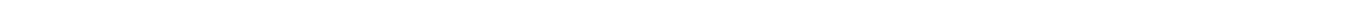




Windows Autopilot Cookbook for Surface devices

Deployment Guide for CSP Partners

Last updated: February 27, 2023



This documentation is confidential and proprietary information of Microsoft Corporation, provided for internal and partner use, for informational purposes only. Microsoft makes no warranties, either express or implied, in this document.

© 2023. Microsoft Corporation. All rights reserved.

Contents

- Introduction 1
 - Autopilot prerequisites..... 1
 - Network connectivity requirements..... 2
 - CSP Microsoft Partner Center requirements 2
 - Get started as a CSP 2
 - Requesting a Customer Relationship..... 3
- Register Surface devices to Autopilot 4
 - CSP partner submits Autopilot registration to Microsoft Support..... 4
 - CSP partner registers Autopilot devices via Microsoft Partner Center 5
 - Format of .csv registration file 6
 - Language dependencies 7
 - Customer self-registers Autopilot devices via Intune..... 9
- Prepare Surface devices for Autopilot..... 10
 - Reset current in-market devices to OOBE..... 10
 - Reset earlier Surface devices to OOBE..... 10
- Prepare Azure demo tenant 11
 - Create demo tenant from CDX 11
 - Select demo user 11
- AAD and Intune setup 13
 - Configure automatic MDM enrollment..... 13
 - Configure company branding..... 13
 - Create Azure AD Group for all new Autopilot devices..... 15
 - Configure Autopilot deployment profile 16
- Intune device configuration..... 19
 - Device profiles 19
 - Enable the enrollment status page..... 21
 - Deploy software – Microsoft 365 Apps 22
 - Windows edition upgrade 24
 - Assign devices to users 26
- End-user experience - Autopilot with Surface 28

DFCI - Intune management of Surface UEFI settings.....	29
Prerequisites.....	29
Configure DFCI management for Surface devices.....	29
Manually Sync Autopilot devices.....	29
Remove devices from Windows Autopilot Enrollment.....	30
Check device registration status in Intune.....	30
Reset devices and deregister from Autopilot.....	31
Reset the device to OOBE.....	31
Deregister the device from Windows Autopilot.....	31
Customer deregisters device via Endpoint Manager.....	32
Partner deregisters device via Microsoft Partner Center.....	32
Return and exchange scenarios.....	33
Prepare devices for repair.....	34
Step 1: Remove devices from Autopilot and DFCI.....	34
Device retirement and deletion.....	34
Step 2: Reset UEFI to enable boot from USB to reimage.....	34
UEFI password prompt.....	34
Unable to change settings or revert settings in UEFI.....	34
Step 3: Enroll device into Autopilot and DFCI to restore previous state.....	35
Appendix.....	36
Generate hardware hash with PowerShell script.....	36
Create and manage Autopilot profiles in MPC.....	37
Configure settings as a partner on behalf of your customer from MPC.....	37
Apply an Autopilot profile to devices in MPC.....	39
Manage devices not supported for OEM enrollment.....	39
Order Specific OS Versions for Windows Autopilot customers.....	39
Learn more.....	41

Introduction

Traditionally, IT pros spend a lot of time building and customizing images that will later be deployed to devices with a perfectly good operating system. Windows Autopilot uses various technologies to set up and configure Windows devices in a zero-touch deployment approach. This enables IT departments to configure and customize images using cloud resources instead of maintaining their own infrastructure. When users first receive a Surface device, they must connect to a network and verify their credentials. Everything after that is fully automated. Windows Autopilot enables IT admins to achieve the following tasks:

- 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 by ensuring the first person who logs into Windows is configured as a standard user.
- Create and auto-assign devices to configuration groups based on a device profile.
- Customize the OOBE (Out of Box Experience) introductory text and branding for the customer's organization.
- Enable the complete configuration of the device using Intune.
- Reset or restart devices remotely.

TIP: Review the [Windows Autopilot FAQ](#), which provides OEMs, partners, administrators, and end users with answers to frequently asked questions about deploying Windows with Autopilot.

To learn more, see: [What is Partner Center? - Partner Center | Microsoft Learn](#).

Autopilot prerequisites

Autopilot requires a Microsoft 365 Enterprise environment in Intune.

Requirement	Description
Azure Active Directory Premium	Required to enroll your devices in your organization and 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 and configure and manage your enrolled devices.
Microsoft 365 Apps for enterprise (Optional)	Microsoft 365 Apps, formerly Office Pro Plus, must include Microsoft Office in your deployment to your enrolled devices.
Windows devices with Windows 10 RS3 1709 or higher	Devices must leave the factory with a minimum version of Windows 10 RS3/1709. Devices manufactured after January 2018 should meet this requirement.

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

License	Description	Learn more
Microsoft 365 E3 or E5	Includes Azure Active Directory Premium, Intune, and Microsoft 365 Apps for enterprise	Compare Microsoft 365 Enterprise plans
Enterprise Mobility Security E3 / E5	Includes Azure Active Directory Premium and Intune	Enterprise Mobility and Security Pricing Options
Microsoft 365 Apps for enterprise E3 or E5	Includes Microsoft 365 Apps for enterprise	Microsoft 365 Apps for enterprise

Network connectivity requirements

Ensure users connect to their corporate network during the OOB setup. The Windows Autopilot Deployment Program uses cloud services that 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>
- ctldl.windowsupdate.com
- download.windowsupdate.com

IMPORTANT: Where not explicitly specified, both HTTPS (443) and HTTP (80) must be accessible. If you're auto-enrolling your devices into Intune or deploying Microsoft Office, follow the networking guidelines for [Intune](#) and [Office 365](#).

CSP Microsoft Partner Center requirements

This guide is intended for [Cloud Solution Providers \(CSPs\)](#) with access to the [Microsoft Partner Center](#). The following roles are also supported:

- **Indirect CSP resellers** can get direct authorization from customers to register devices through the Partner Center UI (manually uploading a .csv file).
- **Indirect CSP provider partners** (distributors) can register devices through the Partner Center UI with an additional option to register devices using the [Microsoft Partner Center APIs](#).
- **Microsoft Partner Center (MPC)** users with Admin Agent permissions.

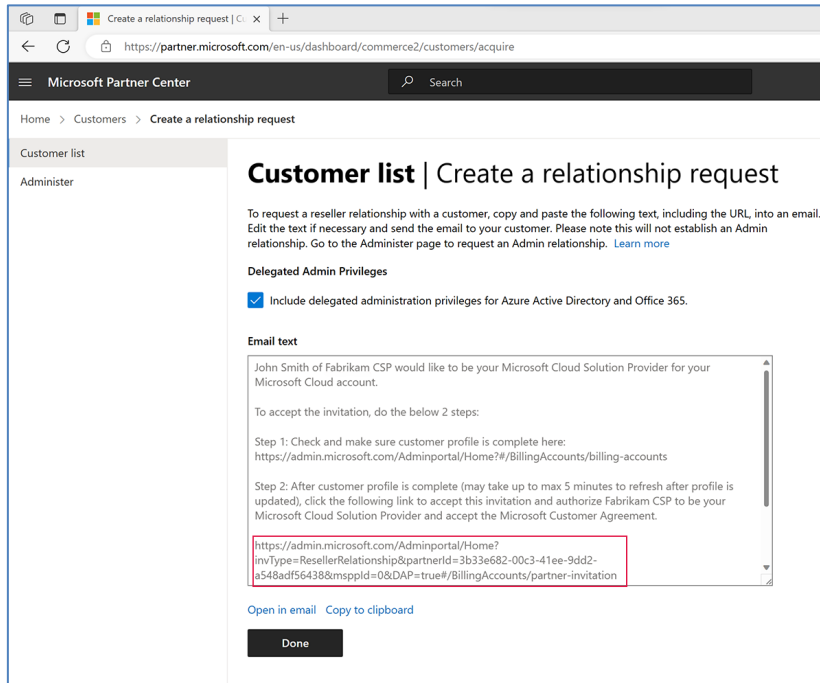
Get started as a CSP

We recommend partners interested in offering Microsoft 365 modern manageability services such as Windows Autopilot investigate the steps needed to become a Microsoft CSP. To learn more, refer to the [Microsoft Cloud Solution Provider landing page](#). You can start by becoming an Indirect Reseller and working with your Indirect Provider to sell licenses and services.

Requesting a Customer Relationship

Enrolling devices into Autopilot on behalf of a customer requires establishing a relationship with that customer in Microsoft Partner Center.

1. Copy the text from the following figure and email it to the PoC tenant administrator to request a relationship. This text includes a link, as highlighted in the following figure:



2. To register and deregister devices to Autopilot, the customer needs to authorize you as a reseller for their account. This can be done in two ways: With or without delegated admin privileges. Ensure you to ask the customer which of these requests you should send.
3. If the customer does not want delegated admin privileges, clear the following checkbox: **Include delegated administration privileges for Azure Active Directory and Office 365**. Regardless of delegated admin rights, you can still register and deregister devices on the customer's AAD tenant.
4. If the customer needs additional permissions - for example, to manage AAD, M365, Intune, or related services -- select **Include delegated administration privileges for Azure Active Directory and Office 365**. To learn more, refer to [request a relationship with a customer](#).

Register Surface devices to Autopilot

To deploy Surface devices using Windows Autopilot, register hardware IDs (HW IDs) to the Autopilot service via one of the following methods:

- [CSP partner submits Autopilot registration to Microsoft Support](#)
- [CSP partner registers Autopilot devices via Microsoft Partner Center](#)
- [Customer self-registers Autopilot devices via Intune](#)

As shown in the table below, supported features vary by Autopilot registration method.

Features	Microsoft Surface registration	CSP partner registration	Self-registration
Device Firmware Configuration Interface (DFCI) support	Yes	Yes	No. Devices manually or self-registered for Autopilot, such as those imported from a CSV file, aren't allowed to use DFCI. By design, DFCI management requires external attestation of the device's commercial acquisition via a Microsoft CSP partner or Surface registration.
Partner Center support	Yes	Yes	No. CSP partners cannot manage self-registered devices in Partner Center.
Surface device support	All eligible Surface devices	Surface devices produced after January 2018.	All eligible Surface devices running Windows 10 1903 or later
Deregister support	Yes	Yes. Registration and deregistration require the customer to authorize CSP as a reseller, as described in Requesting a Customer Relationship .	Yes

CSP partner submits Autopilot registration to Microsoft Support

Microsoft Support has a simplified process of registering Surface devices for Windows Autopilot deployment. Customers and CSPs can register Surface devices by [submitting requests to Microsoft Support](#). This is the recommended method of registering devices, especially if you encounter issues with the self-serve methods via MPC or Intune. To learn more, see [Surface Registration Support for Windows Autopilot](#).

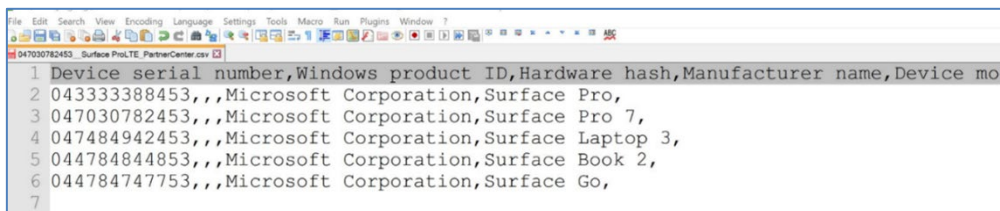
Required information for Autopilot registration requests to Microsoft Support

Required information	Description	Autopilot Registration	Hardware Hash Request	Autopilot Deregistration
Azure Active Directory Tenant ID	Your Azure Active Directory tenant ID is a globally unique identifier (GUID) different from your organization's name or domain. To find your Tenant ID, sign in to the Azure Portal here .	Y	N	Y
Azure Active Directory Domain Name	Your top-level domain name, for example, contoso.com.	Y	N	Y
Proof of ownership	Verify proof of ownership by uploading the original bill of sale or invoice in PDF format. Screenshots are not accepted. The bill of sale or invoice must include the following: - Device serial numbers. - Company name.	Y	Y	Y
Device serial numbers	Upload the Excel file in .csv format with each device serial number in a new line.	Y	Y	Y

CSP partner registers Autopilot devices via Microsoft Partner Center

Microsoft Surface devices can be registered by device resellers (with active CSP partner status) as part of the ordering process. Partners must already have established business relationships with customers. The following information is required.

