



Windows Autopilot Cookbook

Surface Edition

Deployment Guide for CSP Partners

Last updated: August 18, 2022

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.

© 2022. Microsoft Corporation. All rights reserved.

Contents

Introduction	1
Prerequisites for Autopilot.....	1
Network connectivity requirements.....	2
CSP Microsoft Partner Center requirements	2
Register devices to Autopilot.....	4
Microsoft Surface registration: CSP partner submits requests to Microsoft Support.....	5
CSP Partner registers devices using Microsoft Partner Center	5
Getting started	6
Requesting a Customer Relationship.....	6
Self registration: Customer registers devices using Intune	7
Prepare your Surface device.....	8
To reset current in-market devices to OOB.....	9
To reset earlier Surface devices to OOB.....	9
Prepare an Azure tenant	10
Get your demo tenant from CDX	10
Select a demo user	10
AAD and Intune setup	11
Configure automatic MDM enrollment.....	11
Configure company branding.....	12
Create Azure AD Group for all new Autopilot devices.....	13
Configure an Autopilot deployment profile.....	14
Intune device configuration.....	18
Device profiles	18
Enable the enrollment status page.....	19
Deploy software – Microsoft 365 Apps	20
Optional: Windows 10 Edition upgrade	23
Register Devices via Microsoft Partner Center.....	25
Format of .csv registration file	25
Language dependencies	26
Optional: Remove a device from Windows Autopilot Enrollment	29

Check device registration status in Intune	29
Assign the device to a user.....	30
End-user experience - Autopilot with Surface (User-Driven)	31
DHCI - Intune management of Surface UEFI settings.....	32
Prerequisites	32
Configure DHCI management for Surface devices	33
Create DHCI profile	33
Configure DHCI settings on Surface devices.....	34
Block user access to UEFI settings.....	35
Manually Sync Autopilot devices.....	36
Verify UEFI settings on DHCI-managed devices.....	36
Remove DHCI management	36
Optional: Reset the device and deregister the device from Autopilot.....	38
Reset the device to OOBE	38
Deregister the device from Windows Autopilot	39
Customer de-registers device using Endpoint Manager.....	39
Partner de-registers device using Microsoft Partner Center	39
Return and exchange scenarios	40
Prepare the device for repair.....	41
Step 1: Remove the device from Autopilot and DHCI	41
Device retirement and deletion.....	41
Step 2: Reset UEFI to enable boot from USB to re-image	41
UEFI password prompt.....	41
Unable to change settings or settings revert in UEFI	41
Step 3: Enroll device into Autopilot and DHCI to restore previous state.....	42
Appendix	43
Optional: Instructions to use PowerShell Script for generating the HW hash	43
Optional: Create and manage Autopilot profiles in MPC.....	44
To configure settings as a partner on behalf of your customer from MPC	44
Optional: Apply an Autopilot profile to devices in MPC.....	46
Optional: Manage devices not supported for OEM enrollment	46
Order Specific Windows 10 OS Versions for Windows Autopilot customers.....	46
Resources	48
Troubleshooting Autopilot	48

Introduction

Traditionally, IT pros spend a lot of time building and customizing images that will later be deployed to devices that already have 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 need to connect to a network and verify their credentials. Everything after that is fully automated. Windows Autopilot enables IT admins to do 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 that 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 Microsoft Intune.
- Reset or restart devices remotely.

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

Prerequisites for Autopilot

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, configure, and manage your enrolled devices.
Microsoft 365 Apps for enterprise (Optional)	Microsoft 365 Apps, formerly known as Office Pro Plus, is required if you wish to 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. Recommended: Windows 10 1903 or later.

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

License	Description
Microsoft 365 E3 or E5	Includes Azure Active Directory Premium, Microsoft Intune, and Microsoft 365 Apps for enterprise
Enterprise Mobility Security E3 / E5	Includes Azure Active Directory Premium and Microsoft Intune
Microsoft 365 Apps for enterprise E3 or E5	Includes Microsoft 365 Apps for enterprise

Network connectivity requirements

Make sure you require users to connect to their corporate network during the OOBE setup. The Windows Autopilot Deployment Program uses several 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

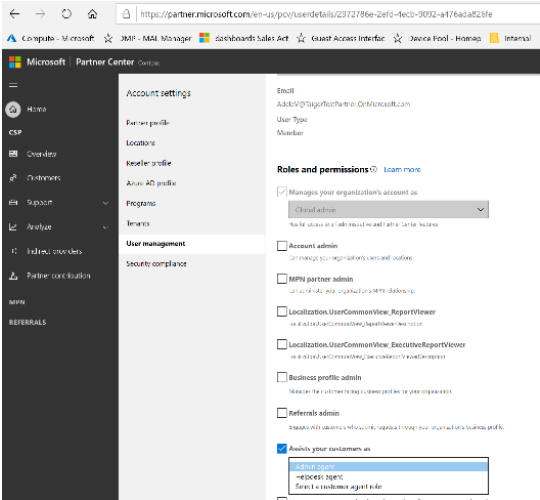
IMPORTANT:

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



Register 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:

- [Microsoft Support registration: CSP partner submits registration requests to Microsoft Support](#)
- [CSP Partner registers devices using Microsoft Partner Center](#)
- [Self-registration: Customer registers devices using 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 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. Self-registered devices cannot be managed by CSP partners 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 higher
Deregister support	Yes	Yes. Registration and deregistration require the customer to authorize CSP as a reseller, as described in Requesting a Customer Relationship .	Yes

Microsoft Surface registration: CSP partner submits requests to Microsoft Support

A simplified process of registering Surface devices for Windows Autopilot deployment is now available from Microsoft Support. 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

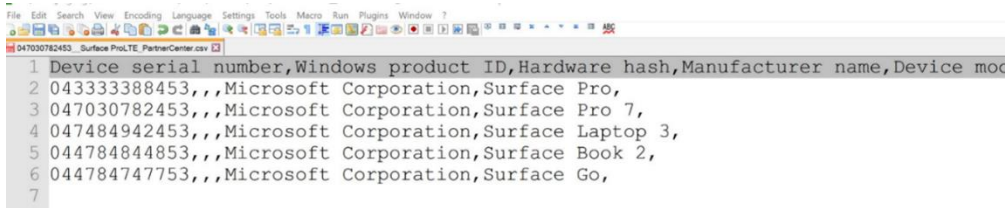
Required information	Description	Autopilot Registration	Hardware Hash Request	Autopilot Deregistration
Azure Active Directory Tenant ID	Your Azure Active Directory tenant ID is a globally unique identifier (GUID) different from your organization's name or domain. To find your Tenant ID, sign in to the 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 Excel file in .csv format with each device serial number in a new line.	Y	Y	Y

CSP Partner registers devices using Microsoft Partner Center

Microsoft Surface devices produced after Jan 2018 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](#).

For more detailed information, refer to [Register Devices via Microsoft Partner Center](#) below.

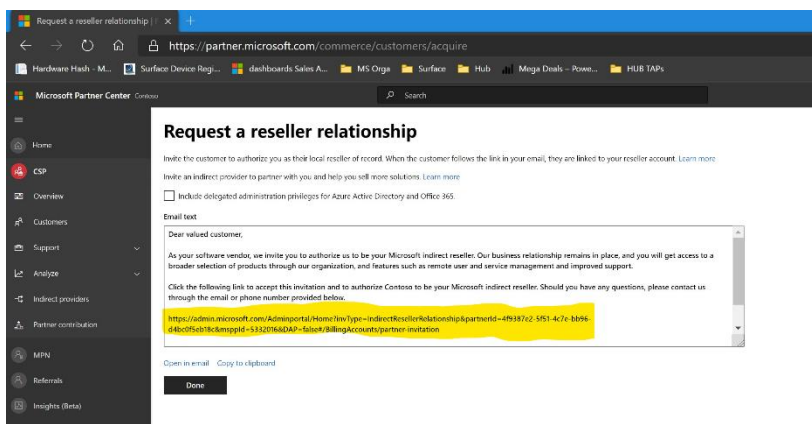
Getting started

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.

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:



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 delegated admin privileges or without delegated admin privileges.

Make sure to ask the customer which of these requests you should be sending.

If the customer does not want delegated admin privileges, clear the following checkbox: **Include delegated admin privileges for AAD and O365**. You can still register and deregister devices on the customer's AAD tenant regardless of delegated admin rights.

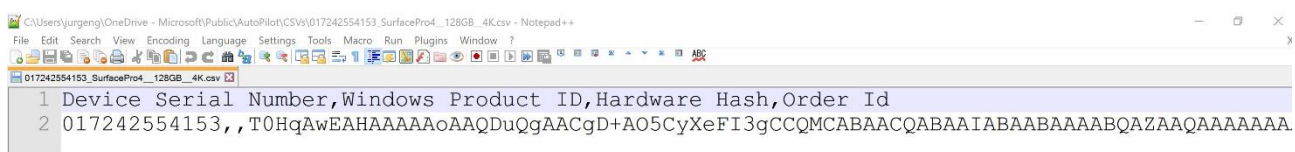
If the customer needs additional permissions - for example, to manage AAD, M365, Intune, or related services -- select **Include delegated administrator privileges for Azure Active Directory and Office365**. To learn more, refer to [request a relationship with a customer](#).

Self-registration: Customer registers devices using 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 the interaction with the Microsoft Partner Center. The Intune registration is more appropriate for testing purposes.)

NOTE: The .csv file format in Intune is different 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:



Prepare your Surface device

- Make sure that you have your Surface device in an OOBE state.
- Before the Surface device gets back onto the network, its HW ID must be registered to the Autopilot service.
- Surface devices are running Windows 10 1903 or higher.

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

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



To reset current in-market devices to OOBE

Fully update the device using Windows Update. Reboot the device.

Sign in with an Admin account.

Open the **Settings** app and select **Update & Security** > **Recovery**. Under **Reset this PC**, select **Get started** and choose **Remove everything**.

