What Is the SFC and How Do I Run It?

by Leo A. Notenboom https://askleo.com

The System File Checker is a little-known, simple-to-run command-line program. It validates that Window's operating files are undamaged.

In order to prevent malware from replacing critical system components with compromised copies, Windows works very hard to maintain the integrity of the system files on your machine. If you try to replace one of the "protected" files, you may get a message that the operating system has put the old approved version back. That's "Windows File Protection", now called "Windows Resource Protection".

Unfortunately, there are occasional ways around system file protection. Sometimes it's as simple as a hard disk error causing a system file to be damaged and become corrupt.

As a result, automated checking is nice, but sometimes you need to take matters into your own hands.

Enter the **SFC**, the System File Checker.

System file protection

The basic premise behind system file protection is that Windows keeps additional information about all the files that are part of Windows. That additional information could be (but certainly isn't limited to) the date/time stamp of the file, its size, and its cryptographic hash. When files are "officially" replaced (or updated by Windows Update), this database of information is also updated to reflect the new official files.

Every so often, Windows checks all those files to make sure they still match. That means that the time stamp, size, and hash value match what is expected. If they don't … well, then something is wrong, and Windows will likely report the error.

Unfortunately, "wrong" can be the result of many different things:

- Malware. Malware was one of the reasons system file protection was implemented in the first place. Malicious software would inject itself into the system by modifying Window's own files. System file protection detects when this happens.
- Set-up programs often replace system components with their own, sometimes breaking things. System file protection notices when this happens.
- Random other failures.

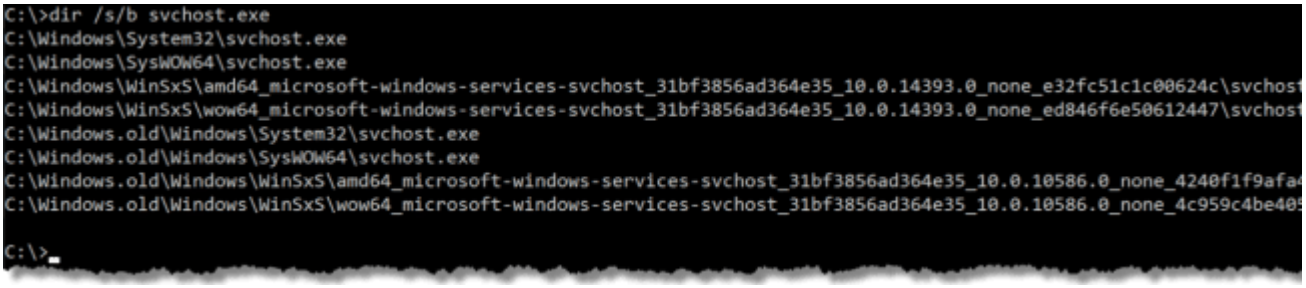
So, what happens when a problem is found?

Repairing altered files

If you've ever searched for a system file on Windows, it's not uncommon to find *several* copies:

- The original file, used by Windows.
- Previous versions of the file saved by Windows Update, so you can uninstall specific updates if needed.
- Cached copies of the file, kept as a performance enhancement that loads the file more quickly when needed.
- Back-up copies of the file.

It's that last one that would be used to restore the file to its original state should something happen.



In addition, many systems now include a copy of Windows on a restore or recovery partition, which can also be used as a source for retrieving original copies of files that need to be restored.