- Serial number of the device
- Microsoft Corporation as the OEM name
- Device model



```

1 Device serial number,Windows product ID,Hardware hash,Manufacturer name,Device model
2 043333388453,,Microsoft Corporation,Surface Pro,
3 047030782453,,Microsoft Corporation,Surface Pro 7,
4 047484942453,,Microsoft Corporation,Surface Laptop 3,
5 044784844853,,Microsoft Corporation,Surface Book 2,
6 044784747753,,Microsoft Corporation,Surface Go,
7

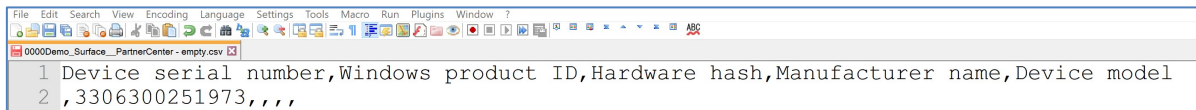
```

For the official device model names, refer to [Surface System SKU reference](#).

NOTE: The registration process can also be automated using [Microsoft Partner Center APIs](#).

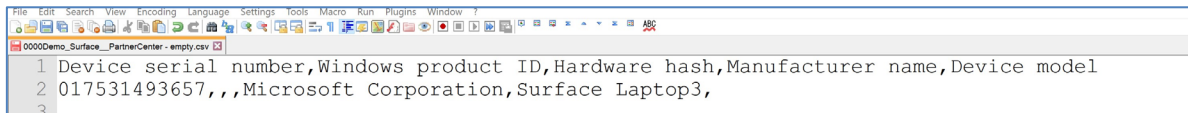
Before applying an Autopilot profile to a device, you must add any new devices not already enrolled in Azure AD or your MDM solution.

1. To register devices using MPC, submit a .csv file containing specific device information, as shown below. Note that this .csv includes all possible fields, including the hardware hash of the device. Ideally, you only need to fill out the *Windows product ID (PKID)* column.



```
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
0000Demo_Surface_PartnerCenter - empty.csv
1 Device serial number,Windows product ID,Hardware hash,Manufacturer name,Device model
2 ,3306300251973,,,,,
```

2. If the product ID is unknown, you can use a convenient alternative method for Surface devices. Fill out a tuple for each device with these three items:
 - Serial number
 - Manufacturer Name
 - Device Model



```
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
0000Demo_Surface_PartnerCenter - empty.csv
1 Device serial number,Windows product ID,Hardware hash,Manufacturer name,Device model
2 017531493657,, ,Microsoft Corporation,Surface Laptop3,
3
```

TIP: This registration step can already occur early in the device procurement process, sometimes as early as devices arrive at the partner location and often before the order is assembled for shipping to the customer.

Establishing practices to allocate and isolate Windows Autopilot orders is recommended, allowing the collection of the product ID (PKID) and serial numbers before their registration and enrollment in Windows Autopilot.

Format of .csv registration file

The .csv file must contain the following elements to register devices:

- The first line is always the header -- line, comma separated: Hardware Hash, Manufacturer Name, Device Model.
- Device Serial Number – obtained from the box sticker or the ordering or purchasing process, such as the invoice or shipping label.
- Windows Product ID – for new Surface devices, this is obtained from the sticker on the box; for the future, this is the preferred option for Surface and OEM devices.
- Hardware Hash – optional for Surface – not needed for the partner center registration.
- Manufacturer Name – for Surface devices, this would-be Microsoft Corporation.
- Device Model – For Surface device model names, see Surface System SKU reference. Or you can run MSInfo32.

Also, ensure that each device line ends with a comma and that you have five commas per line.

Example:

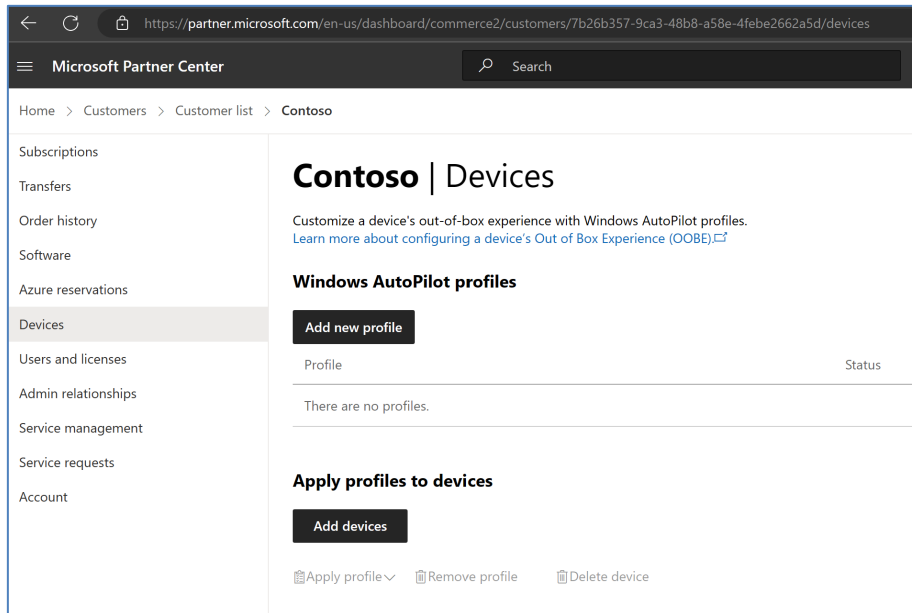
```
0000Demo_Surface_PartnerCenter-M365x876051.csv
1 Device serial number,Windows product ID,Hardware hash,Manufacturer name,Device model
2 017531493657,,,,Microsoft Corporation,Surface Laptop 3,
3
4
```

Language dependencies

IMPORTANT: For international partners, be aware that the header of the .csv file is UI language dependent. We recommend you use Notepad to view and edit the .csv file. If you want to use Excel for the .csv file creation, please ensure your columns are correctly formatted (you need to use a 12-digit number).

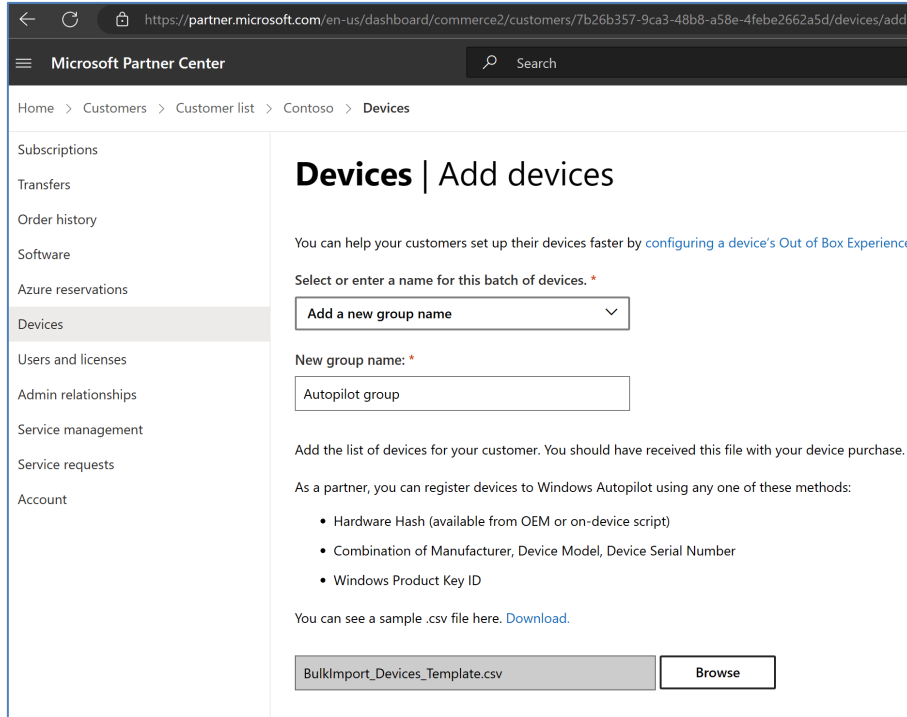
To register devices using a .csv file:

1. Sign in to [MPC](#).
2. Open your customer account from the Customers tab.
3. Under Devices, select **Add devices**.

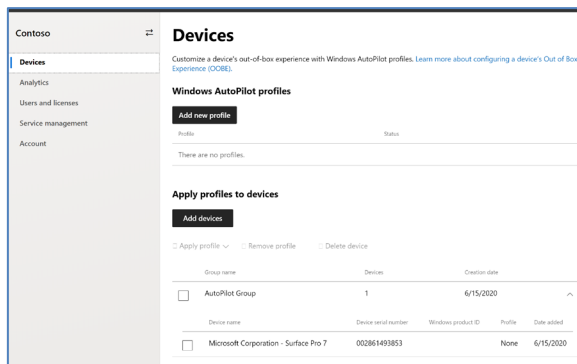


NOTE: Skip the Windows Autopilot profiles option in favor of configuring profiles in the customer's MDM system, which is the appropriate location to manage policies, app deployment, and related features.

4. Name the batch of devices you add or select from an existing group.
5. Select **Browse** to locate and open the .csv file containing the list of device serial numbers to be added.



6. Select **Upload** to upload the .csv file and register the devices. Provide up to 30 minutes for this process to complete and for devices to appear in the list of registered devices under the account. Once the file is uploaded, you will see the device in your customer's devices list.



You can assign names based on the convention or groups that best suit your scenario. For example, the group name can 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, suppose the deployment is a refresh of devices in the accounting department and will include small batches fulfilled intermittently over an extended period, for example, over the summer. In that case, 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" to help determine the cause of failure, often due to formatting or missing data.

NOTE: Devices that the partner registers in the Partner Center will be visible to the customer in AAD, Intune, and Microsoft Store for Business. A partner can deregister these devices using the Partner Center and offer new

automated services around this (like break-and-fix services).

Devices 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. Consequently, a partner cannot control these devices and offer new automated services.

Customer self-registers Autopilot devices via Intune

Customers can use [Microsoft Endpoint Manager](#) and Intune to enroll devices in Windows Autopilot and register the devices as organization owned. To learn more, refer to the [Windows Autopilot Deployment Program documentation](#). (Note, however, that this document focuses on interacting with the Microsoft Partner Center. The Intune registration is more appropriate for testing purposes.)

NOTE: The .csv file format in Intune differs from the .csv file format used for the MPC registration approach.

With Intune, a .csv file containing the hardware IDs of the POC Surface devices needs to be uploaded:

```
1 Device Serial Number,Windows Product ID,Hardware Hash,Order Id
2 017242554153,,T0HqAwEAHAAAAoAAQDuQgAACgD+AO5CyXeFI3gCCQMCABAACQABAAIABAABAAAABQAZAAQAAAAAA
```

Prepare Surface devices for Autopilot

- Ensure your Surface device is in an OOB state.
- Before the Surface device returns to the network, its Hardware ID must be registered to the Autopilot service.

Devices registered in Autopilot as organization-owned initially appear in the organization's Azure Portal. Once devices are deployed with Autopilot and enrolled automatically in the MDM tool, the devices will appear in Intune. They can be managed like any other device on Intune. Policies and apps will deploy to the device according to the user profile logged in. To learn more, refer to the [Intune documentation](#).

TIP: To check the OS version of the device, open a command prompt and enter `winver`. If the device is booting into OOB, enter +F10 for a command prompt. The OS version is printed as a barcode label on the shipping box for current in-market Surface Devices.

Reset current in-market devices to OOB

1. Fully update the device using **Windows Update**. Reboot the device.
2. Sign in with an **Admin account**.
3. Open the **Settings** app and select **Update & Security > Recovery**. Under **Reset this PC**, select **Get started** and choose **Remove everything**.
4. When the reset process is completed, the first OOB screen appears.

