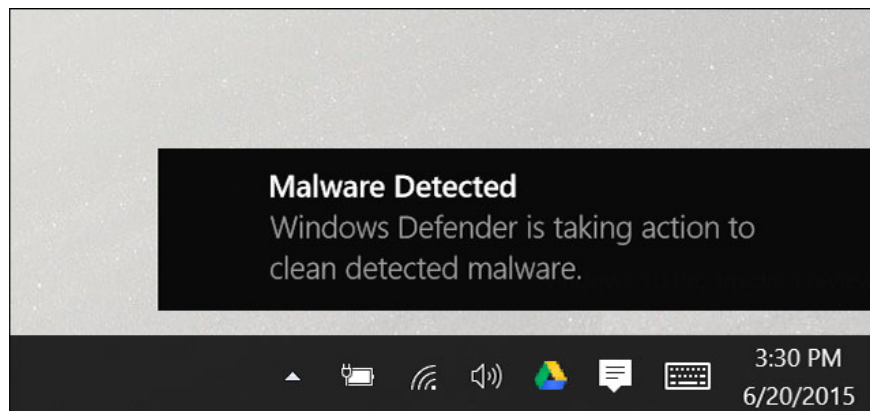


Instructions for using Windows Defender

As we all know, Windows 10 has a built-in real-time anti-virus program called Windows Defender and actual testing shows that this tool works relatively effectively.

As we all know, Windows 10 has a built-in real-time anti-virus program called Windows Defender and actual testing shows that this tool works relatively effectively. By default, Windows Defender will automatically be launched to run in the background to ensure all Windows users, from advanced to universal, can be protected from viruses and other security errors completely. Here's how Windows Defender works.

Starting from Creators update for Windows 10, Windows Defender's interface has been changed a bit as well as being integrated into the Windows Defender Security Center for that result, providing users with access to security tools. Security such as family protection, firewall installation, stable device performance and browser security controls. If you haven't updated your Creators version for Windows 10, don't worry, Windows Defender will still work as usual.

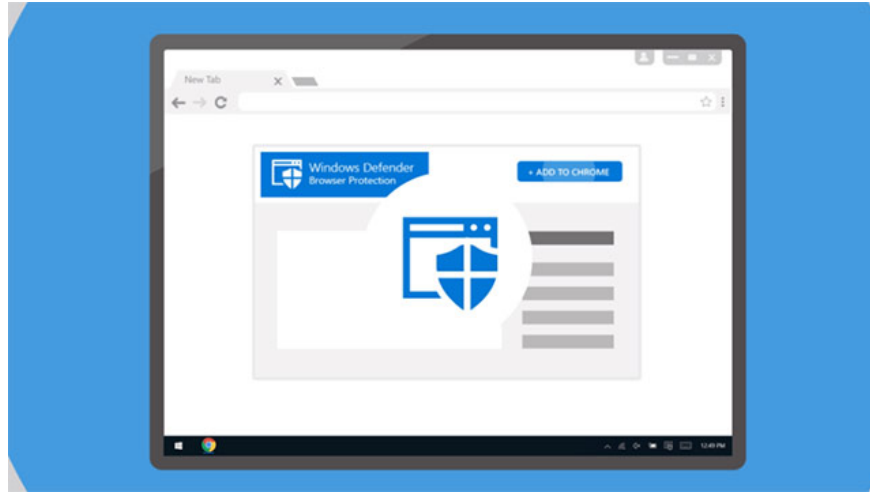


1. How to kill viruses with Windows Defender Offline on Windows 10 Creators

Windows Defender

1. What is Windows Defender?
2. Take advantage of the automatic scanning and updating features
3. See the scan history and the quarantined malware
4. How to perform manual scanning
5. Configure anti-virus protection settings and threats
6. Setup scans some specific folders or files
7. What will Windows Defender do if you install another Antivirus software?

What is Windows Defender?



In the past, Microsoft has developed a standalone antivirus application called Microsoft Security Essentials, and this tool actually works well in Windows XP, Vista and Windows 7. Until Windows 8, Microsoft Security Essentials has been tweaked and developed a bit more, built into new Windows versions and renamed Windows Defender. And of course, due to various security tasks, you cannot expect Windows Defender to work exceptionally perfectly with each feature. Simple example, Windows Defender's anti-virus and anti-virus capabilities are not as good as other specialized software such as BitDefender and Kaspersky. Anyway, Windows Defender is just a comprehensive security tool built in and completely free.

But Windows Defender also has certain advantages. It can be said that Windows Defender is one of the few security applications that will affect most other tasks because it handles everything in the background whenever possible and therefore, will not make you uncomfortable. Windows Defender also 'plays better' than web browsers and other security applications. It respects the security and privacy settings of users more than most anti-virus software appears on the market.

