Microsoft

Windows in cloud configuration

Overview and Setup Guide

Ravi Ashok, Senior Program Manager, Microsoft Endpoint Manager
Stan White, Principal Software Engineer, Microsoft Endpoint Manager

Updated 9-27-2021
Published 2-2-2021

Contents

Deploying less, empowering more

IT departments are currently caught between two trends. First, IT has seen endpoint management complexity explode with challenges meeting the needs of remote workers, frontline workers, and other specialized users – without additional resources to cater to this complexity. Second, a growing population of end users are expressing that their workflow needs are met without a heavy-handed, complex device configuration – an easy-to-use, secure device and a handful of apps delivered by IT enables them to be successful in their roles.

Microsoft sees an opportunity to empower organizations by providing a recommended configuration of Windows for users with focused workflow needs. Windows in cloud configuration helps IT standardize and simplify management for these users. It can be used to pre-configure new devices so they are ready to go when users turn them on for the first time, or to repurpose existing hardware to extend its lifetime. It works on any Windows 10 / 11 Pro, Enterprise, or Education device, and can be deployed using Microsoft Endpoint Manager today without additional device purchases. This document describes the benefits, use cases, and how to deploy the cloud configuration using Microsoft Endpoint Manager.

How does Windows in cloud configuration make things simpler?

Cloud config simplifies both the end user experience and the IT endpoint management experience. Here are some of its key benefits:

- It provides a uniform, simplified configuration optimized for the cloud that can be applied to any Windows 10 / Windows 11 Pro, Enterprise, or Education device. Users enroll with their Azure Active Directory accounts and devices are kept protected and compliant with Microsoft-recommended security settings. User data is redirected to compliant storage in OneDrive.
- It is NOT a new version, edition, or mode of Windows so there is no dependency on new hardware, and there are no operating system restrictions to consider. Cloud config is ready to go today and can be deployed using Microsoft Endpoint Manager.
- Cloud config is also NOT a new or "lite" version of Microsoft Endpoint Manager. Much like how IT manages Windows devices today, it can be applied, removed, and changed anytime using Microsoft Endpoint Manager.
- Devices are configured with Windows endpoint security settings and automatically updated through Windows Update for Business.
- Microsoft Teams, Microsoft Edge, and additional Microsoft 365 apps (optional) can be installed on the device and come securely configured, automatically updated, and ready to go[1].
- Essential line-of-business and productivity apps can be layered on top of cloud config to provide each user with the apps they need to be successful.
- Every PC gets a standard configuration, simplifying troubleshooting and device replacements.

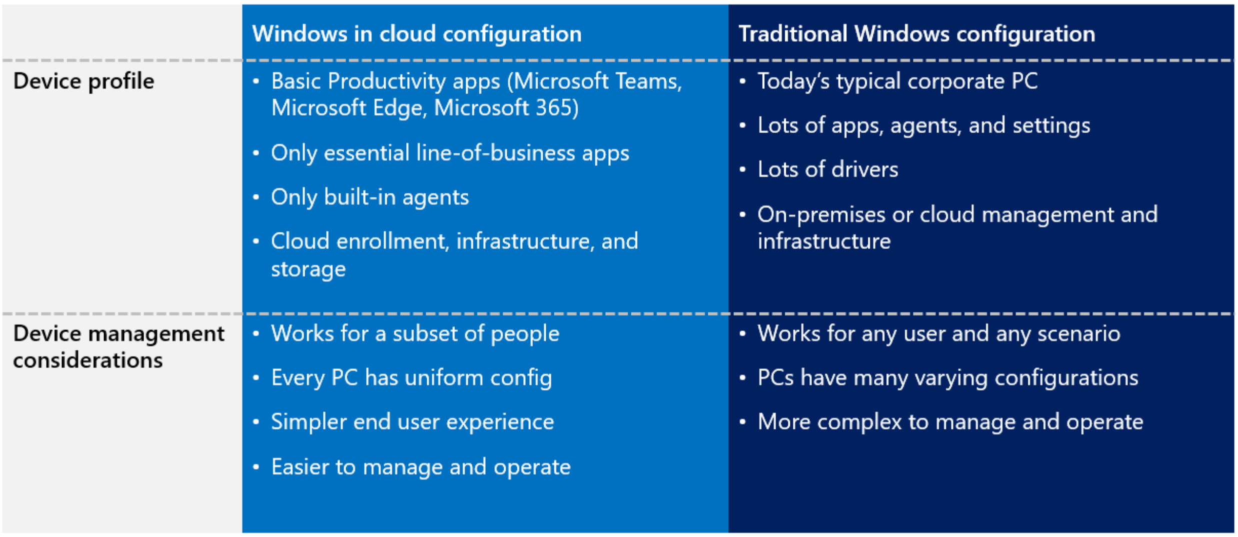
[1] Additional licensing may be required for certain apps and features.

Where does cloud config make sense?

Windows in cloud configuration is designed for users with simplified needs such as productivity and browsing. IT can start by identifying the constituencies in their user bases for whom the cloud configuration might be right. Ideal candidates are groups of end users in the organization who:

- Use devices that do not require complex settings configurations or custom agents.
- Have no dependency on on-premises infrastructure to be successful in their role.
- Use a focused set of apps curated by IT for their workflow needs, like email, Microsoft Teams, Microsoft Edge, and maybe a few essential line-of-business apps.
- IT can deliver apps both directly and through desktop/app virtualization. Cloud config works with any app that can run on a Windows 10 / 11 Pro, Enterprise, or Education device.

Windows configuration approaches



	Windows in cloud configuration	Traditional Windows configuration
Device profile	• Basic Productivity apps (Microsoft Teams, Microsoft Edge, Microsoft 365) • Only essential line-of-business apps • Only built-in agents • Cloud enrollment, infrastructure, and storage	• Today's typical corporate PC • Lots of apps, agents, and settings • Lots of drivers • On-premises or cloud management and infrastructure
Device management considerations	• Works for a subset of people • Every PC has uniform config • Simpler end user experience • Easier to manage and operate	• Works for any user and any scenario • PCs have many varying configurations • More complex to manage and operate

Microsoft has defined the cloud configuration with feedback from customers across industries, geographies, and company sizes. A large healthcare company we recently spoke to saw an opportunity to serve the needs of some of their remote workers with a secured device and a simple configuration. A major airline told us they are looking to empower frontline workers by deploying devices with a simple configuration that are easy to manage and swap out.

Some specific – but not exhaustive – examples of end users from customers where they see great value from cloud configuration include Frontline workers, Operations, and Remote Workers.

Frontline worker

“I work on a team of 150 dispatchers at a hardware store warehouse. When I’m on site, I use Teams all day to communicate with my colleagues as we coordinate on fast-paced tasks processing items throughout the 20,000 sq. ft. warehouse. Away from the warehouse, I check my email and use my company’s line-of-business reporting application to summarize key work items completed in collaboration with my teammates and prepare reports for my managers.”

Operations manager

“I work in an office with 2000 other employees spanning several departments in my company. Last year, some staff started working remotely from home offices across multiple time zones. I split my time between the office and remote work depending on the meetings and projects I am working on. My day-to-day work involves heavy communication over email and Teams and moving quickly between meetings with different departments. I use Microsoft Word and Microsoft Excel heavily to manage key documents for my work. Off hours, I use the VPN my IT department set up on my device to safely access company resources.”

Remote worker

“I live in Belgium and work full time remotely for a company based in Paris. I used to work in one of our office locations, but I have shifted from primarily using the desktop PC at my work desk to working only remotely on my company laptop. My organization’s IT makes my essential applications – including email (Microsoft Outlook), other Microsoft Office apps, and some of my company’s apps – available to me through app virtualization. The first thing I do when I start work is open my VDI client app to access the apps I need. I don’t use any other apps on my PC because my IT-provided virtualized apps give me everything I need.”

Customer scenarios

Some example scenarios are outlined here to help readers understand how their organization can leverage Windows in cloud configuration.

Standardizing device configuration across departments

Fabrikam Industries is a regional textile manufacturer with 15,000 employees across several departments, including business planning, finance, frontline warehouse employees, inventory management, IT, and logistics & delivery coordination. Maurice and his team of IT pros manage devices at Fabrikam. He coordinates with each department to determine what employees need from their devices. He finds that:

- Users have varying needs in terms of productivity apps. The inventory and logistics departments use specialized planning software that requires numerous complex software packages and custom device drivers.
- Almost every user needs at least an email client, a browser, and Microsoft Teams.

Maurice’s team is updating some of Fabrikam’s device inventory, and sees an opportunity to review the organization’s device deployment and make improvements. They start with users that have simpler workflow needs.

Maurice uses Microsoft Endpoint Manager to deploy Windows in cloud configuration to the laptops for the business planning, finance, and frontline warehouse departments. They also deploy essential apps for each department based on what employees need. Since these devices are all configured the same way with essential line-of-business apps delivered to the devices that need them, they are simpler to manage. The cloud configuration delivers endpoint security settings, a compliance policy, and automatic update settings that help keep devices secure, and help the team monitor them for issues.

Users are delighted that devices are configured with just what they need – email, Microsoft Teams, Microsoft Edge, and essential productivity and line-of-business apps for their respective departments.

With data automatically stored in OneDrive, users can be productive knowing their data is safely and automatically synced to cloud storage.

Enabling remote work with virtualization and a simple device configuration

Angelina manages devices at a law firm in New York City with 3500 lawyers and staff members across the country. Until this year, lawyers and other staff worked on site using PCs in offices across 12 cities. Lawyers with high case volumes have laptops so they can be productive whenever they need. To configure apps in one place and keep device costs low, Angelina's team delivers apps to these laptops using app virtualization.

Due to the COVID-19 pandemic, all staff started working remotely from home offices and started conducting key meetings online. Angelina's team has a big challenge – equip every lawyer and staff member with a device to work remotely, keeping costs low, and as soon as possible. Outside of IT, users just need access to email, Microsoft Teams, and Microsoft Office apps to work on and exchange documents. Angelina realizes that she can expand her team's app virtualization approach to all staff. Devices need to be easy to use and have access to the Internet, and users' remaining workflow needs can be handled through the firm's virtualization solution.

The team buys laptops for staff that need them and ship them directly to employee home offices. They also keep and use existing laptops. Using Microsoft Endpoint Manager, they deploy Windows in cloud configuration to all devices. Angelina then deploys the desktop client app for the virtualization solution her team already manages, through which all needed apps are configured and made available. Devices are deployed with Windows Autopilot and are ready to go with endpoint security and Windows Update settings configured.

When users receive their devices, they just open them and sign in with their Azure AD credentials. Windows Autopilot makes device setup easy and the Enrollment Status Page shows setup progress and ensures that users have a consistent, familiar experience when they get started.

Angelina's team is happy that they applied a single configuration to these devices, including laptops previously in circulation. She rests easy knowing it would be easy to reset a device remotely and bring it back to a good state if a user has issues across the country. Her team could even send the user a brand-new device with cloud config applied so they can pick up right where they left off. The CEO congratulates her on a job well done after learning that the whole fleet was deployed and delivered in just a couple of weeks.

Empowering students and teachers

Samantha is an IT administrator at Contoso School District. She and her team manage devices across the district's 25 schools, which includes 75,000 students and 2500 faculty and staff. Contoso is a 1:1 district – each student and faculty/staff member has their own school-managed device for school or work. Samantha's team, in coordination with smaller teams at each school, is responsible for managing multiple device types across multiple platforms – Windows, iOS/iPadOS, and Android.

Through feedback from each school's IT team, she learned that most users have simple needs for their devices. They need an easy-to-use, secure device with minimal configuration. Samantha recently read about Windows in cloud configuration. She thinks it would be useful to implement this in her schools. She uses Microsoft Endpoint Manager to deploy a cloud configuration, to pre-configure devices to enroll with

Windows Autopilot, and deliver Microsoft Teams, Microsoft Edge, and other apps her team chooses. She is delighted that cloud config configures devices to store user data in OneDrive, and keeps devices automatically updated with Windows Update. After deploying cloud config, Samantha coordinates with the teams at each school to deliver essential apps that students and teachers at each location need.

Samantha and her team streamlined Contoso School District's device deployment using Windows in cloud configuration, adding only essential apps as needed. Since every device has a standardized configuration and user data is stored in the cloud, it's easy for her team to troubleshoot issues with devices and quickly swap out devices when needed.

Device requirements

Windows in cloud configuration can be deployed to any Windows 10 / Windows 11 Pro, Enterprise, or Education device. It's a set of configurations and apps that can be changed or removed from devices anytime. All you need are your Windows devices – existing or new – and Microsoft Endpoint Manager to get started.

Licensing recommendations

To meet the minimum requirements to deploy devices in cloud config, you will need licenses covering:

- Azure Active Directory Premium P1
- Microsoft Intune
- Microsoft Teams
- OneDrive for Business
- Windows 10 / Windows 11 Pro, Enterprise, or Education

Microsoft recommends Enterprise Mobility + Security E3 and Office 365 E3, and a Windows device running Windows 10 Pro or Windows 11 Pro. These licenses will equip you with the bare minimum necessary for cloud config.

For a more complete experience, Microsoft 365 E3 will give you the products and services referenced above, plus Windows 10 Enterprise or Windows 11 Enterprise.

Note: *there are several Microsoft 365 subscriptions that may give your users what they need to remain productive and secure, while giving IT what they need to set up and deploy cloud configuration. See Microsoft 365 subscriptions plans and pricing here.*

Use Microsoft Endpoint Manager to configure and deploy cloud config

Note: *Microsoft is always looking to improve Windows in cloud configuration. We will periodically update this document with the latest guidance on recommended configurations.*

Option 1: Guided scenario in Microsoft Endpoint Manager

Use the guided scenario in Microsoft Endpoint Manager to easily deploy the recommended configurations in this document. You can find it on the home page or by going to **Troubleshooting + support > Guided scenarios** **> Deploy Windows in cloud configuration**. You can always change and update your cloud config deployment using Microsoft Endpoint Manager anytime. As cloud config is improved and updated, the guided scenario will also be kept updated so it always deploys the latest recommended configurations in this document.

