



Command-Line Options for SFC

The following table is a list of command-line options for SFC:

Command-Line Options	Description
/CACHESIZE=x	This value is not supported. Windows Server 2003 and Windows XP: Sets the file cache size. The default size of the cache is 0x32 (50 mb).
/CANCEL	This value is not supported.
/ENABLE	The value is not supported.
/FILESONLY	Verify or repair only files. Do not verify or repair registry keys. Windows XP: Not supported.
/OFFBOOTDIR	Use this option for offline repairs. Specify the location of the offline boot directory. Windows XP: Not supported.
/OFFWINDIR	Use this option for offline repairs. Specify the location of the offline Windows directory. Windows XP: Not supported.
/PURGECACHE	The value is not supported. Windows Server 2003 and Windows XP: Empties the file cache and scans all protected system files.
/QUIET	This value is not supported.
/REVERT	Return to default settings. Windows Server 2008 and Windows Vista: Not supported.
/SCANBOOT	This value is not supported. Windows Server 2003 and Windows XP: Scans all protected system files at every boot.
/SCANFILE	Scans and repairs the file located at the specified full path. Windows XP: Not supported.
/SCANNOW	Scans all protected system files immediately.
/SCANONCE	This value is not supported. Windows Server 2003 and Windows XP: Scans all protected system files at the next boot.
/VERIFYFILE	Verifies the file at the specified full path. This option does not repair the file. Windows XP: Not supported.
/VERIFYONLY	Scans all protected system files but does not repair files. Windows XP: Not supported.

DEP Configuration

Windows supports four configurations for hardware DEP and software DEP. They are `OptIn`, `OptOut`, `AlwaysOn`, and `AlwaysOff`. It is highly recommended to configure DEP to operate in either the `AlwaysOn` or `OptOut` setting.



WINDOWS PROTECTION MECHANISMS

Configuration	Description
OptIn	This setting is the default configuration. On systems with processors that can implement hardware-enforced DEP, DEP is enabled by default for limited system binaries and programs that "opt-in." With this option, only Windows system binaries are covered by DEP by default.
OptOut	DEP is enabled by default for all processes. You can manually create a list of specific programs that do not have DEP applied by using the System dialog box in Control Panel. Information technology (IT) professionals can use the Application Compatibility Toolkit to "opt-out" one or more programs from DEP protection. System compatibility fixes, or shims, for DEP do take effect.
AlwaysOn	This setting provides full DEP coverage for the whole system. All processes always run with DEP applied. The exceptions list to exempt specific programs from DEP protection is not available. System compatibility fixes for DEP do not take effect. Programs that have been opted-out by using the Application Compatibility Toolkit run with DEP applied.
AlwaysOff	This setting does not provide any DEP coverage for any part of the system, regardless of hardware DEP support. The processor does not run in Physical Address Extension (PAE) mode unless the /PAE option is present in the Boot.ini file.

Recommended Readings

- **Windows Internals part 2 6th edition:** Chapter 10. Memory Management >Virtual Address Space Layouts
> Read from topic User Address Space Layout through the end of the page.

Recommended Internet Sites

- **Windows File Protection**
<https://web.archive.org/web/20160911121419/https://support.microsoft.com/en-us/kb/222193>
- **Supported Resource Replacement**
[https://web.archive.org/web/20160919063247/http://msdn.microsoft.com/en-us/library/aa382540\(v=vs.85\).aspx](https://web.archive.org/web/20160919063247/http://msdn.microsoft.com/en-us/library/aa382540(v=vs.85).aspx)
- **WRP Detecting Resource Replacement**
[https://web.archive.org/web/20141224195413/http://msdn.microsoft.com:80/en-us/library/windows/desktop/aa382525\(v=vs.85\).aspx](https://web.archive.org/web/20141224195413/http://msdn.microsoft.com:80/en-us/library/windows/desktop/aa382525(v=vs.85).aspx)
- **Create a Test Certificate**
<https://web.archive.org/web/20161117033616/https://msdn.microsoft.com/en-us/library/ff699202.aspx>
- **Windows ISV Software Security Defenses**
<https://web.archive.org/web/20170428235931/https://msdn.microsoft.com/en-us/library/bb430720.aspx>
- **Analysis of ASLR on Windows Vista**
https://web.archive.org/web/20160805140552/http://www.symantec.com/avcenter/reference/Address_Space_Layout_Randomization.pdf
- **DEP**
<https://web.archive.org/web/20170218063427/https://support.microsoft.com/en-us/help/875352/a-detailed-description-of-the-data-execution-prevention-dep-feature-in-windows-xp-service-pack-2,-windows-xp-tablet-pc-edition-2005,-and-windows-server-2003>

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.