When the reset process is completed, the first OOBE screen appears.

To reset earlier Surface devices to OOBE

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

TIP: If the recovery image or existing OS is not running at least Windows 10 1903, upgrade to Windows 10 1903 or later via Windows Update and then reset the OS.

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

Prepare an Azure tenant

Get your demo tenant from CDX

As a Microsoft partner, you can create a new demo tenant 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:

Select **Quick Tenant**, 90 days

Select **tenant location**: your preferred location.

Choose **Microsoft 365 Enterprise Demo content** and select **Create tenant**.

The screenshot shows the 'Create a Tenant' interface. It includes a progress bar with 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. Two content packs are listed: 'Microsoft 365 Business Demo Content' and 'Microsoft 365 Enterprise Demo Content', each with a 'Create Tenant' button. The 'Enterprise Demo Content' is highlighted as the recommended option.

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

The screenshot shows the 'Tenant Details' page for tenant 'M365x335790'. It lists various details: Content pack (M365 Enterprise), Location (Europe, Middle East, Africa), Period (90 day), Expiration Date (9/4/20), Status (Completed), and Content add-ons (No add-ons applied). A 'Delete Tenant' button is visible. The 'Admin Details' section shows the Admin name, Email, and Password, with a 'Copy' button next to the password field.

Select a demo user

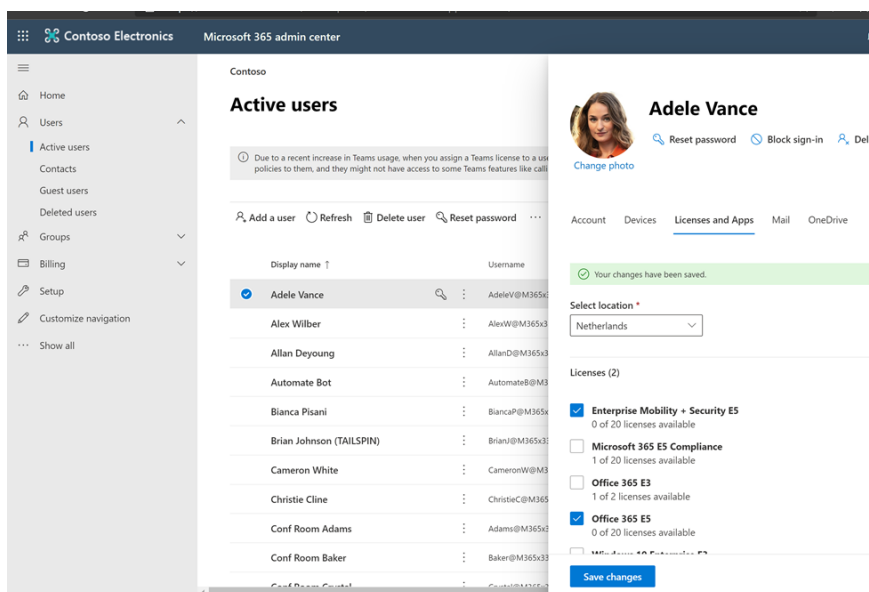
Sign in to your demo tenant as administrator to <https://admin.microsoft.com>, select **Users > Active Users** and choose a user.

Select **Licenses and Apps** and select the following:

Enterprise Mobility Security E5

Office 365 E5

Save Changes.



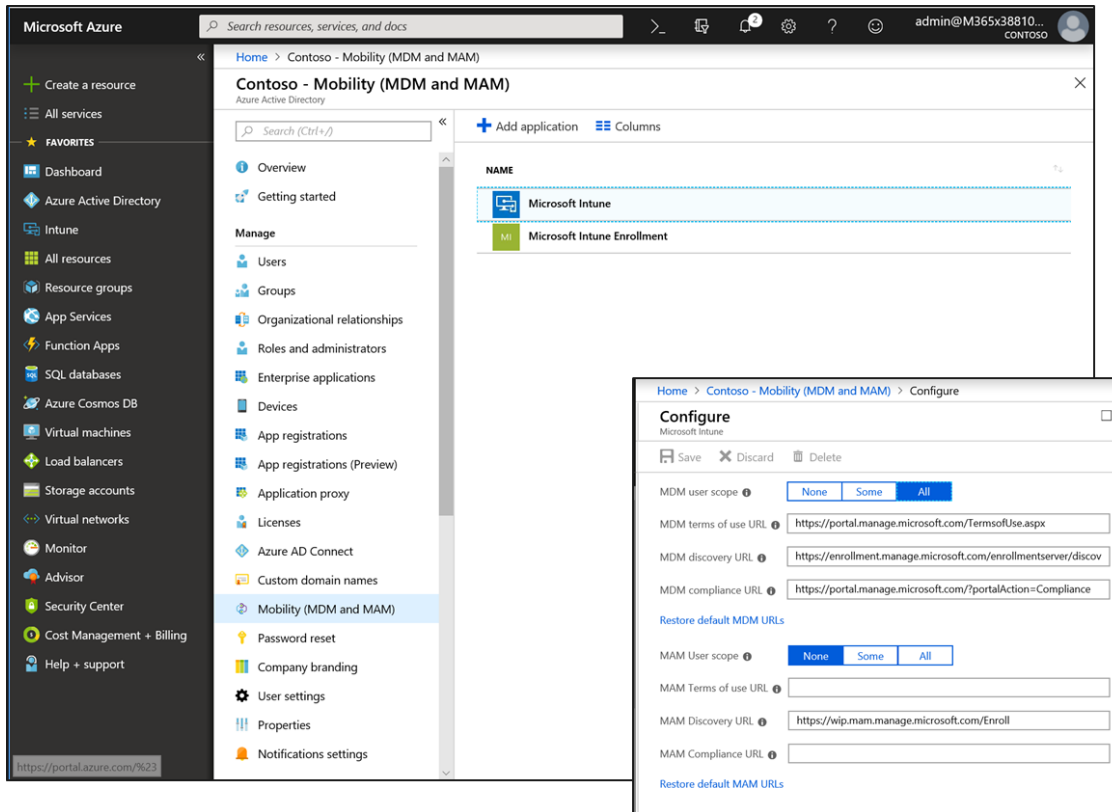
AAD and Intune setup

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

Configure automatic MDM enrollment

Sign in to <https://portal.azure.com> using the admin credentials provided for the tenant and enable MDM for all POC users.

Navigate to **Azure Active Directory** > **Mobility** (MDM and MAM) > select **Microsoft Intune** and ensure **ALL** is selected under MDM user scope. Repeat this for Microsoft Intune Enrollment as well.

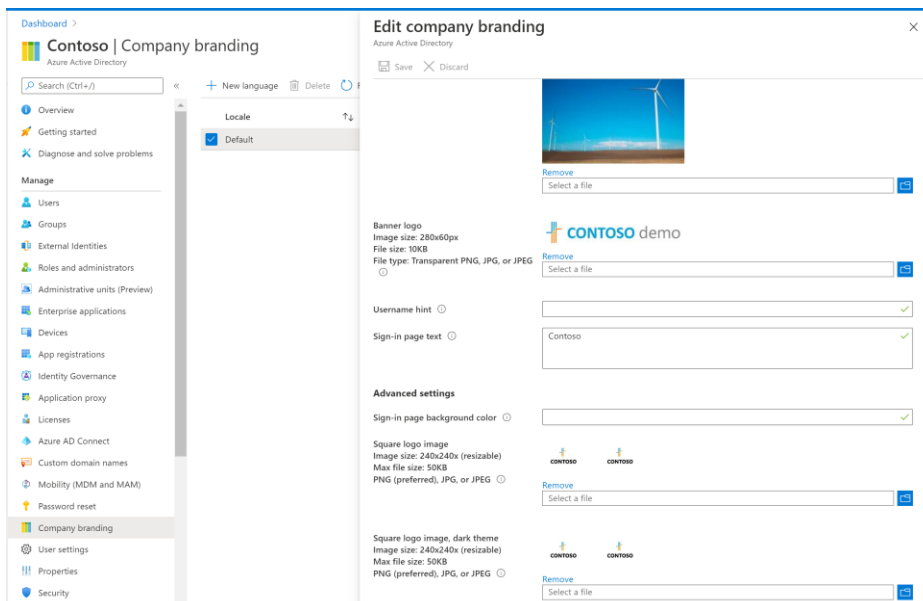


Configure company branding

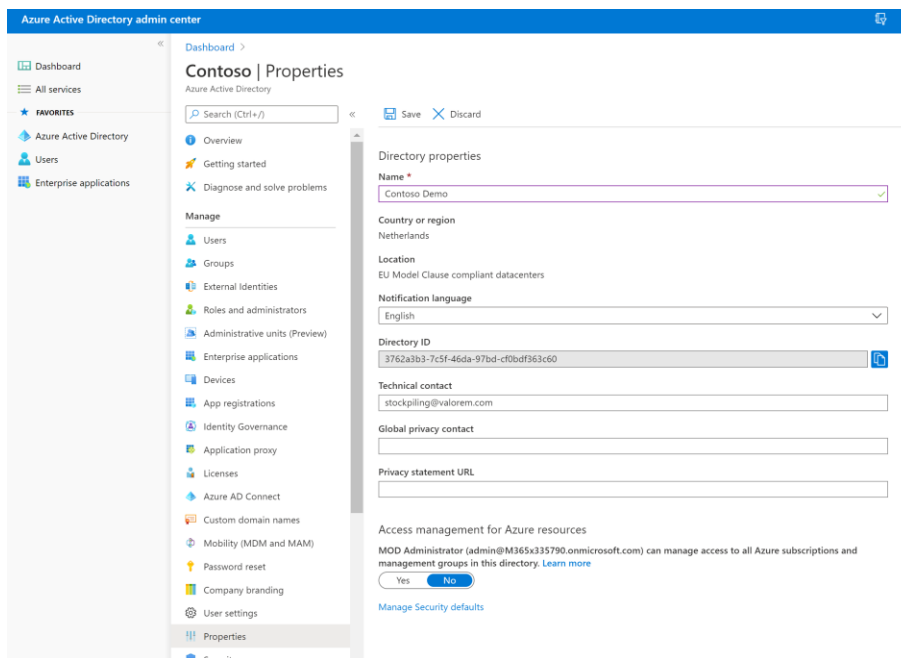
For your company branding to appear during OOB, you must configure it in Azure Active Directory. For more information, see [Add company branding to your directory](#). The following branding settings are required:

Background image, Banner logo, Square logo, and Square logo dark.

