

- Clean Disk Security -

Copyright Kevin Solway 1998-2005

This program has three functions. Firstly, this program can **clean** the FREE SPACE on your hard drive to ensure that deleted files cannot be undeleted. Cleaning the free space of a drive does not affect existing files. Secondly, this program can be used to fully **erase** existing files, so that they cannot be undeleted. And thirdly, this program can create more space on your hard drive by erasing unneeded, temporary files.

For all of FAT12, FAT16, FAT32, and NTFS file systems (Win95, Win98, WinME, WinNT, Win2000, WinXP).

Deleting a file normally just removes the file's directory entry, but the data itself remains on the disk, along with traces of the names of the deleted files. This program completely eliminates the contents of deleted files, as well as the file names, making it impossible to recover them even with specialized equipment. (* details below)

Disk security is achieved by cleaning the disk in nine ways:

1. Cleaning the ordinary free (unused) space on the disk.
2. Cleaning the Windows' swap file.
3. Cleaning the "slack space" associated with each file. (in the registered version only).
4. Cleaning the Recent file list (in the "Documents" menu)
5. Emptying the Windows' Recycle Bin
6. Cleaning the Windows' "Temp" folder
7. Cleaning out temporary Internet files (browser cache and history)
8. Cleaning out the "Cookies" stored on your computer
9. Fully erasing (deleting) existing files or directories that you specify.
10. Optionally erasing traces of names of deleted files in the File Allocation Table.

This program securely cleans your hard drives *without* your having to first remove all the files from that drive. However, if you need to do a *perfect* job of securely cleaning your hard disk then see here for instructions.

You should especially consider thoroughly cleaning your hard drive with this program before selling your hard drive to someone else (eg, when you upgrade to a new hard drive or computer system).

* Normally, the operating system does not actually erase the file that you delete, but only removes the reference to the file from the system's file allocation table (by marking the disk space as unused). *The file data actually remains on the disk*, where anyone can recover it by using any disk maintenance utility capable of direct disk access. The data remains on the disk until that part of the disk is physically over-written by another program, and *even then* it may be possible to recover some or all of the data by studying the disk with specialized equipment.

Even reformatting a disk is not enough to prevent data from being recovered by the right equipment.

This program uses disk cleaning methods (especially the "Gutmann method") which aim to

make it impossible to recover the disk data, even with the most expensive and specialized equipment.

To suit your needs you can select from a range of different disk cleaning methods, including a simple random-character-overwrite, NIS method (National Industrial Security Program Operating Manual of the US Department of Defense), and the very thorough Gutmann method (based on Peter Gutmann's paper *Secure Deletion of Data from Magnetic and Solid-State Memory*).

Cleaning standard free disk space

Selecting this option will clean all the ordinary free (unused) space on your hard disk. This will erase all the data remaining on the drive from previously deleted files. Select the method you want to use to clean the free disk space. Please note that cleaning only this free space does not clean the "slack space" associated with each file.

Cleaning file "slack space"

This feature is only available with the registered version of the program.

In addition to free disk space there is "slack space" associated with each file and which is completely separate from the ordinary free space on your drive.

Disk space is allocated in "clusters", and each cluster can be as large as 65,536 bytes. This means that a file of only one byte in size can use 65kb of disk space. This additional, unused space allocated to a file is called the "slack space" and can contain old, and possibly valuable data which needs to be cleaned.

This program cannot clean the slack space of the files that are currently in-use, so you should exit from as many programs as possible before using this feature. Generally speaking the only files which cannot be cleaned are the in-use operating system files, which is not normally a problem if the operating system was originally installed on a clean disk, because the slack-space associated with those files cannot be used by other data.

Hints and tips

1. *Perfect cleaning* - when you want to be sure of not leaving a trace:

To *perfectly* clean your disk of all possibly sensitive data it is recommended that you delete *all* the files from it, then clean it with *Clean Disk Security*, then re-format the disk. *Clean Disk Security* does an excellent job on a disk that is full of files, but to be absolutely sure that no sensitive data can be recovered you should erase all the files prior to cleaning and reformatting.

