Secure Eraser

Erase Your Documents and Drives Securely.

© ASCOMP Software GmbH All rights reserved.

Info

Erase Your Documents and Drives Securely.

ASCOMP Software GmbH

Because it's been erased from your hard drive, doesn't mean it's gone forever. As long as the information was not overwritten, anyone can restore it at any time. It gets even more complicated, if a computer has been resold or given away.

Secure Eraser uses the most renowned method of data disposal and overwrites sensitive information in such a sure way that it can never be retrieved – even with specialized software. Our multiple award-winning solutions for definitively destroying data also eliminate any cross-references that could leave traces of deleted files in the allocation table of your hard drive.

This easy-to-use Windows software will overwrite sensitive data even up to 35 times – regardless of whether they are files, folders, drives, recycle bin or traces of surfing. You can also delete files that have already been deleted, but this time for good.

Secure Eraser not only overwrites using random data, it offers the approved US Dod 5220.22-ME and U.S. DoD 5220.22-MECE standards from the US Department of Defense, the German industrial standard and the Peter Gutmann standard. All deletions are logged in details upon request.

Secure Eraser

© ASCOMP Software GmbH

All rights reserved.

Written: März 2022 in Leonberg, Germany.

Company

ASCOMP Software GmbH

Developer

Andreas Ströbel

Betatest

This software has been tested internally and externally.

Content

Part I Information 7
1 Differences between Editions 7
2 Ordering & Contact 7
3 Version History 8
4 Parameter Selection 12

Part II Main Menu 15
1 Start 15
2 Settings 15
3 Journal 16
4 Update 17
5 Help 17
6 Language Switch 18

Part III File & folder deletion 20
1 Overview 20
2 General Information 22

Part IV Drive/partition deletion 24
1 Overview 24
2 General Information 25

Part V Free space deletion 27
1 Overview 27
2 General Information 28

Part VI Registry cleaning 30
1 Overview 30
2 General Information 31

Part VII System cleaning 33
1 Overview 33
2 General Information 37

Part VIII Report administration 39
1 Overview 39
2 General Information 39

© ASCOMP Software GmbH

Part IX Tips & Tricks 41

1 Deletion of USB sticks / SD cards / Flash drives 41

2 Using software for data recovery 41

© ASCOMP Software GmbH

Information

Part I

1 Information

This chapter provides general information about Secure Eraser. It includes the available editions, order and contact information as well as the version history of the software.

1.1 Differences between Editions

Secure Eraser is available in two different editions. The following section is intended to show the differences between the available editions and simplify your decision in selecting the right one for you.

Standard Edition

The Standard Edition of Secure Eraser is available completely free and without any registration for private purposes. It generally provides, all the functions of the other available editions, but occasionally displays an info window.

Users of the Standard Edition will not receive free technical customer support via email.

IMPORTANT NOTICE: It is not allowed to erase business data using the Standard Edition longer than a 14 days trial period!

Professional Edition

Secure Eraser Professional Edition removes any Info window for the software, thereby allowing it to be used for business purposes.

Users of the Professional Edition get free software updates and technical customer support for two years beginning upon the date of purchase.

1.2 Ordering & Contact

Ordering

Ordering the Professional Edition is possible using the Online-Shop for ASCOMP Software GmbH. Besides immediately issuing your login information to download the full version, our shop system also offers favorable conditions to dealers / resellers in particular for reselling of our products.

Secure Eraser Professional is available as a private license for 29.90 USD and as a company license for 49.90 USD (including all applicable taxes).

© ASCOMP Software GmbH

Contact

Secure Eraser is a product of ASCOMP Software GmbH, Germany. You may contact us using any one of the following means.

