What is the Microsoft Network Realtime Inspection Service (NisSrv.exe) and why is it running on the computer?

Windows 10 has Windows Defender that protects your computer from viruses and other threats. The Microsoft Network Realtime Inspection Service, also known as NisSrv.exe, is part of Microsoft's antivirus software.

Windows 10 has Windows Defender that protects your computer from viruses and other threats. The Microsoft Network Realtime Inspection Service, also known as NisSrv.exe, is part of Microsoft's antivirus software.

This process is also available in Windows 7 if you have installed Microsoft Security Essentials antivirus software. This is another part of Microsoft's anti-malware product.

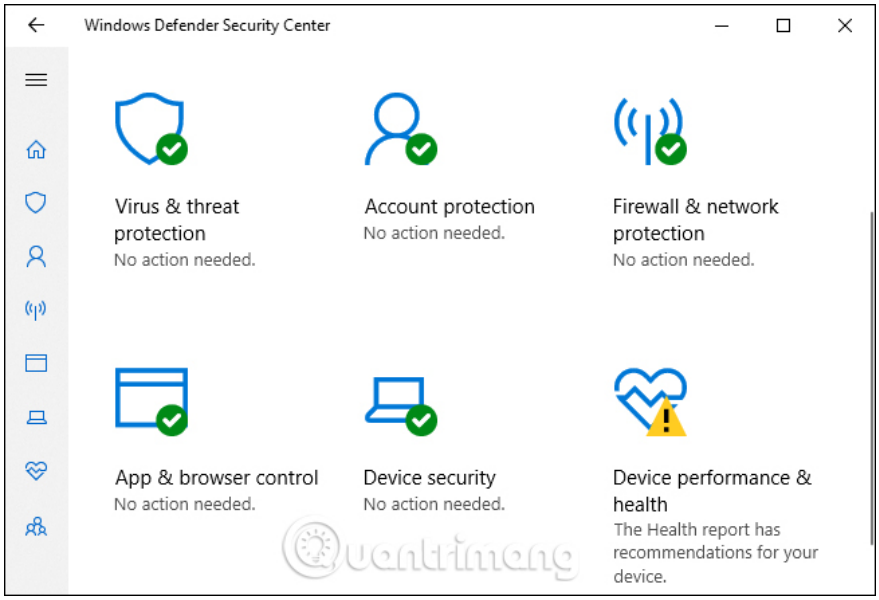
1. Instructions for installing and configuring Microsoft Security Essentials

Basic thing about Windows Defender

On Windows 10, Microsoft's Windows Defender antivirus program is installed by default. Windows Defender automatically runs in the background, scans for malware files before you open them and protects the computer from other types of attacks.

The main Windows Defender process is named Antimalware Service Executable and the file name is MsMpEng.exe. This process checks for malware files when you open them and scans the computer in the background.

On Windows 10, you can use Windows Defender by launching the Windows Defender Security Center application from the Start menu. You can also find it by going to **Settings> Update & Security> Windows Security** > Open **Windows Defender Security Center** . On Windows 7, launch the Microsoft Security Essentials application. This interface allows you to manually scan for malware and configure antivirus software.



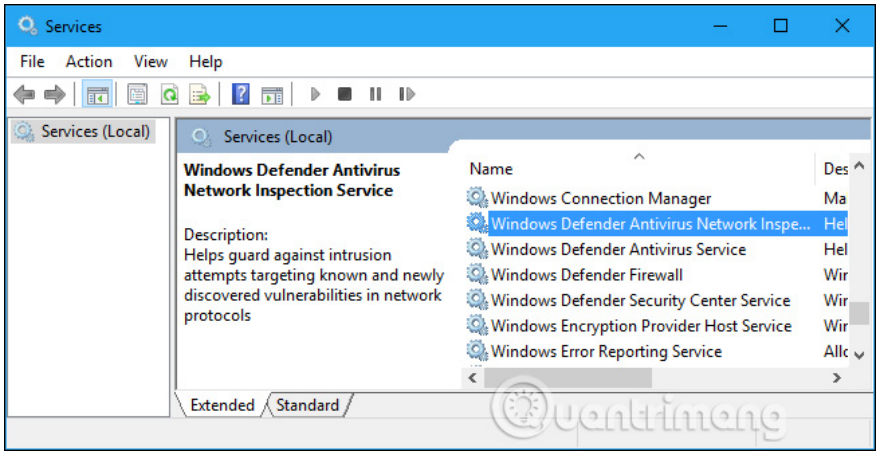
What task does NisSrv.exe perform?

