Windows Sandbox: The Secret App That Lets You Open Anything Without Risk

Using this tool, you can safely check suspicious files, install suspicious software, or browse dangerous websites without risking damage to your main computer.

Windows has a built-in tool that creates a completely isolated environment. Using this tool, you can safely inspect suspicious files, install questionable software, or browse dangerous websites without risking damage to your main computer.

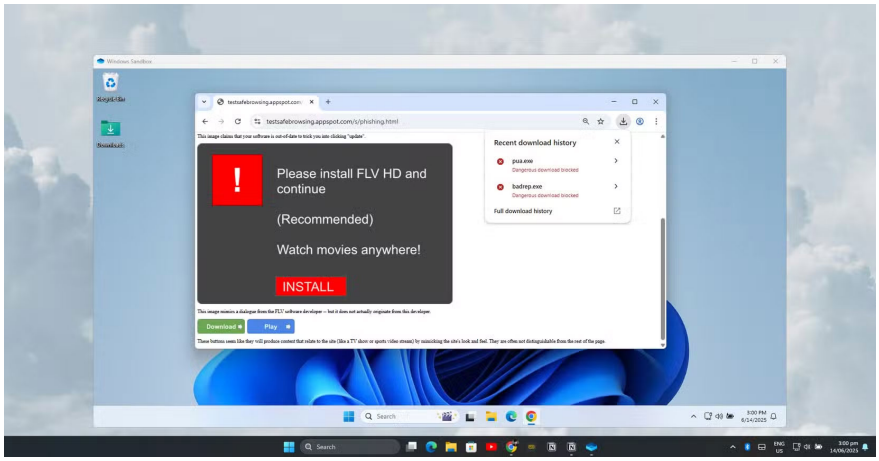
Learn about Windows Sandbox

Windows Sandbox is a built-in security feature found in Windows 10 and 11 Pro, Enterprise, and Education editions. It creates a temporary, isolated Windows environment that's completely separate from your main system. Think of it as a disposable computer inside your computer. Anything you do in the sandbox stays there, and when you close it, all traces are gone. That makes it one of the easiest ways to test whether a download is safe without risking your files or settings.

Unlike traditional virtual machines that require you to install an operating system and set aside a portion of your hard drive, Windows Sandbox uses your existing Windows files to create a temporary, lightweight desktop in seconds. It's designed to be fast, efficient, and incredibly simple for anyone to use - no tech wizardry required!

The temporary nature of Windows Sandbox is both its greatest strength and its defining feature. Every time you launch it, you get a fresh installation of Windows. When you close the sandbox, everything is gone forever. All installed software, downloaded files, registry changes, and system modifications are gone without a trace.

Get started with your first virtual sandbox



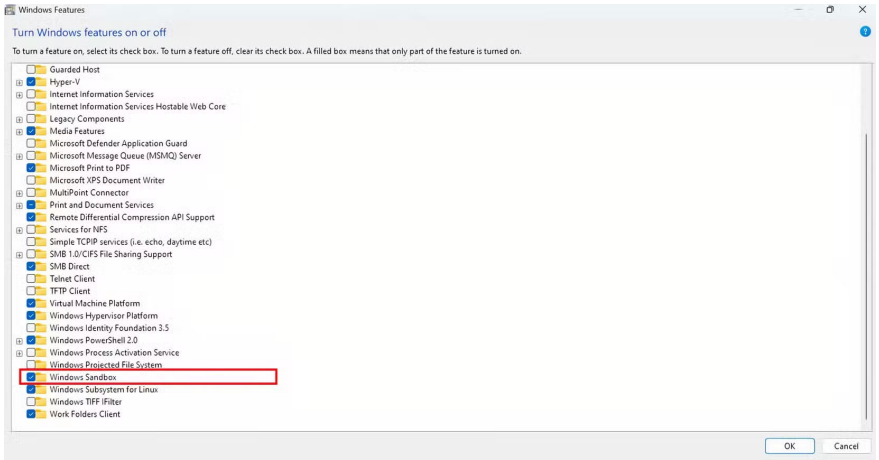
Windows Sandbox combines the security benefits of virtual machines with the efficiency of container technology. Instead of running like a traditional Hyper-V virtual machine, the sandbox behaves more like a process in your main operating system, providing better performance and resource management. The system uses intelligent memory sharing where the sandbox and the host share the same physical memory pages for executable files, through a technology called 'direct mapping'.

Before you can use Windows Sandbox, your computer needs to meet certain requirements. You need Windows 10 or 11 Pro/Enterprise/Education. You must have Hyper-V enabled and virtualization enabled in your BIOS .

