box or from the ordering or purchasing process, for example on the invoice or shipping label.
* Manufacturer Name – for Surface devices this would be **Microsoft Corporation**
* Device Model – For Surface devices this would be:
  + **Surface Book 2** for Surface Book 2 13 inch or 15 inch
  + **Surface Pro** for Surface Pro or Surface Pro with LTE Advanced
  + **Surface Pro 6** for new Surface Pro 6
  + **Surface Laptop** for Surface Laptop
  + **Surface Laptop 2** for Surface Laptop 2
  + **Surface Studio** for Surface Studio
  + **Surface Studio 2** for new Surface Studio 2
  + **Surface Go** for Surface Go and Surface Go LTE
  + Hint: Device Model should match the System Model variable in SMBIOS. You can see this value by running **MSInfo32**.  
    

See the example **BulkImport\_Devices\_Template.csv** to see how the CSV should look with these columns in order. Note that this CSV includes all possible fields, including the hardware hash of the device. Only the Serial Number, Manufacturer Name, and Device Model must be filled out for registration of Surface devices through the Partner Center, as those devices are supported for enrollment by serial number.

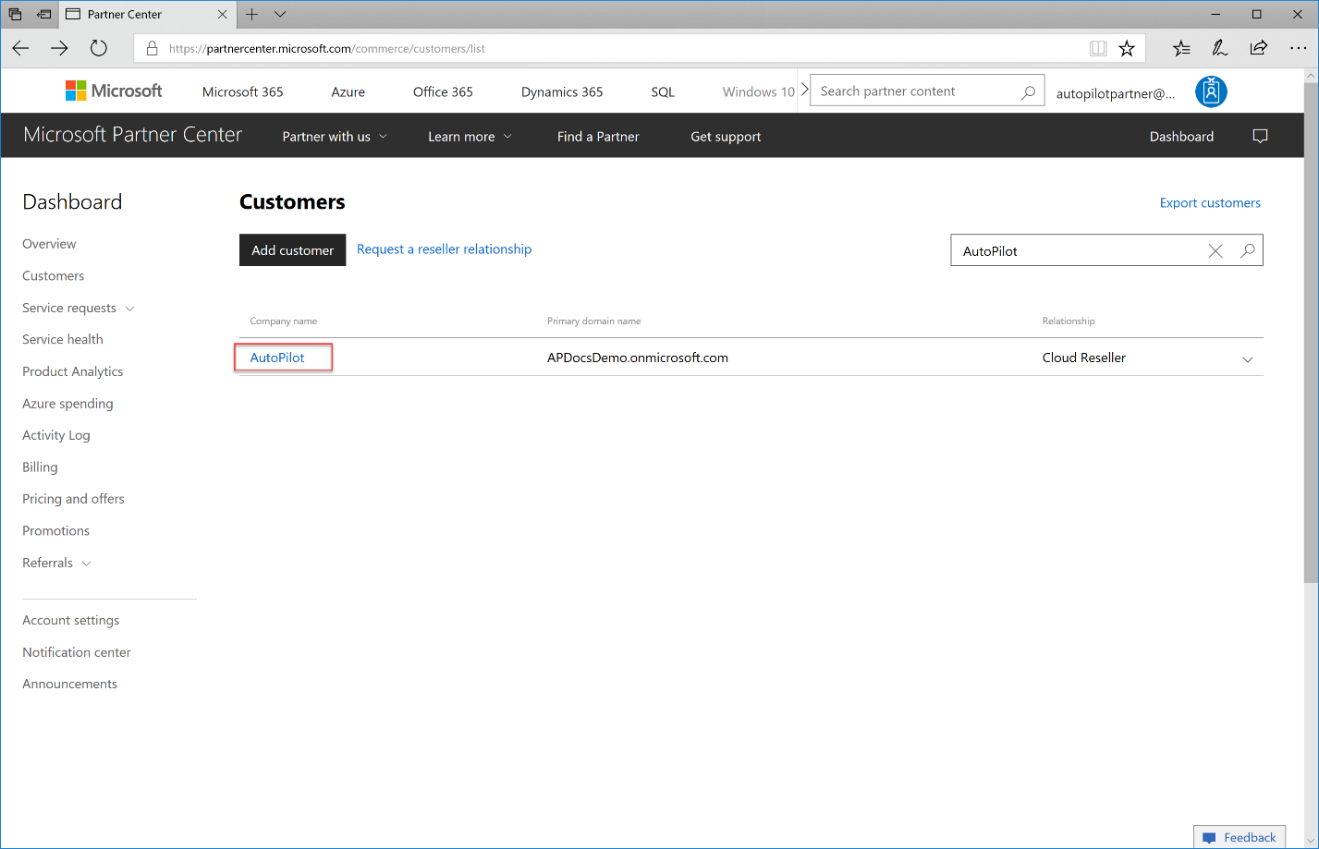
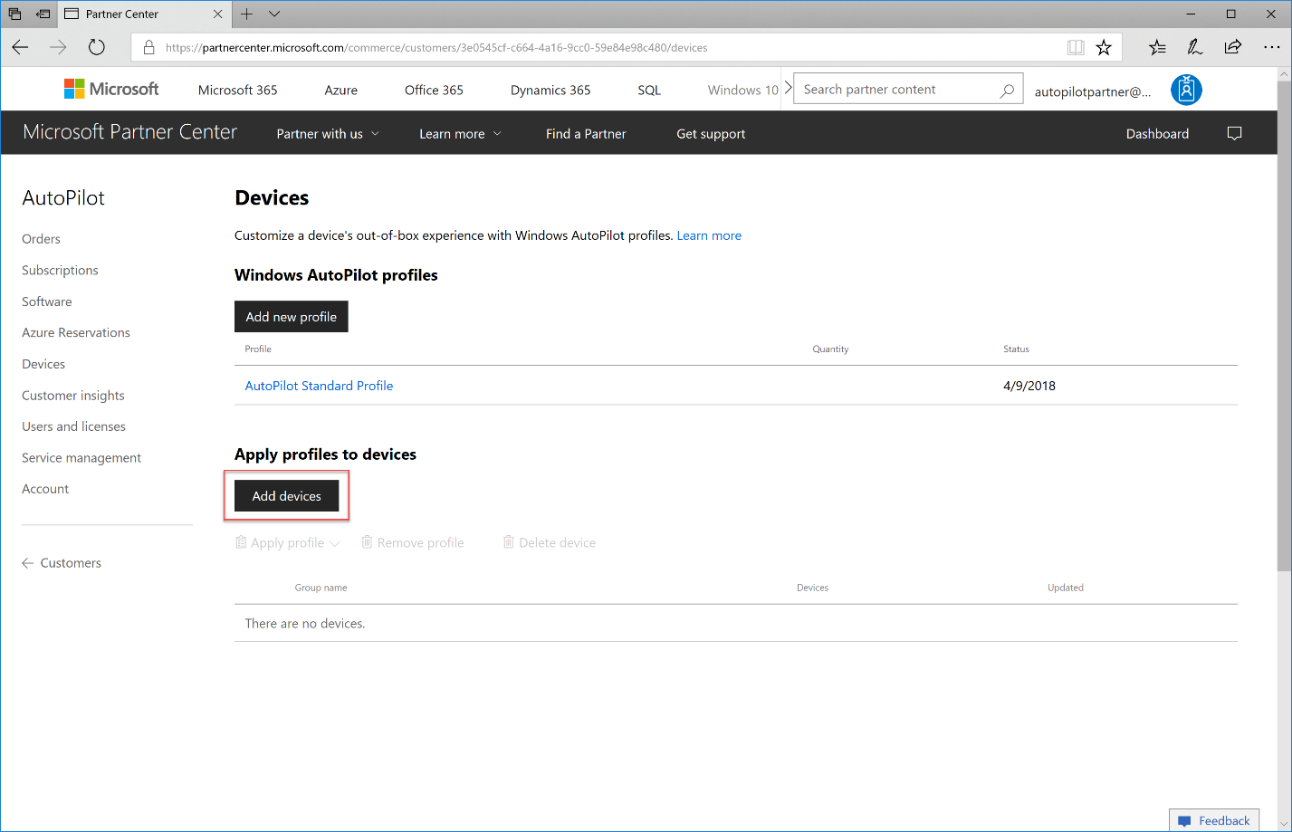
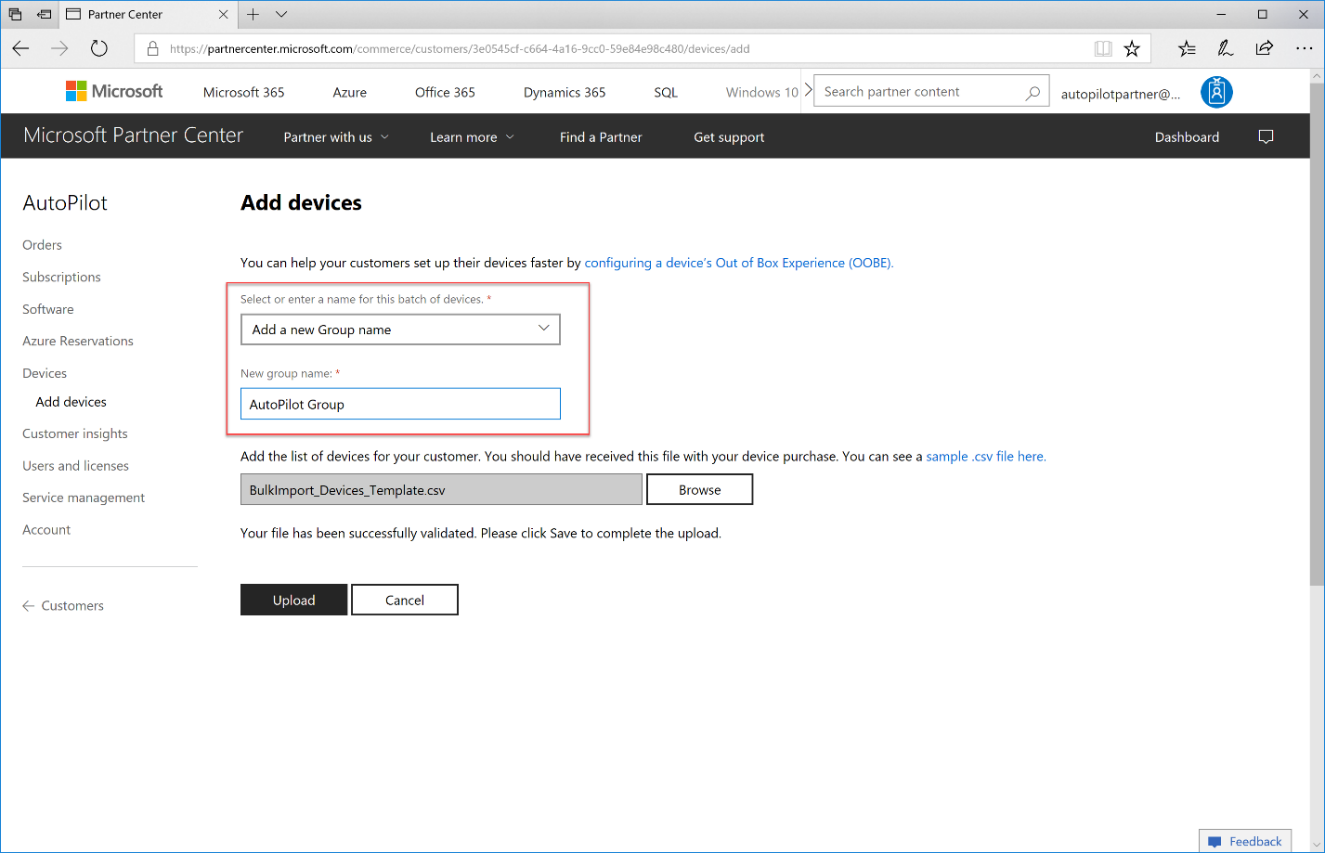
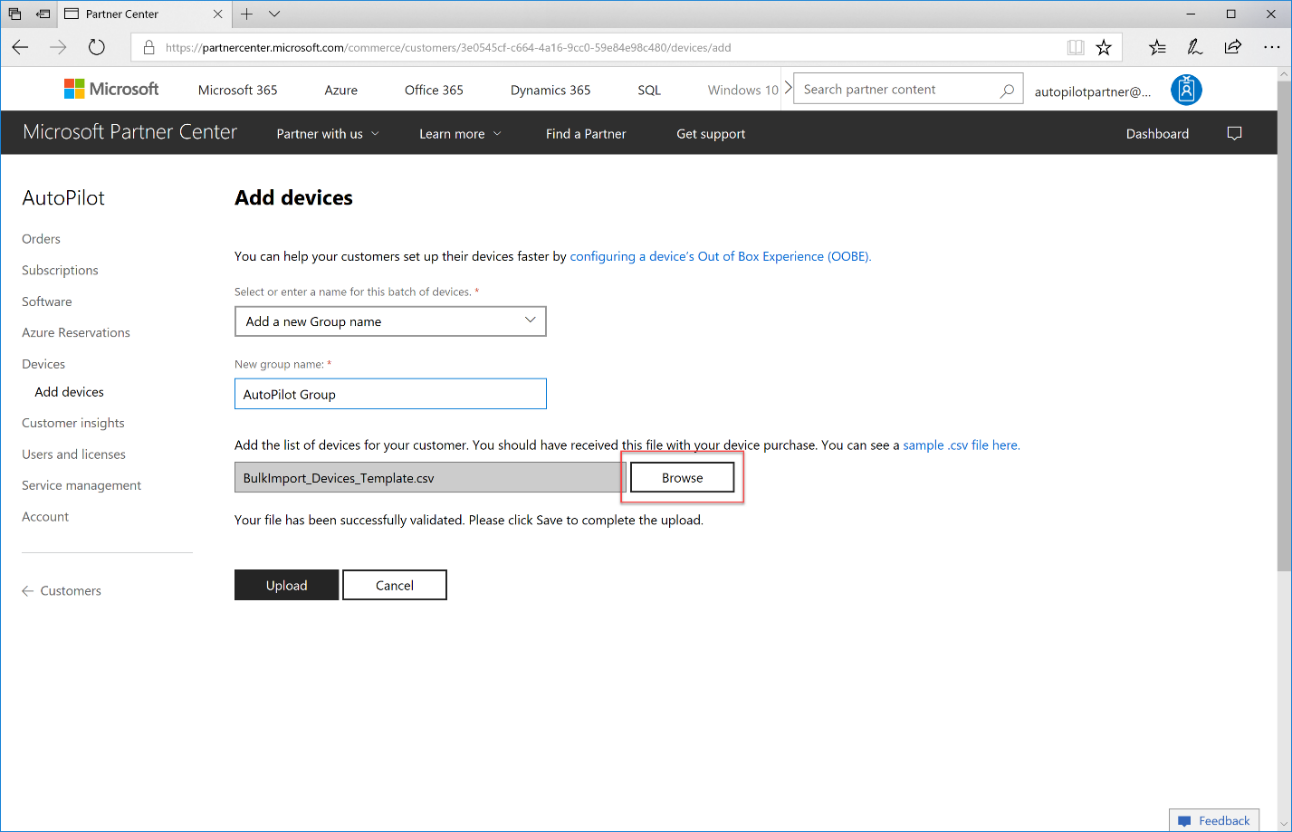
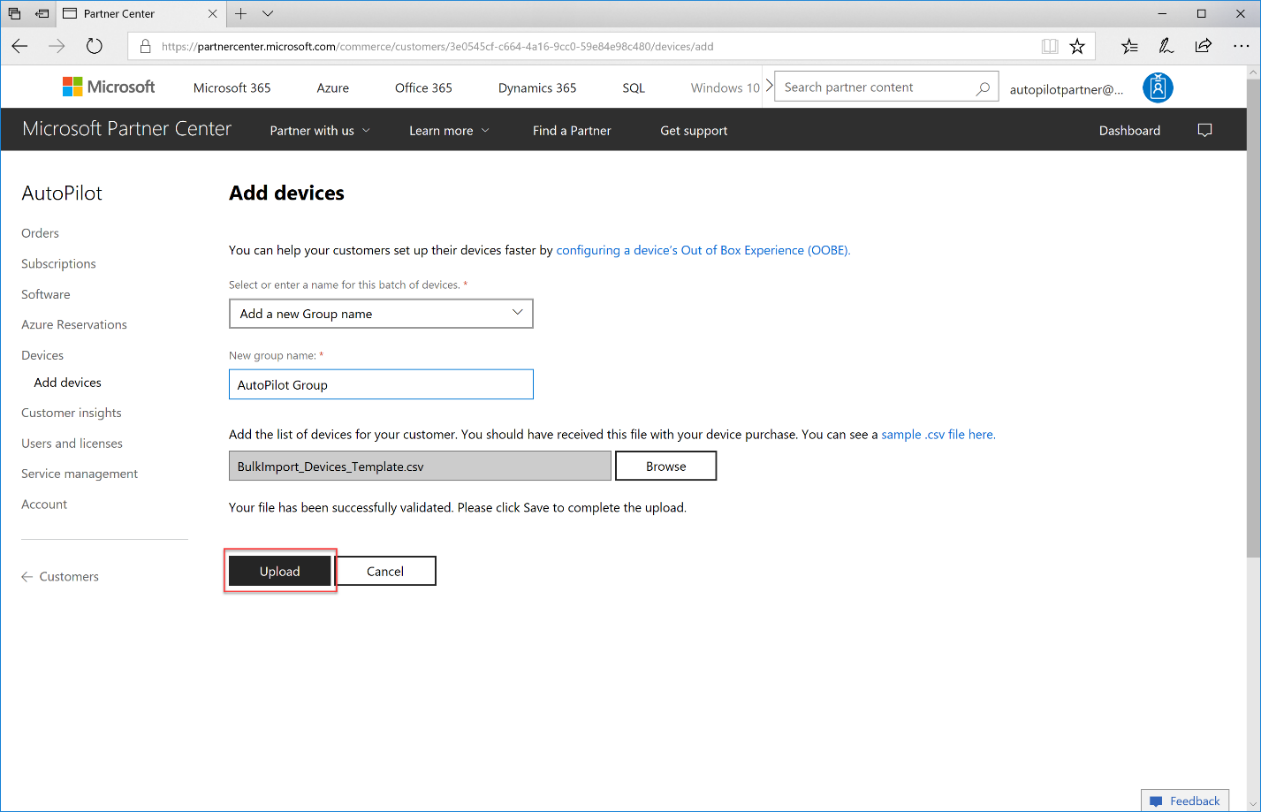


