

(<https://www.alphr.com>).



(<https://www.alphr.com>).

Gaming (<https://www.alphr.com/category/video-games/>).

PC & Mobile (<https://www.alphr.com/category/pc-mobile/>).

Social Media (<https://www.alphr.com/category/social-media/>).

Internet (<https://www.alphr.com/category/internet/>).

HOME (/) > PC & MOBILE (<https://www.alphr.com/category/pc-mobile/>) >

Entertainment (<https://www.alphr.com/category/entertainment/>) > DEVICES (<https://www.alphr.com/category/pc-mobile/pc-mobile-devices/>) >

Windows (<https://www.alphr.com/category/windows/>) > PC-MOBILE-DEVICES/WINDOWS (<https://www.alphr.com/category/windows/>)

About Us (<https://www.alphr.com/about-alphr/>).>

WINDOWS 10 (<https://www.alphr.com/category/pc-mobile/pc-mobile-devices/windows/>)

# How To Disable Windows Defender In Windows 10/11

 Lee Stanton (<https://www.alphr.com/author/arch/>). December 18, 2023



([https://twitter.com/intent/tweet?](https://twitter.com/intent/tweet?text=How)

text=How

to

Disable

Windows

Defender

in

Windows

10/11&url=[https://www.alphr.com/disable-](https://www.alphr.com/disable-windows-defender-windows-10/)

windows-

defender-

windows-

11/) (<https://www.reddit.com/submit>).

Windows Defender is a free, built-in, comprehensive antivirus tool with reliable protection. However, there are some drawbacks to using it. It is resource-intensive and will continue running in the background after being switched off unless permanently disabled. The software can also interfere with other antivirus/malware protection applications, although many have adapted to a coexistence.



Regardless, Microsoft has not made the process of disabling Windows Defender easy. If you turn it off in the **Virus & threat protection settings**, it reverts to being on after a short while or after rebooting, and it does so without warning.

If you do not need it, there are many ways to disable it permanently. Read on for three methods to deactivate Windows Defender for good.

# **Disable Windows Defender using Another Antivirus/Antimalware Application**

Most antivirus/antimalware programs automatically disable Windows Defender to effectively utilize the resources and functions that protect your system/network and prevent incompatibilities. Regardless, this method is perhaps the easiest way to disable Defender. Microsoft has adapted its Windows Security functions to accommodate third-party antivirus/antimalware applications. It allows the developers to change the security options through various codes and commands and integrate them into their installation files.

## **Disable Windows Defender Using Group Policy Settings**

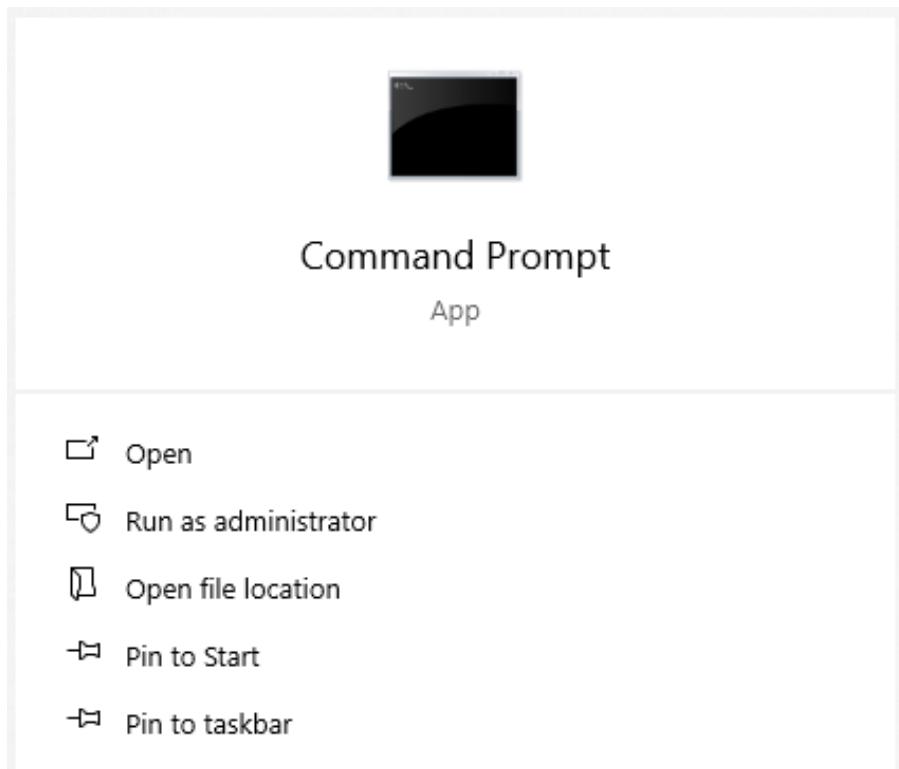
The second way to disable Windows Defender is to use the **Group Policy** security tool, but **you must first enable/install the Group Policy Editor (gpedit.msc) if on Windows 10 or 11 Home Edition and turn off Tamper Protection in the Settings menu for all Windows releases**. Follow the steps below to add gpedit or skip to the next section if enabled.

## **How to Add Group Policy Editor to Windows 10/11 Home Edition**

The Group Policy Editor needs to exist and be activated before you can disable Windows Defender using it. Microsoft thinks Home Edition users don't need the feature since they don't have a network of users or applications that they need to manage. However, the lack of the policy console may stem from Microsoft's desire to push/promote higher versions like Pro and Enterprise or prevent commercial entities from using the Home Edition. Of course, that is just an assumption, but it makes sense.

Regardless, here is how to enable/install the Group Policy Editor in Windows 10/11 Home Edition releases.

1. Type “**cmd**” in the Cortana search box. Select “**Run as Administrator.**”



2. Copy and paste the following command in Windows 11 Home Edition:

```
FOR %F IN ("%SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientTools-Package~*.mum") DO (DISM /Online /NoRestart /Add-Package:"%F")
```

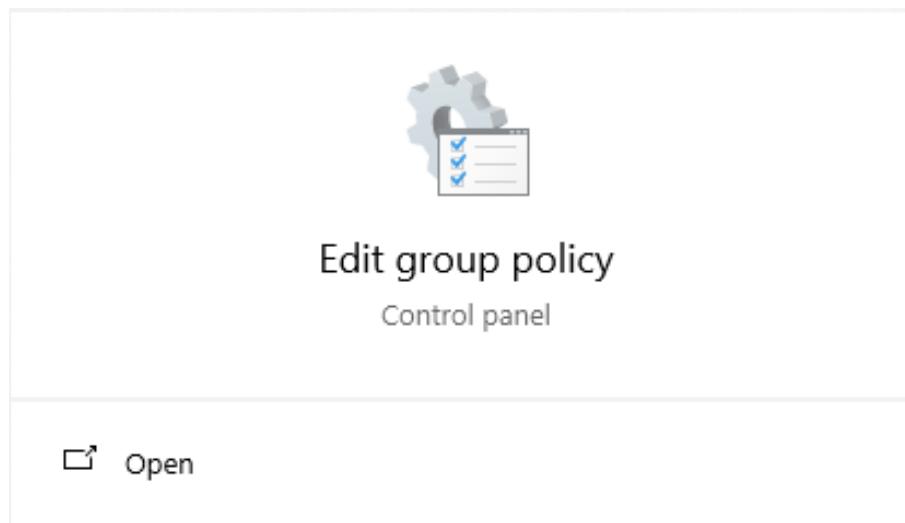
*It will take three or more minutes to complete.* If it appears stuck, it may not be. Try minimizing and maximizing the window or clicking off of the window and back on it.

- Once the first command finishes, copy/paste this command:

```
FOR %F IN ("%SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-  
ClientExtensions-Package~*.mum") DO (DISM /Online /NoRestart /Add-  
Package:"%F")
```

*It will take three or more minutes to complete.* If it appears stuck, it may not be. Try minimizing and maximizing the window or clicking off of the window and back on it.

- After the second command finishes, type “**gpedit.msc**” in the Cortana search box on Windows 10/11 Home, then select it. If it doesn’t appear, you need to use the Command Prompt. No administrator privileges are required.



If you've completed all the steps above correctly, the Group Policy Editor will launch in Windows 10/11 Home Edition, even after rebooting. If you have issues, try copying/pasting the following two commands in an admin terminal, one at a time:

```
foreach ($F in Get-ChildItem -Path  
"$env:SystemRoot\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientTools-  
Package~*.mum") {DISM /Online /NoRestart /Add-Package:"$F"}
```

```
foreach ($_ in (Get-ChildItem -Path  
"$env:SystemRoot\servicing\Packages\Microsoft-Windows-GroupPolicy-  
ClientExtensions-Package~*.mum")) {DISM /Online /NoRestart /Add-Package:"$_"}
```

The next step for any Windows 10/11 edition is to disable “Tamper Protection” to allow changes that remain after restarting/rebooting.

## **How to Disable Tamper Protection on Windows 10/11**

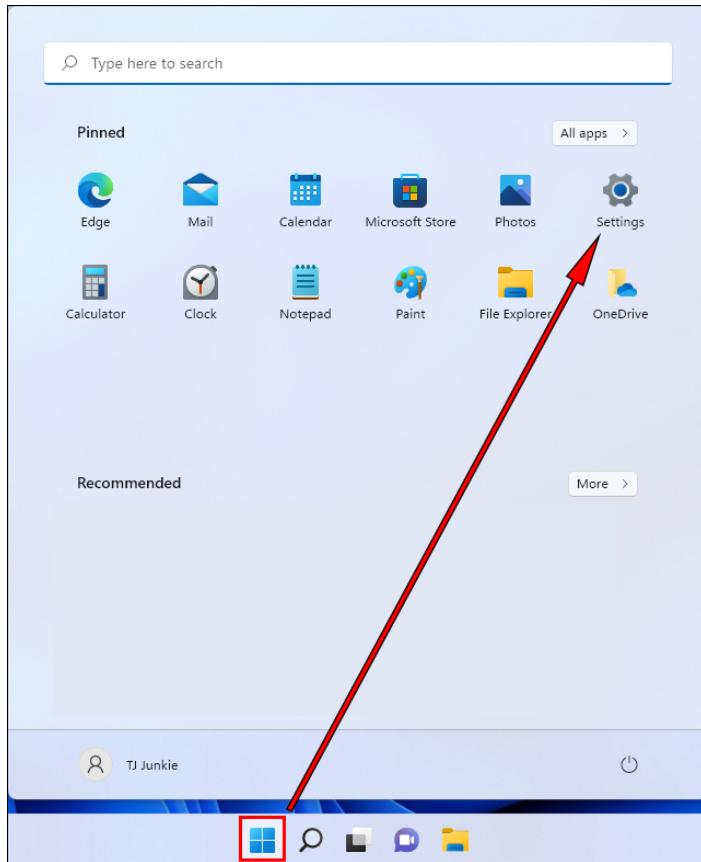
Before adjusting Group Policy settings, **you must ensure that “Tamper Protection” is disabled**, no matter what Windows version you use. Otherwise, changes won’t go through or will remain after rebooting. Here’s how to do it.

1. Open **“Windows Powershell.”**

2. Copy/paste the following command:

```
Get-MpComputerStatus
```

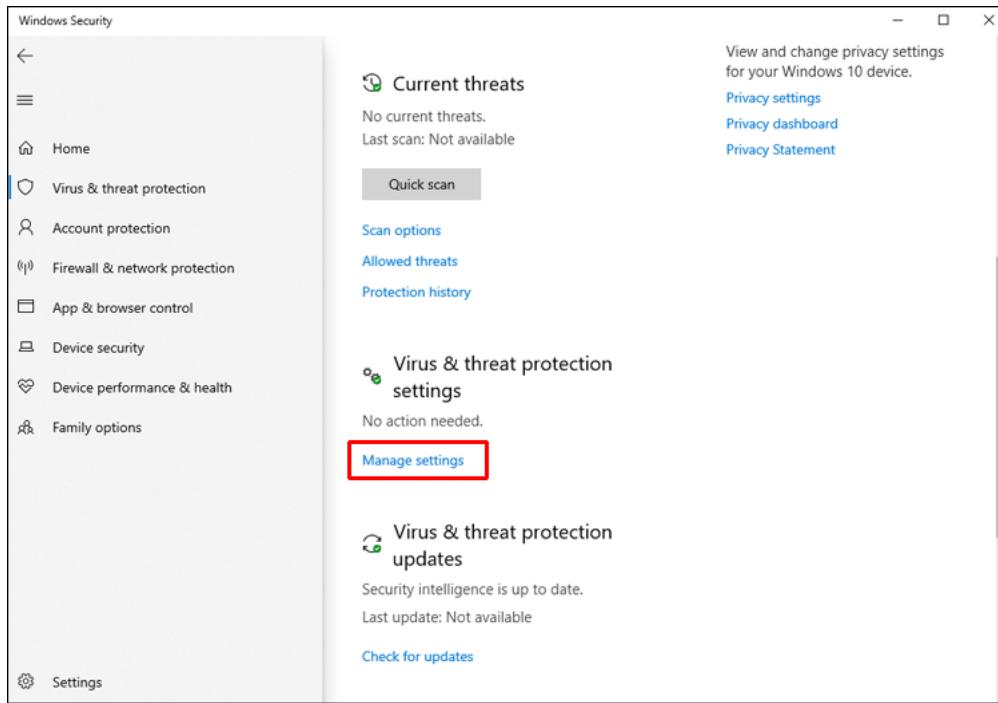
3. Confirm that “IsTamperProtected” is set to “***False.***” If not, go to “***Start -> Settings.***”



4. Choose “***Privacy & security -> Windows Security,*** then select “***Virus & threat protection.***”



5. Click on “**Manage settings.**”



6. Scroll down and toggle “**Tamper Protection**” to the off position.

7. Choose “**Yes**” to confirm the action.



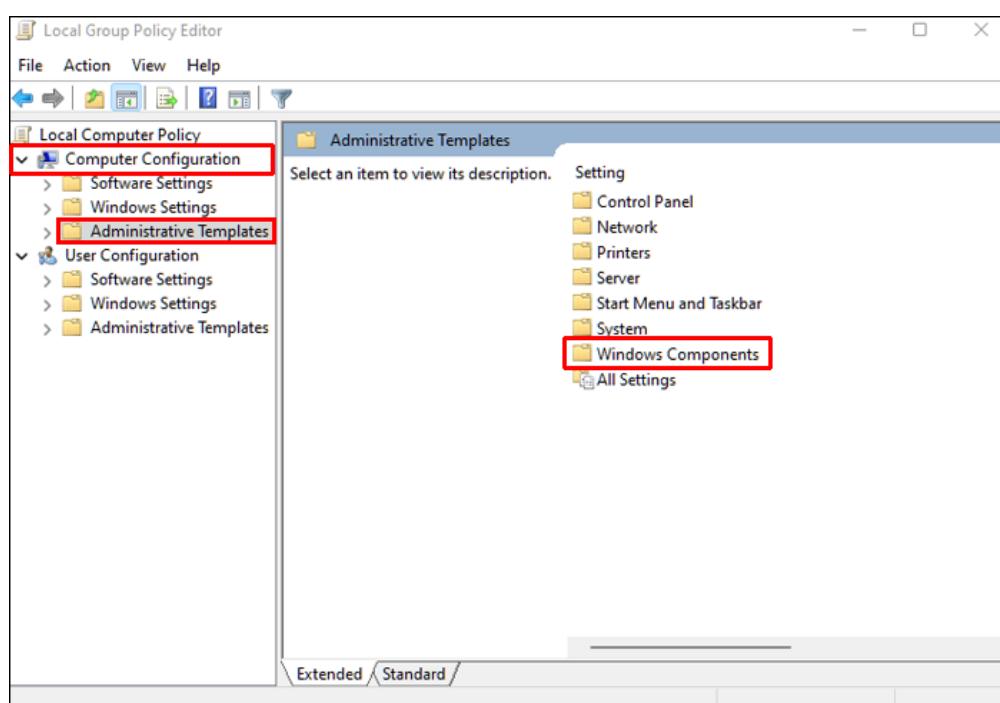
8. In the “Tamper Protection” section, a message will display stating that your device may be vulnerable. You can safely close the window.