Option 2: Configure using this setup guide

You can use the steps in this document to deploy cloud config yourself. Windows in cloud configuration will:

- Optimize devices for the cloud by configuring them to enroll into Intune management with Azure Active Directory. User data is stored in OneDrive automatically with Known Folder Move configured.
- Deliver Microsoft Teams and Microsoft Edge to devices.
- Configure end users to be standard users on devices, giving IT more control over the apps installed on devices.
- Remove built-in apps and the Microsoft Store app, simplifying the end user experience.
- Apply endpoint security settings and a compliance policy to help keep devices secure and help IT monitor device health.
- Ensure that devices are automatically updated through Windows Update for Business.

You can also optionally configure:

- Additional Microsoft 365 applications (such as Outlook, Word, Excel, PowerPoint).
- Essential line-of-business apps that end users need to be successful. Microsoft recommends keeping these apps to a minimum to keep the configuration simple.
- Essential resources such as Wi-Fi profiles, VPN connections, certificates, and printer drivers that are necessary for users' workflows.

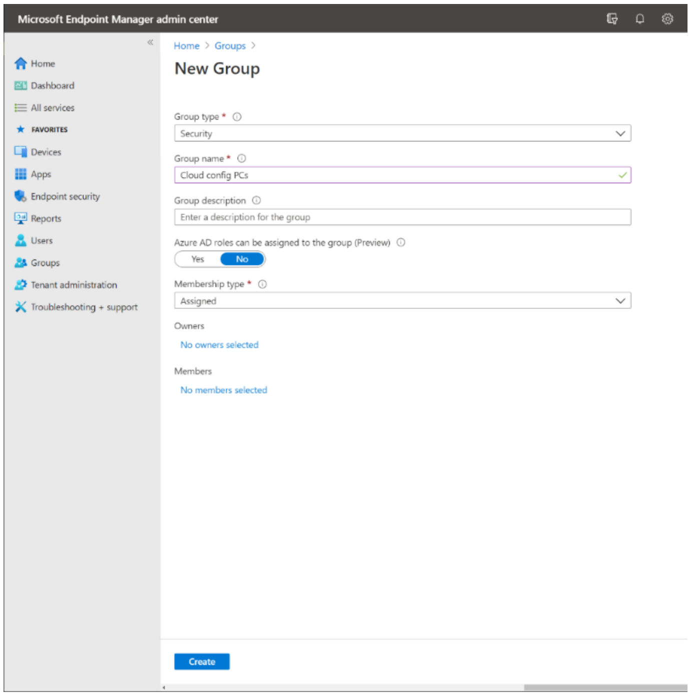
The following sections describe how to use Microsoft Endpoint Manager to set up this configuration, covering these key steps:

1. Create an Azure AD group
2. Configure device enrollment
3. Deploy a script to configure Known Folder Move and remove built-in apps
4. Deploy apps
5. Deploy endpoint security settings
6. Configure Windows Update settings
7. Deploy a Windows compliance policy
8. Additional optional configurations

Step 1: Create an Azure AD group

Create an Azure AD security group that will receive the configurations you deploy in this document. This dedicated group will help you organize devices and easily manage your cloud config resources in Microsoft Endpoint Manager. Microsoft recommends starting by deploying only the configurations recommended in this guide, and adding on essential apps and other device configurations as necessary.

1. In Microsoft Endpoint Manager, go to **Groups > All groups > New group.**
2. For Group type, choose **Security.**
3. Enter a Group name. For example, "Cloud config PCs".
4. For the setting "Azure AD roles can be assigned to the group (Preview)", choose **No.**
5. For Membership type, choose **Assigned.**
6. Choose **Create.**



New Group

Group type * : Security

Group name * : Cloud config PCs

Group description: Enter a description for the group

Azure AD roles can be assigned to the group (Preview): Yes [✓ No]

Membership type * : Assigned

Owners: No owners selected

Members: No members selected

In the next steps, you will create configurations that you will assign to this group. You can add these devices to this group that will receive cloud config:

- Pre-registered Windows Autopilot devices
- Devices that you have already enrolled. Microsoft recommends removing apps and profiles you might have already targeted, and resetting and re-enrolling these devices after deploying cloud config to start fresh. This will provide the most streamlined user experience and ensure that both users and IT enjoy the benefits of cloud config to their full extent. You can then add additional essential apps and ensure devices have just what users need while keeping the device configuration standardized.

Step 2: Configure Device Enrollment

Enable MDM Automatic enrollment

Enable automatic enrollment for the users in your organization that you want to use cloud config.

1. In Microsoft Endpoint Manager, go to **Devices > Windows > Windows enrollment** and select **Automatic Enrollment.**
2. Under **MDM user scope**, select one of the following:
    - Select **Some** if you want to apply the cloud configuration to devices used by a subset of users in your organization. Select the groups of users that will use devices with the cloud configuration applied.
        i. **Note:** At a minimum, select the users for whom you would like to apply the cloud configuration. You can enable auto-enrollment for more users. [Learn more about Windows automatic enrollment.]
    - Select **All** if you want to apply the cloud configuration to all Windows devices that users in your organization will use.
3. Choose **Save** to save your changes.

4. MAM settings are not configured as part of this setup. The settings for **MAM user scope, MAM terms of user URL, MDM discovery URL, and MAM compliance URL** can be left unchanged.

Choose how devices will be enrolled and configure users to be standard users on devices

Choose one of the following options for how to enroll devices and configure users as standard users on their devices.

Enrollment Option 1: Windows Autopilot user-driven enrollment (recommended)
Pre-register devices using Windows Autopilot to configure how they will start up and enroll into device management. Microsoft recommends using Autopilot enrollment and the Enrollment Status Page so admins can get devices ready to go before they have been enrolled. This enrollment method provides a consistent end user experience by displaying a status page during device setup while cloud config is fully applied.

Add Windows Autopilot devices

Follow the instructions in the **Add devices** section of the following document to add your pre-registered Autopilot devices to Microsoft Endpoint Manager. The remaining steps after the **Add devices** section are covered in this document with specific recommended settings, using the group you created in Step 1 to assign devices to.

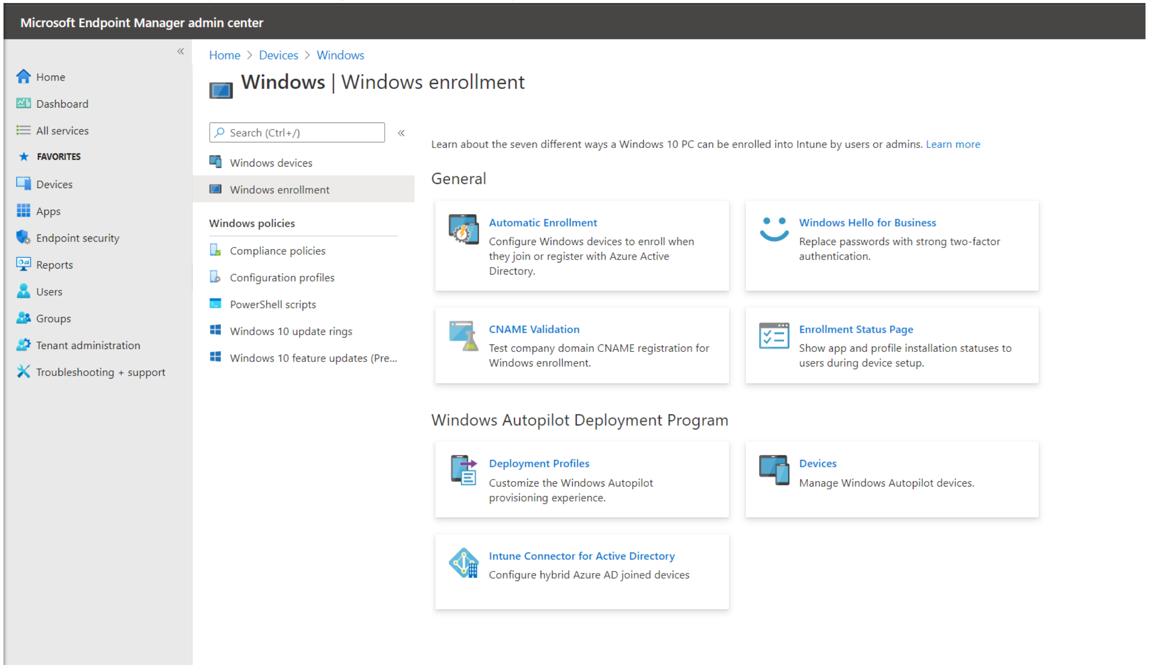
Tutorial - Use Autopilot to enroll devices in Intune - Microsoft Intune | Microsoft Docs

You can manually register devices to use Windows Autopilot. You may be doing this if you are repurposing existing hardware that you had previously not set up with Autopilot. Refer to the following document to learn how to manually register devices:

Manually register devices with Windows Autopilot | Microsoft Docs

Create and assign a Windows Autopilot deployment profile

1. In Microsoft Endpoint Manager, go to **Devices > Windows > Windows enrollment > Windows Autopilot Deployment Program > Deployment profiles**



Windows | Windows enrollment

Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

General

Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business
Replace passwords with strong two-factor authentication.

CNAME Validation
Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page
Show app and profile installation statuses to users during device setup.

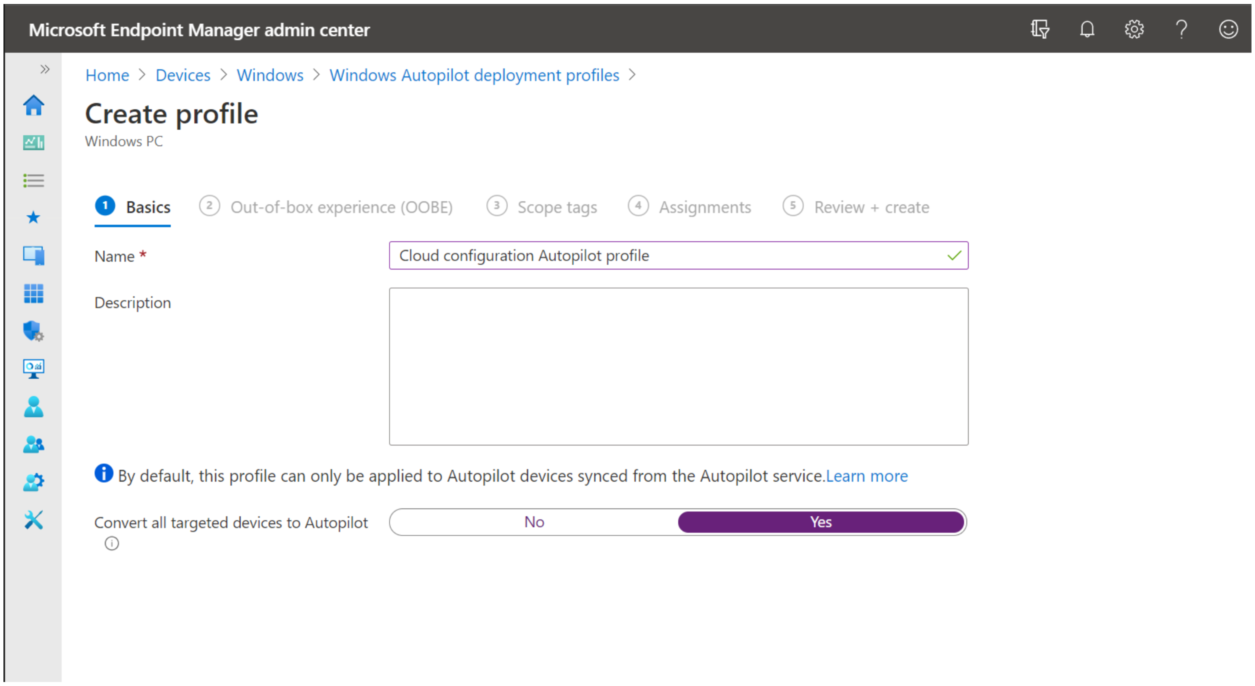
Windows Autopilot Deployment Program

Deployment Profiles
Customize the Windows Autopilot provisioning experience.

Devices
Manage Windows Autopilot devices.

Intune Connector for Active Directory
Configure hybrid Azure AD joined devices

2. Choose **Create profile > Windows PC.** Enter a name for the profile.
3. For the setting **Convert all targeted devices to Autopilot**, select **Yes** and choose **Next**. You can apply cloud config to devices enrolled using enrollment methods other than Autopilot. When you add those devices to your group, they will be converted to Autopilot. The next time they go through the Windows Out of Box Experience (OOBE) after being reset, they will enroll through Autopilot.