Take advantage of the automatic scanning and updating features

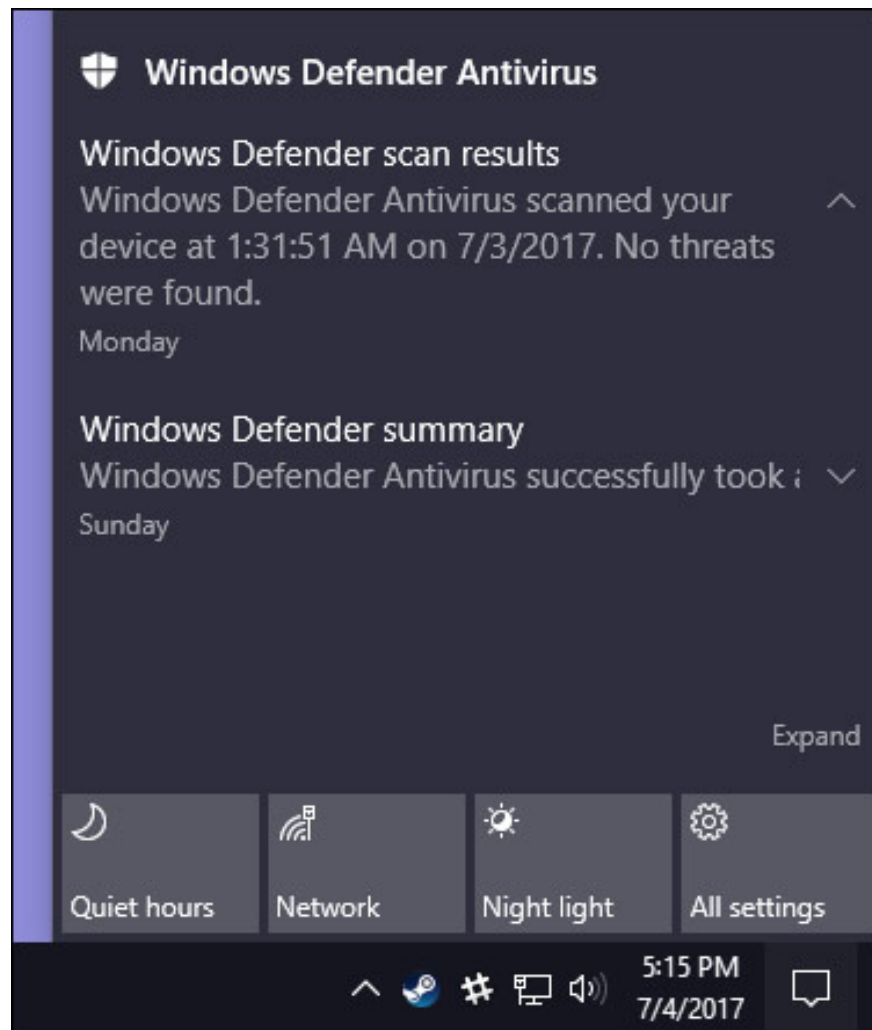
Which security tool to use depends on you, but make sure Windows Defender is not a bad choice (and in fact, most complaints about Windows Defender have been listened to and addressed by Microsoft, relatively thorough from a few years ago). However, for those who often need to work with important data as well as need for more in-depth security, it's best to use proprietary and proprietary anti-malware applications, such as Malwarebytes or Kaspersky. It will bring more obvious effect.

Like other antivirus applications, Windows Defender automatically runs in the background, automatically scans files when they are downloaded, transferred from removable drives to the system and before you open them.

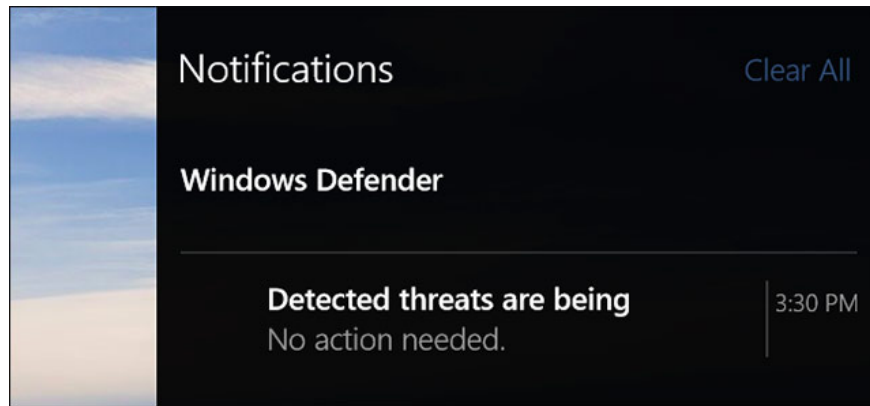
You really don't need to care much about Windows Defender when it is run in the background. Windows Defender will only show up to notify you when it finds any malware. It won't even ask if you want to handle the malware found. Windows Defender simply cleans everything and quarantines malicious files completely.

automatically.