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



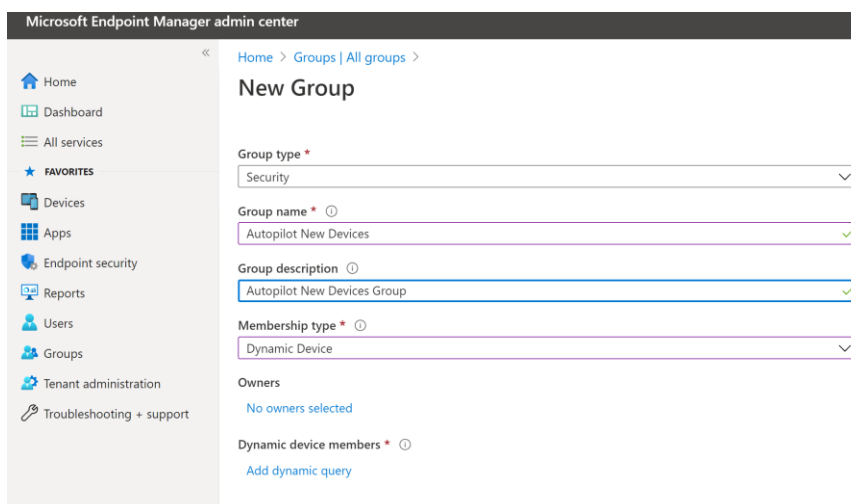
To adjust the tenant name displayed during OOB, open **Azure Active Directory > Properties > Name** and select **Save**.



Create Azure AD Group for all new Autopilot devices

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

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

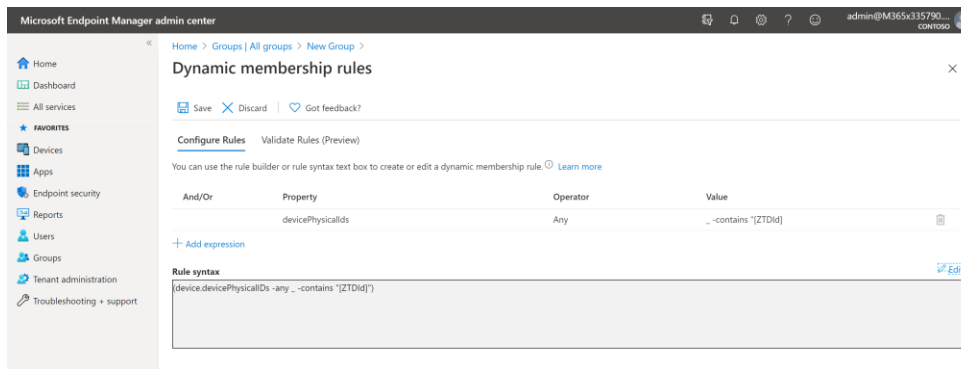


Make it a **Security Group**, name it **Autopilot New Devices**, and add a description (optional). Under Membership type, choose **Dynamic Device** and select **Add dynamic query**.

Select **Edit dynamic query**, select **Edit** (see top right of Rule syntax box), and enter the following rule syntax:

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

Then, select **OK** and then choose **Save**.



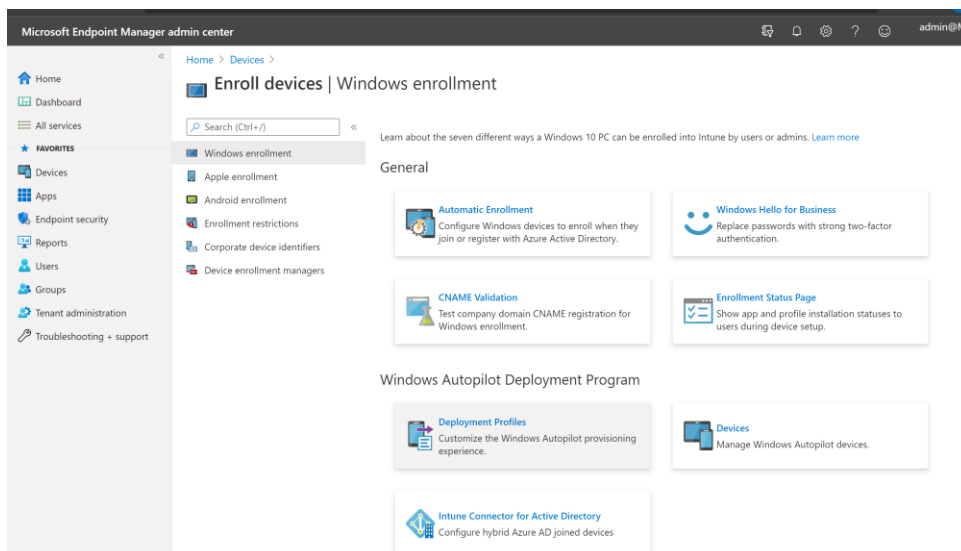
On the New Group page, select **Create**. All devices subsequently registered to Autopilot for this tenant will be members of this group. Refer to the section below to assign profiles and settings to the group.

To assign profiles and settings to an individual device, add it to the **Autopilot New Devices** group.

Configure an Autopilot deployment profile

An Autopilot deployment profile is a collection of settings used to configure a device during a Windows Autopilot deployment. The Autopilot profile allows automation of most aspects of OOBE 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 OOBE are also still presented to the user.

Go to <https://endpoint.microsoft.com> > **Devices** > **Enrollment devices**, make sure Windows enrollment is selected and choose **Deployment Profiles**.



Select **Create profile**. Or, if you use the CDX prepopulated tenant, you can select the already configured Autopilot Profile settings.

On the **Basics** screen, name the profile **Autopilot Profile**, add a description (optional), and then select **Next**.

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

Create profile

Windows PC

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

Name * Autopilot Profile ✓

Description ✓

By default, this profile can only be applied to Autopilot devices synced from the Autopilot service. [Learn more](#)

Convert all targeted devices to Autopilot

☒ No ☐ Yes

Previous Next

On the OOBE page, you will configure a User-Driven deployment mode.

Configure recommended settings, as shown in the following table.

Policy	Recommended setting
Deployment mode	User-Driven
Join to Azure AD	Azure AD joined
Microsoft SW License Terms and Privacy settings	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 White Glove OOBE	No. This scenario does not use the White Glove OOBE option, which allows you to pre-provision the device to speed up the OOBE experience.

Keep Language as OS default	This is the OS language. Also, leave the keyboard to auto-config based on the region selection.
Apply device name	No

Home > Microsoft Intune > Device enrollment | Windows enrollment > Windows Autopilot deployment profiles > Autopilot Profile | Properties > Edit profile

Edit profile

Out-of-box experience (OOBE) Review + save

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

Deployment mode

Join to Azure AD as

Microsoft Software License Terms

Important information about hiding license terms

Privacy settings

The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. [Learn more](#)

Hide change account options

User account type

Allow White Glove OOBE

Language (Region)

Automatically configure keyboard

Apply device name template

Review + save **Cancel**

Select **Next** and assign this profile to the dynamic group **Autopilot New Devices** you created earlier:

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

Create profile

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

Included groups

Assign to

Selected groups
No groups selected
[+ Select groups to include](#)

Excluded groups
No groups selected
[+ Select groups to exclude](#)

Select groups to include

Search

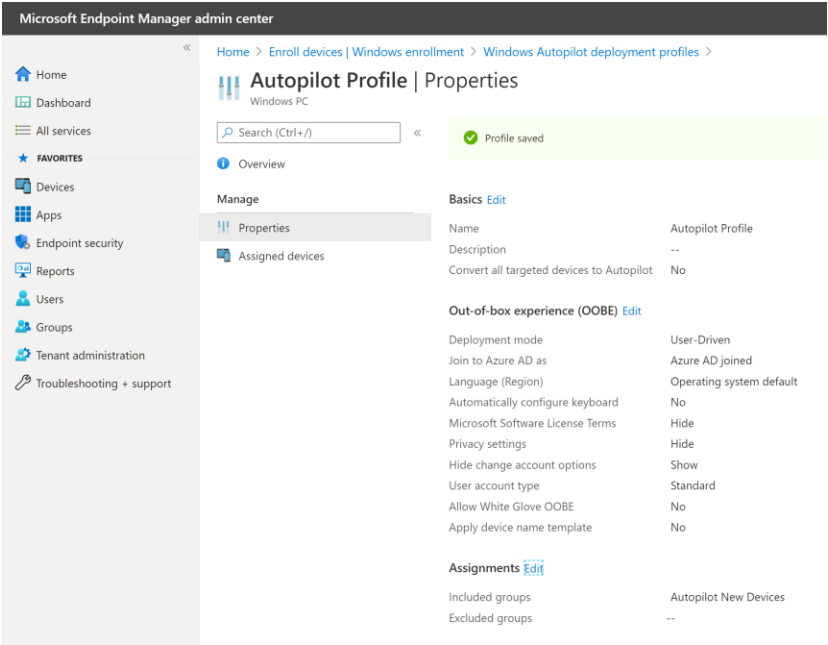
- Autopilot New Devices (Selected)
- Digital Initiative Public Relations
DigitalInitiativePublicRelations@M365a870051.onmicrosoft.com
- Mark @ Project Team
Mark@ProjectTeam@M365a870051.onmicrosoft.com
- Retail
Retail@M365a870051.onmicrosoft.com
- Sales and Marketing
SalesAndMarketing@M365a870051.onmicrosoft.com
- ig-Engineering
- ig-Executive

Selected items
Autopilot New Devices **Remove**

Select **Select**

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

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 common device profiles include Email, Device restrictions, VPN, Wi-Fi, and Administrative templates. Microsoft Intune has 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 <https://endpoint.microsoft.com> > **Devices** > **Configuration profiles** and select **+Create profile**.