Fortunately, such radical cleaning is not needed for most purposes.

2. *Clean Disk Security* cleans file data off your hard disks, but cannot remove the old *file names* from the system file allocation table. Some disk utilities may be able to detect the *names* of removed files even though the file data is not available to them. This may be a problem if you do not want anyone to know that the file was ever on the disk. To remove these old file names from the system file allocation table, run the **Defrag** (disk defragmenter) utility that comes with your Windows software.

3. For best results, exit all other applications before running *Clean Disk Security*.

4. You may need to disable any virus program you have running before you use this program. While cleaning file slack space this program sometimes needs to access "read-only" files. This action can cause virus programs to be alarmed.

5. Run SCANDISK (System utility) to check your drive for errors prior to running *Clean Disk Security* to clean the free space of a drive. This will ensure that the system is providing true information about the amount of free space available on the drive, and will enable *Clean Disk Security* to do its job properly.

Cleaning the Windows' swap file

The Windows' swap file is typically a large file that contains memory data that has been written to disk by the Windows' memory management software. This file may possibly contain sensitive data, and it persists even after you have shut-down Windows. For this reason, if you require tight security, you should opt to clean the Window's swap file.

Win95 and Win98:

Cleaning of the Windows' swap file cannot be done whilst Windows is running (because Windows is using it). So when you select this option your system will temporarily restart in MSDOS mode (for Win95/98) to clean the swap file before returning to Windows.

If your system doesn't automatically restart in DOS mode to do the cleaning then it may be necessary for you to manually restart your system in DOS mode, then execute the program CLNSWAP.EXE to clean the swap file.

WinME:

The only way to clean the swap file in WinME is to boot your computer from a DOS boot diskette (or DOS boot CD) and then manually run the CLNSWAP.EXE program, which is found in the Clean Disk Security folder (It can help if you copy the CLNSWAP.EXE file into the root directory of your drive so you can find it more easily). DOS boot diskettes can be obtained online from places like www.bootdisk.com.

WinNT, Win2000, and WinXP

Users of Windows NT/2000/XP can select to automatically clear the swap file (also known as the paging file, named "PAGEFILE.SYS") at shutdown of Windows. Go to the [configuration dialog](#) and check the box titled "Clean Windows swap file at shutdown". This setting will only take effect once you have restarted your computer.

Cleaning the Recent files list

When you open documents or other files within Windows, the name of the file is automatically added to "Recent Documents" on the "Start Menu". Cleaning the names from this menu does not affect the actual documents the names refer to, but only erases the names from the Recent Documents menu.

To clear Recent Documents, simply select the "Clean Recent Documents" option.

If *Clean Disk Security* does not automatically locate the Recent documents folder then you can manually specify its location from the Configuration dialog.

Emptying the Windows' Recycle Bin

The Recycle Bin is an area for storing "deleted" files (from all disk drives) before their deletion is manually confirmed. To empty the Recycle Bin, select the "Empty Recycle Bin" option.

This feature will only work properly with the following minimum system configuration:

Windows 98, ME, NT4, 2000, XP
or
(Windows 95) with IE 4 or better installed.
[Shell.dll v4.71 or higher]

If your system doesn't meet this criteria *Clean Disk Security* can still clean out the contents of the Recycle Bin, but it won't be able to reinforce its own erasures with the Windows' standard "Empty Recycle Bin" command.

If *Clean Disk Security* does not automatically locate the Recycle Bin folder then you can manually specify its location from the [Configuration dialog](#).

Cleaning the Windows' "Temp" folder

Windows' temporary files (stored in the Windows' "Temp" folder) are created by applications running under Windows. Sometimes these temporary files can be inadvertently left on your computer. These can be a security risk, as well as taking up valuable space and, in extreme cases, can slow down your computer. To remove these files, simply select the "Clean Windows' 'Temp' folder".

If *Clean Disk Security* does not automatically locate the Windows' Temp folder then you can manually specify its location from the [Configuration dialog](#).