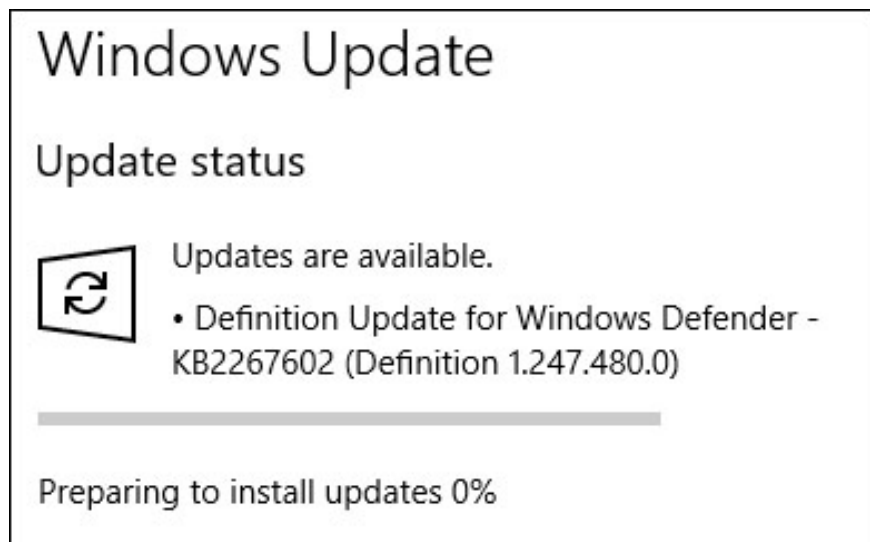
Sometimes you will see the Windows Defender window pop up to let you know when the scan is done and usually you can see details about the last scan by accessing the Action Center. in Windows 10.



If after the scan that Windows Defender found no threat, you will also see a message stating that it is taking the necessary actions to clean up the existing and potential threats, and you will No need to do anything because Windows Defender is a fully automated tool!

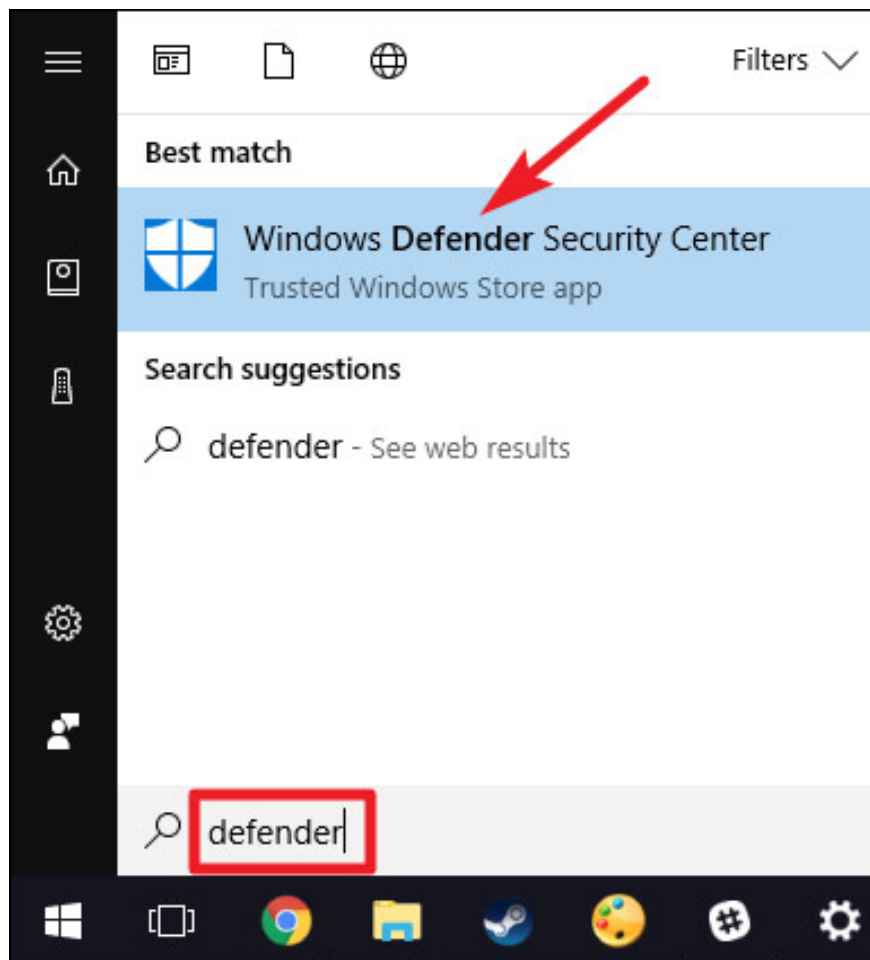


Automatic antivirus updates will be sent to you via Windows Update and installed like any other system update. Updates of this type usually do not require you to restart the computer. That way, you don't need to worry about updating Windows Defender, since all has been handled quietly and automatically in the background of the system.

