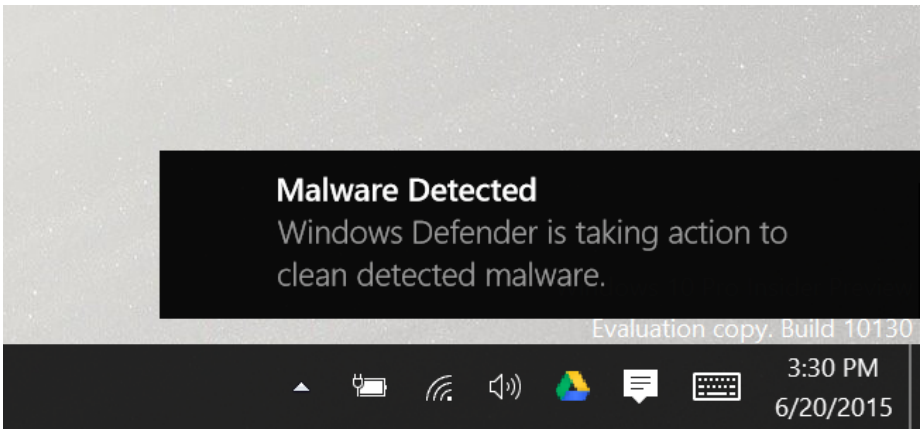
How to Use the Built-in Windows Defender Antivirus on Windows 10



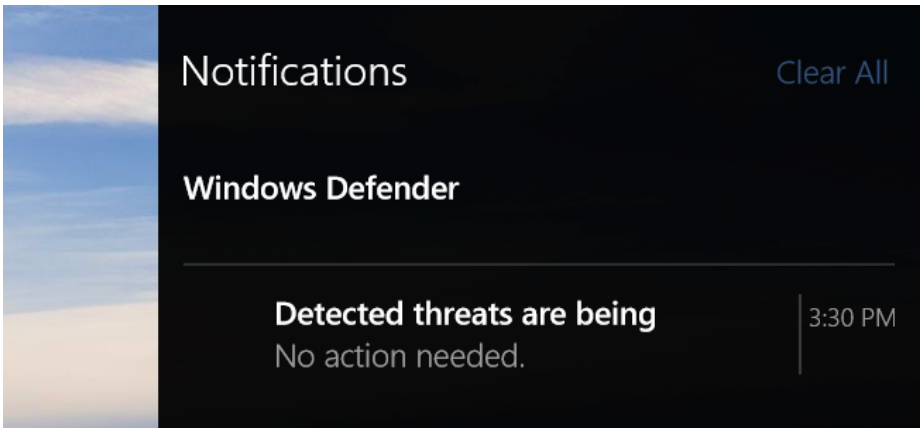
Windows 10 has built-in real-time antivirus, just as Windows 8 did. It automatically runs in the background, ensuring all Windows users have a baseline level of antivirus protection. Windows 10 won't complain at you to install an antivirus, as Windows 7 did.

If you've used Microsoft Security Essentials on Windows 7 or previous versions of Windows, this is the same basic product. It was renamed to "Windows Defender" in Windows 8 and integrated into Windows itself.

Automatic Scans and Updates

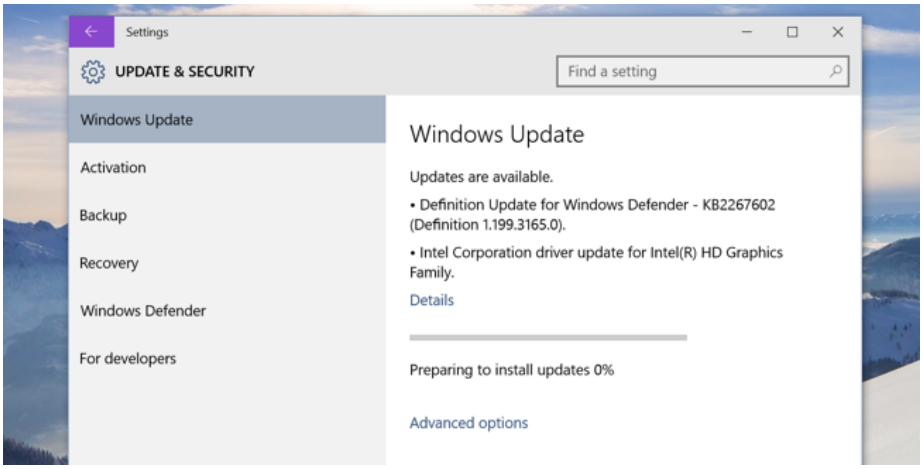
Like other anti-malware applications, Windows Defender automatically runs in the background, scanning files when they're accessed and before you open them.