Cleaning out Cookies

“Cookies” are small files kept on your computer which store information relating to web sites you have visited while surfing the Internet.

Deleting cookies might mean that a web site may no longer be able to remember who you are next time you visit. For example, when you visit a site like Amazon.com, it might not be able to greet you by name.

If *Clean Disk Security* does not automatically locate the Cookies folder then you can manually specify its location from the [Configuration dialog](#).

Removing traces of file names from the Disk

Even after the contents of a file have been properly erased, traces of the names of deleted files can remain in the disk FAT (file allocation table). When this program deletes files it can automatically remove the traces of the names of those files from the FAT. If you want to use this feature then select the option in the "Config" dialog.

If you want to remove *all* traces of the names of deleted files from your disk (ie, not only those you erase using *Clean Disk Security*), then you need to run the Windows' Disk defragmenter ("Defrag") utility.

Viewing disk contents directly

Click on the "View" button to directly view the contents of the selected drive.

You can use this feature to see how *Clean Disk Security* cleans your disks.

There are two view modes:

1. Disk mode.

Here you can view the raw contents of disk on a sector-by-sector basis. Use the horizontal slider at the bottom to view different parts of the disk. You can also enter the sector number directly.

This mode can be used for viewing both the used space of the disk as well as the free space.

2. Directory mode.

In this mode you can view the disk contents via the directory structure, which enables you to view the raw contents of any file on the disk.

This mode cannot be used for viewing the free space of the disk.

Names of deleted files are visible to you (in red).

You can fully erase files, and file names, that you select. Be careful when erasing files, as once they are erased they will not be able to be retrieved.

This program includes a rudimentary undelete function to demonstrate how deleted files can be undeleted. The rudimentary method used here is unable to delete many of the files that can be undeleted by specialist undeletion software. You are not advised to use this routine to undelete important files. Demonstrate the undeletion of files to yourself on small, unimportant files.

Cleaning out the history records

Optionally clean the history records stored on your computer, which record such things as where you have visited on the Internet.

If *Clean Disk Security* does not automatically locate the location of your History folder then you can manually specify it in the Configuration dialog.

Cleaning out temporary Internet files (browser cache)

Your Internet browser stores the contents of files viewed on the Internet in a "cache" on your hard disk, so that when you visit the same site again your browser can load the file directly from the your hard disk rather than have to download all the information through the Internet again, saving much time. As you surf the Internet older files are removed from the cache and newer files are added.

Cleaning out these temporary Internet files can be useful for security purposes, as well as making more space available on your hard disk.

If *Clean Disk Security* does not automatically locate the location of your Internet browser cache or history folder then you can manually specify their location in the [Configuration dialog](#).

Some URLs are stored in a file called "INDEX.DAT", which is sometimes protected by the operating system, and will only be removed once you restart your system.

Note: If you are using *Mozilla Firefox* web browser there is a plugin you can use to clear the browser cache and history. Please read more [here](#).

Mozilla Firefox Web Browser

There is a plugin designed to clean out the Mozilla Firefox Browser Cache and History.

You will need to edit the path names it contains so that they refer to the proper folders on your system, since the folder locations are different on each system. These changes can be made through use of the Plugin Editor or by editing the plugin file directly with a text editor.

Command-line usage and scheduling

This program can be invoked with the use of a scheduling program, allowing you to automatically clean your drive at a pre-scheduled time.

[Your scheduling program may not allow you to specify program command line parameters, in which case you will need to execute CLNDISK.EXE via a batch file. Use a text editor to create a new text file called, say, CLN.BAT, which includes a call to CLNDISK.EXE. Put the name of the batch file in your scheduling program.]