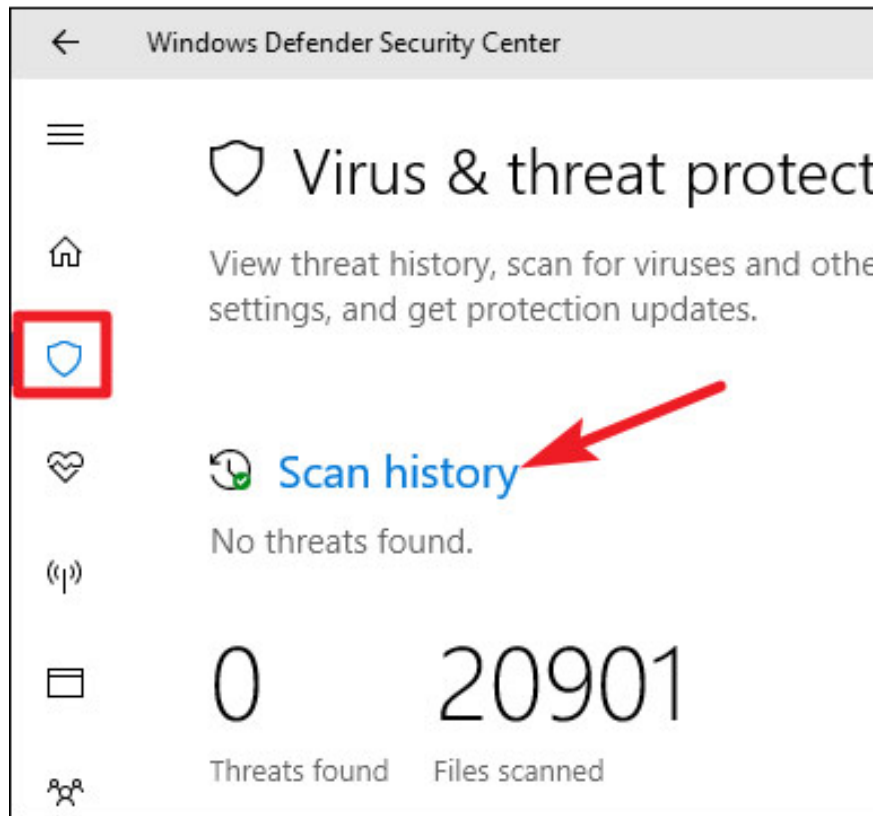


See the scan history and the quarantined malware

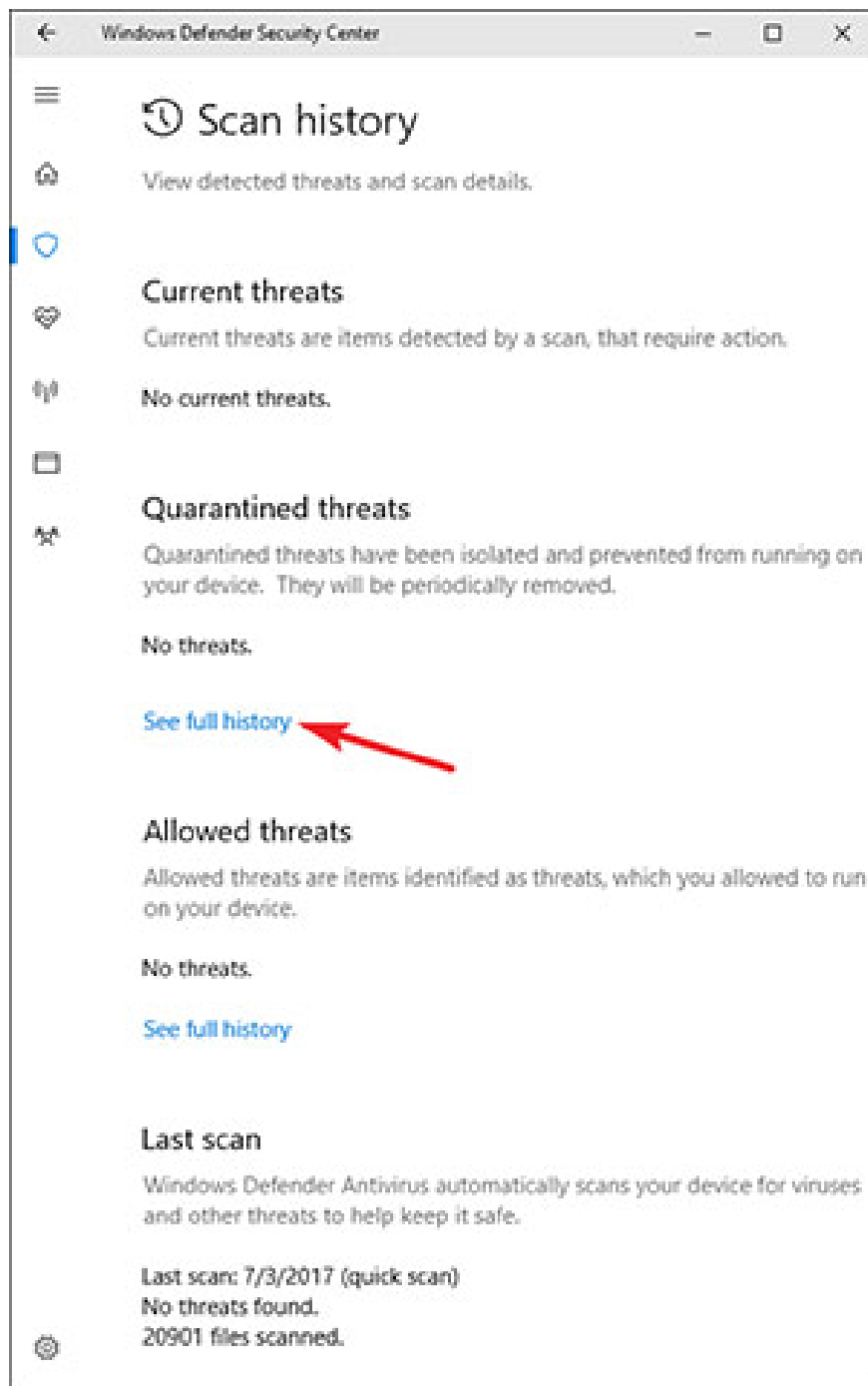
You can view the scan history of Windows Defender at any time if you want and if you are informed that some malware has been blocked, you can also see specific information about these software. To activate **Windows Defender Security Center**, simply press Start, type the keyword 'defender' into the search box and then select **Windows Defender Security Center**.