You don't really have to think about Windows Defender at all. It will only pop up and inform you when it finds malware. It won't even ask you what you want to do with the malicious software it finds — it will clean it up and quarantine the files automatically. You'll see a "Malware detected" notification saying "Windows Defender is taking action to clean detected malware" or "Detected threats are being cleaned." It'll appear in the notification center, too.



Antivirus definition updates will automatically arrive through Windows Update and be installed like any other system

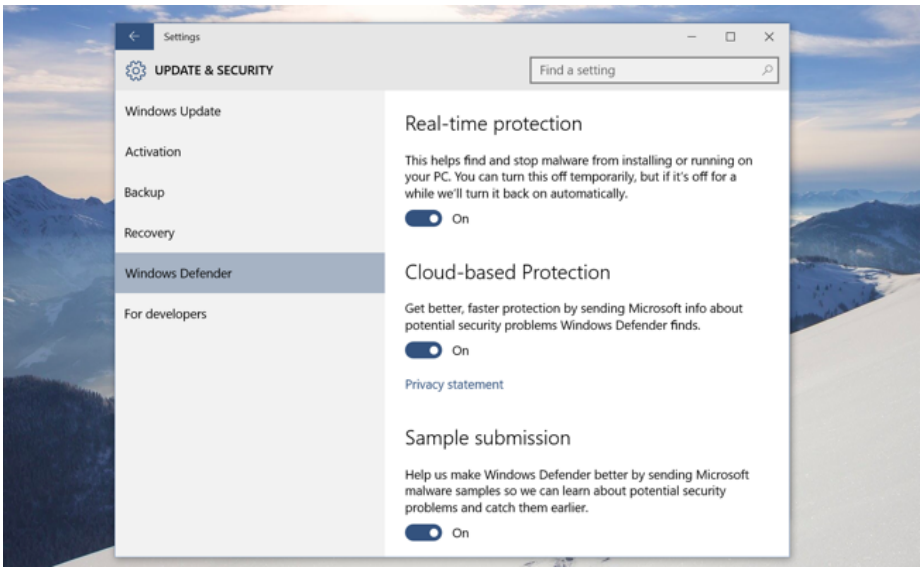
update. These types of updates don't require rebooting your computer. You don't need to worry about updating Windows Defender.



