

## Re: scan for file corruption

**Source:**

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.newusers/2005-02/0618.html>

---

**From:** Venom (*Venom\_at\_discussions.microsoft.com*)

**Date:** 02/03/05

Date: Thu, 3 Feb 2005 05:19:02 -0800

Introduction to using scannow sfc (system file checker)

Windows XP has the ability to protect itself from system instability caused by 3rd party software overwriting important system files. This used to be (and still is in fact), a problem with Windows 95 and Windows 98.

With the introduction of Windows Millennium Edition, Microsoft made a real effort to stop this from happening. Now in Windows XP we have a much more refined protection of these important files.... This system is called:

### Windows File Protection

By default, Windows File Protection is always enabled and allows Windows digitally signed files to replace existing files safely. Currently, signed files are distributed through:

- # Windows Service Packs
- # Hotfix distributions
- # Operating system upgrades
- # Windows Update
- # Windows Device Manager

If you introduce a file replacement in any other way, Windows File protection will overwrite your file!

An important part of Windows File Protection is the command line utility:

## System File Checker (sfc.exe)

You will often see references to scannow sfc in online newsgroups etc. This is a great tool for troubleshooting Windows XP problems.

### How to use scannow sfc...

The main reason for using this utility is when you suspect there may be a problem with a Windows XP system file.

Perhaps you get a dialog box appear informing you of a problem with a .dll file, or your program will just not load! It is therefore worth checking to see if there are any corrupt system files using scannow sfc.

To do this simply go to the Run box on the Start Menu and type in:

```
sfc /scannow
```

This command will immediately initiate the Windows File Protection service to scan all protected files and verify their integrity, replacing any files with which it finds a problem.

The following should appear to give an indication of how long the process is taking.

In an ideal world that would be the end of the story... Any corrupt, missing or incorrect files would be replaced by this process.

However, things can go wrong and the following guide should help!

The #1 complaint with scannow sfc is the following dialog box appearing:

Why does this happen?

Well, in your computer's registry, are several settings that are checked when you run scannow sfc.

As mentioned earlier in this article, the Windows File Protection service constantly monitors for any changes to the main system files. Well Windows XP keeps a cache (copy) of these essential files at the following location:

C:\WINDOWS\System32\Dllcache (assuming C: is your system root which it probably is.)

NB – The dllcache folder is extremely important so Windows XP hides it from you! To view it go to: My Computer > Tools > Folder Options > View > "uncheck" Hide protected operating system files.

If that's the case on your computer then there is normally no need for the original XP CD to be inserted as your computer has a "copy" it can get hold of in this cache...

But, if the Dllcache folder, or part of it, has become corrupted for some reason then you will be prompted for the XP CD – so your computer can get a clean copy!

Having said that not ALL installations of Windows XP have ALL the system files cached into this folder! You may only have around 50MB of files in this folder under Windows XP depending on the quota settings in the registry. (Under Windows 2003 Server the default is 300MB of system files!)

Annoying, YES!

Is there a workaround YES!

As well as having a cache of all the system files on your PC, I like to have the I386 folder from the XP CD installed on the computer as well. After doing this I then modify the registry to tell it the source path for these files... Why? Well not only does this prevent 99% of request for the the XP CD with Windows File Protection. But the I386 folder also contains many other files that are sometimes needed by the operating system and this stops those requests for the XP CD too!

NB – With today's large hard drives you are not going to notice this 475 MB folder on your computer, but older systems may not have the space for this...

Step 1

You will need to get your XP CD and locate the folder called:

I386

This is a major folder and should be one of the first you see, now copy this onto your hard drive into the system root. For most of you that is going to be C:\ so you should end up with a folder that looks like:

C:\WINDOWS\DLLCACHE

---

Step 2

Now you will need to tell your computer you now have the files on your PC. We do this in the registry (type regedit in the Run box on the start menu) by navigating to:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup

You will see various entries here on the right hand side. The one we want is called:

SourcePath

It probably has an entry pointing to your CD-ROM drive, and that is why it is asking for the XP CD. All we need to do is change it to:

C:\

Simply double click the SourcePath setting and a new box will pop up allowing you to make the change.

