Simple way to Turn Off / Disable Windows Defender

zerosalarium.com/2024/12/disable windows defender permanently.html

Zero Salarium December 29, 2024

I. Introduction

I will guide you through two methods on how to stop Defender that I have tested and successfully worked with the latest versions of Windows 10 and Windows 11.

The first method is to use the advanced boot options of Windows to disable Windows Defender permanently. By intervening in the loading process of the antimalware service executable.

The second method, which is extremely simple, is to use the open-source tool "**Windows Defender Manager**" to turn Windows Defender off.

Of course, you may have your reasons for turning off Windows Defender, although this is not recommended. If you want to learn how to protect and keep your computer safe, you can explore my series of articles on Operations Security (OPSEC) to configure and use your computer more securely.

II. How to stop Defender

Windows Defender, now known as Microsoft Defender Antivirus, is a built-in antivirus program included in Windows 10, Windows 11, and Windows Server. It provides real-time protection against malware, viruses, and other security threats.

1. Disable windows defender permanently

In this section, I will guide you on how to disable Defender through the advanced boot options of Windows. This method is effective on both Windows 11 and 10. I will demonstrate it on the latest version of Windows 11, with updates installed up to December 2024.

A. Some basic information you need to know about Windows Defender

When wanting to stop Windows Defender, we need to pay attention to 2 Windows services.

The **Microsoft Defender Antivirus Service** is a core security component of Windows that provides real-time protection against malware, viruses, and other threats. It continuously monitors your system, performs scheduled scans, and updates its threat definitions to keep your device safe. The service runs in the background under the process name “**MsMpEng.exe**” (Antimalware Service Executable) and integrates with the Windows Security app for easy management.

The **Microsoft Defender Core Service** is a vital component of Microsoft Defender Antivirus designed to enhance the stability and performance of the antivirus platform. It integrates with the Experimentation and Configuration Service (ECS) to receive updates on configurations, feature rollouts, and experiment payloads, ensuring that the antivirus protection remains up-to-date and effective. The background process name for the Microsoft Defender Core Service is “**MpDefenderCoreService.exe**”.

Both of these services are protected at the kernel level. This means that regardless of how high the privileges of the user account you are using (Trusted Installer, SYSTEM, Administrator), you will not be able to affect them.

Therefore, as long as you can prevent the execution of the Antimalware Service Executable and Core service from running, it means you have effectively turned off Microsoft Defender.

B. How to disable Defender

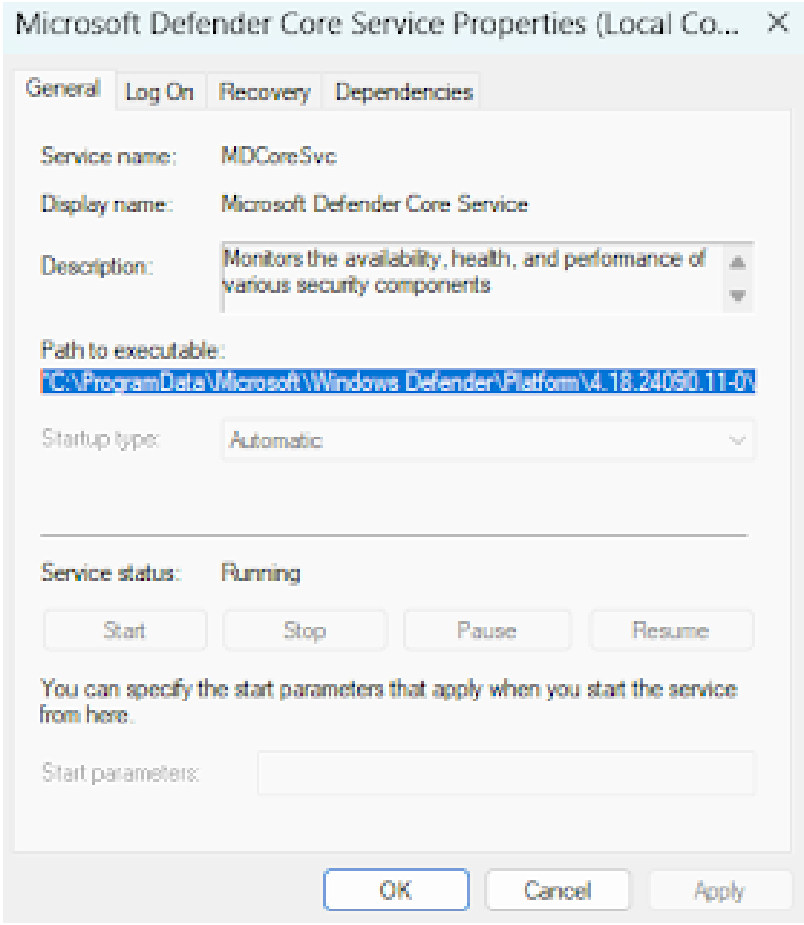
We will use the advanced boot options feature to affect the two services mentioned above. All operations will be performed on Windows 11 version 24H2, updated until December 2024.