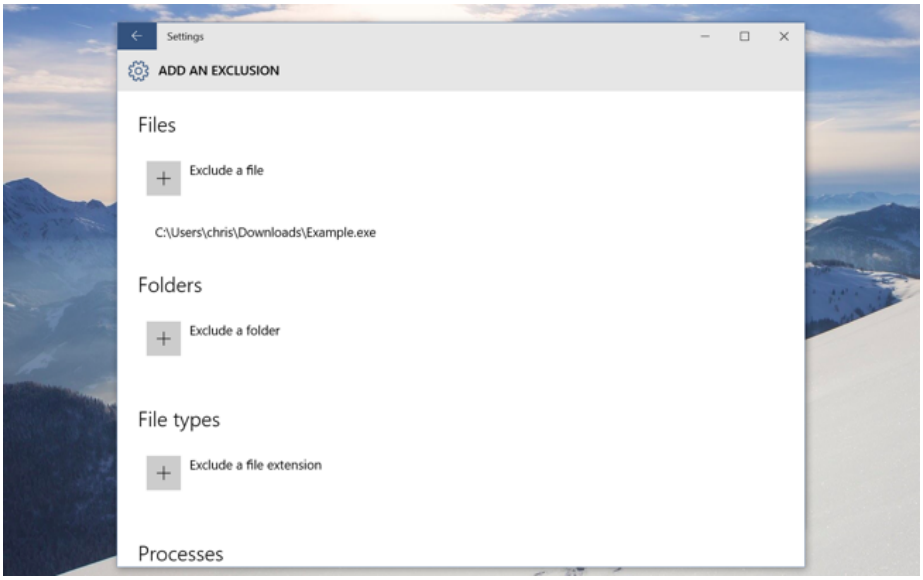
Configuration and Exclusions

Windows Defender settings are now integrated into Windows 10's new Settings app. To access it, open the Start menu and select Settings. Choose the "Update & security" category and select Windows Defender.

By default, Windows Defender automatically enables real-time protection, cloud-based protection, and sample submission. Real-time protection ensures Windows Defender automatically finds malware by scanning your system in real time. You could disable this for a short period of time if necessary for performance reasons, but Windows Defender will automatically re-enable real-time protection to keep you safe later. Cloud-based protection and sample submission allow Windows Defender to share information about threats and the actual malware files it detects with Microsoft.



You can also set Exclusions from here — scroll down and select "Add an exclusion." Exclusions can be specific files, folders, file types, and processes. If the antivirus is dramatically slowing down a certain application you know is safe by scanning it, this can speed things up again. Be careful to use exclusions sparingly and smartly — these reduce your PC's security because they tell Windows Defender not to look in certain places.

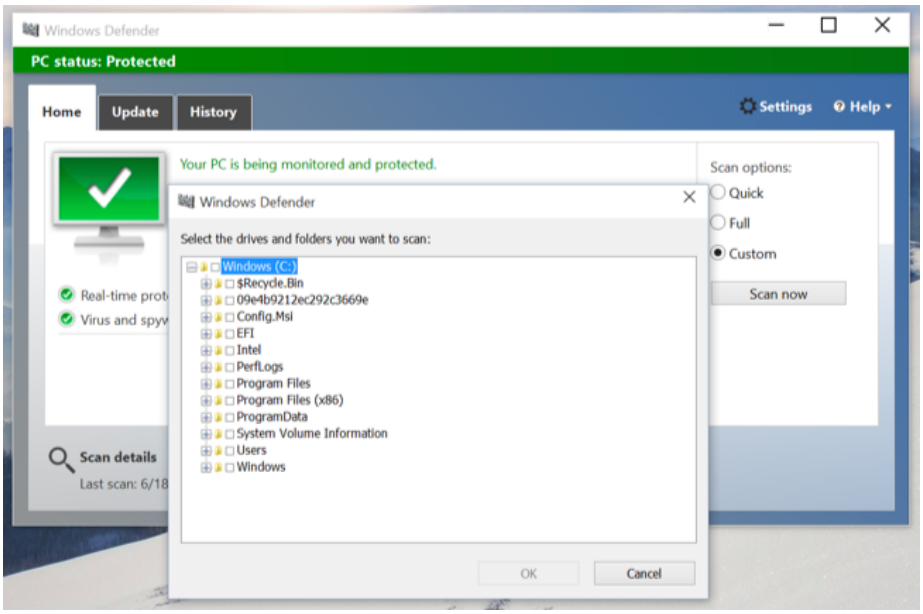


Manual Scans

Scroll down to the Version info section at the bottom of the Windows Defender pane in the Settings window and click "Use Windows Defender" to access the Windows Defender desktop app interface. If you've used Microsoft Security Essentials before, you'll immediately recognize this. (We can probably expect Microsoft to move more of the options here to the Windows Defender pane in the Settings app over time.)

From this window, you can initiate a quick scan, full system scan, or a custom scan of specific folders. For example, you could connect an external hard drive to your computer and perform a Custom scan to scan that entire drive for malware.