Reset earlier Surface devices to OOB

- Apply a recovery image following the instructions on the [Surface Recovery Image Download](#) page.

To demonstrate the client-side experience of Windows Autopilot, use a device running Windows 10/11 Pro, Enterprise, or Education SKUs. (Windows 10/11 Home does not support Autopilot.)

Prepare Azure demo tenant

Create demo tenant from CDX

You can create a new demo tenant as a Microsoft partner by visiting <https://CDX.transform.microsoft.com>.

Sign in with your partner credentials and select **My Environment > My Tenants > Create tenant**, and then choose your preferences:

1. Select **Quick Tenant** to get a tenant without waiting for it to be provisioned.
2. Choose a period: 90 days.
3. Select **tenant location**: your preferred location.
4. Choose **Microsoft 365 Enterprise Demo content** and select **Create tenant**.

The screenshot shows the 'Create a Tenant' page in the CDX portal. It includes a progress indicator for four steps: 1. Select type (Quick Tenant selected), 2. Select period (90 days selected), 3. Select tenant location (Europe, Middle East, Africa selected), and 4. Select your content packs. Under step 4, two content packs are listed: 'Microsoft 365 Business Demo Content' and 'Microsoft 365 Enterprise Demo Content', each with a 'Create Tenant' button. A 'Current Environment Limits' box in the top right shows 90-day tenants at 0 of 1, 1-year tenants at 0 of 1, and custom tenants at 0 of 1.

5. Note the **tenant name** and **access details** for the administrator and user.

The screenshot shows the 'Create Tenant' page with the details for a newly created tenant. The tenant name is 'M365x335790'. The content pack is 'M365 Enterprise', location is 'Europe, Middle East, Africa', and period is '90 days'. The expiration date is '1/4/20' and the status is 'Completed'. The content add-ons section shows 'No add-on applied'. The Admin Details section shows the password, admin name, and email.

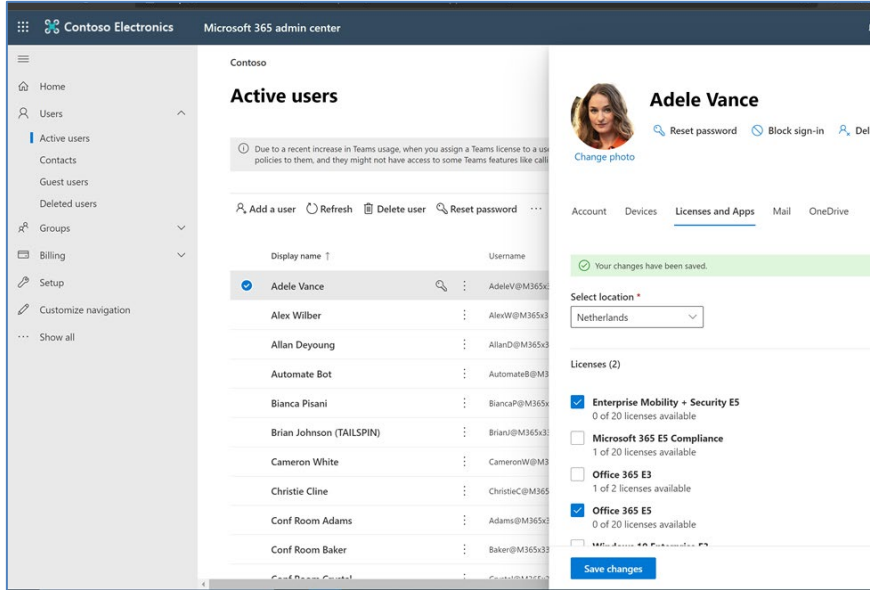
Select demo user

1. Sign in to your demo tenant as administrator to <https://admin.microsoft.com>, select **Users > Active Users** and choose a user.

2. Select Licenses and Apps and select the following:

- Enterprise Mobility + Security E5
- Office 365 E5

Save Changes.

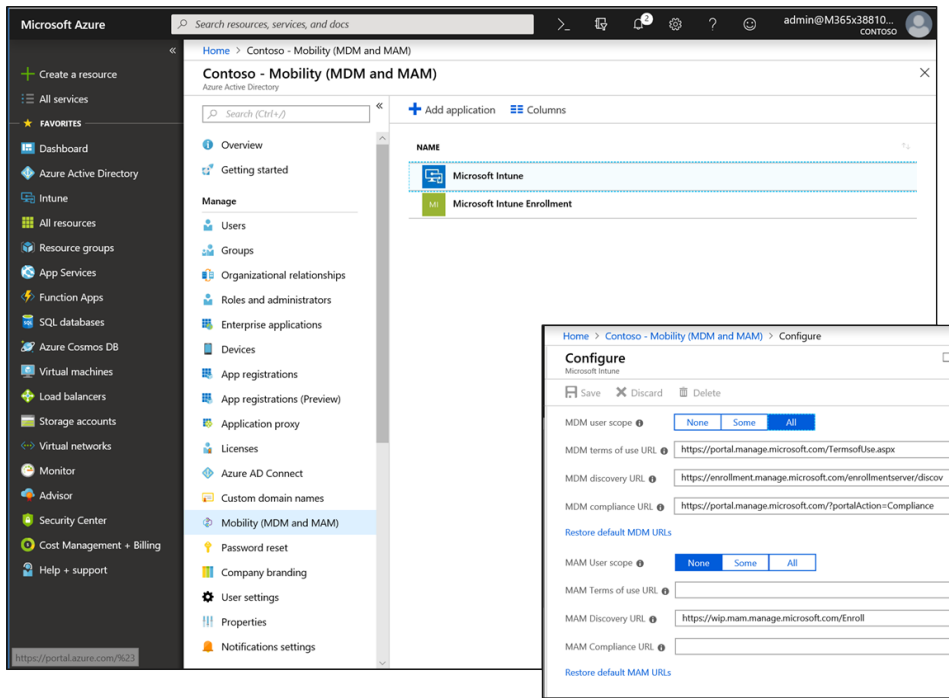


AAD and Intune setup

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

Configure automatic MDM enrollment

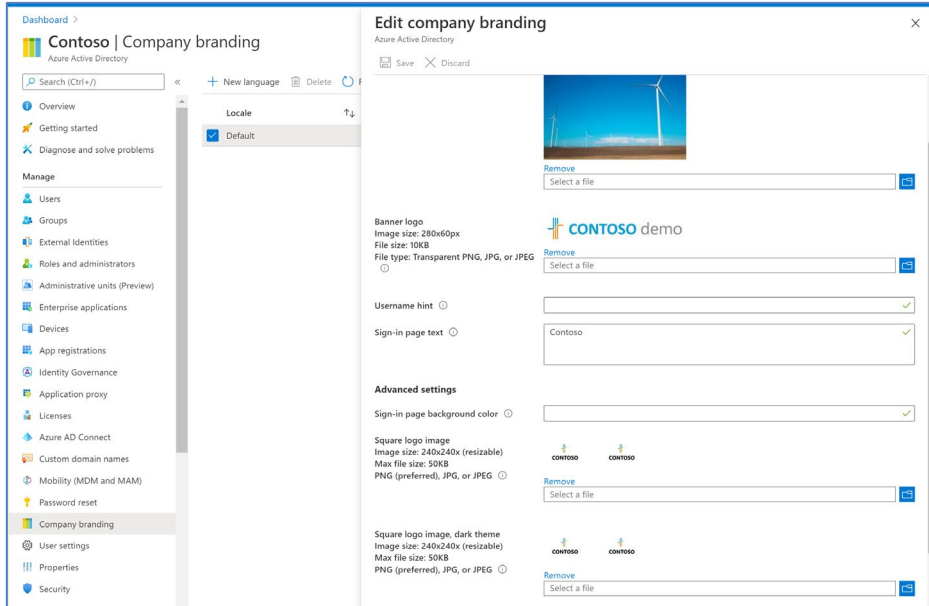
1. Sign in to <https://portal.azure.com> using the admin credentials provided for the tenant and enable MDM for all POC users.
2. Navigate to **Azure Active Directory > Mobility (MDM and MAM) > select Microsoft Intune** and ensure **ALL** is selected under MDM user scope. Repeat this for Intune Enrollment as well.



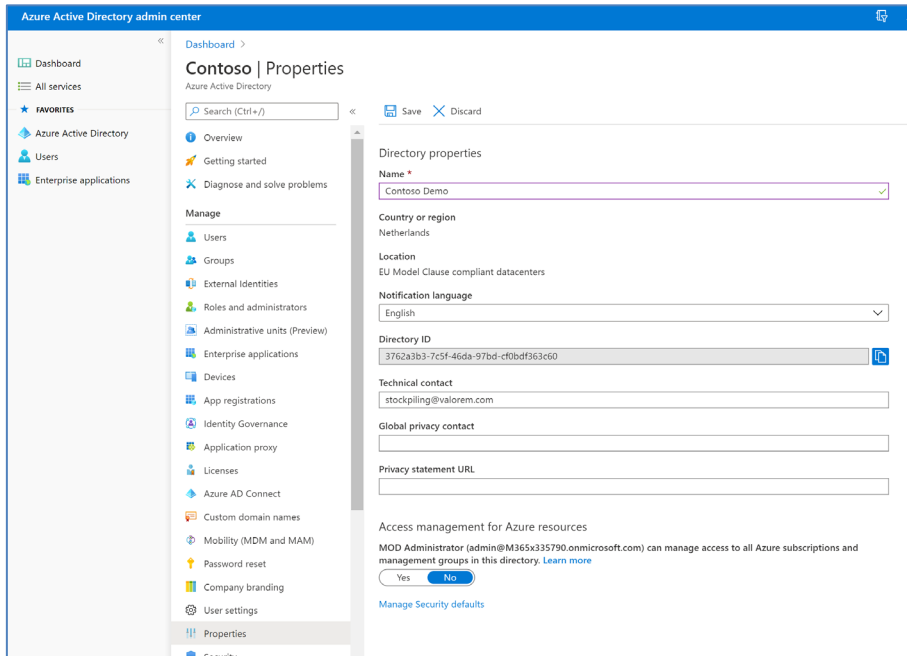
Configure company branding

For your company branding to appear during OOB, you must configure it in Azure Active Directory. For more information, see [Add company branding to your directory](#). The following branding settings are required: Background image, Banner logo, Square logo, and Square logo dark.

1. Select **Azure Active Directory > Company branding > Edit**.



- To adjust the tenant name displayed during OOB, open Azure Active Directory > Properties > Name and select Save.



Create Azure AD Group for all new Autopilot devices

Create an Azure AD group that all new devices automatically join to use Autopilot.

1. Go to <https://endpoint.microsoft.com> > **Groups** and select **+New group**.

Microsoft Endpoint Manager admin center

Home > Groups | All groups >

New Group

Group type *
Security

Group name * ⓘ
Autopilot New Devices

Group description ⓘ
Autopilot New Devices Group

Membership type * ⓘ
Dynamic Device

Owners
No owners selected

Dynamic device members * ⓘ
Add dynamic query

2. Make it a **Security Group**, name it **Autopilot New Devices**, and add a description (optional). Under **Membership type**, choose **Dynamic Device** and select **Add dynamic query**.

Microsoft Endpoint Manager admin center

https://endpoint.microsoft.com/#view/Microsoft_AAD_IAM/AddGroupBlade

All services > Groups | All groups >

New Group

Got feedback?