Finally, you'll also need at least 4GB of RAM (8GB recommended) and at least 1GB of free disk space.

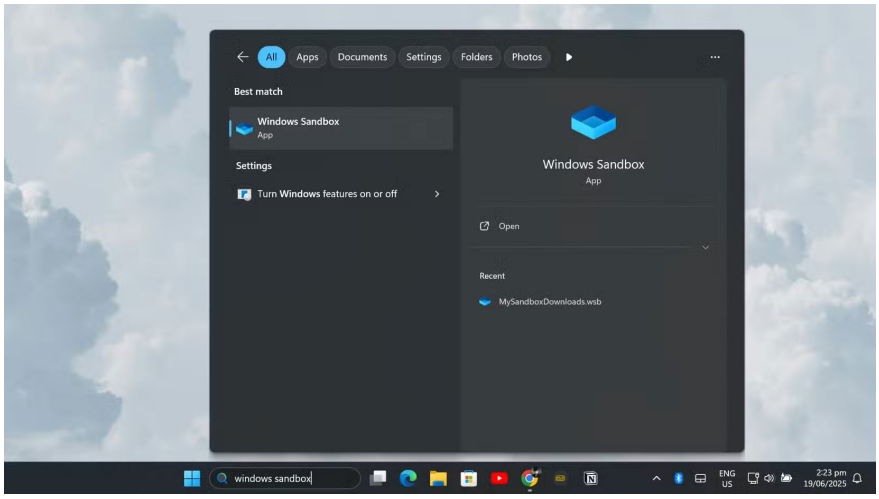
To enable Windows Sandbox, you need to enable the feature in your operating system. Open the Start menu and type "Turn Windows features on or off." Alternatively, you can navigate to the Control Panel, open **Programs and Features** , then click **Turn Windows features on or off** .

In the Windows Features dialog box , scroll down and check the box next to **Windows Sandbox** . Click **OK** and restart your computer when prompted. The installation process will download and configure the necessary components.



Using Sandbox

Once enabled, launching Windows Sandbox is simple. Just open the Start menu, type 'Windows Sandbox,' and click it. Sandbox will launch in its own window, displaying a clean Windows desktop with only basic built-in apps like File Explorer, Control Panel, Notepad, and Microsoft Edge . You can resize the window or maximize it to take up the entire screen, just like any other app.



Putting files into the sandbox is easy thanks to the built-in clipboard. You can copy files from your main computer and paste them directly into the sandbox. Alternatively, you can use the built-in Microsoft Edge browser in the sandbox to download files directly from the Internet .

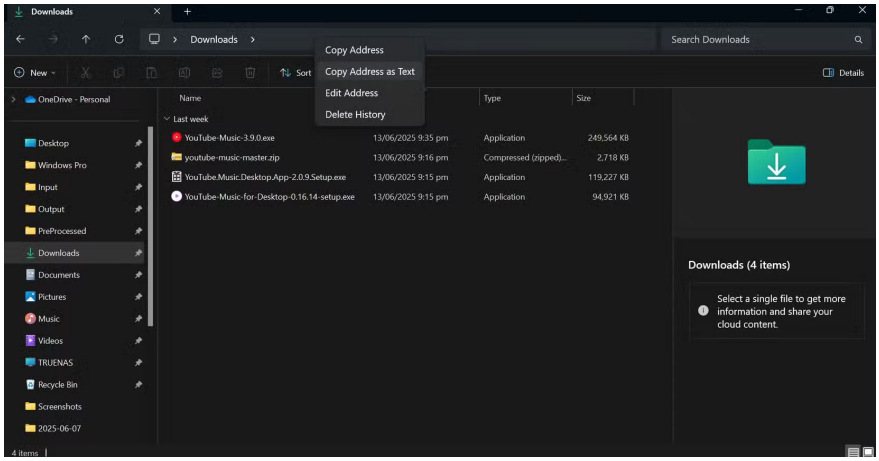
Sandbox has network access by default, so you can browse websites, download software, and access online resources.

How to set up and use Windows Sandbox

Windows Sandbox provides a new, safe space to test apps and files, but downloading the same installer or file over and over again can quickly get boring. That's why you should set up your Sandbox so that it always has access to your **Downloads** folder . That way, whenever you want to try a new program or check if a file is safe, you don't have to waste time downloading it again inside the Sandbox. Just open the file from your real Downloads folder, test it, and move on.

Setting this up is a lot easier than you might think. Here's how to do it:

First, on your regular Windows desktop (not inside Sandbox), open File Explorer and go to your **Downloads** folder . At the top of the window, you'll see an address bar showing the folder's path. Right-click that address bar and select **Copy address as text** from the menu.