## How to Disable Microsoft Defender Using Group Policy Settings

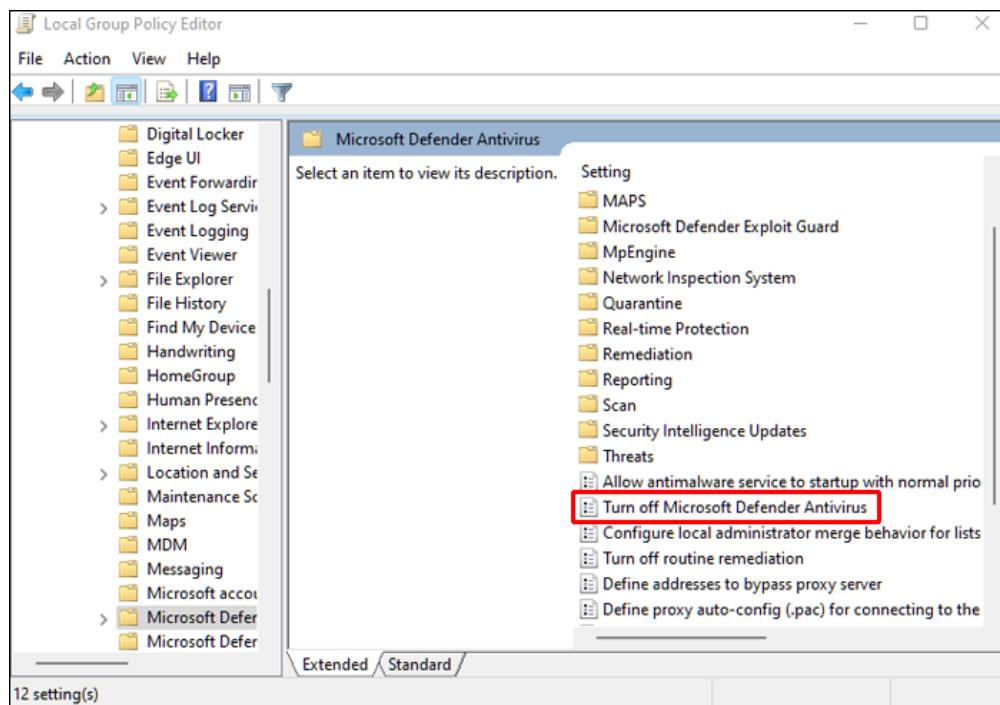
To adjust Group Policy Settings, **you must ensure that “Tamper Protection” is disabled**. See the above instructions.

Once you confirm that “Tamper Protection” is disabled, you can access the Group Policy Editor (gpedit.msc) to turn off Windows Defender. Remember that for Windows 10 or 11 Home Edition, **you must first activate the Group Policy Editor** using the process mentioned in the first section above. You **also need to ensure that “Tamper Protection” is turned off**, as mentioned above. Here’s how to disable Windows Defender using gpedit.msc.

1. From the Taskbar, click the “**search icon**” and type “**gpedit.msc**,” then click the result to run the Group Policy Editor.
2. In the app’s window on the left pane, select “**Computer Configuration -> Administrative Templates**,” then double-click on the “**Windows Components**” folder.

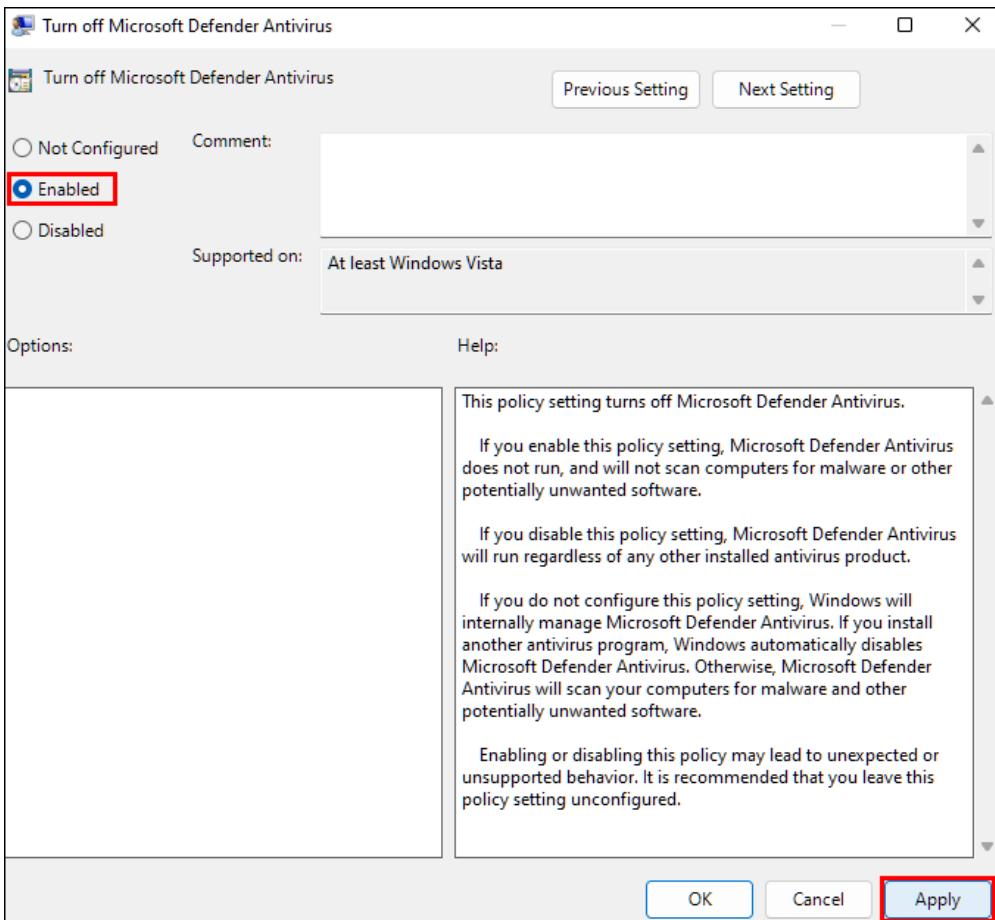


3. Scroll down and double-click on the **“Microsoft Defender Antivirus”** folder.
4. Right-click on **“Turn off Microsoft Defender Antivirus.”**

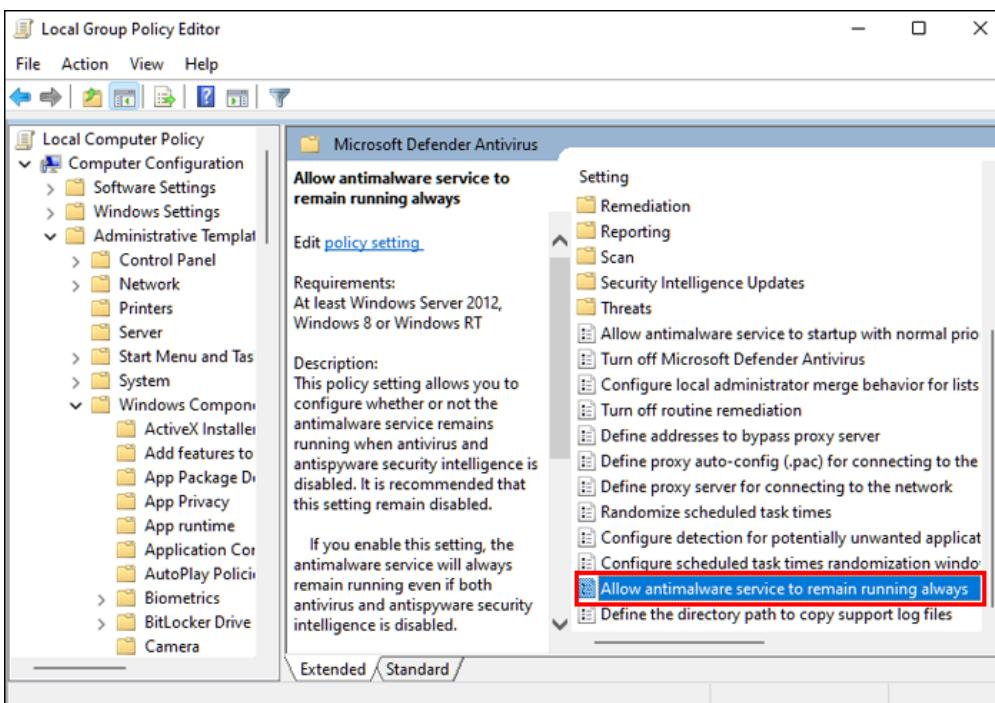


5. Choose **“Edit.”**

6. Check the “**Enabled**” box in the popup window, then choose “**Apply**,” followed by “**OK.**”

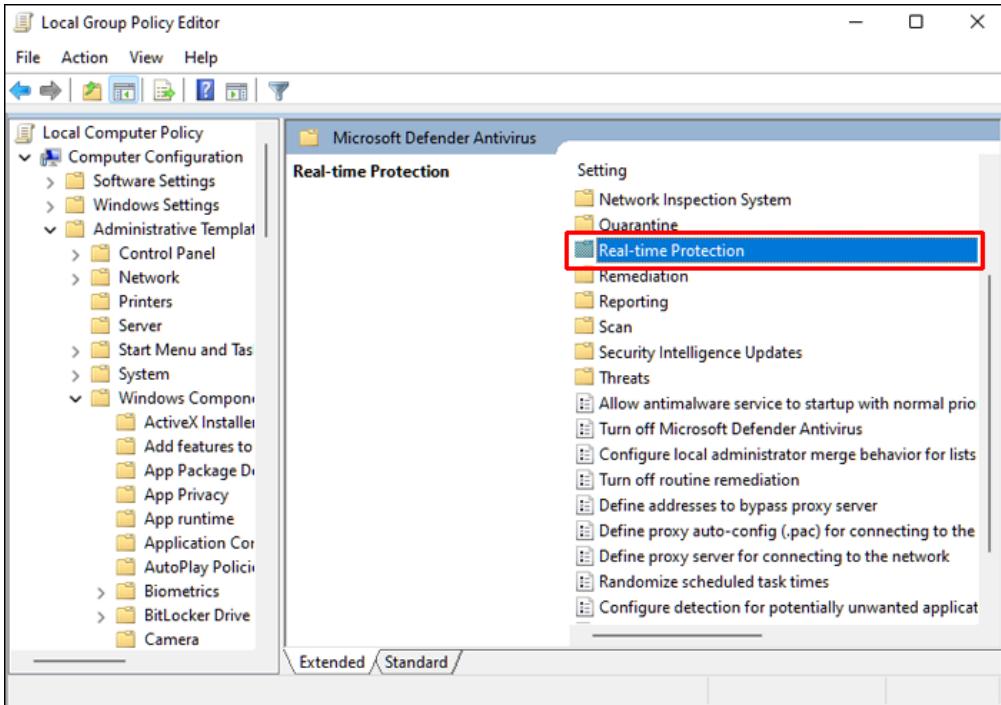


7. Scroll down and right-click on "**Allow antimalware service to remain running always**," then choose "**Edit**."



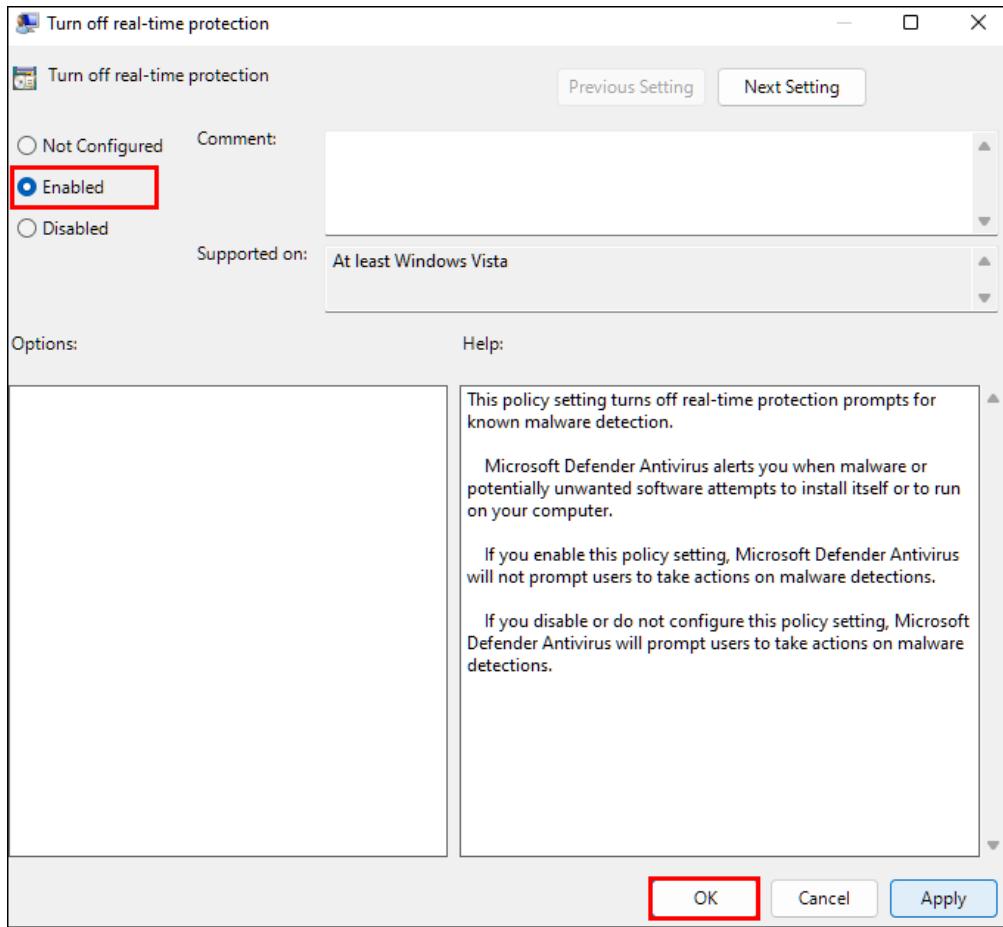
8. This time, check the “**Disabled**” option, then click “**Apply**,” followed by “**OK**.”