Group type * ⓘ
Security

Group name * ⓘ
Autopilot New Devices

Group description ⓘ
All new devices to automatically join to use Autopilot

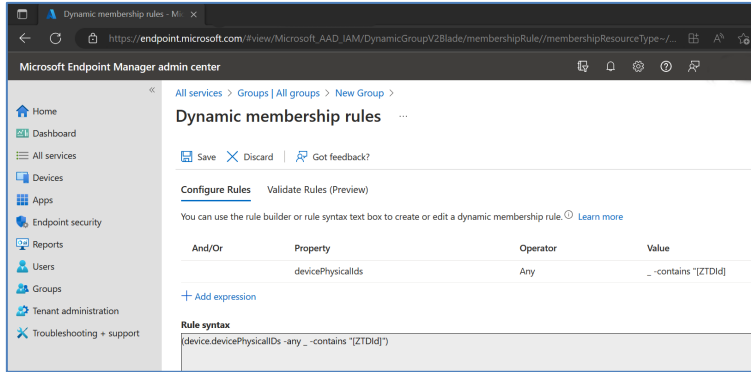
Azure AD roles can be assigned to the group ⓘ
Yes No

Membership type * ⓘ
Assigned
Assigned
Dynamic User
Dynamic Device

No members selected

Create

3. Select **Edit dynamic query**, select **Edit** (see top right of Rule syntax box), and enter the following rule syntax:
(device.devicePhysicalIDs -any _ -contains "[ZTDId]")
4. Select **OK** and then choose **Save**.

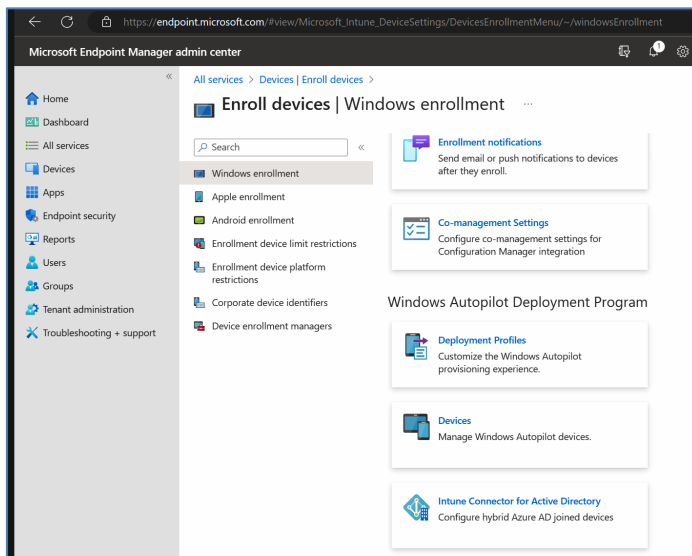


5. On the New Group page, select **Create**. All devices subsequently registered to Autopilot for this tenant will be members of this group. Refer to the section below to assign profiles and settings to the group.
6. To assign profiles and settings to an individual device, add it to the **Autopilot New Devices** group.

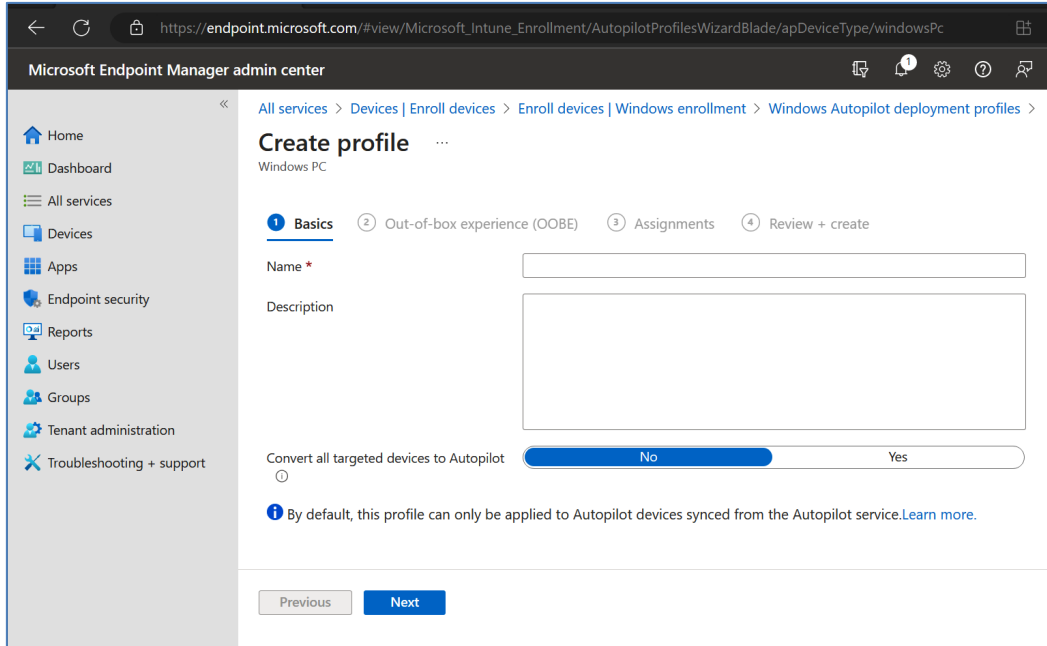
Configure Autopilot deployment profile

An Autopilot deployment profile is a collection of settings used to configure a device during Windows Autopilot deployment. The Autopilot profile allows automation of most aspects of OOBЕ but does not let you skip pages specifying language and keyboard or connecting to Wi-Fi. Users must first join the device to a network to provide connectivity to the Autopilot service. Prompts to configure Windows Hello and PIN that occur after OOBЕ are also still presented to the user.

1. Go to <https://endpoint.microsoft.com> > **Devices** > **Enroll devices** and ensure Windows enrollment is selected and choose **Deployment Profiles**.

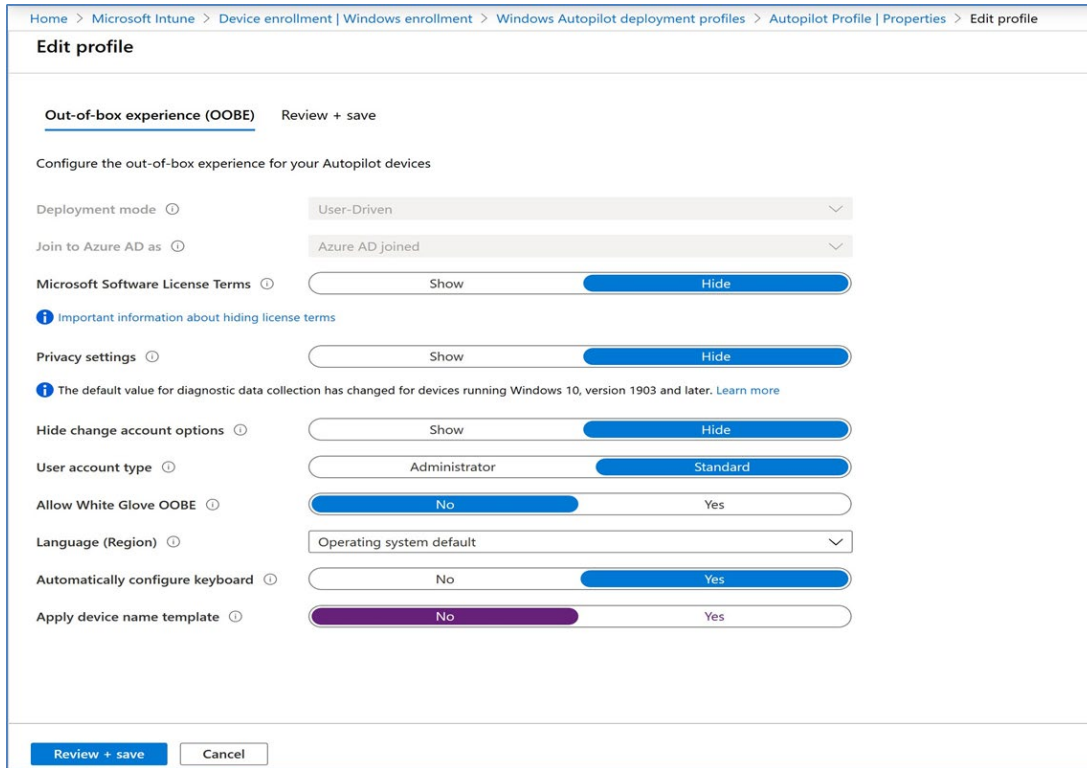


2. Select **Create profile** and choose **Windows PC**. Or, if you use the CDX prepopulated tenant, you can select the already configured Autopilot Profile settings.
3. On the **Basics** screen, name the profile **Autopilot Profile**, add a description (optional), and then select **Next**.

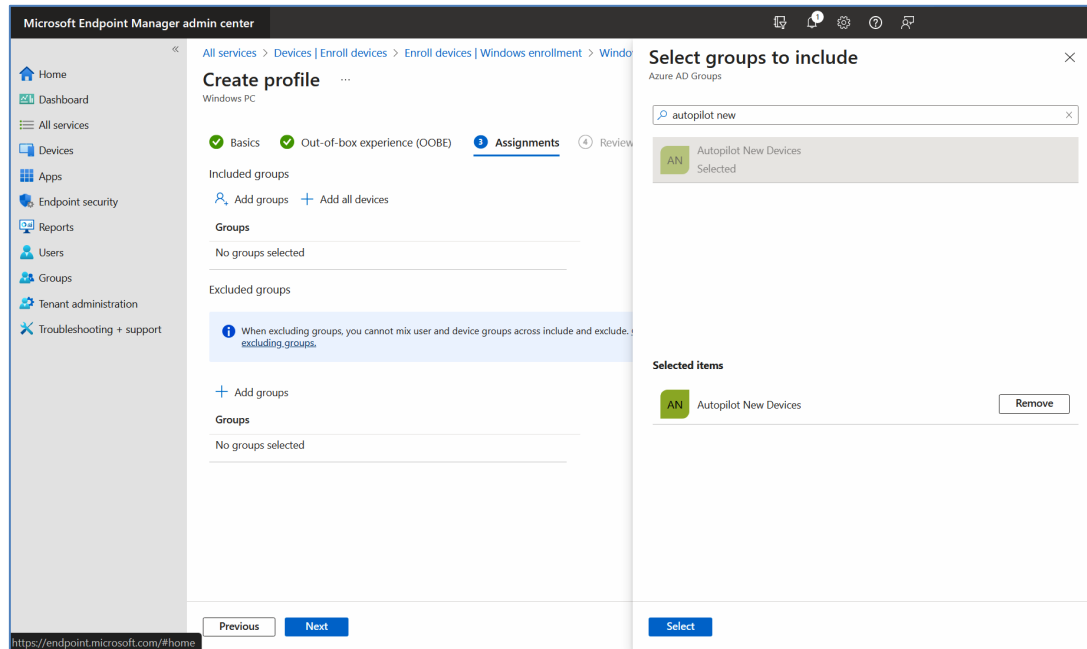


4. On the OOBE page, you will configure a User-Driven deployment mode.
5. Accept the default recommended settings, as shown in the following table.

Policy	Recommended setting (default)
Deployment mode	User-driven
Join to Azure AD	Azure AD joined
Microsoft Software License Terms	Hide. These settings will not be shown to end users.
Privacy settings	Hide. These settings will not be shown to end users.
Hide change account options	Hide. These settings will not be shown to end users.
User account type	Standard. This limits end users to standard privileges on the computer and prevents them from becoming local admins on the device.
Allow pre-provisioned deployment	No. This scenario does not use pre-provisioned deployment (formerly known as white glove), which allows you to speed up the OOBE experience.
Language [Region]	Keep the language as OS default.
Automatically configure keyboard	Leave the keyboard to auto-config based on the region selection.
Apply device name	No



6. Select **Next** and assign this profile to the dynamic group **Autopilot New Devices** you [created earlier](#).



7. Choose **Select** and **Next**.

8. On the **Review + Create** page, check your settings, and select **Create**.

Intune device configuration

Device profiles

A device profile allows you to add and configure settings that can be deployed to enrolled devices across your organization. When devices receive the device profile, the features and settings are applied automatically. Examples of standard device profiles include Email, Device restrictions, VPN, Wi-Fi, and Administrative templates. Intune has settings and features you can enable or disable on different devices within your organization. These settings and features are managed using profiles.