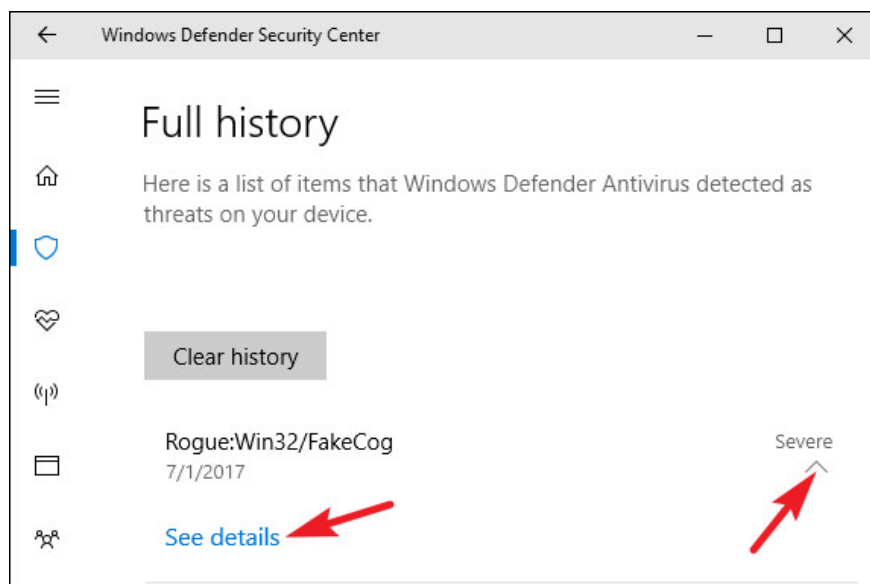
In the **Windows Defender Security Center** window, switch to the **Windows Defender** tab (shield icon) and then click the link that reads **Scan history** .



Scan history window will open and show you information about all existing threats, plus information about the last scan of Windows Defender. If you want to see the entire history of quarantined threats, just click the **See full history link** located in **Scan history** .



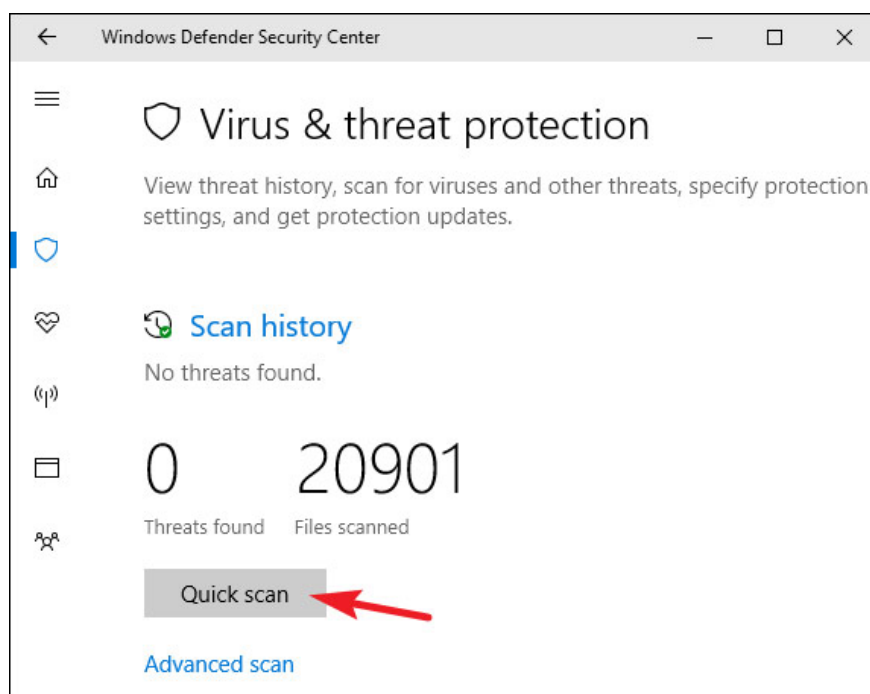
Here, you can see all the threats Windows Defender has successfully quarantined. To display more lists of threats, click the arrow to the right. And to see detailed information about each specific threat, click the **See details** link.