Now restart your computer and try scannow sfc again!

---

Other Problems with scannow sfc...

#1

Has the CD Drive's drive letter changed (perhaps by the addition of another hard drive, partition, or removable drive) since Windows XP was first installed? If so, simply edit the registry key

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\SourcePath to reflect the changed drive letter.

After you restart the computer, WFP and sfc /scannow uses the new source path instead of prompting for the Windows XP installation CD-ROM

#2

Has the registry key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\SourcePath got an incorrect entry? The SourcePath entry does NOT include the path location till the I386 folder. It completes one folder ahead to reach the I386 folder.

Example:

If the I386 directory is at C:\I386, the SourcePath value would be C:\

#3

## microsoft.public.windowsxp.newusers: Re: scan for file corruption

If the problem persists and you have the correct path for your I386 folder then the I386 folder is corrupted. To solve this problem copy I386 folder from the CD-ROM to your system restart the system and then perform `sfc /scannow` again.

#4

You do not have an XP retail CD with an I386 folder on it. If you have a restore CD from your PC manufacturer then you may have to explore the CD to find the folder.

#5

You still keep being prompted for the XP CD yet you have done all in this article! There is another setting in the registry that may be causing the problem. Navigate to:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SourcePath

Make sure the entry here is the same path to the I386 folder as used above.

#6

Systems administrators can enforce security policies that may include changes to the Windows File Protection settings. You will need to speak with your network administrator about this, but it is important to bear in mind when Windows starts up, the Windows File Protection service synchronizes (copies) the WFP settings from the following registry key:

HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\Windows File Protection

to the following registry key:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Therefore, if any of the following values are present in the HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\Windows File Protection key, they will take precedence over the same values under the HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon key.

This will not effect `scannow` `sfc` so much, but WILL make an impact if any of the other `sfc.exe` "switches" have been used! (More about these at the end of this article.)

#7

When you run `scannow` at logon you do not get a progress bar... This can easily be remedied by adding a new DWORD: `SFCShowProgress` to the registry key:

microsoft.public.windowsxp.newusers: Re: scan for file corruption

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

the values available are: 0 = disabled, 1 = enabled

---

What about Windows Updates.....

You may be asking yourself how does sfc.exe know how to check for updated Windows system files? Well during OS upgrades, service pack installations etc.. the dllcache folder should be updated with these new files.

As an example the recent Windows XP Hotfix – KB828035 updated the system file wkssvc.dll A new version of the file was placed in C:\WINDOWS\system32 and a copy in the cache: C:\WINDOWS\system32\dllcache A copy of the old system file is archived in: C:\WINDOWS\\$\NtUninstallKB828035\$

There is another location the Windows File protection service uses and that is the I386 folder in C:\WINDOWS\ServicePackFiles When you install a service pack, like SP1. Any new system drivers are cached in this location too.

If you have odd problems with running scannow sfc and nothing else in the article has resolved it, then take a look at the entry in:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup  
\ServicePackSourcePath

This should be pointing to the location C:\WINDOWS\ServicePackFiles (assuming C:\ is the boot drive.)

---

For those of you who are familiar with sfc.exe under Windows 2000 professional. It is worth noting that the following two options are NOT available under Windows XP.

These are:

sfc /cancel – In Windows 2000, this command immediately cancels all pending scans of protected system files. This option has no effect in Windows XP.

sfc /quiet – In Windows 2000 this sets Windows File Protection to replace any incorrect system files detected with the appropriate version from the dll cache without any user notification. This option has no effect in Windows XP.

Thanks for reading this article  
on scannow sfc.

Re: scan for file corruption

Introduction to windows file protection...

The Windows File Protection "concept" was first introduced by Microsoft into the Windows Millennium operating system, as a way of stabilising the software. In Windows XP we have a much better version of this service and this article has been written to inform the reader of it's benefits.

For those of you who remember using Windows 95 and 98 computers, a frequent problem was the operating system become erratic or just completely freezing for no apparent reason.

Well, the often underlying cause of these woes was the unprotected system files being overwritten, corrupted or even deleted!