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

Under **Profile type**, choose **Device restrictions**.

On the **Basics** page, name the profile **Win10-DeviceConfig-Restrictions** and select **Next**.

TIP: If you use the CDX prepopulated system, you can simply review and edit the existing profile and select **Configuration settings**.

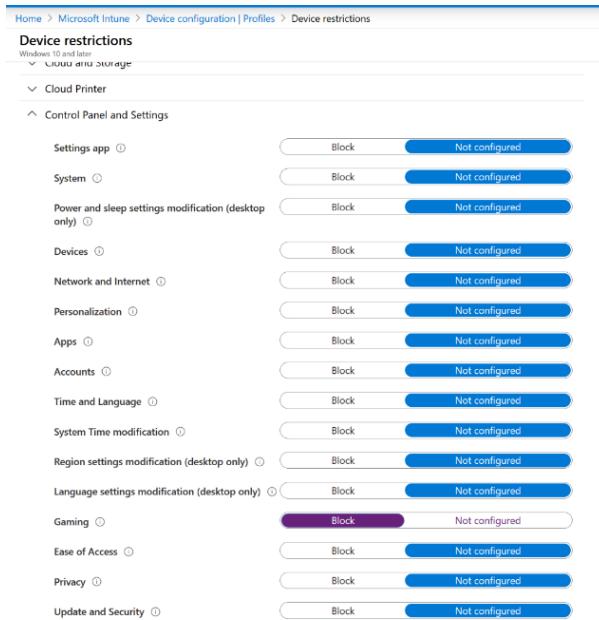
Review the available configuration settings, select **Start restrictions**, and configure some settings.

The screenshot shows the 'Device restrictions' configuration page in Microsoft Intune. The breadcrumb trail at the top is 'Profiles > Initial Configuration > Properties > Device restrictions'. The title is 'Device restrictions' with a subtitle 'Windows 10 and later'. The settings are organized into two columns. The first column lists the settings, and the second column shows the current configuration status.

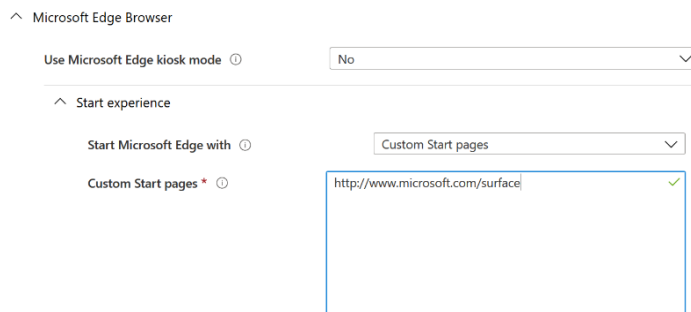
Setting	Configuration Status
Power button	Not configured
User Tile	Not configured
Lock	Not configured
Sign out	Not configured
Shut Down	Not configured
Sleep	Not configured
Hibernate	Not configured
Switch Account	Block
Restart Options	Not configured
Documents on Start	Not configured
Downloads on Start	Not configured
File Explorer on Start	Not configured
HomeGroup on Start	Hide
Music on Start	Not configured
Network on Start	Not configured
Personal folder on Start	Not configured
Pictures on Start	Hide
Settings on Start	Not configured
Videos on Start	Hide

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

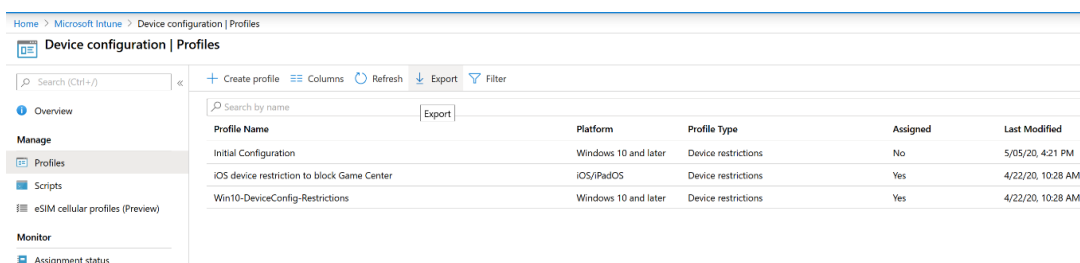
Open Control Panel and Settings and block Gaming.



Open **Microsoft Edge** and set the Start page to a favorite website.



Select **Next** (twice), then under **Assignments**, choose **All users and devices**, select **Next** (twice), and select **Create** after reviewing the settings. Your profile 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.

Navigate to <https://endpoint.microsoft.com> > Device > Enroll Devices > Windows Enrollment > Enrollment Status Page. On the default ESP page, All users and all devices, you can edit and adjust the properties:

Home > Microsoft Intune > Device enrollment Windows enrollment > Enrollment Status Page		
Enrollment Status Page Windows Enrollment		
+ Create		
The enrollment status page appears during initial device setup and during first user sign in. If enabled, users can see the configuration progress of assigned apps and profiles targeted to their device. Learn more		
Priority	Name	Assigned
Default	All users and all devices	Yes

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

Home > Microsoft Intune > Device enrollment | Windows enrollment > Enrollment Status Page > All users and all devices | Properties > Edit profile

Edit profile

Settings Review + save

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

Show app and profile configuration progress: ☐ No ☒ Yes

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

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

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

Allow users to collect logs about installation errors: ☐ No ☒ Yes

Only show page to devices provisioned by out-of-box experience (OOBE): ☐ No ☒ Yes

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

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

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

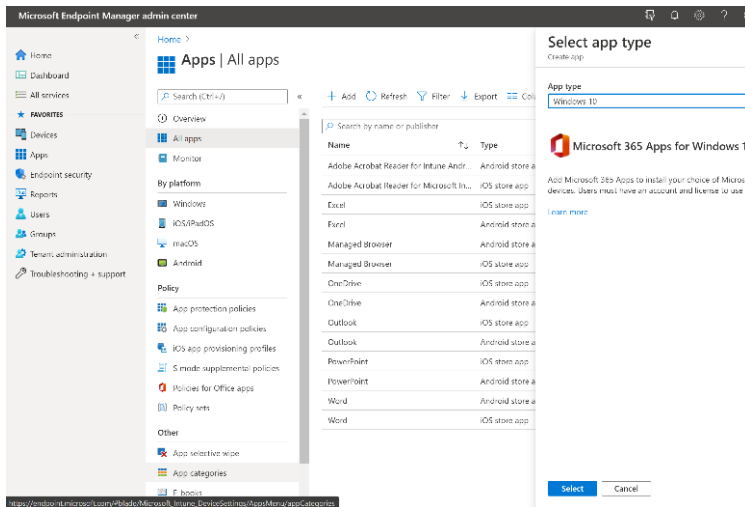
Block device use until these required apps are installed if they are assigned to the user/device: ☒ All ☐ Selected

Review + save Cancel

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

Deploy software – Microsoft 365 Apps

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



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

Home > Apps | All apps >

Add Microsoft 365 Apps

Microsoft 365 Apps (Windows 10)

1 App suite information 2 Configure app suite 3 Assignments 4 Review + create

Suite Name * ⓘ Microsoft 365 Apps for Windows 10

Suite Description * ⓘ Microsoft 365 Apps for Windows 10

Publisher ⓘ Microsoft

Category ⓘ Productivity

Show this as a featured app in the Company Portal ⓘ ☐ Yes ☒ No

Information URL ⓘ <https://products.office.com/en-us/explore-office-for-home>

Privacy URL ⓘ <https://privacy.microsoft.com/en-US/privacystatement>


Developer ⓘ Microsoft

Owner ⓘ Microsoft

Notes ⓘ

Logo ⓘ

Select image



[Previous](#) [Next](#)

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

Add Microsoft 365 Apps
Microsoft 365 Apps (Windows 10)

✓ App suite information **4 Configure app suite** 3 Assignments 4 Review + create

Configuration settings format * Configuration designer

Configure app suite

Select Office apps 0

Select other Office apps (license required): 0

App suite information

These settings apply to all apps you have selected

Architecture 0

Update channel * 0

Remove other versions 0

Version to install 0

Specific version

Properties

Use shared computer activation 0 Yes No

Accept the Microsoft Software License Terms on behalf of users Yes No

Languages 0 No languages selected

Previous Next

Leave the architecture as **64-bit** and ensure the Update Channel is **Semi-Annual Enterprise Channel**.

Select **Yes** to Accept the License Agreement on behalf of the users.

Retain defaults for all other settings and then select **Next**.

Add Microsoft 365 Apps
Microsoft 365 Apps (Windows 10)

✓ App suite information **4 Configure app suite** 3 Assignments 4 Review + create

Configuration settings format * Configuration designer

Configure app suite

Select Office apps 0

Select other Office apps (license required): 0

App suite information

These settings apply to all apps you have selected

Architecture 0

Update channel * 0

Remove other versions 0

Version to install 0

Specific version

Properties

Use shared computer activation 0 Yes No

Accept the Microsoft Software License Terms on behalf of users Yes No

Languages 0 No languages selected


Previous Next

On the Assignment Page, select **+Add all users**.