Email (recommended): support@ascompsoftware.com

Telephone: 0900-1019091 (0,49 Euro from a German landline)

Address: ASCOMP Software GmbH, Graf-Leutrum-Street 10, 71229 Leonberg, Germany

1.3 Version History

Version 6.0 (released on March 7, 2022)

+ Delete deletion report
+ Optimized deletion behavior
+ Icons in files list
+ Performance counter optimized
+ GUI improved
+ Windows 11 support extended

Version 5.3 (released on February 15, 2021)

+ Speed optimized
+ Program interface optimized
+ Deletion procedures optimized
+ Extended 64-bit support
+ Context menus translated
+ Installation routine translated

Version 5.2 (released on April 30, 2020)

+ System cleaning: Chrome support
+ System cleaning: Edge support
+ System cleaning: Firefox support optimized
+ Multi language support optimized
+ GUI optimized
+ Performance increased

Version 5.1 (released on September 3, 2018)

+ Drive modell listed in deletion reports
+ Deletion report comments
+ Select deletion report output folder
+ Memory usage optimized

Version 5.0 (released on February 2, 2016)

+ New user interface
+ Optimized speed
+ Improved user guide
+ Secure data erase: duration display
+ Improved hard drive cleaning

Version 4.3 (released on June 29, 2015)

+ Automatic language selection
+ Save switch status
+ Enhanced program stability
+ Windows 10 support

Version 4.2 (released on February 19, 2013)

+ Overwrite Slack space
+ Selectable application priority
+ New Language file: French
+ Windows 8 support

Version 4.1 (released on November 6, 2012)

+ Detailed deletion report
+ Automatically displayed deletion report
+ Management of deletion report
+ Optimized program interface
+ Revised homepage
+ Optimized user guide

Version 4.0 (released on June 15, 2011)

+ Hard drive / Partition secure deletion
+ MFTs clean up
+ Change Journal deletion
+ Optimized shortcut menu
+ Improved Drag & Drop
+ Parameter /drive

© ASCOMP Software GmbH

+ New Interface

Version 3.3 (released on February 2, 2011)

+ Upgraded hard drive cleaning
+ Deletion profile
+ Optimized progress display
+ Support for compromised disk drives
+ Optimized Registry-Scan (64 Bit)
+ Registry: save selection
+ Faster program start

Version 3.2 (released on July 10, 2010)

+ Expandable main window
+ Items in shortcut menu (64 Bit)
+ Saved window position

Version 3.1 (released on September 28, 2009)

+ Safe folder deletion
+ Improved USB-/SD- support
+ Display of estimated deletion duration
+ Optional deletion confirmation
+ Printing feature for journals
+ Hard drive cleaning: save selection
+ Upgraded help system

Version 3.0 (released on February 28, 2009)

+ Free disk space secure deletion
+ Emptying recycle bin per parameter
+ Parameter /invisible
+ Reports automatically canceled
+ Gutmann-Standard updated
+ Larger database support (> 4 GB)
+ Cancellation of deletion process
+ Unicode-Support
+ New help system

Version 2.2 (released on March 31, 2008)

+ Actions following deletion process
+ File deletion per parameter start

© ASCOMP Software GmbH

+ Window minimization
+ Parameter /exit
+ Optimized registry-scanning process
+ Update-wizard

Version 2.1 (released on October 24, 2007)

+ Multiple languages
+ MFT- data deletion
+ Folder deletion
+ Optimized Design
+ Larger files support (> 2 GB)
+ New menu icons

Version 2.0 (released on August 30, 2007)

+ Hard drive cleaning
+ Registry clean up
+ Extended Journal
+ New program design
+ Improved recycle bin support
+ Read-only files deletion
+ Cancellation of deletion process
+ Start with administrative privileges
+ Error-Reports
+ Complete deinstallation
+ Windows Vista support

Version 1.2 (released on August 12, 2006)

+ Multiple languages
+ Improved performance

Version 1.1 (released on May 10, 2004)

+ New program interface
+ File deletion from recycle bin
+ Activable journal

Version 1.0 (released on December 5, 2002)

© ASCOMP Software GmbH

1.4 Parameter Selection

The program file for Secure Eraser can be run using various parameters, which are described in more details below.

/del1 sample.txt

Starts deleting the following designated file / files using lowest security level (low - Random).

/del2 sample.txt

Starts deleting the following designated file / files using normal security level (Normal - US DoD 5220.22-M E).

/del3 sample.txt

Starts deleting the following designated file / files using high security level (high - German Standard).

/del4 sample.txt

Starts deleting the following designated file / files using very high security level (very high - US DoD 5220.22-M ECE).

