



DE-ENSHITTIFY WINDOWS II



PAUL THURROTT

De-Enshittify Windows 11

How to make Windows 11 work for you, not against you

Paul Thurrott

This book is available at <https://leanpub.com/de-enshittifywindows11>

This version was published on 2026-03-01



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2026 Paul Thurrott

This book is dedicated to Windows users everywhere. You deserve better.

Contents

Introduction	1
The Enshittification of Windows	3
Start Fresh with a New Install of Windows 11	7
🤖 The problems with the Windows Setup OOBE	8
♥ Clean install Windows 11 to minimize or eliminate the enshittification	8
♥ Eliminate other Windows 11 Setup annoyances	24
De-Enshittify an Existing Install of Windows 11	27
♥ De-Enshittify Windows 11 with Win11Debloat	27
♥ Use Win11Debloat effectively	32
Make Windows 11 Respect Your Privacy	36
🤖 The problem with privacy in Windows 11	36
♥ Try to protect your privacy using the tools that Windows 11 provides	38
♥ Take control of your privacy with Win11Debloat	50
Make Windows 11 More Secure	53
🚫 The problems with not using a Microsoft account	53
♥ Windows 11 security first steps	55
♥ Improve your sign-in account security	60
♥ Configure additional security features Windows Security	63
♥ Remove third-party security apps	64
♥ Keep Windows 11 up-to-date	66
De-Enshittify Microsoft Copilot and AI	71
🤖 The problems with Copilot and AI in Windows 11	71
♥ Uninstall or disable Copilot and other AI features in Windows 11 . .	73
De-Enshittify Microsoft Edge	81

🤡	The problems with Microsoft Edge	81
🚫	Uninstall Microsoft Edge?	82
♥️	Use a different web browser as your default	82
♥️	Use Microsoft Edge as your default web browser	85
♥️	Eliminate other Microsoft Edge annoyances	92
De-Enshittify OneDrive		94
🤡	The problems with Microsoft auto-enabling OneDrive Folder Backup	94
♥️	Uninstall OneDrive	95
♥️	Prevent OneDrive from enabling Folder Backup when you set up a PC	96
♥️	Reverse the changes made by OneDrive Folder Backup	98
♥️	Eliminate other OneDrive annoyances	102
Fix Annoyances with Other Windows 11 In-Box Apps and Experiences .		105

Introduction

In 2022, journalist and Internet activist Cory Doctorow coined the term *enshittification* to describe how platform makers “capture more and more of the value that their users generated” for themselves. He then expanded on this concept in early 2023 to formally define how platforms decline in quality over time.

“Here is how platforms die,” he explained. “First, they are good to their users; then they abuse their users to make things better for their business customers; finally, they abuse those business customers to claw back all the value for themselves. Then, they die.

“I call this enshittification, and it is a seemingly inevitable consequence arising from the combination of the ease of changing how a platform allocates value, combined with the nature of a ‘two sided market’, where a platform sits between buyers and sellers, holding each hostage to the other, raking off an ever-larger share of the value that passes between them.”

Once you understand this concept, you see enshittification everywhere, but especially in personal technology products and services. In his book *Enshittification: Why Everything Suddenly Got Worse and What To Do About It*, Doctorow specifically highlights how online services like Amazon, Facebook, the iPhone, and Twitter all became enshittified over time. But the book also doesn’t deliver on its sub-title: There’s nothing that individuals can do about enshittification, he suggests, beyond hoping that antitrust regulators will put a stop to it.

I disagree with that. Antitrust regulation is important and it’s also having a moment here in the mid-2020s, with regulators and governments going after Big Tech companies and their illegal behaviors to a degree we’ve never seen before. But individuals *can* and should do what they can to combat enshittification, if only to improve matters for themselves. If Big Tech companies like Apple, Google, and Microsoft aren’t meeting your needs, you have alternatives. And you can fight back.

In this book, I of course focus specifically on the enshittification of Windows 11. But unlike Doctorow, I also explain what you can do to fight back by

countering the bad behaviors in this platform through fixes, workarounds, and configuration changes. In other words, this book is a pragmatic how-to guide, not a high-level polemic.

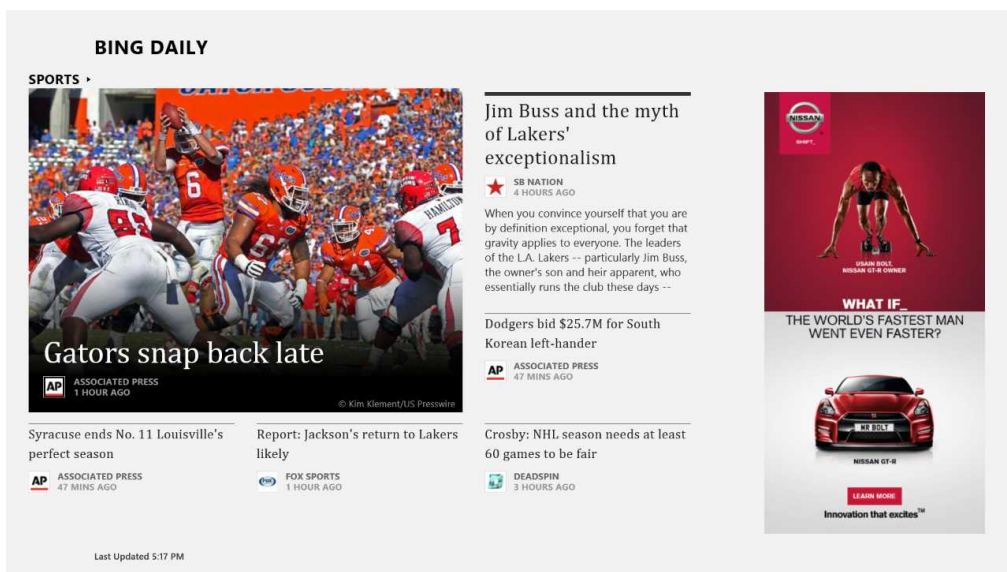
You could switch to an alternative platform, of course. The Mac is well-regarded, for example, and is perhaps the most obvious choice for those looking elsewhere. And other personal computing platforms like Chromebooks, the iPad, and even Linux can be viable choices, depending on your needs and, in the latter case, technical acumen. But having tried them all multiple times, I reject those choices. Despite its problems, Windows is still the best and most productive personal computing platform. And you can overcome all its bad behaviors and make it work the way you prefer.

That's what this book is all about.

Paul Thurrott
February 2026

The Enshittification of Windows

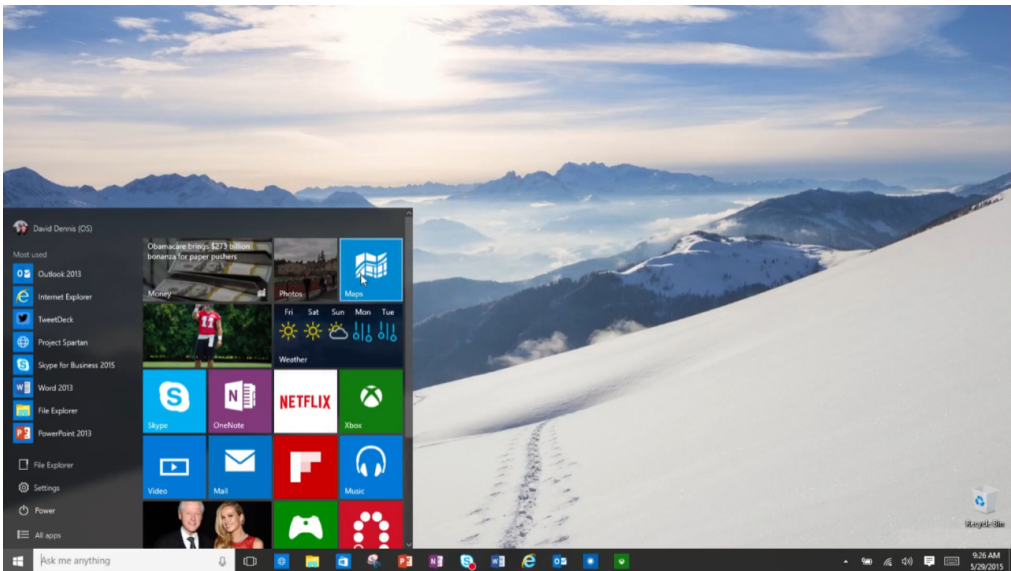
The enshittification of Windows began in 2012 when Microsoft released Windows 8 to nearly universal criticism and disdain. The biggest issue, of course, was the forced usage of a new full-screen “touch-first” user interface that didn’t make sense on the traditional PCs of the day. But Windows 8 was also notable for another negative reason. It was the first version of Windows to include advertising directly in the product, in the form of web-based display ads in Bing News, Bing Sports, Bing Weather, and some other bundled (“in-box”) apps.



At the time, I described this shift, subtle at first, as “a slippery slope.” What I meant was that Microsoft including ads directly in Windows was just the first step in a broader campaign to improve the software giant’s ability to monetize each Windows user. And that it didn’t put some ads in Windows 8 to only put fewer ads in the next version. No, this was going to get worse. Much worse.

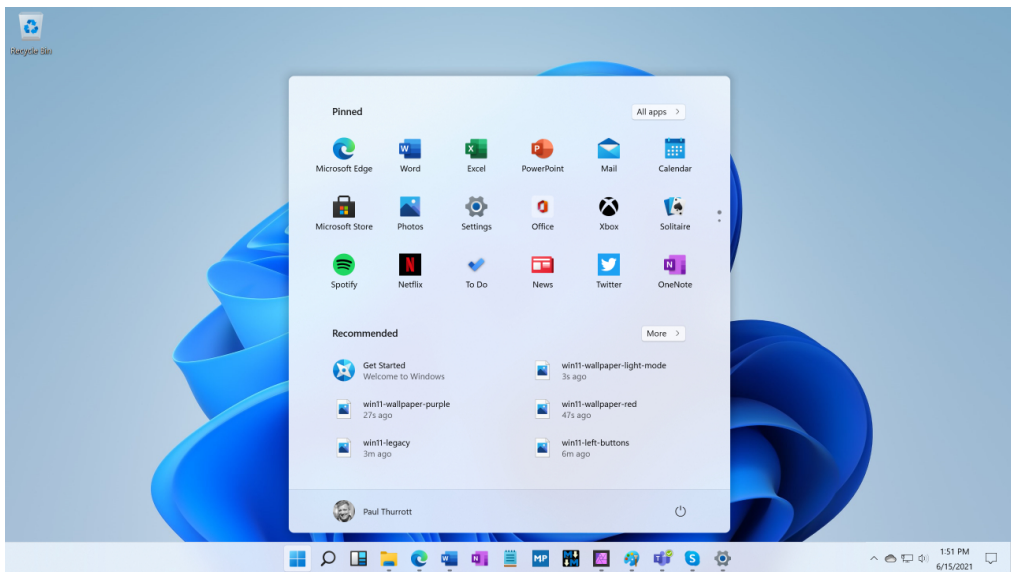
I'm not much of a prognosticator, but I could not have been more right on this count. Things *did* get much worse.

When Windows 10 debuted in 2015, it fixed some of Windows 8's most egregious and obvious problems, most notably by backing off from that touch-first interface and returning to a classic Desktop UI with a Start button, Start menu, and Taskbar. It was also the first truly free upgrade for a major Windows version, giving those still on Windows 7, Windows 8.x, and even some recent Windows Phone versions a way to move forward at no cost.



Well. No *overt* cost. As it turns out, Windows 10 escalated the bad behaviors that Windows 8 had only hinted at. That free upgrade came with hidden costs in the forms of far more in-box advertising, bundled crapware apps from third parties, forced feedback telemetry that could not be disabled, and a dramatic scaling back of one's ability to configure a default web browser and other apps. Worse, customers who adopted Windows 10 would be required to let Microsoft keep it up-to-date using a system called Windows as a Service (WaaS). This wasn't just a buggy and unreliable system, it was a running monthly commitment that would fix bugs *and* add new features to Windows 10. And customers would need to upgrade to a new Windows 10 product version twice ever year, a major, disruptive process that led to a string of major issues over several years.

Microsoft released Windows 11 in 2021, another free upgrade that was perhaps most notable at first for its simple and modern look and feel and a promise of fewer updates, with major product versions now appearing only once each year. But this was a lie: Microsoft instead escalated the release of new features, adding several or dozens more every single month. And Windows 11 carried forward the bad behaviors from Windows 10 while making some even worse.



Windows 11 continued the forced telemetry that Microsoft had introduced in Windows 10. It continued to bundle third-party crapware. It closed the vice on local accounts, forcing more and more users to sign in to the OS using their Microsoft accounts (MSAs). It escalated the bad behaviors in its web browser, Microsoft Edge, by forcing it on users even when they had picked another default browser. It changed the hardware requirements arbitrarily in a bid to force customers to upgrade to new PCs. And it enabled the Folder Backup feature in OneDrive even when users declined multiple offers to do so.

Today, we have a term for this process by which a platform maker, in this case Microsoft, makes a product, in this case Windows, worse for its customers because doing so furthers its strategic aims. That term is *enshittification*. And Windows 11 has emerged as a key example of how a once customer-driven

product can be enshittified to the point where even its most dedicated users begin researching alternatives and plan an exit strategy.

No one has spent more time on this research than me—even with my focus on Windows for over 30 years, I first started experimenting with Linux using the floppy disk-based Slackware distribution in the mid-1990s—and the result of this work is clear. Yes, there are reasonable personal computing alternatives out there, most notably the Mac. And yes, there are possible alternatives for some in the form of an iPad, Chromebook, or even Linux. But there is nothing like Windows. And it's possible, despite Microsoft's best efforts, to make Windows 11 work the way you want. In fact, it's not all that difficult or time consuming. You just need to know where to look and what to do.

Good news. This book is where to look. And it will tell you what to do to de-enshittify Windows 11.

Start Fresh with a New Install of Windows 11


When you buy a new PC or reset an existing PC, Windows 11 initially boots into Windows Setup and displays its Out of Box Experience (OOBE), a multi-step process through which you configure the system for use.


This process is called a *clean install*, which is ironic as there's nothing particularly clean about it: Microsoft uses the Windows Setup OOBE to force and coerce customers to configure Windows 11 in ways that benefit the company more than its users. And a “clean” install of Windows 11 will be enshittified with Microsoft's forced telemetry, preinstalled crapware, forced Microsoft account sign-in, and forced Microsoft Edge usage whether you use the browser or not.

Fortunately, there is a better way to clean install Windows 11. Or, I should say, there are a few *other* ways in which to install Windows 11 in a cleaner configuration than Microsoft would prefer. Which you choose will depend on your needs and wants. Your choices include:

- **Clean install Windows 11 using a Microsoft software image that was lightly modified by a third-party utility.** You can use a tool called [Rufus](#) to modify the stock Microsoft software image to bypass the Windows 11 hardware requirements *and* the forced Microsoft account sign-in. Afterward, you can clean the Windows 11 installation manually or, using a third-party tool, semi-automatically.
- **Clean install Windows 11 using a heavily modified software image that eliminates all the problematic behavior.** In addition to Rufus, you can use a tool called [Tiny11 Builder](#) to create a clean, de-enshittified installation of Windows 11 with none of the problematic behaviors we see in the stock installation. This install is so clean that you may need to install some Windows 11 in-box apps from the Microsoft Store afterward. But I think it's worth it.

This chapter describes both methods for creating a cleaner or truly clean Windows 11 installation.

 **Warning:** Please note that a clean install is destructive, meaning that any existing Windows installation on the PC will be erased and overwritten, as will any of your installed apps and personal data. Unless you're doing this on a new PC or a newly reset PC, you will need to back up anything important first.

 **Learn more:** If this approach is undesirable, jump ahead to the [De-enshittify an existing install of Windows 11](#), where you can learn how to de-enshittify Windows 11 without performing a clean install and losing everything.

The problems with the Windows Setup OOBE

The Windows Setup OOBE is the first thing you see when you start a new PC for the first time or have just reset Windows 11 to bring it back to its initial as-new state. So it is perhaps not surprising that Microsoft has evolved this experience over the years to introduce some bad behaviors. Among them:

Enforced hardware requirements. The OOBE enforces the Windows 11 hardware requirements even though any computer that can run Windows 10 can also run Windows 11 effectively.

Microsoft account requirement. The OOBE requires you to sign in with a Microsoft account or a Microsoft Work or School account and no longer offers a way to use the local account type that many power users prefer.

Privacy theater. The OOBE provides a privacy screen that gives you a false sense of protection, but it ignores the most privacy-adverse behaviors in Windows 11. For example, you cannot disable telemetry.

Advertising. The OOBE advertises Microsoft services like Xbox Game Pass and Microsoft 365

Upsells. The OOBE tries to upsell you to Microsoft 365 Premium if you already have a Microsoft 365 Personal or Family subscription

♥ Clean install Windows 11 to minimize or eliminate the enshittification

Ready to get started? Great. Let's clean install Windows 11.

Gather what you need

To follow the instructions in this chapter, you will need:

- A USB flash drive with at least 8 GB of storage.
- [The current Windows 11 ISO \(disk image\) file from the Microsoft website](#). Scroll down to “Download Windows 11 Disk Image (ISO) for x64 devices,” choose “Windows 11 (multi-edition for x64 devices)” from the Select Download drop-down box, click “Confirm,” choose the product language, click “Confirm,” and then click “64-bit Download.”
- [Rufus](#). This is a utility that can use a Windows 11 ISO to create USB-based installation media. Select the “Standard” download.
- [Tiny11 Builder](#) (Optional). This is a PowerShell script that aggressively de-enshittifies the standard Windows 11 ISO. The download is hidden under the green “Code” button. Select “Download ZIP” and then unarchive the ZIP file you download.
- An Ethernet connection or your Wi-Fi drivers. If you use Tiny11 Builder to create a heavily modified Windows 11 ISO, you will need to connect the PC or Ethernet or have your PC's Wi-Fi drivers ready when you set up the system.

(Optionally) Use Tiny11 Builder to create a heavily-modified Windows 11 ISO

If want to aggressively de-enshittify your clean install of Windows 11, you use Tiny11 Builder to modify the Windows 11 ISO you downloaded. There's nothing like [Tiny11 Builder](#). This is a PowerShell script written by a technical enthusiast that builds what its author describes as “a trimmed-down Windows 11 image.” What he means is that Tiny11 Builder de-enshittifies Windows 11 Setup so that anyone can create a clean, de-enshittified installation of

Windows 11 that includes none of the problematic behaviors we see in the stock installation.

As noted, Tiny11 Builder is *aggressive*. In addition to removing key enshittification vectors like Microsoft Copilot, Microsoft Edge, and OneDrive from the installation, it removes dozens of other apps, including Clipchamp, Media Player, Xbox, and others that might be useful to you. But no worries: You can install any apps you do need from the Microsoft Store later. What you *can't* do is customize the installation to change what installs up-front. You either use Tiny11 Builder as-is or you do not.

→ **Learn more:** This tool may be too radical for you. That's OK. You can optionally de-enshittify any existing installation of Windows 11 and achieve most of what's possible using Tiny11 Builder. This is described in [De-enshittify an existing install of Windows 11](#).

If you're ready to proceed with Tiny11 Builder, here are the steps.

Mount the Windows 11 ISO as a virtual Setup disk. Double-click the Windows 11 ISO you downloaded to mount it as a virtual disk. When it's ready, it will open in a new File Explorer window. Take note of the drive letter that Windows 11 assigned to this disk.

Open an elevated Terminal window. Use Start Search to find the Terminal app. Instead of clicking it normally, right-click it and choose "Run as Administrator" from the context menu that appears.

Bypass script execution blocking. Run the following command in the Terminal window to bypass Windows 11's script execution blocks for this session only.

```
Set-ExecutionPolicy Bypass -Scope Process
```

Run Tiny11 Builder. Navigate to the extracted Tiny11 Builder folder in the Terminal window (`cd C:\Users\paul\Downloads\tiny11builder-main` or similar) and then run Tiny11 Builder using the following command line:

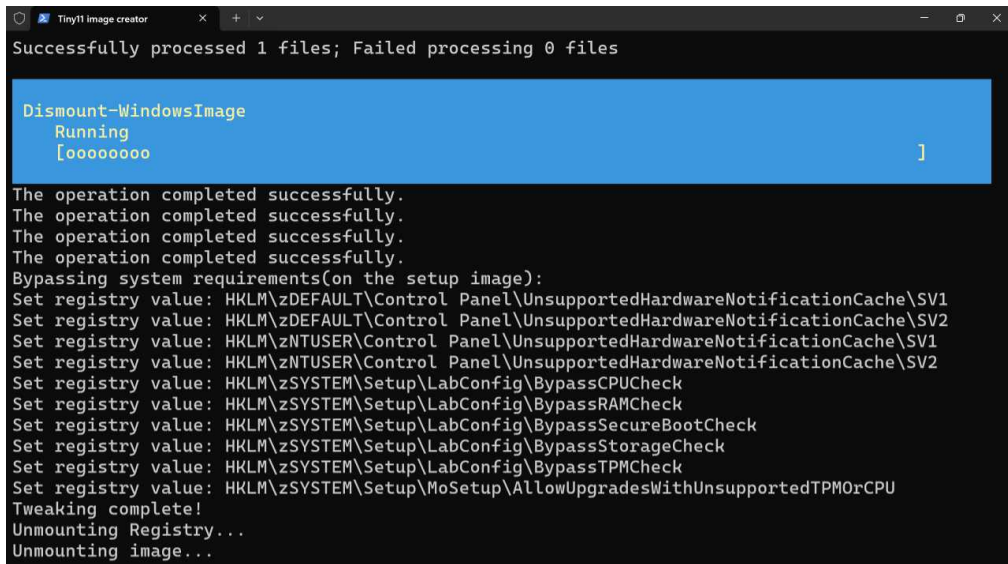
```
.\tiny11maker.ps1
```

Enter the drive letter of the Windows 11 virtual drive as prompted. Tiny11 Builder will ask you to enter the drive letter of the virtual Windows 11 Setup disk. You do so by typing *D* or whatever letter without the colon.

Select the correct Windows 11 product edition. Tiny11 Maker will make a copy of the Setup image (install.wim) and then present you with a list of Windows 11 product editions from which to choose. Enter the appropriate number (1 for Home, 6 for Pro).

✓ **Tip:** It's crucial that you get this right because Windows 11 will not activate if you enter the wrong number. If you're not sure which product edition is correct, you can use *winver* to find it: Open a Run dialog (by typing Windows Key + R), type *winver*, click "OK," and the window that appears will indicate whether you are running Windows 11 Home or Pro.

Sit back and relax. Now, Tiny11 Maker will process the Setup image, make the changes, and export a new ISO (image) file named *tiny.iso*. This process takes about 30 minutes. You will find *tiny.iso* in the extracted Tiny11 Builder folder.



```
Tiny11 image creator
Successfully processed 1 files; Failed processing 0 files

Dismount-WindowsImage
Running
[ooooooooo]

The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
Bypassing system requirements(on the setup image):
Set registry value: HKLM\zDEFAULT\Control Panel\UnsupportedHardwareNotificationCache\SV1
Set registry value: HKLM\zDEFAULT\Control Panel\UnsupportedHardwareNotificationCache\SV2
Set registry value: HKLM\zNTUSER\Control Panel\UnsupportedHardwareNotificationCache\SV1
Set registry value: HKLM\zNTUSER\Control Panel\UnsupportedHardwareNotificationCache\SV2
Set registry value: HKLM\zSYSTEM\Setup\LabConfig\BypassCPUCheck
Set registry value: HKLM\zSYSTEM\Setup\LabConfig\BypassRAMCheck
Set registry value: HKLM\zSYSTEM\Setup\LabConfig\BypassSecureBootCheck
Set registry value: HKLM\zSYSTEM\Setup\LabConfig\BypassStorageCheck
Set registry value: HKLM\zSYSTEM\Setup\LabConfig\BypassTPMCheck
Set registry value: HKLM\zSYSTEM\Setup\MoSetup\AllowUpgradesWithUnsupportedTPMOrCPU
Tweaking complete!
Unmounting Registry...
Unmounting image...
```

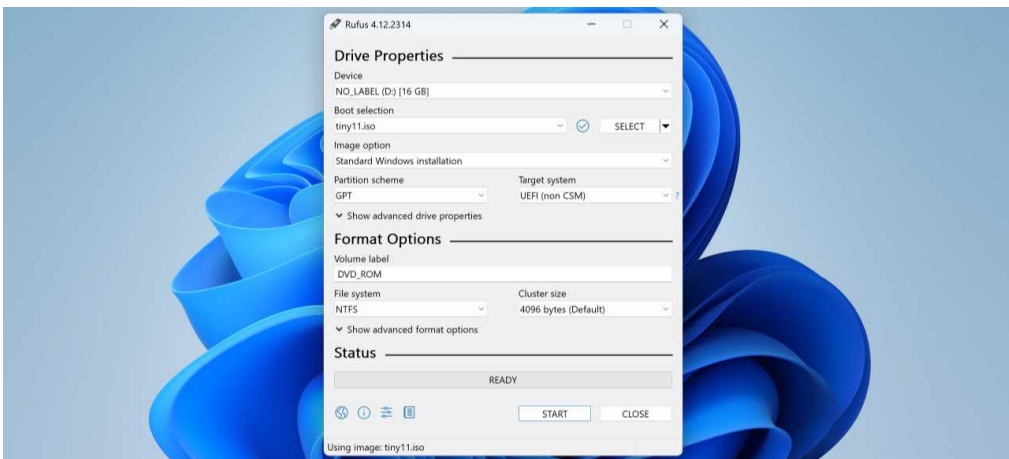
Create the Windows 11 installation media

Microsoft offers a free tool that can be used to create USB-based installation media using the stock Windows 11 ISO file. But we will use [Rufus](#) instead because it can modify the installation media so that Windows Setup doesn't force the Windows 11 hardware requirements or Microsoft account sign-in on you.

Here's the right way to create Windows 11 installation media.

Insert your USB drive into the PC. Remember, its contents will be deleted during this process.