Microsoft Endpoint Manager admin center

Home > Devices > Windows > Windows Autopilot deployment profiles >

Create profile

Windows PC

1 Basics 2 Out-of-box experience (OOBE) 3 Scope tags 4 Assignments 5 Review + create

Name * Cloud configuration Autopilot profile

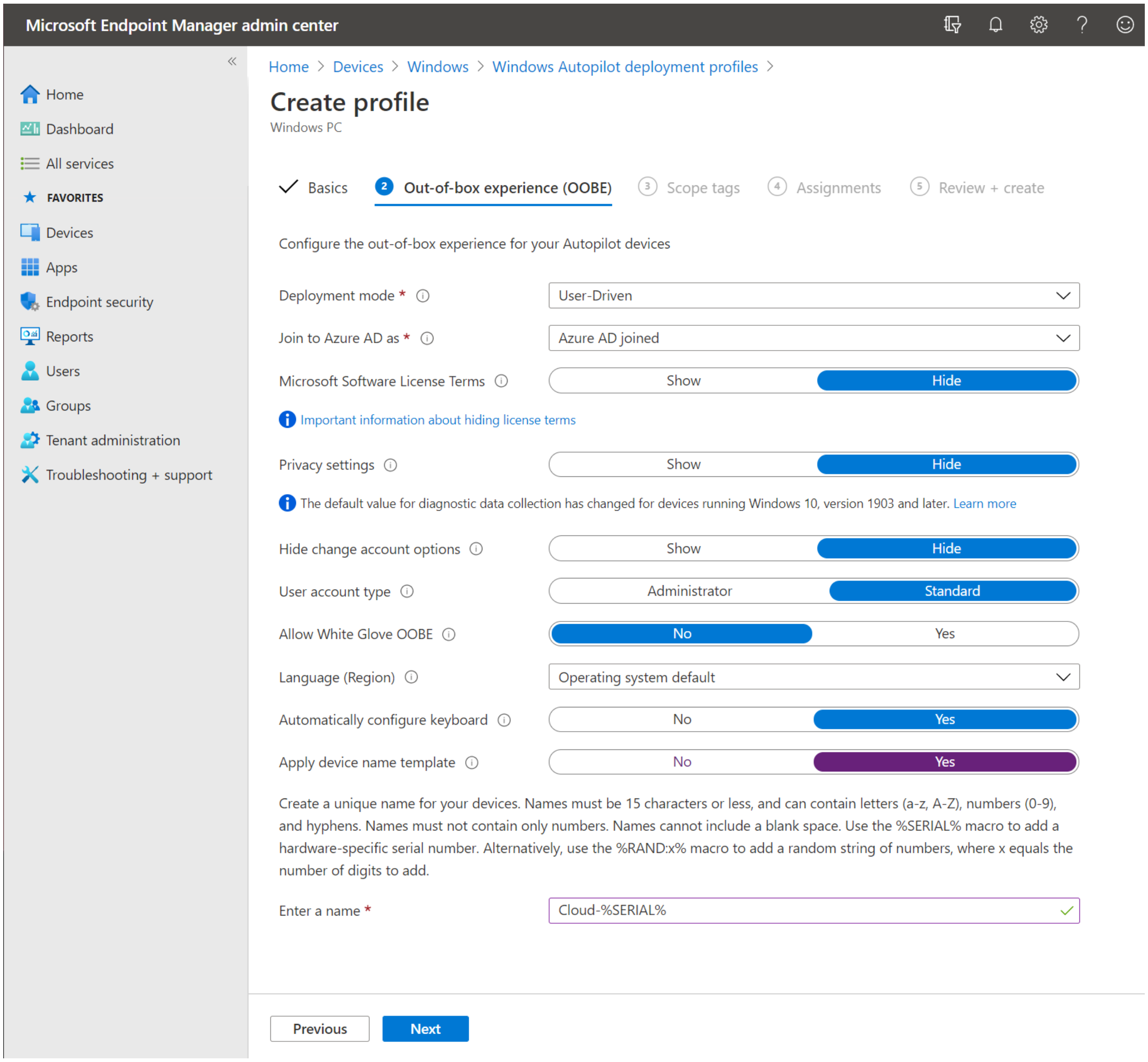
Description

By default, this profile can only be applied to Autopilot devices synced from the Autopilot service.Learn more

Convert all targeted devices to Autopilot No **Yes**

4. In the **Out-of-box experience (OOBE)** step, configure the following values and then click **Next**:

Setting	Value
Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Apply device name template	You can choose to apply a device name template. Use a name prefix that can help you identify your devices with this configuration, for example: Cloud-%SERIAL%



Create profile

Windows PC

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

Deployment mode * : User-Driven

Join to Azure AD as * : Azure AD joined

Microsoft Software License Terms: Show / **Hide**

Important information about hiding license terms

Privacy settings: Show / **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 / **Hide**

User account type: Administrator / **Standard**

Allow White Glove OOBE: **No** / Yes

Language (Region): Operating system default

Automatically configure keyboard: No / **Yes**

Apply device name template: No / **Yes**

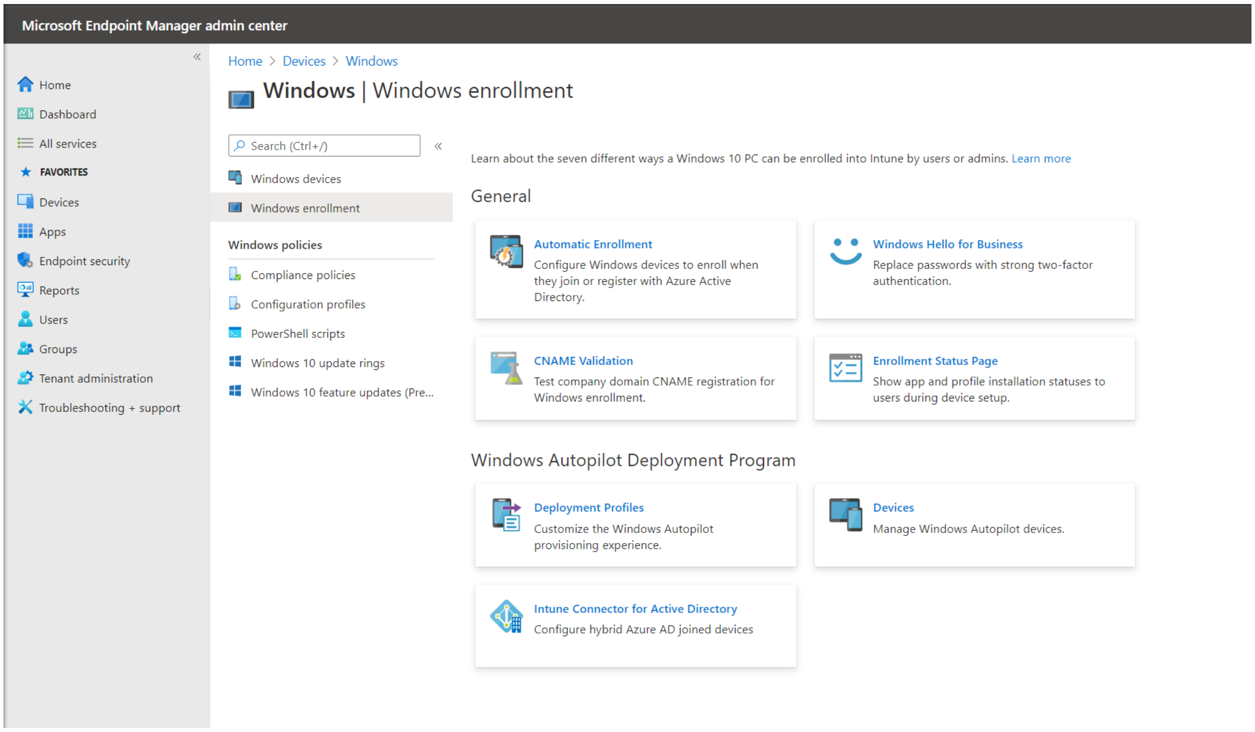
Create a unique name for your devices. Names must be 15 characters or less, and can contain letters (a-z, A-Z), numbers (0-9), and hyphens. Names must not contain only numbers. Names cannot include a blank space. Use the %SERIAL% macro to add a hardware-specific serial number. Alternatively, use the %RAND:x% macro to add a random string of numbers, where x equals the number of digits to add.

Enter a name * : Cloud-%SERIAL%

5. Assign the profile to the group you created in Step 1 (Create an Azure AD group), and then click **Next**.
6. Review the new profile and then click **Create.**

Create and assign an Enrollment Status Page

1. In Microsoft Endpoint Manager, go to **Devices** > **Windows** > **Windows enrollment** > **General** > **Enrollment Status Page**



Windows | Windows enrollment

Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

General

Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business
Replace passwords with strong two-factor authentication.

CNAME Validation
Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page
Show app and profile installation statuses to users during device setup.

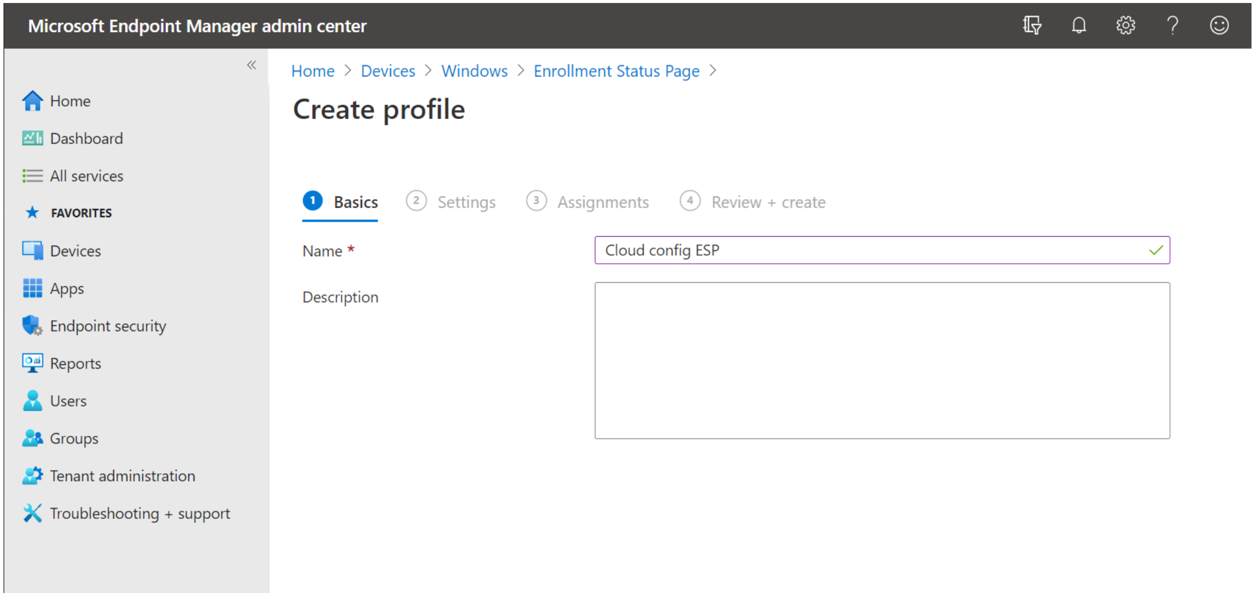
Windows Autopilot Deployment Program

Deployment Profiles
Customize the Windows Autopilot provisioning experience.

Devices
Manage Windows Autopilot devices.

Intune Connector for Active Directory
Configure hybrid Azure AD joined devices

2. Choose **Create** and enter a name for this Enrollment Status Page.



Create profile

Name * Cloud config ESP

Description

3. In the **Settings** step, configure the following values and then click **Next**.

Setting	Value
Show app and profile configuration process	Yes
Show an error when installation takes longer than specified number of minutes	60
Show custom message when time limit error occurs	Yes (you may modify the default message).

Allow users to collect logs about installation errors	Yes
Only show page to devices provisioned by out-of-box experience (OOBE)	Yes
Block device user until all apps and profiles are installed	Yes
Allow users to reset device if installation error occurs	Yes
Allow users to use device if installation error occurs	No
Block device user until these required apps are installed if they are assigned to the user/device	All

Note: *We recommend blocking users from using the device if an installation error occurs to ensure they can only get started after cloud config is fully applied. Based on your deployment needs, you may choose to allow the user to use the device even if an installation error occurs. If you do this, Intune will continue to attempt to apply configurations when the device checks in with Intune again.*

7. In the **Assignments** step, assign the Enrollment Status Page to the group you created in Step 1 (Create an Azure AD group), and then click **Next**.
8. Choose **Create** to create and assign the Enrollment Status Page.

Alternative device enrollment options
Microsoft recommends using Autopilot to pre-configure device settings and keep the user on a status page before all configurations are applied to the device. The following alternative options are available, with some differing steps to ensure users are standard users on their devices. If you configured device enrollment through Windows Autopilot, skip to the next step.

Enrollment Option 2: Bulk enrollment using a provisioning package

You may choose to enroll devices using a provisioning package created using Windows Configuration Designer or the Set up School PCs app. Using this enrollment method, all users are automatically standard users on the device. Learn more about bulk enrollment for Windows devices.

With this enrollment method, you will need to add devices to the group you created at the beginning of this process after they are enrolled so they can receive cloud config.

There is no Enrollment Status Page displayed with this enrollment option, so users can't see progress as all cloud configuration settings are delivered and may start using the device before it is fully applied. Microsoft recommends that IT verify that devices have settings and apps delivered before distributing devices to users.

Enrollment Option 3: Enrollment via Azure AD sign-in in the Out-of-box Experience (OOBE)

With MDM Auto-enrollment enabled in your environment, users can enroll devices by simply signing in with their Azure AD accounts during OOBE.

With this enrollment method, you configure a custom profile using Microsoft Endpoint Manager to restrict local administrators on devices. Be sure to specify a group containing only IT administrators in your environment to be local administrators. The following link includes sample policy definition XML that you use in your custom profile. Assign the custom profile you create to the group you created in Step 1.