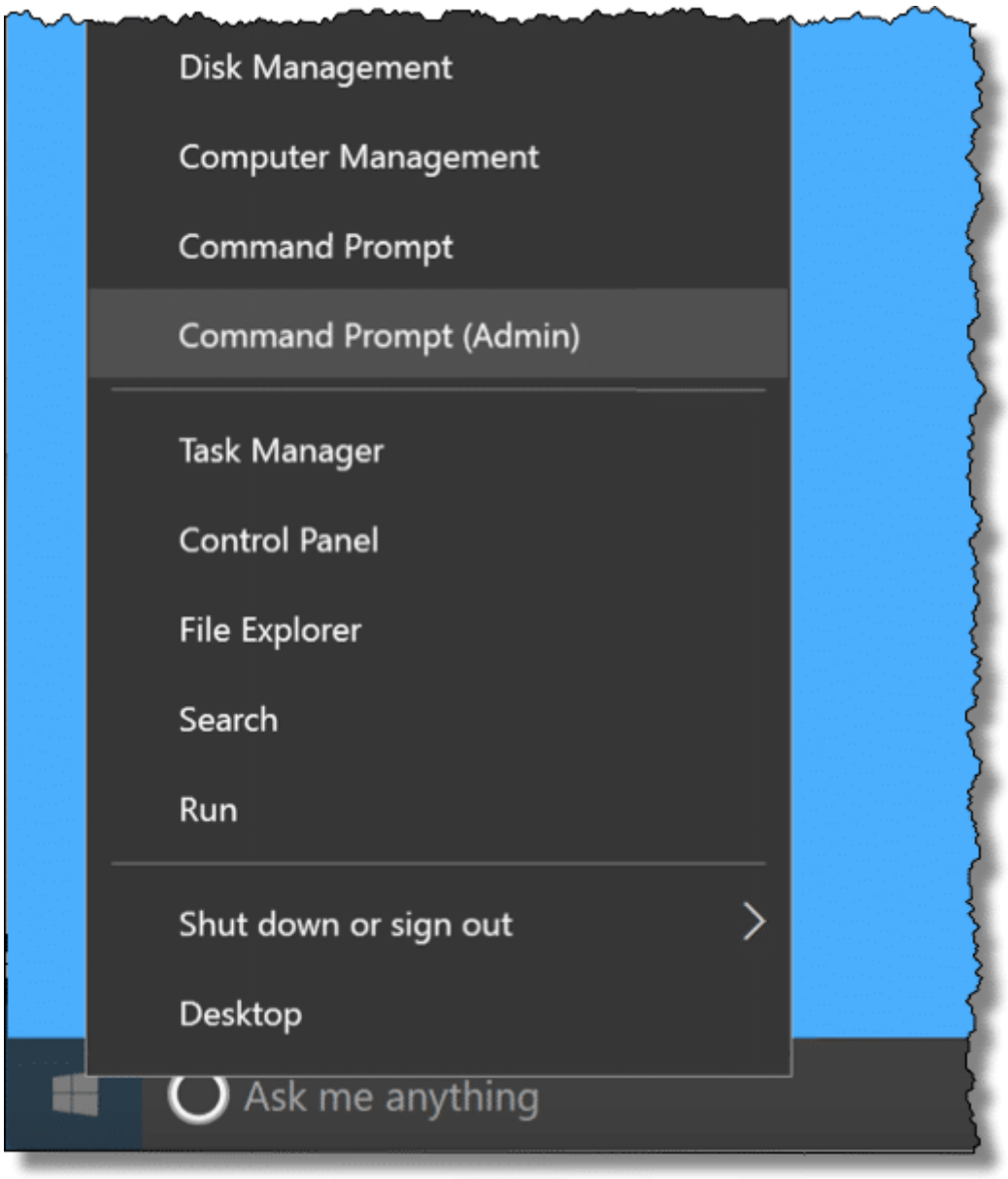
When all else fails, the original Windows installation media might be used, if you have it.

In all cases, the repair process also checks that the copy it's restoring is correct. If it fails to have the expected information, it will be skipped. Because many of those sources are on your hard disk, malware authors attempt to replace or damage them all to prevent the repair process from working.

SFC – the System File Checker

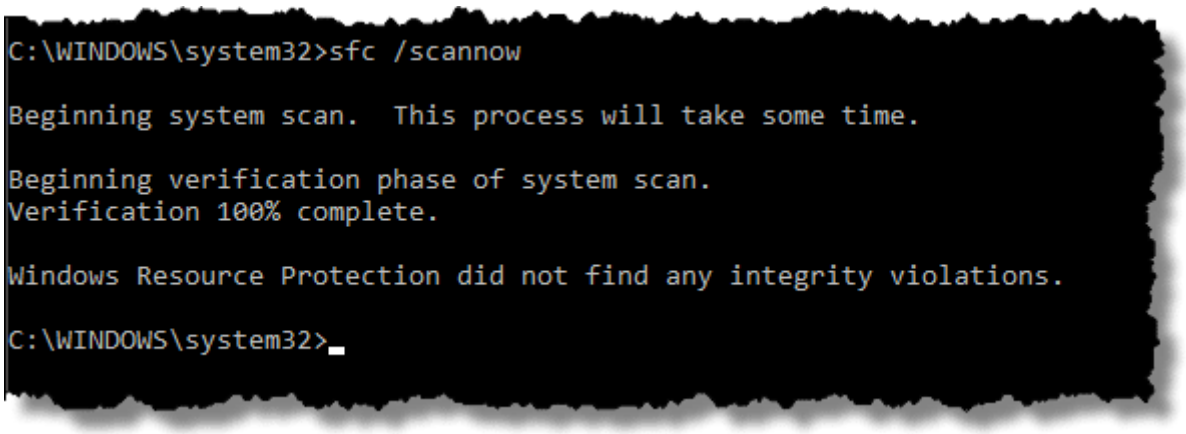
SFC is nothing more than a command-line tool that checks that all of the files covered by Windows system file protection are as they should be, and to try to repair those that are not. It's a good utility to run when you suspect system files have been somehow corrupted, or even if you just think there's "something wrong" with your system.

SFC requires administrative privileges. Right click on the start button, and click on **Command Prompt (Admin)**.



(In earlier versions of Windows, locate the Command Prompt menu item in **Start**, **All Programs**, **Accessories;** then right-click Command Prompt and click **Run as administrator**.)

After confirming any UAC prompts, type "sfc /scannow" in the Command Prompt and press **Enter**.



This causes SFC to scan your system immediately. SFC can take several minutes to run. If you have installation media, such as a DVD, you might have it available, just in case SFC wants to replace a damaged file.

While it's not documented anywhere, I'd reboot your machine if SFC replaces any system files. Why? I just like to be sure that the file replacement actually takes effect.

Microsoft has more detailed SFC documentation, including more options to check at boot time, control the size of the system file protection cache, and so on. There is also Windows Resource Protection documentation, which covers the mechanism Windows uses to keep your system files (and a few other things) safe automatically.