Where is Windows Defender executable?

We will obtain the path information of the Windows Defender executable through the Services Manager.

To open the Services Manager:

1. Press the Start button (Windows icon) or press Windows + X to open the WinX Menu.
2. Select "**Run**" from the menu.
3. Type "**services.msc"** in the Run dialog box and press Enter.
4. In the Services Manager window, locate the two services named "**Microsoft Defender Antivirus Service**" and "**Microsoft Defender Core Service**".
5. Double-click on the found service, and in the new popup window, you will find the path to Windows Defender in the "Path to executable" section.



Disable windows defender permanently

Continuing from above. For my machine, the paths of the executable files for the two services are as follows:

```
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MpDefenderCoreService.exe"
```

```
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MsMpEng.exe"
```

Please note that you should also copy the double quotation marks to avoid any issues with invalid paths.

To facilitate command line operations, I will create a folder "**C:\defend**" Then, in this folder, I will create a text file named "**tmp.txt**"

Paste these two paths into the content of the "**C:\defend\tmp.txt**" file created earlier.

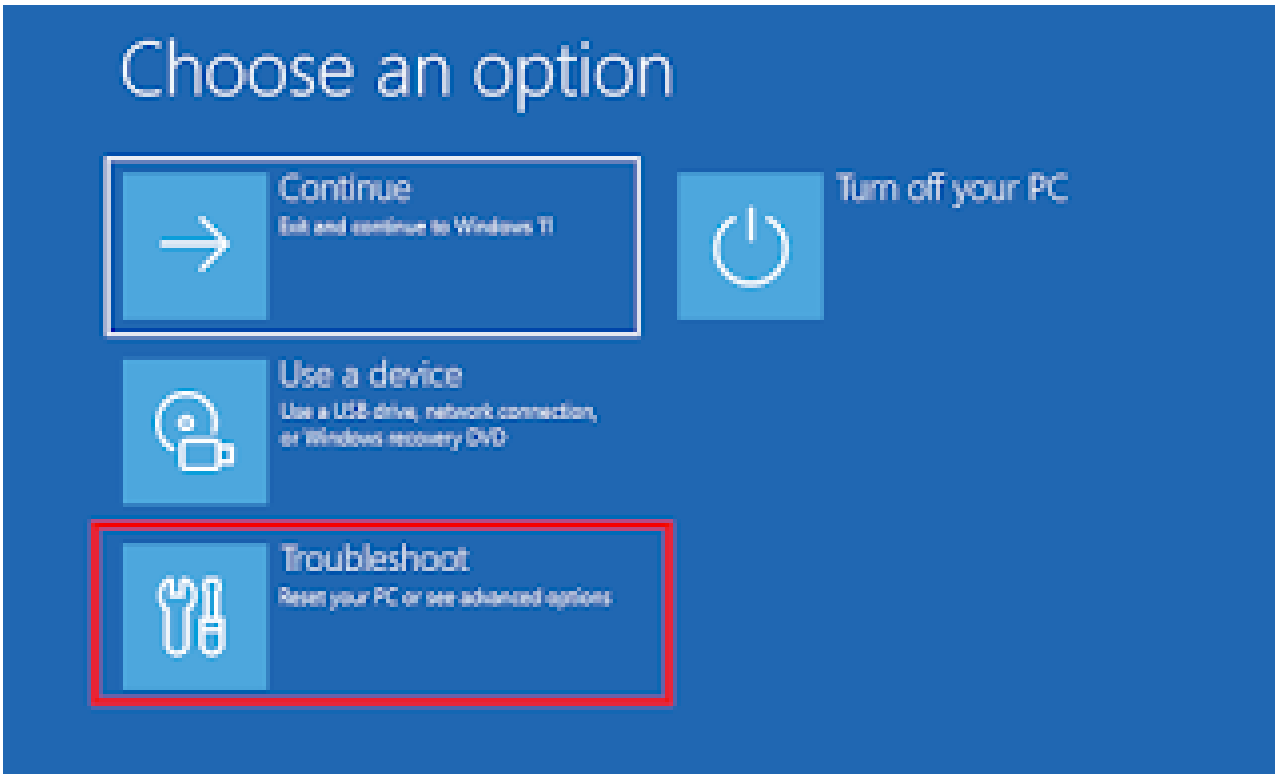
Sequentially copy the two executable files "**MpDefenderCoreService.exe**" and "**MsMpEng.exe**" to the folder "**C:\defend**" and rename them to "**MpDefenderCoreService_backup.exe**" and "**MsMpEng_backup.exe**". The purpose of this is to keep the original two files as a backup, in case you change your mind and want to run Windows Defender again as before.

After completing the steps above, open CMD and execute the command:

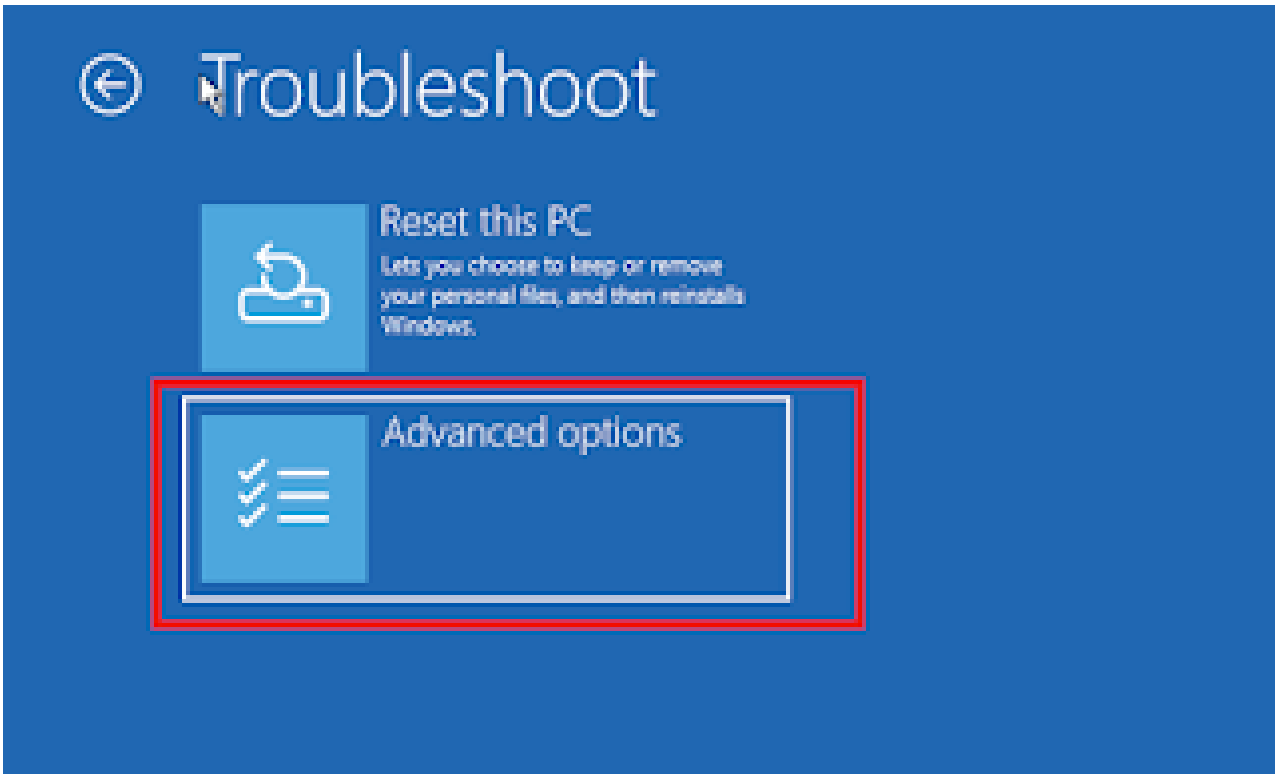
```
shutdown /r /o /f /t 0
```

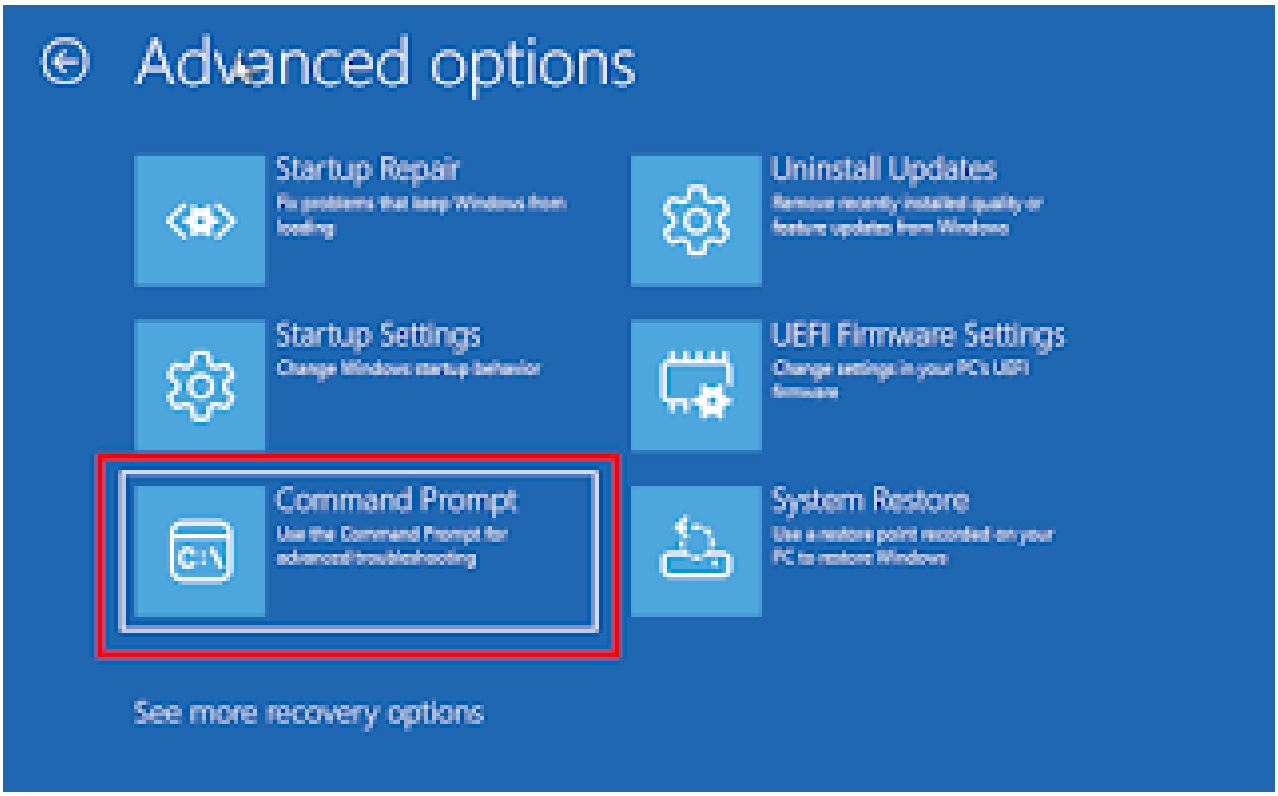
You should close all running programs, as this command will restart Windows.