Policy CSP - LocalUsersAndGroups - Windows Client Management | Microsoft Docs

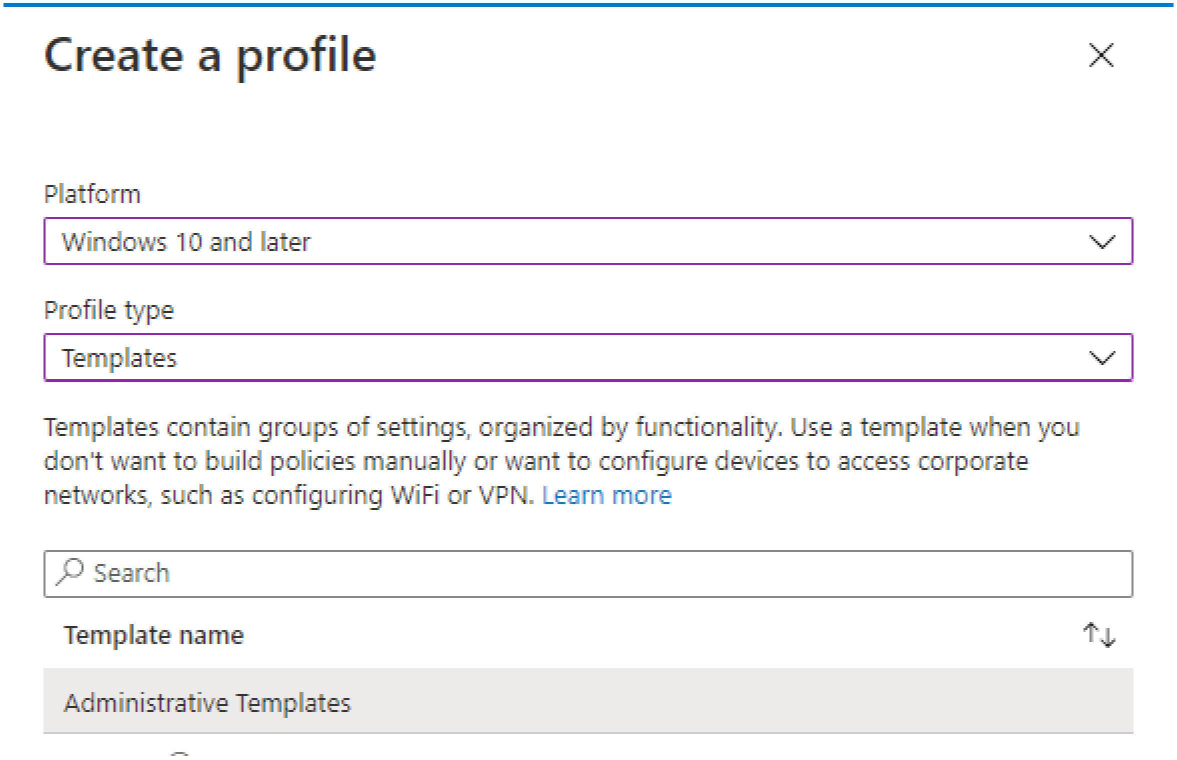
Step 3: Configure OneDrive Known Folder Move and deploy a script to remove built-in apps

This step helps simplify the Windows user experience. When you configure OneDrive Known Folder Move, user files and data are automatically saved in OneDrive. When you remove built-in Windows 10 apps and the Microsoft Store, the Start menu and device experience are simplified.

Configure OneDrive Known Folder move with an Administrative Template

Important Note: *Due to a sync issue with OneDrive Known Folder Move and SharedPC configuration, Microsoft does not recommend using Windows in cloud configuration with a device on which multiple users will be signing in and out.*

1. In Microsoft Endpoint Manager, go to **Devices** > **Windows** > **Configuration profiles** > **Create profile**
2. Choose **Windows 10 and later** for platform and choose **Templates** for profile type.
3. Choose **Administrative Templates** and choose **Create**.



Create a profile

Platform

Windows 10 and later

Profile type

Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

4. Enter a name for the profile and choose **Next**.
5. In the **Configuration settings** section, search for the settings in the following and configure them to their recommended values.

   Note: Your tenant ID can be found in the **Tenant ID** box on the Properties page in Azure Active Directory.

Setting name	Value
Silently move Windows known folders to OneDrive	Enabled **Tenant ID** Enter your organization's tenant ID **Show notification to users after folders have been redirected** Yes You may choose to hide the notification
Silently sign in users to the OneDrive sync app with their Windows credentials	Enabled
Prevent users from moving their Windows known folders to OneDrive	Enabled
Prevent users from redirecting their Windows known folders to their PC	Enabled
Use OneDrive Files On-Demand	Enabled

6. Assign the profile to the group you created at the start of this process.

Deploy a script to remove built-in apps

Microsoft has created a PowerShell script that will remove built-in apps when deploying cloud config. Use the following steps to deploy it. The script also removes the Microsoft Store app from devices to further simplify the user experience.

Note: *If you want to keep the Microsoft Store on devices, you can deploy the alternate script that removes built-in apps but keeps the Microsoft Store. If you have already removed the Microsoft Store, you can redeploy it using Microsoft Endpoint Manager and the Microsoft Store for Business or Microsoft Store for Education. You can also block end users from installing Store apps outside of your organization's private store on Windows 10 / 11 Enterprise and Windows 10 / 11 Education. See Step 8: Additional optional configuration section for more details.*

You can also redeploy individual apps that are removed using this script by adding them to your Microsoft Store for Business or Microsoft Store for Education inventory and assigning them to devices using Microsoft Endpoint Manager. If you do this, Microsoft recommends also keeping the Store app on devices to ensure Store apps stay updated.

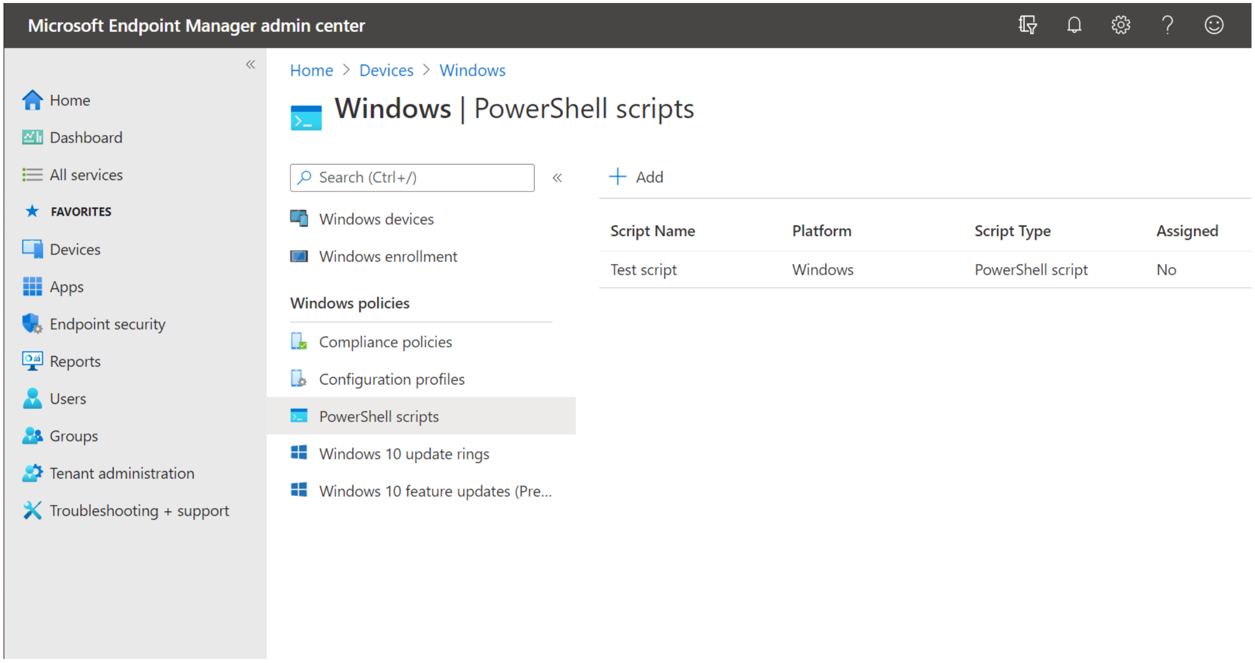
The provided script will attempt to remove built-in apps but may not remove all of them. You may need to modify the script to remove all built-in apps on your devices.

1. Download the PowerShell script here.

   An alternate version of the recommended script which removes built-in apps, but keeps the Microsoft Store, is available here.

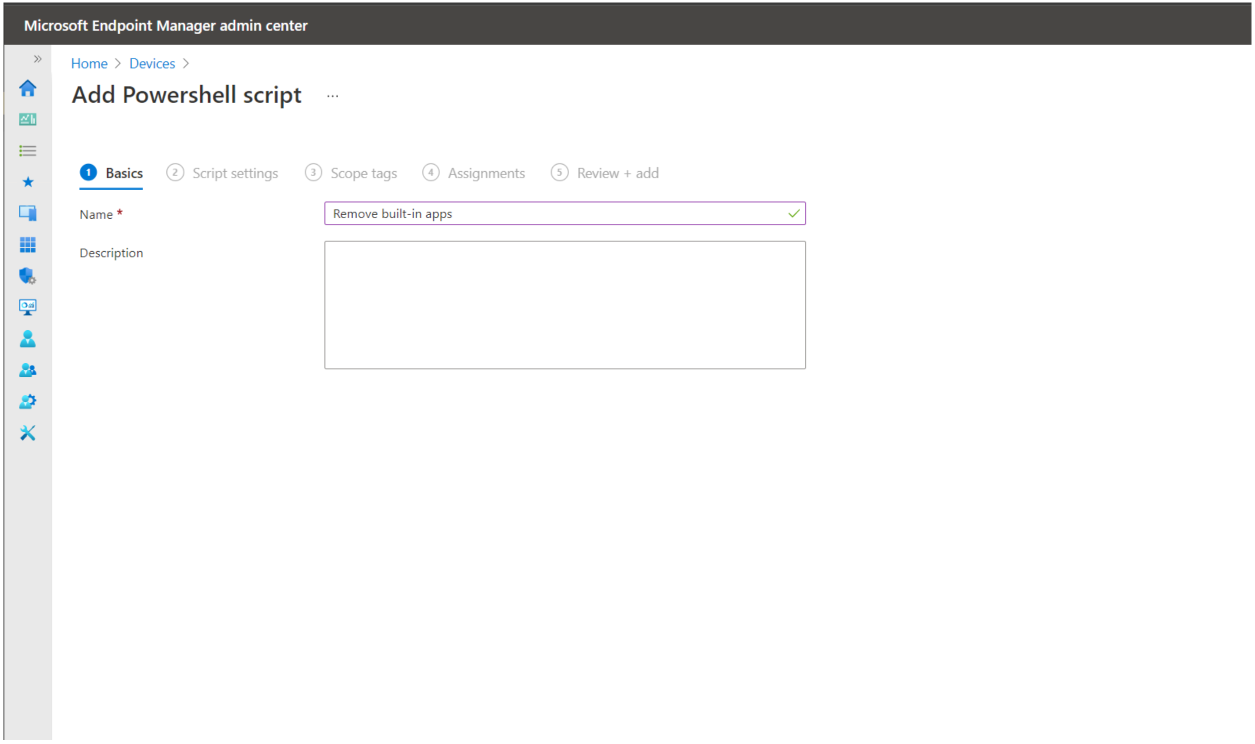
   Note: *The cloud config guided scenario in Microsoft Endpoint Manager deploys the recommended script that removes the Microsoft Store along with built-in apps. If you use the guided scenario to* *deploy cloud config but want to deploy the alternate script, delete the script deployed through the guided scenario and replace it with the alternate script by following these steps. Assign the alternate script to the same group you deployed cloud config to using the guided scenario.*

2. In Microsoft Endpoint Manager, go to **Devices** > **Windows** > **PowerShell scripts** > **Add** to create a new script.



Script Name	Platform	Script Type	Assigned
Test script	Windows	PowerShell script	No

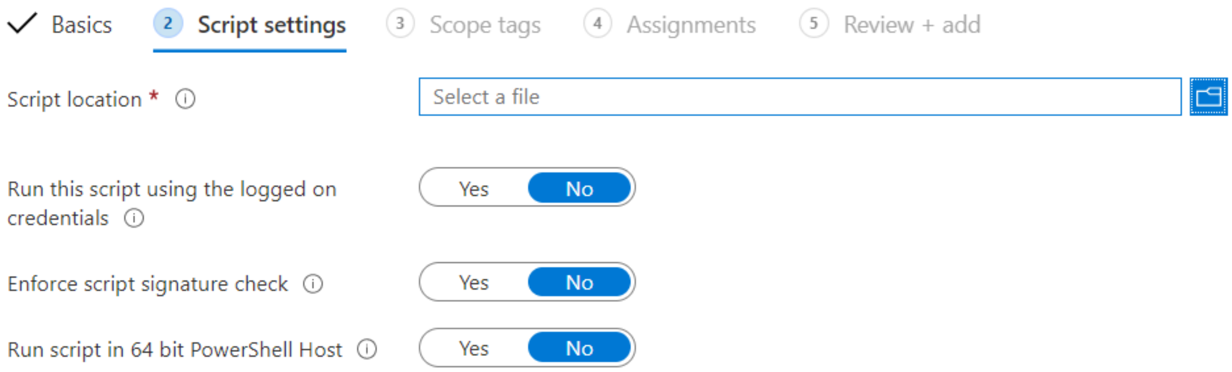
3. In the **Basics** step, enter a name for your script and choose **Next**.



Name * Remove built-in apps

Description

4. In the **Script settings** step, upload the script you download in Step 1. Leave the other settings unchanged and choose **Next**.



Script location * ⓘ: Select a file

Run this script using the logged on credentials ⓘ: Yes [✓ No]

Enforce script signature check ⓘ: Yes [✓ No]

Run script in 64 bit PowerShell Host ⓘ: Yes [✓ No]

5. Assign the script to the group you created in Step 1 (Create an Azure AD group).

Step 4: Deploy apps

Microsoft Edge

Use the following instructions to configure and install the latest version of Microsoft Edge, follow the steps at Add Microsoft Edge for Windows 10 to Microsoft Intune | Microsoft Docs.