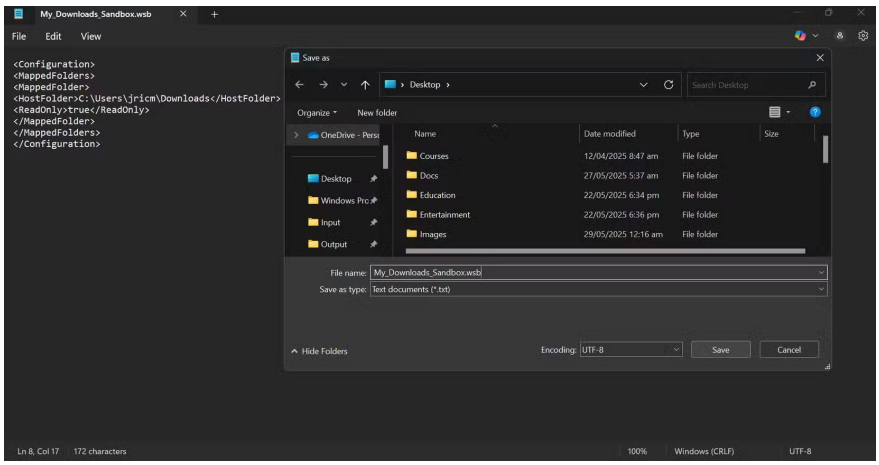
Next, open Notepad and paste the code below:

```
ENTER_FOLDER_ADDRESS_HERE/HostFolder> true
```

Change the part before **HostFolder to the Downloads** folder address copied earlier. In this example, the computer username is 'jricm', so the path will look like this:

```
C:UsersjricmDownloads
```

Then, save this text file as "My-Desktop-Sandbox.wsb" on your desktop (for easy access). Once saved, the file will have the Windows SandBox icon (.wsb).



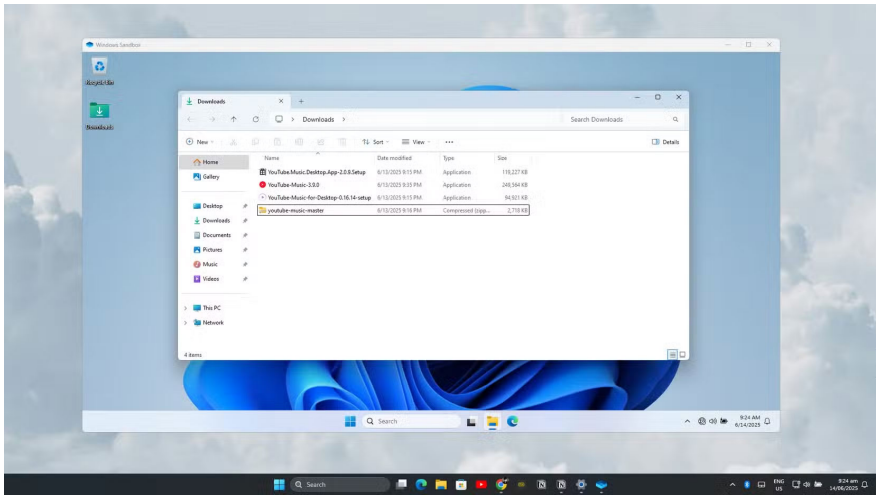
Now, whenever you want to open Windows Sandbox, just double-click this file. The Downloads folder will instantly appear on the Sandbox desktop, and you can open or inspect anything saved there. Since it's mapped as read-only, you never have to worry about accidentally changing or deleting anything in your real Downloads folder. It's all about convenience and peace of mind.

Sometimes you want to go a step further, especially if you're testing a file that might be risky. In those cases, lock down the Sandbox even more by turning off its internet connection. That way, even if something tries to call home or download more junk, it can't get online.

To do this, simply add a line to the top of your configuration file to disable networking:

```
disable C:UsersjricmDownloads true
```

And that's it! Now, when you launch Sandbox using this file, not only do you have instant, read-only access to Downloads, but Sandbox itself is completely cut off from the Internet. No downloads, no uploads, and no sneaky background connections.



This setup makes Windows Sandbox feel like a real personal testing lab. You can quickly try anything in your Downloads folder, confident that nothing will corrupt real files or leak out onto the web. And if you ever want to go back to the default, all you have to do is open the regular Sandbox app from the Start menu.

Windows Sandbox provides the perfect balance between security and usability. It provides enterprise-grade isolation in a way that is accessible to everyday users. By leveraging custom configurations and automated setup, you can create powerful, secure testing environments that protect your main PC while allowing you to safely explore the digital world.