

Windows Autopilot documentation

Windows Autopilot and Windows Autopilot device preparation is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use.

Windows Autopilot solutions

GET STARTED

[Compare Windows Autopilot device preparation and Windows Autopilot](#)

Understand Windows Autopilot device preparation

OVERVIEW

[Overview of Windows Autopilot device preparation](#)

[Requirements](#)

[Reporting and monitoring](#)

Understand Windows Autopilot

OVERVIEW

[Overview of Windows Autopilot](#)

[Requirements](#)

[Device registration overview](#)

[Enrollment Status Page](#)

[Manually register devices](#)

Tutorials

TUTORIAL

[Windows Autopilot scenarios](#)

[Windows Autopilot device preparation scenarios](#)

Compare Windows Autopilot device preparation and Windows Autopilot

Article • 02/13/2025 • Applies to:  Windows 11

Windows Autopilot device preparation vs. Windows Autopilot

[] Expand table

Feature	Windows Autopilot device preparation	Windows Autopilot
Features	<ul style="list-style-type: none">Support for Government Community Cloud High (GCCH) and Department of Defense (DoD) environments.Faster, more consistent provisioning experience.Near real-time monitoring and troubleshooting info.	<ul style="list-style-type: none">Support for multiple device types (HoloLens, Teams Meeting Room).Many customization options for the provisioning experience.
Supported modes	<ul style="list-style-type: none">User-driven.	<ul style="list-style-type: none">User-driven.Pre-provisioned.Self-deploying.Existing devices.
Join types supported	<ul style="list-style-type: none">Microsoft Entra join.	<ul style="list-style-type: none">Microsoft Entra join.Microsoft Entra hybrid join.
Device registration required?	No.	Yes.
What do admins need to configure?	<ul style="list-style-type: none">Windows Autopilot device preparation policy.Device security group with Intune Provisioning Client as owner.	<ul style="list-style-type: none">Windows Autopilot deployment profile.Enrollment Status Page (ESP).

Feature	Windows Autopilot device preparation	Windows Autopilot
What configurations can be delivered during provisioning?	<ul style="list-style-type: none"> • Device-based only during the out-of-box experience (OOBE). • Up to 10 essential applications (line-of-business (LOB), Win32, Microsoft Store, Microsoft 365). • Up to 10 essential PowerShell scripts. 	<ul style="list-style-type: none"> • Device-based during device ESP. • User-based during user ESP. • Up to 100 applications.
Reporting & troubleshooting	<p>Windows Autopilot device preparation deployment report:</p> <ul style="list-style-type: none"> • Shows all Windows Autopilot device preparation deployments. • More data available. • Near real-time. 	<p>Windows Autopilot deployment report:</p> <ul style="list-style-type: none"> • Only shows Windows Autopilot registered devices. • Not real-time.
Supports LOB and Win32 applications in same deployment?	Yes.	No.
Supported versions of Windows	<ul style="list-style-type: none"> • Windows 11, version 24H2 or later. • Windows 11, version 23H2 with KB5035942 or later. • Windows 11, version 22H2 with KB5035942 or later. 	<ul style="list-style-type: none"> • All currently supported versions of Windows 11 General Availability Channel. • All currently supported versions of Windows 10 General Availability Channel.

Which Windows Autopilot solution to use

Which version of Windows Autopilot to use is dependent on many factors and variables, with each environment having different needs. Windows Autopilot device preparation in its initial offering isn't as feature rich as Windows Autopilot, but it does have some advantages and features not available in Windows Autopilot.

In general, the following are some of the major factors when considering between Windows Autopilot device preparation or Windows Autopilot:

[] [Expand table](#)

Requirement	Windows Autopilot device preparation	Windows Autopilot
Government Community Cloud High (GCCH) and Department of Defense (DoD) environments	✓	✗
User-driven scenario	✓	✓
Pre-provisioned scenario	✗	✓
Self-deploying scenario	✗	✓
Existing devices scenario	✗	✓
Autopilot reset support	✗	✓
Microsoft Entra join	✓	✓
Microsoft Entra hybrid join	✗	✓
Windows Autopilot Reset	✗	✓
Windows 11	✓	✓
Windows 10	✗	✓
Deploy Win32 and LOB applications in the same deployment	✓	✗
Simpler deployment configuration and experience	✓	✗
Extensive customization of deployment and OOBE experience	✗	✓
No requirement to pre-stage devices	✓	✗
Install more than 10 applications during OOBE	✗	✓
Run more than 10 PowerShell scripts during OOBE	✗	✓
Near real-time monitoring	✓	✗
Block user from accessing desktop until user based configurations are applied	✗	✓
HoloLens support	✗	✓
Teams Meeting Room support	✗	✓
Device Firmware Configuration Interface (DFCI) Management support	✗	✓
Autopilot into co-management	✗	✓

Using Windows Autopilot device preparation and Windows Autopilot concurrently

Windows Autopilot device preparation and Windows autopilot can be used concurrently and side by side within an organization. However, any one device in an environment can only run one of the two solutions. Windows Autopilot profiles take precedence over Windows Autopilot device preparation policies. If a Windows Autopilot registered device needs to go through a Windows Autopilot device preparation deployment, it must first be removed as a Windows Autopilot device. For more information, see [Deregister a device](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot device preparation: What's new

Article • 10/15/2024 • Applies to: Windows 11

Tip

RSS can be used to notify when new features for Windows Autopilot device preparation are added to this page. For example, the following RSS link includes this article:

url

```
https://learn.microsoft.com/api/search/rss?  
search=%22News+and+resources+about+the+latest+updates+of+Windows+Autopi  
lot+device+preparation.%22&locale=en-us&%24filter=
```

This example includes the `&locale=en-us` variable. The `locale` variable is required, but it can be changed to another supported locale. For example, `&locale=es-es`.

For more information on using RSS for notifications, see [How to use the docs](#) in the Intune documentation.

Diagnostics logs automatically available in Windows Autopilot device preparation deployment status report

Date added: October 9, 2024

Admins can now download diagnostics logs for failed Autopilot device preparation deployments directly from the [Windows Autopilot device preparation deployment status report](#). Logs are available for download in the [Device deployment details](#) when you select a failed deployment under the [Device tab](#). Logs are automatically collected when an error occurs during deployment.

Windows Autopilot Device Preparation Support in Intune operated by 21Vianet in China

Date added: *September 18, 2024*

As part of the 2409 Intune release, we're announcing support for Windows Autopilot Device Preparation policy in [Intune operated by 21Vianet in China](#) cloud. Customers with tenants located in China can now provision devices and manage through Microsoft Intune. For an overview, see [Overview of Windows Autopilot device preparation](#). For a tutorial on how to set up Windows Autopilot device preparation, see [Windows Autopilot device preparation scenarios](#).

enrollmentProfileName property is now populated with the Device preparation policy name

Date added: *September 13, 2024*

As part of the 2409 Intune release, the **enrollmentProfileName** property is now populated with the Device preparation policy name during Autopilot device preparation deployments. The Enrollment profile property of Intune and Microsoft Entra device objects are automatically populated with the name of the Device preparation policy that was applied to the device during provisioning. The **enrollmentProfileName** property enables admins to configure assignment filters and dynamic groups based on the **enrollmentProfileName** property for configurations post-enrollment.

Windows Autopilot device preparation deployment status report available in the Monitor tab under Enrollment

Date added: *August 21, 2024*

In addition to the [Devices | Monitor](#) page, admins can now easily access the **Windows Autopilot device preparation deployment status report** from the **Monitor** tab in the [Devices | Enrollment](#) page. The report can be found using the following steps:

1. Sign into the [Microsoft Intune admin center](#).
2. Navigate to **Home > Devices > Device onboarding | Enrollment**.
3. Select the **Monitor** tab in the [Devices | Enrollment](#) page.

Corporate identifiers can now be used with Windows Autopilot device preparation

Date added: *July 8, 2024*

Customers who are blocking personal device enrollments can now use Windows Autopilot device preparation by pre-uploading the model, manufacturer, and serial number for all devices which will deploy with Autopilot device preparation. For more information, see [Add Windows corporate identifiers](#).

Additional role-based access control (RBAC) permissions for Managed apps and Mobile apps

Date added: *June 18, 2024*

We added additional RBAC permissions for **Managed apps** and **Mobile apps** for the Windows Autopilot device preparation administrator role. For more information, see [Required RBAC permissions](#).

Initial release of Windows Autopilot device preparation

Date added: *June 3, 2024*

Windows Autopilot device preparation is generally available. For an overview, see [Overview of Windows Autopilot device preparation](#). For a tutorial on how to set up Windows Autopilot device preparation, see [Windows Autopilot device preparation scenarios](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Overview of Windows Autopilot device preparation

Article • 02/04/2025 • Applies to:  [Windows 11](#)

Windows Autopilot device preparation is used to set up and configure new devices, getting them ready for productive use. Windows Autopilot device preparation aims to simplify device deployment by delivering consistent configurations, enhancing the overall setup speed, and improving troubleshooting capabilities.

This article explores the capabilities of the Windows Autopilot device preparation, its benefits for administrators, and the user experience it offers including:

- Reducing the time IT spends on deploying devices.
- Reducing the infrastructure required to maintain the devices.
- Maximizing ease of use for all types of end users.
- Improved troubleshooting.
- Near real-time deployment status and monitoring.

Note

This article is for Windows Autopilot device preparation. For Windows Autopilot, see [Overview of Windows Autopilot](#).

Requirements

- Windows 11, version 24H2 or later.
- Windows 11, version 23H2 with [KB5035942](#) or later.
- Windows 11, version 22H2 with [KB5035942](#) or later.
- Microsoft Entra ID - only Microsoft Entra join is supported.
- Device shouldn't be registered or added as a Windows Autopilot device - if the device is registered or added as Windows Autopilot device, the Windows Autopilot profile takes precedence over the Windows Autopilot device preparation policy. If a device needs to be removed as a Windows Autopilot device, see [Deregister a device](#).

For additional detailed requirements, see [Windows Autopilot device preparation requirements](#).

Process overview

When new Windows devices are initially deployed, Windows Autopilot device preparation uses the OEM-optimized version of Windows client. The OEM-optimized version of Windows client is preinstalled on the device, so custom images and drivers don't need to be maintained for every device model. Instead of re-imaging the device, with Windows Autopilot device preparation, the existing Windows installation can be transformed into a "business-ready" state that can:

- Deliver Windows Autopilot device preparation configuration during user authentication during the out-of-box experience (OOBE).
- Automatically add devices to the device security group and receive selected applications and PowerShell scripts assigned to the group.

Windows Autopilot device preparation improvements

Windows Autopilot device preparation is an improved profile experience that incorporates common customer asks. It improves the onboarding experience by providing a profile experience to deploy configurations efficiently, consistently, and remove the complexity out of troubleshooting. Its goal is to be:

- Simple.
- Fast.
- Observable.
- Reliable.

New features in Windows Autopilot device preparation include:

- **Utilizing enrollment time grouping in Intune** - Device is added to a device security group at enrollment time and configuration is delivered immediately. This feature provides a faster and more reliable setup. For more information, see [Enrollment Time Grouping](#).
- **Out of the box granular reporting** - Improved monitoring and troubleshooting. Out of the box monitoring and reporting with near real-time status of deployments, including:
 - Applications status
 - PowerShell scripts status
 - Deployment time. For more information, see [Windows Autopilot device preparation reporting and monitoring](#).

- **Support for Government Community Cloud High (GCCH) and Department of Defense (DoD) environments** - Windows Autopilot device preparation supports GCCH and DoD environments.

Capabilities

Windows Autopilot device preparation capabilities include:

- Set up user-driven deployment flow.
- By default, making sure users are standard non-administrator users.
- Select application and PowerShell script to be delivered during OOBE.
- Simplified and clear OOBE user experience with percentage progress indicator.
- Deployment report for better troubleshooting.

Improved experiences

Admin experience

- Windows Autopilot device preparation simplifies admin configuration by having a single profile to provision all policies in one location, including deployment and OOBE settings.
- Line-of-business (LOB) and Win32 applications can be deployed in the same deployment.

User experience

Windows Autopilot device preparation also improves the user experience in the following ways:

- A simplified view during OOBE where the percentage of progress is displayed.
- The experience is more consistent.
- The user is informed when the OOBE setup is complete.
- When issues arise, logs can be exported with ease.
- The end-user gets to the desktop faster.

Troubleshooting and Reporting

Windows Autopilot device preparation offers near real-time status updates on deployments. Windows Autopilot device preparation monitoring includes application

and PowerShell script status information, allowing for improved troubleshooting and reporting. Deployment monitoring includes the following features:

- Easily track which devices went through Autopilot.
- Track status and deployment phase for each device in near real-time.
- Each device has the following details in the monitoring report:
 - Device details.
 - Profile name and version.
 - Deployment status details.
 - Apps applied with status.
 - Scripts applied with status.

Enrollment Time Grouping

The key to Windows Autopilot device preparation is Enrollment Time Grouping. With Enrollment Time Grouping, when a user authenticates into a device, the device is added to a pre-defined device security group during enrollment. Applications, scripts, and policies assigned to the device group are then deployed to the device. Direct assignment of devices to the device group allows the applications, scripts, and policies assigned to the device group to deploy quicker and more efficiently versus when using a dynamic device group.

Enrollment time grouping consists of the following phases:

- **Configure applications and policies to a security group** - User authenticates and the Windows Autopilot device preparation configuration is delivered.
- **Select applications and PowerShell scripts to get installed during OOB** - Selected applications and PowerShell scripts assigned to the device security group are installed. The device also joins the device security group.

For Windows Autopilot device preparation:

- The device group is selected in the Windows Autopilot device preparation profile.
- Only applications and PowerShell scripts selected in the Windows Autopilot device preparation profile are deployed during OOB. Any additional applications or PowerShell scripts assigned to the device group will be deployed after the Windows Autopilot device preparation deployment is complete.
- For policies, Windows Autopilot device preparation syncs any policies assigned to the device group. However, Windows Autopilot device preparation doesn't track if the policies are applied during the deployment. The policies might be applied either during the deployment or after the deployment is complete.

For more information, see [Enrollment time grouping in Microsoft Intune](#).

Corporate identifiers for Windows

Windows Autopilot device preparation supports the Intune corporate identifier enrollment feature. Corporate identifiers in Intune allows pre-uploading of Windows device identifiers (serial number, manufacturer, model) and ensures only trusted devices go through Windows Autopilot device preparation.

Windows Autopilot device preparation only requires corporate identifiers for Windows if Intune enrollment restrictions are being used to block personal device enrollments. For more information, see:

- [Identify devices as corporate-owned.](#)
- [What are enrollment restrictions?.](#)
- [Create device platform restrictions.](#)

Tutorial

For tutorials with detailed instructions on configuring Windows Autopilot device preparation, see [Windows Autopilot device preparation scenarios](#).

Related content

- [Windows Autopilot device preparation FAQs.](#)
- [Windows Autopilot device preparation tutorial.](#)
- [Windows Autopilot device preparation requirements.](#)
- [Windows Autopilot device preparation reporting and monitoring.](#)
- [Windows Autopilot device preparation known issues.](#)
- [Windows Autopilot device preparation: What's new.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot device preparation requirements

Article • 01/24/2025 • Applies to:  Windows 11

Tip

RSS can be used to notify when requirements are added or updated to this page. For example, the following RSS link includes this article:

url

```
https://learn.microsoft.com/en-us/search/?  
terms=%22Software%2C%20Networking%2C%20Licensing%2C%20Configuration%2C%  
20and%20RBAC%20requirements%20for%20Windows%20Autopilot%20device%22
```

This example includes the `&locale=en-us` variable. The `locale` variable is required, but it can be changed another supported locale. For example, `&locale=es-es`.

For more information on using RSS for notifications, see [How to use the docs](#) in the Intune documentation.

The list of requirements for Windows Autopilot device preparation is organized into five different categories:

- **Software** - OS requirements.
- **Networking** - networking requirements.
- **Licensing** - licensing requirements.
- **Configuration** - configurations required in Microsoft Entra ID and Microsoft Intune.
- **RBAC** - RBAC permissions required for a Windows Autopilot device preparation administrator.

Select the appropriate tab to see the relevant requirements:

 Software

Software requirements

Windows Autopilot device preparation depends on specific features available in Windows client, Microsoft Entra ID, and a mobile device management (MDM) service such as Microsoft Intune. To use Windows Autopilot device preparation and access these features, some software requirements must be met.

Windows 11

- Windows 11, version 24H2 or later
- Windows 11, version 23H2 with [KB5035942](#) or later - Windows installation media dated April 2024 or later has [KB5035942](#) included.
- Windows 11, version 22H2 with [KB5035942](#) or later - Windows installation media dated April 2024 or later has [KB5035942](#) included.

Important

- Verify with OEMs that devices shipped from the OEM have the minimum required update installed.
- If installing Windows from installation media, verify that the media has the minimum required update installed. Updated Windows installation media with the latest cumulative update already installed is available at the [Volume Licensing Service Center \(VLSC\)](#).

The following editions are supported:

- Windows 11 Pro.
- Windows 11 Pro Education.
- Windows 11 Pro for Workstations.
- Windows 11 Enterprise.
- Windows 11 Education.
- [Windows 11 Enterprise LTSC](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Windows Autopilot device preparation reporting and monitoring

Article • 06/03/2024 • Applies to:  Windows 11

Out of the box reporting and monitoring with near real-time status of deployments, including applications and PowerShell scripts details and deployment time. This feature provides improved troubleshooting.

Accessing reports and near real-time monitoring

To access Windows Autopilot device preparation reports and monitor deployments in near real-time:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, select **Monitor**.
4. In the **Devices | Monitor** screen, in the list of reports under **Report name**, select **Windows Autopilot device preparation deployments**.
5. The **Device enrollment - Autopilot deployments** screen opens. In the **Device enrollment - Autopilot deployments** screen, deployments of individual devices is shown. Each device has the following information:
 - **Device name** - the name given to the device during the deployment. Selecting this item goes to the deployment details for the device.
 - **Enrollment date** - the date and time that the device enrolled.
 - **Deployment status** - displays the current status of the deployment on the device. During deployment, the status shows **In progress**. Once deployment is complete, it shows the final outcome of the deployment as either **Success** or **Failed**.
 - **Phase** - shows the last reported phase that the deployment is at.
 - **Serial number** - the hardware serial number of the device.
 - **Deployment time** - the amount of time that the deployment took during the out-of-box experience (OOBE) to complete. If the deployment isn't complete, it shows **In progress**.

- **UPN** - the user that signed into the device during OOB and that the Windows Autopilot device preparation policy was assigned to.

6. Select an individual device under **Device name**. The **Device deployment details** pane opens. The **Device deployment details** pane contains three sections:

a. **Device** - contains information regarding the device, including:

- **Device name** - the name given to the device during the deployment. Selecting this item goes to the device details in Intune.
- **Deployment status** - displays the current status of the deployment on the device. During deployment, the status shows **In progress**. Once deployment is complete, it shows the final outcome of the deployment as either **Success** or **Failed**.
- **Device ID** - the device ID of the device in Intune.
- **Microsoft Entra device ID** - the device ID of the device in Microsoft Entra ID.
- **Serial number** - the hardware serial number of the device.
- **Deployment policy** - the Windows Autopilot device preparation policy the device received.
- **Policy Version** - the version of the Windows Autopilot device preparation policy the device received. The version number increments by one each time a change is made and saved to the Windows Autopilot device preparation policy.
- **OS version** - the version of Windows installed on the device during the deployment.

b. **Apps** - reflects the last reported status for the applications being installed during the Windows Autopilot device preparation including the list of applications being installed. Statuses include:

- **Installed** - application was successfully installed.
- **In progress** - application is currently being installed.
- **Skipped** - usually indicates that the application was selected in the Windows Autopilot device preparation policy, but wasn't assigned to the device group specified in the Windows Autopilot device preparation policy. It can also mean that the application isn't applicable to the device.
- **Failed** - the application failed to install. Check logs for further details.

c. **Scripts** - contains information regarding the PowerShell scripts being run during the Windows Autopilot device preparation including the list of scripts being run. Statuses include:

- **Installed** - the PowerShell script successfully ran.
 - **In progress** - the PowerShell script is currently running.
 - **Skipped** - usually indicates that the PowerShell script was selected in the Windows Autopilot device preparation policy, but wasn't assigned to the device group specified in the Windows Autopilot device preparation policy.
 - **Failed** - the PowerShell script failed to run. Check logs for further details.
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback !\[\]\(0e60d2d9b679b4cf53dbe1e685ee345d_img.jpg\)](#)

Windows Autopilot device preparation FAQ

FAQ

Applies to:

- [Windows 11](#).

This article provides OEMs, partners, administrators, and users with answers to some frequently asked questions about deploying Windows with Windows Autopilot device preparation.

How is Windows Autopilot device preparation different from Windows Autopilot?

Windows Autopilot device preparation is a re-architecture of Windows Autopilot. While the experience to OEMs, IT admins, and users is similar, the underlying architecture is different. The updated architecture in Windows Autopilot Device preparation gives new capabilities that improves the deployment experience.

Who does Windows Autopilot device preparation benefit?

Windows Autopilot device preparation benefits government customers who can now use Windows Autopilot device preparation to streamline their deployments at scale. It also benefits new customers onboarding Windows Autopilot device preparation by reducing the complexity of setting up the deployment.

Is Windows Autopilot device preparation available in all sovereign clouds?

Windows Autopilot device preparation is available for Government Community Cloud (GCC) High and U.S. Department of Defense (DoD). It'll be available for Intune operated

by 21Vianet in China later this year.

What scenarios does Windows Autopilot device preparation support?

Currently Windows Autopilot device preparation only supports the user-driven scenario.

What about the other Windows Autopilot scenarios like pre-provisioning and self-deploying mode?

The pre-provisioning mode and self-deploying mode scenarios will be supported in the future, but aren't part of the initial release.

Why is there a limit on the number of applications and PowerShell scripts in the Windows Autopilot device preparation policy?

We limited the number of applications that can be applied during the out-of-box experience (OOBE) to increase stability and achieve a higher success rate. Looking at our telemetry, almost 90% of all Autopilot deployments are deployed with 10 or fewer apps. This limit is intended to improve the overall user experience so that users can become more productive quickly. We understand that there are outliers and companies that want to target more during setup. However, for the user-driven approach, we want to use the desktop experience for non-essential applications.

Does Windows Autopilot device preparation support deploying both Win32 and line-of-business (LOB) applications in the same deployment?

Yes. While we always recommend Win32 applications, mixing applications in Windows Autopilot deployments might result in errors. With the Windows Autopilot device preparation, we have streamlined the providers so different application types shouldn't affect each other.

What is the guidance on user-based targeting vs device-based targeting?

Only device-based configurations are delivered during OOBE. For this reason:

- Assign security policy to devices.
- Ensure all selected applications in the Windows Autopilot device preparation policy are set to install in the **System** context.
- Ensure all selected applications in the Windows Autopilot device preparation policy are targeted to the device security group specified in the Windows Autopilot device preparation policy.
- Ensure all selected PowerShell scripts in the Windows Autopilot device preparation policy are targeted to the device security group specified in the Windows Autopilot device preparation policy.

How do users know when the required setup is complete?

Many users aren't sure when the provisioning process is complete. To help mitigate confusion and calls to support, we added a completion page in OOBE. The completion page lets the user know that OOBE setup is complete. However, additional installations that were assigned to the device group but not specified in the Windows Autopilot device preparation policy might still be occurring in the background.

Can Windows Autopilot Device preparation be used by non-Microsoft mobile device management (MDM) providers?

Windows Autopilot device preparation will support non-Microsoft MDMs. In this initial release, configuration is only possible via Intune.

Is Windows Autopilot device preparation available on Windows 10 devices?

Currently, Windows Autopilot device preparation is only available on:

- Windows 11, version 23H2 with [KB5035942](#) or later.
- Windows 11, version 22H2 with [KB5035942](#) or later.

Do existing Windows Autopilot profiles need to be migrated to Windows Autopilot device preparation?

There's no need to migrate from existing Windows Autopilot profiles to Windows Autopilot device preparation policies. We expect both solutions to exist in parallel for a while as we work to improve the experience and add more functionality.

Does this mean that Windows Autopilot isn't being invested in any longer?

Not at all! We're continuing to work on Windows Autopilot in parallel with developing Windows Autopilot device preparation. The first release of Windows Autopilot device preparation doesn't have all the scenarios of Windows Autopilot, specifically pre-provisioning and self-deploying modes, so we'll continue to invest in those areas. Additionally, in the future, we plan to add any high value features from Windows Autopilot device preparation to Windows Autopilot to improve the experience for all customers.

Does Windows Autopilot device preparation support Microsoft Entra hybrid join?

No. Windows Autopilot device preparation only supports Microsoft Entra join.

What type of applications does Windows Autopilot device preparation support?

The following types of applications are supported for use with Windows Autopilot device preparation:

- [Line-of-business \(LOB\)](#).
- [Win32](#).
- [Microsoft Store](#) - only Microsoft Store apps that support WinGet are supported.
- [Microsoft 365](#).

Do devices need to be pre-staged with Windows Autopilot device preparation?

No. Windows Autopilot device preparation policies are deployed to a user group and not a device group. Once a user in that user group signs into the device during OOBE, the Windows Autopilot device preparation deployment begins. During the deployment, the device is then automatically added to the device group specified in the Windows Autopilot device preparation policy.

Which Windows Autopilot device preparation policy receives priority if multiple policies are deployed to a user?

If multiple Windows Autopilot device preparation policies are deployed to a user, the policy with the highest priority gets priority. Policy priorities are displayed at the **Home > Enroll devices | Windows enrollment > Device preparation policies** screen. The policy with the highest priority is higher in the list and has the smallest number under the **Priority** column. To change a policy's priority, move it in the list by dragging the policy within the list.

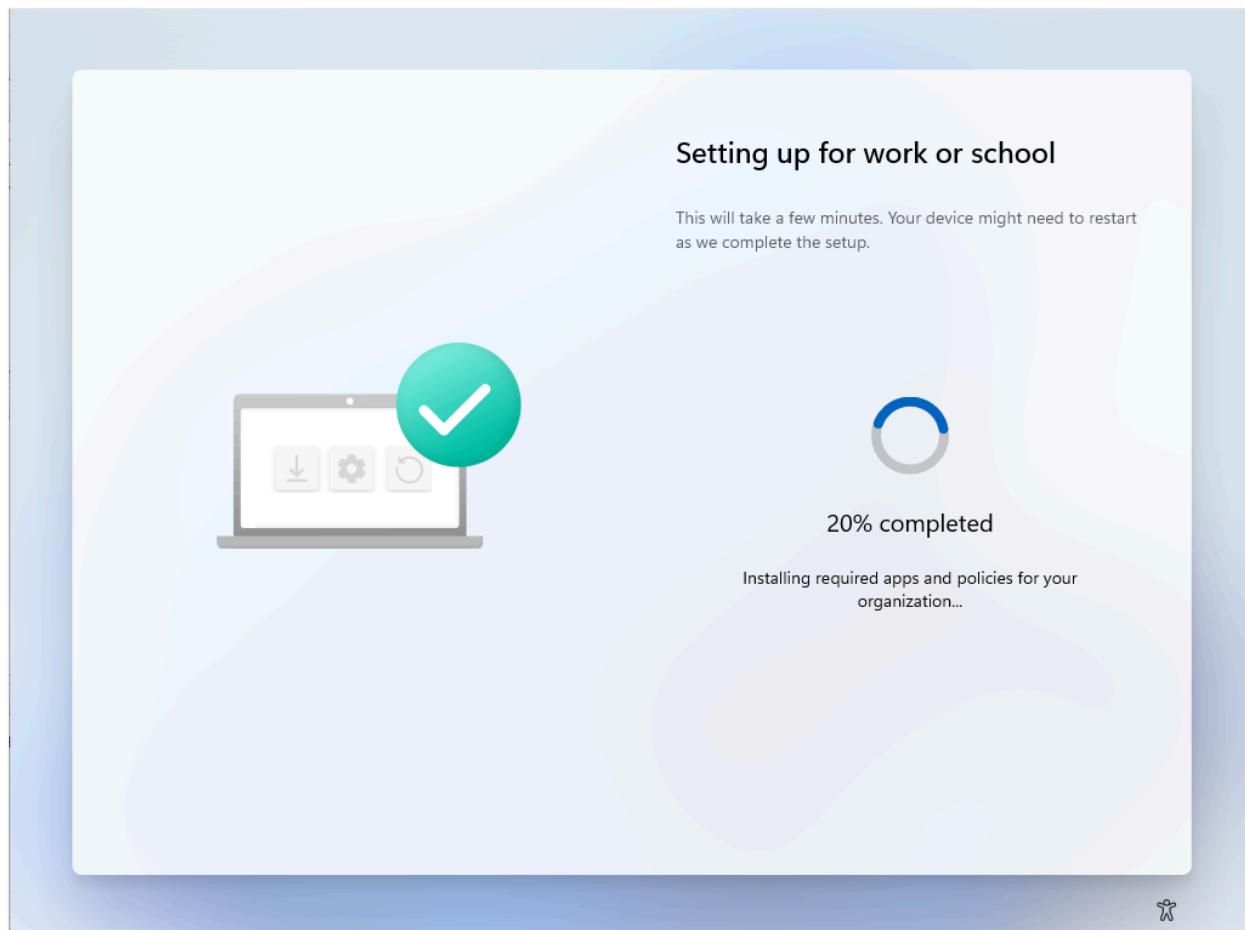
What makes Windows Autopilot device preparation deployments faster and

more efficient than Windows Autopilot?

The key to making Windows Autopilot device preparation deployments faster and more efficient than Windows Autopilot is [Enrollment Time Grouping](#). With Enrollment Time Grouping, devices are automatically added to an assigned device group specified in the Windows Autopilot device preparation policy. Since the device group is assigned instead of dynamic as used in Windows Autopilot, anything assigned to the device group is processed faster and more efficiently. The assigned group eliminates the need to perform queries that are required with dynamic groups.

How does a user know that a Windows Autopilot device preparation deployment is running on their device?

During a Windows Autopilot device preparation deployment, a **Setting up for work or school** window with a round progress bar displays on the device:



Windows Autopilot device preparation doesn't use the Enrollment Status Page (ESP) like Windows Autopilot. If the ESP displays during the deployment, then the device isn't

running a Windows Autopilot device preparation deployment. Instead, the device might be:

- A Windows Autopilot registered device.
- A Windows Autopilot profile is assigned to the device.

Verify that the device isn't registered as a Windows Autopilot device and that a Windows Autopilot profile isn't assigned to the device. Windows Autopilot profiles take precedence over Windows Autopilot device preparation policies.

If a device needs to be removed as a Windows Autopilot device, see [Deregister a device](#).

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) ↗

Windows Autopilot device preparation troubleshooting FAQ

FAQ

Applies to:

- Windows 11.

This article provides troubleshooting for common Windows Autopilot device preparation issues.

Device isn't being added to the device group specified in the Windows Autopilot device preparation policy.

- Verify that **Intune Provisioning Client** is set as the owner for the device group specified in the Windows Autopilot device preparation policy. For more information, [Create a device group](#).
- Verify that the correct device group is specified in the Windows Autopilot device preparation policy. For more information, see [Create a Windows Autopilot device preparation policy](#) and [Create a device group](#).
- Verify that **Microsoft Entra roles can be assigned to the group** setting in the device group is set to **No**. For more information, see [Create a device group](#).
- Verify that the admin creating the Autopilot device preparation policy has the **Enrollment time device membership assignment** RBAC permission. For more information, see [Required RBAC permissions](#).

Windows Autopilot device preparation experience never launches during the out-of-box experience (OOBE).

- Verify that the minimum version of Windows is being used as documented in [Software requirements](#). This requirement includes that the minimum required update is installed before starting the device for the first time:

- Verify with OEMs that devices shipped from the OEM have the minimum required update installed.
- If installing Windows from installation media, verify that the media has the minimum required update installed. Updated Windows installation media with the latest cumulative update already installed is available at the [Volume Licensing Service Center \(VLSC\)](#).
- Windows Autopilot device preparation doesn't use the Enrollment Status Page (ESP). Since Windows Autopilot device preparation doesn't use the ESP, the ESP shouldn't display during a Windows Autopilot device preparation deployment. If the ESP displays during the deployment, then the device isn't running a Windows Autopilot device preparation deployment. Instead, the device might be:
 - A Windows Autopilot registered device.
 - A Windows Autopilot profile is assigned to the device.

Verify that the device isn't registered as a Windows Autopilot device and that a Windows Autopilot profile isn't assigned to the device. Windows Autopilot profiles take precedence over Windows Autopilot device preparation policies.

If a device needs to be removed as a Windows Autopilot device, see [Deregister a device](#).

- Verify that the user signing into the device during OOBE is a member of the user group specified in the Windows Autopilot device preparation policy. For more information, see [Create a Windows Autopilot device preparation policy](#) and [Create a user group](#).
- Verify that a device group is selected in the Windows Autopilot device preparation policy. A Windows Autopilot device preparation policy can be created without selecting a device group. For more information, see [Create a Windows Autopilot device preparation policy](#) and [Create a device group](#).
- If using corporate identifiers in Intune, make sure that a corporate identifier is added for the device. For more information, see [Add Windows corporate identifiers](#).
- Verify that Windows automatic Intune enrollment is configured.
- Verify that users are allowed to join device to Microsoft Entra ID.

Applications or PowerShell scripts aren't getting installed.

- If the applications or PowerShell scripts are showing **Skipped** in the details of the Windows Autopilot device preparation deployment report, verify that they're assigned to the device group specified in the Windows Autopilot device preparation policy. For more information, see [Windows Autopilot device preparation policy configuration settings](#) and [Create a device group](#).
- Verify that the application or PowerShell script is configured to install in the **System** context. During OOBE, applications are installed and PowerShell scripts run when no user is signed in. For this reason, they must be configured to install in the **System** context.

Device security group isn't saving in Windows Autopilot device preparation policy.

This issue usually occurs if **Intune Provisioning Client** with AppID of **f1346770-5b25-470b-88bd-d5744ab7952c** isn't the owner of the device group specified in the Windows Autopilot device preparation policy. When the issue occurs, one of the following error messages might display when saving the Windows Autopilot device preparation policy:

- **There was a problem with the device security group for <policy_name>. Check the group meets the requirements.**
- **Failed to update security group device preparation setting: Updating security group for device preparation setting <policy_name> failed. Something went wrong.**

Additionally, **Device group** in the Windows Autopilot device preparation policy shows **0 groups assigned**.

To fix the issue, add the **Intune Provisioning Client** service principal with AppID of **f1346770-5b25-470b-88bd-d5744ab7952c** as the owner of the device security group specified in the Windows Autopilot device preparation policy. For more information, see [Create a device group](#).

Unable to find Intune Provisioning Client with AppID of f1346770-5b25-

470b-88bd-d5744ab7952c when trying to set the owner of the Windows Autopilot device preparation policy device group.

- In some tenants, the service principal might have the name of **Intune Autopilot ConfidentialClient** instead of **Intune Provisioning Client**. As long as the AppID of the service principal is **f1346770-5b25-470b-88bd-d5744ab7952c**, it's the correct service principal.
- If either **Intune Provisioning Client** or **Intune Autopilot ConfidentialClient** with AppID of **f1346770-5b25-470b-88bd-d5744ab7952c** doesn't exist in the tenant, it must be added via PowerShell commands. For more information, see [Adding the Intune Provisioning Client service principal](#).

Multiple Windows Autopilot device preparation policies exist and the device is getting the wrong policy.

If multiple Windows Autopilot device preparation policies are deployed to a user, the policy with the highest priority gets priority. Policy priorities are displayed at the **Home > Enroll devices | Windows enrollment > Device preparation policies** screen. The policy with the highest priority is higher in the list and has the smallest number under the **Priority** column. To change a policy's priority, move it in the list by dragging the policy within the list.

Related content

- [Windows Autopilot device preparation - known issues.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot device preparation - known issues

Article • 02/05/2025 • Applies to: Windows 11

This article describes known issues that can often be resolved with:

- Configuration changes.
- Cumulative updates.
- Might be resolved automatically in a future release.

💡 Tip

RSS can be used to notify when new known issues are added to this page. For example, the following RSS link includes this article:

url

```
https://learn.microsoft.com/api/search/rss?  
search=%22Information+regarding+known+issues+that+might+occur+during+a+  
Windows+Autopilot+device+preparation%22&locale=en-us&%24filter=
```

This example includes the `&locale=en-us` variable. The `locale` variable is required, but it can be changed to another supported locale. For example, `&locale=es-es`.

For more information on using RSS for notifications, see [How to use the docs](#) in the Intune documentation.

Known issues

Exporting logs during the out-of-box experience (OOBE) doesn't show result

Date added: *January 6, 2025*

When a failure occurs during the provisioning process, an **Export logs** option is displayed to the user. When selected, it saves the file to the first USB drive on the device without displaying the browse dialog. The browse dialog isn't displayed for security reasons. Currently, users don't see failure or success messages to indicate the logs were saved. This issue will be fixed in the future.

Apps and scripts tabs don't display properly when editing the Windows Autopilot device preparation profile

Date added: *December 18, 2024*

During the editing flow of the Windows Autopilot device preparation policy, there's a known issue when displaying the **Applications** and **Scripts** tabs where the tabs might display incorrect information. For example, under the **Scripts** tab, a list of applications might be shown instead of a list of scripts. The issue is impacting only the view in Microsoft Intune and not the configuration being applied to the device. The issue is being investigated.

As a workaround, select the table header **Allowed Applications** or **Allowed Scripts** to reload the table's contents.

Win32 and WinGet applications are skipped when Managed installer policy is enabled for the tenant

Date added: *October 10, 2024*

Date updated: *February 5, 2025*

When the [Managed installer policy](#) is **Active** for a tenant, Win32 apps and Microsoft Store apps aren't delivered during OOBE. The apps are instead installed after the device gets to the Desktop and the Managed installer policy is delivered. The [Windows Autopilot device preparation deployment status report](#) reports the apps as **Skipped**.

ⓘ Note

Managed installer policy is always enabled automatically for Education customers due to the requirements for [Windows 11 SE](#).

For more information, see [Known issue: Windows Autopilot device preparation with Win32 apps and managed installer policy](#).

Security group membership update failures might lead to non-compliant devices

Date added: *September 27, 2024*

If security groups aren't properly configured in Microsoft Intune, devices might lose compliance and be left in an unsecured state. The following are potential reasons for security group membership failures:

- **Retry failures:** Security group membership updates might not succeed during retry windows, leading to delays in group updates.
- **Static to dynamic group changes:** After the Windows Autopilot device preparation profiles are configured, changing a security group from static to dynamic could cause failures.
- **Owner removal:** If the **Intune Provisioning Client** service principal is removed as an owner of a configured security group, updates might fail.
- **Group deletion:** If a configured security group is deleted and devices are deployed before Microsoft Intune detects the deletion, security configurations might fail to apply.

To mitigate the issue, follow these steps:

1. Validate security group configuration before provisioning:

- Ensure the correct security group is selected within the Microsoft Intune admin center or the Microsoft Entra admin center.
- The security group should be configured within the Windows Autopilot device preparation profile.
- The group shouldn't be assignable to other groups.
- The **Intune Provisioning Client** service principal should be an owner of the group.

2. Manually fix the provisioned devices:

- If devices are already deployed or the security group isn't applicable, manually add the affected devices to the correct security group.

Security group membership failures can be prevented by following these steps, ensuring devices remain compliant and secure.

Deployment fails for devices not in the Coordinated Universal Time (UTC) time zone

Date added: *July 8, 2024*

Date updated: *July 23, 2024*

Autopilot device preparation deployments fail when devices aren't in the UTC time zone. The issue is being investigated.

As a workaround, customers can manually set the time zone in OOB via Windows PowerShell until the issue is resolved:

PowerShell

```
Set-TimeZone -Id "UTC"
```

This issue was resolved in July 2024.

BitLocker encryption defaults to 128-bit when 256-bit encryption is configured

Date added: *July 8, 2024*

In some Windows Autopilot device preparation deployments, BitLocker encryption may default to 128-bit even though the admin configured 256-bit encryption due to a known race condition. The issue is being investigated. Microsoft recommends that customers who need 256-bit BitLocker encryption wait for the issue to be resolved before trying to use Windows Autopilot device preparation.

Windows Autopilot device preparation policy shows 0 groups assigned

Date added: *June 18, 2024*

Date updated: *July 23, 2024*

There's a known issue that the Windows Autopilot device preparation policy shows **0 groups assigned** even when:

- An assigned device security group was properly added to the policy.
- The **Intune Provisioning Client** service principal with AppID of **f1346770-5b25-470b-88bd-d5744ab7952c** is the owner of the device security group specified in the policy.

The issue is being investigated. As a workaround, create a new assigned device security group with the **Intune Provisioning Client** service principal with AppID of **f1346770-**

5b25-470b-88bd-d5744ab7952c as the owner, and then assign the new device group to the Windows Autopilot device preparation policy. For more information on creating the assigned device group, see [Create a device group](#).

This issue was resolved in July 2024.

Unable to assign Windows Autopilot device preparation policy to user group

Date added: *June 18, 2024*

Date updated: *July 23, 2024*

There's a known issue where an administrator might not be able to assign the Windows Autopilot device preparation policy to a user group. When the issue occurs, the following error might occur:

Unable to save group assignment for <policy_name>. You do not have permission to save these assignments.

The issue is being investigated. As a workaround, add the following additional role-based access control (RBAC) permission for the Windows Autopilot device preparation administrator role:

- Device configurations
 - Assign

For more information, see [Required RBAC permissions](#).

Note

The [Required RBAC permissions](#) article doesn't list the **Device configurations - Assign** permission. This permission requirement is only temporary until the issue is resolved. However, the article can be used as a guide on how to properly add this permission. **This issue was resolved in July 2024.**

Device is stuck at 100% during the out-of-box experience (OOBE)

Date added: *June 3, 2024*

If during Windows Autopilot device preparation deployment a device gets stuck at 100% during the out-of-box experience (OOBE), the end-user needs to manually restart the device for the deployment to continue. This issue is a known issue and a fix is being worked on.

Object with AppID of f1346770-5b25-470b-88bd-d5744ab7952c displays as Intune Autopilot ConfidentialClient

Date added: *June 3, 2024*

In some tenants, when trying to set the owner of the device group used in the Windows Autopilot device preparation policy, the service principal with AppID of **f1346770-5b25-470b-88bd-d5744ab7952c** displays as **Intune Autopilot ConfidentialClient** instead of **Intune Provisioning Client**. As long as the service principal has an AppID of **f1346770-5b25-470b-88bd-d5744ab7952c**, it's the correct service principal and can be selected.

Conflict between Microsoft Entra ID and Windows Autopilot device preparation local administrator setting

Date added: *June 3, 2024*

There's a compatibility problem between the Windows Autopilot device preparation policy **User account type** setting and the Microsoft Entra ID **Local administrator settings**. Specifically, when the Windows Autopilot device preparation policy **User account type** setting is set to **Standard user** and the Microsoft Entra ID setting **Registering user is added as local administrator on the device during Microsoft Entra join (Preview)** under **Local administrator settings** is set to either **Selected** or **None**, provisioning gets skipped during a Windows Autopilot device preparation deployment. This settings conflict leads to a scenario where users could reach the desktop without having the expected applications installed. The Microsoft Entra ID **Local administrator settings** can be found by signing into the [Azure portal](#) and navigating to **Microsoft Entra ID > Manage | Devices > Manage | Devices settings**.

Until the issue is fixed, for users to be standard non-administrators on their device, make sure that the settings are set to one of the following three setting combinations:

- **Standard user option 1**
 - The Microsoft Entra ID **Local administrator settings** is set to **None**.
 - The Windows Autopilot device preparation policy **User account type** setting is set to **Administrator**.

- **Standard user option 2**
 - The Microsoft Entra ID **Local administrator settings** is set to **Selected** and the standard non-administrator users aren't selected.
 - The Windows Autopilot device preparation policy **User account type** setting is set to **Administrator**.
- **Standard user option 3**
 - The Microsoft Entra ID **Local administrator settings** is set to **All**.
 - The Windows Autopilot device preparation policy **User account type** is set to **Standard user**.

In all three cases, the end result is that the user is a standard non-administrative user on the device.

If the intention is for the user to be a local administrator user on the device, make sure that the settings are set to one of the following two setting combinations:

- **Administrator user option 1**
 - The Microsoft Entra ID **Local administrator settings** is set to **All**.
 - The Windows Autopilot device preparation policy **User account type** setting is set to **Administrator**.
- **Administrator user option 2**
 - The Microsoft Entra ID **Local administrator settings** is set to **Selected** and the administrator users are selected.
 - The Windows Autopilot device preparation policy **User account type** setting is set to **Administrator**.

Initial release of Windows Autopilot device preparation

Date added: *June 3, 2024*

The initial release of Windows Autopilot device preparation has the following known issues and limitations:

- Dependency and supersedence relationships are marked in reports as **Dependent**.
- Application uninstall intent is marked in reports as **Installed** if completed successfully.
- Managed Installer policy during the out-of-box experience (OOBE) isn't supported due to the possibility of incorrect reporting.
- Custom compliance isn't supported during Windows Autopilot device preparation deployments.

- The device health script isn't supported during Windows Autopilot device preparation deployments.

Related content

- [Windows Autopilot device preparation troubleshooting FAQ](#).
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot device preparation scenarios

Article • 06/03/2024 • Applies to:  Windows 11

The following table summarizes the scenarios that are available in Windows Autopilot:

 Expand table

Scenario	Purpose	Description
Windows Autopilot device preparation user-driven mode	Device for a single user	User runs deployment

ⓘ Note

This tutorial is for Windows Autopilot device preparation. For a Windows Autopilot tutorial, see [Windows Autopilot scenarios](#).

Next steps: Scenario walkthroughs

The following list contains links to Windows Autopilot device preparation scenario walkthroughs. The walkthroughs contain step by step instructions on how to configure each of the Windows Autopilot device preparation scenarios:

1. Windows Autopilot device preparation user-driven mode:
 - a. [Microsoft Entra join](#).

Related content

- [Windows Autopilot device preparation overview](#).
- [Windows Autopilot scenarios](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step by step tutorial for Windows Autopilot device preparation user-driven Microsoft Entra join in Intune

Article • 01/14/2025 • Applies to:  Windows 11

This step by step tutorial guides through using Intune to perform a Windows Autopilot device preparation user-driven scenario when the devices are Microsoft Entra joined.

The purpose of this tutorial is a step by step guide for all the configuration steps required for a successful Windows Autopilot device preparation user-driven Microsoft Entra join deployment using Intune. The tutorial is also designed as a walkthrough in a lab or testing scenario, but can be expanded for use in a production environment.

Before beginning, refer to the [How to: Plan your Microsoft Entra join implementation](#) to make sure all requirements are met for joining devices to Microsoft Entra ID.

Windows Autopilot device preparation user-driven Microsoft Entra join overview

Windows Autopilot device preparation user-driven Microsoft Entra join is a solution that automates the configuration of Windows on a new device without the need for IT intervention. Normally the device is delivered directly from an OEM or reseller to the end-user Windows Autopilot device preparation user-driven deployments use the existing Windows installation installed by the OEM at the factory. The end-user only needs to perform a minimal number of actions during the deployment process such as:

- Powering on the device.
- In certain scenarios, selecting the language, locale, and keyboard layout.
- Connecting to a wireless network if the device isn't connected to a wired network.
- Signing into Microsoft Entra ID with the end-user's Microsoft Entra credentials.

Windows Autopilot device preparation user-driven deployments can perform the following tasks during the deployment:

- Joins the device to Microsoft Entra ID.
- Enrolls the device in Intune.
- Installs up to 10 essential applications.
- Runs up to 10 essential PowerShell scripts.

Once the Windows Autopilot device preparation user-driven deployment is complete, the device is ready for the end-user to use and they're immediately sent to the desktop.

Windows Autopilot device preparation user-driven Microsoft Entra join process

During the out-of-box experience (OOBE), a user authenticates with their corporate credentials. If there's a Windows Autopilot device preparation policy assigned to the user signing in, then that policy is delivered to the device. It then determines the configuration that needs to be applied to the device based on the settings configured in the policy. After that, device setup continues in the following order:

1. The device joins Microsoft Entra ID and enrolls in Intune.
2. The Intune management extension installs.
3. When the device is joined to Microsoft Entra ID during the first step, the user is automatically added to the local **Administrators** group on the device. If the user account is configured as a standard user, the setting is enforced by removing the user out of the **Administrators** group.
4. The deployment syncs with the mobile device management (MDM) service such as Intune and checks if line-of-business (LOB) and Microsoft 365 applications are selected in the Windows Autopilot device preparation policy. It also syncs all MDM policy at this time, but application of the policy isn't tracked during the deployment.
5. If there are LOB and Microsoft 365 applications selected in the policy, then they're installed. If a LOB or Microsoft 365 application fails to install, then the deployment fails at this point.
6. The deployment checks if PowerShell scripts are selected in the Windows Autopilot device preparation policy. If there are PowerShell scripts selected in the policy, then they run. If a PowerShell script fails, then the deployment fails at this point.
7. The deployment checks if Win32 and Microsoft Store applications are selected in the Windows Autopilot device preparation policy. If there are Win32 and Microsoft Store applications selected in the policy, then they're installed. If a Win32 or Microsoft Store application fails to install, then the deployment fails at this point.
8. If all steps succeed, the **Required setup complete** page is displayed for the user.

9. Once the **Required setup complete** page is dismissed, the user is automatically signed in and the desktop is displayed.
10. At this point, another sync is triggered and all other configurations are delivered to the device. Additional configurations might include:
 - Applications and PowerShell scripts that were assigned to the device group specified in the Windows Autopilot device preparation policy but weren't explicitly selected in the policy.
 - Any additional MDM policy.
 - User-based configurations.

Workflow

The following steps are needed to configure and then perform a Windows Autopilot device preparation user-driven Microsoft Entra join in Intune:

- ✓ Step 1: Set up Windows automatic Intune enrollment
- ✓ Step 2: Allow users to join devices to Microsoft Entra ID
- ✓ Step 3: Create a device group
- ✓ Step 4: Create a user group
- ✓ Step 5: Assign applications and PowerShell scripts to device group
- ✓ Step 6: Create Windows Autopilot device preparation policy
- ✓ Step 7: Add Windows corporate identifier to device

ⓘ Note

Although the workflow is designed for lab or testing scenarios, it can also be used in a production environment.

Walkthrough

Step 1: Set up Windows automatic Intune enrollment

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot device preparation user-driven Microsoft Entra join: Set up Windows automatic Intune enrollment

Article • 01/14/2025 • Applies to:  Windows 11

Windows Autopilot device preparation user-driven Microsoft Entra join steps:

✓ Step 1: Set up Windows automatic Intune enrollment

- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Create a device group](#)
- Step 4: [Create a user group](#)
- Step 5: [Assign applications and PowerShell scripts to device group](#)
- Step 6: [Create Windows Autopilot device preparation policy](#)
- Step 7: [Add Windows corporate identifier to device](#)

For an overview of the Windows Autopilot device preparation user-driven Microsoft Entra join workflow, see [Windows Autopilot device preparation user-driven Microsoft Entra join overview](#).

Note

If automatic Intune enrollment is already set up, skip this step and move on to [Step 2: Allow users to join devices to Microsoft Entra ID](#).

Set up Windows automatic Intune enrollment

In order for Windows Autopilot device preparation to work, devices need to be able to enroll in Intune automatically. Enrolling devices in Intune automatically can be configured in the [Azure portal](#):

1. Sign in to the [Azure portal](#).
2. Select Microsoft Entra ID.
3. In the Overview screen, under Manage in the left hand pane, select Mobility (MDM and WIP).
4. In the Mobility (MDM and WIP) screen, under Name select Microsoft Intune.

5. In the Microsoft Intune page that opens, under **MDM user scope**, select either **All** or **Some**:

- If **All** is selected, all users can automatically enroll their devices in Intune.
- If **Some** is selected, only users in the groups specified in the link under **Groups** can automatically enroll their devices in Intune. To add groups:
 - a. Select the link under **Groups**.
 - b. In the **Select groups** window that opens, select the desired groups to add. Make sure that the groups selected are Microsoft Entra user groups that contain the desired users.
 - c. Once all of the desired groups are selected, select **Select** to close the **Select groups** window.

6. In the Microsoft Intune screen, if any changes were made, select **Save**.

Next step: Allow users to join devices to Microsoft Entra ID

Step 2: Allow users to join devices to Microsoft Entra ID

Related content

For more information on Windows automatic MDM/Intune enrollment, see the following articles:

- [Enable Windows automatic enrollment](#).
- [Set up Windows automatic enrollment](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot device preparation user-driven Microsoft Entra join: Allow users to join devices to Microsoft Entra ID

Article • 01/14/2025 • Applies to:  Windows 11

Windows Autopilot device preparation user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- ✓ Step 2: **Allow users to join devices to Microsoft Entra ID**
- Step 3: [Create a device group](#)
- Step 4: [Create a user group](#)
- Step 5: [Assign applications and PowerShell scripts to device group](#)
- Step 6: [Create Windows Autopilot device preparation policy](#)
- Step 7: [Add Windows corporate identifier to device](#)

For an overview of the Windows Autopilot device preparation user-driven Microsoft Entra join workflow, see [Windows Autopilot device preparation user-driven Microsoft Entra join overview](#).

Note

If users are already allowed to join devices to Microsoft Entra ID, skip this step and move on to [Step 3: Create a device group](#).

Allow users to join devices to Microsoft Entra ID

In order for Windows Autopilot device preparation to work, users need to be allowed to join devices to Microsoft Entra ID. Allowing users to join devices to Microsoft Entra ID can be configured in the [Azure portal](#):

1. Sign in to the [Azure portal](#).
2. Select Microsoft Entra ID.
3. In the Overview screen, under Manage in the left hand pane, select Devices.

4. In the Devices | Overview screen, under **Manage** in the left hand pane, select **Device Settings**.
5. In the Devices | Device settings screen that opens, under **Users may join devices to Microsoft Entra**, select either **All** or **Selected**:
 - If **All** is selected, all users can join their devices to Microsoft Entra ID.
 - If **Some** is selected, only users specified under **Selected** can join their devices to Microsoft Entra ID. To add users:
 - a. Select the link under **Selected**.
 - b. In the **Members allowed to join devices** page that opens:
 - i. Select **Add**.
 - ii. In the **Add members** window that opens:
 - i. Select the desired users and/or groups to add.
 - ii. Once all of the desired users and groups are selected, select **Select** to close the **Add members** window.
 - iii. Select **OK**.

 **Note**

Any selected groups must be a Microsoft Entra group that contains user objects.

6. In the Devices | Overview screen, if any changes were made, select **Save**.

Next step: Create a device group

[Step 3: Create a device group](#)

Related content

For more information on allowing users to join devices to Microsoft Entra ID, see the following articles:

- [Configure device settings](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Windows Autopilot device preparation user-driven Microsoft Entra join: Create a device group

Article • 01/14/2025 • Applies to:  Windows 11

Windows Autopilot device preparation user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)

Step 3: Create a device group

- Step 4: [Create a user group](#)
- Step 5: [Assign applications and PowerShell scripts to device group](#)
- Step 6: [Create Windows Autopilot device preparation policy](#)
- Step 7: [Add Windows corporate identifier to device](#)

For an overview of the Windows Autopilot device preparation user-driven Microsoft Entra join workflow, see [Windows Autopilot device preparation user-driven Microsoft Entra join overview](#).

Note

The device group created in this step is specific to Windows Autopilot device preparation. Microsoft recommends creating a device group specifically for use with Windows Autopilot device preparation instead of reusing existing device groups used in other Autopilot scenarios.

Create a device group

Device groups are a collection of devices organized into a Microsoft Entra group. Device groups can be either dynamic or assigned:

- **Dynamic groups** - Devices are automatically added to the group based on rules.
- **Assigned groups** - Devices are manually added to the group and are static.

Windows Autopilot device preparation uses a device group as part of the Windows Autopilot device preparation policy. The device group specified in the Windows Autopilot device preparation policy is the device group where devices are added

automatically during the Windows Autopilot device preparation deployment. The device group specified in the Windows Autopilot device preparation policy needs to be an assigned security group.

To create an assigned security device group for use with Windows Autopilot device preparation, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Groups** in the left hand pane.
3. In the **Groups | All groups** screen, make sure **All groups** is selected, and then select **New group**.
4. In the **New Group** screen that opens:
 - a. For **Group type**, select **Security**.
 - b. For **Group name**, enter a name for the device group, such as **Windows Autopilot device preparation device group**.
 - c. For **Group description**, enter a description for the device group.
 - d. For **Microsoft Entra roles can be assigned to the group**, select **No**.
 - e. For **Membership type**, select **Assigned**.
 - f. For **Owners**, select the **No owners selected** link.
 - g. In the **Add owners** screen that opens:
 - i. Scroll through the list of objects and select the service principal **Intune Provisioning Client** with AppId of **f1346770-5b25-470b-88bd-d5744ab7952c**. Alternatively, use the **Search** bar to search for and select **Intune Provisioning Client**.

 **Note**

- In some tenants, the service principal might have the name of **Intune Autopilot ConfidentialClient** instead of **Intune Provisioning Client**. As long as the AppID of the service principal is **f1346770-5b25-470b-88bd-d5744ab7952c**, it's the correct service principal.

- If the **Intune Provisioning Client** or **Intune Autopilot ConfidentialClient** service principal with AppId of **f1346770-5b25-470b-88bd-d5744ab7952c** isn't available either in the list of objects or when searching, see [Adding the Intune Provisioning Client service principal](#).

ii. Once **Intune Provisioning Client** is selected as the owner, select **Select**.

h. Select **Create** to finish creating the assigned device group.

ⓘ Important

Devices are automatically added to this device group during the Windows Autopilot device preparation deployment. Manually adding devices as members of the device group created in this step isn't necessary, but doing so has no impact on the Windows Autopilot device preparation process.

Adding the Intune Provisioning Client service principal

If the **Intune Provisioning Client** service principal with AppId **f1346770-5b25-470b-88bd-d5744ab7952c** isn't available when selecting the owner of the device group, then follow these steps to add the service principal:

1. On a device where Microsoft Intune or Microsoft Entra ID is normally administered, open an elevated **Windows PowerShell** command prompt.
2. In the **Windows PowerShell** command prompt window:

- a. Install the **Microsoft.Graph.Authentication** module by entering the following command:

PowerShell

```
Install-Module Microsoft.Graph.Authentication
```

If prompted to do so:

- Agree to install **NuGet** by entering **Y** or **Yes**, or selecting the **Yes** button.
- Agree to install from the **PSGallery** untrusted repository by entering **Y** or **Yes**, or selecting the **Yes** button.

For more information, see [Microsoft.Graph.Authentication](#) and [Set-PSRepository -InstallationPolicy](#).

- b. Install the **Microsoft.Graph.Applications** module by entering the following command:

```
PowerShell
```

```
Install-Module Microsoft.Graph.Applications
```

If prompted to do so, agree to install from the **PSGallery** untrusted repository by entering **Y** or **Yes**, or selecting the **Yes** button.

For more information, see [Microsoft.Graph.Applications](#) and [Set-PSRepository -InstallationPolicy](#).

- c. Once the **Microsoft.Graph.Authentication** and **Microsoft.Graph.Applications** modules are installed, connect to Microsoft Entra ID by entering the following command:

```
PowerShell
```

```
Connect-MgGraph -Scopes "Application.ReadWrite.All"
```

For more information, see [Connect-MgGraph](#).

- d. If not already authenticated to Microsoft Entra ID, the **Sign in to your account** window appears. Enter the credentials of a Microsoft Entra ID administrator that has permissions to add service principals.
- e. If the **Permissions requested** window appears, select the **Consent on behalf of your organization** checkbox, and then select the **Accept** button.
- f. Once authenticated to Microsoft Entra ID and proper permissions are granted, add the **Intune Provisioning Client** service principal by entering the following command:

```
PowerShell
```

```
New-MgServicePrincipal -AppID f1346770-5b25-470b-88bd-d5744ab7952c
```

For more information, see [New-MgServicePrincipal -BodyParameter](#).

 **Note**

- The following error message is displayed if the **Intune Provisioning Client service principal** already exists in the tenant:

PowerShell

```
New-MgServicePrincipal : The service principal cannot be created, updated, or restored because the service principal name f1346770-5b25-470b-88bd-d5744ab7952c is already in use.  
Status: 409 (Conflict)  
ErrorCode: Request_MultipleObjectsWithSameKeyValue
```

- The following error message is displayed if one of the following conditions is true:
 - The account used to sign in with the `Connect-MgGraph` command doesn't have permissions to add a service principal to the tenant.
 - The `-Scopes "Application.ReadWrite.All"` argument isn't added to the `Connect-MgGraph` command.
 - The **Permissions requested** window isn't accepted.
 - The **Consent on behalf of your organization** checkbox isn't selected in the **Permissions requested** window.

PowerShell

```
New-MgServicePrincipal : Insufficient privileges to complete the operation.  
Status: 403 (Forbidden)  
ErrorCode: Authorization_RequestDenied
```

Next step: Create a user group

Step 4: Create a user group

Related content

For more information on creating groups in Intune, see the following articles:

- [Create device groups.](#)
- [Add groups to organize users and devices.](#)
- [Manage Microsoft Entra groups and group membership.](#)

- Dynamic membership rules for groups in Microsoft Entra ID.
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot device preparation user-driven Microsoft Entra join: Create a user group

Article • 01/14/2025 • Applies to:  Windows 11

Windows Autopilot device preparation user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Create a device group](#)
- ✓ Step 4: [Create a user group](#)
 - Step 5: [Assign applications and PowerShell scripts to device group](#)
 - Step 6: [Create Windows Autopilot device preparation policy](#)
 - Step 7: [Add Windows corporate identifier to device](#)

For an overview of the Windows Autopilot device preparation user-driven Microsoft Entra join workflow, see [Windows Autopilot device preparation user-driven Microsoft Entra join overview](#).

Note

The user group created in this step is specific to Windows Autopilot device preparation. Microsoft recommends creating a user group specifically for use with Windows Autopilot device preparation instead of reusing existing user groups used in other Autopilot scenarios.

Create a user group

User groups are a collection of users organized into a Microsoft Entra group. User groups can be either dynamic or assigned:

- **Dynamic groups** - Users are automatically added to the group based on rules.
- **Assigned groups** - Users are manually added to the group and are static.

Windows Autopilot device preparation uses a user group as part of the Windows Autopilot device preparation policy. The users that are members of the user group specified in the Windows Autopilot device preparation policy are the users that receive

the Windows Autopilot device preparation deployment. The user group specified in the Windows Autopilot device preparation policy needs to be a security group but can be either an assigned or dynamic group.

To create a user security group for use with Windows Autopilot device preparation, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Groups** in the left hand pane.
3. In the **Groups | All groups** screen, make sure **All groups** is selected, and then select **New group**.
4. In the **New Group** screen that opens:
 - a. For **Group type**, select **Security**.
 - b. For **Group name**, enter a name for the user group, such as **Windows Autopilot device preparation user group**.
 - c. For **Group description**, enter a description for the user group.
 - d. For **Microsoft Entra roles can be assigned to the group**, select **No**.
 - e. For **Membership type**:
 - Select **Assigned** to create an assigned user group.
 - Select **Dynamic User** to create a dynamic user group.
 - f. For **Owners**, select the **No owners selected** link.
 - g. In the **Add owners** screen that opens:
 - i. Scroll through the list of objects and select owners for the user group. Alternatively, use the **Search** bar to search for and select owners of the group.
 - ii. Once all of the desired owners are selected, select **Select**.
 - h. For assigned user groups:
 - i. For **Members**, select the **No members selected** link.
 - ii. In the **Add members** screen that opens:
 - i. Scroll through the list of objects and select members that the Windows Autopilot device preparation profiles should be deployed to. Alternatively,

use the **Search** bar to search for and select members for the group. Make sure to only select users or groups that only contain users.

ii. Once all of the desired users or user groups are selected that the Windows Autopilot device preparation profiles should be deployed to, select **Select**.

i. For dynamic user groups:

i. For **Dynamic user members**, select the **Add dynamic query** link.

ii. In the **Dynamic membership rules** screen that opens, create a rule that encompasses the users that should be members of the user group. For more information on creating rules, see [Dynamic membership rules for groups in Microsoft Entra ID](#).

 **Note**

The linked article is in regards to creating dynamic membership rules in Microsoft Entra ID. However, dynamic user groups in Intune are also dynamic user groups in Microsoft Entra ID, so the rule syntax is the same.

j. Select **Create** to finish creating user group.

Next step: Assign applications and PowerShell scripts to device group

Step 5: Assign applications and PowerShell scripts to device group

Related content

For more information on creating groups in Intune, see the following articles:

- [Create device groups](#).
- [Add groups to organize users and devices](#).
- [Manage Microsoft Entra groups and group membership](#).
- [Dynamic membership rules for groups in Microsoft Entra ID](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Windows Autopilot device preparation user-driven Microsoft Entra join: Assign applications and PowerShell scripts to device group

Article • 01/14/2025 • Applies to:  Windows 11

Windows Autopilot device preparation user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Create a device group](#)
 - Step 4: [Create a user group](#)
-  **Step 5: Assign applications and PowerShell scripts to device group**
- Step 6: [Create Windows Autopilot device preparation policy](#)
 - Step 7: [Add Windows corporate identifier to device](#)

For an overview of the Windows Autopilot device preparation user-driven Microsoft Entra join workflow, see [Windows Autopilot device preparation user-driven Microsoft Entra join overview](#).

Assign applications and PowerShell scripts to device group

During the out-of-box experience (OOBE) experience before the end-user is signed in for the first time, Windows Autopilot device preparation allows deployment of up to:

- 10 managed applications
- 10 PowerShell scripts

The applications and PowerShell scripts specified should be the essential applications to install and the essential PowerShell scripts to run before the end-user can start using the device.

Any applications installed or PowerShell scripts that run during a Windows Autopilot device preparation deployment should be configured to install in the **System** context since the applications are installed and the PowerShell scripts ran during OOBE when no user is signed in.

For applications to install and PowerShell scripts work successfully, they must be assigned to the device group created for Windows Autopilot device preparation in Step 3: Create a device group.

Note

The below steps assume that the applications or PowerShell scripts that will be deployed during Windows Autopilot device preparation deployment are already added to Intune. For more information on how to add applications and PowerShell scripts to Intune if they aren't already created, see [Add apps to Microsoft Intune](#) and [Use PowerShell scripts on Windows devices in Intune](#).

Applications

The following types of applications are supported for use with Windows Autopilot device preparation:

- [Line-of-business \(LOB\)](#).
- [Win32](#).
- [Microsoft Store](#) - only Microsoft Store apps that support WinGet are supported.
- [Microsoft 365](#).

In addition, Windows Autopilot device preparation supports deploying both Win32 and line-of-business (LOB) applications in the same deployment.

To assign the desired applications to the device group created for Windows Autopilot device preparation:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Apps** in the left hand pane.
3. In the **Apps | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows apps** screen, scroll through the list of applications and then select the desired application that should be installed during the Windows Autopilot device preparation deployment. Alternatively, use the **Search by name or publisher** box to search for the application, and then select it.
5. Once the application is selected, a new screen opens showing the application. Under **Manage**, select **Properties**.
6. In the **Properties** screen, next to **Assignments**, select **Edit**.

7. In the **Edit application** screen:

- a. Under the **Required** section, select **Add group**. The **Select groups** pane opens.
 - b. In the **Select groups** pane:
 - i. Scroll through the list of groups. Once the Windows Autopilot device preparation device security group is located, select it. Alternatively, use the **Search** box to locate the Windows Autopilot device preparation device security group and then select it.
 - ii. Once the Windows Autopilot device preparation device security group is selected, select **Select**.
 - c. Verify that the Windows Autopilot device preparation device security group is listed under the **Required** section. Additionally, verify that **Group mode** is set to **Included**. When applicable, also verify that **Install Context** is set to **Device context**.
 - d. Once everything is verified, select **Review + save**.
 - e. In the **Review + save** screen, select **Save**.
8. Repeat the steps for any additional applications that need to be installed during the Windows Autopilot device preparation deployment.

PowerShell scripts

To assign the desired PowerShell scripts to the device group created for Windows Autopilot device preparation:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **manage devices**, select **Scripts and remediations**.
4. In the **Devices | Scripts and remediations** screen:
 - a. Select **Platform scripts**.
 - b. Scroll through the list of PowerShell scripts and then select the desired PowerShell script that should run during the Windows Autopilot device preparation deployment. Alternatively, use the **Search** box to search for the PowerShell script, and then select it.

5. Once the PowerShell script is selected, a new screen opens showing the PowerShell script. Under **Manage**, select **Properties**.
6. In the **Properties** screen, next to **Assignments**, select **Edit**.
7. In the **Edit PowerShell script** screen:
 - a. Under the **Included groups** section, select **Add groups**. The **Select groups to include** pane opens.
 - b. In the **Select groups to include** pane:
 - i. Scroll through the list of groups. Once the Windows Autopilot device preparation device security group is located, select it. Alternatively, use the **Search** box to locate the Windows Autopilot device preparation device security group and then select it.
 - ii. Once the Windows Autopilot device preparation device security group is selected, select **Select**.
 - c. Verify that the Windows Autopilot device preparation device security group is listed under the **Included groups** section. Make sure that the Windows Autopilot device preparation device security group wasn't accidentally added under the **Excluded groups** section.
 - d. Once everything is verified, select **Review + save**.
 - e. In the **Review + save** screen, select **Save**.

Next step: Create Windows Autopilot device preparation policy

Step 6: Create Windows Autopilot device preparation policy

Related content

- [Add apps to Microsoft Intune](#).
- [Use PowerShell scripts on Windows devices in Intune](#).
- [Assign apps to groups with Microsoft Intune](#).
- [Win32 app management in Microsoft Intune](#).
- [Add a Windows line-of-business app to Microsoft Intune](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot device preparation user-driven Microsoft Entra join: Create a Windows Autopilot device preparation policy

Article • 01/14/2025 • Applies to:  Windows 11

Windows Autopilot device preparation user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Create a device group](#)
- Step 4: [Create a user group](#)
- Step 5: [Assign applications and PowerShell scripts to device group](#)
- ✓ Step 6: **Create Windows Autopilot device preparation policy**
- Step 7: [Add Windows corporate identifier to device](#)

For an overview of the Windows Autopilot device preparation user-driven Microsoft Entra join workflow, see [Windows Autopilot device preparation user-driven Microsoft Entra join overview](#).

Create user-driven Microsoft Entra join Windows Autopilot device preparation policy

The Autopilot policy specifies how the device is configured during Windows Setup and what is shown during the out-of-box experience (OOBE).

To create a user-driven Microsoft Entra join Windows Autopilot device preparation policy, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the Home screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.

5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot device preparation**, select **Device preparation policies**.
6. In the **Device preparation policies** screen, select **Create**.
7. The **Create profile** screen opens. In the **Introduction** page, select **Next**.
8. In the **Basics** page:
 - a. In the **Name** text box, enter a name for the Windows Autopilot device preparation policy.
 - b. In the **Description** text box, if desired, enter a description for the Windows Autopilot device preparation policy.
 - c. Once a name and description is entered, select **Next**.
9. In the **Device group** page, select the **Search by group name..** box, and then either select or search for the device group created in [Step 3: Create a device group](#). Make sure to select the device group created in [Step 3: Create a device group](#) and not the user group created in [Step 4: Create a user group](#). Once the correct device group is selected, select **Next**.
10. In the **Configuration settings** page, configure the various settings as desired and then select **Next**. For detailed information on the configurations on this page, see the next section [Configuration settings](#).
11. In the **Scope tags** page, select **Next**.

 **Note**

Scope tags are optional. For this tutorial, scope tags are being skipped and left at the default scope tag. However if a custom scope tag needs to be specified, do so at this page. For more information about scope tags, see [Use role-based access control and scope tags for distributed IT](#).

12. In the **Assignments** page, select the **Search by group name..** box, and then either select or search for the user group created in [Step 4: Create a user group](#). Make sure to select the user group created in [Step 4: Create a user group](#) and not the device group created in [Step 3: Create a device group](#). Once the correct user group is selected, select **Next**.
13. In the **Review + create** page, review all settings to make sure they're all correct. Once everything is verified, select **Save** to finish creating the Windows Autopilot

device preparation policy.

Configuration settings

The **Configuration settings** page has several configuration options. The following section describes each option in the **Configuration settings** page and what each option should be set to for a Microsoft Entra join Windows Autopilot device preparation deployment.

In the **Configuration settings** page:

1. Expand the **Out-of-box experience settings** section by selecting it.

- a. **Minutes allowed before showing installation error** - enter the number of minutes allowed before failing a deployment.

The value entered is for the whole deployment and not for an individual application install or PowerShell script. The acceptable value is an integer between 15 and 720.

- b. **Custom error message** - enter a custom message to display to the end-user if the deployment fails.
 - c. **Allow users to skip setup after multiple attempts** - select either **Yes** or **No** as desired by toggling the switch.

Normally after a deployment failure, a **Retry** button is displayed allowing the end-user to retry the deployment. Setting this option as **Yes** also adds a **Continue anyway** button that allows the deployment to just fail, signs the end-user in, and lets them continue to the desktop.

- d. **Show link to diagnostics** - select either **Yes** or **No** as desired by toggling the switch.

If there's a deployment failure, setting this option to **Yes** displays a link at the deployment failure page allowing the end-user to retrieve diagnostic logs.

2. Expand the **Apps** section by selecting it:

The **Apps** section allows selection of up to 10 managed applications reference with the deployment. The applications specified here should be the essential applications that should be installed on the device before the end-user can start using the device.

Important

The applications selected in this setting should be assigned to the device security group previously specified in the **Device group** page. If applicable, the applications should also be configured to install in the **System** context since it's installed during OOME when no user is signed in.

- a. Under **Allowed Applications**, select **Add**. The **Select Apps** pane opens.
- b. In the **Select Apps** pane:
 - i. Scroll through the list of applications or use the **Search** box to search for desired applications.
 - ii. Once a desired application is found, select the **Add** button next to the application. The application is added to the list under **Selected Apps**.
 - iii. Once all of the desired applications are selected, select **Save**.

All of the selected applications should display under **Allowed Applications**.

Note

The following types of applications are supported for use with Windows Autopilot device preparation:

- [Line-of-business \(LOB\)](#).
- [Win32](#).
- [Microsoft Store](#) - only Microsoft Store apps that support WinGet are supported.
- [Microsoft 365](#).

In addition, Windows Autopilot device preparation supports deploying both Win32 and line-of-business (LOB) applications in the same deployment.

3. Expand the **Deployment settings** section by selecting it:
 - a. **Deployment mode** - select **User-driven** in the drop-down menu.
 - b. **Deployment type** - select **Single user** in the drop-down menu.
 - c. **Join type** - select **Microsoft Entra joined** in the drop-down menu.

- d. **User account type** - select either **Standard User** or **Administrator** as desired by toggling the switch.

ⓘ Important

By default, when a device is enrolled in Microsoft Entra ID, the user is automatically added to the **Administrator** group on the device. If this setting is set to **Standard User**, the Windows Autopilot device preparation deployment ensures that the user is removed from the **Administrator** group before the deployment completes, the user is signed in, and the user reaches the desktop.

4. Expand the **Scripts** section by selecting it:

The **Scripts** section allows selection of up to 10 PowerShell scripts to install during the deployment. The PowerShell scripts specified here should be the essential PowerShell scripts that should run on the device before the end-user can start using the device.

ⓘ Important

The PowerShell scripts selected in this setting should be assigned to the device security group previously specified in the **Device group** page. The PowerShell script should also be configured to run in the **System** context since the PowerShell scripts run during OOOB when no user is signed in. The PowerShell script can be set to run in the **System** context by setting the option **Run this script using the logged on credentials** to **No** in the properties of the PowerShell script.

- a. Under **Allowed Scripts**, select **Add**. The **Select Scripts** pane opens.
- b. In the **Select Scripts** pane:
 - i. Scroll through the list of PowerShell scripts or use the **Search** box to search for desired PowerShell scripts.
 - ii. Once a desired PowerShell script is found, select the **Add** button next to the PowerShell script. The PowerShell script is added to the list under **Selected Scripts**.
 - iii. Once all of the desired PowerShell scripts are selected, select **Save**.

All of the selected PowerShell scripts should display under **Allowed Scripts**.

ⓘ Important

Make sure that the device that the Windows Autopilot device preparation deployment is run on isn't registered or added as a Windows Autopilot device. If the device is registered or added as a Windows Autopilot device, the Windows Autopilot profile takes precedence over the Windows Autopilot device preparation policy. In this scenario, the Windows Autopilot deployment runs instead of the Windows Autopilot device preparation deployment. If a device needs to be removed as a Windows Autopilot device, see [Deregister a device](#).

Policy priority

If multiple Windows Autopilot device preparation policies are deployed to a user, the policy with the highest priority as displayed in the [Home > Enroll devices | Windows enrollment > Device preparation policies](#) screen gets priority. The policy with the highest priority is higher in the list and has the smallest number under the **Priority** column. To change a policy's priority, move it in the list by dragging the policy within the list.

Next step: Add Windows corporate identifier to device

Step 7: Add Windows corporate identifier to device

ⓘ Note

Windows Autopilot device preparation only requires [corporate identifiers for Windows](#) if Intune enrollment restrictions are being used to block personal device enrollments. If Intune enrollment restrictions aren't being used to block personal device enrollments, then the next step is to deploy the device.

Feedback

Was this page helpful?



Yes



No

Provide product feedback ↗

Windows Autopilot device preparation user-driven Microsoft Entra join: Add Windows corporate identifier to device

Article • 01/14/2025 • Applies to:  Windows 11

Windows Autopilot device preparation user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Create a device group](#)
 - Step 4: [Create a user group](#)
 - Step 5: [Assign applications and PowerShell scripts to device group](#)
 - Step 6: [Create Windows Autopilot device preparation policy](#)
-  **Step 7: Add Windows corporate identifier to device**

For an overview of the Windows Autopilot device preparation user-driven Microsoft Entra join workflow, see [Windows Autopilot device preparation user-driven Microsoft Entra join overview](#).

Add Windows corporate identifier for devices

Corporate identifiers in Intune allows pre-uploading of Windows device identifiers (serial number, manufacturer, model) and ensures only trusted Windows devices can be enrolled in Intune. If Intune enrollment restrictions are being used to block personal device enrollments, corporate identifiers need to be uploaded for all devices that are enrolled through Windows Autopilot device preparation before deployment. To add corporate identifier for devices in Intune, see [Add Windows corporate identifiers](#).

Important

This step of adding Windows corporate identifiers for devices is specific to Intune enrollments and isn't required if personal devices aren't being blocked in the environment. If personal devices aren't being blocked in the environment, this step can be skipped. The next step would instead be to deploy the device.

For more information, see:

- [Identify devices as corporate-owned](#).

- What are enrollment restrictions?.
- Create device platform restrictions.

Once the corporate identifier is added for the device, then proceed with deploying the device.

Feedback

Was this page helpful?



Yes



No

Provide product feedback ↗

Windows Autopilot: What's new

Article • 02/27/2025 • Applies to:  Windows 11,  Windows 10

Tip

RSS can be used to notify when new features for Windows Autopilot are added to this page. For example, the following RSS link includes this article:

url

```
https://learn.microsoft.com/api/search/rss?  
search=%22News+and+resources+about+the+latest+updates+and+past+versions  
+of+Windows+Autopilot.%22&locale=en-us&%24filter=
```

This example includes the `&locale=en-us` variable. The `locale` variable is required, but it can be changed to another supported locale. For example, `&locale=es-es`.

For more information on using RSS for notifications, see [How to use the docs](#) in the Intune documentation.

Low privileged account for Intune Connector for Active Directory for Hybrid join Windows Autopilot flows

Date added: *February 27, 2025*

We've updated the Intune Connector for Active Directory to use a low privileged account to increase the security of your environment. The old connector will continue to work until deprecation in late May 2025.

For more information, see [Deploy Microsoft Entra hybrid joined devices by using Intune and Windows Autopilot](#).

Update to enrollmentProfileName property for devices deployed via Windows Autopilot for existing devices

Date added: *June 24, 2024*

Devices deployed via Windows Autopilot for existing devices which are also registered for Windows Autopilot would previously have an **enrollmentProfileName** property incorrectly set as **OfflineAutoPilotProfile- <ZtdCorrelationId>**. With a recent change, **enrollmentProfileName** has been updated to correctly display the assigned Windows Autopilot profile. This may impact customers who are using **enrollmentProfileName** for Microsoft Entra dynamic groups or Microsoft Intune assignment filters to distinguish devices deployed via Windows Autopilot for existing devices. For more information, see [Register the device for Windows Autopilot](#).

Windows Autopilot support for Microsoft Teams Rooms

Date added: *June 4, 2024*

Windows Autopilot streamlines provisioning for laptops. Now Windows Autopilot adds the same support for **Microsoft Teams Rooms!** With this combination, Teams Rooms devices can now be deployed and provisioned without needing physical access to the device. Policies and apps are configured and the Teams Rooms console automatically signed in without needing to enter credentials.

For more information on supported scenarios and setup, see [Autopilot and Autologin for Teams Rooms on Windows](#).

Devices are no longer re-enrolled after a motherboard change

Date added: *June 4, 2024*

When a device previously changed its motherboard and the OS remained intact, Autopilot attempted to re-enroll the device to Intune. This re-enrollment no longer occurs if a motherboard swap occurs on a device due to a change in Windows Autopilot. If a motherboard is changed on a device, the new motherboard needs to be re-registered so that Windows Autopilot continues to work upon a reset.

Windows Autopilot self-deploying mode is now generally available

Date added: *February 23, 2024*

Windows Autopilot self-deploying mode is now generally available and out of preview. Windows Autopilot self-deploying mode enables deployment of Windows devices with little to no user interaction. Once the device connects to network, the device provisioning process starts automatically: the device joins Microsoft Entra ID, enrolls in Intune, and syncs all device-based configurations targeted to the device. Self-deploying mode ensures that the user can't access desktop until all device-based configuration is applied. The Enrollment Status Page (ESP) is displayed during OOB so users can track the status of the deployment. For more information, see:

- [Windows Autopilot self-deploying mode](#).
- [Step by step tutorial for Windows Autopilot self-deploying mode in Intune](#).

Windows Autopilot for pre-provisioned deployment is now generally available

Date added: *February 23, 2024*

Windows Autopilot for pre-provisioned deployment is now generally available and out of preview. Windows Autopilot for pre-provisioned deployment is used by organizations that want to ensure devices are business-ready before the user accesses them. With pre-provisioning, admins, partners, or OEMs can access a technician flow from the Out-of-box experience (OOBE) and kick off device setup. Next, the device is sent to the user who completes provisioning in the user phase. Pre-provisioning delivers most the configuration in advance so the end user can get to the desktop faster. For more information, see:

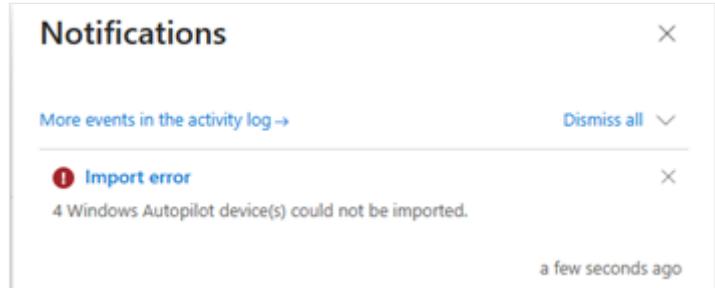
- [Windows Autopilot for pre-provisioned deployment](#).
- [Step by step tutorial for Windows Autopilot for pre-provisioned deployment Microsoft Entra join in Intune](#).
- [Step by step tutorial for Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join in Intune](#).

Updates to error message for manual device uploads

Date added: *October 31, 2023*

The 2310 release of Intune adds more clarity to the manual hardware hash upload in the console. If a device couldn't be imported, a notification shows the import error along with the specific lines of the CSV file that received the error. The error codes also include

more details on why the device failed to upload, whether the device is assigned to another tenant, or the device already registered to the tenant.



A screenshot of the Microsoft Intune Error details page. It lists two errors: "Internal error" with code 808 (ZtdDeviceAssignedToOtherTenant) and CSV line numbers 1 and 3; and "Internal error" with code 819 (ZtdDeviceDuplicated) and CSV line numbers 0 and 2.

Unblock fix pending state for self-deploying and pre-provisioning mode for disabled OEMs

Date added: *October 10, 2023*

Starting in 2310, we're making an update to the self-deployment and pre-provisioning modes for manufacturers that have not opted-in to attesting to removal of Autopilot refurbished devices. Customers using these manufacturers were still subjected to the one-time device-based enrollment block in the self-deployment and pre-provisioning modes. This block means that the device could go through self-deployment or pre-provisioning mode once and then get blocked from doing it again. This behavior could cause problems if the device needed to be reset or redeployed. This change in 2310 enables a button in the Autopilot devices section in Intune to manually unblock those devices. This update only works for certain OEMs and doesn't work on the **Fix pending** status. Reach out to your respective OEM to confirm whether this functionality is enabled for your device.

How to unblock devices

1. Sign into the [Microsoft Intune admin center](#).

2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. Select the device to unblock and the select the **Unblock device** option in the toolbar at the top of the page.

Update to BitLocker Recovery Key Process for Windows Autopilot

Date added: *August 23, 2023*

Microsoft Intune is changing how BitLocker resets occur for reused Windows Autopilot devices in the September (2309) service release. Previously, users could access the BitLocker recovery key via BitLocker self-service when reusing devices that were configured through Windows Autopilot. However, after the change, users will need to contact their IT admin to request a restore or to access the BitLocker recovery key. IT admins will continue to have full access to recovery keys both before and after this change.

User impact

This change affects new primary users of the Autopilot device who are allowed self-service recovery of BitLocker keys to that device. There's no impact if the devices' primary user doesn't change across the device restore or reset.

Self-service BitLocker access can continue to work the same if the IT admin performs either:

- A remote Autopilot Reset. For more information, see [Step by step tutorial for Windows Autopilot Reset in Intune](#), [Reset devices with remote Windows Autopilot Reset](#), and [Windows Autopilot Reset](#).
- Remove the current primary user or reassign to the new intended primary user before the device is reset or reimaged. For more information, see [Change a device's primary user](#).

If the new primary user is unable to access BitLocker self-service after changing from a previous primary user, then the IT admin should update the primary user in the device properties. The primary user on the device then updates to the new user upon the next check-in.

What needs to be done to prepare?

To ensure a smooth transition, notify the organization's help desk of this change.

Additionally, update documentation to one of the following options:

1. Temporarily note the BitLocker recovery key before restoring as documented in the [BitLocker recovery guide](#).
2. To unlock BitLocker self-service access, contact the help desk or IT Admin.

Update: Temporary change

Date added: *August 23, 2023*

When devices that utilize Windows Autopilot are reused, and there's a new device owner, that new device owner must contact an administrator to acquire the BitLocker recovery key for that device. Administrative unit scoped administrators will lose access to BitLocker recovery keys after device ownership changes. These scoped administrators need to contact a non-scoped administrator for the recovery keys. This change is a temporary change for scoped administrators and will be updated once a solution is in place.

Win32 app configurable installation time impacts the Enrollment Status Page

Starting in Intune 2308, Win32 apps allow configuration of an installation time on a per app basis. This time is expressed in minutes. If the app takes longer to install than the set installation time, the deployment fails the app install. To avoid Enrollment Status Page (ESP) timeout failures, any changes made to timeouts for Win32 apps also needs an increase in the ESP timeout to reflect those changes.

Autopilot profile resiliency

Date added: *July 26, 2023*

Downloading the Windows Autopilot policy just got more resilient! A new update is being rolled out that increases the retry attempts for applying the Windows Autopilot policy when a network connection might not be fully initialized. The increased retry attempts help ensure that the profile is applied before the user begins the setup experience and improves the time sync. Install the following quality updates for this feature:

- Windows 10: [KB5028244](#) or later.
- Windows 11: [KB5028245](#) or later.

One step removal of Windows Autopilot registration

Date added: *July 3, 2023*

Starting in 2307, Windows Autopilot is making it easier to manage devices by adding one step removal of a device in Autopilot devices in Intune. One step removal of a device means that the Autopilot registration of a device can now be removed without needing to delete the record in Intune. If the device is still active in Intune, the deletion just removes the registration, but it continues to be managed. To use this feature in Intune:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. Select the device that needs deletion and then select **Delete** in the toolbar at the top.

Device rename occurs during technician phase for pre-provisioning

Date added: *March 28, 2023* Date updated: *April 17, 2023*

Starting in 2303, a new functional change forces the device rename to occur during the technician phase for pre-provisioning for Microsoft Entra join devices. After the technician selects the provision button, we'll immediately perform the device rename and reboot the device, then transition to the device ESP. During the user flow, the device rename is then skipped keeping resources that depend on device name (such as System Center Endpoint Protection (SCEP) certs) intact. To apply this change, for Windows 10, install quality update [KB5023773](#) or later. For Windows 11, install quality update [KB5023778](#) or later.

Install required apps during pre-provisioning

Date added: March 17, 2023*

A new toggle is available in the Enrollment Status Page (ESP) profile that allows selection to attempt to install required applications during pre-provisioning technician phase. We understand that installing as many applications as possible during pre-provisioning is desired to reduce the end user setup time. To help achieve installing as many applications as possible during pre-provisioning, an option has been implemented to attempt the installation of all the required apps assigned to a device during technician phase. If there's app install failure, ESP continues except for the apps specified in the ESP profile. To enable this function, edit the Enrollment Status Page profile by selecting **Yes** on the new setting entitled **Only fail selected apps in technician phase**. This setting only appears if blocking apps are selected. For more information, see [Update to Windows Autopilot pre-provisioning process for app installs](#).

New Microsoft Store apps now supported with the Enrollment Status Page

Date added: March 17, 2023

The Enrollment Status Page (ESP) now supports the new Microsoft store applications during Windows Autopilot. This update enables better support for the new Microsoft Store experience and should be rolling out to all tenants starting with Intune 2303. For related information, see [Set up the Enrollment Status Page](#).

Win32 App Supersedence ESP improvements

Date added: February 10, 2023

Starting in January 2023, we're currently in the process of rolling out Win32 app supersedence GA, which introduces enhancements to ESP behavior around app tracking and app processing. Specifically, admins might notice a change in app counts. For more information, see [Win32 app supersedence improvements](#) and [Add Win32 app supersedence](#).

Support for Temporary Access Pass

Date added: *January 3, 2023* Date updated: *February 15, 2023*

Starting with 2301 Windows Autopilot, Autopilot supports the use of [Temporary Access Pass](#) for Microsoft Entra joined user driven, pre-provisioning and self-deploying mode for shared devices. A Temporary Access Pass is a time-limited passcode that can be configured for multi or single use to allow users to onboard other authentication methods. These authentication methods include passwordless methods such as Microsoft Authenticator, FIDO2, or Windows Hello for Business.

For more information on supported scenarios, see [Temporary Access Pass](#).

Autopilot automatic device diagnostics collection

Date added: *September 23, 2022*

Starting with Intune 2209, Intune automatically captures diagnostics when devices experience a failure during the Autopilot process on currently supported versions of Windows. When logs are finished processing on a failed device, they're automatically captured and uploaded to Intune. Diagnostics might include user identifiable information such as user or device name. If the logs aren't available in Intune, check if the device is powered-on and has access to the internet. Diagnostics are available for 28 days before they're removed.

For more information, see [Collect diagnostics from a Windows device](#).

Updates to Autopilot device targeting infrastructure

Date added: *August 16, 2022*

With Intune 2208, we're updating the Autopilot infrastructure to ensure that the profiles and applications assigned are consistently ready when the devices are deployed. This change reduces the amount of data that needs to be synchronized per-Autopilot device. Additionally, it uses device lifecycle change events to reduce the amount of time that it takes to recover from device resets for Microsoft Entra joined and Microsoft Entra hybrid joined devices. No action is needed to enable this change. It's rolling out to all clients starting August 2022.

Update Intune Connector for Active Directory for Microsoft Entra hybrid joined devices

Date added: *August 3, 2022*

Starting in September 2022, the Intune Connector for Active Directory (ODJ connector) requires .NET Framework version 4.7.2 or later. If .NET 4.7.2 or later isn't used, the Intune Connector might not work for Autopilot hybrid Microsoft Entra deployments resulting in failures. When a new Intune Connector is installed, don't use the connector installation package that was previously downloaded. Before installing a new connector, update the .NET Framework to version 4.7.2 or later. Download a new version from the [Intune Connector for Active Directory](#) section of the [Microsoft Intune admin center](#). If the latest version isn't used, it might continue to work, but the auto-upgrade feature to provide updates to the Intune Connector doesn't work.

Enroll to co-management from Windows Autopilot

Date added: *May 20, 2022*

With the Intune 2205 release, device enrollment in Intune can be configured to enable [co-management](#), which happens during the Autopilot process. This behavior directs the workload authority in an orchestrated manner between Configuration Manager and Intune.

If the device is targeted with an [Autopilot enrollment status page \(ESP\) policy](#), the device waits for Configuration Manager. The Configuration Manager client is installed, registers with the site, and then applies the production co-management policy. The Autopilot ESP then continues.

For more information, see [How to enroll to co-management with Autopilot](#).

Improvements to the enrollment status page

Date added: May 20, 2022

With the Intune 2202 release, the functionality of the [enrollment status page](#) is improved. The application picker for selecting blocking apps has the following improvements:

- Includes a search box for easier selection of apps.
- Fixes an issue where it couldn't differentiate between store apps in online or offline mode.
- Adds a new column for **Version** to see which version of the application is selected.