1. Navigate to <https://endpoint.microsoft.com> > **Devices** > **Configuration profiles** and select **+Create profile**.
2. For the **Platform**, choose **Windows 10 and later**.
3. Under **Profile type**, choose **Templates** > **Device restrictions** > **Create**.
4. On the **Basics** page, name the profile **Win10-DeviceConfig-Restrictions** and select **Next**.

TIP: Using the CDX prepopulated system, you can review and edit the existing profile and select Configuration settings.

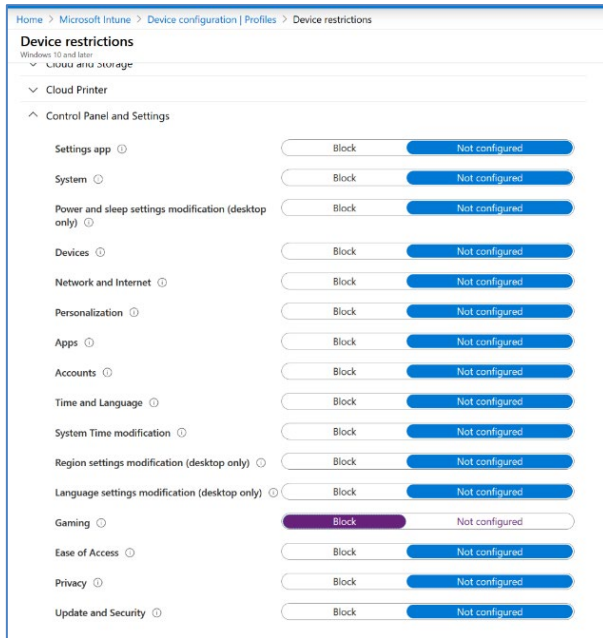
5. Review the available configuration settings, select **Start**, and configure some settings.

The screenshot shows the 'Device restrictions' configuration page in the Intune console. The page is titled 'Device restrictions' and is for 'Windows 10 and later'. It lists various settings that can be configured. The 'Block' and 'Not configured' options are shown as buttons next to each setting. The 'Switch Account' setting is currently set to 'Block'.

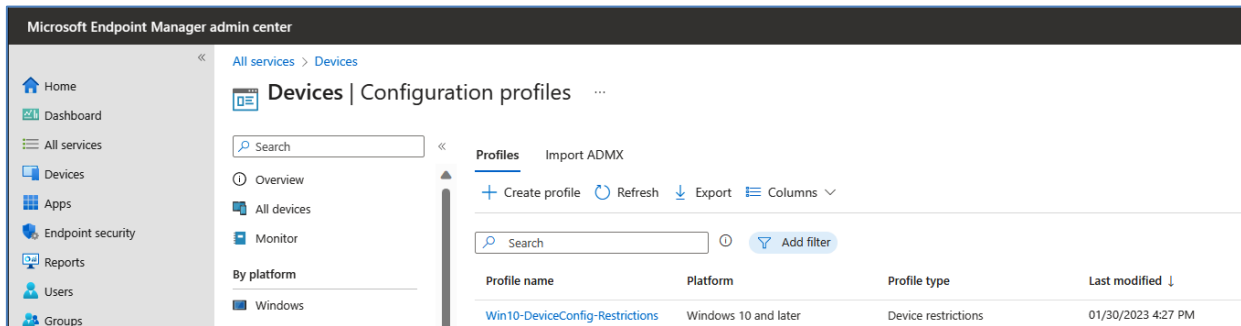
Setting	Block	Not configured
Power button	<input type="radio"/>	<input checked="" type="radio"/>
User Tile	<input type="radio"/>	<input checked="" type="radio"/>
Lock	<input type="radio"/>	<input checked="" type="radio"/>
Sign out	<input type="radio"/>	<input checked="" type="radio"/>
Shut Down	<input type="radio"/>	<input checked="" type="radio"/>
Sleep	<input type="radio"/>	<input checked="" type="radio"/>
Hibernate	<input type="radio"/>	<input checked="" type="radio"/>
Switch Account	<input checked="" type="radio"/>	<input type="radio"/>
Restart Options	<input type="radio"/>	<input checked="" type="radio"/>
Documents on Start	<input type="radio"/>	<input type="radio"/>
Downloads on Start	<input type="radio"/>	<input type="radio"/>
File Explorer on Start	<input type="radio"/>	<input type="radio"/>
HomeGroup on Start	<input type="radio"/>	<input type="radio"/>
Music on Start	<input type="radio"/>	<input type="radio"/>
Network on Start	<input type="radio"/>	<input type="radio"/>
Personal folder on Start	<input type="radio"/>	<input type="radio"/>
Pictures on Start	<input type="radio"/>	<input type="radio"/>
Settings on Start	<input type="radio"/>	<input type="radio"/>
Videos on Start	<input type="radio"/>	<input type="radio"/>

At the bottom of the page, there are two buttons: 'Review + save' and 'Cancel'.

6. Open **Control Panel and Settings** and block **Gaming**.



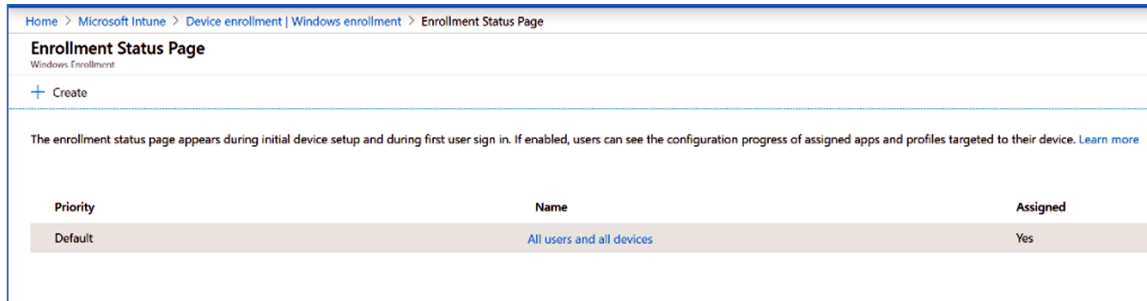
7. Select **Next** (twice), then under **Assignments**, choose **All users and devices**, select **Next** (twice), and select **Create** after reviewing the settings. Your profile's Initial Configuration will be displayed on your list of profiles:



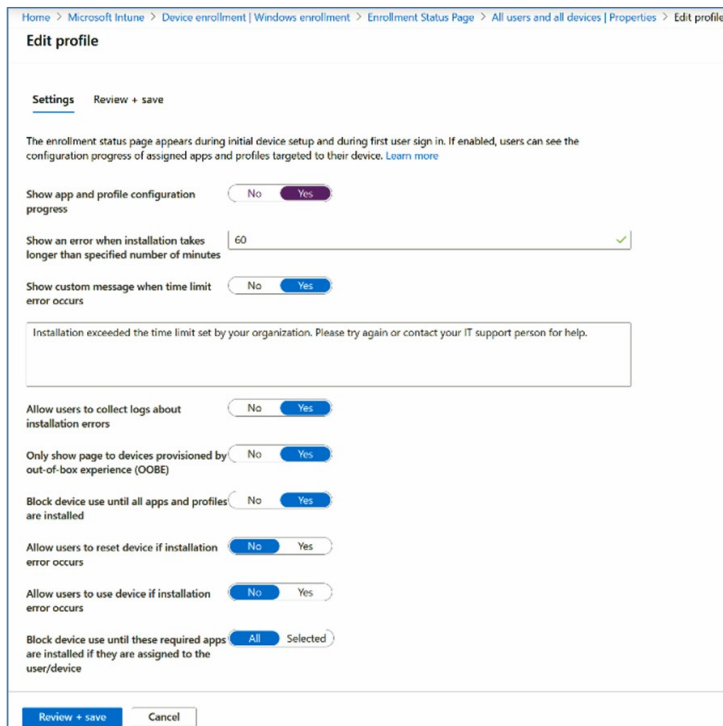
Enable the enrollment status page

You can configure an enrollment status page to appear during the initial device setup and first user sign-in, allowing users to see the progress of assigned apps and profiles targeted to their device.

1. [Endpoint Manager](https://endpoint.microsoft.com) (https://endpoint.microsoft.com) and select **Devices > Enroll Devices > Windows Enrollment > Enrollment Status Page**. On the default ESP page, select **All users and all devices**.



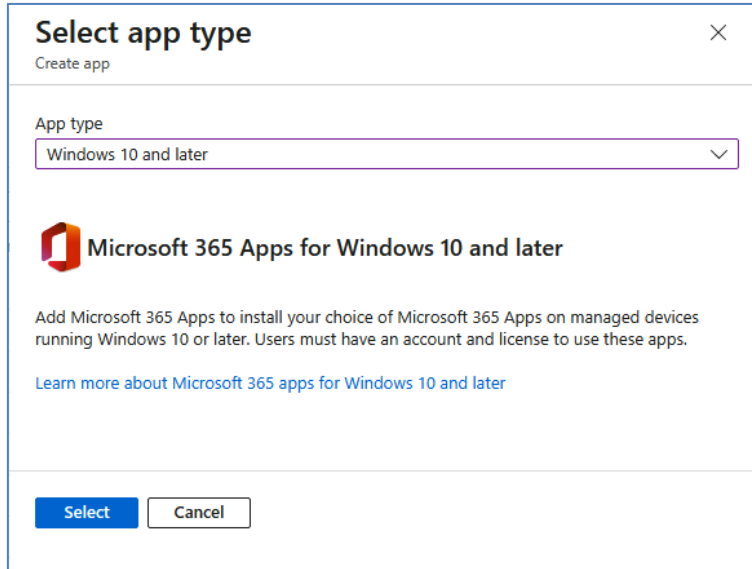
2. Select **Properties > Settings > Edit**, select **Yes** to **Show app and profile installation progress**, and retain the default values for the other settings.



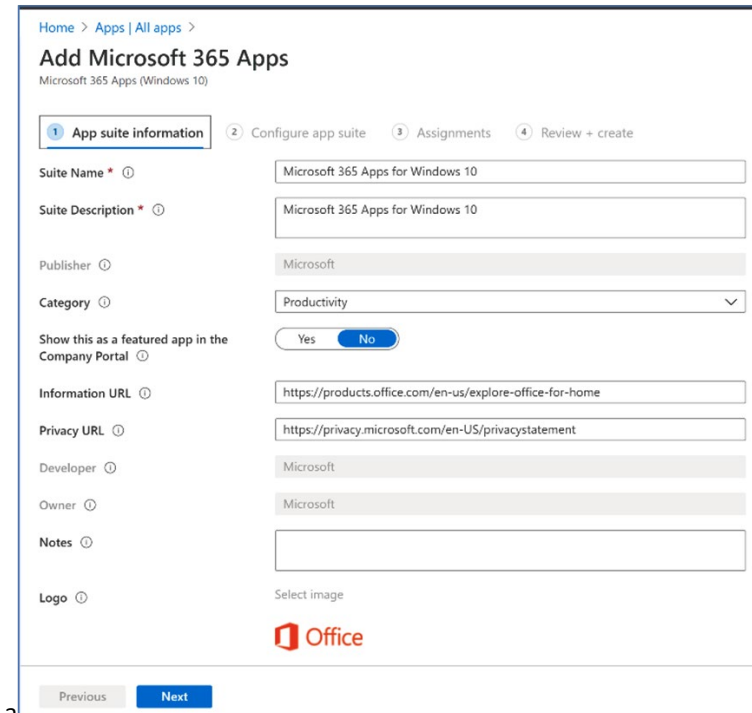
3. Select **Review + Save** to store the settings. This default ESP is then assigned to **All users and devices**.

Deploy software – Microsoft 365 Apps

1. Open [Endpoint Manager](https://endpoint.microsoft.com) (<https://endpoint.microsoft.com>) and navigate to **Apps > All Apps** and select **+Add**.
2. In **Select app type**, under **Microsoft 365 Apps**, choose **Windows 10 and later > Select**.