This led to most of the support issues and was often referred to as "DLL HELL" because things could get so bad...

Now with the Windows File Protection service in place technical support is much easier!

What is windows file protection...

The windows file protection service is an "invisible" service that is enabled by default and runs constantly in the background after a successful logon. (It does not load in safe mode.)

ALL SYS, DLL, EXE, and OCX files that ship on the Windows XP CD are protected. True Type fonts—Micros.ttf, Tahoma.ttf, and Tahoma.ttf – are also protected. They are all "backed up" to a special folder called dllcache. The location of this file is:

`%SYSTEMROOT%\system32\dllcache`

The dllcache folder is extremely important so Windows XP hides it from you! To view it go to: My Computer > Tools > Folder Options > View > "uncheck" Hide protected operating system files. This will also reveal other hidden system files so be careful! e.g. pagefile.sys

Windows File Protection works by detecting the replacement/overwriting of these system files. It then scans the file in question against several catalogue files it has access to (nt5.cat, nt5inf.cat etc...). Should the file not be the correct digitally signed version it is expecting, Windows File Protection will then replace it with the cached version stored in the %SYSTEMROOT%\system32\dllcache folder, or in cases where no cached version exists you may be prompted for the Windows XP CD in order to restore the file with a supported version.

To test this go to the dllcache folder yourself (probably C:\WINDOWS\system32\dllcache on your computer) and rename the file

Re: scan for file corruption

acctres.dll to acctress.dll

Close the explorer window and reopen at the same location. You will now see the windows file protection service has replaced the file acctres.dll (now delete acctress.dll)

This action is recorded in the system Log (via Event Viewer):

---

Event Type: Information  
Event Source: Windows File Protection  
Event Category: None  
Event ID: 64002  
Date: 28/12/2003  
Time: 15:37:42  
User: N/A  
Computer: MARCXP  
Description:  
File replacement was attempted on the protected system file acctres.dll.  
This file was restored to the original version to maintain system stability.  
The file version of the system file is 6.0.2600.0.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

---

Is Windows File Protection a good thing...

YES it IS!

It exists to protect the Windows system files from being modified, whether accidentally or otherwise. As a network administrator I am VERY pleased with this feature "no more running around fixing machines due to someone installing/deleting something they shouldn't have. You'd be surprised what people are told to delete in these email virus hoaxes that are being sent around. Another important reason for having this service running is Trojan/viruses that try to overwrite system files to then pass on information on your machine. If this happens windows file protection will kick in!

For software vendors writing software for Windows XP, they can no longer replace files on your PC as part of the install process. Part of the certification process to get the XP logo for their software products means vendors now have to follow strict rules about how software is installed. This is a GOOD thing!

What about when system files are updated by Microsoft...

If Windows File Protection protects system files then how exactly can they be updated with newer versions?

Well Microsoft has made the following methods Windows File Protection "aware" Meaning the newer files will replace the old system files and a copy

microsoft.public.windowsxp.newusers: Re: scan for file corruption

of the new file will be stored in the dllcache folder. The security catalogues are also updated so the Windows File Protection service always knows what version of the digitally signed file is current!

Replacement of protected system files is supported using the following mechanisms:

• Windows Service Pack installation (UPDATE.EXE) e.g. XP SP1a

• Hotfix distributions installed using (HOTFIX.EXE) e.g. KB825035

• Operating system upgrade (WINNT32.EXE)

• Windows Update Website

• Windows Device Installer

Can I turn off Windows File Protection...

The official answer from Microsoft is NO and this is by design. (The only exception is if you are using a kernel debugger.)

However, there is a way to do it, BUT I can think of no reason for you to do so!!!

On a close inspection of the system file sfc.dll it is possible to see a reference, in part of the code, that checks the value of the SFCDisable in the WinLogon key... (Something we talk about in a moment!)

This key is: 0ffffff9dh

This is NOT a documented feature from Microsoft and should NOT be used unless you REALLY are sure you need to disable the service!