Run Rufus. Run the Rufus EXE directly from the Downloads folder (or wherever you download it to).



Select the Windows 11 (or Tiny11 Builder) ISO image. Click the “SELECT” button and use the Open file dialog that appears to locate and select the stock Windows 11 ISO image file or the tiny11.iso image file you just created with Tiny11 Builder.

Start creating the installation media. Click “Start.” A “Windows User Experience” dialog appears.



Accept the defaults. For the most part, the default options—with “Remove requirement for 4GB+ RAM, Secure Boot and TPM 2.0” and “Remove requirement for an online Microsoft account”—are fine, even if you wish to use a local account for some reason. Click “OK” to create the installation media.

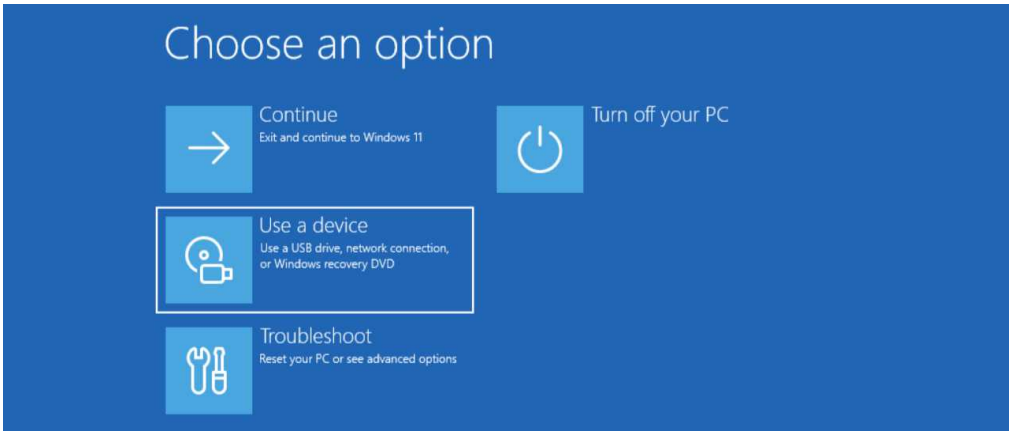
i More info: To be clear, I do not recommend signing in to Windows 11 with a local account instead of using a Microsoft account. I do understand that this is desirable for certain power users.

Boot your PC with the Windows 11 installation media

Now that you’ve created the Windows 11 installation media with Rufus, you can use it to install Windows 11. First, you have to figure out how to boot the PC with that installation media.

All PCs offer some way to boot from a USB drive instead of the normal internal system drive. This can be configured in the PC’s firmware (what we used to call the BIOS). But you can usually tap a certain key—often Esc, F1, F11, F12, or Enter—when the PC first boots up to display a boot menu so you can choose another drive instead. You will need to refer to your PC maker’s documentation to find the method that works for your PC.

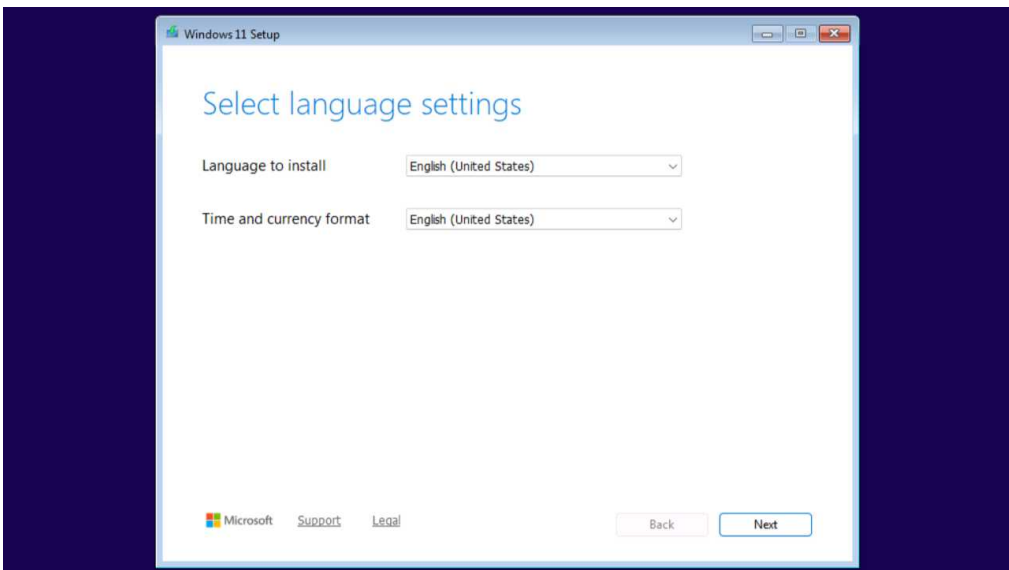
But if you are already running Windows on the PC you’re about to clean up, there’s an easier way: Open the Settings app, navigate to System > Recovery, and click the “Restart now” button next to “Advanced startup.” The PC will reboot into the Windows Recovery Environment (WRE).



Here, select “Use a device” and then “USB” (or similar). Now, the PC will boot using your USB-based Windows 11 installation media.

Step through the Windows Setup first-run experience

Booting with the Windows 11 installation media, you will first encounter the Windows Setup first boot experience, an old-school user interface that hasn’t changed much in over 20 years and is used mostly by PC makers and system builders.



You will step through the following screens:

Select language settings. Click “Next.”

Select keyboard settings. Click “Next.”

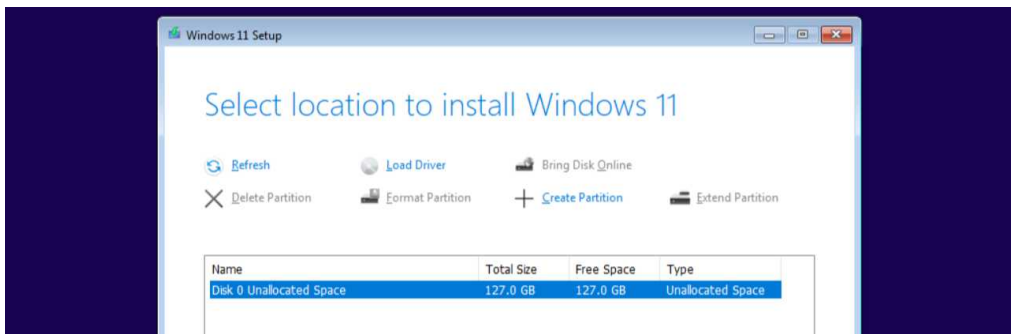
Select Setup option. Make sure “Install Windows 11” is selected, check the box agreeing that you’re about to wipe out the contents of this PC, and click “Next.”

Product key. Click “I don’t have a product key” and then click “Next.” Most PCs have a Windows 11 product key built into their firmware.

Select image. Choose the correct Windows 11 product edition—usually Home or Pro—and then click “Next.”

Applicable notices and license terms. Click “Accept.”

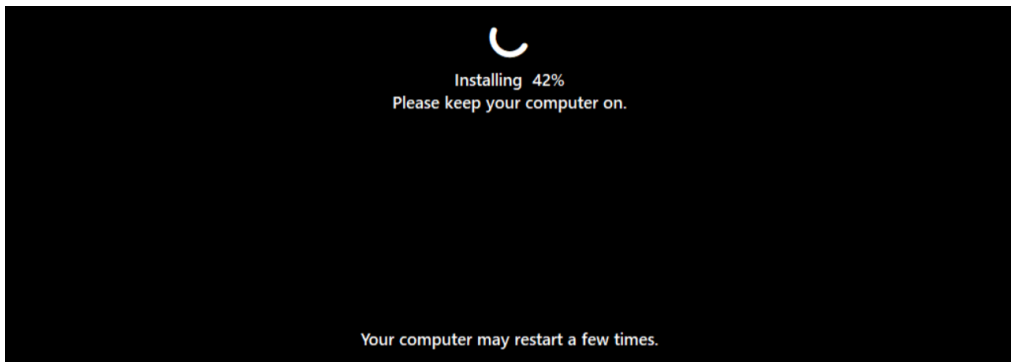
Select location to install Windows 11. Here, you will delete all the partitions on Disk 0. When that’s done, select “Disk 0 Unallocated Space” and click “Next.”



Installing Windows 11. There’s nothing to do during this full-screen medium blue experience except watch and wait. Eventually, the PC will reboot into another full-screen experience ...



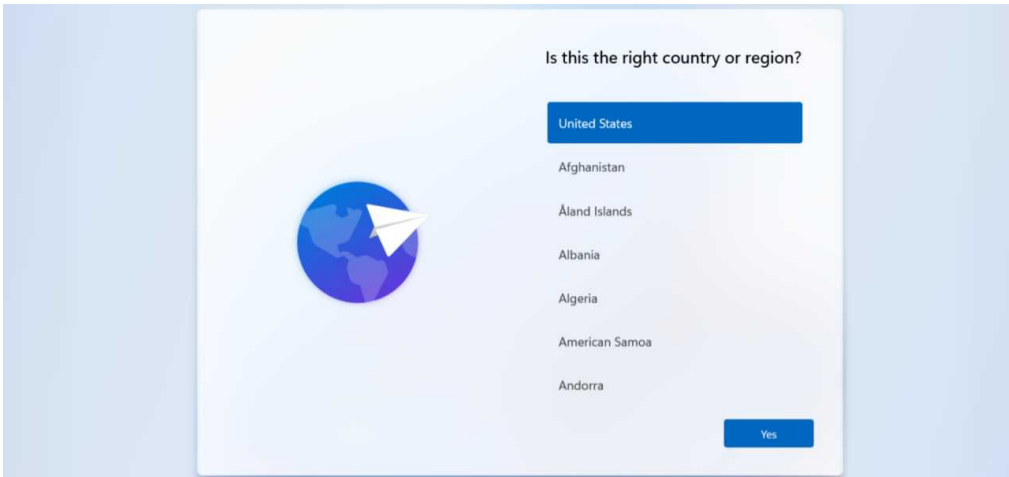
Installing. During this installation phase, the PC could reboot a few times. Here, too, there is nothing to do but wait.



Eventually, the PC will reboot again and display the Windows Setup OOBE.

Step through the Windows Setup Out of Box Experience (OOBE)

The Out of Box Experience (OOBE) is what everyone sees when they power on a new (or newly reset) PC for the first time. This is prettier and more graphical than the first-run experience. But what you see here can vary and will depend in part on which ISO you used to create the installation media.



i More info: If your Windows 11 installation media was modified with Tiny11 Builder, remember that you will need an Ethernet cable or your PC's Wi-Fi drivers to connect to the Internet during the OOBE. And if you are installing Windows 11 on a laptop, its touchpad may not work, in which case you won't see or be able to use the mouse cursor to select items on-screen. To get around that, plug in a mouse if possible or just use keyboard navigation: Tab to move between selectable items and Enter or Space to select one.

Depending on the choices you make, you will step through some or all of the following screens. And because Microsoft changes the OOBE from time-to-time, there could be additional steps not noted here.

Is this the right country or region? Click "Yes."

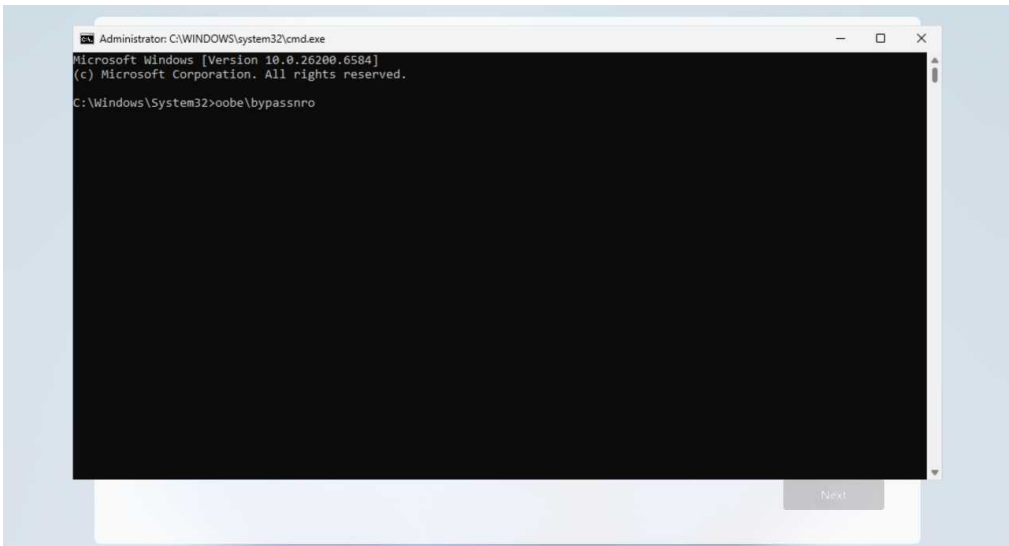
Is this the right keyboard layout or input method? Click "Yes."

Want a second keyboard layout? Click "Skip."

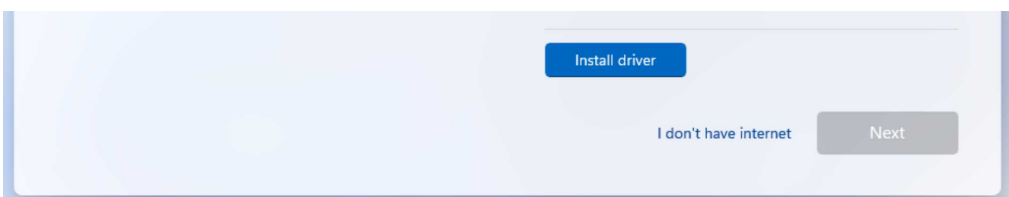
Let's connect you to a network. This is where things get interesting. In this book, I assume that [you will sign in to Windows 11 using a Microsoft account because that's the right choice for most users](#). But power users may want to sign in with a local account instead.

- If you used a stock Windows 11 ISO to create the installation media, you

can connect to your Wi-Fi network now and continue normally. Click “Next.” Power users can optionally type Shift + F10 to open a command line window and type the command `oobe\bypassnro` to reboot the PC to see the “I don’t have internet” option noted below.



- If you used a modified Tiny11 Builder IOS to create the installation media, you will likely see an “Install driver” button and an “I don’t have internet” link. Here, I will assume you connect your PC to the Internet using a wired (Ethernet) connection, in which case that network will appear and you can continue normally. But power users can choose the link and create a local account, bypassing most of the OOBEScreen. Click “Next.”



Name your device. Here, you can optionally name your PC. If you do so now, the PC will reboot before you can continue.

How would you like to set up this device? Here, you can choose to sign in to Windows 11 using your Microsoft account or Microsoft Work or School account. I assume you are doing this on a PC you own, so select “Set up for personal user” and then click “Next.”

Unlock your Microsoft experience. Click “Sign in.”

Let’s add your Microsoft account. Enter your email address, click “Next,” and then sign in and authenticate with your Microsoft account as prompted.

Want to use your face/finger to sign in faster and more securely? If your PC supports Windows Hello facial or fingerprint recognition, you can enroll your face or a finger now by clicking “Yes, set up,” following the prompts, and then clicking “Next.” Otherwise, you can click “Skip for now.”

Got it! Now set up a PIN. Windows 11 requires you to create a PIN—which can be four or more digits and/or include alphabetical characters—when you sign in using an online account like your Microsoft account. So click “Create PIN,” create and confirm the PIN you wish to use, and click “OK.”

Choose privacy settings for your device. Here, you can choose which privacy-related settings you wish to leave enabled. My advice is to leave “Location” and “Find my device” enabled and to disable all other options. Then, click “Accept.”

➔ **Learn more:** You can learn more about these and other Windows 11 privacy options in the [Make Windows 11 respect your privacy](#) chapter.

Let’s customize your experience. Let’s not. Click “Skip.”

Use your phone from your PC. You can set this up later using the Phone Link app. Click “Skip.”

Always have access to your recent browsing data. This is tied to a key enshittification in [Microsoft Edge](#). Do not allow this. Click “Not now.”

Microsoft 365 and Xbox Game Pass promotional screens. Regardless of whether you have a Microsoft 365 or Xbox Game Pass subscription, Microsoft

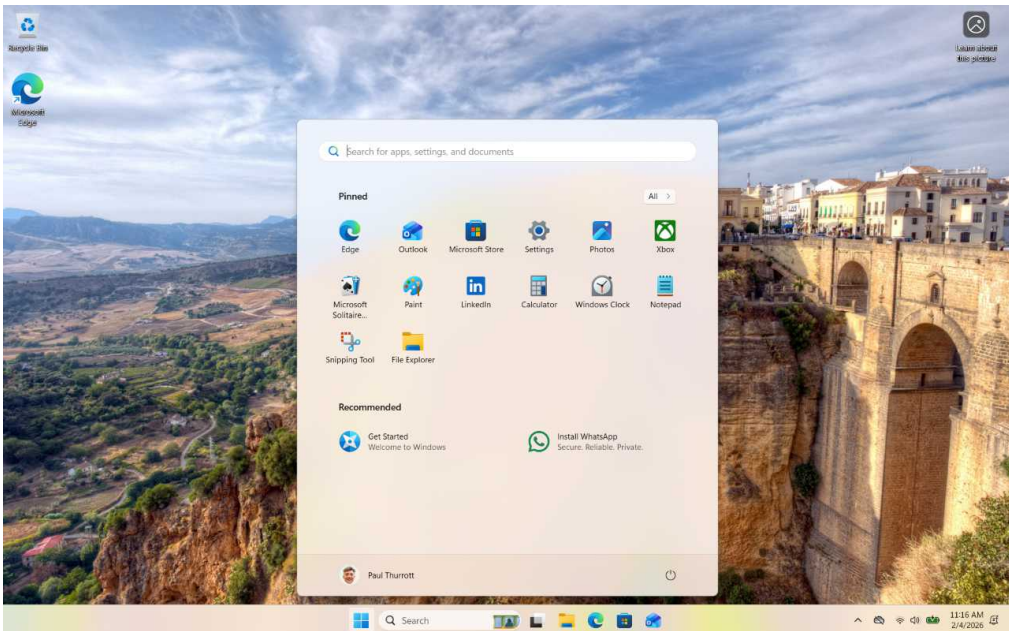
will promote one or both of these services via series of OOBE screens. Skip past them by clicking “Next” or similar as needed.

And with that, you arrive at the Windows 11 Desktop where you can begin the initial post-setup configuration.

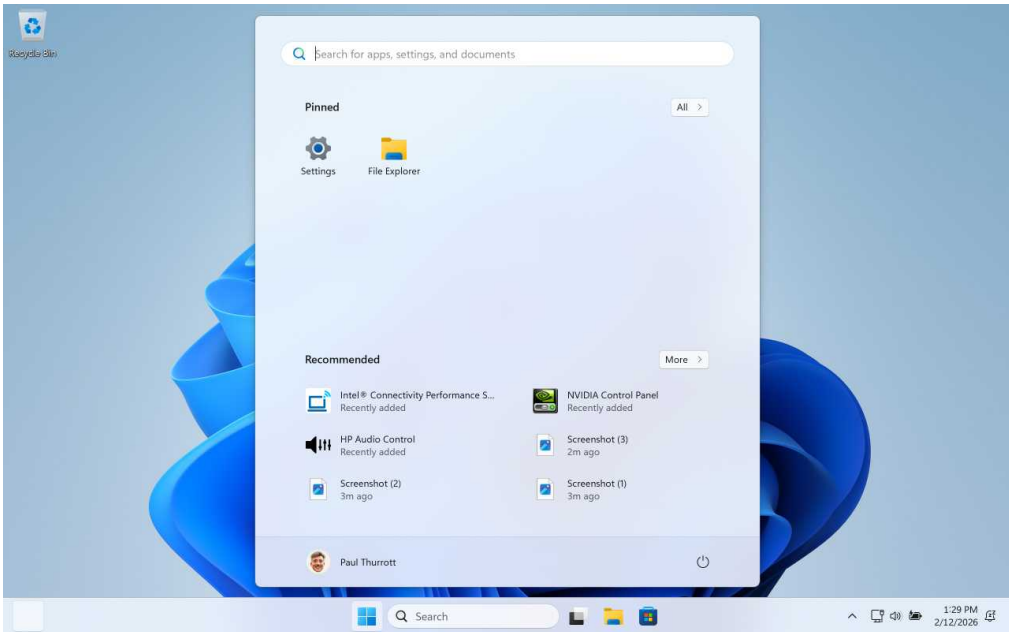
(#initial-config)

Perform initial Windows 11 configuration

What you see when you arrive at the Desktop will depend on how you set up Windows 11. If you used the stock Windows 11 image, you will see a pretty Desktop with a Windows Spotlight background and a Start menu full of apps.



If you used Tiny11 Builder, you will see a decidedly minimalist Desktop and Start menu, the latter of which contains very few app shortcut icons.

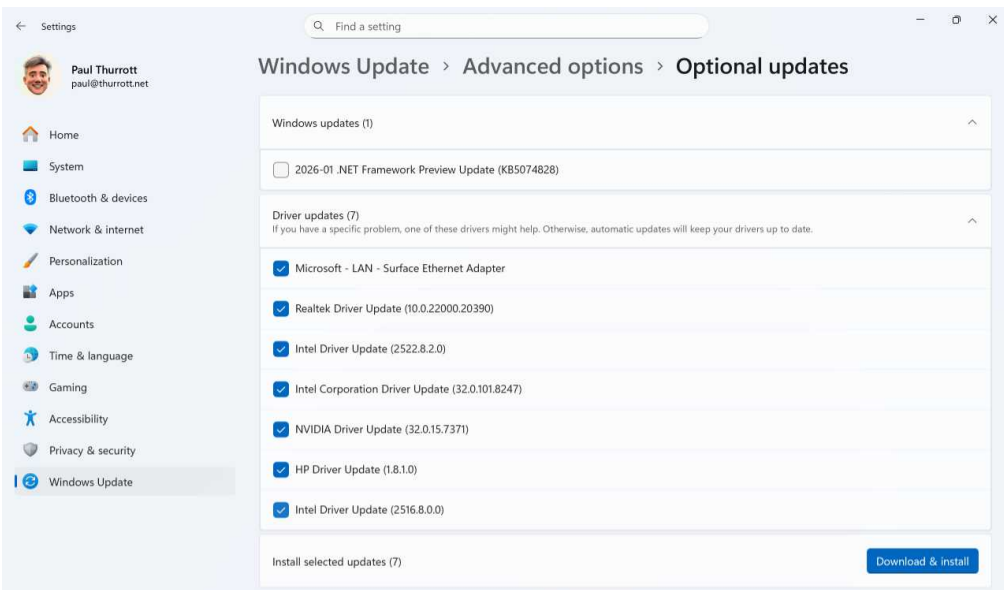


But it doesn't matter which way you went. Now is the time to perform some initial configuration tasks. I recommend doing the following, in this order if possible.

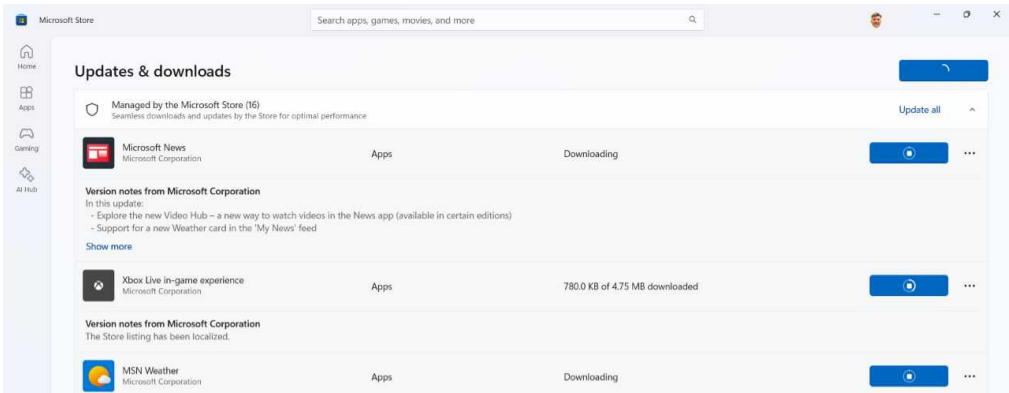
- **Optionally prevent OneDrive Folder Backup from auto-enabling.** If you did not use Tiny11 Builder and you do not want OneDrive to auto-enable Folder Backup, [follow the steps in the OneDrive chapter to prevent Folder Backup from being auto-enabled.](#)
- **Get Windows 11 up-to-date.** Open Settings, navigate to Windows Update, and check for updates. Install all available updates, rebooting as needed, and repeat this process until there are no more updates. This will take longer and involve far more updates if you performed a Tiny11 Builder-based clean install.



- **Install optional updates.** While the above is ongoing, navigate in the Settings app to Windows Update > Advanced options > Optional updates and install all available driver updates. Avoid the Preview Updates unless you want them as well.



- **Get the in-box apps up-to-date.** While the above is ongoing, open the Microsoft Store app, navigate to Downloads, and check for updates. Install all available app updates. And consider repeating this process after the PC has rebooted after installing Windows Updates: The Store often has pending updates that do not install immediately.