/del5 sample.txt

Starts deleting the following designated file / files using the highest possible security level (maximum possible - Peter Gutmann standard).

/drive

Opens the "hard disk / partition secure deletion" menu.

/drive d:

Highlights the "D:\" drive in the lists of drives.

/drive d:\ /delX

Starts deleting the specific drive using the following designated security level below (*/del1* bis */del5)*.

© ASCOMP Software GmbH

/freespace

Opens the"free storage of secure deletion" menu.

/freespace d:

Highlights the "D:\" drive in the list of drives

/freespace d:\ /delX

Starts deleting the specified drive using the following designated security level below (/ del1 up / del5).

/recycler

Opens the "Hard drive clean up" menu and activates the "Windows Recycle Bin" option.

/recycler /delX

Starts deleting files in the Recycle Bin using the following designated security level (/ del1 up / del5).

/exit

Exits the software after completing the deletion.

/invisible

Performs an unseen deletion process (the program window is not displayed; Secure Eraser will automatically stop after completing the deletion).

© ASCOMP Software GmbH

Main Menu

Part II

2 Main Menu

This chapter provides information on the functions of Secure Eraser's main menu, which is placed directly under the window title bar.

2.1 Start

The "Start" menu loads the start page of the software allowing direct access to all important program features.

2.2 Settings

The "Settings" menu allows you to set the program settings.

General

Here you can specify general program settings when using Secure Eraser.

Disregarding errors

Disregards errors during deletion so that it will not be interrupted and can be performed unattended.

Deletion confirmation

Prompts the user for confirmation before starting a deletion.

Application priority

Sets the application priority of Secure Eraser. The application priority determines how many resources is provided a software by the operating system.

Logging

Select the settings that affect the logging functions of Secure Eraser.

Journal creation

Logs the following program events:

© ASCOMP Software GmbH

- Program start
- Program ending
- Starting the deletion process
- Starting the cleaning process

Max. Entries

Specifies the maximum number of entries to be managed in order to minimize storage expenditures.

Creating deletion reports

Specifies whether Secure Eraser should create a detailed HTML report for each deletion.

Besides the general program information, the deletion report contains the following data:

- Deleted files
- Deleted drives
- Revised folder
- Deleted Registry-Keys
- Common deletion standard

Displays

Controls the display of created deletion report (if active).

Output folder

Sets output folder for deletion reports.

2.3 Journal

The "Journal" menu displays journals created by Secure Eraser.

Important events are saved in a Journal by Secure Eraser.

The journal logs the following program events:

- Program start
- Program ending
- Start of the deletion process

© ASCOMP Software GmbH

- Start of the cleaning process

Clearing journals

To delete all entries stored in the journal, use the "Clear Journal" control button.

Printing journals

The journal can be printed using the "Print Journal" control button.

Important Information:

The created journal is saved in the application data folder of the registered user in an encrypted format.

2.4 Update

The "Update" menu ofpens the Update wizard for Secure Eraser.

The Update wizard support you in updating the current version. If a newer version is found on the ASCOMP Software Ltd server, the download and the subsequent installation of the newer version can be started using the "Download" button.

Checks during program initiation

Checks upon the start of Secure Eraser, if a version of the software exists and provides a corresponding status report.

2.5 Help

The "Help" menu enables loading the help system and displays version and support information for Secure Eraser.

Help

Loads the available help system.

Info

© ASCOMP Software GmbH

Displays the program information for Secure Eraser and enables direct contact to the technical support team of ASCOMP Software Ltd.

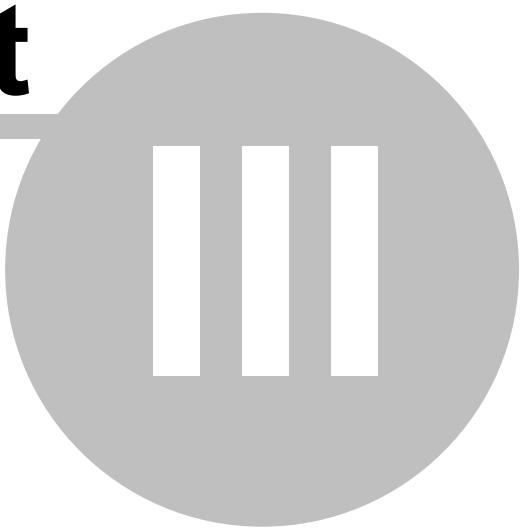
2.6 Language Switch

The language switch on the right side of the main menu allows you to switch among available programming languages that are in voice files format in the program folder of Secure Eraser (.ini).