3. In the **Add Microsoft 365 Apps** pane, select **Next** on the App Suite information screen:



a

- On the Configure app suite, choose **Select Office apps**, and make your choice:

Microsoft Endpoint Manager admin center

Home > Apps | All apps >

Add Microsoft 365 Apps

Microsoft 365 Apps (Windows 10 and later)

App suite information
 Configure app suite
 Assignments
 Review + create

Configuration settings format *

Configure app suite

Select Office apps

Select other Office apps (license required)

App suite information

These settings apply to all apps you have selected in the suite. [Learn more](#)

Architecture

Default file format *

Update channel *

Remove other versions

Version to install

Specific version

Properties

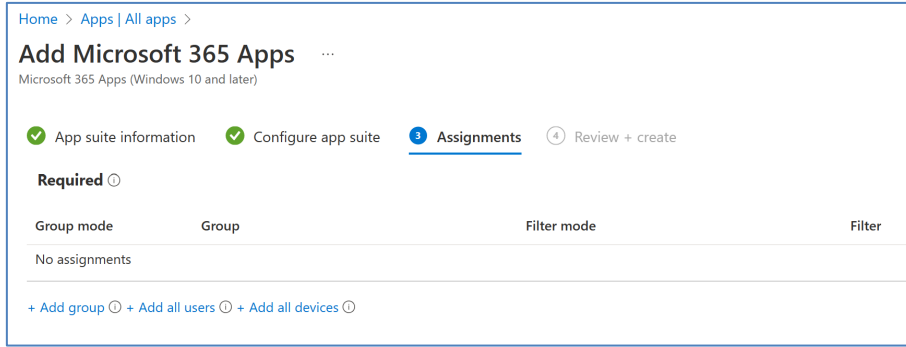
Use shared computer activation

Accept the Microsoft Software License Terms on behalf of users

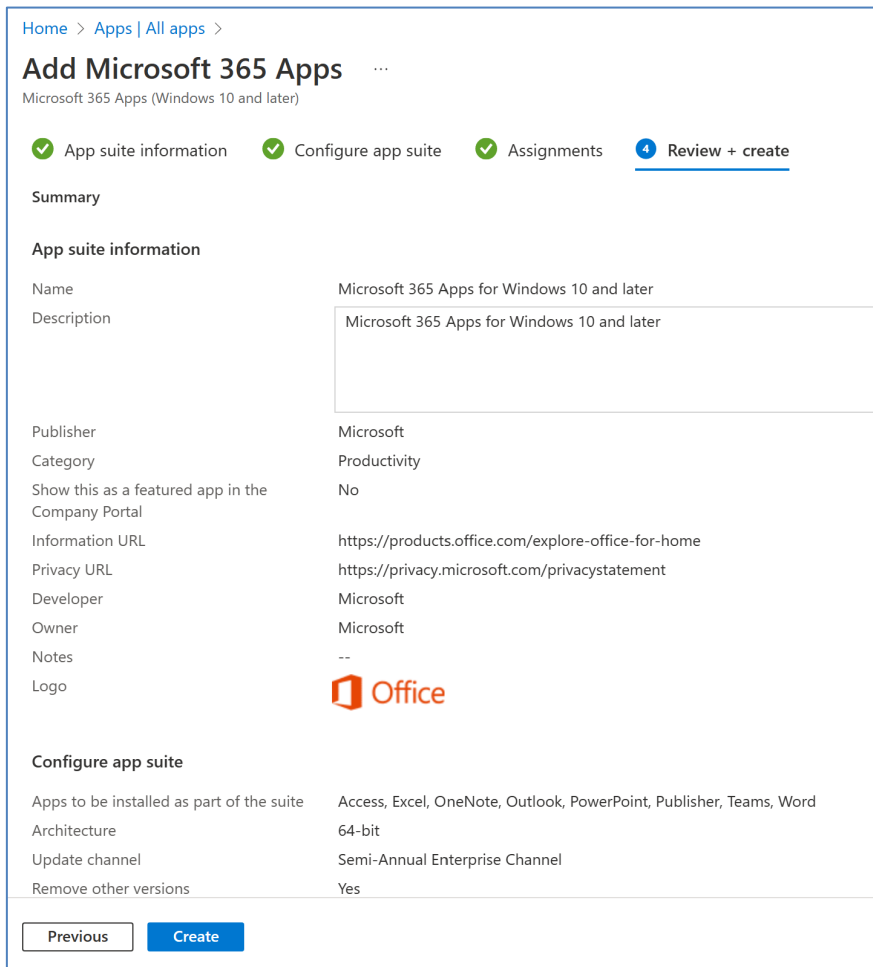
Install background service for Microsoft Search in Bing

Languages

- Leave the architecture as **64-bit**. For Default file format, select **Office Open Document Format**. For Update channel, choose **Semi-Annual Enterprise Channel**.
- For **Accept the Microsoft Software License Terms on behalf of users**, ensure **Yes** is selected.
- Retain defaults for all other settings and select **Next**.
- On the Assignment Page, select **+Add all users**.



9. Select **Next**, review your settings and then select **Create**.



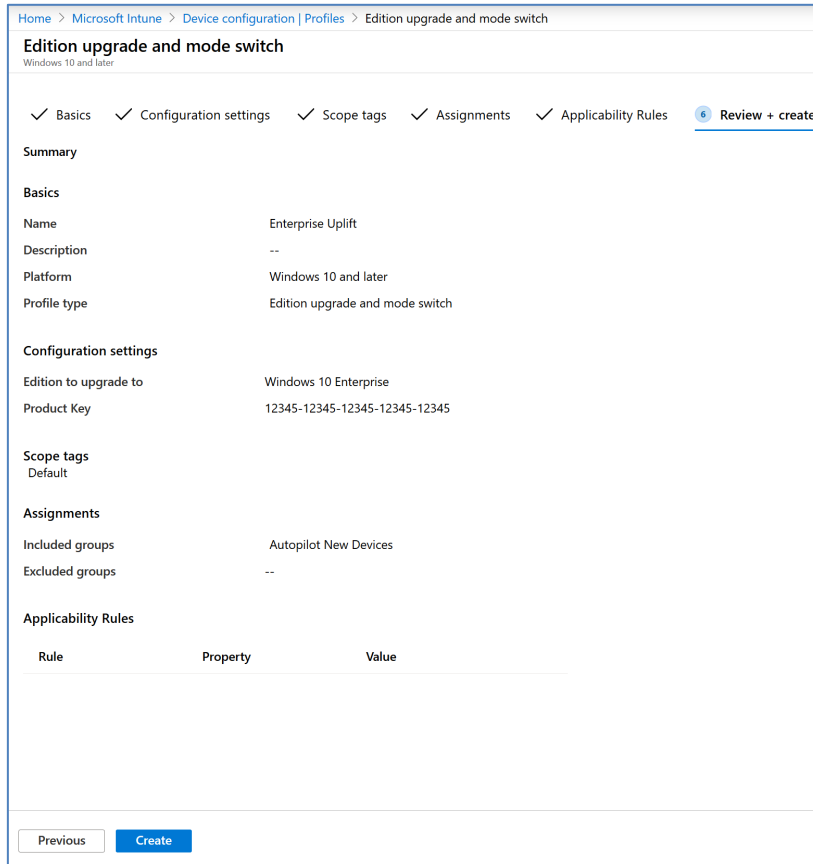
Windows edition upgrade

You can upgrade the factory-installed operating system to Windows 11 Enterprise as part of the automated provisioning process. For users with M365 E3 or E5 licenses, upgrading occurs automatically when the user (with the license assigned) logs in for the first time. For others, you must create a new profile and assign it to all users.

1. Open [Endpoint Manager](https://endpoint.microsoft.com) (<https://endpoint.microsoft.com>) and select **Devices > Configuration profiles > Create profile**.

2. For Platform, select **Windows 10 and later**. For profile, select **Templates > Edition upgrade and mode switch**.
3. Select **Create**, name the new profile **Enterprise Uplift**, and select **Next**.
4. Under the Configuration Settings pane, select **Edition Upgrade > Windows 10/11 Enterprise** and enter the required Product Key.
5. Select **Next > Next >** and assign the profile to your **Autopilot New Devices Group**.

6. Select **Next** to review the settings and then select **Create**.

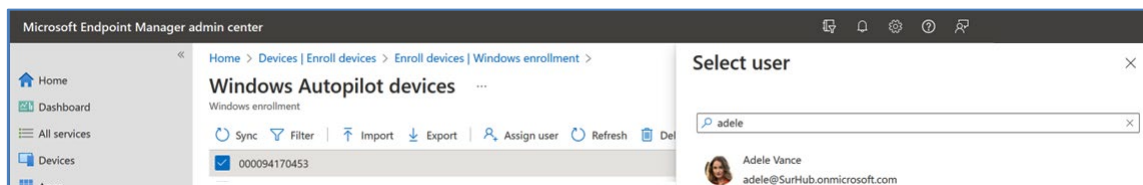


7. On the Assignments page, select **Required** on **+Add all users**. M365 apps are assigned to all users.
8. Select **Next** and then select **Create**.

Assign devices to users

You can assign a specific user to a device. This can help create a customized user experience and remove the need to input their corporate username (as it is captured automatically during the setup process). This capability can be initiated once the device is registered with your tenant as part of the Windows Autopilot service.

1. Go to <https://endpoint.microsoft.com> > **Devices** > **Enroll devices**. Under the Windows Autopilot Deployment Program, select **Devices** and select the device you wish to assign to a specific user.



2. Select the device and then select **Assign user**. Choose the target end-user in the user list. Example: **AdeleV**.
3. Check the properties and then select **Save**.

017531493657 - Properties
Windows Intune/MDM Devices

User
AdeleV@M365a876051.ChMicrosoft.com

User Friendly Name

Serial number
017531493657

Manufacturer
Microsoft Corporation

Model
Surface Laptop 3

Device Name

Group Tag

Profile status
Assigned

Assigned profile
Autopilot Profile

Date assigned
5/05/20, 8:51 PM

Enrollment state
Not enrolled

Associated Intune device
N/A

Associated Azure AD device
017531493657

Last contacted
Never

Windows Ink Workspace

End-user experience - Autopilot with Surface

Windows Autopilot with Surface makes life easier for IT, and your users benefit from automation and simplicity. Users will experience the Windows Out-of-box experience (OOBE) when using the device for the first time. With Autopilot, the OOBE experience has been simplified, with the number of screens the user must go through reduced by 75% from the traditional OOBE experience. Users only need their work account credentials. No local admin permissions are required.

NOTE: The provisioning process takes a little time to complete, though it could be longer depending on the number of applications or policy settings deployed as part of the Autopilot process. Once complete, the device is ready for productive use.

TIP: If OOBE fails, it may be due to a registration issue. Ensure devices meet the minimum requirements and are [correctly registered](#). Or in some cases, you may need to wait up to 24 hours or longer for settings data to fully propagate before OOBE can be completed.

To learn more, see [Windows Autopilot User-Driven Mode](#)

DFCI - Intune management of Surface UEFI settings

With Device Firmware Configuration Interface (DFCI) profiles built into Intune, Surface UEFI management extends the modern management stack to the UEFI hardware level. With Intune's integrated UEFI firmware management capabilities, locking down hardware is simplified with new features for provisioning, security, and streamlined updating in a single [Endpoint Manager](#) console.

DFCI on Surface devices¹ enables zero-touch management, eliminating IT admins' need for manual interaction. DFCI is deployed via Windows Autopilot using the device profiles capability in Intune. DFCI is an additional device profile that enables you to manage UEFI configuration settings from the cloud without maintaining on-premises infrastructure.

Prerequisites

- Register devices to Windows Autopilot by a CSP or Microsoft. It is not possible to use DFCI when self-registering via Intune.
- Fulfill the Autopilot requirements, as indicated earlier in this document.
- Add your target Surface devices to an Azure AD security group (Example: 000AllDFCIdevices).

Configure DFCI management for Surface devices

A DFCI environment requires setting up a DFCI profile containing the settings and an Autopilot profile to apply to registered devices. An enrollment status profile is also recommended to ensure settings are pushed down during OOBE setup when users first start the machine.