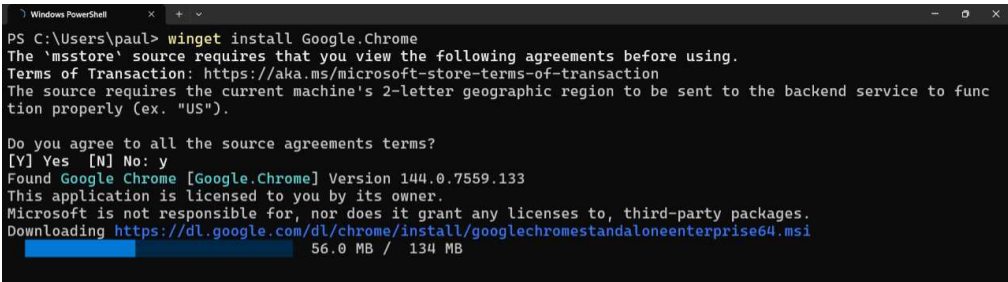


- **Optionally install a web browser and configure it as the default.** Unless you intend to use Microsoft Edge, you should install your favorite web browser. Follow [the instructions in the Microsoft Edge chapter](#) to configure it as the default web browser, prevent Microsoft Edge from running in the background, and prevent Windows 11 from ignoring your default web browser choice. If you used Tiny11 Builder to install Windows 11, you can install a web browser using the Windows Package Manager (winget) command line utility. Open a Terminal window and use a command line like the following examples or **winget search browser-name** to find your favorite browser.

```
winget install Google.Chrome
```

```
winget install Mozilla.Firefox
```

```
winget install Brave.Brave
```



```
Windows PowerShell
PS C:\Users\paul> winget install Google.Chrome
The 'msstore' source requires that you view the following agreements before using.
Terms of Transaction: https://aka.ms/microsoft-store-terms-of-transaction
The source requires the current machine's 2-letter geographic region to be sent to the backend service to function properly (ex. "US").

Do you agree to all the source agreements terms?
[Y] Yes [N] No: y
Found Google Chrome [Google.Chrome] Version 144.0.7559.133
This application is licensed to you by its owner.
Microsoft is not responsible for, nor does it grant any licenses to, third-party packages.
Downloading https://dl.google.com/dl/chrome/install/googlechromestandaloneenterprise64.msi
56.0 MB / 134 MB
```

- **Install the apps you use regularly.** Use your web browser, the Microsoft Store, and/or the Windows Package Manager (winget) to install the other apps you use regularly. If you used Tiny11 Builder to install Windows 11, you can also install any in-box Windows 11 apps that Tiny11 excluded using the Store app (or winget).
- **Ensure that Windows Security is properly configured.** If you click the “Show hidden icons” button (“^”) in the Taskbar’s system tray, you will see a blue Windows Security icon. In most cases, it will have a yellow “bang” overlay indicating that there is at least one recommended action to take. Click Windows Security to open the app and see the recommended action(s). Correct each, typically by clicking a “Turn on” or “Go to settings” button that, in the latter case, will require you to enable an option on a subpage in the app. Reboot if required.

➔ **Learn more:** You can learn more about Windows Security and how to properly secure Windows 11 in the [Make Windows 11 More Secure](#) chapter.

- **Optionally fix the issues with File Explorer.** Use [the instructions in the File Explorer chapter](#) to fix issues with this crucial app if you find the performance lackluster.
- **Further configure the system as needed.** From here, you can perform whatever configuration changes you normally make. Those who used Tiny11 Builder may want to pin key apps to the Start menu, for example. Those who did not will likewise want to [remove superfluous and crapware apps from the Start menu as described below](#).

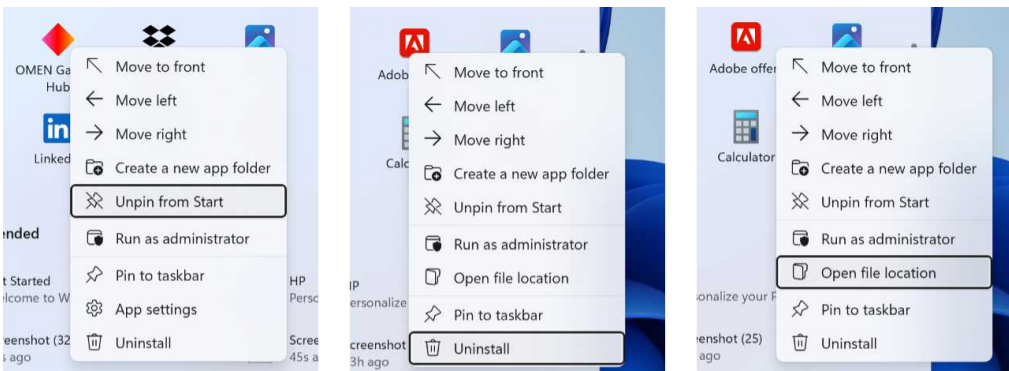
♥ Eliminate other Windows 11 Setup annoyances

Here are a few other issues you may encounter with a clean install of Windows 11.

The Start menu is full of superfluous and crapware apps

🚫 **The problem:** The Start menu is full of crapware and other superfluous apps from Microsoft, its partners, and/or the PC maker.

♥ **The solution:** Any of the pinned apps in the Start menu can be removed or uninstalled as needed. In most cases, all you have to do is right-click an offending app shortcut and choose “Uninstall” or “Unpin from Start” as needed. However, you may note that some of the shortcuts in Start can’t be removed using those methods. When that happens, right-click and choose “Open file location.” Then, you can delete the shortcut from a File Explorer window.



I signed in with a Microsoft account during the OOB, but I really want to use a local account.

🤡 **The enshittification:** Windows 11 Setup forces me to sign in with a Microsoft account or Microsoft work or school account, but I want to use a local account

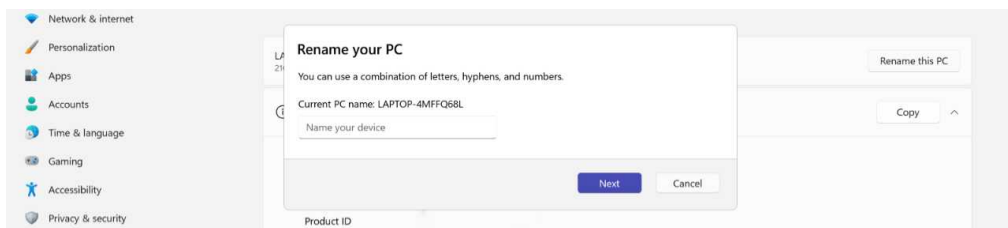
♥ **A workaround:** If you signed in with a Microsoft account, you can simply convert it to a local account after you’ve reached the Desktop. You can do

this with the Settings app by navigating to Accounts > Your info > Account settings.

I didn't name my PC during the OOBE, but I would like to now

🚫 **The problem:** You skipped by the “Name your device” screen during the Windows Setup OOBE.

💚 **The solution:** You can rename your PC at any time using the Setup app: Navigate to System > About and click the “Rename this PC” button. Note that you will need to reboot the PC.



I can't activate Windows 11 because I don't have a valid Windows 11 product key

🚫 **The problem:** I'm building a PC, but Windows 11 is too expensive.

💛 **A workaround:** You can [download a Windows 11 Insider Preview ISO from the Microsoft website](#) for free and install and use that without paying for it.

💚 **The solution:** You can legally buy Windows 11 Home and Windows 11 Pro product keys inexpensively online, often for as little as \$10, and then [download a Windows 11 ISO from the Microsoft website](#), also for free. Install Windows 11 using the ISO and then activate it using the product key you purchased. I've successfully used [Game Card Shop](#), [Productkeys.com](#), [Winandoffice.com](#), and other sites to find inexpensive Windows 11 product keys.

De-Enshittify an Existing Install of Windows 11

If you want to de-enshittify Windows 11 but find [starting over from scratch](#) to be daunting, then this chapter is for you. Here, you will learn how to thoroughly clean any existing Windows 11 installation, automatically removing bad behaviors like telemetry, preinstalled crapware, and even major enshittification vectors like Microsoft Edge and OneDrive, if desired.

As with [the clean install approach to de-enshittifying Windows 11](#), the tool you will use to achieve this is free. But unlike the Tiny11 Builder utility described in that chapter, the tool I document in this chapter, called [Win11Debloat](#), is flexible and granular, so you can eliminate the parts of Windows 11 that you despise while retaining those you value.

Tools that de-enshittify Windows predate the term enshittification by decades, and you may be familiar with some that sought to “clean” or “debloat” Windows over the years. These tools were often designed to strip Windows down so that it could run on lower-end or older PCs with less RAM and storage or allow more configuration options than Microsoft provided in the product itself. Today’s de-enshittification tools work similarly, but the emphasis has shifted to include removing behaviors that are objectively bad for users. Of course, these tools also let you clean and trim down the size of Windows 11 if that’s your goal.

As you might imagine, there are many options out there. But rather than offer a rundown of some of the better tools, I am instead focusing on a single tool because it meets all the de-enshittification needs one might have and it works very well.

De-Enshittify Windows 11 with Win11Debloat

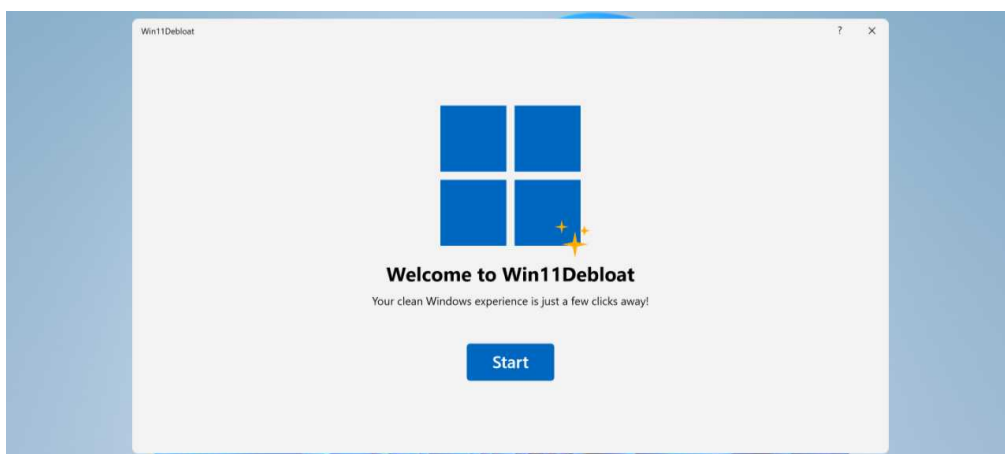
Like Tiny11 Builder, Win11Debloat is a PowerShell script that you can execute remotely from Windows 11. But once Win11Debloat runs, it uses a friendly

graphical interface by default, making it more approachable to mainstream users.

To get started, navigate to [the Win11Debloat page on GitHub](#) with your web browser and scroll down to the “Quick method” instructions under “Usage.” Per those instructions, open a Terminal window with administrator privileges and run the following script:

```
& ([scriptblock]::Create((irm "https://debloat.raphi.re/"))))
```

The script will download the app and, after a User Account Control (UAC) dialog, Win11Debloat appears.



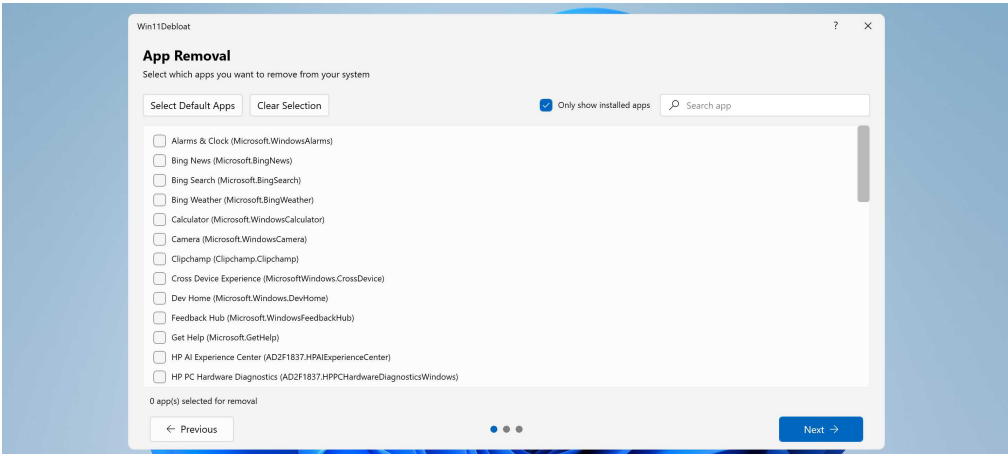
Win11Debloat is deceptively simple, consisting of just three main screens. But there are many dozens of options across those screens, and it’s important to pay attention and choose wisely. From a high-level perspective, Win11Debloat helps you to:

- Uninstall apps, including apps like Microsoft Edge that are normally impossible to uninstall
- Configure many individual Windows 11 features, including some, like forced telemetry, that are normally impossible to disable
- Determine if the changes are made to the current user only or all users on the PC

OK, let’s get started. Literally: Click “Start.”

App Removal

In this first step, you determine which apps to uninstall. It's not clear why this view doesn't show you only those apps that *are* installed, so change “Only show installed apps” to “On” before proceeding.



With two possible exceptions—Microsoft Edge, especially, and OneDrive—none of the apps that Microsoft bundles in Windows 11 are truly enshittified. But you will find crapware and superfluous apps from both Microsoft and your PC maker. And it's worth at least examining this list to see whether there are apps you wish to uninstall, all in a single pass.

⚠ Warning: Do **NOT** remove the Microsoft Store app even if you think you will never use it. This is the only app that cannot be reinstalled easily if removed, and it's used to keep in-box (and Store) apps up-to-date.

I recommend considering uninstalling the following unless you're sure you need them or will use them in some way.

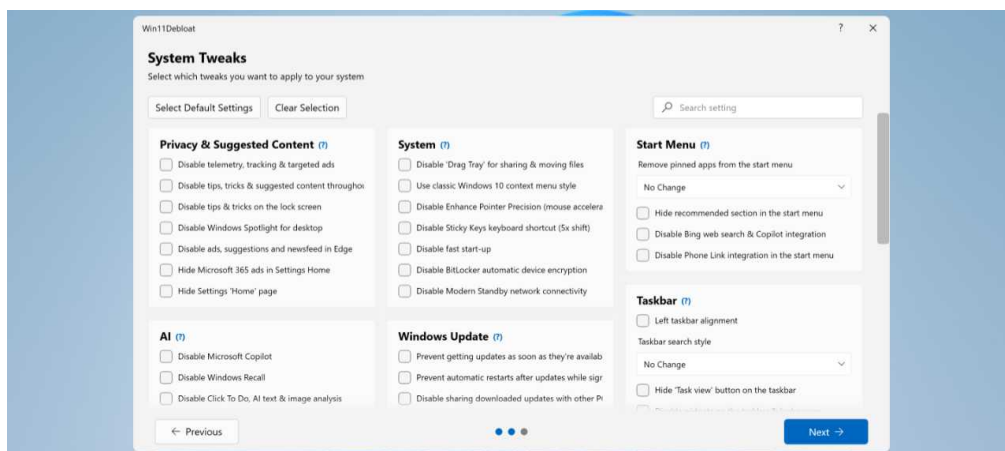
- **Enshittified apps and other potential problems.** These include Microsoft Edge, OneDrive, Office Hub (which is really Microsoft 365 Copilot), and Widgets Experience.

- **Superfluous, low quality in-box apps.** Bing News, Bing Search, Dev Home, Microsoft Journal, Power Automate, Solitaire Collection, and Whiteboard are among these choices.
- **Some apps from your PC maker.** If you see McAfee in there, any PC maker AI chatbot app, or other nonsense, they deserve to be removed.

When you're ready to move on, click "Next."

System Tweaks

Given the sheer volume of choices here, it's likely that you will have to spend a lot of time considering these options. But if you all you care about is enshittification, then that winnows down the list nicely.



To remove the objectively enshittified behaviors in Windows 11, configure each of the following options:

In Privacy & Suggested Content:

- Disable telemetry, tracking & targeted ads
- Disable tips, tricks & suggested content throughout Windows
- Disable tips & tricks on the lock screen
- Disable ads, suggestions and newsfeed in Edge
- Hide Microsoft 365 ads in Settings Home

In AI:

- Disable Microsoft Copilot
- Disable AI features in Microsoft Edge

In Windows Update:

- Prevent automatic restarts after updates while signed in
- Disable sharing downloaded updates with other PCs

In Start menu:

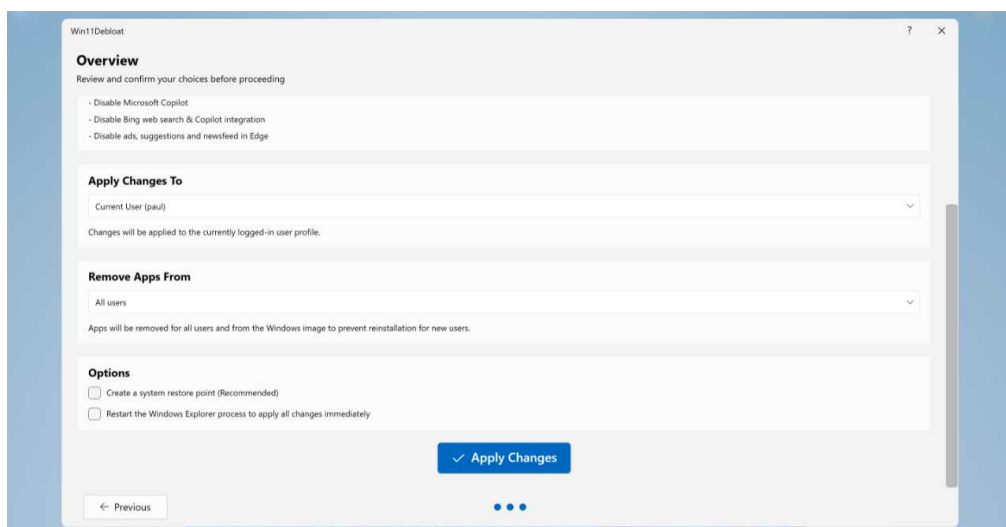
- Disable Bing web search & Copilot integration

And that's it, at least for the enshittification. But if you see other behaviors you don't like in there, disable them as well before moving on.

When you're ready, click "Next."

Overview

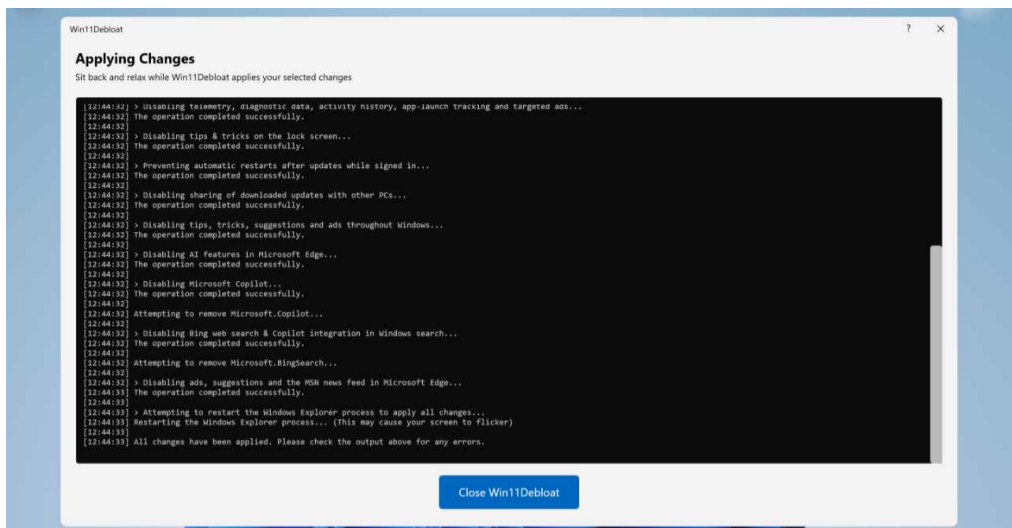
The Overview screen lets you review the choices you made, but it also provides four very important options.



They are:

- **Apply changes to.** By default, the “system tweak” changes you are making will apply to the current user only, but you can optionally have them apply to all users configured on the PC.
- **Remove apps from.** By default, the apps you are removing will apply to all users configured on the PC. But you can optionally have them removed only for the current user.
- **Create a system restore point.** You definitely want to create a restore point: If something goes wrong, you can restore from that restore point and go back to your previous configuration.
- **Restart Windows Explorer.** If you’re making any changes to File Explorer, you should check this option so that those changes will occur immediately.

Click “Apply Changes.” Win11Debloat will now do its thing, and you can see that occur in a command line as it does so. Eventually, you will be told that “all changes have been applied” and advised to scan through the command line output to see whether there were any issues.



♥ Use Win11Debloat effectively

Before moving on, here are some additional points about this process.

Update apps *before* using Win11Debloat

➖ **The problem:** The Microsoft Store just reinstalled an app I removed with Win11Debloat.

♥ **The solution:** This may seem illogical, but if you want to run Win11Debloat after performing a clean install or reset of Windows 11, you should use the Microsoft Store to update all the in-box apps first. Otherwise, you may find that the Store app silently reinstalls some of the apps you removed when it finally gets around to updating. So get everything up-to-date first, and then remove the apps you don't want using Win11Debloat.

Win11Debloat doesn't "see" all the apps I want to remove

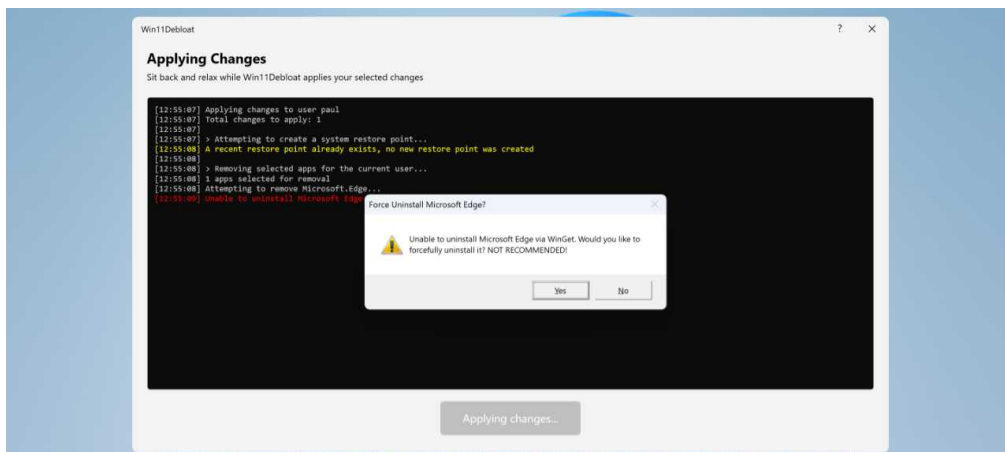
➖ **The problem:** After using Win11Debloat, you may notice that there are still crapware and superfluous apps in the Start menu.

♥ **The solution:** Win11Debloat is terrific, but it will sometimes miss the occasional app. If this happens, just uninstall the app normally from Start by right-clicking it and choosing "Uninstall."

Microsoft Edge doesn't want to be removed

➖ **The problem:** Microsoft Edge is a bit trickier to uninstall than other apps and requires an additional step.

♥ **The solution:** Perhaps because of its deep integrations with Windows 11, Microsoft Edge removal fails on the first pass and then Win11Debloat prompts to you "forcefully uninstall it." This process is "NOT RECOMMENDED," the app adds, but I disagree: This removal method has always worked properly in my experience. And besides, you made a restore point, right?



→ **Learn more:** If you *do* remove Microsoft Edge, you will need to download another web browser, configure it as the default web browser in Windows 11, and use a free third-party utility to force Windows 11 to *always* use this browser. This is all explained in the [De-Enshittify Microsoft Edge](#) chapter.

Some apps require Microsoft Edge

➖ **The problem:** I used Win11Debloater to remove Microsoft Edge and I later saw that it had somehow reinstalled itself.

♥ **The solution:** Some of the in-box apps in Windows 11 and third party apps are web apps that require the Microsoft Edge runtime. For this reason, you may inadvertently reinstall Microsoft Edge if you later install an app from the Microsoft Store or elsewhere. If this happens, try installing [the Microsoft Edge WebView2 runtime](#) and then use Win11Debloater to remove the Microsoft Edge app again.

The changes that Win11Debloater makes are all reversible

➖ **The problem:** I made a mistake and want to revert a change that was made with Win11Debloater.

♥ **The solution:** As the developer of Win11Debloat explains, all the changes this app makes to Windows 11 can be easily reversed. Likewise, almost all the apps you remove with Win11Debloat can be reinstalled through the Microsoft Store or by using the Windows Package Manager (winget). The only major exception is the Microsoft Store app itself. Again, do not uninstall Store.

i More info: You can learn how to revert any of the changes you made with Win11Debloat on the app's website.

Take your time with Win11Debloat

➖ **The problem:** There are so many options in Win11Debloat that I'm not sure where to start.

♥ **The solution:** You don't have to make all your configuration and app removal changes at the same time. Go slow, make a few changes to see how Win11Debloat works and gain some confidence in the process. You can simply re-run Win11Debloat again and again as needed.

What about the future?

➖ **The problem:** I'm worried that Windows 11 will simply overturn a change that I made with Win11Debloat.

♥ **The solution:** One of the (many) concerns with Windows 11 is that Microsoft may in the future install an annual feature update or a monthly "security" update that alters your configuration and reverts features to the default configuration, ignoring the changes you made manually or with a tool like Win11Default. I am actively seeking a tool that will monitor for these types of changes, but for now, you can always re-run Win11Debloat if you notice any unwanted changes.

Make Windows 11 Respect Your Privacy

Thanks to its forced telemetry and in-box tracking and advertising, Windows 11 is anything but private. Microsoft does provide you with some surface-level control over Windows 11 privacy settings, but you need to do a lot of spelunking in the Settings app to find options that are purposefully scattered throughout. And you can't completely rein in the bad behaviors without digging even deeper and using a third-party app to fully disable the terribleness.