You don't really need to do anything else here, but if Windows Defender does not automatically delete threats when it is found, you will also be given the option to do this. In addition, you can also restore an item from the quarantine, but you should only do this when you are absolutely sure that the item is not a malware. Don't rush to do anything if you're not 100% sure about it!

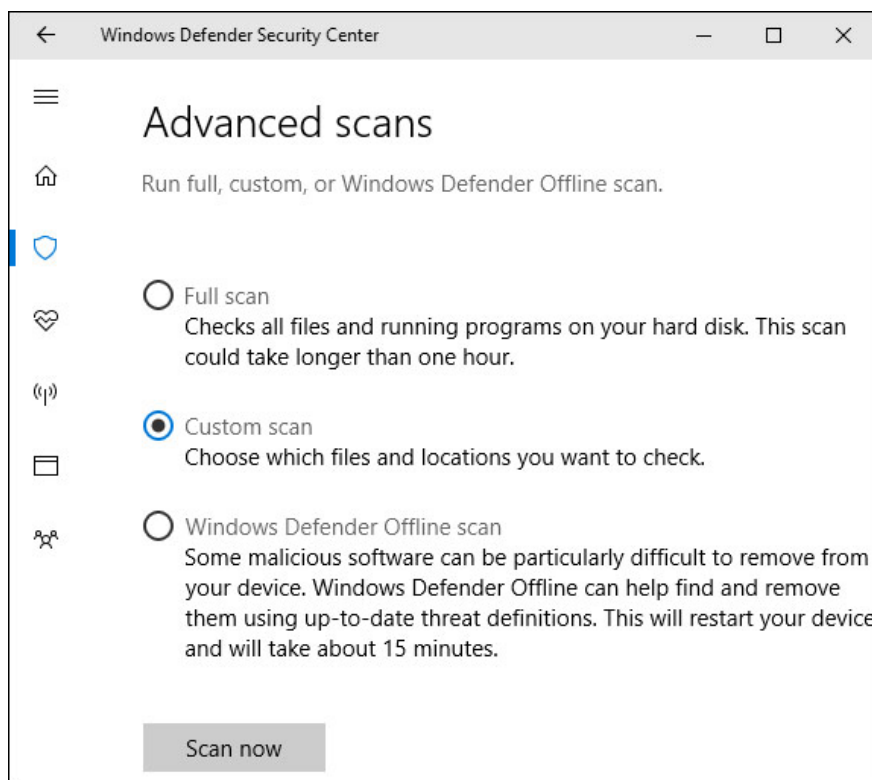
How to perform manual scanning

Back to the main tab is **Windows Defender**, you can also install Windows Defender to run the manual scan quickly by clicking the **Quick Scan** button. Normally, you will not need to bother with this because Windows Defender provides real-time protection and also conducts regular automatic scans. However, if you want something more secure, for example, performing manual scans doesn't hurt!



Alternatively, you can click on the **Advanced scan** link on the screen to run three different types of scans, including:

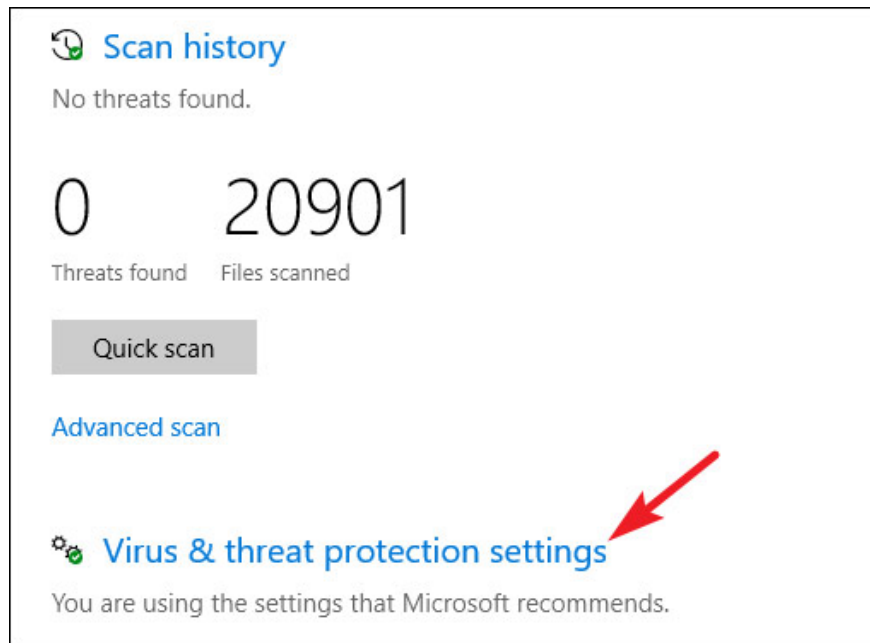
1. **Full scan:** With fast scanning, Windows Defender will only perform scans on your memory as well as other generic locations, while a full scan will carefully check every file and program being running on the system, so this scan mode can easily take up to an hour or longer. It's best to do this when you're not planning to use your computer much, or during a break.
2. **Custom scan:** Custom scanning allows you to select a specific folder to scan. You can also do this by right-clicking any folder on your PC and selecting the **Scan with Windows Defender option** in the menu.
3. **Offline Scan (Windows Defender Offline scan):** Some malware is hard to remove while Windows is running. When you choose offline scanning, Windows will restart and run the scanner before being loaded on the PC.