9. Scroll up and double-click on the folder named ***“Real-time Protection.”***



10. Right-click on "**Turn off real-time protection**," then choose "**Edit**."

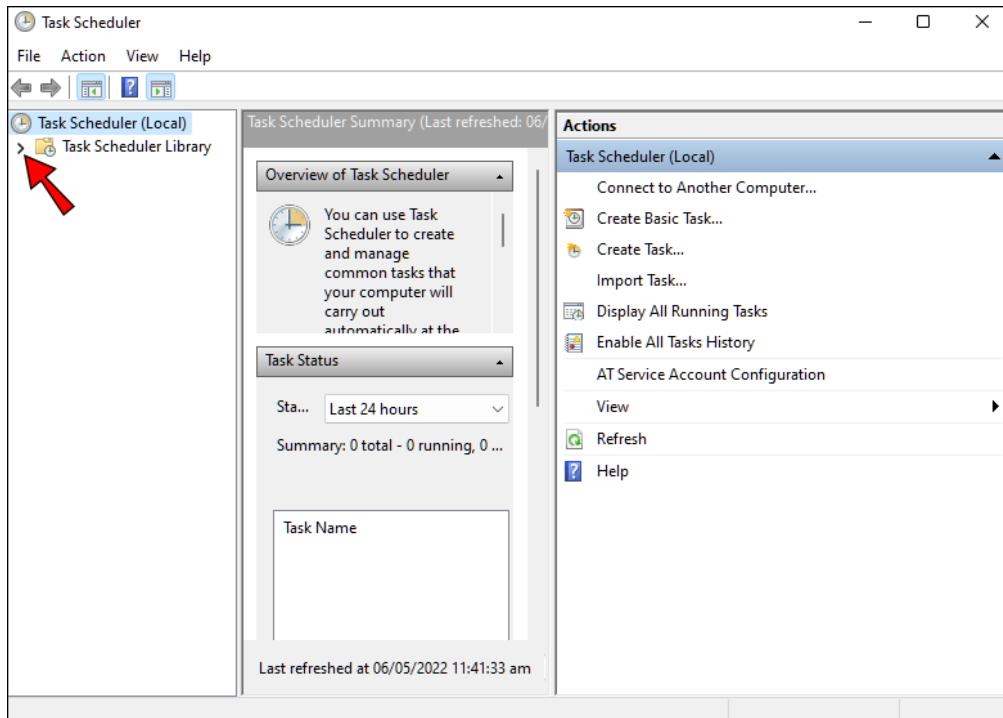
11. Check the "**Enabled**" box, then click "**Apply**" followed by "**OK**." Close the window.



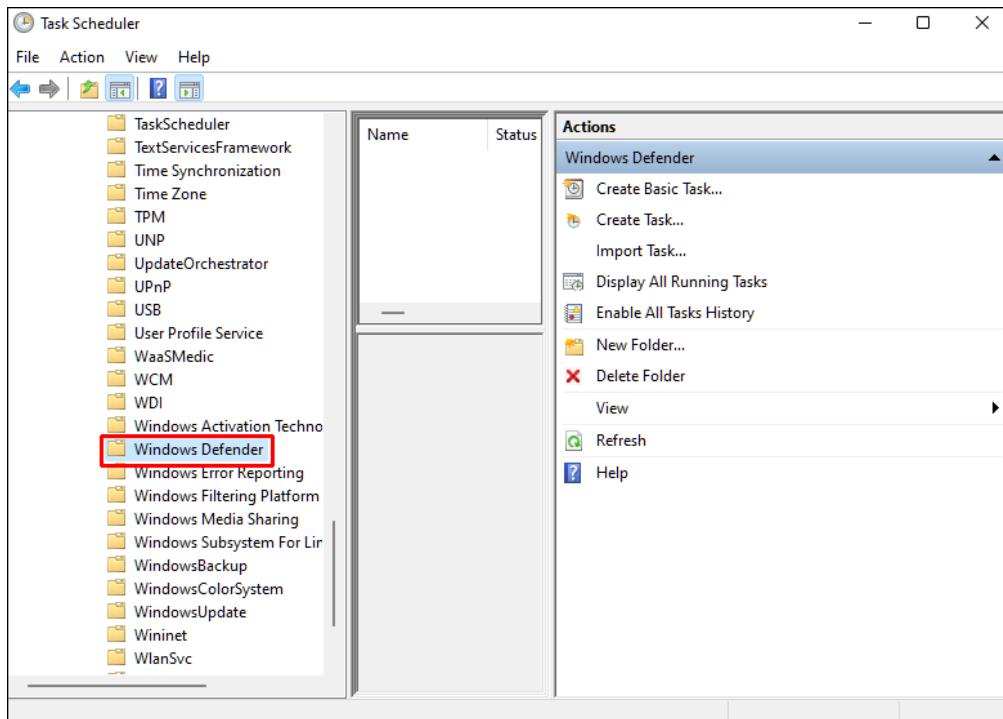
Now, you have configured the group policy. Next, you'll need to set up a **Task Scheduler** entry to stop certain services from running and avoid errors now that Windows Defender has been disabled.

1. Search for “**Task scheduler**” in the Cortana search box, then open it.

2. Expand the “**Task Scheduler Library**” folder in the left pane.



3. Navigate to "**“Microsoft -> Windows -> Windows Defender”** in the left pane.



4. Right-click and choose “**Disable**” on the following four tasks:

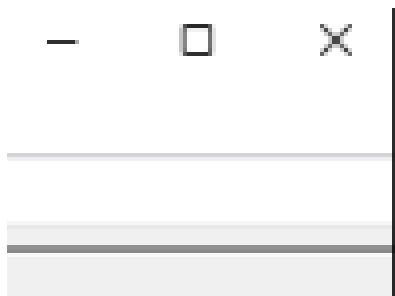
Windows Defender Cache Maintenance

Windows Defender Cleanup

Windows Defender Scheduled Scan

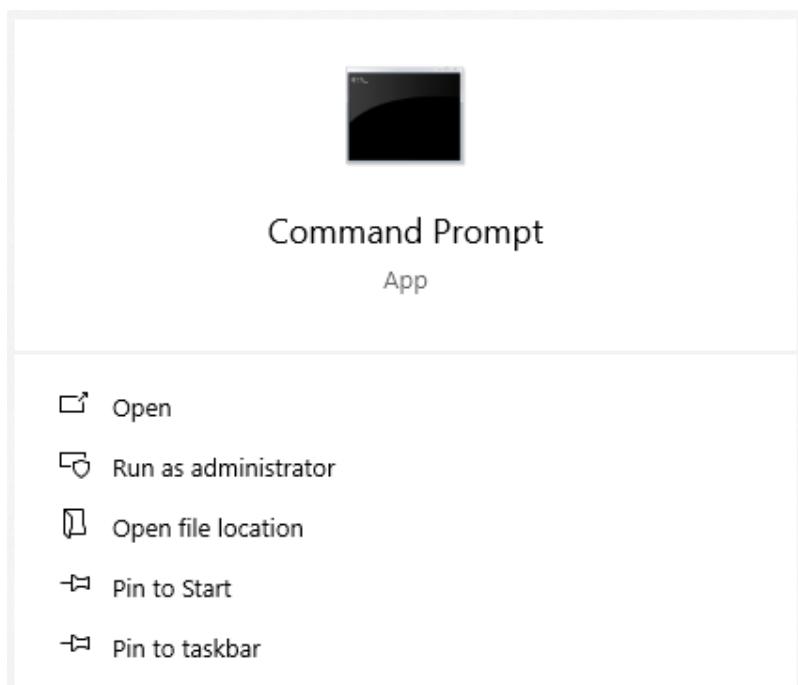
Windows Defender Verification

5. Close Task Scheduler.



Now, you need to update the computer to the adjusted group policy settings and user policies:

1. Type “**cmd**” in the Cortana search box, then choose “**Run as administrator**” in the “Command Prompt” app options.



2. Run the following command:

```
gpupdate/force
```

Windows Defender should now be disabled and will not start up with Windows.

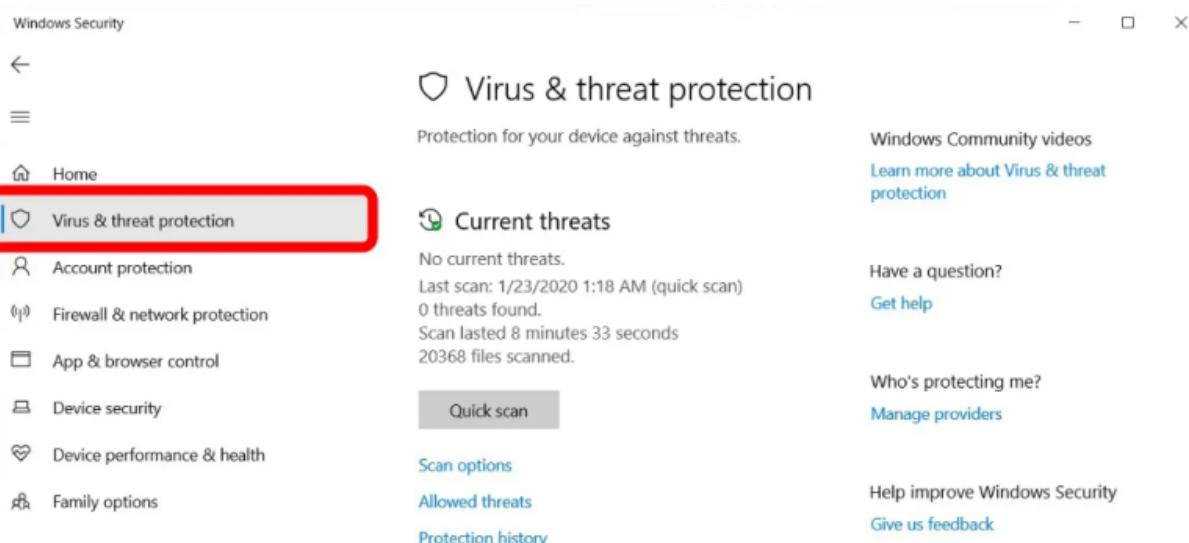
## Disable Windows Defender by Modifying the Registry

Modifying the registry is another way to “potentially” deactivate Windows Defender protection. Like the Group Policy option, **this method requires the “Tamper Protection” setting to be disabled and all Defender options to be turned off.**

Doing so stops the Defender settings from being automatically adjusted/reactivated.

Follow these steps to do that:

1. Navigate to “**Settings -> Update & Security -> Open Windows Security**,” select “**Virus & threat protection**,” then click “**Manage Settings**” or simply click the “**Windows Security**” icon in the taskbar.



2. Disable all Defender Options: Turn off “**Real-time protection**,” “**Cloud-delivered protection**,” and “**Automatic sample submission**.”

#### • Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

##### Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.



##### Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

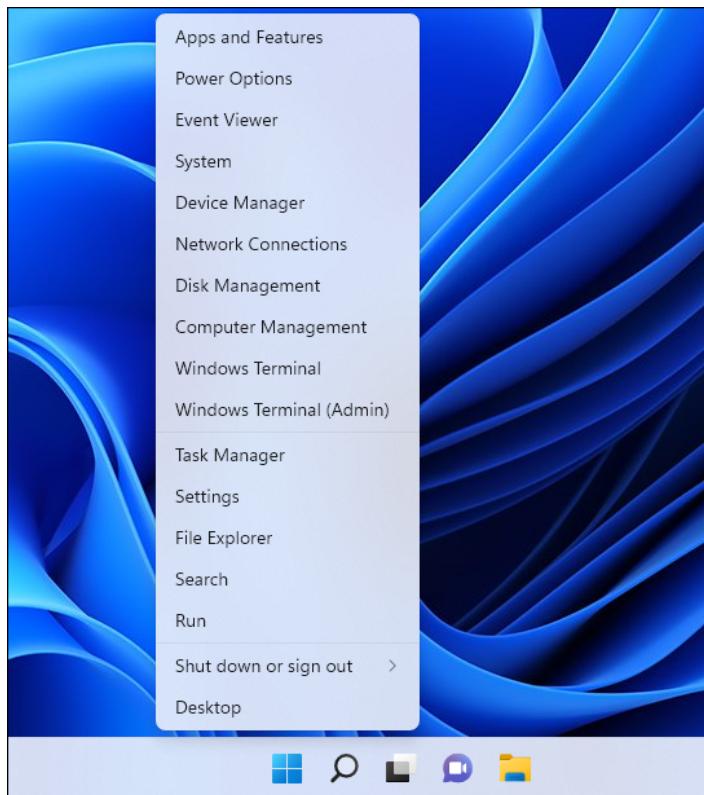
⚠ Cloud-delivered protection is off. Your device may be **vulnerable**. [Dismiss](#)



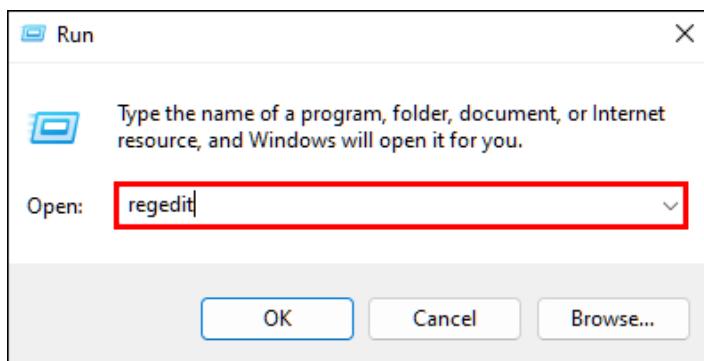
[Privacy statement](#)

3. If not done already, disable “**Tamper Protection**” (see section above). This step is crucial.

4. Right-click on the “**Start Menu**” and select “**Run.**”



5. Type “**regedit**” in the text field, then press “**Enter.**”

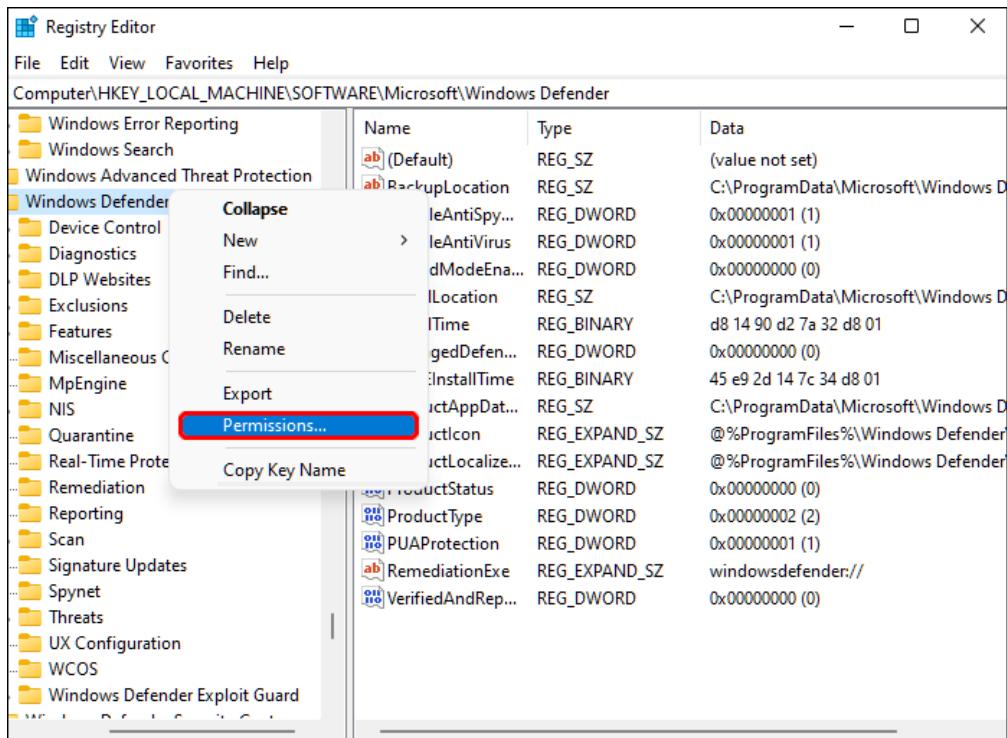


6. In the Registry Editor, insert the following path in the “**address field**” and press “**Enter.**”

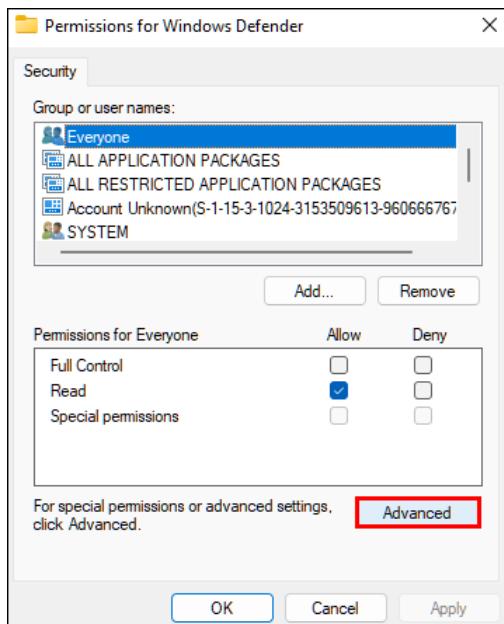
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Defender

To edit or add a value to this folder, change the owner first. By default, the owner is **System**. Follow these steps to change the folder owner:

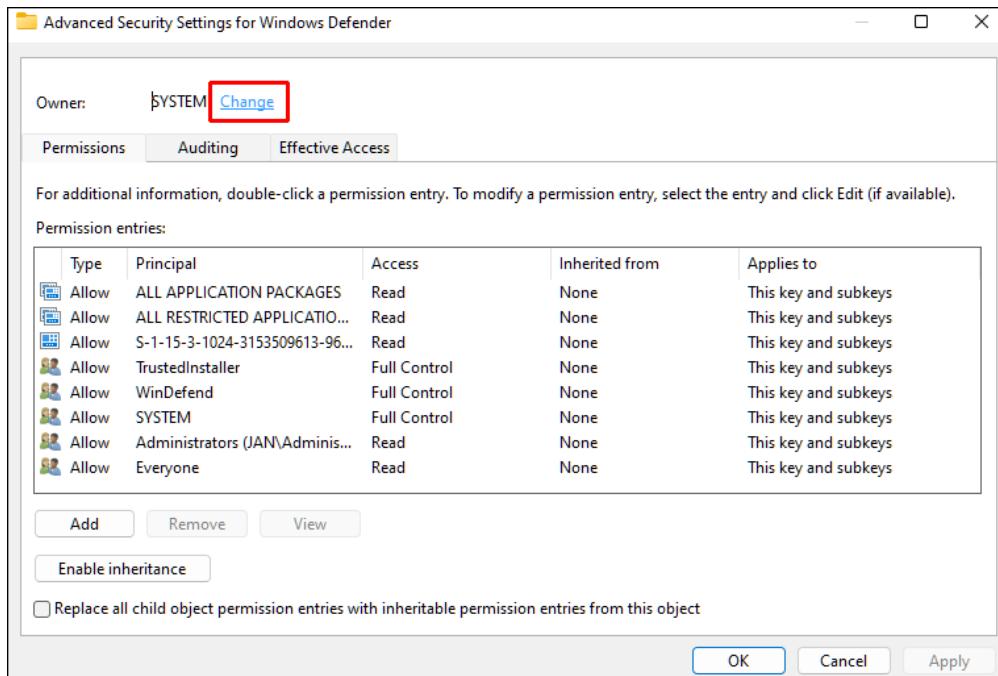
1. Right-click on the “**Windows Defender**” folder, then choose “**Permissions.**”



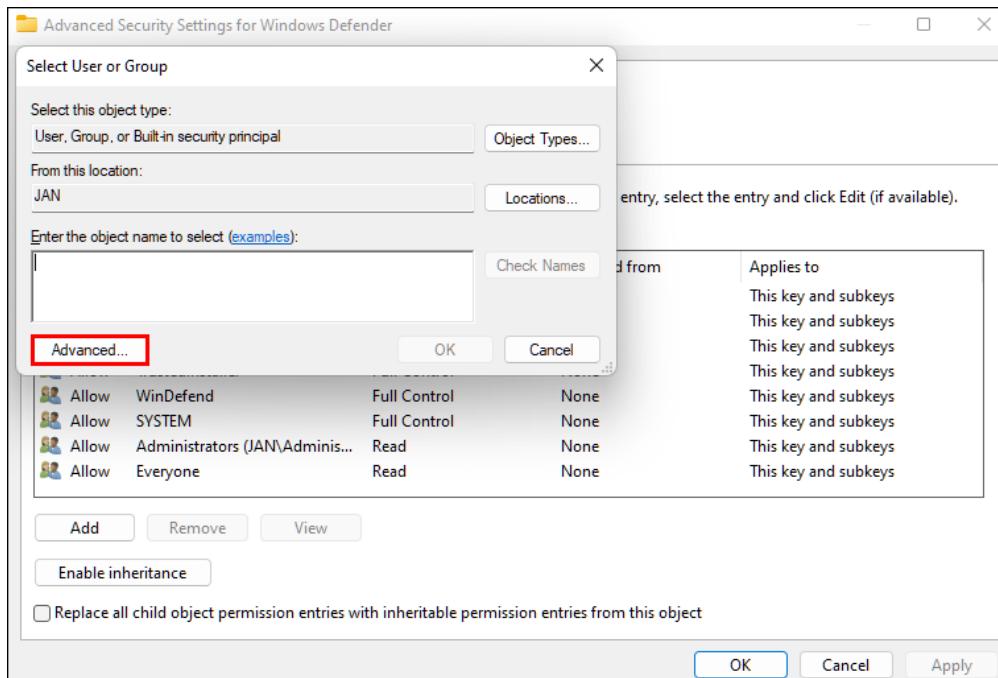
2. Click on “Advanced.”