(NB – It is interesting to note that the virus "W32/CodeRed.D", that caused so much mayhem by shutting down Internet Servers in the summer of 2002, used this very same undocumented setting to stop the Windows File protection service from running. The virus could then release its Trojan payload to do damage and replicate itself around the Internet!

The registry key to change is:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\SFCDisable
```

By default, SFCDisable is set to 0, which means Windows File Protection is active.

Setting SFCDisable to 1 will disable Windows File Protection . Setting SFCDisable to 2 will disable Windows File Protection for the next system restart only (without a prompt to re-enable).

Re: scan for file corruption

Important: You must have a kernel debugger attached to the system via null modem cable to use SFCDisable = 1 or SFCDisable = 2.

After Windows File Protection is disabled using the SFCDisable = 1 setting, the following message will appear after logon:

Warning! Windows File Protection is not active on this system. Would you like to enable Windows File Protection now? This will enable Windows File Protection until the next system restart. <Yes> <No>.

Clicking Yes will reactivate Windows File Protection until the next system restart. This message will appear at every successful logon until SFCDisable is set to 0.

NOTE: The above message will only be presented to Administrators.

To verify that Windows File Protection has been disabled after rebooting click on Start menu > Control Panel > Administrative Tools > Event Viewer.

An event will be logged to indicate Windows File Protection is disabled on the PC. If this event hasn't been logged in Event Viewer then the service has NOT been disabled...

#### Customizing Windows File Protection...

The Windows File Protection service can be customized in several ways with the simplest way of modifying the options being through the Group Policy Editor.

Click on Start Menu > Run box > type in gpedit.msc and hit the Ok button.

Expand Computer Configuration > Administrative Templates > System

then select the Windows File Protection folder...

ANY changes made here will update the registry keys at:

HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\Windows File Protection

Administrators PLEASE note:

When Windows XP starts up, the Windows File Protection service synchronizes (copies) the Windows File Protection settings from the following registry key:

HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\Windows File Protection

to the following registry key:

Re: scan for file corruption

microsoft.public.windowsxp.newusers: Re: scan for file corruption

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Therefore, if any of the following values are present in the HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\Windows File Protection key, they will take precedence over the same values under the HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon key.

Other edits include:

All registry settings for this service are located in:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

By default, only Administrators and System will be able to modify these settings.

SFCScan (REG\_DWORD)

0 = do not scan protected files at boot (default).

1 = scan protected files at every boot.

2 = scan protected files once.

SFCQuota (REG\_DWORD)

n = size (in megabytes) of dllcache quota.

FFFFFFFF = all files.

If you don't know hex, here's some samples:

00000099 = 153 (MB).

0000004b = 75 (MB).

00000032 = 50 (MB).

0000000a = 10 (MB).

SFCShowProgress (REG\_DWORD)

0 = System File Checker progress meter is not displayed.

1 = System File Checker progress meter is displayed (default).

SFCDllCacheDir (REG\_EXPAND\_SZ)

Path = local location of dllcache directory (default is

%Systemroot%\system32\Dllcache).

By now you should have a greater understanding of Windows File Protection in Windows XP and how it works.

Please read my separate article on the scannow sfc command line utility that allows you to manually use the Windows File protection service on your PC.

Disclaimer: Modifying the registry can cause serious problems that may require you to reinstall your operating system. I cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk.

Re: scan for file corruption

"Carey Frisch [MVP]" wrote:

- > 1. Go to Start > Run and type: CMD , and hit enter.
- > 2. In the Command Prompt window type: SFC /SCANNOW
- > and hit enter. Have your Windows XP CD available.
- >
- > --
- > Carey Frisch
- > Microsoft MVP
- > Windows XP – Shell/User
- >
- > Be Smart! Protect Your PC!
- > <http://www.microsoft.com/athome/security/protect/default.aspx>
- >
- >

- 
- >
  - > "ms. greenhorn" wrote:
  - >
  - > | tried to find corrupted file by selecting "run" and entering "sfc/scannow"
  - > | w/no luck; repsonse was could not be found, to re-check the file name.
  - > | trying to repair corrupted file (per ms help desk) without re-installing os.
  - > | oh, and thanks for your suggestion, rick, but here i am, again.
  - >