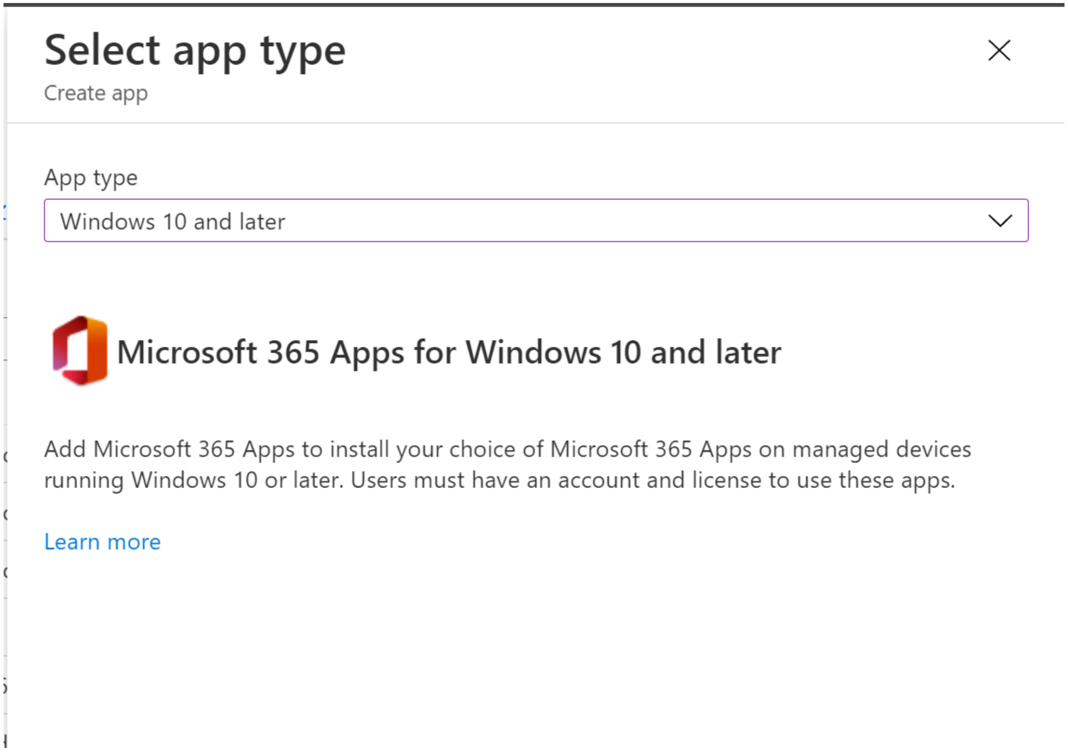
1. For **App settings,** choose the **Stable Channel** for this deployment.
2. Assign the Edge app to the group you created in Step 1 (Create an Azure AD group).

Microsoft Teams and additional Microsoft 365 apps

Configure Teams installation through the Microsoft 365 Suite app in Intune.

1. In Microsoft Endpoint Manager, navigate to **Apps > Windows.**
2. Choose **Add** to create a new app.

3. Under **Microsoft 365 Apps**, select **Windows 10 and later** and choose **Select**.



Select app type

Create app

App type

Windows 10 and later

Microsoft 365 Apps for Windows 10 and later

Add Microsoft 365 Apps to install your choice of Microsoft 365 Apps on managed devices running Windows 10 or later. Users must have an account and license to use these apps.

Learn more

4. Choose a name for **Suite Name** or leave the suggested name unchanged. Choose **Next**.
5. Under **Configure app suite**, unselect all apps except for Teams.
    - **Optional:** If you want to deploy additional Microsoft 365 apps, choose them from this list:
        - Excel
        - OneNote
        - Outlook
        - PowerPoint
        - Word
        - ***Note:*** *You don't need to choose OneDrive from this list. It's built in to Windows 10 / 11 Pro, Enterprise, and Education.*
6. Under **App suite information**, configure these settings:

Setting	Value
Architecture	64-bit ***Note:*** *cloud config also works with 32-bit. Microsoft recommends choosing 64-bit.*
Update channel	Current channel
Remove other versions	Yes
Version to install	Latest

7. Under **Properties,** configure these settings:

Setting	Value
Use shared computer activation	Yes
Accept the Microsoft Software License Terms on behalf of users	Yes

8. Choose **Next.**
9. Assign the suite to the group you created in Step 1 (Create an Azure AD group).

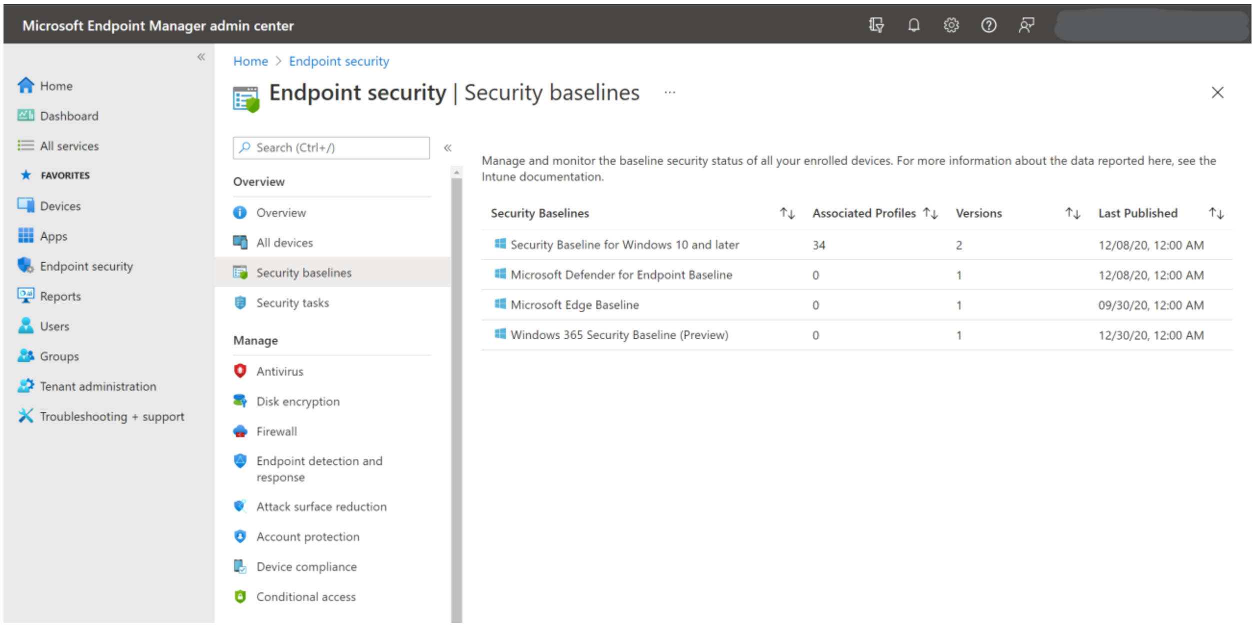
Step 5: Deploy endpoint security settings

Deploy the Windows security baseline

Windows security baselines help keep your devices secure and compliant. Windows is designed to be secure, and security baselines add a layer of protection and monitoring by applying security settings across the operating system and Microsoft Defender. [Learn more about Windows security baselines.]()

For Windows in cloud configuration, Microsoft recommends using the default Windows security baseline configurable in Microsoft Endpoint Manager, with a few settings changed based on your organization's preference.

1. In Microsoft Endpoint Manager, navigate to **Endpoint security** > **Security baselines** > **Security baseline for Windows 10 and later.**



Manage and monitor the baseline security status of all your enrolled devices. For more information about the data reported here, see the Intune documentation.

Security Baselines ↑↓	Associated Profiles ↑↓	Versions ↑↓	Last Published ↑↓
Security Baseline for Windows 10 and later	34	2	12/08/20, 12:00 AM
Microsoft Defender for Endpoint Baseline	0	1	12/08/20, 12:00 AM
Microsoft Edge Baseline	0	1	09/30/20, 12:00 AM
Windows 365 Security Baseline (Preview)	0	1	12/30/20, 12:00 AM

2. Choose **Create profile** to create a new security baseline.
3. Enter a name for your security baseline and choose **Next.**
4. Accept the default configuration settings by choosing **Next.** You may consider adjusting some of the following settings based on your organization's needs:

Setting category	Setting	Reason for changing

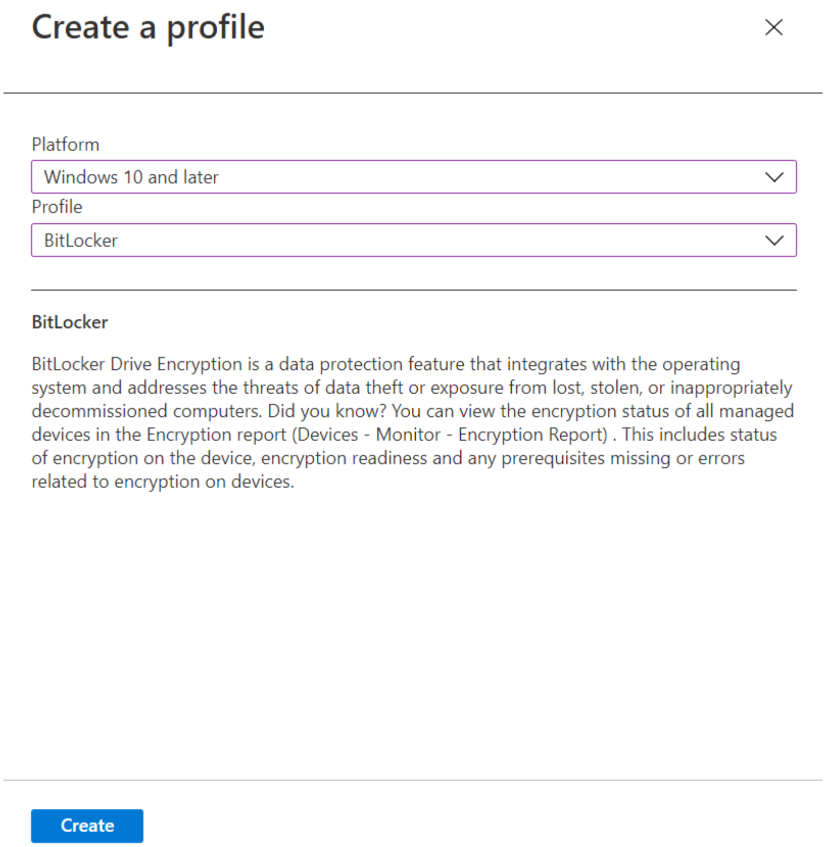
Browser	Block Password Manager	You might consider allowing end users to use password managers.
Remote Assistance	Remote Assistance solicited	You may need to configure these settings if you want to allow your support staff to remotely connect to devices to assist with issues. Microsoft recommends keeping this disabled unless it is required.
Firewall	All Firewall settings	Consider changing the default Firewall settings if you need to allow certain connections to devices based on your organization's needs.

5. In the **Assignments** step, select the group that you created in Step 1 (Create an Azure AD group).
6. Choose **Create** to create and assign the baseline.

Deploy additional BitLocker settings with a drive encryption endpoint security profile

Some additional BitLocker settings help keep your devices secure.

1. In Microsoft Endpoint Manager, navigate to **Endpoint security** > **Disk encryption** > **Create Policy.**
2. For Platform, choose **Windows 10 and later.**
3. For Profile, choose **BitLocker** and choose **Create.**



Create a profile

Platform

Windows 10 and later

Profile

BitLocker

BitLocker

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Did you know? You can view the encryption status of all managed devices in the Encryption report (Devices - Monitor - Encryption Report) . This includes status of encryption on the device, encryption readiness and any prerequisites missing or errors related to encryption on devices.

4. In the **Basics** step, choose a name for your profile.
5. In the **Configuration settings** step, choose the following settings.

Setting category	Setting	Value
BitLocker – Base settings	Enable full disk encryption for OS and fixed data drives	Yes
BitLocker – Fixed Drive Settings	BitLocker fixed drive policy	Configure
	Block write access to fixed data-drives not protected by BitLocker	Yes
	Configure encryption method for fixed data-drives	AES 128bit XTS
BitLocker – OS Drive Settings	BitLocker system drive policy	Configure
	Startup authentication required	Yes
	Compatible TPM startup	Allowed
	Compatible TPM startup PIN	Allowed
	Compatible TPM startup key	Required
	Compatible TPM startup key and PIN	Allowed
	Disable BitLocker on devices where TPM is incompatible	Yes
	Configure encryption method for Operating System drives	AES 128bit XTS
BitLocker – Removable Drive Settings	BitLocker removable drive policy	Configure
	Configure encryption method for removable data-drives	AES 128bit CBC
	Block write access to removable data-drives not protected by BitLocker	Yes

7. In the **Assignments** step, assign the profile to the group that you created in Step 1 (Create an Azure AD group).
8. Choose **Create** to create and assign the profile.

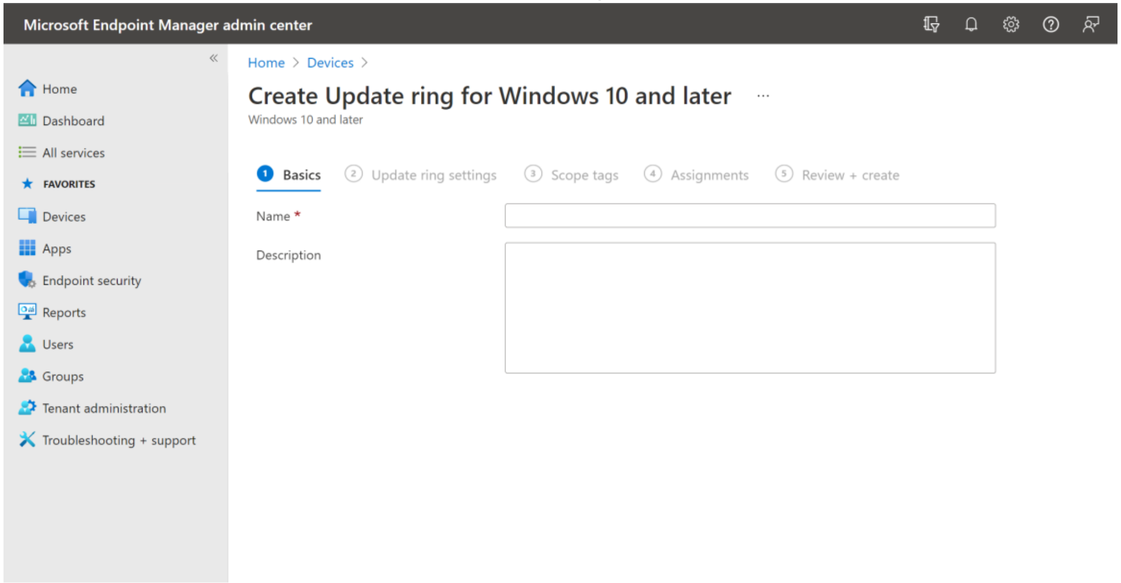
Step 6: Configure Windows Update settings

Windows Update Ring

Configure a Windows update ring to keep devices automatically updated. The settings in this guide align with the recommended settings in the Windows Update Baseline.