Command line usage:

CLNDISK [drives]or[file path] [simple/nis/gutmann] [slack] [swapfile] [history] [cache] [cookies] [recent] [temp] [plugins] [clipboard] [nowarnings] [test]

For example,

```
clndisk c nis slack swapfile plugins cache nowarnings
```

(to clean Drive C:, cleaning the normal free disk space, and using NIS erasure, and cleaning the file slack space, and process the plugins, and clean the Internet browser cache, with no warning messages or prompts)

or,

```
clndisk df simple
```

(to clean Drives D: and F: using normal erasure)

or,

```
clndisk d test
```

(. . . if you want to test the program on Drive D:..Ascii character #10 will be written to the free space of the drive in a single pass. You can then examine the disk with the disk view function to satisfy yourself that the disk has indeed been cleaned. Note that the unregistered version of this program will not clean the file "slack space")

or,

```
clndisk c:\bdata
```

(. . . to fully erase a directory called "c:\bdata", along with all the files and directories that may be contained within it.)

or,

```
cmdisk c:\temp\*.doc
```

(. . . to fully erase all the files with a ".doc" extension in a directory called c:\temp)

Testing this program

In the test mode ascii character #10 will be written to the free space of the drive in a single pass. You can then examine the disk with the disk view function to satisfy yourself that the disk has indeed been cleaned. (Note that the unregistered version of this program will not clean the file "slack space")

Test mode is not available on WinNT/2000/XP compressed drives, due to the way the compression algorithm compresses the test pattern.

There are two ways to make *Clean Disk Security* work in test mode.

1. Select the option in the "method" group box.
or
2. Include the word "test" in the command parameters (after the drive letter) if you want to test this program.

for example,

```
clndisk d test
```

(. . . to test the program on Drive D:)

Configuration dialog

Configuring folder locations

Be very careful whenever deleting files with this program, because if you make a mistake and delete the wrong files then you won't be able to recover them again.

In the "Config" dialog you can specify the folder locations for the "recent files list" (usually in Windows/recent), the Windows' "temp" folder (usually Windows/temp), the recycle bin (usually C:\recycled) and the folder for your Internet browser cache (the location of this folder varies depending on which browser you are using, and its release version).

On most systems *Clean Disk Security* is able to automatically detect the location of these folders, but this is not possible on all systems.

*** Before any files are erased from your system *Clean Disk Security* will verify with you that you are sure you want to delete the contents of the specified directory, and will tell you the number of files that will be erased by the operation. This is a safety precaution for your benefit. It is important to carefully verify any file deletions if you don't want to risk losing valuable data.**

Other settings:

- On WinNT/2000/XP you can select to clear the Windows swap file (paging file) on shutdown.
- Select to be prompted to verify erasure of folders (and their contents). This is a safety measure.
- Select to erase traces of names in the FAT (on FAT16 and FAT32 systems).
- Select to maintain a log of cleaning activities. (Stored in CLNDISKLOG.TXT).
 - From here you can also view the log, or reset the log (to empty).

Troubleshooting

1. This program creates a temporary file called DRVCLN.\$\$\$ in the root directory of the drive being cleaned and writes special data to it until the drive is full. This temporary file is then erased. If this program should terminate abnormally then you may need to delete the temporary file manually to recover the space.
2. If you get a "low disk space" warning while using this program, just ignore it. This program temporarily fills-up all the space on the disk in order to wipe it clean. As soon as the disk is fully cleaned the free space is made available again.
3. If the program ceases activity when it is almost finished cleaning, this means that the system is providing false information about the amount of free space left on the drive. In this case run SCANDISK (System utility) to fix the problem, then re-clean the drive.
4. On **WinME** and **XP** you are recommended to switch off "System Restore" before using Clean Disk Security, as WinME's system recovery wasn't designed to cope with the large number of changes to the disk made by Clean Disk Security.

Having System Restore enabled can also greatly slow down the cleaning process.

On WinME

Open Control Panel -> System -> Performance Tab -> File System ->
Troubleshooting area -> Disable System Restore

On WinXP

Open Control Panel -> System -> System Restore.
Then switch off System Restore

5. Some disk utilities may report that files which have been removed with *Clean Disk Security* can still be recovered, because it can recover part of the file *names*. This is because while *Clean Disk Security* securely cleans the *file data* off your hard disks it cannot remove *all* of the fragments of old *file names* from the system file allocation table. Some disk utilities may be able to detect parts of the *names* of removed files even though the file data is not available to them. To remove these fragments of old file names from the system file allocation table, run the **Defrag** (disk defragmenter) utility that comes with your Windows software.