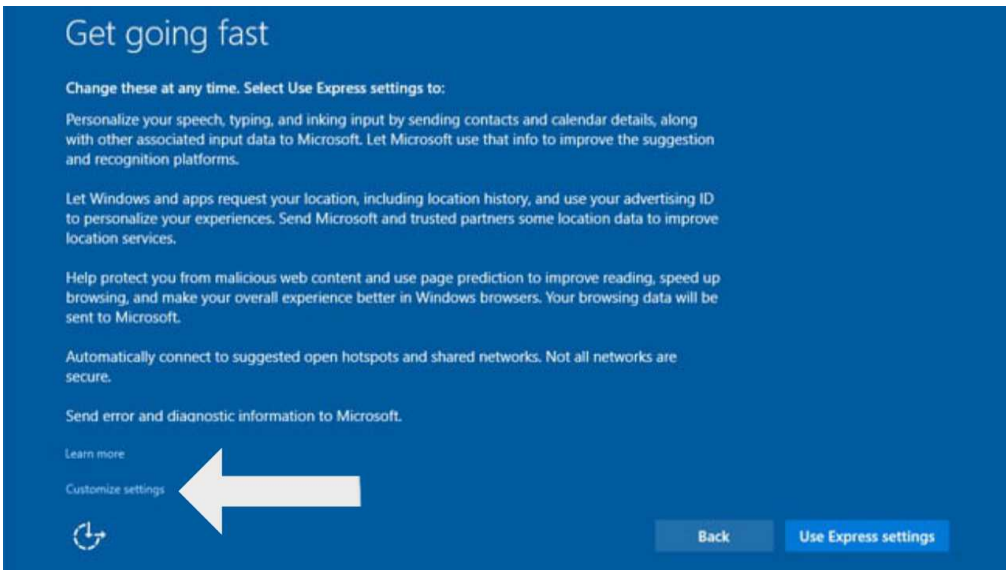
The problem with privacy in Windows 11

The problem with privacy in Windows 11 is easily stated: There isn't any. Microsoft violates your privacy by default and does everything it can, from using dark patterns to outright harassment, to convince you to lower your defenses and allow it to gain more access to your personal information. It does this so that it can track you online, build a profile, sell that information to advertisers, and use it against you in advertisements of its own.

This behavior didn't happen suddenly. It started subtly, as is so often the case when one of the world's biggest companies decides it's going to start violating the privacy of its own customers: Beginning with Windows 8 in 2012, Microsoft began assigning a unique *advertising ID* to each PC, just as it does with its Bing search engine, so that it can collect usage data and sell it to third-party advertisers so they could provide users with more personalized search results. This advertising ID was anonymous and still is, and it can still be disabled today, though you have to know it's happening and where to look.

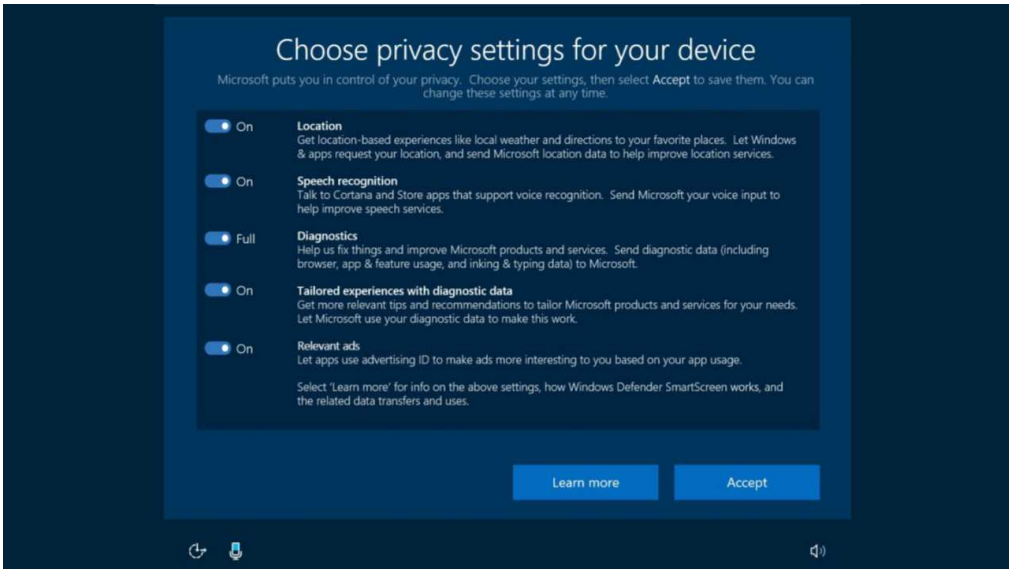
Microsoft's privacy violations escalated dramatically with Windows 10 in 2015. Microsoft made data collection mandatory in this release, in part to help with product quality: The idea was that Microsoft could keep Windows "secure, up-to-date, and running properly" because it was collecting all this data. But there were three levels of data collection—Full, Enhanced, and Basic—and even Basic was an overreach.

Perhaps sensing the obvious backlash, Microsoft used dark patterns to obfuscate its activities. During Windows Setup, for example, there was a “Get going fast” screen that described some of the data that Windows 10 would collect if you just agreed to let it do so. And while there was a prominent and pre-select “Use Express Settings” button, the opt-out choice, a “Customize settings” text link, was both tiny and difficult to read.



Because of this, antitrust regulators began asking questions. And so Microsoft in early 2017 [revealed](#) that it would proactively make three major changes to its data collecting behaviors.

- It would switch from three levels of data collection to two and reduce the amount of data collected when the user chose the Basic data collection level.
- It agreed to change Windows Setup and replace the “Get going fast” screen and its Express Settings option with a new privacy settings screen that would “clearly show you simple but important settings” and require you to “choose your settings before you can move forward with setup.”



- It would launch a web-based [privacy dashboard](#) so so you could “see and control your activity data from Microsoft including location, search, browsing”, and more.

When Microsoft implemented these changes, [it fooled some regulators](#) but [not others](#). I described them as “superficial tomfoolery” and “privacy theater” because Microsoft had simply replaced unclear choices with new but still unclear choices, none of which solved the underlying problem: You can flip switches all you want, but today Microsoft still tracks your activities online with Windows 11.

You may want to prevent that and other privacy-invasive behaviors in Windows 11. In this chapter, you will learn what’s possible using the tools built into the product itself. And how you can completely prevent Windows 11 from tracking you online using a free utility.

♥ Try to protect your privacy using the tools that Windows 11 provides

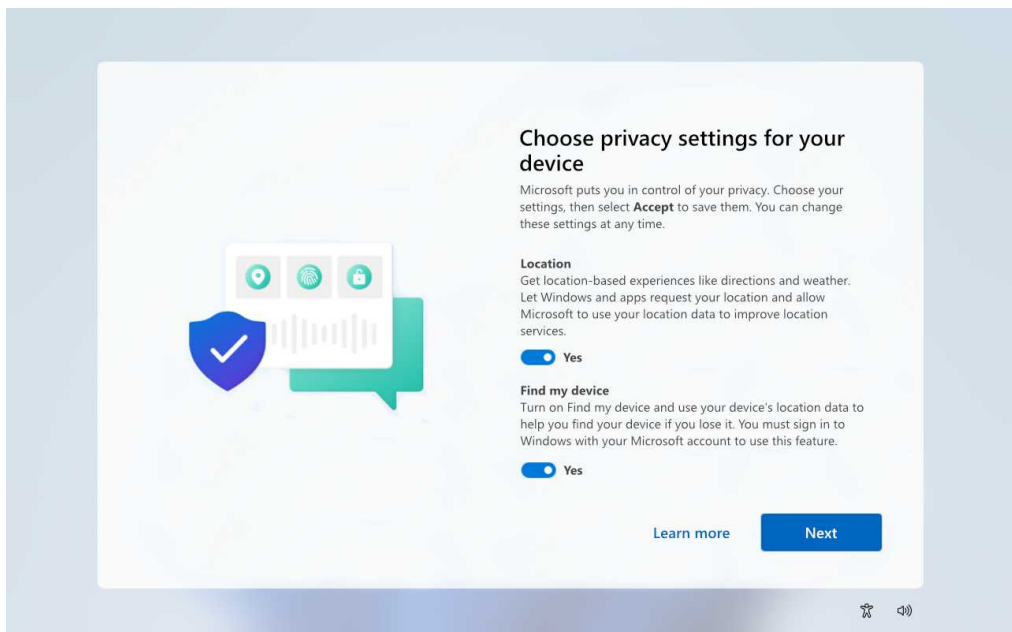
With Windows 11, Windows Setup displays an updated version of the privacy settings screen that debuted in Windows 10 in 2017. But now as then, you

can also more fully configure privacy settings at any time in the Windows 11 Settings app.

Configure Windows 11 privacy settings during Windows Setup

As noted in [Start Fresh with a New Install of Windows 11](#), the Windows Setup Out of Box Experience (OOBE) displays a screen, like the one in Windows 10 Setup but updated, in which you can configure several high-level privacy options. It's worth configuring each of these correctly when you set up a computer, but that's not enough. You should also review your privacy configurations later in the Settings app and take other steps to fully protect your privacy from Windows 11 and Microsoft.

➔ **Learn more:** These topics are both described later in this chapter, in [Properly configure Windows 11 privacy settings at any time](#) and [Take control of your privacy with Win11Debloat](#), respectively.



All the options you see here are enabled by default.

♥ Location

When left enabled, Windows 11 will permit Widgets, the Weather app, and other built-in experiences to access your location data, other apps can request access, and Microsoft will use your data to improve its location services. For most, this is a fair trade-off, even though location data is a key contributor to *fingerprinting*, by which online trackers can build a profile of you even when you take steps to protect your privacy: Many enjoy seeing the local weather display on the Widgets icon on the Taskbar, for example.

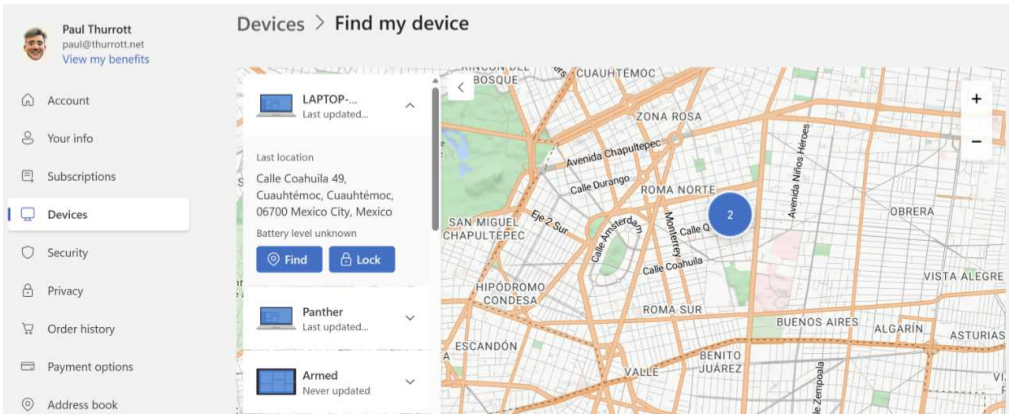
My advice: Leave this enabled.

➔ **Learn more:** Even if you decide you wish to enable Location, take the time to [review Location privacy settings as described later in this chapter](#). Location services isn't a simple on/off switch, and there are numerous related options to consider.

♥ Find my device

Tied to Location, Find my device remembers the most recent location of the PC you are using and associates it with your Microsoft account. This is incredibly useful as Find my device is used to help you recover a lost or stolen computer. You can see the PCs associated with your account when you sign in to [the Microsoft account website](#) and navigate to [Devices](#). Each PC you see here displays that location, if available, and provides a “Find my device” link so you can view it on a map.

My advice: Leave this enabled.



✔ **Tip:** Find my device is a basic On/Off switch in Settings, unlike Location.

❌ Diagnostic data

By default, Windows 11 sends *diagnostic data*, a euphemism for telemetry, which is data used for both good and bad. Basic telemetry can help detect, diagnose, and fix problems with Windows, which is fine. But Microsoft *really* wants you to grant it expanded access to your telemetry data, which includes your web browsing history, connectivity and configuration data, inking and speech data, typing data, and more. And that's a mix of good and bad, as some of that data will be used by Microsoft and its advertising partners to track your activities online and target you with advertising.

You can't turn off telemetry data entirely here. But you *can* toggle this option to "Off" to change the configuration from "Send optional data" to "Required only." And I strongly urge you to do so.

My advice: Disable this option (changing it to "Off," or "Required only").

➔ **Learn more:** Like Find my device, Diagnostic data is a simple On/Off switch in Settings, where "On" equates to "Send required *and* optional

data” and “Off” is “Send required data only.” That said, [there are additional related options in the Settings app](#) you should consider, as described later. And while you can’t disable diagnostic data (telemetry) entirely in the Settings app, I discuss how you can use a free utility to do so in the [Take control of your privacy with Win11Debloat](#) section later in this chapter as well.

♥ Inking & typing

This setting is one of the more innocuous choices from a privacy perspective: If left enabled, Windows 11 will send additional and optional data associated with inking and typing to Microsoft so that it can improve its language recognition and suggestion capabilities. That said, it’s still optional and feels unnecessary.

My advice: Disable this option.

➔ **Learn more:** Inking & typing is also a simple On/Off switch in Settings, though there is a related option to consider in Settings, as described later in the chapter.

🚫 Tailored experiences

This is another example of overreach by Microsoft: When Tailored experiences is left enabled, Windows 11 will send Microsoft diagnostic data, including optional diagnostic data (aside from web browsing history), so that it can offer you customized “tips, ads, and recommendations.” To be clear, this is only about Microsoft optimizing the advertising it delivers to you through Windows 11, and our goal here is to minimize if not eliminate that advertising in the first place.

My advice: Disable this option.

♥ Presence sensing

You will only see this option if your PC supports Windows 11-compatible *presence sensing* capabilities, which use your webcam and other sensors to detect when you or others approach or leave the PC. This allows the PC to automatically wake up so that you can authenticate more quickly via Windows Hello facial recognition when you approach and then go to sleep and sign you out when you leave. That's obviously useful, but in my experience, it's also incredibly annoying, and after spending many months trying to configure it properly and use it day-to-day, I decided to disable presence sensing and never look back. But that's subjective: You may find value in this feature and want to leave it enabled.

My advice: Disable this option.

➔ **Learn more:** If you are going to use presence sensing, at least spend the time to configure it correctly for your needs and wants. [You do so in the Settings app as described later in this chapter.](#)

To be clear, when I configure PCs for my own use, which I do dozens of times every year, I leave Location and Find my device enabled but I disable all the other options.

Properly configure Windows 11 privacy settings at any time

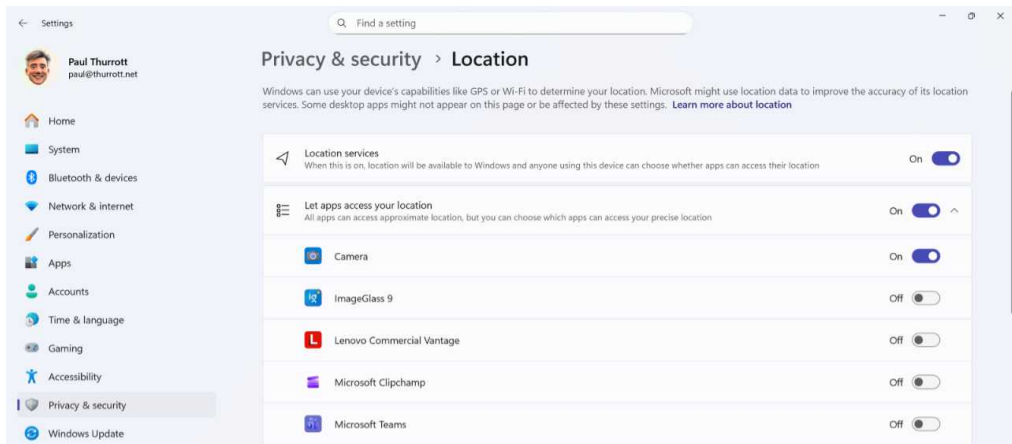
The privacy settings screen in Windows Setup is just “privacy theater” in that it's designed to give you some confidence that you are, in Microsoft's words, “in control of your privacy.” But if that's all you configure, you're missing out on some of the more egregious privacy violations in Windows 11, which is the point. And though Setup notes that “you can change these settings at any time,” it doesn't explain how or where you do so. Microsoft doesn't want you to make any changes, nor does it want you to ever think about this again.

But you're smarter than that. Here's a rundown of the privacy options you can and should configure in Windows 11 that actually make a difference. All these options are found in the Settings app, though they are scattered throughout by design.

Location services

As noted above, Microsoft uses location services so that Windows, in-box apps, and third-party apps can use that data and so that Microsoft can improve the service. Generally speaking, this is acceptable—you want a weather app to know your location for obvious reasons—but Location privacy and security settings in the Settings app provides more granular control over this capability so that you can determine exactly which apps can access your location. There are also several other related options options to consider.

You can find this interface in the Settings app by navigating to Privacy & security > Location.



Here, you will see the following options:

Location services. This is the master toggle switch for location services, and it's tied to the Location option you saw in the Windows Setup privacy page. If you configure this to “Off,” location services is disabled globally, but the Find my device functionality is also disabled and the “Let apps access your location” section, below, is grayed out and unavailable.

Let apps access your location. This misnamed option is really about *precise* location. When Location services, above, is enabled, Windows and all apps can access your approximate location. When this option is enabled, you can specify which apps can access your precise location, including, interestingly, some classic desktop apps, none of which can be configured individually. My advice is to disable precise location for almost any app you see in this list.

Default location. This option lets you use a map to configure a default location that's used when Windows can't determine your approximate or precise location. This is generally useful, but it is perhaps most useful for those who wish to leave location services disabled but still want some basic weather or news data from Widgets or whatever apps.

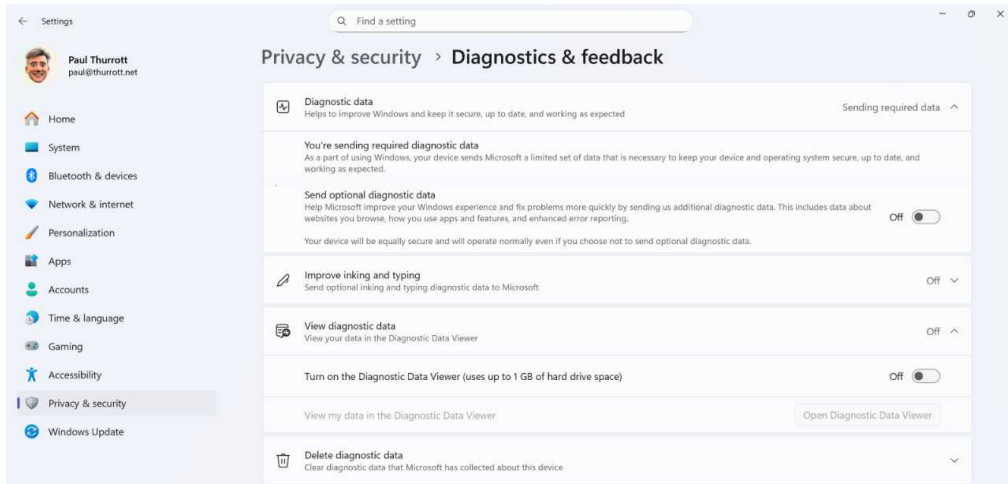
Allow location override. This setting does not impact most users and can be safely ignored. It's designed to let a cloud-hosted or remote PC that you connect to from Windows 11 on your PC use *their* location instead of your PC's location. If that doesn't sound like something you'll ever do, then you're normal and can move on.

Recent activity. If you're curious about which apps are accessing your location information, you can expand this option and find out. Well, sort of. Some of the apps you will see here, like Microsoft Edge, are expected. Some are just curious, like Windows (File) Explorer. And some are inscrutable, like "COM Surrogate." It may be worth stepping through the list to see whether there's anything suspicious, but I can't say I've seen anything unusual beyond how often Zoom Meetings accesses my location information: It appears to do so every few seconds during online meetings.

Diagnostics & feedback (telemetry)

Telemetry—or what Microsoft calls “Diagnostic data” or “Diagnostics & feedback”—is one of the more controversial aspects of Windows 11. As noted previously, Microsoft doesn't allow you to fully disable telemetry in Windows 11. But it does let you provide just basic telemetry (“required data”) and enhanced telemetry (“optional data”) and access a few other related options in the Settings app. You should review these options.

You can find this interface in the Settings app by navigating to Privacy & security > Diagnostics & feedback.



Options to examine here include:

Diagnostic data. Microsoft offers two levels of forced telemetry: You can send only the required data, which the company claims is only used to “improve Windows and keep it secure, up to date, and working as expected,” or you can send optional diagnostic to “help Microsoft improve your Windows experience and fix problems more quickly by sending additional diagnostic.” That additional data includes “data about websites you browse, how you use apps and features, and enhanced error reporting,” and there is absolutely no reason to agree to that.

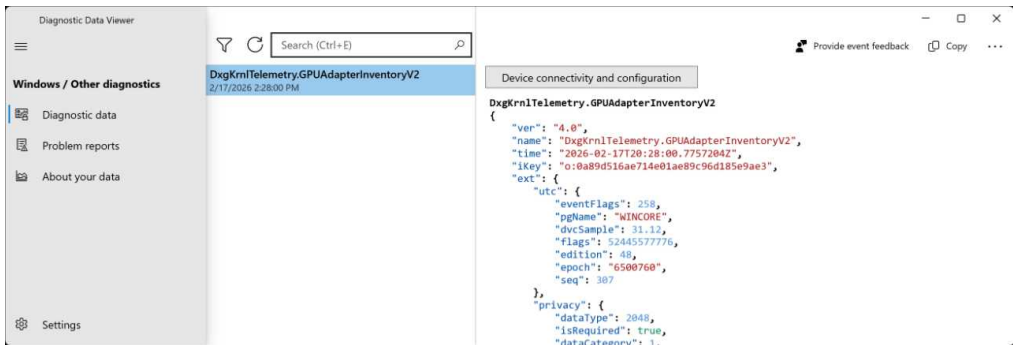
➔ **Learn more:** Notably absent here is the choice, “Never send Microsoft any= telemetry data.” But you can find out how to do just that in the [Take control of your privacy with Win11Debloat](#) section later in this chapter.

Improve inking and typing. Microsoft would like you to send optional inking and typing diagnostic data to. Don’t.

Tailored experiences. As discussed previously, this will “let Microsoft use your diagnostic data for personalized tips, ads, and recommendations,” or what one would succinctly call targeted advertising. Just say no.

View diagnostic data. This one would be interesting if it were useful, but it’s not. You can optionally enable a Diagnostic Data Viewer to see the data

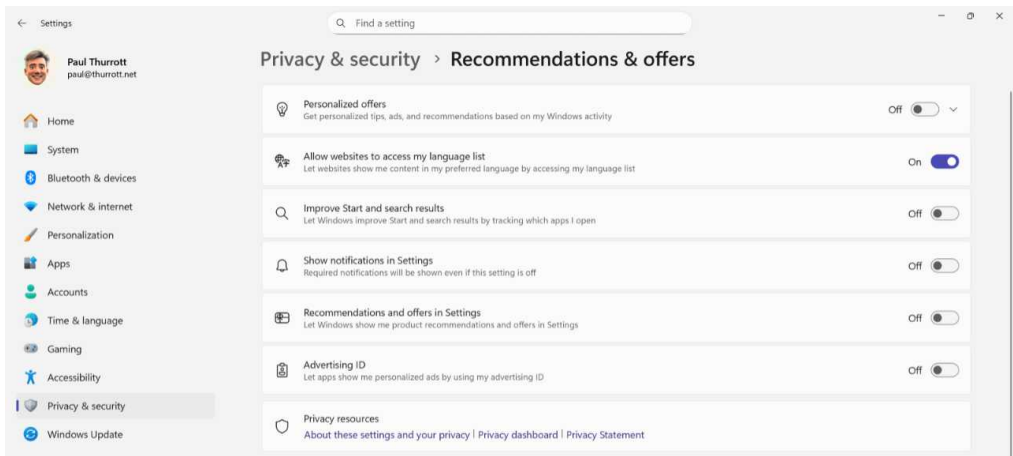
that Windows 11 sends to Microsoft. Unfortunately, you have to install the app, it takes up 1 GB of disk space, and the output is in an XML format that, while technically “human readable,” is literally indiscernible in practice. Well, except for one thing: If you leave it running, you will see that Windows 11 sends a metric ton of data to Microsoft all day, every day. Don't bother.



Delete diagnostic data. This option lets you delete all the diagnostic data that Microsoft collected from this PC and now stores in the cloud. Do so.

Recommendations and offers

Windows 11 is awash in subtle and overt advertisements that masquerade as “personalized offers,” “recommendations,” and other nonsense. But you can go a long way towards eliminating all that in the Settings app by navigating to Privacy & security > Recommendations & offers.



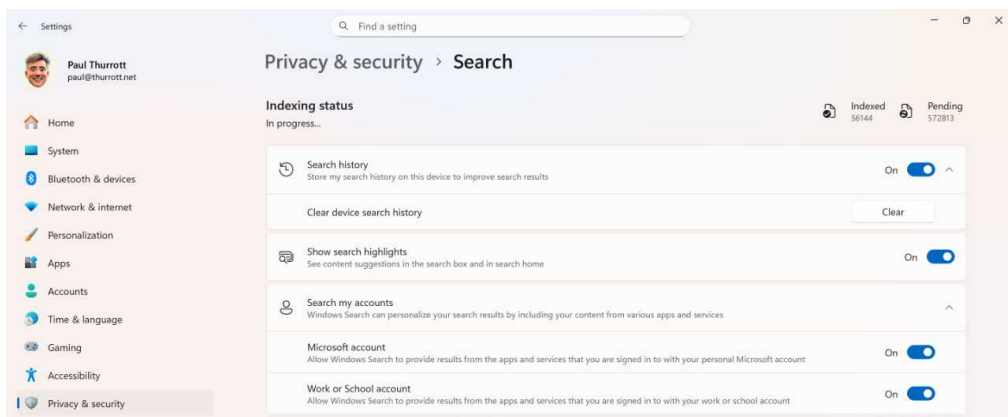
This is mostly obvious, so I will cut to the chase: Set the following options to “Off”:

- Personalized offers
- Improve Start and search results
- Recommendations and offers in Settings
- Advertising ID

Search

By default, Windows Search integrates with your Microsoft account (and/or your Microsoft Work or School account) so that it can return results using content in your OneDrive cloud storage even when that content is not synced locally to your PC. That may be useful to you, but Windows Search also displays a Search highlights experience by default that’s designed solely to put you in front of Microsoft advertising displayed on Microsoft online services like MSN and Bing.

You can configure these and a few other related Windows Search features in the Settings app by navigating to Privacy & search > Security.