© ASCOMP Software GmbH

File & folder deletion

Part



3 File & folder deletion

This chapter provides information on the "File & folder deletion" function for Secure Eraser.

3.1 Overview

Use the "files / folders secure deletion" function of Secure Erasure to permanently and irretrievably delete existing files and folders.

File list

All designated files for deletion are listed on the file list. Using the "Load delete profile" and "Save delete profile" icons the data and security levels selection can be loaded or stored as a profile.

Important Information:

The delete profile saves your selections as is. This means that using the "Add folder" function, read folders are reanalyzed when reloading the profile and its content is thus also re-read. The file list can therefore differ depending on the database.

A popup menu which provides additional options can be downloaded by right clicking on the file list with the mouse.

Adding files

Adds new files to the file list using the "Open File" dialog for Windows. Use this option if you want to select individual files.

The "Add files" control button offers the same functionality.

Adding folders

Adds all files and subfolders from a freely selectable folder to the file list using the "Search Folder" dialog for Windows. Use this option if you want to read all directory structures.

The "Add folder" control button offers the same functionality.

Did you know...

...that all files/folders contained in the subfolder are imported using this option?

Selecting All

Select all files and folders included on the list for deletion.

© ASCOMP Software GmbH

Deselecting All

Deselect the option to delete all files and folders on the file list.

Clearing file list

Remove all files and folders included on the file list. The files/folders are in this case **not** deleted.

The "Empty file list" control button offers the same functionality.

Security level

Allows you to select the level of security which is applicable when deleting selected files / folders. You will also receive information on the security level underlying deletion standard.

After deletion

You can determine the actions of Secure Eraser using the EX, SD, RB and S switches after completing the deletion process. If the switch is displayed in green, the corresponding option is activated. If the switch is blue that means this function does not apply.

EX

Exits the software after completing the deletion.

SD

Shuts down the operating system after completing the deletion.

RB

Reboots the operating system after completing the deletion.

SB

Sets the operating system on standby after completing the deletion.

Initiate deletion process

© ASCOMP Software GmbH

Starts the deletion process with due regard to changes previously made.

Cancel deletion

A deletion that is currently taking place can be canceled at any time using the "cancel deletion" button.

Files already deleted can **not** be restored.

It is possible that files currently being edited are only partially deleted and should again be removed using Secure Eraser for the sake of security.

3.2 General Information

Important Information:

1. Securely deleted files can **not** be recovered. ASCOMP Software Ltd has no way of restoring deleted data!
2. It is recommended that the operating system be rebooted after the deletion process, since parts of the deleted files might be remaining in the cache.
3. Files/folders that are not selected/not marked with a tick on the file list are ignored by Secure Eraser and therefore not deleted!
4. After the deletion process, error-free deleted files/folders are removed from the file list. File/ folders that could not be cleared by Secure Eraser will still appear on the file list.
5. After deleting files, that are stored on Solid State Drives, Solid State Drives, the free space of each drive should also definitely be safely deleted.

© ASCOMP Software GmbH

Drive/partition deletion

4 Drive/partition deletion

This chapter provides information on the "Drive/partition deletion" function for Secure Eraser.

4.1 Overview

Use the "Drive/partition deletion" function to securely delete all existing files and already deleted files from hard drive/partition.

Drive list

The supported drive for secure deletion of data are displayed in the drive list. To select a drive, click on the corresponding entry with the left mouse button.

Important Information:

The system partition can not be selected, because there are important files for its operation on this.

Options

Allows the selection of various additional options which can be performed after the actual deletion.

MFT clean up

Cleans the Master File Table for the selected drive/partition. Enable this option if Secure Eraser should also delete the file names of deleted files from the Master File Table (*recommended*).