If you want to assure yourself that the file data cannot be recovered, even though the old file name has been recovered, let the disk utility try to recover the data and see what happens.

6. If you have selected to clean the Windows swap file and your system doesn't automatically restart in DOS mode to do the job then it may be necessary for you to manually restart your system in DOS mode, then execute the program CLNSWAP.EXE to clean the swap file. You may need a DOS boot diskette (which you can obtain from www.bootdisk.com)

7. If you get warning messages from virus software while using this program then disable those programs temporarily. While cleaning file slack space this program sometimes needs to access "read-only" files. This action can cause virus programs to be alarmed.

8. The NIS and the Gutmann methods especially are not designed for use with compressed drives. If you try to clean a compressed drive with either of these methods pseudo-random data will be written to the disk instead, as it will clean compressed drives more effectively.

Erasure methods

1. **Simple method**: (up to 6 passes)
 - Overwrite with random characters
2. **NIS (DoD) method**: (7 passes)
 - from the National Industrial Security Program Operating Manual
3. **Gutmann method**: (35 passes)
 - based on the paper *Secure Deletion of Data from Magnetic and Solid-State Memory*, by Peter Gutmann (Department of Computer Science, University of Auckland), 1996

Simple method (random characters)

This method is the one to use if it is not likely that your disk will be examined by expensive, specialized equipment, like an electron microscope. This method is quite adequate for ordinary needs (eg, home use, or small business), as it will prevent anyone from recovering the data with software (disk utility programs).

Random characters are written to the disk, erasing the original contents. Choose the number of passes you require (between 1 and 6). Six passes will take six times as long as one pass, but provides additional security. A single pass is sufficient for most needs.

NIS (DoD) Erasure method

Use this seven-pass method for tighter security. Different patterns of bytes are written to the disk as described in the table below. Using this method is probably even safer than using the simple method (with 6 passes).

This method is described in the National Industrial Security Program Operating Manual (NISPOM a.k.a. DoD 5220.22-M) of the US Department of Defense (January 1995; chapter 8, section 3, 8-306. Maintenance).

The free disk space is overwritten seven times:

Pass	Data
1	A random character, $n = [0, 255]$
2	A random character, n
3	Complement of previous character, $\sim n$
4	A random character, n
5	A random character, n
6	Complement of previous character, $\sim n$
7	A random character, n

However, if you want to be absolutely sure of your data security, use the Gutmann method, below.

Gutmann method

This method offers the most tight security for the whole range of disk drive types. You should use this method if your data is very valuable and you think your disk could possibly be scrutinized by expensive, specialized equipment.

The method used by *Clean Disk Security* is based on that described in the paper *Secure Deletion of Data from Magnetic and Solid-State Memory*, by Peter Gutmann (Department of Computer Science University of Auckland. pgut001@cs.auckland.ac.nz), and is included in *Clean Disk Security* with his permission.

The paper was first published in the Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996.

The first four and last four passes are pseudo-random data (created with additive congruential pseudo-random number generator) and other passes are made in random order.