To get started, follow the instructions in [Manage DFCI on Surface devices](#), which covers the following topics:

- [DFCI policy settings reference for Surface devices](#)
- [Prevent users from changing UEFI settings](#)
- [Verify UEFI settings on DFCI-managed devices](#)
- [Remove DFCI policy settings](#)

Manually Sync Autopilot devices

Although Intune policy settings typically get applied almost immediately, there may be a delay of 10 minutes before the settings affect targeted devices. In rare circumstances, delays of up to eight hours are possible. You can manually sync the target devices to ensure settings apply as soon as possible (in test scenarios).

1. In [Endpoint Manager](#), (<https://endpoint.microsoft.com>), go to **Devices > Device enrollment > Windows enrollment > Windows Autopilot Devices** and select **Sync**.

NOTE: When adjusting settings directly in UEFI, you must ensure the device fully restarts to the standard Windows login.

¹ Surface Go and Surface Go 2 use a third-party UEFI and do not support DFCI. Find out more about managing Surface UEFI settings at <https://docs.microsoft.com/surface/manage-surface-uefi-settings>.

Remove devices 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:

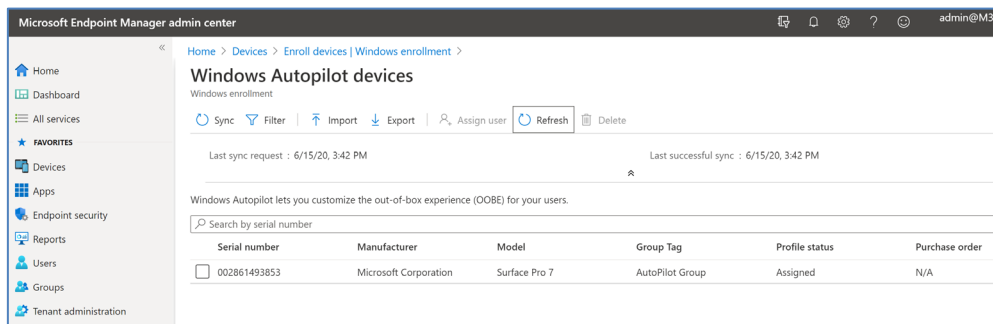
1. Open your customer account in the Partner Center from the **Customers** tab.
2. From Devices, in the **Assign and delete devices** pane, select the devices that you want to configure. To select an entire batch, select the checkbox next to the batch name.
3. Select **Remove profile**. The devices will then show the Autopilot profile name of **None** in the Profile column. If the customer organization no longer owns the device, the device or batch can be deleted from the customer with the **Delete** option.

Check device registration status in Intune

1. Return to the PoC Tenant at <https://endpoint.microsoft.com> > **Devices** > **Enrolled Devices** > **Devices**.
2. Select **Sync** and **Refresh**.

The device you registered in the Partner Center should now appear on the list. Also, note the Group Tag that was chosen in the Partner Center. Check the profile status, which should appear initially as **Not assigned**. The device will be added to the dynamic devices group **New Autopilot Devices** you created earlier. The Autopilot profile will then be assigned to devices in this group.

This is why you get a profile Status that first shows **Updating** and finally **Assigned**. This can take a little while, and while waiting for this to happen, go to the next step.

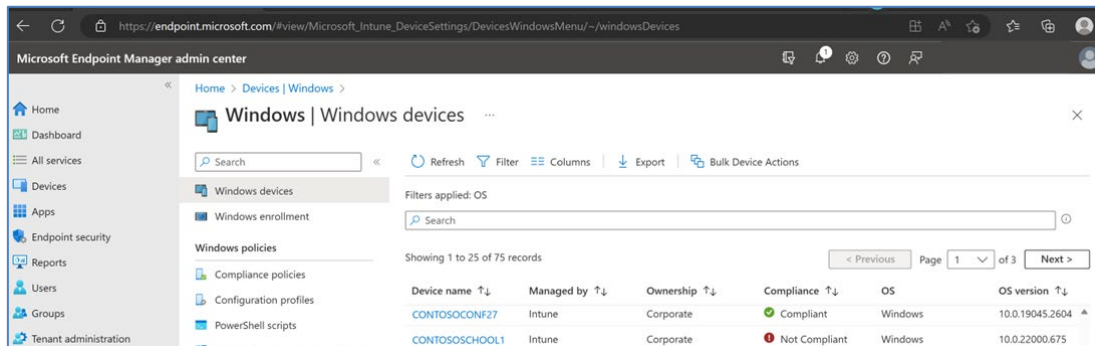


Reset devices and deregister from Autopilot

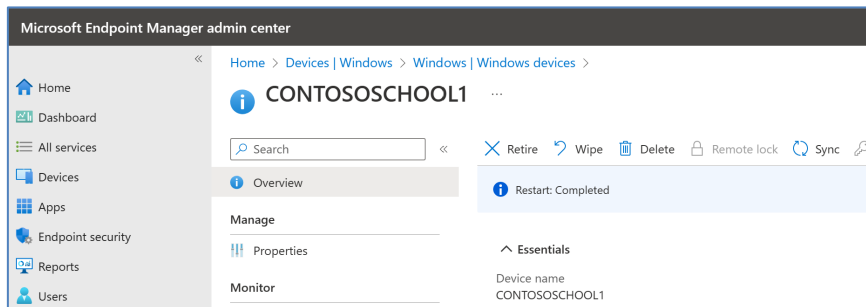
A typical end-of-life scenario would be factory resetting the device and deleting its Windows Autopilot registration.

Reset the device to OOB

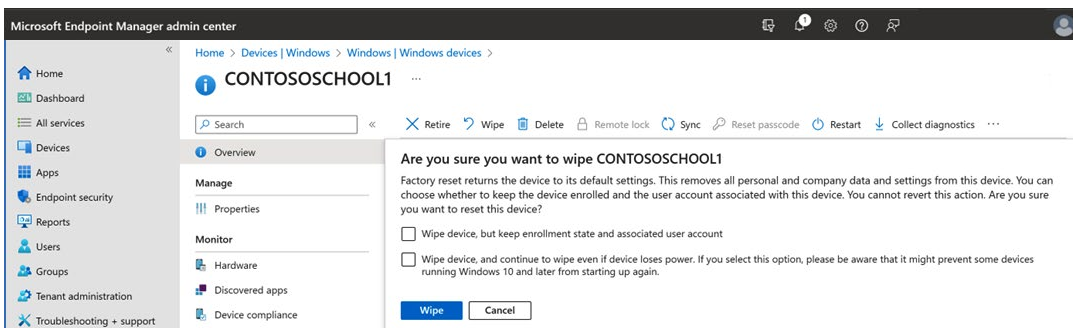
1. If you go back to [Endpoint manager](#) > **Devices** > **Windows**, you can see all the enrolled devices.



2. Select the device you want to reset and select Wipe on the next screen.



3. If you select Yes, the device will be reset to its factory defaults, and the Intune object will also be deleted.



Deregister the device from Windows Autopilot

There are two options to deregister the device from Autopilot:

- Customers can deregister it via the Endpoint Manager UI.
- CSP partners who registered the device can deregister the device in MPC.

Customer deregisters device via Endpoint Manager

1. Go to [Endpoint Manager \(https://endpoint.microsoft.com\)](https://endpoint.microsoft.com) > **Devices** > **Enroll devices** > **Windows enrollment**. Under Windows Autopilot Deployment Program, select **Manage Windows Autopilot devices**.
2. Select the device in the list and select **Delete** to remove it from Autopilot.

Partner deregisters device via Microsoft Partner Center

If a CSP registered the device, CSP partners can deregister the device as follows:

1. Sign in to the [Microsoft Partner Center](#).
2. Go to **Customers** and choose the appropriate customer from the customer list.
3. Under **Devices**, find the target device (select the serial number).
4. Select **Delete device**. This deletes the device from Autopilot and may take several minutes.

Devices

Customize a device's out-of-box experience with Windows AutoPilot profiles. [Learn more about configuring a device's Out of Box Experience \(OOBE\)](#).

Windows AutoPilot profiles

[Add new profile](#)

Profile	Status
There are no profiles.	

Apply profiles to devices

[Add devices](#)

Apply profile Remove profile Delete device

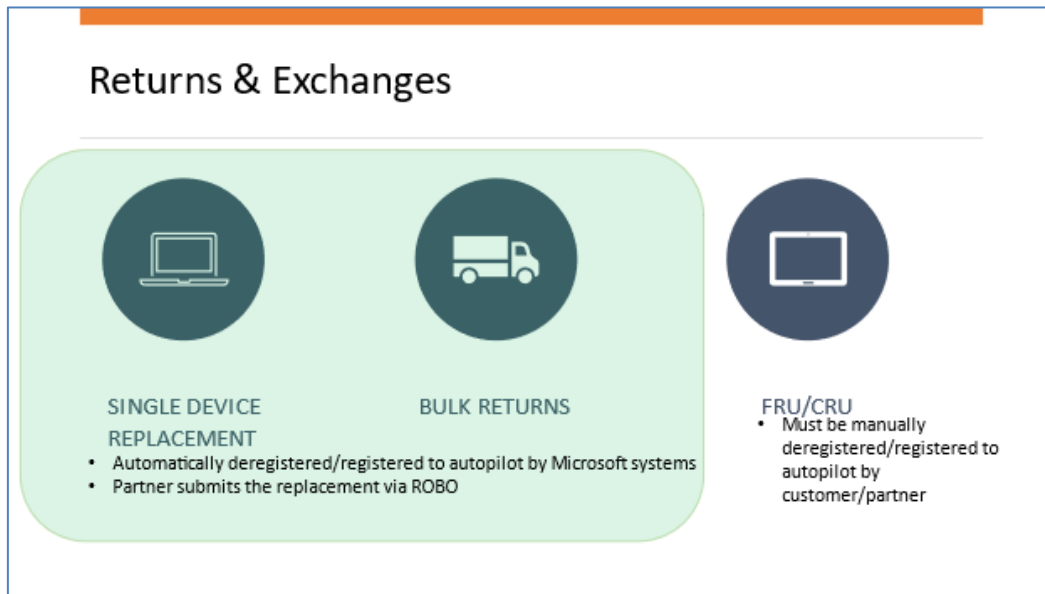
Group name	Devices	Creation date
<input checked="" type="checkbox"/> AutoPilot Group	1	6/15/2020

Device name	Device serial number	Windows product ID	Profile	Date added
<input checked="" type="checkbox"/> Microsoft Corporation - Surface Pro 7	002861493853		Autopilot Profile	6/15/2020

Return and exchange scenarios

Depending on the return scenario, the partner may or may not play a role in the deregistration of the broken device and registration of the new replacement device. Additional steps may need to be taken by the customer or partner for returns and exchanges.

In most returns and exchange scenarios, Microsoft will automatically deregister the returned device and register the replacement device. The partner only needs to ensure the request is submitted to Microsoft via the ROBO tool. In the case of Field or Customer Replaceable Units (FRU/CRU), follow the additional steps below.



Prepare devices for repair

Step 1: Remove devices from Autopilot and DFCI

Whether a commercial device is returning to the same customer or being sent back to Microsoft, it is crucial to have the customer retire the device and delete it from their tenant before submitting it for repair.

Device retirement and deletion

1. Go to [Endpoint Manager](https://endpoint.microsoft.com) (<https://endpoint.microsoft.com>). In the **Devices** pane, select **All Devices**.
2. Select the name of the device that you want to retire.
3. In the pane that shows the device name, select **Retire**. To confirm, select **Yes**.
4. Select the device's name you just retired in the Devices pane and select **Delete** to remove it from the tenant.
5. In [Endpoint Manager](#), go to **Devices > Device enrollment > Windows enrollment > Windows Autopilot Devices** and select **Sync**.
6. Wait 15 minutes before moving forward with any additional work on the device.

Step 2: Reset UEFI to enable boot from USB to reimage

Access to the UEFI boot screen is required for the successful repair processing of Surface devices. This section describes the UEFI screen's security states and relevant procedures.

UEFI password prompt

If the UEFI screen prompts for a password:

1. Attempt to obtain the UEFI password from the customer.
2. If unable to obtain the password, the device is not eligible for ASP repair and should be returned to Microsoft for servicing.