The NisSrv.exe process is also called the 'Windows Defender Antivirus Network Inspection Service'. According to Microsoft's description of the service, it 'helps protect against intrusion attempts aimed at known and newly discovered vulnerabilities in network protocols'.

In other words, the service is always running in the background in the computer, monitoring and checking network traffic in real time. It is looking for suspicious behavior that suggests an attacker is trying to exploit security holes in the network protocol to attack your computer. If it detects such an attack, Windows Defender will turn it off immediately.

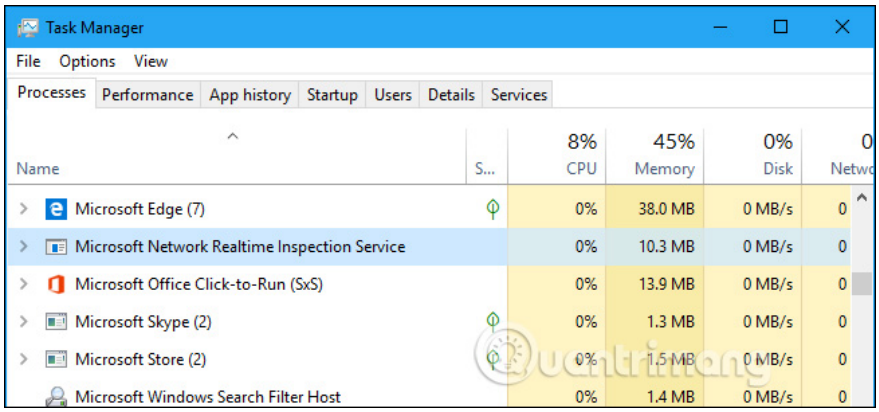
The update for the network inspection service contains information about new threats through definition updates (definition update) for Windows Defender or Microsoft Security Essentials, if you are using a Windows 7 computer.

This feature was first added to Microsoft's antivirus program in 2012. A Microsoft blog post explains a little more detail: 'This is a protection feature against zero-day vulnerabilities, blocking traffic. network matches the known exploits'. Therefore, when a new security vulnerability is found in Windows or the application, Microsoft can immediately release a temporary network inspection service update to protect it. Then, Microsoft or the application provider can work on security updates and fix security vulnerabilities permanently.



Does this process monitor users?