Overwrite Data

PassNo.	Data Written	Encoding Scheme Targeted
1	Random	
2	Random	
3	Random	
4	Random	
5	01010101 01010101 01010101 0x55	(1,7) RLL MFM
6	10101010 10101010 10101010 0xAA	(1,7) RLL MFM
7	10010010 01001001 00100100 0x92 0x49 0x24	(2,7) RLL MFM
8	01001001 00100100 10010010 0x49 0x24 0x92	(2,7) RLL MFM
9	00100100 10010010 01001001 0x24 0x92 0x49	(2,7) RLL MFM
10	00000000 00000000 00000000 0x00	(1,7) RLL (2,7) RLL
11	00010001 00010001 00010001 0x11	(1,7) RLL
12	00100010 00100010 00100010 0x22	(1,7) RLL
13	00110011 00110011 00110011 0x33	(1,7) RLL (2,7) RLL
14	01000100 01000100 01000100 0x44	(1,7) RLL
15	01010101 01010101 01010101 0x55	(1,7) RLL MFM
16	01100110 01100110 01100110 0x66	(1,7) RLL (2,7) RLL
17	01110111 01110111 01110111 0x77	(1,7) RLL
18	10001000 10001000 10001000 0x88	(1,7) RLL
19	10011001 10011001 10011001 0x99	(1,7) RLL (2,7) RLL
20	10101010 10101010 10101010 0xAA	(1,7) RLL MFM
21	10111011 10111011 10111011 0xBB	(1,7) RLL
22	11001100 11001100 11001100 0xCC	(1,7) RLL (2,7) RLL
23	11011101 11011101 11011101 0xDD	(1,7) RLL
24	11101110 11101110 11101110 0xEE	(1,7) RLL
25	11111111 11111111 11111111 0xFF	(1,7) RLL (2,7) RLL
26	10010010 01001001 00100100 0x92 0x49 0x24	(2,7) RLL MFM
27	01001001 00100100 10010010 0x49 0x24 0x92	(2,7) RLL MFM
28	00100100 10010010 01001001 0x24 0x92 0x49	(2,7) RLL MFM

29 01101101 10110110 11011011 0x6D 0xB6 0xDB(2,7) RLL
30 10110110 11011011 01101101 0xB6 0xDB 0x6D(2,7) RLL
31 11011011 01101101 10110110 0xDB 0x6D 0xB6(2,7) RLL
32 Random
33 Random
34 Random
35 Random

Fully erasing (deleting) existing files

For safety reasons, this feature is only available through the Windows right-click context menu in "Explorer" (or other Windows file manager, like "Control3"). This feature should be used with *extreme caution*, as any files or directories that are erased will **not** be recoverable by any means.

You should take *special* precaution before deleting directories, because all subdirectories within a directory, along with all the files they contain, will also be thoroughly erased. It is entirely possible to erase something you need if you do not check very carefully beforehand.

Usage:

When using Windows Explorer (or "Control3" file manager) right-click your mouse while pointing at the file or directory you want to fully erase. You can also mark a number of files or directories for erasure before right-clicking. On the pop-up context menu that appears will be an option to "Erase fully". If you select this option *Clean Disk Security* will count the total number of files and directories that will be erased and verify with you that you do indeed want to fully erase them. Only upon your confirmation will the entries be fully erased.

If you right-click on a *drive letter* (eg, D:) then the context menu will contain the entry "Clean Disk Security". Selecting this option will start-up *Clean Disk Security* in normal mode (not in file deleting mode), where you can select to clean the free (unused) space of the drive, as well as the file slack space (in the registered version).

How the files are fully erased:

Clean Disk Security firstly opens a file that is to be erased then wipes-over it's data a number of times (using the erasure method you specify). The file slack space associated with the file is wiped at the same time. The file buffers are flushed each time the data is overwritten to ensure that the data doesn't remain cached in memory. The file size is then set to zero before the file is finally closed, then file times and dates are reset, and the file is deleted. Lastly, any traces of the file names are removed from the FAT (file allocation table).

Keeping a Log of Activities

In the configuration dialog you can select to keep a log of cleaning activities. Records are kept in a file called CLNDISKLOG.TXT. You can view this log by clicking in the "View log" button in the config dialog.

Control3 file manager

Control3 is a replacement for Windows "Explorer", and provides you with much more functionality and ease of use. You can download it from the Control3 web page:

<http://www.theabsolute.net/sware/control3.html>

Registering this program

Price: \$25 (US)

When you purchase *Clean Disk Security* you will receive:

1. A key code to unlock the full features of the program and remove the shareware reminder screens.. After a period of time the shareware reminder screens will increase in frequency.
2. The satisfaction of knowing that you have paid for quality software and that you have supported the shareware industry that brings you software faster and more cheaply than by any other means.. The shareware industry operates largely on trust.
3. Entitlement to **free** upgrades, for both major and minor upgrades, for an unlimited time.