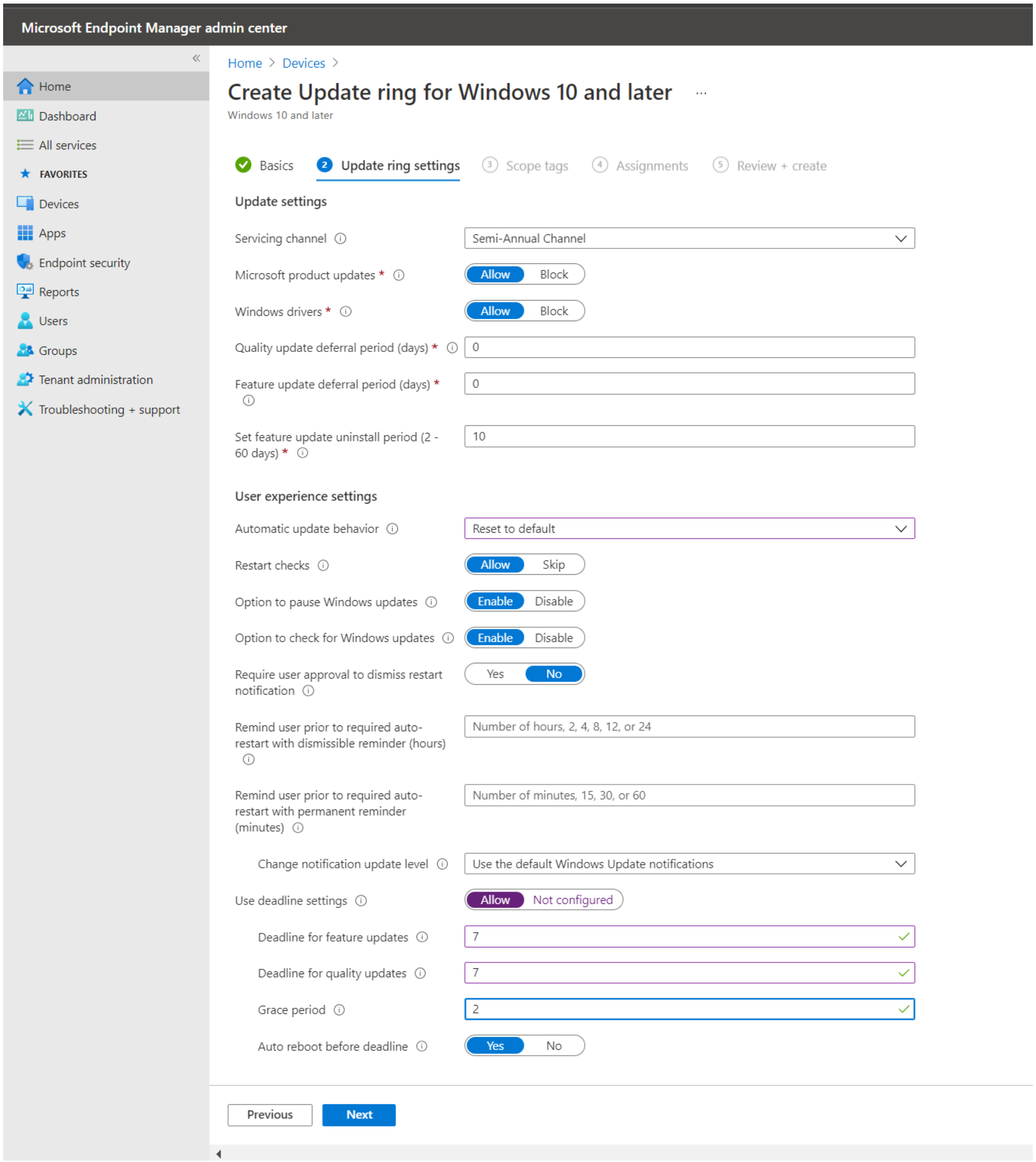
1. In Microsoft Endpoint Manager, navigate to **Devices > Update rings for Windows 10 and later > Create profile.**

2. In the **Basics** step, enter a name for the update ring.



3. In the **Update ring settings** step, configure the following values and choose **Next**.

Setting	Value
Servicing channel	Semi-annual channel
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	0
Set feature update uninstall period	10
Automatic update behavior	Reset to default
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Require user approval to dismiss restart notification	No
Remind user prior to required auto-restart with dismissible reminder (hours)	*Leave this setting unconfigured*
Remind user prior to required auto-restart with permanent reminder (minutes)	*Leave this setting unconfigured*
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	7
Deadline for quality updates	2
Grace period	2
Auto reboot before deadline	Yes



Create Update ring for Windows 10 and later

Windows 10 and later

Update settings

Servicing channel: Semi-Annual Channel

Microsoft product updates *: [✓ Allow] Block

Windows drivers *: [✓ Allow] Block

Quality update deferral period (days) *: 0

Feature update deferral period (days) *: 0

Set feature update uninstall period (2 - 60 days) *: 10

User experience settings

Automatic update behavior: Reset to default

Restart checks: [✓ Allow] Skip

Option to pause Windows updates: [✓ Enable] Disable

Option to check for Windows updates: [✓ Enable] Disable

Require user approval to dismiss restart notification: Yes [✓ No]

Remind user prior to required auto-restart with dismissible reminder (hours): Number of hours, 2, 4, 8, 12, or 24

Remind user prior to required auto-restart with permanent reminder (minutes): Number of minutes, 15, 30, or 60

Change notification update level: Use the default Windows Update notifications

Use deadline settings: [✓ Allow] Not configured

Deadline for feature updates: 7

Deadline for quality updates: 7

Grace period: 2

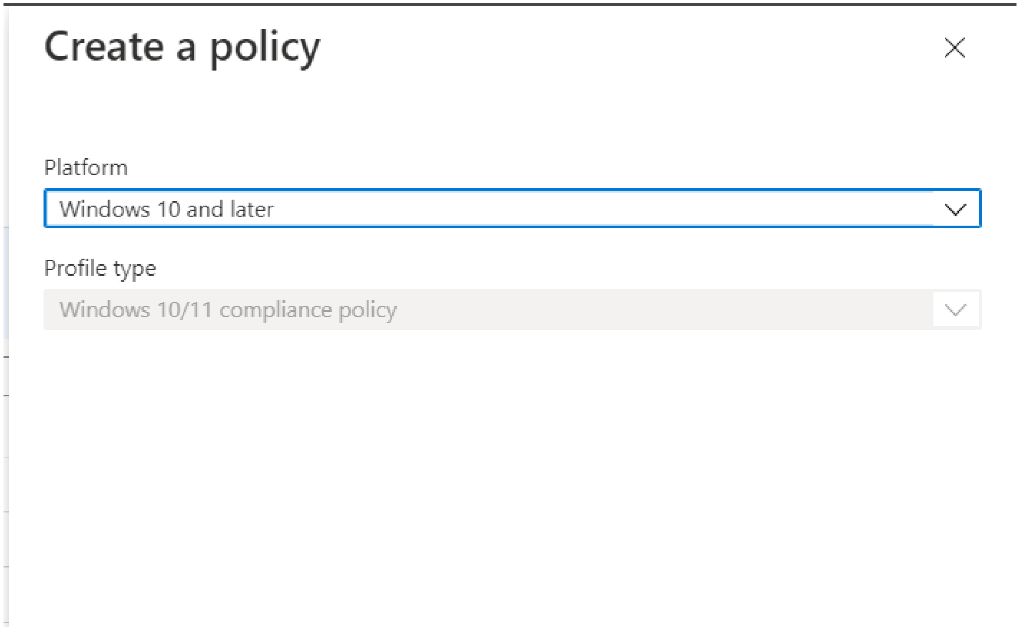
Auto reboot before deadline: [✓ Yes] No

4. Assign the Update Ring to the group you created in Step 1 (Create an Azure AD group).

Step 7: Deploy a Windows compliance policy

Configure a compliance policy to help monitor device compliance and health. The policy will be configured to report on noncompliance while still allowing users to use devices. You can choose how to address noncompliance with additional actions based on the organization's processes.

1. In Microsoft Endpoint Manager, navigate to **Devices > Compliance Policies > Policies > Create Policy.** For Platform, choose **Windows 10 and later > Create.**

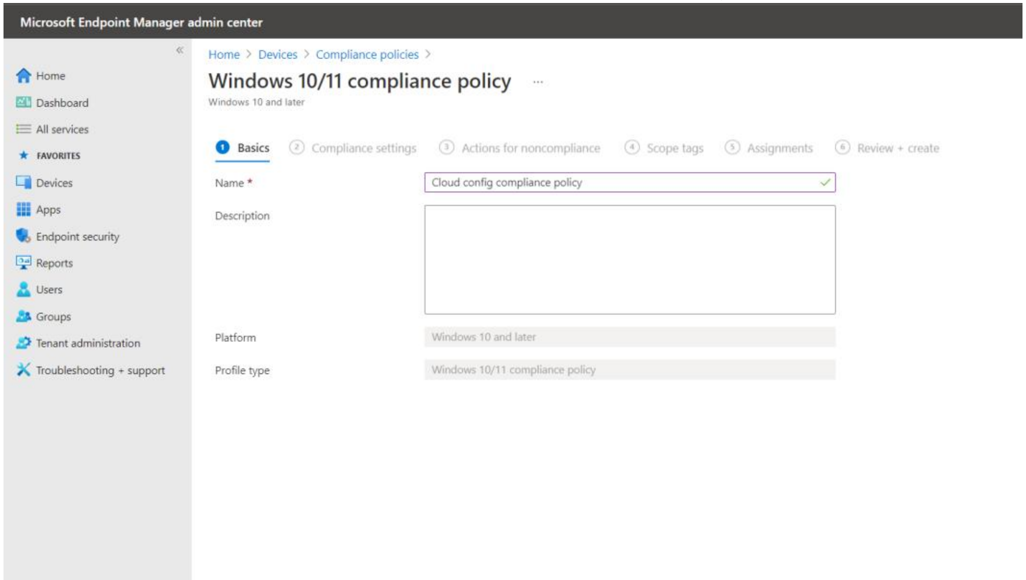


Create a policy

Platform: Windows 10 and later

Profile type: Windows 10/11 compliance policy

2. In the **Basics** section, choose a name for the compliance policy and choose **Next**.



Windows 10/11 compliance policy

Windows 10 and later

Name *: Cloud config compliance policy

Description:

Platform: Windows 10 and later

Profile type: Windows 10/11 compliance policy

3. In the **Compliance settings** section, configure the following values and choose **Next**.

Setting category	Setting	Value
Device Health	Require BitLocker	Require
	Require Secure Boot to be enabled on the device	Require
	Require code integrity	Require
System Security	Firewall	Require
	Antivirus	Require
	Antispyware	Require
	Require a password to unlock mobile devices	Require

	Simple passwords	Block
	Password type	Alphanumeric
	Minimum password length	8
	Maximum minutes of inactivity before password is required	1 Minute
	Password expiration (days)	41
	Number of previous passwords to prevent reuse	5
Defender	Microsoft Defender Antimalware	Require
	Microsoft Defender Antimalware security intelligence up-to-date	Require
	Real-time protection	Require

4. In the **Actions for noncompliance** section, for the Action "Marking device noncompliant", configure **Schedule (days after noncompliance)** to **1** (day). You can configure a different grace period based on your organization's preferences.

   If you are using Conditional Access policies in your organization, Microsoft recommends configuring a grace period so noncompliant devices do not immediately lose access to organization resources.
5. You can add an action to email users informing them of noncompliance with instructions on remediation.
6. Assign the compliance policy to the group you created in Step 1 (Create an Azure AD group).

Step 8: Optional additional configuration

Deploy additional essential productivity and line-of-business apps

You may have a few essential line-of-business apps that all devices need. Choose a minimum number of these apps to deploy. If you are delivering apps through a virtualization solution, deploy the virtualization client app to devices.

While there are no restrictions on the number or size of additional apps that can be deployed on top of the other apps defined in the cloud configuration, Microsoft recommends keeping these additional apps to a minimum based on what users need for their roles. Assign these essential apps to the group you created at the start of this process.

You may find that you need to deploy several line-of-business to some of your devices, or that these apps have complex packaging or procedure requirements. Consider moving these apps out of your cloud config deployment or keeping the devices that need these apps in your existing Windows management model. Cloud config is recommended for devices that need just a few key apps on top of collaboration and browsing.

Deploy resources that users might need to access organization resources

Be sure to configure essential resources that users may need depending on your organization's processes. These include certificates, printers, VPN connections, and Wi-Fi profiles.

In Microsoft Endpoint Manager, assign these resources to the group you created at the start of this process.

Configure preferred tenant domain name

Configure devices to automatically use your tenant's domain name for user sign-ins, so users don't have to type their whole UPN to sign in.

1. In Microsoft Endpoint Manager, navigate to **Devices > Windows > Configuration profiles** and choose **Create profile**.
2. For platform, choose **Windows 10 and later**. For Profile, choose **Device restrictions** and choose **Create**.
3. Choose a name for the profile and choose **Next**.
4. Under **Password**, configure the **Preferred Azure AD tenant domain** – enter the domain name that users will use to sign in to devices.
5. Assign the profile to the group you created at the start of this process.