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

Add Microsoft 365 Apps
Microsoft 365 Apps (Windows 10)

App suite information

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	https://products.office.com/en-us/explore-office-for-home
Privacy URL	https://privacy.microsoft.com/en-US/privacystatement
Developer	Microsoft
Owner	Microsoft
Notes	...
Logo	

Configure app suite

Apps to be installed as part of the suite	Excel, OneDrive Desktop, OneNote 2016, Outlook, PowerPoint, Word
Architecture	64-bit
Update channel	Semi-Annual Enterprise Channel
Remove other versions	Yes
Version to install	Latest
Use shared computer activation	No
Accept the Microsoft Software License Terms on behalf of users	Yes
Apps to be installed as part of the suite	No languages selected

Assignments

Required	All users
Available for enrolled devices	--

Optional: Windows 10 Edition upgrade

As part of the automated provisioning process, you can upgrade the factory-installed operating systems from Windows 10 Pro to Windows 10 Enterprise. 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 will need to create a new profile and assign it to all users.

Open Intune and navigate to **Device configuration > Profiles > Create profile**.

For Platform, select **Windows 10 and later**. For profile, select **Edition upgrade and mode switch**.

Select **Create** and then name the new profile **Enterprise Uplift**.

Under the Configuration Settings pane, select **Windows 10 Enterprise** and fill in the required Product Key information.

Select **Next > Next >** and assign the profile to your **Autopilot New Devices Group**.

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

Home > Microsoft Intune > Device configuration | Profiles > Edition upgrade and mode switch

Edition upgrade and mode switch

Windows 10 and later

✓ Basics

✓ Configuration settings

✓ Scope tags

✓ Assignments

✓ Applicability Rules

6 Review + create

Summary

Basics

Name

Enterprise Uplift

Description

--

Platform

Windows 10 and later

Profile type

Edition upgrade and mode switch

Configuration settings

Edition to upgrade to

Windows 10 Enterprise

Product Key

12345-12345-12345-12345-12345

Scope tags

Default

Assignments

Included groups

Autopilot New Devices

Excluded groups

--

Applicability Rules

Rule

Property

Value

Previous

Create

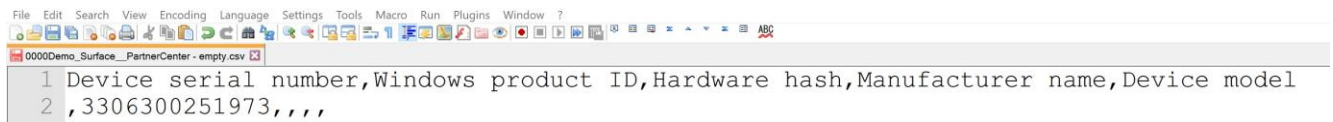
On the Assignments page, select under **Required** on **+Add all users**. M365 apps are assigned to all users. Select **Next** and then select **Create**.

This completes the basic configuration of the customer tenant.

Register Devices via Microsoft Partner Center

Before you can apply an Autopilot profile to a device, you will need to first add any new devices that are not already enrolled in Azure AD or your MDM solution.

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



```

1 Device serial number,Windows product ID,Hardware hash,Manufacturer name,Device model
2 ,3306300251973,,,,,

```

If the product ID is not known to you, then for Surface devices, you can simply use a convenient alternative method. Fill out a tuple for each device with these three items:

- Serial number,
- Manufacturer Name
- Device Model



```

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.

It is recommended to establish practices to allocate and isolate Windows Autopilot orders, 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 sticker on the box or from 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, make sure 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
```

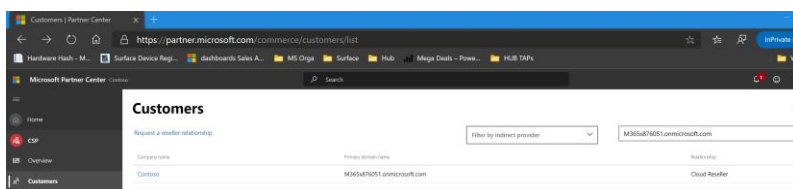
Language dependencies

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

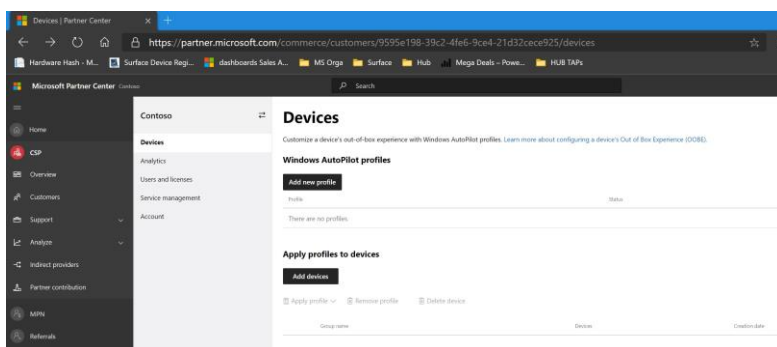
To register devices using a .csv file:

Sign in to MPC.

Open your customer account from the Customers tab.



Under Devices, select **Add devices**.

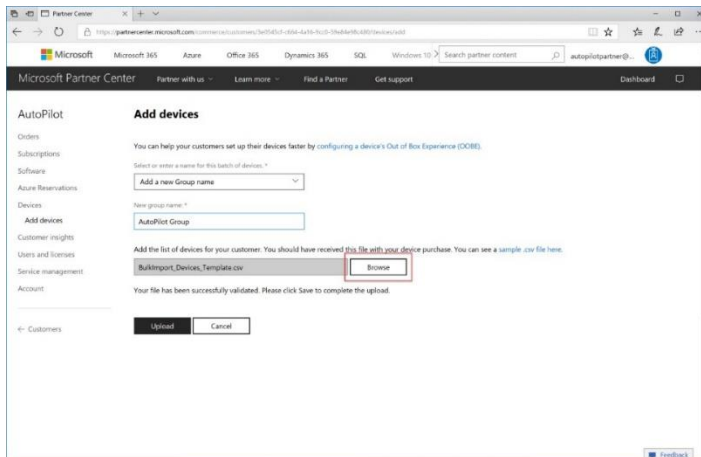


NOTE: Skip the Windows Autopilot profiles option in favor of configuring profiles in the customer's MDM system, which is the appropriate location to manage policies, app deployment, and so on.

Name the batch of devices you are adding or select from an existing group.

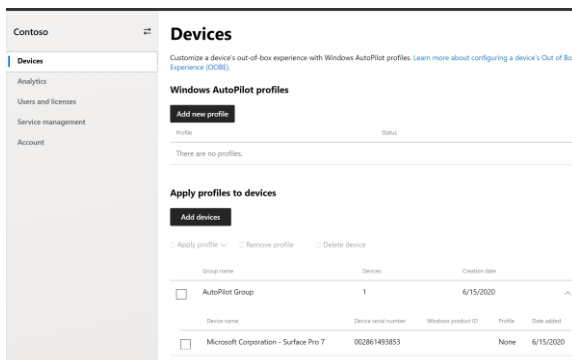
Select Browse to locate the .csv file containing the list of device serial numbers to be added. Select Open to select

the .csv file.



Select **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. 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 when naming device groups during registration. 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 cannot offer new automated services.

Optional: 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:

Open your customer account in the Partner Center from the **Customers** tab.

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.

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

Go back to the PoC Tenant at <https://endpoint.microsoft.com> > **Devices** > **Enrolled Devices** > **Devices**

Select **Sync** and **Refresh**.

The device you have just registered in the Partner Center should now appear in 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** that 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 you are waiting for this to happen, go to the next step.

Microsoft Endpoint Manager admin center

Home > Devices > Enroll devices | Windows enrollment >

Windows Autopilot devices

Windows enrollment

Sync Filter Import Export Assign user Refresh Delete

Last sync request : 6/15/20, 3:42 PM Last successful sync : 6/15/20, 3:42 PM

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

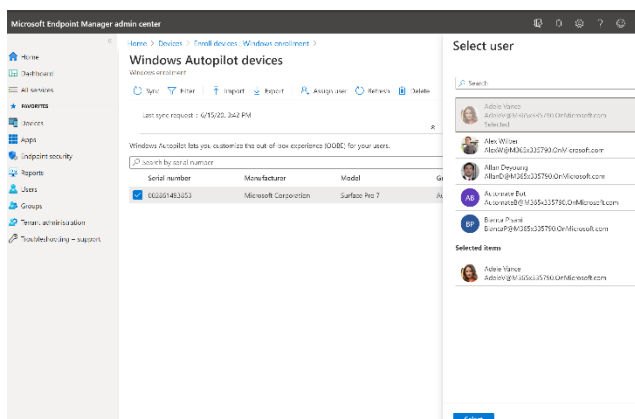
Search by serial number

Serial number	Manufacturer	Model	Group Tag	Profile status	Purchase order
<input type="checkbox"/> 002861493853	Microsoft Corporation	Surface Pro 7	AutoPilot Group	Assigned	N/A

Assign the device to a user

You can assign a specific user to a device. This can help create a customized experience for your users 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 to your tenant as part of the Windows Autopilot service.

Go to <https://endpoint.microsoft.com> > **Devices** > **Enroll devices** > **Devices** and select the device you wish to assign to a specific user.



Select the device and then select **Assign user**. Choose our target end-user in the user list. Example: **AdeleV**.

Check the properties and then select **Save**.



End-user experience - Autopilot with Surface (User-Driven)

Not only does Windows Autopilot with Surface make life easier for IT, but 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 simplified, with the number of screens the user has to 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, policies, etc., that are being 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. Make sure 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.