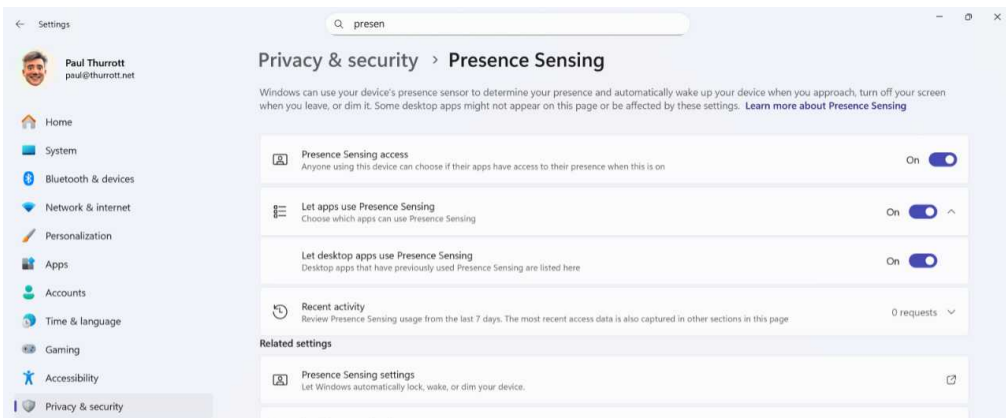
My recommendation is to configure “Show search highlights” to “Off.” And if you don’t want Windows Search to access your OneDrive-based files for whatever reason—I personally find that useful—configure the options under “Search my accounts” and “Search the contents of online files” to “Off.”

Presence sensing

Presence sensing isn't available on all PCs, and it's possible or even likely that you may find it useful. As noted above, I find it irritating, and so I disable it fully when available.

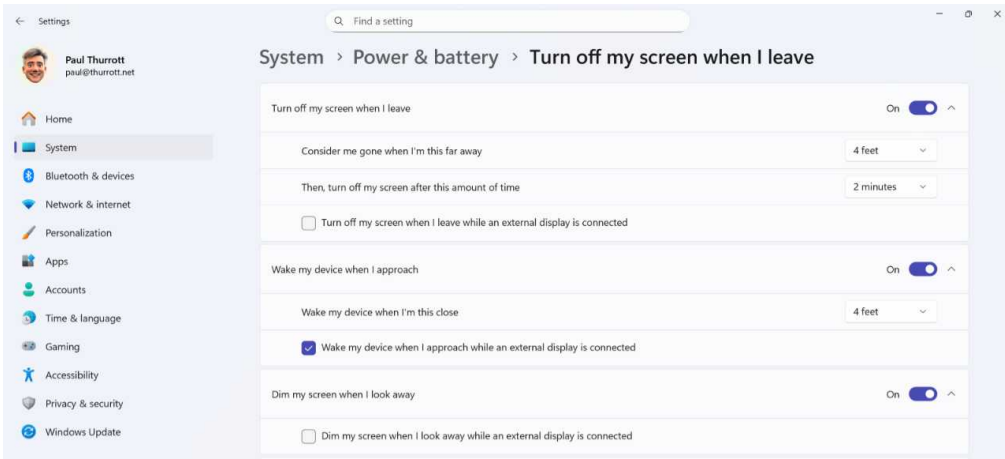
There are two sets of presence sensing options in the Settings app in Windows 11, one tied to privacy and one to the functionality itself.

To configure whether presence sensing is available to apps, open Settings and navigate to **Privacy & security > Presence Sensing**.



Here, just configure “Presence Sensing access” to “Off” if you don't intend to use this feature at all.

Then, click the “Presence Settings settings” link. The Settings page you navigate to lets you configure individual presence sensing features.



Here, you can enable or disable the following features and configure them to some degree:

- Turn off my screen when I leave
- Wake my device when I approach
- Dim my screen when I look away

➔ **Learn more:** What about AI and privacy? This is such a big topic that I have an entire chapter, [De-Enshittify Copilot and AI](#), that you can reference.

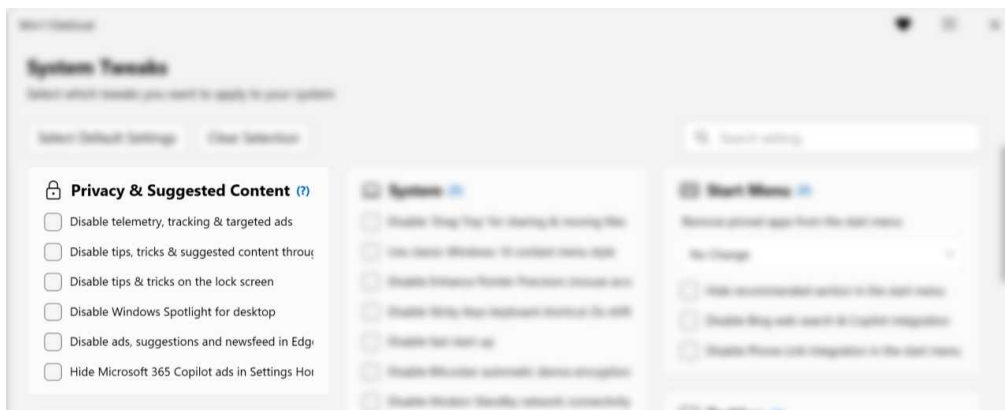
♥ Take control of your privacy with Win11Debloat

In [De-Enshittify an Existing Install of Windows 11](#), you can learn how to use the free utility [Win11Debloat](#) to de-enshittify an existing Windows 11 installation. Among the changes I recommend making with this app is something you cannot accomplish in Windows 11 directly: You can completely disable all its telemetry and tracking. So let's take a look at that in more detail.

As per that chapter, you access Win11Debloat by opening a Terminal window with administrator privileges and running the following script:

& ([scriptblock]::Create((irm "https://debloat.raphi.re/"))))

The script will download the app and, after a User Account Control (UAC) dialog, Win11Debloat appears. Click “Start” and “Next” to arrive at the System Tweaks screen. Here, you will focus only on the first section, “Privacy & Suggested Content.”



This section in Win11Debloat offers the following several options.

Disable telemetry, tracking, and targeted ads. Check this box to disable telemetry and tracking entirely. This is the magic option because it prevents your PC from sending any telemetry data to Microsoft.

Disable tips, tricks, suggestions, and ads throughout Windows. Check this box to disable these advertisements.

Disable tips and tricks on the lock screen. Check this box to disable the advertisements that Microsoft puts on the lock screen.

Disable Windows Spotlight on the desktop. This one is subjective, as you may enjoy the high-quality wallpapers provided by Windows Spotlight. But if you would like similar functionality without the superfluous Desktop icon, you could try an alternative wallpaper app like [Bing Wallpaper](#). Though if you do choose that, be sure to uncheck the option it presents to make Bing your default search engine and disable all its widgets so there is nothing superfluous on-screen.

Disable ads, suggestions, and newsfeed in Edge. This is a no-brainer: Check this box to disable all the distractions in Microsoft Edge.

Hide Microsoft 365 Copilot ads in the Settings Home page. This likely won't impact you unless you sign in to Windows with a Microsoft Work or School account, but it won't hurt you to check this box to disable ads in the Settings home page.

➔ **Learn more:** There are many more useful options to configure in Win11Debloat. Check out [De-Enshittify an Existing Install of Windows 11](#) for a more complete rundown.

Make Windows 11 More Secure

In sharp contrast with [its approach to privacy](#), Windows 11 security is in a good place, with no major enshittification issues. However, security is too big an issue to ignore, and Windows 11 ironically doesn't always provide the most secure possible default configuration in the name of—wait for it—privacy. And so it's important to make sure that Windows 11 is as secure as possible.

✔ **Tip:** If you are buying a new PC, the most secure and reliable option is a Copilot+ PC using a Qualcomm Snapdragon X-series processor that runs Windows 11 on Arm. All Copilot+ PCs, including the less reliable x64 models with Intel- or AMD-based processors, offer dramatic security improvements over normal Windows 11 PCs. But Windows 11 on ARM with Snapdragon X is the best choice overall.

Fortunately, most people reading this will sign into Windows 11 using a Microsoft account. Doing so will configure your PC in a reasonably secure manner, though there are additional steps to consider. But some power users may prefer to sign in using a *local account* that is specific to that PC and is too easy to configure in a non-secure manner. So let's look at account security first.

🚫 The problems with not using a Microsoft account

When you first set up Windows 11 on a new or recently reset PC, you complete [the Windows Setup Out of Box Experience \(OOBE\)](#), during which you typically sign in with a Microsoft account. Doing so is nearly mandatory, but it comes with some pros and cons, the latter of which are tied to enshittification via online tracking, targeted advertising, upsells, and more. Those behaviors can be overcome, at least, and signing in with a Microsoft account comes with important security advantages that I feel outweigh the problems.

These advantages include:

- Your Microsoft account can (and should) be secured with two-factor authentication (2FA), a form of passwordless authentication that is more secure than using just a password.
- Windows 11 creates a device-bound passkey for your Microsoft account when you sign in that way, and this is used for passthrough authentication to in-box apps and experiences like OneDrive, the Microsoft Store, Microsoft Edge, and more.
- Your Microsoft account can be recovered if it is compromised.
- Your Microsoft account automatically backs up some Windows 11 configurations to the cloud so that they can be recovered and automatically reused when you sign into a different PC or reset this PC.
- The disk on which Windows 11 is installed is automatically encrypted when you sign in with a Microsoft account, protecting your private data and other contents if the PC is ever lost or stolen. The recovery key for that encrypted disk is automatically stored in the OneDrive cloud storage associated with your Microsoft account.
- Windows 11 will automatically configure OneDrive Folder Backup when you sign in with a Microsoft account to ensure that any documents or other files you save to the Desktop, Documents, and Pictures folders on your PC are automatically synced to the cloud, ensuring that they will be secure and available on other PCs and devices.

Power users often cite the forced Microsoft account sign-in as a key example of enshittification, and while there is some truth to that, the local account alternative is less secure, especially if you don't take steps to correct that. Key issues with a local account include:

- A local account is local to that one PC only, so it can't be recovered if it's compromised.
- A local account can be configured without a password, which is inherently insecure and all too easy to do.
- A local account without a password can't be configured to use a PIN, an additional layer of security that Windows 11 requires of any account with a password.
- A local account can't be configured with 2FA or any other passwordless authentication system, any of which are more secure than using just a password.

- A local account can't take advantage of key Windows 11 security features, including automatic full disk encryption, Windows Hello biometric authentication, and OneDrive Folder Backup unless you take additional steps after the fact.

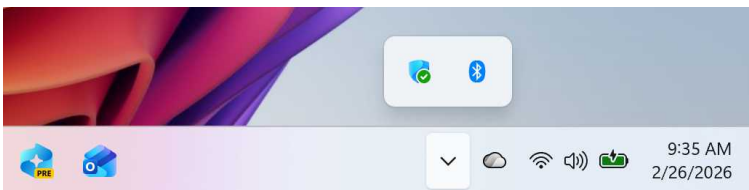
Though I don't recommend using a local account, this chapter will explain how to properly secure Windows 11 regardless of which type of sign-in account you choose.

♥ Windows 11 security first steps

Ideally, you will properly secure Windows 11 when you configure a new or newly reset PC. But you can also do so later. In [Start Fresh with a New Install of Windows 11](#), there's a short section about some of [the initial configuration tasks you will undergo after clean installing Windows 11](#). Among those tasks are some related to securing the PC.

Take any actions suggested by Windows Security

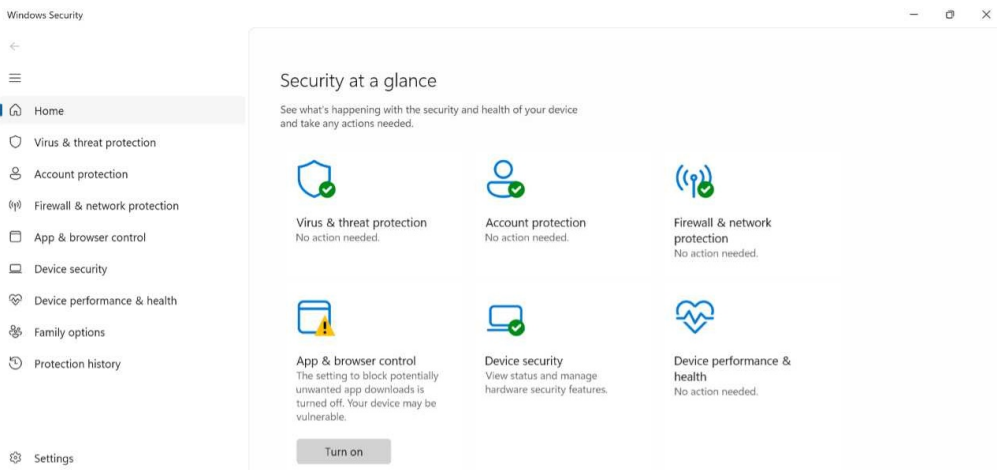
Windows Security is a dashboard for most of Windows 11's security features. It auto-runs at boot time, and you will find an icon for this app in the hidden icons pop-up to the left of the system tray in the Taskbar. To see it, click "Show hidden icons" ("^").



When there are no suggested or required actions, the Windows Security icon will display a green checkmark overlay indicating "No actions needed." But you may see a yellow "bang," a yield sign-like overlay, indicating a "Recommended action" or, worse, a red "bang" indicating a "Required action."



In either case, click the Windows Security icon to launch the app, which displays a grid of top-level security areas in its default Home view. Here, you will typically see one or more items that need attention.



On most PCs, you will see at least one security feature, “App & browser control,” that needs to be enabled. You should click “Turn on” to enable this feature.

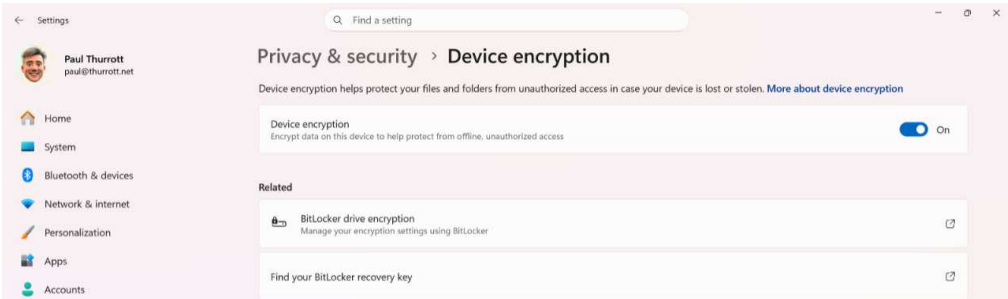
You should likewise enable any other features that are flagged by Windows Security as recommended. For example, if Local Security Authority protection is disabled, there’s no “Turn on” button in the Home view. But if you click “Go to settings,” Windows Security will display the Device security view where you can enable the option “Kernel-mode Hardware-enforced Stack Protection.” When you do so, Windows Security will prompt you to reboot the PC so that this feature is properly enabled. Do that.

→ **Learn more:** There are other features in Windows Security you should consider enabling. [Those features are discussed later in this chapter.](#)

Correctly configure device encryption

If you signed in with a Microsoft account (or a Microsoft Work or School account), Windows 11 will automatically configure a full disk encryption feature called Device encryption that automatically protects the data stored on your PC from physical attacks if it's lost or stolen. If you signed in with a local account, this feature is not automatically enabled and you will need to do so manually.

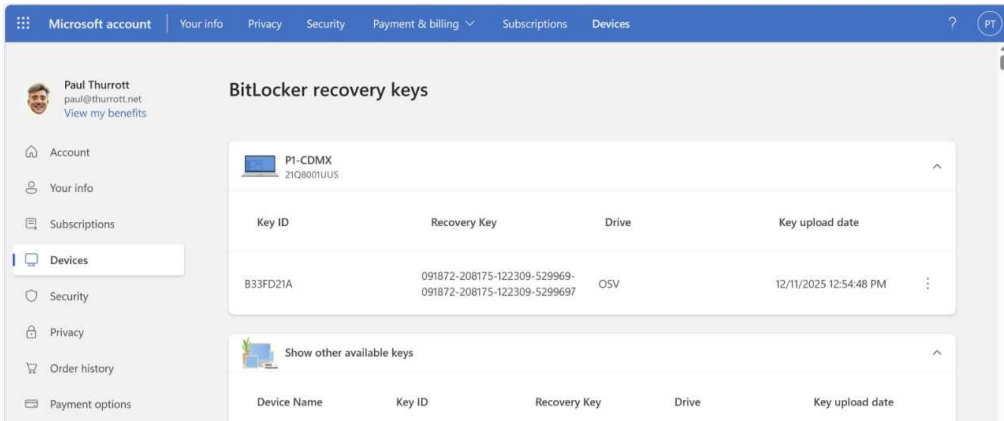
To check the status of Device encryption, open the Settings app and navigate to Privacy & security > Device encryption.



If “Device encryption” is configured to “On,” you’re all set: The disk is encrypted and your data is safe.

A few related tasks include:

Know how to access your recovery key. If your PC experiences issues in the future, you may be asked to supply a *recovery key*, a 48-character numeric code, to regain access to the encrypted disk. This key is stored in your Microsoft account, and you can find it by navigating to aka.ms/myrecoverykey with your web browser. The number of keys you will see on this page will vary by the individual, but you can find the correct key by searching for the PC’s name or key ID, the latter of which Windows 11 will prompt you for if required.



✔ **Tip:** If you signed in with a Microsoft Work or School account, the recovery key is available at aka.ms/aadrecoverykey.

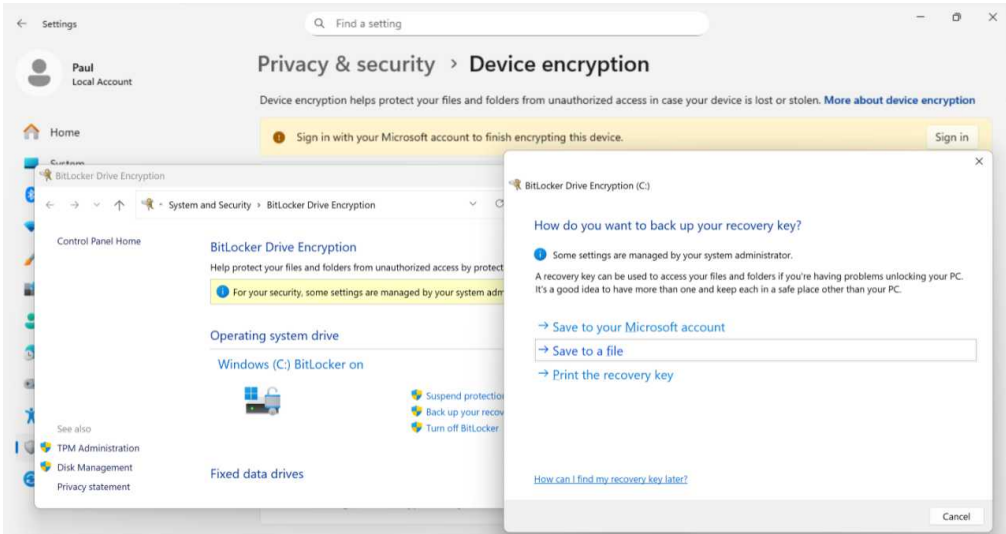
Local account only: Enable Device encryption and back up your recovery key. If you sign into Windows 11 with a local account, Device encryption is not fully enabled by default because doing so requires you to back up your recovery key first. If you are running Windows 11 Home, you can only save this recovery key to a Microsoft account, so you will need to click “Sign in” in the yellow infobar that reads “Sign in with your Microsoft account to finish encrypting this device.”



✔ **Tip:** If you have Windows 11 Pro, however, you can click the “BitLocker drive encryption” link instead to launch the BitLocker Drive Encryption control panel, where you can click “Back up your recovery key” and then choose where to save the recovery key as noted below.

✔ **Tip:** As a workaround to the above, I recommend that those who wish to use a local account with Windows 11 initially sign-in with a Microsoft account. This will enable Device encryption automatically and then you can convert the Microsoft account to local account (in Settings > Accounts > Your info). Or, you can add a local sign-in account (in Settings > Accounts > Other users), change its account type to “Administrator,” sign in with that account, and then delete the initial Microsoft account (also in Settings > Accounts > Other users).

Windows 11 Pro only: Further configure Device encryption with the BitLocker Drive Encryption control panel. If you’re running Windows 11 Home, there’s nothing further to do. But if you have Windows 11 Pro, you can run the BitLocker Drive Encryption control panel to back up your recovery key to another location, add BitLocker To Go encryption to removable USB storage, and perform other disk encryption-related tasks. There’s a link to this app in the Device encryption page in Settings, or you can find it using Start Search.

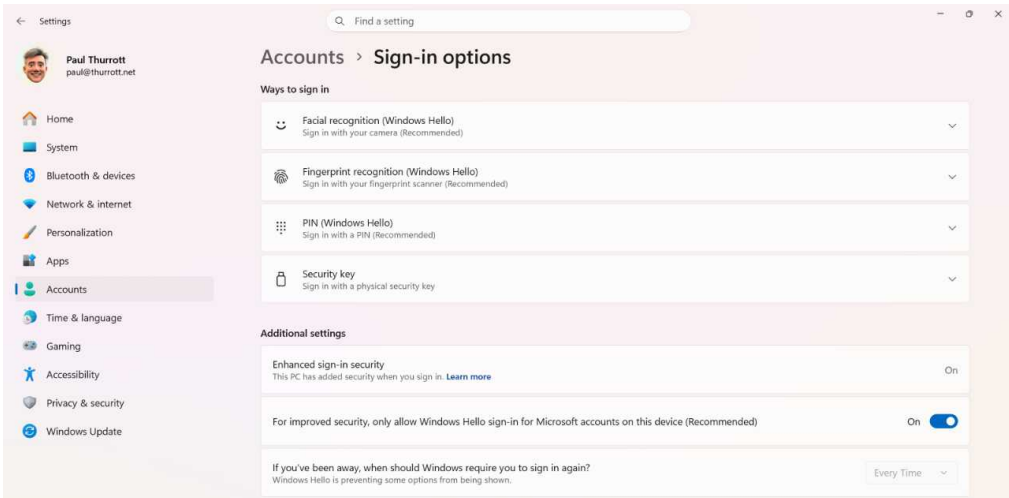


♥ Improve your sign-in account security

If you sign into Windows 11 using a Microsoft account, it will typically have an associated password and Windows Setup requires you to create a PIN. And if your PC supports Windows Hello facial and/or fingerprint recognition, you were prompted to configure one of those authentication methods as well.

If you sign into Windows 11 using a local account, it's possible you didn't even configure a password, let alone a PIN.

Whatever you chose during Setup, you can configure account sign-in options at any time. I recommend you do so now to improve security. To get started, open Settings and navigate to Account > Sign-in options.



There are several relevant options to consider and configure here.

Facial recognition (Windows Hello)

If your PC supports Windows Hello facial recognition, you can enroll here to sign into Windows 11 using your face. Or, if this feature is already configured, you can (and should) perform two important additional steps:

- **Enhance facial recognition protection.** Enable this option to help improve Windows Hello's spoofing protection, which will prevent others from masquerading as you to attempt to get into your computer. When you enable this option, you will need to restart the PC.
- **Make your sign-in more personal.** If you switch between contacts (or not wearing glasses) and glasses, click the "Improve recognition" button to (re)enroll your face with or without glasses. That is, you should scan your face once with glasses and once without.

Fingerprint recognition (Windows Hello)

If your PC supports Windows Hello fingerprint recognition, you can enroll one or more fingers here to sign into Windows 11 using your finger. Or, if this feature is already configured, you can perform one or more additional steps:

- **Set up another finger.** You can click an “Add a finger” button to enroll another finger so that you have multiple options for fingerprint recognition.
- **Set up the same finger again.** Less obvious, you can also use “Add a finger” to re-enroll the same finger you already enrolled to make recognition more accurate. This is an undocumented but useful option if you find that fingerprint recognition often fails.

✓ **Tip:** If your PC supports facial *and* fingerprint recognition, I recommend enabling both so that you have multiple options for signing in, each of which is faster and more convenient than typing a password or PIN.

PIN (Windows Hello)

If you signed in with a Microsoft account (or a Microsoft Work or School account), or if you signed in with a local account and created a password, you were prompted to create a PIN during Windows Setup. This PIN is an additional layer of security and a convenience since it will typically be faster to sign-in this way than typing a full password.

✓ **Tip:** Few people do this, but if you have multiple PCs and/or other devices, you should use a different PIN on each PC/device to improve security.

If you signed in with a local account but didn't create a password, do so now (in Settings > Accounts > Sign-in options > Password). Then, create a PIN here. Once you do so, you can enable Windows Hello facial and/or fingerprint recognition, depending on which your PC supports. Be sure to do so now, as described above.

Enhanced sign-in security

If you have a Copilot+ PC or another PC that supports Windows Hello Enhanced Sign-in Security (ESS), this option will be enabled and the option “If you’ve been away, when should Windows require you to sign in again?” will be grayed out and automatically configured to “Every Time.” This is the correct configuration.

For improved security, only allow Windows Hello sign-in for Microsoft accounts on this device (recommended)

By default, this option will be configured to “On” when you sign-in with a Microsoft account. This is the correct configuration.

Configure additional security features Windows Security

As noted previously, I recommend taking any recommended or required actions in Windows Security when you first set up Windows 11. But there are additional security features in Windows Security that aren’t usually enabled by default that you should at least consider as well.

They are:

Controlled folder access. If you sign-in with a Microsoft account, you get automatic ransomware protection through OneDrive when you store your files there and real-time protection against malware and other malicious software. But if you navigate to Virus & threat protection > Ransomware protection > Controlled folder access, you can enable an additional layer of protection against malicious apps that attempt to modify your files and the PC’s memory. To enable this feature, click “Manage controlled folder access” and turn it on. By default, Windows 11 will protect files stored in your Desktop, Documents, Pictures, Music, and Videos folders, but you can add other folders and unblock apps you trust that were flagged by Controller folder access.