Clearing Change Journal

Clears the USN Change Journal. The USN Change Journal logs all file operations on NTFS drives (if enabled) and thus contains the complete file and directory names.

After deletion

The actions of Secure Eraser after completing the deletion process can be determined using the EX, SD, RB and S switches. If the switch is displayed in green, the corresponding option is activated. If the switch is blue that means this function does not apply.

EX

© ASCOMP Software GmbH

Exits the software after completing the deletion.

SD

Shuts down the operating system after completing the deletion.

RB

Reboots the operating system after completing the deletion.

SB

Sets the operating system on standby after completing the deletion.

Initiating deletion process

Opens a popup menu, which allows the selection of one of the five available deletion methods. To start the deletion, click on the desired deletion method with the left mouse button.

4.2 General Information

Important Information:

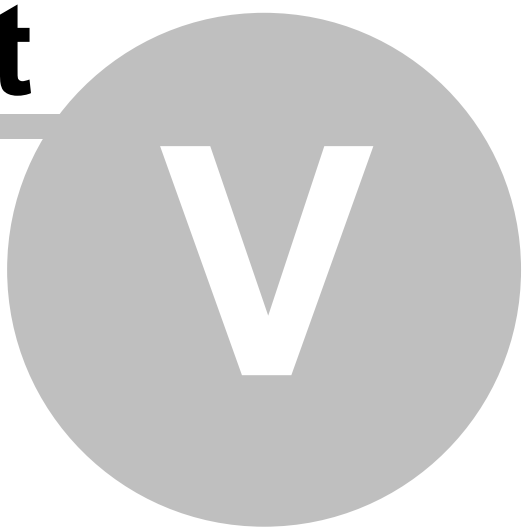
1. During the deletion process, a Windows "Low Disk Space" notification may appear. This message can be ignored.

2. During the deletion process, you should not work on the computer. Close all currently running applications ideally before starting the deletion process.

3. Secure Eraser writes one or several files with the designation $$ delete.tmp or $$ deleteX.tmp in the root directory of the selected drive. Should Secure Eraser close during the deletion process via the Windows task manager, these files must be deleted manually. Take particular care not to merely shift the files to the recycle bin, but to delete them using the key combination Shift + Del.

© ASCOMP Software GmbH

Free space deletion



5 Free space deletion

This chapter provides information on the "Free space deletion" function of Secure Eraser.

5.1 Overview

Use the "Free space deletion" function to safely delete previously deleted files from a hard drive.

Drive list

The supported drive for secure data deletion are displayed on the drive list. To select a drive, click on the corresponding entry with the left mouse button.

Options

Allows you to select various additional options that can be performed after the actual deletion.

MFT clean up

Cleans the Master File Table for the selected hard drive/partition. Enable this option if Secure Eraser should also delete the file names for files deleted from the Master File Table (*recommended*).

Clearing Change Journal

Clears the USN Change Journal. The USN Change Journal logs all file operations on NTFS drives (if enabled) and thus contains the complete file and directory names.

Overwriting Slackspace

Overwrites the Slack space for all existing files. The Slack space, also known as Cluster Tip Area may contain file fragments of deleted files in a conventional manner.

After deletion

The actions of Secure Eraser after completing the deletion process, can be determined using the EX, SD, RB and S switches. If the switch is displayed in green, the corresponding option is activated. If the switch is blue that means this function does not apply.

EX

© ASCOMP Software GmbH

Exits the software after completing the deletion.

SD

Shuts down the operating system after completing the deletion.

RB

Reboots the operating system after completing the deletion.

SB

Sets the operating system on standby after completing the deletion.

Initiating deletion

Opens a popup menu, which allows the selection of one of the five available deletion methods. To start the deletion, click on the desired deletion method with the left mouse button.

5.2 General Information

Important Information:

1. Secure Eraser overwrites all hard drive areas on which no required data is found, using the selected deletion method.
2. Only free hard drive space of the selected drive will be securely overwritten. Existing files are unaffected.
3. During the deletion process, a Windows notification "Low Disk Space" may appear. This message can be disregarded.
4. During deletion process, work should not be done on the computer. Close all applications that are currently running ideally before starting the deletion.
5. Secure Eraser writes one or several files with the designation $tmp in the root directory of the selected drive. Should Secure Eraser close during the deletion process via the task manager for Windows, these files must be deleted manually. Take particular care not to merely shift the files to the recycle bin, but to delete them using the key combination Shift + Del.