Select apps X

Managed apps

Search by name or publisher

Application	Publisher	Version
<input type="checkbox"/> Excel Mobile (Online)	Microsoft Corporation	
<input type="checkbox"/> Kiosk Browser (Online)	Microsoft Corporation	
<input type="checkbox"/> Kiosk Browser (Offline)	Microsoft Corporation	
<input type="checkbox"/> Microsoft Edge for ...	Microsoft	
<input type="checkbox"/> Office	Microsoft	
<input type="checkbox"/> OneNote for Windo...	Microsoft Corporation	
<input type="checkbox"/> Orca [broken]	Test	
<input type="checkbox"/> PowerPoint Mobile (...)	Microsoft Corporation	
<input type="checkbox"/> Sway (Online)	Microsoft Corporation	
<input type="checkbox"/> Test app 1	Test	3.1
<input checked="" type="checkbox"/> Test App 2	Test	2.7
<input checked="" type="checkbox"/> Test App 3-F	Test	2.3
<input type="checkbox"/> Test App 4	Test	
<input type="checkbox"/> test App 5	Test	1.0
<input type="checkbox"/> Test App F	Test	1.0
<input type="checkbox"/> Word Mobile (Online)	Microsoft Corporation	

One-time self-deployment and pre-provisioning

Date added: *May 20, 2022*

We made a change to the Windows Autopilot self-deployment mode and pre-provisioning mode experience, adding in a step to delete the device record as part of the device reuse process. This change impacts all Windows Autopilot deployments where the Autopilot profile is set to self-deployment or pre-provisioning mode. This change only affects a device when reused or reset, and it attempts to redeploy.

For more information, see [Updates to the Windows Autopilot sign-in and deployment experience ↗](#).

Update to the Windows Autopilot sign-in experience

Date added: *May 20, 2022*

Users must enter their credentials at initial sign-in during enrollment. We no longer allow pre-population of the Microsoft Entra user principal name (UPN).

For more information, see [Updates to the Windows Autopilot sign-in and deployment experience ↗](#).

MFA changes to Windows Autopilot enrollment flow

Date added: *May 20, 2022*

To improve the baseline security for Microsoft Entra ID, we changed Microsoft Entra behavior for multifactor authentication (MFA) during device registration. Previously, if a user completed MFA as part of their device registration, the MFA claim was carried over to the user state after registration was complete.

Now the MFA claim isn't preserved after registration. Users are prompted to redo MFA for any apps that require MFA by policy.

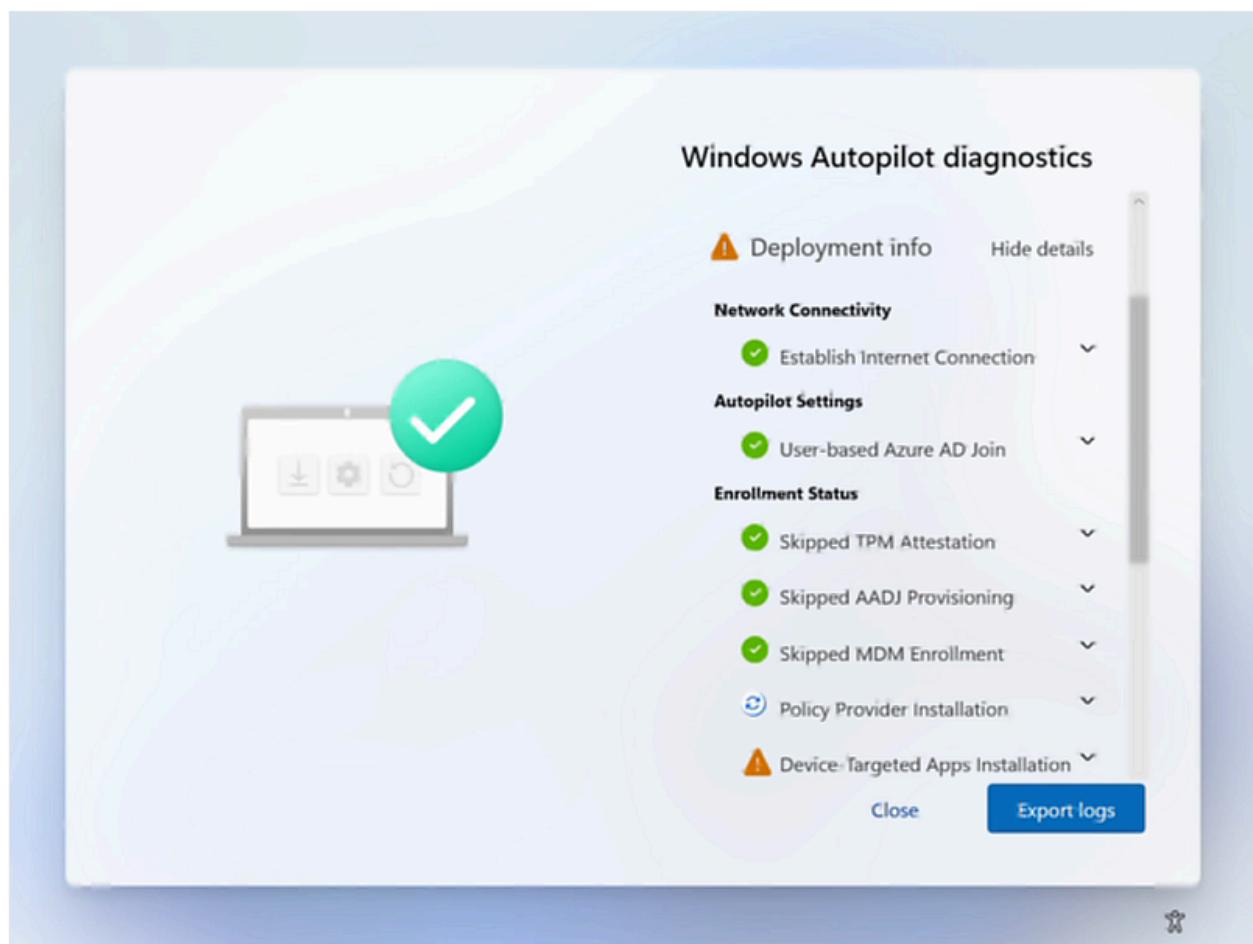
For more information, see [Windows Autopilot MFA changes to enrollment flow ↗](#).

Windows Autopilot diagnostics page

Date added: May 20, 2022

When Windows 11 is deployed with Autopilot, users can be enabled to view detailed troubleshooting information about the Autopilot provisioning process. A new **Windows Autopilot diagnostics** page is available, which provides a user-friendly view to troubleshoot Windows Autopilot failures.

The following example shows details for **Deployment info**, which includes **Network Connectivity**, **Autopilot Settings**, and **Enrollment Status**. The **Export logs** button can also be used for detailed [troubleshooting](#) analysis.



To enable the diagnostics page, go to the [ESP profile](#). Make sure **Show app and profile configuration progress** is selected to **Yes**, and then select **Yes** next to **Turn on log collection and diagnostics page for end users**.

The diagnostics page is currently supported when signing in with a Work or School account during a Windows Autopilot user-driven deployment. It's currently available on Windows 11. Windows 10 users can still collect and export diagnostic logs when this setting is enabled in Intune.

Related content

- [What's new in Microsoft Intune.](#)
 - [What's new in Windows client.](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Overview of Windows Autopilot

Article • 06/11/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

Windows Autopilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. Windows Autopilot can be used to deploy Windows PCs or HoloLens 2 devices. For more information about deploying HoloLens 2 with Autopilot, see [Windows Autopilot for HoloLens 2](#).

Windows Autopilot can also be used to reset, repurpose, and recover devices. This solution enables an IT department to achieve these goals with little to no infrastructure to manage, with a process that's easy and simple.

Windows Autopilot simplifies the Windows device lifecycle, for both IT and end users, from initial deployment to end of life. Using cloud-based services, Windows Autopilot:

- Reduces the time IT spends on deploying, managing, and retiring devices.
- Reduces the infrastructure required to maintain the devices.
- Maximizes ease of use for all types of end users.

See the following video:

<https://www.microsoft.com/en-us/videoplayer/embed/RE4C7G9?autoplay=false&postJsIMsg=true>

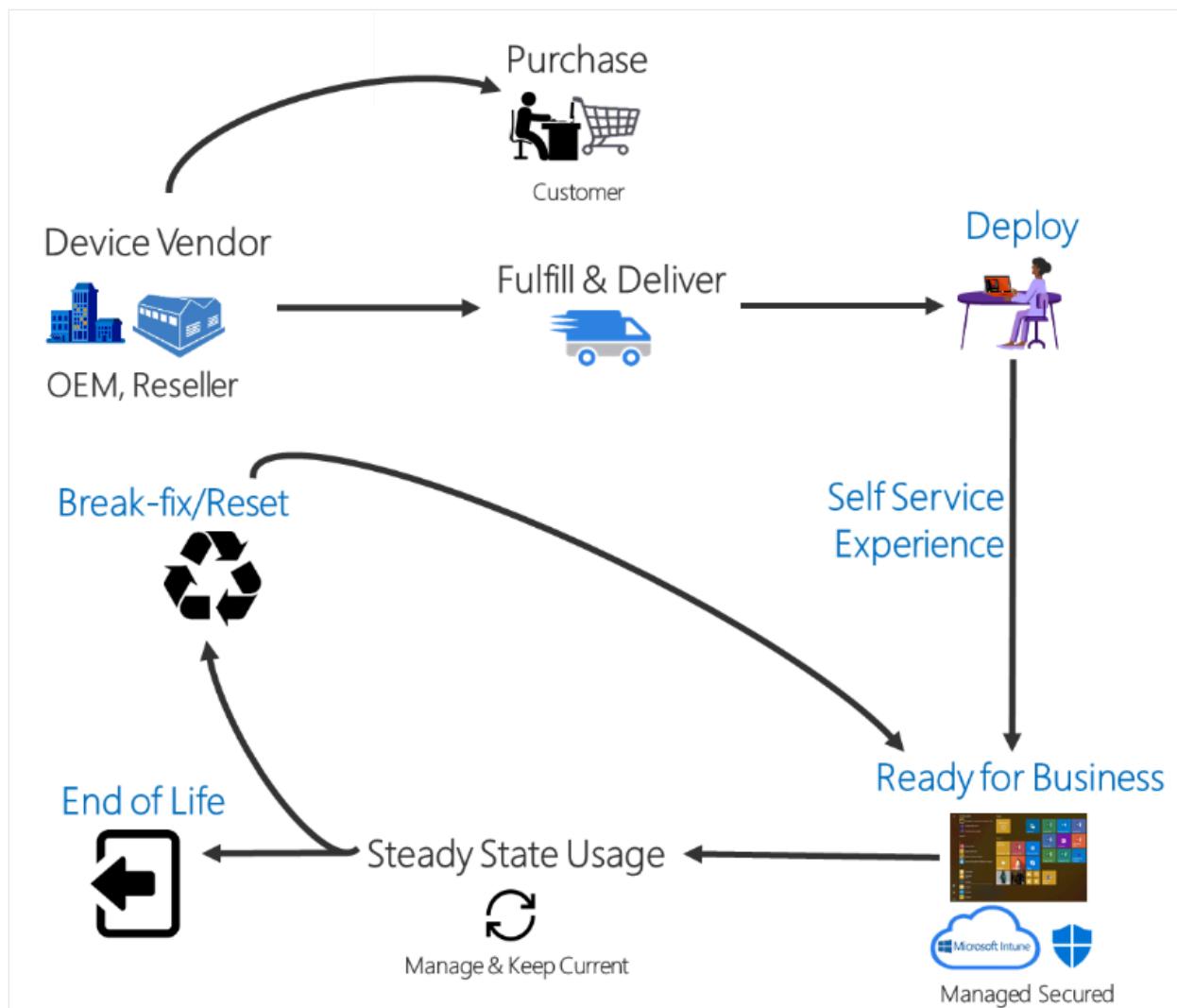
Note

This article is for **Windows Autopilot**. For **Windows Autopilot device preparation**, see [Overview of Windows Autopilot device preparation](#).

Process overview

When new Windows devices are initially deployed, Windows Autopilot uses the OEM-optimized version of Windows client. This version is preinstalled on the device, so custom images and drivers for every device model don't have to be maintained. Instead of re-imaging the device, the existing Windows installation can be transformed into a "business-ready" state that can:

- Apply settings and policies.
- Install apps.
- Change the edition of Windows being used to support advanced features. For example, from Windows Pro to Windows Enterprise.



Once deployed, Windows devices can be managed with:

- Microsoft Intune.
- Windows Update for Business.
- Microsoft Configuration Manager.
- Other similar tools from non-Microsoft parties.

Requirements

A [supported version](#) of Windows semi-annual channel is required to use Windows Autopilot. For more information, see [Windows Autopilot software, networking, configuration](#), and [licensing requirements](#).

Summary

Traditionally, IT pros spend significant time building and customizing images that are later deployed to devices. Windows Autopilot introduces a new approach.

- From the user's perspective, it only takes a few simple operations to make their device ready to use.
- From the IT pro's perspective, the only interaction required from the end user is to connect to a network and to verify their credentials. Everything beyond that is automated.

Windows Autopilot enables the following functionality:

- Automatic joining of devices to Microsoft Entra ID or Active Directory (via Microsoft Entra hybrid join). For more information about the differences between these two join options, see [Introduction to device management in Microsoft Entra ID](#).
- Auto-enrollment of devices into mobile device management (MDM) services, such as Microsoft Intune (*Requires a Microsoft Entra ID P1 or P2 subscription for configuration*).
- Creation and auto-assignment of devices to configuration groups based on a device's profile.
- Customization of the out-of-box experience (OOBE) content specific to the organization.

Existing device can also be quickly prepared for a new user with [Windows Autopilot Reset](#). The Reset capability is also useful in break/fix scenarios to quickly bring a device back to a business-ready state.

Tutorial

For a tutorial with detailed instructions on configuring Windows Autopilot, see [Windows Autopilot scenarios](#).

Related content

- [Enroll Windows devices in Intune by using Windows Autopilot](#).
- [Windows Autopilot scenarios and capabilities](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot requirements

Article • 11/25/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

Tip

RSS can be used to notify when requirements are added or updated to this page. For example, the following RSS link includes this article:

url

```
https://learn.microsoft.com/en-us/search/?  
terms=%22The%20list%20of%20requirements%20for%20Windows%20Autopilot%20i  
s%20organized%20into%20four%20different%20categories%22
```

This example includes the `&locale=en-us` variable. The `locale` variable is required, but it can be changed to another supported locale. For example, `&locale=es-es`.

For more information on using RSS for notifications, see [How to use the docs](#) in the Intune documentation.

The list of requirements for Windows Autopilot is organized into four different categories:

- **Software** - OS requirements.
- **Networking** - networking requirements.
- **Licensing** - licensing requirements.
- **Configuration** - configurations required in Microsoft Entra ID and Microsoft Intune.

Select the appropriate tab to see the relevant requirements:

 Software

Software requirements

Windows Autopilot depends on specific features available in Windows client, Microsoft Entra ID, and the mobile device management (MDM) service such as Microsoft Intune. To use Windows Autopilot and access these features, some software requirements must be met.

Note

For a list of OEMs that currently support Windows Autopilot, see the Participant device manufacturers section at [Windows Autopilot](#).

Windows 11

A [supported version](#) of Windows 11 General Availability Channel is required.

The following editions of Windows 11 are supported:

- Windows 11 Pro.
- Windows 11 Pro Education.
- Windows 11 Pro for Workstations.
- Windows 11 Enterprise.
- Windows 11 Education.
- [Windows 11 Enterprise LTSC](#).

Windows 10

A [supported version](#) of Windows 10 is required.

The following editions of Windows 10 are supported:

- Windows 10 Pro.
- Windows 10 Pro Education.
- Windows 10 Pro for Workstations.
- Windows 10 Enterprise.
- Windows 10 Education.
- [Windows 10 Enterprise LTSC](#).

HoloLens

- Windows Autopilot for HoloLens 2 requires a currently supported version of Windows Holographic. For more information, see [Windows Autopilot for HoloLens 2](#).

Note

Procedures for deploying Windows Autopilot might refer to specific products and versions. The inclusion of these products in this content doesn't imply an

extension of support for a version that is beyond its support lifecycle. Windows Autopilot doesn't support products that are beyond their support lifecycle. For more information, see [Microsoft Lifecycle Policy](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot FAQ

FAQ

Applies to:

- [Windows 11](#).
- [Windows 10](#).

This article provides OEMs, partners, administrators, and end users with answers to some frequently asked questions about deploying Windows with Autopilot.

Microsoft Partner Center

In the Partner Center, does the Tenant ID need to be provided with every device file upload? Is it needed to allow the business customer to access their devices in Microsoft Store for Business (MSfB)?

No. Providing the Tenant ID is a one-time entry in the Partner Center that can be reused with future device uploads.

How does the customer or tenant know that their devices are ready to be claimed in MSfB?

After the device file upload is completed in the Partner Center, the tenant can see the devices available for Windows Autopilot setup in MSfB. The OEM needs to advise the tenant to access MSfB. Autonotification from MSfB to the tenant is being developed.

How does a customer authorize an OEM or Channel Partner to register Autopilot devices on the customer's behalf?

Before an OEM or Channel Partner can register a device for Autopilot for a customer, the customer must first give them consent. The consent process begins with the OEM or

Channel Partner sending a link to the customer that directs the customer to a consent page in MSfB. For more information, see [Registration](#).

Do any restrictions apply if a business customer who registers devices in MSfB wants to later manage those devices through a Cloud Solution Provider (CSP) using the Partner Center?

The business customer must delete the devices in MSfB before the CSP can upload and manage them in the Partner Center.

Does Windows Autopilot support removing the option to enable a local administrator account?

No. Windows Autopilot doesn't support removing the local admin account. However, it does support restricting the user performing Microsoft Entra domain join during the out-of-box experience (OOBE) to a standard account versus an administrator account by default.

How can I test the Windows Autopilot comma-separated value (CSV) file in the Partner Center?

Only CSP partners have access to the Partner Center portal. If you're a CSP, you can create a sales agent user account that has access to devices for testing the file. This test can be done today in the Partner Center.

For more information, see [Create user accounts](#).

Is it required to become a CSP to participate in Windows Autopilot?

This requirement doesn't apply to top volume OEMs because they can use the OEM Direct API. All others who choose to use the Microsoft Partner Center (MPC) to register devices must become CSPs to access MPC.

Do the different CSP levels have all the same capabilities when it comes to Windows

Autopilot?

For the purposes of Windows Autopilot, there are three different types of CSPs, each with different levels of authority and access:

1. **Direct CSP**: Gets direct authorization from the customer to register devices
2. **Indirect CSP provider**: Gets implicit permission to register devices through the relationship their CSP reseller partner has with the customer. Indirect CSP providers register devices through the Microsoft Partner Center.
3. **Indirect CSP reseller**: Gets direct authorization from the customer to register devices. At the same time, their indirect CSP provider partner also gets authorization, which means that either the indirect provider or the indirect reseller can register devices for the customer. However, the indirect CSP reseller must register devices through the Partner Center user interface by manually uploading the CSV file. The indirect CSP provider can register devices using the Partner Center APIs.

Is there such a thing as a single, worldwide CSP account?

No. The CSP sales regions depend on the location of the Microsoft Entra tenant. A CSP partner can only sell or manage customers with a tenant located in the same CSP region. A partner's CSP region is based on the location of the tenant the CSP partner is using to transact. If the customer tenant was created in the US, only a partner that has a CSP enrollment in the US can establish a reseller relationship with this customer.

For Autopilot & Intune, the location of the end user or device doesn't matter. An employee located in Germany can enroll a device using the Autopilot profile created in the US tenant and manage it through the Intune service instance in the US. The user in Germany also authenticates in the US-based Microsoft Entra instance.

If a partner wants to manage customers globally, they need to have a global presence. They need multiple CSP enrollments in each of the CSP sales regions where they conduct business.

It's not possible to create user accounts that have access to all CSP tenants. This scenario would translate into 18 user accounts for a CSP admin agent that wants to manage all customers around the world.

In summary, the location of the user and devices doesn't matter. The location of the customer tenant matters. Cross-border device registration isn't the problem. The problem is cross-border sales via CSP.

Does the Partner Center have access to the profiles created in Intune or Microsoft Store for Business?

No. The Partner Center doesn't have access to profiles created in Intune or Microsoft Store for Business. It only has access to the Autopilot profiles created through the Partner Center.

Manufacturing

What changes need to be made in the factory OS image for customer configuration settings?

No changes are required on the factory floor to enable Windows Autopilot deployment.

What version of the OA3 tool meets Windows Autopilot deployment requirements?

Windows Autopilot can work with any version of the OA3 tool. We recommend using a supported version of Windows to generate the 4K hardware hash (4K HH).

When placing an order, do customers need to be state whether they want it with or without Windows Autopilot options?

Yes. If they want Windows Autopilot, a supported version of Windows is needed. A customer should also receive the CSV file or have the file upload completed on their behalf.

Does the OEM need to manage or collect any custom imaging files from customers? Do they need to upload any images to Microsoft?

No. OEMs just send the Computer Build Report (CBR) as usual to Microsoft. No images are sent to Microsoft to enable Windows Autopilot. Windows Autopilot only customizes OOOE and allows policy configurations.

Are there any customer issues with upgrading to a currently supported version of Windows?

The devices must be running a supported version of Windows general availability channel to enroll in Windows Autopilot deployment. Otherwise, there's generally no issue. For more information, see [Windows Autopilot - known issues](#).

Will the existing CBR with 4K hardware hash ever change?

No.

What new information needs to be sent from the OEM to Microsoft?

Nothing, unless the OEM opts to register the device on the customer's behalf. In this case, they must upload the device ID CSV file to the Microsoft Partner Center or use the OEM direct API.

Is there a contract or amendment for an OEM to participate in an Autopilot deployment?

No.

CSV schema

Can a comma be used in the CSV file?

No.

Is there a limit to the number of devices that can be listed in the CSV file?

Yes. The CSV file can only contain 500 devices to apply to a single profile. If more than 500 devices need to be applied to a profile, the devices need to be uploaded through multiple CSV files.

Does Microsoft have any recommendations on how an OEM should provide the CSV file to their customers?

Encrypt the CSV file when sending it to the business customer to self-register their Windows Autopilot devices through MPC, MSfB, or Intune.

Hardware hash

What data does the hardware hash need to include?

Every hardware hash submitted by the OEM has to contain the following data:

- **SMBIOS UUID:** A universally unique identifier.
- **MAC address:** The network card unique identifier.
- **Unique disk serial number:** If you use the Windows OEM Activation 3.0 tool.

Since Windows Autopilot is based on the ability to uniquely identify devices applying for cloud configuration, it's critical to submit hardware hashes that meet the outlined requirement.

Why are the SMBIOS UUID, MAC address, and disk serial number required in the hardware hash details?

As parts of the device are added or removed, these fields are needed to identify a device when creating the hardware hash. Since we don't have a unique identifier for Windows devices, these fields are the best logic to identify a device.

What's the difference between the OA3 hardware hash, the 4K hardware hash, and the Windows Autopilot hardware hash?

None. They're different names for the same thing. The OA3 tool output is called the OA3 hash, which is 4K in size, and is used for the Windows Autopilot deployment scenario.

Note

If an older unsupported Windows version of the OA3 tool is used, a different-sized hash is generated. This hash can't be used for a Windows Autopilot deployment.

If I need to replace hardware like the disk or network card, does that invalidate the hardware hash?

Yes. If you replace parts, you might need to generate a new hardware hash. It depends on the parts that were replaced, and the characteristics of the parts.

For example, if you replace the TPM or motherboard, it's a new device and you must get a new hardware hash. If you replace one network card, it's probably not a new device, and the device functions with the old hardware hash.

In general, after any hardware changes, assume the old hardware hash is invalid and get a new hardware hash. This process is recommended anytime you replace parts.

Motherboard replacement

How does Autopilot handle motherboard replacement scenarios?

Motherboard replacement is out of scope for Autopilot. Any repaired or serviced device that alters the ability to identify the device for Windows Autopilot must go through the normal OOBE process. It must manually select the right settings or apply a custom image.

To reuse the same device for Windows Autopilot after a motherboard replacement, use the following process:

1. Unregister the device from Autopilot.
2. Replace the motherboard.
3. Generate a new 4K hardware hash.
4. Register the device with the new 4K hardware hash or device ID.

Note

An OEM can't use the OEM direct API to re-register the device, which only accepts a tuple or PKID. In this case, the OEM can send the new 4K hardware hash information using a CSV file to customer, and let the customer re-register the device using MSfB or Intune.

SMBIOS

Are there any specific requirements for the SMBIOS UUID?

It must be unique as specified in the Windows hardware requirements.

What's the requirement on the SMBIOS table to meet the Windows Autopilot hardware hash need?

It must meet all the Windows hardware requirements. For more information, see [Windows Hardware Compatibility Program Specifications and Policies](#).

If the SMBIOS supports UUID and Serial Number, is it enough for the OA3 tool to generate the hardware hash?

No. At a minimum, the following SMBIOS fields need to have unique values:

- `ProductKeyID`.
- `SmbiosSystemManufacturer`.
- `SmbiosSystemProductName`.
- `SmbiosSystemSerialNumber`.
- `SmbiosSkuNumber`.
- `SmbiosSystemFamily`.
- `MacAddress`.
- `SmbiosUuid`.
- `DiskSerialNumber`.
- `TPM`.
- `EkPub`.

Technical interface

What's the interface to get the MAC address and disk serial number? How does the OA tool get this information?

The method for getting this information varies depending on the scenario, but in general:

- The disk serial number comes from `IOCTL_STORAGE_QUERY_PROPERTY` with `StorageDeviceProperty/PropertyStandardQuery`.
- The network MAC address is from `IOCTL_NDIS_QUERY_GLOBAL_STATS` from `OID_802_3_PERMANENT_ADDRESS`.

If a device has multiple network cards or disks, how does the OA3 tool choose which MAC address and disk serial number to use?

All available values are used, although there can be specific usage rules. The serial number of the system disk is more important than the other disks available. Network interfaces that are removable shouldn't be used if detected as they're removable. LAN vs WLAN shouldn't matter, as both are used.

End-user experience

How do I know that I received Autopilot?

A device has received an Autopilot configuration but hasn't yet applied it when the selection page is skipped and are immediately taken to a sign-in page.

Why did a user end up as an administrator when the Autopilot profile was configured otherwise?

Microsoft Entra administrators are always local administrators even if Windows Autopilot is configured to disable this configuration.

To help troubleshoot, run `licensingdiag.exe` and send the `.cab` (cabinet) file to AutopilotHelp@microsoft.com. If possible, also collect an ETL from Windows Performance Recorder (WPR).

Often in these cases, users aren't signing into the right Microsoft Entra tenant, or are creating local user accounts.

For a complete list of support options, see [Windows Autopilot support](#).

If I make changes to an existing Autopilot profile, do the changes take effect on devices that have that profile assigned to them and are already deployed?

No. Windows Autopilot profiles aren't resident on the device. They're downloaded during OOB and settings are defined at the time are applied. The profile is then discarded on the device. If the device is reimaged or reset, the new profile settings will take effect the next time the device goes through OOB.

What's the experience if a device isn't registered or if I don't configure Windows Autopilot before an end user attempts to self-deploy?

If the device isn't registered, it doesn't receive the Windows Autopilot experience, and the end user goes through normal OOB. The Windows Autopilot configurations won't be applied until the user runs through OOB again, after registration. If a device is started before a mobile device management (MDM) profile is created, the device goes through standard OOB experience. You then have to manually enroll that device into the MDM. The next time the device is reset, it will go through the Windows Autopilot OOB experience.

Why didn't I receive a customized sign-in screen during Autopilot?

To receive a customized sign-in experience, configure tenant branding in the [Azure portal](#).

What happens if a device is registered with Microsoft Entra ID but doesn't have a Windows Autopilot profile assigned?

Since no Windows Autopilot profile is assigned to the device, the user sees the default OOB.

How can I collect logs on Autopilot?

The best way to collect logs on Windows Autopilot performance is to collect a WPR trace during OOB. The XML file (WPRP extension) for this trace can be provided upon request.

MDM

Does Autopilot require the use of Microsoft Intune?

No. Any MDM works with Autopilot, but others might not have the same full suite of Windows Autopilot features as Intune. The best experience is with Intune.

Does Intune support preinstalling Win32 apps?

Yes. Intune supports Win32 apps using MSI and MSIX wrappers.

What is co-management?

Co-management enables you to concurrently manage currently supported versions of Windows by using both Microsoft Configuration Manager and Microsoft Intune. It lets you cloud-attach your existing investment in Configuration Manager by adding new functionality. By using co-management, you have the flexibility to use the technology solution that works best for your organization.

When a Windows device has the Configuration Manager client and is enrolled to Intune, you get the benefits of both services. You control which workloads, if any, you switch the authority from Configuration Manager to Intune. Configuration Manager continues to manage all other workloads, including those workloads that you don't switch to Intune, and all other features of Configuration Manager that co-management doesn't support.

For more information, see the following articles:

- [What is co-management?](#).
- [How to enroll with co-management when provision with Windows Autopilot.](#)

Does Autopilot require Configuration Manager?

No. It isn't required, but you can use it together with Autopilot in the following scenarios:

- Co-management.
- Autopilot for existing devices.

Features

What's self-deploying mode?

Self-deploying mode only requires the user to power on the device. It's useful for scenarios where a standard user account isn't needed. For example, shared or kiosk devices.

For more information, see [Windows Autopilot self-deploying mode](#).

What's Microsoft Entra hybrid join?

ⓘ Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. For more information, see [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization](#).

Microsoft Entra hybrid joined devices connect to an on-premises Active Directory domain and Microsoft Entra ID.

For more information, see [Introduction to device management in Microsoft Entra ID](#).

What's Windows Autopilot reset?

Windows Autopilot reset removes user apps and settings from a device, but maintains Microsoft Entra domain join and MDM enrollment. This feature is useful when you transfer a device from one user to another.

For more information, see [Windows Autopilot reset](#).

What's Autopilot personalization?

You can add the following customizations to the OOB experience:

- A personalized welcome message.
- Personalize the username hint.
- Your organization's logo.

What's Autopilot for existing devices?

Autopilot for existing devices offers an upgrade path to currently supported versions of Windows for an existing Windows device.

For more information, see [Autopilot for existing devices](#).

General

Which manufacturers are enabled for pre-population of username and automatic re-enrollment of pre-provisioning devices?

Current manufacturers enabled for this change are Dell, Dynabook, HP, Lenovo, and Microsoft Surface. We're working to add other manufacturers and will update this list once they're onboarded. For more information, see [Return of key functionality for Windows Autopilot sign-in and deployment](#).

If I wipe the machine and restart, do I still receive the Windows Autopilot experience?

Yes. If the device is still registered for Autopilot and is running a supported version of Windows, it receives the Autopilot experience.

Can I harvest the device fingerprint on existing devices?

Yes. If the device is running a supported version of Windows, you can harvest device fingerprints for registration. There are no plans to backport the functionality to earlier releases. There's no way to harvest them on devices running unsupported versions of Windows.

Is Windows Autopilot supported on other SKUs, for example, Surface Hub or HoloLens?

- Surface Hub and other SKUs not covered in [Software requirements](#) aren't supported with Windows Autopilot.
- HoloLens 1 doesn't support Windows Autopilot.
- HoloLens 2 supports Windows Autopilot self-deploying mode with Microsoft Intune and a currently supported version of Windows Holographic. Non-Microsoft MDM providers aren't supported.

For more information on HoloLens 2, see [Windows Autopilot for HoloLens 2](#).

Does Windows Autopilot work after motherboard replacement or image reinstallation?

Yes. For more information, see [Windows Autopilot motherboard replacement scenario guidance](#).

What does the error message "This user isn't authorized to enroll, error code 801c0003" mean?

There are limits to the number of devices a particular Microsoft Entra user can enroll in Microsoft Entra ID, and the number of devices that are supported per user in Intune. These limits are configurable, but not infinite. If you reuse devices, or roll back to previous virtual machine snapshots, this error occurs frequently.

What happens if a device is registered to a malicious agent?

By design, Windows Autopilot doesn't apply a profile until the user signs in with the matching tenant for the configured profile using the Microsoft Entra sign-in process. For example, `badguys.com` registers a device owned by `contoso.com`. At worst, the user is directed to sign in to `badguys.com`. When the user enters their email and password, the sign-in information is redirected through Microsoft Entra ID to the proper Microsoft Entra authentication and the user is prompted to then sign into `contoso.com`. Since `contoso.com` doesn't match `badguys.com` as the tenant, the malicious profile isn't applied and the user sees the regular OOB.

Where is Windows Autopilot data stored?

Windows Autopilot data is stored within the European Union (EU). It isn't stored in a sovereign cloud, even when the Microsoft Entra tenant is registered in a sovereign cloud. This storage applies to all Windows Autopilot data, whatever portal is used to deploy Autopilot.

Why is Windows Autopilot data stored in the US and not in a sovereign cloud?

Customer data isn't stored, only business data that enables Microsoft to provide a service. For that reason, it's appropriate for the data to be stored in the US. Customers can stop subscribing to the service at any time. In that event, Microsoft removes the business data. Autopilot isn't currently supported in any sovereign cloud.

How many ways are there to register a device for Windows Autopilot?

There are six ways to register a device, depending on who does the process:

1. OEM direct API, which is only available to TVOs.
2. MPC using the MPC API, which is only available to CSPs.
3. MPC using manual upload of CSV file in the UI, which is only available to CSPs.
4. MSfB using CSV file upload.
5. Intune using CSV file upload.
6. Microsoft 365 Business Premium portal using CSV file upload.

How many ways are there to create a Windows Autopilot profile?

There are four ways to create and assign a Windows Autopilot profile:

1. Through MPC, which is only available to CSPs.
2. Through MSfB.
3. Through Intune or another MDM service.
4. Microsoft 365 Business Premium portal.

Microsoft recommends creation and assignment of profiles through Intune.

What are some common causes of registration failures?

1. Bad or missing hardware hash entries can lead to faulty registration attempts.
2. Hidden special characters in CSV files. To avoid this issue, after creating your CSV file, open it in Notepad to look for hidden characters, trailing spaces, or other corruptions.

Is Autopilot supported in all countries/regions?

Autopilot only supports customers using global Azure. Global Azure doesn't include the following three entities:

- Azure Germany.
- Azure China 21Vianet.
- Azure Government.

If you use global Azure, there are no region restrictions. For example, Contoso uses global Azure but has employees working in China. The Contoso employees working in China can still use Autopilot to deploy devices. If Contoso uses Azure China 21Vianet, the Contoso employees can't use Autopilot.

While Autopilot is available in global tenants, users in China can experience poor connectivity and high latency when deploying due to ISP-related issues. If you're experiencing these issues when deploying in the region, contact your local ISP for support.

Why does TPM provisioning/attestation take longer during the first boot on a device?

TPM provisioning involves generating and processing strong cryptographic keys. Depending on the characteristics of the TPM hardware used on a device, it can take longer than a minute on first boot.

Why don't applications install after the ESP is finished on an Intune managed device when using autologon with Windows Autopilot self-deploying mode?

When autologon with Windows Autopilot self-deploying mode is used, autologon uses the KioskUser0 local account. By default, user ESP isn't processed for local accounts, including KioskUser0, and a device token isn't issued until user ESP is processed. When using autologon, in order for applications to install after the ESP finishes, skip user ESP by using the custom OMA-URI [SkipUserStatusPage](#). For more information, see the following articles:

- [How can I disable the user ESP portion of the Enrollment Status Page \(ESP\) if an ESP has been configured on the device?.](#)
- [Deploy OMA-URIs to target a CSP through Intune, and a comparison to on-premises.](#)

When Windows Autopilot for pre-provisioned deployment is used, the device shows as compliant in Microsoft Entra ID after completing the Technician flow. However, after starting the User flow, the device changes to noncompliant in Microsoft Entra ID. Why did it change from compliant to noncompliant in Microsoft Entra ID?

Device compliance in Microsoft Entra ID is reset during the User flow. Once the User flow completes, compliance is reevaluated and updated. This behavior is expected.

Intune Connector for Active Directory

What is the difference between the updated and legacy Intune Connector for Active Directory?

The updated Intune Connector for Active Directory strengthens security and follows least privilege principles by using a [Managed Service Account \(MSA\)](#) instead of using the

computer account (SYSTEM) of the server that runs the Intune Connector for Active Directory.

If the administrator installing and configuring the Intune Connector for Active Directory has the permissions outlined in the requirements, do they also have to follow the steps to increase the computer account limit in the OUs?

No. the Intune Connector for Active Directory installer takes care of setting up all of the proper permissions needed by the MSA in the OUs. The steps to increase the computer account limit in the OUs only need to be followed if the administrator installing and configuring the Intune Connector for Active Directory doesn't have the permissions outlined in [Intune Connector for Active Directory Requirements](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot troubleshooting FAQ

FAQ

Applies to:

- Windows 11.
- Windows 10.

This article provides troubleshooting for common Windows Autopilot issues.

Troubleshooting Windows Autopilot overview

What concepts should be understood when troubleshooting Windows Autopilot?

Windows Autopilot is designed to simplify all parts of the Windows device lifecycle, but there are always situations where issues might arise. When troubleshooting an issue, it's helpful to understand:

- The Windows Autopilot [process flow](#).
- How Windows Autopilot [device profiles](#) are downloaded.
- [Key activities](#) to perform during troubleshooting.

What is the Windows Autopilot process flow?

Whether performing user-driven or self-deploying device deployments, the troubleshooting process is about the same. It's useful to understand the flow for a specific device:

1. A network connection is established. The connection can be a wireless (Wi-fi) or wired (Ethernet) connection.
2. The Windows Autopilot profile is downloaded. When a wired connection is used, or a wireless connection is established, the profile downloads from the Windows Autopilot deployment service as soon as the network connection is in place.

3. User authentication occurs. During a user-driven deployment, the user enters their Microsoft Entra credentials, which is then validated.
4. Microsoft Entra join occurs. For user-driven deployments, the device is joined to Microsoft Entra ID using the specified user credentials. For self-deploying scenarios, the device is joined without specifying any user credentials.
5. Automatic mobile device management (MDM) enrollment occurs. As part of the Microsoft Entra join process, the device enrolls in the MDM service configured in Microsoft Entra ID (for example, Microsoft Intune).
6. Settings are applied. If the [enrollment status page](#) is configured, most settings are applied while the enrollment status page is displayed. If not configured or available, settings will be applied after the user is signed in.

How are Windows Autopilot device profiles downloaded?

When an Internet-connected Windows device boots up, it attempts to connect to the Windows Autopilot service and download a Windows Autopilot profile. The Windows Autopilot profile is downloaded as soon as possible, and again after each reboot.

Note

At this stage, it's important that a Windows Autopilot profile exists in the tenant so that a blank profile isn't cached locally on the device. If necessary, a new Windows Autopilot profile can be retrieved by rebooting the device.

If a computer needs to be rebooted during the Windows out-of-box experience (OOBE) to retrieve a new Windows Autopilot profile:

1. Select Shift-F10 to open a command prompt window.
2. In the command prompt window, enter one of the following two commands:
 - `shutdown.exe /r /t 0` to **restart** immediately.
 - `shutdown.exe /s /t 0` to **shut down** immediately.

For more information, see [Windows Setup Command-Line Options](#).

What are the key activities to perform when troubleshooting Windows Autopilot?

The key troubleshooting activities to perform are:

- Review configuration: Are Microsoft Entra ID and Microsoft Intune or a non-Microsoft mobile device management (MDM) service configured as specified in [Windows Autopilot configuration requirements](#)?
- Check network connectivity: Can the device access the services described in [Windows Autopilot networking requirements](#)?
- Windows out-of-box experience (OOBE) behavior: Are the [expected OOB](#) screens displayed? Is the Microsoft Entra credentials page customized with organization-specific details as expected?
- Microsoft Entra join issues: Is the device able to [join Microsoft Entra ID](#)?
- MDM enrollment issues: Is the device able to [enroll in Microsoft Intune](#) or non-Microsoft MDM service?
- Review logs that are automatically collected upon Windows Autopilot failure. For more information, see [Collect diagnostics from a Windows device](#).

How can additional detailed troubleshooting information be enabled?

On [Windows 11](#), the Windows Autopilot diagnostic page can be opened to view additional detailed troubleshooting information about the Windows Autopilot provisioning process. To enable the Windows Autopilot diagnostics page:

1. Go to the [ESP profile](#) where the Windows Autopilot diagnostics page needs to be enabled.
2. Make sure that **Show app and profile configuration progress** is selected to **Yes**.
3. Make sure that **Turn on log collection and diagnostics page for end users** is selected to **Yes**.

To access any diagnostic information once the diagnostic page is enabled, select the **View Diagnostics** button or enter the keystroke **CTRL + SHIFT + D**. The diagnostics page is currently supported under the following conditions:

- Windows 11.

- Windows Autopilot user-driven mode.
- When signing in with a Work or School account. Personal Microsoft accounts aren't supported.

ⓘ Note

- By default diagnostics are automatically collected upon a Windows Autopilot failure. For more information, see [Collect diagnostics from a Windows device](#).
- For diagnostics to be able to upload successfully from the client, make sure that the URL `lgmsapewe.u.blob.core.windows.net` isn't blocked on the network.

Where does Windows Autopilot log to?

Windows Autopilot logs entries into the event log. The log entries can be used to see details related to the Windows Autopilot profile settings and **OOBE** flow. These entries can be viewed using Event Viewer. Review the information in Event Viewer at **Application and Services Logs -> Microsoft -> Windows -> ModernDeployment-Diagnostics-Provider -> Autopilot**.

What do the different Event IDs mean in the Windows Autopilot event log entries in Event Viewer?

The following events might be recorded, depending on the scenario and profile configuration:

[+] Expand table

Event ID	Type	Message	Description
100	Warning	Autopilot policy [name] not found.	This error is typically a temporary problem, while the device is waiting for a Windows Autopilot profile to be downloaded.

Event ID	Type	Message	Description
101	Info	AutopilotGetPolicyDwordByName succeeded: policy name = [setting name]; policy value = [value].	This message shows Windows Autopilot retrieving and processing numeric OOBE settings.
103	Info	AutopilotGetPolicyStringByName succeeded: policy name = [name]; value = [value].	This message shows Windows Autopilot retrieving and processing OOBE setting strings such as the Microsoft Entra tenant name.
109	Info	AutopilotGetOobeSettingsOverride succeeded: OOBE setting [setting name]; state = [state].	This message shows Windows Autopilot retrieving and processing state-related OOBE settings.
111	Info	AutopilotRetrieveSettings succeeded.	This message means that the settings stored in the Windows Autopilot profile that control the OOBE behavior were retrieved successfully.
153	Info	AutopilotManager reported the state changed from [original state] to [new state].	Usually, this message says ProfileState_Unknown to ProfileState_Available . This case indicates that a profile was available and downloaded for the device and that the device is ready to deploy using Windows Autopilot.

Event ID	Type	Message	Description
160	Info	AutopilotRetrieveSettings beginning acquisition.	This message shows that Windows Autopilot is getting ready to download the needed Windows Autopilot profile settings.
161	Info	AutopilotManager retrieve settings succeeded.	The Windows Autopilot profile was successfully downloaded.
163	Info	AutopilotManager determined download isn't required and the device is already provisioned. Clean or reset the device to change this.	This message indicates that a Windows Autopilot profile is present on the device. The Sysprep /Generalize process typically removes a Windows Autopilot profile.
164	Info	AutopilotManager determined Internet is available to attempt policy download.	
171	Error	AutopilotManager failed to set TPM identity confirmed. HRESULT=[error code].	This message indicates an issue performing TPM attestation, needed to complete the self-deploying mode process.
172	Error	AutopilotManager failed to set Autopilot profile as available. HRESULT=[error code].	This error is typically related to event ID 171.
807	Error	ZtdDevicesNotRegistered	Validate that the device's hardware hash is properly uploaded to Intune and that the

Event ID	Type	Message	Description
			device is assigned to a deployment profile.
809	Error	ZtdDeviceHasNoAssignedProfile - Assigned profile does not exist.	The Windows Autopilot profile assigned to the device was deleted without first getting cleaned up. Assign a different Windows Autopilot profile to the device and then attempt to re-enroll the device.
815	Error	ZtdDeviceHasNoAssignedProfile - No profile assigned to the device, and no default profile found in the tenant.	A Windows Autopilot profile wasn't found assigned to the device. Validate that a Windows Autopilot profile is assigned to the device.
908	Error	SerialNumberMismatch ProductKeyIdMismatch	There's a mismatch between the serial number or product key recorded in Windows Autopilot and the physical hardware that is preventing enrollment. Reregister the device and then attempt to re-enroll the device.

Where are the Windows Autopilot profile settings received from the Windows Autopilot deployment service stored?

Windows Autopilot profile settings received from the Windows Autopilot deployment service are stored in the device's registry. This information can be found in the registry at the following registry key:

HKLM\SOFTWARE\Microsoft\Provisioning\Diagnostics\Autopilot

Available registry entries include:

[+] Expand table

Value	Description
AadTenantId	The GUID of the Microsoft Entra tenant the user signed into. The user receives an error if this entry doesn't match the tenant that was used to register the device.
CloudAssignedTenantDomain	The Microsoft Entra tenant the device is registered with, for example, <code>contosomn.onmicrosoft.com</code> . If the device isn't registered with Windows Autopilot, this value is blank.
CloudAssignedTenantId	The GUID of the Microsoft Entra tenant the device registered with. The GUID corresponds to the tenant domain from the CloudAssignedTenantDomain registry value. If the device isn't registered with Windows Autopilot, this value is blank.
IsAutopilotDisabled	If set to 1, this registry value indicates that the device isn't registered with Windows Autopilot. This state could also indicate that the Windows Autopilot profile couldn't be downloaded because of network connectivity or firewall issues, or network timeouts.
TenantMatched	This entry is set to 1 if the user's tenant ID matches the tenant ID that the device was registered with. If this registry value is 0, the user would be shown an error and forced to start over.
CloudAssignedOobeConfig	A bitmap that shows which Windows Autopilot settings were configured. Values include: <code>SkipCortanaOptIn</code> = 1, <code>OobeUserNotLocalAdmin</code> = 2, <code>SkipExpressSettings</code> = 4, <code>SkipOemRegistration</code> = 8, <code>SkipEula</code> = 16

Can ETW tracing be used with Windows Autopilot?

ETW tracing can be used to get detailed information from Windows Autopilot and related components. The ETW trace files can be viewed using the Windows Performance Analyzer or similar tools. For more information, see [Troubleshooting Windows Autopilot](#).

Why is the Intune Connector not logging in Event Viewer even though logging is enabled?

The Intune Connector originally logged in the Event Viewer directly under **Applications and Services Logs** in a log called **ODJ Connector Service**. However, logging for the Intune Connector has since moved to the path **Applications and Services Logs > Microsoft > Intune > ODJConnectorService**. If the ODJ Connector Service log at the original location is empty or not updating, check the new path location instead.

Troubleshooting Windows Autopilot device import and enrollment

Why is error code "0x80180014" occurring when trying to re-enroll a previously enrolled device?

Error code **0x80180014** can occur under either of the following scenarios:

1. Microsoft Intune changed the Windows Autopilot self-deployment mode and pre-provisioning mode experience. To reuse a device, the device record created by Intune must be deleted.

This change impacts all Windows Autopilot deployments that use the self-deployment or pre-provisioning mode. This change impacts devices when they are reused, reset, or when redeploying a profile.

To resolve and fix the issue in this scenario and redeploy the device using Windows Autopilot, follow these steps:

- a. Sign into the [Microsoft Intune admin center](#).
- b. In the **Home** screen, select **Devices** in the left hand pane.
- c. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
- d. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.

- e. In the **Windows | Enrollment** screen, under **Windows Autopilot**, select **Devices**.
- f. Select the device that is experiencing the error, and then in the toolbar select **Unblock device**.
- g. Redeploy the Windows Autopilot deployment profile.

 **Note**

A success message might not display after selecting **Unblock device**, but the device is ready to be used again.

2. Windows MDM enrollment is disabled in the Intune tenant.

To resolve and fix the issue in this scenario and redeploy the device using Windows Autopilot, follow these steps:

- a. Sign into the [Microsoft Intune admin center](#).
- b. In the **Home** screen, select **Devices** in the left hand pane.
- c. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
- d. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
- e. In the **Windows | Enrollment** screen, under **Enrollment options**, select **Device platform restriction**.
- f. In the **Enrollment restrictions** screen, under **Device type restrictions**, select **All Users** under the **Name** column.
- g. In the **All Users** screen that opens, under **Manage**, select **Properties**.
- h. In the **Properties** screen that opens, next to **Platform settings**, select the **Edit** link.
- i. In the **Edit restriction** screen that opens:
- j. Locate **Windows (MDM)** under the **Type** column.
- k. Make sure that **Windows (MDM)** is set to **Allow** under the **Platform** column.
- l. If **Windows (MDM)** is set to **Block**, change it to **Allow**.

- m. Select **Review + save**, and then either **Save** if a setting was changed, or **Cancel** if not settings were changed.
- n. Repeat the above steps for any additional restrictions that might exist in the **Enrollment restrictions** screen other than **All Users**. Only restrictions for the **Windows** platform need to be verified.

 **Note**

When multiple restrictions exist, restrictions might exist that only allow certain groups MDM enrollment. Some of the restrictions blocking MDM enrollment might be valid based on what group the restrictions are assigned to. When experiencing this problem, verify that the device isn't a member of one of the groups where there's MDM enrollment is blocked. Alternatively, if applicable change the MDM enrollment setting for that restriction to **Allow**.

In both of these scenarios, in addition to error **0x80180014** occurring, the Event Tracing for Windows (ETW) logs might also show the following mobile device management (MDM) error:

```
MDM Enroll: Server Returned Fault/Code/Subcode/Value=(DeviceNotSupported)  
Fault/Reason/Text=(Enrollment blocked for AP device by SDM One Time Limit Check)
```

When trying to import a CSV file with a device hardware hash, why does nothing happen when selecting Import?

This issue usually occurs because the device hash in the CSV file is incorrectly formatted. The issue can be confirmed by running a network trace while the issue occurs. Most likely the device hash in the CSV file is incorrectly formatted if an error **400** occurs in the network trace. The message body of the **400** error message shows:

```
Cannot convert the literal '[DEVICEHASH]' to the expected type 'Edm.Binary'
```

Anything that corrupts the collected hash can cause this error. One possibility is that the hash itself fails to be decoded, even if the hash is valid.

The device hash is Base64. At the device level, it's encoded as unpadded Base64, but Windows Autopilot expects padded Base64. Usually, the payload doesn't require padding and the process works. Sometimes, however, the payload doesn't line up cleanly and padding is necessary. In this case, the **400** error message occurs.

PowerShell's Base64 decoder also expects padded Base64, so this decoder can be used to validate that the hash is properly padded.

The "A" characters at the end of the hash are effectively empty data. Each character in Base64 is 6 bits. A in Base64 is 6 bits equal to 0. Deleting or adding As at the end doesn't change the actual payload data.

To resolve and fix this issue, the hash needs to be modified. The new value then needs to be tested until PowerShell succeeds in decoding the hash. The result is mostly illegible, which is fine as long as the error **Invalid length for a Base-64 char array or string** isn't displayed.

To test the base64, use the following PowerShell:

```
PowerShell  
  
[System.Text.Encoding]::ascii.GetString()  
[System.Convert]::FromBase64String("DEVICE HASH")
```

As an example:

```
PowerShell  
  
[System.Text.Encoding]::ascii.GetString()  
[System.Convert]::FromBase64String("Q29udG9zbwAAA")
```

This particular example isn't a device hash, but it's a misaligned unpadded Base64 so it's good for testing.

Now for the padding rules. The padding character is "=" . The padding character can only be at the end of the hash, and there can only be a maximum of two padding characters. Here's the basic logic.

- Does decoding the hash fail?
 - Yes: Are the last two characters "="?
 - Yes: Replace both "=" with a single "A" character, then try again
 - No: Add another "=" character at the end, then try again
 - No: That hash is valid

Looping the logic on the previous example hash, we get the following permutations:

- Q29udG9zbwAAA
- Q29udG9zbwAAA=
- Q29udG9zbwAAA==

- Q29udG9zbwAAAA
- Q29udG9zbwAAAA=
- **Q29udG9zbwAAAA==** - This result has valid padding.

Replace the collected hash with this new padded hash then try to import again.

Why is the Windows Autopilot profile not applied after a hardware change occurred on a device?

The Windows Autopilot profile isn't applied if the following conditions are met:

- A hardware change occurs on a device.
- The device is reimaged to a Windows version before one of the following versions:
 - Windows 11, version 21H2 with [KB5017383](#).
 - [Windows 10, versions 22H2](#).

This behavior is expected.

The message **Fix pending** or **Attention required** might also be displayed in the **Windows Autopilot devices** page for the device. These messages indicate that a hardware change occurred on the device. When the link for the **Fix pending** status is selected, the following message appears:

We've detected a hardware change on this device. We're trying to automatically register the new hardware. You don't need to do anything now; the status will be updated at the next check in with the result.

To resolve and fix this issue, deregister and re-register the device. For more information including how to deregister a device, see the following articles:

- [Deregister a device](#).
- [Return of key functionality for Windows Autopilot sign-in and deployment experience](#).
- [Windows Autopilot motherboard replacement scenario guidance](#).

Why is the join type for a device showing as "Microsoft Entra registered" instead of "Microsoft Entra joined"?

This issue occurs if the device was previously registered in Microsoft Entra ID before it was joined to Microsoft Entra ID. The device possibly registered in Microsoft Entra ID via something like a [Workplace join](#). If the Microsoft Entra ID registered device isn't deleted from Microsoft Entra ID before the device is joined to Microsoft Entra ID, then the previous trust type is retained in the record. Joining an existing Microsoft Entra registered device to Microsoft Entra ID results in the Windows Autopilot device showing as **Microsoft Entra registered** instead of **Microsoft Entra joined**.

To resolve and fix this issue, before registering an existing Microsoft Entra ID registered device as a Windows Autopilot device, the following existing device objects for the device should be deleted:

- Microsoft Intune.
- Microsoft Entra ID.
- Windows Autopilot.

After all device objects are deleted, re-register the device as a Windows Autopilot device and then re-enroll the device. For more information on properly deleting all of the device objects, see [Deregister a device](#).

Why is enrollment in Microsoft Intune or a non-Microsoft MDM solution failing with an error code "80180018"?

To troubleshoot enrollment issues in Microsoft Intune such as the error code 80180018 in the **Something went wrong** error page, see [Troubleshooting Windows device enrollment errors in Intune](#). Common issues can include:

- Incorrect or missing licenses assigned to the user.
- Too many devices enrolled for the user.

Why does Windows Autopilot Reset fail immediately with an error?

See [Windows Autopilot Reset: Troubleshooting](#) for more help if Windows Autopilot Reset fails immediately with the error:

Ran into trouble. Please sign in with an administrator account to see why and reset manually.

Troubleshooting Windows OOB issues during Windows Autopilot

Why is the Windows out-of-box experience (OOBE) not running as expected during Windows Autopilot?

It's useful to check if the device received a Windows Autopilot profile. If the device did receive a Windows Autopilot profile, verify that the settings in the profile are correct.

What is the cause of the error message "Can't connect to the URL of your organization's MDM terms of use."?

This error message usually indicates an issue with licensing. The complete error message reads:

Something went wrong

Can't connect to the URL of your organization's MDM terms of use. Try again, or contact your system administrator with the problem information from this page.

Verify that the user who is signing into the device has a valid Intune, EMS, or Microsoft 365 license.

Troubleshooting Microsoft Entra join issues

What is the most common issue joining a device to Microsoft Entra ID?

The most common issue joining a device to Microsoft Entra ID is related to Microsoft Entra permissions. Make sure that the correct configuration is in place to allow users to join devices to Microsoft Entra ID. For more information, see [Configuration requirements](#).

What happens if a user attempts to join more devices to Microsoft Entra ID than allowed?

Errors occur if a user exceeds the allowed number of devices they can join. This default limit is 50 devices but can be configured in Microsoft Entra ID. For more information, see [Understand Intune and Microsoft Entra device limit restrictions](#).

Why did deleting a device's object in Microsoft Entra ID cause the device to not be able to join Microsoft Entra ID any longer?

A Microsoft Entra device is created upon import. It's important this object isn't deleted. The object acts as Windows Autopilot's anchor in Microsoft Entra ID for group membership and targeting, including the profile. Deleting it might lead to Microsoft Entra join errors. If this object is deleted, the issue can be fixed by deleting and reimporting the device as a Windows Autopilot device. Deleting and reimporting the device as a Windows Autopilot device recreates the associated object in Microsoft Entra ID.

Troubleshooting policy conflicts with Windows Autopilot

Why is the web sign-in option missing at the Windows sign-in screen after Windows Autopilot pre-provisioning completes?

The [Device password policies](#) in the Security Baseline causes issues after pre-provisioning. To resolve, change the password settings in Security Baseline to **Not Configured** or assign the baseline to a user group.

Can policies conflict with Windows Autopilot working correctly?

There are a significant number of policy settings available for Windows, including:

- Native mobile device management (MDM) policies.
- Group policy (ADMX-backed) settings.

Some policy settings can cause issues in some Windows Autopilot scenarios. These issues can arise because of how the policies change Windows behavior. If any of these issues are discovered, remove the policy in question to resolve the issue.

What are some of the known policies that conflict with Windows Autopilot?

The following policies are known to cause issues with Windows Autopilot. Make sure to configure the policies appropriately so that they don't conflict with Windows Autopilot:

[+] Expand table

Policy	More information
Disallow changing of language/region/keyboard	This group policy object (GPO) isn't supported during the out-of-box experience (OOBE) flow as it impacts the autologon experience. If this policy needs to be set for users, select to hide these pages in the Windows Autopilot profile to prevent users from making changes.
AppLocker CSP	The AppLocker configuration service provider (CSP) isn't supported in the Enrollment Status Page as it triggers a reboot when a policy is applied or a deletion occurs.
Device restriction/Password Policy	<p>The out-of-box experience (OOBE) or user desktop autologon can fail when a device reboots during the device Enrollment Status Page (ESP). This failure can occur when certain DeviceLock policies are applied to a device. Such policies can include:</p> <ul style="list-style-type: none">• Minimum password length and password complexity• Any similar group policy settings (including any that disable autologon) <p>This possible failure is especially true for kiosk scenarios where passwords are automatically generated.</p>
Windows Security Baseline/Administrator elevation prompt behavior	These policies require a reboot, as a result more prompts might appear when modifying user account control (UAC) settings during the OOBE

Policy	More information
Windows Security Baseline / Enable virtualization based security	<p>using the device Enrollment Status Page (ESP). Increased prompts are more likely if the device reboots after policies are applied. To work around this issue, the policies can be targeted to users instead of devices so that they apply later in the process.</p>
Device restrictions/Cloud and Storage/Microsoft Account sign-in assistant	<p>Setting this policy to "disabled" turns off the Microsoft Sign-in Assistant service (wlidsvc). Windows Autopilot requires this service to get the Windows Autopilot profile.</p>
Registry keys that affect Windows Autopilot if a device setting requires a reboot during device ESP	<p>Registry key: If the AutoAdminLogon registry key is set to 0 (disabled), this breaks Windows Autopilot.</p> <p>Registry path: <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Automatic logon</code></p>
MDM wins over Group Policy	<p>This policy allows control of which policy is used when both the MDM policy and its equivalent Group Policy (GP) are set on the device.</p>
Group Policy Objects (GPOs) that affect Windows Autopilot for pre-provisioned deployment	<p>Windows Autopilot pre-provisioning doesn't work when any of the four GPO policy settings listed here are enabled.</p> <p>GPO path: <code>Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options</code></p> <p>Policies:</p> <ul style="list-style-type: none"> Interactive logon: Message title for users attempting to log on Interactive logon: Message text for users attempting to log on Interactive logon: Require Windows Hello for Business or smart card

Policy	More information
	User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode - Prompt for credentials on the secure desktop
PreferredAadTenantDomainName	When this policy is enabled, it adds the preferred domain to DefaultUser0 , which causes autologon to fail.

Troubleshooting application install issues during Windows Autopilot

Why is the error message "Another installation is in progress, please try again later" occurring during the ESP of a Windows Autopilot deployment?

The Enrollment Status Page (ESP) used by Windows Autopilot doesn't support mixing of line-of-business (LOB) and Win32 applications. Both LOB and Win32 applications use **TrustedInstaller** which doesn't allow simultaneous installations. If both an LOB and Win32 application attempt to install at the same time, the following error message occurs during ESP:

Another installation is in progress, please try again later.

For more information, see [Set up the Enrollment Status Page - Device setup: Apps](#).

If mixing LOB and Win32 apps is required, consider using [Windows Autopilot device preparation](#), which doesn't use ESP so therefore supports mixing of LOB and Win32 apps.

During the ESP of a Windows Autopilot deployment, why does the Microsoft 365 Click-to-Run version of Office fail to install the Teams Machine-Wide Installer, or cause other Win32 app MSI based installs to fail?

The Teams Machine-Wide Installer component of the Microsoft 365 Click-to-Run version of Office includes an MSI installation. ESP doesn't track the Teams Machine-Wide Installer MSI install. Because ESP doesn't track the Teams Machine-Wide Installer MSI install, it can cause a conflict when other Win32 app MSI based installs attempt to install during ESP. MSIs install via **TrustedInstaller** which doesn't allow simultaneous installations. This conflict can cause either the Teams Machine-Wide Installer to fail or other MSI based installs to fail during ESP. For more information, see [Set up the Enrollment Status Page - Device setup: Apps](#).

This issue might be random and might not always occur. The issue occurs due to a timing issue between the Teams Machine-Wide Installer MSI install and other Win32 app MSI installs.

To work around the issue or avoid the error, use one of the following solutions:

1. Don't install **Teams** as part of the Microsoft 365 Click-to-Run install of Office. Instead, deploy **Teams** as a Win32 app after the Windows Autopilot deployment completes.
2. Don't install the Microsoft 365 Click-to-Run version of Office during ESP. Instead, deploy the Microsoft 365 Click-to-Run install of Office after the Windows Autopilot deployment completes.
3. Use a custom PowerShell script for Intune Management Extension (IME) that checks if **TrustedInstaller** is currently installing another MSI. If it is, then wait for the current MSI to finish installing before launching a new MSI install.
4. For Windows 11 deployments, use [Windows Autopilot device preparation](#). Windows Autopilot device preparation doesn't use ESP so therefore supports mixing of LOB and Win32 apps.
5. Continue on error for ESP failures. If the problem occurs with this option enabled, some applications including **Teams** might not install. However, ESP continues and doesn't fail.

Troubleshooting the Intune Connector for Active Directory

Why is the Intune Connector for Active Directory not logging in Event Viewer even though logging is enabled?

The Intune Connector for Active Directory originally logged in the Event Viewer directly under Applications and Services Logs in a log called **ODJ Connector Service**. However, logging for the Intune Connector for Active Directory has since moved to the path **Applications and Services Logs > Microsoft > Intune > ODJConnectorService**. If the **ODJ Connector Service** log at the original location is empty or not updating, check the new path location instead.

Why does uninstalling the Intune Connector for Active Directory through the Settings app not fully remove the application?

The Intune Connector for Active Directory needs to be uninstalled using both the Settings app and the Intune Connector for Active Directory installed executable **ODJConnectorBostrapper.exe**. When uninstalling the Intune Connector for Active Directory, run **ODJConnectorBostrapper.exe** and select the **Uninstall** option. The **ODJConnectorBostrapper.exe** installer version needs to match the version of the connector that's being uninstalled.

Why is the error "The MSA account couldn't be granted permission to create computer objects in the following OUs" occurring when installing the Intune Connector for Active Directory?

This error might occur for several different type of failures including:

- The administrator installing and configuring the Intune Connector for Active Directory doesn't have the required permissions as outlined in the [Intune Connector for Active Directory Requirements](#).
- The organization unit (OU) specified in the Intune Connector for Active Directory **ODJConnectorEnrollmentWiazard.exe.config** XML configuration file doesn't exist.

For detailed information on the error and what caused it, see the **ODJConnectorUI.log** normally located in the folder **C:\Program Files\Microsoft Intune\ODJConnector\ODJConnectorEnrollmentWizard**.

For more information, see [Install the Intune Connector for Active Directory on the server](#).

Why did enrollments start failing when using the Intune Connector for Active Directory?

Make sure that the Intune Connector for Active Directory is updated to version 6.2501.2000.5 or later and that the legacy version isn't still being used. For more information, see [Intune Connector for Active Directory Requirements](#).

Related content

- [Windows Autopilot - known issues.](#)
- [Collect MDM logs.](#)
- [Collect diagnostics from a Windows device.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot - known issues

Article • 02/27/2025 • Applies to:  Windows 11,  Windows 10

This article describes known issues that can often be resolved with configuration changes or via cumulative updates. Some known issues might also be resolved automatically in a future release.

Tip

RSS can be used to notify when new known issues are added to this page. For example, the following RSS link includes this article:

url

```
https://learn.microsoft.com/api/search/rss?  
search=%22Be+informed+about+known+issues+that+might+occur+during+Window  
s+Autopilot+deployment.%22&locale=en-us&%24filter=
```

This example includes the `&locale=en-us` variable. The `locale` variable is required, but it can be changed to another supported locale. For example, `&locale=es-es`.

For more information on using RSS for notifications, see [How to use the docs](#) in the Intune documentation.

Note

For issues with Autopilot with Co-management, see [Windows Autopilot with co-management](#).

Known issues

Windows Autopilot report incorrectly shows failure even though the deployment was successful

Date added: *February 11, 2025*

The Windows Autopilot report automatically updates deployment status from **In progress** to **Failed** after 4 hours if Intune didn't receive a success or failure status. It's possible that the report didn't receive the latest status from the device before the device

is powered off which results in an incorrect **Failed** status, even when the deployment is successful.

Local Administrator Password Solution (LAPS) policy isn't being applied during the Technician Flow

Date added: *December 9, 2024*

During Windows Autopilot pre-provisioning technical flow, if a LAPS policy is targeted to the device or user, it isn't applied until the user phase begins.

Windows Autopilot deployment report and AutopilotEvents Graph API only returns 50 records at a time

Date added: *December 4, 2024*

In Intune's 2411 release, we've updated the backend infrastructure of the Windows Autopilot deployment report for consistency with other Intune reports. With this change, the Windows Autopilot deployment report and the [AutopilotEvents Microsoft Graph API](#) now return 50 records at a time. To show more than 50 records at a time:

- Use the `skipToken` parameter to get additional pages of data with the AutopilotEvents Graph API.
- Use the [export API](#) with `reportName` `AutopilotV1DeploymentStatus` to get all records.

DFCI enrollment fails for Professional editions of Windows 11, version 24H2

Date added: *October 9, 2024*

Date updated: *January 15, 2025*

DFCI can't currently be configured during the out-of-box experience (OOBE) on devices with Professional editions of Windows 11, version 24H2

For devices that have already been provisioned and have Professional editions of Windows 11, version 24H2, install [KB5046740](#) or later to enroll in DFCI. Devices with Professional editions of Windows 11, version 24H2 that have KB5046740 or later installed are automatically enrolled in DFCI after a reboot.

If DFCI needs to be configured during OOBE provisioning on 24H2 devices, follow these steps:

1. During OOBE onboarding, ensure the device is upgraded to the Enterprise edition of Windows 11, version 24H2.
2. After upgrading to the Enterprise edition of Windows 11, version 24H2, sync the device.
3. Once the device is synced, reboot it to get it enrolled in DFCI.

Autopilot deployment report doesn't support sorting

Date added: *August 29, 2024*

The Autopilot deployment report was updated to a new infrastructure that doesn't currently support column sorting. The issue will be addressed in the future.

Auto logon for Kiosk device profile only partially fixed

Date added: *August 21, 2024*

The known issue of [Kiosk device profiles not auto logging in when auto logon was enabled](#) was previously reported as fixed. However, there are scenarios where the issue might still occur when using autologon with Kiosks and [Assigned Access](#). If multiple reboots or unexpected reboots occur during the Windows out-of-box experience (OOBE) when initially configuring the Kiosk, the autologon entries in the registry might be deleted. The issue is being investigated.

The following workarounds are available until the issue is resolved:

1. Apply or reapply the kiosk profile after Windows Autopilot completes.
2. Apply the autologon registry entries either manually or via a script. For example:

Windows Command Prompt

```
reg.exe add "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon" /v "AutoAdminLogon" /t REG_SZ /d 1 /f  
  
reg.exe add "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon" /v "DefaultDomainName" /t REG_SZ /d "." /f  
  
reg.exe add "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon" /v "DefaultUserName" /t REG_SZ /d  
"kioskUser0" /f
```

3. Exclude items the required reboots during OOBE from Windows Autopilot.

4. Manually enter the kiosk user credentials.

For more information, see [Assigned Access recommendations - Automatic sign-in](#). For additional assistance, contact support.

BitLocker encryption defaults to 128-bit when 256-bit encryption is configured

Date added: *July 8, 2024*

In some Windows Autopilot deployments of unregistered devices, BitLocker encryption might default to 128-bit even though the admin configured 256-bit encryption due to a known race condition. The issue is being investigated. Microsoft recommends that customers who need 256-bit BitLocker encryption register devices for Autopilot.

Required apps aren't shown on the Enrollment Status Page (ESP) after an Autopilot Reset

Date added: *May 17, 2024*

When an Autopilot Reset happens, the required apps aren't installed on the Enrollment Status Page (ESP) before the user reaches the desktop. The apps aren't tracked on the ESP, but the apps are installed when the user signs in to the desktop.

Enrolled date for Autopilot device is incorrect

Date added: *November 1, 2023*

The **Enrolled date** in the **Devices | All devices** and **Windows | Windows devices** panes display the date the device was registered to Autopilot instead of the date it was enrolled to Autopilot. For a more accurate date for when the device enrolled to the tenant:

1. Use the Intune Graph API to query the device:

```
devices?$filter=physicalIds/any(p: startswith(p,  
'[ZTDID']))&$select=id,deviceId,displayName,physicalIds,createdDateTime
```

For more information, see [Intune devices and apps API overview](#) and [Working with Intune in Microsoft Graph](#).

2. Use the Windows Autopilot deployment report for recently deployed devices.

Filtering Windows Autopilot devices not working as expected

Date added: *July 14, 2023*

Viewing Windows Autopilot devices within Intune might not work as expected if attempting to filter results. While this issue is being worked on, a workaround is to use [Microsoft Graph API](#) to properly query and filter necessary devices.

TPM attestation isn't working on some platforms with Infineon SLB9672 discrete TPMs

Date added: *June 2, 2023*

Platforms with the Infineon SLB9672 TPM with firmware release 15.22 with EK certificate might fail with error message **Something happened, and TPM attestation timed out**. To resolve this issue, contact the OEM for an update.

Kiosk device profile not auto logging in

Date added: *January 30, 2023*

Date updated: *August 21, 2024*

There's currently a known issue in the following Windows Updates released in January 2023:

- Windows 11, version 22H2: [KB5022303 ↗](#)
- Windows 11, version 21H2: [KB5022287 ↗](#)
- Windows 10, version 22H2: [KB5022282 ↗](#)

If these updates are installed on a device, Kiosk device profiles that have auto logon enabled won't auto log on. After Autopilot completes provisioning, the device stays on the sign-in screen prompting for credentials. To work around this known issue, manually enter the kiosk user credentials with the username `kioskUser0` and no password. After the username is entered with no password, it should go to the desktop. This issue should be resolved in cumulative updates released for Windows 11 in April 2023 and Windows 10 in March 2023:

- Windows 11, version 22H2: [KB5025239 ↗](#) or later.
- Windows 11, version 21H2: [KB5025224 ↗](#) or later.

- Windows 10, version 22H2: [KB5023773](#) or later.

Note

This issue was only partially fixed and can still occur under certain conditions. For more information, see [Auto logon for Kiosk device profile only partially fixed](#).

TPM attestation isn't working on AMD platforms with ASP fTPM

Date added: *December 1, 2022*

TPM attestation for AMD platforms with ASP firmware TPM might fail with error code 0x80070490 on Windows systems. This issue is resolved on later versions of AMD firmware. Consult with device manufacturers and firmware release notes for which firmware versions contain the update.

TPM attestation failure with error code 0x81039001

Date added: *October 6, 2022*

Some devices might intermittently fail TPM attestation during Windows Autopilot pre-provisioning technician flow or self-deployment mode with the error code **0x81039001 E_AUTOPILOT_CLIENT_TPM_MAX_ATTESTATION_RETRY_EXCEEDED**. This failure occurs during the **Securing your hardware** step for Windows Autopilot devices deployed using self-deploying mode or pre-provisioning mode. Subsequent attempts to provision might resolve the issue.

Autopilot deployment report shows "failure" status on a successful deployment

Date added: *September 22, 2022*

The Autopilot deployment report (preview) shows a failed status for any device that experiences an initial deployment failure. For subsequent deployment attempts, using the **Try again** or **Continue to desktop** options, the deployment state in the report doesn't update. If the user resets the device, a new deployment row is shown in the report with the previous attempt remaining as failed.

Autopilot deployment report doesn't show deployed device

Date added: *September 22, 2022*

Autopilot deployments that take longer than one hour might display an incomplete deployment status in the deployment report. If the device successfully enrolls but doesn't complete provisioning after more than one hour, the device status might not be updated in the report.

Autopilot profile not being applied when assigned

Date added: *June 15, 2022*

In Windows 10, version 21H2 April 2022 and some May 2022 update releases, there's an issue where the Autopilot profile might fail to apply to the device. Additionally, the hardware hash might not be harvested. As a result, any settings made in the profile might not be configured for the user such as device renaming. To resolve this issue, apply [KB5015020](#) ↗ cumulative update or later to the device.

DefaultuserX profile not deleted

Date added: *March 28, 2022*

When the [EnableWebSignIn CSP](#) is used, the `defaultuserX` profile might not be deleted.

Autopilot reset ran into trouble. Could not find the recovery environment

Date added: *March 28, 2022*

When an Autopilot reset is attempted, the following message is displayed:

Autopilot reset ran into trouble. Could not find the recovery environment

If there isn't an issue with the recovery environment, enter administrator credentials to continue with the reset process.

Device-based Conditional Access policies

Date added: *March 3, 2022*

1. The Intune Enrollment app must be excluded from any Conditional Access policy requiring **Terms of Use** because it isn't supported. See [Per-device terms of use](#).
2. Exceptions to Conditional Access policies to exclude **Microsoft Intune Enrollment** and **Microsoft Intune** cloud apps are needed to complete Autopilot enrollment in cases where restrictive policies are present such as:
 - Conditional Access policy 1: Block all apps except those apps on an exclusion list.
 - Conditional Access policy 2: Require a compliant device for the apps on the exclusion list.

In this case, Microsoft Intune Enrollment and Microsoft Intune should be included in that exclusion list of policy 1.

If a policy is in place such that **all cloud apps** require a compliant device (there's no exclusion list), by default Microsoft Intune Enrollment is excluded, so that the device can register with Microsoft Entra ID and enroll with Intune and avoid a circular dependency.

3. **Hybrid Microsoft Entra devices:** When Hybrid Microsoft Entra devices are deployed with Autopilot, two device IDs are initially associated with the same device - one Microsoft Entra ID and one hybrid. The hybrid compliance state displays as **N/A** when viewed from the devices list in the [Azure portal](#) until a user signs in. Intune only syncs with the Hybrid device ID after a successful user sign-in.

The temporary **N/A** compliance state can cause issues with device based Conditional Access policies that block access based on compliance. In this case, this behavior of Conditional Access is intended. To resolve the conflict, a user must sign in to the device, or the device-based policy must be modified. For more information, see [Conditional Access: Require compliant or Microsoft Entra hybrid joined device](#).

4. Conditional Access policies such as BitLocker compliance require a grace period for Autopilot devices. This grace period is needed because until the device is rebooted, the status of BitLocker and Secure Boot aren't captured. Since the status isn't captured, it can't be used as part of the Compliance Policy. The grace period can be as short as 0.25 days.

Device goes through Autopilot deployment without an assigned profile

Date added: *March 2, 2022*

When a device is registered in Autopilot and no profile is assigned, the default Autopilot profile is taken. This behavior is by design. It makes sure that all devices registered with Autopilot go through the Autopilot experience. If the device shouldn't go through an Autopilot deployment, remove the Autopilot registration.

White screen during Microsoft Entra hybrid joined deployment

Date added: *February 19, 2022*

There's a UI bug on Autopilot Microsoft Entra hybrid joined deployments where the Enrollment Status page is displayed as a white screen. This issue is limited to the UI and shouldn't affect the deployment process.

This issue was resolved in September 2022.

Virtual machine failing at "Preparing your device for mobile management"

Date added: *February 19, 2022*

When trying to use Windows Autopilot on a virtual machine (VM), the following error might occur:

"Preparing your device for mobile management

To resolve the issue, make sure the virtual machine is configured with a minimum of 2 processors and 4 GB of memory.

ODJConnectorSvc.exe leaks memory

Date added: *February 19, 2022*

When a proxy server is used with the ODJConnector service, the memory file can get too large when processing requests resulting in impacts to performance. The current workaround for this issue is to restart the ODJConnectSvc.exe service.

Reset button causes pre-provisioning to fail on retry

Date added: *February 19, 2022*

When ESP fails during the pre-provisioning flow and the user selects the reset button, TPM attestation might fail during the retry.

TPM attestation failure on Windows 11 error code 0x81039023

Date added: *February 19, 2022*

Some devices might fail TPM attestation on Windows 11 during the pre-provisioning technician flow or self-deployment mode with the error code 0x81039023. To resolve the issue, apply the May 2022 cumulative update for Windows 11, version 21H2 [KB5013943 ↗](#) or later to the device.

Duplicate device objects with Microsoft Entra hybrid deployments

Date added: *January 9, 2022*

A device object is pre-created in Microsoft Entra ID once a device is registered in Autopilot. If a device goes through a hybrid Microsoft Entra deployment, by design, another device object is created resulting in duplicate entries.

TPM attestation failure on Windows 11 error code 0x81039024

Date added: *December 8, 2021*

Some devices might fail TPM attestation on Windows 11 during the pre-provisioning technician flow or self-deployment mode with the error code 0x81039024. This error code indicates that there are known vulnerabilities detected with the TPM and as a result attestation fails. If this error occurs, visit the PC manufacturer's website to update the TPM firmware.

Delete device record in Intune before reusing devices in self-deployment mode or Pre-Provisioning mode

Devices are enrolled using Autopilot self-deployment mode or pre-provisioning mode. If a device is redeployed so that it reruns the Autopilot deployment again, it fails with a `0x80180014` error code.

To resolve this error, use one of the following work around methods:

- Delete the device record in Intune, and then redeploy the device so that it reruns the Autopilot deployment. For more information, see [Deregister a device](#).
- Remove the device enrollment restriction for Windows (MDM) personally owned devices. For more information, see [Set enrollment restrictions in Microsoft Intune](#).

For more information on this issue, see [Troubleshooting Windows Autopilot device import and enrollment](#).

A non-assigned user can sign in when using user-driven mode with Active Directory Federation Services (ADFS)

In a Windows Autopilot user-driven Microsoft Entra joined environment, a user can be pre-assigned to a device. If the user is a cloud-native Microsoft Entra account, the username is enforced and the user is only asked for their password. There's no way to sign in with another user ID. However, when ADFS is used, the username assignment isn't enforced. A different user than the one assigned can sign in on the device.

Intune connector is inactive but still appears in the Intune Connectors

Inactive Intune connectors will be automatically cleaned up after 30 days of inactivity without admin interaction.

Autopilot sign-in page displays HTML tags from company branding settings

When [customizations are applied to the company branding settings](#), the HTML tags might be visible and not rendered correctly on the update password page. This issue should be fixed in future versions of Windows.

TPM attestation isn't working on Intel Tiger Lake platforms

TPM attestation support for Intel firmware TPM Tiger Lake platforms on devices with Windows 10, version 21H2 require the November 2021 cumulative update [KB5007253](#) or later. Older versions of Windows aren't supported.

Blocking apps specified in a user-targeted Enrollment Status Profile are ignored during device ESP

The services responsible for determining the list of apps that should be blocking during device ESP aren't able to determine the correct ESP profile containing the list of apps because they don't know the user identity. As a workaround, enable the default ESP profile (which targets all users and devices) and place the blocking app list there. To avoid this issue, target the ESP profile to [device groups](#).

That username looks like it belongs to another organization. Try signing in again or start over with a different account

Confirm that all of the information is correct in the registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Provisioning\Diagnostics\Autopilot`

For more information, see [Where are the Windows Autopilot profile settings received from the Windows Autopilot deployment service stored?](#).

Windows Autopilot user-driven hybrid Microsoft Entra deployments don't grant users Administrator rights even when specified in the Windows Autopilot profile

This issue occurs when there's another user on the device that already has Administrator rights. For example, a PowerShell script or policy could create another local account that is a member of the Administrators group. To ensure this works properly, don't create another account until after the Windows Autopilot process is complete.

Windows Autopilot device provisioning can fail

These failures might be because of TPM attestation errors or ESP timeouts on devices where the real-time clock is off by a significant amount of time. For example, several minutes or more.

To fix this issue:

- Boot the device to the start of the out-of-box experience (OOBE).
- Establish a network connection (wired or wireless).
- Run the command `w32tm /resync /force` to sync the time with the default time server (`time.windows.com`).

Windows Autopilot for existing devices doesn't work

During a Windows Autopilot for existing devices deployment, screens that are disabled in the Windows Autopilot profile are shown, such as the Windows License Agreement screen.

This issue happens because Windows deletes the `AutopilotConfigurationFile.json` file when `Sysprep.exe` runs with the `/Generalize` parameter. The **Prepare Windows for Capture** task in a Configuration Manager task sequence runs `Sysprep.exe` with the `/Generalize` parameter.

To fix this issue:

- Edit the Configuration Manager task sequence and disable the **Prepare Windows for Capture** step.
- Add a new **Run command-line** step that runs the following command:

Windows Command Prompt

```
C:\Windows\System32\sysprep\sysprep.exe /oobe /reboot
```

For more information, see [Modify the task sequence to account for Sysprep command line configuration](#) and [Prepare Windows for Capture](#).

Windows Autopilot self-deploying mode fails with an error code

For more information on this scenario, see [Windows Autopilot self-deploying mode](#).

[+] Expand table

Error code	Description
0x800705B4	This general error indicates a timeout. A common cause of this error in self-deploying mode is that the device isn't TPM 2.0 capable. For example, it's a virtual machine. Devices that aren't TPM 2.0 capable can't be used with self-deploying mode.
0x801c03ea	This error indicates that TPM attestation failed, causing a failure to join Microsoft Entra ID with a device token.
0xc1036501	The device can't do an automatic MDM enrollment because there are multiple MDM configurations in Microsoft Entra ID.

Pre-provisioning gives an error screen and the Microsoft-Windows-User Device Registration/Admin event log displays HResult error code 0x801C03F3

This issue can happen if Microsoft Entra ID can't find a Microsoft Entra device object for the device that is being deployed. This issue occurs the object was manually deleted. To fix it, remove the device from Microsoft Entra ID, Intune, and Autopilot, then re-register it with Autopilot, which recreates the Microsoft Entra device object. For more information, see [Deregister a device](#).

To get troubleshooting logs, run the following command:

Windows Command Prompt

```
Mdmdiagnosticstool.exe -area Autopilot;TPM -cab c:\autopilot.cab
```

Pre-provisioning gives an error screen

Pre-provisioning isn't supported on a VM.

Error importing Windows Autopilot devices from a .csv file

Ensure that the .csv file isn't edited in Microsoft Excel or an editor other than Notepad. Some of these editors can introduce extra characters causing the file format to be invalid.

Windows Autopilot for existing devices doesn't follow the Autopilot OOB experience

Ensure that the JSON profile file is saved in **ANSI/ASCII** format, not Unicode or UTF-8.

Something went wrong is displayed page during OOB

The client is likely unable to access all the required Microsoft Entra ID/MSA-related URLs. For more information, see [Networking requirements](#).

Using a provisioning package in combination with Windows Autopilot can cause issues, especially if the

PPKG contains join, enrollment, or device name information

Using PPKGs in combination with Windows Autopilot isn't recommended.

Related content

- [Collect MDM logs.](#)
 - [Troubleshooting Windows Autopilot overview.](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot scenarios

Article • 06/19/2024 • Applies to:  Windows 11,  Windows 10

Due to different environments, different configurations, and different needs, Windows Autopilot offers several different scenarios. The following table summarizes the scenarios that are available in Windows Autopilot:

 Expand table

Scenario	Purpose	Description
Windows Autopilot user-driven mode	Device for a single user	User runs deployment
Windows Autopilot for pre-provisioned	Device for a single user	Deployment is split between IT admin/OEM/reseller and user
Windows Autopilot self-deploying mode	Kiosk device or device for multiple users	Deployment is completely automated
Windows Autopilot for existing devices	Prepare device where Windows OS needs to be reinstalled for a Windows Autopilot deployment	Utilizes Microsoft Configuration Manager to install a fresh Windows OS on an existing device before running a Windows Autopilot deployment
Windows Autopilot Reset	Resets an existing device back to the factory default installation of Windows	Utilizes the existing installation of Windows on a device to rebuild Windows and restore it back to the factory installation of Windows

Note

This tutorial is for **Windows Autopilot**. For the **Windows Autopilot device preparation** tutorial, see [Windows Autopilot device preparation scenarios](#).

Scenario capabilities

The following table compares the different capabilities for each Autopilot scenario:

 Expand table

Scenario	User-driven	Pre-provisioned	Self-deploying	Existing devices	Reset
Supports Microsoft Entra join	Yes	Yes	Yes	Yes	Yes
Supports Microsoft Entra hybrid join	Yes	Yes	No	Yes	No
Deployment requires interaction by user	Yes	Yes	No	NA	Local reset
Deployment requires interaction by IT admin/OEM/reseller	No	Yes	No	Yes	Remote reset
Supports assigning user to device	Yes	Yes	No	NA	NA
Minimizes time user interacts with deployment	No	Yes	Yes	NA	NA
User authenticates	Yes	User flow	No	NA	Local reset
TPM authenticates	No	Technician flow	Yes	NA	NA
Needs to be registered as Autopilot device before deployment	Yes	Yes	Yes	No	Yes

ⓘ Note

The **Windows Autopilot for existing devices** scenario is a method to completely reinstall Windows on a device in preparation to run a Windows Autopilot deployment. However the Windows Autopilot for existing devices scenario itself isn't technically an Autopilot deployment. After the Windows Autopilot for existing devices process completes, it automatically runs an Autopilot scenario.

The above table lists what the Windows Autopilot for existing devices scenario can potentially support. However, a given Windows Autopilot scenario might not always be supported once the **Windows Autopilot for existing devices** scenario completes.

Scenario pros and cons

The following table describes the pros and cons of each Windows Autopilot scenario during the deployment process.

[Expand table](#)

Scenario	Pros	Cons
User-driven	<ul style="list-style-type: none"> Requires no interaction from admin/OEM/reseller. Doesn't require TPM attestation so works on physical devices and VMs. 	<ul style="list-style-type: none"> Takes longer for user than the pre-provisioned scenario since user has to go through both device ESP and user ESP.
Pre-provisioned	<ul style="list-style-type: none"> Faster for user since IT admin/OEM/reseller handles bulk of device ESP during the technician flow. 	<ul style="list-style-type: none"> Requires interaction by IT admin/OEM/reseller. Requires TPM attestation during technician flow so only works on physical devices with supported TPM (doesn't work in VMs even with virtual TPM).
Self-deploying	<ul style="list-style-type: none"> Requires no interaction from user or admin/OEM/reseller. 	<ul style="list-style-type: none"> Can't assign a user to the device. User ESP doesn't run during the Autopilot deployment since no user is assigned. Requires TPM attestation so only works on physical devices with supported TPM (doesn't work in VMs even with virtual TPM). Doesn't support Microsoft Entra hybrid join devices.
Existing devices	<ul style="list-style-type: none"> Can use custom images. Can use ConfigMgr task sequences. Can reinstall a fresh copy of Windows in cases of severe corruption in Windows installation. Good scenario to upgrade a device from domain joined or Microsoft Entra hybrid join to Microsoft Entra join. 	<ul style="list-style-type: none"> Requires Microsoft Configuration Manager. Not an actual Autopilot deployment so doesn't work on its own - only works alongside one a supported Autopilot scenario. Takes longer since device has to undergo both task sequence and Autopilot deployment. JSON file only supports user-driven Autopilot scenarios. Pre-provisioning and self-deploying Autopilot scenarios are only supported when the device is already an Autopilot device and there's an Autopilot profile assigned to the device.
Reset	<ul style="list-style-type: none"> Easily allows resetting an existing broken or repurposed device to a business ready state. 	<ul style="list-style-type: none"> Doesn't work if there's severe corruption in Windows installation. Doesn't support Microsoft Entra hybrid join devices.

Microsoft Entra join and Microsoft Entra hybrid join vs. Autopilot scenarios

Microsoft Entra join and Microsoft Entra hybrid join aren't Autopilot scenarios, but instead [device identity](#) options. All Autopilot scenarios support Microsoft Entra join, while only the **User-driven**, **Pre-provisioned**, and **Existing devices** scenarios support Microsoft Entra hybrid join. When deciding which Autopilot scenario to use, keep in mind the following factors:

- Device identities currently being used in the environment.
- Device identities being used going forward.
- Possible device identities being used in the future.

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. Microsoft Entra join provides the best user experience. However, current environment configurations and restrictions might require the continued use of on-premises Active Directory. In scenarios where on-premises Active Directory is still needed, Microsoft Entra hybrid join can be used. However, consider moving new devices to Microsoft Entra join while keeping existing devices on Microsoft Entra hybrid join. Microsoft Entra hybrid join can also be seen as a way to transition from on-premises Active Directory to purely Microsoft Entra ID.

Also keep in mind that for the Autopilot deployments that support Microsoft Entra hybrid join, Microsoft Entra hybrid join requires connectivity to a domain controller. If the device undergoing an Autopilot deployment is a remote device and isn't able to connect to a domain controller either on-premises or via a VPN connection, then only Microsoft Entra join is an option.

For more information on Microsoft Entra join versus Microsoft Entra hybrid join, see the following articles:

- [Microsoft Entra joined vs. Microsoft Entry hybrid joined in cloud-native endpoints](#).
- [What is a device identity?](#).
- [Learn more about cloud-native endpoints](#).
- [Tutorial: Set up and configure a cloud-native Windows endpoint with Microsoft Intune](#).
- [How to: Plan your Microsoft Entra join implementation](#).
- [A framework for Windows endpoint management transformation ↗](#).
- [Understanding hybrid Azure AD and co-management scenarios ↗](#).
- [Success with remote Windows Autopilot and hybrid Azure Active Directory join ↗](#).

Which Autopilot scenario to use

Which Autopilot scenario should be used depends on various factors including the environment and the needs of the organization. The first thing to account for is which type of device identity (Microsoft Entra ID or hybrid Microsoft Entra ID) is currently being used in the environment. Which device identity is being used may restrict which Autopilot scenarios can be used in the environment.

The following guide makes general suggestions on which Autopilot scenario to use:

User-driven

- Windows Autopilot user-driven supports both Microsoft Entra join and Microsoft Entra hybrid join.
- The device is intended to be used primarily by a single user.
- If the device needs to be shipped and delivered directly to the end-user without IT admin intervention.
- If the OEM or reseller is unable to perform the technician flow of the Windows Autopilot pre-provision scenario.
- If virtual machines (VMs) need to undergo the Windows Autopilot deployment process.

Pre-provisioned

- Windows Autopilot for pre-provisioned supports both Microsoft Entra join and Microsoft Entra hybrid join.
- The device is intended to be used primarily by a single user.
- The deployment time that the end-user experiences needs to be minimized.
- Is an IT admin, an OEM, or a reseller able to handle the technician flow and the first half of the deployment. If an IT admin handles the technician flow, then the device may need to be first shipped to the IT admin to perform the technician flow, followed by the device shipped or delivered to the end-user.
- In Microsoft Entra hybrid join scenarios, if the OEM or reseller is performing the technician flow, their environment must have connectivity to a domain controller for the organization.
- Windows Autopilot for pre-provisioned uses [TPM attestation](#) for authentication during the technician flow so only devices that have a supported TPM are supported. For this reason, virtual machines (VMs) aren't supported even when the VM has a virtual TPM.

Self-deploying mode

- Windows Autopilot self-deploying mode only supports Microsoft Entra join. It doesn't support Microsoft Entra hybrid join.
- The device is intended to be used as a kiosk device or by multiple users.
- If the device isn't going to be assigned to a user.
- The deployment needs to be automated as much as possible with no user interaction during the deployment process. For example, the end-user having to sign into Microsoft Entra ID during the deployment process.
- Windows Autopilot self-deploying mode uses [TPM attestation](#) for authentication during the technician flow so only devices that have a supported TPM are supported. For this reason, virtual machines (VMs) aren't supported even when the VM has a virtual TPM.

Existing devices

- Windows Autopilot for existing devices isn't a Windows Autopilot deployment itself, but a method to prepare an existing device for an Autopilot deployment. As part of the Windows Autopilot for existing devices deployment, a JSON file is added to the device. The JSON file defines which Autopilot deployment to run once the Windows Autopilot for existing devices deployment completes.
- The device doesn't need to be a current Autopilot device.
- On existing devices that are already part of the environment. For example, when repurposing a device and the Windows OS need to be reinstalled.
- On existing devices where the Windows OS needs to be reinstalled. For example, the previous Windows OS installation is corrupted and needs to be reinstalled, or if the hard drive of the device is replaced.
- For converting devices from Microsoft Entra hybrid join to Microsoft Entra join.
- When custom images of Windows installations are desired.
- When task sequences are desired to run complex application deployments.

Reset

- Windows Autopilot Reset isn't a Windows Autopilot deployment itself, but a method to reset an existing Autopilot device to a business ready state.
- The device needs to be registered as an Autopilot device.
- Windows Autopilot Reset only supports existing Microsoft Entra join devices. It doesn't support existing Microsoft Entra hybrid join devices.
- When the current Windows installation is in a stable non-corrupted state. If the Windows installation is in a corrupted state, use Windows Autopilot for existing

devices instead.

- When the device needs to be repurposed, for example to a new user.
 - When the device needs to be reset to resolve ongoing problems on the device.
- Sometimes it's better and quicker to reset a device than to troubleshoot and fix ongoing problems on the device.

Next steps: Scenario walkthroughs

The following list contains links to Autopilot scenario walkthroughs. The walkthroughs contain step by step instructions on how to configure each of the Autopilot scenarios:

1. Windows Autopilot user-driven mode:
 - a. [Microsoft Entra join](#).
 - b. [Microsoft Entra hybrid join](#).
2. Windows Autopilot for pre-provisioned deployment:
 - a. [Microsoft Entra join](#).
 - b. [Microsoft Entra hybrid join](#).
3. [Windows Autopilot self-deploying mode](#).
4. [Windows Autopilot for existing devices](#).
5. [Windows Autopilot Reset](#).