Note: if you want to use Excel, then please make sure that you have column a proper formatted, need to be a 12 digit number!!





To add the devices via a CSV file, follow these steps:

1. Open your customer account in the Partner Center from the **Customers** tab.  
   
2. From **Devices**, select **Add devices**.  
   
3. Name the batch of devices that you are adding or select from an existing group.  
   
4. Click **Browse** to locate the CSV file containing the list of device serial numbers to be added. Click **Open** to select the CSV file.  
   
5. Click **Upload** to upload the CSV file and register the devices. It may take some time for the devices to be validated and registered to the account, please provide up to 30 minutes for this process to complete and for devices to appear in the list of registered devices under the account.  
   

When naming device groups during registration, you can assign names based on the convention or groups that best suit your scenario. For example, the group name can be used to record each invoice as those devices are registered, the PO on which the devices were ordered, or a name for a larger initiative. For example, if the deployment is a refresh of devices in the accounting department and will include small batches fulfilled intermittently over an extended period of time, for example over the summer, the group name could be **Accounting Summer Refresh**.

If you encounter errors uploading your CSV file, the Partner Center will produce an **errors** CSV file that you can analyze to determine the cause of failure, often due to formatting or missing data.

**Note:** Devices that are registered by the partner in the Partner Center will be visible to the customer in AAD, Intune, and Microsoft Store for Business. A partner can de-register these devices using the partner center and is so able to offer new automated services around this ( like break-and-fix services for instance )

Devices that are registered by the customer, for example through Microsoft Store for Business, do not appear in Partner Center and cannot be configured through the Partner Center for AutoPilot. As a consequence a partner has no control over these devices and cannot offer new automated services offers for theses devices.