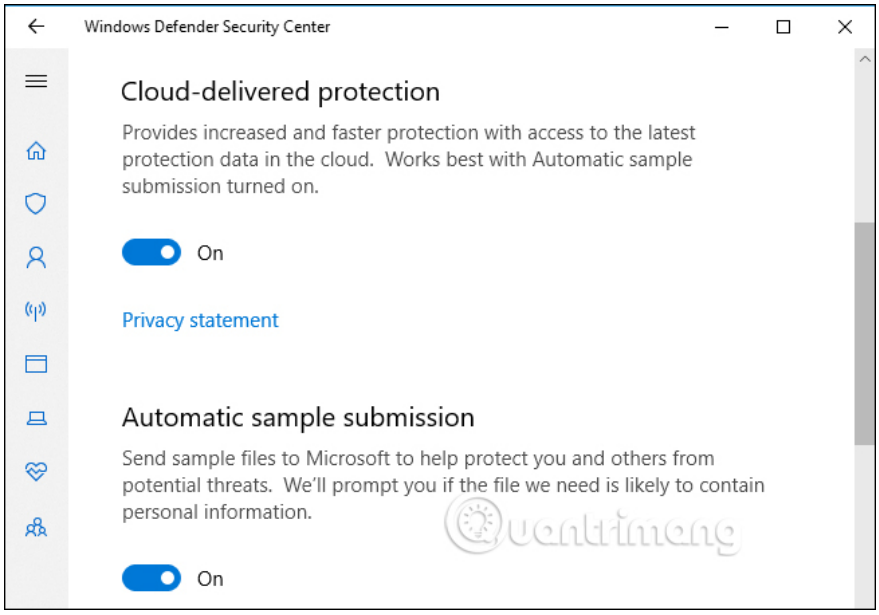
The name "Microsoft Network Realtime Inspection Service" at first seems a bit scary, but it's really just a process of checking your network traffic to see if any attacks are known. If an attack is detected, it will turn off. This feature works like a standard antivirus file scan, checks the files you open and whether they are dangerous. If you are opening a dangerous file, the anti-malware service will stop you.



This special service does not report information about your web browsing and normal network activities to Microsoft. However, with the default 'Full' system remote installation, the web address information you access in Microsoft Edge and Internet Explorer will be sent to Microsoft.

Windows Defender is configured to report the attacks it detects to Microsoft. You can disable this option if you want by opening the Windows Defender Security Center application, clicking **Virus & Threat Protection** in the sidebar and then clicking **Virus & Threat Protection Settings** , disabling the **Cloud-** option. **Delivered protection** and **Automatic sample submission** .

However, you should not disable this feature because the information sent to Microsoft can protect other users. Cloud-delivered protection can help your computer get new definitions faster and protect you against zero-day attacks.



Can this process be disabled?

This service is an important part of Microsoft's anti-malware software, and you cannot easily disable it on Windows 10. You can temporarily disable real-time protection in the Windows Defender Security Center, but it will reactivate itself.

However, if you install another antivirus program, Windows Defender will automatically disable itself. This also disables the Microsoft Network Realtime Inspection Service. Other antivirus applications may have its own network protection component.

In other words, you cannot turn this feature off and you should not do so, as it helps protect your computer. If you install another antivirus tool, this feature will be disabled, but just because another antivirus tool is doing the same job and Windows Defender doesn't want to hinder it.

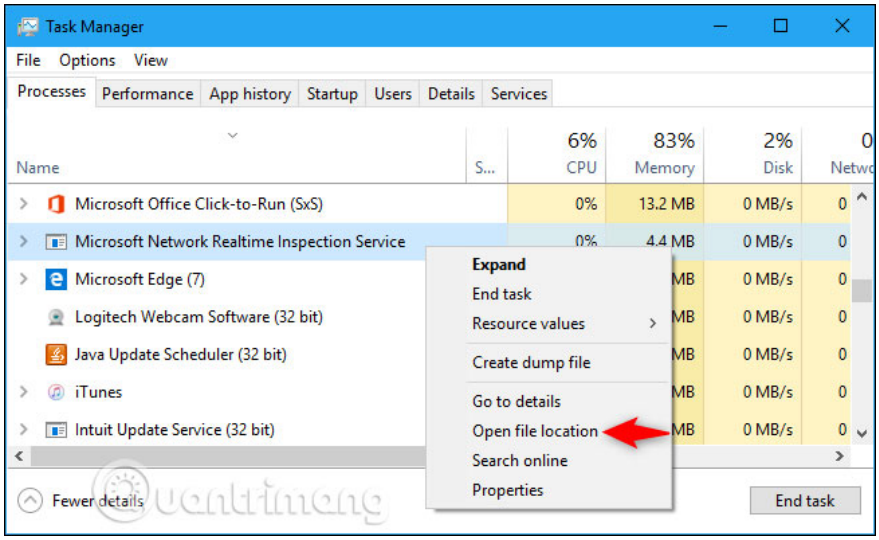
1. Turn off Windows Defender on Windows 10

Is it a virus?