© ASCOMP Software GmbH

Registry cleaning

Part VI

6 Registry cleaning

This chapter provides information on the "Registry cleaning" function for Secure Eraser.

6.1 Overview

Use the "Registry cleaning" function to identify and remove the unneeded, orphaned or invalid entries in the registry database for Windows.

Item selection

The item selection supports targeted cleaning the Windows Registry.

Activate the desired check boxes to scan the corresponding areas of the Windows registry and to identify unneeded, orphaned or invalid entries.

Did you know...

...that the registry check makes no changes to the registry database?

Initiating checks

Starts checking the registry and submits unneeded, orphaned or invalid entries for deletion.

Preview

The item selection displays a preview of all matching entries after beginning a check. All information are classified in the previously defined area.

You can check or uncheck the items of a scan-range by clicking the displayed range title in blue text with the left mouse button.

After deletion

The actions of Secure Eraser can be determined using the switches EX, SD, RB and S after completing the deletion process. If the switch is displayed in green, the corresponding option is activated. If the switch is blue that means this function does not apply.

EX

© ASCOMP Software GmbH

Exits the software after completing the deletion.

SD

Shuts down the operating system after completing the deletion.

RB

Reboots the operating system after completing the deletion.

SB

Sets the operating system on standby after completing the deletion.

Initiating deletion

Deletes the highlighted items in the selection of items from the Windows Registry.

6.2 General Information

Important Information:

1. Registry items are not suitable for secure data deletion and are therefore deleted with normal Windows functions.
2. Please check all suggested items to be erased by Secure Eraser carefully!

© ASCOMP Software GmbH

System cleaning

Part VII

7 System cleaning

This chapter provides information on the "System cleaning" function for Secure Eraser.

7.1 Overview

Use the "System cleaning" function to delete temporarily saved files and profiles from the system partition.

Windows

Areas in the "Windows" category contain data that have been created by the system or other applications.

Temp-directory (User)

Deletes all files and folders contained in the updated registered user temp directory.

Temp-directory (System)

Deletes all files and folders contained in the temp directory of the system.

Recently used document

Clears the list of recently opened/used documents.

Important Information:

Recently used documents are **not** deleted this way! It is cleared only from the Windows managed list of recently opened documents ("recent documents"), which allows quicker access to the relevant documents directly from the Windows Start menu.

Recycle bin

Deletes files from the recycle bin.

Did you know...

...that Secure Eraser automatically inscribes in the shortcut menu of all files, folders and

© ASCOMP Software GmbH

the Windows Recycle Bin, so as to ensure a more comfortable data deletion?

Internet Explorer

Files in the "Internet Explorer" category contain data which have been created by the Microsoft Internet Explorer.

Addresses list

Deletes URL addresses entered in the address bar of Internet Explorer.

Important Information:

The address list is stored in the Windows Registry. These data are not suitable for secure data deletion and are therefore cleared with normal Windows functions.

Cookies

Deletes cookies cached by Internet Explorer.

Cookies contain information about visited websites and allow, for example, "Quick Login" to discussion forums, imputing your information and list boxes with previously stored values and as wells as for faster and automated processing of web pages and web forms.

Temporary internet files

Deletes all files and folders contained in the temporary Internet Files-Folders for Internet Explorer.

Edge

Data can be deleted using the "Edge" category, created by Microsoft Edge.

Browsing history and downloads

Deletes the browsing history of Edge and the list of recently downloaded files.

Cookies

Deletes cookies cached by Edge.

Cookies contain information about visited websites and allow, for example, "Quick Login" to discussion forums, imputing your information and list boxes with previously stored values and

© ASCOMP Software GmbH

as wells as for faster and automated processing of web pages and web forms.

Temporary internet Files

Deletes all temporary files from Mozilla Firefox.

Google Chrome

Data can be deleted using the "Google Chrome" category, created by Google Chrome.