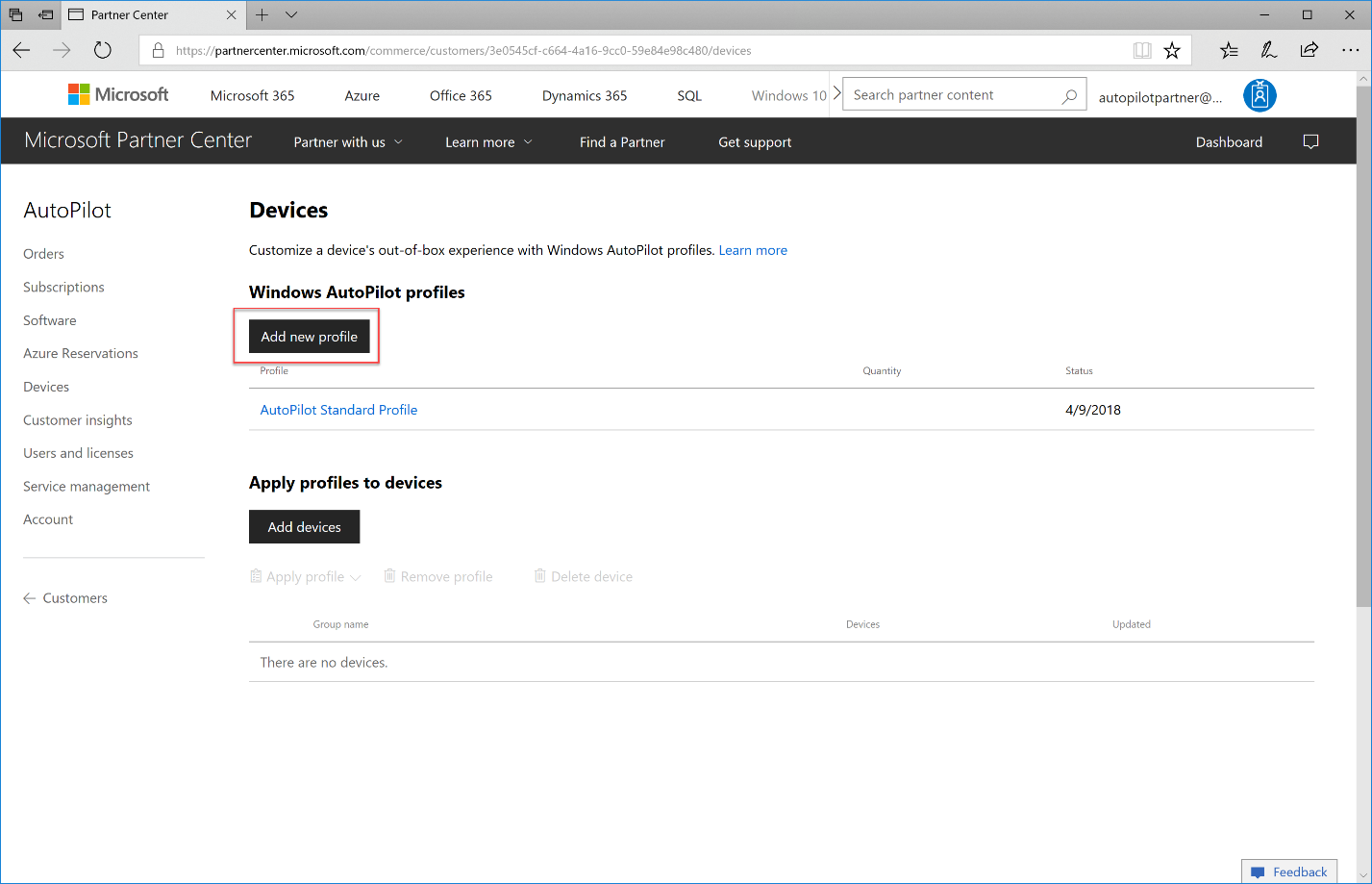
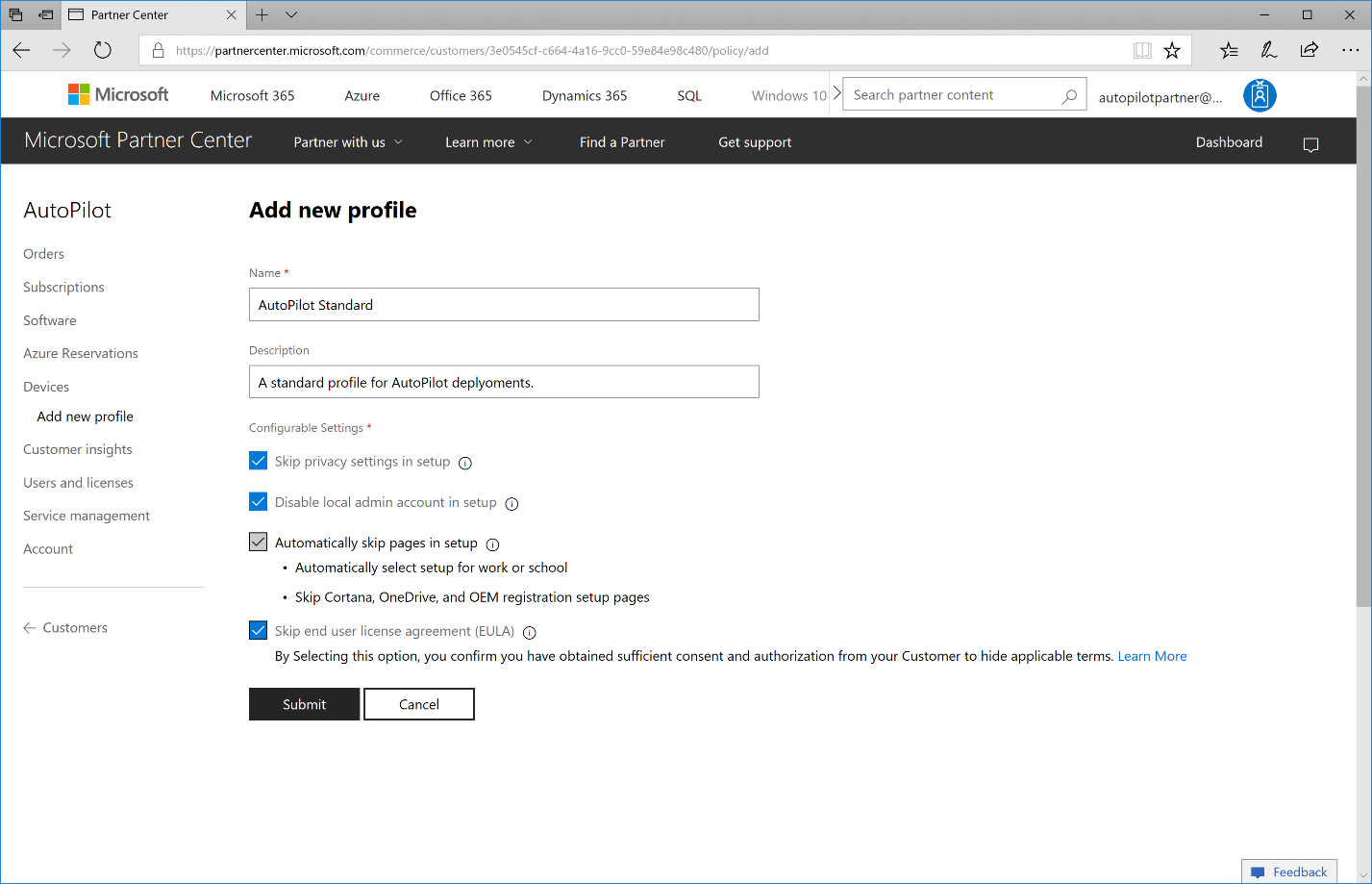
Configuring the devices registered by the partner with policies, apps, and settings must be done in the customer’s management tools, for example the Azure Portal, Intune, or Microsoft Store for Business.