3. Click on “**Change**” in the “Owner:” field.

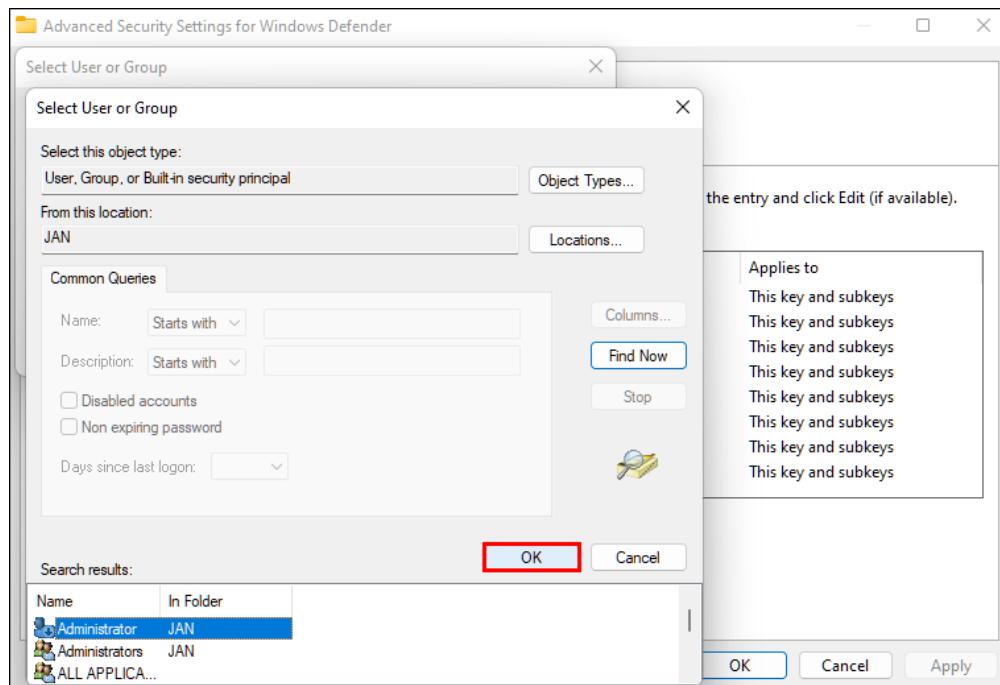


4. Choose “**Advanced**” in the “Select User or Group” window.

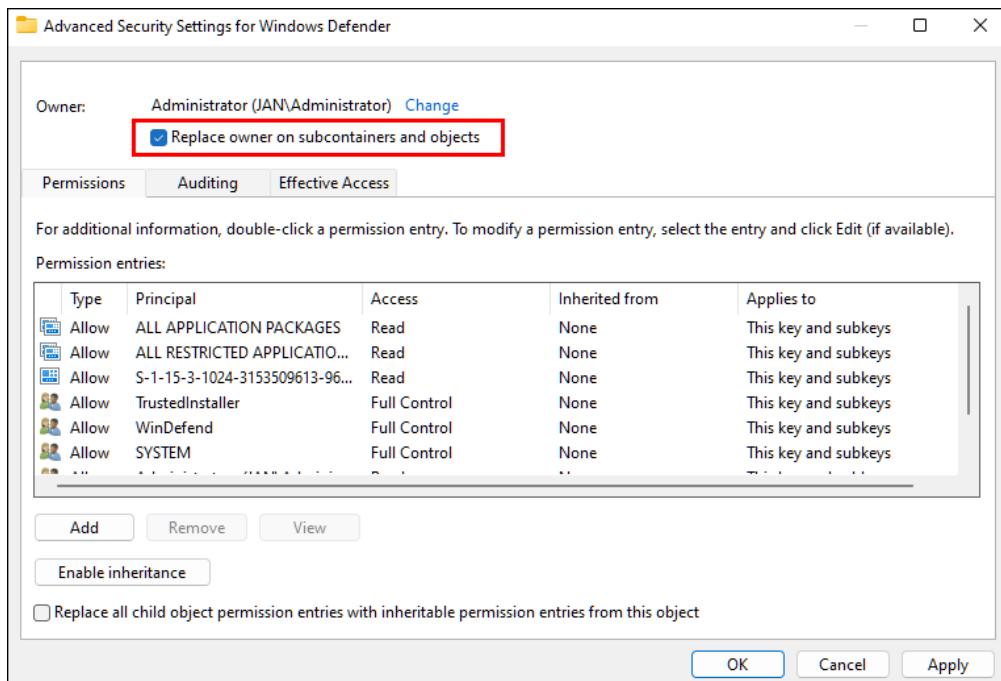


5. Click “***Find Now.***”

6. Select the “***Administrators***” group. Click “***OK***,” then “***OK***” again to confirm the changes.



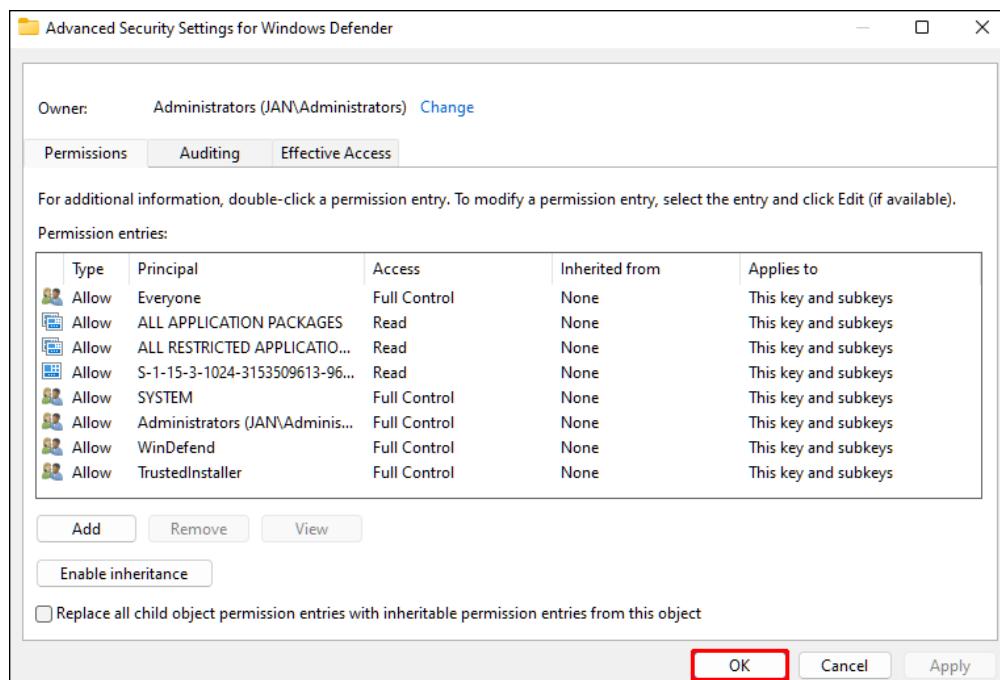
7. Check off the “***Replace owner on subcontainers and objects***” box.



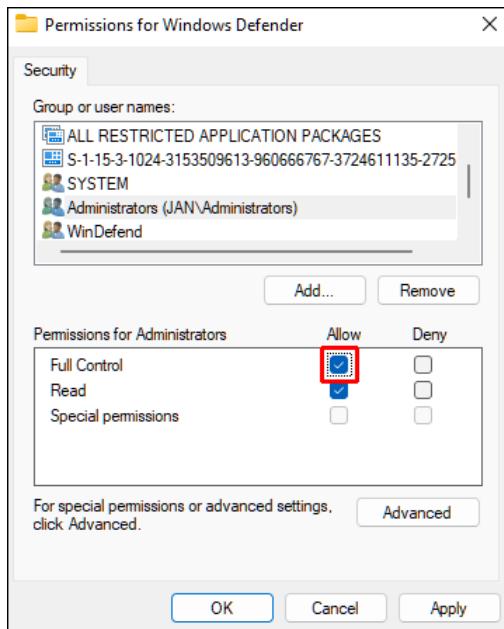
8. Next, check off the “***Replace all child object permission entries with inheritable permission entries from this object***” box.

9. Click “**Apply**,” then select “**Yes**” in the “Windows Security” warning popup.

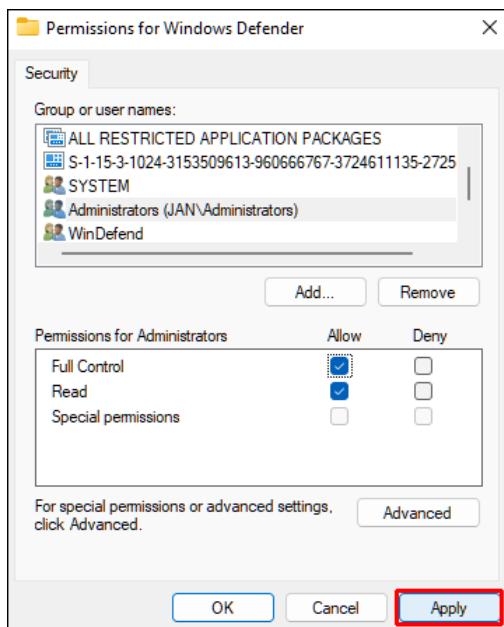
10. Click “**OK**” again to close the advanced security settings window.



11. In the “Permissions for Windows Defender” window, go to the “Permissions for Administrators” section and select the “**Allow**” box next to the “Full Control” option.

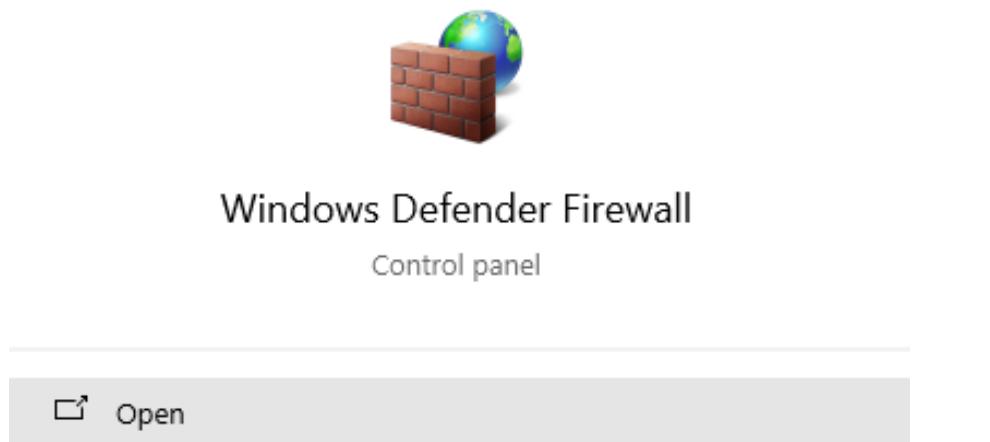


12. Click “**Apply**” then “**OK**” to confirm the change.

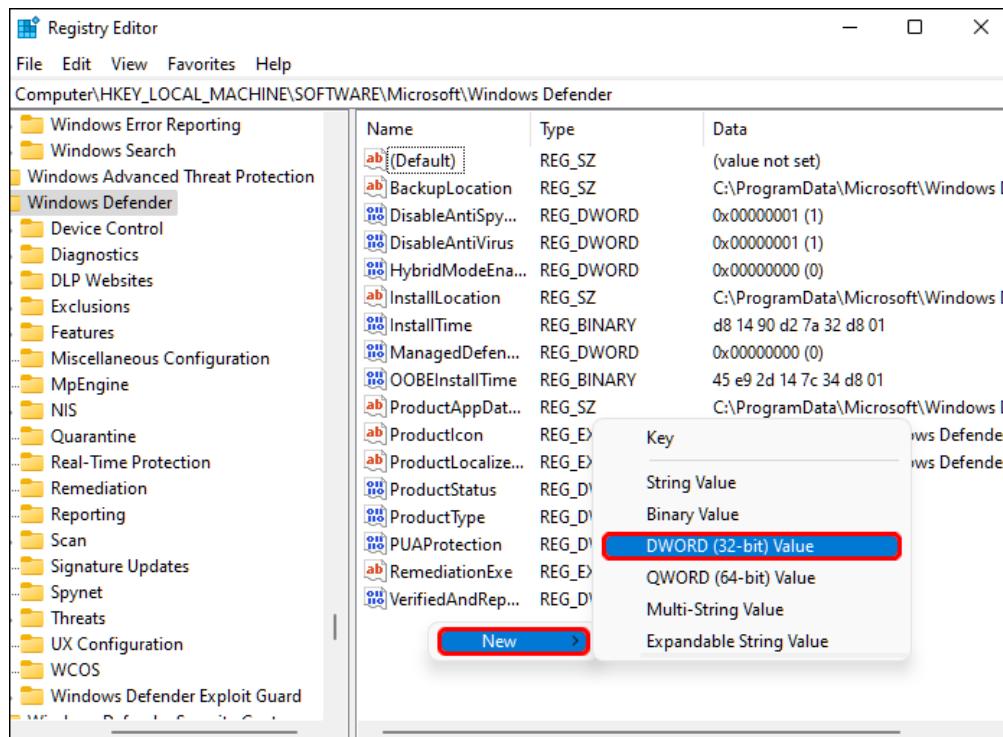


Finally, to edit the registry:

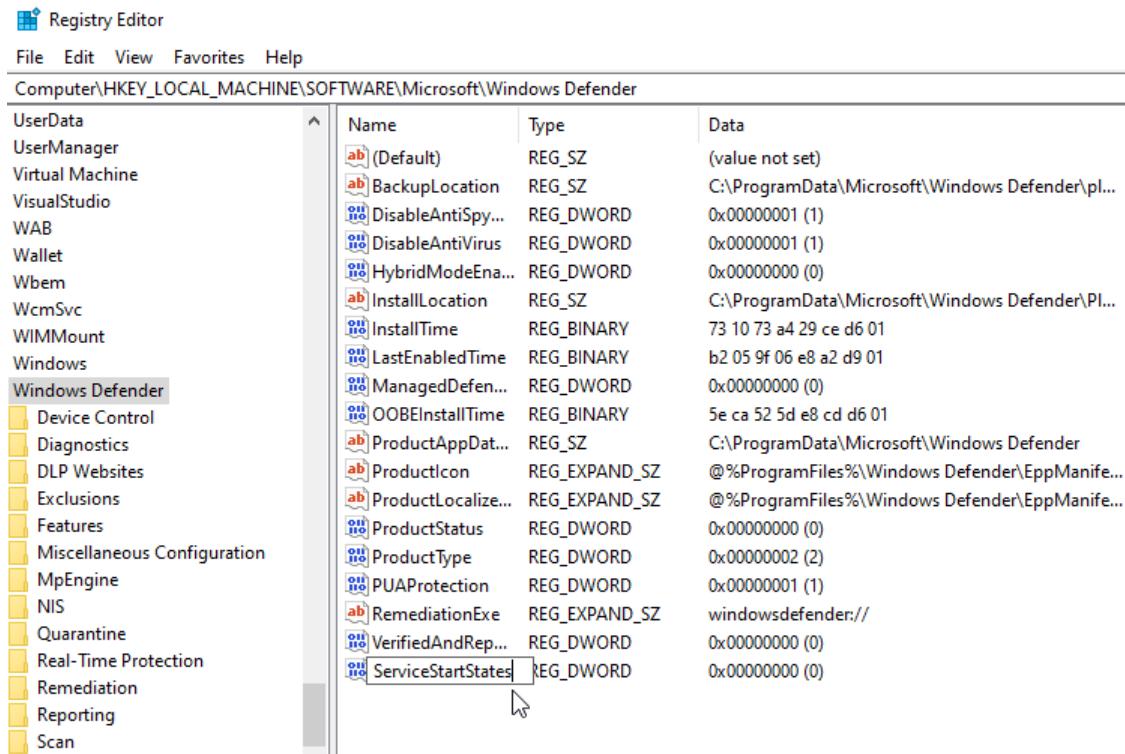
1. Return to the “**Windows Defender**” branch/folder in the Registry Editor ( HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Defender ).



2. Right-click any white space within the right pane, select “**New**,” and choose “**DWORD (32-bit) Value**.”



3. Create a total of three “**DWORD (32-bit)**” values using “Step 2” above.



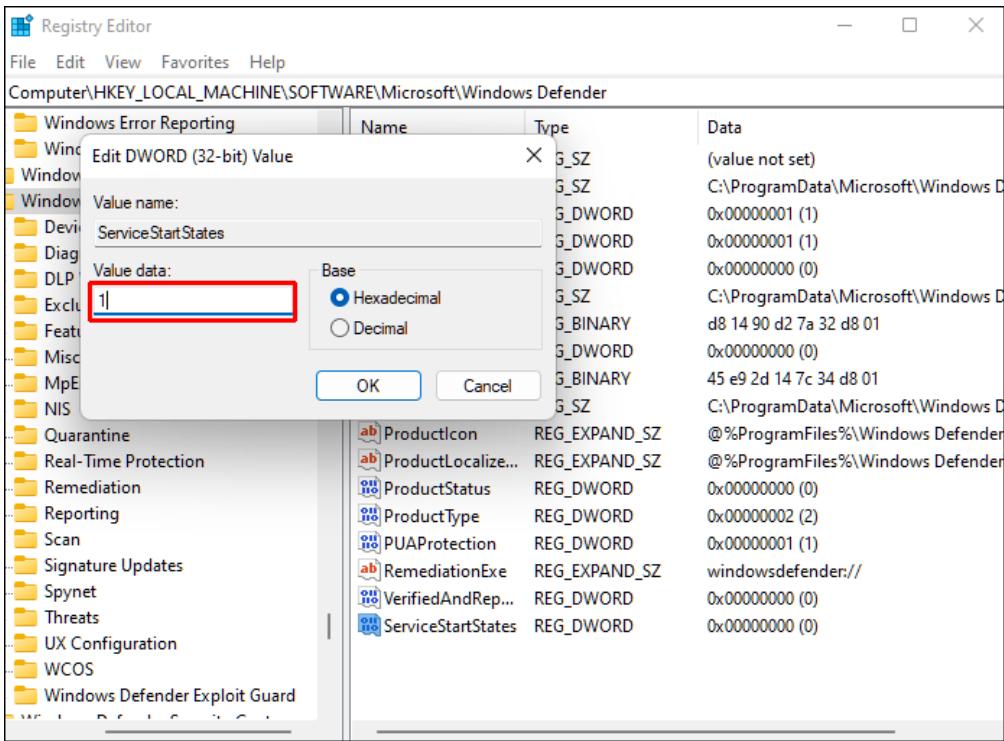
Name/ rename the three values to the following:

DisableAntiVirus

DisableAntiSpyware

ServiceStartStates

4. Right-click each new value from above, select “**Modify,**” then change the “Value data” field to “**1,**” then click “**OK.**” Close and reboot.



Once your computer restarts, Windows Defender should be disabled.