Browsing history, downloads and tabs

Deletes the browsing history of Google Chrome, the list of recently downloaded files and opened tabs.

Cookies

Deletes cookies cached by Google Chrome.

Cookies contain information about visited websites and allow, for example, "Quick Login" to discussion forums, imputing your information and list boxes with previously stored values and as wells as for faster and automated processing of web pages and web forms.

Temporary internet Files

Deletes all temporary files from Mozilla Firefox.

Mozilla Firefox

Data can be deleted using the "Mozilla Firefox" category, created by Mozilla Firefox.

Bookmarks, browsing history and downloads

Deletes bookmarks of Mozilla Firefox, the browsing history and the list of recently downloaded files.

Cookies

Deletes cookies cached by Mozilla Firefox.

Cookies contain information about visited websites and allow, for example, "Quick Login" to discussion forums, imputing your information and list boxes with previously stored values and as wells as for faster and automated processing of web pages and web forms.

© ASCOMP Software GmbH

Forms

Login information stored by Mozilla Firefox for forms, discussion forum, Webmail-Accounts et al. can be deleted, while this item is selected.

Temporary internet Files

Deletes all temporary files from Mozilla Firefox.

After deletion

The actions of Secure Eraser after completing the deletion process can be determined using the EX, SD, RB and S switches. If the switch is displayed in green, the corresponding option is activated. If the switch is blue that means this function does not apply.

EX

Exits the software after completing the deletion.

SD

Shuts down the operating system after completing the deletion.

RB

Reboots the operating system after completing the deletion.

SB

Sets the operating system on standby after completing the deletion.

Initiates deletion

Opens a popup menu, which allows the selection of one of the five available deletion methods. To start the deletion, click on the desired deletion method with the left mouse button.

© ASCOMP Software GmbH

7.2 General Information

Important Information:

1. You will receive additional information by placing the mouse on the respective checkbox and waiting until the Tool tip appears. This denotes the origin of the folder on the hard disk.

2. The folder contents can be displayed by clicking the magnifying glass icon using the left side of the mouse.

3. The terms "files" and "storage space" refer to the contents of the folder and show the subsequently reserved memory in case of a deletion.

© ASCOMP Software GmbH

Report administration

Part VIII

8 Report administration

This chapter provides information on the "Report administration" function for Secure Eraser.

8.1 Overview

The "Report administration" menu displays all deletion reports produced by Secure Eraser. Deletion reports provide detailed information on performed deletions.

Deletion reports

By double-clicking on it, a highlighted deletion report can be opened in the Internet browser and printed on demand.

A shortcut menu can be opened by right-clicking on it; It offers advanced functions, such as sending or deleting the selected deletion reports.

8.2 General Information

Important Information:

1. Deletion reports are stored in the application data folder of registered users.

2. Deletion reports contain sensitive information such as filenames and should be deleted when they are no longer needed! If you want to forego creating deletion reports, please deactivate the corresponding option in the settings.

© ASCOMP Software GmbH

Tips & Tricks

Part IX

9 Tips & Tricks

This chapter provides Tips & Tricks for using Secure Eraser.

9.1 Deletion of USB sticks / SD cards / Flash drives

Please note the following information, which deals with secure data deletion of files and folders that are located on the so-called Solid State Drives.

Solid State Drives

Unlike ordinary hard drives SSD store files and folders so that selective overwriting of unused hard drive sectors is not possible. We recommend that you ask the manufacturer of the SSD being used for the designated deletion software and the deletion method for this model.

Alternatively, you can in most cases safely delete files and folders from SSD using Secure Eraser, by following the instructions below:

1. Delete existing files and folders using the "secure file deletion" function. This way, files and folder names can be deleted successfully from the medium index, so that later no conclusions about the contained data can be drawn. Use the "Low - Random" deletion method in order not to negatively influence the service life of the SDD.

2. After deleting files and folders, the entire free space of the medium should be deleted so that all available file contents are securely overwritten. You can use the "Free space secure deletion" function.

9.2 Using software for data recovery

Safely deleted files and folders carried out by Secure Eraser can **not** be restored with data recovery software. So please pay attention when selecting data so that important files and folders are not selected!

© ASCOMP Software GmbH