## Creating and Managing AutoPilot Profiles

An *AutoPilot profile* is a collection of settings used to configure a device during a Windows AutoPilot deployment. This AutoPilot profile can be created by the organization where devices are being deployed, or by the partner on behalf of their customers. It contains the tenant information for joining an organizations’ AAD environment, which is automatically populated when you add devices to a customer through the Partner Center, as well as settings for automating OOBE. A list of available settings for AutoPilot profiles is available at the [Overview of Windows AutoPilot](https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-10-autopilot).

Note that the AutoPilot profile allows automation of most aspects of OOBE, but does not automate or suppress the pages for specifying your language and keyboard, or for connecting to WiFi. The user must first proceed through these settings to join the device to a network in order to provide connectivity to the AutoPilot service. Prompts to configure Windows Hello and PIN that occur after OOBE are also still presented to the user.

To configure settings as a partner on behalf of your customer from the Partner Center:

1. Open your customer account in the Partner Center from the **Customers** tab.
2. From **Devices**, click **Add new profile**.   
   
3. Name the profile. for example, **AutoPilot Standard Profile** as shown in the example.  
   
4. Configure the OOBE settings. For example, check **Skip privacy settings in setup** to disable the telemetry and privacy settings page in OOBE. Note that the checkbox for **Automatically skip pages in setup** is checked by default for all Windows AutoPilot deployments.
5. Click **Submit** to save the profile.

**Note:** AutoPilot profiles created in the Partner Center will be visible to the customer in the Microsoft Store for Business and Microsoft Intune, however profiles created by the customer in the Microsoft Store for Business and Microsoft Intune will not be visible to the partner in Partner Center.

## Applying an AutoPilot Profile to Devices

1. Open your customer account in the Partner Center from the **Customers** tab.
2. From **Devices**, in the **Assign and delete devices** pane, select the devices that you want to configure. To select an entire batch, click the checkbox next to the batch name.
3. Click **Apply profile** and select the AutoPilot profile. The devices will then show the AutoPilot profile name in the **Profile** column.

After registering devices, creating a new profile, and applying that profile to devices it is recommended to test the configuration on a device to ensure OOBE is properly managed according to your AutoPilot profile configuration.

## How to remove a device from Windows AutoPilot Enrollment

If Windows AutoPilot deployment is no longer desired for a device, you can remove the AutoPilot profile assigned via the Partner Center with the following steps:

1. Open your customer account in the Partner Center from the **Customers** tab.
2. From **Devices**, in the **Assign and delete devices** pane, select the devices that you want to configure. To select an entire batch, click the checkbox next to the batch name.
3. Click **Remove profile.** The devices will then show the AutoPilot profile name of **None** in the **Profile** column.

If the device is no longer owned by the customer organization, the device or batch can be deleted from the customer altogether with the **Delete** option.

## Microsoft Intune, Azure Active Directory, and Windows AutoPilot

Devices that are registered as organization-owned by partners in the Partner Center will appear in the organizations Azure Portal, however the devices will not appear in Microsoft Intune until the device has proceeded through Windows AutoPilot deployment and been enrolled automatically in MDM. Once the device has completed auto-enrollment, it can be managed like any other device in Microsoft Intune. Management of policies, deployment of apps, etc. will deploy to the device according to the user profile logged in. See the [Microsoft Intune documentation](https://docs.microsoft.com/en-us/intune/) at Microsoft Docs for more information.

You can also use Microsoft Intune to enroll devices in Windows AutoPilot and to register devices as organization owned. You can find instructions at Enroll Windows devices by using the [Windows AutoPilot Deployment Program documentation](https://docs.microsoft.com/en-us/intune/enrollment-autopilot) from the Microsoft Intune section of the Microsoft Docs library.

## Managing Devices Not Supported for OEM Enrollment

Support for enrollment in Windows AutoPilot by serial number, device model, and manufacturer name is provided by the manufacturer of the device. Providing this support requires that the device manufacturer take steps during the manufacturing process to harvest the hardware hash value for each device. These values are then provided to the Windows AutoPilot enrollment service and are matched with a device when that device is registered to fill in the missing hardware hash value.

This solution is the ideal scenario for Windows AutoPilot enrollment as it results in a seamless experience where devices can be enrolled in Windows AutoPilot without even needing to open the box prior to the user receiving the device. There are, however, many devices for which this process will not be supported, including Surface devices that are manufactured with Windows 10 Version 1703 or earlier and devices from OEMs that have not yet enabled support for the enrollment by serial number, device model, and manufacturer name.