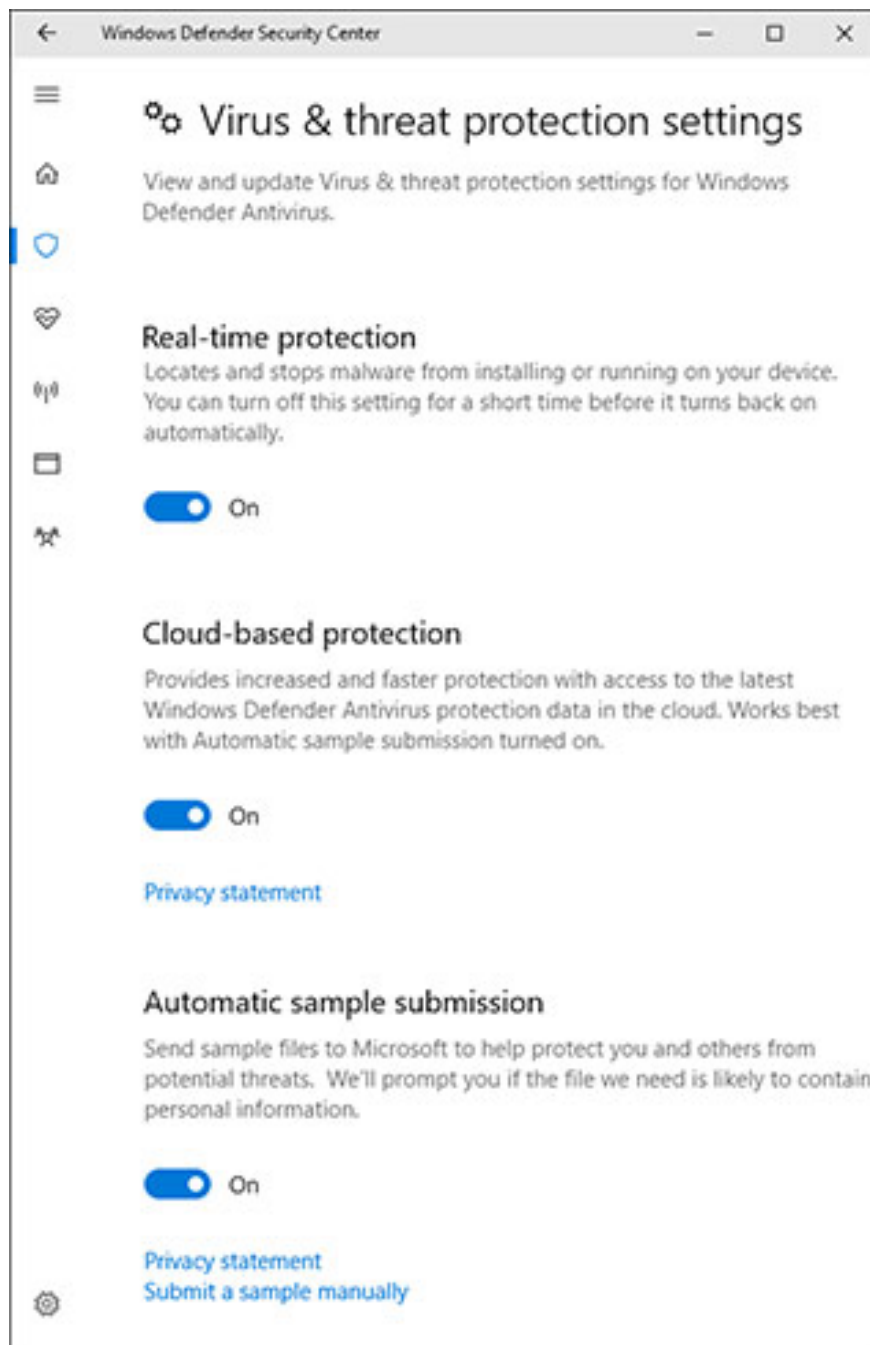
Configure anti-virus protection settings and threats

By default, Windows Defender automatically sets up real-time protection, cloud-based protection and sends templates. Real-time protection will ensure Windows Defender can automatically find malware by scanning your system in real time. You can turn this feature off for a short time if necessary for performance reasons, but note that Windows Defender will automatically turn on real-time protection to keep you safe. All right after that. Cloud-based protection and submission allows Windows Defender to share information about the actual malware threats and files it has detected with Microsoft so that the publisher will have moves to support users and find ways to overcome malware in the future.