Unable to change settings or revert settings in UEFI

If you cannot change settings in UEFI or the settings you changed revert to prior values on reboot, the customer may have enabled a DFCI policy on the device in their Intune tenant.

To remove DFCI policy from the device:

1. [Retire the device from Intune and delete it from the tenant](#).
2. Wait 10 minutes before moving forward with any additional work on the device.
3. Connect the device to wired internet with a Surface-branded ethernet adapter.
4. Restart the device and open the UEFI menu (press and hold the volume-up button while pressing and releasing the power button).
5. Select **Management > Configure > Refresh from Network** and then choose **Opt-Out**.
 - If you receive a **Success** message, continue to Step 6.
 - If you receive a State 0 error code, try again after an hour. This state can require multiple attempts.

- If you receive a State 3 error code, too much time has elapsed since Step 1 was completed. Wait 24 hours before trying this again.
6. Once the process is complete, ensure that changes to UEFI remain.
 7. Once UEFI changes are confirmed, continue with repair operations.

NOTE: If you cannot remove the DFCI policy or UEFI settings continue to not be accessible, the device must be returned to Microsoft for servicing.

Step 3: Enroll device into Autopilot and DFCI to restore previous state

The device returned to the customer must be re-enrolled into their tenant to benefit from Autopilot and DFCI policy. Procedures vary depending on how the customer's devices were initially enrolled.

- Microsoft Partner via Partner Center (preferred method) – the customer's contracted Microsoft Partner can use the following documentation to learn more: [Customize a device's out-of-box experience - Partner Center](#).
- If the customer does not have a Microsoft Partner and wishes for Microsoft to handle the device registration, they can begin the process at this link: [Surface Registration Support for Windows Autopilot](#).

NOTE: Do not open the .csv file in Excel, as reformatting the information can corrupt the file. Instead, use Notepad to open the .csv. Once you have a .csv file with the device details, you can add the devices to the Autopilot Deployment Service via Intune.

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

- For a project with many devices, the PS1 script is too time-consuming, as you must manually touch each device.
- Microsoft Supply Chain Support team can provide a bulk-upload-ready .csv list of HW hashes in Intune.
- Work with your PMM here. You must send a list of the Surface device serial numbers to Microsoft with Proof of Purchase (PO or Invoice). Microsoft returns the Hardware Hash list in a .csv format that the partner or customer can upload.

Create and manage Autopilot profiles in MPC

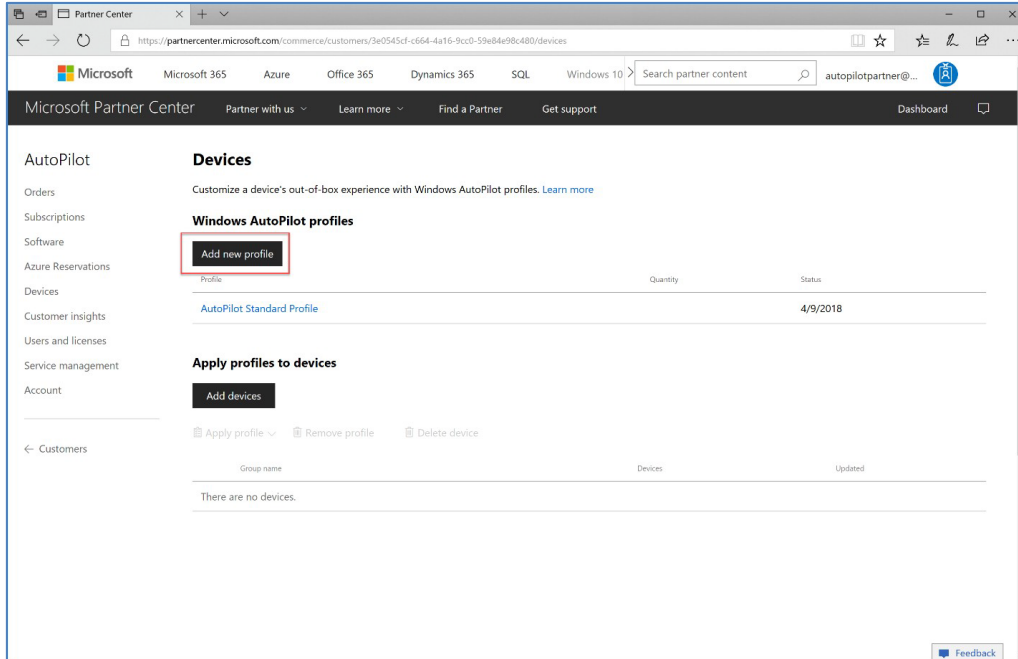
An *Autopilot profile* is a set of settings that configure a device during a Windows Autopilot deployment. This Autopilot profile can be created by the organization where devices are being deployed or limited by the partner on behalf of their customers. It contains the tenant information for joining an organization's AAD environment, automatically populated when you add devices to a customer through the Partner Center and settings for automating OOB. A list of available settings for Autopilot profiles is available at

[Overview of Windows Autopilot.](#)

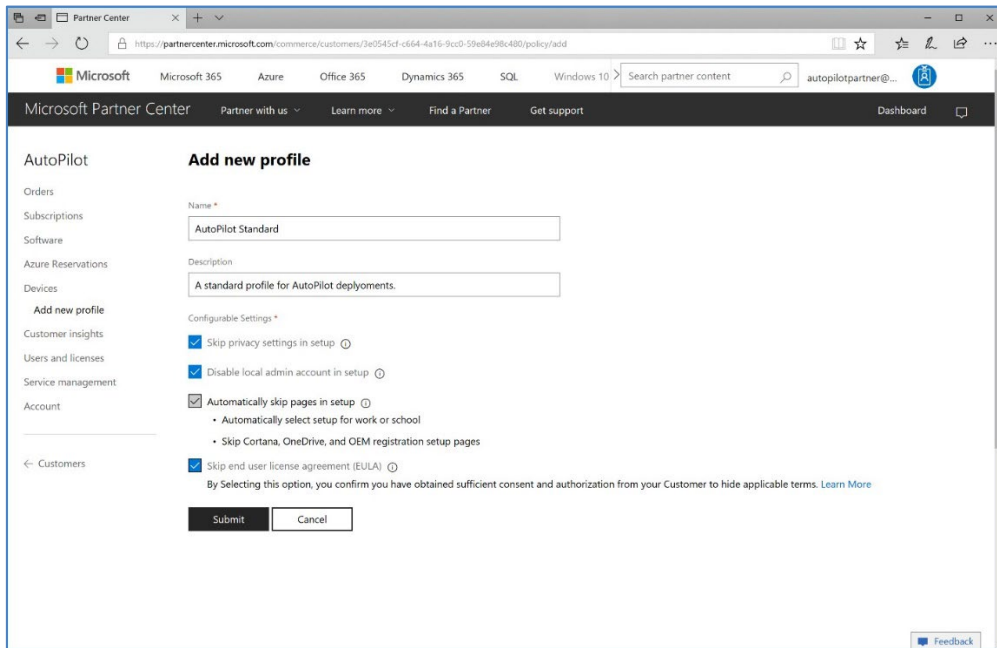
Note that the Autopilot profile allows automation of most aspects of OOB but does not automate or suppress the pages for specifying your language and keyboard or connecting to Wi-Fi. The user must first proceed through these settings to join the device to a network to provide connectivity to the Autopilot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

Configure settings as a partner on behalf of your customer from MPC

1. Open your customer account in the Partner Center from the Customers tab.
2. From **Devices**, select **Add new profile**.



3. Name the profile. For example, **Autopilot Standard Profile**, as shown in the example.



4. Configure the OOBE settings. For example, select **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 selected by default for all Windows Autopilot deployments.
5. Select **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 Intune; however, profiles created by the customer in the Microsoft Store for Business and Intune will

not be visible to the partner in Partner Center.

Apply an Autopilot profile to devices in MPC

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, select the checkbox next to the batch name.
3. Select **Apply profile** and select the **Autopilot profile**. The devices will then show the Autopilot profile name in the Profile column.
4. After registering devices, creating a new profile, and applying that profile to devices, test the configuration on a device to ensure OOBE is appropriately managed according to your Autopilot profile configuration.

Manage devices not supported for OEM enrollment

The device's manufacturer supports enrollment in Windows Autopilot by serial number, device model, and manufacturer name. 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. It results in a seamless experience where devices can be enrolled in Windows Autopilot without even needing to open the box before the user receives the device. However, there are some devices for which this process will not be supported, such as devices from OEMs that still need to enable support for enrollment by serial number, device model and manufacturer name.

Order Specific OS Versions for Windows Autopilot customers

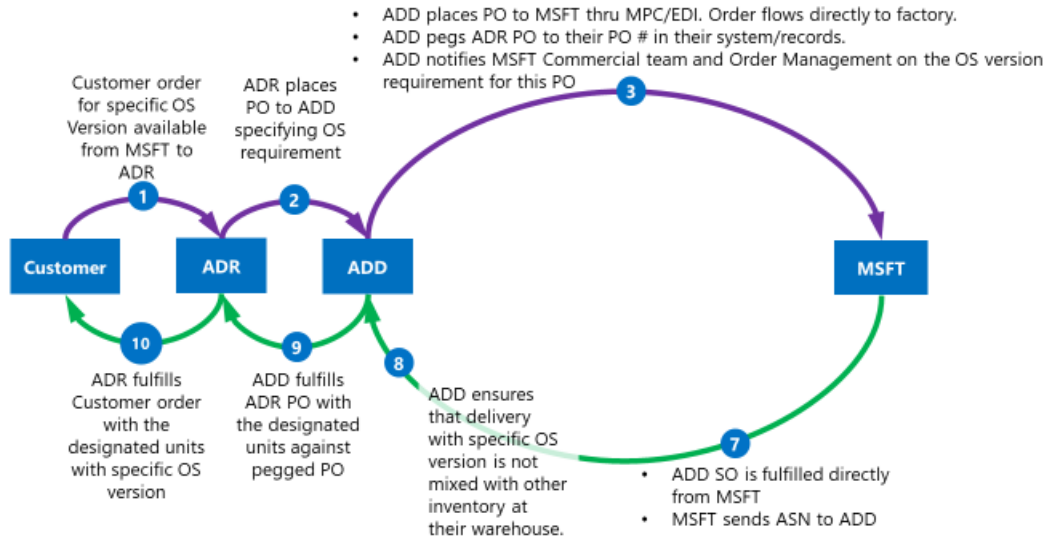
Fill the customers' orders with devices using the OS version they use in their environment. There are two ways to get the correct OS version on the device:

- If the offering is available from the ADR, ADRs or ADDs can re-image devices to the exact OS version.
- If the customer-requested OS version is what Microsoft ships, ADRs and ADDs can follow a *pegged PO* process to bypass the channel inventory and get devices directly from Microsoft (see Fig. 1). This process is done manually by the ADD pegging the ADR PO to their PO # in their system/records and notifying the MSFT commercial and Order management team of the OS version requirement. Surface devices come with different OS versions depending on the product and timeframe. As new OS versions are injected into the factory at different times, each product may have a different OS version at any given time. Contact your Microsoft representative to find out each product's current OS versions shipping from Microsoft. Support for pegging orders is required for partners listed on the [Windows Autopilot for Surface devices](#).

Customer Ordering with ADD Pegged PO for Specific OS Version available from Microsoft

Order Flow

Delivery Flow



Learn more

- [Windows Autopilot FAQ](#)
- [Windows Autopilot and Surface devices](#)
- [Surface Registration Support for Windows Autopilot](#)
- [What is device management in Azure Active Directory?](#)
- [Windows Autopilot product site](#)
- [Overview of Windows Autopilot](#)
- [Windows Subscription Activation](#)
- [Manage Windows device deployment with Windows Autopilot Deployment](#)
- [PowerShell scripts for Autopilot](#)
- [Automatic registration of existing devices - Windows Autopilot](#)
- [Windows Autopilot troubleshooting overview](#)