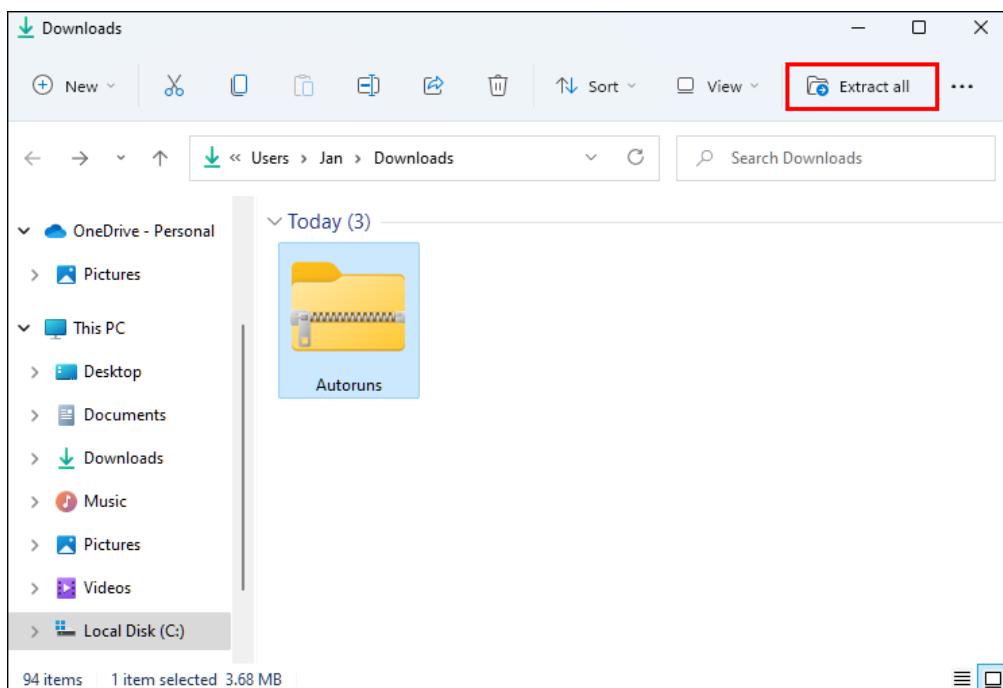
## Disable Windows Defender Using Autoruns

You can permanently disable Windows Defender using the **Autoruns for Windows** utility tool. Here's how:

1. Download the latest version of [Autoruns](https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns) (<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>) for Windows.

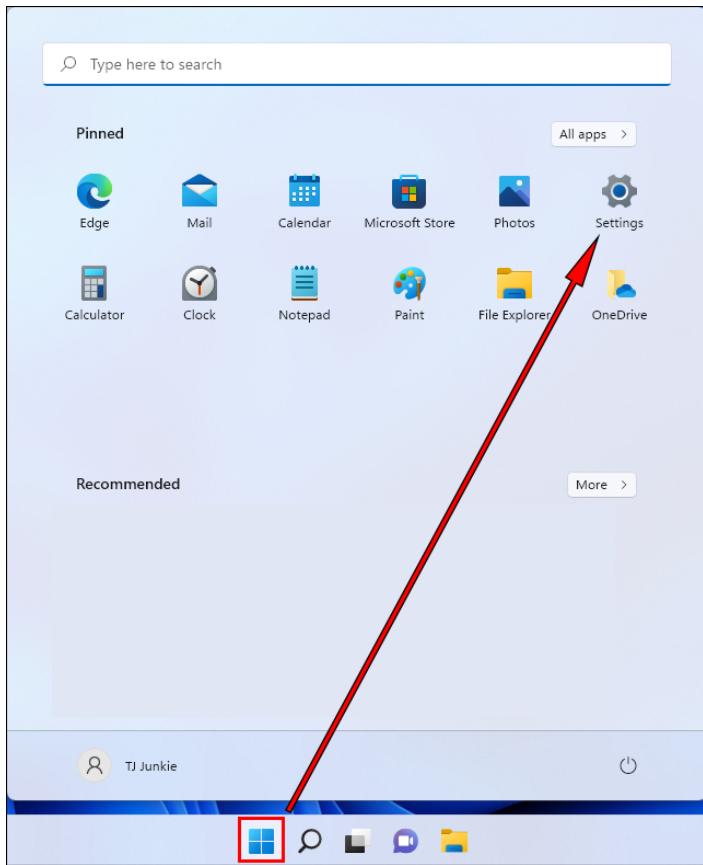
The screenshot shows a Microsoft Docs page for 'Autoruns for Windows v14.09'. The left sidebar lists various Sysinternals tools, with 'AutoRuns' selected. The main content area displays the title 'Autoruns for Windows v14.09', published on February 16, 2022. A download link 'Download Autoruns and Autorunsc (3.7 MB)' is highlighted with a red box.

2. Open the downloaded file and right-click on the **Autoruns** folder to **Extract All**. Consider extracting the folder to your desktop for easy access.

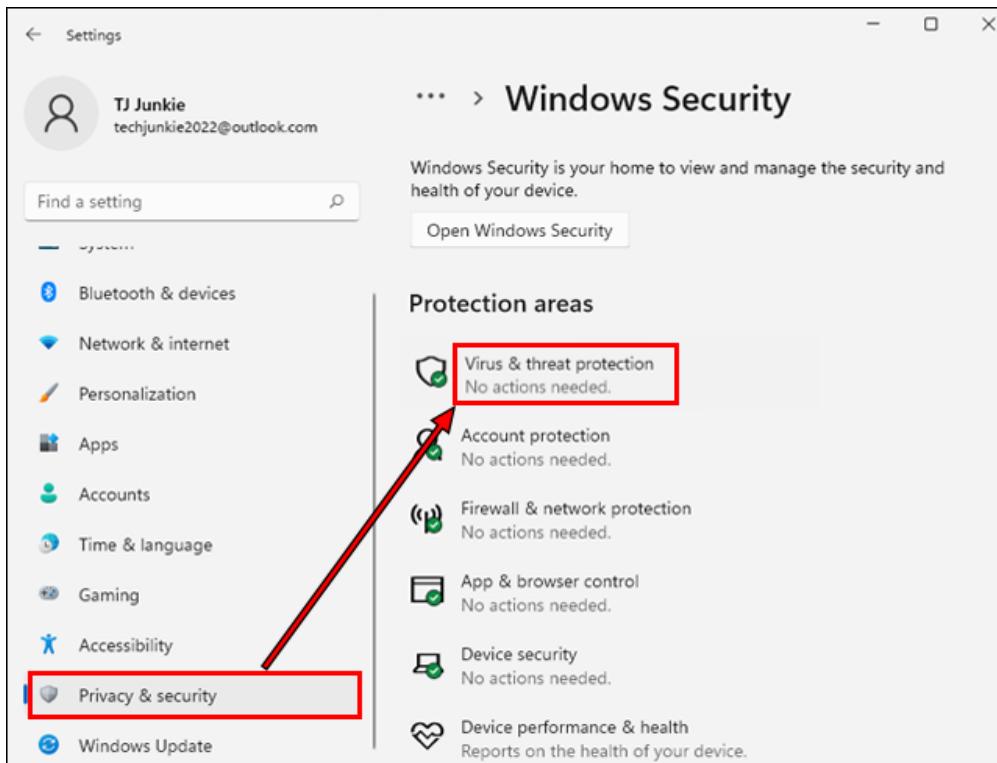


Now you'll need to disable permanent protection and boot in safe mode:

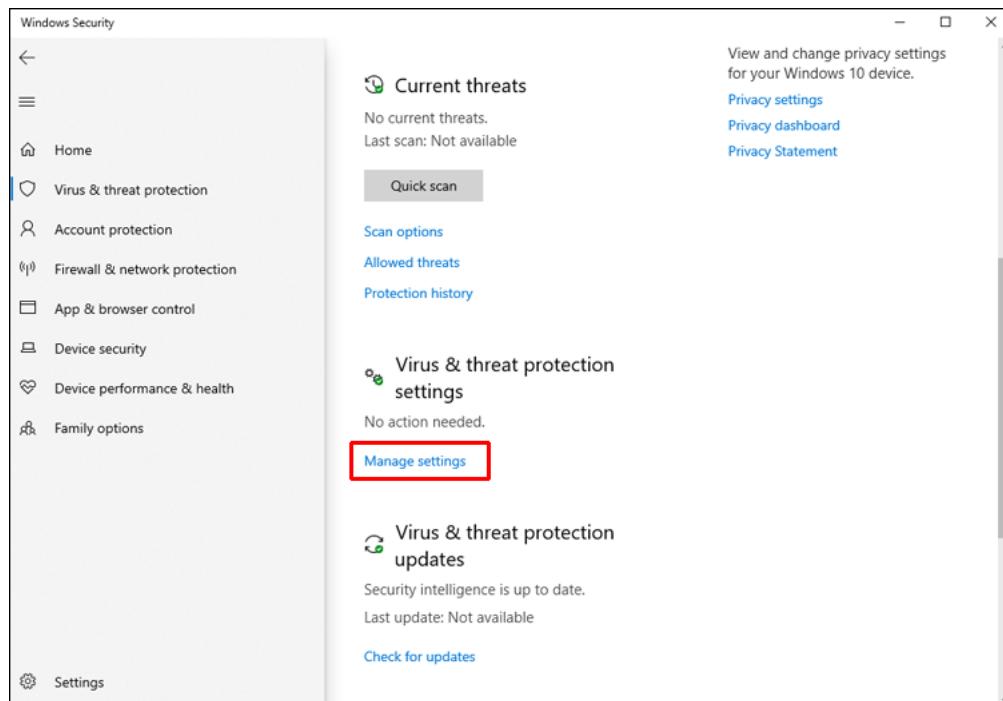
1. Press the **Windows icon** from the taskbar, then choose **Settings**.



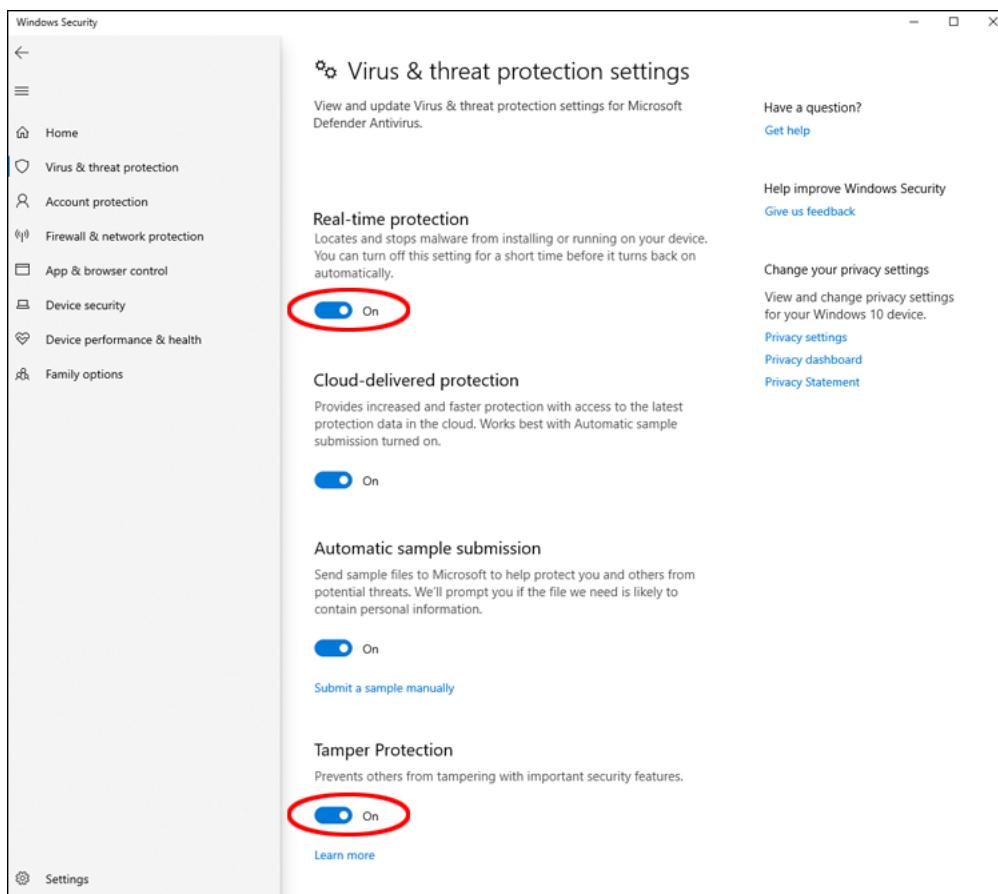
2. Choose **Privacy & security, Windows Security**, then **Virus & threat protection**.



3. Under the **Virus & threat protection** section, select **Manage settings**.



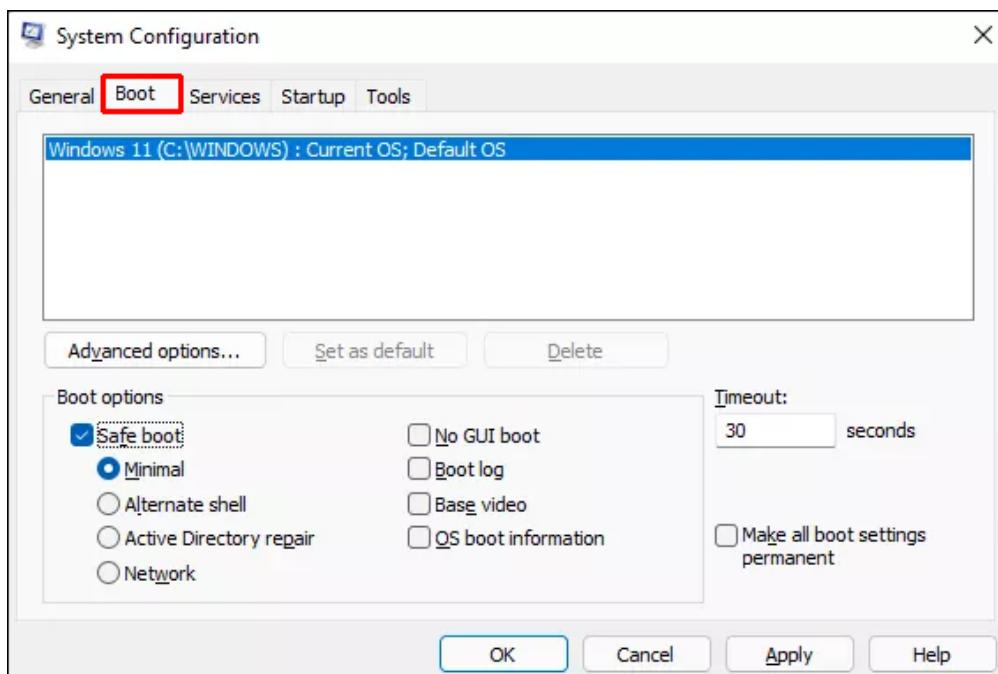
4. Press the **Real-time Protection** and **Tamper Protection** sliders to deactivate them.