To enable or disable any of these settings, click the **Virus & threat protection settings link** on the **Windows Defender** tab.



And then switch the settings that appear on the screen.



Setup scans some specific folders or files

If you scroll down to the bottom of the same **Virus & threat protection settings page** , you will see an exception set for some files, folders, file types or processes that you do not want Windows Defender to scan. Just click the **Add or remove exclusions link**.

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

[Privacy statement](#)

[Submit a sample manually](#)

Exclusions

Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.

[Add or remove exclusions](#)



If the antivirus feature significantly affects the response rate of a particular application, it is important to make sure that the application is completely clean, set Windows Defender to not scan the application. use it again, this will greatly improve the application response speed.If you use a virtual machine, you may also want to exclude large files from the Windows Defender scanning process.If you own a large image or video library that you know is safe, there is no need to scan because the virus scan will slow down the application in particular and the system in general.

To add exceptions, click the **Add an exclusion** button , in the menu that appears, select the type of data you want to apply and then point Windows Defender to any item you want to exclude.

Exclusions

Add or remove items that you want to exclude from Windows Defender Antivirus scans.

Add an exclusion

File
Folder
File type
Process



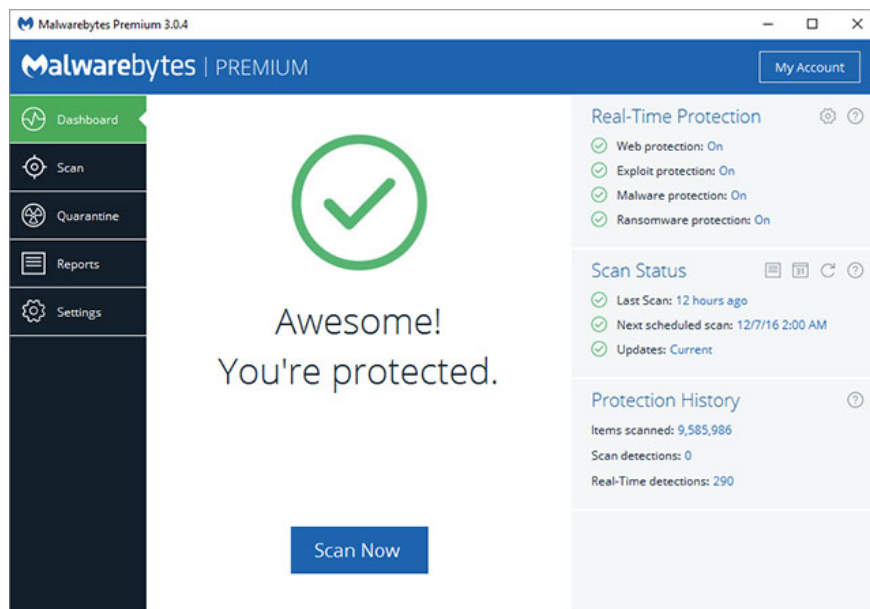
Be careful in using this selective scanning feature.In short, you should only make exceptions for files that you make sure it's really safe.

What will Windows Defender do if you install another Antivirus software?

Windows 10 will automatically disable Windows Defender if you install another antivirus application. Specifically, while another antivirus application is installed, Windows Defender will not continue to deploy scans in real time, so it will not interfere with your other applications. However, you can still use Windows Defender to perform manual or offline scanning, then use the Windows Defender scanner as a backup feature, to complement the tool. Your main antivirus.

If you uninstall third-party antivirus software, Windows Defender will automatically activate and take over your device again, providing normal antivirus protection.

However, note that some anti-malware applications such as Malwarebytes can be installed and run in tandem with Windows Defender and both will provide real-time protection for you.



summary

Regardless of which antivirus product you prefer, the built-in antivirus protectors like Windows Defender are not bad. Although it may not be perfect, but at least know how to do your job well, less impact on users, and furthermore, is very well compatible with other safe browsing and computing methods. of the publisher, while for the majority of computer users today, such features can be said to be more than enough.

Wish you build yourself an optimal protection system!

See more:

1. How to do, customize in the article will help your Windows 10 "as fast as the wind"
2. Ways to troubleshoot audio on Windows 10
3. Vietnamese translation for Windows 10
4. Fix keyboard error not working on Windows 10

You finished reading the article "**Instructions for using Windows Defender**" 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.