Related content

For more information on Autopilot scenarios, see the following articles:

- [Windows Autopilot scenarios and capabilities](#).
- [Windows Autopilot deployment process](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step by step tutorial for Windows Autopilot user-driven Microsoft Entra join in Intune

Article • 09/13/2024 • Applies to:  Windows 11,  Windows 10

This step by step tutorial guides through using Intune to perform a Windows Autopilot user-driven scenario when the devices are strictly Microsoft Entra joined.

The purpose of this tutorial is a step by step guide for all the configuration steps required for a successful Autopilot user-driven Microsoft Entra join deployment using Intune. The tutorial is also designed as a walkthrough in a lab or testing scenario, but can be expanded for use in a production environment.

Before beginning, refer to the [How to: Plan your Microsoft Entra join implementation](#) to make sure all requirements are met for joining devices to Microsoft Entra ID.

Windows Autopilot user-driven Microsoft Entra join overview

Windows Autopilot user-driven Microsoft Entra join is an Autopilot solution that automates the configuration of Windows on a new device. Normally, the device is delivered directly from an OEM or reseller to the end-user without the need for IT intervention. Windows Autopilot user-driven deployments use the existing Windows installation installed by the OEM at the factory. The end-user only needs to perform a minimal number of actions during the deployment process such as:

- Powering on the device.
- In certain scenarios, selecting the language, locale, and keyboard layout.
- Connecting to a wireless network if the device isn't connected to a wired network.
- Signing into Microsoft Entra ID with the end-user's Microsoft Entra credentials.

Windows Autopilot user-driven deployments can perform the following tasks during the deployment:

- Joins the device to Microsoft Entra ID.
- Enrolls the device in Intune.
- Installs applications.
- Applies device configuration policies such as BitLocker and Windows Hello for Business.

- Checks for compliance.
- Enrollment Status Page (ESP) can be used to prevent an end-user from using the device until it's fully configured.

Windows Autopilot user-driven deployments consist of two phases:

- Device ESP phase: Windows is configured and applications and policies assigned to the device are applied.
- User ESP phase: Applications and policies assigned to the user are applied.

Once the Windows Autopilot user-driven deployment is complete, the device is ready for the end-user to use and they're immediately sent to the desktop.

Workflow

The following steps are needed to configure and then perform a Windows Autopilot user-driven Microsoft Entra join in Intune:

- ✓ Step 1: Set up Windows automatic Intune enrollment
- ✓ Step 2: Allow users to join devices to Microsoft Entra ID
- ✓ Step 3: Register devices as Autopilot devices
- ✓ Step 4: Create a device group
- ✓ Step 5: Configure and assign Autopilot Enrollment Status Page (ESP)
- ✓ Step 6: Create and assign Autopilot profile
- ✓ Step 7: Assign Autopilot device to a user (optional)
- ✓ Step 8: Deploy the device

ⓘ Note

Although the workflow is designed for lab or testing scenarios, it can also be used in a production environment. Some of the steps in the workflow are interchangeable and interchanging some of the steps might make more sense in a production environment. For example, the **Create a device group** step followed by the **Register devices as Autopilot devices** step might make more sense in a production environment.

Walkthrough

Step 1: Set up Windows automatic Intune enrollment

Related content

For more information on Windows Autopilot user-driven Microsoft Entra join, see the following article:

- [User-driven mode for Microsoft Entra join.](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

User-driven Microsoft Entra join: Set up Windows automatic Intune enrollment

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra join steps:

Step 1: Set up Windows automatic Intune enrollment

- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Register devices as Autopilot devices](#)
- Step 4: [Create a device group](#)
- Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 6: [Create and assign Autopilot profile](#)
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
- Step 8: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra join workflow, see [Windows Autopilot user-driven Microsoft Entra join overview](#).

Note

If automatic Intune enrollment is already set up, skip this step and move on to [Step 2: Allow users to join devices to Microsoft Entra ID](#).

Set up Windows automatic Intune enrollment

In order for Windows Autopilot to work, devices need to be able to enroll in Intune automatically. Enrolling devices in Intune automatically can be configured in the Azure portal:

1. Sign in to the [Azure portal](#).
2. Select **Microsoft Entra ID**.
3. In the **Overview** screen, under **Manage** in the left hand pane, select **Mobility (MDM and WIP)**.
4. In the **Mobility (MDM and WIP)** screen, under **Name** select **Microsoft Intune**.
5. In the **Microsoft Intune** page that opens, under **MDM user scope**, select either **All** or **Some**:

- If **All** is selected, all users can automatically enroll their devices in Intune.
 - If **Some** is selected, only users in the groups specified in the link under **Groups** can automatically enroll their devices in Intune. To add groups:
 - a. Select the link under **Groups**.
 - b. In the **Select groups** window that opens, select the desired groups to add. Make sure that the groups selected are Microsoft Entra user groups that contain the desired users.
 - c. Once all of the desired groups are selected, select **Select** to close the **Select groups** window.
6. In the **Microsoft Intune** screen, if any changes were made, select **Save**.

Next step: Allow users to join devices to Microsoft Entra ID

Step 2: Allow users to join devices to Microsoft Entra ID

Related content

For more information on Windows automatic MDM/Intune enrollment, see the following articles:

- [Enable Windows automatic enrollment](#).
- [Set up Windows automatic enrollment](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

User-driven Microsoft Entra join: Allow users to join devices to Microsoft Entra ID

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- ✓ Step 2: **Allow users to join devices to Microsoft Entra ID**
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
 - Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 6: [Create and assign Autopilot profile](#)
 - Step 7: [Assign Autopilot device to a user \(optional\)](#)
 - Step 8: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra join workflow, see [Windows Autopilot user-driven Microsoft Entra join overview](#).

Note

If users are already allowed to join devices to Microsoft Entra ID, skip this step and move on to [Step 3: Register devices as Autopilot devices](#).

Allow users to join devices to Microsoft Entra ID

In order for Windows Autopilot to work, users need to be allowed to join devices to Microsoft Entra ID. Allowing users to join devices to Microsoft Entra ID can be configured in the Azure portal:

1. Sign in to the [Azure portal](#).
2. Select Microsoft Entra ID.
3. In the Overview screen, under Manage in the left hand pane, select Devices.

4. In the Devices | Overview screen, under **Manage** in the left hand pane, select **Device Settings**.
5. In the Devices | Device settings screen that opens, under **Users may join devices to Microsoft Entra**, select either **All** or **Selected**:
 - If **All** is selected, all users can join their devices to Microsoft Entra ID.
 - If **Some** is selected, only users specified under **Selected** can join their devices to Microsoft Entra ID. To add users:
 - a. Select the link under **Selected**.

- b. In the **Members allowed to join devices** page that opens:
 - i. Select **Add**.
 - ii. In the **Add members** window that opens:
 - i. Select the desired users and/or groups to add.
 - ii. Once all of the desired users and groups are selected, select **Select** to close the **Add members** window.
 - iii. Select **OK**.

 **Note**

Any selected groups must be a Microsoft Entra group that contains user objects.

6. In the Devices | Overview screen, if any changes were made, select **Save**.

 **Note**

This step of allowing users to join devices to Microsoft Entra ID is only needed for the Windows Autopilot scenarios involving Microsoft Entra join. This setting doesn't apply to Windows Autopilot scenarios involving Microsoft Entra hybrid join.

Next step: Register devices as Autopilot devices

Step 3: Register devices as Autopilot devices

Related content

For more information on allowing users to join devices to Microsoft Entra ID, see the following articles:

- [Configure device settings.](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

User-driven Microsoft Entra join: Register devices as Autopilot devices

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)

Step 3: Register devices as Autopilot devices

- Step 4: [Create a device group](#)
- Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 6: [Create and assign Autopilot profile](#)
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
- Step 8: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra join workflow, see [Windows Autopilot user-driven Microsoft Entra join overview](#).

Note

If devices are already registered as Autopilot devices, skip this step and move on to [Step 4: Create a device group](#).

Register devices as Autopilot devices

Before a device can use Autopilot, the device must be registered as an Autopilot device. Registering a device as an Autopilot device can be thought of as importing the device into Autopilot so that Autopilot service can be used on the device. Registering a device as an Autopilot device doesn't mean that the device has used the Autopilot service. It just makes the Autopilot service available to the device.

Also note that a device registered in Autopilot doesn't mean the device is enrolled in Intune. A device might be registered as an Autopilot device but might not exist in Intune. It's not until an Autopilot registered device goes through the Autopilot process for the first time that it becomes enrolled in Intune. After the Autopilot device undergoes the Autopilot process and enrolls in Intune, the Autopilot device appears as a device in both Microsoft Entra ID and Intune.

There are several methods to register a device as an Autopilot device in Intune:

- Manually registering devices into Intune as an Autopilot device via the hardware hash. The hardware hash of a device can be collected via one of the following methods:
 - [Configuration Manager](#).
 - [PowerShell script](#).
 - [Diagnostics page hash export](#).
 - [Desktop hash export](#).

These methods of obtaining the hardware hash of a device are well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

- Automatically registering device via:
 - An [OEM](#), including [Microsoft Surface](#) devices.
 - A [partner](#).

Registering a device via an OEM or partner is also well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

For most organizations, using an OEM or partner to register devices as Autopilot devices is the preferred, most common, and most secure method. However for smaller organizations, for testing/lab scenarios, and for emergency scenarios, manually registering devices as Autopilot devices via the hardware hash is also used.

ⓘ Important

The following type of devices shouldn't be registered as a Windows Autopilot device:

- [Microsoft Entra registered](#) devices, also known as "workplace joined" devices.
- [Intune MDM-only enrollment](#) devices.

These options are intended for users to join personally owned devices to their organization's network. Windows Autopilot registered devices are registered as corporate owned devices.

If a device is already one of these two types of devices, to register it as a Windows Autopilot device, first remove it from Microsoft Intune and Microsoft Entra ID. For more information, see [Device appears as Microsoft Entra registered instead of Microsoft Entra joined](#) and [Deregister a device](#).

Note

Assuming that a device isn't currently enrolled Intune, remember that registering a device in Autopilot doesn't make it an Intune enrolled device. That device doesn't enroll into Intune until Autopilot runs on the device for the first time.

Importing the hardware hash CSV file for devices into Intune

Several of the methods in the previous section on obtaining the hardware hash when manually registering devices as Autopilot devices produces a CSV file that contains the hardware hash of the device. This CSV file with the hardware hash needs to be imported into Intune to register the device as an Autopilot device.

After the CSV file is created, it can be imported into Intune via the following steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, select **Import**.
 - a. In the **Add Autopilot devices** window that opens:
 - i. Under **Specify the path to the list you want to import.**, select the blue file folder.
 - ii. Browse to the CSV file obtained using one of the above methods to obtain the hardware hash of a device.
 - iii. After selecting the CSV file, verify that the correct CSV file is selected under **Specify the path to the list you want to import.**, and then select **Import**. Selecting **Import** closes the **Add Autopilot devices** window. Importing can take several minutes.
 - b. After the import is complete, select **Sync**.

A message displays saying that the sync is in progress. The sync process might take a few minutes to complete, depending on how many devices are being synchronized.

 **Note**

If another sync is attempted within 10 minutes after initiating a sync, an error will be displayed. Syncs can only occur once every 10 minutes. To attempt a sync again, wait at least 10 minutes before trying again.

- c. Select **Refresh** to refresh the view. The newly imported devices should display within a few minutes. If the devices aren't yet displayed, wait a few minutes, and then select **Refresh** again.

Next step: Create a device group

Step 4: Create a device group

Related content

For more information on registering devices as Autopilot devices, see the following articles:

- [Manually register devices with Windows Autopilot](#).
- [Windows Autopilot customer consent](#).

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

User-driven Microsoft Entra join: Create a device group

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Register devices as Autopilot devices](#)

Step 4: Create a device group

- Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 6: [Create and assign Autopilot profile](#)
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
- Step 8: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra join workflow, see [Windows Autopilot user-driven Microsoft Entra join overview](#).

Note

If device groups are already created, skip this step and move on to [Step 5: Configure and assign Autopilot Enrollment Status Page \(ESP\)](#). However, if deploying multiple different Autopilot scenarios to different devices, separate device groups are required for each Autopilot scenario.

Create a device group

Device groups are a collection of devices organized into a Microsoft Entra group. Device groups are used in Autopilot to target devices for specific configurations such as what policies to apply to a device and what applications to install on the device. They're also used by Autopilot to target Enrollment Status Page (ESP) configurations, Autopilot profile configurations, and domain join profiles to devices.

Device groups can be either dynamic or assigned:

- **Dynamic groups** - Devices are automatically added to the group based on rules
- **Assigned groups** - Devices are manually added to the group and are static

When an admin configures Autopilot in an enterprise environment, dynamic groups are primarily used since a large number of devices are normally involved. Adding the devices in automatically using rules makes management of the group a lot easier. Adding a large amount of device in manually via an assigned group would be impractical. However, if there's only a few devices, for example for testing purposes, an assigned group can be used instead.

To create a dynamic device group for use with Autopilot, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Groups** in the left hand pane.
3. In the **Groups | All groups** screen, make sure **All groups** is selected, and then select **New group**.
4. In the **New Group** screen that opens:
 - a. For **Group type**, select **Security**.
 - b. For **Group name**, enter a name for the device group.
 - c. For **Group description**, enter a description for the device group.
 - d. For **Microsoft Entra roles can be assigned to the group**, select **No**.
 - e. For **Membership type**, select **Dynamic Device**. Setting the **Membership type** option to **Dynamic Device** changes the option **Members** to **Dynamic device members**.
 - f. For **Owners**, select the **No owners selected** link.
 - g. In the **Add owners** screen that opens:
 - i. Scroll through the list of objects and select owners for the user group. Alternatively, use the **Search** bar to search for and select owners of the group.
 - ii. Once all of the desired owners are selected, select **Select**.
 - h. For **Dynamic device members**, select **Add dynamic query**. The **Dynamic membership rules** screen opens.
 - i. In the **Dynamic membership rules** screen:
 - i. Make sure that **Configure Rules** is selected at the top.

ii. Select **Add expression**. Rules and expressions can be added that defines what devices are added to the device group.

Rules can be entered in the rule builder via the drop-down boxes.

Alternatively, the rule syntax can be entered directly via the **Edit** option in the **Rule syntax** section.

The most common type of dynamic device group when using Windows Autopilot is a device group that contains all Windows Autopilot devices. A dynamic device group that contains all Windows Autopilot devices has the following syntax:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```

To enter in this rule:

i. Select the **Edit** option in the **Rule syntax** section.

ii. Paste in the following rule in the **Edit rule syntax** screen under **Rule syntax**:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```

iii. Once the rule is pasted in, select **OK**.

iii. Once the desired rule is entered, select **Save** on the toolbar to close the **Dynamic membership rules** window.

For more information on creating rules for dynamic groups, see [Dynamic membership rules for groups in Microsoft Entra ID](#).

j. Select **Create** to finish creating the dynamic device group.

Note

The above steps are creating a dynamic group in Microsoft Entra that is used by Intune and Windows Autopilot solutions. Although the groups can be accessed in the Intune portal, they're Microsoft Entra groups.

Tip

For Configuration Manager admins, device groups are similar to device based collections. Dynamic device groups are similar to query based device collections while assigned device groups are similar to direct membership device collections.

Next step: Configure and assign the Enrollment Status Page (ESP)

Step 5: Configure and assign Autopilot Enrollment Status Page (ESP)

Related content

For more information on creating groups in Intune, see the following articles:

- [Create device groups.](#)
- [Add groups to organize users and devices.](#)
- [Manage Microsoft Entra groups and group membership.](#)
- [Dynamic membership rules for groups in Microsoft Entra ID.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

User-driven Microsoft Entra join: Configure and assign the Enrollment Status Page (ESP)

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Register devices as Autopilot devices](#)
- Step 4: [Create a device group](#)

Step 5: Configure and assign Autopilot Enrollment Status Page (ESP)

- Step 6: [Create and assign Autopilot profile](#)
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
- Step 8: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra join workflow, see [Windows Autopilot user-driven Microsoft Entra join overview](#).

Note

If an ESP is already configured, assigned, and uses the same settings for the user-driven Microsoft Entra join scenario, skip this step and move on to [Step 6: Create and assign Autopilot profile](#).

The Enrollment Status Page (ESP)

The main feature of the Enrollment Status Page (ESP) is to display progress and current status to the end user while the device is being set up and enrolled via the Autopilot process. The other main feature of the ESP is to block a user from signing in and using the device until all required policies and applications are installed. Multiple ESP profiles can be created with different settings and assigned appropriately based on different needs and scenarios.

Out of box there's a default ESP that is assigned to all devices. The default setting in the default ESP is to not show app and profile progress during the Autopilot process. However, Microsoft recommends changing this default via a separate custom ESP to

show app and profile progress. Enabling and configuring an ESP allows end users to properly see the progress of their device being set up and prevents them using the device until the device is fully configured and provisioned. A user signing into the device before being fully configured and provisioned can cause issues.

The ESP has two phases:

- **Device ESP** - The portion of the ESP that runs during the OOBE process and applies device policies and installs device applications.
- **User ESP** - The portion of the ESP that sets up user account, applies user policies, and installs user applications.

Device ESP runs first followed by the User ESP.

Tip

For Configuration Manager admins, an ESP is similar and analogous to Configuration Manager client settings.

Autopilot Enrollment Status Page (ESP) configuration options

When the Enrollment Status Page (ESP) is configured, it has several options that can be configured to meet the needs of the organization. The following lists the different options and their possible configurations:

- **Show an error when installation takes longer than specified number of minutes:**
 - The default time-out is 60 minutes. Enter a higher value if more time is needed to install applications on the devices.
- **Show custom message when time limit or error occur:**
 - **No:** The default message is shown to users when an error occurs. That message is: **Setup could not be completed. Please try again or contact your support person for help.**
 - **Yes:** A custom message is shown to users when an error occurs. Enter a custom message in the provided text box.
- **Turn on log collection and diagnostics page for end users:**
 - **No:** The collect logs button isn't shown to users when an installation error occurs. The Windows Autopilot diagnostics page isn't shown on devices running

Windows 11.

- **Yes:** The collect logs button is shown to users when an installation error occurs. The Windows Autopilot diagnostics page is shown on devices running Windows 11. Logs and diagnostics might aid with troubleshooting. For this reason, Microsoft recommends enabling this option.
- **Only show page to devices provisioned by out-of-box experience (OOBE):**
 - **No:** The enrollment status page (ESP) is shown during the device phase and the out-of-box experience (OOBE). The page is also shown during the user phase to every user who signs into the device for the first time.
 - **Yes:** The enrollment status page (ESP) is shown during the device phase and the OOBE. The page is also shown during the user phase, but only to the first user who signs into the device. It isn't shown to subsequent users who sign into the device.
- **Block device use until all apps and profiles are installed:**
 - **No:** Users can leave the ESP before Intune is finished setting up the device.
 - **Yes:** Users can't leave the ESP until Intune is done setting up the device.
Enabling this option unlocks the following additional options:
 - **Allow users to reset device if installation error occurs:**
 - **No:** The ESP doesn't give users the option to reset their devices when an installation fails.
 - **Yes:** The ESP gives users the option to reset their devices when an installation fails.
 - **Allow users to use device if installation error occurs:**
 - **No:** The ESP doesn't give users the option to bypass the ESP when an installation fails.
 - **Yes:** The ESP gives users the option to bypass the ESP and use their devices when an installation fails.
 - **Block device use until these required apps are installed if they are assigned to the user/device:**
 - **All:** All assigned apps must be installed before users can use their devices.

- **Selected:** Selected apps must be installed before users can use their devices. After enabling this option, select **Select apps** to select the managed apps from Intune that are required to be installed before users can use their device.

Configure and assign the Enrollment Status Page (ESP)

To configure and assign the Autopilot Enrollment Status Page (ESP), follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
 1. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
 2. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Enrollment Status Page**.
 3. In the **Enrollment Status Page** screen that opens, select **Create**.
 4. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the ESP profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.
 5. In the **Settings** page, toggle the option **Show app and profile configuration progress** to **Yes**.
 - a. After the option **Show app and profile configuration progress** is toggled to **Yes**, several new options will appear. Configure these options based on the desired behavior for the ESP as described in the section [Autopilot Enrollment Status Page \(ESP\) configuration options](#):
 - b. Once the different ESP options under the **Settings** page are configured as desired, select **Next**.
 6. In the **Assignments** page:

- a. Under **Included groups**, select **Add groups**.
- b. In the **Select groups to include** window that opens, select the device groups to target the ESP profile. The device groups selected would normally be the device groups created in the **Create device group** step.
- c. After selecting the device group, select **Select** to close the **Select groups to include** window.

 **Tip**

After selecting the device groups, the **Edit filter** option can be selected on each device group added to the assignment to further refine what devices are targeted for the ESP profile. For example, further filtering can be useful if some of the devices that are members in the device groups selected need to be excluded.

- d. Select **Next**.

 **Note**

An ESP is assigned to a device group and not directly to individual devices. To assign an ESP to a specific device, the device must be a member of a device group that has an ESP assigned to it.

7. In the **Scope tags** page, select **Next**.

 **Note**

Scope tags are optional and are a method to control who has access to the ESP configuration. For this tutorial, scope tags are being skipped and left at the default scope tag. However if a custom scope tag needs to be specified, do so at this screen. For more information about scope tags, see [Use role-based access control and scope tags for distributed IT](#).

8. In the **Review + create** page, verify that the settings are correct and configured as desired. Once verified, select **Create** to save the changes and assign the ESP profile.

Next step: Create and assign user-driven Microsoft Entra join Autopilot profile

Step 6: Create and assign Autopilot profile

Related content

For more information on the Enrollment Status Page (ESP), see the following articles:

- [Windows Autopilot Enrollment Status Page](#).
- [Set up the Enrollment Status Page](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

User-driven Microsoft Entra join: Create and assign user-driven Microsoft Entra join Autopilot profile

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
 - Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
-  **Step 6: Create and assign Autopilot profile**
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
 - Step 8: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra join workflow, see [Windows Autopilot user-driven Microsoft Entra join overview](#).

Create and assign user-driven Microsoft Entra join Autopilot profile

The Autopilot profile specifies how the device is configured during Windows Setup and what is shown during the out-of-box experience (OOBE).

When an admin creates an Autopilot profile for the user-driven scenario, devices with this Autopilot profile are associated with the user enrolling the device. User credentials are required to enroll the device.

The difference between an Autopilot user-driven Microsoft Entra join and an Autopilot Microsoft Entra hybrid join is that the user-driven Microsoft Entra join scenario only joins Microsoft Entra ID during Autopilot. The Microsoft Entra hybrid join scenario joins both an on-premises domain and Microsoft Entra ID during Autopilot.

Tip

For Configuration Manager admins, the Autopilot profile is similar to some of the configuration that takes place during a task sequence via an `unattend.xml` file. The

`unattend.xml` file is configured during the **Apply Windows Settings** and **Apply Network Settings** steps. Note however that Autopilot doesn't use `unattend.xml` files.

To create a user-driven Microsoft Entra join Autopilot profile, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Deployment Profiles**.
6. In the **Windows Autopilot deployment profiles** screen, select the **Create Profile** drop down menu and then select **Windows PC**.
7. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the Autopilot profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.

Note

Microsoft recommends setting the option **Convert all targeted devices to Autopilot** to **Yes**. This tutorial concentrates on new devices where the device is manually imported as an Autopilot device using the hardware hash. However, this option can be helpful when assigning Autopilot profiles to device groups that contain existing devices. For example, this option is helpful when using the [Windows Autopilot for existing devices](#) scenario. With Windows Autopilot for existing devices, existing devices might need to be registered as an Autopilot device after the Autopilot deployment completes. For more information, see [Register device for Windows Autopilot](#).

8. In the **Out-of-box experience (OOBE)** page:

- For **Deployment mode**, select **User-driven**.
- For **Join to Microsoft Entra ID as**, select **Microsoft Entra joined**.
- For **Microsoft Software License Terms**, select **Hide** to skip the EULA page.
- For **Privacy settings**, select **Hide** to skip the privacy settings.
- For **Hide change account options**, select **Hide**.
- For **User account type**, select the desired account type for the user. The options are either **Administrator** or **Standard** user. If **Administrator** is chosen, the user is added to the local Administrator group for the device.
- For **Allow pre-provisioned deployment**, select **No**.

 **Note**

For the Windows Autopilot for pre-provisioned deployment Microsoft Entra join scenario, see [Step by step tutorial for Windows Autopilot for pre-provisioned deployment Microsoft Entra join in Intune](#)

- For **Language (Region)**, select **Operating system default** to use the default language for the operating system being configured. If another language is desired, select the desired language from the drop-down list.
- For **Automatically configure keyboard**, select **Yes** to skip the keyboard selection page.
- For **Apply device name template**, select **No**. Alternatively, **Yes** can be chosen to apply a device name template. Be aware of the following if the name template is selected to **Yes**:
 - Names must be 15 characters or less, and can have letters, numbers, and hyphens.
 - Names can't be all numbers.
 - Use the **%SERIAL%** macro to add a hardware-specific serial number.
 - Use the **%RAND:x%** macro to add a random string of numbers, where x equals the number of digits to add.

 **Note**

The above settings are selected to minimize needed user interaction during device setup. However, some of the settings that are hidden can instead be

shown as desired. For example, some regions might require that **Privacy settings** always be shown.

 **Note**

If the language/region and keyboard screens are set to hidden, they might still be displayed if there's no network connectivity at the start of the Autopilot deployment. The settings to hide these screens are defined in the Autopilot profile. However, if there's no network connectivity, the Autopilot profile with the settings hasn't downloaded yet which results in the screens being displayed. Once network connectivity is established, the Autopilot profile is downloaded and any additional screen settings should work as expected.

9. Once the options in the **Out-of-box experience (OOBE)** page are configured as desired, select **Next**.

10. In the **Assignments** page:

- Under **Included groups**, select **Add groups**.

 **Note**

Make sure to add the correct device groups under **Included groups** and not under **Excluded groups**. Accidentally adding the desired device groups under **Excluded groups** prevents devices in those device groups from receiving the Autopilot profile.

- In the **Select groups to include** window that opens, select the groups that the Windows Autopilot profile should be assigned to. These device groups are normally the device groups created in the previous **Create device group** step. Once done, select **Select**.

- Under **Included groups > Groups**, ensure the correct groups are selected, and then select **Next**.

11. In the **Review + Create** page, verify that all settings are set correctly, and then select **Create** to create the Autopilot profile.

Verify device has an Autopilot profile assigned to it

Before deploying a device, ensure that an Autopilot profile is assigned to a device group that the device is a member of. Autopilot profile assignment to a device can take some time after the Autopilot profile is assigned to the device group or after the device is added to the device group. To verify that the profile is assigned to a device, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens:
 - a. Find the desired device that Autopilot deployment profile assignment status needs to be checked.
 - b. Once the device is located, its current status is listed under the **Profile status** column. The status has one of the following values:
 - **Not assigned:** An Autopilot deployment profile isn't assigned to the device.
 - **Assigning:** An Autopilot deployment profile is being assigned to the device.
 - **Assigned:** An Autopilot deployment profile is assigned to the device.
 - **Fix pending:** When a hardware change occurs on a device, this status displays while Intune tries to register the new hardware. When the link for the **Fix pending** status is selected, the following message appears:

We've detected a hardware change on this device. We're trying to automatically register the new hardware. You don't need to do anything now; the status will be updated at the next check in with the result.

- If Intune is able to successfully register the new hardware, Intune updates the profile status when the device next checks into Intune. For more information on the **Fix pending** status, see the following articles:
- [Autopilot profile not applied after reimaging to an older OS version](#).
 - [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
 - [Windows Autopilot motherboard replacement scenario guidance](#)
- **Attention required:** If Intune is unable to register the new hardware after a hardware change occurs on a device, the device can't receive the Autopilot profile until the device is reset and the device re-registers. For more information on this status and how to deregister/re-register a device, see the following articles:
 - [Autopilot profile not applied after reimaging to an older OS version](#).
 - [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
 - [Windows Autopilot motherboard replacement scenario guidance](#)
 - [Deregister a device](#)

Before starting the Autopilot deployment process on a device, make sure that in the **Windows Autopilot devices** page:

- The device's **Profile status** status is **Assigned**.
- In the properties of the device, **Date assigned** has a value.
- In the properties of the device, **Assigned profile** displays the expected Autopilot profile.

Note

Intune periodically checks for new devices in the assigned device groups, and then begins the process of assigning profiles to those devices. Due to several different factors involved in the process of Autopilot profile assignment, an estimated time for the assignment can vary from scenario to scenario. These factors can include Microsoft Entra groups, membership rules, hash of a device, Intune and Autopilot services, and internet connection. The assignment time varies depending on all the factors and variables involved in a specific scenario.

Next step: Assign Autopilot device to a user (optional)

Step 7: Assign Autopilot device to a user (optional)

If a user isn't being assigned to the device, then skip to [Step 8: Deploy the device](#).

Step 8: Deploy the device

Related content

For more information on configuring Autopilot profiles, see the following articles:

- [Configure Autopilot profiles](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

User-driven Microsoft Entra join: Assign Autopilot device to a user (optional)

Article • 06/19/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
 - Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 6: [Create and assign Autopilot profile](#)
- Step 7: Assign Autopilot device to a user (optional)**
- Step 8: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra join workflow, see [Windows Autopilot user-driven Microsoft Entra join overview](#).

Assign Autopilot device to a user (optional)

A device that is registered as an Autopilot device can also be assigned to a user. If an Autopilot device is assigned to a user, then any user policies and application installs assigned to that user is applied to the device during the Autopilot process.

Tip

For testing purposes, especially for hybrid Microsoft Entra scenarios, it might be better to first test an Autopilot deployment before assigning the device to a user. Not assigning a user limits the scope of applications, policies, and configurations processed during the Autopilot process.

Tip

For Configuration Manager admins, assigning a user to a device is similar to user device affinity in Configuration Manager.

To assign an Autopilot device to a user, follow these steps:

1. Sign in to the Microsoft Intune admin center [↗](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, locate the device to assign a user to.
7. Once the desired device is located, select the box to the left of the device, making sure that there's check mark in the box, and then select **Assign user** in the toolbar at the top of page.
8. In the **Select user** window that opens, find and select a user for the device, and then select **Select** to close the window. If necessary, use the **Search** box to find the desired user.

 **Note**

The selected user must be an Azure user licensed to use Intune.

9. In the Autopilot device's property window that automatically opens on the right hand side, under **User friendly name**, verify the default value. If the value is empty or a different friendly name is desired, enter the desired friendly name for the user under **User friendly name**, and then select **Save** to close the property window.
10. The user assignment can be verified by selecting the Autopilot device in the **Windows Autopilot devices** screen. Once the Autopilot device is selected, it highlights and the Autopilot device's property window automatically opens on the right hand side. The assigned user is listed under **User** and **User friendly name**.

Assigning Autopilot device to a user via hardware hash CSV file

A user can be manually assigned to a Windows Autopilot device in the Windows Autopilot device's properties. However, a user can also be assigned to the Autopilot device when the device was initially imported into Autopilot as an Autopilot device. Assigning a user when the device is imported as an Autopilot device can be done by

editing the hardware hash CSV file and adding the **Assigned User** column after the **Hardware Hash** column. The user's User Principal Name (UPN) should then be added as a value under the **Assigned User** column.

 **Important**

Use a plain-text editor such as **Notepad** to edit the CSV file. Don't use Microsoft Excel. Editing the CSV file in Excel doesn't generate a proper usable file for importing into Intune.

For more information on editing the CSV file to add an assigned user to the Autopilot device, see [Manually register devices with Windows Autopilot: Ensure that the CSV file meets requirements](#).

Next step: Deploy the device

Step 8: Deploy the device

Related content

For more information on assigning a user to an Autopilot device, see the following article:

- [Assign a user to a specific Autopilot device](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

User-driven Microsoft Entra join: Deploy the device

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Register devices as Autopilot devices](#)
- Step 4: [Create a device group](#)
- Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 6: [Create and assign Autopilot profile](#)
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
- ✓ Step 8: **Deploy the device**

For an overview of the Windows Autopilot user-driven Microsoft Entra join workflow, see [Windows Autopilot user-driven Microsoft Entra join overview](#).

Deploy the device

<https://www.microsoft.com/en-us/videoplayer/embed/RW15DG8?postJsIIMsg=true> ↗

Once all of the configurations for the Windows Autopilot user-driven Microsoft Entra join deployment are completed in Intune and in Microsoft Entra ID, the next step is to start the Autopilot deployment process on the device. If desired, deploy any additional applications and policies that should run during the Autopilot deployment to a device group that the device is a member of.

To start the Windows Autopilot deployment process on the device, acquire a device that is part of the device group created in the previous [Create a device group](#) step. Once the device is acquired, follow these steps:

1. If a wired network connection is available, connect the device to the wired network connection.
2. Power on the device.
3. Once the device boots up, one of two things occurs depending on the state of network connectivity:

- If the device is connected to a wired network and has network connectivity, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
- If the device isn't connected to a wired network or if it doesn't have network connectivity, it prompts to connect to a network. Connectivity to the Internet is required:
 - a. The out-of-box experience (OOBE) begins and a screen asking for a country or region appears. Select the appropriate country or region, and then select **Yes**.
 - b. The keyboard screen appears to select a keyboard layout. Select the appropriate keyboard layout, and then select **Yes**.
 - c. An additional keyboard layouts screen appears. If needed, select additional keyboard layouts via **Add layout**, or select **Skip** if no additional keyboard layouts are needed.

 **Note**

When there's no network connectivity, the device can't download the Autopilot profile to know what country/region and keyboard settings to use. For this reason, when there's no network connectivity, the country/region and keyboard screens appear even if these screens are set to hidden in the Autopilot profile. These settings need to be specified in these screens in order for the network connectivity screens that follow to work properly.

- d. The **Let's connect you to a network** screen appears. At this screen, either plug the device into a wired network (if available), or select and connect to a wireless Wi-Fi network.
 - e. Once network connectivity is established, the **Next** button should become available. Select **Next**.
 - f. At this point, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
4. Once the Windows Autopilot process begins, the Microsoft Entra sign-in page appears. At the Microsoft Entra sign-in page, if a user was assigned to the device,

their username might be pre-populated in this screen. Enter the Microsoft Entra credentials for the user and then select **Next** (Windows 10) or **Sign in** (Windows 11) to sign in. If necessary, proceed through the multi-factor authentication (MFA) screens.

5. After authenticating with Microsoft Entra ID, the Enrollment Status Page (ESP) appears. The Enrollment Status Page (ESP) displays progress during the provisioning process across three phases:

- **Device preparation** (Device ESP)
- **Device setup** (Device ESP)
- **Account setup** (User ESP)

The first two phases of **Device preparation** and **Device setup** are part of the Device ESP while the final phase of **Account setup** is part of the User ESP.

6. Once **Account setup** and the user ESP process completes, the provisioning process completes, the ESP finishes, and the desktop appears. At this point, the end-user can start using the device.

Deployment tips

- Before the Windows Autopilot deployment is started, Microsoft recommends having:
 - At least one type of policy and at least one application assigned to the devices.
 - At least one type of policy and at least one application assigned to the users.

These assignments ensure proper testing of the Windows Autopilot deployment during both the device ESP phase and user ESP phase of the ESP. It might also prevent possible issues when there are either no policies or no applications assigned to the devices or the users.

- Depending on how the Autopilot profile was configured at the **Create and assign Autopilot profile** step, additional screens might appear during the Autopilot deployment appear such as:
 - **Language/Country/Region** or **Keyboard** screens before the Microsoft Entra sign-in page.
 - **Privacy** screen when the user ESP/Account setup begins but before the user is automatically signed in.

- To view and hide detailed progress information in the ESP during the provisioning process:
 - **Windows 10:** To show details, next to the appropriate phase select **Show details**. To hide the details, next to the appropriate phase select **Hide details**.
 - **Windows 11:** To show details, next to the appropriate phase select V. To hide the details, next to the appropriate phase select A.
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Step by step tutorial for Windows Autopilot user-driven Microsoft Entra hybrid join in Intune

Article • 09/13/2024 • Applies to:  Windows 11,  Windows 10

Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. For more information, see [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization](#).

This step by step tutorial guides through using Intune to perform a Windows Autopilot user-driven scenario when the devices are also joined to an on-premises domain, also known as Microsoft Entra hybrid join.

The purpose of this tutorial is a step by step guide for all the configuration steps required for a successful Autopilot user-driven Microsoft Entra hybrid join deployment using Intune. The tutorial is also designed as a walkthrough in a lab or testing scenario, but can be expanded for use in a production environment.

Before beginning, refer to the [Plan your Microsoft Entra hybrid join implementation](#) to make sure all requirements are met for joining on-premises AD devices to Microsoft Entra ID.

Windows Autopilot user-driven Microsoft Entra hybrid join overview

Windows Autopilot user-driven Microsoft Entra hybrid join is an Autopilot solution that automates the configuration of Windows on a new device. The device is normally delivered directly from an OEM or reseller to the end-user without the need for IT intervention. Windows Autopilot user-driven deployments use the existing Windows installation installed by the OEM at the factory. The end-user only needs to perform a minimal number of actions during the deployment process such as:

- Powering on the device.
- In certain scenarios, selecting the language, locale, and keyboard layout.

- Connecting to a wireless network if the device isn't connected to a wired network.
- Signing into the device with the end-user's on-premises domain credentials.
- In certain scenarios, signing into Microsoft Entra ID with the end-user's Microsoft Entra credentials.

Windows Autopilot user-driven deployments can perform the following tasks during the deployment:

- Joins the device to an on-premises domain.
- Registers the device with Microsoft Entra ID.
- Enrolls the device in Intune.
- Installs applications.
- Applies device configuration policies such as BitLocker and Windows Hello for Business.
- Checks for compliance.
- The Enrollment Status Page (ESP) prevents an end-user from using the device until the device is fully configured.

Windows Autopilot user-driven deployments consist of two phases:

- Device ESP phase: Windows is configured and applications and policies assigned to the device are applied.
- User ESP phase: End-user signs into the device for the first time using on-premises domain credentials and applications and policies assigned to the user are applied.

Once the Windows Autopilot user-driven deployment is complete, it prompts the end-user to sign out of the device. Once the end-user is signed out of the device, it's ready for use. The end-user can then sign in with their on-premises domain credentials and begin to use the device.

Workflow

The following steps are needed to configure and then perform a Windows Autopilot user-driven Microsoft Entra hybrid join in Intune:

- ✓ Step 1: Set up Windows automatic Intune enrollment
- ✓ Step 2: Install the Intune Connector
- ✓ Step 3: Increase the computer account limit in the Organizational Unit (OU)
- ✓ Step 4: Register devices as Autopilot devices
- ✓ Step 5: Create a device group
- ✓ Step 6: Configure and assign Autopilot Enrollment Status Page (ESP)
- ✓ Step 7: Create and assign Microsoft Entra hybrid join Autopilot profile

- ✓ Step 8: Configure and assign domain join profile
- ✓ Step 9: Assign Autopilot device to a user (optional)
- ✓ Step 10: Deploy the device

Note

Although the workflow is designed for lab or testing scenarios, it can also be used in a production environment. Some of the steps in the workflow are interchangeable and interchanging some of the steps might make more sense in a production environment. For example, the **Create a device group** step followed by the **Register devices as Autopilot devices** step might make more sense in a production environment.

Walkthrough

Step 1: Set up Windows automatic Intune enrollment

Related content

For more information on Windows Autopilot user-driven Microsoft Entra hybrid join, see the following article:

- [Deploy Microsoft Entra hybrid joined devices by using Intune and Windows Autopilot.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

User-driven Microsoft Entra hybrid join: Set up Windows automatic Intune enrollment

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra hybrid join steps:

Step 1: Set up Windows automatic Intune enrollment

- Step 2: [Install the Intune Connector](#)
- Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
- Step 4: [Register devices as Autopilot devices](#)
- Step 5: [Create a device group](#)
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
- Step 8: [Configure and assign domain join profile](#)
- Step 9: [Assign Autopilot device to a user \(optional\)](#)
- Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

Note

If automatic Intune enrollment is already set up, skip this step and move on to [Step 2: Install the Intune Connector](#).

Set up Windows automatic Intune enrollment

In order for Windows Autopilot to work, devices need to be able to enroll in Intune automatically. Enrolling devices in Intune automatically can be configured in the Azure portal:

1. Sign in to the [Azure portal](#).
2. Select **Microsoft Entra ID**.
3. In the **Overview** screen, under **Manage** in the left hand pane, select **Mobility (MDM and WIP)**.

4. In the **Mobility (MDM and WIP)** screen, under **Name** select **Microsoft Intune**.
5. In the **Microsoft Intune** page that opens, under **MDM user scope**, select either **All** or **Some**:
 - If **All** is selected, all users can automatically enroll their devices in Intune.
 - If **Some** is selected, only users in the groups specified in the link under **Groups** can automatically enroll their devices in Intune. To add groups:
 - a. Select the link under **Groups**.
 - b. In the **Select groups** window that opens, select the desired groups to add. Make sure that the groups selected are Microsoft Entra user groups that contain the desired users.
 - c. Once all of the desired groups are selected, select **Select** to close the **Select groups** window.
6. In the **Microsoft Intune** screen, if any changes were made, select **Save**.

Next step: Install the Intune Connector

Step 2: Install the Intune Connector

Related content

For more information on Windows automatic MDM/Intune enrollment, see the following articles:

- [Enable Windows automatic enrollment](#).
- [Set up Windows automatic enrollment](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

User-driven Microsoft Entra hybrid join: Install the Intune Connector

Article • 02/27/2025 •

Applies Windows 11, Windows 10, Windows Server 2025, Windows Server 2022, to: Windows Server 2019, Windows Server 2016

Windows Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- ✓ **Step 2: Install the Intune Connector**
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Windows Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Windows Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Windows Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Windows Autopilot device to a user \(optional\)](#)
 - Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

ⓘ Note

If the Intune Connector is already installed and configured, skip this step and move on to [Step 3: Increase the computer account limit in the Organizational Unit \(OU\)](#).

Install the Intune Connector for Active Directory

The purpose of the Intune Connector for Active Directory, also known as the Offline Domain Join (ODJ) Connector, is to join computers to an on-premises domain during the Windows Autopilot process. The Intune Connector for Active Directory creates computer objects in a specified Organizational Unit (OU) in Active Directory during the domain join process.

Important

Starting with Intune 2501, Intune uses an updated Intune Connector for Active Directory that strengthens security and follows least privilege principles by using a [Managed Service Account \(MSA\)](#). When the Intune Connector for Active Directory is downloaded from within Intune, the updated Intune Connector for Active Directory is downloaded. The previous legacy Intune Connector for Active Directory is still available for download at [Intune Connector for Active Directory](#), but Microsoft recommends using the updated Intune Connector for Active Directory installer going forward. The previous legacy Intune Connector for Active Directory will continue to work through sometime in May 2025. However, it needs to be updated to the updated Intune Connector for Active Directory before then to avoid loss of functionality. For more information, see [Intune Connector for Active Directory with low-privileged account for Autopilot Hybrid Microsoft Entra join deployments](#).

Updating of the Intune Connector for Active Directory to the updated version isn't done automatically. The legacy Intune Connector for Active Directory needs to be manually uninstalled followed by the updated connector manually downloaded and installed. Instructions for the manual uninstall and install process of the Intune Connector for Active Directory are provided in the following sections.

Select the tab that corresponds to the version of the Intune Connector for Active Directory that is being installed:



Updated Connector

Before beginning the installation, make sure that all of the [Intune connector server requirements](#) are met.

Tip

It's preferable, but not required, that the administrator installing and configuring the Intune Connector for Active Directory has appropriate domain rights as documented in [Intune Connector for Active Directory requirements](#). This requirement allows the Intune Connector for Active Directory installer and configuration process to properly set permissions for the MSA on the Computer container or OUs where computer objects are created. If the administrator doesn't have these permissions, an administrator that does have

the appropriate permissions needs to follow the section [Increase the computer account limit in the Organizational Unit](#).

Turn off Internet Explorer Enhanced Security Configuration

By default Windows Server has Internet Explorer Enhanced Security Configuration turned on. Internet Explorer Enhanced Security Configuration might cause problems signing into the Intune Connector for Active Directory. Since Internet Explorer is deprecated and in most instances, not even installed on Windows Server, Microsoft recommends turning off Internet Explorer Enhanced Security Configuration. To turn off Internet Explorer Enhanced Security Configuration:

1. Sign into the server where the Intune Connector for Active Directory is being installed with an account that has local administrator rights.
2. Open **Server Manager**.
3. In the left pane of Server Manager, select **Local Server**.
4. In the right **PROPERTIES** pane of Server Manager, select the **On or Off** link next to **IE Enhanced Security Configuration**.
5. In the **Internet Explorer Enhanced Security Configuration** window, select **Off** under **Administrators:**, and then select **OK**.

Download the Intune Connector for Active Directory

1. On the server where the Intune Connector for Active Directory is being installed, sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Intune Connector for Active Directory**.
6. In the **Intune Connector for Active Directory** screen, select **Add**.
7. In the **Add connector** window that opens, under **Configuring the Intune Connector for Active Directory**, select **Download the on-premises Intune**

Connector for Active Directory. The link downloads a file called `ODJConnectorBootstrapper.exe`.

Install the Intune Connector for Active Directory on the server

Important

The Intune Connector for Active Directory installation needs to be done with an account that has the following domain rights:

- **Required** - Create `msDs-ManagedServiceAccount` objects in the Managed Service Accounts container.
- **Optional** - Modify permissions in OUs in Active Directory - if the administrator installing the updated Intune Connector for Active Directory doesn't have this right, additional configuration steps are required by an administrator who has these rights. For more information, see the step/section **Increase the computer account limit in the Organizational Unit**.

1. Sign into the server where the Intune Connector for Active Directory is being installed with an account that has local administrator rights.
2. If the previous legacy Intune Connector for Active Directory is installed, uninstall it first before installing the updated Intune Connector for Active Directory. For more information, see [Uninstall the Intune Connector for Active Directory](#).

Important

When uninstalling the previous legacy Intune Connector for Active Directory, make sure to run the legacy **Intune Connector for Active Directory** installer as part of the uninstall process. If the legacy Intune Connector for Active Directory installer prompts to **Uninstall** it when it's run, select to uninstall it. This step ensures that the previous legacy Intune Connector for Active Directory is fully uninstalled. The legacy Intune Connector for Active Directory installer can be downloaded from [Intune Connector for Active Directory](#).

Tip

In domains with only a single Intune Connector for Active Directory, Microsoft recommends first installing the updated Intune Connector for Active Directory on another server. Installing the updated Intune Connector for Active Directory on another server should be done before uninstalling the legacy Intune Connector for Active Directory on the current server. Installing the Intune Connector for Active Directory on another first avoids any downtime while the Intune Connector for Active Directory is being updated on the current server.

3. Open the `ODJConnectorBootstrapper.exe` file that downloaded to launch the **Intune Connector for Active Directory Setup** install.
4. Step through the **Intune Connector for Active Directory Setup** install.
5. At the end of the install, select the checkbox **Launch Intune Connector for Active Directory**.

 **Note**

If **Intune Connector for Active Directory Setup** install is accidentally closed without selecting the checkbox **Launch Intune Connector for Active Directory**, the **Intune Connector for Active Directory** configuration can be reopened by selecting **Intune Connector for Active Directory > Intune Connector for Active Directory** from the Start menu.

Sign in to the Intune Connector for Active Directory

1. In the **Intune Connector for Active Directory** window, under the **Enrollment** tab, select **Sign In**.
2. Under the **Sign In** tab, sign in with the Microsoft Entra ID credentials of an Intune administrator role. The user account must have an assigned Intune license. The sign in process might take a few minutes to complete.

 **Note**

The account used to enroll the Intune Connector for Active Directory is only a temporary requirement at the time of installation. The account isn't used going forward after the server is enrolled.

3. Once the sign in process completes:
 - a. A **The Intune Connector for Active Directory successfully enrolled** confirmation window appears. Select **OK** to close the window.
 - b. An **A Managed Service Account with name "<MSA_name>" was successfully set up** confirmation window appears. The name of the MSA is in the format `msaODJ#####` where ##### are five random characters. Notate the name of the MSA that was created, and then select **OK** to close the window. The name of the MSA might be needed later to configure the MSA to allow creating computer objects in OUs.
4. The **Enrollment** tab shows **Intune Connector for Active Directory** is enrolled. The **Sign In** button is greyed out and **Configure Managed Service Account** is enabled.
5. Close the **Intune Connector for Active Directory** window.

Verify the Intune Connector for Active Directory is active

After authenticating, the Intune Connector for Active Directory finishes installing. Once it finishes installing, verify that it's active in Intune by following these steps:

1. Go to the [Microsoft Intune admin center](#) if it's still open. If the **Add connector** window is still displayed, close it.

If the **Microsoft Intune admin center** isn't still open:

- a. Sign into the [Microsoft Intune admin center](#).
- b. In the **Home** screen, select **Devices** in the left hand pane.
- c. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
- d. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
- e. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Intune Connector for Active Directory**.

2. In the **Intune Connector for Active Directory** page:

- Confirm that the server is displayed under **Connector name** and shows as **Active** under **Status**
- For the updated Intune Connector for Active Directory, make sure the version is greater than **6.2501.2000.5**.

If the server isn't displayed, select **Refresh** or navigate away from the page, and then navigate back to the **Intune Connector for Active Directory** page.

! Note

- It can take several minutes for the newly enrolled server to appear in the **Intune Connector for Active Directory** page of the [Microsoft Intune admin center](#). The enrolled server only appears if it can successfully communicate with the Intune service.
- Inactive Intune Connectors for Active Directory still appear in the **Intune Connector for Active Directory** page and will automatically be cleaned up after 30 days.

After the Intune Connector for Active Directory is installed, it will start logging in the **Event Viewer** under the path **Applications and Services Logs > Microsoft > Intune > ODJConnectorService**. Under this path, **Admin** and **Operational** logs can be found.

Configure the MSA to allow creating objects in OUs (optional)

By default, MSAs only have access to create computer objects in the **Computers** container. MSAs don't have access to create computer objects in Organizational Units (OUs). To allow the MSA to create objects in OUs, the OUs need to be added to the `ODJConnectorEnrollmentWizard.exe.config` XML file found in `ODJConnectorEnrollmentWizard` directory where the Intune Connector for Active Directory was installed, normally `C:\Program Files\Microsoft Intune\ODJConnector\`.

To configure the MSA to allow creating objects in OUs, follow these steps:

1. On the server where the Intune Connector for Active Directory is installed, navigate to `ODJConnectorEnrollmentWizard` directory where the Intune Connector for Active Directory was installed, normally `C:\Program Files\Microsoft Intune\ODJConnector\`.
2. In the `ODJConnectorEnrollmentWizard` directory, open the `ODJConnectorEnrollmentWizard.exe.config` XML file in a text editor, for example, **Notepad**.

3. In the `ODJConnectorEnrollmentWiazard.exe.config` XML file, add in any desired OUs that the MSA should have access to create computer objects in. The OU name should be the distinguished name and if applicable, needs to be escaped. The following example is an example XML entry with the OU distinguished name:

```
XML

<appSettings>

    <!-- Semicolon separated list of OUs that will be used for
        Hybrid Autopilot, using LDAP distinguished name format.
        The ODJ Connector will only have permission to create
        computer objects in these OUs.
        The value here should be the same as the value in the
        Hybrid Autopilot configuration profile in the Azure portal -
        https://learn.microsoft.com/en-us/mem/intune/configuration/domain-
        join-configure

        Usage example (NOTE: PLEASE ENSURE THAT THE DISTINGUISHED
        NAME IS ESCAPED PROPERLY):
        Domain contains the following OUs:
        - OU=HybridDevices,DC=contoso,DC=com
        -
        OU=HybridDevices2,OU=IntermediateOU,OU=TopLevelOU,DC=contoso,DC=com

        Value:
        "OU=HybridDevices,DC=contoso,DC=com;OU=HybridDevices2,OU=Intermedia
        teOU,OU=TopLevelOU,DC=contoso,DC=com" -->

        <add key="OrganizationalUnitsUsedForOfflineDomainJoin"
        value="OU=SubOU,OU=TopLevelOU,DC=contoso,DC=com;OU=Mine,DC=contoso,
        DC=com" />
    </appSettings>
```

4. Once all desired OUs are added, save the `ODJConnectorEnrollmentWiazard.exe.config` XML file.
5. As an administrator that has appropriate permissions to modify OU permissions, open the **Intune Connector for Active Directory** by navigating to **Intune Connector for Active Directory > Intune Connector for Active Directory** from the **Start** menu.

Important

If the administrator installing and configuring the Intune Connector for Active Directory doesn't have permissions to modify OU permissions, then the section/steps **Increase the computer account limit in the**

Organizational Unit need to be followed instead by an administrator that does have permissions to modify OU permissions.

6. Under the **Enrollment** tab in the **Intune Connector for Active Directory** window, select **Configure Managed Service Account**.
7. An **A Managed Service Account with name "<MSA_name>" was successfully set up** confirmation window appears. Select **OK** to close the window.

Next step: Increase the computer account limit in the Organizational Unit (OU)

Step 3: Increase the computer account limit in the Organizational Unit (OU)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

User-driven Microsoft Entra hybrid join: Increase the computer account limit in the Organizational Unit (OU)

Article • 02/27/2025 • Applies to:  Windows 11,  Windows 10

Windows Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Install the Intune Connector](#)
- ✓ Step 3: **Increase the computer account limit in the Organizational Unit (OU)**
 - Step 4: [Register devices as Windows Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Windows Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Windows Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Windows Autopilot device to a user \(optional\)](#)
 - Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

Note

If the computer account limit for the proper Organizational Unit (OU) is already increased, skip this step and move on to [Step 4: Register devices as Windows Autopilot devices](#).

Increase the computer account limit in the Organizational Unit (OU)

Updated Connector

Important

This step is only needed under one of the following conditions:

- The administrator that installed and configured the Intune Connector for Active Directory didn't have appropriate rights as outlined in [Intune Connector for Active Directory Requirements](#).
- The `ODJConnectorEnrollmentWiazard.exe.config` XML file wasn't modified to add OUs that the MSA should have permissions for.

The purpose of Intune Connector for Active Directory is to join computers to a domain and add them to an OU. For this reason, the [Managed Service Account \(MSA\)](#) being used for the Intune Connector for Active Directory needs to have permissions to create computer accounts in the OU where the computers are joined to the on-premises domain.

With default permissions in Active Directory, domain joins by the Intune Connector for Active Directory might initially work without any permission modifications to the OU in Active Directory. However after MSA attempts to join more than 10 computers to the on-premises domain, it would stop working because by default, Active Directory only allows any single account to join up to 10 computers to the on-premises domain.

The following users aren't restricted by the 10 computer domain join limitation:

- Users in the Administrators or Domain Administrators groups: In order to comply with the least privilege principles model, Microsoft doesn't recommend making the MSA an administrator or domain administrator.
- Users with delegated permissions on Organizational Unit (OUs) and containers in Active Directory to create computer accounts: This method is recommended since it follows the least privilege principles model.

To fix this limitation, the MSA needs the **Create computer accounts** permission in the Organizational Unit (OU) where the computers are joined to in the on-premises domain. The Intune Connector for Active Directory sets the permissions for the MSAs to the OUs as long as one of the following conditions is met:

- The administrator installing the Intune Connector for Active Directory has the necessary permissions to set permissions on the OUs.
- The administrator configuring the Intune Connector for Active Directory has the necessary permissions to set permissions on the OUs.

If the administrator installing or configuring the Intune Connector for Active Directory doesn't have the necessary permissions to set permissions on the OUs, then the following steps need to be followed:

1. Sign into a computer that has access to the **Active Directory Users and Computers** console with an account that has the necessary permissions to set permissions on OUs.
2. Open the **Active Directory Users and Computers** console by running **DSA.msc**.
3. Expand the desired domain and navigate to the organizational unit (OU) that computers are joining to during Windows Autopilot.

 **Note**

The OU that computers join during the Windows Autopilot deployment is specified later during the **Configure and assign domain join profile** step.

4. Right-click on the OU and select **Properties**.

 **Note**

If computers are joining the default **Computers** container instead of an OU, right-click on the **Computers** container and select **Delegate Control**.

5. In the OU **Properties** window that opens, select the **Security** tab.
6. In the **Security** tab, select **Advanced**.
7. In the **Advanced Security Settings** window, select **Add**.
8. In the **Permission Entry** window, next to **Principal**, select the **Select a principal** link.
9. In the **Select User, Computer, Service Account, or Group** window, select the **Object Types...** button.
10. In the **Object Types** window, select the **Service Accounts** check box, and then select **OK**.
11. In the **Select User, Computer, Service Account, or Group** window, under **Enter the object name to select**, enter the name of the MSA being used for the Intune Connector for Active Directory.

 **Tip**

The MSA was created during the **Install the Intune Connector for Active Directory** step/section and has the name format of `msaODJ#####` where ##### are five random characters. If the MSA name isn't known, follow these steps to find the MSA name:

- a. On the server running the Intune Connector for Active Directory, right-click on the **Start** menu and then select **Computer Management**.
- b. In the **Computer Management** window, expand **Services and Applications** and then select **Services**.
- c. In the results pane, locate the service with the name **Intune ODJConnector for Active Service**. The name of the MSA is listed in the **Log On As** column.

12. Select **Check Names** to validate the MSA name entry. Once the entry is validated, select **OK**.
13. In the **Permission Entry** windows, select the **Applies to:** drop-down menu and then select **This object only**.
14. Under **Permissions**, unselect all items, and then only select the **Create Computer objects** check box.
15. Select **OK** to close the **Permission Entry** window.
16. In the **Advanced Security Settings** window, select either **Apply** or **OK** to apply the changes.

Next step: Register devices as Windows Autopilot devices

Step 4: Register devices as Windows Autopilot devices

Related content

For more information on increasing the computer account limit in an Organizational Unit, see the following articles:

- [Increase the computer account limit in the Organizational Unit](#).
- [Default limit to number of workstations a user can join to the domain](#).

- Add workstations to domain.
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

User-driven Microsoft Entra hybrid join: Register devices as Autopilot devices

Article • 06/19/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Install the Intune Connector \(OU\)](#)
- Step 3: [Increase the computer account limit in the Organizational Unit](#)

Step 4: Register devices as Autopilot devices

- Step 5: [Create a device group](#)
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
- Step 8: [Configure and assign domain join profile](#)
- Step 9: [Assign Autopilot device to a user \(optional\)](#)
- Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

Note

If devices are already registered as Windows Autopilot devices, skip this step and move on to [Step 5: Create a device group](#).

Register devices as Autopilot devices

Before a device can use Autopilot, the device must be registered as an Autopilot device. Registering a device as an Autopilot device can be thought of as importing the device into Autopilot so that Autopilot service can be used on the device. Registering a device as an Autopilot device doesn't mean that the device has used the Autopilot service. It just makes the Autopilot service available to the device.

Also note that a device registered in Autopilot doesn't mean the device is enrolled in Intune. A device might be registered as an Autopilot device but might not exist in Intune. It's not until an Autopilot registered device goes through the Autopilot process for the first time that it becomes enrolled in Intune. After the Autopilot device

undergoes the Autopilot process and enrolls in Intune, the Autopilot device appears as a device in both Microsoft Entra ID and Intune.

There are several methods to register a device as an Autopilot device in Intune:

- Manually registering devices into Intune as an Autopilot device via the hardware hash. The hardware hash of a device can be collected via one of the following methods:
 - [Configuration Manager](#).
 - [PowerShell script](#).
 - [Diagnostics page hash export](#).
 - [Desktop hash export](#).

These methods of obtaining the hardware hash of a device are well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

- Automatically registering device via:
 - An [OEM](#), including [Microsoft Surface](#) devices.
 - A [partner](#).

Registering a device via an OEM or partner is also well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

For most organizations, using an OEM or partner to register devices as Autopilot devices is the preferred, most common, and most secure method. However for smaller organizations, for testing/lab scenarios, and for emergency scenarios, manually registering devices as Autopilot devices via the hardware hash is also used.

Important

The following type of devices shouldn't be registered as a Windows Autopilot device:

- [Microsoft Entra registered](#) devices, also known as "workplace joined" devices.
- [Intune MDM-only enrollment](#) devices.

These options are intended for users to join personally owned devices to their organization's network. Windows Autopilot registered devices are registered as corporate owned devices.

If a device is already one of these two types of devices, to register it as a Windows Autopilot device, first remove it from Microsoft Intune and Microsoft Entra ID. For

more information, see [Device appears as Microsoft Entra registered instead of Microsoft Entra joined](#) and [Deregister a device](#).

 **Note**

Assuming that a device isn't currently enrolled Intune, remember that registering a device in Autopilot doesn't make it an Intune enrolled device. That device doesn't enroll into Intune until Autopilot runs on the device for the first time.

Importing the hardware hash CSV file for devices into Intune

Several of the methods in the previous section on obtaining the hardware hash when manually registering devices as Autopilot devices produces a CSV file that contains the hardware hash of the device. This CSV file with the hardware hash needs to be imported into Intune to register the device as an Autopilot device.

After the CSV file is created, it can be imported into Intune via the following steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, select **Import**.
 - a. In the **Add Autopilot devices** window that opens:
 - i. Under **Specify the path to the list you want to import.**, select the blue file folder.
 - ii. Browse to the CSV file obtained using one of the above methods to obtain the hardware hash of a device.
 - iii. After selecting the CSV file, verify that the correct CSV file is selected under **Specify the path to the list you want to import.**, and then select **Import**.

Selecting **Import** closes the **Add Autopilot devices** window. Importing can take several minutes.

- b. After the import is complete, select **Sync**.

A message displays saying that the sync is in progress. The sync process might take a few minutes to complete, depending on how many devices are being synchronized.

 **Note**

If another sync is attempted within 10 minutes after initiating a sync, an error will be displayed. Syncs can only occur once every 10 minutes. To attempt a sync again, wait at least 10 minutes before trying again.

- c. Select **Refresh** to refresh the view. The newly imported devices should display within a few minutes. If the devices aren't yet displayed, wait a few minutes, and then select **Refresh** again.

Next step: Create a device group

Step 5: Create a device group

Related content

For more information on registering devices as Autopilot devices, see the following articles:

- [Manually register devices with Windows Autopilot](#).
- [Windows Autopilot customer consent](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

User-driven Microsoft Entra hybrid join: Create a device group

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Autopilot devices](#)
-  **Step 5: Create a device group**
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Autopilot device to a user \(optional\)](#)
 - Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

 **Note**

If device groups from are already created, skip this step and move on to [Step 6: Configure and assign Autopilot Enrollment Status Page \(ESP\)](#). However, if deploying multiple and/or different Autopilot scenarios to different devices, separate device groups are required for each Windows Autopilot scenario.

Create a device group

Device groups are a collection of devices organized into a Microsoft Entra group. Device groups are used in Autopilot to target devices for specific configurations such as what policies to apply to a device and what applications to install on the device. They're also used by Autopilot to target Enrollment Status Page (ESP) configurations, Autopilot profile configurations, and domain join profiles to devices.

Device groups can be either dynamic or assigned:

- **Dynamic groups** - Devices are automatically added to the group based on rules

- **Assigned groups** - Devices are manually added to the group and are static

When an admin configures Autopilot in an enterprise environment, dynamic groups are primarily used since a large number of devices are normally involved. Adding the devices in automatically using rules makes management of the group a lot easier. Adding a large amount of device in manually via an assigned group would be impractical. However, if there's only a few devices, for example for testing purposes, an assigned group can be used instead.

To create a dynamic device group for use with Autopilot, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Groups** in the left hand pane.
3. In the **Groups | All groups** screen, make sure **All groups** is selected, and then select **New group**.
4. In the **New Group** screen that opens:
 - a. For **Group type**, select **Security**.
 - b. For **Group name**, enter a name for the device group.
 - c. For **Group description**, enter a description for the device group.
 - d. For **Microsoft Entra roles can be assigned to the group**, select **No**.
 - e. For **Membership type**, select **Dynamic Device**. Setting the **Membership type** option to **Dynamic Device** changes the option **Members** to **Dynamic device members**.
 - f. For **Owners**, select the **No owners selected** link.
 - g. In the **Add owners** screen that opens:
 - i. Scroll through the list of objects and select owners for the user group. Alternatively, use the **Search** bar to search for and select owners of the group.
 - ii. Once all of the desired owners are selected, select **Select**.
 - h. For **Dynamic device members**, select **Add dynamic query**. The **Dynamic membership rules** screen opens.
 - i. In the **Dynamic membership rules** screen:

- i. Make sure that **Configure Rules** is selected at the top.
- ii. Select **Add expression**. Rules and expressions can be added that defines what devices are added to the device group.

Rules can be entered in the rule builder via the drop-down boxes. Alternatively, the rule syntax can be entered directly via the **Edit** option in the **Rule syntax** section.

The most common type of dynamic device group when using Windows Autopilot is a device group that contains all Windows Autopilot devices. A dynamic device group that contains all Windows Autopilot devices has the following syntax:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```

To enter in this rule:

- i. Select the **Edit** option in the **Rule syntax** section.
- ii. Paste in the following rule in the **Edit rule syntax** screen under **Rule syntax**:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```
- iii. Once the rule is pasted in, select **OK**.
- iii. Once the desired rule is entered, select **Save** on the toolbar to close the **Dynamic membership rules** window.

For more information on creating rules for dynamic groups, see [Dynamic membership rules for groups in Microsoft Entra ID](#).

- j. Select **Create** to finish creating the dynamic device group.

Note

The above steps are creating a dynamic group in Microsoft Entra that is used by Intune and Windows Autopilot solutions. Although the groups can be accessed in the Intune portal, they're Microsoft Entra groups.

Tip

For Configuration Manager admins, device groups are similar to device based collections. Dynamic device groups are similar to query based device collections while assigned device groups are similar to direct membership device collections.

Next step: Configure and assign the Enrollment Status Page (ESP)

Step 5: Configure and assign Autopilot Enrollment Status Page (ESP)

Related content

For more information on creating groups in Intune, see the following articles:

- [Create device groups.](#)
- [Add groups to organize users and devices.](#)
- [Manage Microsoft Entra groups and group membership.](#)
- [Dynamic membership rules for groups in Microsoft Entra ID.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

User-driven Microsoft Entra hybrid join: Configure and assign the Enrollment Status Page (ESP)

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Autopilot devices](#)
 - Step 5: [Create a device group](#)
-  **Step 6: Configure and assign Autopilot Enrollment Status Page (ESP)**
- Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Autopilot device to a user \(optional\)](#)
 - Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

Note

If an ESP is already configured and assigned and the same settings for the ESP should be used for the user-driven Microsoft Entra hybrid join scenario, skip this step and move on to [Step 7: Create and assign Microsoft Entra hybrid join Autopilot profile](#).

The Enrollment Status Page (ESP)

The main feature of the Enrollment Status Page (ESP) is to display progress and current status to the end user while the device is being set up and enrolled via the Autopilot process. The other main feature of the ESP is to block a user from signing in and using the device until all required policies and applications are installed. Multiple ESP profiles can be created with different settings and assigned appropriately based on different needs and scenarios.

Out of box there's a default ESP that is assigned to all devices. The default setting in the default ESP is to not show app and profile progress during the Autopilot process. However, Microsoft recommends changing this default via a separate custom ESP to show app and profile progress. Enabling and configuring an ESP allows end users to properly see the progress of their device being set up and prevents them using the device until the device is fully configured and provisioned. A user signing into the device before being fully configured and provisioned can cause issues.

The ESP has two phases:

- **Device ESP** - The portion of the ESP that runs during the OOB process and applies device policies and installs device applications.
- **User ESP** - The portion of the ESP that sets up user account, applies user policies, and installs user applications.

Device ESP runs first followed by the User ESP.

Tip

For Configuration Manager admins, an ESP is similar and analogous to Configuration Manager client settings.

Autopilot Enrollment Status Page (ESP) configuration options

When the Enrollment Status Page (ESP) is configured, it has several options that can be configured to meet the needs of the organization. The following lists the different options and their possible configurations:

- **Show an error when installation takes longer than specified number of minutes:**
 - The default time-out is 60 minutes. Enter a higher value if more time is needed to install applications on the devices.
- **Show custom message when time limit or error occur:**
 - **No:** The default message is shown to users when an error occurs. That message is: **Setup could not be completed. Please try again or contact your support person for help.**
 - **Yes:** A custom message is shown to users when an error occurs. Enter a custom message in the provided text box.

- Turn on log collection and diagnostics page for end users:
 - No: The collect logs button isn't shown to users when an installation error occurs. The Windows Autopilot diagnostics page isn't shown on devices running Windows 11.
 - Yes: The collect logs button is shown to users when an installation error occurs. The Windows Autopilot diagnostics page is shown on devices running Windows 11. Logs and diagnostics might aid with troubleshooting. For this reason, Microsoft recommends enabling this option.
- Only show page to devices provisioned by out-of-box experience (OOBE):
 - No: The enrollment status page (ESP) is shown during the device phase and the out-of-box experience (OOBE). The page is also shown during the user phase to every user who signs into the device for the first time.
 - Yes: The enrollment status page (ESP) is shown during the device phase and the OOBE. The page is also shown during the user phase, but only to the first user who signs into the device. It isn't shown to subsequent users who sign into the device.
- Block device use until all apps and profiles are installed:
 - No: Users can leave the ESP before Intune is finished setting up the device.
 - Yes: Users can't leave the ESP until Intune is done setting up the device. Enabling this option unlocks the following additional options:
 - Allow users to reset device if installation error occurs:
 - No: The ESP doesn't give users the option to reset their devices when an installation fails.
 - Yes: The ESP gives users the option to reset their devices when an installation fails.
 - Allow users to use device if installation error occurs:
 - No: The ESP doesn't give users the option to bypass the ESP when an installation fails.
 - Yes: The ESP gives users the option to bypass the ESP and use their devices when an installation fails.

- **Block device use until these required apps are installed if they are assigned to the user/device:**
 - **All:** All assigned apps must be installed before users can use their devices.
 - **Selected:** Selected apps must be installed before users can use their devices. After enabling this option, select **Select apps** to select the managed apps from Intune that are required to be installed before users can use their device.

Configure and assign the Enrollment Status Page (ESP)

To configure and assign the Autopilot Enrollment Status Page (ESP), follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
- 1 In the **Devices | Overview** screen, under **By platform**, select **Windows**.
 1. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
 2. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Enrollment Status Page**.
 3. In the **Enrollment Status Page** screen that opens, select **Create**.
 4. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the ESP profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.
 5. In the **Settings** page, toggle the option **Show app and profile configuration progress** to **Yes**.
 - a. After the option **Show app and profile configuration progress** is toggled to **Yes**, several new options will appear. Configure these options based on the desired behavior for the ESP as described in the section [Autopilot Enrollment Status Page \(ESP\) configuration options](#):

- b. Once the different ESP options under the **Settings** page are configured as desired, select **Next**.
6. In the **Assignments** page:
 - a. Under **Included groups**, select **Add groups**.
 - b. In the **Select groups to include** window that opens, select the device groups to target the ESP profile. The device groups selected would normally be the device groups created in the **Create device group** step.
 - c. After selecting the device group, select **Select** to close the **Select groups to include** window.

 **Tip**

After selecting the device groups, the **Edit filter** option can be selected on each device group added to the assignment to further refine what devices are targeted for the ESP profile. For example, further filtering can be useful if some of the devices that are members in the device groups selected need to be excluded.

- d. Select **Next**.

 **Note**

An ESP is assigned to a device group and not directly to individual devices. To assign an ESP to a specific device, the device must be a member of a device group that has an ESP assigned to it.

7. In the **Scope tags** page, select **Next**.

 **Note**

Scope tags are optional and are a method to control who has access to the ESP configuration. For this tutorial, scope tags are being skipped and left at the default scope tag. However if a custom scope tag needs to be specified, do so at this screen. For more information about scope tags, see [Use role-based access control and scope tags for distributed IT](#).

8. In the Review + create page, verify that the settings are correct and configured as desired. Once verified, select **Create** to save the changes and assign the ESP profile.

Next step: Create and assign user-driven Microsoft Entra hybrid join Autopilot profile

Step 7: Create and assign Microsoft Entra hybrid join Autopilot profile

Related content

For more information on the Enrollment Status Page (ESP), see the following articles:

- [Windows Autopilot Enrollment Status Page](#).
- [Set up the Enrollment Status Page](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

User-driven Microsoft Entra hybrid join: Create and assign user-driven Microsoft Entra hybrid join Autopilot profile

Article • 09/13/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
-  **Step 7: Create and assign Microsoft Entra hybrid join Autopilot profile**
- Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Autopilot device to a user \(optional\)](#)
 - Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

Create and assign user-driven Microsoft Entra hybrid join Autopilot profile

The Autopilot profile specifies how the device is configured during Windows Setup and what is shown during the out-of-box experience (OOBE).

When an admin creates an Autopilot profile for the user-driven scenario, devices with this Autopilot profile are associated with the user enrolling the device. User credentials are required to enroll the device.

The difference between a Microsoft Entra join and a Microsoft Entra hybrid join is that the Microsoft Entra hybrid join scenario joins both an on-premises domain and Microsoft Entra ID during Autopilot. The user-driven Microsoft Entra join scenario only joins Microsoft Entra ID during Autopilot.

 **Tip**

For Configuration Manager admins, the Autopilot profile is similar to some of the configuration that takes place during a task sequence via an unattend.xml file. The unattend.xml file is configured during the **Apply Windows Settings** and **Apply Network Settings** steps. Note however that Autopilot doesn't use unattend.xml files.

To create a user-driven Microsoft Entra hybrid join Autopilot profile, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Deployment Profiles**.
6. In the **Windows Autopilot deployment profiles** screen, select the **Create Profile** drop down menu and then select **Windows PC**.
7. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the Autopilot profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.

 **Note**

Microsoft recommends setting the option **Convert all targeted devices to Autopilot** to **Yes**. This tutorial concentrates on new devices where the device is manually imported as an Autopilot device using the hardware hash. However, this option can be helpful when assigning Autopilot profiles to device groups that contain existing devices. For example, this option is helpful when using the [Windows Autopilot for existing devices](#) scenario. With Windows Autopilot for existing devices, existing devices might need to be registered as an Autopilot device after the Autopilot deployment completes. For more information, see [Register device for Windows Autopilot](#).

8. In the Out-of-box experience (OOBE) page:

- For **Deployment mode**, select **User-driven**.
- For **Join to Microsoft Entra ID as**, select **Microsoft Entra hybrid joined**. After this option is selected, several the options underneath this option will change.
- For **Skip AD connectivity check**, select **No**. This section of the tutorial assumes that the device undergoing Windows Autopilot is an on-premises internal client that has direct connectivity to the on-premises domain and domain controllers. For off-premise/Internet scenarios where VPN connectivity is required, see [Off-premises/Internet scenarios and VPN connectivity](#).
- For **Microsoft Software License Terms**, select **Hide** to skip the EULA page.
- For **Privacy settings**, select **Hide** to skip the privacy settings.
- For **Hide change account options**, select **Hide**.
- For **User account type**, select either **Administrator** or **Standard user** depending on the desired account type for the user. If **Administrator** is chosen, the user is added to the local Administrator group on the device.
- For **Allow pre-provisioned deployment**, select **No**.

 **Note**

For the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join scenario, see [Step by step tutorial for Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join in Intune](#)

- For **Language (Region)**, select **Operating system default** to use the default language for the operating system being configured. If another language is desired, select the desired language from the drop-down list.
- For **Automatically configure keyboard**, select **Yes** to skip the keyboard selection page.
- The **Apply device name template** is greyed out for Microsoft Entra hybrid join scenarios. Although not as robust, device names can be specified during the [Configure and assign domain join profile](#) step.

① Note

The above settings are selected to minimize user interaction during device setup. However, some of the options that are set as hidden can instead be shown as desired. For example, some regions might require that **Privacy settings** always be shown.

① Note

If the language/region and keyboard screens are set to hidden, they might still be displayed if there's no network connectivity at the start of the Windows Autopilot deployment. When there's no network connectivity at the start of the deployment, the Windows Autopilot profile, where the settings to hide these screens is defined, hasn't downloaded yet. Once network connectivity is established, the Autopilot profile is downloaded and any additional screen settings should work as expected.

9. Once the options in the **Out-of-box experience (OOBE)** page are configured as desired, select **Next**.
10. In the **Assignments** page:
 - a. Under **Included groups**, select **Add groups**.

① Note

Make sure to add the correct device groups under **Included groups** and not under **Excluded groups**. Accidentally adding the desired device groups under **Excluded groups** prevents devices in those device groups from receiving the Autopilot profile.

- a. In the **Select groups to include** window that opens, select the groups that the Windows Autopilot profile should be assigned to. These device groups are normally the device groups created in the previous **Create device group** step. Once done, select **Select**.
 - b. Under **Included groups > Groups**, ensure the correct groups are selected, and then select **Next**.
11. In the **Review + Create** page, verify that all settings are set correctly, and then select **Create** to create the Autopilot profile.

Verify device has an Autopilot profile assigned to it

Before deploying a device, ensure that an Autopilot profile is assigned to a device group that the device is a member of. Autopilot profile assignment to a device can take some time after the Autopilot profile is assigned to the device group or after the device is added to the device group. To verify that the profile is assigned to a device, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens:
 - a. Find the desired device that Autopilot deployment profile assignment status needs to be checked.
 - b. Once the device is located, its current status is listed under the **Profile status** column. The status has one of the following values:
 - **Not assigned**: An Autopilot deployment profile isn't assigned to the device.
 - **Assigning**: An Autopilot deployment profile is being assigned to the device.
 - **Assigned**: An Autopilot deployment profile is assigned to the device.
 - **Fix pending**: When a hardware change occurs on a device, this status displays while Intune tries to register the new hardware. When the link for the **Fix pending** status is selected, the following message appears:

We've detected a hardware change on this device. We're trying to automatically register the new hardware. You don't need to do anything now; the status will be updated at the next check in with the result.

If Intune is able to successfully register the new hardware, Intune updates the profile status when the device next checks into Intune. For more information on the **Fix pending** status, see the following articles:

- [Why is the Windows Autopilot profile not applied after a hardware change occurred on a device?](#).
 - [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
 - [Windows Autopilot motherboard replacement scenario guidance](#)
- **Attention required:** If Intune is unable to register the new hardware after a hardware change occurs on a device, the device can't receive the Autopilot profile until the device is reset and the device re-registers. For more information on this status and how to deregister/re-register a device, see the following articles:
 - [Why is the Windows Autopilot profile not applied after a hardware change occurred on a device?](#).
 - [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
 - [Windows Autopilot motherboard replacement scenario guidance](#)
 - [Deregister a device](#)

Before starting the Autopilot deployment process on a device, make sure that in the [Windows Autopilot devices](#) page:

- The device's **Profile status** status is **Assigned**.
- In the properties of the device, **Date assigned** has a value.
- In the properties of the device, **Assigned profile** displays the expected Autopilot profile.

Note

Intune periodically checks for new devices in the assigned device groups, and then begins the process of assigning profiles to those devices. Due to several different factors involved in the process of Autopilot profile assignment, an estimated time for the assignment can vary from scenario to scenario. These factors can include Microsoft Entra groups, membership rules, hash of a device, Intune and Autopilot services, and internet connection. The assignment time varies depending on all the factors and variables involved in a specific scenario.

Off-premises/Internet scenarios and VPN connectivity

Windows Autopilot user-driven Microsoft Entra hybrid join supports off-premises/Internet scenarios where direct connectivity to Active directory and domain controllers isn't available. However, an off-premises/Internet scenario doesn't eliminate the need for connectivity to Active Directory and a domain controller during the domain join. In an off-premises/Internet scenario, connectivity to Active Directory and a domain controller can be established via a VPN connection during the Autopilot process.

For off-premises/Internet scenarios requiring VPN connectivity, the only change in the Autopilot profile would be in the setting **Skip AD connectivity check**. In the [Create and assign user-driven Microsoft Entra hybrid join Autopilot profile](#) section, the **Skip AD connectivity check** setting should be set to **Yes** instead of to **No**. Setting this option to **Yes** prevents the deployment from failing since there's no direct connectivity to Active Directory and domain controllers until the VPN connection is established.

In addition to changing the **Skip AD connectivity check** setting to **Yes** in the Autopilot profile, VPN support also relies on the following requirements:

- The VPN solution can be deployed and installed with Intune.
- The VPN solution needs to support one of the following options:
 - Lets the user manually establish a VPN connection from the Windows sign-in screen.
 - Automatically establishes a VPN connection as needed.

The VPN solution would need to be installed and configured via Intune during the Autopilot process. Configuration would need to include deploying any required device certificates if needed by the VPN solution. Once the VPN solution is installed and configured on the device, the VPN connection can be established, either automatically or manually by the user, at which point the domain join can occur. For more information and support on VPN solutions during Windows Autopilot, consult the respective VPN vendor.

Note

Some VPN configurations aren't supported because the connection isn't initiated until the user signs into Windows. Unsupported VPN configurations include:

- VPN solutions that use user certificates.
- Non-Microsoft UWP VPN plug-ins from the Windows Store.

Next step: Configure and assign domain join profile

Step 8: Configure and assign domain join profile

Related content

For more information on configuring Autopilot profiles, see the following articles:

- [Configure Autopilot profiles.](#)
- [User-driven mode for Microsoft Entra hybrid join with VPN support.](#)
- [VPNs.](#)

Feedback

Was this page helpful?



[Provide product feedback](#)

User-driven Microsoft Entra hybrid join: Create and assign a domain join profile

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
-  **Step 8: Configure and assign domain join profile**
- Step 9: [Assign Autopilot device to a user \(optional\)](#)
 - Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

Note

If a domain join profile is already created with the desired settings and assignments, move on to the [Next step: Assign Autopilot device to a user \(optional\)](#) section.

Create and assign a domain join profile

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **Manage devices**, select **Configuration**.
4. In the **Devices | Configuration** screen:
 - a. At the top, make sure **Policies** is selected.
 - b. Select the **Create** drop down menu and then select **New Policy**.

5. In the **Create a profile** window that opens:
 - a. Under **Platform**, select **Windows 10 and later**.
 - b. Under **Profile type**, select **Templates**.
 - c. When the templates appear, under **Template name**, select **Domain join**. If **Domain join** isn't visible, scroll through the **Template name** list until **Domain join** is visible or search for **Domain join** in the **Search by profile name** box.
 - d. Select **Create** to close the **Create a profile** window.

6. The **Domain Join** screen opens. In the **Basics** page:

- a. Next to **Name**, enter a name for the domain join profile.
- b. Next to **Description**, enter a description for the domain join profile.
- c. Select **Next**.

7. In the **Configuration settings** page:

- a. Next to **computer name prefix**, enter a prefix for computer names. This field is required. This prefix is used on all computer names. The rest of the computer name after the prefix is randomly generated up to 15 characters.

 **Note**

This field doesn't support the **%SERIAL%** or **%RAND:x%** variables that can be used with the **Apply device name template** in the Microsoft Entra join scenario.

- b. Next to **Domain name**, enter the FQDN of the domain that devices should join. This field is required. Make sure to specify the FQDN of the domain and not the NETBIOS name of the domain. For example, enter in **contoso.com** and not just **CONTOSO**.
- c. Next to **Organizational unit**, enter the full path to the Organizational Unit (OU) in the domain that the computer accounts should be created in. For example, **OU=OU-Name,DC=contoso,DC=com**. This field is optional. If the OU isn't specified, the computer accounts are created in the **Computer** container.

 **Note**

The OU specified in this step should be the same OU that permissions were set for and computer account limits increased in the step **Increase the computer account limit in the Organizational Unit (OU)**. Make sure that the step **Increase the computer account limit in the Organizational Unit (OU)** is followed for the OU specified in this field. Skipping the step that sets permissions correctly on the OU results in computers failing to join the domain.

ⓘ Important

If computers are joining the **Computers** container, leave this field blank. Don't specify the **Computers** container in this field via **CN=Computers,DC=contoso,DC=com**. The **Computers** container is a container and not an OU. When no OU is specified in this field and the field is left blank, devices automatically join the **Computers** container. If the **Computers** container is specified, it causes domain joins to fail.

d. Once the settings in the **Configuration settings** page are complete, select **Next**.

8. In the **Assignments** page:

a. Under **Included groups**, select **Add all devices**.

ⓘ Note

- Microsoft recommends selecting and assigning to **Add all devices** instead of selecting and assigning to the device group created in the **Create device group** step. Assigning to all devices ensures that the domain join profile works when using:
 - [Windows Autopilot deployment for existing devices](#) scenario.
 - A Windows Autopilot deployment that utilizes Microsoft Entra hybrid join and runs after the Windows Autopilot deployment for existing devices deployment.
- Make sure to add the correct device groups under **Included groups** and not under **Excluded groups**. Accidentally adding the desired device groups under **Excluded groups** results in those devices being excluded and they don't receive the configuration profile.

- b. Under **Included groups > Groups**, ensure that **All devices** is selected, and then select **Next**.
9. In the **Applicability Rules** page, select **Next**. For this tutorial, applicability rules are being skipped. However if applicability rules are needed, do so at this screen. For more information about scope tags, see [Applicability rules](#).
10. In the **Review + Create** page, review and verify that all of the settings are set as desired, and then select **Create** to create the domain join profile.

Next step: Assign Autopilot device to a user (optional)

[Step 9: Assign Autopilot device to a user \(optional\)](#)

If a user isn't being assigned to the device, then skip to [Step 10: Deploy the device](#).

[Step 10: Deploy the device](#)

Related content

For more information on domain join profiles, see the following article:

- [Create and assign a Domain Join profile](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

User-driven Microsoft Entra hybrid join: Assign Autopilot device to a user (optional)

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector \(OU\)](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit](#)
 - Step 4: [Register devices as Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
- Step 9: Assign Autopilot device to a user (optional)**
- Step 10: [Deploy the device](#)

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

Assign Autopilot device to a user (optional)

A device that is registered as an Autopilot device can also be assigned to a user. If an Autopilot device is assigned to a user, then any user policies and application installs assigned to that user is applied to the device during the Autopilot process.

Tip

For testing purposes, especially for hybrid Microsoft Entra scenarios, it might be better to first test an Autopilot deployment before assigning the device to a user. Not assigning a user limits the scope of applications, policies, and configurations processed during the Autopilot process.

Tip

For Configuration Manager admins, assigning a user to a device is similar to user device affinity in Configuration Manager.

To assign an Autopilot device to a user, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, locate the device to assign a user to.
7. Once the desired device is located, select the box to the left of the device, making sure that there's check mark in the box, and then select **Assign user** in the toolbar at the top of page.
8. In the **Select user** window that opens, find and select a user for the device, and then select **Select** to close the window. If necessary, use the **Search** box to find the desired user.

 **Note**

The selected user must be an Azure user licensed to use Intune.

9. In the Autopilot device's property window that automatically opens on the right hand side, under **User friendly name**, verify the default value. If the value is empty or a different friendly name is desired, enter the desired friendly name for the user under **User friendly name**, and then select **Save** to close the property window.
10. The user assignment can be verified by selecting the Autopilot device in the **Windows Autopilot devices** screen. Once the Autopilot device is selected, it highlights and the Autopilot device's property window automatically opens on the right hand side. The assigned user is listed under **User** and **User friendly name**.

Assigning Autopilot device to a user via hardware hash CSV file

A user can be manually assigned to a Windows Autopilot device in the Windows Autopilot device's properties. However, a user can also be assigned to the Autopilot device when the device was initially imported into Autopilot as an Autopilot device. Assigning a user when the device is imported as an Autopilot device can be done by editing the hardware hash CSV file and adding the **Assigned User** column after the **Hardware Hash** column. The user's User Principal Name (UPN) should then be added as a value under the **Assigned User** column.

Important

Use a plain-text editor such as **Notepad** to edit the CSV file. Don't use Microsoft Excel. Editing the CSV file in Excel doesn't generate a proper usable file for importing into Intune.

For more information on editing the CSV file to add an assigned user to the Autopilot device, see [Manually register devices with Windows Autopilot: Ensure that the CSV file meets requirements](#).

Next step: Deploy the device

[Step 10: Deploy the device](#)

Related content

For more information on assigning a user to an Autopilot device, see the following article:

- [Assign a user to a specific Autopilot device.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

User-driven Microsoft Entra hybrid join: Deploy the device

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Autopilot device to a user \(optional\)](#)
- Step 10: Deploy the device**

For an overview of the Windows Autopilot user-driven Microsoft Entra hybrid join workflow, see [Windows Autopilot user-driven Microsoft Entra hybrid join overview](#).

Deploy the device

Once all of the configurations for the Windows Autopilot user-driven Microsoft Entra hybrid join deployment are completed in Intune and in Microsoft Entra ID, the next step is to start the Autopilot deployment process on the device. If desired, deploy any additional applications and policies that should run during the Autopilot deployment to a device group that the device is a member of.

Important

The Microsoft Entra hybrid join process requires connectivity to both the Internet and a domain controller. If the connected network doesn't have connectivity to a domain controller, a solution such as a VPN that has connectivity to a domain controller is required.

To start the Autopilot deployment process on the device, acquire a device that is part of the device group created in the previous [Create a device group](#) step. Once the device is acquired, follow these steps:

1. If a wired network connection is available, connect the device to the wired network connection.
2. Power on the device.
3. Once the device boots up, one of two things occurs depending on the state of network connectivity:
 - If the device is connected to a wired network and has network connectivity, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
 - If the device isn't connected to a wired network or if it doesn't have network connectivity, it prompts to connect to a network. Connectivity to the Internet is required:
 - a. The out-of-box experience (OOBE) begins and a screen asking for a country or region appears. Select the appropriate country or region, and then select **Yes**.
 - b. The keyboard screen appears to select a keyboard layout. Select the appropriate keyboard layout, and then select **Yes**.
 - c. An additional keyboard layouts screen appears. If needed, select additional keyboard layouts via **Add layout**, or select **Skip** if no additional keyboard layouts are needed.
- d. The **Let's connect you to a network** screen appears. At this screen, either plug the device into a wired network (if available), or select and connect to a wireless Wi-Fi network.

 **Note**

When there's no network connectivity, the device can't download the Autopilot profile to know what country/region and keyboard settings to use. For this reason, when there's no network connectivity, the country/region and keyboard screens appear even if these screens are set to hidden in the Autopilot profile. These settings need to be specified in these screens in order for the network connectivity screens that follow to work properly.

- e. Once network connectivity is established, the **Next** button should become available. Select **Next**.
 - f. At this point, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
4. Once the Autopilot process begins, the Microsoft Entra sign-in page appears. At the Microsoft Entra sign-in page, if a user was assigned to the device, their username might be pre-populated in this screen. Enter the Microsoft Entra credentials for the user.
- If on-premises domain end-user credentials are different from Microsoft Entra end-user credentials, make sure that **Microsoft Entra end-user credentials** are used to sign in at this step. Don't use on-premises credentials to sign in at this step.
5. Once the credentials are entered, select **Next** (Windows 10) or **Sign in** (Windows 11) to sign in. If necessary, proceed through the multi-factor authentication (MFA) screens.
 6. After authenticating with Microsoft Entra ID, the Enrollment Status Page (ESP) appears. The ESP displays progress during the provisioning process across three phases:

- **Device preparation** (Device ESP)
- **Device setup** (Device ESP)
- **Account setup** (User ESP)

The first two phases of **Device preparation** and **Device setup** are part of the Device ESP while the final phase of **Account setup** is part of the User ESP.

7. Once the **Device setup** phase of the Device ESP is complete, user ESP begins and the **User setup** phase starts. The ESP is temporarily dismissed and the Windows sign-on screen appears:
 - a. Enter the keystroke **CTRL** + **ALT** + **DEL** to initiate Windows sign-on.
 - b. Enter the on-premises domain credentials for the end-user.

If on-premises domain end-user credentials are different from Microsoft Entra end-user credentials, make sure that the **on-premises domain end-user credentials** are used to sign into the device at this step. Don't use the Microsoft Entra end-user credentials to attempt to sign into the device at this step.

- c. Select **ENTER** on the keyboard to sign the end-user into the device.
8. The Enrollment Status Page (ESP) appears again and the **Account setup** phase of the user ESP continues.
- After a short period of time, the Microsoft Entra sign-in page might appear. Sign in with the end-user's Microsoft Entra credentials.

If on-premises domain end-user credentials are different from Microsoft Entra end-user credentials, make sure that **Microsoft Entra end-user credentials** are used to sign in at this step. Don't use on-premises credentials to sign in at this step.
 - Once the credentials are entered, select **Next**.
 - The **Stay signed in to all your apps** screen appears. Make sure that the option **Allow my organization to manage my device** is selected, and then select **OK**.
 - The **You're all set!** screen appears. Select **Done**.

 **Note**

Under certain circumstances, the Microsoft Entra sign-in and subsequent pages might not appear and the end-user might be automatically signed into Microsoft Entra ID. For example, if using [Active Directory Federation Services \(ADFS\)](#) and [single sign-on \(SSO\)](#). If the end-user is automatically signed into Microsoft Entra ID, then the Autopilot deployment will proceed on to the next step automatically.

9. Once **Account setup** and the user ESP process completes, the provisioning process completes and the ESP finishes. Select the **Sign out** button to dismiss the ESP and go to the Windows sign-on screen. At this point, the end-user can sign into the device using their on-premises domain end-user credentials and start using the device.

Deployment tips

- Before the Windows Autopilot deployment is started, Microsoft recommends having:
 - At least one type of policy and at least one application assigned to the devices.
 - At least one type of policy and at least one application assigned to the users.

These assignments ensure proper testing of the Windows Autopilot deployment during both the device ESP phase and user ESP phase of the ESP. It might also prevent possible issues when there are either no policies or no applications assigned to the devices or the users.

- Depending on how the Autopilot profile was configured at the **Create and assign Autopilot profile** step, additional screens might appear during the Autopilot deployment such as:
 - **Language/Country/Region** or **Keyboard** screens before the Microsoft Entra sign-in page.
 - **Privacy** screen when the user ESP/Account setup begins but before the Windows sign-on screen appears.
- If the device is left alone with no interaction during the **Account setup** phase of the ESP, the device might enter the Windows lock screen. If the device does enter the Windows lock screen during **Account setup** of the ESP, unlock the device by entering the keystroke **CTRL** + **ALT** + **DEL**, entering the on-premises domain credentials for the end-user, and then selecting **ENTER** on the keyboard. Unlocking the device should go back to the Enrollment Status Page (ESP) and display the current progress of **Account setup**.
- To view and hide detailed progress information in the ESP during the provisioning process:
 - **Windows 10:** To show details, next to the appropriate phase select **Show details**. To hide the details, next to the appropriate phase select **Hide details**.
 - **Windows 11:** To show details, next to the appropriate phase select **V**. To hide the details, next to the appropriate phase select **A**.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Step by step tutorial for Windows Autopilot for pre-provisioned deployment Microsoft Entra join in Intune

Article • 09/13/2024 • Applies to: Windows 11, Windows 10

This step by step tutorial guides through using Intune to perform a Windows Autopilot for pre-provisioned deployment scenario when the devices are strictly Microsoft Entra joined.