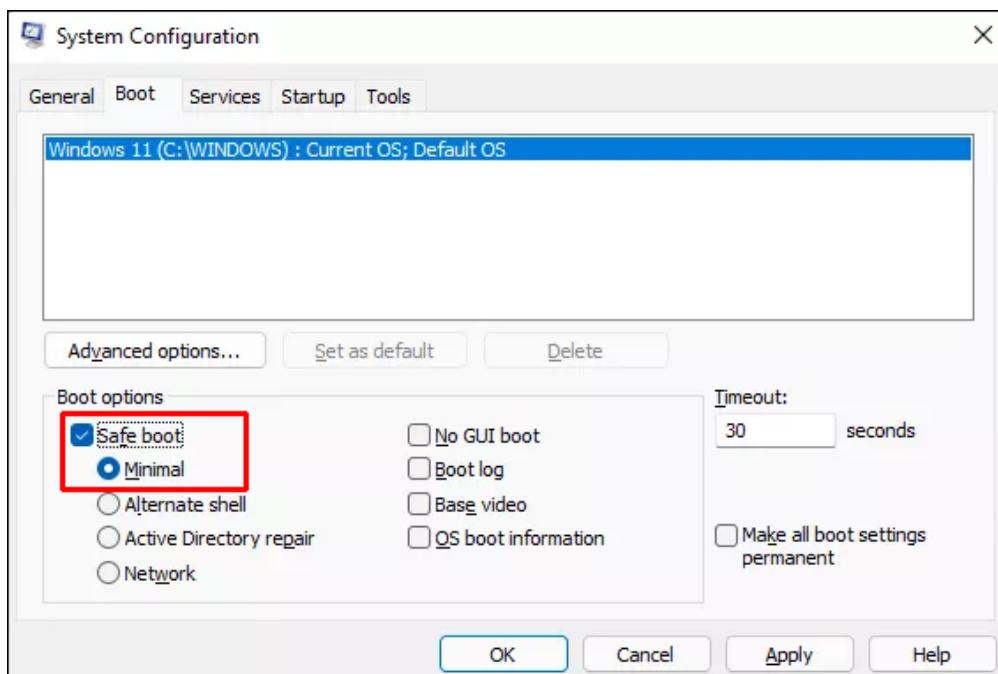
5. Next, to put your computer in **Safe Mode**, enter a search to find the **System Configuration** app, then open it.



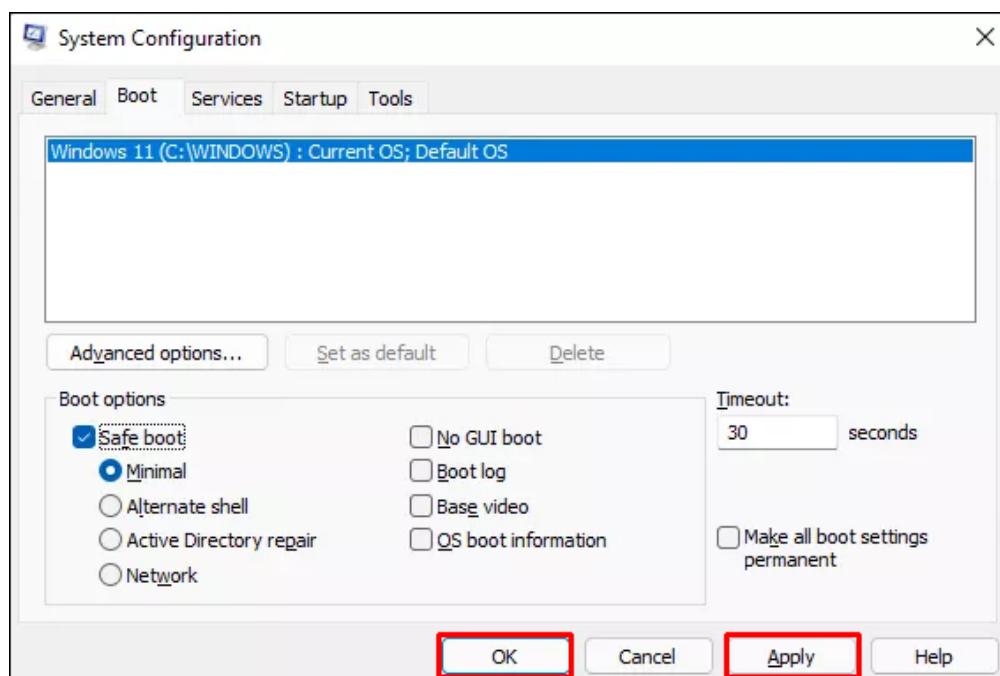
6. In **System Configuration**, select the **Boot** tab.



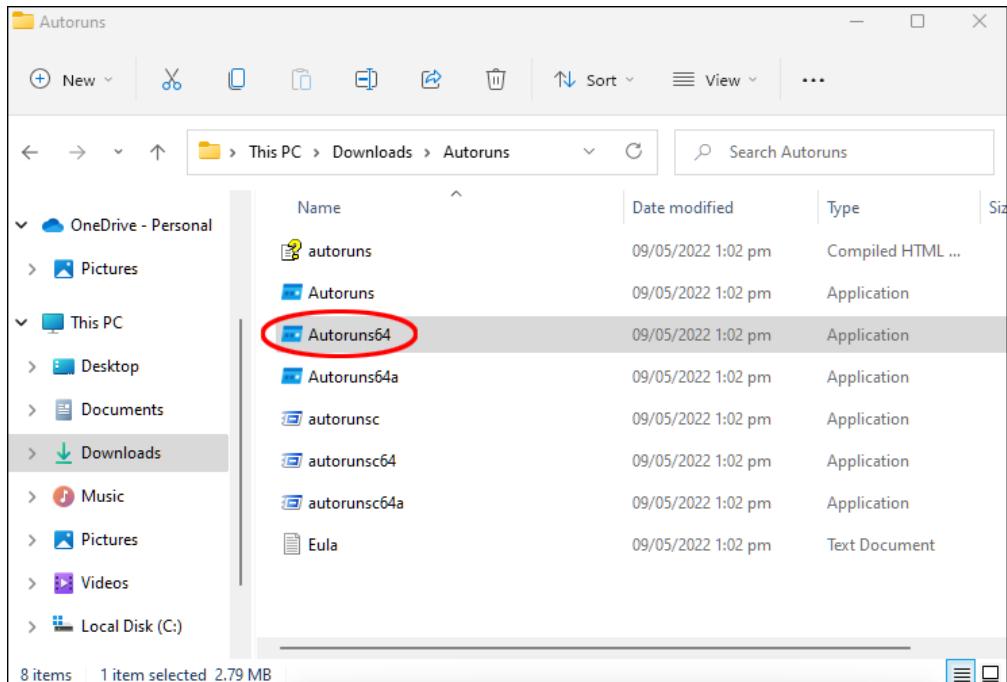
7. Under **Boot options**, check the **Safe boot** box, and the **Minimal** option will set automatically.



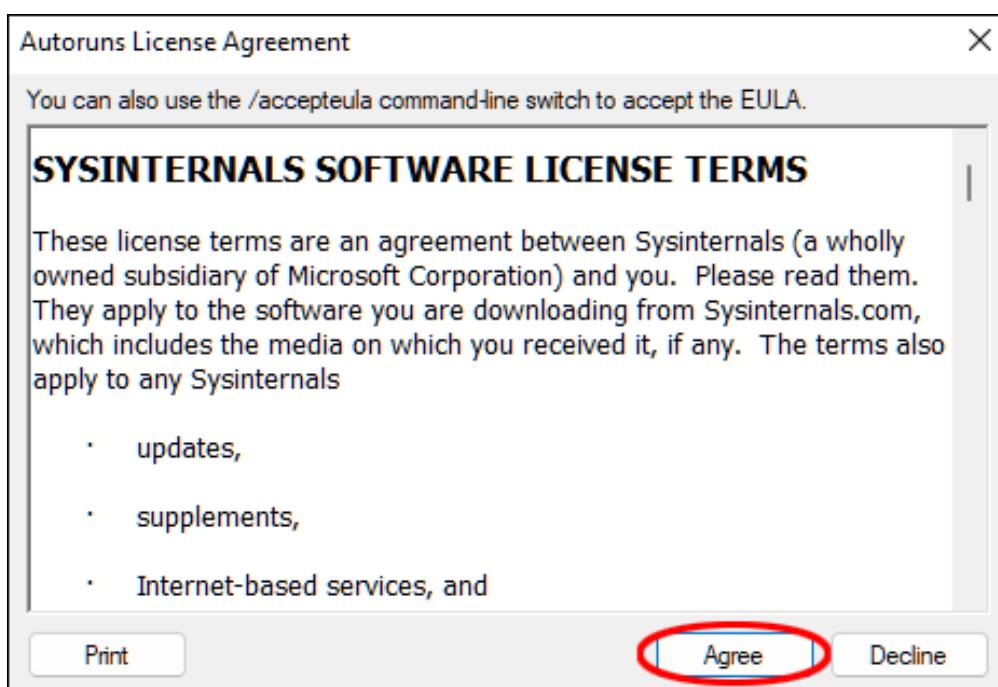
8. Hit **Apply**, **OK**, then **Restart**.



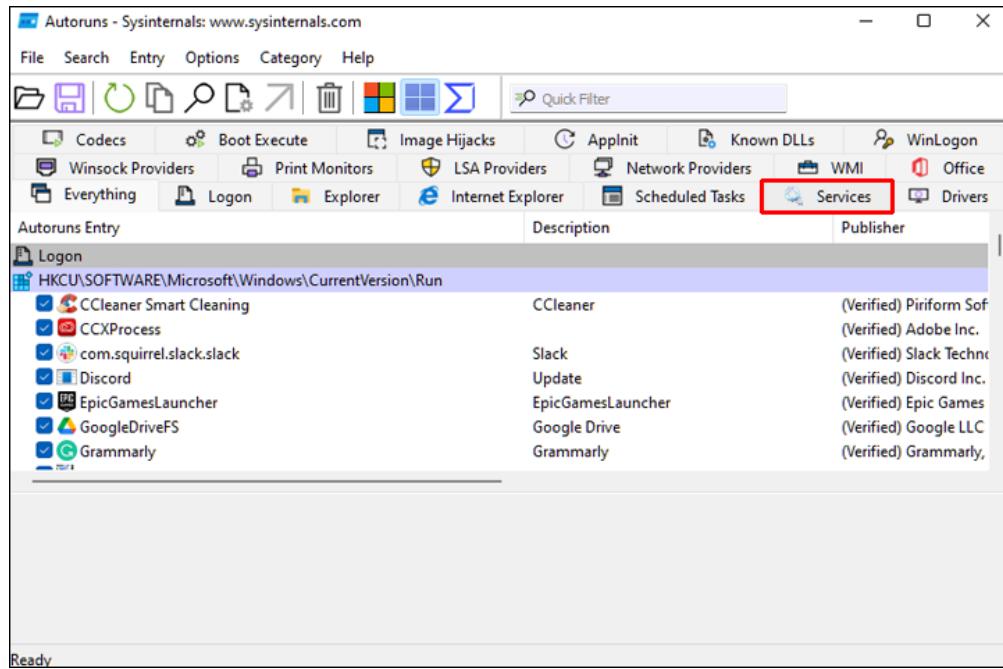
9. Open the **Autoruns** folder on your desktop, click the **Autoruns64.exe** file, then **Run** to start it.



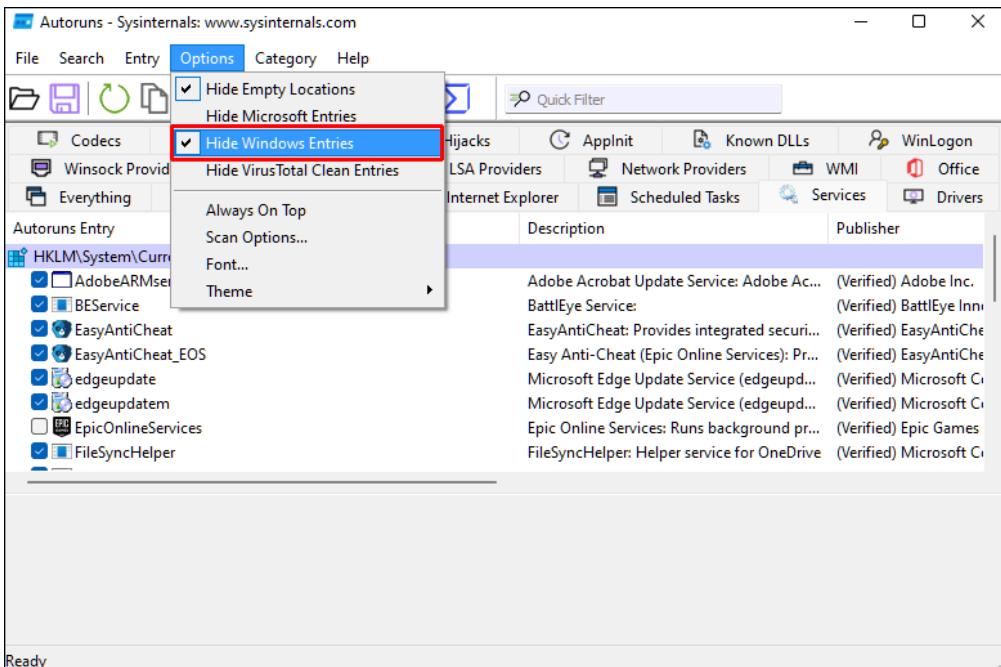
10. An **Autoruns License Agreement** window will display. If you agree with the terms, click **Agree** to continue.



