

What is Antimalware Service Executable and why is it running on the computer?

Windows 10 developed a new feature Windows Defender, Windows' integrated antivirus program. The Antimalware Service Executable process is the background process of Windows Defender, it is also known as MsMpEng.exe, part of the Windows operating system.

Windows 10 developed a new feature Windows Defender, Windows' integrated antivirus program. The Antimalware Service Executable process is the background process of Windows Defender, it is also known as MsMpEng.exe, part of the Windows operating system.

1. 10 things to know about Windows Defender

What is the Antimalware Service Executable process?

Windows Defender is part of Windows 10, and the "successor" of free Microsoft Security Essentials antivirus program for Windows 7. This program ensures all Windows 10 users have an antivirus program installed. Available and running even if not selected for installation. If you install an outdated antivirus software, Windows 10 will turn it off and activate Windows Defender.

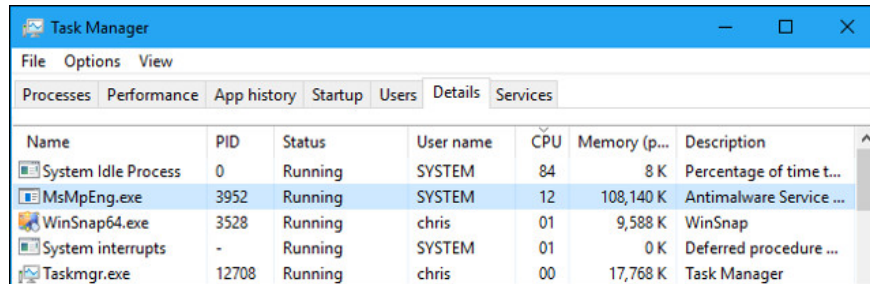
Name	CPU	Memory	Disk	Network
Antimalware Service Executable	13.5%	99.8 MB	2.4 MB/s	0 Mbps
Desktop Window Manager	0.3%	22.2 MB	0 MB/s	0 Mbps
WinSnap	0.2%	9.1 MB	0 MB/s	0 Mbps
Windows Defender Security Center	0.2%	13.9 MB	0 MB/s	0 Mbps
Task Manager	0.2%	14.6 MB	0 MB/s	0 Mbps
OVRServer_x64.exe 409268-public TCID...	0.2%	56.2 MB	0.1 MB/s	0 Mbps

1. 10 most effective antivirus software for Windows 2018

The Antimalware Service Executable process is Windows Defender's background service and it always runs in the background. This process checks for malware in files when you access them, performs background system scans to check for malicious software, install anti-virus updates and anything that an application does. Security applications like Windows Defender need.

Although the process is called Antimalware Service Executable on the **Processes** tab in **Task Manager** , its file name is MsMpEng.exe on the **Details** tab.

1. All problems about using Task Manager

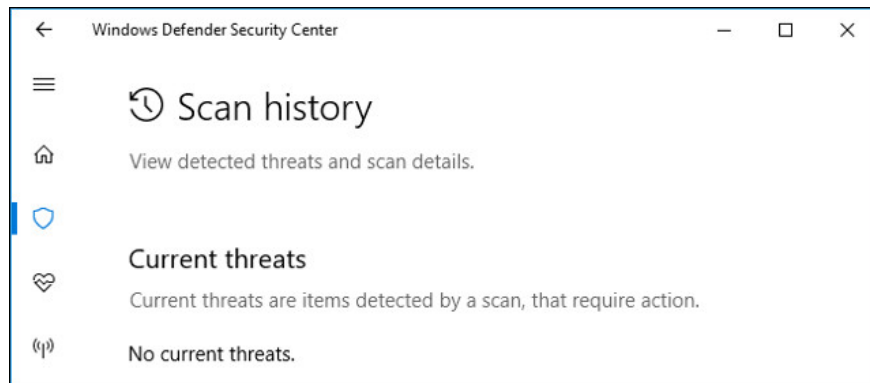


The screenshot shows the Windows Task Manager window with the 'Details' tab selected. The table below represents the data shown in the task list:

Name	PID	Status	User name	CPU	Memory (p...	Description
System Idle Process	0	Running	SYSTEM	84	8 K	Percentage of time t...
MsMpEng.exe	3952	Running	SYSTEM	12	108,140 K	Antimalware Service ...
WinSnap64.exe	3528	Running	chris	01	9,588 K	WinSnap
System interrupts	-	Running	SYSTEM	01	0 K	Deferred procedure ...
Taskmgr.exe	12708	Running	chris	00	17,768 K	Task Manager

You can configure Windows Defender, perform a scan and check its scan history from the Windows Defender Security Center application included in Windows 10.

To start it, use the "Windows Defender Security Center" shortcut in the **Start** menu. You can also right-click the shield icon in the notification area on the taskbar and select ' **Open** ' or go to **Settings> Update & security> Windows Defender> Open Windows Defender Security Center** .



Why does it use too much CPU?

If you see the Antimalware Service Executable process using a large amount of CPU or disk resources, it may be scanning the malware on the computer. Like other antivirus tools, Windows Defender regularly scans files on your computer.

It also scans files when you open them and regularly installs updates with new malware information. The use of this CPU may also occur when it is installing an update or you have just opened a very large file Windows Defender needs more time to analyze.

Windows Defender usually only performs background scans when your computer is inactive and not being used. However, it is still possible to use CPU resources to perform updates or scan files when you open them, even if you are using a computer but it does not perform background scans.

This is perfectly normal for any antivirus program, because it needs to use some resources to check your computer and protect you.

Can this process be disabled?

You should not disable Windows Defender antivirus tool if you do not install another antivirus software on your computer. In fact, you cannot permanently disable it. You can open the Windows Defender Security Center application from the **Start** menu, navigate to settings for **Virus & threat protection**> **Virus & threat protection** and disable **Real-time protection** . However, this operation is only temporarily disabled and Windows Defender will reactivate itself after a short time if it does not detect any antivirus applications installed.

1. Turn off Windows Defender on Windows 10

Windows Defender performs the scan as a system maintenance task so you can't disable it, even disabling its task on Task Scheduler is not helpful. It only stops permanently if you install another antivirus program to replace it.



If you install another antivirus program such as Avira or BitDefender, Windows Defender will automatically disable itself. If you access **Windows Defender Security Center**> **Virus & threat protection** you will see a message saying ' **You're using other antivirus providers** ' (You are using another antivirus program) if you install and activate the removal program. another virus. This means that Windows Defender has been disabled. The process can run in the background but it does not use CPU resources or disk resources to scan the system.

However, there is a way to use both your antivirus program and Windows Defender. On the same screen above, you can expand the Windows Defender Antivirus option and enable **Periodic scanning** . Windows Defender will perform background scans regularly even if you are using another antivirus program. This can help find out what the main antivirus program might miss.

If you see Windows Defender using the CPU even after installing other antivirus tools and want to stop it, go to Windows Defender Security Center and make sure that the Periodic scanning feature has been changed to ' **Off** '. If you want, you can still enable this periodic scan to add additional protection, but this feature is off by default.



Is this process a virus?

No reports have shown that the virus tampered with the Antimalware Service Executable process. Windows Defender is an antivirus software, so it will prevent any software that can do it. As long as you are using Windows and activating Windows Defender, it is perfectly normal to run this process.

If you still feel anxious, you can scan the program with another antivirus software to confirm there is no malicious component on your computer.

See more:

1. [How to kill viruses with Windows Defender Offline on Windows 10 Creators](#)
2. [How to turn off the Windows Defender Summary notification on Windows 10](#)
3. [Windows Defender is disabled or inactive, this is a fix](#)

You finished reading the article "**What is Antimalware Service Executable and why is it running on the computer?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.