The purpose of this tutorial is a step by step guide for all the configuration steps required for a successful Autopilot for pre-provisioned deployment Microsoft Entra join deployment using Intune. The tutorial is also designed as a walkthrough in a lab or testing scenario, but can be expanded for use in a production environment.

Before beginning, refer to the [How to: Plan your Microsoft Entra join implementation](#) to make sure all requirements are met for joining devices to Microsoft Entra ID.

Note

Before attempting the Windows Autopilot pre-provisioned Microsoft Entra join scenario, Microsoft recommends that the [Windows Autopilot user-driven Microsoft Entra join](#) scenario is first configured, tested, and working. The Windows Autopilot for pre-provisioned deployment Microsoft Entra join builds on top of Windows Autopilot user-driven Microsoft Entra join scenario. If the Windows Autopilot user-driven Microsoft Entra join scenario isn't working, then most likely the Windows Autopilot pre-provisioned deployment Microsoft Entra join scenario won't work either.

Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview

Windows Autopilot for pre-provisioned deployment Microsoft Entra join is an Autopilot solution that automates the configuration of Windows on a new device delivered directly from an IT department, OEM, or reseller. Windows Autopilot for pre-provisioned deployment uses the existing Windows installation installed by the OEM at the factory.

The end-user only needs to perform a minimal number of actions during the deployment process such as:

- Powering on the device.
- In certain scenarios, selecting the language, locale, and keyboard layout.
- Connecting to a wireless network if the device isn't connected to a wired network.
- Signing into Microsoft Entra ID with the end-user's Microsoft Entra credentials.

Windows Autopilot for pre-provisioned deployment can perform the following tasks during the deployment:

- Joins the device to Microsoft Entra ID.
- Enrolls the device in Intune.
- Installs applications.
- Applies device configuration policies such as BitLocker and Windows Hello for Business.
- Checks for compliance.
- Enrollment Status Page (ESP) prevents an end-user from using the device until the device is fully configured.

Windows Autopilot for pre-provisioned deployment consists of two phases:

- Device ESP phase: Windows is configured and applications and policies assigned to the device are applied.
- User ESP phase: Applications and policies assigned to the user are applied.

Once the Windows Autopilot for pre-provisioned deployment is complete, the device is ready for the end-user to use and they're immediately sent to the desktop.

Differences between Windows Autopilot user-driven deployment and Windows Autopilot for pre-provisioned deployment

The main difference between Windows Autopilot user-driven deployment and Windows Autopilot for pre-provisioned deployment is:

- Windows Autopilot user-driven deployment: Both the Device ESP phase and the User ESP phase occur when the end-user goes through the Autopilot deployment after turning on the device for the first time.
- Windows Autopilot for pre-provisioned deployment: Device ESP phase and user ESP phase are split and occur at two different points in time.

- The IT department, OEM, or reseller handles the device ESP phase. This phase is known as the **Technician flow**. Once the Technician flow is complete, the device is powered down and delivered to the end-user.
- When the end-user receives the device, they turn it on for the first time, and the device undergoes the user ESP phase. A portion of device ESP also reruns to ensure there are no new applications or policies assigned to the device since the Technician flow ran. This phase is known as the **User flow**.

The deployment is split up between the Technician flow and User flow phases so that the deployment is faster when the end-user receives the device. The deployment is faster when the end-user receives the device because the IT department, OEM, or reseller completed the first portion of the deployment during the Technician flow.

Windows Autopilot for pre-provisioned deployment might have one disadvantage over Windows Autopilot user-driven deployment. If the OEM or reseller is unable to perform the Technician flow, then the device might need to first go to the organization's IT department to complete the Technician flow. The organization's IT department then needs to run the Technician flow once they receive the device followed by delivering the device to the end-user. This extra step prevents the device from being shipped and delivered to the end-user directly from the OEM or reseller. This extra step can lengthen the amount of time before the end-user receives the device.

Workflow

The following steps are needed to configure and then perform a Windows Autopilot for pre-provisioned deployment Microsoft Entra join in Intune:

- ✓ Step 1: Set up Windows automatic Intune enrollment
- ✓ Step 2: Allow users to join devices to Microsoft Entra ID
- ✓ Step 3: Register devices as Autopilot devices
- ✓ Step 4: Create a device group
- ✓ Step 5: Configure and assign Autopilot Enrollment Status Page (ESP)
- ✓ Step 6: Create and assign Autopilot profile
- ✓ Step 7: Assign Autopilot device to a user (optional)
- ✓ Step 8: Technician flow
- ✓ Step 9: User flow

Note

Although the workflow is designed for lab or testing scenarios, it can also be used in a production environment. Some of the steps in the workflow are

interchangeable and interchanging some of the steps might make more sense in a production environment. For example, the **Create a device group** step followed by the **Register devices as Autopilot devices** step might make more sense in a production environment.

Walkthrough

Step 1: Set up Windows automatic Intune enrollment

Related content

For more information on Windows Autopilot for pre-provisioned deployment Microsoft Entra join, see the following articles:

- [Windows Autopilot for pre-provisioned deployment](#).
- [User-driven mode for Microsoft Entra join](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: Set up Windows automatic Intune enrollment

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra join steps:

Step 1: Set up Windows automatic Intune enrollment

- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Register devices as Autopilot devices](#)
- Step 4: [Create a device group](#)
- Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 6: [Create and assign Autopilot profile](#)
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
- Step 8: [Technician flow](#)
- Step 9: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

Note

If automatic Intune enrollment is already set up, skip this step and move on to [Step 2: Allow users to join devices to Microsoft Entra ID](#).

Set up Windows automatic Intune enrollment

In order for Windows Autopilot to work, devices need to be able to enroll in Intune automatically. Enrolling devices in Intune automatically can be configured in the Azure portal:

1. Sign in to the [Azure portal](#).
2. Select **Microsoft Entra ID**.
3. In the **Overview** screen, under **Manage** in the left hand pane, select **Mobility (MDM and WIP)**.

4. In the **Mobility (MDM and WIP)** screen, under **Name** select **Microsoft Intune**.
5. In the **Microsoft Intune** page that opens, under **MDM user scope**, select either **All** or **Some**:
 - If **All** is selected, all users can automatically enroll their devices in Intune.
 - If **Some** is selected, only users in the groups specified in the link under **Groups** can automatically enroll their devices in Intune. To add groups:
 - a. Select the link under **Groups**.
 - b. In the **Select groups** window that opens, select the desired groups to add. Make sure that the groups selected are Microsoft Entra user groups that contain the desired users.
 - c. Once all of the desired groups are selected, select **Select** to close the **Select groups** window.

6. In the **Microsoft Intune** screen, if any changes were made, select **Save**.

Next step: Allow users to join devices to Microsoft Entra ID

Step 2: Allow users to join devices to Microsoft Entra ID

Related content

For more information on Windows automatic MDM/Intune enrollment, see the following articles:

- [Enable Windows automatic enrollment](#).
- [Set up Windows automatic enrollment](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: Allow users to join devices to Microsoft Entra ID

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- ✓ Step 2: **Allow users to join devices to Microsoft Entra ID**
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
 - Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 6: [Create and assign Autopilot profile](#)
 - Step 7: [Assign Autopilot device to a user \(optional\)](#)
 - Step 8: [Technician flow](#)
 - Step 9: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

Note

If users are already allowed to join devices to Microsoft Entra ID, skip this step and move on to [Step 3: Register devices as Autopilot devices](#).

Allow users to join devices to Microsoft Entra ID

In order for Windows Autopilot to work, users need to be allowed to join devices to Microsoft Entra ID. Allowing users to join devices to Microsoft Entra ID can be configured in the Azure portal:

1. Sign in to the [Azure portal](#).
2. Select Microsoft Entra ID.

3. In the **Overview** screen, under **Manage** in the left hand pane, select **Devices**.
4. In the **Devices | Overview** screen, under **Manage** in the left hand pane, select **Device Settings**.
5. In the **Devices | Device settings** screen that opens, under **Users may join devices to Microsoft Entra**, select either **All** or **Selected**:
 - If **All** is selected, all users can join their devices to Microsoft Entra ID.
 - If **Some** is selected, only users specified under **Selected** can join their devices to Microsoft Entra ID. To add users:
 - a. Select the link under **Selected**.
 - b. In the **Members allowed to join devices** page that opens:
 - i. Select **Add**.
 - ii. In the **Add members** window that opens:
 - i. Select the desired users and/or groups to add.
 - ii. Once all of the desired users and groups are selected, select **Select** to close the **Add members** window.
 - iii. Select **OK**.

⚠ Note

Any selected groups must be a Microsoft Entra group that contains user objects.

6. In the **Devices | Overview** screen, if any changes were made, select **Save**.

⚠ Note

This step of allowing users to join devices to Microsoft Entra ID is only needed for the Autopilot user-driven Microsoft Entra join and Autopilot for pre-provisioned deployment Microsoft Entra join scenarios. This setting doesn't apply to Microsoft Entra hybrid joined devices and Microsoft Entra joined devices using Windows Autopilot self-deployment mode as these methods work in a userless context.

Next step: Register devices as Autopilot devices

Step 3: Register devices as Autopilot devices

Related content

For more information on allowing users to join devices to Microsoft Entra ID, see the following articles:

- [Configure device settings.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: Register devices as Autopilot devices

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)

Step 3: Register devices as Autopilot devices

- Step 4: [Create a device group](#)
- Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 6: [Create and assign Autopilot profile](#)
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
- Step 8: [Technician flow](#)
- Step 9: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

Note

If devices are already registered as Autopilot devices, skip this step and move on to [Step 4: Create a device group](#).

Register devices as Autopilot devices

Before a device can use Autopilot, the device must be registered as an Autopilot device. Registering a device as an Autopilot device can be thought of as importing the device into Autopilot so that Autopilot service can be used on the device. Registering a device as an Autopilot device doesn't mean that the device has used the Autopilot service. It just makes the Autopilot service available to the device.

Also note that a device registered in Autopilot doesn't mean the device is enrolled in Intune. A device might be registered as an Autopilot device but might not exist in Intune. It's not until an Autopilot registered device goes through the Autopilot process for the first time that it becomes enrolled in Intune. After the Autopilot device

undergoes the Autopilot process and enrolls in Intune, the Autopilot device appears as a device in both Microsoft Entra ID and Intune.

There are several methods to register a device as an Autopilot device in Intune:

- Manually registering devices into Intune as an Autopilot device via the hardware hash. The hardware hash of a device can be collected via one of the following methods:
 - [Configuration Manager](#).
 - [PowerShell script](#).
 - [Diagnostics page hash export](#).
 - [Desktop hash export](#).

These methods of obtaining the hardware hash of a device are well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

- Automatically registering device via:
 - An [OEM](#), including [Microsoft Surface](#) devices.
 - A [partner](#).

Registering a device via an OEM or partner is also well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

For most organizations, using an OEM or partner to register devices as Autopilot devices is the preferred, most common, and most secure method. However for smaller organizations, for testing/lab scenarios, and for emergency scenarios, manually registering devices as Autopilot devices via the hardware hash is also used.

Important

The following type of devices shouldn't be registered as a Windows Autopilot device:

- [Microsoft Entra registered](#) devices, also known as "workplace joined" devices.
- [Intune MDM-only enrollment](#) devices.

These options are intended for users to join personally owned devices to their organization's network. Windows Autopilot registered devices are registered as corporate owned devices.

If a device is already one of these two types of devices, to register it as a Windows Autopilot device, first remove it from Microsoft Intune and Microsoft Entra ID. For

more information, see [Device appears as Microsoft Entra registered instead of Microsoft Entra joined](#) and [Deregister a device](#).

 **Note**

Assuming that a device isn't currently enrolled Intune, remember that registering a device in Autopilot doesn't make it an Intune enrolled device. That device doesn't enroll into Intune until Autopilot runs on the device for the first time.

Importing the hardware hash CSV file for devices into Intune

Several of the methods in the previous section on obtaining the hardware hash when manually registering devices as Autopilot devices produces a CSV file that contains the hardware hash of the device. This CSV file with the hardware hash needs to be imported into Intune to register the device as an Autopilot device.

After the CSV file is created, it can be imported into Intune via the following steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, select **Import**.
 - a. In the **Add Autopilot devices** window that opens:
 - i. Under **Specify the path to the list you want to import.**, select the blue file folder.
 - ii. Browse to the CSV file obtained using one of the above methods to obtain the hardware hash of a device.
 - iii. After selecting the CSV file, verify that the correct CSV file is selected under **Specify the path to the list you want to import.**, and then select **Import**.

Selecting **Import** closes the **Add Autopilot devices** window. Importing can take several minutes.

- b. After the import is complete, select **Sync**.

A message displays saying that the sync is in progress. The sync process might take a few minutes to complete, depending on how many devices are being synchronized.

 **Note**

If another sync is attempted within 10 minutes after initiating a sync, an error will be displayed. Syncs can only occur once every 10 minutes. To attempt a sync again, wait at least 10 minutes before trying again.

- c. Select **Refresh** to refresh the view. The newly imported devices should display within a few minutes. If the devices aren't yet displayed, wait a few minutes, and then select **Refresh** again.

Next step: Create a device group

Step 4: Create a device group

Related content

For more information on registering devices as Autopilot devices, see the following articles:

- [Manually register devices with Windows Autopilot](#).
- [Windows Autopilot customer consent](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: Create a device group

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Allow users to join devices to Microsoft Entra ID](#)
- Step 3: [Register devices as Autopilot devices](#)

Step 4: Create a device group

- Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 6: [Create and assign Autopilot profile](#)
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
- Step 8: [Technician flow](#)
- Step 9: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

Note

If device groups are already created, skip this step and move on to [Step 5: Configure and assign Autopilot Enrollment Status Page \(ESP\)](#). However, if deploying multiple different Autopilot scenarios to different devices, separate device groups are required for each Autopilot scenario.

Create a device group

Device groups are a collection of devices organized into a Microsoft Entra group. Device groups are used in Autopilot to target devices for specific configurations such as what policies to apply to a device and what applications to install on the device. They're also used by Autopilot to target Enrollment Status Page (ESP) configurations, Autopilot profile configurations, and domain join profiles to devices.

Device groups can be either dynamic or assigned:

- **Dynamic groups** - Devices are automatically added to the group based on rules

- **Assigned groups** - Devices are manually added to the group and are static

When an admin configures Autopilot in an enterprise environment, dynamic groups are primarily used since a large number of devices are normally involved. Adding the devices in automatically using rules makes management of the group a lot easier. Adding a large amount of device in manually via an assigned group would be impractical. However, if there's only a few devices, for example for testing purposes, an assigned group can be used instead.

To create a dynamic device group for use with Autopilot, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Groups** in the left hand pane.
3. In the **Groups | All groups** screen, make sure **All groups** is selected, and then select **New group**.
4. In the **New Group** screen that opens:
 - a. For **Group type**, select **Security**.
 - b. For **Group name**, enter a name for the device group.
 - c. For **Group description**, enter a description for the device group.
 - d. For **Microsoft Entra roles can be assigned to the group**, select **No**.
 - e. For **Membership type**, select **Dynamic Device**. Setting the **Membership type** option to **Dynamic Device** changes the option **Members** to **Dynamic device members**.
 - f. For **Owners**, select the **No owners selected** link.
 - g. In the **Add owners** screen that opens:
 - i. Scroll through the list of objects and select owners for the user group. Alternatively, use the **Search** bar to search for and select owners of the group.
 - ii. Once all of the desired owners are selected, select **Select**.
 - h. For **Dynamic device members**, select **Add dynamic query**. The **Dynamic membership rules** screen opens.
 - i. In the **Dynamic membership rules** screen:

- i. Make sure that **Configure Rules** is selected at the top.
- ii. Select **Add expression**. Rules and expressions can be added that defines what devices are added to the device group.

Rules can be entered in the rule builder via the drop-down boxes. Alternatively, the rule syntax can be entered directly via the **Edit** option in the **Rule syntax** section.

The most common type of dynamic device group when using Windows Autopilot is a device group that contains all Windows Autopilot devices. A dynamic device group that contains all Windows Autopilot devices has the following syntax:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```

To enter in this rule:

- i. Select the **Edit** option in the **Rule syntax** section.
- ii. Paste in the following rule in the **Edit rule syntax** screen under **Rule syntax**:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```
- iii. Once the rule is pasted in, select **OK**.
- iii. Once the desired rule is entered, select **Save** on the toolbar to close the **Dynamic membership rules** window.

For more information on creating rules for dynamic groups, see [Dynamic membership rules for groups in Microsoft Entra ID](#).

- j. Select **Create** to finish creating the dynamic device group.

Note

The above steps are creating a dynamic group in Microsoft Entra that is used by Intune and Windows Autopilot solutions. Although the groups can be accessed in the Intune portal, they're Microsoft Entra groups.

Tip

For Configuration Manager admins, device groups are similar to device based collections. Dynamic device groups are similar to query based device collections while assigned device groups are similar to direct membership device collections.

Next step: Configure and assign the Enrollment Status Page (ESP)

Step 5: Configure and assign Autopilot Enrollment Status Page (ESP)

Related content

For more information on creating groups in Intune, see the following articles:

- [Create device groups.](#)
- [Add groups to organize users and devices.](#)
- [Manage Microsoft Entra groups and group membership.](#)
- [Dynamic membership rules for groups in Microsoft Entra ID.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: Configure and assign the Enrollment Status Page (ESP)

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Autopilot for pre-provisioned deployment Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
-  **Step 5: Configure and assign Autopilot Enrollment Status Page (ESP)**
- Step 6: [Create and assign Autopilot profile](#)
 - Step 7: [Assign Autopilot device to a user \(optional\)](#)
 - Step 8: [Technician flow](#)
 - Step 9: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

Note

If an ESP is already configured and assigned from another Autopilot scenario and the same settings for the ESP should be used for the pre-provisioned Microsoft Entra join scenario, skip this step and move on to [Step 6: Create and assign Autopilot profile](#).

The Enrollment Status Page (ESP)

The main feature of the Enrollment Status Page (ESP) is to display progress and current status to the end user while the device is being set up and enrolled via the Autopilot process. The other main feature of the ESP is to block a user from signing in and using the device until all required policies and applications are installed. Multiple ESP profiles can be created with different settings and assigned appropriately based on different needs and scenarios.

Out of box there's a default ESP that is assigned to all devices. The default setting in the default ESP is to not show app and profile progress during the Autopilot process. However, Microsoft recommends changing this default via a separate custom ESP to show app and profile progress. Enabling and configuring an ESP allows end users to properly see the progress of their device being set up and prevents them using the device until the device is fully configured and provisioned. A user signing into the device before being fully configured and provisioned can cause issues.

The ESP has two phases:

- **Device ESP** - The portion of the ESP that runs during the OOB process and applies device policies and installs device applications.
- **User ESP** - The portion of the ESP that sets up user account, applies user policies, and installs user applications.

Device ESP runs first followed by the User ESP.

Tip

For Configuration Manager admins, an ESP is similar and analogous to Configuration Manager client settings.

Autopilot Enrollment Status Page (ESP) configuration options

When the Enrollment Status Page (ESP) is configured, it has several options that can be configured to meet the needs of the organization. The following lists the different options and their possible configurations:

- **Show an error when installation takes longer than specified number of minutes:**
 - The default time-out is 60 minutes. Enter a higher value if more time is needed to install applications on the devices.
- **Show custom message when time limit or error occur:**
 - **No:** The default message is shown to users when an error occurs. That message is: **Setup could not be completed. Please try again or contact your support person for help.**
 - **Yes:** A custom message is shown to users when an error occurs. Enter a custom message in the provided text box.

- Turn on log collection and diagnostics page for end users:
 - No: The collect logs button isn't shown to users when an installation error occurs. The Windows Autopilot diagnostics page isn't shown on devices running Windows 11.
 - Yes: The collect logs button is shown to users when an installation error occurs. The Windows Autopilot diagnostics page is shown on devices running Windows 11. Logs and diagnostics might aid with troubleshooting. For this reason, Microsoft recommends enabling this option.
- Only show page to devices provisioned by out-of-box experience (OOBE):
 - No: The enrollment status page (ESP) is shown during the device phase and the out-of-box experience (OOBE). The page is also shown during the user phase to every user who signs into the device for the first time.
 - Yes: The enrollment status page (ESP) is shown during the device phase and the OOBE. The page is also shown during the user phase, but only to the first user who signs into the device. It isn't shown to subsequent users who sign into the device.
- Block device use until all apps and profiles are installed:
 - No: Users can leave the ESP before Intune is finished setting up the device.
 - Yes: Users can't leave the ESP until Intune is done setting up the device. Enabling this option unlocks the following additional options:
 - Allow users to reset device if installation error occurs:
 - No: The ESP doesn't give users the option to reset their devices when an installation fails.
 - Yes: The ESP gives users the option to reset their devices when an installation fails.
 - Allow users to use device if installation error occurs:
 - No: The ESP doesn't give users the option to bypass the ESP when an installation fails.
 - Yes: The ESP gives users the option to bypass the ESP and use their devices when an installation fails.

- **Block device use until these required apps are installed if they are assigned to the user/device:**
 - **All:** All assigned apps must be installed before users can use their devices.
 - **Selected:** Selected apps must be installed before users can use their devices. After enabling this option, select **Select apps** to select the managed apps from Intune that are required to be installed before users can use their device.

Configure and assign the Enrollment Status Page (ESP)

To configure and assign the Autopilot Enrollment Status Page (ESP), follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
- 1 In the **Devices | Overview** screen, under **By platform**, select **Windows**.
 1. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
 2. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Enrollment Status Page**.
 3. In the **Enrollment Status Page** screen that opens, select **Create**.
 4. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the ESP profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.
 5. In the **Settings** page, toggle the option **Show app and profile configuration progress** to **Yes**.
 - a. After the option **Show app and profile configuration progress** is toggled to **Yes**, several new options will appear. Configure these options based on the desired behavior for the ESP as described in the section [Autopilot Enrollment Status Page \(ESP\) configuration options](#):

- b. Once the different ESP options under the **Settings** page are configured as desired, select **Next**.
6. In the **Assignments** page:
 - a. Under **Included groups**, select **Add groups**.
 - b. In the **Select groups to include** window that opens, select the device groups to target the ESP profile. The device groups selected would normally be the device groups created in the **Create device group** step.
 - c. After selecting the device group, select **Select** to close the **Select groups to include** window.

 **Tip**

After selecting the device groups, the **Edit filter** option can be selected on each device group added to the assignment to further refine what devices are targeted for the ESP profile. For example, further filtering can be useful if some of the devices that are members in the device groups selected need to be excluded.

- d. Select **Next**.

 **Note**

An ESP is assigned to a device group and not directly to individual devices. To assign an ESP to a specific device, the device must be a member of a device group that has an ESP assigned to it.

7. In the **Scope tags** page, select **Next**.

 **Note**

Scope tags are optional and are a method to control who has access to the ESP configuration. For this tutorial, scope tags are being skipped and left at the default scope tag. However if a custom scope tag needs to be specified, do so at this screen. For more information about scope tags, see [Use role-based access control and scope tags for distributed IT](#).

8. In the Review + create page, verify that the settings are correct and configured as desired. Once verified, select **Create** to save the changes and assign the ESP profile.

Next step: Create and assign a pre-provisioned Microsoft Entra join Autopilot profile

Step 6: Create and assign Autopilot profile

Related content

For more information on the Enrollment Status Page (ESP), see the following articles:

- [Windows Autopilot Enrollment Status Page](#).
- [Set up the Enrollment Status Page](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: Create and assign a pre-provisioned Microsoft Entra join Autopilot profile

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
 - Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
-  **Step 6: Create and assign Autopilot profile**
- Step 7: [Assign Autopilot device to a user \(optional\)](#)
 - Step 8: [Technician flow](#)
 - Step 9: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

Create and assign a pre-provisioned Microsoft Entra join Autopilot profile

The Autopilot profile specifies how the device is configured during Windows Setup and what is shown during the out-of-box experience (OOBE).

When an admin creates an Autopilot profile for the pre-provisioned scenario, devices with this Autopilot profile are associated with the user enrolling the device. User credentials are required to enroll the device.

The difference between an Autopilot pre-provisioned Microsoft Entra join and an Autopilot Microsoft Entra hybrid join is that the pre-provisioned Microsoft Entra join scenario only joins Microsoft Entra ID during Autopilot. The Microsoft Entra hybrid join scenario joins both an on-premises domain and Microsoft Entra ID during Autopilot.

 **Tip**

For Configuration Manager admins, the Autopilot profile is similar to some of the configuration that takes place during a task sequence via an `unattend.xml` file. The `unattend.xml` file is configured during the **Apply Windows Settings** and **Apply Network Settings** steps. Autopilot doesn't use `unattend.xml` files.

To create a pre-provisioned Microsoft Entra join Autopilot profile, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Deployment Profiles**.
6. In the **Windows Autopilot deployment profiles** screen, select the **Create Profile** drop down menu and then select **Windows PC**.
7. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the Autopilot profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.

Note

Microsoft recommends setting the option **Convert all targeted devices to Autopilot to Yes**. This tutorial concentrates on new devices where the device is manually imported as an Autopilot device using the hardware hash. However, this option can be helpful when assigning Autopilot profiles to device groups that contain existing devices. For example, this option is helpful when using the [Windows Autopilot for existing devices](#) scenario. With Windows Autopilot for existing devices, existing devices might need to be registered as an Autopilot device after the Autopilot deployment completes. For more information, see [Register device for Windows Autopilot](#).

8. In the **Out-of-box experience (OOBE)** page:

- For **Deployment mode**, select **User-driven**.
- For **Join to Microsoft Entra ID as**, select **Microsoft Entra joined**.
- For **Microsoft Software License Terms**, select **Hide** to skip the EULA page.
- For **Privacy settings**, select **Hide** to skip the privacy settings.
- For **Hide change account options**, select **Hide**.
- For **User account type**, select the desired account type for the user (**Administrator** or **Standard** user). If **Administrator** is chosen, the user is added to the local Admin group.
- For **Allow pre-provisioned deployment**, select **Yes**.
- For **Language (Region)**, select **Operating system default** to use the default language for the operating system being configured. If another language is desired, select the desired language from the drop-down list.
- For **Automatically configure keyboard**, select **Yes** to skip the keyboard selection page.
- For **Apply device name template**, select **No**. Alternatively, **Yes** can be chosen to apply a device name template. Be aware of the following if the name template is selected to **Yes**:
 - Names must be 15 characters or less, and can have letters, numbers, and hyphens.
 - Names can't be all numbers.
 - Use the [%SERIAL% macro](#) to add a hardware-specific serial number.
 - Use the [%RAND:x% macro](#) to add a random string of numbers, where x equals the number of digits to add.

 **Note**

The above settings are selected to minimize needed user interaction during device setup. However, some of the settings that are hidden can instead be shown as desired. For example, some regions might require that **Privacy settings** always be shown.

 **Note**

If the language/region and keyboard screens are set to hidden, they might still be displayed if there's no network connectivity at the start of the Autopilot deployment. When there's no network connectivity at the start of the deployment, the Autopilot profile, where the settings to hide these screens is defined, hasn't downloaded yet. Once network connectivity is established, the Autopilot profile is downloaded and any additional screen settings should work as expected.

9. Once the options in the **Out-of-box experience (OOBE)** page are configured as desired, select **Next**.
10. In the **Assignments** page:
 - a. Under **Included groups**, select **Add groups**.

 **Note**

Make sure to add the correct device groups under **Included groups** and not under **Excluded groups**. Accidentally adding the desired device groups under **Excluded groups** prevents devices in those device groups from receiving the Autopilot profile.

- a. In the **Select groups to include** window that opens, select the groups that the Windows Autopilot profile should be assigned to. These device groups are normally the device groups created in the previous **Create device group** step. Once done, select **Select**.
 - b. Under **Included groups > Groups**, ensure the correct groups are selected, and then select **Next**.
11. In the **Review + Create** page, verify that all settings are set correctly, and then select **Create** to create the Autopilot profile.

Verify device has an Autopilot profile assigned to it

Before deploying a device, ensure that an Autopilot profile is assigned to a device group that the device is a member of. Autopilot profile assignment to a device can take some time after the Autopilot profile is assigned to the device group or after the device is added to the device group. To verify that the profile is assigned to a device, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens:
 - a. Find the desired device that Autopilot deployment profile assignment status needs to be checked.
 - b. Once the device is located, its current status is listed under the **Profile status** column. The status has one of the following values:
 - **Not assigned:** An Autopilot deployment profile isn't assigned to the device.
 - **Assigning:** An Autopilot deployment profile is being assigned to the device.
 - **Assigned:** An Autopilot deployment profile is assigned to the device.
 - **Fix pending:** When a hardware change occurs on a device, this status displays while Intune tries to register the new hardware. When the link for the **Fix pending** status is selected, the following message appears:

We've detected a hardware change on this device. We're trying to automatically register the new hardware. You don't need to do anything now; the status will be updated at the next check in with the result.

If Intune is able to successfully register the new hardware, Intune updates the profile status when the device next checks into Intune. For more information on the **Fix pending** status, see the following articles:
 - [Autopilot profile not applied after reimaging to an older OS version](#).
 - [Return of key functionality for Windows Autopilot sign-in and deployment experience](#).
 - [Windows Autopilot motherboard replacement scenario guidance](#) - **Attention required:** If Intune is unable to register the new hardware after a hardware change occurs on a device, the device can't receive the Autopilot

profile until the device is reset and the device re-registers. For more information on this status and how to deregister/re-register a device, see the following articles:

- [Autopilot profile not applied after reimaging to an older OS version.](#)
- [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
- [Windows Autopilot motherboard replacement scenario guidance](#)
- [Deregister a device](#)

Before starting the Autopilot deployment process on a device, make sure that in the [Windows Autopilot devices](#) page:

- The device's **Profile status** status is **Assigned**.
- In the properties of the device, **Date assigned** has a value.
- In the properties of the device, **Assigned profile** displays the expected Autopilot profile.

Note

Intune periodically checks for new devices in the assigned device groups, and then begins the process of assigning profiles to those devices. Due to several different factors involved in the process of Autopilot profile assignment, an estimated time for the assignment can vary from scenario to scenario. These factors can include Microsoft Entra groups, membership rules, hash of a device, Intune and Autopilot services, and internet connection. The assignment time varies depending on all the factors and variables involved in a specific scenario.

Next step: Assign Autopilot device to a user (optional) or Technician flow

[Step 7: Assign Autopilot device to a user \(optional\)](#)

If a user isn't being assigned to the device, then skip to [Step 8: Technician flow](#).

[Step 8: Technician flow](#)

Related content

For more information on configuring Autopilot profiles, see the following articles:

- Configure Autopilot profiles.
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: Assign Autopilot device to a user (optional)

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
 - Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 6: [Create and assign Autopilot profile](#)
- Step 7: Assign Autopilot device to a user (optional)**
- Step 8: [Technician flow](#)
 - Step 9: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

Assign Autopilot device to a user (optional)

A device that is registered as an Autopilot device can also be assigned to a user. If an Autopilot device is assigned to a user, then any user policies and application installs assigned to that user is applied to the device during the Autopilot process.

Tip

For testing purposes, especially for hybrid Microsoft Entra scenarios, it might be better to first test an Autopilot deployment before assigning the device to a user. Not assigning a user limits the scope of applications, policies, and configurations processed during the Autopilot process.

Tip

For Configuration Manager admins, assigning a user to a device is similar to user device affinity in Configuration Manager.

To assign an Autopilot device to a user, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, locate the device to assign a user to.
7. Once the desired device is located, select the box to the left of the device, making sure that there's check mark in the box, and then select **Assign user** in the toolbar at the top of page.
8. In the **Select user** window that opens, find and select a user for the device, and then select **Select** to close the window. If necessary, use the **Search** box to find the desired user.

 **Note**

The selected user must be an Azure user licensed to use Intune.

9. In the Autopilot device's property window that automatically opens on the right hand side, under **User friendly name**, verify the default value. If the value is empty or a different friendly name is desired, enter the desired friendly name for the user under **User friendly name**, and then select **Save** to close the property window.
10. The user assignment can be verified by selecting the Autopilot device in the **Windows Autopilot devices** screen. Once the Autopilot device is selected, it highlights and the Autopilot device's property window automatically opens on the right hand side. The assigned user is listed under **User** and **User friendly name**.

Assigning Autopilot device to a user via hardware hash CSV file

A user can be manually assigned to a Windows Autopilot device in the Windows Autopilot device's properties. However, a user can also be assigned to the Autopilot device when the device was initially imported into Autopilot as an Autopilot device. Assigning a user when the device is imported as an Autopilot device can be done by editing the hardware hash CSV file and adding the **Assigned User** column after the **Hardware Hash** column. The user's User Principal Name (UPN) should then be added as a value under the **Assigned User** column.

Important

Use a plain-text editor such as **Notepad** to edit the CSV file. Don't use Microsoft Excel. Editing the CSV file in Excel doesn't generate a proper usable file for importing into Intune.

For more information on editing the CSV file to add an assigned user to the Autopilot device, see [Manually register devices with Windows Autopilot: Ensure that the CSV file meets requirements](#).

Next step: Technician flow

[Step 8: Technician flow](#)

Related content

For more information on assigning a user to an Autopilot device, see the following articles:

- [Assign a user to a specific Autopilot device](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: Technician flow

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
 - Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 6: [Create and assign Autopilot profile](#)
 - Step 7: [Assign Autopilot device to a user \(optional\)](#)
- Step 8: Technician flow**
- Step 9: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

Technician flow

Once all of the configurations for Windows Autopilot for pre-provisioned deployment are completed in Intune and in Microsoft Entra ID, the next step is to start the Windows Autopilot deployment process on the device. For Windows Autopilot for pre-provisioned deployment, the Autopilot process is split into two different phases that run at two different points in time by two different sets of individuals:

- The first phase is known as the **technician flow** and is normally run by the IT department, OEM, or reseller.
- The second phase is known as the **user flow** and is normally run by the end-user.

To start the technician flow, select a device that is part of the device group created in the previous [Create a device group](#) step, and then follow these steps:

1. If a wired network connection is available, connect the device to the wired network connection.
2. Power on the device.

3. Once the device boots up, one of two things occurs depending on the state of network connectivity:

- If the device is connected to a wired network and has network connectivity, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
- If the device isn't connected to a wired network or if it doesn't have network connectivity, it prompts to connect to a network. Connectivity to the Internet is required:
 - a. The out-of-box experience (OOBE) begins and a screen asking for a country or region appears. Select the appropriate country or region, and then select **Yes**.
 - b. The keyboard screen appears to select a keyboard layout. Select the appropriate keyboard layout, and then select **Yes**.
 - c. An additional keyboard layouts screen appears. If needed, select additional keyboard layouts via **Add layout**, or select **Skip** if no additional keyboard layouts are needed.

 **Note**

When there's no network connectivity, the device can't download the Autopilot profile to know what country/region and keyboard settings to use. For this reason, when there's no network connectivity, the country/region and keyboard screens appear even if these screens are set to hidden in the Autopilot profile. These settings need to be specified in these screens in order for the network connectivity screens that follow to work properly.

- d. The **Let's connect you to a network** screen appears. At this screen, either plug the device into a wired network (if available), or select and connect to a wireless Wi-Fi network.
- e. Once network connectivity is established, the **Next** button should become available. Select **Next**.
- f. At this point, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.

4. At the Microsoft Entra sign-in page, DON'T sign in or select the **Next/Sign in** button. Instead, press the **WIN** key on the keyboard five times. Pressing the **WIN** key five times should display a **What would you like to do?** options screen instead.

5. From the **What would you like to do?** options screen:

- For Windows 10, select the **Windows Autopilot provisioning** option, and then select **Continue**.
- For Windows 11, select the **Pre-provision with Windows Autopilot** option, and then select **Next**.

6. In the **Windows Autopilot Configuration** screen (Windows 10) or the **Pre-provision with Windows Autopilot** screen (Windows 11), it displays the following information about the deployment:

- The name of the organization for the device.
- The name of the Autopilot deployment profile assigned to the device during the **Create and assign Autopilot profile** step.
- The user assigned to the device if a user was assigned to the device in the **Assign Autopilot device to a user (optional)** step (if applicable).
- A QR code containing a unique identifier for the device. This code can be used to look up the device in Intune to perform actions such as verifying configurations, make any necessary changes, etc.

7. Validate that the information in the **Windows Autopilot Configuration** screen is correct. Once all information is confirmed as correct, select **Provision** (Windows 10) or **Next** (Windows 11) to begin the provisioning process.

8. The device might reboot, followed by the Enrollment Status Page (ESP) appearing. The Enrollment Status Page (ESP) displays progress during the provisioning process across three phases:

- **Device preparation** (Device ESP)
- **Device setup** (Device ESP)
- **Account setup** (User ESP)

The first two phases of **Device preparation** and **Device setup** are part of the Device ESP while the final phase of **Account setup** is part of the User ESP.

For technician flow of the Windows Autopilot for pre-provisioned deployment, only the first two Device ESP phases of **Device preparation** and **Device setup** run.

The last User ESP phase of **Account setup** will run during the next step of **User flow**.

9. Once **Device setup** and the device ESP process completes, a status screen is displayed showing whether the provisioning process either succeeded or failed:

- If the pre-provisioning process completes successfully, a success status screen appears with information about the deployment. Information presented includes the previously presented information of organization name, Autopilot deployment profile name, QR code (Windows 10 only), and if applicable, assigned user. The elapsed time of the provisioning process is also provided.

Select **Reseal** to shut down the device. At that point, the device can be delivered to the end-user.

 **Important**

Outside of testing scenarios, if the intention is to deliver the device to an end-user, **DON'T** turn the device back on at this point. Instead, deliver the device to the end-user where they perform the last step of **User flow**.

- If the pre-provisioning process fails, an error status screen appears with information about why the deployment failed including an error. The error screen also displays the previously presented information of organization name, Autopilot deployment profile name, QR code (Windows 10 only), and if applicable, assigned user. The elapsed time of the provisioning process is also provided.

From this screen, diagnostic logs can be gathered from the device to troubleshoot the issue by using the following methods:

- In Windows 10, select **View diagnostics**.
- In Windows 11, enter the keystroke **CTRL + SHIFT + D** and then select **Export Logs**.

If the issue can be easily fixed, for example resolving network connectivity, then select the **Retry** button to retry provisioning the device. Otherwise if the issue can't be immediately fixed or can't be fixed without a reset, then select the **Reset** button so that the process starts over again.

Technician flow tips

- Before the Windows Autopilot deployment is started, Microsoft recommends having:
 - At least one type of policy and at least one application assigned to the devices.
 - At least one type of policy and at least one application assigned to the users.

These assignments ensure proper testing of the Windows Autopilot deployment during both the device ESP phase and user ESP phase of the ESP. It might also prevent possible issues when there are either no policies or no applications assigned to the devices or the users.

- Depending on how the Autopilot profile was configured at the **Create and assign Autopilot profile** step, additional screens might appear during the Autopilot deployment before the Microsoft Entra sign-in page such as:
 - **Language/Country/Region.**
 - **Keyboard.**
 - **License Terms.**
- The QR codes can be scanned using a companion app. The app can be used to assign a user to the device. The Autopilot team published to GitHub an [open-source sample of the companion app](#) that integrates with Intune using the Graph API.
- To view and hide detailed progress information in the ESP during the provisioning process:
 - **Windows 10:** To show details, next to the appropriate phase select **Show details**. To hide the details, next to the appropriate phase select **Hide details**.
 - **Windows 11:** To show details, next to the appropriate phase select v. To hide the details, next to the appropriate phase select \wedge .
- The technician flow inherits behavior from [self-deploying mode](#). Self-deploying mode uses the Enrollment Status Page (ESP) to hold the device in a provisioning state. It also prevents the user from proceeding to the desktop after enrollment but before applications and configurations are done applying. If the ESP is disabled, the **Reseal** button might appear before applications and configurations are done applying. Disabling the ESP might inadvertently allow proceeding to the user flow before technician flow provisioning is complete. The success status screen validates that enrollment was successful, not that the technician flow is

necessarily complete. For this reason, Microsoft recommends not to disable the ESP. Instead enable the ESP as suggested in the **Configure and assign Autopilot Enrollment Status Page (ESP)** step.

Next step: User flow

Step 8: User flow

Related content

For more information on the technician flow of a Windows Autopilot for pre-provisioned deployment, see the following articles:

- [Technician flow](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra join: User flow

Article • 07/23/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Allow users to join devices to Microsoft Entra ID](#)
 - Step 3: [Register devices as Autopilot devices](#)
 - Step 4: [Create a device group](#)
 - Step 5: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 6: [Create and assign Autopilot profile](#)
 - Step 7: [Assign Autopilot device to a user \(optional\)](#)
 - Step 8: [Technician flow](#)
-  **Step 9: User flow**

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra join overview](#).

User flow

Once the technician flow step of the pre-provisioning process completes successfully and the device is resealed, the device can be delivered to the end-user. The end-user then completes the normal Windows Autopilot user-driven process. This final step is known as the user flow and involves the following steps:

1. If a wired network connection is available, connect the device to the wired network connection.
2. Power on the device.
3. Once the device boots up, one of two things occurs depending on the state of network connectivity:
 - If the device is connected to a wired network and has network connectivity, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.

- If the device isn't connected to a wired network or if it doesn't have network connectivity, it prompts to connect to a network. Connectivity to the Internet is required:
 - a. The out-of-box experience (OOBE) begins and a screen asking for a country or region appears. Select the appropriate country or region, and then select **Yes**.
 - b. The keyboard screen appears to select a keyboard layout. Select the appropriate keyboard layout, and then select **Yes**.
 - c. An additional keyboard layouts screen appears. If needed, select additional keyboard layouts via **Add layout**, or select **Skip** if no additional keyboard layouts are needed.

 **Note**

When there's no network connectivity, the device can't download the Autopilot profile to know what country/region and keyboard settings to use. For this reason, when there's no network connectivity, the country/region and keyboard screens appear even if these screens are set to hidden in the Autopilot profile. These settings need to be specified in these screens in order for the network connectivity screens that follow to work properly.

- d. The **Let's connect you to a network** screen appears. At this screen, either plug the device into a wired network (if available), or select and connect to a wireless Wi-Fi network.
 - e. Once network connectivity is established, the **Next** button should become available. Select **Next**.
 - f. At this point, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
4. Once the Autopilot process begins, the Microsoft Entra sign-in page appears. At the Microsoft Entra sign-in page, if a user was assigned to the device, their username might be pre-populated in this screen. Enter the Microsoft Entra credentials for the user and then select **Next** (Windows 10) or **Sign in** (Windows 11) to sign in. If necessary, proceed through the multi-factor authentication (MFA) screens.

5. After authenticating with Microsoft Entra ID, the Enrollment Status Page (ESP) appears. The Enrollment Status Page (ESP) appears. The Enrollment Status Page (ESP) displays progress during the provisioning process across three phases:

- **Device preparation** (Device ESP)
- **Device setup** (Device ESP)
- **Account setup** (User ESP)

The first two phases of **Device preparation** and **Device setup** are part of the Device ESP while the final phase of **Account setup** is part of the User ESP.

For the user flow of Windows Autopilot for pre-provisioned deployment, the **Device setup** phase of the Device ESP and the **Account setup** phase of the User ESP runs. The **Device preparation** phase of the Device ESP doesn't run during the user flow since it already ran during the [Technician flow](#).

The **Device setup** phase of the Device ESP runs again during the user flow in case any new or additional policies or applications assigned to the device became available between the technician flow phase and the user flow phase.

6. Once **Account setup** and the user ESP process completes, the provisioning process completes, the ESP finishes, and the desktop appears. At this point, the end-user can start using the device.

User-flow tips

- Depending on how the Autopilot profile was configured at the **Create and assign Autopilot profile** step, additional screens might appear during the Autopilot deployment appear such as:
 - **Language/Country/Region** or **Keyboard** screens before the Microsoft Entra sign-in page.
 - **Privacy** screen when the user ESP/**Account setup** begins but before the user is automatically signed in.
- To view and hide detailed progress information in the ESP during the provisioning process:
 - **Windows 10**: To show details, next to the appropriate phase select **Show details**. To hide the details, next to the appropriate phase select **Hide details**.
 - **Windows 11**: To show details, next to the appropriate phase select **v**. To hide the details, next to the appropriate phase select **Λ**.

- For tokens to refresh properly between the Technician flow and the User flow, wait at least 90 minutes after running the Technician flow before running the User flow. This scenario mainly affects lab and testing scenarios, such as this tutorial, when the User flow is run within 90 minutes after the Technician flow completes.
- The User flow should be run within six months after the Technician flow finishes. Waiting more than six months can cause the certificates used by the Intune Management Engine (IME) to no longer be valid leading to errors such as:

```
Error code: [Win32App][DetectionActionHandler] Detection for policy with id:  
<policy_id> resulted in action status: Failed and detection state:  
NotComputed.
```

- Compliance in Microsoft Entra ID is reset during the User flow. Devices might show as compliant in Microsoft Entra ID after the Technician flow completes, but then show as noncompliant once the User flow starts. Allow enough time after the User flow completes for compliance to reevaluate and update.

Related content

For more information on the user flow of a Windows Autopilot for pre-provisioned deployment, see the following articles:

- [User flow](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Step by step tutorial for Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join in Intune

Article • 09/13/2024 • Applies to:  Windows 11,  Windows 10

Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. For more information, see [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization](#).

This step by step tutorial guides through using Intune to perform a Windows Autopilot for pre-provisioned deployment scenario when the devices are also joined to an on-premises domain, also known as Microsoft Entra hybrid join.

The purpose of this tutorial is a step by step guide for all the configuration steps required for a successful Autopilot for pre-provisioned deployment Microsoft Entra hybrid join deployment using Intune. The tutorial is also designed as a walkthrough in a lab or testing scenario, but can be expanded for use in a production environment.

Before beginning, refer to the [Plan your Microsoft Entra hybrid join implementation](#) to make sure all requirements are met for joining on-premises AD devices to Microsoft Entra ID.

Note

Before attempting the Windows Autopilot pre-provisioned Microsoft Entra hybrid join scenario, Microsoft recommends that the [Windows Autopilot user-driven Microsoft Entra hybrid join](#) scenario is first configured, tested, and working. The Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join builds on top of Windows Autopilot user-driven Microsoft Entra hybrid join scenario. If the Windows Autopilot user-driven Microsoft Entra hybrid join scenario isn't working, then most likely the Windows Autopilot pre-provisioned deployment Microsoft Entra hybrid join scenario won't work either.

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join is an Autopilot solution that automates the configuration of Windows on a new device. The device is normally delivered directly from one of the following sources to the end user:

- IT department.
- OEM.
- Reseller.

Windows Autopilot for pre-provisioned deployment uses the existing Windows installation installed by the OEM at the factory. The end-user only needs to perform a minimal number of actions during the deployment process such as:

- Powering on the device.
- In certain scenarios, selecting the language, locale, and keyboard layout.
- Connecting to a wireless network if the device isn't connected to a wired network.
- Signing into the device with the end-user's on-premises domain credentials.
- In certain scenarios, signing into Microsoft Entra ID with the end-user's Microsoft Entra credentials.

Windows Autopilot for pre-provisioned deployment can perform the following tasks during the deployment:

- Joins the device to an on-premises domain.
- Registers the device with Microsoft Entra ID.
- Enrolls the device in Intune.
- Installs applications.
- Applies device configuration policies such as BitLocker and Windows Hello for Business.
- Checks for compliance.
- The Enrollment Status Page (ESP) prevents an end-user from using the device until the device is fully configured.

Windows Autopilot for pre-provisioned deployment consists of two phases:

- Device ESP phase: Windows is configured and applications and policies assigned to the device are applied.
- User ESP phase: End-user signs into the device for the first time using on-premises domain credentials and applications and policies assigned to the user are applied.

Once the Windows Autopilot for pre-provisioned deployment is complete, the device is ready for the end-user to use. The Autopilot deployment prompts the end-user to sign out of the device. Once the device is signed out, the end-user can sign back in with their on-premises domain credentials and begin to use the device.

Differences between Windows Autopilot user-driven deployment and Windows Autopilot for pre-provisioned deployment

The main difference between Windows Autopilot user-driven deployment and Windows Autopilot for pre-provisioned deployment is:

- Windows Autopilot user-driven deployment: Both the Device ESP phase and the User ESP phase occur when the end-user goes through the Autopilot deployment after turning on the device for the first time.
- Windows Autopilot for pre-provisioned deployment: Device ESP phase and user ESP phase are split and occur at two different points in time.
 - The IT department, OEM, or reseller handles the device ESP phase. This phase is known as the **Technician flow**. Once the Technician flow is complete, the device is powered down and delivered to the end-user.
 - When the end-user receives the device, they turn it on for the first time, and the device undergoes the user ESP phase. A portion of device ESP also reruns to ensure there are no new applications or policies assigned to the device since the Technician flow ran. This phase is known as the **User flow**.

The deployment is split up between the Technician flow and User flow phases so that the deployment is faster when the end-user receives the device. The deployment is faster when the end-user receives the device because the IT department, OEM, or reseller completed the first portion of the deployment during the Technician flow.

There's one possible disadvantage of Windows Autopilot for pre-provisioned deployment over Windows Autopilot user-driven deployment. If the OEM or reseller is unable to perform the Technician flow, then the device might need to first go to the organization's IT department. The organization's IT department then needs to run the Technician flow once they receive the device followed by delivering the device to the end-user. This extra step prevents the device from being shipped and delivered to the end-user directly from the OEM or reseller. This extra step can lengthen the amount of time before the end-user receives the device.

Workflow

The following steps are needed to configure and then perform a Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join in Intune:

- ✓ Step 1: Set up Windows automatic Intune enrollment
- ✓ Step 2: Install the Intune Connector
- ✓ Step 3: Increase the computer account limit in the Organizational Unit (OU)
- ✓ Step 4: Register devices as Autopilot devices
- ✓ Step 5: Create a device group
- ✓ Step 6: Configure and assign Autopilot Enrollment Status Page (ESP)
- ✓ Step 7: Create and assign Microsoft Entra hybrid join Autopilot profile
- ✓ Step 8: Configure and assign domain join profile
- ✓ Step 9: Assign Autopilot device to a user (optional)
- ✓ Step 10: Technician flow
- ✓ Step 11: User flow

ⓘ Note

Although the workflow is designed for lab or testing scenarios, it can also be used in a production environment. Some of the steps in the workflow are interchangeable and interchanging some of the steps might make more sense in a production environment. For example, the **Create a device group** step followed by the **Register devices as Autopilot devices** step might make more sense in a production environment.

Walkthrough

Step 1: Set up Windows automatic Intune enrollment

Related content

For more information on Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join, see the following articles:

- [Windows Autopilot for pre-provisioned deployment.](#)
- [Deploy Microsoft Entra hybrid joined devices by using Intune and Windows Autopilot.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra hybrid join: Set up Windows automatic Intune enrollment

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

Step 1: Set up Windows automatic Intune enrollment

- Step 2: [Install the Intune Connector](#)
- Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
- Step 4: [Register devices as Autopilot devices](#)
- Step 5: [Create a device group](#)
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
- Step 8: [Configure and assign domain join profile](#)
- Step 9: [Assign Autopilot device to a user \(optional\)](#)
- Step 10: [Technician flow](#)
- Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Note

If automatic Intune enrollment is already set up, skip this step and move on to [Step 2: Install the Intune Connector](#).

Set up Windows automatic Intune enrollment

In order for Windows Autopilot to work, devices need to be able to enroll in Intune automatically. Enrolling devices in Intune automatically can be configured in the Azure portal:

1. Sign in to the [Azure portal](#).
2. Select **Microsoft Entra ID**.

3. In the **Overview** screen, under **Manage** in the left hand pane, select **Mobility (MDM and WIP)**.
4. In the **Mobility (MDM and WIP)** screen, under **Name** select **Microsoft Intune**.
5. In the **Microsoft Intune** page that opens, under **MDM user scope**, select either **All** or **Some**:
 - If **All** is selected, all users can automatically enroll their devices in Intune.
 - If **Some** is selected, only users in the groups specified in the link under **Groups** can automatically enroll their devices in Intune. To add groups:
 - a. Select the link under **Groups**.
 - b. In the **Select groups** window that opens, select the desired groups to add. Make sure that the groups selected are Microsoft Entra user groups that contain the desired users.
 - c. Once all of the desired groups are selected, select **Select** to close the **Select groups** window.
6. In the **Microsoft Intune** screen, if any changes were made, select **Save**.

Next step: Install the Intune Connector

[Step 2: Install the Intune Connector](#)

Related content

For more information on Windows automatic MDM/Intune enrollment, see the following articles:

- [Enable Windows automatic enrollment](#).
- [Set up Windows automatic enrollment](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra hybrid join: Install the Intune Connector

Article • 02/27/2025 •

Applies Windows 11, Windows 10, Windows Server 2022, Windows Server 2019, to: Windows Server 2016

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- ✓ **Step 2: Install the Intune Connector**
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Windows Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Windows Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Windows Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Windows Autopilot device to a user \(optional\)](#)
 - Step 10: [Technician flow](#)
 - Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

ⓘ Note

If the Intune Connector is already installed and configured, skip this step and move on to [Step 3: Increase the computer account limit in the Organizational Unit \(OU\)](#).

Install the Intune Connector for Active Directory

The purpose of the Intune Connector for Active Directory, also known as the Offline Domain Join (ODJ) Connector, is to join computers to an on-premises domain during the Windows Autopilot process. The Intune Connector for Active Directory creates

computer objects in a specified Organizational Unit (OU) in Active Directory during the domain join process.

Important

Starting with Intune 2501, Intune uses an updated Intune Connector for Active Directory that strengthens security and follows least privilege principles by using a [Managed Service Account \(MSA\)](#). When the Intune Connector for Active Directory is downloaded from within Intune, the updated Intune Connector for Active Directory is downloaded. The previous legacy Intune Connector for Active Directory is still available for download at [Intune Connector for Active Directory](#), but Microsoft recommends using the updated Intune Connector for Active Directory installer going forward. The previous legacy Intune Connector for Active Directory will continue to work through sometime in May 2025. However, it needs to be updated to the updated Intune Connector for Active Directory before then to avoid loss of functionality. For more information, see [Intune Connector for Active Directory with low-privileged account for Autopilot Hybrid Microsoft Entra join deployments](#).

Updating of the Intune Connector for Active Directory to the updated version isn't done automatically. The legacy Intune Connector for Active Directory needs to be manually uninstalled followed by the updated connector manually downloaded and installed. Instructions for the manual uninstall and install process of the Intune Connector for Active Directory are provided in the following sections.

Select the tab that corresponds to the version of the Intune Connector for Active Directory that is being installed:



Updated Connector

Before beginning the installation, make sure that all of the [Intune connector server requirements](#) are met.

Tip

It's preferable, but not required, that the administrator installing and configuring the Intune Connector for Active Directory has appropriate domain rights as documented in [Intune Connector for Active Directory requirements](#). This requirement allows the Intune Connector for Active Directory installer and configuration process to properly set permissions for the MSA on the Computer container or OUs where computer objects are created. If the

administrator doesn't have these permissions, an administrator that does have the appropriate permissions needs to follow the section [Increase the computer account limit in the Organizational Unit](#).

Turn off Internet Explorer Enhanced Security Configuration

By default Windows Server has Internet Explorer Enhanced Security Configuration turned on. Internet Explorer Enhanced Security Configuration might cause problems signing into the Intune Connector for Active Directory. Since Internet Explorer is deprecated and in most instances, not even installed on Windows Server, Microsoft recommends turning off Internet Explorer Enhanced Security Configuration. To turn off Internet Explorer Enhanced Security Configuration:

1. Sign into the server where the Intune Connector for Active Directory is being installed with an account that has local administrator rights.
2. Open **Server Manager**.
3. In the left pane of Server Manager, select **Local Server**.
4. In the right **PROPERTIES** pane of Server Manager, select the **On or Off** link next to **IE Enhanced Security Configuration**.
5. In the **Internet Explorer Enhanced Security Configuration** window, select **Off** under **Administrators:**, and then select **OK**.

Download the Intune Connector for Active Directory

1. On the server where the Intune Connector for Active Directory is being installed, sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Intune Connector for Active Directory**.
6. In the **Intune Connector for Active Directory** screen, select **Add**.

7. In the **Add connector** window that opens, under **Configuring the Intune Connector for Active Directory**, select **Download the on-premises Intune Connector for Active Directory**. The link downloads a file called `ODJConnectorBootstrapper.exe`.

Install the Intune Connector for Active Directory on the server

Important

The Intune Connector for Active Directory installation needs to be done with an account that has the following domain rights:

- **Required** - Create **msDs-ManagedServiceAccount** objects in the Managed Service Accounts container.
- **Optional** - Modify permissions in OUs in Active Directory - if the administrator installing the updated Intune Connector for Active Directory doesn't have this right, additional configuration steps are required by an administrator who has these rights. For more information, see the step/section **Increase the computer account limit in the Organizational Unit**.

1. Sign into the server where the Intune Connector for Active Directory is being installed with an account that has local administrator rights.
2. If the previous legacy Intune Connector for Active Directory is installed, uninstall it first before installing the updated Intune Connector for Active Directory. For more information, see [Uninstall the Intune Connector for Active Directory](#).

Important

When uninstalling the previous legacy Intune Connector for Active Directory, make sure to run the legacy **Intune Connector for Active Directory** installer as part of the uninstall process. If the legacy Intune Connector for Active Directory installer prompts to **Uninstall** it when it's run, select to uninstall it. This step ensures that the previous legacy Intune Connector for Active Directory is fully uninstalled. The legacy Intune Connector for Active Directory installer can be downloaded from [Intune Connector for Active Directory](#).

💡 Tip

In domains with only a single Intune Connector for Active Directory, Microsoft recommends first installing the updated Intune Connector for Active Directory on another server. Installing the updated Intune Connector for Active Directory on another server should be done before uninstalling the legacy Intune Connector for Active Directory on the current server. Installing the Intune Connector for Active Directory on another first avoids any downtime while the Intune Connector for Active Directory is being updated on the current server.

3. Open the `ODJConnectorBootstrapper.exe` file that downloaded to launch the **Intune Connector for Active Directory Setup** install.
4. Step through the **Intune Connector for Active Directory Setup** install.
5. At the end of the install, select the checkbox **Launch Intune Connector for Active Directory**.

⚠ Note

If **Intune Connector for Active Directory Setup** install is accidentally closed without selecting the checkbox **Launch Intune Connector for Active Directory**, the **Intune Connector for Active Directory** configuration can be reopened by selecting **Intune Connector for Active Directory > Intune Connector for Active Directory** from the **Start** menu.

Sign in to the Intune Connector for Active Directory

1. In the **Intune Connector for Active Directory** window, under the **Enrollment** tab, select **Sign In**.
2. Under the **Sign In** tab, sign in with the Microsoft Entra ID credentials of an Intune administrator role. The user account must have an assigned Intune license. The sign in process might take a few minutes to complete.

⚠ Note

The account used to enroll the Intune Connector for Active Directory is only a temporary requirement at the time of installation. The account isn't

used going forward after the server is enrolled.

3. Once the sign in process completes:
 - a. A **The Intune Connector for Active Directory successfully enrolled** confirmation window appears. Select **OK** to close the window.
 - b. An **A Managed Service Account with name "<MSA_name>" was successfully set up** confirmation window appears. The name of the MSA is in the format `msa0DJ#####` where ##### are five random characters. Notate the name of the MSA that was created, and then select **OK** to close the window. The name of the MSA might be needed later to configure the MSA to allow creating computer objects in OUs.
4. The **Enrollment** tab shows **Intune Connector for Active Directory** is enrolled. The **Sign In** button is greyed out and **Configure Managed Service Account** is enabled.
5. Close the **Intune Connector for Active Directory** window.

Verify the Intune Connector for Active Directory is active

After authenticating, the Intune Connector for Active Directory finishes installing. Once it finishes installing, verify that it's active in Intune by following these steps:

1. Go to the [Microsoft Intune admin center](#) if it's still open. If the **Add connector** window is still displayed, close it.

If the **Microsoft Intune admin center** isn't still open:

 - a. Sign into the [Microsoft Intune admin center](#).
 - b. In the **Home** screen, select **Devices** in the left hand pane.
 - c. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
 - d. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
 - e. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Intune Connector for Active Directory**.
2. In the **Intune Connector for Active Directory** page:
 - Confirm that the server is displayed under **Connector name** and shows as **Active** under **Status**

- For the updated Intune Connector for Active Directory, make sure the version is greater than 6.2501.2000.5.

If the server isn't displayed, select **Refresh** or navigate away from the page, and then navigate back to the **Intune Connector for Active Directory** page.

① Note

- It can take several minutes for the newly enrolled server to appear in the **Intune Connector for Active Directory** page of the [Microsoft Intune admin center](#). The enrolled server only appears if it can successfully communicate with the Intune service.
- Inactive Intune Connectors for Active Directory still appear in the **Intune Connector for Active Directory** page and will automatically be cleaned up after 30 days.

After the Intune Connector for Active Directory is installed, it will start logging in the **Event Viewer** under the path **Applications and Services Logs > Microsoft > Intune > ODJConnectorService**. Under this path, **Admin** and **Operational** logs can be found.

Configure the MSA to allow creating objects in OUs (optional)

By default, MSAs only have access to create computer objects in the **Computers** container. MSAs don't have access to create computer objects in Organizational Units (OUs). To allow the MSA to create objects in OUs, the OUs need to be added to the `ODJConnectorEnrollmentWiazard.exe.config` XML file found in `ODJConnectorEnrollmentWizard` directory where the Intune Connector for Active Directory was installed, normally `C:\Program Files\Microsoft Intune\ODJConnector\`.

To configure the MSA to allow creating objects in OUs, follow these steps:

1. On the server where the Intune Connector for Active Directory is installed, navigate to `ODJConnectorEnrollmentWizard` directory where the Intune Connector for Active Directory was installed, normally `C:\Program Files\Microsoft Intune\ODJConnector\`.
2. In the `ODJConnectorEnrollmentWizard` directory, open the `ODJConnectorEnrollmentWiazard.exe.config` XML file in a text editor, for

example, Notepad.

3. In the `ODJConnectorEnrollmentWiazaard.exe.config` XML file, add in any desired OUs that the MSA should have access to create computer objects in. The OU name should be the distinguished name and if applicable, needs to be escaped. The following example is an example XML entry with the OU distinguished name:

XML

```
<appSettings>

    <!-- Semicolon separated list of OUs that will be used for
        Hybrid Autopilot, using LDAP distinguished name format.
        The ODJ Connector will only have permission to create
        computer objects in these OUs.

        The value here should be the same as the value in the
        Hybrid Autopilot configuration profile in the Azure portal -
        https://learn.microsoft.com/en-us/mem/intune/configuration/domain-
        join-configure

        Usage example (NOTE: PLEASE ENSURE THAT THE DISTINGUISHED
        NAME IS ESCAPED PROPERLY):
        Domain contains the following OUs:
        - OU=HybridDevices,DC=contoso,DC=com
        -
        OU=HybridDevices2,OU=IntermediateOU,OU=TopLevelOU,DC=contoso,DC=com

        Value:
        "OU=HybridDevices,DC=contoso,DC=com;OU=HybridDevices2,OU=Intermedia
        teOU,OU=TopLevelOU,DC=contoso,DC=com" -->

    <add key="OrganizationalUnitsUsedForOfflineDomainJoin"
        value="OU=SubOU,OU=TopLevelOU,DC=contoso,DC=com;OU=Mine,DC=contoso,
        DC=com" />
</appSettings>
```

4. Once all desired OUs are added, save the

`ODJConnectorEnrollmentWiazaard.exe.config` XML file.

5. As an administrator that has appropriate permissions to modify OU permissions, open the **Intune Connector for Active Directory** by navigating to **Intune Connector for Active Directory > Intune Connector for Active Directory** from the **Start** menu.

 **Important**

If the administrator installing and configuring the Intune Connector for Active Directory doesn't have permissions to modify OU permissions, then the section/steps **Increase the computer account limit in the Organizational Unit** need to be followed instead by an administrator that does have permissions to modify OU permissions.

6. Under the **Enrollment** tab in the **Intune Connector for Active Directory** window, select **Configure Managed Service Account**.
7. An **A Managed Service Account with name "<MSA_name>" was successfully set up** confirmation window appears. Select **OK** to close the window.

Next step: Increase the computer account limit in the Organizational Unit (OU)

Step 3: Increase the computer account limit in the Organizational Unit (OU)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra hybrid join: Increase the computer account limit in the Organizational Unit (OU)

Article • 02/27/2025 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Install the Intune Connector](#)
- ✓ Step 3: **Increase the computer account limit in the Organizational Unit (OU)**
 - Step 4: [Register devices as Windows Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Windows Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Windows Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Windows Autopilot device to a user \(optional\)](#)
 - Step 10: [Technician flow](#)
 - Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Note

If the computer account limit for the proper Organizational Unit (OU) is already increased, skip this step and move on to [Step 4: Register devices as Windows Autopilot devices](#).

Increase the computer account limit in the Organizational Unit (OU)

Updated Connector

Important

This step is only needed under one of the following conditions:

- The administrator that installed and configured the Intune Connector for Active Directory didn't have appropriate rights as outlined in [Intune Connector for Active Directory Requirements](#).
- The `ODJConnectorEnrollmentWiazard.exe.config` XML file wasn't modified to add OUs that the MSA should have permissions for.

The purpose of Intune Connector for Active Directory is to join computers to a domain and add them to an OU. For this reason, the [Managed Service Account \(MSA\)](#) being used for the Intune Connector for Active Directory needs to have permissions to create computer accounts in the OU where the computers are joined to the on-premises domain.

With default permissions in Active Directory, domain joins by the Intune Connector for Active Directory might initially work without any permission modifications to the OU in Active Directory. However after MSA attempts to join more than 10 computers to the on-premises domain, it would stop working because by default, Active Directory only allows any single account to join up to 10 computers to the on-premises domain.

The following users aren't restricted by the 10 computer domain join limitation:

- Users in the Administrators or Domain Administrators groups: In order to comply with the least privilege principles model, Microsoft doesn't recommend making the MSA an administrator or domain administrator.
- Users with delegated permissions on Organizational Unit (OUs) and containers in Active Directory to create computer accounts: This method is recommended since it follows the least privilege principles model.

To fix this limitation, the MSA needs the **Create computer accounts** permission in the Organizational Unit (OU) where the computers are joined to in the on-premises domain. The Intune Connector for Active Directory sets the permissions for the MSAs to the OUs as long as one of the following conditions is met:

- The administrator installing the Intune Connector for Active Directory has the necessary permissions to set permissions on the OUs.
- The administrator configuring the Intune Connector for Active Directory has the necessary permissions to set permissions on the OUs.

If the administrator installing or configuring the Intune Connector for Active Directory doesn't have the necessary permissions to set permissions on the OUs,

then the following steps need to be followed:

1. Sign into a computer that has access to the **Active Directory Users and Computers** console with an account that has the necessary permissions to set permissions on OUs.
2. Open the **Active Directory Users and Computers** console by running **DSA.msc**.
3. Expand the desired domain and navigate to the organizational unit (OU) that computers are joining to during Windows Autopilot.

 **Note**

The OU that computers join during the Windows Autopilot deployment is specified later during the **Configure and assign domain join profile** step.

4. Right-click on the OU and select **Properties**.

 **Note**

If computers are joining the default **Computers** container instead of an OU, right-click on the **Computers** container and select **Delegate Control**.

5. In the OU **Properties** window that opens, select the **Security** tab.
6. In the **Security** tab, select **Advanced**.
7. In the **Advanced Security Settings** window, select **Add**.
8. In the **Permission Entry** window, next to **Principal**, select the **Select a principal** link.
9. In the **Select User, Computer, Service Account, or Group** window, select the **Object Types...** button.
10. In the **Object Types** window, select the **Service Accounts** check box, and then select **OK**.
11. In the **Select User, Computer, Service Account, or Group** window, under **Enter the object name to select**, enter the name of the MSA being used for the Intune Connector for Active Directory.

Tip

The MSA was created during the **Install the Intune Connector for Active Directory** step/section and has the name format of `msaODJ#####` where ##### are five random characters. If the MSA name isn't known, follow these steps to find the MSA name:

- a. On the server running the Intune Connector for Active Directory, right-click on the **Start** menu and then select **Computer Management**.
- b. In the **Computer Management** window, expand **Services and Applications** and then select **Services**.
- c. In the results pane, locate the service with the name **Intune ODJConnector for Active Service**. The name of the MSA is listed in the **Log On As** column.

12. Select **Check Names** to validate the MSA name entry. Once the entry is validated, select **OK**.
13. In the **Permission Entry** windows, select the **Applies to:** drop-down menu and then select **This object only**.
14. Under **Permissions**, unselect all items, and then only select the **Create Computer objects** check box.
15. Select **OK** to close the **Permission Entry** window.
16. In the **Advanced Security Settings** window, select either **Apply** or **OK** to apply the changes.

Next step: Register devices as Windows Autopilot devices

Step 4: Register devices as Windows Autopilot devices

Related content

For more information on increasing the computer account limit in an Organizational Unit, see the following articles:

- Increase the computer account limit in the Organizational Unit.
 - Default limit to number of workstations a user can join to the domain.
 - Add workstations to domain.
-

Feedback

Was this page helpful?



Yes



No

Provide product feedback ↗

Pre-provision Microsoft Entra hybrid join: Register devices as Autopilot devices

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Install the Intune Connector \(OU\)](#)
- Step 3: [Increase the computer account limit in the Organizational Unit](#)

Step 4: Register devices as Autopilot devices

- Step 5: [Create a device group](#)
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
- Step 8: [Configure and assign domain join profile](#)
- Step 9: [Assign Autopilot device to a user \(optional\)](#)
- Step 10: [Technician flow](#)
- Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Note

If devices are already registered as Autopilot devices, skip this step and move on to [Step 5: Create a device group](#).

Register devices as Autopilot devices

Before a device can use Autopilot, the device must be registered as an Autopilot device. Registering a device as an Autopilot device can be thought of as importing the device into Autopilot so that Autopilot service can be used on the device. Registering a device as an Autopilot device doesn't mean that the device has used the Autopilot service. It just makes the Autopilot service available to the device.

Also note that a device registered in Autopilot doesn't mean the device is enrolled in Intune. A device might be registered as an Autopilot device but might not exist in Intune. It's not until an Autopilot registered device goes through the Autopilot process for the first time that it becomes enrolled in Intune. After the Autopilot device undergoes the Autopilot process and enrolls in Intune, the Autopilot device appears as a device in both Microsoft Entra ID and Intune.

There are several methods to register a device as an Autopilot device in Intune:

- Manually registering devices into Intune as an Autopilot device via the hardware hash. The hardware hash of a device can be collected via one of the following methods:
 - [Configuration Manager](#).
 - [PowerShell script](#).
 - [Diagnostics page hash export](#).
 - [Desktop hash export](#).

These methods of obtaining the hardware hash of a device are well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

- Automatically registering device via:
 - An [OEM](#), including [Microsoft Surface](#) devices.
 - A [partner](#).

Registering a device via an OEM or partner is also well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

For most organizations, using an OEM or partner to register devices as Autopilot devices is the preferred, most common, and most secure method. However for smaller organizations, for testing/lab scenarios, and for emergency scenarios, manually registering devices as Autopilot devices via the hardware hash is also used.

Important

The following type of devices shouldn't be registered as a Windows Autopilot device:

- [Microsoft Entra registered](#) devices, also known as "workplace joined" devices.
- [Intune MDM-only enrollment](#) devices.

These options are intended for users to join personally owned devices to their organization's network. Windows Autopilot registered devices are registered as corporate owned devices.

If a device is already one of these two types of devices, to register it as a Windows Autopilot device, first remove it from Microsoft Intune and Microsoft Entra ID. For more information, see [Device appears as Microsoft Entra registered instead of Microsoft Entra joined](#) and [Deregister a device](#).

ⓘ Note

Assuming that a device isn't currently enrolled in Intune, remember that registering a device in Autopilot doesn't make it an Intune enrolled device. That device doesn't enroll into Intune until Autopilot runs on the device for the first time.

Importing the hardware hash CSV file for devices into Intune

Several of the methods in the previous section on obtaining the hardware hash when manually registering devices as Autopilot devices produces a CSV file that contains the hardware hash of the device. This CSV file with the hardware hash needs to be imported into Intune to register the device as an Autopilot device.

After the CSV file is created, it can be imported into Intune via the following steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, select **Import**.
 - a. In the **Add Autopilot devices** window that opens:
 - i. Under **Specify the path to the list you want to import.**, select the blue file folder.

- ii. Browse to the CSV file obtained using one of the above methods to obtain the hardware hash of a device.
- iii. After selecting the CSV file, verify that the correct CSV file is selected under **Specify the path to the list you want to import.**, and then select **Import**. Selecting **Import** closes the **Add Autopilot devices** window. Importing can take several minutes.

- b. After the import is complete, select **Sync**.

A message displays saying that the sync is in progress. The sync process might take a few minutes to complete, depending on how many devices are being synchronized.

 **Note**

If another sync is attempted within 10 minutes after initiating a sync, an error will be displayed. Syncs can only occur once every 10 minutes. To attempt a sync again, wait at least 10 minutes before trying again.

- c. Select **Refresh** to refresh the view. The newly imported devices should display within a few minutes. If the devices aren't yet displayed, wait a few minutes, and then select **Refresh** again.

Next step: Create a device group

Step 5: Create a device group

Related content

For more information on registering devices as Autopilot devices, see the following articles:

- [Manually register devices with Windows Autopilot](#).
- [Windows Autopilot customer consent](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Pre-provision Microsoft Entra hybrid join: Create a device group

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Autopilot devices](#)
-  **Step 5: Create a device group**
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Autopilot device to a user \(optional\)](#)
 - Step 10: [Technician flow](#)
 - Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Note

If device groups are already created, skip this step and move on to [Step 6: Configure and assign Autopilot Enrollment Status Page \(ESP\)](#). However, if deploying multiple different Autopilot scenarios to different devices, separate device groups are required for each Autopilot scenario.

Create a device group

Device groups are a collection of devices organized into a Microsoft Entra group. Device groups are used in Autopilot to target devices for specific configurations such as what policies to apply to a device and what applications to install on the device. They're also used by Autopilot to target Enrollment Status Page (ESP) configurations, Autopilot profile configurations, and domain join profiles to devices.

Device groups can be either dynamic or assigned:

- **Dynamic groups** - Devices are automatically added to the group based on rules
- **Assigned groups** - Devices are manually added to the group and are static

When an admin configures Autopilot in an enterprise environment, dynamic groups are primarily used since a large number of devices are normally involved. Adding the devices in automatically using rules makes management of the group a lot easier. Adding a large amount of device in manually via an assigned group would be impractical. However, if there's only a few devices, for example for testing purposes, an assigned group can be used instead.

To create a dynamic device group for use with Autopilot, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Groups** in the left hand pane.
3. In the **Groups | All groups** screen, make sure **All groups** is selected, and then select **New group**.
4. In the **New Group** screen that opens:
 - a. For **Group type**, select **Security**.
 - b. For **Group name**, enter a name for the device group.
 - c. For **Group description**, enter a description for the device group.
 - d. For **Microsoft Entra roles can be assigned to the group**, select **No**.
 - e. For **Membership type**, select **Dynamic Device**. Setting the **Membership type** option to **Dynamic Device** changes the option **Members** to **Dynamic device members**.
 - f. For **Owners**, select the **No owners selected** link.
 - g. In the **Add owners** screen that opens:
 - i. Scroll through the list of objects and select owners for the user group. Alternatively, use the **Search** bar to search for and select owners of the group.
 - ii. Once all of the desired owners are selected, select **Select**.
 - h. For **Dynamic device members**, select **Add dynamic query**. The **Dynamic membership rules** screen opens.
 - i. In the **Dynamic membership rules** screen:

- i. Make sure that **Configure Rules** is selected at the top.
- ii. Select **Add expression**. Rules and expressions can be added that defines what devices are added to the device group.

Rules can be entered in the rule builder via the drop-down boxes. Alternatively, the rule syntax can be entered directly via the **Edit** option in the **Rule syntax** section.

The most common type of dynamic device group when using Windows Autopilot is a device group that contains all Windows Autopilot devices. A dynamic device group that contains all Windows Autopilot devices has the following syntax:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```

To enter in this rule:

- i. Select the **Edit** option in the **Rule syntax** section.
- ii. Paste in the following rule in the **Edit rule syntax** screen under **Rule syntax**:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```
- iii. Once the rule is pasted in, select **OK**.
- iii. Once the desired rule is entered, select **Save** on the toolbar to close the **Dynamic membership rules** window.

For more information on creating rules for dynamic groups, see [Dynamic membership rules for groups in Microsoft Entra ID](#).

- j. Select **Create** to finish creating the dynamic device group.

Note

The above steps are creating a dynamic group in Microsoft Entra that is used by Intune and Windows Autopilot solutions. Although the groups can be accessed in the Intune portal, they're Microsoft Entra groups.

Tip

For Configuration Manager admins, device groups are similar to device based collections. Dynamic device groups are similar to query based device collections while assigned device groups are similar to direct membership device collections.

Next step: Configure and assign the Enrollment Status Page (ESP)

Step 5: Configure and assign Autopilot Enrollment Status Page (ESP)

Related content

For more information on creating groups in Intune, see the following articles:

- [Create device groups.](#)
- [Add groups to organize users and devices.](#)
- [Manage Microsoft Entra groups and group membership.](#)
- [Dynamic membership rules for groups in Microsoft Entra ID.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Pre-provision Microsoft Entra hybrid join: Configure and assign the Enrollment Status Page (ESP)

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Autopilot devices](#)
 - Step 5: [Create a device group](#)
-  **Step 6: Configure and assign Autopilot Enrollment Status Page (ESP)**
- Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Autopilot device to a user \(optional\)](#)
 - Step 10: [Technician flow](#)
 - Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Note

If an ESP is already configured, assigned, and uses the same settings for the pre-provisioned Microsoft Entra hybrid join scenario, skip this step and move on to [Step 7: Create and assign Microsoft Entra hybrid join Autopilot profile](#).

The Enrollment Status Page (ESP)

The main feature of the Enrollment Status Page (ESP) is to display progress and current status to the end user while the device is being set up and enrolled via the Autopilot process. The other main feature of the ESP is to block a user from signing in and using the device until all required policies and applications are installed. Multiple ESP profiles can be created with different settings and assigned appropriately based on different needs and scenarios.

Out of box there's a default ESP that is assigned to all devices. The default setting in the default ESP is to not show app and profile progress during the Autopilot process. However, Microsoft recommends changing this default via a separate custom ESP to show app and profile progress. Enabling and configuring an ESP allows end users to properly see the progress of their device being set up and prevents them using the device until the device is fully configured and provisioned. A user signing into the device before being fully configured and provisioned can cause issues.

The ESP has two phases:

- **Device ESP** - The portion of the ESP that runs during the OOB process and applies device policies and installs device applications.
- **User ESP** - The portion of the ESP that sets up user account, applies user policies, and installs user applications.

Device ESP runs first followed by the User ESP.

Tip

For Configuration Manager admins, an ESP is similar and analogous to Configuration Manager client settings.

Autopilot Enrollment Status Page (ESP) configuration options

When the Enrollment Status Page (ESP) is configured, it has several options that can be configured to meet the needs of the organization. The following lists the different options and their possible configurations:

- **Show an error when installation takes longer than specified number of minutes:**
 - The default time-out is 60 minutes. Enter a higher value if more time is needed to install applications on the devices.
- **Show custom message when time limit or error occur:**
 - **No:** The default message is shown to users when an error occurs. That message is: **Setup could not be completed. Please try again or contact your support person for help.**
 - **Yes:** A custom message is shown to users when an error occurs. Enter a custom message in the provided text box.

- Turn on log collection and diagnostics page for end users:
 - No: The collect logs button isn't shown to users when an installation error occurs. The Windows Autopilot diagnostics page isn't shown on devices running Windows 11.
 - Yes: The collect logs button is shown to users when an installation error occurs. The Windows Autopilot diagnostics page is shown on devices running Windows 11. Logs and diagnostics might aid with troubleshooting. For this reason, Microsoft recommends enabling this option.
- Only show page to devices provisioned by out-of-box experience (OOBE):
 - No: The enrollment status page (ESP) is shown during the device phase and the out-of-box experience (OOBE). The page is also shown during the user phase to every user who signs into the device for the first time.
 - Yes: The enrollment status page (ESP) is shown during the device phase and the OOBE. The page is also shown during the user phase, but only to the first user who signs into the device. It isn't shown to subsequent users who sign into the device.
- Block device use until all apps and profiles are installed:
 - No: Users can leave the ESP before Intune is finished setting up the device.
 - Yes: Users can't leave the ESP until Intune is done setting up the device. Enabling this option unlocks the following additional options:
 - Allow users to reset device if installation error occurs:
 - No: The ESP doesn't give users the option to reset their devices when an installation fails.
 - Yes: The ESP gives users the option to reset their devices when an installation fails.
 - Allow users to use device if installation error occurs:
 - No: The ESP doesn't give users the option to bypass the ESP when an installation fails.
 - Yes: The ESP gives users the option to bypass the ESP and use their devices when an installation fails.

- **Block device use until these required apps are installed if they are assigned to the user/device:**
 - **All:** All assigned apps must be installed before users can use their devices.
 - **Selected:** Selected apps must be installed before users can use their devices. After enabling this option, select **Select apps** to select the managed apps from Intune that are required to be installed before users can use their device.

Configure and assign the Enrollment Status Page (ESP)

To configure and assign the Autopilot Enrollment Status Page (ESP), follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
- 1 In the **Devices | Overview** screen, under **By platform**, select **Windows**.
 1. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
 2. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Enrollment Status Page**.
 3. In the **Enrollment Status Page** screen that opens, select **Create**.
 4. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the ESP profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.
 5. In the **Settings** page, toggle the option **Show app and profile configuration progress** to **Yes**.
 - a. After the option **Show app and profile configuration progress** is toggled to **Yes**, several new options will appear. Configure these options based on the desired behavior for the ESP as described in the section [Autopilot Enrollment Status Page \(ESP\) configuration options](#):

- b. Once the different ESP options under the **Settings** page are configured as desired, select **Next**.
6. In the **Assignments** page:
 - a. Under **Included groups**, select **Add groups**.
 - b. In the **Select groups to include** window that opens, select the device groups to target the ESP profile. The device groups selected would normally be the device groups created in the **Create device group** step.
 - c. After selecting the device group, select **Select** to close the **Select groups to include** window.

 **Tip**

After selecting the device groups, the **Edit filter** option can be selected on each device group added to the assignment to further refine what devices are targeted for the ESP profile. For example, further filtering can be useful if some of the devices that are members in the device groups selected need to be excluded.

- d. Select **Next**.

 **Note**

An ESP is assigned to a device group and not directly to individual devices. To assign an ESP to a specific device, the device must be a member of a device group that has an ESP assigned to it.

7. In the **Scope tags** page, select **Next**.

 **Note**

Scope tags are optional and are a method to control who has access to the ESP configuration. For this tutorial, scope tags are being skipped and left at the default scope tag. However if a custom scope tag needs to be specified, do so at this screen. For more information about scope tags, see [Use role-based access control and scope tags for distributed IT](#).

8. In the Review + create page, verify that the settings are correct and configured as desired. Once verified, select **Create** to save the changes and assign the ESP profile.

Next step: Create and assign pre-provisioned Microsoft Entra hybrid join Autopilot profile

Step 7: Create and assign Microsoft Entra hybrid join Autopilot profile

Related content

For more information on the Enrollment Status Page (ESP), see the following articles:

- [Windows Autopilot Enrollment Status Page](#).
- [Set up the Enrollment Status Page](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Pre-provision Microsoft Entra hybrid join: Create and assign a pre-provisioned Microsoft Entra hybrid join Autopilot profile

Article • 09/13/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Install the Intune Connector](#)
- Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
- Step 4: [Register devices as Autopilot devices](#)
- Step 5: [Create a device group](#)
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- ✓ Step 7: **Create and assign Microsoft Entra hybrid join Autopilot profile**
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Autopilot device to a user \(optional\)](#)
 - Step 10: [Technician flow](#)
 - Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Create and assign a pre-provisioned Microsoft Entra hybrid join Autopilot profile

The Autopilot profile specifies how the device is configured during Windows Setup and what is shown during the out-of-box experience (OOBE).

The difference between a Microsoft Entra join and a Microsoft Entra hybrid join is that the Microsoft Entra hybrid join scenario joins both an on-premises domain and Microsoft Entra ID during Autopilot. The pre-provisioned Microsoft Entra join scenario only joins Microsoft Entra ID during Autopilot.

 Tip

For Configuration Manager admins, the Autopilot profile is similar to some of the configuration that takes place during a task sequence via an `unattend.xml` file. The `unattend.xml` file is configured during the **Apply Windows Settings** and **Apply Network Settings** steps. Note however that Autopilot doesn't use `unattend.xml` files.

To create a pre-provisioned Microsoft Entra hybrid join Autopilot profile, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Deployment Profiles**.
6. In the **Windows Autopilot deployment profiles** screen, select the **Create Profile** drop down menu and then select **Windows PC**.
7. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the Autopilot profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.

Note

Microsoft recommends setting the option **Convert all targeted devices to Autopilot** to **Yes**. This tutorial concentrates on new devices where the device is manually imported as an Autopilot device using the hardware hash. However, this option can be helpful when assigning Autopilot profiles to device groups that contain existing devices. For example, this option is helpful when using the [Windows Autopilot for existing devices](#) scenario. With Windows Autopilot for existing devices, existing devices might need to be registered as an Autopilot device after the Autopilot deployment.

completes. For more information, see [Register device for Windows Autopilot](#).

8. In the **Out-of-box experience (OOBE)** page:

- For **Deployment mode**, select **User-driven**.
- For **Join to Microsoft Entra ID as**, select **Microsoft Entra hybrid joined**. After this option is selected, several the options underneath this option will change.
- For **Skip AD connectivity check**, select **No**. This section of the tutorial assumes that the device undergoing Autopilot is an on-premises internal client and that has direct connectivity to the on-premises domain and domain controllers. For off-premise/Internet scenarios where VPN connectivity is required, see [Off-premises/Internet scenarios and VPN connectivity](#).
- For **Microsoft Software License Terms**, select **Hide** to skip the EULA page.
- For **Privacy settings**, select **Hide** to skip the privacy settings.
- For **Hide change account options**, select **Hide**.
- For **User account type**, select the desired account type for the user (**Administrator** or **Standard user**). If **Administrator** is chosen, the user is added to the local Admin group.
- For **Allow pre-provisioned deployment**, select **Yes**.
- For **Language (Region)**, select **Operating system default** to use the default language for the operating system being configured. If another language is desired, select the desired language from the drop-down list.
- For **Automatically configure keyboard**, select **Yes** to skip the keyboard selection page.
- The **Apply device name template** is greyed out for Microsoft Entra hybrid join scenarios. Although not as robust, device names can be specified during the [Configure and assign domain join profile](#) step.

 **Note**

The above settings are selected to minimize needed user interaction during device setup. However, some of the settings that are hidden can instead be shown as desired. For example, some regions might require that **Privacy settings** always be shown.

! Note

If the language/region and keyboard screens are set to hidden, they might still be displayed if there's no network connectivity at the start of the Autopilot deployment. When there's no network connectivity at the start of the deployment, the Autopilot profile, where the settings to hide these screens is defined, hasn't downloaded yet. Once network connectivity is established, the Autopilot profile is downloaded and any additional screen settings should work as expected.

9. Once the options in the **Out-of-box experience (OOBE)** page are configured as desired, select **Next**.

10. In the **Assignments** page:

- Under **Included groups**, select **Add groups**.

! Note

Make sure to add the correct device groups under **Included groups** and not under **Excluded groups**. Accidentally adding the desired device groups under **Excluded groups** prevents devices in those device groups from receiving the Autopilot profile.

- In the **Select groups to include** window that opens, select the groups that the Windows Autopilot profile should be assigned to. These device groups are normally the device groups created in the previous **Create device group** step. Once done, select **Select**.

- Under **Included groups > Groups**, ensure the correct groups are selected, and then select **Next**.

11. In the **Review + Create** page, verify that all settings are set correctly, and then select **Create** to create the Autopilot profile.

Verify device has an Autopilot profile assigned to it

Before deploying a device, ensure that an Autopilot profile is assigned to a device group that the device is a member of. Autopilot profile assignment to a device can take some time after the Autopilot profile is assigned to the device group or after the device is added to the device group. To verify that the profile is assigned to a device, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens:
 - a. Find the desired device that Autopilot deployment profile assignment status needs to be checked.
 - b. Once the device is located, its current status is listed under the **Profile status** column. The status has one of the following values:
 - **Not assigned**: An Autopilot deployment profile isn't assigned to the device.
 - **Assigning**: An Autopilot deployment profile is being assigned to the device.
 - **Assigned**: An Autopilot deployment profile is assigned to the device.
 - **Fix pending**: When a hardware change occurs on a device, this status displays while Intune tries to register the new hardware. When the link for the **Fix pending** status is selected, the following message appears:

We've detected a hardware change on this device. We're trying to automatically register the new hardware. You don't need to do anything now; the status will be updated at the next check in with the result.

If Intune is able to successfully register the new hardware, Intune updates the profile status when the device next checks into Intune. For more information on the **Fix pending** status, see the following articles:

- [Why is the Windows Autopilot profile not applied after a hardware change occurred on a device?](#).
 - [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
 - [Windows Autopilot motherboard replacement scenario guidance](#)
- **Attention required:** If Intune is unable to register the new hardware after a hardware change occurs on a device, the device can't receive the Autopilot profile until the device is reset and the device re-registers. For more information on this status and how to deregister/re-register a device, see the following articles:
 - [Why is the Windows Autopilot profile not applied after a hardware change occurred on a device?](#).
 - [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
 - [Windows Autopilot motherboard replacement scenario guidance](#)
 - [Deregister a device](#)

Before starting the Autopilot deployment process on a device, make sure that in the [Windows Autopilot devices](#) page:

- The device's **Profile status** status is **Assigned**.
- In the properties of the device, **Date assigned** has a value.
- In the properties of the device, **Assigned profile** displays the expected Autopilot profile.

Note

Intune periodically checks for new devices in the assigned device groups, and then begins the process of assigning profiles to those devices. Due to several different factors involved in the process of Autopilot profile assignment, an estimated time for the assignment can vary from scenario to scenario. These factors can include Microsoft Entra groups, membership rules, hash of a device, Intune and Autopilot services, and internet connection. The assignment time varies depending on all the factors and variables involved in a specific scenario.

Off-premises/Internet scenarios and VPN connectivity

Windows Autopilot for pre-provisioned Microsoft Entra hybrid join supports off-premises/Internet scenarios where direct connectivity to Active directory and domain controllers isn't available. However, an off-premises/Internet scenario doesn't eliminate the need for connectivity to Active Directory and a domain controller during the domain join. In an off-premises/Internet scenario, connectivity to Active Directory and a domain controller can be established via a VPN connection during the Autopilot process.

For off-premises/Internet scenarios requiring VPN connectivity, the only change in the Autopilot profile would be in the setting **Skip AD connectivity check**. In the [Create and assign pre-provisioned Microsoft Entra hybrid join Autopilot profile](#) section, the **Skip AD connectivity check** setting should be set to **Yes** instead of to **No**. Setting this option to **Yes** prevents the deployment from failing since there's no direct connectivity to Active Directory and domain controllers until the VPN connection is established.

In addition to changing the **Skip AD connectivity check** setting to **Yes** in the Autopilot profile, VPN support also relies on the following requirements:

- The VPN solution can be deployed and installed with Intune.
- The VPN solution needs to support one of the following options:
 - Lets the user manually establish a VPN connection from the Windows sign-in screen.
 - Automatically establishes a VPN connection as needed.

The VPN solution would need to be installed and configured via Intune during the Autopilot process. Configuration would need to include deploying any required device certificates if needed by the VPN solution. Once the VPN solution is installed and configured on the device, the VPN connection can be established, either automatically or manually by the user, at which point the domain join can occur. For more information and support on VPN solutions during Autopilot, consult the respective VPN vendor.

Note

Some VPN configurations aren't supported because the connection isn't initiated until the user signs into Windows. Unsupported VPN configurations include:

- VPN solutions that use user certificates
- Non-Microsoft UWP VPN plug-ins from the Windows Store

Next step: Configure and assign domain join profile

Step 8: Configure and assign domain join profile

Related content

For more information on configuring Autopilot profiles, see the following articles:

- [Configure Autopilot profiles.](#)
- [User-driven mode for Microsoft Entra hybrid join with VPN support.](#)
- [VPNs.](#)

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Pre-provision Microsoft Entra hybrid join: Create and assign a domain join profile

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit \(OU\)](#)
 - Step 4: [Register devices as Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
-  **Step 8: Configure and assign domain join profile**
- Step 9: [Assign Autopilot device to a user \(optional\)](#)
 - Step 10: [Technician flow](#)
 - Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Note

If a domain join profile is already created with the desired settings and assignments, move on to the [Next step: Assign Autopilot device to a user \(optional\)](#) section.