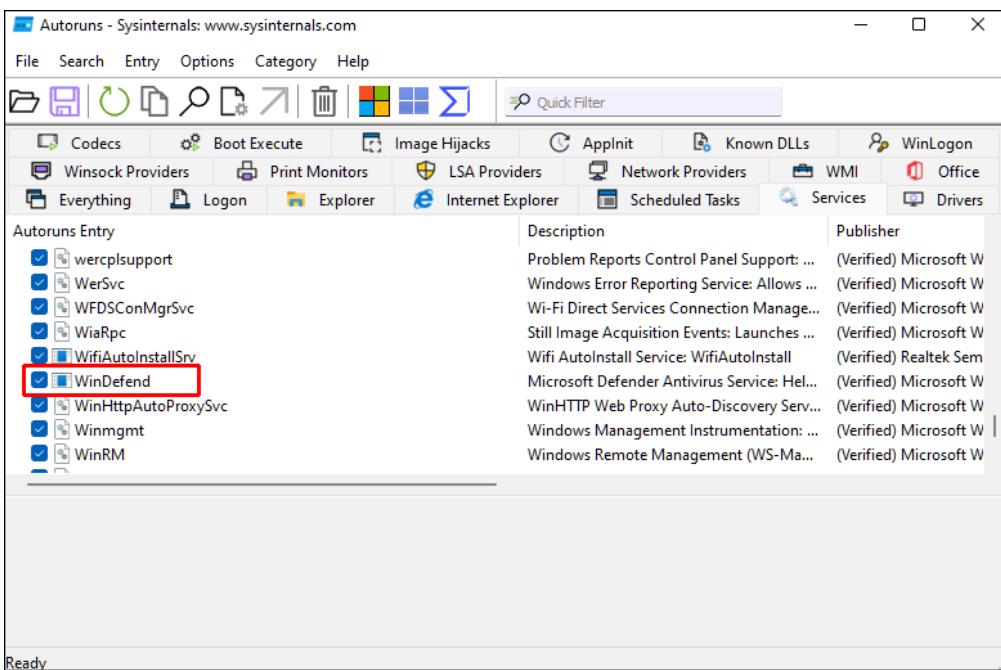
11. In the **Autoruns** window, choose the **Services** tab.



12. By default, Windows services are hidden. To make them visible, click on **Options** from the main menu, then uncheck the **Hide Windows Entries**.



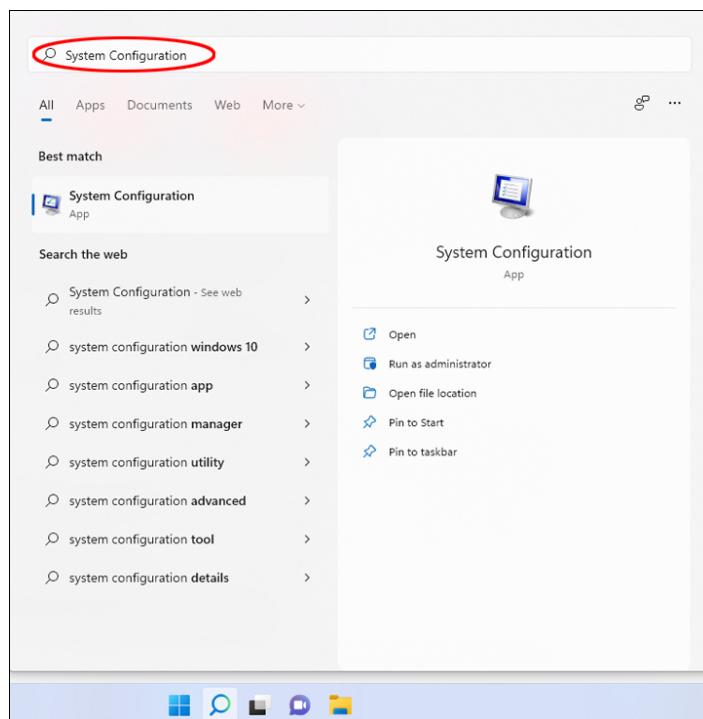
13. Go through the list of services for Windows Defender and uncheck the **WinDefend** box. This will disable the automatic startup for Windows Defender each time the computer reboots.



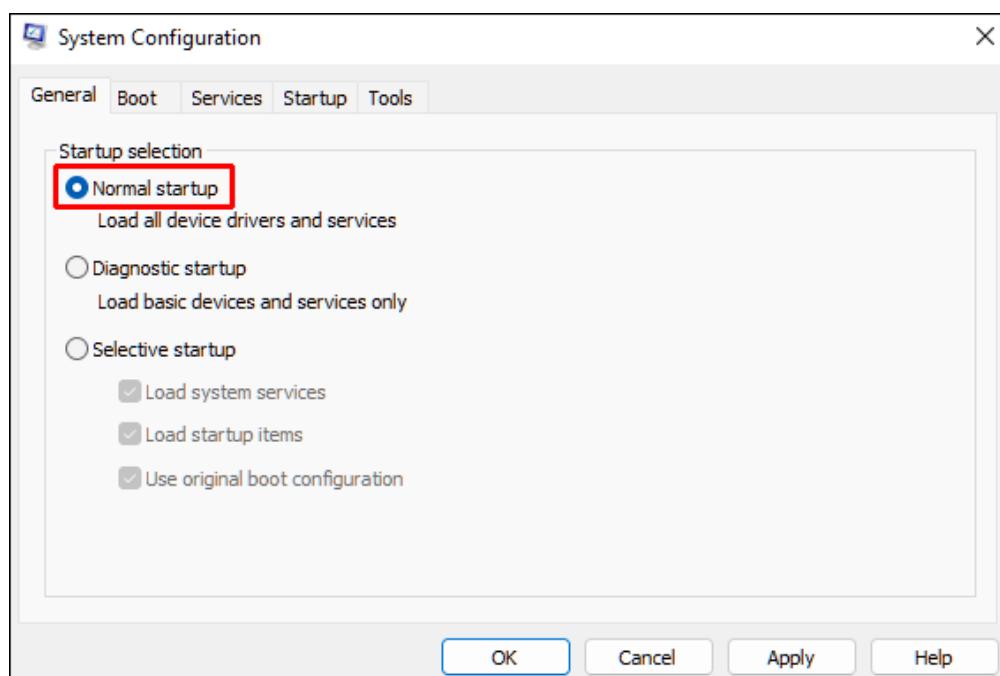
14. Now close **Autoruns**, then reboot your computer into normal mode.

To reboot your computer into normal mode:

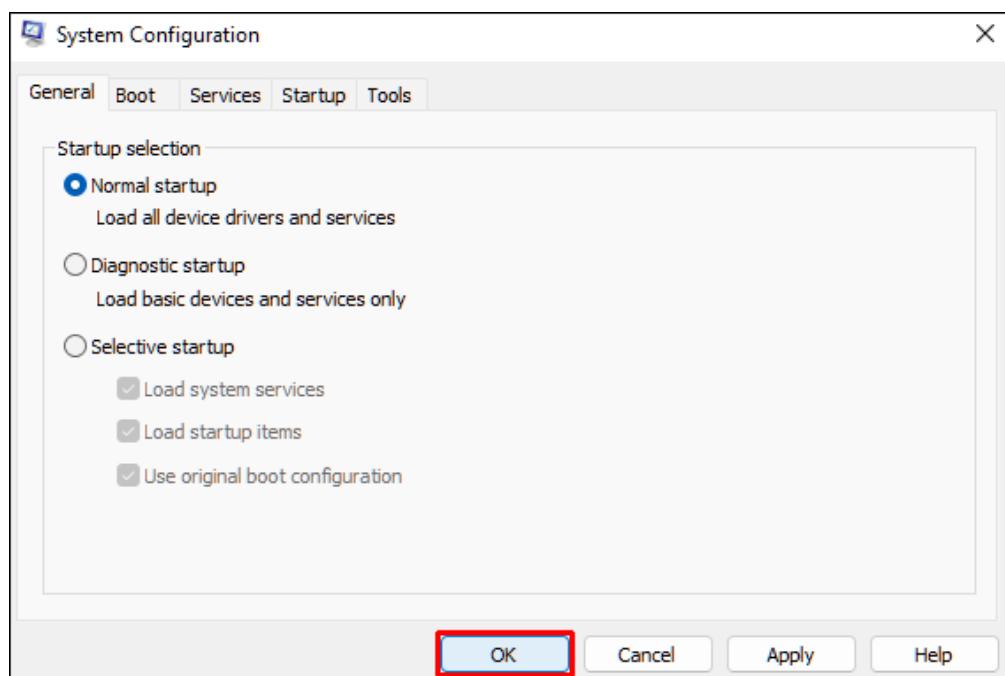
1. Press the **Search** icon on the taskbar and select **System Configuration**.



2. Check the **Normal startup** option.



3. Click **Apply**, **OK**, then **Restart**.



Once your computer has rebooted, launch **Task Manager** and check if the Windows Defender service is running:

1. Open **Settings** to see the **Virus & threat protection** status. To get there, go to **Privacy & security**, **Windows Security**, **Virus & threat protection**, then **Home**.



2. Verify that the **Virus & threat protection** status is set to **Unknown**.



**Note:** Avoid clicking on the Defender tile as it updates its information or displays the "Unknown" status. If you click on it during that time, Defender will be enabled again.

# Time to Stop Defending Windows Defender

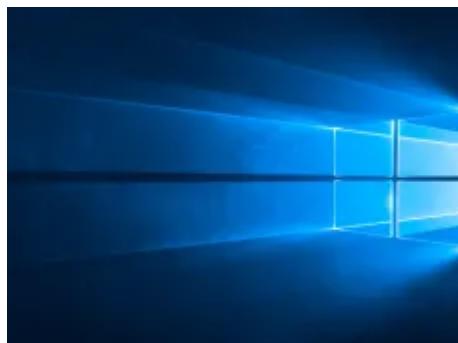
By default, the free antivirus software Windows Defender is set to remain enabled, even after being turned off via **Virus & threat protection**. To stop Windows Defender for good requires a permanent or “hard” deactivation. This can be done by updating the policy, modifying the registry, or disabling it using the “Autoruns for Windows” utility tool. Any of these three methods ensures Defender will not reactivate at will.

Let us know which option worked/didn't work for you in the comments below!

## Related Posts



**How To Disable Show More Options in**  
[\(https://www.alphr.com/windows-11-show-more-options/\)](https://www.alphr.com/windows-11-show-more-options/)



**How to Disable the Windows 10 Update from Downloading**  
[\(https://www.alphr.com/microsoft-microsoft-windows-10-update/\)](https://www.alphr.com/microsoft-microsoft-windows-10-update/)



**How to Disable Spotify Opening on Startup in**  
[\(https://www.alphr.com/how-to-disable-spotify-startup/\)](https://www.alphr.com/how-to-disable-spotify-startup/)



**How to Disable Administrator Account in**  
[\(https://www.alphr.com/disable-administrator-account/\)](https://www.alphr.com/disable-administrator-account/)



**How to Disable BitLocker in Windows**  
[\(https://www.alphr.com/disable-bitlocker/\)](https://www.alphr.com/disable-bitlocker/)



**How to Disable OneDrive in Windows 11**  
[\(https://www.alphr.com/disable-onedrive-windows-11/\)](https://www.alphr.com/disable-onedrive-windows-11/)

**How To Disable the Touchpad  
in Windows 11, 10, 8,  
[\(https://www.alphr.com/disable-touchpad-windows/\)](https://www.alphr.com/disable-touchpad-windows/)**

**How To Disable Sticky Keys  
on a Windows PC, Mac, or  
[\(https://www.alphr.com/disable-sticky-keys/\)](https://www.alphr.com/disable-sticky-keys/)**

# How To Disable the Camera on a Windows PC

(<https://www.alphr.com/disable-camera-windows/>)

*Disclaimer: Some pages on this site may include an affiliate link. This does not effect our editorial in any way.*

## You may also like



## **How to Add Controller Support to Minecraft Java Edition** **(<https://www.alphr.com/add-controller-minecraft-java/>).**

Lee Stanton December 22, 2023



## [How to Test the Camera on a Windows 10 PC](https://www.alphr.com/how-to-test-the-camera-on-a-windows-10-pc/)

Lee Stanton December 21, 2023

# Todays Highlights

## [How to Change the Location on a FireStick](https://www.alphr.com/change-location-firestick/)

Lee Stanton April 1, 2023

## [How to View Your Google Search History](https://www.alphr.com/view-google-search-history/)

Steve Larner March 7, 2023

## [How to Change Your User Name in Zoom](https://www.alphr.com/user-name-zoom/)

Lee Stanton August 23, 2022

## [How to Use Inspect Element](https://www.alphr.com/how-to-use-inspect-element/)

Lee Stanton August 16, 2022

## [How to Download Photos from Google Photos](https://www.alphr.com/download-photos-from-google-photos/)

Cassandra McBride  
December 3, 2022

## [How to Change Your Username on Fortnite](https://www.alphr.com/how-to-change-your-username-on-fortnite/)

Lee Stanton February 20, 2023

(<https://www.alphr.com>).

(<https://www.alphr.com/contact-us/>).

## Categories

### Gaming

(<https://www.alphr.com/category/video-games/>).

### Social Media

(<https://www.alphr.com/media/>).

### PC & Mobile

(<https://www.alphr.com/category/pc-mobile/>).

### Internet

(<https://www.alphr.co>).

## Latest

### How to Remove Netflix

#### Recently Watched Shows

(<https://www.alphr.com/netflix/1003298/how-to-remove-netflix-recently-watched-shows/>).

Cassandra McBride July 27, 2022

### How to Use a VPN with an

#### Android Device

(<https://www.alphr.com/use-vpn-android/>).

Lee Stanton April 1, 2023

© Guiding Tech Media 2024

About Us (<https://www.alphr.com/about-alphr/>) | Contact Us (<https://www.alphr.com/contact-us/>) | Privacy Policy (<https://www.alphr.com/privacy-policy/>) | TOS (<https://www.alphr.com/tos/>) | All Rights Reserved

[Update Privacy Preferences](#)

A RAPTIVE PARTNER SITE