After the above command is executed, Windows will restart to the "**Advanced boot options**" screen. Here, you should select "**Troubleshoot**".



On the "**Troubleshoot**" screen, select "**Advanced options**". Then select "**Command Prompt**" to open the CMD window.





In the newly opened CMD, execute the following two commands:

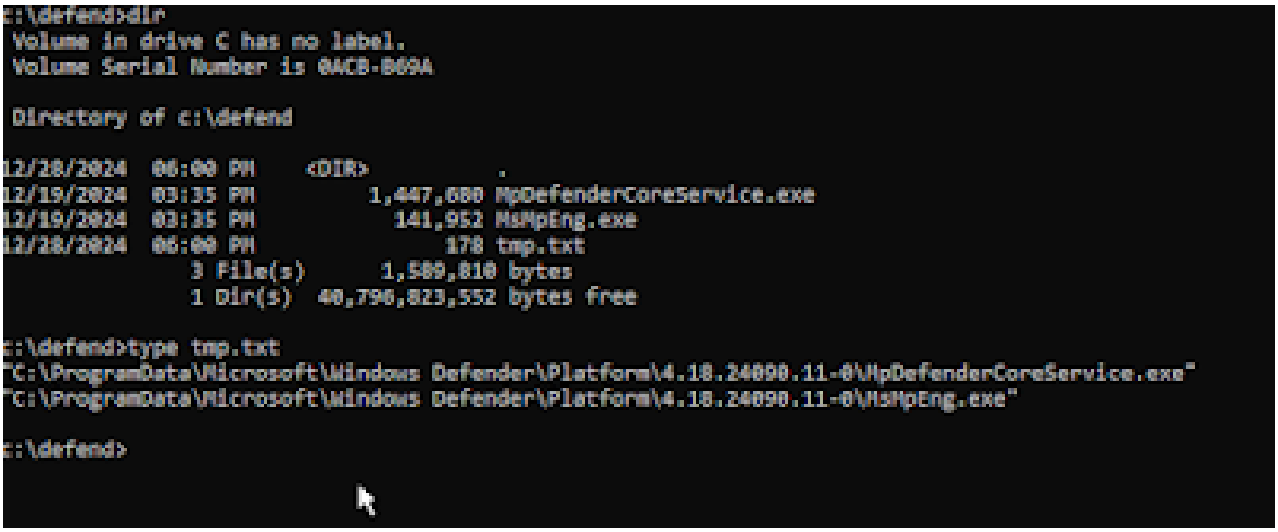
```
c:
```

```
cd c:\defend
```

If you executed correctly, you should now be in the directory "**C:\defend**".