Smart App Control. This feature provides another layer of protection against malicious or suspicious apps. By default, Smart App Control is configured in

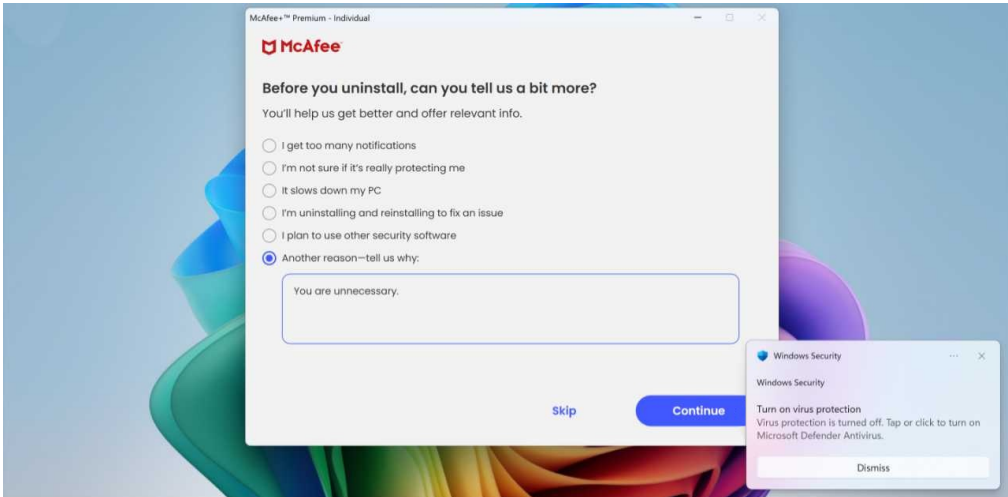
an evaluation mode when you first bring up a new Windows 11 installation, and it will either silently disable itself if it never detects any questionable app behavior or enable itself and alert you with a pop-up notification. Unless you are a developer, you should enable Smart App Control. To do so, navigate to App & browser control > Smart App Control and change the setting to “On.”



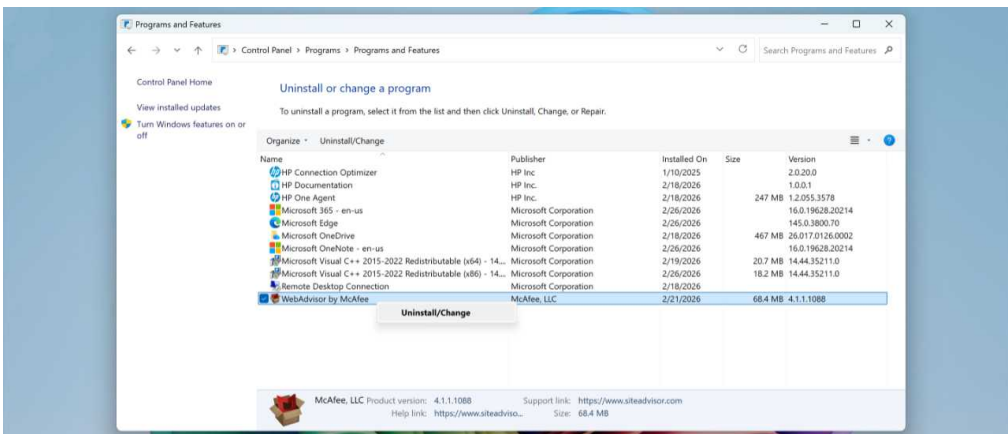
♥ Remove third-party security apps

Many PCs come with third-party security apps like McAfee that are superfluous because of the strong built-in protections in Windows 11. Worse, these solutions often require an unnecessary paid subscription to keep the protection active. You can safely remove these apps, and you should.

How you do so will vary by app. But the best way to remove most third-party security apps is to open Settings, navigate to Apps > Installed apps, and locate the offending app in the list. Then, click its “More options” (“...”) link and select “Uninstall” from the pop-up menu that appears. After confirming that you really do want to uninstall this app, you will likely have to put up with some nonsense from the app’s maker. Ignore its pleading and the Windows Security notification that claims your virus protection is turned off, as the built-in protections will automatically enable. Then, reboot when prompted.



You may not be done. Some security solutions, like McAfee, install a second superfluous security app that isn't visible in the Installed apps list in Settings, a behavior one might logically characterize as malicious. To check for this, open Control Panel (which you can find with Start Search), click "Uninstall a program" (under "Programs"), and look at the list of apps it presents. Here, for example, you can see WebAdvisor by McAfee. Right-click it, choose "Uninstall/Change," and get rid of this nonsense for good.



Other security apps, like HP Wolf, have multiple entries in the Installed apps list that you will need to uninstall. After you uninstall HP Wolf and reboot,

open Settings again, navigate to Apps > Installed apps, and uninstall the related apps, in this case HP Security Update Service and HP Wolf Console.

Yes, these companies purposefully make this process difficult.

♥ Keep Windows 11 up-to-date

In [Start Fresh with a New Install of Windows 11](#), there's a short section about some of [the initial configuration tasks you will undergo after clean installing Windows 11](#). Among those tasks are some related to updating Windows and its in-box apps using Windows Update (Settings > Windows Update) and the Microsoft Store app, respectively. But it's important to keep Windows 11 fully up-to-date at all times, so there are some additional steps to take.

Properly configure Windows Update

Microsoft updates Windows 11 on an aggressive schedule through a feature called Windows Update, with new features and security fixes appearing at least once each month via what's now (erroneously) called a Security Update. These are *cumulative* updates, meaning that each builds on the previous month's Security Update, dating back to the previous annual *feature update* that usually arrives each October. And they typically appear on the second Tuesday or each month, on what's called *Patch Tuesday*, though Microsoft also sometimes ships out-of-band Security Updates if there is a serious issue to address.

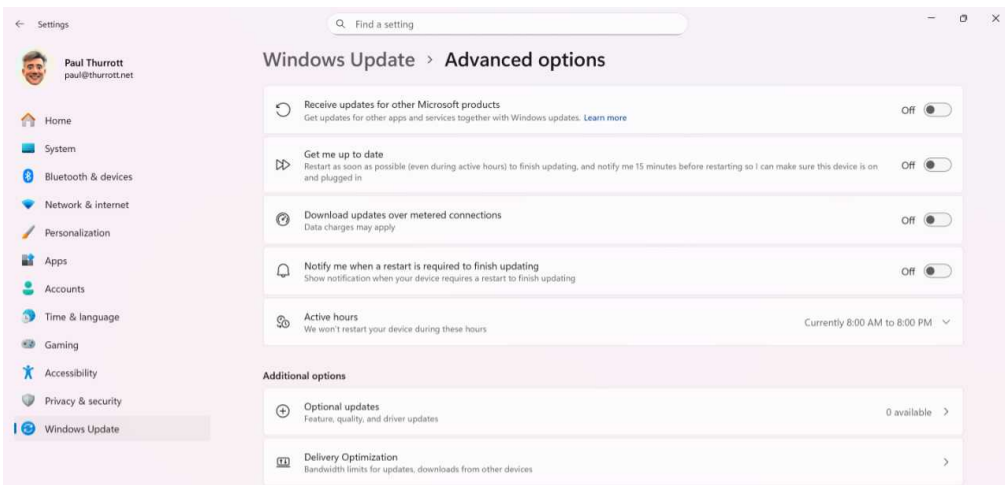
Security Updates are mandatory for individuals. That is, there is no option to skip a Security Update, though Windows Update lets you pause updates temporarily, for one week at a time.

In between the monthly Security Updates, Microsoft also ships a Preview Update, usually on the fourth Tuesday of the month. This doesn't have a fun name, but we often refer to these updates, which are optional, as "Week D" updates, because of Microsoft's update schedule. (The Patch Tuesday update typically occurs on "Week B.") These Preview Updates are literally an early peek at the next month's Security Update, and they are made available for anyone who wishes to get new features as quickly as possible.

Which is ironic because most of the new features that Microsoft ships in its Security Updates, Preview Updates, and annual feature updates are delivered

via a technology called Controlled Feature Release (CFR). That's another horrible name: These features are rolled out randomly on no schedule whatsoever, so those with multiple PCs will often, if not always, see different mixes of features on each.

Windows Update is available in the Settings app: Just navigate to Windows Update and click "Check for updates" if it doesn't automatically do so. But given the chaotic nature of Windows 11 updates, you should spend a few minutes to configure *how* the system installs updates so you're not disrupted by an unexpected reboot while you're working.



I recommend the following configuration changes in Windows Update > Advanced options:

Get me up to date. Configure this to "Off" so that Windows Update doesn't restart your PC to install updates as quickly as possible.

Notify me when a restart is required to finish updating. Configure this to "On" so that Windows Update doesn't simply restart the PC when it wants to install updates, which can lead to data loss if you have unsaved documents.

Active hours. Windows Update won't restart your PC to install updates during active hours, which is configured to be between 7:00 am and 10:00 pm. This is likely a good schedule for most, but if you work evenings or odd hours, you may want to adjust it.

Delivery optimization. By default, Windows Update is configured to “allow downloads from other devices,” which seems like a good idea: One PC on your network could download available updates from Windows Update and then others could get those updates from the PC on the network instead of from Microsoft over the Internet. But in practice, this can cause bandwidth issues on your PCs, and so I recommend disabling this feature.

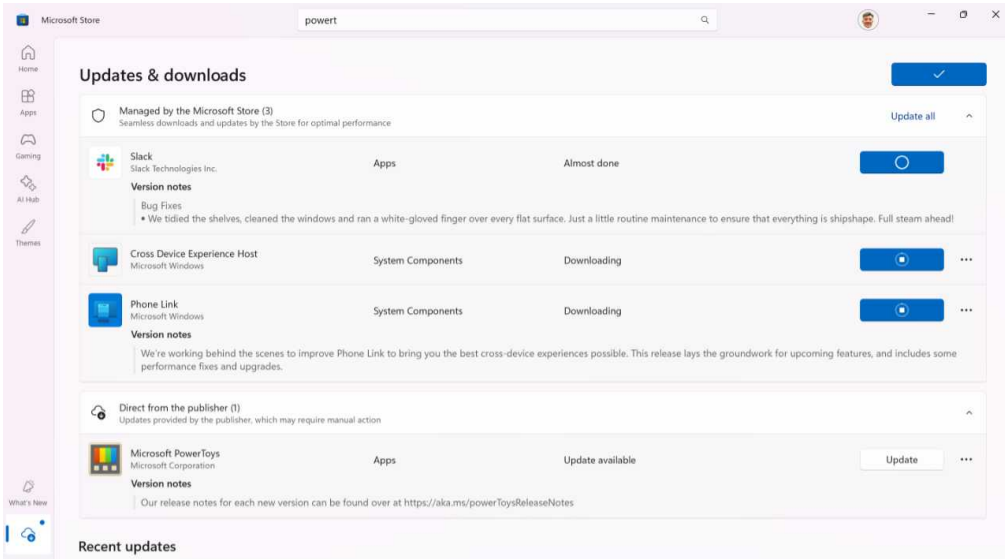
✔ **Tip:** If you’re familiar with the [Win11Debloat](#) utility I recommend elsewhere in this book, you can use it to make three of the four changes recommended above.

Keep apps up-to-date

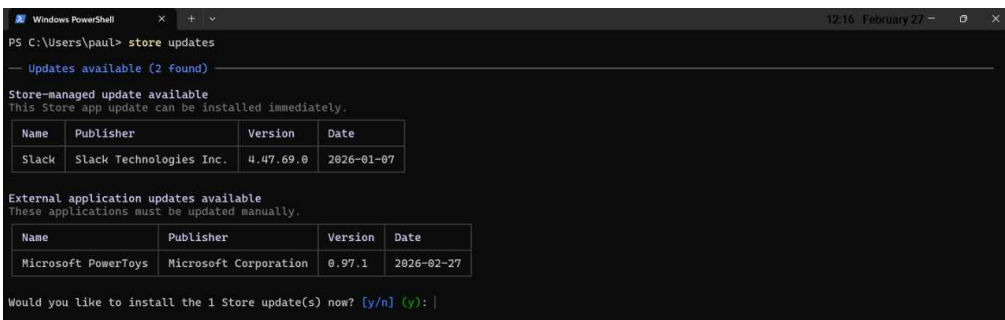
As a Windows user, you will typically install apps from the web or from the Microsoft Store. Apps downloaded from the web typically have their own updating mechanisms and will often alert you when there is an update. And apps downloaded from the Store will typically update through the Store, though there are exceptions. Either way, you don’t have to think too much about app updates. They will occur automatically in the background, or apps will alert you when there’s a pending update.

That said, you may want to keep certain apps as up-to-date as possible. And in addition to using the Store to check for app updates when you first configure Windows 11, you may want to check manually from time-to-time as well. There are different ways to do so, only one of which is obvious.

Microsoft Store. You can check for app updates in the Microsoft Store app by navigating to Downloads and clicking “Check for updates.” Most apps with pending updates will update automatically, but in some cases, like Microsoft PowerToys, you will have to manually click an “Update” button to trigger an update.



Store CLI. Microsoft recently introduced a command line Store CLI app, **store**, that you can run from Terminal. Among its many uses, you can use this app to update an individual app or, better still, use the command **store updates** to update all apps with pending updates. These updates happen in the background, so you don't have to babysit them in any way.



Windows Package Manager. Windows 11 includes another command line app, the Windows Package Manager, which can be used to install and update apps from the web and the Microsoft Store. To see all pending app updates across both sources, you can use the command **winget update** in Terminal. And to update them all at once, you can use **winget update --all --silent**. (The --silent bit requires a Terminal window with administrator privileges.)

```

C:\Users\paul> winget update --all --silent
-----
Name                               Id                               Version           Available         Source
-----
DS Clock                            DualitySoftware.DSCLock        2.6.3            5.1.2.0          winget
Git                                  Git.Git                         2.52.0           2.53.0           winget
Epic Games Launcher                 EpicGames.EpicGamesLauncher    1.3.161.0        1.3.173.0        winget
Visual Studio Community 2026 Insiders Microsoft.VisualStudio.Community.Insiders 18.3.11429.125 18.4.11519.219  winget
Microsoft Windows Desktop Runtime - 9.0.11 (x64) Microsoft.DotNet.DesktopRuntime.9 9.0.11           9.0.13           winget
EA app                              ElectronicArts.EADesktop        13.621.0.6134   13.649.2.6163   winget
Microsoft .NET SDK 9.0.308 (x64)    Microsoft.DotNet.SDK.9         9.0.308         9.0.311         winget
Microsoft .NET Runtime - 8.0.23 (x64) Microsoft.DotNet.Runtime.8     8.0.23         8.0.24         winget
Opera Stable 127.0.5778.76         Opera.Opera                     127.0.5778.76  128.0.5807.25  winget
PowerToys (Preview) x64           XP89DCGQ3K6VLD                0.97.1          0.97.2          msstore
Microsoft Teams                    Microsoft.Teams                  25332.1210.4188.1171 26032.208.4399.5  winget
Foundry Local Model Server        Microsoft.FoundryLocal          0.8.117.0       0.8.119.102    winget
13 upgrades available.

The following packages have an upgrade available, but require explicit targeting for upgrade:
-----
Name                               Id                               Version           Available         Source
-----
Discord Discord.Discord 1.0.9220 1.0.9226  winget

Agreements for Microsoft PowerToys [XP89DCGQ3K6VLD] Version 0.97.2
Version: 0.97.2
Publisher: Microsoft Corporation
Publisher Url: https://aka.ms/powertoys
Publisher Support Url: https://aka.ms/powertoysReportBug
License: https://aka.ms/powertoys-license
Privacy Url: http://go.microsoft.com/fwlink/?LinkId=521839
Copyright: ms-windows-store://pdp/?ProductId=XP89DCGQ3K6VLD
Agreements:
  Category: Developer tools
  Pricing: Free
  Free Trial: No
  Terms of Transaction: https://aka.ms/microsoft-store-terms-of-transaction
  Seizure Warning: https://aka.ms/microsoft-store-seizure-warning
  Store License Terms: https://aka.ms/microsoft-store-license

The publisher requires that you view the above information and accept the agreements before installing.
Do you agree to the terms?
[Y] Yes [N] No: y
Installing dependencies:
    
```

Because the Windows Package Manager offers the broadest coverage, I recommend using it to check for app updates when you want to make sure everything is as up-to-date as possible. I do this approximately once each week.

De-Enshittify Microsoft Copilot and AI

Windows 11 was born in enshittification, but the rise of Copilot and Microsoft's AI ambitions has only made matters worse.

The problems here are many, but key among them are the speed at which AI moves, in this case driving constant change in Windows 11, and how we as users and customers can separate the good from the bad. Though many have a visceral reaction to AI for whatever reasons, there are truly useful AI-based features in Windows 11. And some that are not so useful, of course.

The problems with Copilot and AI in Windows 11

When Microsoft first announced Windows 11 in mid-2021, it seemed that the company was going to reverse one of the more controversial examples of enshittification in Windows 10 by switching from a biannual feature update—that is, a major version upgrade—schedule to releasing just one feature update each year. Windows 11 would also continue to receive monthly security updates, which seemed reasonable.

But it was lie. Yes, Microsoft would technically only issue one feature update each year, but it would also deliver new features to Windows 11 every single month via a rebranding of Windows as a Service (WaaS) as “[continuous innovation](#)”. This allowed Microsoft to escalate the introduction of new features dramatically, while eroding the quality of the platform and leading to monthly chaos.

And then it got worse.

In early 2023, Microsoft triggered the AI era when it announced what would later be called Copilot in a special event that February. This was an major new strategy for the company and a fundamental shift from its previous focus on cloud computing. Windows, like the rest of Microsoft, would need to get on board. Among other things, it planned to integrate a Copilot app in Windows 11 that would debut in that year's feature update, called Windows 11 version 23H2.

Microsoft needed to get Copilot deeply embedded across its ecosystem as quickly as possible, but it faced one major logistical hurdle: The enterprise customers that represent the majority of the Windows userbase demand and are given more lenient upgrade policies which allow them, among other things, to delay or even skip feature updates. And it was clear that these customers would simply skip Windows 11 version 23H2, delaying the deployment of Copilot in Windows 11 for most customers for at least a year.

Given the speed at which AI moves and the rapid gains made by the competition, Microsoft couldn't afford that delay. And so it did something unprecedented in the history of Windows: It shipped almost all the new features in Windows 11 version 23H2 in a normal monthly security update for Windows 11 versions 21H2 and 22H2 one month ahead of the release of that feature update. This meant that all customers, including those in the enterprise that would delay or skip 23H2, got the integrated Copilot app and related features whether they wanted them or not. This is a textbook example of enshittification in which Microsoft's needs usurped its business customers' needs.

This shift marked two other important changes that persist to this day.

First, the quality of these monthly "security" updates declined yet again, with Microsoft rushing to put more and more AI-based features in Windows 11 every single month. Microsoft briefly marketed them as "Moments," as if this was a positive development customers would want. But when those moments became overly negative because of the lack of quality and all too frequent because the monthly cadence, that came to a close.

Second, Microsoft slyly overcame another blocker tied to the desires of its enterprise customers to delay feature and security updates as long as possible. With this shift, it began making each supported Windows 11 version functionally identical. So enterprises could stick to whatever version of Windows 11 they preferred, but it wouldn't matter because they would still get the same new features every single month that Microsoft was delivering to a newer version of Windows 11 too. On paper, Microsoft was doing what its enterprise customers asked for—fewer updates—but in reality, it was the reverse: They could stay on an older Windows 11 version, but they were getting new features every month. What's in a name?

And then, incredibly, it got even worse.

In mid-2024, Microsoft announced its Copilot+ PC initiative. This represented

a another new escalation of feature delivery via a new type of computer. Copilot+ PCs would get exclusive AI-based features that were artificially constrained to work on the NPU, or neural processing unit, that they contained. These also tend to be premium PCs with higher than average price tags, and this was an attempt to revive PC sales during the post-pandemic sales lull. But this created yet another strange and artificial bifurcation of features: In addition to Windows 11 Pro, which offers some features not found in Windows 11 Home, PC makers were now offering Copilot+ PCs that offer some features not found in other PCs running Windows 11 Home or Pro.

If that was Microsoft's only sin with Copilot+ PC, it would barely warrant a mention here. But Copilot+ PC triggered the most controversial episode of Microsoft's AI era so far: It would ship with a feature called Recall that critics believed would be a privacy and security nightmare despite the impressive protections built in to the platform. The resulting outcry from customers and so-called security experts, none of whom even owned a Copilot+ PC, was over the top, wrong-headed, and simply wrong. But it was enough to delay the release of Recall by several months.

The privacy and security issues with Recall were imaginary, making those complaints ridiculous. But this episode clearly demonstrated that customers were tired of Microsoft jamming Copilot and other AI features down their collective throats via forced monthly updates—sorry, “continuous innovation”—and that Microsoft's hubris was a big part of the problem. Somehow, incredibly, the software giant never saw the tsunami of hate coming despite everything it had done to enshittify Windows 11.

The Recall incident did have one positive outcome, thankfully. Originally, Recall was going to be auto-enabled for customers who bought a new Copilot+ PC and customers who didn't want it could later opt-out. But thanks to the outcry, Microsoft made Recall opt-in. This is clearly the right approach for any powerful AI feature that works with your personal data, and at the time of this writing, it seems that Microsoft finally got the message: It appears that future similar AI-based features in Windows 11, Copilot+ PC or not, will likewise be opt-in and not opt-out.

No one can predict the future, but hopefully Microsoft will now take a kinder, gentler approach to introducing Copilot and other AI features in Windows 11. In the meantime, you have this chapter so you can learn what you can do with the Copilot and AI features in Windows 11 that we're stuck with today. Some of

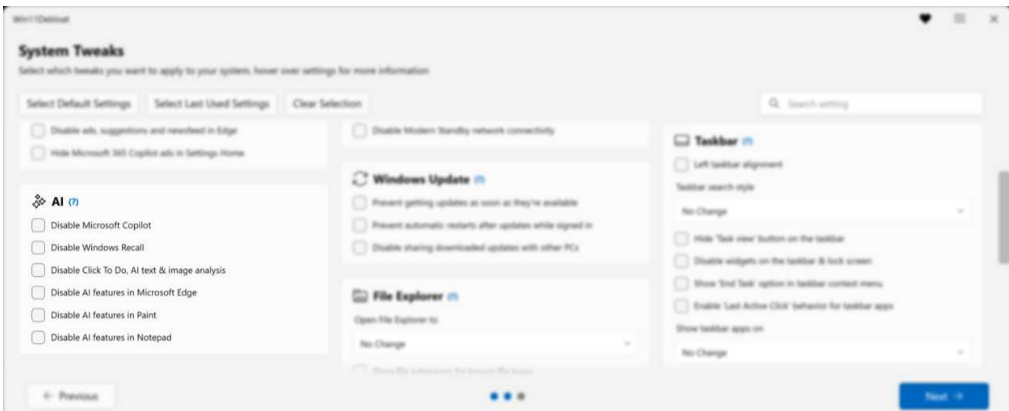
💛 Uninstall or disable Copilot and other AI features in Windows 11

When it comes to uninstalling or disabling Copilot and the other AI features in Windows 11 I have good news and I have bad news. The good news is that most of it *can* be removed, some of it quite easily. The bad news is that there isn't a single utility, yet, that we can use to easily uninstall or disable any or all the Copilot and AI features in Windows 11. This isn't anyone's fault, given the speed at which Microsoft adds new AI features to Windows 11. But it means we will have a bit of work to do if the goal is a full exorcism.

Given this, let's start with what we can automate. And then manually work on the stragglers.

💚 Automate the removal of some AI features using Win11Debloat

As is so often the case, the easiest way to bulk remove Copilot and several other AI features is to use [Win11Debloat](#). It has a section for AI tools on its System Tweaks page.



➔ **Learn more:** Win11Debloat is central to the clean installation process

discussed in [De-Enshittify an Existing Install of Windows 11](#).

To use Win11Debloat, visit [its home page on GitHub](#), where you will find the following URL for its underlying PowerShell script. Open a Terminal window with administrator privileges and enter the following:

```
& ([scriptblock]::Create((irm "https://debloat.raphi.re/")))
```

When the Win11Debloat app runs, choose “Custom Setup.” Then, click “Next” in the App Removal screen to get to System Tweaks. The following options are available in the AI section:

Disable Microsoft Copilot

This option will uninstall the Microsoft Copilot app and remove the Copilot shortcut from the Windows 11 Taskbar. That’s pretty straightforward, and since most people seem to prefer a third-party AI chat like Anthropic Claude, Google Gemini, or OpenAI ChatGPT, either on the web or, when available, via a standalone Windows app, it’s an obvious choice for many.

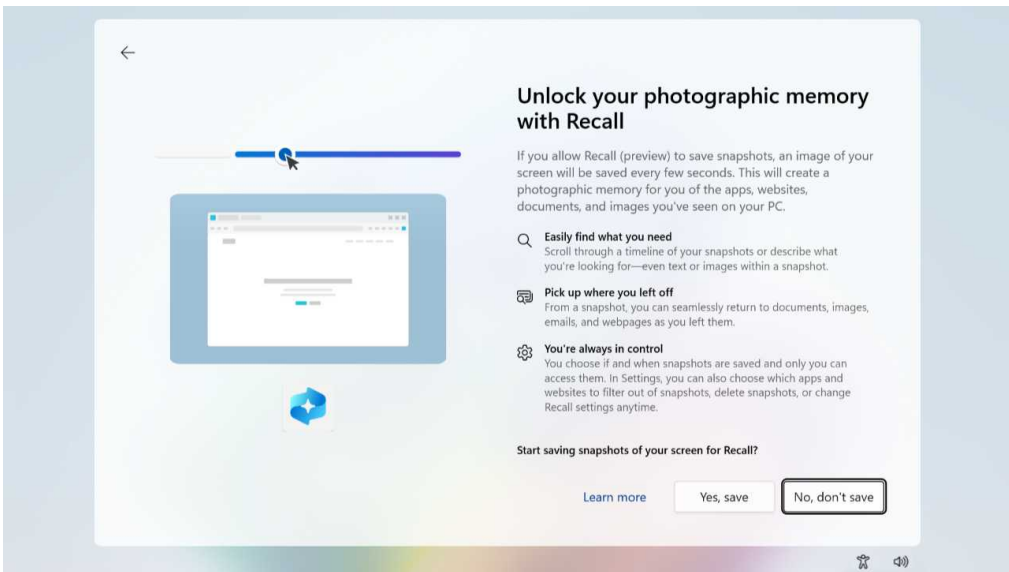
✓ **Tip:** Microsoft Copilot can be manually uninstalled by right-clicking its Start menu icon and choosing “Uninstall” from the context menu that appears. Or, you can open the Settings app, navigate to Apps > Installed apps, locate Microsoft Copilot in the list, click its “More options” (“...”) link, and then choose “Uninstall” from the context menu that appears.