Configure recommended settings for OneDrive Known Folder Move

Refer to this document with additional OneDrive settings recommended for Known Folder Move. These are not required configurations for Known Folder Move to work, but may help provide a better user experience.
[Recommended sync app configuration - OneDrive | Microsoft Docs]

Configure recommended Edge app settings

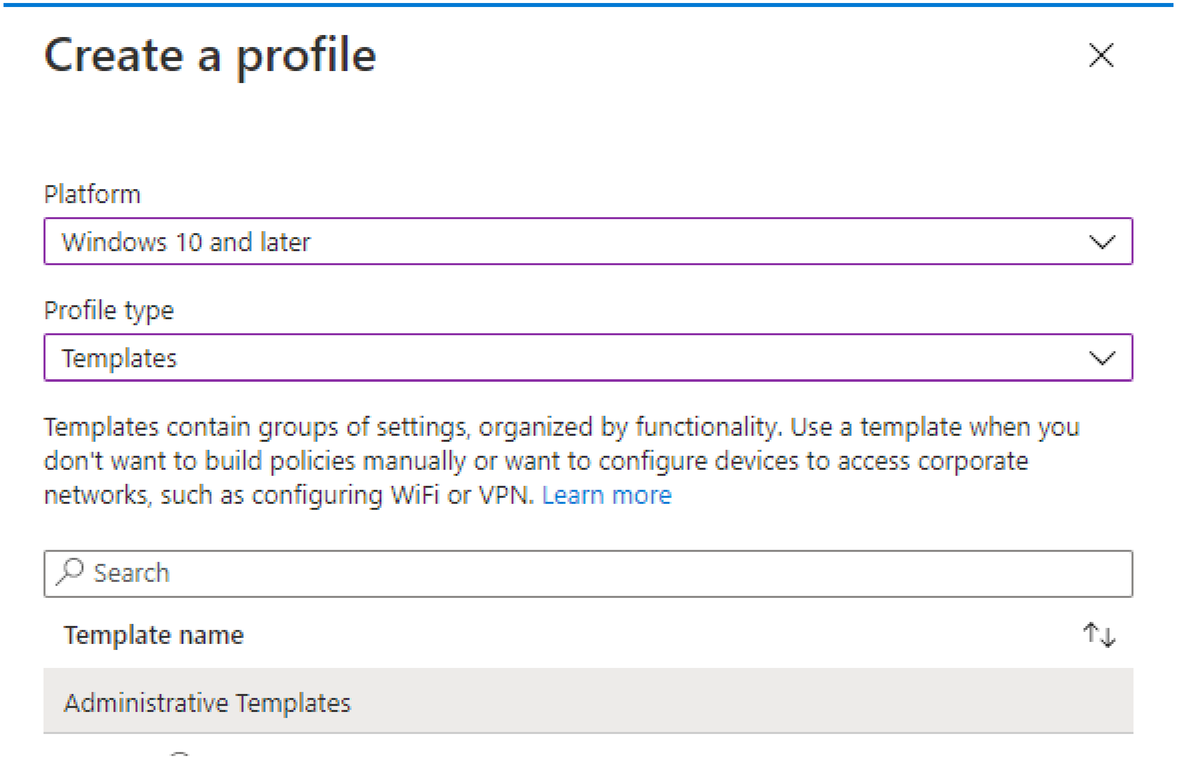
A few app settings for Edge can be configured to provide the best user experience. The following table lists the recommended settings. You can configure additional settings based on requirements or preference for the user experience. The SmartScreen settings are also enforced by Microsoft Defender. Configuring them through the Edge app will enable the Edge app to enforce them directly.

Setting Category	Setting	Value(s)
N/A	Configure Internet Explorer integration	Enabled, Internet Explorer mode
SmartScreen settings	Configure Microsoft Defender SmartScreen	Enabled
SmartScreen settings	Force Microsoft Defender SmartScreen checks on downloads from trusted sources	Enabled
SmartScreen settings	Configure Microsoft Defender SmartScreen to block potentially unwanted apps	Enabled

Use the following steps to configure these recommended settings:

1. In Microsoft Endpoint Manager, navigate to **Devices > Windows > Configuration profiles > Create profile.**
2. Choose **Windows 10 and later** for platform and choose **Administrative Templates** for profile type.

3. Choose **Administrative Templates** and choose **Create**.



Create a profile

Platform

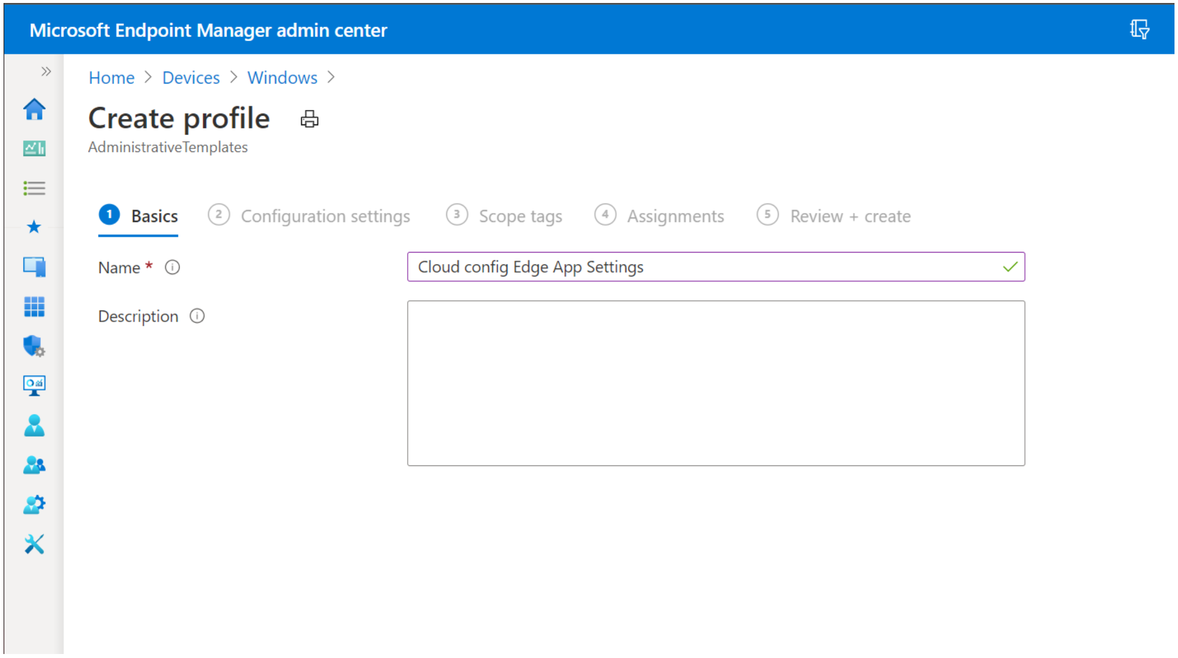
Windows 10 and later

Profile type

Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

4. Enter a name for the profile and choose **Next**.



Microsoft Endpoint Manager admin center

Home > Devices > Windows >

Create profile

AdministrativeTemplates

Name * : Cloud config Edge App Settings

Description :

5. In the **Configuration settings** section, search for the settings in the table above and configure them to their recommended values.
6. Assign the profile to the group you created at the start of this process.

Redeploy the Microsoft Store app if needed

If you removed the Microsoft Store using the recommended script in Step 3 and you want to restore it, you can do so using Microsoft Endpoint Manager and the Microsoft Store for Business or Microsoft Store for Education. Add the Microsoft Store app to your organization's app inventory and deploy it to devices using Microsoft Endpoint Manager.

Learn more about how to deploy Microsoft Store apps using Microsoft Store for Business or Microsoft Store for Education | Microsoft Docs

Get the Microsoft Store app on the Microsoft Store for Business

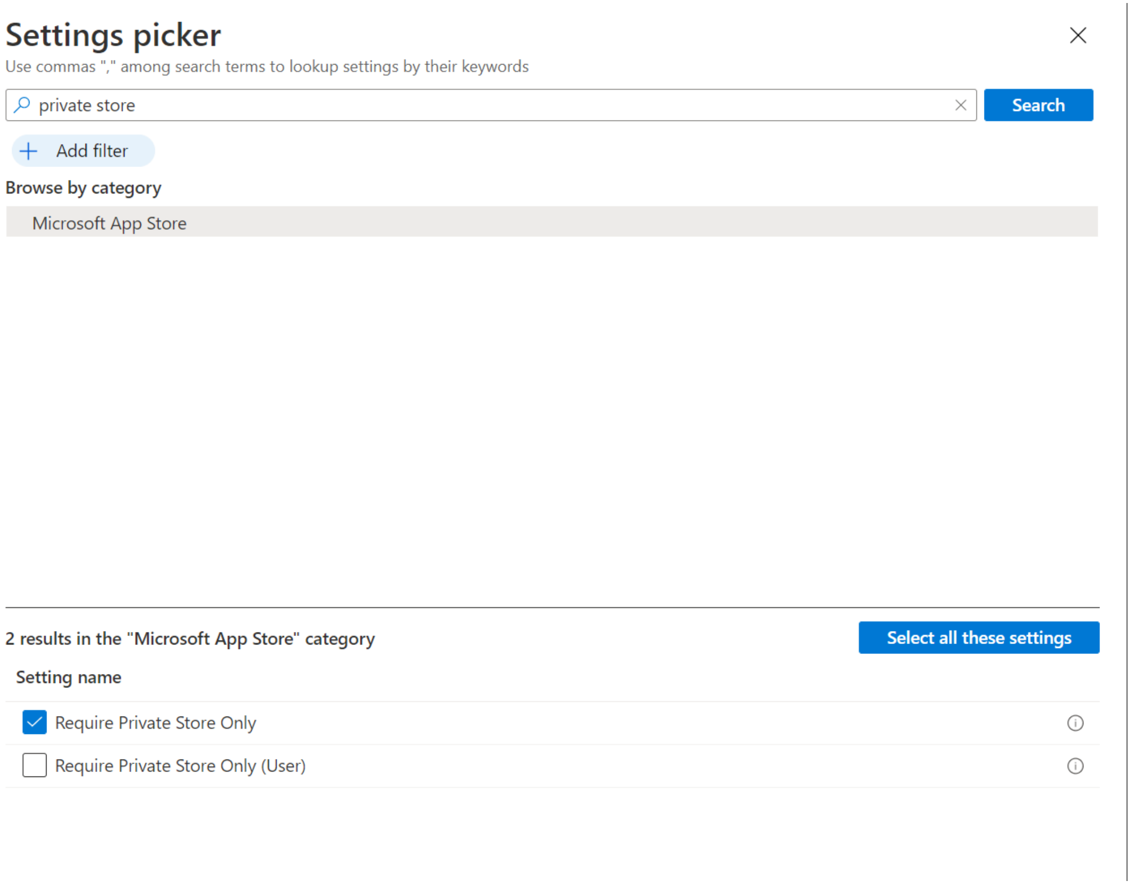
Get the Microsoft Store app on the Microsoft Store for Education

Block users from installing Microsoft Store apps on Windows 10 / 11 Enterprise and Windows 10 / 11 Education

If you keep or redeploy the Microsoft Store on devices, you can prevent users from installing apps outside of your organization's private store on Windows 10 / 11 Enterprise and Windows 10 / 11 Education.

1. In Microsoft Endpoint Manager, go to **Devices > Windows > Configuration profiles > Create profile**.
2. Choose **Windows 10 and later** for platform and choose **Settings catalog** for profile type. Select **Create**.
3. In the **Basics** step, choose a name for your profile.
4. In the **Configuration settings** step, choose **Add settings**.

5. In the Settings picker, search for “private store”. In the search results under the **Microsoft App Store** category, select **Require Private Store Only**.



Settings picker

Use commas "," among search terms to lookup settings by their keywords

private store

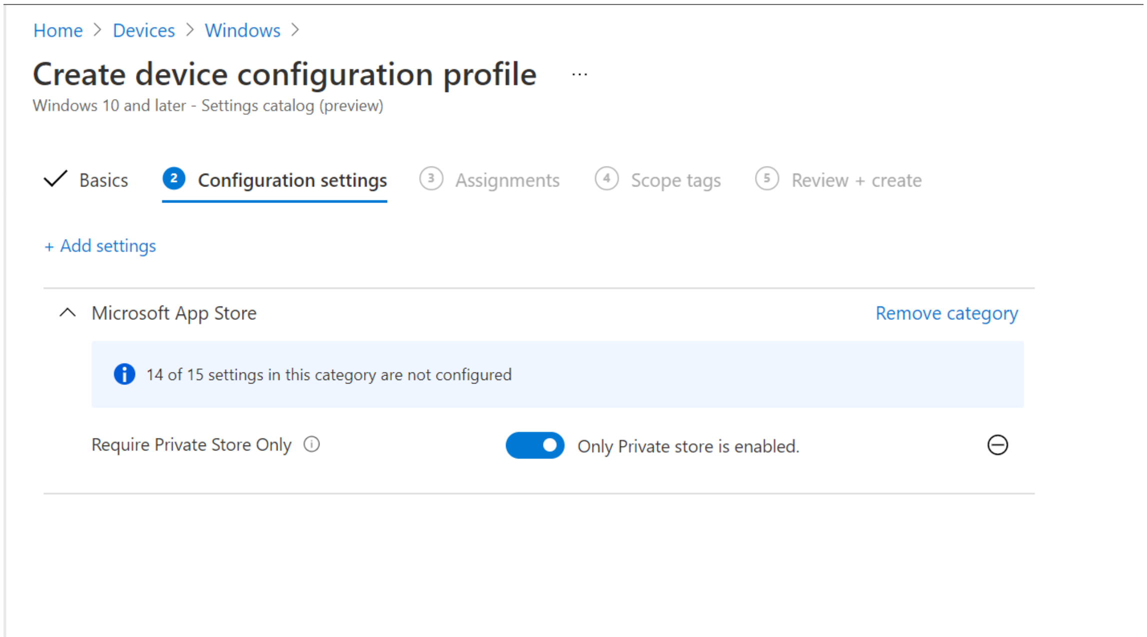
Browse by category

Microsoft App Store

2 results in the "Microsoft App Store" category

Setting name
☑ Require Private Store Only
□ Require Private Store Only (User)

6. In the **Configuration settings** step, set the **Require Private Store Only** setting to **Only Private store is enabled** and choose **Next**.



Home > Devices > Windows >

Create device configuration profile ...

Windows 10 and later - Settings catalog (preview)

Microsoft App Store

14 of 15 settings in this category are not configured

Require Private Store Only: Only Private store is enabled.

7. In the **Assignments** step, assign the profile to the group you created in Step 1.

8. In the **Review + create** step, review your profile and choose **Create**.

Monitoring the status of cloud config

Now that you have applied cloud config to your devices, you can use Microsoft Endpoint Manager to monitor the status of apps and device configurations.