Create and assign a domain join profile

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **Manage devices**, select **Configuration**.
4. In the **Devices | Configuration** screen:

- a. At the top, make sure **Policies** is selected.
 - b. Select the **Create** drop down menu and then select **New Policy**.
5. In the **Create a profile** window that opens:
- a. Under **Platform**, select **Windows 10 and later**.
 - b. Under **Profile type**, select **Templates**.
 - c. When the templates appear, under **Template name**, select **Domain join**. If **Domain join** isn't visible, scroll through the **Template name** list until **Domain join** is visible or search for **Domain join** in the **Search by profile name** box.
 - d. Select **Create** to close the **Create a profile** window.
6. The **Domain Join** screen opens. In the **Basics** page:
- a. Next to **Name**, enter a name for the domain join profile.
 - b. Next to **Description**, enter a description for the domain join profile.
 - c. Select **Next**.
7. In the **Configuration settings** page:
- a. Next to **computer name prefix**, enter a prefix for computer names. This field is required. This prefix is used on all computer names. The rest of the computer name after the prefix is randomly generated up to 15 characters.
-  **Note**

This field doesn't support the **%SERIAL%** or **%RAND:x%** variables that can be used with the **Apply device name template** in the Microsoft Entra join scenario.
- b. Next to **Domain name**, enter the FQDN of the domain that devices should join. This field is required. Make sure to specify the FQDN of the domain and not the NETBIOS name of the domain. For example, enter in **contoso.com** and not just **CONTOSO**.
 - c. Next to **Organizational unit**, enter the full path to the Organizational Unit (OU) in the domain that the computer accounts should be created in. For example, **OU=OU-Name,DC=contoso,DC=com**. This field is optional. If the OU isn't specified, the computer accounts are created in the **Computer** container.

Note

The OU specified in this step should be the same OU that permissions were set for and computer account limits increased in the step **Increase the computer account limit in the Organizational Unit (OU)**. Make sure that the step **Increase the computer account limit in the Organizational Unit (OU)** is followed for the OU specified in this field. Skipping the step that sets permissions correctly on the OU results in computers failing to join the domain.

Important

If computers are joining the **Computers** container, leave this field blank. Don't specify the **Computers** container in this field via **CN=Computers,DC=contoso,DC=com**. The **Computers** container is a container and not an OU. When no OU is specified in this field and the field is left blank, devices automatically join the **Computers** container. If the **Computers** container is specified, it causes domain joins to fail.

d. Once the settings in the **Configuration settings** page are complete, select **Next**.

8. In the **Assignments** page:

a. Under **Included groups**, select **Add all devices**.

Note

- Microsoft recommends selecting and assigning to **Add all devices** instead of selecting and assigning to the device group created in the **Create device group** step. Assigning to all devices ensures that the domain join profile works when using:
 - [Windows Autopilot deployment for existing devices](#) scenario.
 - A Windows Autopilot deployment that utilizes Microsoft Entra hybrid join and runs after the Windows Autopilot deployment for existing devices deployment.
- Make sure to add the correct device groups under **Included groups** and not under **Excluded groups**. Accidentally adding the desired

device groups under **Excluded groups** results in those devices being excluded and they don't receive the configuration profile.

- b. Under **Included groups > Groups**, ensure that **All devices** is selected, and then select **Next**.
9. In the **Applicability Rules** page, select **Next**. For this tutorial, applicability rules are being skipped. However if applicability rules are needed, do so at this screen. For more information about scope tags, see [Applicability rules](#).
10. In the **Review + Create** page, review and verify that all of the settings are set as desired, and then select **Create** to create the domain join profile.

Next step: Assign Autopilot device to a user (optional)

Step 9: Assign Autopilot device to a user (optional)

If a user isn't being assigned to the device, then skip to [Step 10: Technician flow](#).

Step 10: Technician flow

Related content

For more information on domain join profiles, see the following article:

- [Create and assign a Domain Join profile](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Pre-provision Microsoft Entra hybrid join: Assign Autopilot device to a user (optional)

Article • 06/19/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Install the Intune Connector \(OU\)](#)
- Step 3: [Increase the computer account limit in the Organizational Unit](#)
- Step 4: [Register devices as Autopilot devices](#)
- Step 5: [Create a device group](#)
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
- Step 8: [Configure and assign domain join profile](#)

Step 9: Assign Autopilot device to a user (optional)

- Step 10: [Technician flow](#)
- Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Assign Autopilot device to a user (optional)

A device that is registered as an Autopilot device can also be assigned to a user. If an Autopilot device is assigned to a user, then any user policies and application installs assigned to that user is applied to the device during the Autopilot process.

Tip

For testing purposes, especially for hybrid Microsoft Entra scenarios, it might be better to first test an Autopilot deployment before assigning the device to a user. Not assigning a user limits the scope of applications, policies, and configurations processed during the Autopilot process.

💡 Tip

For Configuration Manager admins, assigning a user to a device is similar to user device affinity in Configuration Manager.

To assign an Autopilot device to a user, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, locate the device to assign a user to.
7. Once the desired device is located, select the box to the left of the device, making sure that there's check mark in the box, and then select **Assign user** in the toolbar at the top of page.
8. In the **Select user** window that opens, find and select a user for the device, and then select **Select** to close the window. If necessary, use the **Search** box to find the desired user.

❗ Note

The selected user must be an Azure user licensed to use Intune.

9. In the Autopilot device's property window that automatically opens on the right hand side, under **User friendly name**, verify the default value. If the value is empty or a different friendly name is desired, enter the desired friendly name for the user under **User friendly name**, and then select **Save** to close the property window.
10. The user assignment can be verified by selecting the Autopilot device in the **Windows Autopilot devices** screen. Once the Autopilot device is selected, it highlights and the Autopilot device's property window automatically opens on the right hand side. The assigned user is listed under **User** and **User friendly name**.

Assigning Autopilot device to a user via hardware hash CSV file

A user can be manually assigned to a Windows Autopilot device in the Windows Autopilot device's properties. However, a user can also be assigned to the Autopilot device when the device was initially imported into Autopilot as an Autopilot device. Assigning a user when the device is imported as an Autopilot device can be done by editing the hardware hash CSV file and adding the **Assigned User** column after the **Hardware Hash** column. The user's User Principal Name (UPN) should then be added as a value under the **Assigned User** column.

Important

Use a plain-text editor such as **Notepad** to edit the CSV file. Don't use Microsoft Excel. Editing the CSV file in Excel doesn't generate a proper usable file for importing into Intune.

For more information on editing the CSV file to add an assigned user to the Autopilot device, see [Manually register devices with Windows Autopilot: Ensure that the CSV file meets requirements](#).

Next step: Technician flow

[Step 10: Technician flow](#)

Related content

For more information on assigning a user to an Autopilot device, see the following article:

- [Assign a user to a specific Autopilot device.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Pre-provision Microsoft Entra hybrid join: Technician flow

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Install the Intune Connector \(OU\)](#)
 - Step 3: [Increase the computer account limit in the Organizational Unit](#)
 - Step 4: [Register devices as Autopilot devices](#)
 - Step 5: [Create a device group](#)
 - Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
 - Step 8: [Configure and assign domain join profile](#)
 - Step 9: [Assign Autopilot device to a user \(optional\)](#)
-  **Step 10: Technician flow**
- Step 11: [User flow](#)

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

Technician flow

Important

The technician flow portion of the Microsoft Entra hybrid join process only requires connectivity to the Internet. It doesn't require connectivity to a domain controller. Connectivity to a domain controller to perform an on-premises domain join isn't needed until the next step of [User flow](#) runs.

Once all of the configurations for Windows Autopilot for pre-provisioned deployment are completed in Intune and in Microsoft Entra ID, the next step is to start the Windows Autopilot deployment process on the device. For Windows Autopilot for pre-provisioned deployment, the Autopilot process is split into two different phases that run at two different points in time by two different sets of individuals:

- The first phase is known as the **technician flow** and is normally run by the IT department, OEM, or reseller.
- The second phase is known as the **user flow** and is normally run by the end-user.

To start the technician flow, select a device that is part of the device group created in the previous **Create a device group** step, and then follow these steps:

1. If a wired network connection is available, connect the device to the wired network connection.
2. Power on the device.
3. Once the device boots up, one of two things occurs depending on the state of network connectivity:
 - If the device is connected to a wired network and has network connectivity, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
 - If the device isn't connected to a wired network or if it doesn't have network connectivity, it prompts to connect to a network. Connectivity to the Internet is required:
 - a. The out-of-box experience (OOBE) begins and a screen asking for a country or region appears. Select the appropriate country or region, and then select **Yes**.
 - b. The keyboard screen appears to select a keyboard layout. Select the appropriate keyboard layout, and then select **Yes**.
 - c. An additional keyboard layouts screen appears. If needed, select additional keyboard layouts via **Add layout**, or select **Skip** if no additional keyboard layouts are needed.

Note

When there's no network connectivity, the device can't download the Autopilot profile to know what country/region and keyboard settings to use. For this reason, when there's no network connectivity, the country/region and keyboard screens appear even if these screens are set to hidden in the Autopilot profile. These settings need to be

specified in these screens in order for the network connectivity screens that follow to work properly.

- d. The **Let's connect you to a network** screen appears. At this screen, either plug the device into a wired network (if available), or select and connect to a wireless Wi-Fi network.
 - e. Once network connectivity is established, the **Next** button should become available. Select **Next**.
 - f. At this point, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
4. At the Microsoft Entra sign-in page, **DON'T** sign in or select the **Next/Sign in** button. Instead, press the **WIN** key on the keyboard five times. Pressing the **WIN** key five times should display a **What would you like to do?** options screen instead.
5. From the **What would you like to do?** options screen:
- For Windows 10, select the **Windows Autopilot provisioning** option, and then select **Continue**.
 - For Windows 11, select the **Pre-provision with Windows Autopilot** option, and then select **Next**.
6. In the **Windows Autopilot Configuration** screen (Windows 10) or the **Pre-provision with Windows Autopilot** screen (Windows 11), it displays the following information about the deployment:
- The name of the organization for the device.
 - The name of the Autopilot deployment profile assigned to the device during the **Create and assign Autopilot profile** step.
 - The user assigned to the device if a user was assigned to the device in the **Assign Autopilot device to a user (optional)** step (if applicable).
 - A QR code containing a unique identifier for the device. This code can be used to look up the device in Intune to perform actions such as verifying configurations, make any necessary changes, etc.
7. Validate that the information in the **Windows Autopilot Configuration** screen is correct. Once all information is confirmed as correct, select **Provision** (Windows 10) or **Next** (Windows 11) to begin the provisioning process.

8. The device might reboot, followed by the Enrollment Status Page (ESP) appearing. The Enrollment Status Page (ESP) displays progress during the provisioning process across three phases:

- **Device preparation** (Device ESP)
- **Device setup** (Device ESP)
- **Account setup** (User ESP)

The first two phases of **Device preparation** and **Device setup** are part of the Device ESP while the final phase of **Account setup** is part of the User ESP.

For technician flow of the Windows Autopilot for pre-provisioned deployment, only the first two Device ESP phases of **Device preparation** and **Device setup** run. The last User ESP phase of **Account setup** will run during the next step of **User flow**.

9. Once **Device setup** and the device ESP process completes, a status screen is displayed showing whether the provisioning process either succeeded or failed:

- If the pre-provisioning process completes successfully, a success status screen appears with information about the deployment. Information presented includes the previously presented information of organization name, Autopilot deployment profile name, QR code (Windows 10 only), and if applicable, assigned user. The elapsed time of the provisioning process is also provided.

Select **Reseal** to shut down the device. At that point, the device can be delivered to the end-user.

Important

Outside of testing scenarios, if the intention is to deliver the device to an end-user, **DON'T** turn the device back on at this point. Instead, deliver the device to the end-user where they perform the last step of **User flow**.

- If the pre-provisioning process fails, an error status screen appears with information about why the deployment failed including an error. The error screen also displays the previously presented information of organization name, Autopilot deployment profile name, QR code (Windows 10 only), and if applicable, assigned user. The elapsed time of the provisioning process is also provided.

From this screen, diagnostic logs can be gathered from the device to troubleshoot the issue by using the following methods:

- In Windows 10, select **View diagnostics**.
- In Windows 11, enter the keystroke **CTRL + SHIFT + D** and then select **Export Logs**.

If the issue can be easily fixed, for example resolving network connectivity, then select the **Retry** button to retry provisioning the device. Otherwise if the issue can't be immediately fixed or can't be fixed without a reset, then select the **Reset** button so that the process starts over again.

Technician flow tips

- Before the Windows Autopilot deployment is started, Microsoft recommends having:
 - At least one type of policy and at least one application assigned to the devices.
 - At least one type of policy and at least one application assigned to the users.

These assignments ensure proper testing of the Windows Autopilot deployment during both the device ESP phase and user ESP phase of the ESP. It might also prevent possible issues when there are either no policies or no applications assigned to the devices or the users.

- Depending on how the Autopilot profile was configured at the **Create and assign Autopilot profile** step, additional screens might appear during the Autopilot deployment before the Microsoft Entra sign-in page such as:
 - **Language/Country/Region**.
 - **Keyboard**.
 - **License Terms**.
- The QR codes can be scanned using a companion app. The app can be used to assign a user to the device. The Autopilot team published to GitHub an [open-source sample of the companion app](#) that integrates with Intune using the Graph API.
- To view and hide detailed progress information in the ESP during the provisioning process:

- Windows 10: To show details, next to the appropriate phase select **Show details**. To hide the details, next to the appropriate phase select **Hide details**.
- Windows 11: To show details, next to the appropriate phase select V. To hide the details, next to the appropriate phase select A.
- The technician flow inherits behavior from [self-deploying mode](#). Self-deploying mode uses the Enrollment Status Page (ESP) to hold the device in a provisioning state. It also prevents the user from proceeding to the desktop after enrollment but before applications and configurations are done applying. If the ESP is disabled, the **Reseal** button might appear before applications and configurations are done applying. Disabling the ESP might inadvertently allow proceeding to the user flow before technician flow provisioning is complete. The success status screen validates that enrollment was successful, not that the technician flow is necessarily complete. For this reason, Microsoft recommends not to disable the ESP. Instead enable the ESP as suggested in the [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#) step.

Next step: User flow

[Step 11: User flow](#)

Related content

For more information on the technician flow of a Windows Autopilot for pre-provisioned deployment, see the following articles:

- [Technician flow](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Pre-provision Microsoft Entra hybrid join: User flow

Article • 07/23/2024 • Applies to: Windows 11, Windows 10

Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Install the Intune Connector \(OU\)](#)
- Step 3: [Increase the computer account limit in the Organizational Unit](#)
- Step 4: [Register devices as Autopilot devices](#)
- Step 5: [Create a device group](#)
- Step 6: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 7: [Create and assign Microsoft Entra hybrid join Autopilot profile](#)
- Step 8: [Configure and assign domain join profile](#)
- Step 9: [Assign Autopilot device to a user \(optional\)](#)
- Step 10: [Technician flow](#)

Step 11: User flow

For an overview of the Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join workflow, see [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join overview](#).

User flow

Important

The user flow portion of the Microsoft Entra hybrid join process requires connectivity to both the Internet and a domain controller. If the connected network doesn't have connectivity to a domain controller, a solution such as a VPN that has connectivity to a domain controller is required.

Once the technician flow step of the pre-provisioning process completes successfully and the device is resealed, the device can be delivered to the end-user. The end-user then completes the normal Windows Autopilot user-driven process. This final step is known as the user flow and involves the following steps:

1. If a wired network connection is available, connect the device to the wired network connection.

2. Power on the device.
3. Once the device boots up, one of two things occurs depending on the state of network connectivity:
 - If the device is connected to a wired network and has network connectivity, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
 - If the device isn't connected to a wired network or if it doesn't have network connectivity, it prompts to connect to a network. Connectivity to the Internet is required:
 - a. The out-of-box experience (OOBE) begins and a screen asking for a country or region appears. Select the appropriate country or region, and then select **Yes**.
 - b. The keyboard screen appears to select a keyboard layout. Select the appropriate keyboard layout, and then select **Yes**.
 - c. An additional keyboard layouts screen appears. If needed, select additional keyboard layouts via **Add layout**, or select **Skip** if no additional keyboard layouts are needed.

 **Note**

When there's no network connectivity, the device can't download the Autopilot profile to know what country/region and keyboard settings to use. For this reason, when there's no network connectivity, the country/region and keyboard screens appear even if these screens are set to hidden in the Autopilot profile. These settings need to be specified in these screens in order for the network connectivity screens that follow to work properly.

- d. The **Let's connect you to a network** screen appears. At this screen, either plug the device into a wired network (if available), or select and connect to a wireless Wi-Fi network.
- e. Once network connectivity is established, the **Next** button should become available. Select **Next**.

- f. At this point, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
4. Once the Autopilot process begins, the Enrollment Status Page (ESP) appears. The ESP displays progress during the provisioning process across three phases:
- **Device preparation** (Device ESP)
 - **Device setup** (Device ESP)
 - **Account setup** (User ESP)
- The first two phases of **Device preparation** and **Device setup** are part of the Device ESP while the final phase of **Account setup** is part of the User ESP.
- For the user flow of Windows Autopilot for pre-provisioned deployment, the **Device setup** phase of the Device ESP and the **Account setup** phase of the User ESP runs. The **Device preparation** phase of the Device ESP doesn't run during the user flow since it already ran and completed during the [Technician flow](#). The **Device setup** phase of the Device ESP runs again during the user flow in case any new or additional policies or applications assigned to the device became available during the time frame that the technician flow ran and when the user flow runs after the device was delivered to the end-user.
5. Once the **Device setup** phase of the Device ESP is complete, user ESP begins and the **User setup** phase starts. The ESP is temporarily dismissed and the Windows sign-on screen appears:
- a. Enter the keystroke **CTRL** + **ALT** + **DEL** to initiate Windows sign-on.
 - b. Enter the on-premises domain credentials for the end-user.

If on-premises domain end-user credentials are different from Microsoft Entra end-user credentials, make sure that the **on-premises domain end-user credentials** are used to sign into the device at this step. Don't use the Microsoft Entra end-user credentials to attempt to sign into the device at this step.
- c. Select **ENTER** on the keyboard to sign the end-user into the device.
6. The Enrollment Status Page (ESP) appears again and the **Account setup** phase of the user ESP continues.
- a. After a short period of time, the Microsoft Entra sign-in page might appear. Sign in with the end-user's Microsoft Entra credentials.

If on-premises domain end-user credentials are different from Microsoft Entra end-user credentials, make sure that **Microsoft Entra end-user credentials** are used to sign in at this step. Don't use on-premises credentials to sign in at this step.

- b. Once the credentials are entered, select **Next**.
- c. The **Stay signed in to all your apps** screen appears. Make sure that the option **Allow my organization to manage my device** is selected, and then select **OK**.
- d. The **You're all set!** screen appears. Select **Done**.

Note

Under certain circumstances, the Microsoft Entra sign-in page might not appear and the end-user might be automatically signed into Microsoft Entra ID. For example, if using [**Active Directory Federation Services \(ADFS\)**](#) and [**single sign-on \(SSO\)**](#). If the end-user is automatically signed into Microsoft Entra ID, then the Autopilot deployment will proceed on to the next step automatically.

7. Once **Account setup** and the user ESP process completes, the provisioning process completes and the ESP finishes. Select the **Sign out** button to dismiss the ESP and go to the Windows sign-on screen. At this point, the end-user can sign into the device using their on-premises domain end-user credentials and start using the device.

User-flow tips

- Depending on how the Autopilot profile was configured at the **Create and assign Autopilot profile** step, additional screens might appear during the Autopilot deployment such as:
 - **Language/Country/Region** or **Keyboard** screens before the Microsoft Entra sign-in page.
 - **Privacy** screen when the user ESP/Account setup begins but before the Windows sign-on screen appears.
- If the device is left alone with no interaction during the **Account setup** phase of the ESP, the device might enter the Windows lock screen. If the device does enter the Windows lock screen during **Account setup** of the ESP, unlock the device by

entering the keystroke **CTRL** + **ALT** + **DEL**, entering the on-premises domain credentials for the end-user, and then selecting **ENTER** on the keyboard. Unlocking the device should go back to the Enrollment Status Page (ESP) and display the current progress of **Account setup**.

- To view and hide detailed progress information in the ESP during the provisioning process:
 - **Windows 10:** To show details, next to the appropriate phase select **Show details**. To hide the details, next to the appropriate phase select **Hide details**.
 - **Windows 11:** To show details, next to the appropriate phase select **v**. To hide the details, next to the appropriate phase select **Λ**.
- For tokens to refresh properly between the Technician flow and the User flow, wait at least 90 minutes after running the Technician flow before running the User flow. This scenario mainly affects lab and testing scenarios, such as this tutorial, when the User flow is run within 90 minutes after the Technician flow completes.
- The User flow should be run within six months after the Technician flow finishes. Waiting more than six months can cause the certificates used by the Intune Management Engine (IME) to no longer be valid leading to errors such as:

```
Error code: [Win32App][DetectionActionHandler] Detection for policy with id:  
<policy_id> resulted in action status: Failed and detection state:  
NotComputed.
```

- Compliance in Microsoft Entra ID is reset during the User flow. Devices might show as compliant in Microsoft Entra ID after the Technician flow completes, but then show as noncompliant once the User flow starts. Allow enough time after the User flow completes for compliance to reevaluate and update.

Related content

For more information on the user flow of a Windows Autopilot for pre-provisioned deployment, see the following articles:

- [User flow](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Step by step tutorial for Windows Autopilot self-deploying mode in Intune

Article • 09/13/2024 • Applies to:  Windows 11,  Windows 10

This step by step tutorial guides through using Intune to perform a Windows Autopilot self-deploying mode scenario.

The purpose of this tutorial is a step by step guide for all the configuration steps required for a successful Autopilot self-deploying mode deployment using Intune. The tutorial is also designed as a walkthrough in a lab or testing scenario, but can be expanded for use in a production environment.

Before beginning, refer to the [How to: Plan your Microsoft Entra join implementation](#) to make sure all requirements are met for joining devices to Microsoft Entra ID.

Windows Autopilot self-deploying mode overview

Windows Autopilot self-deploying mode is an Autopilot solution that automates the configuration of Windows on a new device delivered directly from an IT department, OEM, or reseller to the end-user. Windows Autopilot for pre-provisioned deployment uses the existing Windows installation installed by the OEM at the factory. Windows Autopilot self-deploying mode is designed for kiosk like devices or devices shared by multiple users. For this reason, Windows Autopilot self-deploying mode doesn't support assigning users to the device. Additionally, Windows Autopilot self-deploying mode only supports Microsoft Entra join. It doesn't support Microsoft Entra hybrid join.

The main advantage of Windows Autopilot self-deploying mode over other Autopilot deployments methods is that it minimizes the interaction needed during the initial deployment of the device. Interactions are minimized because there's no single user assigned to the device. After first powering on the device, usually the only interactions needed, if any, are:

- In certain scenarios, selecting the language, locale, and keyboard layout.
- Connecting to a wireless network if the device isn't connected to a wired network.

In certain scenarios after first turning on the device, such as when the device is on a wired network connection, zero interaction might be possible.

Windows Autopilot self-deploying mode can perform the following tasks during the deployment:

- Joins the device to Microsoft Entra ID.
- Enrolls the device in Intune.
- Installs applications.
- Applies device configuration policies such as BitLocker and Windows Hello for Business.
- Checks for compliance.

Once the Windows Autopilot self-deploying mode is complete, the device goes to the Windows sign-on screen and is ready for use. Any end-user signing into the device needs to sign on with their Microsoft Entra credentials. For devices such as kiosks, it's also possible to configure Intune policies that automatically sign a user into the device.

Workflow

The following steps are needed to configure and then perform a Windows Autopilot self-deploying mode in Intune:

- ✓ Step 1: Set up Windows automatic Intune enrollment
- ✓ Step 2: Register devices as Autopilot devices
- ✓ Step 3: Create a device group
- ✓ Step 4: Configure and assign Autopilot Enrollment Status Page (ESP)
- ✓ Step 5: Create and assign Autopilot profile
- ✓ Step 6: Deploy the device

Note

Although the workflow is designed for lab or testing scenarios, it can also be used in a production environment. Some of the steps in the workflow are interchangeable and interchanging some of the steps might make more sense in a production environment. For example, the **Create a device group** step followed by the **Register devices as Autopilot devices** step might make more sense in a production environment.

Walkthrough

Step 1: Set up Windows automatic Intune enrollment

Related content

For more information on Windows Autopilot self-deploying mode, see the following article:

- [Windows Autopilot self-deploying mode.](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Self-deploying mode: Set up Windows automatic Intune enrollment

Article • 06/20/2024 • Applies to:  Windows 11,  Windows 10

Autopilot self-deploying mode steps:

Step 1: Set up Windows automatic Intune enrollment

- Step 2: [Register devices as Autopilot devices](#)
- Step 3: [Create a device group](#)
- Step 4: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- Step 5: [Create and assign Autopilot profile](#)
- Step 6: [Deploy the device](#)

For an overview of the Windows Autopilot self-deploying mode workflow, see [Windows Autopilot self-deploying overview](#).

Note

If automatic Intune enrollment is already set up, skip this step and move on to [Step 2: Register devices as Autopilot devices](#).

Set up Windows automatic Intune enrollment

In order for Windows Autopilot to work, devices need to be able to enroll in Intune automatically. Enrolling devices in Intune automatically can be configured in the Azure portal:

1. Sign in to the [Azure portal](#).
2. Select Microsoft Entra ID.
3. In the Overview screen, under Manage in the left hand pane, select Mobility (MDM and WIP).
4. In the Mobility (MDM and WIP) screen, under Name select Microsoft Intune.
5. In the Microsoft Intune page that opens, under MDM user scope, select either All or Some:
 - If All is selected, all users can automatically enroll their devices in Intune.

- If **Some** is selected, only users in the groups specified in the link under **Groups** can automatically enroll their devices in Intune. To add groups:
 - a. Select the link under **Groups**.
 - b. In the **Select groups** window that opens, select the desired groups to add. Make sure that the groups selected are Microsoft Entra user groups that contain the desired users.
 - c. Once all of the desired groups are selected, select **Select** to close the **Select groups** window.
6. In the **Microsoft Intune** screen, if any changes were made, select **Save**.

Next step: Allow users to join devices to Microsoft Entra ID

Step 2: Register devices as Autopilot devices

Related content

For more information on Windows automatic MDM/Intune enrollment, see the following articles:

- [Enable Windows automatic enrollment](#).
- [Set up Windows automatic enrollment](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Self-deploying mode: Register devices as Autopilot devices

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot self-deploying mode steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- ✓ **Step 2: Register devices as Autopilot devices**
 - Step 3: [Create a device group](#)
 - Step 4: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 5: [Create and assign Autopilot profile](#)
 - Step 6: [Deploy the device](#)

For an overview of the Windows Autopilot self-deploying mode workflow, see [Windows Autopilot self-deploying overview](#).

Note

If devices are already registered as Windows Autopilot devices, skip this step and move on to [Step 3: Create a device group](#).

Register devices as Autopilot devices

Before a device can use Autopilot, the device must be registered as an Autopilot device. Registering a device as an Autopilot device can be thought of as importing the device into Autopilot so that Autopilot service can be used on the device. Registering a device as an Autopilot device doesn't mean that the device has used the Autopilot service. It just makes the Autopilot service available to the device.

Also note that a device registered in Autopilot doesn't mean the device is enrolled in Intune. A device might be registered as an Autopilot device but might not exist in Intune. It's not until an Autopilot registered device goes through the Autopilot process for the first time that it becomes enrolled in Intune. After the Autopilot device undergoes the Autopilot process and enrolls in Intune, the Autopilot device appears as a device in both Microsoft Entra ID and Intune.

There are several methods to register a device as an Autopilot device in Intune:

- Manually registering devices into Intune as an Autopilot device via the hardware hash. The hardware hash of a device can be collected via one of the following methods:
 - [Configuration Manager](#).
 - [PowerShell script](#).
 - [Diagnostics page hash export](#).
 - [Desktop hash export](#).

These methods of obtaining the hardware hash of a device are well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

- Automatically registering device via:
 - An [OEM](#), including [Microsoft Surface](#) devices.
 - A [partner](#).

Registering a device via an OEM or partner is also well documented. The corresponding documentation can be viewed by selecting the appropriate link from the above list.

For most organizations, using an OEM or partner to register devices as Autopilot devices is the preferred, most common, and most secure method. However for smaller organizations, for testing/lab scenarios, and for emergency scenarios, manually registering devices as Autopilot devices via the hardware hash is also used.

Important

The following type of devices shouldn't be registered as a Windows Autopilot device:

- [Microsoft Entra registered](#) devices, also known as "workplace joined" devices.
- [Intune MDM-only enrollment](#) devices.

These options are intended for users to join personally owned devices to their organization's network. Windows Autopilot registered devices are registered as corporate owned devices.

If a device is already one of these two types of devices, to register it as a Windows Autopilot device, first remove it from Microsoft Intune and Microsoft Entra ID. For more information, see [Device appears as Microsoft Entra registered instead of Microsoft Entra joined](#) and [Deregister a device](#).

Note

Assuming that a device isn't currently enrolled Intune, remember that registering a device in Autopilot doesn't make it an Intune enrolled device. That device doesn't enroll into Intune until Autopilot runs on the device for the first time.

Importing the hardware hash CSV file for devices into Intune

Several of the methods in the previous section on obtaining the hardware hash when manually registering devices as Autopilot devices produces a CSV file that contains the hardware hash of the device. This CSV file with the hardware hash needs to be imported into Intune to register the device as an Autopilot device.

After the CSV file is created, it can be imported into Intune via the following steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, select **Windows enrollment**
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens, select **Import**.
 - a. In the **Add Autopilot devices** window that opens:
 - i. Under **Specify the path to the list you want to import.**, select the blue file folder.
 - ii. Browse to the CSV file obtained using one of the above methods to obtain the hardware hash of a device.
 - iii. After selecting the CSV file, verify that the correct CSV file is selected under **Specify the path to the list you want to import.**, and then select **Import**. Selecting **Import** closes the **Add Autopilot devices** window. Importing can take several minutes.
 - b. After the import is complete, select **Sync**.

A message displays saying that the sync is in progress. The sync process might take a few minutes to complete, depending on how many devices are being synchronized.

 **Note**

If another sync is attempted within 10 minutes after initiating a sync, an error will be displayed. Syncs can only occur once every 10 minutes. To attempt a sync again, wait at least 10 minutes before trying again.

- c. Select **Refresh** to refresh the view. The newly imported devices should display within a few minutes. If the devices aren't yet displayed, wait a few minutes, and then select **Refresh** again.

Next step: Create a device group

Step 3: Create a device group

Related content

For more information on registering devices as Autopilot devices, see the following articles:

- [Manually register devices with Windows Autopilot](#).
- [Windows Autopilot customer consent](#).

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) ↗

Self-deploying mode: Create a device group

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot self-deploying mode steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Register devices as Autopilot devices](#)
- ✓ **Step 3: Create a device group**
 - Step 4: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 5: [Create and assign Autopilot profile](#)
 - Step 6: [Deploy the device](#)

For an overview of the Windows Autopilot self-deploying mode workflow, see [Windows Autopilot self-deploying overview](#).

Note

If device groups are already created, skip this step and move on to [Step 4: Configure and assign Autopilot Enrollment Status Page \(ESP\)](#). However, if deploying multiple different Autopilot scenarios to different devices, separate device groups are required for each Autopilot scenario.

Create a device group

Device groups are a collection of devices organized into a Microsoft Entra group. Device groups are used in Autopilot to target devices for specific configurations such as what policies to apply to a device and what applications to install on the device. They're also used by Autopilot to target Enrollment Status Page (ESP) configurations, Autopilot profile configurations, and domain join profiles to devices.

Device groups can be either dynamic or assigned:

- **Dynamic groups** - Devices are automatically added to the group based on rules
- **Assigned groups** - Devices are manually added to the group and are static

When an admin configures Autopilot in an enterprise environment, dynamic groups are primarily used since a large number of devices are normally involved. Adding the devices in automatically using rules makes management of the group a lot easier.

Adding a large amount of device in manually via an assigned group would be impractical. However, if there's only a few devices, for example for testing purposes, an assigned group can be used instead.

To create a dynamic device group for use with Autopilot, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Groups** in the left hand pane.
3. In the **Groups | All groups** screen, make sure **All groups** is selected, and then select **New group**.
4. In the **New Group** screen that opens:
 - a. For **Group type**, select **Security**.
 - b. For **Group name**, enter a name for the device group.
 - c. For **Group description**, enter a description for the device group.
 - d. For **Microsoft Entra roles can be assigned to the group**, select **No**.
 - e. For **Membership type**, select **Dynamic Device**. Setting the **Membership type** option to **Dynamic Device** changes the option **Members** to **Dynamic device members**.
 - f. For **Owners**, select the **No owners selected** link.
Alternatively, use the **Search** bar to search for and select owners of the group.
 - ii. Once all of the desired owners are selected, select **Select**.
- h. For **Dynamic device members**, select **Add dynamic query**. The **Dynamic membership rules** screen opens.
 - i. In the **Dynamic membership rules** screen:
 - i. Make sure that **Configure Rules** is selected at the top.
 - ii. Select **Add expression**. Rules and expressions can be added that defines what devices are added to the device group.

Rules can be entered in the rule builder via the drop-down boxes.

Alternatively, the rule syntax can be entered directly via the **Edit** option in the **Rule syntax** section.

The most common type of dynamic device group when using Windows Autopilot is a device group that contains all Windows Autopilot devices. A dynamic device group that contains all Windows Autopilot devices has the following syntax:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```

To enter in this rule:

- i. Select the **Edit** option in the **Rule syntax** section.
- ii. Paste in the following rule in the **Edit rule syntax** screen under **Rule syntax**:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]"))
```

- iii. Once the rule is pasted in, select **OK**.
- iii. Once the desired rule is entered, select **Save** on the toolbar to close the **Dynamic membership rules** window.

For more information on creating rules for dynamic groups, see [Dynamic membership rules for groups in Microsoft Entra ID](#).

- j. Select **Create** to finish creating the dynamic device group.

Note

The above steps are creating a dynamic group in Microsoft Entra that is used by Intune and Windows Autopilot solutions. Although the groups can be accessed in the Intune portal, they're Microsoft Entra groups.

Tip

For Configuration Manager admins, device groups are similar to device based collections. Dynamic device groups are similar to query based device collections while assigned device groups are similar to direct membership device collections.

Next step: Configure and assign the Enrollment Status Page (ESP)

Step 4: Configure and assign Autopilot Enrollment Status Page (ESP)

Related content

For more information on creating groups in Intune, see the following articles:

- [Create device groups.](#)
- [Add groups to organize users and devices.](#)
- [Manage Microsoft Entra groups and group membership.](#)
- [Dynamic membership rules for groups in Microsoft Entra ID.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Self-deploying mode: Configure and assign the Enrollment Status Page (ESP)

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Autopilot self-deploying mode steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Register devices as Autopilot devices](#)
- Step 3: [Create a device group](#)

Step 4: Configure and assign Autopilot Enrollment Status Page (ESP)

- Step 5: [Create and assign Autopilot profile](#)
- Step 6: [Deploy the device](#)

For an overview of the Windows Autopilot self-deploying mode workflow, see [Windows Autopilot self-deploying overview](#).

Note

If an ESP is already configured, assigned, and uses the same settings for the Windows Autopilot self-deploying mode scenario, skip this step and move on to [Step 5: Create and assign Autopilot profile](#).

The Enrollment Status Page (ESP)

The main feature of the Enrollment Status Page (ESP) is to display progress and current status to the end user while the device is being set up and enrolled via the Autopilot process. The other main feature of the ESP is to block a user from signing in and using the device until all required policies and applications are installed. Multiple ESP profiles can be created with different settings and assigned appropriately based on different needs and scenarios.

Out of box there's a default ESP that is assigned to all devices. The default setting in the default ESP is to not show app and profile progress during the Autopilot process. However, Microsoft recommends changing this default via a separate custom ESP to show app and profile progress. Enabling and configuring an ESP allows end users to properly see the progress of their device being set up and prevents them using the device until the device is fully configured and provisioned. A user signing into the device before being fully configured and provisioned can cause issues.

The ESP has two phases:

- **Device ESP** - The portion of the ESP that runs during the OOBE process and applies device policies and installs device applications.
- **User ESP** - The portion of the ESP that sets up user account, applies user policies, and installs user applications.

Device ESP runs first followed by the User ESP.

 **Tip**

For Configuration Manager admins, an ESP is similar and analogous to Configuration Manager client settings.

Autopilot Enrollment Status Page (ESP) configuration options

When the Enrollment Status Page (ESP) is configured, it has several options that can be configured to meet the needs of the organization. The following lists the different options and their possible configurations:

- **Show an error when installation takes longer than specified number of minutes:**
 - The default time-out is 60 minutes. Enter a higher value if more time is needed to install applications on the devices.
- **Show custom message when time limit or error occur:**
 - **No:** The default message is shown to users when an error occurs. That message is: **Setup could not be completed. Please try again or contact your support person for help.**
 - **Yes:** A custom message is shown to users when an error occurs. Enter a custom message in the provided text box.
- **Turn on log collection and diagnostics page for end users:**
 - **No:** The collect logs button isn't shown to users when an installation error occurs. The Windows Autopilot diagnostics page isn't shown on devices running Windows 11.
 - **Yes:** The collect logs button is shown to users when an installation error occurs. The Windows Autopilot diagnostics page is shown on devices running Windows

11. Logs and diagnostics might aid with troubleshooting. For this reason, Microsoft recommends enabling this option.

- **Only show page to devices provisioned by out-of-box experience (OOBE):**
 - **No:** The enrollment status page (ESP) is shown during the device phase and the out-of-box experience (OOBE). The page is also shown during the user phase to every user who signs into the device for the first time.
 - **Yes:** The enrollment status page (ESP) is shown during the device phase and the OOBE. The page is also shown during the user phase, but only to the first user who signs into the device. It isn't shown to subsequent users who sign into the device.
- **Block device use until all apps and profiles are installed:**
 - **No:** Users can leave the ESP before Intune is finished setting up the device.
 - **Yes:** Users can't leave the ESP until Intune is done setting up the device.
Enabling this option unlocks the following additional options:
 - **Allow users to reset device if installation error occurs:**
 - **No:** The ESP doesn't give users the option to reset their devices when an installation fails.
 - **Yes:** The ESP gives users the option to reset their devices when an installation fails.
 - **Allow users to use device if installation error occurs:**
 - **No:** The ESP doesn't give users the option to bypass the ESP when an installation fails.
 - **Yes:** The ESP gives users the option to bypass the ESP and use their devices when an installation fails.
 - **Block device use until these required apps are installed if they are assigned to the user/device:**
 - **All:** All assigned apps must be installed before users can use their devices.
 - **Selected:** Selected apps must be installed before users can use their devices. After enabling this option, select **Select apps** to select the managed apps from Intune that are required to be installed before users can use their device.

Configure and assign the Enrollment Status Page (ESP)

To configure and assign the Autopilot Enrollment Status Page (ESP), follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
- 1 In the **Devices | Overview** screen, under **By platform**, select **Windows**.
 1. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
 2. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Enrollment Status Page**.
 3. In the **Enrollment Status Page** screen that opens, select **Create**.
 4. The **Create profile** screen opens. In the **Basics** page:
 - a. Next to **Name**, enter a name for the ESP profile.
 - b. Next to **Description**, enter a description.
 - c. Select **Next**.
 5. In the **Settings** page, toggle the option **Show app and profile configuration progress** to **Yes**.
 - a. After the option **Show app and profile configuration progress** is toggled to **Yes**, several new options will appear. Configure these options based on the desired behavior for the ESP as described in the section [Autopilot Enrollment Status Page \(ESP\) configuration options](#):
 - b. Once the different ESP options under the **Settings** page are configured as desired, select **Next**.
 6. In the **Assignments** page:
 - a. Under **Included groups**, select **Add groups**.
 - b. In the **Select groups to include** window that opens, select the device groups to target the ESP profile. The device groups selected would normally be the device groups created in the **Create device group** step.

- c. After selecting the device group, select **Select** to close the **Select groups to include** window.

 **Tip**

After selecting the device groups, the **Edit filter** option can be selected on each device group added to the assignment to further refine what devices are targeted for the ESP profile. For example, further filtering can be useful if some of the devices that are members in the device groups selected need to be excluded.

- d. Select **Next**.

 **Note**

An ESP is assigned to a device group and not directly to individual devices. To assign an ESP to a specific device, the device must be a member of a device group that has an ESP assigned to it.

7. In the **Scope tags** page, select **Next**.

 **Note**

Scope tags are optional and are a method to control who has access to the ESP configuration. For this tutorial, scope tags are being skipped and left at the default scope tag. However if a custom scope tag needs to be specified, do so at this screen. For more information about scope tags, see [Use role-based access control and scope tags for distributed IT](#).

8. In the **Review + create** page, verify that the settings are correct and configured as desired. Once verified, select **Create** to save the changes and assign the ESP profile.

Next step: Create and assign self-deploying mode Autopilot profile

[Step 5: Create and assign Autopilot profile](#)

Related content

For more information on the Enrollment Status Page (ESP), see the following articles:

- [Windows Autopilot Enrollment Status Page](#).
 - [Set up the Enrollment Status Page](#).
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Self-deploying mode: Create and assign self-deploying Autopilot profile

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Autopilot self-deploying mode steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
- Step 2: [Register devices as Autopilot devices](#)
- Step 3: [Create a device group](#)
- Step 4: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
- ✓ Step 5: **Create and assign Autopilot profile**
- Step 6: [Deploy the device](#)

For an overview of the Windows Autopilot self-deploying mode workflow, see [Windows Autopilot self-deploying overview](#).

Create and assign self-deploying Autopilot profile

The Autopilot profile specifies how the device is configured during Windows Setup and what is shown during the out-of-box experience (OOBE).

Tip

For Configuration Manager admins, the Autopilot profile is similar to some of the configuration that takes place during a task sequence via an `unattend.xml` file. The `unattend.xml` file is configured during the **Apply Windows Settings** and **Apply Network Settings** steps. Note however that Autopilot doesn't use `unattend.xml` files.

To create a self-deploying mode Autopilot profile, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.

4. In the Windows | Windows devices screen, under Device onboarding, select Enrollment.
5. In the Windows | Windows enrollment screen, under Windows Autopilot, select Deployment Profiles.
6. In the Windows Autopilot deployment profiles screen, select the Create Profile drop down menu and then select Windows PC.
7. The Create profile screen opens. In the Basics page:
 - a. Next to Name, enter a name for the Autopilot profile.
 - b. Next to Description, enter a description.
 - c. Select Next.

 Note

Microsoft recommends setting the option **Convert all targeted devices to Autopilot** to Yes. This tutorial concentrates on new devices where the device is manually imported as an Autopilot device using the hardware hash. However, this option can be helpful when assigning Autopilot profiles to device groups that contain existing devices. For example, this option is helpful when using the [Windows Autopilot for existing devices](#) scenario. With Windows Autopilot for existing devices, existing devices might need to be registered as an Autopilot device after the Autopilot deployment completes. For more information, see [Register device for Windows Autopilot](#).

8. In the Out-of-box experience (OOBE) page:
 - For Deployment mode, select Self-Deploying.
 - Join to Microsoft Entra ID as defaults to Microsoft Entra joined, is greyed out, and can't be changed. Only Microsoft Entra joined is available because self-deploying mode only supports Microsoft Entra join. Self-deploying modes doesn't support Microsoft Entra hybrid join.
 - Microsoft Software License Terms defaults to Hide, is greyed out, and can't be changed.
 - Privacy settings defaults to Hide, is greyed out, and can't be changed.

- **Hide change account options** defaults to **Hide**, is greyed out, and can't be changed.
- **User account type** defaults to **Standard**, is greyed out, and can't be changed.
- For **Language (Region)**, select **Operating system default** to use the default language for the operating system being configured. If another language is desired, select the desired language from the drop-down list.
- For **Automatically configure keyboard**, select **Yes** to skip the keyboard selection page.

 **Note**

If users should select their keyboard layout, then select **No** instead. However, the purpose of Autopilot self-deploying mode is to deploy a device with minimal to no user interaction. Setting **Automatically configure keyboard** to **No** requires additional user interaction.

- For **Apply device name template**, select **No**. Alternatively, **Yes** can be chosen to apply a device name template. Be aware of the following if the name template is selected to **Yes**:
 - Names must be 15 characters or less, and can have letters, numbers, and hyphens.
 - Names can't be all numbers.
 - Use the **%SERIAL%** macro to add a hardware-specific serial number.
 - Use the **%RAND:x%** macro to add a random string of numbers, where x equals the number of digits to add.

 **Note**

If the language/region and keyboard screens are set to hidden, they might still be displayed if there's no network connectivity at the start of the Autopilot deployment. When there's no network connectivity at the start of the deployment, the Autopilot profile, where the settings to hide these screens is defined, hasn't downloaded yet. Once network connectivity is established, the Autopilot profile is downloaded and any additional screen settings should work as expected.

9. Once the options in the **Out-of-box experience (OOBE)** page are configured as desired, select **Next**.

10. In the **Assignments** page:

- a. Under **Included groups**, select **Add groups**.

 **Note**

Make sure to add the correct device groups under **Included groups** and not under **Excluded groups**. Accidentally adding the desired device groups under **Excluded groups** prevents devices in those device groups from receiving the Autopilot profile.

- a. In the **Select groups to include** window that opens, select the groups that the Windows Autopilot profile should be assigned to. These device groups are normally the device groups created in the previous **Create device group** step. Once done, select **Select**.

- b. Under **Included groups > Groups**, ensure the correct groups are selected, and then select **Next**.

11. In the **Review + Create** page, verify that all settings are set correctly, and then select **Create** to create the Autopilot profile.

Verify device has an Autopilot profile assigned to it

Before deploying a device, ensure that an Autopilot profile is assigned to a device group that the device is a member of. Autopilot profile assignment to a device can take some time after the Autopilot profile is assigned to the device group or after the device is added to the device group. To verify that the profile is assigned to a device, follow these steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen that opens:

- a. Find the desired device that Autopilot deployment profile assignment status needs to be checked.
- b. Once the device is located, its current status is listed under the **Profile status** column. The status has one of the following values:
 - **Not assigned:** An Autopilot deployment profile isn't assigned to the device.
 - **Assigning:** An Autopilot deployment profile is being assigned to the device.
 - **Assigned:** An Autopilot deployment profile is assigned to the device.
 - **Fix pending:** When a hardware change occurs on a device, this status displays while Intune tries to register the new hardware. When the link for the **Fix pending** status is selected, the following message appears:

We've detected a hardware change on this device. We're trying to automatically register the new hardware. You don't need to do anything now; the status will be updated at the next check in with the result.

If Intune is able to successfully register the new hardware, Intune updates the profile status when the device next checks into Intune. For more information on the **Fix pending** status, see the following articles:

- [Autopilot profile not applied after reimaging to an older OS version](#).
- [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
- [Windows Autopilot motherboard replacement scenario guidance](#)
- **Attention required:** If Intune is unable to register the new hardware after a hardware change occurs on a device, the device can't receive the Autopilot profile until the device is reset and the device re-registers. For more information on this status and how to deregister/re-register a device, see the following articles:
 - [Autopilot profile not applied after reimaging to an older OS version](#).
 - [Return of key functionality for Windows Autopilot sign-in and deployment experience ↗](#).
 - [Windows Autopilot motherboard replacement scenario guidance](#)
 - [Deregister a device](#)

Before starting the Autopilot deployment process on a device, make sure that in the **Windows Autopilot devices** page:

- The device's **Profile status** status is **Assigned**.
- In the properties of the device, **Date assigned** has a value.
- In the properties of the device, **Assigned profile** displays the expected Autopilot profile.

 **Note**

Intune periodically checks for new devices in the assigned device groups, and then begins the process of assigning profiles to those devices. Due to several different factors involved in the process of Autopilot profile assignment, an estimated time for the assignment can vary from scenario to scenario. These factors can include Microsoft Entra groups, membership rules, hash of a device, Intune and Autopilot services, and internet connection. The assignment time varies depending on all the factors and variables involved in a specific scenario.

Next step: Deploy the device

[Step 6: Deploy the device](#)

Related content

For more information on configuring Autopilot profiles, see the following articles:

- [Configure Autopilot profiles](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Self-deploying mode: Deploy the device

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot self-deploying mode steps:

- Step 1: [Set up Windows automatic Intune enrollment](#)
 - Step 2: [Register devices as Autopilot devices](#)
 - Step 3: [Create a device group](#)
 - Step 4: [Configure and assign Autopilot Enrollment Status Page \(ESP\)](#)
 - Step 5: [Create and assign Autopilot profile](#)
- Step 6: Deploy the device**

For an overview of the Windows Autopilot self-deploying mode workflow, see [Windows Autopilot self-deploying overview](#).

Deploy the device

Once all of the configurations for the Windows Autopilot self-deploying deployment are on the Intune and Microsoft Entra ID side, the next step is to start the Autopilot deployment process on the device. If desired, deploy any additional applications and policies that should run during the Autopilot deployment to a device group that the device is a member of.

To start the Windows Autopilot deployment process on the device, acquire a device that is part of the device group created in the previous [Create a device group](#) step. Once the device is acquired, follow these steps:

1. If a wired network connection is available, connect the device to the wired network connection.
2. Power on the device.
3. Once the device boots up, one of two things occurs depending on the state of network connectivity:
 - If the device is connected to a wired network and has network connectivity, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
 - If the device isn't connected to a wired network or if it doesn't have network connectivity, it prompts to connect to a network. Connectivity to the Internet

is required:

- a. The out-of-box experience (OOBE) begins and a screen asking for a country or region appears. Select the appropriate country or region, and then select **Yes**.
- b. The keyboard screen appears to select a keyboard layout. Select the appropriate keyboard layout, and then select **Yes**.
- c. An additional keyboard layouts screen appears. If needed, select additional keyboard layouts via **Add layout**, or select **Skip** if no additional keyboard layouts are needed.

 **Note**

When there's no network connectivity, the device can't download the Autopilot profile to know what country/region and keyboard settings to use. For this reason, when there's no network connectivity, the country/region and keyboard screens appear even if these screens are set to hidden in the Autopilot profile. These settings need to be specified in these screens in order for the network connectivity screens that follow to work properly.

- d. The **Let's connect you to a network** screen appears. At this screen, either plug the device into a wired network (if available), or select and connect to a wireless Wi-Fi network.
 - e. Once network connectivity is established, the **Next** button should become available. Select **Next**.
 - f. At this point, the device might reboot to apply critical security updates (if available or applicable). After the reboot to apply critical security updates, the Autopilot process begins.
4. The Enrollment Status Page (ESP) appears. The Enrollment Status Page (ESP) displays progress during the provisioning process across three phases:
- **Device preparation** (Device ESP)
 - **Device setup** (Device ESP)
 - **Account setup** (User ESP)

The first two phases of **Device preparation** and **Device setup** are part of the Device ESP while the final phase of **Account setup** is part of the User ESP. For

Windows Autopilot self-deploying mode, only the Device ESP and its related two related phases (**Device preparation** and **Device setup**) run. User ESP and **Account setup** don't run until after the Windows Autopilot self-deploying deployment is complete and a user signs in.

5. Once **Device setup** and the device ESP process completes, the Windows Autopilot self-deploying deployment is complete, and the Windows sign-on screen appears.
6. At this point, the end-user can sign into the device using their Microsoft Entra credentials. When the user signs in, the user ESP and **Account setup** phase runs. Once user ESP and **Account setup** completes, the provisioning process completes, the desktop appears, and the end-user can start using the device.

Deployment tips

- Before the Autopilot deployment is started, Microsoft recommends having:
 - At least one type of policy and at least one application assigned to the devices.
 - At least one type of policy and at least one application assigned to the users.

These assignments ensure proper testing of the Windows Autopilot deployment during the Device ESP phase. It might also prevent possible issues when there are either no policies or no applications assigned to the device.

- For Windows Autopilot self-deploying mode:
 - Any user assigned to the device is ignored during the Windows Autopilot self-deploying deployment.
 - User ESP doesn't run until after the Windows Autopilot self-deploying deployment completes and a user signs in.

However, for testing purposes, assigning at least one policy and at least one application to users is still recommended.

- Depending on how the Autopilot profile was configured at the [Create and assign Autopilot profile](#) step, the **Keyboard** screen might appear at the start of the deployment.
- To view and hide detailed progress information in the ESP during the provisioning process:
 - **Windows 10:** To show details, next to the appropriate phase select **Show details**. To hide the details, next to the appropriate phase select **Hide details**.

- o Windows 11: To show details, next to the appropriate phase select V. To hide the details, next to the appropriate phase select A.
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Step by step tutorial for Windows Autopilot deployment for existing devices in Intune and Configuration Manager

Article • 06/19/2024 • Applies to: Windows 11, Windows 10

This step by step tutorial guides through using Intune and Microsoft Configuration Manager to perform a Windows Autopilot deployment for existing devices.

The purpose of this tutorial is a step by step guide for all the configuration steps required for a successful Autopilot deployment for existing devices using Intune and Microsoft Configuration Manager. The tutorial is also designed as a walkthrough in a lab or testing scenario, but can be expanded for use in a production environment. This tutorial assumes familiarity with Microsoft Configuration Manager and that Microsoft Configuration Manager is already set up and configured to support operating system deployments.

Windows Autopilot deployment for existing devices overview

The main use case scenario for Windows Autopilot is to automate the configuration of Windows on a new device delivered directly from an IT department, OEM, or reseller. However, sometimes existing devices in an environment need to be repurposed, fixed, or updated to a later version of Windows by reinstalling Windows on the device.

Reinstalling of Windows is usually performed via a reimage of the device, which is outside the capabilities of Windows Autopilot. Windows Autopilot also isn't able to perform a fresh install of Windows if the version of Windows is different than the one that is currently installed on the device. There might also be other conditions that prevent Windows Autopilot from performing a fresh install of Windows on the device. For example, corruption of the current Windows install or a hard drive failure.

Windows Autopilot can utilize Microsoft Configuration Manager task sequences for scenarios where Windows needs to be:

- Reinstalled to a later version of Windows using a fresh installation of Windows.
- Updated to a later version of Windows using a fresh installation of Windows.

Microsoft Configuration Manager task sequences can reimagine a device and perform a fresh installation of Windows. The Configuration Manager task sequence can also pre-install a Windows Autopilot profile on the device via a JSON file. Once the Configuration Manager task sequence is done, the device can then automatically run the Windows Autopilot deployment defined in the Windows Autopilot profile JSON file. When the Windows Autopilot profile JSON file is pre-installed on the device, the Windows Autopilot deployment can run on the device without having to first perform the following actions:

- Import the device into Intune as an Autopilot device.
- Assign an Autopilot profile to the device.

Windows Autopilot deployment for existing devices is useful for the following scenarios:

- Repurpose an existing device that isn't yet an Autopilot device.
- Migrate an on-premises domain joined device that isn't part of Microsoft Entra ID to a Microsoft Entra join device.
- Convert an on-premises domain joined device that is Microsoft Entra hybrid joined to a Microsoft Entra join device.
- Reinstall Windows on devices that need to be repaired. For example, a device that has a corrupted Windows installation or where the hard drive was replaced.
- Upgrade older versions of Windows that don't support Microsoft Entra ID (Windows 8.1) to a version of Windows that does support Microsoft Entra ID (Windows 10/Windows 11).
- Using custom Windows images instead of the OEM provided Windows installation.

Windows Autopilot deployment for existing devices can be viewed as a method to prepare an existing device for an Autopilot deployment.

Note

The JSON file for Windows Autopilot for existing devices only supports user-driven Microsoft Entra ID and user-driven hybrid Microsoft Entra Autopilot profiles. Self-deploying and pre-provisioning Autopilot profiles aren't supported with JSON files due to these scenarios requiring TPM attestation. TPM attestation only works where there's an existing Autopilot device since the TPM attestation information is stored in the Autopilot device object.

However, during the Windows Autopilot for existing devices deployment, if the following conditions are true:

- Device is already a Windows Autopilot device before the deployment begins
- Device has an Autopilot profile assigned to it

then the assigned Autopilot profile takes precedence over the JSON file installed by the task sequence. In this scenario, if the assigned Autopilot profile is either a self-deploying or pre-provisioning Autopilot profile, then the self-deploying and pre-provisioning scenarios are supported.

Workflow

The following steps are needed to configure and then perform a Windows Autopilot deployment for existing devices deployment using Intune and Microsoft Configuration Manager:

- ✓ Step 1: Set up a Windows Autopilot profile
- ✓ Step 2: Install required modules to obtain Autopilot profiles from Intune
- ✓ Step 3: Create JSON file for Autopilot profiles
- ✓ Step 4: Create and distribute package for JSON file in Configuration Manager
- ✓ Step 5: Create Autopilot task sequence in Configuration Manager
- ✓ Step 6: Create collection in Configuration Manager
- ✓ Step 7: Deploy Autopilot task sequence to collection in Configuration Manager
- ✓ Step 8: Speed up the deployment process (optional)
- ✓ Step 9: Run Autopilot task sequence on device
- ✓ Step 10: Register device for Windows Autopilot

ⓘ Important

If enrollment restrictions are configured to block personal devices from enrolling, Autopilot for existing devices can't be used. For more information, see [What are enrollment restrictions?: Blocking personal Windows devices](#).

Walkthrough

Step 1: Set up a Windows Autopilot profile

Related content

For more information on Windows Autopilot deployment for existing devices, see the following articles:

- [Windows Autopilot deployment for existing devices](#).

- New Windows Autopilot capabilities and expanded partner support simplify modern device deployment ↗ .
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Windows Autopilot deployment for existing devices: Set up a Windows Autopilot profile

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

Step 1: Set up a Windows Autopilot profile

- Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
- Step 3: [Create JSON file for Autopilot profiles](#)
- Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
- Step 5: [Create Autopilot task sequence in Configuration Manager](#)
- Step 6: [Create collection in Configuration Manager](#)
- Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
- Step 8: [Speed up the deployment process \(optional\)](#)
- Step 9: [Run Autopilot task sequence on device](#)
- Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Set up a Windows Autopilot profile

Windows Autopilot deployment for existing devices isn't an Autopilot deployment where an Autopilot profile is downloaded and applied to a device during the out-of-box experience (OOBE) of Windows Setup. Instead, it prepares a device to receive an Autopilot profile by performing the following actions:

- Wipes the device.
- Installs a fresh copy of Windows.
- Installs a JSON file that contains the information for an existing Autopilot profile.

The first step in a Windows Autopilot for existing devices deployment is to make sure there's already an existing valid Autopilot profile in Intune so that the JSON file can be created. Since the JSON file only supports the user-driven Microsoft Entra join and user-driven Microsoft Entra hybrid join Autopilot scenarios, one of the following steps from the respective scenario workflows can be used to create a valid Autopilot profile:

- User-driven Microsoft Entra join: Create and assign user-driven Microsoft Entra join Autopilot profile
- User-driven Microsoft Entra hybrid join: Create and assign user-driven Microsoft Entra hybrid join Autopilot profile

 **Note**

In the above steps, it's not necessary to assign the Autopilot profile for Windows Autopilot deployment for existing devices scenario to work. The Autopilot profile only needs to be created so that the JSON file can then be created.

Once a valid Windows Autopilot profile is created and confirmed working on an existing Autopilot device, then proceed to [Step 2: Install required modules to obtain Autopilot profiles from Intune](#).

Next step: Install required modules to obtain Autopilot profiles from Intune

Step 2: Install required modules to obtain Autopilot profiles from Intune

Related content

For more information on configuring Autopilot profiles, see the following articles:

- [Configure Autopilot profiles](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Windows Autopilot deployment for existing devices: Install required modules to obtain Autopilot profiles from Intune

Article • 06/26/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
- ✓ Step 2: **Install required modules to obtain Autopilot profiles from Intune**
- Step 3: [Create JSON file for Autopilot profiles](#)
- Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
- Step 5: [Create Autopilot task sequence in Configuration Manager](#)
- Step 6: [Create collection in Configuration Manager](#)
- Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
- Step 8: [Speed up the deployment process \(optional\)](#)
- Step 9: [Run Autopilot task sequence on device](#)
- Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Install required modules to obtain Autopilot profiles from Intune

Note

The PowerShell code snippets in this section were updated in July of 2023 to use the Microsoft Graph PowerShell modules instead of the deprecated AzureAD Graph PowerShell modules. The Microsoft Graph PowerShell modules might require approval of additional permissions in Microsoft Entra ID when they're first used. The code snippets were also updated to force using an updated version of the WindowsAutoPilot module. For more information, see [AzureAD](#) and [Important: Azure AD Graph Retirement and PowerShell Module Deprecation](#).

After making sure there's a valid Autopilot profile, the next step is to download the existing Autopilot profiles from Intune as JSON files. The JSON files contain all of the information regarding the Intune tenant and the Autopilot profile. After the JSON files are downloaded from Intune, Configuration Manager packages that contain the JSON files are created. The Configuration Manager packages are then used to install the JSON file on the device during the Windows Autopilot deployment for existing devices task sequence.

The JSON file is installed on the device to the offline Windows installation during the WinPE portion of the Configuration Manager task sequence. The JSON file makes the Autopilot profile available to the Windows out-of-box experience (OOBE) so that it can run the Autopilot deployment when Windows is started for the first time. The JSON file eliminates the need for Windows OOBE to have to first download the Autopilot profile from Intune.

Note

Windows OOBE still checks to see if there are any Autopilot profiles assigned to the device even if a JSON file is present. If the device is an Autopilot device and there's an Autopilot profile assigned to the device, the Autopilot profile is downloaded from Intune and used instead of the JSON file.

Before the Autopilot profiles are downloaded from Intune as JSON files, certain modules need to be installed on the device where the Autopilot profile will be downloaded. These modules are required to obtain the Autopilot profile from Intune. For this tutorial and to simplify the process, installation of these modules is performed on the Configuration Manager site server. However, any device with access to Intune can be used.

To install the necessary modules to download the Autopilot profiles as a JSON file, follow these steps:

1. Sign into the Configuration Manager site server or other device that can access Intune.
2. On the device, open a PowerShell window as an administrator by right-clicking on the **Start** menu and selecting **Windows PowerShell (Admin)/Windows Terminal (Admin)** and then selecting **Yes** at the **User Account Control (UAC)** prompt.
3. Copy the following commands by selecting **Copy** at the top right corner of the below **PowerShell** code block:

PowerShell

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Install-Module -Name WindowsAutopilotIntune -MinimumVersion 5.4.0 -Force
Install-Module -Name Microsoft.Graph.Groups -Force
Install-Module -Name Microsoft.Graph.Authentication -Force
Install-Module Microsoft.Graph.Identity.DirectoryManagement -Force

Import-Module -Name WindowsAutopilotIntune -MinimumVersion 5.4
Import-Module -Name Microsoft.Graph.Groups
Import-Module -Name Microsoft.Graph.Authentication
Import-Module -Name Microsoft.Graph.Identity.DirectoryManagement
```

4. Paste the commands into the elevated PowerShell window and then select **Enter** on the keyboard to run the commands. **Enter** might need to be selected a second time to run the last command in the code block. Once all the commands run successfully, the required modules are installed.

Verify that Autopilot profiles from Intune can be viewed

Once the required modules are installed, the following steps can be taken to verify that Autopilot profiles from Intune can be viewed:

ⓘ Note

The following steps don't export the Autopilot profiles as a JSON file. It only verifies that the Autopilot profiles can be viewed.

1. Copy the following command by selecting **Copy** at the top right corner of the below **PowerShell** code block:

PowerShell

```
Connect-MgGraph -Scopes "Device.ReadWrite.All",
"DeviceManagementManagedDevices.ReadWrite.All",
"DeviceManagementServiceConfig.ReadWrite.All", "Domain.ReadWrite.All",
"Group.ReadWrite.All", "GroupMember.ReadWrite.All", "User.Read"
```

2. Paste the command into the elevated PowerShell window and then select **Enter** on the keyboard to run the command.
3. A **Sign in to your account** window appears. Sign in with a Microsoft Entra account that has access to Intune and the Autopilot profiles.

4. Copy the following command by selecting **Copy** at the top right corner of the below **PowerShell** code block:

PowerShell

```
Get-AutopilotProfile | ConvertTo-AutopilotConfigurationJSON
```

5. Paste the command into the elevated PowerShell window and then select **Enter** on the keyboard to run the command.

6. All Autopilot profiles available in Intune are displayed in the PowerShell window in JSON format. Each individual Autopilot profile is encapsulated within braces ({}).

Next step: Create JSON file for Autopilot profiles

Step 3: Create JSON file for Autopilot profiles

Related content

For more information on installing the required modules to obtain Autopilot profiles from Intune, see the following articles:

- [Install required modules.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot deployment for existing devices: Create JSON file for Autopilot profiles

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
- Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
- ✓ Step 3: [Create JSON file for Autopilot profiles](#)
 - Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
 - Step 5: [Create Autopilot task sequence in Configuration Manager](#)
 - Step 6: [Create collection in Configuration Manager](#)
 - Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
 - Step 8: [Speed up the deployment process \(optional\)](#)
 - Step 9: [Run Autopilot task sequence on device](#)
 - Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Create JSON file for Autopilot profiles

Note

The PowerShell code snippets in this section were updated in July of 2023 to use the Microsoft Graph PowerShell modules instead of the deprecated AzureAD Graph PowerShell modules. The Microsoft Graph PowerShell modules might require approval of additional permissions in Microsoft Entra ID when they're first used. For more information, see [AzureAD](#) and [Important: Azure AD Graph Retirement and PowerShell Module Deprecation](#).

Once the proper modules are installed to allow exporting of Autopilot profiles from Intune, the next step is to export the Autopilot profiles as JSON files. The JSON files are used to create a package in Configuration Manager.

To export the Autopilot profiles as JSON files, follow these steps:

1. Sign into the Configuration Manager site server or other device where the required modules were installed in the [Install required modules to obtain Autopilot profiles from Intune](#) step.
2. On the device, open a PowerShell window as an administrator by right-clicking on the **Start** menu and selecting **Windows PowerShell (Admin)/Windows Terminal (Admin)** and then selecting **Yes** at the **User Account Control** (UAC) prompt.
3. Copy the following commands by selecting **Copy** at the top right corner of the below **PowerShell** code block:

PowerShell

```
Connect-MgGraph -Scopes "Device.ReadWrite.All",
"DeviceManagementManagedDevices.ReadWrite.All",
"DeviceManagementServiceConfig.ReadWrite.All", "Domain.ReadWrite.All",
"Group.ReadWrite.All", "GroupMember.ReadWrite.All", "User.Read"
$AutopilotProfile = Get-AutopilotProfile
$targetDirectory = "C:\Autopilot"
$AutopilotProfile | ForEach-Object {
    New-Item -ItemType Directory -Path
"$targetDirectory\$($_.displayName)"
    $_ | ConvertTo-AutopilotConfigurationJSON | Set-Content -Encoding
Ascii
"$targetDirectory\$($_.displayName)\AutopilotConfigurationFile.json"
}
```

4. Paste the commands into the elevated PowerShell window and then select **Enter** on the keyboard to run the commands. If the elevated PowerShell command window isn't already signed into Intune, a **Sign in to your account** window appears. Sign in with a Microsoft Entra account that has access to Intune and the Autopilot profiles.
5. Once signed into Intune, **Enter** might need to be selected a second time to run the last command in the code block.
6. Once all the commands run successfully, the Autopilot profiles appears in a subfolder under the folder specified by the `$targetDirectory` variable. By default, the `$targetDirectory` variable is `C:\AutoPilot`, but it can be changed to another location if desired. The subfolder has the name of the Autopilot profile from Intune. If there are multiple Autopilot profiles, each profile has its own subfolder. In each folder, there's a JSON file named `AutopilotConfigurationFile.json`.

 **Note**

The above script exports all Autopilot profiles from Intune. In addition to supported user-driven Autopilot profiles, it also downloads unsupported pre-provisioning Autopilot profiles and self-deploying Autopilot profiles if they exist in the environment.

Next step: Create and distribute package for JSON file in Configuration Manager

Step 4: Create and distribute package for JSON file in Configuration Manager

Related content

For more information on creating the JSON file, see the following articles:

- [Create the JSON file.](#)
- [Get Autopilot profiles for existing devices.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot deployment for existing devices: Create and distribute package for JSON file in Configuration Manager

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
 - Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
 - Step 3: [Create JSON file for Autopilot profiles](#)
- Step 4: Create and distribute package for JSON file in Configuration Manager**
- Step 5: [Create Autopilot task sequence in Configuration Manager](#)
 - Step 6: [Create collection in Configuration Manager](#)
 - Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
 - Step 8: [Speed up the deployment process \(optional\)](#)
 - Step 9: [Run Autopilot task sequence on device](#)
 - Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Create packages for JSON files in Configuration Manager

Once the JSON files are created for the Autopilot profiles, a package needs to be created in Configuration Manager that contains the contents of the JSON files.

Important

The JSON files used by Windows Autopilot deployment for existing devices only support [Windows Autopilot user-driven Microsoft Entra join](#) and [Windows Autopilot user-driven Microsoft Entra hybrid join](#) Autopilot profiles. When creating the packages for JSON files in Configuration Manager, make sure the

JSON files are only for user-driven Microsoft Entra join and user-driven Microsoft Entra hybrid join Autopilot profiles.

To create a package containing the JSON file in Configuration Manager, follow these steps:

1. Copy the folders containing the JSON files created in the [Create JSON file for Autopilot profiles](#) step to a new empty folder in the organization's UNC network path. The UNC network path should be the path that contains package sources for Configuration Manager packages.
2. On a device where the Configuration Manager console is installed, such as a Configuration Manager site server, open the Configuration Manager console.
3. In the left hand pane of the Configuration Manager console, navigate to **Software Library > Overview > Application Management**.
4. Select **Packages** and then on the ribbon, select **Create Package**. Alternatively, right-click **Packages** and select **Create Package**.
5. The **Create Package and Program Wizard** window appears:
 - a. In the **Specify information about this package** page, enter the following details for the package:
 - i. Next to **Name**, enter an identifiable name for the Autopilot scenario that the JSON file is for.
 - ii. Next to **Description**, enter a description for the Autopilot scenario that the JSON file is for.
 - iii. Select the checkbox **This package contains source files**, and then select **Browse** next to **Source folder**:
 - iv. The **Set Source Folder** window appears. In the **Set Source Folder** window:
 - i. Select **Browse** and navigate to the folder containing the individual **AutopilotConfigurationFile.json** JSON file from the UNC path in Step 1.
 - ii. Once in the folder containing the **AutopilotConfigurationFile.json** JSON file, select **Select Folder**.
 - iii. Confirm the path under **Source folder** is correct, and then select **OK**.

 **Important**

If multiple Autopilot profiles were copied to a UNC network path, make sure to select the folder that contains the individual **AutopilotConfigurationFile.json** JSON file and not the parent folder that contains all of the different Autopilot profiles. Each Autopilot JSON file requires an individual package in Configuration Manager.

- b. Select the **Next >** button.
 - c. In the **Choose the program type that you want to create** page, select the **Do not create a program** option, and then select the **Next >** button.
 - d. In the **Confirm the settings** page, verify all settings are correct, and then select the **Next >** button.
 - e. When the **Create Package and Program Wizard** completes with **The task "Create Package and Program Wizard" completed successfully** message, select the **Close** button.
6. If there are multiple Autopilot JSON files, repeat the above steps for any additional supported Autopilot profile JSON files that were exported as part of the [Create JSON file for Autopilot profiles](#) step. Make sure that each package has a unique identifiable name.

Distribute packages for JSON files in Configuration Manager

Once the package containing the Autopilot profile JSON file is created, the package needs to be distributed to Configuration Manager distribution points. To distribute the package containing the Autopilot profile JSON file in Configuration Manager, follow these steps:

1. On a device where the Configuration Manager console is installed, such as a Configuration Manager site server, open the Configuration Manager console.
2. In the left hand pane of the Configuration Manager console, navigate to **Software Library > Overview > Application Management**.
3. Expand **Packages** and locate the Autopilot profile JSON packages created in the section [Create packages for JSON files in Configuration Manager](#).
4. Select the Autopilot profile JSON package and in the ribbon select **Distribute Content**. As an alternative, right-click the Autopilot profile JSON package and

select **Distribute Content**.

5. The **Distribute Content Wizard** appears:

- a. In the **Review selected content** page, verify the correct package is selected and then select the **Next >** button.
 - b. In the **Specify the content destination** page, select **Add**, and then select either **Distribution Point** or **Distribution Point Group**.
 - The **Add Distribution Points** or **Add Distribution Point Groups** window appears. Select the desired distribution points or distribution point groups to distribute the package to and then select **OK**.
 - c. Select the **Next >** button.
 - d. In the **Confirm the settings** page, verify all settings are correct, and then select the **Next >** button.
 - e. When the **Distribute Content Wizard** completes with **The task "Distribute Content Wizard" completed successfully** message, select the **Close** button.
6. With the package still selected under **Packages**, in the lower pane of the Configuration Manager console under **Related Objects**, select **Content Status**.
7. Monitor the distribution of the package until it successfully distributes to all distribution points. For details of the distribution status to each distribution point, under **Completion Statistics** in the lower pane of the Configuration Manager console, select the **View Status** option.
8. If there are multiple Autopilot JSON file packages, repeat the above steps for any additional Autopilot profile JSON file packages created in the section [Create packages for JSON files in Configuration Manager](#).

Next step: Create Autopilot task sequence in Configuration Manager

[Step 5: Create Autopilot task sequence in Configuration Manager](#)

Related content

For more information on creating and distributing the JSON package in Configuration Manager, see the following articles:

- Create a package containing the JSON file.
 - Packages and programs in Configuration Manager.
 - Distribute content to distribution points.
-

Feedback

Was this page helpful?



Yes



No

Provide product feedback ↗

Windows Autopilot deployment for existing devices: Create Autopilot task sequence in Configuration Manager

Article • 06/27/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
 - Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
 - Step 3: [Create JSON file for Autopilot profiles](#)
 - Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
- Step 5: Create Autopilot task sequence in Configuration Manager**
- Step 6: [Create collection in Configuration Manager](#)
 - Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
 - Step 8: [Speed up the deployment process \(optional\)](#)
 - Step 9: [Run Autopilot task sequence on device](#)
 - Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Create Autopilot task sequence for existing devices in Configuration Manager

Once the packages containing the Autopilot profile JSON files are created and distributed in Configuration Manager, the next step is to create a task sequence that performs the following functions:

- Wipes the device.
- Installs a fresh copy of Windows on the device.
- Copies the Autopilot profile JSON file to the device.

Copying of the Autopilot profile JSON file is done in WinPE when the newly installed Windows OS is offline. When the task sequence completes, the device boots into the newly installed Windows OS for the first time and runs the out-of-box experience (OOBE). The OOBE process then processes the Autopilot profile JSON file, which initiates the Autopilot deployment.

Note

If using multiple Autopilot profiles and multiple Autopilot profile JSON files were created, a separate task sequence is needed for each of the Autopilot profiles.

To create the Autopilot for existing devices task sequence in Configuration Manager, follow these steps:

1. On a device where the Configuration Manager console is installed, such as a Configuration Manager site server, open the Configuration Manager console.
2. In the left hand pane of the Configuration Manager console, navigate to **Software Library > Overview > Operating Systems**.
3. Select **Task Sequences** and then on the ribbon, select **Create Task Sequence**. Alternatively, right-click **Task Sequences** and select **Create Task Sequence**.
4. The **Create Task Sequence Wizard** window appears:
 - a. In the **Create new task sequence** page, select the option to **Deploy Windows Autopilot for existing devices**, and then select the **Next >** button.
 - b. In the **Specify task sequence information** page:
 - i. Next to **Name**, enter an identifiable name for the Autopilot scenario for the task sequence. For example, **Autopilot user-driven Microsoft Entra join**.
 - ii. Next to **Description**, enter a description for the Autopilot scenario for the task sequence.
 - iii. Next to **Boot image**: select the **Browse** button.
 - In the **Select a Boot Image** windows that appears, under **Boot images**: select a boot image, and then select the **OK** button.
 - iv. Select the **Next >** button.
 - c. In the **Install the Windows operating system** page:
 - i. Next to **Image package**: select the **Browse** button. In the **Select an Operating System Image** window that appears, under **Operating system images**: locate and select the desired Windows operating system image, and then select the **OK** button.

- ii. Next to **Image index**, select the desired Windows version. For example, **Enterprise**.
- iii. Make sure the option **Partition and format the target computer before installing the operating system** is selected and enabled.
- iv. Make sure the option **Configure task sequence for use with BitLocker** isn't selected. If BitLocker encryption is desired, Microsoft recommends enabling via Intune policies that are applied during the Windows Autopilot deployment.

 **Note**

Although BitLocker encryption could technically be enabled via the task sequence, it might result in undesired outcomes. For example, instead of saving BitLocker recovery keys to Intune or Microsoft Entra ID, they might be saved to:

- Configuration Manager BitLocker Management.
- On-premises Active Directory.

Additionally, if BitLocker settings specified in the task sequence don't match the BitLocker policy settings in Intune, then this mis-match could cause the device to show as non-compliant. Resolving issues like this could mean having to decrypt and then re-encrypt the drive to resolve. Therefore Microsoft recommends not enabling BitLocker as part of the task sequence and instead enabling BitLocker as part of Intune policies deployed during Windows Autopilot.

- v. Leave **Product key** blank. The Autopilot for existing devices task sequence runs the [Windows System Preparation Tool \(Sysprep\)](#) at the end of the task sequence. Sysprep clears any product key that is specified.
- vi. Leave the option of **Randomly generate the local administrator password and disable the account on all support platforms (recommended)** selected. Alternatively, the option of **Enable the account and specify the local administrator password** can be selected and a password specified. However, the password specified will only be useful after the **Setup Windows and ConfigMgr** task and if the task sequence fails and doesn't complete successfully. If the task sequence completes successfully, the password is cleared at the end of the task sequence by Sysprep.

vii. Once all options are configured in the **Install the Windows operating system** page, select the **Next >** button.

 **Note**

If using the alternate [Speed up the deployment process \(optional\)](#) step later in this tutorial, Sysprep never runs as part of the task sequence. However, the product key and local administrator password never get processed since the `unattend.xml` file that contains the product key and local administrator password is deleted as part of this optional step. For this reason, when using the alternate [Speed up the deployment process \(optional\)](#) step, the settings specified for these two options are irrelevant since they're never processed.

- d. In the **Install the Configuration Manager client** page, add any necessary Configuration Manager client installation properties for the environment. For example, since the device is a Workgroup device and not domain joined during the Windows Autopilot for existing devices task sequence, the **SMSMP** or **SMSMPLIST** parameters might be needed to run certain tasks such as the **Install Application** or **Install Software Updates** tasks. Once finished adding any Configuration Manager client installation properties, select the **Next >** button.
- e. In the **Install software updates** page, select the desired option to install software updates during the task sequence. For the Autopilot for existing devices task sequence, Microsoft recommends leaving the option to the default of **Do not install any software updates** and not install any software updates during the task sequence. Once the desired option is selected, select the **Next >** button.

 **Tip**

Microsoft recommends not installing software updates during the Autopilot for existing devices task sequence because doing so significantly increases the time for the task sequence to complete. Instead, consider installing updates using one of the following two options:

- The Configuration Manager offline image servicing feature of [Scheduled Updates](#)
- Every month, download the latest monthly ISO for the version of Windows that's being installing and then update the **Operating**

System Images package in Configuration Manager with the new updated `install.wim` image from the ISO. The ISOs are updated monthly and have the latest updates in them.

- f. In the **Install applications** page, select the desired applications to install during the task sequence. Once the desired applications are added, select the **Next >** button. If no applications need to be installed, then select the **Next >** button without selecting any applications.

 **Tip**

Instead of installing applications during the task sequence, Microsoft recommends installing all applications and configurations from Microsoft Intune or Configuration Manager co-management. This process provides a consistent experience between users receiving new devices and those using Windows Autopilot for existing devices.

- g. On the **Prepare System for Windows Autopilot** page, select the package that includes the Autopilot JSON file created in the step [Create and distribute package for JSON file in Configuration Manager](#). Once the package with the Autopilot JSON file is selected, select the **Next >** button.

 **Note**

Leave the option **Shutdown computer after this task sequence completes** unchecked. This option is configured later in the section [Modify the task sequence to account for Sysprep command line configuration](#).

- h. On the **Confirm the settings** page, verify that all settings are correct, and then select the **Next >** button.
 - i. When the **Create Task Sequence Wizard** completes with **The task "Create Task Sequence Wizard" completed successfully** message, select the **Close** button.
5. If using multiple Autopilot profiles and multiple Autopilot profile JSON files were created, repeat the above steps to create additional task sequences. Each Autopilot profile JSON file needs its own separate task sequence.

 **Note**

For Windows Autopilot for existing devices task sequence, the **Create Task Sequence Wizard** purposely skips configuring and adding the **Apply Network Settings** task. If the **Apply Network Settings** task isn't specified in a task sequence, it uses Windows default behavior, which is to join a workgroup.

The Windows Autopilot for existing devices task sequence runs the **Prepare Windows for capture** step, which uses the Windows System Preparation Tool (Sysprep). If the device is joined to a domain, Sysprep fails, so therefore the Windows Autopilot for existing devices task sequence joins a workgroup. For this reason, it isn't necessary to add the **Apply Network Settings** task to a Windows Autopilot for existing devices task sequence.

Modify the task sequence to account for Sysprep command line configuration

The Autopilot for existing devices task sequence adds the **Prepare Windows for Capture** task to the task sequence. The **Prepare Windows for Capture** task is the task that runs Sysprep. Sysprep needs to run so that on the next boot, OOBE runs and processes the Autopilot profile JSON file. However, the **Prepare Windows for Capture** task adds the `/Generalize` parameter to the Sysprep command line. The `/Generalize` parameter causes Sysprep to delete the Autopilot profile JSON file. The `/Generalize` parameter for Sysprep is normal for traditional build and capture task sequences not associated with Autopilot, but it breaks Autopilot deployments since the Autopilot profile JSON file is deleted. Deletion of the Autopilot profile JSON file causes Autopilot to never run during Windows Setup and OOBE.

To resolve the issue, the **Prepare Windows for Capture** task needs to be removed from the task sequence and replaced with a **Run Command Line** task that runs Sysprep without the `/Generalize` parameter. This resolution can be accomplished by following these steps:

Note

If the optional step of [Speed up the deployment process \(optional\)](#) is going to be followed, then skip this section and proceed to the next step of [Step 6: Create collection in Configuration Manager](#).

1. On a device where the Configuration Manager console is installed, such as a Configuration Manager site server, open the Configuration Manager console.

2. In the left hand pane of the Configuration Manager console, navigate to **Software Library > Overview > Operating Systems**.

3. Expand **Task Sequences** and then locate the Autopilot for existing devices task sequence created in the [Create Autopilot task sequence for existing devices in Configuration Manager](#) section.

4. Once the Autopilot for existing devices task sequence is located, select it and then on the ribbon, select **Edit**. Alternatively, right-click on the Autopilot for existing devices task sequence and select **Edit**.

5. In the **Task Sequence Editor** window that opens:

a. Select the **Prepare Windows for Capture** task.

b. Select the **Add** drop down menu in the top left of the task sequence editor and then select **General > Run Command Line**. A **Run Command Line** task is added immediately after the **Prepare Windows for Capture** task.

c. Select the **Run Command Line** task and then configure with the following settings:

- **Name:** Sysprep
- **Command Line:** Based on the desired behavior, select one of the following two Sysprep command lines by selecting **Copy** at the top right corner of the desired **Windows Command Prompt** code block and then pasting the copied Sysprep command line into the **Command Line** text box:
 - Restart device after running Sysprep. OOB and that Autopilot deployment will start immediately after the task sequence completes and the device restarts:

```
Windows Command Prompt  
C:\Windows\System32\Sysprep\Sysprep.exe /oobe /reboot
```

- Shut down device after running Sysprep. After the device shuts down, OOB and the Autopilot deployment won't start until the device is turned on for the first time by the end-user:

```
Windows Command Prompt  
C:\Windows\System32\Sysprep\Sysprep.exe /oobe /shutdown
```

Note

Sysprep can either shut down or restart the device when it finishes running:

- **Restarting** the device causes the device to restart as soon as the task sequence completes and then immediately boots into Windows for the first time and runs Windows Setup and OOBE. When Windows Setup and OOBE run, the Autopilot JSON file is processed and the Autopilot deployment starts.
- **Shutting down** the device shuts down and powers off the device as soon as the task sequence completes. Shutting down and powering off the device give the option to further prepare the device and then deliver it to an end-user. Windows Setup, OOBE, and the Autopilot deployment then start when the end-user turns on the device for the first time.

- d. Select the **Prepare Windows for Capture** task again and then select the **Remove** option in the top left of the task sequence editor. A confirmation dialog box appears confirming to delete the step. Select the **Yes** button to remove the **Prepare Windows for Capture** task.
- e. Select the **OK** button in the **Task Sequence Editor** to save the changes to the task sequence.

Next step: Create collection in Configuration Manager

Step 6: Create collection in Configuration Manager

Related content

For more information on creating an Autopilot task sequence in Configuration Manager, see the following articles:

- [Create a task sequence](#).
- [Windows System Preparation Tool \(Sysprep\)](#).
- [Windows Autopilot for existing devices doesn't work](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Windows Autopilot deployment for existing devices: Create collection in Configuration Manager

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
- Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
- Step 3: [Create JSON file for Autopilot profiles](#)
- Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
- Step 5: [Create Autopilot task sequence in Configuration Manager](#)

Step 6: Create collection in Configuration Manager

- Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
- Step 8: [Speed up the deployment process \(optional\)](#)
- Step 9: [Run Autopilot task sequence on device](#)
- Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Create collection in Configuration Manager

Once the Autopilot for existing devices task sequence is created, the next step is to create a collection in Configuration Manager to deploy the task sequence to the target devices.

Note

If a collection with the desired devices to target already exists, then this step can be skipped. Proceed to the step [Deploy Autopilot task sequence to collection in Configuration Manager](#).

To create the Autopilot for existing devices task sequence in Configuration Manager, follow these steps:

1. On a device where the Configuration Manager console is installed, such as a Configuration Manager site server, open the Configuration Manager console.
2. In the left hand pane of the Configuration Manager console, navigate to **Assets and Compliance > Overview**.
3. Select **Device Collections**.
4. In the ribbon, select **Create**, and then select **Create Device Collection**. As an alternative, right-click on **Device Collections**, and then select **Create Device Collection**.
5. In the **Create Device Collection Wizard** window that appears:
 - a. In the **Specify details for this collection** page, configure the following settings:
 - i. Next to **Name**: enter a desired name for the collection. For example, **Autopilot for existing devices**.
 - ii. Next to **Comment**: if desired, add an optional comment to further describe the collection
 - iii. Next to **Limiting collection**: select the **Browse** button. In the **Select Collection** window that appears, select a desired collection to limit this collection to. To not limit this collection, select the **All Systems** collection. Once the desired collection is selected, select the **OK** button.
 - iv. Select the **Next >** button.
 - b. In the **Define membership rules for this collection** page, via the **Add Rule** drop-down menu, create a rule that includes the desired devices to run the Autopilot for existing devices task sequence. For more information on creating rules for a collection to include the desired devices, see [How to create collections in Configuration Manager](#). Once the appropriate rules are created that include the desired devices, select the **Next >** button.
 - c. In the **Confirm the settings** page, verify that everything is configured as desired, and then select the **Next >** button.
 - d. When the **Create Device Collection Wizard** completes with **The task "Create Device Collection Wizard" completed successfully** message, select the **Close** button.
6. With **Device Collections** still selected, select **F5** on the keyboard to refresh the list of collections in the right pane. Verify that the newly created collection appears. If

it doesn't appear, wait a few minutes, and then try to refresh again. Depending on the environment, it might take some time for the newly created collection to appear.

7. Once the newly created collection appears, open it by double-clicking on it. Alternatively, to open the collection, right-click on the collection and then select **Show Members**. The members of the collection appear in the right pane.
8. Verify that the listed devices are the expected devices for the collection that should receive the Autopilot for existing devices task sequence.

Next step: Deploy Autopilot task sequence to collection in Configuration Manager

Step 7: Deploy Autopilot task sequence to collection in Configuration Manager

Related content

For more information on creating a collection in Configuration Manager, see the following articles:

- [Deploy the Autopilot task sequence](#).
- [How to create collections in Configuration Manager](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot deployment for existing devices: Deploy Autopilot task sequence to collection in Configuration Manager

Article • 06/19/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
 - Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
 - Step 3: [Create JSON file for Autopilot profiles](#)
 - Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
 - Step 5: [Create Autopilot task sequence in Configuration Manager](#)
 - Step 6: [Create collection in Configuration Manager](#)
- Step 7: Deploy Autopilot task sequence to collection in Configuration Manager**
- Step 8: [Speed up the deployment process \(optional\)](#)
 - Step 9: [Run Autopilot task sequence on device](#)
 - Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Deploy Autopilot task sequence to collection in Configuration Manager

Once the Autopilot for existing devices task sequence and the collection with devices to deploy the task sequence to are created, the next step is to deploy the task sequence to the collection. To deploy the task sequence to the collection, follow these steps:

1. On a device where the Configuration Manager console is installed, such as a Configuration Manager site server, open the Configuration Manager console.
2. In the left hand pane of the Configuration Manager console, navigate to **Software Library > Overview > Operating Systems**.

3. Expand **Task Sequences** and then locate the Autopilot for existing devices task sequence created in the [Create Autopilot task sequence for existing devices in Configuration Manager](#) step.
 4. Once the Autopilot for existing devices task sequence is located, select it and then on the ribbon, select **Deploy**. Alternatively, right-click on the Autopilot for existing devices task sequence and select **Deploy**.
5. In the **Deploy Software Wizard** window that appears:
- a. In the **General/Specify general information for this deployment** page, configure the following settings:
 - i. Next to **Task Sequence**, the Autopilot for existing devices task sequence should already be selected.
 - ii. Next to **Collection**, select the **Browse** button. In the **Select Collection** window that appears, under **Select a collection**, select the collection created in the step [Create collection in Configuration Manager](#), and then select the **OK** button.
 - iii. Select the **Next >** button.

- b. In the **Deployment Settings/Specify settings to control this deployment** page, configure the settings as desired:

- i. For **Purpose**, normally **Available** is selected. Making the deployment available usually means that someone such as an admin or end-user has to manually trigger and start the deployment by selecting the task sequence through methods such:
 - The Configuration Manager Software Center.
 - Booting from a PXE enabled distribution point
 - Booting from task sequence bootable media.

Warning

The deployment can instead be set to **Required**. Setting the deployment to **Required** causes the deployment to start automatically without any end-user intervention when the deployment assignment time is reached. However, Microsoft recommends not making a deployment required due to the potential destructive behavior that a required task sequence can have. For example, a required task sequence can unexpectedly wipe devices without any user interaction if:

- The task sequence is accidentally deployed to the wrong collection.
- The wrong devices are added to the collection that the task sequence is deployed to.

If using the option of **Required**, do so with extreme caution making sure the task sequence is deployed to the correct collection that contains expected devices.

ii. Under **Make available to the following:**, select where the task sequence appears and when the task sequence can run:

- **Only Configuration Manager clients:** The task sequence appears in the Configuration Manager Software Center on existing devices that has Windows already installed and has the Configuration Manager client installed. The task sequence doesn't appear when booting from a PXE enabled distribution point or when booting from task sequence bootable media.
- **Only media and PXE:** The task sequence appears when booting from a PXE enabled distribution point or when booting from task sequence bootable media. The task sequence doesn't appear in the Configuration Manager Software Center on existing devices that has Windows already installed and has the Configuration Manager client installed.
- **Configuration Manager clients, media and PXE:** The task sequence appears when booting from a PXE enabled distribution point or when booting from task sequence bootable media. It also appears in the Configuration Manager Software Center on existing client devices that has the Configuration Manager client installed.

Warning

When the deployment is set to **Required**, the above options are the scenarios when the deployment can automatically run when the deployment assignment time is reached. For example, if the deployment is set to **Required** and **Only media and PXE**, the task sequence doesn't ever run automatically while in Windows. However, it runs automatically when the device is booted from a PXE enabled distribution point or when booted from task sequence bootable media.

iii. Select the **Next >** button.

- c. In the **Scheduling/Specify the schedule for this deployment** page, schedule when the deployment should occur:
- Select the checkbox next to **Schedule when this deployment will become available**: and then select a date and time. This date and time is the date and time that the task sequence starts to appear:
 - In the Configuration Manager Software Center.
 - When booting from a PXE enabled distribution point.
 - When booting from task sequence bootable media.
 - If the deployment is required, next to **Assignment schedule**: select the New button. In the **Assignment Schedule** window that appears, configure the settings as needed. The settings selected here determine when the task sequence runs automatically without end-user intervention. Once complete. Once complete, select the **OK** button.
 - Select the **Next >** button.
- d. In the **User Experience/Specify the user experience for the installation of this software** page, select the options as desired, and then select the **Next >** button.
- e. In the **Alerts/Specify Configuration Manager and Operations Manager** page, select the options as desired, and then select the **Next >** button.
- f. In the **Distribution Points/Specify how to run the content for this program** page, select the options as desired, and then select the **Next >** button.
- g. In the **Summary/Confirm the settings for this new deployment** page, verify that everything is configured as desired, and then select the **Next >** button.
- h. When the **Deploy Software Wizard** completes with **The task "Deploy Software Wizard" completed successfully** message, select the **Close** button.
6. If there are multiple task sequences with different Autopilot profiles, repeat the above steps for each task sequence.

 **Note**

The instructions in this step don't fully go into detail all of the options available when running the **Deploy Software Wizard**. For full details on the options available, see [Deploy a task sequence](#).

Next step: Speed up the deployment process (optional)

Step 8: Speed up the deployment process (optional)

If the preference is to use an unmodified out-of-box Autopilot task sequence created by the [Create Task Sequence Wizard](#) in Configuration Manager, then skip to [Step 9: Run Autopilot task sequence on device](#).

Step 9: Run Autopilot task sequence on device

Related content

For more information on deploying the Autopilot task sequence, see the following articles:

- [Deploy the Autopilot task sequence.](#)
- [Deploy a task sequence.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot deployment for existing devices: Speed up the deployment process (optional)

Article • 06/19/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
- Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
- Step 3: [Create JSON file for Autopilot profiles](#)
- Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
- Step 5: [Create Autopilot task sequence in Configuration Manager](#)
- Step 6: [Create collection in Configuration Manager](#)
- Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
- ✓ Step 8: **Speed up the deployment process (optional)**
 - Step 9: [Run Autopilot task sequence on device](#)
 - Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Windows Autopilot for existing devices task sequence process

When the Windows Autopilot for existing devices task sequence runs on a device, the Autopilot deployment doesn't run when the device boots into Windows for the first time during the **Setup Windows and ConfigMgr** task of the task sequence. Instead, the Autopilot deployment doesn't run until after the task sequence completes.