Disable Microsoft Recall

Recall triggered a lot of controversy when it was introduced as the key new feature exclusive to Copilot+ PCs in mid-2024, but there’s nothing controversial about it. When enabled, Recall records snapshots—i.e. screenshots—of your activities on the PC and then lets you navigate back in time later to find something you did. These snapshots are stored locally on your PC in a

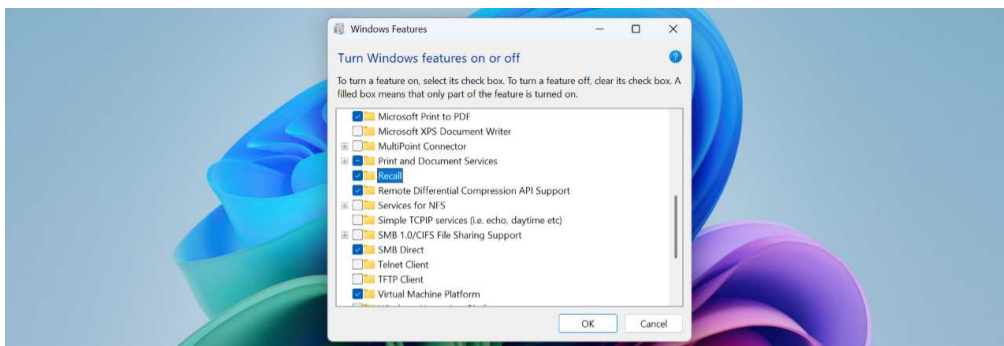
secure enclave separated from the rest of the system and are protected by the unique security capabilities in Copilot+ PCs.

When you bring up a Copilot+ PC for the first time, Windows Setup will prompt you to enable Recall. But, as noted, this feature is optional, and you can simply choose “No, don’t save” and skip right by this step.



If you use Win11Debloat to disable Recall, it will turn off snapshots and the underlying service, and remove the feature from Windows 11.

✓ **Tip:** Windows 11 lets you uninstall Recall, but not via the Settings app. Instead, you open the Windows Features app (use Start search to find it), locate and uncheck “Recall,” and then click “OK” and reboot the PC.



Disable Click to Do, AI text and image analysis

Click to Do has emerged as the single best feature unique to Copilot+ PCs: It uses visual intelligence to analyze the text and graphics you see on-screen in Windows 11 and in any apps.



Given its usefulness, I don't recommend removing Click to Do. But Win11Debloater lets you do so easily enough if you feel otherwise.

✔ **Tip:** You can also uninstall Click to Do manually using the Settings app in Windows 11, but not in the normal location. To do so, open Settings and navigate to Privacy & security > Click to Do (under Windows permissions). There, you can simply configure Click to Do to “Off.”

Disable AI features in Microsoft Edge

It shouldn't be surprising that Microsoft is building extensive AI capabilities into its web browser. But for the same reasons noted above with Microsoft Copilot in Windows 11, most people prefer and use other AI chatbots, making the built-in AI functionality in Microsoft Edge more of a distraction than useful.

Win11Debloater removes all the AI-based functionality in Microsoft Edge, including the Copilot icon in the Edge toolbar and the pane/window it uses, Ask Copilot, writing assistance, and Copilot Mode and its unique New tab page.

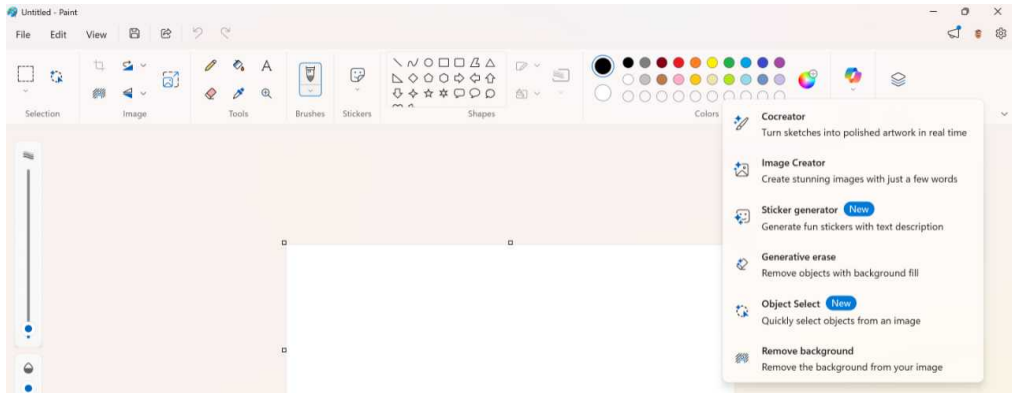
✔ **Tip:** You can remove Copilot and other AI features from Microsoft Edge manually as well. It's just more tedious: In Edge settings, you will basically disable every relevant option in Appearance > Copilot and sidebar, Appearance > Copilot and sidebar > App specific settings > Copilot, and AI innovations. A better approach? Disable or uninstall Microsoft Edge entirely.

Disable (some of) the AI features in Paint

Microsoft has been building out new features in the in-box Paint app for the past few years, some based on AI and some not, and while some of them are stinkers, most of them are quite useful. Because this is all or nothing configuration, I do not recommend disabling any AI features in Paint.

Confusing matters, the AI features you see in Paint will vary by PC. All PCs will see features like Image Creator, Generative erase, and Remove

background, and those with a Copilot+ PC will also see additional features powered by local AI, like Cocreator, Object Select, and Sticker Generator.

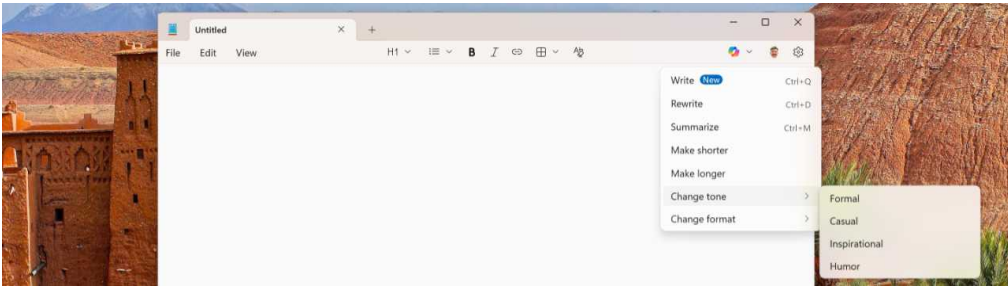


In my experience, Win11Debloat removes some but not all of the AI features in Paint, regardless of which type of PC you have.

✓ **Tip:** There is no way to disable the AI features in Microsoft Paint from within the app's settings interface or otherwise.

Disable the AI features in Notepad

Similarly to Paint, Microsoft has dramatically improved Notepad in recent years by modernizing the user interface and adding support for tabs and multiple documents, Markdown “light formatting,” and, of course, AI-based writing tools.



✓ **Tip:** You can simply disable all the AI features in Notepad by opening the app's settings interface, scrolling down to AI Features and configuring "Copilot" to "Off."

i More info: If you need to revert any of these changes, [the maker of Win11Debloat](#) provides the necessary Registry scripts on GitHub.

De-Enshittify Microsoft Edge

Microsoft Edge is the modern successor to Internet Explorer, but it's also a key vector for enshittification in Windows 11. For this reason, it's important to configure this web browser correctly. And that's true whether you intend to use Microsoft Edge or not.

 **Warning:** Do not ignore this chapter if you use a different web browser.

The problems with Microsoft Edge

Microsoft Edge is the most malicious software that Microsoft bundles with Windows 11. The problems with this app are many. But key malicious behaviors include:

Online tracking. Microsoft Edge tracks your online activities so Microsoft can harvest your personal data, target you with advertising, and sell that information to other data brokers and online advertisers that will expand this abuse.

Online tracking with other apps. Because Microsoft Edge is the basis for the web app platform in Windows 11, many in-box and third-party apps are secretly running Microsoft Edge in the background. And that means you are still being tracked online, even if you use a different web browser.

Windows 11 ignores your default web browser choice. If you configure another web browser as the default, as most will, Windows 11 will ignore your choice and launch Microsoft Edge when you perform certain actions in Windows 11, ignoring your choice include clicking a widget or news feed article in Widgets, clicking a web link in Search highlights, clicking a web link in the Get Help in-box app, and using the Copilot app in Windows 11.

Microsoft uses dark patterns that fool users into agreeing to even more online tracking. If you choose to use Microsoft Edge, the browser uses dark

patterns—*lies*—when you initially set it up to convince you to change the default configuration in ways that benefit Microsoft but open you up to even *more* online tracking.

Microsoft Edge ignores your web browser customizations. If you use Microsoft Edge and customize it in certain ways, it will harass you to change the configuration back to the defaults because they benefit Microsoft. This happens when you change the default search engine away from Bing, disable certain features in the default New Tab page (which displays content from Microsoft Start and other Microsoft services and is full of hidden tracking and advertising), change the New Tab page to a third-party option, and more. In some cases, Edge will even change the configuration back to the Microsoft default without informing you.

Microsoft Edge continues harassing you to enable optional features that will further expose you to more Microsoft tracking and advertising. If you use Microsoft Edge and make no configuration changes, the browser will still harass you. It will use dark patterns when it prompts you to make configuration changes that it claims are for your benefit but are designed only to ensure that you are exposed to more online tracking, data harvesting, and Microsoft advertising. These suggestions use language like “Make Microsoft Edge better for you and others” to misrepresent the true intent of the configuration changes it wishes you to enable. In other words, it lies to you to fool you into making a mistake.

Uninstall Microsoft Edge?

If Microsoft simply allowed Windows 11 users to uninstall Microsoft Edge, this book would be a lot shorter and many people’s lives would be at least a little bit happier. But in most of the world that’s not possible, and so most will have to deal with the workarounds I outline in this chapter instead. That said, there *are* ways to install Windows 11 in such a way that Microsoft Edge is never installed in the first place. You can learn more in the [Setup](#) chapter.

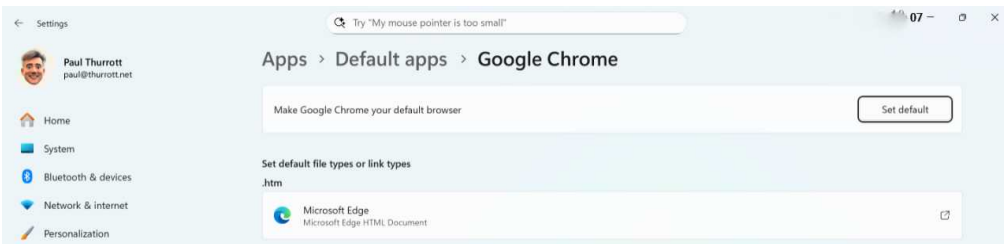
Use a different web browser as your default

Most people will choose Google Chrome, Mozilla Firefox, Brave, or another web browser and not Microsoft Edge. If that’s what you want, you need to do more than just install your preferred web browser.

♥️ Configure your preferred web browser as the default

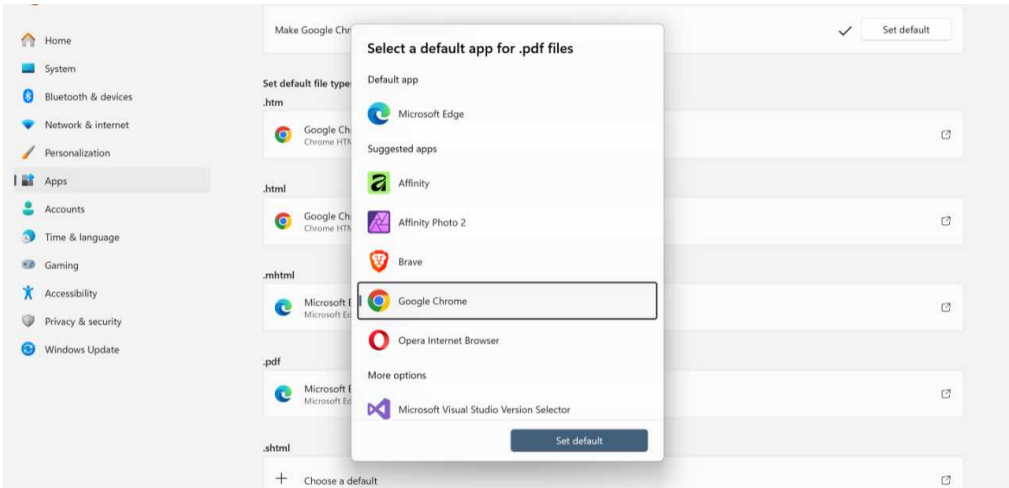
When you install and configure Google Chrome or another web browser, it will prompt you to configure it as the default. Regardless of whether you did so, you should review this change again to make sure it's how you want it.

To do so, open the Settings app and navigate to Apps > Default apps. Then, find and select your preferred web browser in the list of apps under “Set defaults for applications.”



At the top of this page, click the “Set default” button next to “Make [this web browser] your default browser.” When you do, Windows 11 changes four file and link types—`.htm`, `.html`, `HTTP`, and `HTTPS`—to use your preferred web browser. Note, however, that the other file and link types remain configured to use Microsoft Edge.

Most of these are not particularly important. But you should also configure PDF files—the `.pdf` file type in this list—to open with your preferred web browser. To do so, locate `.pdf` in the list and click the “Open with” icon to its right. Then, select your preferred web browser in the “Select a default app for `.pdf` files” dialog that appears.



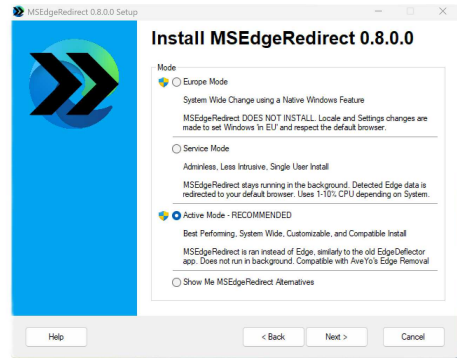
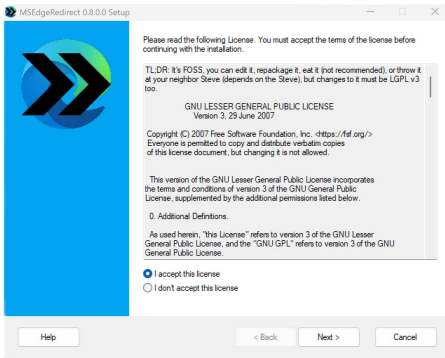
♥ Prevent Microsoft Edge from running in the background

Microsoft Edge runs at startup every time you boot your computer and sign-in. You can safely prevent that from happening if you use a different web browser.

To do so, open the Settings app and navigate to Apps > Startup. After optionally sorting the list of apps you see here by Status, locate Microsoft Edge and configure it to “Off”.

♥ Prevent Windows 11 from ignoring your default web browser choice

It's not possible to fully thwart the bad behaviors associated with Microsoft Edge using the tools provided by Windows 11. To prevent Windows 11 from ignoring your default web browser choice fully, you need to use a free third-party utility called [MSEdgeDirect](#).



When you install this useful app, it will prompt you to choose between three modes. Choose “Active Mode.” In the next admittedly confusing screen, just click “Install”. Then, click “Finish” to complete the installation.

Now, Windows 11 will respect your default web browser choice, even when you click a link in Widgets, Search highlights, or the Get Help or Copilot apps.

🧡 Use Microsoft Edge as your default web browser

So, you’ve decided to use Microsoft Edge. I will (try to) not judge you for this mistake, but I do have some advice about how to configure this web browser correctly to minimize the malicious behaviors.

🧡 Configure Microsoft Edge correctly at first run

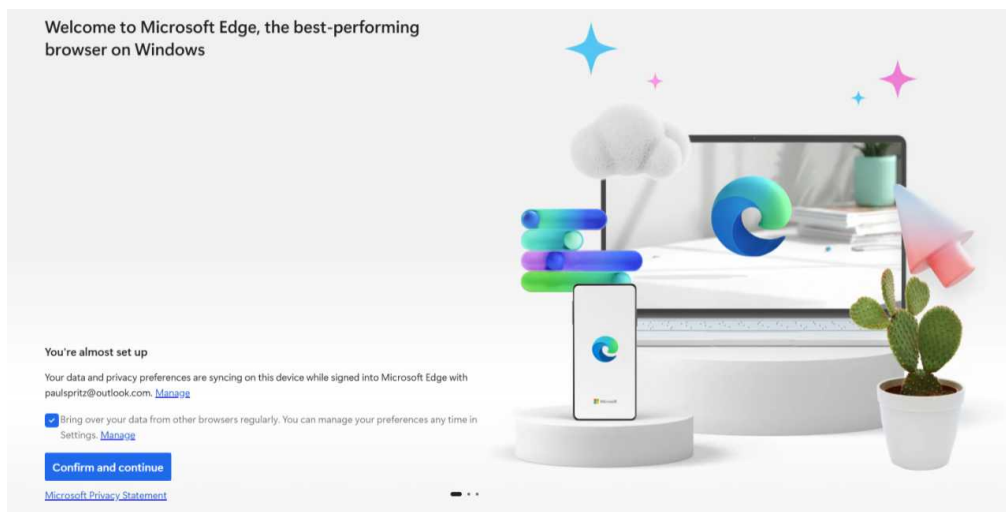
If you just bought a new PC or reset an existing PC and run Microsoft Edge for the first time, it steps you through an initial configuration in which Microsoft uses dark patterns to get you to lower your guard and allow it to maximize its control over your web browser. Be careful here. You should reject each of its default recommendations.

➡ **Learn more:** If you are already using Microsoft Edge, jump ahead to [Configure Microsoft Edge correctly after you’ve started using it](#) to reverse any mistakes you made during its initial configuration.

Here are the configuration steps you have to complete.

Welcome to Microsoft Edge, the best performing browser on Windows

There are two sets of configurations to consider here.

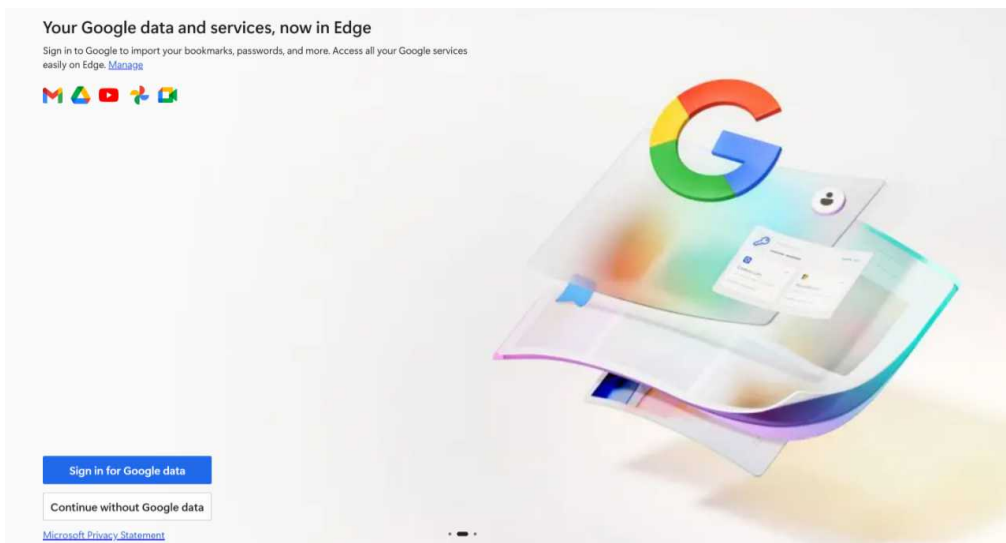


- **Your data and privacy preferences are syncing on this device while signed into Microsoft Edge with [your Microsoft account].** If you use Microsoft Edge, you obviously want to sync data like favorites (bookmarks), extensions, (some) settings, and the like. But you can click the “Manage” link next to this text to determine exactly which data and settings you will sync.
- **Bring over your data from other browsers regularly.** This is the the malicious option: If you leave this checked/enabled, Microsoft will siphon all your browsing data from Google Chrome (and not other browsers, despite the description) so that it can obtain a more complete record of your web browsing activities and use that information to target you with advertising while selling it to third-party advertisers as well. **Uncheck this option.**

Your Google data and services, now in Edge

Here, Microsoft Edge prompts you to sign in to your Google account so it can import your bookmarks, passwords, and other personal data. If you agree to

do so and successfully sign in to your Google account, Microsoft Edge will save your login information in its integrated Microsoft Password Manager by default.

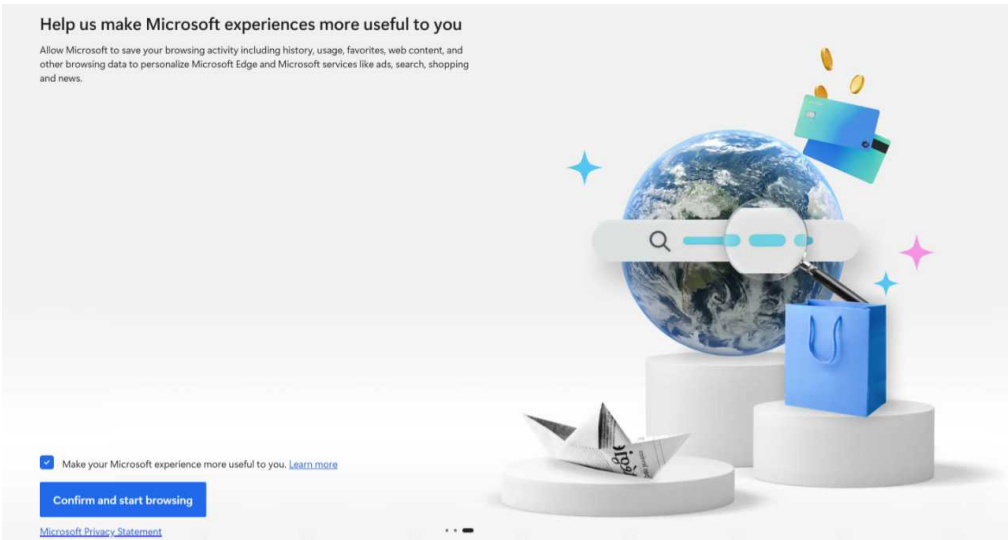


There is no reason to do this. If you need to import any data from Chrome or any other web browser, Microsoft Edge supports doing so using a one-time import that doesn't require your Google (or other account) login information.

Click "Continue without Google data" here.

Help us make Microsoft experiences more useful to you

This full-screen dark pattern is the most nefarious you will encounter while setting up Microsoft Edge. It suggests that allowing it to have more access to your personal data will somehow benefit you. But this will really benefit Microsoft and its advertising partners by exposing you to more online tracking, data harvesting, and Microsoft advertising.



Do not allow this. **Uncheck the option “Make your Microsoft experience more useful to you” before continuing.**

Express yourself by customizing Microsoft Edge with themes and Welcome to your AI browser

Next, Microsoft Edge displays two tabs that let you customize the browser further and learn more about its unique features. These are mostly innocuous and can be safely ignored.

- **Express yourself by customizing Microsoft Edge with themes.** [In this screen](#) you can configure a few options related to how the browser looks and works. If you don't make any changes here, Microsoft Edge will display using the same mode (Light or Dark) as Windows 11, using a horizontal tab layout, and using the default theme.
- **Welcome to your AI browser.** [This screen](#) presents a multi-page look at unique Microsoft Edge features you may want to know about.

♥ **Configure Microsoft Edge correctly after you've started using it**

If you're already using Microsoft Edge, you should ensure that you didn't enable any of the bad behaviors Microsoft tried to trick you into during the initial configuration. Each of these options can be found in Microsoft Edge settings.

Microsoft Edge can sync your history, passwords, and other browser data across all your signed-in devices

Navigate to Profiles > Sync in Microsoft Edge settings to view and potentially modify which data you sync between this PC and the Microsoft Edge installs on other PCs and devices.

(Do not) import browsing data at each browser launch

Navigate to Profiles > Import browser data > Import browsing data at each browser launch in Microsoft Edge settings to ensure that the option “Import browsing data from Google Chrome on each launch” is configured to “Off.”

Import your browser data from other browsers and passwords managers

Navigate to Profiles > Import browser data > Other import locations in Microsoft Edge settings to perform a one-time import of data from other web browsers and password managers. Doing so will not create a connection between Edge and other products or online accounts.

Select your privacy settings for Microsoft Edge

Navigate to Privacy, search, and services > Privacy in Microsoft Edge settings and locate the option “Allow Microsoft to save your browsing activity including history, usage, favorites, web content, and other browsing data to personalize Microsoft Edge and Microsoft services like ads, search, shopping and news” at the bottom. Ensure that this is configured to “Off.”

♥ Further configure Microsoft Edge to minimize the bad behaviors

Aside from the configurations noted above, you should at least consider making the following configuration changes to better protect yourself from this web browser and its maker.

Change the default New Tab page

The default New Tab page in Microsoft Edge is a cesspool of tracking, data harvesting, advertising, low-quality content, and other noise. You can configure this page using the “Page settings” (gear) icon in its upper-right,

but you will be better served by replacing it and never exposing yourself to its malicious behaviors again.

I recommend using a third-party New Tab page like [Momentum](#) or [Bonjour](#), both of which you can install from [the Microsoft Edge Add-ons website](#). Either extension will replace the default New Tab page in Microsoft Edge, preserving your safety, privacy, and sanity.