Script status

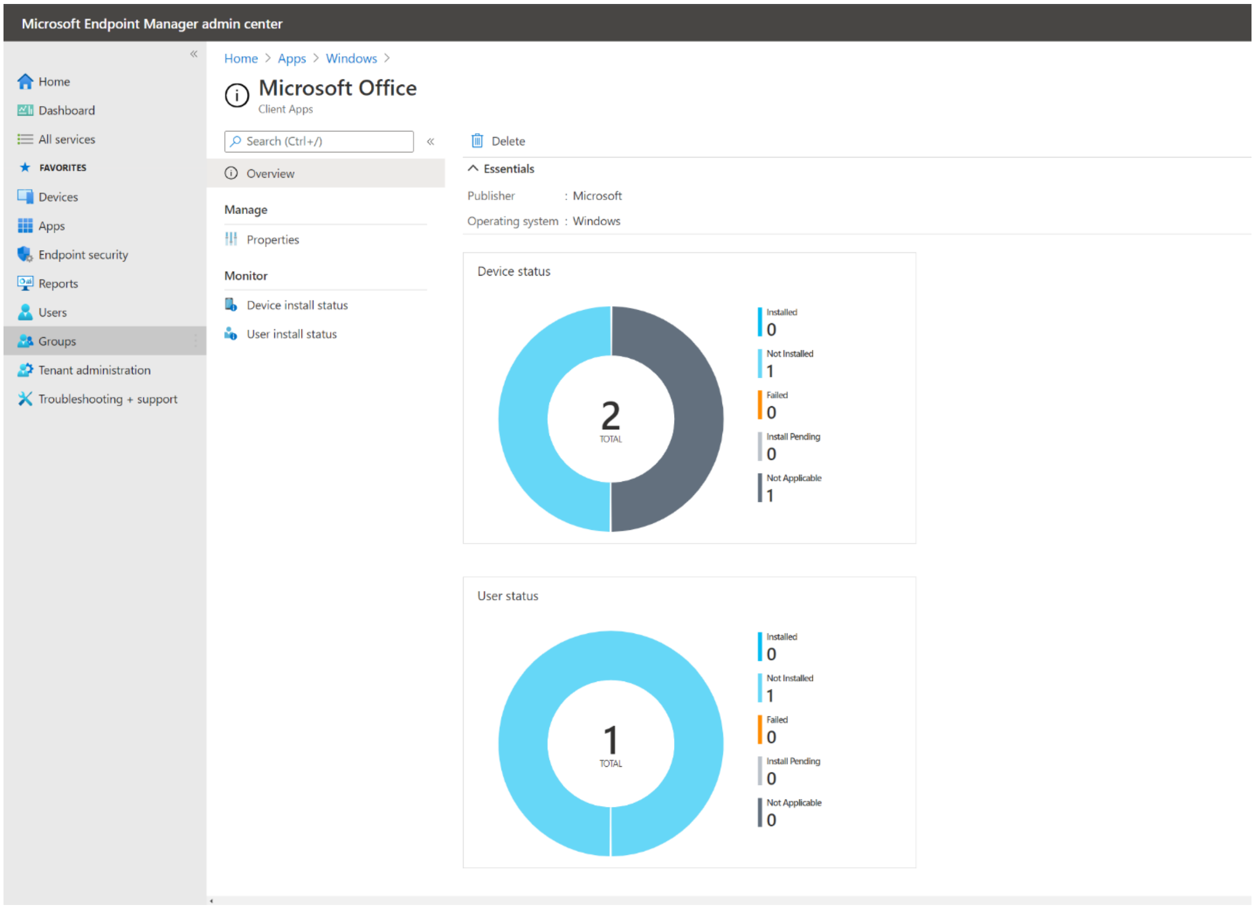
Use Microsoft Endpoint Manager to monitor the installation status of the script deployed to remove built-in Windows apps.

In Microsoft Endpoint Manager, go to **Devices > Windows > PowerShell scripts** and select the script you deployed from the list. In the script details page, choose **Device status** to view details on the installation of the script on managed devices.

App installations

App installation status can be monitored by navigating to an app in Microsoft Endpoint Manager and checking its device and/or user install status.

In Microsoft Endpoint Manager, go to **Apps > Windows > Windows apps**. Select one of the apps that you deployed as part of the cloud configuration (for example, the Microsoft 365 App Suite). Choose **Device install status** or **User install status** to view details on the installation status of the app.



Publisher : Microsoft
Operating system : Windows

You can also use troubleshooting tools to diagnose issues that individual devices or users may be experiencing. Review the following document to learn more about troubleshooting app issues with Microsoft Endpoint Manager:

Troubleshoot app installation issues - Intune | Microsoft Docs

Security baseline

In Microsoft Endpoint Manager, go to **Endpoint security > Security baselines** and choose the security baseline you deployed as part of clou config. The Overview pane displays information to help you monitor your baseline.

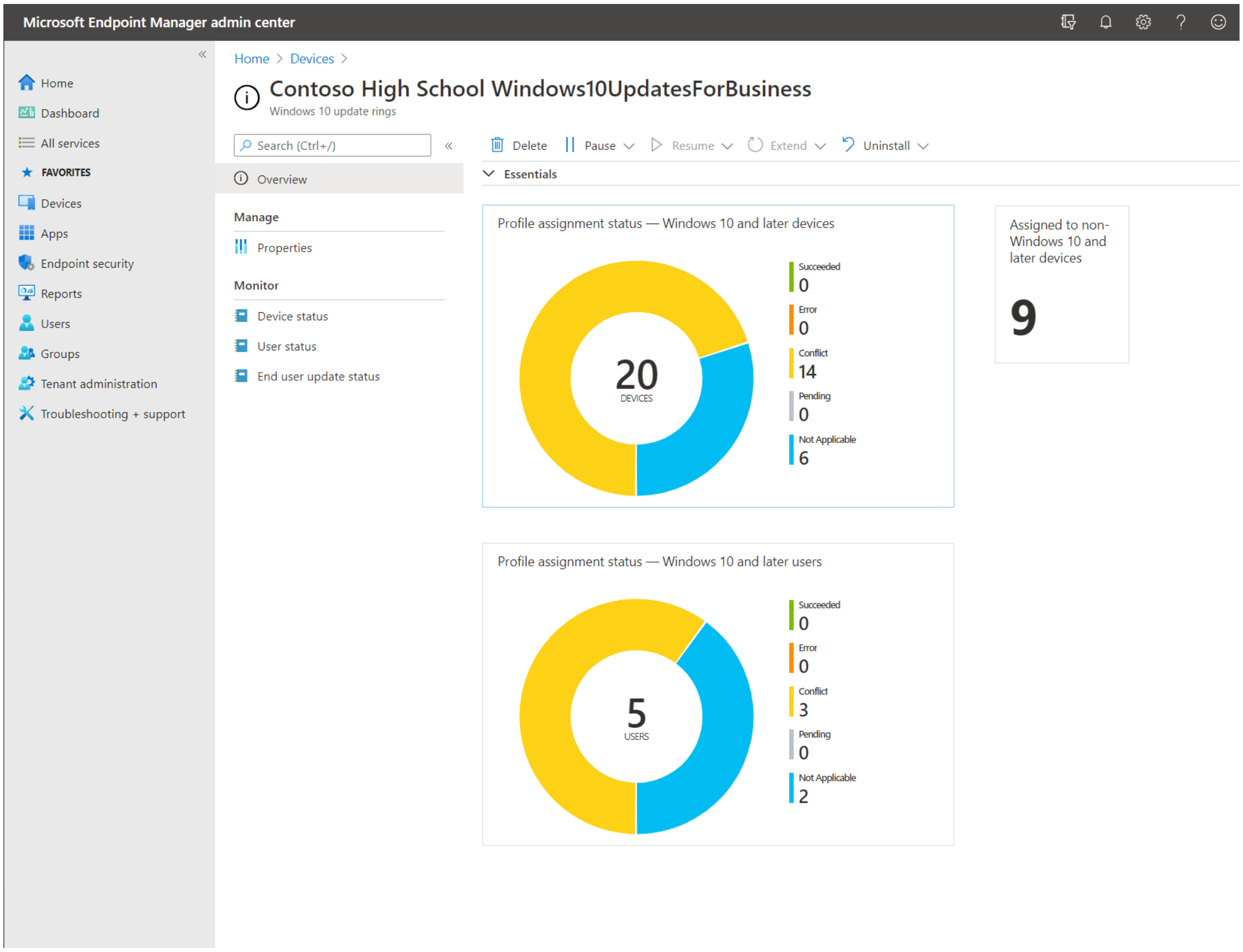
Check the success or failure of security baselines in Microsoft Intune - Azure | Microsoft Docs

Disk encryption profile (additional BitLocker settings)

In Microsoft Endpoint Manager, go to **Endpoint security > Disk encryption** and choose the disk encryption profile you deployed as part of cloud config. Choose **Device install status** or **User install status** to view details on the installation status of the profile.

Windows Update settings

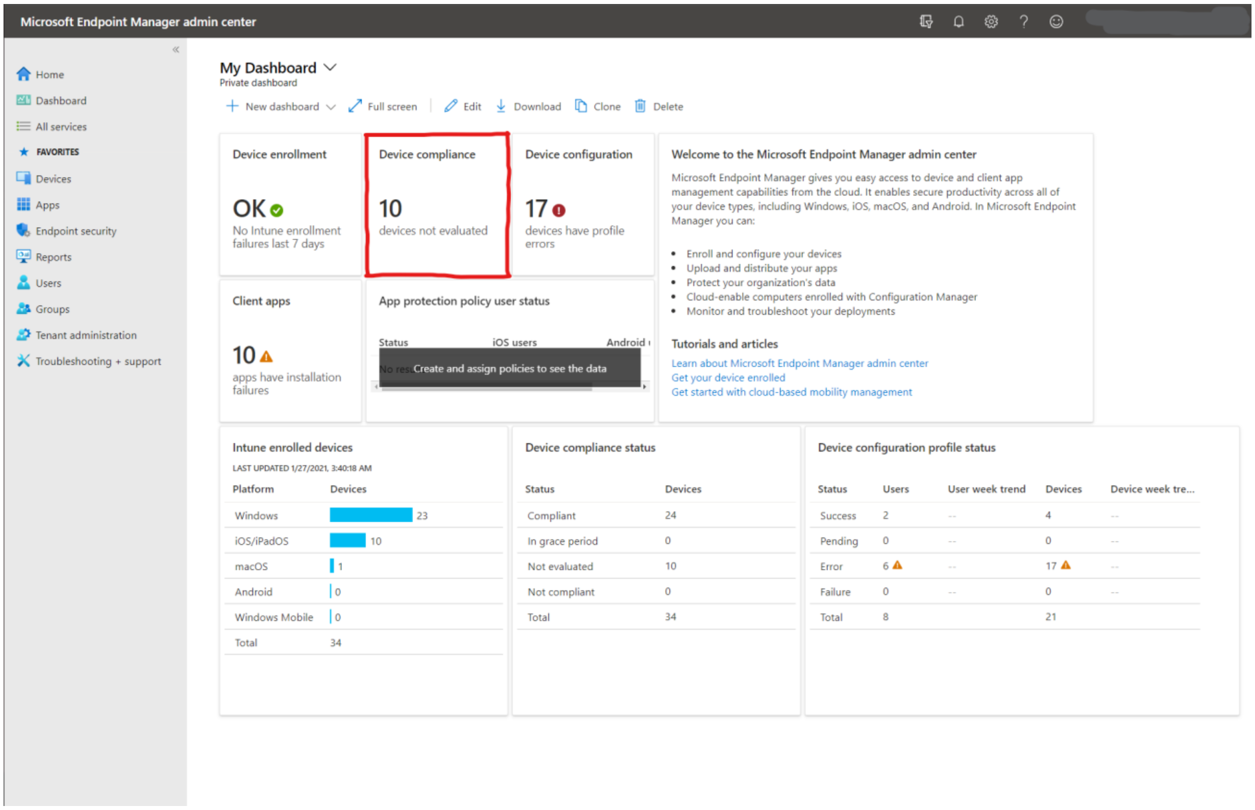
In Microsoft Endpoint Manager, go to **Devices > Update rings for Windows 10 and later** and choose the update ring you deployed as part of the cloud configuration. Choose **Device status, User status,** or **End user update status** to monitor the status of your update ring settings.



Compliance policy

Monitor device health using Microsoft Endpoint Manager to assess and take action on devices in a noncompliant state.

In Microsoft Endpoint Manager, go to **Dashboard** and select the **Device compliance** tile on the default dashboard.



My Dashboard
Private dashboard

Device enrollment

OK ✓
No Intune enrollment failures last 7 days

Device compliance

10
devices not evaluated

Device configuration

17 ●
devices have profile errors

Client apps

10 ⚠
apps have installation failures

App protection policy user status

Status	iOS users	Android u
No resu		

Create and assign policies to see the data

Welcome to the Microsoft Endpoint Manager admin center

Microsoft Endpoint Manager gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types, including Windows, iOS, macOS, and Android. In Microsoft Endpoint Manager you can:

- Enroll and configure your devices
- Upload and distribute your apps
- Protect your organization's data
- Cloud-enable computers enrolled with Configuration Manager
- Monitor and troubleshoot your deployments

Tutorials and articles

Learn about Microsoft Endpoint Manager admin center
Get your device enrolled
Get started with cloud-based mobility management

Intune enrolled devices

LAST UPDATED 1/27/2021, 3:40:18 AM

Platform	Devices
Windows	23
iOS/iPadOS	10
macOS	1
Android	0
Windows Mobile	0
Total	34

Device compliance status

Status	Devices
Compliant	24
In grace period	0
Not evaluated	10
Not compliant	0
Total	34

Device configuration profile status

Status	Users	User week trend	Devices	Device week tre...
Success	2	--	4	--
Pending	0	--	0	--
Error	6 ⚠	--	17 ⚠	--
Failure	0	--	0	--
Total	8		21	

The device compliance monitoring view provides detailed information on the assignment status and assignment failures of your compliance policies, along with views to quickly find noncompliant devices and take action.