Do you remember the "**tmp.txt**" file you created earlier? Execute the following command:

```
type tmp.txt
```



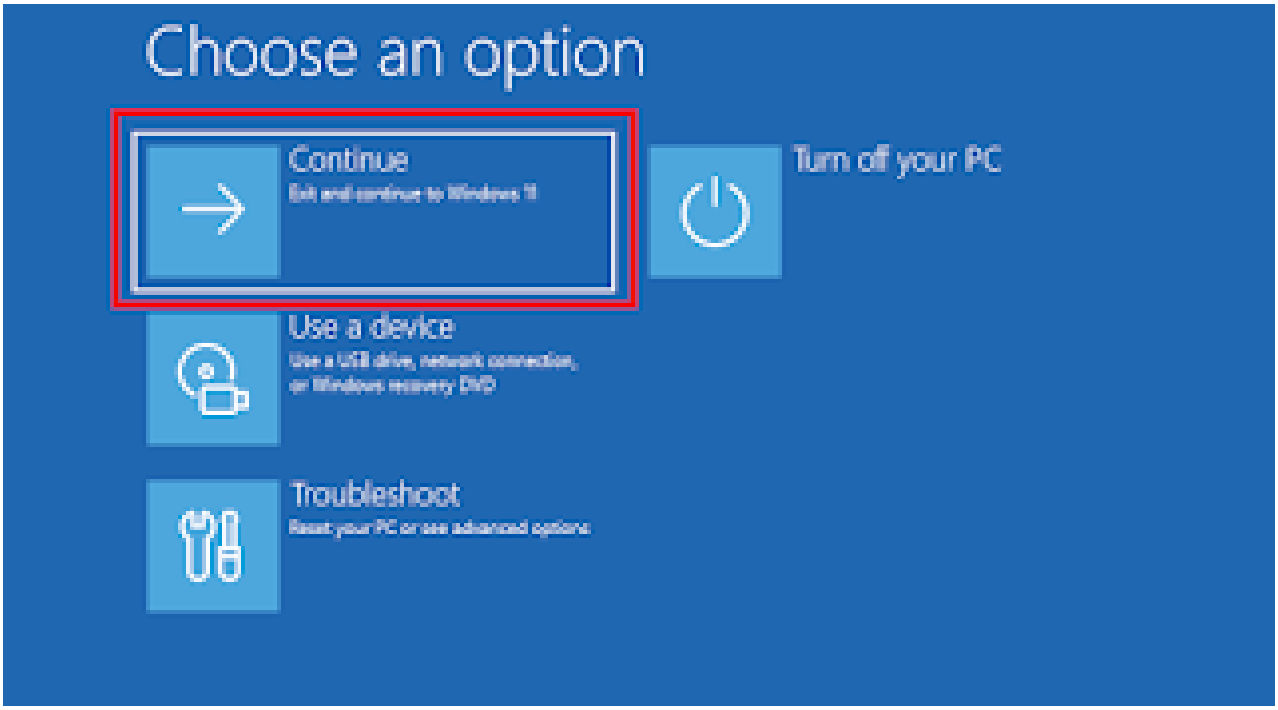
We will need the paths to the executable files of the two services that were found earlier.

Execute the two commands below to overwrite the original service files.