Determine what Microsoft Edge displays when you start the browser

By default, Microsoft Edge is configured to display its New Tab page when you start the browser. Even if you want to use this page, and you don't, it's more likely that you will prefer to preserve your previous browsing session when you start Microsoft Edge.

To change this, navigate to Start, home, and new tab page in Microsoft Edge settings and configure "On startup" to "Open the tabs from the previous session."

Minimize how Microsoft Edge tracks your online activities

Microsoft Edge includes an integrated Tracking protection feature that purports to block online trackers to protect your privacy. But if you check the tracker blocking efficacy of a clean install of Microsoft Edge with the Electronic Frontier Foundation's [Cover Your Tracks](#) website, you will discover that this browser doesn't protect you at all.



Our tests indicate that you are not protected against tracking on the Web.

IS YOUR BROWSER:

Blocking tracking ads?	<u>No</u>
Blocking invisible trackers?	<u>No</u>
Protecting you from fingerprinting?	Your browser has a unique fingerprint

See how trackers view your browser

To be clear, **Microsoft Edge doesn't block tracking ads or invisible trackers and it doesn't protect you against fingerprinting, another method by which Microsoft and its advertising partners track your activities online.**

Given this, you can safely ignore the Tracking protection feature in Microsoft Edge and install the [Privacy Badger](#) and [AdBlock Plus](#) browser extensions from the Microsoft Edge Add-ons site to actually protect yourself against on-line tracking and fingerprinting. After doing so, you will see that Cover Your Tracks reports that you are protected against tracking and fingerprinting on the web.

✔ **Tip:** You can use a VPN (virtual private network) to protect your privacy further by routing all the data that travels between your browser and the Internet through a secure, encrypted connection. I recommend using a VPN when using Microsoft Edge to access websites that contain sensitive financial or personal information, especially when you're using a public and potentially vulnerable Wi-Fi hotspot. Edge includes a built-in VPN called Microsoft Edge Secure Network, but it is borderline useful. So I recommend using a third-party VPN. The best free option is [Proton VPN](#).

Configure Microsoft Edge safety features

Microsoft Edge includes several useful features related to safety and security, and while most of them are configured properly by default, it's worth examining these options to make sure. You do so by navigating to Privacy, search, and services > Security in Microsoft Edge settings.

The following security features are not enabled by default, and you should consider enabling them.

Automatically switch to more secure connections with Automatic HTTPS.

When enabled, Microsoft Edge will force websites that support the more secure HTTPS protocol to use it rather than the less secure HTTP.

Enhance your security on the web. Toggling this option to "On" will enable Enhanced security mode, which uses advanced security features in Windows 11 to protect you against potentially malicious websites. When enabled, you can choose between two modes, Balanced and Strict, the latter of which may prevent some websites from working correctly.

♥ Remove Copilot from Microsoft Edge

Even those who use Microsoft Edge have likely picked OpenAI ChatGPT, Anthropic Claude, or some other third-party AI chatbot and ignore or reject Microsoft Copilot. But Copilot is integrated into Microsoft Edge and there's a big, hard-to-ignore Copilot button taking up valuable real estate in the Microsoft Edge toolbar. The good news? You can remove Copilot from Microsoft Edge and prevent it from appearing in the browser.

To do so, open Microsoft Edge settings, navigate to Appearance > Copilot and sidebar > App specific settings and configure the option "Show Copilot button on the sidebar" to "Off".

Then, navigate to AI innovations in Microsoft Edge settings and configure "Copilot Mode" to "Off". This will disable the other options you see on this page.

Then, navigate to Languages in Microsoft Edge settings and scroll down to the "Writing assistance" section. There, configure "Use Copilot for writing on the web" to "Off".

♥ Eliminate other Microsoft Edge annoyances

If you're going to use Microsoft Edge, there are a few other annoyances you may wish to curtail.

Microsoft Edge tabs appear in Alt-Tab

➖ **The problem:** By default, Alt + Tab displays the three most recent Microsoft Edge tabs and not just running apps.

♥ **The solution:** You can configure Windows 11 to display the 3, 5, or 20 most recent Edge tabs in Alt + Tab, or you can configure it to display no tabs. To do so, open the Settings app, navigate to Multitasking, and review the options associated with "Show tabs from apps when snapping or pressing Alt + Tab."

Change your search engine

➖ **The problem:** By default, Microsoft Edge uses Bing for its search engine.

♥ **The solution:** You can configure Microsoft Edge to use Google Search or the search engine you prefer. To do so, open Microsoft Edge settings and navigate to Privacy, search, and services > Search and connected experiences > Address bar and search > Search engines. Then, click the “More options” (“...”) button next to the search engine you prefer and select “Make default” from the context menu that appears.

Streamline how Microsoft Edge downloads files from the Internet

➖ **The problem:** By default, Microsoft Edge displays a prompt with “Open” and “Save as” buttons every time you try to download a file.

♥ **The solution:** You can configure Microsoft Edge to just download files immediately like other web browsers do. Open Microsoft Edge settings, navigate to Downloads, and configure the option “Ask where to save each file before downloading” to “Off”.

Disable Microsoft Shopping assistance

➖ **The problem:** By default, Microsoft Edge displays annoying shopping notifications when you visit a shopping site. (This feature is U.S.-only.)

♥ **The solution:** Microsoft tracks your activities online if you leave this feature enabled. But you can disable this behavior: Open Microsoft Edge settings, navigate to Privacy, search, and services > Search and connected experiences and configure the option “Save time and money with Shopping in Microsoft Edge” to “Off”.

De-Enshittify OneDrive

OneDrive is Microsoft's cloud storage service for consumers and a key integration in Windows 11 when you sign in using a Microsoft account. But Windows 11 auto-enables a OneDrive feature called Folder Backup for many users without telling them that it is doing so, to drive customers to subscribe to Microsoft 365, which includes additional OneDrive storage over the 5 GB provided to all users.

i More info: Which users will see this behavior? I'm still trying to track this down, but it impacts many millions of people worldwide and has been happening for years. Based on limited evidence, I believe it is tied to the amount or percentage of cloud storage used, or both. If you don't see this, great. Consider yourself lucky. But if you do, this chapter can help you fight back against this inexcusable tactic.

The problems with Microsoft auto-enabling OneDrive Folder Backup

In Windows 11 version 25H2, Microsoft has subtly changed how Microsoft OneDrive Folder Backup works. And though some of the changes are improvements over the previous behavior, problems remain. Among them:

OneDrive never tells the user that it is enabling Folder Backup. OneDrive will silently enable Folder Backup, which syncs the Desktop, Documents, and Pictures folders on your PC to the corresponding folders in OneDrive, without informing you.

You may not want OneDrive to sync the Desktop, Documents, and/or Picture folders to OneDrive. Depending on how you work, you may not wish for all the files and folders in the Desktop, Documents, and Picture folders to sync to the cloud. Regardless of how you work, these folders often contain

files that shouldn't be synced to all your PCs and other devices. For example, many games save game data to your Documents folder and syncing that content to the cloud unnecessarily takes up storage space and may lead to you needing more storage. Which you have to pay for.

When you disable Folder Backup for a particular folder, OneDrive asks you where to put the content in that folder. This sounds like a good idea—you can choose to keep the content in OneDrive or move it to the local version of the folder on your PC—but it's half-baked. When Windows 11 silently enabled Folder Backup, it commingled the contents of the local folders with the content of the OneDrive-based folders. So when you choose to reverse this change, OneDrive prompts you where to keep the content. And all the content in each folder, including whatever was already in OneDrive, will be moved to the location you choose. If you choose to keep it on your PC, you may not have enough storage space. And the files and folders are all mixed up with whatever was in OneDrive already.

i More info: In previous versions of Windows 11, Microsoft would prompt you to enable OneDrive Folder Backup during Windows Setup when you first configured the PC and later using a pop-up notification. Then, it would simply ignore your choice and auto-enable Folder Backup if you declined the offer previously. In Windows 11 version 25H2, Microsoft no longer prompts you to use OneDrive Folder Backup. Instead, it simply auto-enables this feature after you sign in to Windows 11 with a Microsoft account.

Uninstall OneDrive

OneDrive is useful for all kinds of reasons, including even the Folder Backup feature that this chapter is largely concerned with. But if you don't use OneDrive, perhaps because you use a rival service like Google Drive instead, you can easily uninstall OneDrive in Windows 11. Doing so will free up system resources and clean up the File Explorer user interface a bit.

To uninstall OneDrive, open Settings and navigate to Apps > Installed apps. Then, locate Microsoft OneDrive in the list of apps installed on your PC. Click

the “More options” (“...”) link to its right and then select “Uninstall” from the context menu that appears. Then, click “Uninstall” when prompted that this app and its related info will be uninstalled.

You don’t need to reboot after this change. But File Explorer will continue to display one vestigial OneDrive feature, the Gallery item in its navigation bar on the left. To remove Gallery from File Explorer, open Terminal with administrator privileges and use the following command line:

```
reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desk  
0e1c-4e20-9aa6-edcd0212c87c}"
```

Gallery will be removed from File Explorer instantly.

✔ **Tip:** Uninstalling OneDrive in Windows 11 doesn’t remove any files you may have stored in Microsoft’s cloud storage service. You can still access those files using [the OneDrive website](#) or via the OneDrive app on your other PCs and devices.

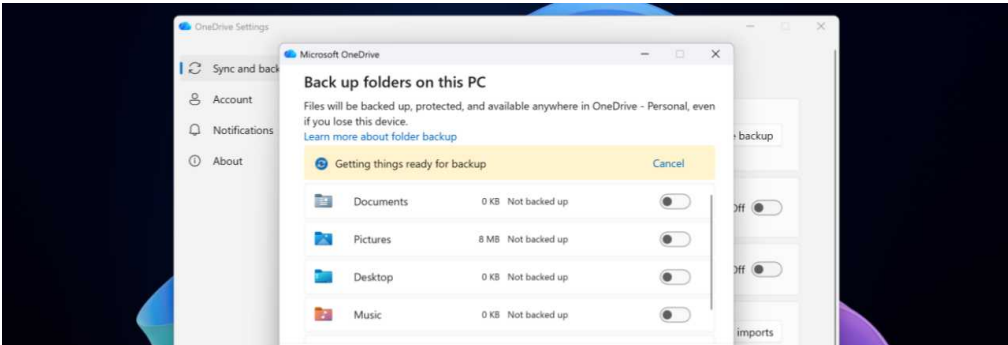
♥ Prevent OneDrive from enabling Folder Backup when you set up a PC

If you are setting up a new PC or a newly reset PC, you may be able to prevent OneDrive from auto-enabling Folder Backup if you move quickly and know the trick: You have to do this right after you complete the Windows Setup Out of Box Experience (OOBE) and arrive at the Desktop for the first time.

Wait for the OneDrive icon to appear in the Taskbar’s system tray area. When it first appears, it will display with an angled line through it, indicating that Windows 11 is updating the app.

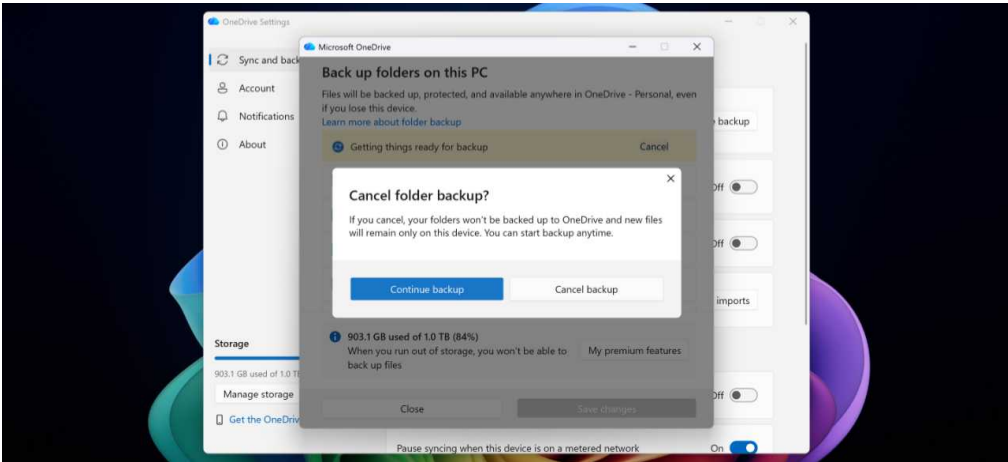


When the update is complete, OneDrive will restart, so the icon in the system will disappear and then re-appear. When it signs into your Microsoft account again, the angled line will disappear. Then, click the OneDrive system icon and open OneDrive settings by clicking Help & Settings (gear) and then Settings. In the “OneDrive Settings” window that appears, select Sync & backup and then “Manage backup” next to “Back up important PC folders to OneDrive.” The “Back up folders on this PC” window appears.



If you're lucky, you will see a yellow info bar at the top of this window with the text “Getting things ready for backup.” To prevent Folder Backup from auto-enabling, click the “Cancel” link.

✓ **Tip:** How long do you have to click this “Cancel” link before it disappears forever? In my experience, the yellow info bar will appear in the “Back up folders on this PC” window until shortly after OneDrive finishes processing all the files you have in the cloud. So it depends on how much storage you're using. In my case, using about 900 GB, this takes about about 30 minutes.

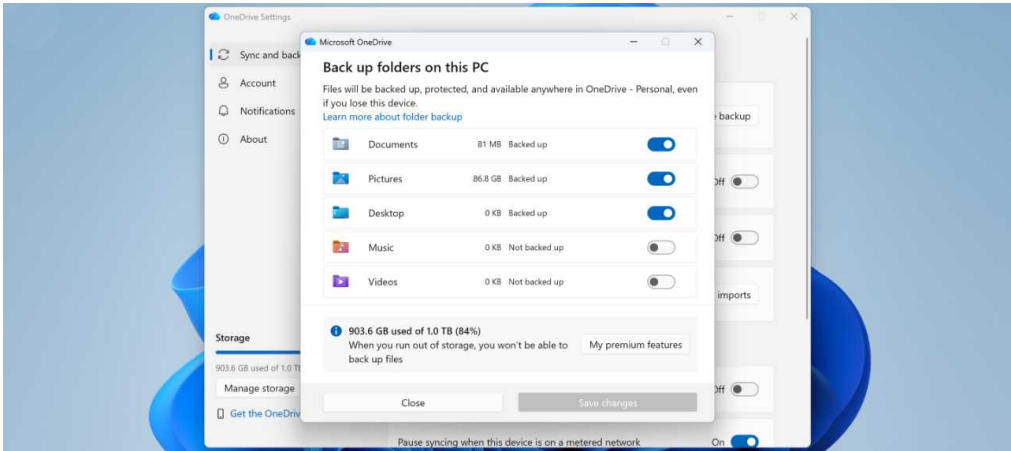


In the “Cancel folder backup?” window that appears, click “Cancel backup.” Now, OneDrive Folder Backup won’t molest you further.

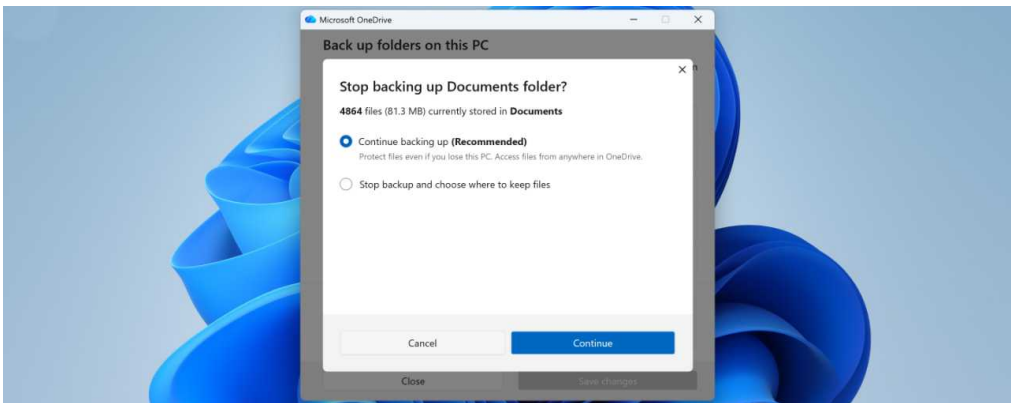
♥ Reverse the changes made by OneDrive Folder Backup

If OneDrive Folder Backup is already enabled on your PC, you can reverse that for any or all of the three folders—Desktop, Documents, and Pictures—it includes. When you do so, OneDrive will prompt you to decide where the contents of each folder should reside, in the cloud in OneDrive or locally, on your PC.

To disable OneDrive Folder Backup, open OneDrive settings, navigate to the Sync and backup page if required, and click the “Manage backup” button next to “Back up important PC folders to OneDrive.” The “Back up folders on this PC” window will appear.



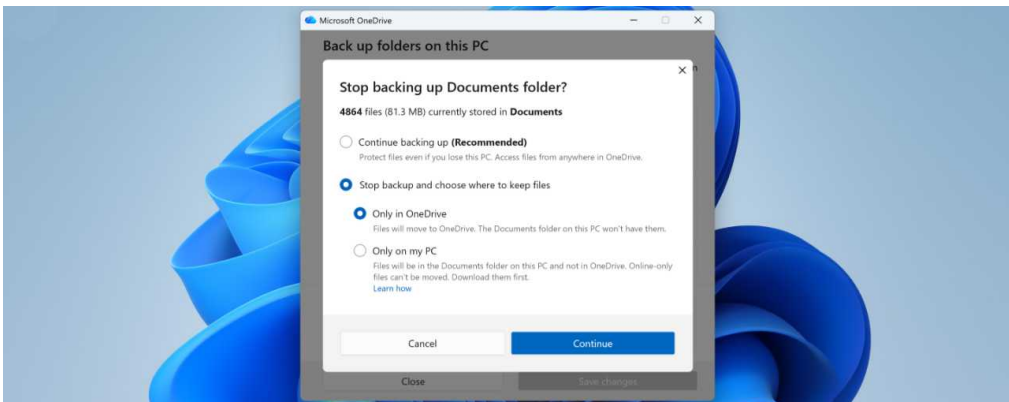
Unless you've changed this configuration, you will see that the Desktop, Documents, and Pictures folders are being synced with OneDrive. And that you can optionally enable this sync with the Music and Video folders as well. To disable folder backup, configure one of the synced folders to "Off". When you do, a "Stop backing up [Folder name] folder?" window appears.



i More info: This window explains how many files there are in this folder and the amount of disk space they require. That information might be

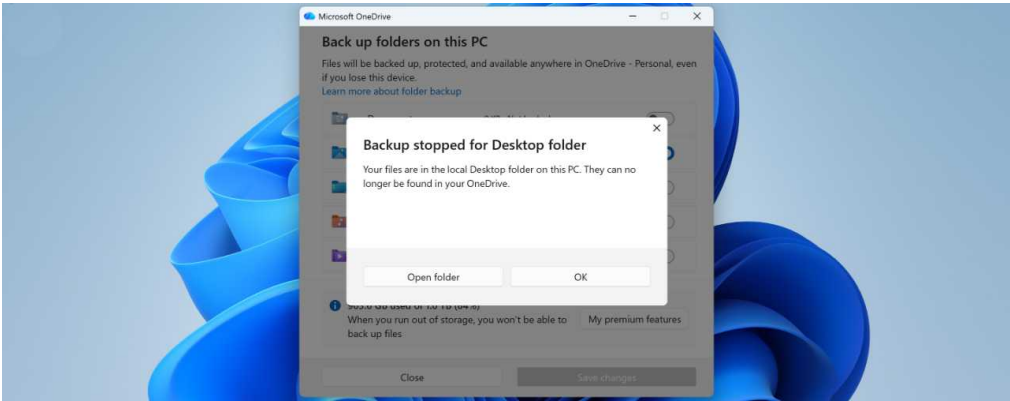
crucial if you want to move the contents of this folder to your PC and it doesn't have enough disk space.

Click “Stop backup and choose where to keep files.” Now, OneDrive prompts you to choose *where* you will store the files in this folder, only in OneDrive or only on your PC.

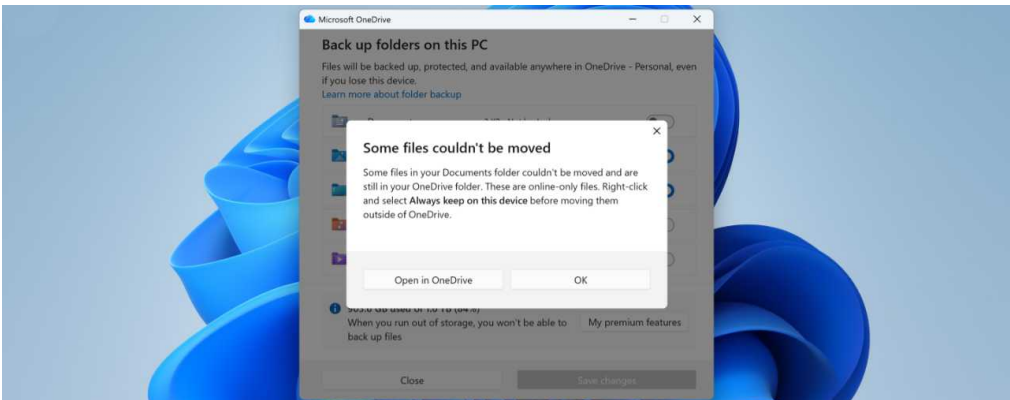


i More info: In case it's not obvious, when Windows 11 automatically enabled OneDrive Folder Backup, it commingled the contents of each local folder with the contents of the corresponding folder in OneDrive. For example, if your local Pictures folder contained 119 items occupying 183 MB of disk space, and the Pictures folder in OneDrive originally contained 12 items occupying 15.7 MB of disk space, the Pictures folder in OneDrive now contains 131 items occupying 198.7 MB of disk space. So OneDrive will move *all* the items in this folder to your local Pictures folder if you disable Folder Backup for that folder. This may or may not be desirable.

Click “Only on my PC.” OneDrive will attempt to move all the items in the cloud-based folder to the corresponding local folder. If successful, you will see a “Backup stopped for [Folder name] folder” dialog.



i More info: In some cases, OneDrive may fail to move some or all of the items to your local folder. In this case, it will display a “Some files couldn’t be moved” dialog explaining what happened: Those files are still in OneDrive. So your only recourse is to move them manually using File Explorer.



If the change is successful, the files and folders that were once only on your PC and the files and folders that were once only in OneDrive will be combined into a single set of items that is only on your PC. This introduces two potential problems.


You may not want this. Unfortunately, OneDrive isn't smart enough to differentiate between the items that used to be only on your PC and those that used to be only in OneDrive. So it's on you to browse through the files and folders you just moved and optionally find those you wish to now move back to OneDrive. Sorry.


You may not have enough storage space on your PC to contain the commingled items. If the OneDrive folder you're now disabling contained lots of files, perhaps consuming many gigabytes of storage, you may not have enough storage space on your PC to contain the items you wish to move. In this case, the operation will fail and those items will remain in OneDrive. However, Folder Backup is disabled, so you can use File Explorer to manually move at least some of the items out of OneDrive and to your PC.

Eliminate other OneDrive annoyances

Aside from its forced Folder Backup usage, OneDrive integration in Windows 11 is mostly excellent and can be quite useful. But there are a few small annoyances you may need to address.

You need more OneDrive storage

 **The problem:** Microsoft provides everyone with a Microsoft account with 5 GB of OneDrive cloud storage. But that's not enough if you're going to rely on OneDrive for work, backing up your phone photos, or just about anything else.

 **A workaround:** Sadly, there's no getting around the 5 GB limit in OneDrive: If you need more storage, you need to pay, and not just once but monthly or annually in the form of a [Microsoft 365 subscription](#). The cheapest is Microsoft 365 Basic, which provides 100 GB of additional cloud storage for \$19.99 per year. But most will be better off with Microsoft 365 Personal (\$99.99 per year) or Microsoft 365 Family (\$129.99 per year), each of which provides an additional 1 TB of OneDrive storage per user (in the latter case for up to 6 accounts/people). If you pay for Microsoft 365 Personal or Family and require even more storage, Microsoft offers add-on storage plans in 200 GB (\$1.99 per month), 1 TB (\$9.99 per month), 5 TB (\$49.99 per month), and 10 TB (\$99.99 per month) increments as well.

✔ **Tip:** If you don't mind switching services, you can save some money by using a paid Google One plan instead. Everyone with a free Gmail account gets 15 GB of Google Drive storage, or you can get a Google One Basic (100 GB, \$19.99 per year), Google One Standard (200 GB, \$29.99 per year), or Google One Premium or Google AI Premium (2 TB, \$99.99 per year) subscription.

OneDrive displays annoying “Memories” notifications

➖ **The problem:** OneDrive displays “On this day” memory notifications every day if you have any photos in your cloud storage from the same day but in the past. This is the type of thing most people already see on their phones, so some will find this additional PC-based notification superfluous if not annoying.

♥ **The solution:** You can disable this feature. To do so, open OneDrive settings, navigate to the Notifications tab, and configure the option “Notify me when ‘On this day’ memories are available” to “Off”.

You want to move OneDrive to a different disk

➖ **The problem:** You would like to move your OneDrive files to another disk, but Windows 11 configures it to live on your C: drive by default (at C:\Users\username\OneDrive).

♥ **The solution:** While the default location of your OneDrive files in Windows 11 is ideal for those with a single SSD or other disk, those with two or more drives may wish to move OneDrive to a new location. To do so, open OneDrive settings, navigate to the Account tab, and click the “Unlink this PC” link. In the “Unlink account on this PC?” dialog that appears, click “Unlink account.” A “Set up OneDrive” window appears. Sign-in to your Microsoft account as prompted and then step through the mostly promotional screens until you get to “Your OneDrive folder.” Click “Change location” and choose the new location for your OneDrive folder.

✔ **Tip:** You still need to delete the previous version of your OneDrive folder to regain that disk space. And if you use Files on Demand, you will need to resync whichever folders and files you prefer to make available when your PC is offline.

Fix Annoyances with Other Windows

11 In-Box Apps and Experiences

COMING SOON