DFCI - Intune management of Surface UEFI settings

With Device Firmware Configuration Interface (DFCI) profiles built into Microsoft Intune, Surface UEFI management extends the modern management stack down to the UEFI hardware level. DFCI on Surface devices¹ supports zero-touch provisioning, eliminates BIOS passwords, provides control of security settings, including boot options and built-in peripherals, and lays the groundwork for advanced security scenarios in the future. In contrast to other Windows 10 devices available in the market today, Microsoft Surface provides IT admins with the ability to configure and manage firmware through a rich set of UEFI configuration settings. This provides a layer of hardware control on top of software-based policy management as implemented via mobile device management (MDM) policies. For example, organizations deploying devices in highly secure areas with sensitive information can prevent camera use by removing functionality at the hardware level. Turning the camera off via a firmware setting is equivalent to physically removing the camera from a device standpoint. Compare the added security of managing at the firmware level to relying only on operating system software settings. For example, if you disable the Windows audio service via a policy setting in a domain environment, a local admin could still re-enable the service.

With the integrated UEFI firmware management capabilities in Microsoft Intune, locking down hardware is simplified with new features for provisioning, security, and streamlined updating in a single Endpoint Manager console.

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

For more information about DFCI and supported devices, see [Manage DFCI on Surface devices](#)

Prerequisites

- Register devices to Windows Autopilot by a CSP or Microsoft. It is not possible to use DFCI when self-registering via Intune.

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>.

- 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 that contains the settings and an Autopilot profile to apply the settings to registered devices. An enrollment status profile is also recommended to ensure settings are pushed down during OOB setup when users first start the machine. This guide explains how to configure the DFCI environment and manage UEFI configuration settings for targeted Surface devices.

Create DFCI profile

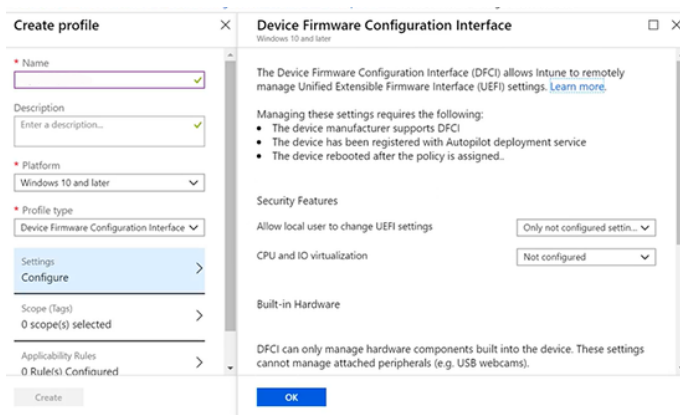
Before configuring DFCI policy settings, first create a DFCI profile and assign it to the Azure AD security group that contains your target devices.

Sign in to your tenant at <https://endpoint.microsoft.com>

In the Microsoft Endpoint Manager Admin Center, select **Devices > Configuration profiles > Create profile** and enter a name; for example, **DFCI Configuration Policy**.

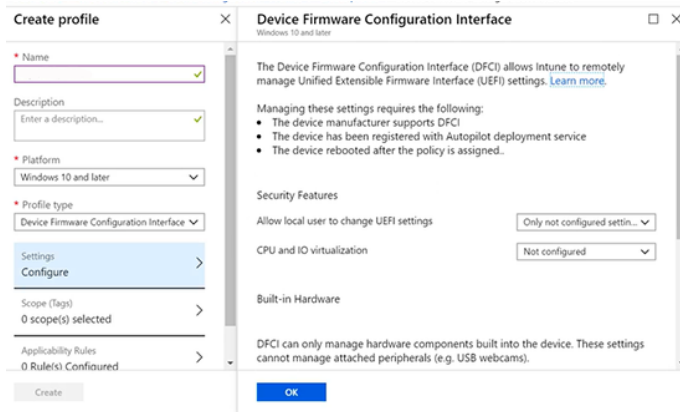
Select **Windows 10 and later** for platform type.

In the Profile type drop-down list, select **Device Firmware Configuration Interface** to open the DFCI blade containing all available policy settings. You can configure DFCI settings during the initial setup process or later by editing the DFCI profile.



Select **OK** and then select **Create**.

Select **Assignments** and under **Select groups to include** select the Azure AD security group that contains your target devices, as shown in the following figure. Select **Save**.



Next, make sure that you assign the Autopilot profile to your DFCI devices group.

In Endpoint Manager, select **Devices > Windows enrollment** and scroll down to Deployment profiles.

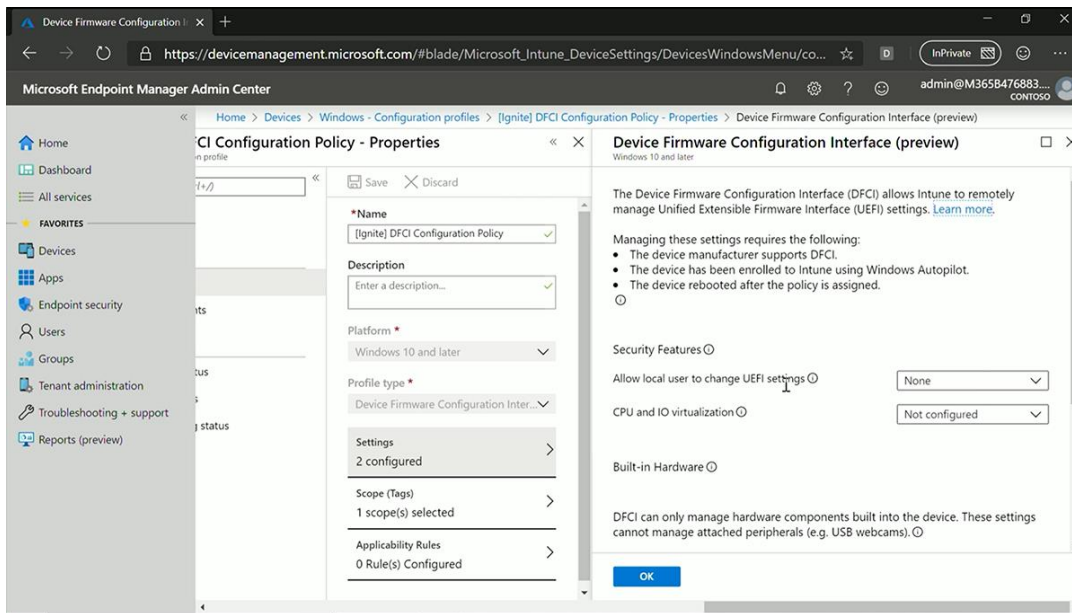
Select the Autopilot profile you created in the preceding section, and under the Assignments page, choose **Select groups** to include and select your Azure AD security group (Example 00AIIIDFCIdevices).

Select **Next** and save the settings.

Configure DFCI settings on Surface devices

DFCI includes a streamlined set of UEFI configuration policies that provide an extra level of security by locking down devices at the hardware level. DFCI is designed to be used with mobile device management settings at the software level. Note that DFCI settings only affect hardware components built into Surface devices and do not extend to attached peripherals such as USB webcams. (However, you can use Device restriction policies in Intune to turn off access to attached peripherals at the software level). You configure DFCI policy settings by editing the DFCI profile from Endpoint Manager, as shown in the figure below.

In [Endpoint Manager](#) select **Devices > Windows > Configuration Profiles > DFCI profile name > Properties > Settings**.



Block user access to UEFI settings

For many customers, the ability to block users from changing UEFI settings is critically important and a primary reason to use DFCI. This is managed via the setting "Allow local user to change UEFI settings." If you do not edit or configure this setting, local users could change any UEFI setting not managed by Intune. Therefore, it is highly recommended to disable "Allow local user to change UEFI settings." The rest of the DFCI settings enable you to turn off functionality that would otherwise be available to users. For example, suppose you need to protect sensitive information in highly secure areas. In that case, you can disable the camera, and if you do not want users booting from USB drives, you can disable that also.

Device management goal	Configuration steps
Block local users from changing UEFI settings	Under Security Features > Allow local user to change UEFI settings , select None .
Disable cameras	Under Built in Hardware > Cameras , select Disabled .
Disable Microphones and speakers	Under Built in Hardware > Microphones and speakers , select Disabled .
Disable radios (Bluetooth, Wi-Fi)	Under Built in Hardware > Radios (Bluetooth, Wi-Fi, etc.) , select Disabled .

Device management goal	Configuration steps
Disable boot from external media (USB, SD)	Under Built in Hardware > Boot Options > Boot from external media (USB, SD), select Disabled.

CAUTION: The **Disable radios (Bluetooth, Wi-Fi)** setting should only be used on devices with a wired Ethernet connection.

NOTE: DFCI in Intune includes three settings that do not currently apply to Surface devices: (1) CPU and IO virtualization, (2) Disable boot from network adapters, and (3) Windows Platform Binary Table (WPBT).

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).

In [Endpoint Manager](#), 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.

Verify UEFI settings on DFCI-managed devices

In your test environment, you can verify settings in the Surface UEFI interface.

After a reboot, boot into Surface UEFI by pressing the Volume+ and Power buttons simultaneously.

Select Devices. The UEFI menu will reflect configured settings, as shown in the following figure.

As you can see, the settings are grayed out because, in Intune, we set the "Allow local user to change UEFI" setting to None. Audio is set to off because Microphones and speakers are set to Disabled.

Remove DFCI management

To remove DFCI management and return the device to factory new state:

Retire the device from Intune: In [Endpoint Manager](#), choose **Groups > All Devices**. Select the devices you want to retire and select **Retire/Wipe**.

Delete the Autopilot registration from Intune: Select **Device enrollment > Windows enrollment > Devices**. Under Windows Autopilot devices, choose the devices you want to delete, and then select **Delete**.

Connect the device to wired internet with a Surface-branded ethernet adapter (USB-A or USB-C or Surface Dock)

Restart the device and open the UEFI menu (press and hold the volume-up button while pressing and releasing the power button). Select **Management > Configure > Refresh from Network** and then choose **Opt-out**.