The Autopilot deployment normally runs when Windows boots for the first time and Windows Setup and the out-of-box experience (OOBE) run. However, during a Windows Autopilot for existing devices task sequence, even though the task sequence injected an Autopilot profile JSON file into the offline Windows installation, the file isn't processed when Windows first boots because the task sequence also creates and injects an `unattend.xml` file. When there's both an `unattend.xml` file and an Autopilot profile JSON

file during Windows Setup, Windows Setup ignores the Autopilot profile JSON file, and it only processes the `unattend.xml` file.

After Windows Setup is done, the task sequence resumes and deletes the existing `unattend.xml`. Later in the task sequence when the task sequence runs Sysprep on the device, it doesn't specify or add a new `unattend.xml` file. Once the task sequence finishes running Sysprep, the task sequence completes and the device is rebooted. When the device reboots, Windows starts and Windows Setup runs for a second time. Since there's no `unattend.xml` file and only the Autopilot profile JSON file exists, Windows Setup processes the Windows Autopilot profile JSON file and the Autopilot deployment starts.

An overview of the Windows Autopilot for existing devices task sequence process is as follows:

1. Task sequence starts in Windows PE.
2. Task sequence formats and partitions the disk.
3. Task sequence applies the Windows OS and creates the `unattend.xml` file.
4. Task sequence injects the Autopilot profile JSON file.
5. Task sequence boots into Windows for the first time.
6. Windows setup runs for the first time and processes the `unattend.xml` file.
Windows Autopilot profile JSON file is ignored.
7. Task sequence resumes in the newly installed Windows OS.
8. Task sequence deletes the `unattend.xml` file.
9. Task sequence installs the Configuration Manager client.
10. Task sequence runs additional tasks (**Install Application**, **Install Software Updates**, **Install Package**, **Enable BitLocker**, etc.)
11. Task sequence uninstalls the Configuration Manager client.
12. Task sequence Syspreps the device.
13. Task sequence completes and device reboots.
14. Windows setup runs for the second time and processes the Autopilot profile JSON file since there's no `unattend.xml` file.
15. Autopilot deployment starts.

Additional tasks running during a Windows Autopilot for existing devices task sequence

When using the **Create Task Sequence Wizard** in Configuration Manager to create the Windows Autopilot for existing devices task sequence, it assumes that additional tasks need to be run via the task sequence before the Autopilot deployment runs. Examples

of additional tasks running via the task sequence before the Autopilot deployment runs include:

- Installing applications via the **Install Application** task.
- Installing software updates via the **Install Software Updates** task.
- Installing packages via the **Install Package** task.
- Enabling BitLocker via the **Enable BitLocker** task.
- Other customizations.

In order for these additional tasks to run, the task sequence deployment process performs the following processes after it boots out of Windows PE:

- Boots into the Windows OS for the first time and runs Windows Setup and OOB.
- Continues the task sequence in the full Windows OS.
- Installs the Configuration Manager client to support running tasks such as the **Install Application** or **Install Software Updates** tasks.
- Runs the additional tasks.
- Removes the Configuration Manager client.
- Syspreps the device so that after the task sequence completes and the device reboots, it can rerun Windows Setup and OOB, which then launches the Autopilot deployment.

The above steps are necessary if additional tasks need to run during the task sequence. However, if additional tasks don't need to run during the task sequence, then several of the above steps aren't needed. Running the above steps when they aren't needed can potentially cause several issues including:

- Needlessly adding time to the deployment process.
- Needlessly installing the Configuration Manager client on the device. It's best practice to avoid installing the Configuration Manager client if not needed during the task sequence and if it's eventually going to be uninstalled.
- Needlessly running Windows Setup and OOB multiple times.
- Needlessly running Sysprep.

Speed up the deployment process

Tip

If a task sequence is needed to run additional tasks before running the Autopilot deployment, then skip to the next step of [Run Autopilot task sequence on device](#).

However, even if additional tasks are needed, instead of using the task sequence to run these tasks, consider running the additional tasks using alternate methods. For example:

- Install applications via Intune.
- Enable BitLocker via Intune.
- Install software updates via offline servicing and [Configuration Manager Scheduled Updates](#).

When possible, Microsoft recommends using the above methods to run the additional tasks instead of running them via the task sequence. Using the above methods allows using this solution to speed up the deployment.

If no additional tasks are needed via a task sequence before running the Autopilot deployment, then the Windows Autopilot for existing devices task sequence can be modified to eliminate unneeded tasks and processes. Eliminating unneeded tasks and processes speeds up the deployment process and the time it takes for the deployment to finish. Examples of processes that can be eliminated to speed up the deployment include:

- Running Windows Setup additional times via the **Setup Windows and ConfigMgr** task.
- Installing the Configuration Manager client via the **Setup Windows and ConfigMgr**.
- Uninstalling the Configuration Manager client via the **Prepare ConfigMgr Client for Capture** task.
- Running Sysprep via the **Prepare Windows for Capture/Sysprep** tasks.

The solution to speed up the deployment deletes the `unattend.xml` file and eliminates the unnecessary tasks so that the Autopilot profile JSON file is processed during the first boot into Windows. After the solution is applied, the updated overview of the Windows Autopilot for existing devices task sequence process is as follows:

1. Task sequence starts in Windows PE.
2. Task sequence formats and partitions the disk.
3. Task sequence applies the Windows OS and creates the `unattend.xml` file.
4. Task sequence injects the Autopilot profile JSON file.
5. Task sequence deletes the `unattend.xml` file.
6. Task sequence boots into Windows for the first time.
7. Windows setup runs for the first time and processes the Autopilot profile JSON file since there's no `unattend.xml` file.

8. Autopilot deployment starts.

The solution to speed up the deployment reduces the number of steps in the deployment process from 15 to 8.

Note

The steps for the solution to speed up the deployment are optional. The out-of-box Windows Autopilot for existing devices task sequence still works without any modification. The below steps are only designed to reduce the time it takes to run the deployment and potentially avoid some issues. If the preference is to not modify the existing Windows Autopilot for existing devices task sequence, then skip to the next step of [Run Autopilot task sequence on device](#).

To modify the Windows Autopilot for existing devices task sequence to speed up the deployment process, follow these steps:

1. On a device where the Configuration Manager console is installed, such as a Configuration Manager site server, open the Configuration Manager console.
2. In the left hand pane of the Configuration Manager console, navigate to **Software Library > Overview > Operating Systems**.
3. Expand **Task Sequences** and then locate the Autopilot for existing devices task sequence created in the [Create Autopilot task sequence in Configuration Manager](#) step.
4. Once the Autopilot for existing devices task sequence is located, select it and then on the ribbon, select **Edit**. Alternatively, right-click on the Autopilot for existing devices task sequence and select **Edit**.
5. In the **Task Sequence Editor** window that opens:
 - a. Select the **Prepare device for Windows Autopilot** group and then select the **Remove** option in the top left of the task sequence editor. A confirmation dialog box appears confirming to delete the step. Select the **Yes** button to remove the **Prepare device for Windows Autopilot** group.
 - b. Select the **Setup Operating System** group and then select the **Remove** option in the top left of the task sequence editor. A confirmation dialog box appears confirming to delete the step. Select the **Yes** button to remove the **Setup Operating System** group.

Note

If there were any additional tasks or groups after the **Setup Windows and Configuration Manager** task, then also remove those tasks and groups by selecting the **Remove** option in the top left of the task sequence editor for each one of those tasks or groups. For each removal, a confirmation dialog box appears confirming to delete the step or group. Select the **Yes** button to remove each additional task or group.

- c. Select the last task in the task sequence.
 - d. Select the **Add** drop down menu in the top left of the task sequence editor and then select **General > Run Command Line**. A **Run Command Line** task is added as the last task in the task sequence.
 - e. Select the **Run Command Line** task and then configure with the following settings:
 - **Name:** Remove unattend.xml from Panther
 - **Command Line:** Select **Copy** at the top right corner of the below **Windows Command Prompt** code block and then paste into the **Command Line** text box:

Windows Command Prompt

```
cmd.exe /c del
%OSDTargtSystemDrive%\Windows\Panther\unattend.xml /s
```
 - f. Select the **OK** button in the **Task Sequence Editor** to save the changes to the task sequence.
6. If there are multiple Windows Autopilot for existing devices task sequences, then repeat the above steps for each task sequence.

Shut down device after the task sequence completes (optional)

When the task sequence modified to speed up the deployment process finishes running and is complete, the device restarts and then immediately boot into Windows for the first time. After booting into Windows for the first time, it will run Windows Setup and

OOBE. When Windows Setup and OOB run, the Autopilot JSON file is processed and the Autopilot deployment begins.

However, the device can be shut down instead of restarting when the task sequence completes. Shutting down the device instead of restarting it when the task sequence completes can be useful, for example, to give the option to further prepare the device and then deliver it to an end-user. Windows Setup, OOB, and the Autopilot deployment then instead starts when the end-user turns on the device for the first time.

If the default behavior of restarting the device when the task sequence completes is desired, then skip this section and proceed to the next step of [Run Autopilot task sequence on device](#). Otherwise, to shut down the device instead of restarting it when the task sequence completes, follow these steps:

1. On a device where the Configuration Manager console is installed, such as a Configuration Manager site server, open the Configuration Manager console.
2. In the left hand pane of the Configuration Manager console, navigate to **Software Library > Overview > Operating Systems**.
3. Expand **Task Sequences** and then locate the Autopilot for existing devices task sequence modified in the [Speed up the deployment process](#) section.
4. Once the Autopilot for existing devices task sequence is located, select it and then on the ribbon, select **Edit**. Alternatively, right-click on the Autopilot for existing devices task sequence and select **Edit**.
5. In the **Task Sequence Editor** window that opens:
 - a. Select the last task in the task sequence.
 - b. Select the **Add** drop down menu in the top left of the task sequence editor and then select **General > Run Command Line**. A **Run Command Line** task is added as the last task in the task sequence.
 - c. Select the **Run Command Line** task and then configure with the following settings:
 - **Name:** Shutdown
 - **Command Line:** Select **Copy** at the top right corner of the below **Windows Command Prompt** code block and then paste into the **Command Line** text box:

Windows Command Prompt

```
wpeutil.exe shutdown
```

- d. Select the **OK** button in the **Task Sequence Editor** to save the changes to the task sequence.
6. If there are multiple Windows Autopilot for existing devices task sequences, then repeat the above steps for each task sequence.

Next step: Run Autopilot task sequence on device

Step 9: Run Autopilot task sequence on device

Related content

For more information on speeding up the deployment process, see the following articles:

- [Speeding up Windows Autopilot for existing devices](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot deployment for existing devices: Run Autopilot task sequence on device

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
 - Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
 - Step 3: [Create JSON file for Autopilot profiles](#)
 - Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
 - Step 5: [Create Autopilot task sequence in Configuration Manager](#)
 - Step 6: [Create collection in Configuration Manager](#)
 - Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
 - Step 8: [Speed up the deployment process \(optional\)](#)
- Step 9: Run Autopilot task sequence on device**
- Step 10: [Register device for Windows Autopilot](#)

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Run Autopilot task sequence on device

Once the Autopilot for existing devices is created, modified as needed, and deployed, the task sequence can be run on a device by following these steps:

1. Start the task sequence using the desired method based on how the task sequence deployment was configured:
 - Configuration Manager Software Center
 - PXE enabled distribution point
 - Task sequence bootable media
2. Allow the task sequence to complete.
3. Once the task sequence completes, the device either restarts or shuts down depending on the shutdown or restart behavior selected in one of the following two steps:

- [Create Autopilot task sequence in Configuration Manager.](#)
- [Speed up the deployment process.](#)

The behavior of the device after the task sequence completes depends on whether the device restarted or shut down:

- **Restart:** the device restarts as soon as the task sequence completes and then immediately boot into Windows for the first time and run OOBE. When OOBE runs, the Autopilot JSON file is processed and the Autopilot deployment starts.
- **Shutdown:** the device shuts down and power off as soon as the task sequence completes. Shutting down the device gives the option to further prepare the device and then deliver it to an end-user. OOBE and the Autopilot deployment start when the end-user turns on the device for the first time.

 **Important**

A Windows Autopilot profile downloaded from Intune is used instead of the Windows Autopilot profile from the JSON file if the following conditions are met after the task sequence completes:

- Device is registered as an Autopilot device in Intune.
- Device has an Autopilot profile assigned to it in Intune.

The Windows Autopilot profile downloaded from Intune has priority over the local Windows Autopilot profile from the JSON file.

Next step: Register device for Windows Autopilot

[Step 10: Register device for Windows Autopilot](#)

Related content

For more information on running the Autopilot task sequence on the device, see the following article:

- [Complete the deployment process.](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Windows Autopilot deployment for existing devices: Register device for Windows Autopilot

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

Autopilot user-driven Microsoft Entra join steps:

- Step 1: [Set up a Windows Autopilot profile](#)
 - Step 2: [Install required modules to obtain Autopilot profiles from Intune](#)
 - Step 3: [Create JSON file for Autopilot profiles](#)
 - Step 4: [Create and distribute package for JSON file in Configuration Manager](#)
 - Step 5: [Create Autopilot task sequence in Configuration Manager](#)
 - Step 6: [Create collection in Configuration Manager](#)
 - Step 7: [Deploy Autopilot task sequence to collection in Configuration Manager](#)
 - Step 8: [Speed up the deployment process \(optional\)](#)
 - Step 9: [Run Autopilot task sequence on device](#)
-  **Step 10: Register device for Windows Autopilot**

For an overview of the Windows Autopilot deployment for existing devices workflow, see [Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#).

Register device for Windows Autopilot

Running the Autopilot for existing devices task sequence and the Autopilot deployment on a device doesn't automatically register the device for Windows Autopilot. The Autopilot profile JSON makes the Autopilot deployment available to the device and allows the device to run that particular Autopilot deployment, but it doesn't register the device for Windows Autopilot. If the device ever undergoes a reset, when it runs Windows Setup and the out-of-box experience (OOBE) for the first time after the reset, it won't run the Autopilot deployment again even though it has previously run an Autopilot deployment.

To ensure that the device can run a Windows Autopilot deployment after a reset, the device must be registered for Windows Autopilot. The device can be registered as a Windows Autopilot device by using one of the following methods:

1. [Manually register devices with Windows Autopilot](#): Manually registering a device includes manually registering devices into Intune as an Autopilot device via the

hardware hash. The hardware hash of a device can be collected via one of the following methods:

- Configuration Manager
- PowerShell script
- Diagnostics page hash export
- Desktop hash export

2. In an Autopilot profile that is deployed to a device group that the device is a member of, make sure the option **Convert all targeted devices to Autopilot** is set to **Yes**. For more information on creating and assigning Autopilot profiles, see one of the following articles on creating and assigning an Autopilot profile for each of the different Autopilot scenarios:

- [User-driven Microsoft Entra join: Create and assign user-driven Microsoft Entra join Autopilot profile](#)
- [User-driven Microsoft Entra hybrid join: Create and assign user-driven Microsoft Entra hybrid join Autopilot profile](#)
- [Pre-provisioning Microsoft Entra join: Create and assign a pre-provisioned Microsoft Entra join Autopilot profile](#)
- [Pre-provisioning Microsoft Entra hybrid join: Create and assign a pre-provisioned Microsoft Entra hybrid join Autopilot profile](#)
- [Self-deploying mode: Create and assign self-deploying Autopilot profile](#)

Importing the hardware hash CSV file for devices into Intune

Several of the methods in the previous section on obtaining the hardware hash when manually registering devices as Autopilot devices produces a CSV file that contains the hardware hash of the device. This CSV file with the hardware hash needs to be imported into Intune to register the device as an Autopilot device.

After the CSV file is created, it can be imported into Intune via the following steps:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.

5. In the Windows | Windows enrollment screen, under Windows Autopilot, select Devices.

6. In the Windows Autopilot devices screen that opens, select Import.

a. In the Add Autopilot devices window that opens:

i. Under Specify the path to the list you want to import., select the blue file folder.

ii. Browse to the CSV file obtained using one of the above methods to obtain the hardware hash of a device.

iii. After selecting the CSV file, verify that the correct CSV file is selected under Specify the path to the list you want to import., and then select Import.

Selecting Import closes the Add Autopilot devices window. Importing can take several minutes.

b. After the import is complete, select Sync.

A message displays saying that the sync is in progress. The sync process might take a few minutes to complete, depending on how many devices are being synchronized.

 Note

If another sync is attempted within 10 minutes after initiating a sync, an error will be displayed. Syncs can only occur once every 10 minutes. To attempt a sync again, wait at least 10 minutes before trying again.

c. Select Refresh to refresh the view. The newly imported devices should display within a few minutes. If the devices aren't yet displayed, wait a few minutes, and then select Refresh again.

Ensure domain join profile is assigned to all devices

For Autopilot scenarios that utilize Microsoft Entra hybrid join and run after the Windows Autopilot deployment for existing devices task sequence completes, make sure that the domain join profile is assigned to All devices. This modification can be done at the followings steps:

- For the [Windows Autopilot user-driven Microsoft Entra hybrid join scenario at Step 8: Configure and assign domain join profile](#).
- For the [Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join scenario at Step 8: Configure and assign domain join profile](#).

The domain join profile needs to be assigned to **All devices** because:

- If the existing device has never joined Microsoft Entra ID before the Windows Autopilot deployment runs, then there isn't a Microsoft Entra ID device object for the device in Intune. The Microsoft Entra ID device object is created in Intune when the device joins Microsoft Entra ID as part of the Windows Autopilot deployment.
- If the existing device has never registered as a Windows Autopilot device before the Windows Autopilot deployment runs, then there isn't a Windows Autopilot device object for the device in Intune. Normally a device has to be a Windows Autopilot device before the Windows Autopilot deployment can run on it. However, for the Windows Autopilot deployment for existing devices scenario, registering the device as an Autopilot device isn't required since it instead uses the Autopilot profile JSON file. The device is instead registered as an Autopilot device after the Autopilot deployment completes via the methods in the [Register device for Windows Autopilot](#) section.

In both of the above scenarios, there's no device that can be added to a device group before the Autopilot deployment begins. Since there's no device group that contains the device, there's no device group that the domain join profile can be assigned to before the Autopilot deployment begins. Assigning the domain join profile to **All devices** resolves this problem and ensures that the device can pick up the domain join profile before it's either a Microsoft Entra device or Autopilot device.

Related content

For more information on registering the device for Windows Autopilot, see the following articles:

- [Register the device for Windows Autopilot](#).
- [Manually register devices with Windows Autopilot](#).
- [Create an Autopilot deployment profile](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Step by step tutorial for Windows Autopilot Reset in Intune

Article • 10/09/2024 • Applies to: Windows 11, Windows 10

Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. In addition, once the Windows Autopilot Reset begins, it blocks the user from accessing the desktop until information is restored, including reapplying any provisioning packages. Windows Autopilot Reset also blocks the new user from accessing the desktop until an Intune sync is completed.

Important

Windows Autopilot Reset only supports Microsoft Entra join devices. Windows Autopilot Reset doesn't support Microsoft Entra hybrid join devices. For Microsoft Entra hybrid join devices, a [full device wipe](#) is required. When a hybrid Microsoft Entra device goes through a full device reset, it might take up to 24 hours for it to be ready to be deployed again. This request can be expedited by re-registering the device. Consider also using the [Windows Autopilot deployment for existing devices](#) scenario to wipe the device.

Information removed and reset by a Windows Autopilot Reset

The Windows Autopilot Reset process removes or resets the following information from the existing device:

- The device's primary user is removed when a remote Windows Autopilot Reset is used. The next user who signs in after the Windows Autopilot Reset will be set as the primary user. Shared devices will remain shared after the remote Autopilot Reset.
- The device's owner in Microsoft Entra is removed when a remote Windows Autopilot Reset is used. The next user who signs in after the Windows Autopilot Reset will be set as the owner.
- Removes personal files, apps, and settings.
- Reapplies a device's original settings.
- Sets the region, language, and keyboard to the original values.

Information kept and migrated after a Windows Autopilot Reset

The Windows Autopilot Reset process automatically keeps the following information from the existing device:

- Maintains the device's identity connection to Microsoft Entra ID.
- Maintains the device's management connection to Intune.
- Wi-Fi connection details.
- Provisioning packages previously applied to the device.
- A provisioning package present on a USB drive when the reset process is started.
- Microsoft Entra device membership and Intune enrollment information.
- System Center Endpoint Protection (SCEP) certificates.
- The device's primary user and owner in Microsoft Entra aren't updated when a local Windows Autopilot Reset is used.

Windows Autopilot Reset requirements

- Enrolled in Microsoft Entra ID. Only Microsoft Entra join devices are supported. Microsoft Entra hybrid join devices aren't supported.
- Enrolled in Intune.
- [Windows Recovery Environment \(WinRE\)](#) is correctly configured and enabled on the device where Windows Autopilot Reset is used.
- User initiating [local Windows Autopilot Reset](#) must be a local administrator on the device.
- Admins initiating a [remote Windows Autopilot Reset](#) must be a member of the Intune Service Administrator role.

Windows Autopilot Reset Scenarios in Intune

Windows Autopilot Reset in Intune supports two scenarios:

- [Local reset](#) - a Windows Autopilot Reset started locally on the device by a user.
- [Remote reset](#) - a Windows Autopilot Reset started remotely by an Intune admin in Microsoft Intune.

How Windows Autopilot Reset works

Windows Autopilot Reset works by using the [push-button reset](#) feature in Windows. The following actions occur during a Windows Autopilot Reset:

- A new OS of the same version is created by reconstructing it from the WinSxS store.
- Migration of data is performed between the old OS and the new OS to preserve the items from [Information kept and migrated after a Windows Autopilot Reset](#).
- All existing user profiles and data are deleted.
- Non-Microsoft apps are uninstalled.

Walkthrough

Both local Windows Autopilot Reset and remote Windows Autopilot Reset require a minimal number of steps to implement. Unlike other Autopilot scenarios, instructions with multiple steps aren't needed. Select the desired Windows Autopilot Reset scenario for instructions on how to implement the scenario:

[Local Windows Autopilot Reset](#)

[Remote Windows Autopilot Reset](#)

Related content

For more information on Windows Autopilot Reset, see the following articles:

- [Windows Autopilot self-deploying mode](#).
- [Push-button reset](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Enable local Windows Autopilot Reset

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

To enable a local Windows Autopilot Reset, the **DisableAutomaticReDeploymentCredentials** policy must be configured. This policy is documented in the [Policy CSP](#). By default, local Windows Autopilot Reset is disabled. This default ensures that a local Autopilot Reset isn't accidentally triggered.

Workflow

The following steps are required to enable and trigger local Windows Autopilot Reset:

1. Create a configuration profile in Intune that enables local Windows Autopilot Reset.
2. Make sure WinRE is installed on device where Windows Autopilot Reset is triggered.
3. Trigger Windows Autopilot Reset locally on device with an account that has local administrator privileges.

Enable local Windows Autopilot Reset in Intune

To create a configuration profile that sets the **DisableAutomaticReDeploymentCredentials** policy and enables local Windows Autopilot Reset in Intune, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **Manage devices**, select **Configuration**.
4. In the **Devices | Configuration** screen:
 - a. At the top, make sure **Policies** is selected.
 - b. Select the **Create** drop down menu and then select **New Policy**.
5. In the **Create a profile** window that opens:
 - a. Under **Platform**, select **Windows 10 and later**.
 - b. Under **Profile type**, select **Templates**.

- c. When the templates appear, under **Template name**, select **Device restrictions**. If **Device restrictions** isn't visible, scroll through the **Template name** list until **Device restrictions** is visible or search for **Device restrictions** in the **Search by profile name** box.
- d. Select **Create** to close the **Create a profile** window.
6. In the **Device restrictions** screen that opens:
- a. In the **Basics** page:
 - i. Next to **Name**, enter a name for the domain join profile.
 - ii. Next to **Description**, enter a description for the domain join profile.
 - iii. Select **Next**.
 - b. In the **Configuration settings** page:
 - i. Scroll through the list and locate **General**.
 - ii. Select **General** to expand it.
 - iii. Under **General**, scroll down and locate **Autopilot Reset**.
 - iv. Next to **Autopilot Reset**, select **Allow**.
 - v. select **Next**.
7. In the **Assignments** page:
- a. Under **Included groups**, select **Add groups**.
 - b. In the **Select groups to include** window that opens, select the groups that the configuration profile should be assigned to and then select **Select**. The device groups selected here are normally the same device groups created when implementing the different [Autopilot scenarios](#).

 **Note**

Make sure to add the correct device groups under **Included groups** and not under **Excluded groups**. Accidentally adding the desired device groups under **Excluded groups** results in those devices being excluded and they don't receive the Autopilot profile.

- c. Under **Included groups > Groups**, ensure the correct groups are selected, and then select **Next**.
8. In the **Applicability Rules** page, select **Next**. For this tutorial, applicability rules are being skipped. However if applicability rules are needed, do so at this screen. For more information about scope tags, see [Applicability rules](#).
9. In the **Review + Create** page, review and verify that all of the settings are set as desired, and then select **Create** to create the domain join profile.

Trigger local Windows Autopilot Reset

To trigger a local Windows Autopilot Reset on a device, follow these steps:

1. Make sure that the [Windows Recovery Environment \(WinRE\)](#) is correctly configured and enabled on the device where the Windows Autopilot Reset is being performed. WinRE can be enabled with the [REAgentC.exe tool](#) via the following command:

```
Windows Command Prompt
```

```
reagentc.exe /enable
```

2. Make sure that the device is in the device group where the Windows Autopilot Reset configuration profile was assigned to.
3. If a provisioning package was created that should be applied during the local Windows Autopilot Reset, plug in the USB drive that contains the provisioning package.
4. From the Windows device lock screen, enter the keystroke **CTRL** + **WIN** + **R**.
5. To trigger the local Autopilot Reset, sign into the device with an account that has local administrator credentials.

Once the local Autopilot Reset is triggered, the reset process starts. Once provisioning is complete, the device is again ready for use.

Related content

For more information on local Windows Autopilot Reset, see the following articles:

- [Reset devices with local Windows Autopilot Reset](#).

- Windows Recovery Environment (WinRE).
 - REAgentC.exe tool.
-

Feedback

Was this page helpful?



Provide product feedback ↗

Reset devices with remote Windows Autopilot Reset

Article • 06/20/2024 • Applies to: Windows 11, Windows 10

Intune can be used to start the remote Windows Autopilot Reset process. Resetting in this way avoids the need for someone to visit each device that needs to be reset to start the Windows Autopilot Reset process. Unlike [local Windows Autopilot reset](#), a configuration profile doesn't need to be configured or assigned for remote Windows Autopilot Reset to work. Remote Windows Autopilot Reset is available on any Microsoft Entra join device that is an Autopilot device without any additional configuration.

Workflow

The following steps are required to enable and trigger local Windows Autopilot Reset:

1. Make sure WinRE is installed on device where Windows Autopilot Reset is triggered.
2. Make sure Intune admin has appropriate privileges in Intune to perform remote Windows Autopilot Resets.
3. In Intune, remotely trigger Windows Autopilot Reset on device.
4. Force device to start the remote Windows Autopilot Reset (optional).

Triggering a remote Windows Autopilot Reset

To trigger a remote Windows Autopilot Reset via Intune, follow these steps:

1. Make sure that the [Windows Recovery Environment \(WinRE\)](#) is correctly configured and enabled on the device where the Windows Autopilot Reset is being performed. WinRE can be enabled with the [REAgentC.exe tool](#) via the following command:

```
Windows Command Prompt
```

```
reagentc.exe /enable
```

2. Make sure the Intune admin initiating the remote Windows Autopilot Reset is a member of the Intune Service Administrator role. For more information, see [Add users and grant administrative permission to Intune](#).
3. Sign in to the [Microsoft Intune admin center](#).

4. In the **Home** screen, select **Devices** in the left pane.
5. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
6. In the **Windows | Windows devices** screen, under **Device name** select the targeted devices to perform the Windows Autopilot Reset.
7. In the page that opens that displays the properties of the device, select **Autopilot Reset** in the toolbar at the top of the window.
8. An Autopilot Reset warning message is displayed. Select **Yes** to continue.
9. A message should display confirming that the Autopilot reset is initiated. The Windows Autopilot Reset should start shortly thereafter on the device.

Once the Autopilot Reset is complete, the device is again ready for use.

Forcing a device to start the remote Windows Autopilot Reset

Unlike [local Windows Autopilot reset](#), when the remote Windows Autopilot Reset is initiated for a device, the reset might not start immediately. Instead, the reset will occur when the device next checks in with Intune and gets updated policy. For more information, see [Policy refresh intervals](#)

A Windows Autopilot Reset can be forced to start sooner on a device by forcing the device to obtain the latest Intune policy. Forcing remote Windows Autopilot Reset to start sooner can be done either remotely or locally on the device.

Remotely force a device to start the remote Windows Autopilot Reset

To force the device to obtain the latest Intune policy remotely, follow these steps:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device name** select the devices where the remote Windows Autopilot Reset was initiated.

5. In the page that opens that displays the properties of the device, select **Sync** in the toolbar at the top of the window.

6. A Sync warning message is displayed. Select **Yes** to continue.

These steps should force the device to obtain the latest Intune policy. The Autopilot Reset should start shortly thereafter.

Locally force a device to start the remote Windows Autopilot Reset

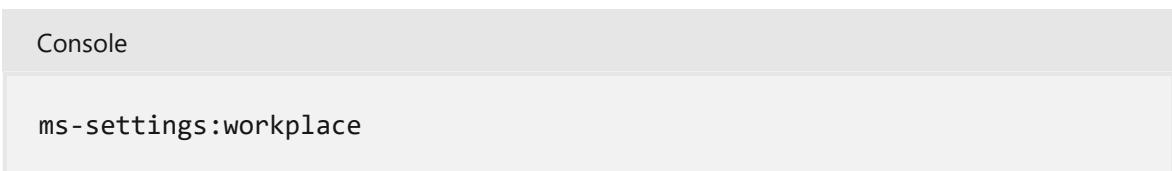
To force the device to obtain the latest Intune policy locally on the device, sign into the device where the remote Autopilot Reset was initiated. Once signed into the device, open the **Accounts > Access work or school** pane in the **Settings** app by selecting the following link:

[Access work or school](#)

Or

1. Right-click on the **Start** menu and select **Run**.

2. In the **Run** window, next to **Open:**, enter:



and then select **OK**.

Or

1. Right-click on the **Start** menu and select **Settings**.

2. In the **Settings** app:

- Windows 11
 - a. Select **Accounts** in the left hand pane.
 - b. In the **Accounts** page, select **Access work or school**.
- Windows 10
 - a. Select **Accounts**.
 - b. In the left hand pane, select **Access work or school**.

Once the **Access work or school** pane is open in the **Settings** app, follow these steps:

1. In the Accounts > Access work or school pane, select Connected by <user@domain> to expand the section.
2. In the expanded section, next to Managed by <organization>, select the Info button.
3. In the Accounts > Access work or school > Managed by <organization> page, under Device sync status, select the Sync button.

These steps should force the device to obtain the latest Intune policy. The Autopilot Reset should start shortly thereafter.

Related content

For more information on local Windows Autopilot Reset, see the following articles:

- [Reset devices with remote Windows Autopilot Reset](#).
- [Windows Recovery Environment \(WinRE\)](#).
- [REAgentC.exe tool](#).
- [Add users and grant administrative permission to Intune](#).
- [Policy refresh intervals](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot scenarios and capabilities

Article • 06/11/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

Scenarios

Windows Autopilot supports a growing list of scenarios that organizations commonly need. These needs vary based on:

- Organization type.
- Progress moving to the latest version of Windows.
- The state of transitioning to [modern management](#).

The following Windows Autopilot scenarios are described in this guide:

[Expand table](#)

Scenario	Description
Windows Autopilot user-driven mode	Deploy and configure devices so that an end user can set it up for themselves.
Windows Autopilot self-deploying mode	Deploy devices to be automatically configured for shared use, as a kiosk, or as a digital signage device.
Windows Autopilot Reset	Redeploy a device in a business-ready state.
Pre-provisioning	Pre-provision a device with up-to-date applications, policies, and settings.
Windows Autopilot for existing devices	Deploy Windows on an existing Windows device.

These scenarios are summarized in the following video:

<https://learn-video.azurefd.net/vod/player?id=7e47e04e-7f51-4eba-9a23-d65f3411b425&locale=en-us&embedUrl=%2Fautopilot%2Fwindows-autopilot-scenarios>

Windows Autopilot capabilities

Temporary Access Pass

Organizations using [Temporary Access Pass](#) can use this feature with Windows Autopilot Microsoft Entra join user driven, pre-provisioning, and self-deploying mode for shared devices. The native Windows sign-in credential provider doesn't support Temporary Access Pass so it requires the enablement of WebSign-in. To enable this feature in the organization, follow the Configuration Service Provider (CSP) details outlined in [Policy CSP - Authentication](#). This feature isn't supported with Windows Autopilot Microsoft Entra hybrid join devices and isn't applicable on self-deploying mode kiosks.

Cortana voiceover and speech recognition during OOBE

In Windows 10, Cortana voiceover and speech recognition during the out-of-box experience (OOBE) is **DISABLED** by default. This default applies to all Windows Pro, Education, and Enterprise editions. This feature isn't available in versions of Windows after Windows 10.

Cortana voiceover and speech recognition can be enabled during OOBE by creating the registry key value `EnableVoiceForAllEditions` in the following registry key:

`HKLM\Software\Microsoft\Windows\CurrentVersion\OOBE\`

This registry key value doesn't exist by default.

The key value is a DWORD with 0 = disabled and 1 = enabled.

[+] Expand table

Value	Description
0	Cortana voiceover is disabled
1	Cortana voiceover is enabled
No value	Device falls back to default behavior of the edition

To change this key value, use the Windows Configuration Designer (WCD) tool to create as PPKG as documented in [EnableCortanaVoice](#).

For more information, see [Cortana voice support](#).

! Note

Microsoft deprecated the Windows Cortana standalone app. The Cortana productivity assistant is still available. For more information on deprecated features

on Windows client, go to [Deprecated features for Windows client](#).

BitLocker encryption

With Windows Autopilot, BitLocker encryption settings can be configured to apply before automatic encryption is started. For more information, see [Setting the BitLocker encryption algorithm for Autopilot devices](#).

Related content

- [Windows Autopilot: What's new.](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot Enrollment Status Page

Article • 06/11/2024 • Applies to: Windows 11, Windows 10

When a user signs into a device for the first time, the Enrollment Status Page (ESP) displays the device's configuration progress. The ESP also makes sure the device is in the expected state before the user can access the desktop for the first time.

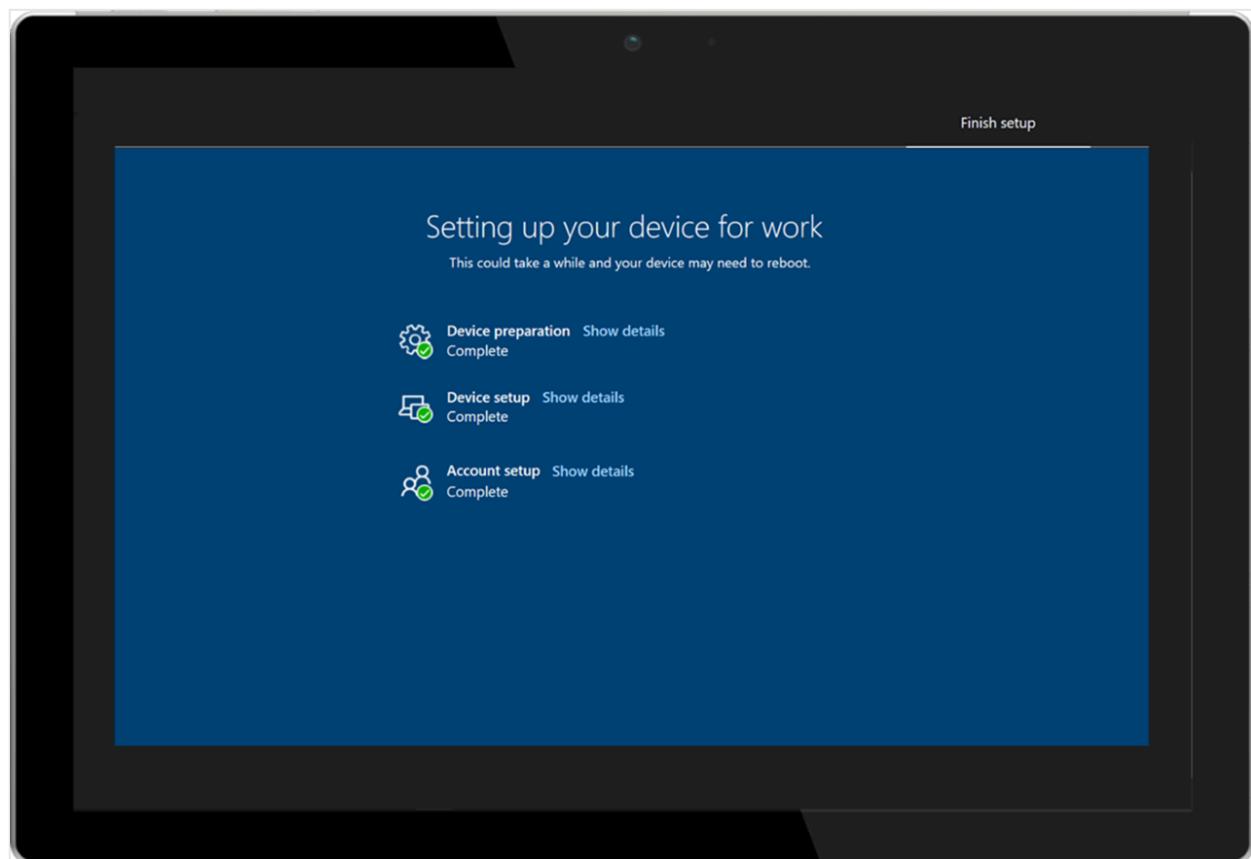
The ESP tracks the installation of applications, security policies, certificates, and network connections.

ESP profiles

An administrator can deploy ESP profiles to a licensed Intune user and configure specific settings within the ESP profile. A few of these settings include:

- Force the installation of specified applications.
- Allow users to collect troubleshooting logs.
- Specify what a user can do if device setup fails.

For more information, see [Set up the Enrollment Status Page](#).



Related content

- FirstSyncStatus details in the DMClient CSP.
 - Support Tip: Office C2R installation is now tracked during ESP ↗.
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Windows Autopilot deployment process

Article • 06/11/2024 • Applies to: Windows 11, Windows 10

Windows Autopilot deployment processes are summarized in the following poster:

[Windows Autopilot deployment chart ↗](#)

The poster is two pages in portrait mode (11x17).

Note

The Windows Autopilot for existing devices process is included in the [Microsoft Configuration Manager deployment poster](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot registration overview

Article • 06/19/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

Before a device is deployed using Windows Autopilot, the device must be registered with the Windows Autopilot deployment service.

Successful registration requires that two processes are complete:

1. The device's unique [hardware identity](#) (known as a hardware hash) is captured and uploaded to the Autopilot service.
2. The device is associated to an Azure tenant ID.

Ideally, the OEM, reseller, or distributor performs both of these processes from which the devices were purchased. An OEM or other device provider uses the [registration authorization](#) process to perform device registration on behalf of the organization.

Registration can also be performed within the organization by collecting the hardware identity from new or existing devices and [uploading it manually](#). If devices meet certain requirements, they can also be configured for [automatic registration](#) with Windows Autopilot. For more information about the ways in which devices can be registered with Windows Autopilot, see the following overview articles:

- [OEM registration](#)
- [Reseller, distributor, or partner registration](#)
- [Automatic registration](#)
- [Manual registration](#)

When an Autopilot device is registered, it automatically creates a Microsoft Entra object. The Autopilot deployment process needs this object to identify the device before the user signs in. If the object is deleted, the device can fail to enroll through Autopilot.

Important

The following type of devices shouldn't be registered as a Windows Autopilot device:

- [Microsoft Entra registered](#) devices, also known as "workplace joined" devices.
- [Intune MDM-only enrollment](#) devices.

These options are intended for users to join personally owned devices to their organization's network. Windows Autopilot registered devices are registered as

corporate owned devices.

If a device is already one of these two types of devices, to register it as a Windows Autopilot device, first remove it from Microsoft Intune and Microsoft Entra ID. For more information, see [Device appears as Microsoft Entra registered instead of Microsoft Entra joined](#) and [Deregister a device](#).

If a profile isn't assigned to a Windows Autopilot device, it receives the default Windows Autopilot profile. If a device shouldn't go through Autopilot, remove the Windows Autopilot registration.

Terms

The following terms are used to refer to various steps in the registration process:

 Expand table

Term	Definition
Device registration	Device registration happens when a device's hardware hash is associated with the Windows Autopilot service. This process can be automated for new enterprise devices manufactured by OEMs that are Windows Autopilot partners.
Add devices	Adding a device is the process of registering a device with the Windows Autopilot service (if it isn't already registered) and associating it to a tenant ID .
Import devices	Importing devices is the process of uploading a comma-separated-values (CSV) file that contains device information in order to manually add devices. The device information includes information such as the model and serial number.
Enroll devices	Enrolling a device is the process of adding devices to Intune.

Device identification

To identify a device with Windows Autopilot, the device's unique hardware hash must be captured and uploaded to the service. As previously mentioned, this step is ideally done by the hardware vendor (OEM, reseller, or distributor) automatically associating the device with an organization. It's also possible to do identify a device with a [harvesting process](#) that collects the device's hardware hash from within a running Windows installation.

The hardware hash contains details about the device, such as:

- Manufacturer.

- Model.
- Device serial number.
- Hard drive serial number.
- Details about when the ID was generated.
- Many other attributes that can be used to uniquely identify the device.

The hardware hash changes each time it's generated because it includes details about when it was generated. When the Windows Autopilot deployment service attempts to match a device, it considers changes like that. It also considers large changes such as a new hard drive, and is still able to match successfully. But large changes to the hardware, such as a motherboard replacement, wouldn't match, so a new hash would need to be generated and uploaded.

For more information about device IDs, see the following articles:

- [Windows Autopilot device guidelines](#).
- [Add devices to a customer account](#).

Windows Autopilot devices

Devices that are registered with the Windows Autopilot service are displayed in the [Intune admin center](#) under **Devices > Enrollment > Windows > Windows Autopilot > Devices**:

 **Note**

Devices that are listed in Intune under **Devices > Windows > Windows devices** aren't the same as Windows Autopilot devices **Devices > Enrollment > Windows > Windows Autopilot > Devices**. Windows Autopilot devices are added to the list of **Windows devices** when both of the following are complete:

- The Autopilot registration process is successful.
- A [licensed](#) user has signed in on the device.

Deregister a device

Whenever a device permanently leaves an organization, the device should always be deregistered from Autopilot. For example, the device leaves the organization for repair or because the device is at the end of its life cycle.

Below we describe the steps an admin would go through to deregister a device from Intune and Autopilot.

Delete from Intune

Before a device is deregistered from Autopilot, it first has to be deleted from Intune. To delete an Autopilot device from Intune:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. Under **Device name**, find the device that needs to be deleted and then select the device. If necessary, use the **Search** box.
5. In the properties screen for the device, make a note of the serial number listed under **Serial number**.
6. After making a note of the serial number of the device, select **Delete** in the toolbar at the top of the page.
7. A warning dialog box appears to confirm the deletion of the device from Intune. Select **Yes** to confirm deleting the device.

Deregister from Autopilot using Intune

Once the device is deleted from Intune, it can then be deregistered from Autopilot. To deregister a device from Autopilot:

1. Make sure the device is deleted from Intune as described in the [Delete from Intune](#) section.
2. Sign in to the [Microsoft Intune admin center](#).
3. In the **Home** screen, select **Devices** in the left pane.
4. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
5. In the **Windows | Windows enrollment** screen, select **Windows enrollment**
6. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.

7. In the **Windows Autopilot devices** screen that opens, under **Serial number**, find the device that needs to be deregistered by its serial number as determined in the [Delete from Intune](#) section. If necessary, use the **Search by serial number** box.
8. Select the device by selecting the checkbox next to the device.
9. Select the extended menu icon (...) on the far right end of the line containing the device. A menu appears with the option **Unassign user**.
 - If the **Unassign user** option is available and not greyed out, then select it. A warning dialog box appears confirming to unassign the user from the device. Select **OK** to confirm unassigning the device from the user.
 - If the **Unassign user** option isn't available and greyed out, then move on to the next step.
10. With the device still selected, select **Delete** in the toolbar at the top of the page.
11. A warning dialog box appears to confirm the deletion of the device from Autopilot. Select **Yes** to confirm deleting the device.
12. The deregistration process might take some time. The process can be accelerated by selecting the **Sync** button in the toolbar at the top of the page.
13. Every few minutes select **Refresh** in the toolbar at the top of the page until the device is no longer present.

ⓘ Important

- For Microsoft Entra join devices, no additional steps are necessary to remove the device from Intune and Autopilot. Unneeded steps include manually deleting the device from Microsoft Entra ID. Manually deleting the device from Microsoft Entra ID might cause unexpected problems, issues, and behavior. If needed, the device will be automatically removed from Microsoft Entra ID after these steps are followed.
- For Microsoft Entra hybrid join devices, delete the computer object from the on-premises Active Directory Domain Services (AD DS) environment. Deleting the computer object from the on-premises AD DS ensures that the computer object isn't resynced back to Microsoft Entra ID. After the computer object is deleted from the on-premises AD DS environment, no additional steps are necessary to remove the device from Intune and Autopilot. Unneeded steps include manually deleting the device from Microsoft Entra ID. Manually

deleting the device from Microsoft Entra ID might cause unexpected problems, issues, and behavior. If needed, the device will be automatically removed from Microsoft Entra ID after these steps are followed.

The above steps deregister the device from Autopilot, unenroll the device from Intune, and disjoin the device from Microsoft Entra ID. It might appear that only deregistering the device from Autopilot is needed. However, there are barriers in Intune that require all the above steps to avoid problems with lost or unrecoverable devices. To prevent the possibility of orphaned devices in the Autopilot database, Intune, or Microsoft Entra ID, it's best to complete all the steps. If a device gets into an unrecoverable state, contact the appropriate [Microsoft support alias](#) for assistance.

Deregister from Autopilot using Microsoft 365 admin center

The device can be deregistered from Autopilot in [Microsoft 365 admin center](#) if using the Microsoft 365 admin center instead of Intune. To deregister an Autopilot device from the Microsoft 365 admin center:

1. Sign into to the [Microsoft 365 admin center](#).
2. Navigate to **Devices > Autopilot**.
3. Select the device to be deregistered and then select **Delete device**.

Deregister from Autopilot in Microsoft Partner Center (MPC)

To deregister an Autopilot device from the Microsoft Partner Center (MPC), a Cloud Solution Partner (CSP) would:

1. Sign into the Microsoft Partner Center (MPC).
2. Navigate to **Customer > Devices**.
3. Select the device to be deregistered and then select **Delete device**.

The screenshot shows the Microsoft Partner Center (MPC) interface. On the left, there's a sidebar with links like Order history, Subscriptions, Software, Azure reservations, Devices (which is selected), Analytics, Users and licenses, Service management, and Account. The main content area is titled 'Devices' and has a sub-section 'Windows AutoPilot profiles'. It features a large 'Add new profile' button. Below it, a message says 'There are no profiles.' In another section titled 'Apply profiles to devices', there's an 'Add devices' button, followed by three icons: 'Apply profile', 'Remove profile', and 'Delete device' (which is highlighted with a red box). There's also a 'Group name' field containing 'BKTTestGroup1' with a checked checkbox.

Partners deregistering a device from Autopilot in Microsoft Partner Center (MPC) only deregisters the device from Autopilot. It doesn't perform any of the following actions:

- Unenroll the device from the mobile device management (MDM) solution, such as Intune.
- Disjoin the device from Microsoft Entra ID.

For these reasons, the OEM or CSP should work with the customer IT administrators to have the device fully removed by following the steps in the [Deregister a device](#) section.

An OEM or CSP with integrated OEM Direct APIs can also deregister a device with the **AutopilotDeviceRegistration API**. Make sure the **TenantID** and **TenantDomain** fields are left blank.

Note

If an admin registered a device via another portal other than the Microsoft Partner Center (MPC) such as Intune or the [Microsoft 365 admin center](#), the device doesn't show up in Microsoft Partner Center (MPC). For a partner to register a device in the Microsoft Partner Center (MPC), the device first needs to be deregistered using the steps outlined in the [Deregister a device](#) section.

Related content

- [Register devices manually.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

OEM registration

Article • 06/28/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

Device registration process

When devices are purchased from an OEM, the OEM can automatically register the devices with the Windows Autopilot. For the list of OEMs that support registration, see the **Participant device manufacturers and resellers** section of the [Windows Autopilot page](#).

Note

While the hardware hashes, also known as hardware IDs, are generated as part of the OEM device manufacturing process, the hardware hashes aren't normally provided directly to customers or Cloud Solution Partners (CSPs). Instead, the OEM should register devices on the customer's behalf. In cases where CSPs register devices, OEMs might provide PKID information to those partners to support the device registration process.

OEMs must follow [device guidelines](#) for Windows Autopilot devices.

Service data

Microsoft manages and maintains Windows Autopilot. This service provides the backend database that associates hardware hashes with customer tenants. When an OEM registers devices for a customer, they're writing that data to this database and not directly to the customer's tenant. No permissions to the customer's tenant are granted or required for OEMs to register devices on the customer's behalf.

Customer consent

Before an OEM can register devices for an organization, the organization must grant the OEM permission to do so. The OEM begins this process with approval granted by a Microsoft Entra Global Administrator from the organization. For more information, see [OEM authorization](#).

Important

Microsoft recommends using roles with the fewest permissions. Using lower permissioned accounts helps improve security for an organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when an existing role can't be used.

Microsoft Surface registration

For Surface devices, see [Surface registration support for Windows Autopilot](#).

Related content

- [Registration overview](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Reseller, distributor, or partner registration

Article • 06/28/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

Customers can purchase devices from resellers, distributors, or other partners. As long as these resellers, distributors, and partners are part of the [Cloud Solution Partners \(CSP\) program](#), they too can register devices for the customer.

As with OEMs, CSP partners must be granted permission to register devices for an organization. This process is described in the [CSP authorization](#) section of the Windows Autopilot customer consent article. In summary:

- The CSP partner requests a relationship with the organization. That organization's Global Administrator approves the request.
- After the approval, CSP partners add devices using [Partner Center](#), either directly through the web site or via available APIs that can automate the same tasks.

For Surface devices, Microsoft Support can help with device registration. For more information, see [Surface Registration Support for Windows Autopilot](#).

Windows Autopilot doesn't require delegated administrator permissions when establishing the relationship between the CSP partner and the organization. As part of the Global Administrator's approval process, they can choose to uncheck the **Include delegated administration permissions** checkbox.

Important

Microsoft recommends using roles with the fewest permissions. Using lower permissioned accounts helps improve security for an organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when an existing role can't be used.

Tip

While resellers, distributors, or partners could boot each new Windows device to obtain the hardware hash for purposes of providing them to customers or direct registration by the partner, this method isn't recommended. Instead, these partners should register devices using the PKID information obtained from the device

packaging, such as the barcode, or obtained electronically from the OEM or upstream partner/distributor.

 **Note**

Partner Center doesn't have access to profiles created in Intune or Microsoft Store for Business. It only has access to the Autopilot profiles created through Partner Center.

Related content

- [Registration overview.](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) 

Automatic registration of existing devices

Article • 06/11/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

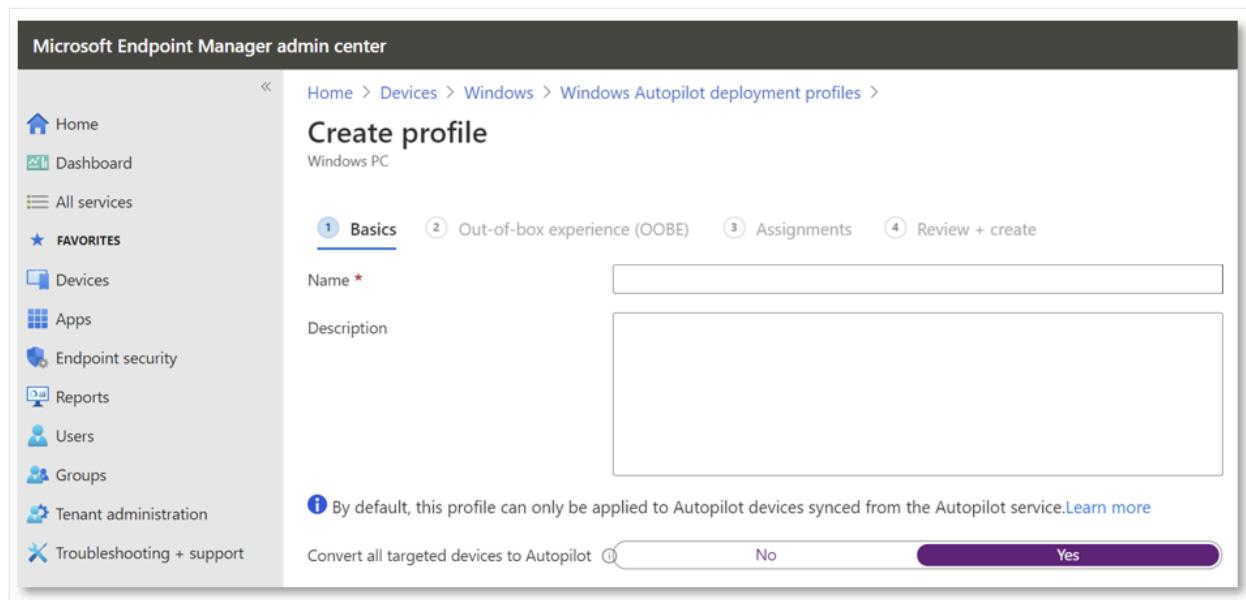
Requirements

An existing device can automatically register if it's:

- Running a [supported version](#) of Windows
- Enrolled in a mobile device management (MDM) service such as Intune
- A corporate device that isn't already registered with Autopilot

For devices that meet these requirements, the MDM service can ask the device for the hardware hash. After it has that, it can automatically register the device with Windows Autopilot.

For more information on how to automatically register devices for Windows Autopilot with Microsoft Intune, see [Create an Autopilot deployment profile](#) and review the description of the **Convert all targeted devices to Autopilot** setting. See the following example:



The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left is a navigation sidebar with various icons and links like Home, Dashboard, All services, Favorites, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled 'Create profile' under 'Windows PC'. It has four tabs: Basics (selected), Out-of-box experience (OOBE), Assignments, and Review + create. Under Basics, there are fields for 'Name' (marked with a red asterisk) and 'Description'. A note at the bottom states: 'By default, this profile can only be applied to Autopilot devices synced from the Autopilot service.' Below this is a switch labeled 'Convert all targeted devices to Autopilot' with options 'No' and 'Yes'.

! Note

Using the setting **Convert all targeted devices to Autopilot** in the Autopilot profile doesn't automatically convert existing hybrid Microsoft Entra device in the assigned groups into a Microsoft Entra device. The setting only registers the devices in the

assigned groups for the Autopilot service. For more information, see [Create an Autopilot deployment profile](#).

Windows Autopilot for existing devices

When the [Windows Autopilot for existing devices](#) scenario is used, devices don't need to be preregistered with Windows Autopilot. Instead, a configuration file (AutopilotConfigurationFile.json) containing all the Windows Autopilot profile settings is used. The device can then be registered with Windows Autopilot using the same [Convert all targeted devices to Autopilot](#) setting.

Related content

- [Registration overview](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

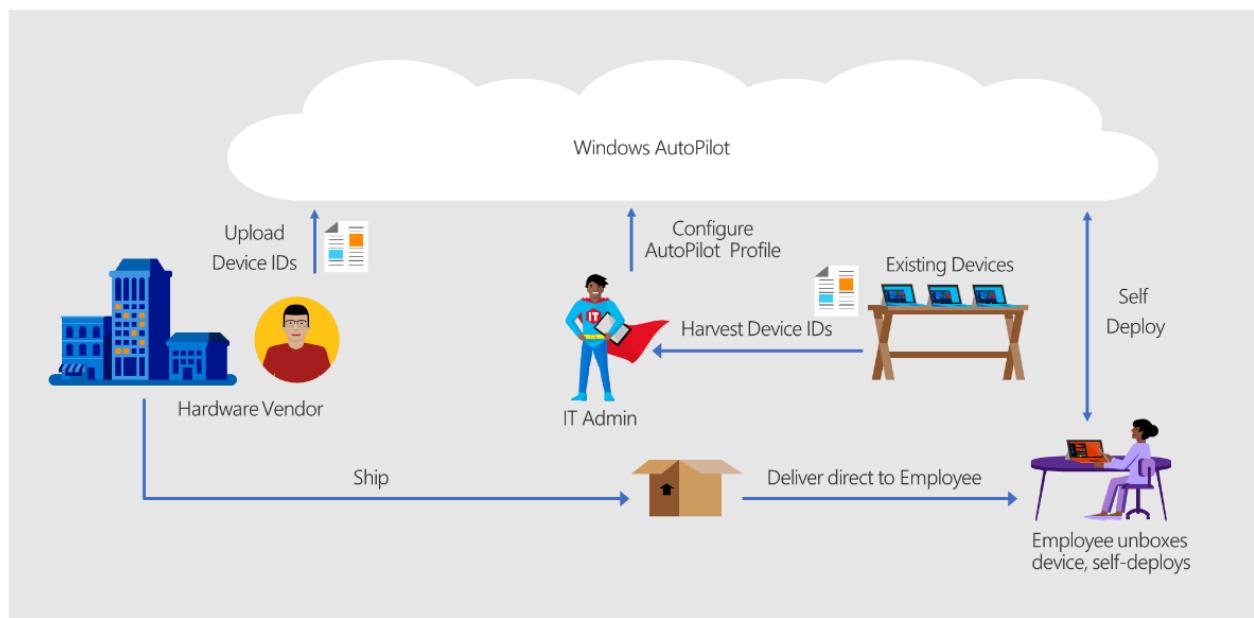
Manual registration overview

Article • 06/11/2024 • Applies to: ✓ Windows 11, ✓ Windows 10, ✓ Windows Holographic

Ideally, the OEM, reseller, or distributor from which the device was purchased performs the registration of a device with Windows Autopilot. However it's also possible to register devices manually. A device might need to be registered manually if:

- The device was obtained from a non-participant device manufacturer or reseller.
- The device is a virtual machine (VM).
- The device doesn't otherwise qualify for automatic registration, such as an existing legacy device.

The following diagram shows how manual registration and OEM registration might be used to deploy both new and existing devices with Windows Autopilot.



For a list of participant device manufacturers and device resellers, see [Autopilot device manufacturers and resellers](#).

To [manually register a device](#), a device's hardware hash first has to be captured. Once this process is completed, the resulting hardware hash can be uploaded to the Windows Autopilot service. Because this process requires booting the device into Windows to obtain the hardware hash, manual registration is intended primarily for testing and evaluation scenarios.

ⓘ Note

Customers can only register devices with a hardware hash. Other methods (PKID, tuple) are available through OEMs or CSP partners as described in the previous

sections.

Platforms for device registration

After the hardware hashes are captured from existing devices, they can be uploaded in any of the following ways:

- **Microsoft Intune** - Intune is the preferred mechanism for all customers.
 - The Microsoft Intune admin center is used for Intune device enrollment.
- Partner Center - Partner Center is used by CSP partners to register devices on behalf of customers.
- Microsoft 365 Business & Office 365 Admin - Microsoft 365 Business & Office 365 Admin is typically used by small and medium businesses (SMBs) who manage their devices using Microsoft 365 Business.
- Microsoft Store for Business - Since Microsoft Store for Business is deprecated, use another method instead.

ⓘ Important

Microsoft Store for Business and Microsoft Store for Education is deprecated. The current capabilities of free apps can be used while they're still available. For more information about this change, see [Evolving the Microsoft Store for Business and Education](#) and [Microsoft Store for Business and Education](#).

A summary of each platform's capabilities is provided in the following table:

[\[+\] Expand table](#)

Platform/Portal	Register devices?	Create/Assign profile	Acceptable Device ID
OEM Direct API	YES - 1000 at a time max	NO	Tuple or PKID
Partner Center	YES - 1000 at a time max	YES ³	Tuple or PKID or 4K HH
Intune	YES - 500 at a time max	YES ¹²	4K HH

Platform/Portal	Register devices?	Create/Assign profile	Acceptable Device ID
Microsoft Store for Business	YES - 1000 at a time max	YES ⁴	4K HH
Microsoft 365 Business Premium	YES - 1000 at a time max	YES ³	4K HH

- ¹ Microsoft recommended platform to use.
- ² Intune license required.
- ³ Feature capabilities are limited.
- ⁴ Device profile assignment will be retired from Microsoft Store for Business in the coming months.

For more information about device IDs, see the following articles:

- [Device identification](#).
- [Windows Autopilot device guidelines](#).
- [Add devices to a customer account](#).

Related content

- [Registration overview](#).
- [Manually register devices with Windows Autopilot](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot user-driven mode

Article • 06/11/2024 • Applies to: Windows 11, Windows 10

Windows Autopilot user-driven mode lets a new Windows device to be configured to automatically transform them from their factory state to a ready-to-use state. This process doesn't require that IT personnel touch the device.

The process is simple. Devices can be shipped or distributed to the end user directly with the following instructions:

1. Unbox the device, plug it in, and turn it on.
2. If it uses multiple languages, choose a language, locale, and keyboard.
3. Connect it to a wireless or wired network with internet access. If using wireless, first connect to the wi-fi network.
4. Specify an e-mail address account and password for the organization.

The rest of the process is automated. The device does the following steps:

1. Join the organization.
2. Enroll in Microsoft Intune or another mobile device management (MDM) service.
3. Get configured as defined by the organization.

Other prompts can be suppressed during the out-of-box experience (OOBE). For more information on the available options, see [Configuring Autopilot profiles](#).

Important

If Active Directory Federation Services (ADFS) is being used, there's a [known issue](#) that can enable the end user to sign in with a different account than the one assigned to that device.

Windows Autopilot user-driven mode supports Microsoft Entra join and Microsoft Entra hybrid joined devices. For more information about these two join options, see the following articles:

- [What is a device identity?](#).
- [Learn more about cloud-native endpoints](#).
- [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints](#).
- [Tutorial: Set up and configure a cloud-native Windows endpoint with Microsoft Intune](#).
- [How to: Plan your Microsoft Entra join implementation](#).
- [A framework for Windows endpoint management transformation ↗](#).

- Success with remote Windows Autopilot and Microsoft Entra hybrid join .

The steps of the user-driven process are as follows:

1. After the device connects to a network, the device downloads a Windows Autopilot profile. The profile defines the settings used for the device. For example, define the prompts suppressed during OOB.
2. Windows checks for critical OOB updates. If updates are available, they're automatically installed. If necessary, the device restarts.
3. The user is prompted for Microsoft Entra credentials. This customized user experience shows the Microsoft Entra tenant name, logo, and sign-in text.
4. The device joins Microsoft Entra ID or Active Directory, depending on the Windows Autopilot profile settings.
5. The device enrolls to Intune or another configured MDM service. Depending on the organizational needs, this enrollment occurs either:
 - During the Microsoft Entra join process, using MDM auto-enrollment.
 - Before the Active Directory-join process.
6. If configured, it displays the [enrollment status page](#) (ESP).
7. After the device configuration tasks complete, the user is signed into Windows using the credentials they previously provided. If the device restarts during the device ESP process, the user must reenter their credentials. These details don't persist after restart.
8. After sign-in, the enrollment status page displays for user-targeted configuration tasks.

If any issues are found during this process, see [Windows Autopilot troubleshooting](#).

For more information on the available join options, see the following sections:

- [Microsoft Entra join](#) is available if devices don't need to join an on-premises Active Directory domain.
- [Microsoft Entra hybrid join](#) is available for devices that need to join both Microsoft Entra ID and the on-premises Active Directory domain.

User-driven mode for Microsoft Entra join

To complete a user-driven deployment using Windows Autopilot, follow these preparation steps:

1. Make sure that the users performing user-driven mode deployments can join devices to Microsoft Entra ID. For more information, see [Configure device settings](#) in the Microsoft Entra documentation.
2. Create an Autopilot profile for user-driven mode with the desired settings.
 - In Intune, this mode is explicitly chosen when a profile is created.
 - In Microsoft Store for Business and Partner Center, user-driven mode is the default.
3. If using Intune, create a device group in Microsoft Entra ID, and assign the Autopilot profile to that group.

For each device that is deployed using user-driven deployment, these extra steps are needed:

- Add the device to Windows Autopilot. This step can be done in two ways:
 - Automatically by an OEM or partner when the device is purchased.
 - Manually as described in [Adding devices to Windows Autopilot](#).
- Assign an Autopilot profile to the device:
 - If using Intune and Microsoft Entra dynamic device groups, this assignment can be done automatically.
 - If using Intune and Microsoft Entra static device groups, manually add the device to the device group.
 - If using other methods, like Microsoft Store for Business or Partner Center, manually assign an Autopilot profile to the device.

Tip

If the intended end-state of the device is co-management, device enrollment can be configured in Intune to enable co-management, which happens during the Autopilot process. This behavior directs the workload authority in an orchestrated manner between Configuration Manager and Intune. For more information, see [How to enroll with Autopilot](#).

User-driven mode for Microsoft Entra hybrid join

ⓘ Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. For more information, see [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization](#).

Windows Autopilot requires that devices be Microsoft Entra joined. For an on-premises Active Directory environment, devices can be joined to the on-premises domain. To join the devices, configure Autopilot devices to be [hybrid-joined to Microsoft Entra ID](#).

ⓘ Tip

As Microsoft talks with customers that are using Microsoft Intune and Microsoft Configuration Manager to deploy, manage, and secure their client devices, we often get questions regarding co-managing devices and Microsoft Entra hybrid joined devices. Many customers confuse these two topics. Co-management is a management option, while Microsoft Entra ID is an identity option. For more information, see [Understanding hybrid Microsoft Entra and co-management scenarios](#). This blog post aims to clarify Microsoft Entra hybrid join and co-management, how they work together, but aren't the same thing.

The Configuration Manager client can't be deployed while provisioning a new computer in Windows Autopilot user-driven mode for Microsoft Entra hybrid join. This limitation is due to the identity change of the device during the Microsoft Entra join process. Deploy the Configuration Manager client after the Autopilot process. See [Client installation methods in Configuration Manager](#) for alternative options for installing the client.

Requirements for user-driven mode with hybrid Microsoft Entra ID

- Create a Windows Autopilot profile for user-driven mode.

In the Autopilot profile, under **Join to Microsoft Entra ID as**, select **Microsoft Entra hybrid joined**.

- If using Intune, a device group is needed in Microsoft Entra ID. Assign the Windows Autopilot profile to the group.
- If using Intune, create and assign a Domain Join profile. A Domain Join configuration profile includes on-premises Active Directory domain information.
- The device needs to access the internet. For more information, see the [networking requirements](#).
- Install the Intune Connector for Active Directory.

 **Note**

The Intune Connector joins the device to the on-premises domain. Users don't need permissions to join devices to the on-premises domain. This behavior assumes that the connector is configured for this action on the user's behalf. For more information, see [Increase the computer account limit in the Organizational Unit](#).

- If using a proxy, enable and configure the Web Proxy Auto-Discovery Protocol (WPAD) Proxy settings option.

In addition to these core requirements for user-driven Microsoft Entra hybrid join, the following extra requirements apply to on-premises devices:

- The device has a currently supported version of Windows.
- The device is connected to the internal network and has access to an Active Directory domain controller.
 - It needs to resolve the DNS records for the domain and the domain controllers.
 - It needs to communicate with the domain controller to authenticate the user.

User-driven mode for Microsoft Entra hybrid join with VPN support

Devices joined to Active Directory require connectivity to an Active Directory domain controller for many activities. These activities include validating the user's credentials when they sign-in, and applying group policy settings. The Autopilot user-driven

process for Microsoft Entra hybrid joined devices validates that the device can contact a domain controller by pinging that domain controller.

With the addition of VPN support for this scenario, the Microsoft Entra hybrid join process can be configured to skip the connectivity check. This change doesn't eliminate the need for communicating with a domain controller. Instead, to allow connection to the organization's network, Intune delivers the needed VPN configuration before the user attempts to sign in to Windows.

Requirements for user-driven mode with hybrid Microsoft Entra ID and VPN

In addition to the [core requirements](#) for user-driven mode with Microsoft Entra hybrid join, the following extra requirements apply to a remote scenario with VPN support:

- A currently supported version of Windows.
- In the Microsoft Entra hybrid join profile for Autopilot, enable the following option:
Skip domain connectivity check.
- A VPN configuration with one of the following options:
 - Can be deployed with Intune, and lets the user manually establish a VPN connection from the Windows sign-in screen.
 - Automatically establishes a VPN connection as needed.

The specific VPN configuration required depends on the VPN software and authentication being used. For non-Microsoft VPN solutions, this configuration typically involves deploying a Win32 app via Intune Management Extensions. This app would include the VPN client software and any specific connection information. For example, VPN endpoint host names. For configuration details specific to that provider, see the VPN provider's documentation.

Note

The VPN requirements aren't specific to Autopilot. For example, if a VPN configuration is implemented to enable remote password resets, that same configuration can be used with Windows Autopilot. This configuration would allow a user to sign in to Windows with a new password when not on the organization's network. Once the user signs in and their credentials are cached, subsequent sign-in attempts don't need connectivity since Windows uses the cached credentials.

If the VPN software requires certificate authentication, use Intune to also deploy the required device certificate. This deployment can be done using the Intune certificate enrollment capabilities, targeting the certificate profiles to the device.

Some configurations aren't supported because they aren't applied until the user signs into Windows:

- User certificates
- Non-Microsoft UWP VPN plug-ins from the Windows Store

Validation

Before attempting a Microsoft Entra hybrid join using VPN, it's important to confirm that the user-driven mode for Microsoft Entra hybrid join process works on the internal network. This test simplifies troubleshooting by making sure the core process works before adding the VPN configuration.

Next, confirm Intune can be used to deploy the VPN configuration and its requirements. Test these components with an existing device that's already Microsoft Entra hybrid joined. For example, some VPN clients create a per-machine VPN connection as part of the installation process. Validate the configuration using the following steps:

1. Verify that at least one per-machine VPN connection is created.

```
PowerShell  
  
Get-VpnConnection -AllUserConnection
```

2. Attempt to manually start the VPN connection.

```
Windows Command Prompt  
  
RASDIAL.EXE "ConnectionName"
```

3. Sign out of Windows. Verify that the **VPN connection** icon appears on the Windows sign-in page.

4. Move the device off the internal network and try to establish the connection using the icon on the Windows sign-in page. Sign into an account that doesn't have cached credentials.

For VPN configurations that automatically connect, the validation steps might be different.

Note

An always-on VPN can be used for this scenario. For more information, see [Deploy always-on VPN](#).

Next steps

- Deploy Microsoft Entra hybrid joined devices using Intune and Windows Autopilot.
- How to enroll with Autopilot.
- Try out Autopilot hybrid join over VPN in your Azure lab ↗.

Related content

- What is a device identity?.
- Learn more about cloud-native endpoints.
- Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints.
- Tutorial: Set up and configure a cloud-native Windows endpoint with Microsoft Intune.
- How to: Plan your Microsoft Entra join implementation.
- A framework for Windows endpoint management transformation ↗.
- Understanding hybrid Azure AD and co-management scenarios ↗.
- Success with remote Windows Autopilot and hybrid Azure Active Directory join ↗.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Windows Autopilot self-deploying mode

Article • 09/13/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

Note

For more information about using Windows Autopilot to deploy HoloLens 2 devices, see [Windows Autopilot for HoloLens 2](#).

Tip

For a guided walkthrough of Windows Autopilot self-deploying mode, see [Step by step tutorial for Windows Autopilot self-deploying mode in Intune](#).

Windows Autopilot self-deploying mode allows deployment of a device with little to no user interaction. For devices with an Ethernet connection, no user interaction is required. For devices connected via Wi-Fi, the user must only:

- Select the language, locale, and keyboard.
- Make a network connection.

Self-deploying mode provides all the following features:

- Joins the device to Microsoft Entra ID.
- Enrolls the device in Intune or another mobile device management (MDM) service using Microsoft Entra ID for automatic MDM enrollment.
- Makes sure that all policies, applications, certificates, and networking profiles are provisioned on the device.
- Uses the Enrollment Status Page to prevent access until the device is fully provisioned.

Note

Autopilot self-deploying mode is only supported for Microsoft Entra join devices. Autopilot self-deploying mode isn't supported for Microsoft Entra hybrid join devices.

Self-deploying mode allows deployment of a Windows device as a kiosk, digital signage device, or a shared device.

Autopilot now has a kiosk mode that supports Kiosk Browser, Microsoft Store apps, and specific versions of Microsoft Edge.

The [Kiosk Browser](#) can be used when setting up a kiosk device. This app is built on Microsoft Edge and can be used to create a tailored, MDM-managed browsing experience.

The device configuration can be automated by combining self-deploying mode with MDM policies. Use the MDM policies to create a local account configured to automatically sign in. For more information, see:

- [Simplifying kiosk management for IT with Windows 10](#).
- [Set up a kiosk or digital sign in Intune or other MDM service](#).

Optionally, a [device-only subscription](#) service can be used that helps manage devices that aren't affiliated with specific users. The Intune device SKU is licensed per device per month.

Note

Intune doesn't automatically configure a primary user when using self-deploying mode in Autopilot to provision a Windows device. Some Intune capabilities rely on a primary user being set on a device. These features include user self-service BitLocker recovery key retrieval and using the Company Portal to install software. Using self-provisioning mode for Autopilot doesn't preclude a licensed user from logging into the device and using features entitled to that user such as conditional access. For more information, see [Windows Autopilot scenarios and capabilities](#).

If desired, a primary user can be manually set after device provisioning via the Intune admin center. For more information, see [Change a devices primary user](#).

Requirements

Important

A device can't automatically re-enroll through Windows Autopilot after an initial deployment with self-deploying mode. Instead, delete the device record in the [Microsoft Intune admin center](#). From the Microsoft Intune admin center, select **Devices > All devices** > select the devices to delete > **Delete**. For more information, see [Updates to the Windows Autopilot sign-in and deployment experience](#).

Self-deploying mode uses a device's Trusted Platform Module (TPM) 2.0 hardware to authenticate the device into an organization's Microsoft Entra tenant. Therefore, devices without TPM 2.0 can't be used with this mode. Devices must also support TPM device attestation. All new Windows devices should meet these requirements. The TPM attestation process also requires access to a set of HTTPS URLs that are unique for each TPM provider. For more information, see the entry for Autopilot self-Deploying mode and Autopilot pre-provisioning in [Networking requirements](#). For Windows Autopilot software requirements, see [Windows Autopilot software requirements](#).

 **Important**

If a self-deploying mode deployment is attempted on a device that doesn't have support for TPM 2.0 or on a virtual machine, the process fails when verifying the device with an **0x800705B4** timeout error. This limitation includes Hyper-V virtual TPMs.

See [Windows Autopilot known issues](#) and [Troubleshooting Windows Autopilot device import and enrollment](#) to review other known errors and solutions.

An organization-specific logo and organization name can be displayed during the Autopilot process. To do so, Microsoft Entra Company Branding must be configured with the images and text that need to be displayed. See [Quickstart: Add company branding to your sign-in page in Microsoft Entra ID](#) for more details.

Step by step

To deploy in self-deploying mode Windows Autopilot, the following preparation steps need to be completed:

1. Create an Autopilot profile for self-deploying mode with the desired settings. In Microsoft Intune, this mode is explicitly chosen when creating the profile. It isn't possible to create a profile in the Microsoft Store for Business or Partner Center for self-deploying mode.
2. If using Intune, create a device group in Microsoft Entra ID and assign the Autopilot profile to that group. Ensure that the profile is assigned to the device before attempting to deploy that device.
3. Boot the device, connecting it to Wi-Fi if necessary, then wait for the provisioning process to complete.

Validation

When using Windows Autopilot to deploy in self-deploying mode, the following end-user experience should be observed:

- Once the device connects to a network, the Autopilot profile is downloaded.
- If connected to Ethernet, and the Autopilot profile is configured to skip them, the following pages aren't displayed:
 - Language and locale.
 - Keyboard layout.

Otherwise, manual steps are required:

- If multiple languages are preinstalled in Windows, the user must pick a language.
- The user must pick a locale and a keyboard layout, and optionally a second keyboard layout.
- If connected via Ethernet, no network prompt is expected. If no Ethernet connection is available and Wi-Fi is built in, the user needs to connect to a wireless network.
- Windows checks for critical out-of-box experience (OOBE) updates, and if any are available they're automatically installed, rebooting if necessary.
- The device joins Microsoft Entra ID.
- The device enrolls in Intune or other configured MDM services after it joins Microsoft Entra ID.
- The [enrollment status page](#) is displayed.
- Depending on the device settings deployed, the device will either:
 - Remain at the sign-on screen, where any member of the organization can sign in by specifying their Microsoft Entra credentials.
 - Automatically sign in as a local account, for devices configured as a kiosk or digital signage.

ⓘ Note

Deploying Exchange ActiveSync (EAS) policies using self-deploying mode for kiosk deployments causes autologon functionality to fail.

In case the observed results don't match these expectations, consult the [Troubleshooting Windows Autopilot overview](#) documentation.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot Reset

Article • 10/09/2024 • Applies to:  Windows 11,  Windows 10

Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically, Windows Autopilot Reset:

- Removes personal files, apps, and settings.
- Reapplies a device's original settings.
- Sets the region, language, and keyboard to the original values.
- Maintains the device's identity connection to Microsoft Entra ID.
- Maintains the device's management connection to Intune.

The Windows Autopilot Reset process automatically keeps information from the existing device:

- Wi-Fi connection details.
- Provisioning packages previously applied to the device.
- A provisioning package present on a USB drive when the reset process is started.
- Microsoft Entra device membership and mobile device management (MDM) enrollment information.
- Simple Certificate Enrollment Protocol (SCEP) certificates.

Windows Autopilot Reset blocks the user from accessing the desktop until this information is restored, including reapplying any provisioning packages. For devices enrolled in an MDM service, Windows Autopilot Reset also blocks until an MDM sync is completed.

Note

Autopilot Reset doesn't support Microsoft Entra hybrid joined devices. For Microsoft Entra hybrid joined devices, a full device wipe is required. When a hybrid device goes through a full device reset, it might take up to 24 hours for it to be ready to be deployed again. The request can be expedited by re-registering the device.

Scenarios

Windows Autopilot Reset supports two scenarios:

- [Local reset](#) started by IT personnel or other administrators from the organization.

- [Remote reset](#) started remotely by IT personnel via an MDM service such as Microsoft Intune.

Additional requirements and configuration details apply with each scenario.

Reset devices with local Windows Autopilot Reset

IT admins can use a local Windows Autopilot Reset to:

- Quickly remove personal files, apps, and settings.
- Reset Windows devices from the lock screen.
- Apply original settings and management enrollment (Microsoft Entra ID and device management).

The device is then ready to use. With a local Autopilot Reset, devices are returned to a fully configured or known IT-approved state.

To enable local Autopilot Reset in supported versions of Windows:

1. [Enable the policy for the feature.](#)
2. [Trigger a reset for each device.](#)

Enable local Windows Autopilot Reset

To enable a local Windows Autopilot Reset, the `DisableAutomaticReDeploymentCredentials` policy must be configured. This policy is documented in the [CredentialProviders](#), `CredentialProviders/DisableAutomaticReDeploymentCredentials` configuration service provider (CSP) policy. By default, local Windows Autopilot Reset is disabled. This default ensures that a local Autopilot Reset isn't triggered accidentally.

The policy can be set using one of these methods:

- MDM provider.
 - When Intune is used, a new device configuration profile can be created with the following settings:
 - **Platform = Windows 10 or later.**
 - **Profile type = Device restrictions.**
 - **Category = General.**
 - **Autopilot Reset = Allow.** Deploy this setting to all devices where a local reset should be permitted.

- If using an MDM provider other than Intune, check the MDM provider's documentation on how to set this policy.
- Windows Configuration Designer.

[Windows Configuration Designer](#) can be used to set the **Runtime settings > Policies > CredentialProviders > DisableAutomaticReDeploymentCredentials** setting to `0` and then create a provisioning package.

- Set up School PCs app.

The latest release of the [Set up School PCs](#) app supports enabling local Windows Autopilot Reset.

Trigger local Windows Autopilot Reset

A local Windows Autopilot Reset is a two-step process:

1. Trigger the Windows Autopilot Reset.
2. Authenticate.

Once these two steps are performed, the Windows Autopilot Reset executes. Once the Windows Autopilot Reset is done, the device is again ready for use.

To trigger a local Autopilot Reset:

On the device where the local Windows Autopilot reset is being performed:

1. If a provisioning package was created, plug in the USB drive that contains the provisioning package.
2. From the Windows device lock screen, enter the keystroke `CTRL + WIN + R`.

These keystrokes open up a custom sign-in screen for the local Autopilot Reset.

The screen serves two purposes:

- a. Confirm/verify that the end user has the right to trigger Local Autopilot Reset.
- b. Notify the user in case a provisioning package, created using Windows Configuration Designer, is being used as part of the process.

3. To trigger the local Autopilot Reset, sign into the device with an account that has local admin credentials.

Once the local Autopilot Reset is triggered, the reset process starts. Once provisioning is complete, the device is again ready for use.

Note

When local Autopilot Reset is used on a device, the device's primary user and the Microsoft Entra device owner aren't updated. Admins can update them manually after the Autopilot Reset completes.

Reset devices with remote Windows Autopilot Reset

An MDM service such as Microsoft Intune can be used to start the remote Windows Autopilot reset process. Resetting in this way avoids the need for IT staff to visit each machine to start the process.

To enable a device for a remote Windows Autopilot Reset, the device must be MDM managed and joined to Microsoft Entra ID. Additionally, for Intune, the Intune Service Administrator role is required for remote Windows Autopilot Reset. For more information, see [Add users and grant administrative permission to Intune](#).

Triggering a remote Windows Autopilot Reset

To trigger a remote Windows Autopilot Reset via Intune, follow these steps:

1. Navigate to **Devices** tab in the Intune admin center.
2. In the **All devices** view, select the targeted reset devices and then select **More** to view device actions.
3. Select **Autopilot Reset** to start the reset task.

Once the reset is complete, the device is again ready for use.

Note

When remote Autopilot Reset is used on a device, the device's primary user and the Microsoft Entra device owner is removed. The next user who signs in after the reset will be set as the primary user and Microsoft Entra device owner. Shared devices will remain shared after the Autopilot Reset.

Troubleshooting

Windows Autopilot Reset requires that the [Windows Recovery Environment \(WinRE\)](#) is correctly configured and enabled on the device. Before the Windows Autopilot Reset is started, it checks if WinRE is configured and enabled. If WinRE isn't configured and enabled, then the Windows Autopilot reset fails immediately on the device and an error such as `Error code: ERROR_NOT_SUPPORTED (0x80070032)` is reported in the logs.

To make sure WinRE is enabled, use the [REAgentC.exe](#) tool to run the following command:

```
Windows Command Prompt
```

```
reagentc.exe /enable
```

If Windows Autopilot Reset fails after enabling WinRE, or WinRE can't be enabled, contact [Microsoft Support](#) for assistance.

Feedback

Was this page helpful?

 Yes

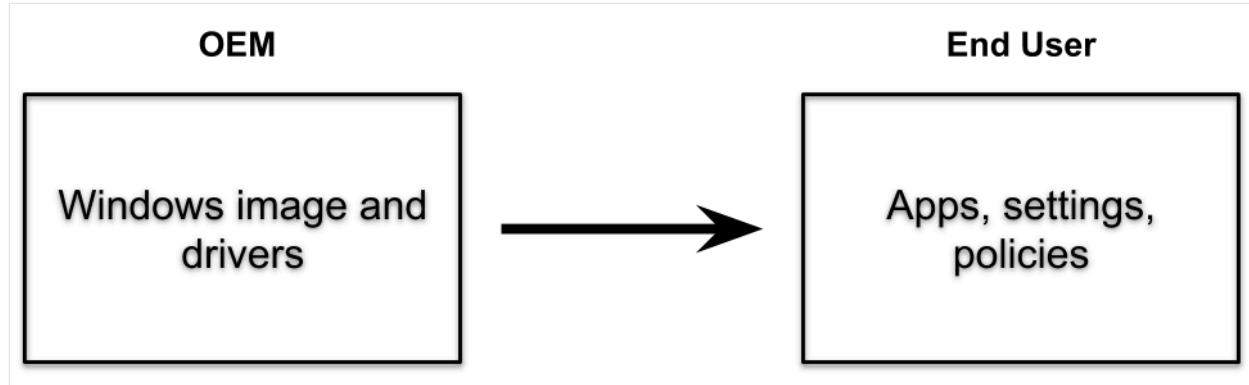
 No

[Provide product feedback](#)

Windows Autopilot for pre-provisioned deployment

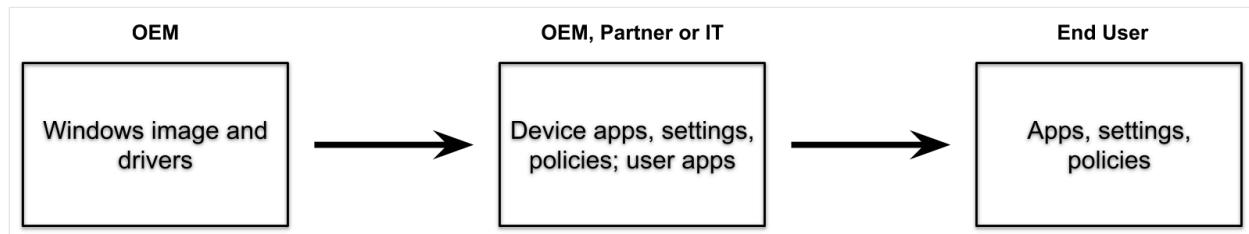
Article • 09/13/2024 • Applies to: ✓ Windows 11, ✓ Windows 10

Windows Autopilot helps organizations easily provision new devices by using the preinstalled OEM image and drivers. This functionality lets end users get their devices business-ready by using a simple process.



Windows Autopilot can also provide a *pre-provisioning* service that helps partners or IT staff pre-provision a fully configured and business-ready Windows PC. From the end user's perspective, the Windows Autopilot user-driven experience is unchanged, but getting their device to a fully provisioned state is faster.

With **Windows Autopilot for pre-provisioned deployment**, the provisioning process is split. The time-consuming portions are done by IT, partners, or OEMs. The end user simply completes a few necessary settings and policies and then they can begin using their device.



Pre-provisioned deployments use Microsoft Intune in currently supported versions of Windows. Such deployments build on existing Windows Autopilot [user-driven scenarios](#) and support user-driven mode scenarios for both Microsoft Entra joined and Microsoft Entra hybrid joined devices.

Requirements

(i) Important

A device can't automatically re-enroll through Windows Autopilot after an initial deployment with pre-provisioning mode. Instead, delete the device record in the [Microsoft Intune admin center](#). From the Microsoft Intune admin center, select **Devices > All devices** > select the devices to delete > **Delete**. For more information, see [Updates to the Windows Autopilot sign-in and deployment experience](#).

In addition to [Windows Autopilot requirements](#), Windows Autopilot for pre-provisioned deployment also requires:

- A currently supported version of Windows.
- Windows Pro, Enterprise, or Education editions.
- An Intune subscription.
- Physical devices that support Trusted Platform Module (TPM) 2.0 and device attestation. Virtual machines aren't supported. The pre-provisioning process uses Windows Autopilot self-deploying capabilities, so TPM 2.0 is required. The TPM attestation process also requires access to a set of HTTPS URLs that are unique for each TPM provider. For more information, see the entry for Autopilot self-Deploying mode and Autopilot pre-provisioning in [Networking requirements](#).
- Network connectivity. Using wireless connectivity requires selecting region, language and keyboard before being able to connect and start provisioning.
- An enrollment status page (ESP) profile must be targeted to the device.

(i) Important

- Because the OEM or vendor performs the pre-provisioning process, this process **doesn't require access to an end-user's on-prem domain infrastructure**. The pre-provisioning process is unlike a typical Microsoft Entra hybrid joined scenario because rebooting the device is postponed. The device is resealed before the time when connectivity to a domain controller is expected. Instead the domain network is contacted when the device is unboxed on-premises by the end-user.
- See [Windows Autopilot known issues](#) and [Troubleshooting Windows Autopilot device import and enrollment](#) to review known issues and their solutions.

Preparation

Devices slated for pre-provisioning are registered for Autopilot via the normal registration process.

To be ready to try out Windows Autopilot for pre-provisioned deployment, make sure that existing Windows Autopilot user-driven scenarios can be successfully used:

- User-driven Microsoft Entra join. Make sure that devices can be deployed using Windows Autopilot and join them to a Microsoft Entra ID tenant.
- User-driven with Microsoft Entra hybrid join. To enable the features of Microsoft Entra hybrid join, make sure that the following actions can be performed:
 - Deploy devices using Windows Autopilot.
 - Join the devices to an on-premises Active Directory domain.
 - Register the devices with Microsoft Entra ID.

Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. For more information, see [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization](#).

If these scenarios can't be completed, Windows Autopilot for pre-provisioned deployment also doesn't succeed since it builds on top of these scenarios.

Before the pre-provisioning process can be started in the provisioning service facility, another Autopilot profile setting must be configured. A detailed tutorial on how to configure an Autopilot profile for pre-provisioning is available in the following articles:

- [Step by step tutorial for Windows Autopilot for pre-provisioned deployment Microsoft Entra join in Intune](#)
- [Step by step tutorial for Windows Autopilot for pre-provisioned deployment Microsoft Entra hybrid join in Intune](#)

The pre-provisioning process applies all device-targeted policies from Intune. Those policies include certificates, security templates, settings, apps, and more - anything targeting the device. Additionally, any Win32 or line-of-business (LOB) apps are installed if they meet the following conditions:

- Configured to install in the device context.

- Assigned to either the device or to the user preassigned to the Autopilot device.

Important

Make sure not to target both Win32 and LOB apps to the same device. If both Win32 and LOB apps need to be targeted to the device, consider using [Windows Autopilot device preparation](#). For more information, see [Add a Windows line-of-business app to Microsoft Intune](#).

Note

To ensure easy access into pre-provisioning mode, select the language mode as user specified in Autopilot profiles. The pre-provisioning technician phase installs all device-targeted apps and any user-targeted, device-context apps that are targeted to the assigned user. If there's no assigned user, then it only installs the device-targeted apps. Other user-targeted policies aren't applied until the user signs into the device. To verify these behaviors, be sure to create appropriate apps and policies targeted to devices and users.

Scenarios

Windows Autopilot for pre-provisioned deployment supports two distinct scenarios:

- User-driven deployments with Microsoft Entra join. The device is joined to a Microsoft Entra tenant.
- User-driven deployments with Microsoft Entra hybrid join. The device is joined to an on-premises Active Directory domain, and separately registered with Microsoft Entra ID.

Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. For more information, see [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization](#).

Each of these scenarios consists of two parts, a technician flow and a user flow. At a high level, these parts are the same for Microsoft Entra join and Microsoft Entra hybrid join.

The differences are primarily seen by the end user in the authentication steps.

Technician flow

After the customer or IT Admin targets all the apps and settings they want for their devices through Intune, the pre-provisioning technician can begin the pre-provisioning process. The technician could be a member of the IT staff, a services partner, or an OEM - each organization can decide who should perform these activities. Regardless of the scenario, the process done by the technician is the same:

- Boot the device.
- From the first out-of-box experience (OOBE) screen (which could be a language selection, locale selection screen, or the Microsoft Entra sign-in page), don't select **Next**. Instead, press the Windows key five times to view another options dialog. From that screen, select the **Windows Autopilot provisioning** option and then select **Continue**.
- On the **Windows Autopilot Configuration** screen, it displays the following information about the device:
 - The Autopilot profile assigned to the device.
 - The organization name for the device.
 - The user assigned to the device (if there's one).
 - A QR code containing a unique identifier for the device. This code can be used to look up the device in Intune, which might be needed to make configuration changes. For example, assign a user or add the device to groups needed for app or policy targeting.

① Note

The QR codes can be scanned using a companion app. The app also configures the device to specify who it belongs to. The Autopilot team created an open-source sample of a companion app that integrates with Intune by using the Graph API. It's available on [GitHub](#).

- Validate the information displayed. If any changes are needed, make the changes, and then select **Refresh** to redownload the updated Autopilot profile details.
- Select **Provision** to begin the provisioning process.

If the pre-provisioning process completes successfully:

- A success status screen appears with information about the device, including the same details presented previously. For example, Autopilot profile, organization name, assigned user, and QR code. The elapsed time for the pre-provisioning steps is also provided.
- Select **Reseal** to shut down the device. At that point, the device can be shipped to the end user.

Note

Technician flow inherits behavior from [self-deploying mode](#). Self-Deploying Mode uses the Enrollment Status Page to hold the device in a provisioning state. The device being in a provisioning state prevents the user from proceeding to the desktop after enrollment but before software and configuration are done applying. As such, if Enrollment Status Page is disabled, the reseal button can appear before software and configuration is done applying. This behavior can allow proceeding to the user flow before the technician flow provisioning is complete. The success screen validates that enrollment was successful, not that the technician flow is necessarily complete.

If the pre-provisioning process fails:

- An error status screen appears with information about the device, including the same details presented previously. For example, Autopilot profile, organization name, assigned user, and QR code. The elapsed time for the pre-provisioning steps is also provided.
- Diagnostic logs can be gathered from the device, and then it can be reset to start the process over again.

User flow

Important

- In order to make sure tokens are refreshed properly between the Technician flow and the User flow, wait at least 90 minutes after running the Technician flow before running the User flow. This scenario mainly affects lab and testing scenarios when the User flow is run within 90 minutes after the Technician flow completes.

- The User flow should be run within six months after the Technician flow finishes. Waiting more than six months can cause the certificates used by the Intune Management Engine (IME) to no longer be valid leading to errors such as:

```
Error code: [Win32App][DetectionActionHandler] Detection for policy with id: <policy_id> resulted in action status: Failed and detection state: NotComputed.
```

- Compliance in Microsoft Entra ID is reset during the User flow. Devices might show as compliant in Microsoft Entra ID after the Technician flow completes, but then show as noncompliant once the User flow starts. Allow enough time after the User flow completes for compliance to reevaluate and update.