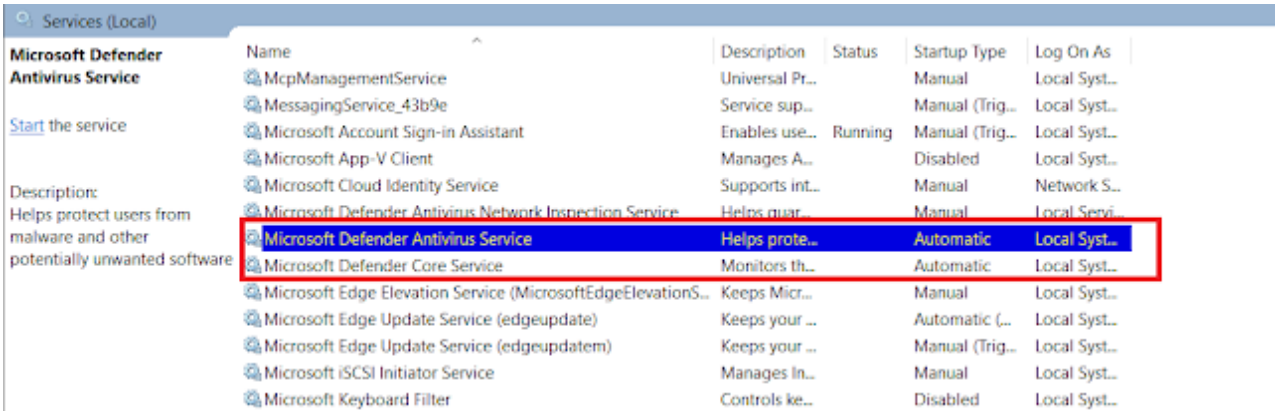
```
copy /y c:\windows\system32\cmd.exe "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MpDefenderCoreService.exe"

copy /y c:\windows\system32\cmd.exe "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MsMpEng.exe"
```

```
c:\defend>type tmp.txt
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MpDefenderCoreService.exe"
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MsMpEng.exe"

c:\defend>copy /y c:\Windows\System32\cmd.exe "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MpDefe
nderCoreService.exe"
        1 file(s) copied.

c:\defend>copy /y c:\Windows\System32\cmd.exe "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24090.11-0\MsMpEn
g.exe"
        1 file(s) copied.
```

After the copy is successful, close the CMD window and select "**Continue**" to boot Windows normally.



At this point, when you return to the "**Services Manager**" you will see that the two Windows Defender services are no longer running. The processes "**MsMpEng.exe**" and "**MpDefenderCoreService.exe**" will also no longer exist.



2. Turn off Windows Defender with open-source tool

This method will be extremely simple and more suitable for everyone. By using a tool called "**Windows Defender Manager**".

You can download this tool via the GitHub link: Windows Defender Manager

This tool, once installed, will run in the background and check every minute. Whenever the "**Real-time protection**" feature is somehow enabled, the background program will automatically disable it.

In other words, the following features of Defender are always disabled:

- Real-time protection
- Cloud-delivered protection
- Automatic sample submission

"**Windows Defender Manager**" requires the "**Tamper Protection**" feature to be disabled. Since it needs to interact with Defender's configurations, the program will not function if this feature is enabled.

To turn off Tamper Protection in Windows Defender, follow these steps:

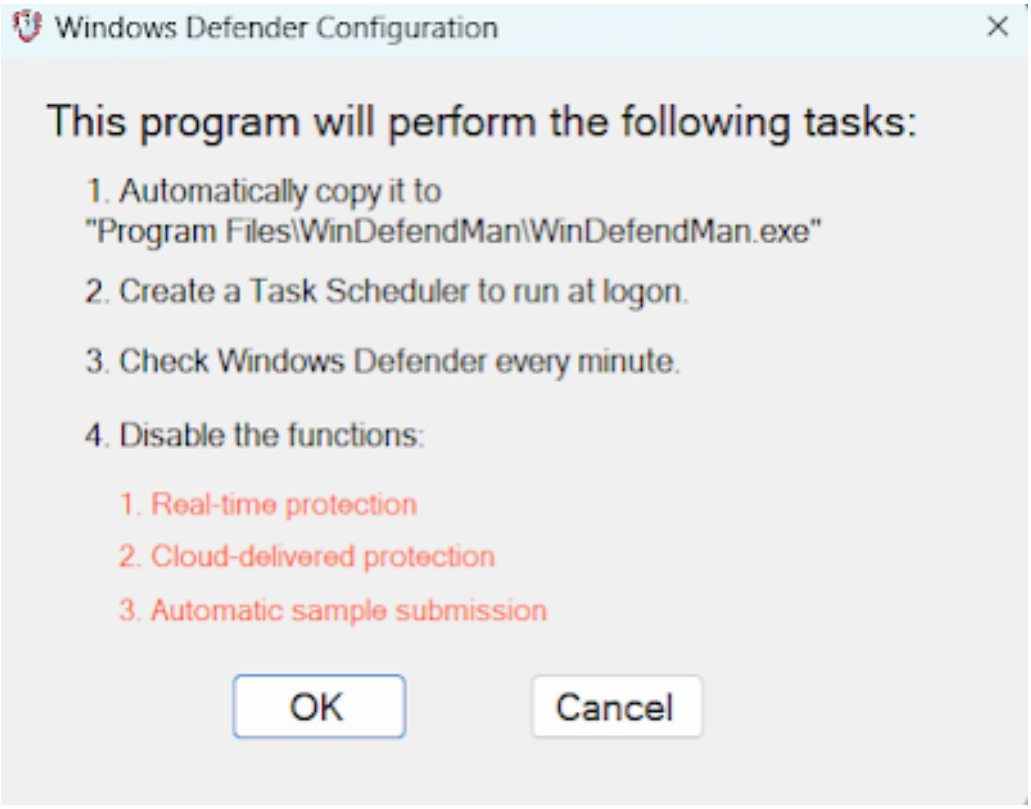
Open Windows Security:

1. Press Windows + I to open the Settings app.
2. Go to Update & Security > Windows Security.
3. Go to Virus & Threat Protection:
4. Click on Virus & threat protection in the Windows Security window.

Manage Settings:

1. Click on Manage settings under Virus & threat protection settings.
2. Scroll down to find Tamper Protection and toggle the switch to Off.

After downloading and extracting, you run the program "**WinDefendMan.exe**". At this point, Windows SmartScreen may issue a warning because the program lacks a digital signature and was downloaded from the Internet. You can select "**Run Anyway**".

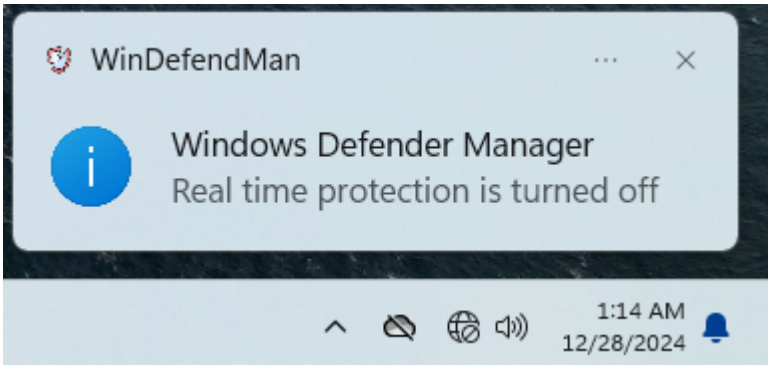


The program will display a message indicating what it will do; you can click "**OK**" to continue.

If no errors occur, the program will display a popup notification indicating successful installation. Alternatively, it will provide a message explaining the reason for the installation failure.

You should restart your computer or log out and log back in to activate the newly installed "Windows Defender Manager".

Each time you log in, "Windows Defender Manager" will display a status notification in the notification area at the bottom of the screen.



At this point, you will see that Windows Defender Real-time protection has been disabled.

III. Conclusion

Microsoft Windows Defender is an antivirus that comes pre-installed on Windows. It is protected at the kernel level.

The "**Real-time protection**" feature of Defender will automatically re-enable itself upon Windows startup.

We can disable Windows Defender permanently by using advanced boot options.

"**Windows Defender Manager**" is a tool that operates as a background program, ensuring that the "Real-time protection" feature of Defender remains disabled.

Windows Defender exists to ensure your safety. However, relying solely on antivirus is not enough; you should explore configuration methods and safe computer usage through my series on basic Operations Security. This series will be continuously updated to keep pace with technological changes.