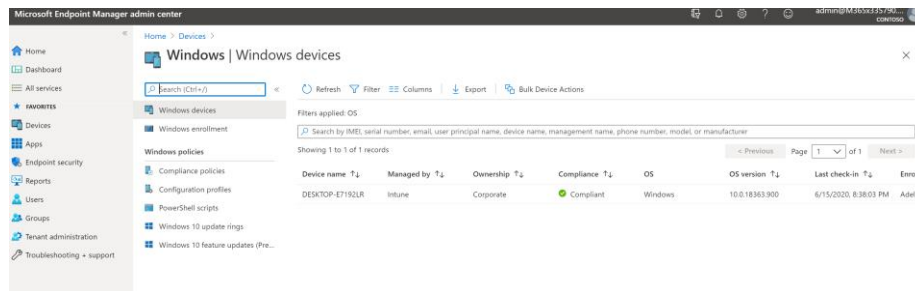
TIP: To keep managing the device with Intune but without DFCI management, self-register the device to Autopilot and enroll it in Intune. DFCI will not be applied to self-registered devices.

Optional: Reset the device and deregister the device from Autopilot

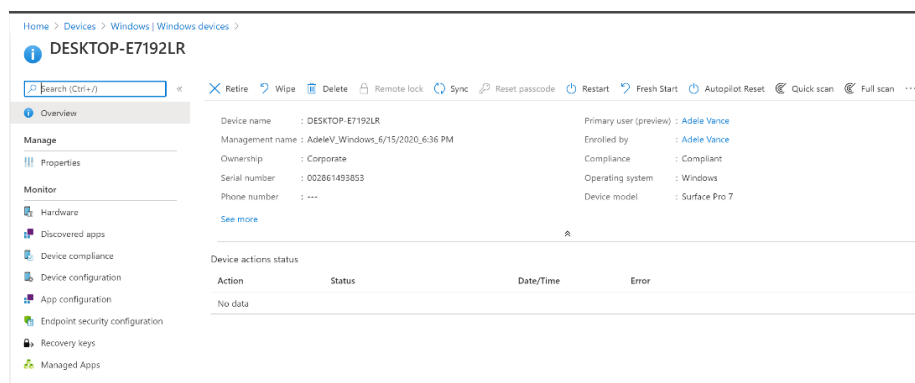
A typical end-of-life scenario would be factory resetting the device and deleting its Windows Autopilot registration.

Reset the device to OOB

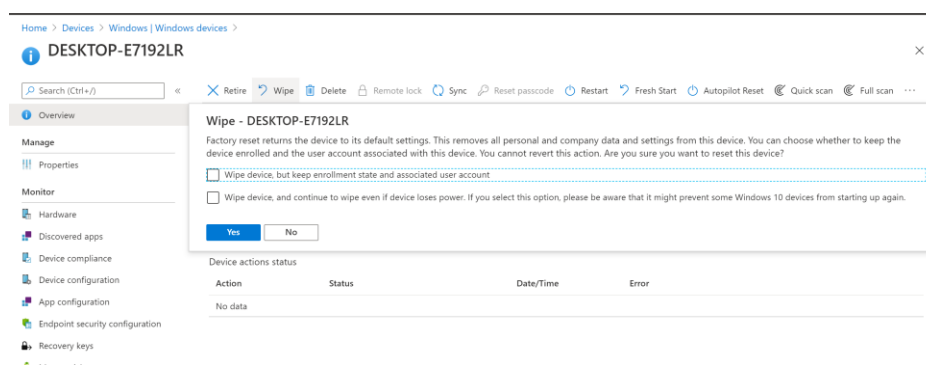
If you go back to the [Endpoint manager](#) > **Devices** > **Windows devices**, you can also see all enrolled devices.



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



If you select **Yes**, the device will be reset to its factory defaults, and the Intune object will be deleted as well.



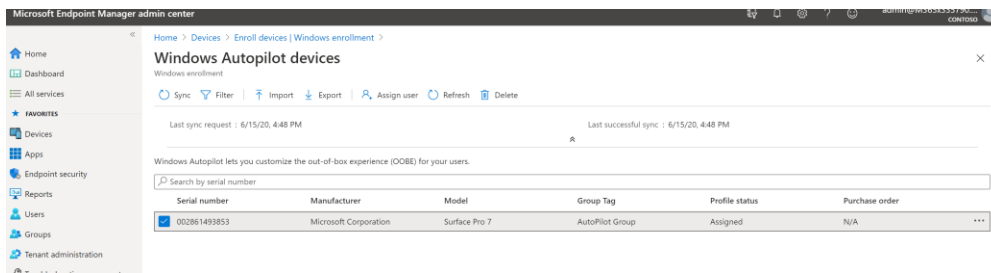
Deregister the device from Windows Autopilot

There are two options to deregister the device from Autopilot:

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

Customer de-registers device using Endpoint Manager

Go to <https://endpoint.microsoft.com> > **Devices** > **Enroll devices** > **Windows enrollment**.



Select the device in the list and select **Delete** to delete it from Autopilot

Partner de-registers device using Microsoft Partner Center

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

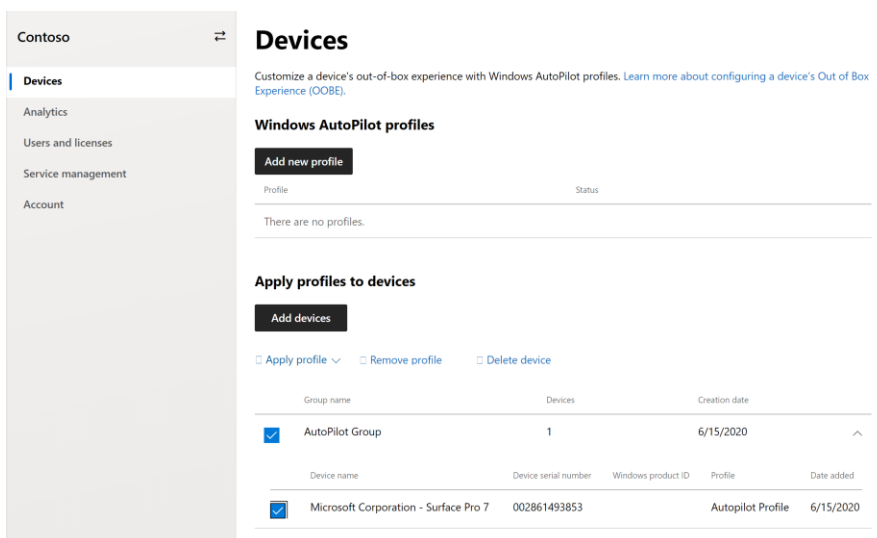
Sign in to the Microsoft Partner Center.

Go to **Customers** and choose the appropriate customer from the customer list.

Find under **Devices** the target device (check the serial number).

Check the box.

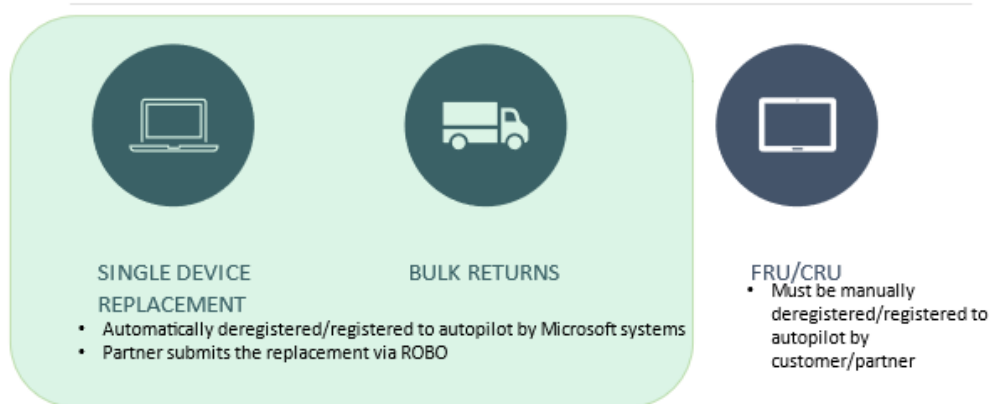
Select **Delete device**. This deletes the device from Autopilot and may take a few minutes.



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.

Returns & Exchanges



Microsoft will automatically deregister the returned device and register the replacement device in most returns and exchange scenarios. The partner only needs to make sure 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 the device for repair

Step 1: Remove the device from Autopilot and DFCI

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

Device retirement and deletion

Sign in to the [Microsoft Endpoint Manager admin center](#).

In the **Devices** pane, select **All Devices**.

Select the name of the device that you want to retire.

In the pane that shows the device name, select **Retire**. To confirm, select **Yes**.

Select the device's name you just retired in the Devices pane and select **Delete** to remove it from the tenant.

In [Endpoint Manager](#), go to **Devices > Device enrollment > Windows enrollment > Windows Autopilot Devices** and select **Sync**.

Wait 15 minutes before moving forward with any additional work on the device.

Step 2: Reset UEFI to enable boot from USB to re-image

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

UEFI password prompt

If the UEFI screen prompts for a password:

Attempt to obtain the UEFI password from the customer.

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 settings revert 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:

[Retire the device from the Intune and delete it from the tenant.](#)

Wait 10 minutes before moving forward with any additional work on the device.

Connect the device to wired internet with a Surface-branded ethernet adapter.

Restart the device and open the UEFI menu (press and hold the volume-up button while pressing and releasing the power button).

Select **Management** > **Configure** > **Refresh from Network** and then choose **Opt-Out**.

If you receive a **Success** message – you are good to continue to step 6.

If you receive a State 0 error code – please, 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.

Once the process is complete, ensure that changes to UEFI remain.

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 sent back to the customer will need to be re-enrolled into their tenant to gain the benefits of 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 | Microsoft Docs](#)
- 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 - Surface | Microsoft Docs](#)

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 will then return the Hardware Hash list in a .csv format that can be used to upload by the partner or customer.