If the pre-provisioning process completed successfully and the device was resealed, deliver the device to the end user. The end user completes the normal Windows Autopilot user-driven process following these steps:

- Power on the device.
- Select the appropriate language, locale, and keyboard layout.
- Connect to a network (if using Wi-Fi). Internet access is always required. If using Microsoft Entra hybrid join, there must also be connectivity to a domain controller.
- If using Microsoft Entra join, on the branded sign-on screen, enter the user's Microsoft Entra credentials.
- If using Microsoft Entra hybrid join, the device will reboot; after the reboot, enter the user's Active Directory credentials.

① Note

In certain circumstances, Microsoft Entra credentials might also be prompted for during a Microsoft Entra hybrid join scenario. For example, if ADFS isn't being used.

- More policies and apps are delivered to the device, as tracked by the Enrollment Status Page (ESP). Once complete, the user can access the desktop.

The device ESP reruns during the user flow so that both device and user ESP run when the user logs in. This behavior allows the ESP to install other policies that are assigned to

the device after the device completes the technician phase.

Note

If the Microsoft Account Sign-In Assistant (wlidsvc) is disabled during the Technician Flow, the Microsoft Entra sign-in option might not show. Instead, users are asked to accept the EULA, and create a local account, which might not be the desired behavior.

Deploying a device

For more information on starting a deployment on a device when using Windows Autopilot for pre-provisioned, see the Technician flow and User flow steps of the Windows Autopilot for pre-provisioned deployment tutorials:

- Microsoft Entra join:
 - Technician flow.
 - User flow.
- Microsoft Entra hybrid:
 - Technician flow.
 - User flow.

Related content

- Pre-provisioning video .
- What is a device identity?.
- Learn more about cloud-native endpoints.
- Tutorial: Set up and configure a cloud-native Windows endpoint with Microsoft Intune.
- How to: Plan your Microsoft Entra join implementation.
- A framework for Windows endpoint management transformation .
- Understanding hybrid Azure AD and co-management scenarios .
- Success with remote Windows Autopilot and hybrid Azure Active Directory join .

Feedback

Was this page helpful?



Provide product feedback ↗

Windows Autopilot deployment for existing devices

Article • 09/13/2024 • Applies to:  Windows 11,  Windows 10

Modern desktop deployment with Windows Autopilot helps easily deploy the latest version of Windows to existing devices. Apps used by the organization can be automatically installed. If Windows user data is managed with OneDrive for work or school, data is synchronized, so users can resume working right away.

Windows Autopilot for existing devices allows reimaging and provisioning a Windows device for Autopilot user-driven mode using a single, native Configuration Manager task sequence. The existing device can be on-premises domain-joined. The end result is a Windows device joined to either Microsoft Entra ID or Active Directory (Microsoft Entra hybrid join).

Note

The JSON file for Windows Autopilot for existing devices only supports user-driven Microsoft Entra ID and user-driven hybrid Microsoft Entra Autopilot profiles. Self-deploying and pre-provisioning Autopilot profiles aren't supported with JSON files due to these scenarios requiring TPM attestation.

However, during the Windows Autopilot for existing devices deployment, if the following conditions are true:

- Device is already a Windows Autopilot device before the deployment begins
- Device has an Autopilot profile assigned to it

then the assigned Autopilot profile takes precedence over the JSON file installed by the task sequence. In this scenario, if the assigned Autopilot profile is either a self-deploying or pre-provisioning Autopilot profile, then the self-deploying and pre-provisioning scenarios are supported.

Tip

Using Autopilot for existing devices could be used as a method to convert existing hybrid Microsoft Entra devices into Microsoft Entra devices. Using the setting **Convert all targeted devices to Autopilot** in the Autopilot profile doesn't automatically convert existing hybrid Microsoft Entra device in the assigned groups into a Microsoft Entra device. The setting only registers the devices in the assigned groups for the Autopilot service.

Requirements

- A currently supported version of Microsoft Configuration Manager current branch.
- Assigned Microsoft Intune licenses.
- Microsoft Entra ID P1 or P2.
- A supported version of Windows imported into Configuration Manager as an [OS image](#).
- The [Windows Management Framework](#) is required for Windows Server 2012/2012 R2 when running the PowerShell commands and scripts that [installs the required modules](#).
- Enrollment restrictions aren't configured to block personal devices. For more information, see [What are enrollment restrictions?: Blocking personal Windows devices](#).

Configure the Enrollment Status Page (optional)

If desired, an [enrollment status page](#) (ESP) for Autopilot can be set up using Intune.

1. Open the [Microsoft Intune admin center](#).
2. Go to **Devices > Device onboarding | Enrollment**. Make sure **Windows** is selected at the top and then under **Windows Autopilot**, select **Enrollment Status Page** and [Set up the Enrollment Status Page](#).
3. Go to **Microsoft Entra ID > Manage | Mobility (MDM and WIP) > Microsoft Intune** and [enable Windows automatic enrollment](#). Configure the MDM user scope for some or all users.

Install required modules

Note

The PowerShell code snippets in this section were updated in July of 2023 to use the Microsoft Graph PowerShell modules instead of the deprecated AzureAD Graph PowerShell modules. The Microsoft Graph PowerShell modules might require approval of additional permissions in Microsoft Entra ID when they're first used. It was also updated to force using an updated version of the WindowsAutoPilot module. For more information, see [AzureAD](#) and [Important: Azure AD Graph Retirement and PowerShell Module Deprecation](#).

1. On an internet-connected Windows PC or server, open an elevated Windows PowerShell command window.
2. Enter the following commands to install and import the necessary modules:

```
PowerShell

Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Install-Module -Name WindowsAutopilotIntune -MinimumVersion 5.4.0 -Force
Install-Module -Name Microsoft.Graph.Groups -Force
Install-Module -Name Microsoft.Graph.Authentication -Force
Install-Module -Name Microsoft.Graph.Identity.DirectoryManagement -Force

Import-Module -Name WindowsAutopilotIntune -MinimumVersion 5.4
Import-Module -Name Microsoft.Graph.Groups
Import-Module -Name Microsoft.Graph.Authentication
Import-Module -Name Microsoft.Graph.Identity.DirectoryManagement
```

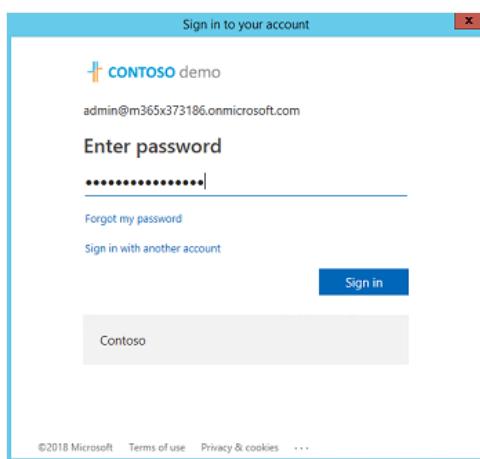
3. Enter the following commands and provide Intune administrative credentials:

Make sure the specified user account has sufficient administrative rights.

```
PowerShell

Connect-MgGraph -Scopes "Device.ReadWrite.All", "DeviceManagementManagedDevices.ReadWrite.All",
"DeviceManagementServiceConfig.ReadWrite.All", "Domain.ReadWrite.All", "Group.ReadWrite.All",
"GroupMember.ReadWrite.All", "User.Read"
```

Windows requests the username and password for the account with a standard Microsoft Entra ID form. Type the username and password, and then select **Sign in**.



The first time Intune Graph APIs are used on a device, it prompts to enable Microsoft Intune PowerShell read and write permissions. To enable these permissions, select **Consent on behalf of your organization** and then **Accept**.

Get Autopilot profiles for existing devices

Get all the Autopilot profiles available in the Intune tenant, and display them in JSON format:

```
PowerShell
```

Get-AutopilotProfile | ConvertTo-AutopilotConfigurationJSON

See the following sample output:

PowerShell

```
PS C:\> Get-AutopilotProfile | ConvertTo-AutopilotConfigurationJSON
{
    "CloudAssignedTenantId": "1537de22-988c-4e93-b8a5-83890f34a69b",
    "CloudAssignedForcedEnrollment": 1,
    "Version": 2049,
    "Comment_File": "Profile Autopilot Profile",
    "CloudAssignedAadServerData": "{\"ZeroTouchConfig\": {
        \"CloudAssignedTenantUpn\":\"\\\", \"CloudAssignedTenantDomain\":\"M365x373186.onmicrosoft.com\"}
    }",
    "CloudAssignedTenantDomain": "M365x373186.onmicrosoft.com",
    "CloudAssignedDomainJoinMethod": 0,
    "CloudAssignedOobeConfig": 28,
    "ZtdCorrelationId": "7F9E6025-1E13-45F3-BF82-A3E8C5B59EAC"
}
```

Each profile is encapsulated within braces ({ }). The previous example displays a single profile.

JSON file properties

[Expand table](#)

Property	Type	Required	Description
Version	Number	Optional	The version number that identifies the format of the JSON file.
CloudAssignedTenantId	GUID	Required	The Microsoft Entra tenant ID that should be used. This property is the GUID for the tenant, and can be found in properties of the tenant. The value shouldn't include braces.
CloudAssignedTenantDomain	String	Required	The Microsoft Entra tenant name that should be used. For example: <code>tenant.onmicrosoft.com</code> .
CloudAssignedOobeConfig	Number	Required	This property is a bitmap that shows which Autopilot settings were configured. <ul style="list-style-type: none">• 1: SkipCortanaOptIn• 2: OobeUserNotLocalAdmin• 4: SkipExpressSettings• 8: SkipOemRegistration• 16: SkipEula
CloudAssignedDomainJoinMethod	Number	Required	This property specifies whether the device should join Microsoft Entra ID or Active Directory (Microsoft Entra hybrid join). <ul style="list-style-type: none">• 0: Microsoft Entra joined• 1: Microsoft Entra hybrid joined
CloudAssignedForcedEnrollment	Number	Required	Specifies that the device should require Microsoft Entra join and MDM enrollment. <ul style="list-style-type: none">• 0: Not required• 1: required
ZtdCorrelationId	GUID	Required	A unique GUID (without braces) provided to Intune as part of the registration process. This ID is included in the enrollment message as the <code>OfflineAutopilotEnrollmentCorrelator</code> . This attribute is present only if enrollment happens on a device registered with Zero Touch Provisioning via offline registration.
CloudAssignedAadServerData	Encoded JSON string	Required	An embedded JSON string used for branding. It requires enabling Microsoft Entra organization branding. For example: <code>"CloudAssignedAadServerData": "{\"ZeroTouchConfig\": {\"CloudAssignedTenantUpn\":\"\\\", \"CloudAssignedTenantDomain\":\"tenant.onmicrosoft.com\"}}"</code>

Property	Type	Required	Description
CloudAssignedDeviceName	String	Optional	The name automatically assigned to the computer. This name follows the naming pattern convention configured in the Intune Autopilot profile. An explicit name can also be specified.

Create the JSON file

Save the Autopilot profile as a JSON file in ASCII or ANSI format. Windows PowerShell defaults to Unicode format. If redirecting output of the commands to a file, also specify the file format. The following PowerShell example saves the file in ASCII format. The Autopilot profiles appear in a subfolder under the folder specified by the `$targetDirectory` variable. By default, the `$targetDirectory` variable is `C:\AutoPilot`, but it can be changed to another location if desired. The subfolder has the name of the Autopilot profile from Intune. If there are multiple Autopilot profiles, each profile has its own subfolder. In each folder, there's a JSON file named

`AutopilotConfigurationFile.json`

```
PowerShell

Connect-MgGraph -Scopes "Device.ReadWrite.All", "DeviceManagementManagedDevices.ReadWrite.All",
"DeviceManagementServiceConfig.ReadWrite.All", "Domain.ReadWrite.All", "Group.ReadWrite.All",
"GroupMember.ReadWrite.All", "User.Read"
$AutopilotProfile = Get-AutopilotProfile
$targetDirectory = "C:\AutoPilot"
$AutopilotProfile | ForEach-Object {
    New-Item -ItemType Directory -Path "$targetDirectory\$($_.displayName)"
    $_ | ConvertTo-AutopilotConfigurationJSON | Set-Content -Encoding Ascii
"$targetDirectory\$($_.displayName)\AutopilotConfigurationFile.json"
}
```

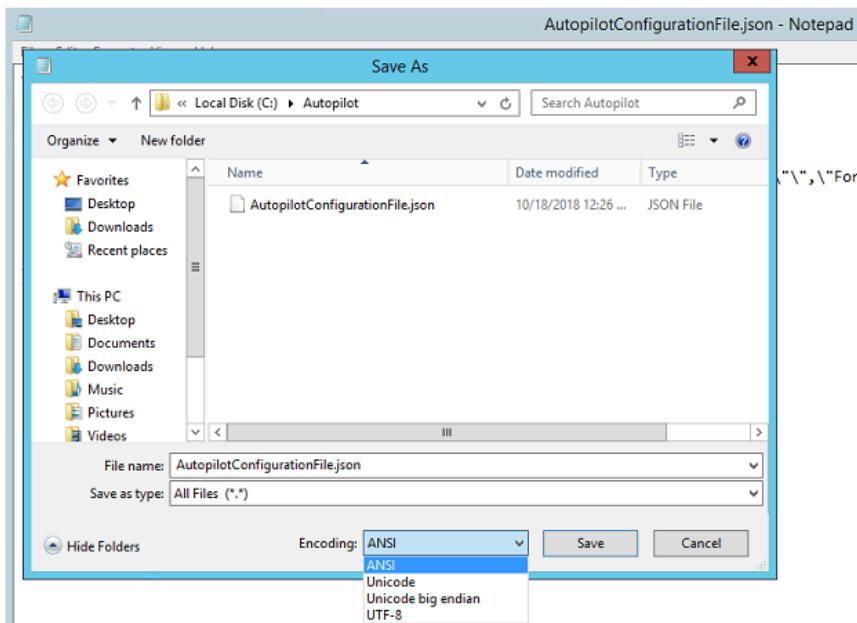
Tip

When the PowerShell cmdlet `Out-File` is used to redirect the JSON output to a file, it uses Unicode encoding by default. This cmdlet might also truncate long lines. Use the `Set-Content` cmdlet with the `-Encoding ASCII` parameter to set the proper text encoding.

Important

The file name has to be `AutopilotConfigurationFile.json` and encoded as ASCII or ANSI.

The profile can also be saved to a text file and edit in Notepad. In Notepad, when choosing **Save as**, select the save as type: **All Files**, and then select **ANSI** for the **Encoding**.



After saving the file, move it to a location for a Microsoft Configuration Manager package source.

Important

The configuration file can only contain one profile. Multiple JSON profile files can be used, but each one must be named `AutopilotConfigurationFile.json`. This requirement is for OOBE to follow the Autopilot experience. To use more than one Autopilot profile, create separate Configuration Manager packages.

Windows OOBE doesn't follow the Autopilot experience if the file is saved with one of the following criteria:

- Unicode encoding.
- UTF-8 encoding.
- A file name other than `AutopilotConfigurationFile.json`.

Create a package containing the JSON file

1. In the Configuration Manager console, go to the **Software Library** workspace, expand **Application Management**, and select the **Packages** node.
2. On the ribbon, select **Create Package**.
3. In the Create Package and Program Wizard, enter the following details for the package:

- **Name:** Autopilot for existing devices config
- **Select This package contains source files**
- **Source folder:** Specify the UNC network path that contains the `AutopilotConfigurationFile.json` file

For more information, see [Packages and programs in Configuration Manager](#).

4. For the program, select the **Program Type:** **Don't create a program**
5. Complete the wizard.

Note

If the user-driven Autopilot profile settings in Intune are changed at a later date, make sure to recreate and update the JSON file. After updating the JSON file, redistribute the associated Configuration Manager package.

Create a target collection

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace, and select the **Device Collections** node.
2. On the ribbon, select **Create**, and then select **Create Device Collection**. An existing collection can also be used. If using an existing collection, proceed to the [Create a task sequence](#) section.
3. In the Create Device Collection Wizard, enter the following **General** details:
 - **Name:** Autopilot for existing devices collection
 - **Comment:** Add an optional comment to further describe the collection
 - **Limiting collection:** All Systems or if desired, an alternate collection.

4. On the **Membership Rules** page, select **Add Rule**. Specify either a direct or query-based collection rule to add the target Windows devices to the new collection.

For example, if the hostname of the computer to be wiped and reloaded is `PC-01`, and **Name** is being used as the attribute:

- a. Select **Add Rule**, select **Direct Rule** to open the Create Direct Membership Rule Wizard, and select **Next** on the Welcome page.
 - b. On the **Search for Resources** page, enter **PC-01** as the **Value**.
 - c. Select **Next**, and select **PC-01** in the **Resources**.
5. Complete the wizard with the default settings.

For more information, see [How to create collections in Configuration Manager](#).

Create a task sequence

1. In the Configuration Manager console, go to the **Software Library** workspace, expand **Operating Systems** and select the **Task Sequences** node.
2. In the **Home** ribbon, select **Create Task Sequence**.
3. In the **Create new task sequence** page, select the option to **Deploy Windows Autopilot for existing devices**.
4. In the **Task sequence information** page, specify the following information:
 - A name for the task sequence. For example, **Autopilot for existing devices**.
 - Optionally add a description to better describe the task sequence.
 - Select a boot image. For more information on supported boot image versions, see [Support for the Windows ADK in Configuration Manager](#).
5. In the **Install Windows** page, select the **Windows Image package**. Then configure the following settings:
 - **Image index**: Select either Enterprise, Education, or Professional, as required by the organization.
 - Enable the option to **Partition and format the target computer before installing the operating system**.
 - **Configure task sequence for use with Bitlocker**: If this option is enabled, the task sequence includes the steps necessary to enable BitLocker.
 - **Product key**: If a product key needs to be specified for Windows activation, enter it here.
 - Select one of the following options to configure the local administrator account in Windows:
 - **Randomly generate the local administrator password and disable the account on all support platforms (recommended)**
 - **Enable the account and specify the local administrator password**
6. In the **Install the Configuration Manager client** page, add any necessary Configuration Manager client installation properties for the environment. For example, since the device is a Workgroup device and not domain joined during the Windows Autopilot for existing devices task sequence, the **SMSMP** or **SMSMPLIST** parameters might be needed to run certain tasks such as the **Install Application** or **Install Software Updates** tasks.
7. The **Include updates** page selects by default the option to **Do not install any software updates**.
8. In the **Install applications** page, applications to install during the task sequence can be selected. However, Microsoft recommends that to mirror the signature image approach with this scenario. After the device provisions with Autopilot, apply all applications and configurations from Microsoft Intune or Configuration Manager co-management. This process provides a consistent experience between users receiving new devices and those using Windows Autopilot for existing devices.
9. In the **System Preparation** page, select the package that includes the Autopilot configuration file. By default, the task sequence restarts the computer after it runs Windows Sysprep. The option to **Shutdown computer after this task sequence completes** can also be selected. This option allows preparation of a device and then delivery to a user for a consistent Autopilot experience.
10. Complete the wizard.

The Windows Autopilot for existing devices task sequence results in a device joined to Microsoft Entra ID.

Note

For Windows Autopilot for existing devices task sequence, the **Create Task Sequence Wizard** purposely skips configuring and adding the **Apply Network Settings** task. If the **Apply Network Settings** task isn't specified in a task sequence, it uses Windows default behavior, which is to join a workgroup.

The Windows Autopilot for existing devices task sequence runs the **Prepare Windows for capture** step, which uses the Windows System Preparation Tool (Sysprep). If the device is joined to a domain, Sysprep fails, so therefore the Windows Autopilot for existing devices task sequence joins a workgroup. For this reason, it isn't necessary to add the **Apply Network Settings** task to a Windows Autopilot for existing devices task sequence.

For more information on creating the task sequence, including information on other wizard options, see [Create a task sequence to install an OS](#).

If the task sequence is viewed, it's similar to the default task sequence to apply an existing OS image. This task sequence includes the following extra steps:

- **Apply Windows Autopilot configuration:** This step applies the Autopilot configuration file from the specified package. It's not a new type of step, it's a **Run Command Line** step to copy the file.
- **Prepare Windows for Capture:** This step runs Windows Sysprep, and has the setting to **Shutdown the computer after running this action**. For more information, see [Prepare Windows for Capture](#).

For more information on editing the task sequence, see [Use the task sequence editor](#) and [Task sequence steps](#).

 **Note**

The **Prepare Windows for Capture** step deletes the `AutopilotConfigurationFile.json` file. For more information and a workaround, see [Modify the task sequence to account for Sysprep command line configuration](#) and [Windows Autopilot - known issues: Windows Autopilot for existing devices doesn't work](#).

To make sure the user's data is backed up before the Windows upgrade, use OneDrive for work or school [known folder move](#).

Distribute content to distribution points

Next distribute all content required for the task sequence to distribution points.

1. Select the **Autopilot for existing devices** task sequence, and in the ribbon select **Distribute Content**.
2. On the **Specify the content destination** page, select **Add** to specify either a **Distribution Point** or **Distribution Point Group**.
3. Specify content destinations that let the devices get the content.
4. After specifying content distribution, complete the wizard.

For more information, see [Manage task sequences to automate tasks](#).

Deploy the Autopilot task sequence

1. Select the **Autopilot for existing devices** task sequence, and in the ribbon select **Deploy**.

2. In the Deploy Software Wizard, specify the following details:

- **General**
 - *Task Sequence:* **Autopilot for existing devices**
 - *Collection:* **Autopilot for existing devices collection**
- **Deployment Settings**
 - *Action:* **Install**.
 - *Purpose:* **Available**.
 - *Make available to the following:* **Only Configuration Manager Clients**.

 **Note**

Select the option here that is relevant for the context of testing. If the target client doesn't have the Configuration Manager agent or Windows installed, the task sequence needs to be started via PXE or Boot Media.

- **Scheduling**
 - Set a time for when this deployment becomes available
- **User Experience**
 - Select **Show Task Sequence progress**

- Distribution Points
 - Deployment options: Download content locally when needed by the running task sequence

3. Complete the wizard.

Complete the deployment process

1. On the target Windows device, go to the **Start** menu, enter **Software Center**, and open it.
2. In the Software Library, under **Operating Systems**, select **Autopilot for existing devices**, and then select **Install**.

The task sequence runs and does the following actions:

1. Downloads content.
2. Restarts the device into WinPE.
3. Formats the drive.
4. Installs Windows from the specified OS image.
5. Prepares for Autopilot.
6. After the task sequence completes, the device boots into OOBE for the Autopilot experience:

 Note

If devices need to be joined to Active Directory as part of a Microsoft Entra hybrid join scenario, don't do so through the task sequence and the **Apply Network Settings Task**. Instead, create a **Domain Join** device configuration profile. Since there's no Microsoft Entra device object for the computer to do group-based targeting, target the profile to **All Devices**. For more information, see [User-driven mode for Microsoft Entra hybrid join](#).

Register the device for Windows Autopilot

Devices provisioned with Autopilot only receive the guided OOBE Autopilot experience on first boot.

After Windows is updated on an existing device, make sure to register the device so it has the Autopilot experience when the PC resets. Automatic registration can be enabled for a device by using the **Convert all targeted devices to Autopilot** setting in the Autopilot profile that is assigned to a group that the device is a member of. For more information, see [Create an Autopilot deployment profile](#).

Also see [Adding devices to Windows Autopilot](#).

 Note

- Typically, the target device isn't registered with the Windows Autopilot service. If the device is already registered, the assigned profile takes precedence. The Autopilot for existing devices profile only applies if the online profile times out.
- When the assigned profile is applied, the **enrollmentProfileName** property of the device object in Microsoft Intune and Microsoft Entra ID match the Windows Autopilot profile name.
- When the Windows Autopilot for existing devices profile is applied, the **enrollmentProfileName** property of the device object in Microsoft Intune and Microsoft Entra ID are **OfflineAutoPilotProfile-<ZtdCorrelationId>**.

How to speed up the deployment process

To speed up the deployment process, see [Windows Autopilot deployment for existing devices: Speed up the deployment process](#) section of the [Autopilot Tutorial](#).

Tutorial

For a detailed tutorial on configuring Windows Autopilot for existing devices, see the following article:

[Step by step tutorial for Windows Autopilot deployment for existing devices in Intune and Configuration Manager](#)

Related content

- [New Windows Autopilot capabilities and expanded partner support simplify modern device deployment ↗](#).

Feedback

Was this page helpful? [!\[\]\(8fd41f21be8d48dd6683445409d74a3e_img.jpg\) Yes](#) [!\[\]\(e00be9217bfd04eb04081fdd0230ec03_img.jpg\) No](#)

[Provide product feedback ↗](#)

Manually register devices with Windows Autopilot

Article • 02/21/2025 • Applies to: Windows 11, Windows 10, Windows Holographic

Within an organization, Windows Autopilot device registration required the following actions:

1. Manually collecting the hardware identity of devices, known as hardware hashes.
2. Uploading the hardware hash information in a comma-separated-values (CSV) file.

Capturing the hardware hash for manual registration requires booting the device into Windows. For this reason, this process is primarily for testing and evaluation scenarios.

Up to 500 devices can be manually registered via a CSV file uploaded through the portal. Before proceeding with additional devices, check that the previous CSV file batch is successfully registered. If transferring devices hashes from one tenant to another tenant, see [Support tip: How to transfer Windows Autopilot devices between tenants](#) for additional guidance.

Device owners can only register their devices with a hardware hash. Other methods (PKID, tuple) are available through OEMs or CSP partners.

This article provides step-by-step guidance for manual registration. For more information about registration, see:

- [Windows Autopilot registration overview](#).
- [Manual registration overview](#).
- [Windows Autopilot for HoloLens 2](#).

Requirements

- [Intune subscription](#).
- [Windows automatic enrollment enabled](#).
- [Microsoft Entra ID P1 or P2 subscription](#).

Required permissions

Device enrollment requires *Intune Administrator* or *Policy and Profile Manager* permissions. A custom Autopilot device manager role can also be created by using [role-based access control \(RBAC\)](#). Autopilot device management requires only that all

permissions under **Enrollment programs** are enabled, except for the four token management options.

① Note

In both Intune Administrator and role-based access control methods, the administrative user also requires consent to use the Microsoft Intune PowerShell and Microsoft Graph PowerShell enterprise applications.

Collect the hardware hash

The following methods are available to harvest a hardware hash from existing devices:

- Using [Microsoft Configuration Manager](#).
- Using [Windows PowerShell](#).
- During the out-of-box experience (OOBE) by using the [Diagnostics Page](#) (Windows 11 only).
- Directly on the device using the [Access work or school](#) pane in the [Settings app](#).

For a description of each method, select the link for the method.

① Note

If OOBE is restarted too many times, it can enter a recovery mode and fail to run the Autopilot configuration. This scenario can be identified if OOBE displays multiple configuration options on the same page, including language, region, and keyboard layout. The normal OOBE process displays each of these configuration options on a separate page. The following registry key value tracks the count of OOBE retries:

`HKCU\Software\Microsoft\Windows\CurrentVersion\UserOOBE`

To ensure that OOBE hasn't restarted too many times, change this registry key value to `1`.

Configuration Manager

Microsoft Configuration Manager automatically collects the hardware hashes for existing Windows devices. For more information, see [Gather information from Configuration Manager for Windows Autopilot](#). The hash information can be extracted from Configuration Manager into a CSV file.

PowerShell

The hardware hash for an existing device is available through Windows Management Instrumentation (WMI). The PowerShell script [Get-WindowsAutopilotInfo.ps1](#) can be used to get a device's hardware hash and serial number. The serial number is useful for quickly seeing which device the hardware hash belongs to.

To use the `Get-WindowsAutopilotInfo.ps1` script, it needs to be downloaded and then run on a device using either of the following methods:

- [Save the hardware hash locally on a devices as a CSV file](#) - the `Get-WindowsAutopilotInfo.ps1` script saves the hardware hash locally on the device as a CSV file. This method is normally used on devices that already underwent Windows Setup and OOB.
- [Directly upload the hardware hash to a mobile device management \(MDM\) service such as Intune](#) - the `Get-WindowsAutopilotInfo.ps1` script directly uploads the hardware hash to the MDM service. This method is normally used on devices that are undergoing Windows Setup and OOB.

Note

The `Get-WindowsAutopilotInfo` script used in this section was updated in July of 2023 to use the Microsoft Graph PowerShell modules instead of the deprecated AzureAD Graph PowerShell modules. Make sure to use the latest version of the script. The Microsoft Graph PowerShell modules might require approval of additional permissions in Microsoft Entra ID when the modules are first used. For more information, see [AzureAD](#) and [Important: Azure AD Graph Retirement and PowerShell Module Deprecation](#).

Save the hardware hash locally on a device as a CSV file

Saving the hardware hash locally on a device as a CSV file is normally done on devices that already underwent Windows Setup and OOB. To capture and save the hardware hash locally on a device:

1. Sign into the device.
2. On the device, open an elevated Windows PowerShell prompt.
3. Run the following commands from the elevated Windows PowerShell prompt:

```
PowerShell

[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
New-Item -Type Directory -Path "C:\HWID"
Set-Location -Path "C:\HWID"
$env:Path += ";C:\Program Files\WindowsPowerShell\Scripts"
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
Install-Script -Name Get-WindowsAutopilotInfo
Get-WindowsAutopilotInfo -OutputFile AutopilotHWID.csv
```

ⓘ Note

On first run, the `Get-WindowsAutopilotInfo.ps1` script prompts to approve the required app registration permissions.

The hardware hash is saved locally on the device in the directory `C:\HWID` with the filename `AutopilotHWID.csv`. The CSV file can then be used to [import the device](#) into an MDM service such as Intune.

Instead of running the PowerShell commands directly on devices, they can instead be run remotely on devices as long as the following requirements are met on the remote device:

- WMI permissions are in place.
- WMI is accessible through Windows Firewall on the remote device.

Directly upload the hardware hash to an MDM service

Directly uploading the hardware hash to an MDM service such as Microsoft Intune can be done on any device, but it's especially useful for a device currently undergoing Windows Setup and OOBE. To directly upload the hardware hash for a device:

1. On a device that is:
 - Currently undergoing Windows Setup and OOBE:

- a. At the sign-in prompt after OOBE starts, open a command prompt window with the keystroke `Shift + F10`.
- b. In the command prompt window that opens, start PowerShell by running the following command:

```
Windows Command Prompt
```

```
powershell.exe
```

- Already undergone Windows Setup and OOBE:
 - a. Sign into the device.
 - b. Open an elevated Windows PowerShell prompt.

2. At the `PS` PowerShell command prompt, run the following PowerShell commands:

```
PowerShell
```

```
[Net.ServicePointManager]::SecurityProtocol =  
[Net.SecurityProtocolType]::Tls12  
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned  
Install-Script -Name Get-WindowsAutopilotInfo -Force  
Get-WindowsAutopilotInfo -Online
```

If prompted to do so, agree to install **NuGet** from the **PSGallery**.

3. When the last command of `Get-WindowsAutopilotInfo -Online` runs, a Microsoft Entra ID sign-on prompt is displayed. Sign in with an account that is at least an Intune Administrator.

 **Note**

On first run, the `Get-WindowsAutopilotInfo.ps1` script prompts to approve the required app registration permissions.

4. After the sign-in is successful, the device hash uploads automatically.
5. Verify that the hardware hash uploaded successfully and the device is showing as a registered Windows Autopilot device using the instructions in the section [Verify the hardware hash uploaded](#).
6. For devices undergoing Windows Setup and OOBE, restart the device. The device should pick up the Windows Autopilot profile and OOBE should run through the

Windows Autopilot provisioning process.

Verify the hardware hash uploaded

To confirm the hardware hash for the device was uploaded into Intune and that the device shows as a Windows Autopilot device:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen, select **Sync** in the toolbar.
7. Wait for the sync to finish. The sync might take several minutes.
8. After the sync completes and the device appears in the device list in the **Windows Autopilot devices** screen in Intune, the device is ready for a Windows Autopilot deployment as long as a Windows Autopilot profile is assigned to the device.

Note

Microsoft recommends registering devices through Microsoft Intune via a 4K hardware hash only for testing or other limited scenarios for the following reasons:

- Availability of free and inexpensive accounts in Intune that lack robust vetting.
- 4K hardware hashes contain sensitive information that only device owners should maintain.

In most cases, instead use the Microsoft Partner Center for Windows Autopilot device registration.

For more information about running the `Get-WindowsAutopilotInfo.ps1` script, see the script's help by running the following command at PowerShell command prompt:

PowerShell

```
Get-Help Get-WindowsAutopilotInfo
```

Diagnostics page hash export

To export a hardware hash using the [Windows Autopilot Diagnostics Page](#), the device must be running Windows 11.

Windows Autopilot Diagnostics are available in OOB.

During OOB, enter the keystroke `CTRL + SHIFT + D` to bring up the Diagnostics Page. From this page, logs can be exported to a thumb drive. The logs include a CSV file with the hardware hash.

Desktop hash export

Sign into the device where the hardware hash needs to be exported. Once signed into the device, open the **Accounts > Access work or school** pane in the **Settings** app by selecting the following link:

[Access work or school](#)

Or

1. Right-click on the **Start** menu and select **Run**.
2. In the **Run** window, next to **Open:**, enter:

```
Console  
ms-settings:workplace
```

and then select **OK**.

Or

1. Right-click on the **Start** menu and select **Settings**.
2. In **Settings**, select **Accounts** in the left hand pane.
3. In the **Accounts** page, select **Access work or school**.

Once the **Access work or school** pane is open in the **Settings** app, export the log files:

- Windows 11: In the **Export your management log files** section, select the **Export** button.
- Windows 10: Select the **Export your management log files** link.

The logs include a CSV file with the hardware hash. Log files are exported to the `C:\Users\Public\Documents\MDMDiagnostics` directory.

For more information, see [Collect MDM logs](#).

Ensure that the CSV file meets requirements

Device information in the hardware hashes CSV file should include:

[] [Expand table](#)

Item	Required	Optional
Serial number		
Windows product ID	Partners uploading into Intune.	Admins uploading directly into Intune.
Hardware hash		
Group tag		
Assigned user		

The required items of serial number and hardware can be collected into an individual device CSV file using the following methods:

- The `Get-WindowsAutopilotInfo` script documented in the [Save the hardware hash locally on a device as a CSV file](#) section.
- The Desktop hash export documented in the [Desktop hash export](#) section.

The information from the individual device CSV files can be then used to create a CSV file with multiple devices to [import](#) multiple devices at once into an MDM service such as Intune.

The multiple devices CSV file can have up to 500 rows of devices. The header and line format must have the following format:

```
csv
Device Serial Number,Windows Product ID,Hardware Hash,Group Tag,Assigned User
```

```
<serialNumber>,<ProductID>,<hardwareHash>,<optionalGroupTag>,  
<optionalAssignedUser>
```

Keep these other requirements for the CSV file in mind:

- Extra columns aren't allowed.
- Quotation marks aren't allowed.
- Only ANSI-format text files are allowed. Unicode isn't allowed.
- Headers are case-sensitive.

Important

Use a plain-text editor such as Notepad with this CSV file. Don't use Microsoft Excel. Editing and saving the CSV file with Microsoft Excel doesn't generate a usable file for importing to Intune.

When a CSV file is uploaded to assign a user, make sure to assign a valid User Principal Names (UPNs). If an invalid UPN/incorrect username is uploaded, the device might be inaccessible until the invalid assignment is removed.

During upload of a CSV file, the only validation that Microsoft performs on the **Assigned User** column is to check that the domain name is valid. Microsoft doesn't perform individual UPN validation to ensure that an existing or correct user is being assigned.

Add devices

Once the hardware hashes are captured in a CSV file, Windows Autopilot devices can be added by importing the file. To import the file by using Intune:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen, select **Import** in the toolbar.

7. In the **Add Autopilot devices** screen:
 - a. browse to the CSV file that lists the devices that need to be added.
 - b. Select **Import** to start importing the device information. Importing can take several minutes.
8. After import is complete, in the **Windows Autopilot devices** screen, select **Sync** in the toolbar.

A message says that the synchronization is in progress. The process might take a few minutes to complete, depending on how many devices are being synchronized.
9. Select **Refresh** in the toolbar until the new devices appear.

Edit Autopilot device attributes

After an Autopilot device is uploaded, certain attributes of the device can be edited:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen, select the device that needs to be edited.
7. In the pane on the right of the screen, the following items can be edited:
 - Device name.
 - Group tag.
 - Username (if a user is assigned).
8. Select **Save**.

 **Note**

Device names can be configured for all devices but are ignored in Hybrid Microsoft Entra deployments. The device name still comes from the domain join profile for Hybrid Microsoft Entra devices.

Delete Autopilot devices

Windows Autopilot devices that aren't enrolled in Intune can be deleted:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen, select the devices that need deletion, and then select **Delete** in the toolbar. The deletion process can take a few minutes to complete.

Completely removing a device from a tenant requires the device records in Intune, Microsoft Entra ID, and Windows Autopilot to all be deleted. These deletions can all be done from Intune but need to be done in the following order. For more information, see [Deregister a device](#).

Troubleshooting registration failures

1. **StorageError**: This error is a generic error that can occur for various reasons. Most of the time it's not possible to determine the exact cause of the error until further investigation is done. If this error is encountered, the best course of action is to try again later. If the issue persists, contact support.
2. **ZtdDeviceAssignedToAnotherTenant**: This error occurs when the uploaded hardware hash matches a device that is already registered to a different tenant. If this error occurs, search for the serial number corresponding to the duplicate in the CSV file. Then, search for the serial number in the **Windows Autopilot devices** pane in Intune. If the device is already registered, don't import it again.

3. **ZtdDeviceAlreadyAssigned**: This error occurs when the uploaded hardware hash matches a device that is already registered to the tenant. If this error occurs, search for the serial number corresponding to the duplicate in the CSV file. Then, search for the serial number in the **Windows Autopilot devices** pane in Intune. If the device is already registered, don't import it again. If the device isn't registered, it can be imported again.
4. **ZtdDeviceDuplicated**: This error occurs when there are duplicate hardware hashes in the CSV file. Only one of the duplicates is processed, and the others result in this error. If this error occurs, look for the other duplicates of the same device to see what the actual result was. If a duplicate that was successfully processed is found, the duplicate row from the CSV file can be removed.
5. **InvalidZtdHardwareHash**: This error occurs when one or more fields in the hardware hash are invalid or empty. Both the manufacturer and serial number information need to be included. If they're not, the device can't be registered for Windows Autopilot. To check the serial number and manufacturer information, open a command prompt and run the following command:

```
Windows Command Prompt  
wmic baseboard get manufacturer, serialnumber
```

Related content

- [Create device groups](#) to apply Autopilot deployment profiles.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Create device groups for Windows Autopilot

Article • 09/13/2024 • Applies to:  Windows 11,  Windows 10,  Windows Holographic

Note

HoloLens 2 devices require Windows Autopilot self-deploying mode. For more information about using Windows Autopilot to deploy HoloLens 2 devices, see [Windows Autopilot for HoloLens 2](#). **Assign to User** isn't applicable for self-deployment Autopilot mode on HoloLens 2.

Create an Autopilot device group using Intune

1. In the [Microsoft Intune admin center](#), select **Groups > New group**.
2. In **New Group**, configure the following properties:
 - **Group type:** Select **Security**.
 - **Group name** and **Group description:** Enter a name and description for the group.
 - **Microsoft Entra roles can be assigned to the group:** Select **No**, Microsoft Entra roles aren't assigned to this group.

For more information, see [Use cloud groups to manage role assignments in Microsoft Entra ID](#).

 - **Membership type:** Select how devices become members of this group. Select **Dynamic Device**. For more information, see [Add groups to organize users and devices](#).
 - **Owners:** Select users that own the group. Owners can also delete this group.
 - **Dynamic device members:** Select **Add dynamic query > Add expression**.

Create rules using Autopilot device attributes. Autopilot devices that meet these rules are automatically added to the group. Creating an expression using non-autopilot attributes doesn't guarantee that devices included in the group are registered to Autopilot.

When creating expressions:

- To create a group that includes all of the Autopilot devices, enter:
`(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]")).`
- Intune's group tag field maps to the `OrderID` attribute on Microsoft Entra devices. To create a group that includes all Autopilot devices with a specific group tag (the Microsoft Entra device `OrderID`), enter:
`(device.devicePhysicalIDs -any (_ -eq "[OrderID]:179887111881")).`
- To create a group that includes all the Autopilot devices with a specific Purchase Order ID, enter: `(device.devicePhysicalIDs -any (_ -eq "[PurchaseOrderId]:76222342342"))`

Save the expressions.

3. Select **Create**.

 **Note**

Anything assigned to these attributes is only assigned if the device is registered with Autopilot.

For a detailed tutorial on creating a device group for each of the Windows Autopilot scenarios using Intune, see the following links:

- [User-driven Microsoft Entra join: Create a device group.](#)
- [User-driven Microsoft Entra hybrid join: Create a device group.](#)
- [Pre-provision Microsoft Entra join: Create a device group.](#)
- [Pre-provision Microsoft Entra hybrid join: Create a device group.](#)
- [Self-deploying mode: Create a device group.](#)

Add devices

The dynamic device group that includes Autopilot devices automatically adds existing Autopilot devices to the device group. To manually add new devices as Windows Autopilot devices using a CSV file so that they become part of the device group, see [Manually register devices with Windows Autopilot](#).

Assign a user to a specific Autopilot device

A licensed Intune user can be assigned to a specific Autopilot device. For supported OEMs, this assignment will:

- Pre-populate the Microsoft Entra user Principal Name (UPN) under the pre-provisioning landing page and Microsoft Entra sign-in page.
- Allows setting of a custom greeting name.

For more information including a list of supported OEMs, see [Return of key functionality for Windows Autopilot sign-in and deployment experience](#).

 **Note**

Assigning a licensed user to a specific Autopilot device only affects pre-populating the UPN and setting of a custom greeting name. It doesn't affect assigned policies and applications that are deployed to the device or to the user. The assigned policies and applications are still deployed regardless of the OEM. For more information, see [Windows Autopilot for pre-provisioned deployment](#).

 **Important**

Assigning a user to a specific Autopilot device doesn't work if using Active Directory Federation Services (ADFS).

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen, select a device, and then in the toolbar select **Assign user**.
7. Select a Microsoft Entra ID user licensed to use Intune and select **Select**.
8. In the **User Friendly Name** box, enter a friendly name or just accept the default.
9. Select **Save**.

For a detailed tutorial on assigning a user for each of the Windows Autopilot scenarios via Intune, see the following articles:

- User-driven Microsoft Entra join: [Assign Autopilot device to a user](#).
- User-driven Microsoft Entra hybrid join: [Assign Autopilot device to a user](#).
- Pre-provision Microsoft Entra join: [Assign Autopilot device to a user](#).
- Pre-provision Microsoft Entra hybrid join: [Assign Autopilot device to a user](#).

Using Autopilot in other portals

If there isn't interest in mobile device management (MDM), Autopilot can be used in other portals. While using other portals is an option, Microsoft recommends only using Intune to manage Autopilot deployments. When Intune is used with another portal, Intune isn't able to:

- Display changes to profiles created in Intune, but edited in another portal.
- Synchronize profiles created in another portal.
- Display changes to profile assignments done in another portal.
- Synchronize profile assignments done in another portal.
- Display changes to the device list that were made in another portal.

Windows Autopilot for existing devices

When enrolling Windows devices via [Autopilot for existing devices](#), a correlator ID can be used to group the Windows devices. The correlator ID is a parameter of the Autopilot configuration file. The [Microsoft Entra device attribute enrollmentProfileName](#) is automatically set to equal `OfflineAutopilotprofile- <correlator ID>`. Arbitrary Microsoft Entra dynamic groups can be created when using the correlator ID from the [enrollmentprofileName](#) attribute.

Warning

Because the correlator ID isn't pre-listed in Intune, the device might report any correlator ID they want. If the user creates a correlator ID matching an Autopilot or Apple ADE profile name, the device is added to any dynamic Microsoft Entra device group based off the `enrollmentProfileName` attribute. To avoid this conflict:

- Always create dynamic group rules matching against the *entire* `enrollmentProfileName` value.

- Never name Autopilot or Apple ADE profiles beginning with **OfflineAutopilotprofile-**.

If all devices in the groups should automatically register to Autopilot, in any Autopilot profiles assigned to the groups, set the setting **Convert all targeted devices to Autopilot** to **Yes**. All non-Autopilot devices in assigned groups register with the Autopilot deployment service. Allow 48 hours for the registration to be processed. When the device is unenrolled and reset, Autopilot enrolls it again. After a device is registered in this way, disabling this setting or removing the profile assignment won't remove the device from the Autopilot deployment service. The device must be removed by deregistering the device from Autopilot. For more information on how to properly deregister a device, see [Deregister a device](#).

For a full tutorial on Windows Autopilot for existing devices, see the following article:

- [Step by step tutorial for Windows Autopilot deployment for existing devices in Intune and Configuration Manager.](#)

Next steps

After a device group is created, a Windows Autopilot deployment profile can be configured and deployed to each device in the group. Deployment profiles determine the deployment mode, and customize the OOB for the end users. For more information, see [Configure deployment profiles](#).

For a detailed tutorial on configuring and assigning a Windows Autopilot deployment profile, see the following articles. Each article has detailed instructions on configuring and assigning a Windows Autopilot deployment profile in Intune for each of the Autopilot scenarios:

- [User-driven Microsoft Entra join: Create and assign user-driven Microsoft Entra join Autopilot profile.](#)
- [User-driven Microsoft Entra hybrid join: Create and assign user-driven Microsoft Entra hybrid join Autopilot profile.](#)
- [Pre-provision Microsoft Entra join: Create and assign a pre-provisioned Microsoft Entra join Autopilot profile.](#)
- [Pre-provision Microsoft Entra hybrid join: Create and assign a pre-provisioned Microsoft Entra hybrid join Autopilot profile.](#)
- [Self-deploying mode: Create and assign self-deploying Autopilot profile.](#)

For more information about managing Windows Autopilot devices, see [What is Microsoft Intune device management?](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Configure Autopilot profiles

Article • 09/13/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

After the [device group](#) is created, a Windows Autopilot deployment profile can be applied to each device in the group. Deployment profiles determine the deployment mode, and customize the out-of-box experience (OOBE) for end users.

Autopilot profiles can be created via:

1. [Microsoft 365 admin center](#).
2. [Intune admin center](#).
3. [Intune graph](#).

For Intune managed devices, pre-provisioning, self-deploying, and co-management profiles can only be created and assigned in Intune.

Create an Autopilot deployment profile

Autopilot deployment profiles are used to configure the Autopilot devices. Up to 350 profiles can be created per tenant.

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Deployment Profiles**
6. In the **Windows Autopilot deployment profiles** screen, select the **Create Profile** drop down menu and then select either **Windows PC** or **HoloLens**. This article explains how to set up Autopilot for Windows PC. For more information about Autopilot and HoloLens, see [Windows Autopilot for HoloLens 2](#).
7. In the **Create profile** screen, on the **Basics** page, enter a **Name** and optional **Description**.
8. If all devices in the assigned groups should automatically register to Autopilot, set **Convert all targeted devices to Autopilot** to **Yes**. All corporate owned, non-

Autopilot devices in assigned groups register with the Autopilot deployment service. Personally owned devices aren't registered to Autopilot. Allow 48 hours for the registration to be processed. When the device is unenrolled and reset, Autopilot enrolls it again. After a device is registered in this way, disabling this setting or removing the profile assignment won't remove the device from the Autopilot deployment service. The device must instead be [removed directly](#).

 **Note**

Using the setting **Convert all targeted devices to Autopilot** doesn't automatically convert existing Microsoft Entra hybrid device in the assigned groups into a Microsoft Entra device. The setting only registers the devices in the assigned groups for the Autopilot service.

9. Select **Next**.
10. On the **Out-of-box experience (OOBE)** page, for **Deployment mode**, select one of these two options:
 - **User-driven:** Devices with this profile are associated with the user enrolling the device. User credentials are required to enroll the device.
 - **Self-deploying:** Devices with this profile aren't associated with the user enrolling the device. User credentials aren't required to enroll the device.
When a device has no user associated with it, user-based compliance policies don't apply to it. When self-deploying mode is used, only compliance policies targeting the device are applied.

Create profile

Windows PC

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

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

Deployment mode *	User-Driven	<input type="button" value="▼"/>
Join to Azure AD as *	Azure AD joined	<input type="button" value="▼"/>
Microsoft Software License Terms	Show	<input type="button" value="Hide"/>
 ⓘ Important information about hiding license terms		
Privacy settings	Show	<input type="button" value="Hide"/>
 ⓘ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more		
Hide change account options	Show	<input type="button" value="Hide"/>
User account type	Administrator	<input type="button" value="Standard"/>
Allow White Glove OOB	No	Yes
Language (Region)	Operating system default	<input type="button" value="▼"/>
Automatically configure keyboard	No	<input type="button" value="Yes"/>
Apply device name template	No	Yes

ⓘ Note

Options that are dimmed or shaded in the selected deployment mode aren't currently supported.

11. In the **Join to Microsoft Entra ID as** box, select **Microsoft Entra joined**.

12. Configure the following options:

- **Microsoft Software License Terms:** Select whether or not to show the EULA to users.
- **Privacy settings:** Select whether or not to show privacy settings to users.

ⓘ Important

The default value for the Diagnostic Data setting is set to Full during the out-of-box experience. For more information, see [Windows Diagnostics](#)

Data

- **Hide change account options:** Select **Hide** to prevent change account options from displaying on the company sign-in and domain error pages. This option requires [company branding to be configured in Microsoft Entra ID](#).
- **User account type:** Select the user's account type (**Administrator** or **Standard** user). We allow the user joining the device to be a local Administrator by adding them to the local Admin group. We don't enable the user as the default administrator on the device.
- **Allow pre-provisioned deployment** ([Requirements](#)): Select **Yes** to allow pre-provisioning support.

Note

When setting **Allow pre-provisioned deployment** to **No**, it's still possible to press the Windows key five times during OOOE to invoke pre-provisioning and progress down that path. However, Intune enforces this setting and a pre-provisioning failure with error code 0x80180005 occurs.

- **Language (Region):** Select the language to use for the device. This option is available in all Deployment modes.
- **Automatically configure keyboard:** If a **Language (Region)** is selected, select **Yes** to skip the keyboard selection page. This option is available in all Deployment modes.

Note

Language and keyboard settings require ethernet connectivity. Wi-fi connectivity isn't supported because of the requirement to select a language, locale, and keyboard to make that Wi-fi connection.

- **Apply device name template** (requires Microsoft Entra join type): Select **Yes** to create a template to use when naming a device during enrollment. Names must be 15 characters or less, and can have letters, numbers, and hyphens. Names can't be all numbers. Use the [%SERIAL% macro](#) to add a hardware-specific serial number. Or, use the [%RAND:x% macro](#) to add a random string

of numbers, where x equals the number of digits to add. Only a prefix can be provided for hybrid devices in a [domain join profile](#).

13. Select **Next**.

14. On the **Assignments** page, select **Selected groups** for **Assign to**.

The screenshot shows the 'Create profile' wizard in progress, specifically the 'Assignments' step (step 3 of 4). The top navigation bar includes 'Home > Devices > Windows > Windows Autopilot deployment profiles > Create profile' and 'Windows PC'. The main area shows 'Included groups' with 'Assign to' set to 'Selected groups'. Under 'Selected groups', 'Autopilot Lab' is listed with a 'Remove' link. A note below states: 'When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.' The 'Excluded groups' section is empty. At the bottom, there are 'Previous' and 'Next' buttons.

15. Select **Select groups to include**, and select the groups to include in this profile.

16. To exclude any groups, select **Select groups to exclude**, and select the groups to exclude.

① Note

When the assignment **All Devices** is used, exclusions aren't supported. Attempting to exclude groups while targeting to all devices might cause assignment problems and might require uploading device hashes again.

17. Select **Next**.

18. On the **Review + Create** page, select **Create** to create the profile.

Create profile

Windows PC

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

Summary

Basics

Name	test profile
Description	--
Convert all targeted devices to Autopilot	No
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Autopilot Lab
Excluded groups	--

Previous

Create

Assignment of Autopilot deployment profiles to devices

Intune periodically checks for new devices in the assigned groups, and then begin the process of assigning deployment profiles to those devices. Due to several different factors involved in the process of Autopilot profile assignment, an estimated time for the assignment can vary from scenario to scenario. These factors can include Microsoft Entra ID groups, membership rules, hash of a device, Intune and Autopilot service, and internet connection. The assignment time varies depending on all the factors and variables involved in a specific scenario.

Before deploying a device, ensure that a Windows Autopilot deployment profile is assigned to the device. To ensure the process is complete:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
6. In the **Windows Autopilot devices** screen, monitor the **Profile Status** column for a device that just had a deployment profile assigned to it. The profile status changes from **Unassigned** to **Assigning** and finally to **Assigned**.
7. Once the device is showing **Assigned**, open the properties of the device by selecting it.
8. In the device properties pane that opens, ensure that **Date assigned** is populated. If **Date assigned** isn't yet populated, wait until it populates before deploying the device.

Edit an Autopilot deployment profile

After the Autopilot deployment profile is created, certain parts of the deployment profile can be edited.

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Deployment profiles**.
6. Select the profile to edit.

7. Select **Properties** to change the name or description of the deployment profile.
Select **Save** after making changes.
8. Select **Settings** to make changes to the OOBE settings. Select **Save** after making changes.

 **Note**

Changes to the profile are applied to devices assigned to that profile. However, the updated profile won't be applied to a device that is already enrolled in Intune until after the device is reset and enrolled again.

If a device is registered in Autopilot and a profile isn't assigned, it receives the default Autopilot profile. If a device shouldn't go through Autopilot, the Autopilot registration must be removed.

Autopilot profile priority

If a group is assigned to multiple Autopilot profiles, the device would receive the oldest created profile to resolve the conflict. If no other profile is applicable to the device and there's a default profile (any Autopilot profile assigned to all devices), then the default profile is applied. If a device is assigned to a security group that isn't assigned to Autopilot profile, then it would receive the default profile targeted to all devices. To see when an Autopilot profile is created:

1. Sign into the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left hand pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
4. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
5. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Deployment Profiles**.
6. In the **Windows Autopilot deployment profiles** screen, under **Name**, select the Autopilot profile name where the create date needs to be viewed.
7. When the Windows Autopilot deployment profile screen opens, the date the Windows Autopilot deployment profile was created is displayed under **Essentials** and next to **Created**.

Autopilot deployments report

Details on each device deployed through Windows Autopilot can be seen through a report. To see the report, go to the [Microsoft Intune admin center](#), select **Devices > Monitor > Windows Autopilot deployment status**. The data is available for 30 days after deployment.

This report is in preview. Only new Intune enrollment events trigger device deployment records. Deployments that don't trigger a new Intune enrollment don't appear in this report. This case includes any kind of reset that maintains enrollment and the user portion of Autopilot pre-provisioning.

Autopilot profile tutorials

The following articles are tutorials on configuring and assigning a Windows Autopilot deployment profile for each of the Windows Autopilot scenarios via Intune:

- [User-driven Microsoft Entra join: Create and assign user-driven Microsoft Entra join Autopilot profile.](#)
- [User-driven Microsoft Entra hybrid join: Create and assign user-driven Microsoft Entra hybrid join Autopilot profile.](#)
- [Pre-provision Microsoft join: Create and assign a pre-provisioned Microsoft Entra join Autopilot profile.](#)
- [Pre-provision Microsoft Entra hybrid join: Create and assign a pre-provisioned Microsoft Entra hybrid join Autopilot profile.](#)
- [Self-deploying mode: Create and assign self-deploying Autopilot profile.](#)

Related content

- [How are Windows Autopilot device profiles downloaded?](#)
- [Registering devices.](#)

Feedback

Was this page helpful?



[Provide product feedback](#)

Deploy Microsoft Entra hybrid joined devices by using Intune and Windows Autopilot

Article • 02/27/2025 •

Applies Windows 11, Windows 10, Windows Server 2025, Windows Server 2022, to: Windows Server 2019, Windows Server 2016

Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Windows Autopilot. For more information, see [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization](#).

Intune and Windows Autopilot can be used to set up Microsoft Entra hybrid joined devices. To do so, follow the steps in this article. For more information about Microsoft Entra hybrid join, see [Understanding Microsoft Entra hybrid join and co-management](#).

Requirements

The list of requirements for performing Microsoft Entra hybrid join during Windows Autopilot is organized into three different categories:

- **General** - general requirements.
- **Device enrollment** - device enrollment requirements.
- **Intune connector** - Intune Connector for Active Directory requirements.

Select the appropriate tab to see the relevant requirements:

General

- Successfully configured the [Microsoft Entra hybrid joined devices](#). Be sure to [verify the device registration](#) by using the `Get-MgDevice` cmdlet.
- If [Domain and OU-based filtering](#) is configured as part of Microsoft Entra Connect, ensure that the default organizational unit (OU) or container intended for the Autopilot devices is included in the sync scope.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Setting the BitLocker encryption algorithm for Autopilot devices

Article • 06/11/2024 • Applies to:  Windows 11,  Windows 10

BitLocker [automatically encrypts](#) internal drives during the out-of-box experience (OOBE) for devices that support [Modern Standby](#) or meet the [Hardware Security Testability Specification \(HSTI\)](#). By default, BitLocker uses XTS-AES 128-bit used space only for automatic encryption.

With Windows Autopilot, BitLocker encryption settings can be configured to apply before automatic encryption starts. This configuration makes sure the default encryption algorithm or type isn't applied automatically. A device that receives these settings after encrypting automatically needs to be decrypted before changing the encryption algorithm.

Encryption algorithm

BitLocker uses the specified BitLocker encryption algorithm when BitLocker is first enabled. During Autopilot, BitLocker will be enabled after the device setup portion of the [enrollment status page](#). The following encryption algorithms are available:

- AES-CBC 128-bit.
- AES-CBC 256-bit.
- XTS-AES 128-bit (default).
- XTS-AES 256-bit.

For more information about the recommended encryption algorithms to use, see [BitLocker Configuration Service Provider \(CSP\)](#).

To make sure the desired BitLocker encryption algorithm is set before automatic encryption occurs for Autopilot devices:

1. Configure the [encryption method settings](#) in the Endpoint Security disk encryption policy. The settings are available under **Endpoint Security > Disk encryption > Create policy > Platform = Windows 10 and later, Profile type = BitLocker**.
2. [Assign the policy](#) to the Autopilot device group. The encryption policy must be assigned to **devices** in the group, not users.
3. Enable the Autopilot [enrollment status page](#) for these devices. If this feature isn't enabled, the policy doesn't apply before encryption starts.

Full disk or used space-only encryption

There are two types of encryption, full disk or used space-only. Configuration of [silent enablement](#) and hardware support for modern standby automatically determines the type of encryption used. The type of encryption used can be enforced by configuring the [SystemDrivesEncryptionType](#) setting. Like the encryption algorithm, BitLocker uses the encryption type when BitLocker is first enabled. For more information on the expected encryption type behavior, see [Manage BitLocker policy](#).

To enforce the type of drive encryption used:

1. Configure the **Enforce drive encryption type on operating system drives** setting within the [settings catalog](#). This setting is available in the **Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives** category from the settings picker.
2. [Assign the policy](#) to the Autopilot device group. The encryption policy must be assigned to **devices** in the group, not users.
3. Enable the Autopilot [enrollment status page](#) for these devices. If this feature isn't enabled, the policy doesn't apply before encryption starts.

Related content

- [BitLocker overview](#).
- [Manage BitLocker policy for Windows devices with Intune](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Device Firmware Configuration Interface (DFCI) Management

Article • 02/27/2025 • Applies to:  Windows 11,  Windows 10

With Windows Autopilot Deployment and Intune, Unified Extensible Firmware Interface (UEFI) settings can be managed after the device is enrolled. UEFI settings can be managed by using the Device Firmware Configuration Interface (DFCI). DFCI [enables Windows to pass management commands](#) from Intune to UEFI for Autopilot deployed devices. This capability allows limiting end user's control over BIOS settings. For example, the boot options can be locked down to prevent users from booting up another OS, such as one that doesn't have the same security features.

If a user reinstalls a previous Windows version, installs a separate OS, or formats the hard drive, they can't override DFCI management. This feature can also prevent malware from communicating with OS processes, including elevated OS processes. DFCI's trust chain uses public key cryptography, and doesn't depend on local UEFI password security. This layer of security blocks local users from accessing managed settings from the device's UEFI menus.

For an overview of DFCI benefits, scenarios, and requirements, see [Device Firmware Configuration Interface \(DFCI\) Introduction](#).

Important

A device automatically enrolls in DFCI management during Autopilot provisioning when the following actions occur:

- The OEM enables the device for DFCI.
- The device is registered for Autopilot via the OEM or a Cloud Solution Partner (CSP) in Partner Center.

Enrollment in DFCI management triggers an additional reboot during the out-of-box experience (OOBE).

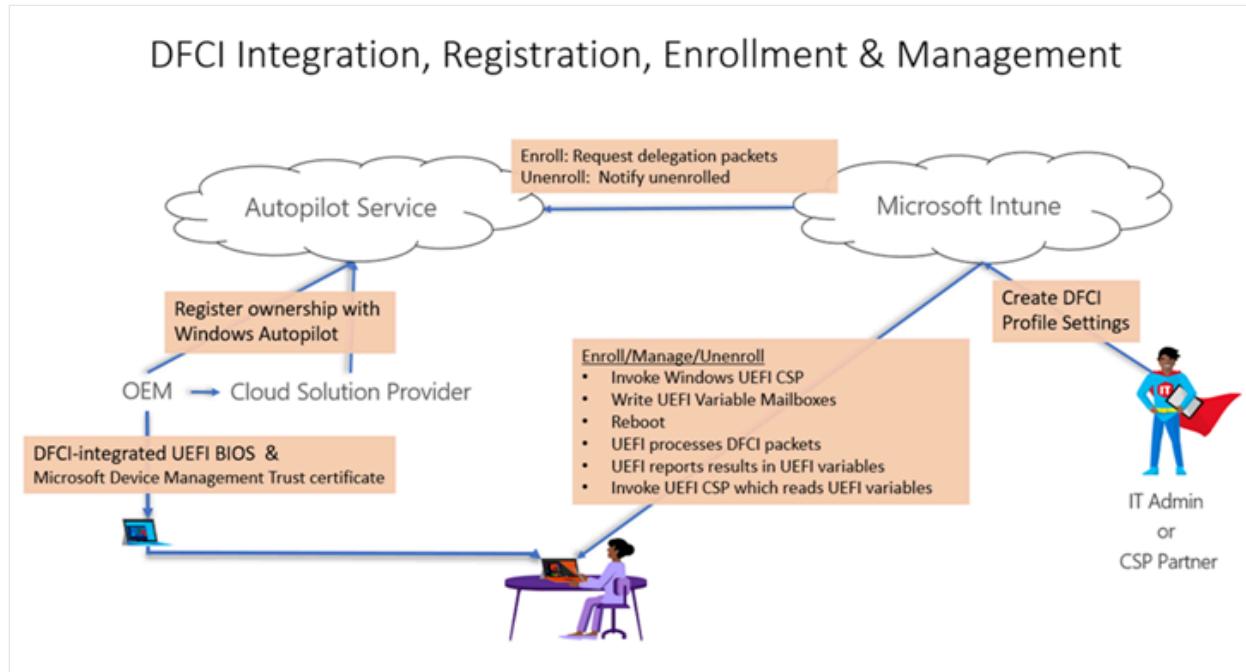
DFCI management lifecycle

The DFCI management lifecycle includes the following processes:

- UEFI integration.

- Device registration.
- Profile creation.
- Enrollment.
- Management.
- Retirement.
- Recovery.

See the following figure:



Requirements

- A currently supported version of Windows and a supported UEFI is required.
- The device manufacturer must have DFCI added to their UEFI firmware in the manufacturing process, or as a firmware update that can be installed. Work with the device vendors to determine the [manufacturers that support DFCI](#), or the firmware version needed to use DFCI.
- The device must be managed with Microsoft Intune. For more information, see [Enroll Windows devices in Intune using Windows Autopilot](#).
- The device must be registered for Windows Autopilot by a [Microsoft Cloud Solution Provider \(CSP\) partner](#), or registered directly by the OEM. For Surface devices, Microsoft registration support is available at [Microsoft Devices Autopilot Support](#).

ⓘ Important

Devices manually registered for Autopilot (such as by [importing from a CSV file](#)) aren't allowed to use DFCI. By design, DFCI management requires external

attestation of the device's commercial acquisition through an OEM or a Microsoft CSP partner registration to Windows Autopilot. When the device is registered, its serial number is displayed in the list of Windows Autopilot devices.

Managing DFCI profile with Windows Autopilot

There are four basic steps in managing DFCI profile with Windows Autopilot:

1. Create an Autopilot Profile
2. Create an Enrollment status page profile
3. Create a DFCI profile
4. Assign the profiles

See [Create the profiles](#) and [Assign the profiles, and reboot](#) for details.

The existing [DFCI settings](#) can also be changed on devices that are in use. In the existing DFCI profile, change the settings and save the changes. Since the profile is already assigned, the new DFCI settings take effect when next time the device syncs or the device reboots.

To identify whether a device is DFCI ready, the following Intune Graph API call can be used:

```
managedDevice/deviceFirmwareConfigurationInterfaceManaged
```

For more information, see [Intune devices and apps API overview](#) and [Working with Intune in Microsoft Graph](#).

OEMs that support DFCI

- Acer.
- Asus.
- Dynabook.
- Fujitsu.
- [Microsoft Surface](#).
- Panasonic.
- VAIQ.
- Samsung.

Other OEMs are pending.

Known issues

DFCI enrollment fails for Professional editions of Windows 11, version 24H2

Date added: *October 9, 2024* Date updated: *February 11, 2025*

DFCI can't currently be configured during the out-of-box experience (OOBE) on devices with Professional editions of Windows 11, version 24H2

For devices that have already been provisioned and have Professional editions of Windows 11, version 24H2, install [KB5046740](#) or later to enroll in DFCI. Devices with Professional editions of Windows 11, version 24H2 that have KB5046740 or later installed are automatically enrolled in DFCI after a reboot.

If DFCI needs to be configured during OOBE provisioning on 24H2 devices, follow these steps:

1. During OOBE onboarding, ensure the device is upgraded to the Enterprise edition of Windows 11, version 24H2.
2. After upgrading to the Enterprise edition of Windows 11, version 24H2, sync the device.
3. Once the device is synced, reboot it to get it enrolled in DFCI.

Related content

- [Microsoft DFCI Scenarios](#).
- [Windows Autopilot and Surface devices](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Windows Autopilot FAQ

FAQ

Applies to:

- [Windows 11](#).
- [Windows 10](#).

This article provides OEMs, partners, administrators, and end users with answers to some frequently asked questions about deploying Windows with Autopilot.

Microsoft Partner Center

In the Partner Center, does the Tenant ID need to be provided with every device file upload? Is it needed to allow the business customer to access their devices in Microsoft Store for Business (MSfB)?

No. Providing the Tenant ID is a one-time entry in the Partner Center that can be reused with future device uploads.

How does the customer or tenant know that their devices are ready to be claimed in MSfB?

After the device file upload is completed in the Partner Center, the tenant can see the devices available for Windows Autopilot setup in MSfB. The OEM needs to advise the tenant to access MSfB. Autonotification from MSfB to the tenant is being developed.

How does a customer authorize an OEM or Channel Partner to register Autopilot devices on the customer's behalf?

Before an OEM or Channel Partner can register a device for Autopilot for a customer, the customer must first give them consent. The consent process begins with the OEM or

Channel Partner sending a link to the customer that directs the customer to a consent page in MSfB. For more information, see [Registration](#).

Do any restrictions apply if a business customer who registers devices in MSfB wants to later manage those devices through a Cloud Solution Provider (CSP) using the Partner Center?

The business customer must delete the devices in MSfB before the CSP can upload and manage them in the Partner Center.

Does Windows Autopilot support removing the option to enable a local administrator account?

No. Windows Autopilot doesn't support removing the local admin account. However, it does support restricting the user performing Microsoft Entra domain join during the out-of-box experience (OOBE) to a standard account versus an administrator account by default.

How can I test the Windows Autopilot comma-separated value (CSV) file in the Partner Center?

Only CSP partners have access to the Partner Center portal. If you're a CSP, you can create a sales agent user account that has access to devices for testing the file. This test can be done today in the Partner Center.

For more information, see [Create user accounts](#).

Is it required to become a CSP to participate in Windows Autopilot?

This requirement doesn't apply to top volume OEMs because they can use the OEM Direct API. All others who choose to use the Microsoft Partner Center (MPC) to register devices must become CSPs to access MPC.

Do the different CSP levels have all the same capabilities when it comes to Windows

Autopilot?

For the purposes of Windows Autopilot, there are three different types of CSPs, each with different levels of authority and access:

1. **Direct CSP**: Gets direct authorization from the customer to register devices
2. **Indirect CSP provider**: Gets implicit permission to register devices through the relationship their CSP reseller partner has with the customer. Indirect CSP providers register devices through the Microsoft Partner Center.
3. **Indirect CSP reseller**: Gets direct authorization from the customer to register devices. At the same time, their indirect CSP provider partner also gets authorization, which means that either the indirect provider or the indirect reseller can register devices for the customer. However, the indirect CSP reseller must register devices through the Partner Center user interface by manually uploading the CSV file. The indirect CSP provider can register devices using the Partner Center APIs.

Is there such a thing as a single, worldwide CSP account?

No. The CSP sales regions depend on the location of the Microsoft Entra tenant. A CSP partner can only sell or manage customers with a tenant located in the same CSP region. A partner's CSP region is based on the location of the tenant the CSP partner is using to transact. If the customer tenant was created in the US, only a partner that has a CSP enrollment in the US can establish a reseller relationship with this customer.

For Autopilot & Intune, the location of the end user or device doesn't matter. An employee located in Germany can enroll a device using the Autopilot profile created in the US tenant and manage it through the Intune service instance in the US. The user in Germany also authenticates in the US-based Microsoft Entra instance.

If a partner wants to manage customers globally, they need to have a global presence. They need multiple CSP enrollments in each of the CSP sales regions where they conduct business.

It's not possible to create user accounts that have access to all CSP tenants. This scenario would translate into 18 user accounts for a CSP admin agent that wants to manage all customers around the world.

In summary, the location of the user and devices doesn't matter. The location of the customer tenant matters. Cross-border device registration isn't the problem. The problem is cross-border sales via CSP.

Does the Partner Center have access to the profiles created in Intune or Microsoft Store for Business?

No. The Partner Center doesn't have access to profiles created in Intune or Microsoft Store for Business. It only has access to the Autopilot profiles created through the Partner Center.

Manufacturing

What changes need to be made in the factory OS image for customer configuration settings?

No changes are required on the factory floor to enable Windows Autopilot deployment.

What version of the OA3 tool meets Windows Autopilot deployment requirements?

Windows Autopilot can work with any version of the OA3 tool. We recommend using a supported version of Windows to generate the 4K hardware hash (4K HH).

When placing an order, do customers need to be state whether they want it with or without Windows Autopilot options?

Yes. If they want Windows Autopilot, a supported version of Windows is needed. A customer should also receive the CSV file or have the file upload completed on their behalf.

Does the OEM need to manage or collect any custom imaging files from customers? Do they need to upload any images to Microsoft?

No. OEMs just send the Computer Build Report (CBR) as usual to Microsoft. No images are sent to Microsoft to enable Windows Autopilot. Windows Autopilot only customizes OOOE and allows policy configurations.

Are there any customer issues with upgrading to a currently supported version of Windows?

The devices must be running a supported version of Windows general availability channel to enroll in Windows Autopilot deployment. Otherwise, there's generally no issue. For more information, see [Windows Autopilot - known issues](#).

Will the existing CBR with 4K hardware hash ever change?

No.

What new information needs to be sent from the OEM to Microsoft?

Nothing, unless the OEM opts to register the device on the customer's behalf. In this case, they must upload the device ID CSV file to the Microsoft Partner Center or use the OEM direct API.

Is there a contract or amendment for an OEM to participate in an Autopilot deployment?

No.

CSV schema

Can a comma be used in the CSV file?

No.

Is there a limit to the number of devices that can be listed in the CSV file?

Yes. The CSV file can only contain 500 devices to apply to a single profile. If more than 500 devices need to be applied to a profile, the devices need to be uploaded through multiple CSV files.

Does Microsoft have any recommendations on how an OEM should provide the CSV file to their customers?

Encrypt the CSV file when sending it to the business customer to self-register their Windows Autopilot devices through MPC, MSfB, or Intune.

Hardware hash

What data does the hardware hash need to include?

Every hardware hash submitted by the OEM has to contain the following data:

- **SMBIOS UUID:** A universally unique identifier.
- **MAC address:** The network card unique identifier.
- **Unique disk serial number:** If you use the Windows OEM Activation 3.0 tool.

Since Windows Autopilot is based on the ability to uniquely identify devices applying for cloud configuration, it's critical to submit hardware hashes that meet the outlined requirement.

Why are the SMBIOS UUID, MAC address, and disk serial number required in the hardware hash details?

As parts of the device are added or removed, these fields are needed to identify a device when creating the hardware hash. Since we don't have a unique identifier for Windows devices, these fields are the best logic to identify a device.

What's the difference between the OA3 hardware hash, the 4K hardware hash, and the Windows Autopilot hardware hash?

None. They're different names for the same thing. The OA3 tool output is called the OA3 hash, which is 4K in size, and is used for the Windows Autopilot deployment scenario.

Note

If an older unsupported Windows version of the OA3 tool is used, a different-sized hash is generated. This hash can't be used for a Windows Autopilot deployment.

If I need to replace hardware like the disk or network card, does that invalidate the hardware hash?

Yes. If you replace parts, you might need to generate a new hardware hash. It depends on the parts that were replaced, and the characteristics of the parts.

For example, if you replace the TPM or motherboard, it's a new device and you must get a new hardware hash. If you replace one network card, it's probably not a new device, and the device functions with the old hardware hash.

In general, after any hardware changes, assume the old hardware hash is invalid and get a new hardware hash. This process is recommended anytime you replace parts.

Motherboard replacement

How does Autopilot handle motherboard replacement scenarios?

Motherboard replacement is out of scope for Autopilot. Any repaired or serviced device that alters the ability to identify the device for Windows Autopilot must go through the normal OOBE process. It must manually select the right settings or apply a custom image.

To reuse the same device for Windows Autopilot after a motherboard replacement, use the following process:

1. Unregister the device from Autopilot.
2. Replace the motherboard.
3. Generate a new 4K hardware hash.
4. Register the device with the new 4K hardware hash or device ID.

Note

An OEM can't use the OEM direct API to re-register the device, which only accepts a tuple or PKID. In this case, the OEM can send the new 4K hardware hash information using a CSV file to customer, and let the customer re-register the device using MSfB or Intune.

SMBIOS

Are there any specific requirements for the SMBIOS UUID?

It must be unique as specified in the Windows hardware requirements.

What's the requirement on the SMBIOS table to meet the Windows Autopilot hardware hash need?

It must meet all the Windows hardware requirements. For more information, see [Windows Hardware Compatibility Program Specifications and Policies](#).

If the SMBIOS supports UUID and Serial Number, is it enough for the OA3 tool to generate the hardware hash?

No. At a minimum, the following SMBIOS fields need to have unique values:

- `ProductKeyID`.
- `SmbiosSystemManufacturer`.
- `SmbiosSystemProductName`.
- `SmbiosSystemSerialNumber`.
- `SmbiosSkuNumber`.
- `SmbiosSystemFamily`.
- `MacAddress`.
- `SmbiosUuid`.
- `DiskSerialNumber`.
- `TPM`.
- `EkPub`.

Technical interface

What's the interface to get the MAC address and disk serial number? How does the OA tool get this information?

The method for getting this information varies depending on the scenario, but in general:

- The disk serial number comes from `IOCTL_STORAGE_QUERY_PROPERTY` with `StorageDeviceProperty/PropertyStandardQuery`.
- The network MAC address is from `IOCTL_NDIS_QUERY_GLOBAL_STATS` from `OID_802_3_PERMANENT_ADDRESS`.

If a device has multiple network cards or disks, how does the OA3 tool choose which MAC address and disk serial number to use?

All available values are used, although there can be specific usage rules. The serial number of the system disk is more important than the other disks available. Network interfaces that are removable shouldn't be used if detected as they're removable. LAN vs WLAN shouldn't matter, as both are used.

End-user experience

How do I know that I received Autopilot?

A device has received an Autopilot configuration but hasn't yet applied it when the selection page is skipped and are immediately taken to a sign-in page.

Why did a user end up as an administrator when the Autopilot profile was configured otherwise?

Microsoft Entra administrators are always local administrators even if Windows Autopilot is configured to disable this configuration.

To help troubleshoot, run `licensingdiag.exe` and send the `.cab` (cabinet) file to AutopilotHelp@microsoft.com. If possible, also collect an ETL from Windows Performance Recorder (WPR).

Often in these cases, users aren't signing into the right Microsoft Entra tenant, or are creating local user accounts.

For a complete list of support options, see [Windows Autopilot support](#).

If I make changes to an existing Autopilot profile, do the changes take effect on devices that have that profile assigned to them and are already deployed?

No. Windows Autopilot profiles aren't resident on the device. They're downloaded during OOB and settings are defined at the time are applied. The profile is then discarded on the device. If the device is reimaged or reset, the new profile settings will take effect the next time the device goes through OOB.

What's the experience if a device isn't registered or if I don't configure Windows Autopilot before an end user attempts to self-deploy?

If the device isn't registered, it doesn't receive the Windows Autopilot experience, and the end user goes through normal OOB. The Windows Autopilot configurations won't be applied until the user runs through OOB again, after registration. If a device is started before a mobile device management (MDM) profile is created, the device goes through standard OOB experience. You then have to manually enroll that device into the MDM. The next time the device is reset, it will go through the Windows Autopilot OOB experience.

Why didn't I receive a customized sign-in screen during Autopilot?

To receive a customized sign-in experience, configure tenant branding in the [Azure portal](#).

What happens if a device is registered with Microsoft Entra ID but doesn't have a Windows Autopilot profile assigned?

Since no Windows Autopilot profile is assigned to the device, the user sees the default OOB.

How can I collect logs on Autopilot?

The best way to collect logs on Windows Autopilot performance is to collect a WPR trace during OOB. The XML file (WPRP extension) for this trace can be provided upon request.

MDM

Does Autopilot require the use of Microsoft Intune?

No. Any MDM works with Autopilot, but others might not have the same full suite of Windows Autopilot features as Intune. The best experience is with Intune.

Does Intune support preinstalling Win32 apps?

Yes. Intune supports Win32 apps using MSI and MSIX wrappers.

What is co-management?

Co-management enables you to concurrently manage currently supported versions of Windows by using both Microsoft Configuration Manager and Microsoft Intune. It lets you cloud-attach your existing investment in Configuration Manager by adding new functionality. By using co-management, you have the flexibility to use the technology solution that works best for your organization.

When a Windows device has the Configuration Manager client and is enrolled to Intune, you get the benefits of both services. You control which workloads, if any, you switch the authority from Configuration Manager to Intune. Configuration Manager continues to manage all other workloads, including those workloads that you don't switch to Intune, and all other features of Configuration Manager that co-management doesn't support.

For more information, see the following articles:

- [What is co-management?](#).
- [How to enroll with co-management when provision with Windows Autopilot.](#)

Does Autopilot require Configuration Manager?

No. It isn't required, but you can use it together with Autopilot in the following scenarios:

- Co-management.
- Autopilot for existing devices.

Features

What's self-deploying mode?

Self-deploying mode only requires the user to power on the device. It's useful for scenarios where a standard user account isn't needed. For example, shared or kiosk devices.

For more information, see [Windows Autopilot self-deploying mode](#).

What's Microsoft Entra hybrid join?

ⓘ Important

Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Autopilot. For more information, see [Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization](#).

Microsoft Entra hybrid joined devices connect to an on-premises Active Directory domain and Microsoft Entra ID.

For more information, see [Introduction to device management in Microsoft Entra ID](#).

What's Windows Autopilot reset?

Windows Autopilot reset removes user apps and settings from a device, but maintains Microsoft Entra domain join and MDM enrollment. This feature is useful when you transfer a device from one user to another.

For more information, see [Windows Autopilot reset](#).

What's Autopilot personalization?

You can add the following customizations to the OOB experience:

- A personalized welcome message.
- Personalize the username hint.
- Your organization's logo.

What's Autopilot for existing devices?

Autopilot for existing devices offers an upgrade path to currently supported versions of Windows for an existing Windows device.

For more information, see [Autopilot for existing devices](#).

General

Which manufacturers are enabled for pre-population of username and automatic re-enrollment of pre-provisioning devices?

Current manufacturers enabled for this change are Dell, Dynabook, HP, Lenovo, and Microsoft Surface. We're working to add other manufacturers and will update this list once they're onboarded. For more information, see [Return of key functionality for Windows Autopilot sign-in and deployment](#).

If I wipe the machine and restart, do I still receive the Windows Autopilot experience?

Yes. If the device is still registered for Autopilot and is running a supported version of Windows, it receives the Autopilot experience.

Can I harvest the device fingerprint on existing devices?

Yes. If the device is running a supported version of Windows, you can harvest device fingerprints for registration. There are no plans to backport the functionality to earlier releases. There's no way to harvest them on devices running unsupported versions of Windows.

Is Windows Autopilot supported on other SKUs, for example, Surface Hub or HoloLens?

- Surface Hub and other SKUs not covered in [Software requirements](#) aren't supported with Windows Autopilot.
- HoloLens 1 doesn't support Windows Autopilot.
- HoloLens 2 supports Windows Autopilot self-deploying mode with Microsoft Intune and a currently supported version of Windows Holographic. Non-Microsoft MDM providers aren't supported.

For more information on HoloLens 2, see [Windows Autopilot for HoloLens 2](#).

Does Windows Autopilot work after motherboard replacement or image reinstallation?

Yes. For more information, see [Windows Autopilot motherboard replacement scenario guidance](#).

What does the error message "This user isn't authorized to enroll, error code 801c0003" mean?

There are limits to the number of devices a particular Microsoft Entra user can enroll in Microsoft Entra ID, and the number of devices that are supported per user in Intune. These limits are configurable, but not infinite. If you reuse devices, or roll back to previous virtual machine snapshots, this error occurs frequently.

What happens if a device is registered to a malicious agent?

By design, Windows Autopilot doesn't apply a profile until the user signs in with the matching tenant for the configured profile using the Microsoft Entra sign-in process. For example, `badguys.com` registers a device owned by `contoso.com`. At worst, the user is directed to sign in to `badguys.com`. When the user enters their email and password, the sign-in information is redirected through Microsoft Entra ID to the proper Microsoft Entra authentication and the user is prompted to then sign into `contoso.com`. Since `contoso.com` doesn't match `badguys.com` as the tenant, the malicious profile isn't applied and the user sees the regular OOB.

Where is Windows Autopilot data stored?

Windows Autopilot data is stored within the European Union (EU). It isn't stored in a sovereign cloud, even when the Microsoft Entra tenant is registered in a sovereign cloud. This storage applies to all Windows Autopilot data, whatever portal is used to deploy Autopilot.

Why is Windows Autopilot data stored in the US and not in a sovereign cloud?

Customer data isn't stored, only business data that enables Microsoft to provide a service. For that reason, it's appropriate for the data to be stored in the US. Customers can stop subscribing to the service at any time. In that event, Microsoft removes the business data. Autopilot isn't currently supported in any sovereign cloud.

How many ways are there to register a device for Windows Autopilot?

There are six ways to register a device, depending on who does the process:

1. OEM direct API, which is only available to TVOs.
2. MPC using the MPC API, which is only available to CSPs.
3. MPC using manual upload of CSV file in the UI, which is only available to CSPs.
4. MSfB using CSV file upload.
5. Intune using CSV file upload.
6. Microsoft 365 Business Premium portal using CSV file upload.

How many ways are there to create a Windows Autopilot profile?

There are four ways to create and assign a Windows Autopilot profile:

1. Through MPC, which is only available to CSPs.
2. Through MSfB.
3. Through Intune or another MDM service.
4. Microsoft 365 Business Premium portal.

Microsoft recommends creation and assignment of profiles through Intune.

What are some common causes of registration failures?

1. Bad or missing hardware hash entries can lead to faulty registration attempts.
2. Hidden special characters in CSV files. To avoid this issue, after creating your CSV file, open it in Notepad to look for hidden characters, trailing spaces, or other corruptions.

Is Autopilot supported in all countries/regions?

Autopilot only supports customers using global Azure. Global Azure doesn't include the following three entities:

- Azure Germany.
- Azure China 21Vianet.
- Azure Government.

If you use global Azure, there are no region restrictions. For example, Contoso uses global Azure but has employees working in China. The Contoso employees working in China can still use Autopilot to deploy devices. If Contoso uses Azure China 21Vianet, the Contoso employees can't use Autopilot.

While Autopilot is available in global tenants, users in China can experience poor connectivity and high latency when deploying due to ISP-related issues. If you're experiencing these issues when deploying in the region, contact your local ISP for support.

Why does TPM provisioning/attestation take longer during the first boot on a device?

TPM provisioning involves generating and processing strong cryptographic keys. Depending on the characteristics of the TPM hardware used on a device, it can take longer than a minute on first boot.

Why don't applications install after the ESP is finished on an Intune managed device when using autologon with Windows Autopilot self-deploying mode?

When autologon with Windows Autopilot self-deploying mode is used, autologon uses the KioskUser0 local account. By default, user ESP isn't processed for local accounts, including KioskUser0, and a device token isn't issued until user ESP is processed. When using autologon, in order for applications to install after the ESP finishes, skip user ESP by using the custom OMA-URI [SkipUserStatusPage](#). For more information, see the following articles:

- [How can I disable the user ESP portion of the Enrollment Status Page \(ESP\) if an ESP has been configured on the device?.](#)
- [Deploy OMA-URIs to target a CSP through Intune, and a comparison to on-premises.](#)

When Windows Autopilot for pre-provisioned deployment is used, the device shows as compliant in Microsoft Entra ID after completing the Technician flow. However, after starting the User flow, the device changes to noncompliant in Microsoft Entra ID. Why did it change from compliant to noncompliant in Microsoft Entra ID?

Device compliance in Microsoft Entra ID is reset during the User flow. Once the User flow completes, compliance is reevaluated and updated. This behavior is expected.

Intune Connector for Active Directory

What is the difference between the updated and legacy Intune Connector for Active Directory?

The updated Intune Connector for Active Directory strengthens security and follows least privilege principles by using a [Managed Service Account \(MSA\)](#) instead of using the

computer account (SYSTEM) of the server that runs the Intune Connector for Active Directory.

If the administrator installing and configuring the Intune Connector for Active Directory has the permissions outlined in the requirements, do they also have to follow the steps to increase the computer account limit in the OUs?

No. the Intune Connector for Active Directory installer takes care of setting up all of the proper permissions needed by the MSA in the OUs. The steps to increase the computer account limit in the OUs only need to be followed if the administrator installing and configuring the Intune Connector for Active Directory doesn't have the permissions outlined in [Intune Connector for Active Directory Requirements](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot troubleshooting FAQ

FAQ

Applies to:

- Windows 11.
- Windows 10.

This article provides troubleshooting for common Windows Autopilot issues.

Troubleshooting Windows Autopilot overview

What concepts should be understood when troubleshooting Windows Autopilot?

Windows Autopilot is designed to simplify all parts of the Windows device lifecycle, but there are always situations where issues might arise. When troubleshooting an issue, it's helpful to understand:

- The Windows Autopilot [process flow](#).
- How Windows Autopilot [device profiles](#) are downloaded.
- [Key activities](#) to perform during troubleshooting.

What is the Windows Autopilot process flow?

Whether performing user-driven or self-deploying device deployments, the troubleshooting process is about the same. It's useful to understand the flow for a specific device:

1. A network connection is established. The connection can be a wireless (Wi-fi) or wired (Ethernet) connection.
2. The Windows Autopilot profile is downloaded. When a wired connection is used, or a wireless connection is established, the profile downloads from the Windows Autopilot deployment service as soon as the network connection is in place.

3. User authentication occurs. During a user-driven deployment, the user enters their Microsoft Entra credentials, which is then validated.
4. Microsoft Entra join occurs. For user-driven deployments, the device is joined to Microsoft Entra ID using the specified user credentials. For self-deploying scenarios, the device is joined without specifying any user credentials.
5. Automatic mobile device management (MDM) enrollment occurs. As part of the Microsoft Entra join process, the device enrolls in the MDM service configured in Microsoft Entra ID (for example, Microsoft Intune).
6. Settings are applied. If the [enrollment status page](#) is configured, most settings are applied while the enrollment status page is displayed. If not configured or available, settings will be applied after the user is signed in.

How are Windows Autopilot device profiles downloaded?

When an Internet-connected Windows device boots up, it attempts to connect to the Windows Autopilot service and download a Windows Autopilot profile. The Windows Autopilot profile is downloaded as soon as possible, and again after each reboot.

Note

At this stage, it's important that a Windows Autopilot profile exists in the tenant so that a blank profile isn't cached locally on the device. If necessary, a new Windows Autopilot profile can be retrieved by rebooting the device.

If a computer needs to be rebooted during the Windows out-of-box experience (OOBE) to retrieve a new Windows Autopilot profile:

1. Select Shift-F10 to open a command prompt window.
2. In the command prompt window, enter one of the following two commands:
 - `shutdown.exe /r /t 0` to **restart** immediately.
 - `shutdown.exe /s /t 0` to **shut down** immediately.

For more information, see [Windows Setup Command-Line Options](#).

What are the key activities to perform when troubleshooting Windows Autopilot?

The key troubleshooting activities to perform are:

- Review configuration: Are Microsoft Entra ID and Microsoft Intune or a non-Microsoft mobile device management (MDM) service configured as specified in [Windows Autopilot configuration requirements](#)?
- Check network connectivity: Can the device access the services described in [Windows Autopilot networking requirements](#)?
- Windows out-of-box experience (OOBE) behavior: Are the [expected OOB](#) screens displayed? Is the Microsoft Entra credentials page customized with organization-specific details as expected?
- Microsoft Entra join issues: Is the device able to [join Microsoft Entra ID](#)?
- MDM enrollment issues: Is the device able to [enroll in Microsoft Intune](#) or non-Microsoft MDM service?
- Review logs that are automatically collected upon Windows Autopilot failure. For more information, see [Collect diagnostics from a Windows device](#).

How can additional detailed troubleshooting information be enabled?

On [Windows 11](#), the Windows Autopilot diagnostic page can be opened to view additional detailed troubleshooting information about the Windows Autopilot provisioning process. To enable the Windows Autopilot diagnostics page:

1. Go to the [ESP profile](#) where the Windows Autopilot diagnostics page needs to be enabled.
2. Make sure that **Show app and profile configuration progress** is selected to **Yes**.
3. Make sure that **Turn on log collection and diagnostics page for end users** is selected to **Yes**.

To access any diagnostic information once the diagnostic page is enabled, select the **View Diagnostics** button or enter the keystroke **CTRL + SHIFT + D**. The diagnostics page is currently supported under the following conditions:

- Windows 11.

- Windows Autopilot user-driven mode.
- When signing in with a Work or School account. Personal Microsoft accounts aren't supported.

ⓘ Note

- By default diagnostics are automatically collected upon a Windows Autopilot failure. For more information, see [Collect diagnostics from a Windows device](#).
- For diagnostics to be able to upload successfully from the client, make sure that the URL `lgmsapewe.u.blob.core.windows.net` isn't blocked on the network.

Where does Windows Autopilot log to?

Windows Autopilot logs entries into the event log. The log entries can be used to see details related to the Windows Autopilot profile settings and **OOBE** flow. These entries can be viewed using Event Viewer. Review the information in Event Viewer at **Application and Services Logs -> Microsoft -> Windows -> ModernDeployment-Diagnostics-Provider -> Autopilot**.

What do the different Event IDs mean in the Windows Autopilot event log entries in Event Viewer?

The following events might be recorded, depending on the scenario and profile configuration:

[+] Expand table

Event ID	Type	Message	Description
100	Warning	Autopilot policy [name] not found.	This error is typically a temporary problem, while the device is waiting for a Windows Autopilot profile to be downloaded.

Event ID	Type	Message	Description
101	Info	AutopilotGetPolicyDwordByName succeeded: policy name = [setting name]; policy value = [value].	This message shows Windows Autopilot retrieving and processing numeric OOBE settings.
103	Info	AutopilotGetPolicyStringByName succeeded: policy name = [name]; value = [value].	This message shows Windows Autopilot retrieving and processing OOBE setting strings such as the Microsoft Entra tenant name.
109	Info	AutopilotGetOobeSettingsOverride succeeded: OOBE setting [setting name]; state = [state].	This message shows Windows Autopilot retrieving and processing state-related OOBE settings.
111	Info	AutopilotRetrieveSettings succeeded.	This message means that the settings stored in the Windows Autopilot profile that control the OOBE behavior were retrieved successfully.
153	Info	AutopilotManager reported the state changed from [original state] to [new state].	Usually, this message says ProfileState_Unknown to ProfileState_Available . This case indicates that a profile was available and downloaded for the device and that the device is ready to deploy using Windows Autopilot.

Event ID	Type	Message	Description
160	Info	AutopilotRetrieveSettings beginning acquisition.	This message shows that Windows Autopilot is getting ready to download the needed Windows Autopilot profile settings.
161	Info	AutopilotManager retrieve settings succeeded.	The Windows Autopilot profile was successfully downloaded.
163	Info	AutopilotManager determined download isn't required and the device is already provisioned. Clean or reset the device to change this.	This message indicates that a Windows Autopilot profile is present on the device. The Sysprep /Generalize process typically removes a Windows Autopilot profile.
164	Info	AutopilotManager determined Internet is available to attempt policy download.	
171	Error	AutopilotManager failed to set TPM identity confirmed. HRESULT=[error code].	This message indicates an issue performing TPM attestation, needed to complete the self-deploying mode process.
172	Error	AutopilotManager failed to set Autopilot profile as available. HRESULT=[error code].	This error is typically related to event ID 171.
807	Error	ZtdDevicesNotRegistered	Validate that the device's hardware hash is properly uploaded to Intune and that the

Event ID	Type	Message	Description
			device is assigned to a deployment profile.
809	Error	ZtdDeviceHasNoAssignedProfile - Assigned profile does not exist.	The Windows Autopilot profile assigned to the device was deleted without first getting cleaned up. Assign a different Windows Autopilot profile to the device and then attempt to re-enroll the device.
815	Error	ZtdDeviceHasNoAssignedProfile - No profile assigned to the device, and no default profile found in the tenant.	A Windows Autopilot profile wasn't found assigned to the device. Validate that a Windows Autopilot profile is assigned to the device.
908	Error	SerialNumberMismatch ProductKeyIdMismatch	There's a mismatch between the serial number or product key recorded in Windows Autopilot and the physical hardware that is preventing enrollment. Reregister the device and then attempt to re-enroll the device.