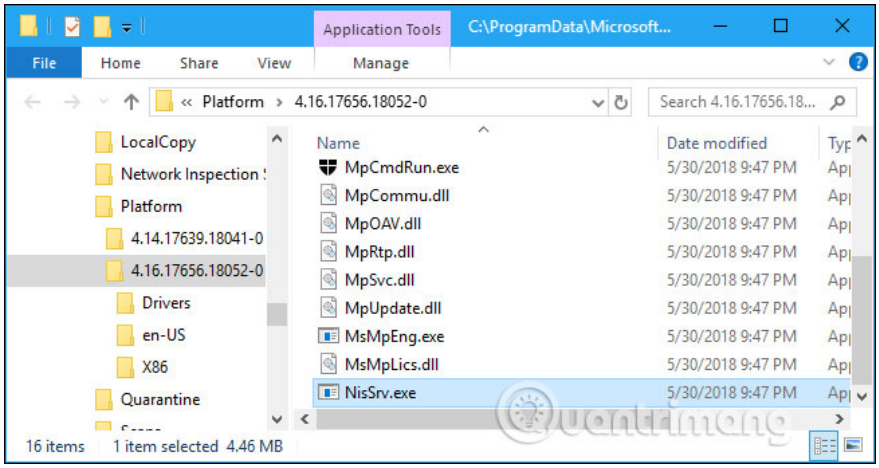
This software is not a virus, it is part of Windows 10 operating system and is installed on Windows 7 if you have Microsoft Security Essentials on the system. It can also be installed as part of other Microsoft anti-malware tools, such as Microsoft System Center Endpoint Protection.

Viruses and other malware often try to hide themselves into legitimate processes, but there have not been any reports of malware impersonating the NisSrv.exe process. This is the way to check the file is legitimate if you are interested.

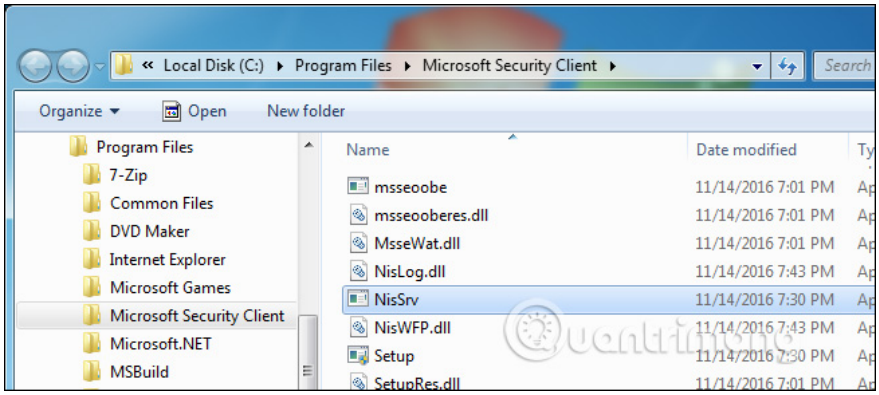
On Windows 10, right-click on the ' **Microsoft Network Realtime Inspection Service** ' process in **Task Manager** and select ' **Open File Location** '.



On the latest versions of Windows 10, you will see the process in a directory like **C: ProgramDataMicrosoftWindows DefenderPlatform4.16.17656.18052-0** , although the number of directories may be different.



On Windows 7, the NisSrv.exe file will appear in **C: Program FilesMicrosoft Security Client** .



If the NisSrv.exe file is in a different location or if you are in doubt, scan your computer with your favorite antivirus software.

See more:

1. Learn the Windows Modules Installer Worker process
2. What is the Client Server Runtime Process or csrss.exe and why does it run on the computer?
3. What is the Host Process for Windows Tasks and why does it run much on the computer?

You finished reading the article "**What is the Microsoft Network Realtime Inspection Service (NisSrv.exe) 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.