Optional: Create and manage Autopilot profiles in MPC

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 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

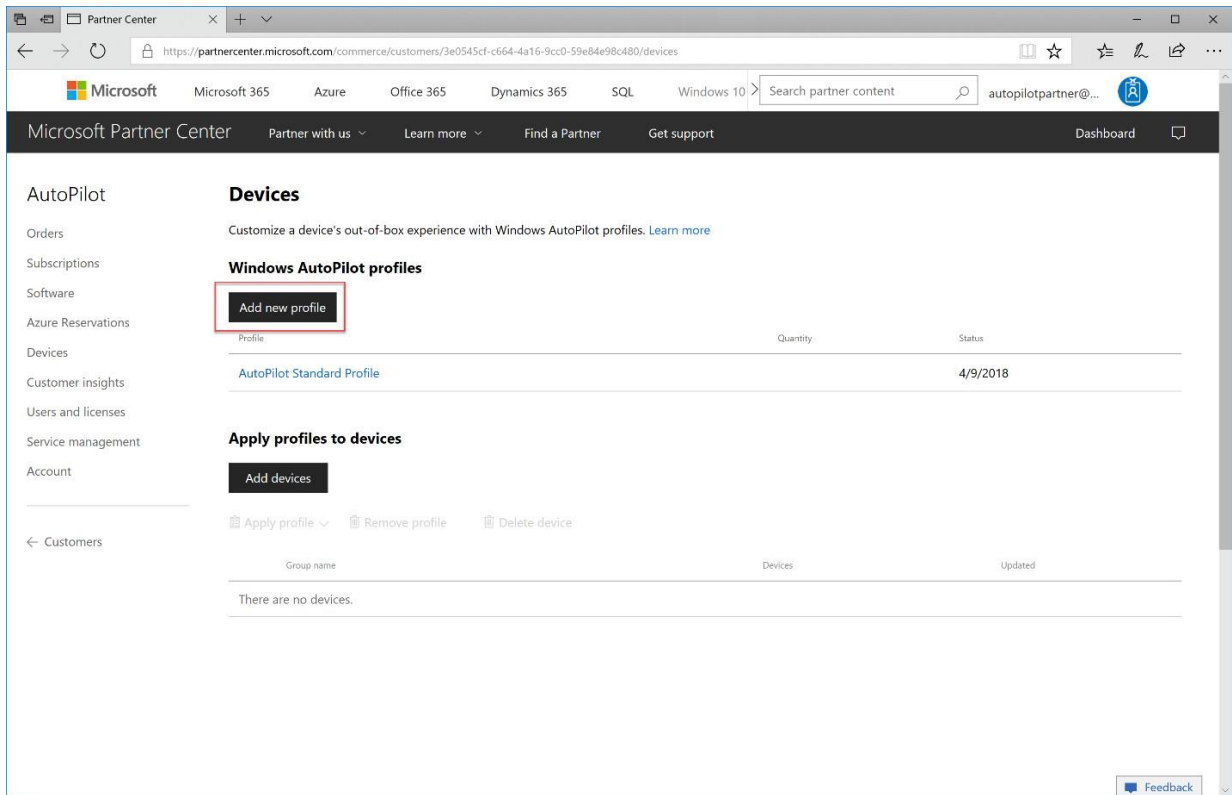
[Overview of Windows Autopilot](#).

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.

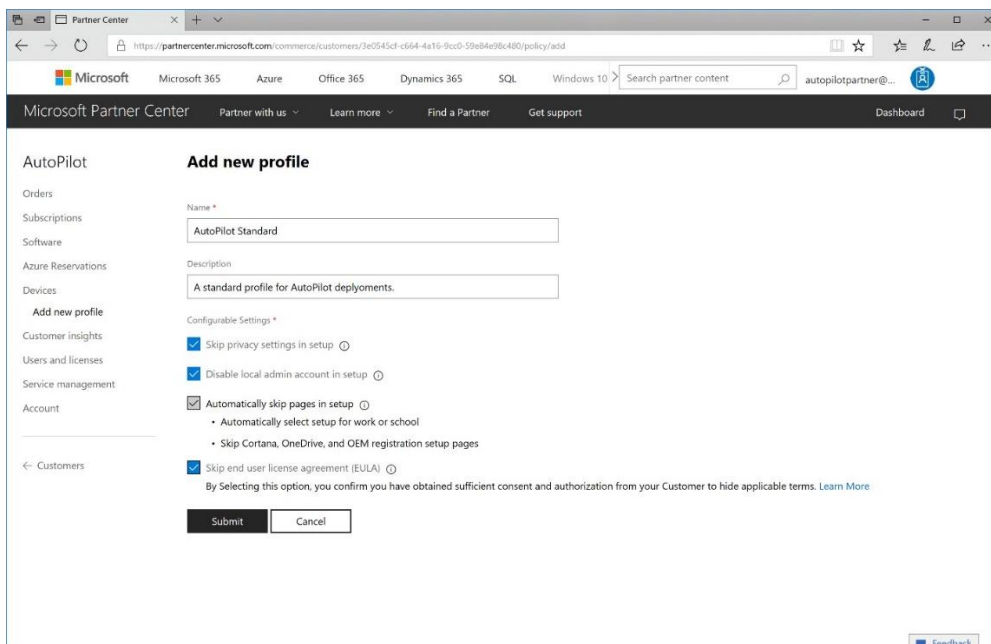
To configure settings as a partner on behalf of your customer from MPC

Open your customer account in the Partner Center from the Customers tab.

From **Devices**, select **Add new profile**.



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



Configure the OOB settings. For example, select **Skip privacy settings** in setup to disable the telemetry and privacy settings page in OOB. Note that the checkbox for **Automatically skip pages in setup** is selected by default for all Windows Autopilot deployments.

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 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.

Optional: Apply an Autopilot profile to devices in MPC

Open your customer account in the Partner Center from the Customers tab.

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.

Select **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, test the configuration on a device to ensure OOBE is appropriately managed according to your Autopilot profile configuration.

Optional: Manage devices not supported for OEM enrollment

The device's manufacturer provides support for 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 many devices for which this process will not be supported, including Surface devices 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.

Order Specific Windows 10 OS Versions for Windows Autopilot customers

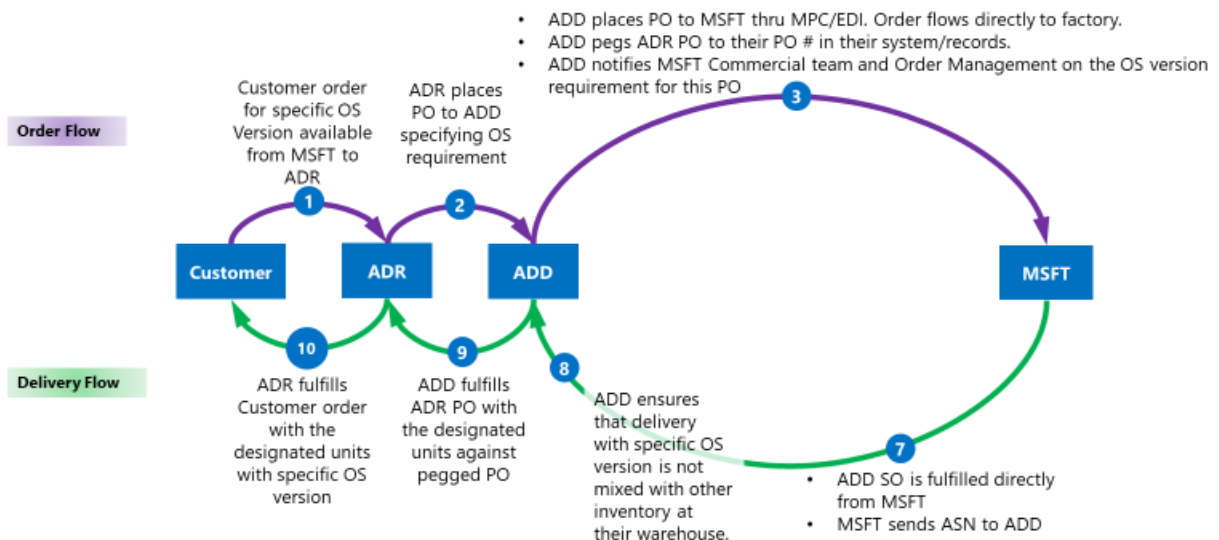
Fill the customers' orders with devices using the OS version they're using in their environment.

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 directly, 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. While a Surface Pro 7 may ship from the factory with Windows 10 1903, a Surface Laptop 3 may ship with Windows 10 1909 in May 2020. As new OS versions are injected in the factory at different times, each product may have a different OS version at any given time. Contact your Microsoft representative to find out the current OS versions shipping from Microsoft for each product. Support for pegging orders is required for partners listed on the [Windows Autopilot for Surface devices](#) page.

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



Resources

- [Windows Autopilot FAQ | Microsoft Docs](#)
- [Windows Autopilot and Surface devices | Microsoft Docs](#)
- [Surface Registration Support for Windows Autopilot | Microsoft Docs](#)
- [What is device management in Azure Active Directory?](#)
- [Windows Autopilot product site](#)
- [Overview of Windows Autopilot](#)
- [Windows 10 Subscription Activation](#)
- [Manage Windows device deployment with Windows Autopilot Deployment](#)
- [PowerShell scripts for Autopilot](#)
- [Automatically register existing device in Autopilot](#)

Troubleshooting Autopilot

- [Troubleshooting Windows Autopilot, a reference](#)
- [Troubleshooting Windows Autopilot Hybrid Azure AD Join](#)

Additional capabilities

Here is a list and description of "a la carte" options for layering additional capabilities and scenarios to the base POC.

[Surface Diagnostic Toolkit \(SDT\) for Business](#)

The Microsoft Surface Diagnostic Toolkit for Business 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](#)

Windows Update for Business enables information technology administrators to keep the Windows 10 devices in their organization continually updated with the latest security defenses and Windows features by directly connecting these systems to the 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 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.