Where are the Windows Autopilot profile settings received from the Windows Autopilot deployment service stored?

Windows Autopilot profile settings received from the Windows Autopilot deployment service are stored in the device's registry. This information can be found in the registry at the following registry key:

HKLM\SOFTWARE\Microsoft\Provisioning\Diagnostics\Autopilot

Available registry entries include:

[+] Expand table

Value	Description
AadTenantId	The GUID of the Microsoft Entra tenant the user signed into. The user receives an error if this entry doesn't match the tenant that was used to register the device.
CloudAssignedTenantDomain	The Microsoft Entra tenant the device is registered with, for example, <code>contosomn.onmicrosoft.com</code> . If the device isn't registered with Windows Autopilot, this value is blank.
CloudAssignedTenantId	The GUID of the Microsoft Entra tenant the device registered with. The GUID corresponds to the tenant domain from the CloudAssignedTenantDomain registry value. If the device isn't registered with Windows Autopilot, this value is blank.
IsAutopilotDisabled	If set to 1, this registry value indicates that the device isn't registered with Windows Autopilot. This state could also indicate that the Windows Autopilot profile couldn't be downloaded because of network connectivity or firewall issues, or network timeouts.
TenantMatched	This entry is set to 1 if the user's tenant ID matches the tenant ID that the device was registered with. If this registry value is 0, the user would be shown an error and forced to start over.
CloudAssignedOobeConfig	A bitmap that shows which Windows Autopilot settings were configured. Values include: <code>SkipCortanaOptIn</code> = 1, <code>OobeUserNotLocalAdmin</code> = 2, <code>SkipExpressSettings</code> = 4, <code>SkipOemRegistration</code> = 8, <code>SkipEula</code> = 16

Can ETW tracing be used with Windows Autopilot?

ETW tracing can be used to get detailed information from Windows Autopilot and related components. The ETW trace files can be viewed using the Windows Performance Analyzer or similar tools. For more information, see [Troubleshooting Windows Autopilot](#).

Why is the Intune Connector not logging in Event Viewer even though logging is enabled?

The Intune Connector originally logged in the Event Viewer directly under **Applications and Services Logs** in a log called **ODJ Connector Service**. However, logging for the Intune Connector has since moved to the path **Applications and Services Logs > Microsoft > Intune > ODJConnectorService**. If the ODJ Connector Service log at the original location is empty or not updating, check the new path location instead.

Troubleshooting Windows Autopilot device import and enrollment

Why is error code "0x80180014" occurring when trying to re-enroll a previously enrolled device?

Error code **0x80180014** can occur under either of the following scenarios:

1. Microsoft Intune changed the Windows Autopilot self-deployment mode and pre-provisioning mode experience. To reuse a device, the device record created by Intune must be deleted.

This change impacts all Windows Autopilot deployments that use the self-deployment or pre-provisioning mode. This change impacts devices when they devices are reused, reset, or when redeploying a profile.

To resolve and fix the issue in this scenario and redeploy the device using Windows Autopilot, follow these steps:

- a. Sign into the [Microsoft Intune admin center](#).
- b. In the **Home** screen, select **Devices** in the left hand pane.
- c. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
- d. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.

- e. In the **Windows | Enrollment** screen, under **Windows Autopilot**, select **Devices**.
- f. Select the device that is experiencing the error, and then in the toolbar select **Unblock device**.
- g. Redeploy the Windows Autopilot deployment profile.

 **Note**

A success message might not display after selecting **Unblock device**, but the device is ready to be used again.

2. Windows MDM enrollment is disabled in the Intune tenant.

To resolve and fix the issue in this scenario and redeploy the device using Windows Autopilot, follow these steps:

- a. Sign into the [Microsoft Intune admin center](#).
- b. In the **Home** screen, select **Devices** in the left hand pane.
- c. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
- d. In the **Windows | Windows devices** screen, under **Device onboarding**, select **Enrollment**.
- e. In the **Windows | Enrollment** screen, under **Enrollment options**, select **Device platform restriction**.
- f. In the **Enrollment restrictions** screen, under **Device type restrictions**, select **All Users** under the **Name** column.
- g. In the **All Users** screen that opens, under **Manage**, select **Properties**.
- h. In the **Properties** screen that opens, next to **Platform settings**, select the **Edit** link.
- i. In the **Edit restriction** screen that opens:
- j. Locate **Windows (MDM)** under the **Type** column.
- k. Make sure that **Windows (MDM)** is set to **Allow** under the **Platform** column.
- l. If **Windows (MDM)** is set to **Block**, change it to **Allow**.

- m. Select **Review + save**, and then either **Save** if a setting was changed, or **Cancel** if not settings were changed.
- n. Repeat the above steps for any additional restrictions that might exist in the **Enrollment restrictions** screen other than **All Users**. Only restrictions for the **Windows** platform need to be verified.

 **Note**

When multiple restrictions exist, restrictions might exist that only allow certain groups MDM enrollment. Some of the restrictions blocking MDM enrollment might be valid based on what group the restrictions are assigned to. When experiencing this problem, verify that the device isn't a member of one of the groups where there's MDM enrollment is blocked. Alternatively, if applicable change the MDM enrollment setting for that restriction to **Allow**.

In both of these scenarios, in addition to error **0x80180014** occurring, the Event Tracing for Windows (ETW) logs might also show the following mobile device management (MDM) error:

```
MDM Enroll: Server Returned Fault/Code/Subcode/Value=(DeviceNotSupported)  
Fault/Reason/Text=(Enrollment blocked for AP device by SDM One Time Limit Check)
```

When trying to import a CSV file with a device hardware hash, why does nothing happen when selecting Import?

This issue usually occurs because the device hash in the CSV file is incorrectly formatted. The issue can be confirmed by running a network trace while the issue occurs. Most likely the device hash in the CSV file is incorrectly formatted if an error **400** occurs in the network trace. The message body of the **400** error message shows:

```
Cannot convert the literal '[DEVICEHASH]' to the expected type 'Edm.Binary'
```

Anything that corrupts the collected hash can cause this error. One possibility is that the hash itself fails to be decoded, even if the hash is valid.

The device hash is Base64. At the device level, it's encoded as unpadded Base64, but Windows Autopilot expects padded Base64. Usually, the payload doesn't require padding and the process works. Sometimes, however, the payload doesn't line up cleanly and padding is necessary. In this case, the **400** error message occurs.

PowerShell's Base64 decoder also expects padded Base64, so this decoder can be used to validate that the hash is properly padded.

The "A" characters at the end of the hash are effectively empty data. Each character in Base64 is 6 bits. A in Base64 is 6 bits equal to 0. Deleting or adding As at the end doesn't change the actual payload data.

To resolve and fix this issue, the hash needs to be modified. The new value then needs to be tested until PowerShell succeeds in decoding the hash. The result is mostly illegible, which is fine as long as the error **Invalid length for a Base-64 char array or string** isn't displayed.

To test the base64, use the following PowerShell:

```
PowerShell  
  
[System.Text.Encoding]::ascii.GetString(  
[System.Convert]::FromBase64String("DEVICE HASH"))
```

As an example:

```
PowerShell  
  
[System.Text.Encoding]::ascii.GetString(  
[System.Convert]::FromBase64String("Q29udG9zbwAAA"))
```

This particular example isn't a device hash, but it's a misaligned unpadded Base64 so it's good for testing.

Now for the padding rules. The padding character is "="". The padding character can only be at the end of the hash, and there can only be a maximum of two padding characters. Here's the basic logic.

- Does decoding the hash fail?
 - Yes: Are the last two characters "=="?
 - Yes: Replace both "=" with a single "A" character, then try again
 - No: Add another "=" character at the end, then try again
 - No: That hash is valid

Looping the logic on the previous example hash, we get the following permutations:

- Q29udG9zbwAAA
- Q29udG9zbwAAA=
- Q29udG9zbwAAA==

- Q29udG9zbwAAAA
- Q29udG9zbwAAAA=
- **Q29udG9zbwAAAA==** - This result has valid padding.

Replace the collected hash with this new padded hash then try to import again.

Why is the Windows Autopilot profile not applied after a hardware change occurred on a device?

The Windows Autopilot profile isn't applied if the following conditions are met:

- A hardware change occurs on a device.
- The device is reimaged to a Windows version before one of the following versions:
 - Windows 11, version 21H2 with [KB5017383](#).
 - [Windows 10, versions 22H2](#).

This behavior is expected.

The message **Fix pending** or **Attention required** might also be displayed in the **Windows Autopilot devices** page for the device. These messages indicate that a hardware change occurred on the device. When the link for the **Fix pending** status is selected, the following message appears:

We've detected a hardware change on this device. We're trying to automatically register the new hardware. You don't need to do anything now; the status will be updated at the next check in with the result.

To resolve and fix this issue, deregister and re-register the device. For more information including how to deregister a device, see the following articles:

- [Deregister a device](#).
- [Return of key functionality for Windows Autopilot sign-in and deployment experience](#).
- [Windows Autopilot motherboard replacement scenario guidance](#).

Why is the join type for a device showing as "Microsoft Entra registered" instead of "Microsoft Entra joined"?

This issue occurs if the device was previously registered in Microsoft Entra ID before it was joined to Microsoft Entra ID. The device possibly registered in Microsoft Entra ID via something like a [Workplace join](#). If the Microsoft Entra ID registered device isn't deleted from Microsoft Entra ID before the device is joined to Microsoft Entra ID, then the previous trust type is retained in the record. Joining an existing Microsoft Entra registered device to Microsoft Entra ID results in the Windows Autopilot device showing as **Microsoft Entra registered** instead of **Microsoft Entra joined**.

To resolve and fix this issue, before registering an existing Microsoft Entra ID registered device as a Windows Autopilot device, the following existing device objects for the device should be deleted:

- Microsoft Intune.
- Microsoft Entra ID.
- Windows Autopilot.

After all device objects are deleted, re-register the device as a Windows Autopilot device and then re-enroll the device. For more information on properly deleting all of the device objects, see [Deregister a device](#).

Why is enrollment in Microsoft Intune or a non-Microsoft MDM solution failing with an error code "80180018"?

To troubleshoot enrollment issues in Microsoft Intune such as the error code 80180018 in the **Something went wrong** error page, see [Troubleshooting Windows device enrollment errors in Intune](#). Common issues can include:

- Incorrect or missing licenses assigned to the user.
- Too many devices enrolled for the user.

Why does Windows Autopilot Reset fail immediately with an error?

See [Windows Autopilot Reset: Troubleshooting](#) for more help if Windows Autopilot Reset fails immediately with the error:

Ran into trouble. Please sign in with an administrator account to see why and reset manually.

Troubleshooting Windows OOB issues during Windows Autopilot

Why is the Windows out-of-box experience (OOBE) not running as expected during Windows Autopilot?

It's useful to check if the device received a Windows Autopilot profile. If the device did receive a Windows Autopilot profile, verify that the settings in the profile are correct.

What is the cause of the error message "Can't connect to the URL of your organization's MDM terms of use."?

This error message usually indicates an issue with licensing. The complete error message reads:

Something went wrong

Can't connect to the URL of your organization's MDM terms of use. Try again, or contact your system administrator with the problem information from this page.

Verify that the user who is signing into the device has a valid Intune, EMS, or Microsoft 365 license.

Troubleshooting Microsoft Entra join issues

What is the most common issue joining a device to Microsoft Entra ID?

The most common issue joining a device to Microsoft Entra ID is related to Microsoft Entra permissions. Make sure that the correct configuration is in place to allow users to join devices to Microsoft Entra ID. For more information, see [Configuration requirements](#).

What happens if a user attempts to join more devices to Microsoft Entra ID than allowed?

Errors occur if a user exceeds the allowed number of devices they can join. This default limit is 50 devices but can be configured in Microsoft Entra ID. For more information, see [Understand Intune and Microsoft Entra device limit restrictions](#).

Why did deleting a device's object in Microsoft Entra ID cause the device to not be able to join Microsoft Entra ID any longer?

A Microsoft Entra device is created upon import. It's important this object isn't deleted. The object acts as Windows Autopilot's anchor in Microsoft Entra ID for group membership and targeting, including the profile. Deleting it might lead to Microsoft Entra join errors. If this object is deleted, the issue can be fixed by deleting and reimporting the device as a Windows Autopilot device. Deleting and reimporting the device as a Windows Autopilot device recreates the associated object in Microsoft Entra ID.

Troubleshooting policy conflicts with Windows Autopilot

Why is the web sign-in option missing at the Windows sign-in screen after Windows Autopilot pre-provisioning completes?

The [Device password policies](#) in the Security Baseline causes issues after pre-provisioning. To resolve, change the password settings in Security Baseline to **Not Configured** or assign the baseline to a user group.

Can policies conflict with Windows Autopilot working correctly?

There are a significant number of policy settings available for Windows, including:

- Native mobile device management (MDM) policies.
- Group policy (ADMX-backed) settings.

Some policy settings can cause issues in some Windows Autopilot scenarios. These issues can arise because of how the policies change Windows behavior. If any of these issues are discovered, remove the policy in question to resolve the issue.

What are some of the known policies that conflict with Windows Autopilot?

The following policies are known to cause issues with Windows Autopilot. Make sure to configure the policies appropriately so that they don't conflict with Windows Autopilot:

[+] Expand table

Policy	More information
Disallow changing of language/region/keyboard	This group policy object (GPO) isn't supported during the out-of-box experience (OOBE) flow as it impacts the autologon experience. If this policy needs to be set for users, select to hide these pages in the Windows Autopilot profile to prevent users from making changes.
AppLocker CSP	The AppLocker configuration service provider (CSP) isn't supported in the Enrollment Status Page as it triggers a reboot when a policy is applied or a deletion occurs.
Device restriction/Password Policy	<p>The out-of-box experience (OOBE) or user desktop autologon can fail when a device reboots during the device Enrollment Status Page (ESP). This failure can occur when certain DeviceLock policies are applied to a device. Such policies can include:</p> <ul style="list-style-type: none">• Minimum password length and password complexity• Any similar group policy settings (including any that disable autologon) <p>This possible failure is especially true for kiosk scenarios where passwords are automatically generated.</p>
Windows Security Baseline/Administrator elevation prompt behavior	These policies require a reboot, as a result more prompts might appear when modifying user account control (UAC) settings during the OOBE

Policy	More information
Windows Security Baseline / Enable virtualization based security	<p>using the device Enrollment Status Page (ESP). Increased prompts are more likely if the device reboots after policies are applied. To work around this issue, the policies can be targeted to users instead of devices so that they apply later in the process.</p>
Device restrictions/Cloud and Storage/Microsoft Account sign-in assistant	<p>Setting this policy to "disabled" turns off the Microsoft Sign-in Assistant service (wlidsvc). Windows Autopilot requires this service to get the Windows Autopilot profile.</p>
Registry keys that affect Windows Autopilot if a device setting requires a reboot during device ESP	<p>Registry key: If the AutoAdminLogon registry key is set to 0 (disabled), this breaks Windows Autopilot.</p> <p>Registry path: <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Automatic logon</code></p>
MDM wins over Group Policy	<p>This policy allows control of which policy is used when both the MDM policy and its equivalent Group Policy (GP) are set on the device.</p>
Group Policy Objects (GPOs) that affect Windows Autopilot for pre-provisioned deployment	<p>Windows Autopilot pre-provisioning doesn't work when any of the four GPO policy settings listed here are enabled.</p> <p>GPO path: <code>Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options</code></p> <p>Policies:</p> <ul style="list-style-type: none"> Interactive logon: Message title for users attempting to log on Interactive logon: Message text for users attempting to log on Interactive logon: Require Windows Hello for Business or smart card

Policy	More information
	User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode - Prompt for credentials on the secure desktop
PreferredAadTenantDomainName	When this policy is enabled, it adds the preferred domain to DefaultUser0 , which causes autologon to fail.

Troubleshooting application install issues during Windows Autopilot

Why is the error message "Another installation is in progress, please try again later" occurring during the ESP of a Windows Autopilot deployment?

The Enrollment Status Page (ESP) used by Windows Autopilot doesn't support mixing of line-of-business (LOB) and Win32 applications. Both LOB and Win32 applications use **TrustedInstaller** which doesn't allow simultaneous installations. If both an LOB and Win32 application attempt to install at the same time, the following error message occurs during ESP:

Another installation is in progress, please try again later.

For more information, see [Set up the Enrollment Status Page - Device setup: Apps](#).

If mixing LOB and Win32 apps is required, consider using [Windows Autopilot device preparation](#), which doesn't use ESP so therefore supports mixing of LOB and Win32 apps.

During the ESP of a Windows Autopilot deployment, why does the Microsoft 365 Click-to-Run version of Office fail to install the Teams Machine-Wide Installer, or cause other Win32 app MSI based installs to fail?

The Teams Machine-Wide Installer component of the Microsoft 365 Click-to-Run version of Office includes an MSI installation. ESP doesn't track the Teams Machine-Wide Installer MSI install. Because ESP doesn't track the Teams Machine-Wide Installer MSI install, it can cause a conflict when other Win32 app MSI based installs attempt to install during ESP. MSIs install via **TrustedInstaller** which doesn't allow simultaneous installations. This conflict can cause either the Teams Machine-Wide Installer to fail or other MSI based installs to fail during ESP. For more information, see [Set up the Enrollment Status Page - Device setup: Apps](#).

This issue might be random and might not always occur. The issue occurs due to a timing issue between the Teams Machine-Wide Installer MSI install and other Win32 app MSI installs.

To work around the issue or avoid the error, use one of the following solutions:

1. Don't install **Teams** as part of the Microsoft 365 Click-to-Run install of Office. Instead, deploy **Teams** as a Win32 app after the Windows Autopilot deployment completes.
2. Don't install the Microsoft 365 Click-to-Run version of Office during ESP. Instead, deploy the Microsoft 365 Click-to-Run install of Office after the Windows Autopilot deployment completes.
3. Use a custom PowerShell script for Intune Management Extension (IME) that checks if **TrustedInstaller** is currently installing another MSI. If it is, then wait for the current MSI to finish installing before launching a new MSI install.
4. For Windows 11 deployments, use [Windows Autopilot device preparation](#). Windows Autopilot device preparation doesn't use ESP so therefore supports mixing of LOB and Win32 apps.
5. Continue on error for ESP failures. If the problem occurs with this option enabled, some applications including **Teams** might not install. However, ESP continues and doesn't fail.

Troubleshooting the Intune Connector for Active Directory

Why is the Intune Connector for Active Directory not logging in Event Viewer even though logging is enabled?

The Intune Connector for Active Directory originally logged in the Event Viewer directly under **Applications and Services Logs** in a log called **ODJ Connector Service**. However, logging for the Intune Connector for Active Directory has since moved to the path **Applications and Services Logs > Microsoft > Intune > ODJConnectorService**. If the **ODJ Connector Service** log at the original location is empty or not updating, check the new path location instead.

Why does uninstalling the Intune Connector for Active Directory through the Settings app not fully remove the application?

The Intune Connector for Active Directory needs to be uninstalled using both the Settings app and the Intune Connector for Active Directory installed executable **ODJConnectorBostrapper.exe**. When uninstalling the Intune Connector for Active Directory, run **ODJConnectorBostrapper.exe** and select the **Uninstall** option. The **ODJConnectorBostrapper.exe** installer version needs to match the version of the connector that's being uninstalled.

Why is the error "The MSA account couldn't be granted permission to create computer objects in the following OUs" occurring when installing the Intune Connector for Active Directory?

This error might occur for several different type of failures including:

- The administrator installing and configuring the Intune Connector for Active Directory doesn't have the required permissions as outlined in the [Intune Connector for Active Directory Requirements](#).
- The organization unit (OU) specified in the Intune Connector for Active Directory **ODJConnectorEnrollmentWiazard.exe.config** XML configuration file doesn't exist.

For detailed information on the error and what caused it, see the **ODJConnectorUI.log** normally located in the folder **C:\Program Files\Microsoft Intune\ODJConnector\ODJConnectorEnrollmentWizard**.

For more information, see [Install the Intune Connector for Active Directory on the server](#).

Why did enrollments start failing when using the Intune Connector for Active Directory?

Make sure that the Intune Connector for Active Directory is updated to version 6.2501.2000.5 or later and that the legacy version isn't still being used. For more information, see [Intune Connector for Active Directory Requirements](#).

Related content

- [Windows Autopilot - known issues.](#)
- [Collect MDM logs.](#)
- [Collect diagnostics from a Windows device.](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot - known issues

Article • 02/27/2025 • Applies to:  Windows 11,  Windows 10

This article describes known issues that can often be resolved with configuration changes or via cumulative updates. Some known issues might also be resolved automatically in a future release.

Tip

RSS can be used to notify when new known issues are added to this page. For example, the following RSS link includes this article:

url

```
https://learn.microsoft.com/api/search/rss?  
search=%22Be+informed+about+known+issues+that+might+occur+during+Window  
s+Autopilot+deployment.%22&locale=en-us&%24filter=
```

This example includes the `&locale=en-us` variable. The `locale` variable is required, but it can be changed to another supported locale. For example, `&locale=es-es`.

For more information on using RSS for notifications, see [How to use the docs](#) in the Intune documentation.

Note

For issues with Autopilot with Co-management, see [Windows Autopilot with co-management](#).

Known issues

Windows Autopilot report incorrectly shows failure even though the deployment was successful

Date added: *February 11, 2025*

The Windows Autopilot report automatically updates deployment status from **In progress** to **Failed** after 4 hours if Intune didn't receive a success or failure status. It's possible that the report didn't receive the latest status from the device before the device

is powered off which results in an incorrect **Failed** status, even when the deployment is successful.

Local Administrator Password Solution (LAPS) policy isn't being applied during the Technician Flow

Date added: *December 9, 2024*

During Windows Autopilot pre-provisioning technical flow, if a LAPS policy is targeted to the device or user, it isn't applied until the user phase begins.

Windows Autopilot deployment report and AutopilotEvents Graph API only returns 50 records at a time

Date added: *December 4, 2024*

In Intune's 2411 release, we've updated the backend infrastructure of the Windows Autopilot deployment report for consistency with other Intune reports. With this change, the Windows Autopilot deployment report and the [AutopilotEvents Microsoft Graph API](#) now return 50 records at a time. To show more than 50 records at a time:

- Use the `skipToken` parameter to get additional pages of data with the AutopilotEvents Graph API.
- Use the [export API](#) with `reportName` `AutopilotV1DeploymentStatus` to get all records.

DFCI enrollment fails for Professional editions of Windows 11, version 24H2

Date added: *October 9, 2024*

Date updated: *January 15, 2025*

DFCI can't currently be configured during the out-of-box experience (OOBE) on devices with Professional editions of Windows 11, version 24H2

For devices that have already been provisioned and have Professional editions of Windows 11, version 24H2, install [KB5046740](#) or later to enroll in DFCI. Devices with Professional editions of Windows 11, version 24H2 that have KB5046740 or later installed are automatically enrolled in DFCI after a reboot.

If DFCI needs to be configured during OOBE provisioning on 24H2 devices, follow these steps:

1. During OOBE onboarding, ensure the device is upgraded to the Enterprise edition of Windows 11, version 24H2.
2. After upgrading to the Enterprise edition of Windows 11, version 24H2, sync the device.
3. Once the device is synced, reboot it to get it enrolled in DFCI.

Autopilot deployment report doesn't support sorting

Date added: *August 29, 2024*

The Autopilot deployment report was updated to a new infrastructure that doesn't currently support column sorting. The issue will be addressed in the future.

Auto logon for Kiosk device profile only partially fixed

Date added: *August 21, 2024*

The known issue of [Kiosk device profiles not auto logging in when auto logon was enabled](#) was previously reported as fixed. However, there are scenarios where the issue might still occur when using autologon with Kiosks and [Assigned Access](#). If multiple reboots or unexpected reboots occur during the Windows out-of-box experience (OOBE) when initially configuring the Kiosk, the autologon entries in the registry might be deleted. The issue is being investigated.

The following workarounds are available until the issue is resolved:

1. Apply or reapply the kiosk profile after Windows Autopilot completes.
2. Apply the autologon registry entries either manually or via a script. For example:

Windows Command Prompt

```
reg.exe add "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon" /v "AutoAdminLogon" /t REG_SZ /d 1 /f  
  
reg.exe add "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon" /v "DefaultDomainName" /t REG_SZ /d "." /f  
  
reg.exe add "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon" /v "DefaultUserName" /t REG_SZ /d  
"kioskUser0" /f
```

3. Exclude items the required reboots during OOBE from Windows Autopilot.

4. Manually enter the kiosk user credentials.

For more information, see [Assigned Access recommendations - Automatic sign-in](#). For additional assistance, contact support.

BitLocker encryption defaults to 128-bit when 256-bit encryption is configured

Date added: *July 8, 2024*

In some Windows Autopilot deployments of unregistered devices, BitLocker encryption might default to 128-bit even though the admin configured 256-bit encryption due to a known race condition. The issue is being investigated. Microsoft recommends that customers who need 256-bit BitLocker encryption register devices for Autopilot.

Required apps aren't shown on the Enrollment Status Page (ESP) after an Autopilot Reset

Date added: *May 17, 2024*

When an Autopilot Reset happens, the required apps aren't installed on the Enrollment Status Page (ESP) before the user reaches the desktop. The apps aren't tracked on the ESP, but the apps are installed when the user signs in to the desktop.

Enrolled date for Autopilot device is incorrect

Date added: *November 1, 2023*

The **Enrolled date** in the **Devices | All devices** and **Windows | Windows devices** panes display the date the device was registered to Autopilot instead of the date it was enrolled to Autopilot. For a more accurate date for when the device enrolled to the tenant:

1. Use the Intune Graph API to query the device:

```
devices?$filter=physicalIds/any(p: startswith(p,  
'[ZTDID']))&$select=id,deviceId,displayName,physicalIds,createdDateTime
```

For more information, see [Intune devices and apps API overview](#) and [Working with Intune in Microsoft Graph](#).

2. Use the Windows Autopilot deployment report for recently deployed devices.

Filtering Windows Autopilot devices not working as expected

Date added: *July 14, 2023*

Viewing Windows Autopilot devices within Intune might not work as expected if attempting to filter results. While this issue is being worked on, a workaround is to use [Microsoft Graph API](#) to properly query and filter necessary devices.

TPM attestation isn't working on some platforms with Infineon SLB9672 discrete TPMs

Date added: *June 2, 2023*

Platforms with the Infineon SLB9672 TPM with firmware release 15.22 with EK certificate might fail with error message **Something happened, and TPM attestation timed out**. To resolve this issue, contact the OEM for an update.

Kiosk device profile not auto logging in

Date added: *January 30, 2023*

Date updated: *August 21, 2024*

There's currently a known issue in the following Windows Updates released in January 2023:

- Windows 11, version 22H2: [KB5022303 ↗](#)
- Windows 11, version 21H2: [KB5022287 ↗](#)
- Windows 10, version 22H2: [KB5022282 ↗](#)

If these updates are installed on a device, Kiosk device profiles that have auto logon enabled won't auto log on. After Autopilot completes provisioning, the device stays on the sign-in screen prompting for credentials. To work around this known issue, manually enter the kiosk user credentials with the username `kioskUser0` and no password. After the username is entered with no password, it should go to the desktop. This issue should be resolved in cumulative updates released for Windows 11 in April 2023 and Windows 10 in March 2023:

- Windows 11, version 22H2: [KB5025239 ↗](#) or later.
- Windows 11, version 21H2: [KB5025224 ↗](#) or later.

- Windows 10, version 22H2: [KB5023773](#) or later.

Note

This issue was only partially fixed and can still occur under certain conditions. For more information, see [Auto logon for Kiosk device profile only partially fixed](#).

TPM attestation isn't working on AMD platforms with ASP fTPM

Date added: *December 1, 2022*

TPM attestation for AMD platforms with ASP firmware TPM might fail with error code 0x80070490 on Windows systems. This issue is resolved on later versions of AMD firmware. Consult with device manufacturers and firmware release notes for which firmware versions contain the update.

TPM attestation failure with error code 0x81039001

Date added: *October 6, 2022*

Some devices might intermittently fail TPM attestation during Windows Autopilot pre-provisioning technician flow or self-deployment mode with the error code **0x81039001 E_AUTOPILOT_CLIENT_TPM_MAX_ATTESTATION_RETRY_EXCEEDED**. This failure occurs during the **Securing your hardware** step for Windows Autopilot devices deployed using self-deploying mode or pre-provisioning mode. Subsequent attempts to provision might resolve the issue.

Autopilot deployment report shows "failure" status on a successful deployment

Date added: *September 22, 2022*

The Autopilot deployment report (preview) shows a failed status for any device that experiences an initial deployment failure. For subsequent deployment attempts, using the **Try again** or **Continue to desktop** options, the deployment state in the report doesn't update. If the user resets the device, a new deployment row is shown in the report with the previous attempt remaining as failed.

Autopilot deployment report doesn't show deployed device

Date added: *September 22, 2022*

Autopilot deployments that take longer than one hour might display an incomplete deployment status in the deployment report. If the device successfully enrolls but doesn't complete provisioning after more than one hour, the device status might not be updated in the report.

Autopilot profile not being applied when assigned

Date added: *June 15, 2022*

In Windows 10, version 21H2 April 2022 and some May 2022 update releases, there's an issue where the Autopilot profile might fail to apply to the device. Additionally, the hardware hash might not be harvested. As a result, any settings made in the profile might not be configured for the user such as device renaming. To resolve this issue, apply [KB5015020](#) ↗ cumulative update or later to the device.

DefaultuserX profile not deleted

Date added: *March 28, 2022*

When the [EnableWebSignIn CSP](#) is used, the `defaultuserX` profile might not be deleted.

Autopilot reset ran into trouble. Could not find the recovery environment

Date added: *March 28, 2022*

When an Autopilot reset is attempted, the following message is displayed:

Autopilot reset ran into trouble. Could not find the recovery environment

If there isn't an issue with the recovery environment, enter administrator credentials to continue with the reset process.

Device-based Conditional Access policies

Date added: *March 3, 2022*

1. The Intune Enrollment app must be excluded from any Conditional Access policy requiring **Terms of Use** because it isn't supported. See [Per-device terms of use](#).
2. Exceptions to Conditional Access policies to exclude **Microsoft Intune Enrollment** and **Microsoft Intune** cloud apps are needed to complete Autopilot enrollment in cases where restrictive policies are present such as:
 - Conditional Access policy 1: Block all apps except those apps on an exclusion list.
 - Conditional Access policy 2: Require a compliant device for the apps on the exclusion list.

In this case, Microsoft Intune Enrollment and Microsoft Intune should be included in that exclusion list of policy 1.

If a policy is in place such that **all cloud apps** require a compliant device (there's no exclusion list), by default Microsoft Intune Enrollment is excluded, so that the device can register with Microsoft Entra ID and enroll with Intune and avoid a circular dependency.

3. **Hybrid Microsoft Entra devices:** When Hybrid Microsoft Entra devices are deployed with Autopilot, two device IDs are initially associated with the same device - one Microsoft Entra ID and one hybrid. The hybrid compliance state displays as **N/A** when viewed from the devices list in the [Azure portal](#) until a user signs in. Intune only syncs with the Hybrid device ID after a successful user sign-in.

The temporary **N/A** compliance state can cause issues with device based Conditional Access policies that block access based on compliance. In this case, this behavior of Conditional Access is intended. To resolve the conflict, a user must sign in to the device, or the device-based policy must be modified. For more information, see [Conditional Access: Require compliant or Microsoft Entra hybrid joined device](#).

4. Conditional Access policies such as BitLocker compliance require a grace period for Autopilot devices. This grace period is needed because until the device is rebooted, the status of BitLocker and Secure Boot aren't captured. Since the status isn't captured, it can't be used as part of the Compliance Policy. The grace period can be as short as 0.25 days.

Device goes through Autopilot deployment without an assigned profile

Date added: *March 2, 2022*

When a device is registered in Autopilot and no profile is assigned, the default Autopilot profile is taken. This behavior is by design. It makes sure that all devices registered with Autopilot go through the Autopilot experience. If the device shouldn't go through an Autopilot deployment, remove the Autopilot registration.

White screen during Microsoft Entra hybrid joined deployment

Date added: *February 19, 2022*

There's a UI bug on Autopilot Microsoft Entra hybrid joined deployments where the Enrollment Status page is displayed as a white screen. This issue is limited to the UI and shouldn't affect the deployment process.

This issue was resolved in September 2022.

Virtual machine failing at "Preparing your device for mobile management"

Date added: *February 19, 2022*

When trying to use Windows Autopilot on a virtual machine (VM), the following error might occur:

"Preparing your device for mobile management

To resolve the issue, make sure the virtual machine is configured with a minimum of 2 processors and 4 GB of memory.

ODJConnectorSvc.exe leaks memory

Date added: *February 19, 2022*

When a proxy server is used with the ODJConnector service, the memory file can get too large when processing requests resulting in impacts to performance. The current workaround for this issue is to restart the ODJConnectSvc.exe service.

Reset button causes pre-provisioning to fail on retry

Date added: *February 19, 2022*

When ESP fails during the pre-provisioning flow and the user selects the reset button, TPM attestation might fail during the retry.

TPM attestation failure on Windows 11 error code 0x81039023

Date added: *February 19, 2022*

Some devices might fail TPM attestation on Windows 11 during the pre-provisioning technician flow or self-deployment mode with the error code 0x81039023. To resolve the issue, apply the May 2022 cumulative update for Windows 11, version 21H2 [KB5013943 ↗](#) or later to the device.

Duplicate device objects with Microsoft Entra hybrid deployments

Date added: *January 9, 2022*

A device object is pre-created in Microsoft Entra ID once a device is registered in Autopilot. If a device goes through a hybrid Microsoft Entra deployment, by design, another device object is created resulting in duplicate entries.

TPM attestation failure on Windows 11 error code 0x81039024

Date added: *December 8, 2021*

Some devices might fail TPM attestation on Windows 11 during the pre-provisioning technician flow or self-deployment mode with the error code 0x81039024. This error code indicates that there are known vulnerabilities detected with the TPM and as a result attestation fails. If this error occurs, visit the PC manufacturer's website to update the TPM firmware.

Delete device record in Intune before reusing devices in self-deployment mode or Pre-Provisioning mode

Devices are enrolled using Autopilot self-deployment mode or pre-provisioning mode. If a device is redeployed so that it reruns the Autopilot deployment again, it fails with a `0x80180014` error code.

To resolve this error, use one of the following work around methods:

- Delete the device record in Intune, and then redeploy the device so that it reruns the Autopilot deployment. For more information, see [Deregister a device](#).
- Remove the device enrollment restriction for Windows (MDM) personally owned devices. For more information, see [Set enrollment restrictions in Microsoft Intune](#).

For more information on this issue, see [Troubleshooting Windows Autopilot device import and enrollment](#).

A non-assigned user can sign in when using user-driven mode with Active Directory Federation Services (ADFS)

In a Windows Autopilot user-driven Microsoft Entra joined environment, a user can be pre-assigned to a device. If the user is a cloud-native Microsoft Entra account, the username is enforced and the user is only asked for their password. There's no way to sign in with another user ID. However, when ADFS is used, the username assignment isn't enforced. A different user than the one assigned can sign in on the device.

Intune connector is inactive but still appears in the Intune Connectors

Inactive Intune connectors will be automatically cleaned up after 30 days of inactivity without admin interaction.

Autopilot sign-in page displays HTML tags from company branding settings

When [customizations are applied to the company branding settings](#), the HTML tags might be visible and not rendered correctly on the update password page. This issue should be fixed in future versions of Windows.

TPM attestation isn't working on Intel Tiger Lake platforms

TPM attestation support for Intel firmware TPM Tiger Lake platforms on devices with Windows 10, version 21H2 require the November 2021 cumulative update [KB5007253](#) or later. Older versions of Windows aren't supported.

Blocking apps specified in a user-targeted Enrollment Status Profile are ignored during device ESP

The services responsible for determining the list of apps that should be blocking during device ESP aren't able to determine the correct ESP profile containing the list of apps because they don't know the user identity. As a workaround, enable the default ESP profile (which targets all users and devices) and place the blocking app list there. To avoid this issue, target the ESP profile to [device groups](#).

That username looks like it belongs to another organization. Try signing in again or start over with a different account

Confirm that all of the information is correct in the registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Provisioning\Diagnostics\Autopilot`

For more information, see [Where are the Windows Autopilot profile settings received from the Windows Autopilot deployment service stored?](#).

Windows Autopilot user-driven hybrid Microsoft Entra deployments don't grant users Administrator rights even when specified in the Windows Autopilot profile

This issue occurs when there's another user on the device that already has Administrator rights. For example, a PowerShell script or policy could create another local account that is a member of the Administrators group. To ensure this works properly, don't create another account until after the Windows Autopilot process is complete.

Windows Autopilot device provisioning can fail

These failures might be because of TPM attestation errors or ESP timeouts on devices where the real-time clock is off by a significant amount of time. For example, several minutes or more.

To fix this issue:

- Boot the device to the start of the out-of-box experience (OOBE).
- Establish a network connection (wired or wireless).
- Run the command `w32tm /resync /force` to sync the time with the default time server (`time.windows.com`).

Windows Autopilot for existing devices doesn't work

During a Windows Autopilot for existing devices deployment, screens that are disabled in the Windows Autopilot profile are shown, such as the Windows License Agreement screen.

This issue happens because Windows deletes the `AutopilotConfigurationFile.json` file when `Sysprep.exe` runs with the `/Generalize` parameter. The **Prepare Windows for Capture** task in a Configuration Manager task sequence runs `Sysprep.exe` with the `/Generalize` parameter.

To fix this issue:

- Edit the Configuration Manager task sequence and disable the **Prepare Windows for Capture** step.
- Add a new **Run command-line** step that runs the following command:

Windows Command Prompt

```
C:\Windows\System32\sysprep\sysprep.exe /oobe /reboot
```

For more information, see [Modify the task sequence to account for Sysprep command line configuration](#) and [Prepare Windows for Capture](#).

Windows Autopilot self-deploying mode fails with an error code

For more information on this scenario, see [Windows Autopilot self-deploying mode](#).

[+] Expand table

Error code	Description
0x800705B4	This general error indicates a timeout. A common cause of this error in self-deploying mode is that the device isn't TPM 2.0 capable. For example, it's a virtual machine. Devices that aren't TPM 2.0 capable can't be used with self-deploying mode.
0x801c03ea	This error indicates that TPM attestation failed, causing a failure to join Microsoft Entra ID with a device token.
0xc1036501	The device can't do an automatic MDM enrollment because there are multiple MDM configurations in Microsoft Entra ID.

Pre-provisioning gives an error screen and the Microsoft-Windows-User Device Registration/Admin event log displays HResult error code 0x801C03F3

This issue can happen if Microsoft Entra ID can't find a Microsoft Entra device object for the device that is being deployed. This issue occurs the object was manually deleted. To fix it, remove the device from Microsoft Entra ID, Intune, and Autopilot, then re-register it with Autopilot, which recreates the Microsoft Entra device object. For more information, see [Deregister a device](#).

To get troubleshooting logs, run the following command:

```
Windows Command Prompt
```

```
Mdmdiagnosticstool.exe -area Autopilot;TPM -cab c:\autopilot.cab
```

Pre-provisioning gives an error screen

Pre-provisioning isn't supported on a VM.

Error importing Windows Autopilot devices from a .csv file

Ensure that the .csv file isn't edited in Microsoft Excel or an editor other than Notepad. Some of these editors can introduce extra characters causing the file format to be invalid.

Windows Autopilot for existing devices doesn't follow the Autopilot OOB experience

Ensure that the JSON profile file is saved in **ANSI/ASCII** format, not Unicode or UTF-8.

Something went wrong is displayed page during OOB

The client is likely unable to access all the required Microsoft Entra ID/MSA-related URLs. For more information, see [Networking requirements](#).

Using a provisioning package in combination with Windows Autopilot can cause issues, especially if the

PPKG contains join, enrollment, or device name information

Using PPKGs in combination with Windows Autopilot isn't recommended.

Related content

- [Collect MDM logs.](#)
 - [Troubleshooting Windows Autopilot overview.](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot support information

Article • 08/02/2024 • Applies to: Windows 11, Windows 10

The following table displays support information for the Windows Autopilot program.

Before contacting the following resources listed for Windows Autopilot-related issues, check the [Windows Autopilot FAQ](#) and [Windows Autopilot troubleshooting FAQ](#).

[+] Expand table

Audience	Support contact
OEM or Channel Partner registering devices as a Cloud Solution Partner (CSP) via Microsoft Partner Center	Use the help resources available in the Microsoft Partner Center. CSPs registering Autopilot devices through Microsoft Partner Center, either manually or through the Microsoft Partner Center API, the first option for support should be the Microsoft Partner Center Help resources https://partner.microsoft.com within Microsoft Partner Center. This support policy is true for both named partners and channel partners (distributor, reseller, SI, etc.)
OEM registering/deregistration devices using OEM Direct API	Contact the msoemops support alias. Response time depends on priority: Low - 120 hours Normal - 72 hours High - 24 hours Immediate - 4 hours The msoemops support alias is only accessible and available for OEMs who are using OEM Direct API for Windows Autopilot service.
Enterprise customers (Company IT Administrator)	Contact the Technical Account Manager (TAM), Account Technology Strategist (ATS), or Customer Service Support (CSS) representative.
End-user	Contact the IT administrator or the Channel Partner/OEM.
Microsoft Partner Center users	Use the help resources available in Microsoft Partner Center.
Intune users (IT Admin)	From the Microsoft Intune admin center , select Help and support .
Microsoft 365 Business Premium	Support is accessible directly through the Microsoft 365 Business Premium portal when logged in: https://support.microsoft.com/ .
Queries relating to MDA testing	Contact MDAHelp@microsoft.com .

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows Autopilot customer consent

Article • 06/28/2024 • Applies to:  Windows 11,  Windows 10

This article describes how a cloud service provider (CSP) partner (direct bill, indirect provider, or indirect reseller) or an OEM can get customer authorization to register Windows Autopilot devices on the customer's behalf.

CSP authorization

CSP partners can get customer authorization to register Windows Autopilot devices on the customer's behalf per the following restrictions:

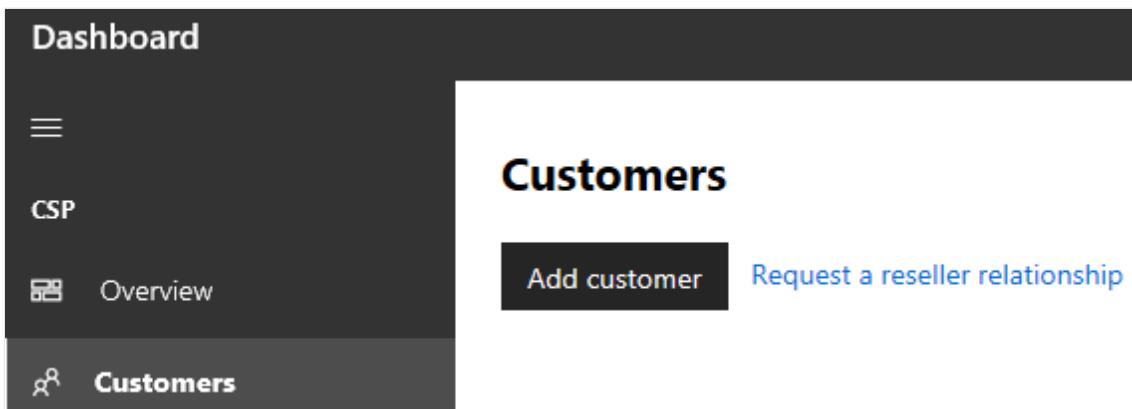
 Expand table

Method	Description
Direct CSP	Gets direct authorization from the customer to register devices.
Indirect CSP Provider	Gets implicit permission to register devices through the relationship their CSP Reseller partner has with the customer. Indirect CSP Providers register devices through Microsoft Partner Center.
Indirect CSP Reseller	Gets direct authorization from the customer to register devices. At the same time, their indirect CSP Provider partner also gets authorization, which means that either the Indirect Provider or the Indirect Reseller can register devices for the customer. However, the Indirect CSP Reseller must register devices through the Microsoft Partner Center UI (manually uploading CSV file). The Indirect CSP Provider can register devices using the Microsoft Partner Center APIs.

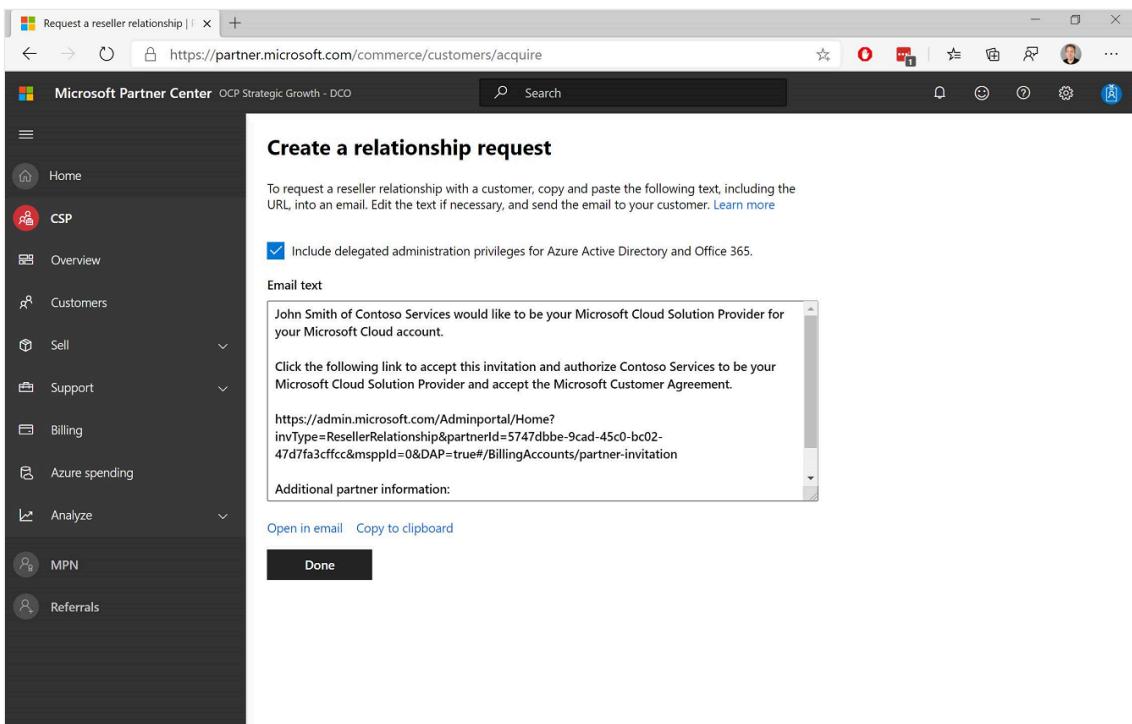
Steps

For a CSP to register Windows Autopilot devices for a customer, the customer must first grant that CSP partner permission using the following process:

1. CSP sends link to customer requesting authorization/consent to register/manage devices on their behalf. To do so:
 - a. CSP logs into Microsoft Partner Center.
 - b. Select **Dashboard** on the top menu.
 - c. Select **Customer** on the side menu.
 - d. Select the **Request a reseller relationship** link:



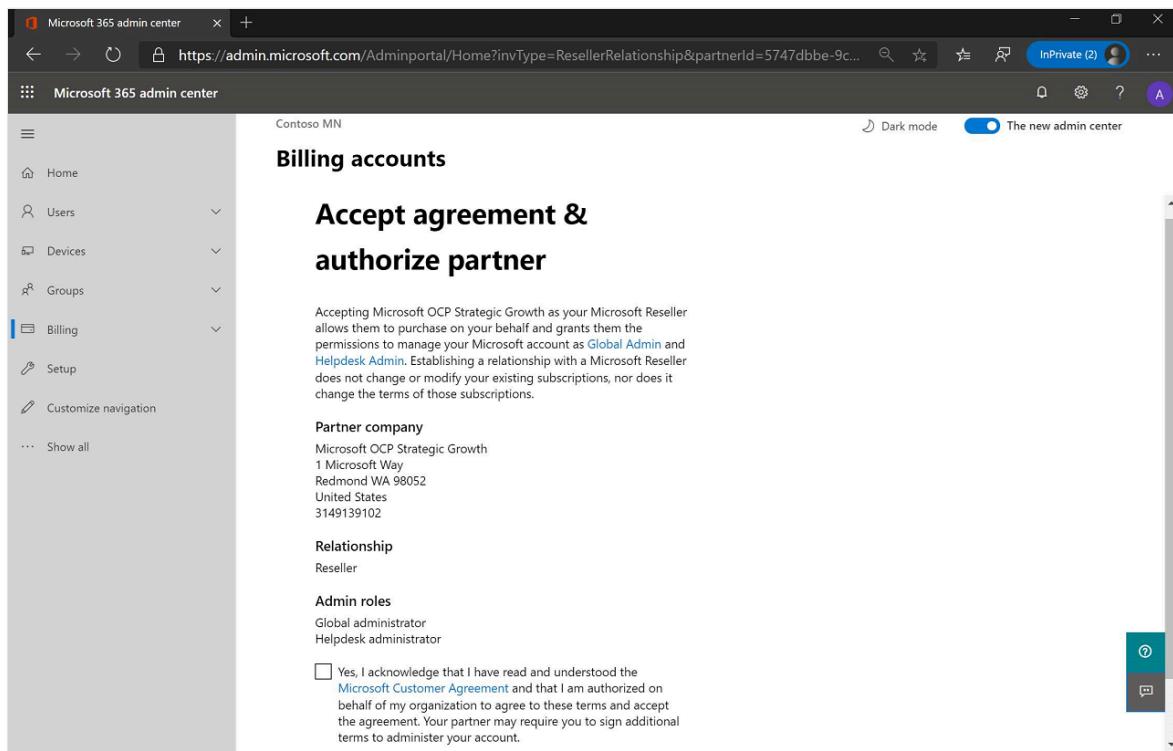
- e. Select the checkbox indicating if delegated admin rights are desired:



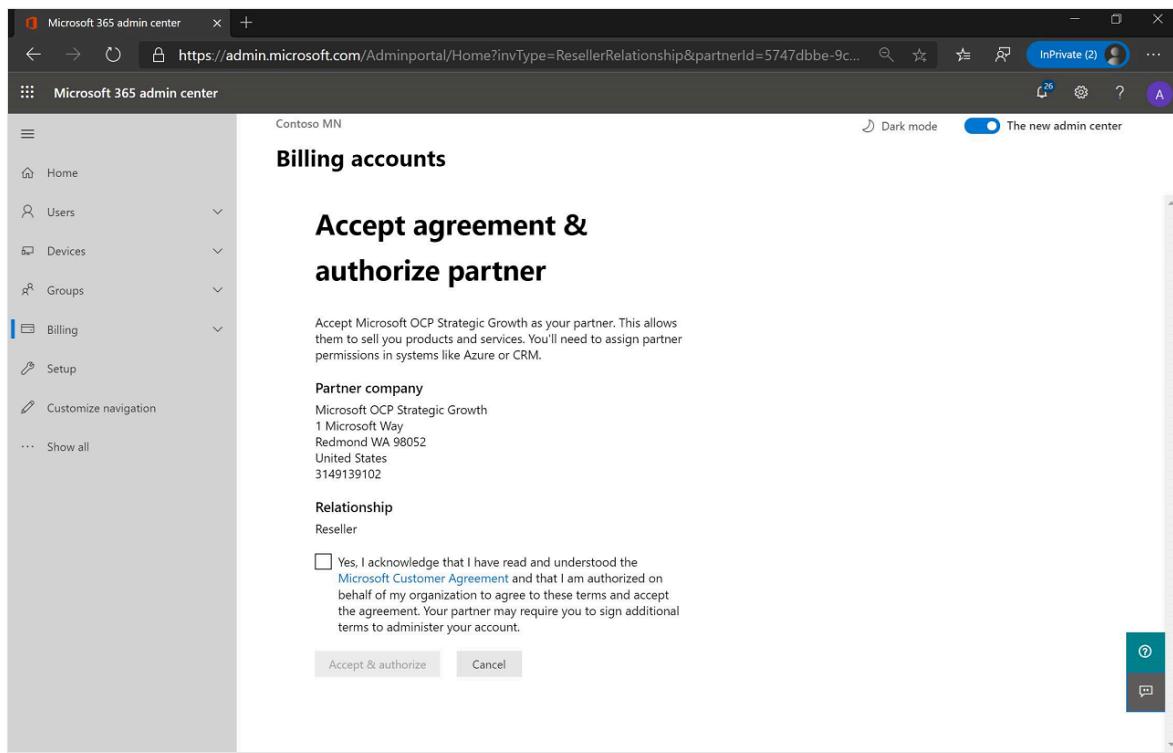
ⓘ Note

Depending on the partner, they might request Delegated Admin Permissions (DAP) when requesting this consent. If possible, it's better to use the newer DAP-free process (shown in this document). If not, their DAP status can be easily removed from the [Microsoft 365 admin center](#). For more information, see [Obtain permissions to manage a customer's service or subscription](#).

- f. Send the template in the previous step to the customer via email.
2. Customer with Microsoft Admin Center global administrator privileges selects the link in email. The link takes them to the following [Microsoft 365 admin center](#) page:

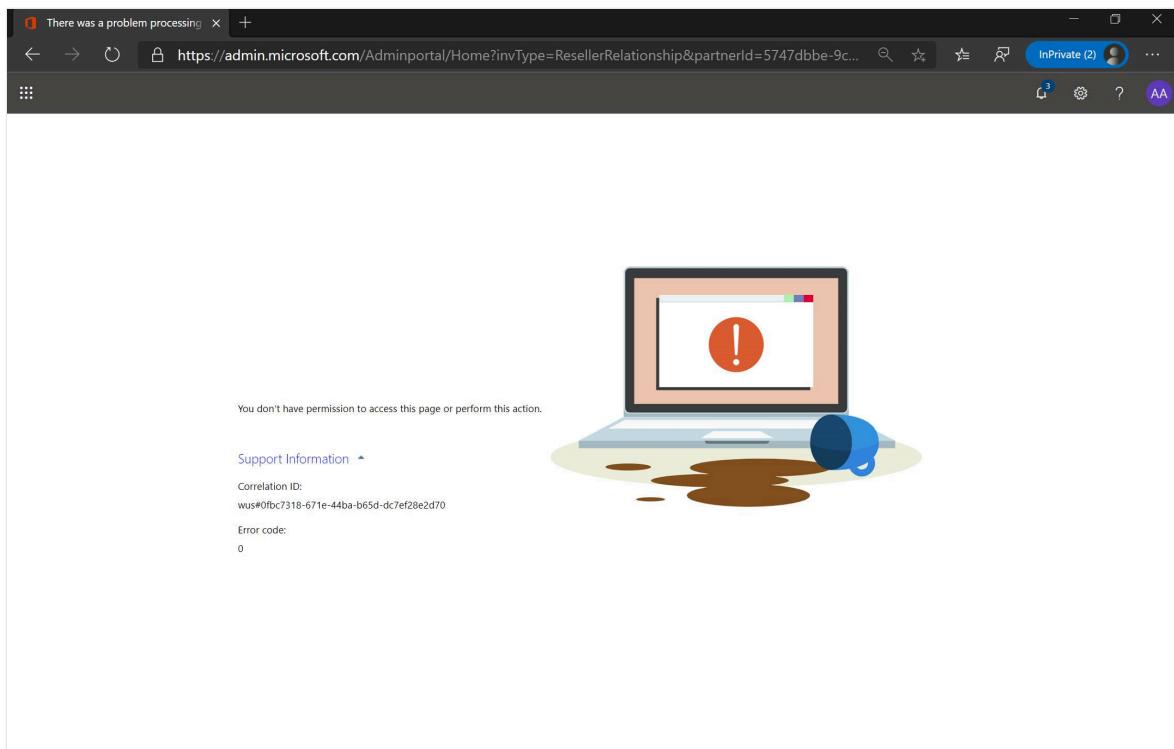


The above image is what the customer sees if they requested delegated admin rights (DAP). The page says what Admin roles are being requested. If the customer didn't request delegated admin rights, they would see the following page:



⚠ Note

A user without global administrator privileges who selects the link sees a message similar to the following message:



3. Customer selects the **Yes** checkbox, followed by the **Accept** button. Authorization happens instantaneously.
4. To check that the authorization request is complete, the CSP can check the **Customers** list in their Microsoft Partner Center account. If the customer is in the list, the request is complete. For example:

(i) Important

Microsoft recommends using roles with the fewest permissions. Using lower permissioned accounts helps improve security for an organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when an existing role can't be used.

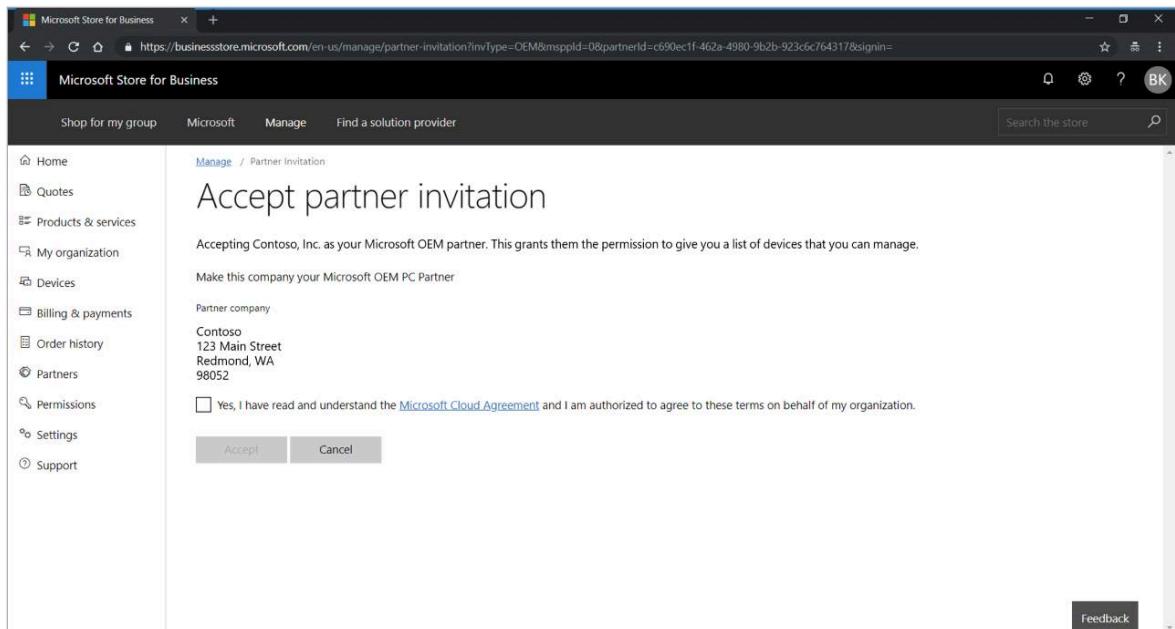
OEM authorization

OEM authorization is only available for those OEMs who are eligible to use OEM Direct API for Windows Autopilot registration and deregistration.

OEMs who are eligible of using Direct API solution have a unique link to provide to their respective customers, which the OEM can request from Microsoft via the **msoemops**

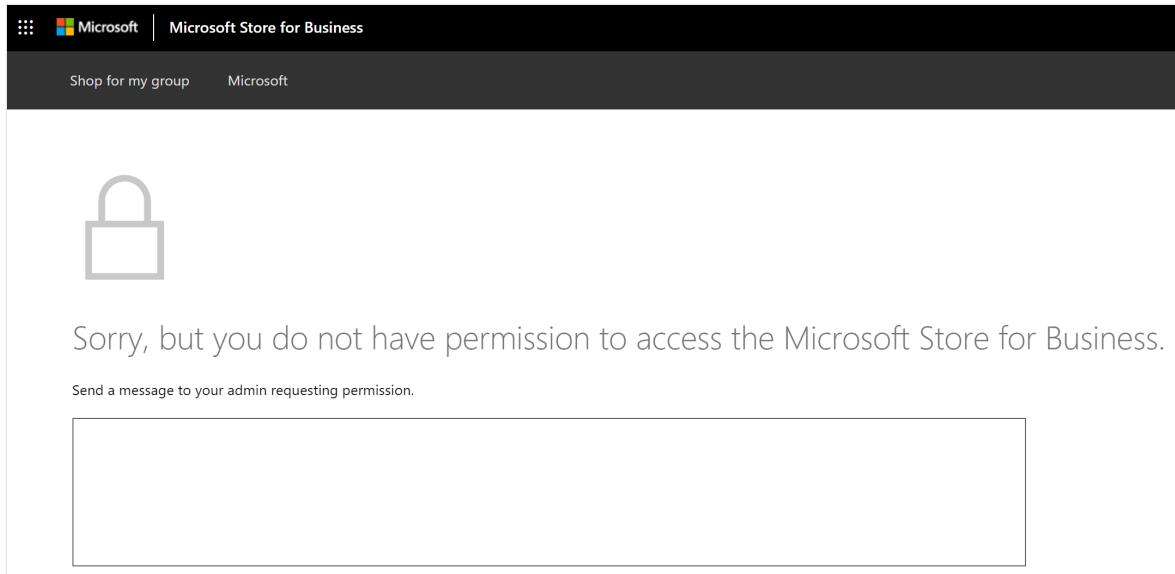
support alias. Contact the organization's account manager to obtain this support alias.

1. OEM emails link to their customer.
2. Customer signs into the [Microsoft 365 admin center](#) using a cloud-native account (for example, [domain].onmicrosoft.com) with global administrator privileges.
3. Customer selects the link in the email, which takes them directly to the following page:



ⓘ Note

A user without global admin privileges who selects the link sees a message similar to the following message:



4. Customer selects the Yes checkbox, followed by the Accept button, and they're done. Authorization happens instantaneously.

(!) Note

Once this process is completed, it isn't currently possible for an administrator to remove an OEM. To remove an OEM or revoke their permissions, send a request to msoemops@microsoft.com

5. The OEM can use the Validate Device Submission Data API to verify the consent is completed.

(!) Note

This API is discussed in the latest version of the [API Whitepaper, p. 14ff](#). This link is only accessible by Microsoft Device Partners. As discussed in this article, it's a best practice recommendation for OEM partners to run the API check to confirm customer consent is received before attempting to register devices. This check can help avoid errors in the registration process.

(!) Note

During the OEM authorization registration process, no delegated admin permissions are granted to the OEM.

Summary

At this stage of the process, Microsoft is no longer involved. The consent exchange happens directly between the OEM and the customer. It all also happens instantaneously - as quickly as buttons are selected.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Windows Autopilot device guidelines

Article • 06/11/2024 • Applies to: Windows 11, Windows 10, Windows Holographic

Hardware and firmware best practice guidelines for Windows Autopilot

All devices using Windows Autopilot should meet the minimum hardware requirements for Windows. For more information, see:

- [Find Windows 11 specs, features, and computer requirements ↗](#).
- [How to Find Windows 10 Computer Specifications & Systems Requirements ↗](#).
- [Windows minimum hardware requirements](#).
- [Windows 11 requirements](#).

The following best practices ensure that devices can easily be provisioned as part of the Windows Autopilot deployment process:

- TPM 2.0 is enabled and in a good state on devices intended for Windows Autopilot self-deploying mode. The TPM shouldn't be in the **Reduced Functionality Mode** state.
- The OEM should provision either of the following information into the [SMBIOS fields](#). The information should follow Microsoft specifications (Manufacturer, Product Name, and Serial Number stored in SMBIOS Type 1 04h, Type 1 05h, and Type 1 07h).
 - Unique tuple info (SmbiosSystemManufacturer, SmbiosSystemProductName, SmbiosSystemSerialNumber)
 - PKID + SmbiosSystemSerialNumber
- Before an OEM ships devices to an Autopilot customer or channel partner, they should upload 4K Hardware Hashes to Microsoft by using the CBR report. The hashes should be collected using the OA3 Tool RS3+ run in Audit mode on full OS.
- Microsoft requires that OEM shipping drivers get published to Windows Update within 30 days of the CBR submission date. System firmware and driver updates are published to Windows Update within 14 days.
- The OEM ensures that the PKID provisioned in the SMBIOS is passed on to the channel.

- When using a VM for Autopilot testing, assign at least 2 processors and 4gb of memory.

Software best practice guidelines for Windows Autopilot

- The Windows Autopilot device should be preinstalled with only a Windows base image plus drivers.
- Licensed versions of Office, such as [Microsoft 365 Apps for enterprise](#), can be preinstalled.
- Unless explicitly requested by the customer, no other preinstalled software should be included.
 - Per OEM Policy, Windows features, including built-in apps, shouldn't be disabled or removed.

Related content

- [Windows Autopilot customer consent](#).
- [Motherboard replacement scenario guidance](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Autopilot motherboard replacement scenario guidance

Article • 06/19/2024 • Applies to: Windows 11, Windows 10

This document offers guidance for Windows Autopilot device repair scenarios that Microsoft partners can use in motherboard replacement situations, and other servicing scenarios.

Repairing Autopilot enrolled devices is complex, as it tries to balance OEM requirements with Windows Autopilot requirements. Specifically, OEM requirements include strict uniqueness across motherboards, MAC addresses, etc. Windows Autopilot requires strict uniqueness at the hardware hash level for each device to enable successful registration. The hardware hash doesn't always accommodate all the OEM hardware component requirements. These requirements are sometimes at odds, which can cause issues with some repair scenarios. The hardware hash is also known as the hardware ID.

If a motherboard is replaced on an Autopilot registered device, then the following process is recommended:

1. [Deregister the device from Windows Autopilot](#).
2. [Replace the motherboard](#).
3. [Capture the new device ID \(4K HH\)](#).
4. [Reregister the device with Windows Autopilot](#).
5. [Reset the device](#).
6. [Return the device](#).

Each of these steps is described in the following sections.

Deregister the Autopilot device from the Autopilot program

Before the device arrives at the repair facility, the entity that registered the device must deregister it.

- If the IT Admin registered the device, they likely did so via Intune, [Microsoft 365 admin center](#), or a legacy portal such as Microsoft Store for Business (MSfB). If so, they should deregister the device from Intune or the [Microsoft 365 admin](#)

[center](#) because devices registered in Intune don't show up in Microsoft Partner Center (MPC).

- If the **OEM or CSP partner** registered the device, they likely did so via the Microsoft Partner Center (MPC). In that case, they should deregister the device from MPC, which also removes it from the customer IT Admin's Intune account.

The below steps describe what an IT Admin would go through to deregister a device from Intune and the steps an OEM or CSP would go through to deregister a device from MPC.

To avoid problems, an OEM or CSP should register Autopilot devices whenever possible. If the customer registers the devices, OEMs or CSPs can't deregister them if, for example, a customer leasing a device goes out of business before deregistering it themselves.

If a customer grants an OEM permission to register devices on their behalf using the automated consent process, an OEM can use the API to deregister devices they didn't register themselves. This deregistration only removes those devices from the Autopilot program. It doesn't unenroll them from Intune or disjoin them from Microsoft Entra ID. Only the customer can unenroll the device from Intune or disjoin the device from Microsoft Entra ID.

Deregister a device

Whenever a device permanently leaves an organization, the device should always be deregistered from Autopilot. For example, the device leaves the organization for repair or because the device is at the end of its life cycle.

Below we describe the steps an admin would go through to deregister a device from Intune and Autopilot.

Delete from Intune

Before a device is deregistered from Autopilot, it first has to be deleted from Intune. To delete an Autopilot device from Intune:

1. Sign in to the [Microsoft Intune admin center](#).
2. In the **Home** screen, select **Devices** in the left pane.
3. In the **Devices | Overview** screen, under **By platform**, select **Windows**.

4. Under **Device name**, find the device that needs to be deleted and then select the device. If necessary, use the **Search** box.
5. In the properties screen for the device, make a note of the serial number listed under **Serial number**.
6. After making a note of the serial number of the device, select **Delete** in the toolbar at the top of the page.
7. A warning dialog box appears to confirm the deletion of the device from Intune. Select **Yes** to confirm deleting the device.

Deregister from Autopilot using Intune

Once the device is deleted from Intune, it can then be deregistered from Autopilot. To deregister a device from Autopilot:

1. Make sure the device is deleted from Intune as described in the [Delete from Intune](#) section.
2. Sign in to the [Microsoft Intune admin center](#).
3. In the **Home** screen, select **Devices** in the left pane.
4. In the **Devices | Overview** screen, under **By platform**, select **Windows**.
5. In the **Windows | Windows enrollment** screen, select **Windows enrollment**.
6. In the **Windows | Windows enrollment** screen, under **Windows Autopilot**, select **Devices**.
7. In the **Windows Autopilot devices** screen that opens, under **Serial number**, find the device that needs to be deregistered by its serial number as determined in the [Delete from Intune](#) section. If necessary, use the **Search by serial number** box.
8. Select the device by selecting the checkbox next to the device.
9. Select the extended menu icon (...) on the far right end of the line containing the device. A menu appears with the option **Unassign user**.
 - If the **Unassign user** option is available and not greyed out, then select it. A warning dialog box appears confirming to unassign the user from the device. Select **OK** to confirm unassigning the device from the user.
 - If the **Unassign user** option isn't available and greyed out, then move on to the next step.

10. With the device still selected, select **Delete** in the toolbar at the top of the page.
11. A warning dialog box appears to confirm the deletion of the device from Autopilot. Select **Yes** to confirm deleting the device.
12. The deregistration process might take some time. The process can be accelerated by selecting the **Sync** button in the toolbar at the top of the page.
13. Every few minutes select **Refresh** in the toolbar at the top of the page until the device is no longer present.

ⓘ Important

- For Microsoft Entra join devices, no additional steps are necessary to remove the device from Intune and Autopilot. Unneeded steps include manually deleting the device from Microsoft Entra ID. Manually deleting the device from Microsoft Entra ID might cause unexpected problems, issues, and behavior. If needed, the device will be automatically removed from Microsoft Entra ID after these steps are followed.
- For Microsoft Entra hybrid join devices, delete the computer object from the on-premises Active Directory Domain Services (AD DS) environment. Deleting the computer object from the on-premises AD DS ensures that the computer object isn't resynced back to Microsoft Entra ID. After the computer object is deleted from the on-premises AD DS environment, no additional steps are necessary to remove the device from Intune and Autopilot. Unneeded steps include manually deleting the device from Microsoft Entra ID. Manually deleting the device from Microsoft Entra ID might cause unexpected problems, issues, and behavior. If needed, the device will be automatically removed from Microsoft Entra ID after these steps are followed.

The above steps deregister the device from Autopilot, unenroll the device from Intune, and disjoin the device from Microsoft Entra ID. It might appear that only deregistering the device from Autopilot is needed. However, there are barriers in Intune that require all the above steps to avoid problems with lost or unrecoverable devices. To prevent the possibility of orphaned devices in the Autopilot database, Intune, or Microsoft Entra ID, it's best to complete all the steps. If a device gets into an unrecoverable state, contact the appropriate [Microsoft support alias](#) for assistance.

Deregister from Autopilot using Microsoft 365 admin center

The device can be deregistered from Autopilot in [Microsoft 365 admin center](#) if using the Microsoft 365 admin center instead of Intune. To deregister an Autopilot device from the Microsoft 365 admin center:

1. Sign into to the [Microsoft 365 admin center](#).
2. Navigate to **Devices > Autopilot**.
3. Select the device to be deregistered and then select **Delete device**.

Deregister from Autopilot in Microsoft Partner Center (MPC)

To deregister an Autopilot device from the Microsoft Partner Center (MPC), a Cloud Solution Partner (CSP) would:

1. Sign into the Microsoft Partner Center (MPC).
2. Navigate to **Customer > Devices**.
3. Select the device to be deregistered and then select **Delete device**.

The screenshot shows the Microsoft Partner Center (MPC) interface. On the left, there's a sidebar with links like Order history, Subscriptions, Software, Azure reservations, and a Devices section containing Analytics, Users and licenses, Service management, and Account. The main content area is titled "Devices" and has a sub-section "Windows AutoPilot profiles". It features a "Add new profile" button and a message stating "There are no profiles." Below this is another section titled "Apply profiles to devices" with a "Add devices" button. At the bottom, there are buttons for "Apply profile", "Remove profile", and "Delete device". The "Delete device" button is highlighted with a red box. There's also a "Group name" field with "BKTestGroup1" and a checked checkbox.

Partners deregistering a device from Autopilot in Microsoft Partner Center (MPC) only deregisters the device from Autopilot. It doesn't perform any of the following actions:

- Unenroll the device from the mobile device management (MDM) solution, such as Intune.
- Disjoin the device from Microsoft Entra ID.

For these reasons, the OEM or CSP should work with the customer IT administrators to have the device fully removed by following the steps in the [Deregister a device](#) section.

An OEM or CSP with integrated OEM Direct APIs can also deregister a device with the **AutopilotDeviceRegistration** API. Make sure the **TenantID** and **TenantDomain** fields are left blank.

 **Note**

If an admin registered a device via another portal other than the Microsoft Partner Center (MPC) such as Intune or the [Microsoft 365 admin center](#), the device doesn't show up in Microsoft Partner Center (MPC). For a partner to register a device in the Microsoft Partner Center (MPC), the device first needs to be deregistered using the steps outlined in the [Deregister a device](#) section.

Because the repair facility doesn't have the user's sign-in credentials, they have to reimagine the device as part of the repair process. The customer should do three things before sending the device to the facility:

1. Copy all important data off the device.
2. Let the repair facility know which version of Windows they should reinstall after the repair.
3. If applicable, let the repair facility know which version of Office they should reinstall after the repair.

Replace the motherboard

Technicians replace the motherboard or other hardware on the broken device. A replacement Digital Product Key (DPK) is injected.

Repair and key replacement processes vary between facilities. Sometimes repair facilities receive motherboard spare parts from OEMs that have replacement DPKs already injected, but sometimes not. Sometimes repair facilities receive fully functional BIOS tools from OEMs, but sometimes not. The quality of the data in the BIOS after a motherboard replacement varies. To ensure the repaired device are still Autopilot capable following its repair, check to make sure the new post-repair BIOS can successfully gather and populate the following information at a minimum:

- DiskSerialNumber.
- SmbiosSystemSerialNumber.
- SmbiosSystemManufacturer.
- SmbiosSystemProductName.
- SmbiosUuid.
- TPM EKPub.
- MacAddress.
- ProductKeyID.
- OSType.

For simplicity, and because processes vary between repair facilities, additional steps often used in a motherboard replacement are excluded, such as:

- Verify that the device is still functional.
- Disable or suspend BitLocker.
- Repair the Boot Configuration Data (BCD).
- Repair and verify the network driver operation.

Capture a new Autopilot device ID (4K HH) from the device

Repair technicians must sign in to the repaired device to capture the new device ID. If the repair technician doesn't have access to the customer's sign-in credentials, they have to reimagine the device to gain access:

1. The repair technician creates a [WinPE bootable USB drive](#).
2. The repair technician boots the device to WinPE.
3. The repair technician [applies a new Windows image to the device](#).

Ideally, the same Windows version that was originally on the device should be reimaged onto the device. Some coordination is required between the repair facility and customer to capture this information at the time the device arrives for repair. Such coordination might include the customer sending the repair facility a customized image (.ppk file) via a USB stick, for example.

4. The repair technician boots the device into the new Windows image.
5. Once on the desktop, the repair technician captures the new device ID (4K HH) off the device using either the OA3 Tool or the PowerShell script.

Those repair facilities with access to the OA3 Tool (which is part of the ADK) can use the tool to capture the 4K Hardware Hash (4K HH).

Instead, the [WindowsAutopilotInfo PowerShell script](#) can be used to capture the 4K HH.

 **Note**

Other methods in addition to Windows PowerShell are also available to capture the hardware hash. For more information, see [Collect the hardware hash](#).

To use the WindowsAutopilotInfo PowerShell script, follow these steps:

1. Install the script from the [PowerShell Gallery](#) or from the command line.
2. Navigate to the script directory and run it on the device when the device is either in Full OS or Audit Mode. See the following example.

```
PowerShell

md c:\HWID
Set-Location c:\HWID
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted -Force
Install-Script -Name Get-WindowsAutopilotInfo -Force
Get-WindowsAutopilotInfo.ps1 -OutputFile AutopilotHWID.csv
```

- If prompted to install the NuGet package, select Yes.
- If after installing the script an error occurs reporting that `Get-WindowsAutopilotInfo.ps1` isn't found, verify that `C:\Program Files\WindowsPowerShell\Scripts` is present in the `PATH` variable.
- If the `Install-Script` cmdlet fails, verify that the default PowerShell repository is registered with the following command:

```
PowerShell

Get-PSRepository
```

If the default PowerShell repository isn't registered, register it with the following command:

```
PowerShell

Register-PSRepository -Default -Verbose
```

ⓘ Note

The `Get-WindowsAutopilotInfo` script was updated in July of 2023 to use the Microsoft Graph PowerShell modules instead of the deprecated AzureAD Graph PowerShell modules. Make sure to use the latest version of the script. The Microsoft Graph PowerShell modules might require approval of additional permissions in Microsoft Entra ID when they're first used. For more information, see [AzureAD](#) and [Important: Azure AD Graph Retirement and PowerShell Module Deprecation ↗](#).

The script creates a `.csv` file that contains the device information, including the complete 4K HH. Save this file so that it can be accessed later. The service facility uses this 4K HH to reregister device as described in the following sections. Be sure to use the `-OutputFile` parameter when saving the file, which ensures that file formatting is correct. Don't attempt to pipe the command output to a file manually.

ⓘ Note

If the repair facility can't run the OA3 tool or PowerShell script to capture the new 4K HH, then the OEM or CSP partners must do it for them. Without some entity capturing the new 4K HH, there's no way to reregister this device as an Autopilot device.

Reregister the repaired device using the new device ID

If an OEM can't reregister the device, there are two options:

- The repair facility or CSP can reregister the device using MPC.
- The customer IT Admin should reregister the device via Intune (or MSfB).

Both ways of reregistering a device are shown in the following sections.

Reregister from Intune

To reregister an Autopilot device from Intune, an IT Admin would:

1. Sign into the [Microsoft Intune admin center ↗](#).

2. Navigate to Devices > Device onboarding | Enrollment > Windows Autopilot | Devices.
3. Select the **Import** option in the toolbar at the top to upload a CSV file containing the device ID of the device to be reregistered. The device ID was the 4K HH captured by the PowerShell script or OA3 tool described in the section [Capture a new Autopilot device ID \(4K HH\) from the device](#).

Reregister from the Microsoft Partner Center (MPC)

To reregister an Autopilot device from the Microsoft Partner Center MPC, an OEM or CSP would:

1. Sign in to the Microsoft Partner Center (MPC).
2. Navigate to the Customer > Devices page.
3. Select **Add devices** to upload the CSV file.

When a repaired device is reregistering through MPC, the uploaded CSV file must contain the 4K HH for the device, and not just the PKID or Tuple (SerialNumber + OEMName + ModelName). If only the PKID or Tuple was used, the Autopilot service would be unable to find a match in the Autopilot database. No match would be found because no 4K HH info was previously submitted for this essentially "new" device and the upload fails, likely returning a **ZtdDeviceNotFound** error. For this reason, only upload the 4K HH. Don't upload the Tuple or PKID.

When including the 4K HH in the CSV file, the PKID or Tuple don't also need to be included. Those columns might be left blank, as shown in the following example:

	A	B	C	D	E
1	Device Serial Number	Windows Product ID	Hardware Hash	Manufacturer name	Device model
2			T0HLAQEAHAAAAAAoAAQDuQgAACgD+....		

Reset the device

The repair facility must reset the image back to a pre-OOBE state before returning it to the customer. This reset is needed because the device was required to be in Full OS or Audit Mode to capture the 4K HH. One way to reset the image is by using the built-in reset feature in Windows.

To use the reset feature in Windows on a device:

Windows 10:

1. Go to **Settings > Update & Security > Recovery**.
2. Select **Get started**.
3. In the **Reset this PC** window:
 - a. Under **Choose an option**, select **Remove everything**.
 - b. Under **How would you like to reinstall Windows?**, select either option.
 - c. Under **Additional settings**, select **Next**.
 - d. Under **Ready to reset this PC**, select the **Reset** button.

Windows 11:

1. Go to **Settings > System > Recovery**.
2. Under **Recovery options**, select the **Reset PC** button next to **Reset this PC**.
3. In the **Reset this PC** window:
 - a. Under **Choose an option**, select **Remove everything**.
 - b. Under **How would you like to reinstall Windows?**, select either option.
 - c. Under **Additional settings**, select **Next**.
 - d. Under **Ready to reset this PC**, select the **Reset** button.

However, the repair facility most likely doesn't have access to Windows because they lack the user credentials to sign in. In this case, they need to use other means to reimagine the device, such as the Deployment Image Servicing and Management (DISM) tool:

- OEM Deployment of Windows 11 desktop editions.
- OEM Deployment of Windows 10 for desktop editions.

Return the repaired device to the customer

The repaired device can now be returned to the customer. The device is auto-enrolled into the Autopilot program on first boot-up during OOOE.

 **Important**

If the repair facility **didn't** reimagine the device, they could be sending it back in a potentially broken state. For example, there's no way to log into the device because it's dissociated from the only known user account.

A device can be **registered** for Autopilot before being powered-on. However, the device isn't actually **deployed** to Autopilot until it goes through OOB. Therefore, resetting the device back to a pre-OOB state is a required step.

Fix pending and Attention required

If the profiles status of a device shows **Fix pending**, Autopilot is in the process of attempting to register the device. If the profile status of a device shows **Fix pending** for an extended period of time and doesn't switch to **Assigned**, or if the profile status of the device switches to **Attention required**, then:

1. Manually deregister the device using the steps in the [Deregister a device](#) section.
2. Reregister the device.

For more information, see [Troubleshoot Autopilot device import and enrollment: Autopilot profile not applied after reimaging to an older OS version](#).

Specific repair scenarios

This section covers the most common repair scenarios, and their impact on Autopilot enablement.

Note

- The scenarios were tested using Intune only. No other MDMs were tested.
- In most test scenarios, the repaired and reregistered device needed to go through OOB again for Autopilot to be enabled.
- Motherboard replacement scenarios often result in lost data. Repair centers or customers should be reminded to back up data before repair.
- When a repair facility can't write device info into the BIOS of the repaired device, new processes need to be created to successfully enable Autopilot.
- Repaired device should have the Product Key (DPK) pre-injected in the BIOS before capturing the new 4K HH (device ID).

For the **Supported** column in the following table:

- **Yes:** the device can be reenabled for Autopilot.
- **No:** the device can't be reenabled for Autopilot.

[Expand table](#)

Scenario	Supported	Microsoft Recommendation
Motherboard Replacement in general	Yes	<p>The recommended course of action for motherboard replacement scenarios is:</p> <ol style="list-style-type: none"> Autopilot device is deregistered from the Autopilot program. The motherboard is replaced. The device is reimaged (with BIOS info and DPK reinjected).¹ A new Autopilot device ID (4K HH) is captured off the device. The repaired device is reregistered for the Autopilot program using the new device ID. The repaired device is reset to boot to OOBE. The repaired device is shipped back to the customer. <p>¹ It's not necessary to reimagine the device if the repair technician has access to the customer's sign-in credentials. It's technically possible to successfully re-enable motherboard replacement and Autopilot without keys or certain BIOS info (serial #, model name, etc.) However, doing so is only recommended for testing/educational purposes.</p>
Motherboard replacement when motherboard has a TPM chip enabled and only one onboard network card that also gets replaced	Yes	<ol style="list-style-type: none"> Deregister damaged device. Replace motherboard. To gain access, reimagine device or sign-in using customer's credentials. Write device info into BIOS. Capture new 4K HH. Reregister repaired device. Reset device back to OOBE. Go through Autopilot OOBE (customer). Autopilot successfully enabled.
Motherboard replacement when motherboard has an enabled TPM chip enabled and a second network interface that	No	<p>This scenario breaks the Autopilot experience. The resulting Device ID won't be stable until after TPM attestation is complete. Even then registration might give incorrect results because of ambiguity with MAC Address resolution. Therefore, this scenario isn't recommended.</p>

Scenario	Supported	Microsoft Recommendation
isn't replaced along with the motherboard		
Motherboard replacement where the NIC card, HDD, and WLAN all remain the same after the repair	Yes	<ol style="list-style-type: none"> 1. Deregister damaged device. 2. Replace motherboard with a new Replacement Digital Product Key (RDPK) preinjected in BIOS. 3. To gain access, reimagine device or sign-in using customer's credentials. 4. Write old device info into BIOS (same s/n, model, etc.) ² 5. Capture new 4K HH. 6. Reregister repaired device. 7. Reset device back to OOBE. 8. Go through Autopilot OOBE (customer). 9. Autopilot successfully enabled.
		<p>² For this and later scenarios, rewriting old device info wouldn't include the TPM 2.0 endorsement key, as the associated private key is locked to the TPM device.</p>
Motherboard replacement where the NIC card remains the same, but the HDD and WLAN are replaced	Yes	<ol style="list-style-type: none"> 1. Deregister damaged device. 2. Replace motherboard (with new RDPK preinjected in BIOS). 3. Insert new HDD and WLAN. 4. Write old device info into BIOS (same s/n, model, etc.) 5. Capture new 4K HH. 6. Reregister repaired device. 7. Reset device back to OOBE. 8. Go through Autopilot OOBE (customer). 9. Autopilot successfully enabled.
Motherboard replacement where the NIC card and WLAN remains the same, but the HDD is replaced	Yes	<ol style="list-style-type: none"> 1. Deregister damaged device. 2. Replace motherboard (with new RDPK preinjected in BIOS). 3. Insert new HDD. 4. Write old device info into BIOS (same s/n, model, etc.) 5. Capture new 4K HH. 6. Reregister repaired device. 7. Reset device back to OOBE. 8. Go through Autopilot OOBE (customer). 9. Autopilot successfully enabled.
Motherboard replacement where only	Yes	<ol style="list-style-type: none"> 1. Deregister damaged device. 2. Replace motherboard (with new RDPK

Scenario	Supported	Microsoft Recommendation
the motherboard is replaced. All other parts remain same. The new motherboard was taken from a previously used device that has never been enabled for Autopilot.		<p>preinjected in BIOS).</p> <ol style="list-style-type: none"> 3. To gain access, reimagine device or sign-in using customer's credentials. 4. Write old device info into BIOS (same s/n, model, etc.) 5. Capture new 4K HH. 6. Reregister repaired device. 7. Reset device back to OOB. 8. Go through Autopilot OOB (customer). 9. Autopilot successfully enabled.
Motherboard replacement where only the motherboard is replaced. All other parts remain same. The new motherboard was taken from a previously used device that has been Autopilot-enabled before.	Yes	<ol style="list-style-type: none"> 1. Deregister old device which motherboard is taken from. 2. Deregister damaged device that needs to be repaired. 3. Replace motherboard in repair device with motherboard from other Autopilot device (with new RDPK preinjected in BIOS). 4. To gain access, reimagine device or sign-in using customer's credentials. 5. Write old device info into BIOS (same s/n, model, etc.) 6. Capture new 4K HH. 7. Reregister repaired device. 8. Reset device back to OOB. 9. Go through Autopilot OOB (customer). 10. Autopilot successfully enabled. <p>The repaired device can also be used successfully as a normal, non-Autopilot device.</p>
BIOS info excluded from motherboard replacement device	No	<p>Repair facility doesn't have BIOS tool to write device info into BIOS after Motherboard replacement.</p> <ol style="list-style-type: none"> 1. Deregister damaged device. 2. Replace motherboard (BIOS does NOT contain device info). 3. Reimage and write DPK into image. 4. Capture new 4K HH. 5. Reregister repaired device. 6. Create Autopilot profile for device. 7. Go through Autopilot OOB (customer). 8. Autopilot FAILS to recognize repaired device.
Motherboard replacement when there's no TPM	Yes	<p>Enabling Autopilot devices without a TPM isn't recommended. However, it's possible to enable an Autopilot device that doesn't have a TPM via</p>

Scenario	Supported	Microsoft Recommendation
		<p>user-driven mode. Pre-provision and self-deploying modes aren't supported without a TPM. When using user-driven mode:</p> <ol style="list-style-type: none"> 1. Deregister damaged device. 2. Replace motherboard. 3. To gain access, reimagine device or sign-in using customer's credentials. 4. Write old device info into BIOS (same s/n, model, etc.) 5. Capture new 4K HH. 6. Reregister repaired device. 7. Reset device back to OOB. 8. Go through Autopilot OOB (customer). 9. Autopilot successfully enabled.
New DPK written into image on repaired Autopilot device with a new motherboard	Yes	<p>Repair facility replaces normal motherboard on damaged device. motherboard doesn't contain any DPK in the BIOS. Repair facility writes DPK into image after motherboard replacement.</p> <ol style="list-style-type: none"> 1. Deregister damaged device. 2. Replace motherboard - BIOS does NOT contain DPK info. 3. To gain access, reimagine device or sign-in using customer's credentials. 4. Write device info into BIOS (same s/n, model, etc.) 5. Capture new 4K HH. 6. Reset or reimagine device to pre-OOB and write DPK into image. 7. Reregister repaired device. 8. Go through Autopilot OOB. 9. Autopilot successfully enabled.
New Repair Product Key (RDPK)	Yes	<p>Using a motherboard with a new RDPK preinjected results in a successful Autopilot refurbishment scenario.</p> <ol style="list-style-type: none"> 1. Deregister damaged device. 2. Replace motherboard (with new RDPK preinjected in BIOS). 3. Reimage or rest image to pre-OOB. 4. Write device info into BIOS. 5. Capture new 4K HH. 6. Reregister repaired device. 7. Reimage or reset image to pre-OOB.

Scenario	Supported	Microsoft Recommendation
		8. Go through Autopilot OOBE. 9. Autopilot successfully enabled.
No Repair Product Key (RDPK) injected	No	This scenario violates Microsoft policy and breaks the Windows Autopilot experience.
Reimage damaged Autopilot device that wasn't deregistered before repair	Yes, but the device is still associated with previous tenant ID, so should only be returned to same customer.	1. Reimage damaged device. 2. Write DPK into image. 3. Go through Autopilot OOBE. 4. Autopilot successfully enabled to same tenant ID as before.
Disk replacement from a non-Autopilot device to an Autopilot device	Yes	1. Don't deregister damaged device before repair. 2. Replace HDD on damaged device. 3. Reimage or reset image back to OOBE. 4. Go through Autopilot OOBE (customer). 5. Autopilot successfully enabled (repaired device recognized as its previous self).
Disk replacement from one Autopilot device to another Autopilot device	Maybe	<p>If the device from which the HDD is taken was itself previously deregistered from Autopilot, then that HDD can be used in a repair device. The newly repaired device won't have the proper Autopilot experience if the HDD wasn't previously deregistered from Autopilot before being used in the repaired device.</p> <p>Assuming the used HDD was previously deregistered (before being used in this repair):</p>
		1. Deregister damaged device. 2. Replace HDD on damaged device using an HDD from another deregistered Autopilot device. 3. Reimage or rest the repaired device back to a pre-OOBE state. 4. Go through Autopilot OOBE (customer). 5. Autopilot successfully enabled.
Non-OEM add-in network card replacement	No	<p>Any scenario where a network card is used other than the OEM on-board NIC breaks the Autopilot experience. These scenarios include the following scenarios:</p> <ul style="list-style-type: none"> • From a non-Autopilot device to an Autopilot

Scenario	Supported	Microsoft Recommendation
		<p>device.</p> <ul style="list-style-type: none"> • From one Autopilot device to another Autopilot device. • From an Autopilot device to a non-Autopilot device. <p>These scenarios aren't recommended.</p>
Memory replacement	Yes	<p>Replacing the memory on a damaged device doesn't negatively affect the Autopilot experience on the device. No deregistration/reregistration is needed. The repair technician simply needs to replace the memory.</p>
GPU replacement	Yes	<p>Replacing one or more GPUs on a damaged device doesn't negatively affect the Autopilot experience on that device. No deregistration/reregistration is needed. The repair technician simply needs to replace the GPU.</p>

Important

When parts are scavenged from another Autopilot device, Microsoft recommends to unregister the scavenged device from Autopilot, scavenge it, and then **never register the scavenged device again for Autopilot**. Reusing parts in this way might cause two active devices to end up with the same ID with no possibility of distinguishing between the two.

The following parts can be replaced without compromising Autopilot enablement or requiring special additional repair steps:

- Memory (RAM or ROM).
- Power Supply.
- Video Card.
- Card Reader.
- Sound card.
- Expansion card.
- Microphone.
- Webcam.
- Fan.
- Heat sink.

- CMOS battery.

Other repair scenarios not yet tested and verified include:

- Daughterboard replacement.
- CPU replacement.
- Wifi replacement.
- Ethernet replacement.

FAQ

[] Expand table

Question	Answer
What to do if another customer's welcome page is displayed?	If another customer's welcome page is displayed on a replacement device or refurbished motherboard, a case needs to be raised to Microsoft to fix the device ownership. A case can be opened through the Microsoft Intune admin center by selecting the Help and Support option outlined here . If there isn't access to Microsoft Intune, a case can be submitted through Microsoft Store for Business by selecting Manage > Support and selecting Technical Support . A case can also be submitted through the Microsoft Volume Licensing Center agreement. Instructions on how to submit a case are outlined at Microsoft Software Assurance - Support Incident Submission . Title all cases Autopilot Deregistration Request to streamline requests.
We have a tool that programs product information into the BIOS after the motherboard replacement. Do we still need to submit a CBR report for the device to be Autopilot-capable?	No. Not if the in-house tool writes the minimum necessary information into the BIOS that the Autopilot program looks for to identify the device, as described earlier in this document.
What if only some components are replaced rather than the full motherboard?	It's true that some limited repairs don't prevent the Autopilot algorithm from successfully matching the post-repair device with the pre-repair device. However, Microsoft recommends to always go through the motherboard replacement steps described in the previous sections to ensure success.
How does a repair technician gain access to a broken device if they	The technician has to reimagine the device and use their own credentials during the repair process.

Question	Answer
don't have the customer's sign-in credentials?	

Related content

- [Device guidelines.](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)