## Pegging Orders for Windows AutoPilot

To ensure the ideal experience for customers who are ordering new devices and intending to deploy with Windows AutoPilot, it is necessary that the customers’ orders are filled with devices where this support is provided by the manufacturer. In the case of Surface devices, this means that Windows AutoPilot orders must be filled with devices manufactured with Windows 10 Version 1709 or above, which began shipping from the factory in January 2018.

To ensure that Surface devices you order as a partner from Microsoft or from your distributor meet this requirement, the order must be *pegged* as an order for Windows AutoPilot. This process is done manually by adding a note to the order identifying the order as a Windows AutoPilot order. It is also necessary that the distributor filling your order supports the pegging of orders for Windows AutoPilot. Support for pegging orders is a requirement for partners listed on the [Windows AutoPilot for Surface devices](https://www.microsoft.com/en-us/itpro/surface/windows-autopilot-for-surface) page. This mechanism is also supported for all orders filled by Microsoft directly.

Ensuring that the devices filling your customers’ orders meet this requirement is the responsibility of the partner. When devices are used to fill your customers’ orders that do not meet this requirement, harvesting of the hardware hash from each device is required.

## Harvesting Hardware Hashes for Partner Center import

**Note:** If you plan to import devices from which you are harvesting the hardware hash via **Get-WindowsAutoPilotInfo** via the Partner Center, use the **-Partner** switch to generate a CSV with the appropriate fields.

# Resources

What is device management in Azure Active Directory?

<https://docs.microsoft.com/en-us/azure/active-directory/devices/overview>

Windows Autopilot

[https://www.microsoft.com/en-us/windowsforbusiness/windows-Autopilot](https://www.microsoft.com/en-us/windowsforbusiness/windows-autopilot)

Windows Autopilot Prerequisites

[https://docs.microsoft.com/en-us/windows/deployment/windows-Autopilot/windows-10-Autopilot#prerequisites](https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-10-autopilot#prerequisites)

Autopilot Network Connectivity Requirements

[https://docs.microsoft.com/en-us/windows/deployment/windows-Autopilot/windows-10-Autopilot#network-connectivity-requirements](https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-10-autopilot#network-connectivity-requirements)

Windows 10 Activation

<https://docs.microsoft.com/en-us/windows/deployment/windows-10-enterprise-subscription-activation>

Windows Autopilot Deployment

<https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices>

Windows Autopilot Video Tutorial

<https://www.youtube.com/watch?v=Hb4V7uaqEm4>

Azure Run-book automation

<https://www.powershellgallery.com/packages/Get-WindowsAutopilotInfo/1.3/DisplayScript>

Download the PS Script [https://www.powershellgallery.com/packages/Get-WindowsAutopilotInfo/](https://www.powershellgallery.com/packages/Get-WindowsAutoPilotInfo/)

Autopilot Automation

[https://rzander.azurewebsites.net/automatically-register-existing-device-in-Autopilot/](https://rzander.azurewebsites.net/automatically-register-existing-device-in-autopilot/)

Overview of Windows Autopilot

[https://docs.microsoft.com/en-us/windows/deployment/windows-Autopilot/windows-Autopilot](https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot)

## Troubleshooting Autopilot

[Troubleshooting Windows Autopilot (level 100/200)](https://blogs.technet.microsoft.com/mniehaus/2017/12/13/troubleshooting-windows-autopilot-level-100200/)

[Troubleshooting Windows Autopilot (level 300/400)](https://blogs.technet.microsoft.com/mniehaus/2017/12/13/troubleshooting-windows-autopilot-level-300400/)

[Troubleshooting Improvements in Windows Autopilot](https://blogs.technet.microsoft.com/mniehaus/2018/05/15/troubleshooting-improvements-in-windows-autopilot/)

# Appendix: Additional Capabilities

Appendix I includes a list and description of “a la carte” options for layering on additional capabilities and scenarios to the base POC.

[**Surface Diagnostic Toolkit (SDT) for Business**](https://docs.microsoft.com/en-us/surface/surface-diagnostic-toolkit-business)

The Microsoft Surface Diagnostic Toolkit for Business (SDT) enables IT administrators to quickly investigate, troubleshoot, and resolve hardware, software, and firmware issues with Surface devices. You can run a range of diagnostic tests and software repairs in addition to obtaining device health insights and guidance for resolving issues.

[**Windows Update for Business**](https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb)

Windows Update for Business enables information technology administrators to keep the Windows 10 devices in their organization always up to date with the latest security defenses and Windows features by directly connecting these systems to Windows Update service. You can use Group Policy or MDM solutions such as Intune to configure the Windows Update for Business settings that control how and when Windows 10 devices are updated. In addition, by using Intune, organizations can manage devices that are not joined to a domain at all or are joined to Microsoft Azure Active Directory (Azure AD) alongside your on-premises domain-joined devices. Windows Update for Business leverages diagnostic data to provide reporting and insights into an organization's Windows 10 devices.

**Windows Store for Business**