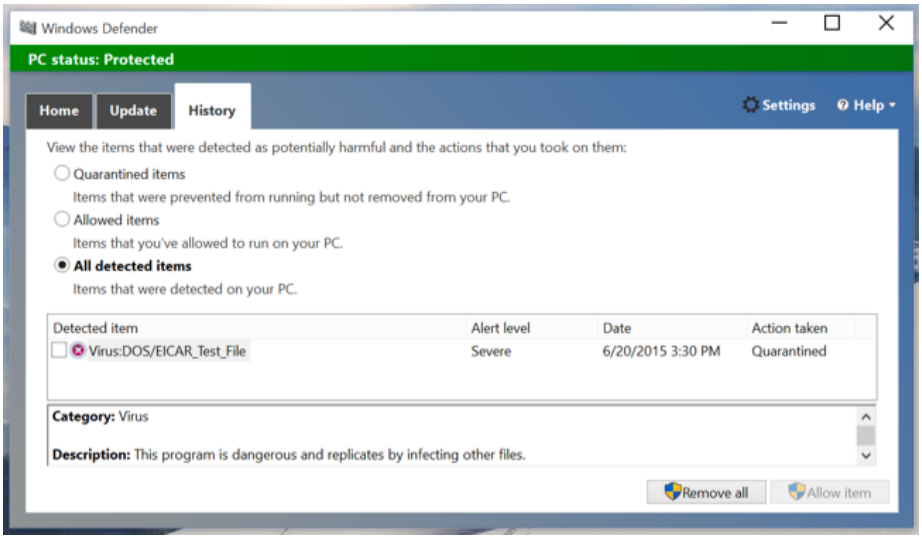
You shouldn't have to regularly perform manual antivirus scans. Windows Defender scans everything in the background anyway, and there's even a scheduled task in Windows that automatically scans your computer on a regular basis. This feature is mostly useful for scanning external media and network locations.



Viewing Quarantined Malware

If Windows Defender informs you that it's blocked malware, you can view the blocked malware from the Windows Defender desktop app. Click the "use Windows Defender" link in the Settings app to access Windows Defender, and then click over to the History tab. Click "View details" to view detected malware. You can see the name of the malware and when it was found and quarantined.

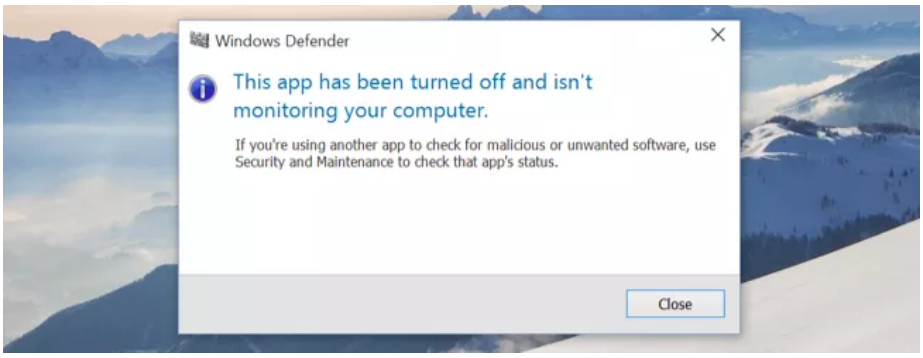
From here, you can remove the malware to delete it entirely from your PC or allow the supposedly malicious file to run. You should only do this if you're absolutely sure the detected malware is a false positive. If you're not absolutely, 100 percent sure, don't allow it to run.



What if You Install Another Antivirus?

Windows 10 will automatically disable Windows Defender if you install another anti-malware program. It won't continue performing real-time scans, so it won't interfere with your other antivirus. Try to open the Windows Defender settings pane with another antivirus installed and you'll find every option grayed out. Click the "Use Windows Defender" link and you'll be informed Windows Defender has been disabled. Windows Defender will pop-up and say "This app has been turned off and isn't monitoring your computer."

If you uninstall the other antivirus, Windows Defender will kick into gear once again and take over, providing antivirus protection.



Whichever antivirus product you prefer, it's good that every single new Windows installation going forward will come with built-in antivirus protection. The Malicious Software Removal Tool Microsoft occasionally delivers through Windows Update is no substitute for a proper anti-malware application.

JOIN THE DISCUSSION (9 REPLIES)

Chris Hoffman is a technology writer and all-around computer geek. He's as at home using the Linux terminal as he is digging into the Windows registry. Connect with him on Google+.

- Published 06/27/15