Payment Options:

Either:

- * Go to the *Clean Disk Security* web page where you can pay by credit card using a **secure online order form**:

<http://www.theabsolute.net/sware/clndisk.html>

or

Fill out the **[secure online order form](#)** at Regsoft.

or

Fill out the **[secure online order form](#)** at Northstar Solutions.

Or

go here: <http://www.nstarsolutions.com/1121.htm>

or here: <http://www.regsoft.net/purchase.php3?productid=34549>

- * Send me email: **software@theabsolute.net**

- A WORD ABOUT USER-SUPPORTED SOFTWARE -

The user supported software concept (usually referred to as shareware) is an attempt to provide software at low cost. The cost of offering a new product by conventional means is staggering, and hence dissuades many independent authors and small companies from developing and promoting their ideas. User supported software is an attempt to develop a new marketing channel, where products can be introduced at low cost.

If user supported software works, then everyone will benefit. The user will benefit by receiving quality products at low cost, and by being able to "test drive" software thoroughly before purchasing it. The author benefits by being able to enter the commercial software arena without first needing large sources of venture capital.

But it can only work with your support. We're not just talking about *Clean Disk Security* here, but about all user supported software. If you find that you are still using a program after a couple of weeks, then pretty obviously it is worth something to you, and you should send in a contribution.

Disclaimer

Clean Disk Security is provided on an "AS IS" basis, without warranty of any kind either express or implied, including warranties of merchantability or fitness for a particular purpose. In no event will the author be liable to you for damages, direct or consequential, which may result from the use of this program. The user must assume the entire risk of using the software. There is no guarantee accompanying this software that it will function perfectly.

Cleaning on NTFS file systems

This program makes special provisions when cleaning NTFS file systems.

- Compressed, encrypted, and sparse files, whose size on disk is different to that which is reported by the system, are given special treatment to ensure that they are properly cleaned. (Note that when erasing compressed files, the amount of data written to the disk to clean them may be smaller than what you expect, because it is the compressed data that is overwritten.)
- The Master File Table (MFT) is cleaned to ensure that the remains of small, MFT-resident files cannot be recovered, and to remove remains of the names of deleted files.

Plugins

A great many software programs keep track of recent user activities. This means that others can easily find out what files you have accessed, what picture you have viewed, what media you have played, and much more. Removing these stored activities will help preserve your data security and privacy.

In the configuration dialog, place a check mark next to the plugins you want to enable when processing plugins.

Please see: [Plugin Editor](#)

NOTE: Clean Disk Security Inc cannot be held responsible for lost data or damage to a system due to the use of the plug-ins contained in Clean Disk Security. You add, edit and customize plug-ins at your own risk.

Plugin Editor

A great many software programs keep track of recent user activities. This means that others can easily find out what files you have accessed, what picture you have viewed, what media you have played, and much more. Removing these stored activities will help preserve your data security and privacy. With Clean Disk Security's Plugin Editor you can create your own plug-ins (*Note: This feature is for advanced users only, as you will need know the registry keys/values and the disk folders/files used by your application to record its tracks*).

Clean Disk Security's plug-ins are files with .cdp extensions containing lists of tasks Clean Disk Security will run when processing each plug-in. You can launch the Plugin Editor in the Clean Disk Security program group from the Windows start menu, or click the Plugin Editor button in the Plug-Ins configuraton dialog.

Registry Actions

Defines the registry key/value actions to erase the tracks for your application.

File/Folder Actions

Defines the disk folder/file actions to erase the tracks for your application. Most of the plug-ins we provided are made using Plugin Editor, so you can use Plugin Editor to open the plug-ins for learning more about Clean Disk Security's plug-ins. ***Important Note: There is no technical support available for edited or customized plug-ins.***

NOTE: Clean Disk Security Inc cannot be held responsible for lost data or damage to a system due to the use of the plug-ins contained in Clean Disk Security. You add, edit and customize plug-ins at your own risk.

